



مرکز ملی فضای مجازی
انستیت پژوهش‌های فضای مجازی

به انضمام لوح الکترونیکی اسناد

سایبر و سازمان ملل متحد

تألیف: دکتر نصراله سلطانی
با مقدمه: دکتر سید ابوالحسن فیروزآبادی



سایبر و سازمان ملل متحد

بررسی عملکرد سایبری ارکان، کمیته‌ها، کمیسیون‌ها

و کارگزاری‌های تخصصی سازمان ملل متحد

تالیف

دکتر نصراله سلطانی

همکار ترجمه

منیره باستانی

۱۴۰۰

سرشناسه	: سلطانی، نصرالله، ۱۳۵۴-
عنوان و نام پدیدآور	: سایبر و سازمان ملل متحد: بررسی عملکرد سایبری ارکان، کمیته‌ها، کمیسیون‌ها و کارگزاری‌های سازمان ملل متحد / تالیف نصراله سلطانی؛ همکار ترجمه منیره باستانی؛ با مقدمه سید ابوالحسن فیروزآبادی؛ [برای] مرکز ملی فضای مجازی انتشارات پژوهشگاه فضای مجازی.
مشخصات نشر	: تهران: انتشارات پژوهشگاه فضای مجازی، ۱۴۰۰-
مشخصات ظاهری	: ۵۸۲ ص
شابک	: ۹۷۸-۶۲۲-۹۷۷۰۰-۹-۲
وضعیت فهرست‌نویسی	: فیپا
یادداشت	: کتابنامه: ص، ۵۷۴-۵۸۲.
عنوان دیگر	: بررسی عملکرد سایبری ارکان، کمیته‌ها، کمیسیون‌ها و کارگزاری‌های سازمان ملل متحد
موضوع	: فضای مجازی -- تدابیر ایمنی -- همکاری‌های بین‌المللی Cyberspace -- Security measures -- International cooperation
موضوع	: سازمان ملل متحد
موضوع	: United Nations
موضوع	: فضای مجازی (حقوق بین‌الملل) Cyberspace (International law*)
شناسه افزوده	: باستانی، منیره، ۱۳۵۶-، مترجم.
شناسه افزوده	: فیروزآبادی، سید ابوالحسن، ۱۳۴۰-، مقدمه‌نویس
شناسه افزوده	: پژوهشگاه فضای مجازی
رده‌بندی کنگره	: HM ۸۵۱
رده‌بندی دیوبی	: ۳۰۳/۴۸۳۳
شماره کتابشناسی ملی	: ۸۷۵۰۴۴۳
اطلاعات رکورد کتابشناسی	: فیپا

مشخصات :

عنوان: سایبر و سازمان ملل متحد

مؤلفان: دکتر نصراله سلطانی، با مقدمه دکتر سید ابوالحسن فیروزآبادی

همکار ترجمه: منیره باستانی

ناشر: انتشارات پژوهشگاه فضای مجازی

صفحه آرا و طراح جلد: میترا مرادیان

سال و نوبت چاپ: ۱۴۰۰- اول

شابک: ۹۷۸-۶۲۲-۹۷۷۰۰-۹-۲

قیمت: ۱۲۰۰۰۰۰ ریال



بند سوم سیاست های ابلاغی مقام معظم رهبری در سال ۹۴
خطاب به شورای عالی فضای مجازی:

«برخورداری از ابتکار عمل و قدرت تعامل با دیگر کشورها در جهت شکل دهی به قواعد و
قوانین مرتبط با فضای مجازی در عرصه جهانی با رویکرد اخلاق مدار و عادلانه»



با تعظیم و احترام، تقدیم به:
سردار شهید حاج قاسم سلیمانی و دانشمند شهید دکتر محسن فخری زاده



سخن ناشر

ماهیت جهان گستر فضای سایبر موجب شده است که تهدیدات، چالش‌ها و مخاطرات این عرصه نوظهور فناورانه نیز ماهیتی بین‌المللی داشته باشد و با درنوردیدن مرزهای جغرافیایی سنتی، شمار کثیری از دولت‌ها و سایر بازیگران فروملی و فراملی را در معرض مخاطره، حمله و آسیب قرار دهد. طبیعی است که در چنین فضایی هیچ بازیگری نتواند به‌تنهایی به نبرد پیروزمندانه با مخاطرات و آسیب‌های این فضا بپردازد، بنابراین مقابله با آسیب‌های این عرصه نیازمند هم‌افزایی بین دولتی در سطح کلان است. ورود دیر هنگام سازمان ملل به‌عنوان یک سازمان جهانی به عرصه مقابله با مخاطرات این فضا و توفیق اندک این سازمان در مقابله و مواجهه با ناهنجاری‌های این حوزه، محل تمرکز این کتاب است. رقابت‌های آشکار و نهان صاحبان قدرت سایبری مانع از آن شده است که این سازمان در مأموریت‌های سایبری خود به‌دستاورهای توجیه‌پذیری دست یابد و دقیقاً به همین خاطر است که هر روز شاهد افزایش مخاطرات این فضا هستیم. عملکرد سایبری ارکان و اجزای مختلف سازمان ملل در این کتاب مورد واکاوی قرار گرفته است.

کتاب حاضر به دو بخش کلی ترجمه و تحلیل تقسیم شده است. هر بخش نیز شامل فصول منسجم و به‌هم‌پیوسته‌ای می‌باشد. نتیجه‌گیری کتاب نیز شامل تحلیل نهایی، آینده‌نگری و توصیه‌های کارشناسی می‌باشد. این کتاب دارای ویژگی‌های انحصاری است؛ گردآوری مطالب با دقت صورت گرفته و در ترجمه اسناد، نهایت حساسیت اعمال شده است.

شایان ذکر است که این ترجمه‌ها غیررسمی است و نمی‌تواند از سوی مراجع رسمی در داخل یا خارج کشور مورد استناد رسمی قرار گیرد. بخش تحلیلی نیز منعکس‌کننده نظرها کارشناسی نویسنده محترم می‌باشد. اشراف نویسنده به موضوع باعث شده که همه ابعاد و اطراف یک سند، مورد موشکافی دقیق قرار گیرد. بانک اطلاعات کتاب که به جهت کثرت و حجم اسناد به صورت فایل الکترونیکی، ضمیمه کتاب می‌باشد در نوع خود بی‌مانند است و تفکیک موضوعی و سازمانی اسناد، بهره‌برداری از آن را برای هر محققى در هر حوزه خاصی از موضوع آسان ساخته است. امید است این کار علمی و پژوهشی بتواند برای جامعه مخاطب خود اعم از محافل دانشگاهی، تصمیم‌گیران و تصمیم‌سازان و عموم علاقه‌مندان و بهره‌برداران مفید واقع شود.

انتشارات پژوهشگاه فضای مجازی

فهرست مطالب

پیشگفتار ۱۷

مقدمه ۲۱

بخش اول: ترجمه

فصل یک: مجمع عمومی

مبحث یک: کمیته اول مجمع عمومی

گفتار یک: قطعنامه‌ها

بند یک: قطعنامه تحولات حوزه اطلاعات و ارتباطات در چهارچوب امنیت بین الملل سال ۱۹۹۸ ۲۷

بند دو: تغییرات قطعنامه تحولات حوزه اطلاعات و ارتباطات در چهارچوب امنیت بین الملل سال

۱۹۹ تا ۲۰۱۵ ۳۰

بند سه: قطعنامه تحولات حوزه اطلاعات و ارتباطات در چهارچوب امنیت بین الملل سال ۲۰۱۶ ۳۳

بند چهار: قطعنامه تحولات حوزه اطلاعات و ارتباطات در چهارچوب امنیت بین الملل سال ۲۰۱۸ ۳۷

بند پنج: قطعنامه پیشرفت رفتار مسئولانه دولت درباره فضای سایبر در چهارچوب امنیت بین الملل

سال ۲۰۱۸ ۴۶

گفتار دو: گزارش‌های گروه کارشناسان دولتی (G.G.E) در حوزه امنیت سایبری

بند یک: گزارش اولین گروه کارشناسان دولتی سال ۲۰۰۵ ۵۱

بند دو: گزارش دومین گروه کارشناسان دولتی سال ۲۰۱۰ ۵۵

بند سه: گزارش سومین گروه کارشناسان دولتی سال ۲۰۱۳ ۶۶

بند چهار: گزارش چهارمین گروه کارشناسان دولتی سال ۲۰۱۵ ۸۳

بند پنج: گزارش پنجمین گروه کارشناسان دولتی در سال ۲۰۱۷ ۱۰۷

بند شش: تشکیل اولین گروه کاری باز (O.E.W.G) در سال ۲۰۱۹ ۱۱۱

گفتار سه: کردار نامه‌ها و کنوانسیون‌ها

- بند یک: کردار نامه بین‌المللی امنیت اطلاعات سال ۲۰۱۱ ۱۱۴
- بند دو: کردار نامه بین‌المللی امنیت اطلاعات سال ۲۰۱۵ ۱۱۹
- بند سه: پیش‌نویس کنوانسیون بین‌المللی امنیت اطلاعات سال ۲۰۱۱ ۱۲۶

مبحث دو: کمیته دوم مجمع عمومی

- بند یک: قطعنامه ایجاد فرهنگ جهانی امنیت سایبری سال ۲۰۰۲ ۱۴۶
- بند دو: قطعنامه ایجاد فرهنگ جهانی امنیت سایبری سال ۲۰۰۳ ۱۵۱
- بند سه: قطعنامه ایجاد فرهنگ جهانی امنیت سایبری ۲۰۰۹ ۱۵۶
- بند چهار: قطعنامه فناوری اطلاعات و ارتباطات برای توسعه سال ۲۰۰۲ ۱۶۲
- بند پنج: قطعنامه فناوری اطلاعات و ارتباطات برای توسعه سال ۲۰۰۷ ۱۶۶
- بند شش: قطعنامه فناوری اطلاعات و ارتباطات برای توسعه سال ۲۰۱۵ ۱۶۸
- بند هفت: قطعنامه فناوری اطلاعات و ارتباطات برای توسعه سال ۲۰۱۸ ۱۷۴
- بند هشت: قطعنامه اجلاس سران در مورد جامعه اطلاعاتی سال ۲۰۰۴ ۱۹۱
- بند نه: قطعنامه اجلاس سران در مورد جامعه اطلاعاتی سال ۲۰۰۶ ۱۹۴

مبحث سه: کمیته سوم مجمع عمومی

- بند یک: قطعنامه مبارزه با سوء استفاده مجرمانه از فناوری‌های اطلاعاتی سال ۲۰۰۱ ۱۹۸
- بند دو: قطعنامه حق حریم خصوصی در عصر دیجیتال سال ۲۰۱۳ ۲۰۱
- بند سه: قطعنامه حق حریم خصوصی در عصر دیجیتال سال ۲۰۱۴ ۲۰۵
- بند چهار: قطعنامه حق حریم خصوصی در عصر دیجیتال سال ۲۰۱۶ ۲۱۱
- بند پنج: قطعنامه برنامه تقویت پیشگیری از جرم و عدالت کیفری سازمان ملل سال ۲۰۱۷ ۲۱۹
- بند شش: قطعنامه مقابله با استفاده از فناوری اطلاعات و ارتباطات برای اهداف مجرمانه سال ۲۰۱۸ ۲۲۲
- بند هفت: قطعنامه مقابله با استفاده از فناوری اطلاعات و ارتباطات برای اهداف مجرمانه سال ۲۰۱۹ ۲۲۵

مبحث چهار: شورای حقوق بشر

- بند یک: قطعنامه ارتقاء، حفاظت و برخورداری از حقوق بشر در اینترنت سال ۲۰۱۲ ۲۳۴
- بند دو: قطعنامه ارتقاء، حفاظت و برخورداری از حقوق بشر در اینترنت سال ۲۰۱۴ ۲۳۶
- بند سه: قطعنامه ارتقاء، حفاظت و برخورداری از حقوق بشر در اینترنت سال ۲۰۱۶ ۲۴۰
- بند چهار: قطعنامه حق حریم خصوصی در عصر دیجیتال سال ۲۰۱۵ ۲۴۶
- بند پنج: قطعنامه نقش آزادی عقیده و بیان در ارتقاء توانمندی‌های زنان سال ۲۰۱۳ ۲۵۲

- بند شش: قطعنامه حقوق کودک: فناوری اطلاعات و ارتباطات و استثمار جنسی کودکان سال ۲۰۱۶ ۲۵۷
- مبحث پنج: کنفرانس تجارت و توسعه ملل متحد (آنکتاد)**
- بند یک: گزارش گروه کارشناسی بین‌دولتی درباره تجارت الکترونیکی و اقتصاد دیجیتال سال ۲۰۱۷ ۲۶۷
- بند دو: گزارش گروه کارشناسی بین‌دولتی درباره تجارت الکترونیکی و اقتصاد دیجیتال سال ۲۰۱۸ ۲۷۳
- بند سه: گزارش گروه کارشناسی بین‌دولتی درباره تجارت الکترونیکی و اقتصاد دیجیتال سال ۲۰۱۹ ۲۷۷
- فصل دو: شورای اقتصادی و اجتماعی (اکوسوک)**
- مبحث یک: مصوبات اکوسوک**
- بند یک: قطعنامه پیشگیری، حفاظت و همکاری بین‌المللی علیه استفاده از فناوری‌های نوین اطلاعاتی به‌منظور سوء استفاده یا استثمار کودکان سال ۲۰۱۱ ۲۸۱
- بند دو: خلاصه‌ای از قطعنامه‌ها تحت عنوان همکاری بین‌المللی در پیشگیری، تحقیق، تعقیب و مجازات کلاهبرداری اقتصادی و جرائم مرتبط با هویت ۲۸۹
- بند سه: قطعنامه ارتقای مساعدت فنی و ظرفیت‌سازی برای تقویت اقدامات ملی و همکاری بین‌المللی جهت مبارزه با جرم سایبری از جمله به اشتراک‌گذاشتن اطلاعات سال ۲۰۱۹ ۲۹۱
- مبحث دو: کمیسیون علم و فناوری برای توسعه**
- بند یک: قطعنامه علم، فناوری و نوآوری برای توسعه سال ۲۰۱۸ ۲۹۷
- بند دو: قطعنامه ارزیابی پیشرفت‌های صورت گرفته در اجرا و تعقیب نتایج اجلاس سران درباره جامعه اطلاعاتی سال ۲۰۱۸ ۳۰۳
- مبحث سه: کمیسیون پیشگیری از جرم و عدالت کیفری**
- بند یک: قطعنامه ارتقای اقدامات مرتبط با مبارزه با جرم سایبری، از جمله مساعدت فنی و ظرفیت‌سازی سال ۲۰۱۱ ۳۲۱
- بند دو: قطعنامه ارتقای مساعدت فنی و ظرفیت‌سازی برای تقویت اقدامات ملی و همکاری بین‌المللی علیه جرم سایبری سال ۲۰۱۳ ۳۲۴
- بند سه: قطعنامه تقویت همکاری بین‌المللی برای مبارزه با جرم سایبری سال ۲۰۱۳ ۳۲۷
- بند چهار: قطعنامه تقویت همکاری بین‌المللی در مبارزه با جرم سایبری سال ۲۰۱۷ ۳۳۴
- بند پنج: قطعنامه مقابله با سوء استفاده و استثمار جنسی برخط از کودکان سال ۲۰۱۹ ۳۴۳
- بند شش: ارتقای مساعدت فنی و ظرفیت‌سازی برای تقویت اقدامات ملی و همکاری بین‌المللی برای مبارزه با جرم سایبری از جمله اشتراک‌گذاری اطلاعات سال ۲۰۱۹ ۳۴۴

- بند هفت: گزارش گروه کارشناسان بین دولتی باز راجع به موضوع جرم سایبری ۲۰۱۸ ۳۴۹
- بند هشت: گزارش گروه کارشناسان بین الدولی باز راجع به موضوع جرم سایبری ۲۰۱۹ ۳۵۱
- مبحث چهار: کمیسیون مبارزه با مواد مخدر:**
- بند یک: قطعنامه اینترنت سال ۲۰۰۰ ۳۵۵
- بند دو: قطعنامه همکاری بین المللی در پیگیری توزیع غیرقانونی مواد مجاز تحت کنترل در سطح بین الملل از طریق اینترنت سال ۲۰۰۷ ۳۵۷
- بند سه: قطعنامه تقویت همکاری بین المللی به منظور پیشگیری از استفاده از اینترنت در ارتکاب مرتبط با مواد مخدر سال ۲۰۰۵ ۳۶۰
- مبحث پنج: اتحادیه بین المللی مخابرات**
- بند یک: بازنگری ۱۰ ساله نتایج اجلاس سران درباره جامعه اطلاعاتی (WSIS+10) سال ۲۰۱۵ ۳۶۱
- مبحث شش: سازمان آموزشی علمی فرهنگی سازمان ملل متحد (یونسکو)**
- بند یک: سند پیش نویس ضوابط اخلاقی برای جامعه اطلاعاتی سال ۲۰۱۱ ۳۷۹

بخش دوم: بررسی و ارزیابی

فصل اول: مجمع عمومی

مبحث اول: اقدامات مبتکرانه روسیه در کمیته های سه گانه مجمع عمومی

- گفتار یک: ارائه اولین قطعنامه امنیت بین الملل سایبری در سال ۱۹۹۸ ۳۸۵
- گفتار دو: پیشنهاد تشکیل اولین گروه کارشناسان دولتی (G.G.E) در سال ۲۰۰۱ ۳۹۴
- گفتار سه: پیشنهاد تشکیل اولین گروه کاری باز ملل متحد در سال ۲۰۱۹ ۴۰۳
- گفتار چهار: ارائه اولین کردارنامه امنیت بین الملل سایبری در سال ۲۰۱۱ ۴۰۶
- گفتار پنج: ارائه پیش نویس اولین کنوانسیون امنیت بین الملل سایبری در سال ۲۰۱۱ ۴۰۷
- گفتار شش: ارائه اولین پیش نویس کنوانسیون مقابله با جرایم سایبری در سال ۲۰۱۷ ۴۰۸
- گفتار هفت: پیشنهاد تشکیل اولین کمیته باز برای تدوین کنوانسیون مقابله با جرایم سایبری ۲۰۱۹ ۴۱۴

مبحث دوم: عملکرد حقوق بشری غرب در کمیته سوم و شورای حقوق بشر مجمع عمومی

- گفتار یک: قطعنامه حق حریم خصوصی در عصر دیجیتال ۴۱۹
- گفتار دو: قطعنامه ارتقاء، حفاظت و برخورداری از حقوق بشر در اینترنت ۴۲۱

مبحث سوم: عملکرد گروه ۷۷ در کمیته دوم مجمع عمومی

- گفتار اول: ارائه پیش نویس قطعنامه فناوری های اطلاعات و ارتباطات برای توسعه ۴۲۵
- گفتار دو: حمایت از قطعنامه اجلاس سران در مورد جامعه اطلاعاتی ۴۳۰

مبحث چهارم: عملکرد کنفرانس توسعه و تجارت ملل متحد (آنکتاد)

- گفتار یک: آنکتاد و فضای سایبر ۴۳۶
- گفتار دو: گروه کارشناسان بین دولتی درباره تجارت الکترونیک و اقتصاد دیجیتال - سال ۲۰۱۷ ۴۳۸
- گفتار سه: خلاصه ای از وضعیت قوانین تصویب شده در ۱۹۳ کشور عضو آنکتاد درباره تجارت الکترونیک ۴۴۱
- گفتار چهار: کارگروه اقدام تجارت الکترونیکی و اقتصاد دیجیتالی ۴۴۳

مبحث پنجم: عملکرد موسسه تحقیقات خلع سلاح ملل متحد (یونیدیر)

- گفتار یک: یونیدیر و فضای سایبر ۴۴۸
- گفتار دو: برگزاری کارگاه هایی با موضوعات امنیت بین المللی سایبری ۴۴۹
- گفتار سه: برگزاری کنفرانس های سالانه ثبات سایبر ۴۶۶
- گفتار چهار: مجموعه نشست هایی در خصوص حقوق بین الملل و رفتار دولت در فضای سایبری ۴۶۷

مبحث ششم: عملکرد کمیسیون های تخصصی مجمع عمومی

- گفتار یک: کمیسیون حقوق بین الملل ۴۷۱
- گفتار دو: کمیسیون خلع سلاح ملل متحد ۴۷۵
- نتیجه گیری فصل اول ۴۷۵

فصل دوم: سایر ارکان

مبحث اول : عملکرد شورای اقتصادی و اجتماعی سازمان ملل(اکوسوک)

- گفتار یک: اکوسوک و فضای سایبر ۴۸۱
- گفتار دو: کمیسیون پیشگیری از جرم و عدالت کیفری ۴۸۲
- گفتار سه: کمیسیون مبارزه با مواد مخدر ۴۸۵
- گفتار چهار: اتحادیه بین المللی مخابرات ۴۸۶
- بند یک: اسناد اجلاس ژنو ۲۰۰۳ ۴۸۶
- بند دو: اسناد اجلاس تونس ۲۰۰۵ ۴۸۷
- بند سه: بازنگری ۱۰ ساله اجلاس سران درباره جامعه اطلاعاتی ۲۰۱۵ (WSIS+10) ۴۹۰
- بند چهار: مجمع حکمرانی اینترنت ۴۹۳
- گفتار پنج: سازمان آموزشی علمی فرهنگی سازمان ملل متحد (یونسکو) ۴۹۷
- بند یک: یونسکو و فضای سایبر ۴۹۷
- بند دو: توصیه در خصوص ارتقاء و استفاده چند زبانی و دسترسی به فضای مجازی ۴۹۸
- بند سه: دیدگاه اندیشه ای و تحلیل یونسکو درباره اینترنت، یونسکو و استفاده از اینترنت در قلمرو
صلاحیت خود ۵۰۰
- بند چهار: سند پیش نویس ضوابط اخلاقی برای جامعه اطلاعاتی سال ۲۰۱۱ ۵۰۲
- بند پنج: اصول و شاخصه های پوشش اینترنت ۵۰۴
- گفتار شش: سازمان جهانی مالکیت معنوی ۵۱۶
- گفتار هفت: سازمان بهداشت جهانی ۵۱۹
- گفتار هشت: سازمان جهانی گمرک ۵۲۳
- گفتار نه: گروه بانک جهانی ۵۲۴
- گفتار ده: سازمان تجارت جهانی ۵۲۷
- گفتار یازده: سازمان جهانی هواشناسی ۵۲۹

مبحث دوم: عملکرد شورای امنیت

- ۵۳۰ گفتار یک: شورای امنیت و فضای سایبر
- ۵۳۳ گفتار دو: عملکرد کمیته ضد تروریسم در مباحث فناوری اطلاعات و ارتباطات
- ۵۳۶ گفتار سه: فرمول آریا

مبحث سوم: عملکرد دبیرخانه

- ۵۳۷ گفتار یک: گزارش کلی از عملکرد دبیر کل سازمان ملل متحد در مورد فضای سایبری
- ۵۳۷ بند یک: گزارش سالانه دبیر کل
- ۵۳۹ بند دو: یادداشت دبیر کل
- ۵۳۹ بند سه: دستور کار دبیر کل برای خلع سلاح
- ۵۴۳ بند چهار: راهبرد دبیر کل درباره فناوری های جدید
- ۵۴۶ گفتار دو: دفتر مقابله با مواد مخدر و جرم ملل متحد
- ۵۵۰ گفتار سه: اداره امور سیاسی و صلح سازی
- ۵۵۱ گفتار چهار: دفتر هماهنگی امور بشر دوستانه
- ۵۵۲ گفتار پنج: کنفرانس خلع سلاح
- ۵۵۲ گفتار شش: اداره امور خلع سلاح ملل متحد
- ۵۵۷ نتیجه گیری فصل دوم
- ۵۶۰ نتیجه گیری نهایی
- ۵۶۰ الف. جمع بندی تحلیلی مطالب
- ۵۶۶ ب. آینده نگری و پیش بینی روندهای آتی
- ۵۶۷ ج. آینده روندهای حقوقی در محیط بین الملل
- ۵۶۸ د. توصیه های کارشناسی و اقدامات پیشنهادی برای:
- ۵۶۸ ۱. محیط داخلی
- ۵۷۰ ۲. محیط بین المللی
- ۵۷۳ منابع و اسناد

فهرست جدول‌ها

- جدول ۱: تغییرات قطعنامه‌های تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌الملل (امنیت سایبری) پیش‌نویس روسیه، مصوب سال‌های ۱۹۹۹ تا ۲۰۱۵ ۳۰
- جدول ۲: تغییرات قطعنامه‌ها ۳۱
- جدول ۳: مشخصات قطعنامه‌های «فناوری‌های اطلاعاتی و ارتباطی برای توسعه» ۲۰۰۲ تا ۲۰۱۸ ۱۹۰
- جدول ۴: مشخصات قطعنامه‌های اجلاس سران در مورد جامعه اطلاعاتی سال ۲۰۰۱ تا ۲۰۰۶ ۱۹۷
- جدول ۵: «همکاری بین‌المللی در پیشگیری، تحقیق، تعقیب و مجازات کلاهبرداری اقتصادی و جرائم مرتبط با هویت» ۲۸۹
- جدول ۶: مشخصات سایر قطعنامه‌های علم، فناوری و نوآوری برای توسعه ۲۰۰۹ تا ۲۰۱۸ ۳۰۲
- جدول ۷: مشخصات قطعنامه‌های ارزیابی پیشرفت‌های صورت گرفته در اجرا و تعقیب نتایج اجلاس سران درباره جامعه اطلاعاتی ۲۰۰۶ تا ۲۰۱۸ ۳۲۰
- جدول ۸: خلاصه‌ای از وضعیت و آمار آرا و مواضع کشورهای مختلف نسبت به قطعنامه روسیه و آمریکا در سال ۲۰۱۸ ۳۹۳
- جدول ۹: خلاصه عملکرد تشکیل ۵ گروه کارشناسان دولتی (GGE) ۳۹۸
- جدول ۱۰: شرکت کشورها در گروه‌های کارشناسان دولتی (GGE) ؟
- جدول ۱۱: مشخصات چهار گزارش ارائه شده در اجلاس کنفرانس عمومی یونسکو ۵۰۰
- جدول ۱۲: مشخصات گزارش‌های سالانه دبیرکل درباره نظر کشورها در زمینه تحولات اطلاعات و ارتباطات ۵۳۸
- جدول ۱۳: آینده روندهای حقوقی در محیط بین‌الملل ۵۶۸

فهرست اشکال

- شکل ۱: توزیع آرا و مواضع کشورها درباره قطعنامه امنیت سایبری روسیه در سال ۲۰۱۸ ۳۹۰
- شکل ۲: توزیع آرا و مواضع کشورها نسبت به قطعنامه امنیت سایبری آمریکا در سال ۲۰۱۸ بر اساس مناطق جغرافیایی ۳۹۲
- شکل ۳: روند شکل‌گیری گروه کارشناسان دولتی (GGE) ۳۹۹
- شکل ۴: فرایند انتخاب گروه کارشناسان و تشکیل دومین اجلاس (GGE) ۴۰۰
- شکل ۵: فرایند شکل‌گیری اولین گروه کاری باز (O.E.W.G) ۴۰۵
- شکل ۶: توزیع آرا و مواضع کشورها نسبت به قطعنامه روسیه در سال ۲۰۱۹ بر اساس مناطق جغرافیایی ۴۱۶

پیشگفتار

سال ۱۳۹۰ (۲۰۱۱ میلادی) بود که روسیه پیش‌نویس یک کنوانسیون تحت عنوان کنوانسیون امنیت بین‌المللی اطلاعات را به جامعه جهانی ارائه کرد. این پیش‌نویس از آن جهت که بسترهای آن آماده نشده بود و به تعبیری جهان آمادگی پذیرش آن را نداشت، عملاً توفیقی به‌دست نیاورد، مخصوصاً که غرب هم از آن حمایت نکرد.

ذکر دلایل عدم حمایت غرب و سایر وقایع مربوط به موضوع در این مجال نمی‌گنجد. اما ضمن مطالعه متن پیش‌نویس، به بررسی ابعاد و اطراف آن پرداختم. موضوع مهم در این میان، سابقه پیش‌نویس بود. زیرا بعید به نظر می‌رسید که روسیه ابتدائاً و بدون هیچ عقبه‌ای به ارائه این کنوانسیون پرداخته باشد. در بررسی‌های خود درباره روند و سابقه موضوع از سال ۲۰۱۱ به سال ۱۹۹۸ رسیدم که روسیه اولین قطعنامه خود موسوم به قطعنامه امنیت بین‌المللی اطلاعات را به مجمع عمومی سازمان ملل ارائه کرده و با اجماع به تصویب رسانده بود. در ادامه متوجه شدم که آمریکا نیز برای اینکه از قافله قطعنامه و رقابت با روسیه عقب نماند در سال ۲۰۰۰ یعنی دو سال بعد از قطعنامه روسیه، پیش‌نویس یک قطعنامه در مورد جرایم سایبری را به کمیته سوم مجمع عمومی ارائه کرده و به همین نیز اکتفا ننموده و در سال ۲۰۰۲ نیز پیش‌نویس قطعنامه دیگری را به کمیته دوم مجمع در مورد فرهنگ جهانی امنیت سایبری ارائه نموده بود. قدر مسلم اینکه ارائه این دو پیش‌نویس از طرف آمریکا جهت مقابله و مهار اقدامات حقوقی

و دیپلماتیک روسیه بود و هیچ یک از دو ابرقدرت در صدد مبارزه و مقابله با معضلات و مشکلات فضای سایبر نبودند که اگر بودند امنیت کنونی فضای سایبر باید بهتر از این می‌بود. این روند که از سال ۱۹۹۸ شروع شده بود تا سال ۲۰۰۵ به همین منوال ادامه داشت. در بررسی‌های خود متوجه شدم که آمریکا در سال ۲۰۰۵ بر خلاف رویه سابق خود به قطعنامه روسیه رأی منفی داده است. هر چند مقامات مسئول در دولت ایالات متحده برای توجیه اقدام خود، ادعاهای زیادی مطرح کرده بودند، اما هیچ‌کدام قانع‌کننده نبود. با بررسی‌های بیشتر معلوم شد که در سال ۲۰۰۵ دولت ایالات متحده در گوشه دیگری از سازمان ملل به نام اتحادیه بین‌المللی مخابرات از جامعه جهانی ضربه کاری دریافت کرده و با دهن کجی و کارشکنی در برابر قطعنامه روسیه سعی کرده‌است این شکست را جبران کند.

توضیح اینکه اتحادیه بین‌المللی مخابرات در سال ۲۰۰۵ در اجلاس موسوم به اجلاس سران در باره جامعه اطلاعاتی در ژنو و تونس، اسناد انقلابی علیه انحصار حکمرانی آمریکا بر فضای سایبر صادر کرده بود که به هیچ وجه خوشایند این کشور نبود. بنابراین اتحادیه بین‌المللی مخابرات را نیز به دامنه تحقیقات و بررسی‌های خود افزودم. ادامه این تحقیقات، بخش‌های دیگری از سازمان ملل را نیز درگیر کرد. در نهایت تصمیم گرفتم که فعالیت‌های سایبری همه ارکان و اجزای سازمان ملل را به صورت منسجم مورد بررسی قرار داده و نتایج حاصل شده و مستخرجه را منتشر نمایم.

نتیجه حدود سه سال مطالعه در این زمینه انتشار کتاب «به سوی کنوانسیون سایبری» بود. اما این کتاب تحلیل محور بوده و باوجود اینکه همه مطالب مستند بود اما احساس نیاز می‌شد که خود اسناد نیز به صورت کامل در اختیار علاقه‌مندان و تصمیم‌گیران کشور قرار گیرد تا با آگاهی بیشتری درباره این تحولات بتوانند در روندهای آتی سایبری در سازمان ملل نقش آفرینی مؤثرتری داشته باشند.

می‌توان گفت که کتاب «به سوی کنوانسیون سایبری» تحلیلی، تاریخی و روند محور است. اما کتاب حاضر، متن محور است و به نویسنده متن نیز توجه دارد. بنابراین اولاً اسناد، بسته به اینکه از طرف کدام بخش سازمان ملل صادر شده، دسته‌بندی شده و ضمن ترجمه کامل سند،

تحلیل مربوط نیز ارائه شده است. در انجام این کار به جهت محدودیت‌های موجود، ملاحظاتی مورد نظر بوده است. مثلاً وقتی یک قطعنامه در طول ۲۰ سال به صورت مرتب (هر سال یک بار) تصویب شده است، آخرین و کامل‌ترین قطعنامه ترجمه شده و سایر قطعنامه‌ها نیز تفاوت‌چندانی با این قطعنامه ندارند. ضمن اینکه عناوین برخی اسناد مهم نیز در بخش ضمیمه آورده شده است، اما بانک کامل اسناد که حدود پنج هزار صفحه می‌باشد، به صورت فایل الکترونیکی و به شکل کاملاً منظم و دسته‌بندی شده به کتاب اصلی پیوست شده که این مجموعه ارزشمند به صورت طبقه‌بندی شده موضوعی در اختیار علاقه‌مندان خواهد بود. در ترجمه اسناد، نهایت دقت به کار رفته و چندین مرتبه کنترل صورت گرفته است و امید می‌رود این کار نقشی هرچند اندک در گفتمان‌سازی حوزه مغفول حقوق و سیاست بین‌الملل سایبری و دیپلماسی سایبری، معاهدات و کنوانسیون‌های مربوط و سایر حوزه‌های مرتبط داشته باشد.

مقدمه

ماهیت و ویژگی‌های خاص فضای سایبر، از جمله جهان‌گستری آن، موجب شده است که تقسیم‌ناپذیری امنیت در این فضا به یک واقعیت انکارناپذیر تبدیل شود. اقدامات محل امنیت در این فضا حتی از یک منبع محدود می‌تواند در اندک زمانی امنیت سایبری قاطبه کشورهای جهان را تحت تأثیر قرار دهد البته برای اقدام امنیت‌زدا هیچ نیازی به اتحاد و ائتلاف در سطح بین‌المللی و حتی منطقه‌ای نیست.

یک سامانه با امکانات ابتدایی متصل به شبکه جهانی می‌تواند با استفاده از یک بدافزار یا باج‌افزار، تعداد کثیری از کشورهای جهان را مورد حمله مخرب خود قرار دهد. اما برعکس، امنیت این فضا نمی‌تواند به صورت نقطه‌ای و جزیره‌ای و پراکنده تأمین شود. حصارکشی سایبری از جانب هر دولتی، قطعاً توفیقات حداقلی در پی خواهد داشت. زیرا با ماهیت این فضا در تعارض است. هم‌افزایی امنیت ساز دولت‌ها در این فضا بیش از هر فضای دیگری یک ضرورت اجتناب‌ناپذیر است. در ادامه، قاعده‌مندسازی فعالیت در این فضا و مقابله با اقدامات غیرقانونی، جرایم و تخلفات، همه‌وهمه با همکاری نخستین و مهم‌ترین تابعان فعال حقوق بین‌الملل یعنی دولت‌ها، امکان تحقق دارد. اما آنچه که تا کنون شاهد آن بوده‌ایم این است که عملکرد غیرسازنده و رویکرد انحصارطلبانه برخی دولت‌های خاص در این فضا و تضاد و تلاقی منافع صاحبان قدرت سایبری، مانع از آن شده است که مساعی و تلاش‌های جمعی دولت‌ها برای تأمین امنیت و قاعده‌مندی این فضا به نتایج

ملموس و قابل قبولی منجر شود. به نحوی که امروز هیچ نسبتی بین روند روزافزون ناامنی در این فضا و فعالیت‌های امنیت‌ساز دولت‌ها وجود ندارد.

ملل متحد یک سازمان جهانی با مأموریت عام‌الشمول است که از ابتدای هزاره جدید، تأمین امنیت بین‌المللی این فضا و قاعده‌مندی آن را وجهه همت خود قرار داده است. اما مأموریت سایبری این ابرسازمان، بنا به دلایلی که قبلاً ذکر شده دستاوردهای بسیار اندکی به همراه داشته است. رقابت‌های پیدا و پنهان قدرت‌های برتر سایبری، فقدان نقش‌آفرینی واقعی دولت-ملتها در این فضا و بدعت شرکت محوری به جای دولت محوری برای امنیت‌سازی در این فضا از جمله دلایل ضعف کارکردی این سازمان در نیل به اهداف سایبری خود بوده است. اجتماع دولت‌ها حول سازمان ملل نه تنها موفقیت‌آمیز نبوده بلکه اعمال حاکمیت ملی دولت‌ها بر فضای سایبر قلمرو خود نیز دچار چالش‌های جدی شده است. کارآمدی اندک و ضعف کارکردی این نهاد بین دولتی در حوزه سایبری موجب اتخاذ رویکردهای منطقه‌ای و ملی شده که در کنار هزینه زیاد، نتایج پایینی به همراه داشته است. بنابراین اگر مسیر درستی برای آینده امنیت و قاعده‌مندی فضای سایبر بتوان پیش‌بینی و ترسیم کرد قطعاً هم‌افزایی بین‌المللی دولت‌های مستقل و ایفای نقش مؤثر توسط آن‌ها و احترام به حاکمیت برابر این دولت‌ها در فضای سایبر، احتراز از اتخاذ رویکردهای چند بی‌نفعی (به اصطلاح چند ذی‌نفعی) و اجتناب از اقدامات جهت‌دار و ناعادلانه از امهات الزامات در تمام ترتیبات و چهارچوب‌های بین‌المللی است که سازمان ملل می‌تواند یکی از مهم‌ترین آن‌ها باشد.

کتاب حاضر حاصل تلاش چند ساله و شبانه‌روزی نگارنده برای تشریح و توصیف فعالیت‌های سایبری تمام اجزاء و ارکان سازمان ملل متحد است و انصافاً از جامعیت بی‌مانندی برخوردار است. تا آنجا که بررسی‌های ما نشان می‌دهد حتی در سایر مراکز پژوهشی معتبر جهان نیز فعالیت‌های سایبری این سازمان با این دقت مورد موشکافی کامل قرار نگرفته است. بخش تحلیلی کتاب سعی دارد ضمن بررسی و ارزیابی روندهای مختلف سایبری در بخش‌های متنوع سازمان ملل، پیش‌بینی مبتنی بر مبانی علمی از آینده این روندها ترسیم کرده و توصیه‌های کارشناسی و تصمیم‌ساز نیز برای تصمیم‌گیران و جامعه دانشگاهی و نخبگان ارائه نماید.

تحوالات سایبری در سازمان ملل، متوقف نشده و در حال حاضر به مراحل حساسی رسیده است. بنابراین شایسته است ضمن پایش و ارزیابی مستمر این تحولات، جامعه علمی و کارشناسی کشور و محافل دانشگاهی بتوانند توصیه‌ها، راهکارها و راهبردهای کلان مواجهه با روندهای بین‌المللی را پیشنهاد دهند و موجبات ارتقای نقش آفرینی کشور در شکل‌دهی به این روندها و جریان‌های بین‌المللی را فراهم نمایند.

دکتر سید ابوالحسن فیروز آبادی



بخش اول: ترجمه

فصل یک: مجمع عمومی مبحث یک: کمیته اول مجمع عمومی

گفتار یک: قطعنامه‌ها

بند یک: قطعنامه تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌الملل سال ۱۹۹۸

ترجمه سند



تاریخ انتشار: ۴ ژوئن ۱۹۹۹

شماره قطعنامه: A/RES/53/70

زبان: انگلیسی

توزیع: عمومی

اجلاس پنجاه و سوم

دستور کار ۶۳

قطعنامه مصوب مجمع عمومی

بر اساس گزارش ارائه شده از سوی کمیته اول؛ شماره گزارش (A/53/576)

۵۳/۷۰ تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌الملل^۱

مجمع عمومی؛

با یادآوری قطعنامه‌های خود در زمینه نقش علم و فناوری در چارچوب امنیت بین‌الملل که در آن علاوه بر اینکه این امر به رسمیت شناخته شده است، توسعه‌های علمی و فناورانه می‌توانند

1. Developments in the field of information and telecommunications in the context of international security

کاربردهای دوگانه نظامی و غیرنظامی داشته باشند؛

باتوجه به اینکه پیشرفت توجه‌پذیری در توسعه و کاربرد آخرین فناوری‌های اطلاعات و ابزارهای ارتباطاتی به‌دست آمده است، همچنین قید شده است که این پیشرفت در علم و فناوری برای کاربردهای غیرنظامی، نیازمند صیانت و تشویق هستند؛

با تأیید اینکه به‌نظر می‌رسد در این روند، فرصت‌های مثبت گسترده‌ای برای توسعه بیشتر تمدن، گسترش فرصت‌ها برای همکاری حول منافع مشترک دولت‌ها، ارتقای قابلیت‌های خلاقانه نوع بشر و علاوه بر آن، افزایش گردش اطلاعات در جامعه جهانی وجود دارد؛

با یادآوری اینکه در این ارتباط، رویکردها و اصولی در کنفرانس جامعه اطلاعاتی و توسعه که در میدرند آفریقای جنوبی از ۱۳ تا ۱۵ می ۱۹۹۶ برگزار شد، ترسیم شده است؛ باتوجه به نتایج کنفرانس وزیران در مورد تروریسم که در تاریخ ۳۰ ژوئیه ۱۹۹۶ در پاریس برگزار شد و باتوجه به توصیه‌های آن کنفرانس؛

باتوجه به اینکه انتشار و استفاده از فناوری اطلاعات و ابزارها بر منافع کل جامعه بین‌المللی تأثیر می‌گذارد و اینکه بهره‌وری مطلوب و بهینه توسط همکاری‌های گسترده بین‌المللی تقویت می‌شود؛

با ابراز نگرانی از اینکه این فناوری‌ها و ابزارها به طور بالقوه می‌توانند برای مقاصدی که با اهداف مرتبط با حفظ ثبات و امنیت بین‌المللی متناقض هستند و ممکن است بر امنیت کشور تأثیر منفی بگذارد، مورد استفاده قرار گیرند؛

باتوجه به اینکه لازم است از سوءاستفاده یا بهره‌برداری از منابع اطلاعاتی یا فناوری اطلاعات برای مقاصد جنایی (اهداف مجرمانه) یا تروریستی پیشگیری شود:

۱. از کشورهای عضو می‌خواهد که در سطوح چندجانبه به بررسی تهدیدات موجود و بالقوه در زمینه امنیت اطلاعات بپردازند؛

۲. از تمام کشورهای عضو دعوت می‌کند تا نظرها و ارزیابی‌های خود را در مورد سؤالات زیر به دبیرکل اعلام کنند:

(a) درک عمومی از مسائل مربوط به امنیت اطلاعات؛

.....
(b) تعریف مفاهیم پایه‌ای مربوط به امنیت اطلاعات، از جمله نفوذ غیرمجاز یا سوءاستفاده از سیستم‌های اطلاعاتی و ارتباطاتی و منابع اطلاعاتی؛

(c) امکان آگاهی بخشی در خصوص توسعه اصول بین‌المللی که امنیت اطلاعات و سیستم‌های ارتباطاتی جهانی را تقویت می‌کند و به مبارزه با تروریسم و جرایم اطلاعاتی کمک می‌کند.
۳. از دبیرکل می‌خواهد که این گزارش (موارد بالا) را به اجلاس پنجم و چهارم مجمع عمومی ارائه دهد.

۴. تصمیم گرفته شد که این موضوع تحت عنوان «تحولات حوزه اطلاعات و ارتباطات در امنیت چارچوب بین‌المللی در دستور کار موقت پنجاه و چهارمین اجلاس مجمع عمومی» قرار گیرد.

جدول ۱: بند دو- تغییرات قطعنامه‌های تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌الملل (امنیت سایبری) پیش‌نویس روسیه، مصوب سال‌های ۱۹۹۹ تا ۲۰۱۵

تغییرات محتوایی	شماره گزارش	شماره دستورکار	شماره اجلاس	شماره قطعنامه	تاریخ انتشار قطعنامه	سال صدور قطعنامه
ندارد	A/54/558	۷۱	۵۴	A/RES/54/49	۲۳ دسامبر ۱۹۹۹	۱۹۹۹
دارد	A/55/554	۶۸	۵۵	A/RES/55/28	۲۰ دسامبر ۲۰۰۰	۲۰۰۰
دارد	A/56/533	۶۹	۵۶	A/RES/56/19	۷ ژانویه ۲۰۰۲	۲۰۰۱
دارد	A/57/505	۶۱	۵۷	A/RES/57/53	۳۰ دسامبر ۲۰۰۲	۲۰۰۲
ندارد	A/58/457	۶۸	۵۸	A/RES/58/32	۱۸ دسامبر ۲۰۰۳	۲۰۰۳
ندارد	A/59/454	۶۰	۵۹	A/RES/59/61	۱۶ دسامبر ۲۰۰۴	۲۰۰۴
دارد	A/60/452	۸۶	۶۰	A/RES/60/45	۶ ژانویه ۲۰۰۶	۲۰۰۵
ندارد	A/61/389	۸۵	۶۱	A/RES/61/54	۱۹ دسامبر ۲۰۰۶	۲۰۰۶
ندارد	A/62/386	۹۳	۶۲	A/RES/62/17	۸ ژانویه ۲۰۰۸	۲۰۰۷
ندارد	A/63/385	۸۵	۶۳	A/RES/63/37	۹ ژانویه ۲۰۰۹	۲۰۰۸
دارد	A/64/386	۹۱	۶۴	A/RES/64/25	۱۴ ژانویه ۲۰۱۰	۲۰۰۹
دارد	A/65/405	۹۲	۶۵	A/RES/65/41	۱۱ ژانویه ۲۰۱۱	۲۰۱۰
ندارد	A/66/407	۹۳	۶۶	A/RES/66/24	۱۳ دسامبر ۲۰۱۱	۲۰۱۱
ندارد	A/67/404	۸۹	۶۷	A/RES/67/27	۱۱ دسامبر ۲۰۱۲	۲۰۱۲
دارد	A/68/406	۹۴	۶۸	A/RES/68/243	۹ ژانویه ۲۰۱۴	۲۰۱۳
ندارد	A/69/435	۹۱	۶۹	A/RES/69/28	۱۱ دسامبر ۲۰۱۴	۲۰۱۴
دارد	A/70/455	۹۲	۷۰	A/RES/70/237	۳۰ دسامبر ۲۰۱۵	۲۰۱۵

۱. توضیح: برای پرهیز از تکرار مفاد قطعنامه‌ها که بخش‌های ثابت آن هر سال تکرار شده، فقط مشخصات قطعنامه جدید و محتوای افزوده شده به این قطعنامه ترجمه شده و از گنجاندن ترجمه بخش‌های تکراری آن اجتناب شده است. بدین ترتیب قطعنامه ۱۹۹۸ سال که اولین قطعنامه می‌باشد و قطعنامه‌های ۲۰۱۶، ۲۰۱۸ و ۲۰۱۹ که آخرین قطعنامه‌ها تا تاریخ نگارش کتاب می‌باشد، به صورت کامل ترجمه و بررسی شده و قطعنامه‌های مربوط به سال‌های بین این قطعنامه‌ها (۲۰۱۵-۱۹۹۹) در حد ارائه مشخصات و مفاد افزوده شده به قطعنامه معرفی و عنداللزوم بررسی شده است. به عنوان مثال بر اساس توضیح بالا باید گفت: قطعنامه ۱۹۹۹ تغییر محتوایی با قطعنامه سال قبل (۱۹۹۸) ندارد.

جدول ۲: تغییرات قطعنامه‌ها

محتوای افزوده شده به قطعنامه سال ۲۰۰۰ به شماره (A/RES/28/55)

با ملاحظه اینکه اهداف چنین اقداماتی می‌تواند از طریق بررسی طرح‌های بین‌المللی مرتبط در جهت تقویت امنیت سامانه‌های اطلاعات و مخابرات (ارتباطات راه دور) به‌کارگرفته شود.

محتوای افزوده شده به قطعنامه سال ۲۰۰۱ به شماره (A/RES/19/56)

با ملاحظه اینکه پیشگیری در استفاده از فناوری‌ها یا منابع اطلاعاتی برای اهداف مجرمانه یا تروریستی ضروری است.

محتوای افزوده شده به قطعنامه سال ۲۰۰۵ به شماره (A/RES/58/32)

مجمع عمومی؛

همچنین با در نظر گرفتن نتایج مرحله اول اجلاس جهانی سران درباره جامعه اطلاعاتی که در تاریخ ۱۰ تا ۱۲ دسامبر ۲۰۰۳ در ژنو برگزار شد،

باتوجه به اینکه انتشار و استفاده از فناوری اطلاعات و ابزار بر منافع کل جامعه بین‌المللی تأثیر می‌گذارد و اینکه اثربخشی مطلوب و بهینه توسط همکاری‌های گسترده بین‌المللی تقویت می‌شود.

با در نظر گرفتن اینکه دبیرکل در اجرای قطعنامه ۵۸/۳۲، ایجاد گروه کارشناسان دولتی در سال ۲۰۰۴، مطابق با وظیفه خود، تهدیدات موجود و بالقوه در حوزه امنیت اطلاعات و اقدامات همکاری‌جویانه ممکن جهت مقابله با آنها را مورد ملاحظه قرار دهد و مطالعه‌ای را در طرح‌های بین‌المللی مرتبط با هدف تقویت امنیت سامانه‌های اطلاعاتی و ارتباطات از راه دور (مخابراتی) هدایت نماید.

۴. باتوجه به گزارش دبیرکل از گروه کارشناسان دولتی در خصوص تحولات در زمینه (حوزه) اطلاعات و مخابرات در چارچوب امنیت بین‌المللی که بر اساس نتایج عملکرد گروه آماده شده است،
د. انجام اقدامات ممکن که توسط جامعه بین‌الملل برای تقویت امنیت اطلاعات در سطح جهانی می‌تواند صورت گیرد.

محتوای افزوده شده به قطعنامه سال ۲۰۰۹ به شماره (A/RES/64/25)

۵. توجه توأم با خرسندی از برگزاری اولین گروه کارشناسان دولتی ایجاد شده توسط دبیرکل، مورخ نوامبر ۲۰۰۹ در ژنو، و توجه به هدف گروه جهت تشکیل سه نشست دیگر در سال ۲۰۱۰ به منظور انجام وظیفه خود همانند آنچه در قطعنامه ۶۳/۳۷ تعیین شده است،

محتوای افزوده شده به قطعنامه سال ۲۰۱۰ به شماره (A/RES/65/41)

مجمع عمومی؛

باتوجه به ارزیابی‌ها و توصیه‌های موجود در گزارش گروه کارشناسان دولتی
۴. از کلیه دولت‌های عضو دعوت می‌کند، با در نظر گرفتن ارزیابی‌ها و توصیه‌های موجود در گزارش گروه کارشناسان دولتی در خصوص تحولات (در زمینه) حوزه اطلاعات و مخابرات در چارچوب امنیت بین‌المللی دیدگاه‌ها و ارزیابی‌های خود را در خصوص مسائل ذیل به اطلاعات دبیرکل برسانند.

محتوای افزوده شده به قطعنامه سال ۲۰۱۳ به شماره (A/RES/68/243)

مجمع عمومی؛

باتوجه به اهمیت احترام به حقوق بشر و آزادی‌های اساسی در استفاده از فناوری‌های اطلاعات و ارتباطات^۱

محتوای افزوده شده به قطعنامه سال ۲۰۱۵ به شماره (A/RES/70/237)

مجمع عمومی؛

با استقبال از نتیجه گروه کارشناسان دولتی در گزارش سال ۲۰۱۳ خود که اشعار می‌دارد حقوق بین‌الملل و به‌ویژه منشور سازمان ملل (بر فضای سایبر)، قابل اعمال می‌باشد و جهت حفظ صلح، پایداری و ارتقای محیط فناوری اطلاعات و ارتباطات صلح‌آمیز باز، امن، پایدار، قابل دسترس ضروری است، هنجارهای غیرالزام‌آور و داوطلبانه، قوانین و اصول رفتار مسئولانه دولت‌ها در استفاده از فناوری‌های اطلاعات و ارتباطات می‌تواند خطرهای صلح بین‌الملل، امنیت و پایداری را کاهش دهد و باتوجه به ویژگی‌های منحصر به فرد این فناوری‌ها، سایر هنجارها را می‌توان در طول زمان توسعه داد.

۱. از گزارش سال ۲۰۱۵ گروه کارشناسان دولتی در خصوص تحولات (در زمینه) حوزه اطلاعات و ارتباطات راه دور (مخابرات) در چارچوب امنیت بین‌الملل استقبال می‌کند

از دولت‌های عضو می‌خواهد

(الف) رهنمون شدن دولت‌ها به استفاده از فناوری‌های اطلاعاتی و ارتباطی با الهام از گزارش سال ۲۰۱۵ گروه کارشناسان دولتی در زمینه تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌الملل

(ب) ارتقای بیشتر ملاحظه، در سطوح چندجانبه، تهدیدات موجود و بالقوه در زمینه امنیت اطلاعات و همچنین اتخاذ راهبردهای ممکن برای مقابله با تهدیداتی که در این حوزه ظاهر می‌شوند؛ در عین سازگاری با نیاز به حفظ جریان

آزاد اطلاعات

۱. به دنبال افشاگری‌های اسنودن در سال ۲۰۱۳، رگه‌هایی از بازخورد‌های آن در قطعنامه دیده می‌شود

بند سه: قطعنامه تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین الملل سال ۲۰۱۶

ترجمه سند



مجمع عمومی
کمیته اول

تاریخ انتشار: ۹ دسامبر ۲۰۱۶

شماره قطعنامه: A/RES/ 71/28

توزیع: عمومی

اجلاس هفتاد و یکم

دستور کار ۹۳

قطعنامه مصوب مجمع عمومی

بر اساس گزارش ارائه شده از سوی کمیته اول؛ شماره گزارش (A/71/445)
۷۱/۲۸. تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین الملل

مجمع عمومی؛

باید آوری قطعنامه های خود شامل:

70/53 of 4 December 49/54 ,1998 of 1 December 28/55 ,1999 of 20
November 19/56 ,2000 of 29 November 53/57 ,2001 of 22 November
32/58 ,2002 of 8 December 61/59 ,2003 of 3 December 45/60 ,2004 of
8 December 54/61 ,2005 of 6 December 17/62 ,2006 of 5 December
37/63 ,2007 of 2 December 25/64 ,2008 of 2 December 41/65 ,2009 of
8 December 24/66 ,2010 of 2 December 27/67 ,2011 of 3 December
243/68 ,2012 of 27 December 28/69 ,2013 of 2 December 2014 and
237/70 of 23 December 2015,

با یادآوری قطعنامه های خود در زمینه نقش علم و فناوری در چارچوب امنیت بین الملل
که در آن علاوه بر اینکه این امر به رسمیت شناخته شده است، توسعه های علمی و فناورانه
می توانند کاربردهای دوگانه نظامی و غیرنظامی داشته باشند و این پیشرفت در علم و فناوری
برای کاربردهای غیر نظامی، نیازمند صیانت و تشویق هستند؛

با در نظر گرفتن نتایج اجلاس سران در مورد جامعه اطلاعاتی که فاز نخست آن از تاریخ ۱۰ تا ۱۲ دسامبر ۲۰۰۳ در ژنو و فاز دوم آن از ۱۶ تا ۱۸ نوامبر ۲۰۰۵ در تونس برگزار شد و بایادآوری قطعنامه شماره ۷۰/۱۲۵ آن در تاریخ ۱۶ دسامبر ۲۰۱۵؛
باتوجه به اینکه پیشرفت قابل توجهی در توسعه و کاربرد آخرین فناوری‌های اطلاعات و ابزارهای ارتباطاتی به دست آمده است؛

با تأیید اینکه به نظر می‌رسد در این روند، فرصت‌های مثبت گسترده‌ای برای توسعه بیشتر تمدن، گسترش فرصت‌ها برای همکاری حول منافع مشترک دولت‌ها، ارتقای قابلیت‌های خلاقانه نوع بشر و علاوه بر آن افزایش گردش اطلاعات در جامعه جهانی وجود دارد؛
باتوجه به اینکه انتشار و استفاده از فناوری اطلاعات و ابزار بر منافع کل جامعه بین‌المللی تأثیر می‌گذارد و این که اثربخشی مطلوب و بهینه توسط همکاری‌های گسترده بین‌المللی تقویت می‌شود؛

با ابراز نگرانی از اینکه این فناوری‌ها و ابزارها به طور بالقوه می‌توانند برای مقاصدی که با اهداف مرتبط با حفظ ثبات و امنیت بین‌المللی متناقض هستند و ممکن است بر انسجام زیرساخت‌های کشورهای تأثیر منفی داشته و امنیت هر دو حوزه نظامی و غیرنظامی را در معرض ضرر قرار دهند، مورد استفاده قرار گیرند؛

با ملاحظه به اینکه پیشگیری در مورد استفاده از فناوری‌ها یا منابع اطلاعاتی برای اهداف مجرمانه یا تروریستی ضروری است؛

باتوجه به اهمیت احترام به حقوق بشر و آزادی‌های اساسی در استفاده از فناوری‌های اطلاعاتی و ارتباطی؛

همچنین باتوجه به مشارکت کشورهای عضو که ارزیابی‌های خود را در مورد مسائل مربوط به امنیت اطلاعات مطابق با بند ۱ تا ۳ قطعنامه‌های ۷۰/۵۳، ۴۹/۵۴، ۲۸/۵۵، ۱۹/۵۶، ۵۳/۵۷، ۳۲/۵۸، ۶۱/۵۹، ۴۵/۶۰، ۵۴/۶۱، ۱۷/۶۲، ۳۷/۶۳، ۲۵/۶۴، ۴۱/۶۵، ۲۴/۶۶، ۲۷/۶۷، ۲۴۳/۶۸ و ۲۸/۶۹ و ۲۳۷/۷۰ به دبیرکل تقدیم کرده‌اند؛

باتوجه به اینکه گزارش‌های دبیرکل، حاوی این ارزیابی‌ها می‌باشد؛

بملاحظه اینکه ارزیابی های دولت های عضو که در گزارش های دبیرکل موجود است، به درک بهتر مفاهیم مربوط به موضوعات حوزه امنیت بین المللی اطلاعات و مفاهیم مرتبط کمک خواهد کرد؛ با استقبال از فعالیت مؤثر گروه کارشناسان دولتی در مورد تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین الملل و گزارش مربوط در مورد نتایج آن که توسط دبیرکل ارائه گردید؛ با استقبال از نتایج مذکور در گزارش گروه کارشناسان دولتی در سال های ۲۰۱۳ و ۲۰۱۵ که اشعار می دارد حقوق بین الملل و مخصوصاً منشور ملل متحد (برفضای سایبر) قابل اعمال است و حتی این امر جهت بهره مندی از محیط فناوری اطلاعاتی و ارتباطی صلح آمیز، پایدار، امن، باز و در دسترس، یک ضرورت است؛ هنجارهای داوطلبانه و غیرالزام آور، قوانین و اصول رفتار مسئولانه دولت ها در استفاده از فناوری های اطلاعاتی و ارتباطی می توانند به کاهش خطرهای که متوجه صلح بین الملل، امنیت و پایداری است بینجامد، باتوجه به ویژگی های منحصر به فرد این فناوری ها، سایر هنجارها را می توان در طول زمان توسعه داد.

۱. از کشورهای عضو می خواهد :

الف) رهنمون شدن دولت ها به استفاده از فناوری های اطلاعاتی و ارتباطی با الهام از گزارش سال ۲۰۱۵ گروه کارشناسان دولتی در زمینه تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین الملل؛

ب) توجه بیشتر به تهدیدات موجود و بالقوه در زمینه امنیت اطلاعات در سطوح چندجانبه و همچنین اتخاذ راهبردهای ممکن برای مقابله با تهدیداتی که در این حوزه ظاهر می شوند؛ در عین سازگاری با نیاز به حفظ جریان آزاد اطلاعات.

۲. با ملاحظه اینکه اهداف چنین اقداماتی می تواند از طریق بررسی طرح های بین المللی مرتبط در جهت تقویت امنیت سامانه های اطلاعات و مخابرات (ارتباطات راه دور) به کار گرفته شود.

۳. از کلیه دولت های عضو دعوت می کند، با در نظر گرفتن ارزیابی ها و توصیه های موجود در گزارش گروه کارشناسان دولتی در خصوص تحولات در حوزه اطلاعات و مخابرات در چارچوب امنیت بین المللی دیدگاه ها و ارزیابی های خود را در خصوص مسائل ذیل به اطلاعات دبیرکل برساند:

(a) درک عمومی از مسائل مربوط به امنیت اطلاعات؛

- (b) تلاش‌های صورت گرفته در سطح ملی برای تقویت امنیت اطلاعات و فراهم کردن همکاری‌های بین‌المللی در این حوزه
- (c) محتوای مفاهیم ذکر شده در بند ۲ بالا
- (d) انجام اقدامات ممکن که توسط جامعه بین‌الملل برای تقویت امنیت اطلاعات در سطح جهانی می‌تواند صورت گیرد.

۴. با استقبال از آغاز به کار گروه کارشناسان دولتی که توسط دبیرکل به موجب قطعنامه ۷۰/۲۳۷ بر اساس توزیع عادلانه جغرافیایی ایجاد شده است که باتوجه به ارزیابی‌ها و توصیه‌های موجود در گزارش فوق، باید با رویکرد فراهم نمودن درک مشترک، به مطالعه در زمینه تهدیدات موجود و بالقوه در حوزه امنیت اطلاعات و اقدامات همکاری‌جویانه ممکن برای مقابله با آن‌ها و نحوه اعمال حقوق بین‌المللی در زمینه استفاده از فناوری اطلاعات و ارتباطات توسط دولت‌ها، و همچنین هنجارها، قوانین و اصول رفتار مسئولانه دولت‌ها، اقدامات اعتمادساز و ظرفیت‌ساز و مفاهیم اشاره شده در بند ۲ بالا پرداخته و گزارش نتایج حاصل از این مطالعه به اجلاس هفتاد و دوم مجمع عمومی ارائه نمایند؛

۵. تصمیم گرفته شد که این موضوع در دستور کار موقت هفتاد و دومین اجلاس مجمع عمومی تحت عنوان «تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌المللی» قرار گیرد.

بند چهار: قطعنامه تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین الملل سال ۲۰۱۸

ترجمه سند



مجمع عمومی
کمیته اول

تاریخ انتشار: ۱۱ دسامبر ۲۰۱۸

شماره قطعنامه: A/RES/73/27

توزیع: عمومی

اجلاس هفتاد و سوم

دستور کار ۹۶

قطعنامه مصوب مجمع عمومی

بر اساس گزارش ارائه شده از سوی کمیته اول؛ شماره گزارش (A/73/505)

تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین الملل

مجمع عمومی؛

با یادآوری قطعنامه‌های خود {به شماره‌های} ۳۶/۱۰۳ مورخ ۹ دسامبر ۱۹۸۱، ۴۳/HY۸ مورخ ۷ دسامبر ۱۹۸۸، ۵۳/۷۰ مورخ ۴ دسامبر ۱۹۹۸، ۵۴/۴۹ مورخ ۱ دسامبر ۱۹۹۹، ۵۵/۲۸ مورخ ۲۰ نوامبر ۲۰۰۰، ۵۶/۱۹ مورخ ۲۹ نوامبر ۲۰۰۱، ۵۷/۵۳ مورخ ۲۲ نوامبر ۲۰۰۲، ۵۸/۳۲ مورخ ۸ دسامبر ۲۰۰۳، ۵۹/۶۱ مورخ ۳ دسامبر ۲۰۰۴، ۶۰/۴۵ مورخ ۸ دسامبر ۲۰۰۵، ۶۱/۵۴ مورخ ۶ دسامبر ۲۰۰۶، ۶۲/۱۷ مورخ ۵ دسامبر ۲۰۰۷، ۶۳/۳۷ مورخ ۲ دسامبر ۲۰۰۸، ۶۴/۲۵ مورخ ۲ دسامبر ۲۰۰۹، ۶۵/۴۱ مورخ ۸ دسامبر ۲۰۱۰، ۶۶/۲۴ مورخ ۲ دسامبر ۲۰۱۱، ۶۷/۲۷ مورخ ۳ دسامبر ۲۰۱۲، ۶۸/۲۴۳ مورخ ۲۷ دسامبر ۲۰۱۳، ۶۹/۲۸ مورخ ۲ دسامبر ۲۰۱۴، ۷۰/۲۳۷ مورخ ۲۳ دسامبر ۲۰۱۵ و ۷۱/۲۸ مورخ ۵ دسامبر ۲۰۱۶،

باتوجه به رشد چشمگیری که در توسعه و به کارگیری آخرین فناوری‌های اطلاعاتی و تجهیزات مخابراتی به دست آمده است،

با تأکید بر آرمان‌های جامعه بین الملل در استفاده صلح آمیز از فناوری‌های اطلاعات و ارتباطات در جهت منافع مشترک بشری، ارتقای و توسعه پایدار تمامی کشورها صرف نظر از توسعه علمی و فناوری آن‌ها؛

باتوجه به ضرورت ظرفیت‌سازی در خصوص همکاری دولت‌ها و اطمینان‌سازی در حوزه امنیت فناوری اطلاعات و ارتباطات؛

با به رسمیت شناختن اینکه برخی کشورها ممکن است در تلاش‌های خود برای از بین بردن شکاف امنیتی در حوزه فناوری اطلاعات و ارتباطات و بهره‌برداری از این فناوری نیازمند مساعدت و کمک باشند؛

باتوجه به اینکه ارائه کمک بر اساس درخواست، جهت ظرفیت‌سازی در حوزه امنیت آی‌سی‌تی، امنیت بین‌المللی ضروری می‌باشد؛

با تأیید اینکه اقدامات ظرفیت‌ساز باید به دنبال ارتقای استفاده صلح‌آمیز از فناوری‌های اطلاعات و ارتباطات باشند؛

با تأیید اینکه فناوری‌های اطلاعات و ارتباطات، فناوری‌هایی با کاربرد دوگانه می‌باشند و می‌توانند {توأم‌ان} برای اهداف قانونی و مخرب به کار روند؛

با ابراز نگرانی از اینکه تعدادی از دولت‌ها، در حال توسعه قابلیت‌های فناوری اطلاعات و ارتباطات برای اهداف نظامی هستند و احتمال استفاده از این فناوری‌ها در مخاصمات آینده بین دولت‌ها مدام در حال افزایش است؛

با تأکید بر اینکه به نفع تمامی دولت‌هاست که با هدف شکل‌دهی به جامعه‌ای با آینده مشترک برای بشریت در فضای سایبر، برای ارتقای کاربرد صلح‌آمیز فناوری‌های اطلاعات و ارتباطات اقدام کنند و همچنین دولت‌ها، منافع مشترکی در پیشگیری از مخاصمات ناشی از کاربرد فناوری‌های اطلاعات و ارتباطات را دارا می‌باشند؛

باتوجه به اینکه سازمان ملل متحد در زمینه ارتقای گفتگو میان دولت‌های عضو جهت توسعه فهم مشترک از امنیت و کاربرد فناوری‌های اطلاعات و ارتباطات و نیز کاربرد حقوق و هنجارها، قوانین و اصول بین‌المللی در خصوص رفتار مسئولانه دولت‌ها در این فضا، هرچند باید نقش راهبری ایفا نماید، با این حال، تلاش‌های منطقه‌ای، ارتقای اقدامات شفاف‌ساز و اعتمادساز و پشتیبانی از ظرفیت‌سازی و انتشار رویه‌های برتر نیز مورد تشویق می‌باشد؛

با ابراز نگرانی از تعبیه و جاسازی کارکردهای مخفی مخرب در فناوری‌های اطلاعات و ارتباطات،

که از طرق مختلفی می‌توانند جهت تأثیر بر امنیت و کاربری مطمئن و زنجیره تأمین این فناوری‌ها در روند تولیدات و خدمات، موجب تضعیف اعتماد در تجارت و خسارت به امنیت ملی شوند، با در نظر قرار دادن ضرورت ممانعت از کاربرد منابع اطلاعاتی یا فناوری‌ها برای اهداف مجرمانه یا تروریستی؛

با تأکید بر اهمیت احترام به حقوق بشر و آزادی‌های اساسی در استفاده از فناوری‌های اطلاعات و ارتباطات؛

با استقبال از عملکرد مؤثر گروه کارشناسان دولتی در خصوص تحولات در حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌المللی و گزارش‌های نتایج مربوط که توسط دبیرکل ارائه گردیده است؛

همچنین با استقبال از اینکه گروه کارشناسان دولتی در گزارش سال ۲۰۱۵ خود، کاربرد و اعمال حقوق بین‌الملل در استفاده دولت‌ها از فناوری‌های اطلاعات و ارتباطات را حائز اهمیت محوری در تعهدات دولت‌ها درباره پیروی از اصول منشور ملل متحد و سایر حقوق بین‌الملل مورد شناسایی قرار داده است: حاکمیت برابر، حل و فصل اختلافات بین‌المللی با ابزار مسالمت‌آمیز به نحوی که صلح و امنیت بین‌المللی و عدالت در معرض خطر قرار نگیرند و ممانعت از تهدید یا استفاده از زور در روابط بین‌المللی دولت‌ها علیه تمامیت ارضی یا استقلال سیاسی هر دولت دیگر یا به هر روشی که با اهداف ملل متحد منافات داشته باشد، احترام به حقوق بشر و آزادی‌های اساسی، عدم مداخله در امور داخلی دیگر دولت‌ها؛

با تأیید نتایج گروه کارشناسان دولتی مندرج در گزارش‌های ۲۰۱۳ و ۲۰۱۵، { دایر بر اینکه } حقوق بین‌الملل، به‌ویژه منشور ملل متحد برای حفظ صلح و ثبات بین‌المللی و ارتقای یک محیط فناوری اطلاعات و ارتباطات صلح‌آمیز، در دسترس، با ثبات، امن و آزاد قابل اعمال و ضروری است، هنجارهای دواطلبانه غیرالزام‌آور، قواعد و اصول رفتار مسئولانه دولت‌ها در استفاده از فناوری‌های اطلاعات و ارتباطات می‌تواند خطرهای صلح، امنیت و ثبات بین‌المللی را کاهش دهد و با توجه به ویژگی‌های منحصر به فرد فناوری‌ها، هنجارهای تکمیلی می‌توانند در بستر زمان ایجاد شوند؛

همچنین با تأیید حاکمیت دولت‌ها و هنجارها و اصول بین‌المللی که ناشی از اعمال حاکمیت در رفتار دولت‌ها در فعالیت‌های مرتبط با فناوری اطلاعات و ارتباطات و {همچنین با تأیید} اعمال صلاحیت دولت‌ها بر زیرساخت‌های فناوری اطلاعات و ارتباطات در قلمرو سرزمینی خود، با تأیید مجدد حق و وظیفه دولت‌ها در چارچوب قانون اساسی خود (امتیاز حاکمیتی) جهت مبارزه علیه انتشار اخبار کذب یا تحریف شده که می‌توانند به‌عنوان مداخله در امور داخلی دولت‌های دیگر یا به‌عنوان عامل مخرب علیه ارتقای صلح، همکاری و روابط دوستانه میان دولت‌ها و ملت‌ها تلقی گردد، با به رسمیت شناختن وظیفه یک دولت جهت امتناع از هر کمپین (کارزار) افتراآمیز، تبلیغات همراه با بهتان یا خصمانه با هدف مداخله مشروع (با اذن دولت مداخله شونده در اموری که خلاف اصول منشور ملل باشد) یا مداخله نامشروع (بدون اذن دولت مداخله شونده) در امور داخلی دولت‌های دیگر؛

با تأکید بر اینکه، باوجود مسئولیت اولیه‌ای که دولت‌ها جهت حفظ محیط فناوری اطلاعات و ارتباطات صلح‌آمیز و امن دارند، همکاری مؤثر بین‌المللی از طریق شناسایی سازوکارهایی برای مشارکت بخش خصوصی، سازمان‌های جامعه مدنی و دانشگاهی به طریق مقتضی مفید خواهد بود:

۱- از تبعیت دولت‌ها از مجموعه قوانین، هنجارها و اصول بین‌المللی درباره رفتار مسئولانه آن‌ها مندرج در گزارش گروه کارشناسان دولتی استقبال می‌نماید، {این امر} در گزارش‌های سال‌های ۲۰۱۳ و ۲۰۱۵ مربوط به گروه کارشناسان دولتی در خصوص تحولات در حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌الملل که از طریق اجماع تصویب گردیدند و در قطعنامه مصوب مجمع عمومی {با شماره} ۷۱/۲۸ مورخ ۵ دسامبر ۲۰۱۵ با عنوان «تحولات در زمینه اطلاعات و ارتباطات در چارچوب امنیت بین‌المللی» ارج نهاده شده‌اند؛

۱-۱- وفق اهداف ملل متحد از جمله، حفظ امنیت و صلح بین‌المللی، دولت‌ها باید در توسعه و اعمال اقدامات جهت افزایش ثبات و امنیت در به‌کارگیری فناوری‌های اطلاعات و ارتباطات

همکاری داشته باشند و از رویه‌های فناوری‌های اطلاعات و ارتباطات که بر مخرب بودن آن‌ها اذعان شده یا اینکه ممکن است موجب خطرهای برای صلح و امنیت بین‌المللی باشد، ممانعت کنند؛

۱-۲- دولت‌ها باید پذیرای تعهدات بین‌المللی خود در ارتباط با اقدامات غیرقانونی منتسب به آن‌ها، ذیل حقوق بین‌الملل باشند، با این حال ادله‌ای که مبین راه اندازی یک فعالیت فناوری اطلاعات و ارتباطات است یا به طرق دیگر بر سرچشمه گرفتن از سرزمین یا اهداف زیرساخت فناوری اطلاعات و ارتباطات یک دولت دلالت می‌نماید، ممکن است کفایت و بسندگی لازم برای انتساب فعالیت بدان دولت را نداشته باشد. دولت‌ها باید توجه داشته باشند که اتهامات علیه دیگر دولت‌ها دایر بر سازماندهی و پیاده‌سازی نامشروع (غیرقانونی) باید اثبات شده باشد. در مورد حوادث فناوری اطلاعات و ارتباطات، دولت‌ها باید تمامی اطلاعات مرتبط، از جمله چارچوبی وسیع‌تر از صرف رویداد، چالش‌های انتساب در محیط فناوری اطلاعات و ارتباطات و ماهیت و گستره پیامدهای آن را در نظر بگیرند؛

۱-۳- دولت‌ها نباید آگاهانه اجازه دهند سرزمینشان جهت اقدامات بین‌المللی غیرقانونی که با استفاده از فناوری‌های اطلاعات و ارتباطات صورت می‌گیرد، مورد استفاده قرار گیرد. دولت‌ها نباید از پراکسی‌ها جهت ارتکاب اقدامات بین‌المللی نامشروع که با استفاده از فناوری‌های اطلاعات و ارتباطات صورت می‌گیرد، استفاده کنند و باید تضمین گردد سرزمین آن‌ها مورد استفاده بازیگران غیر دولتی جهت ارتکاب چنین افعالی قرار نگرفته است؛

۱-۴- دولت‌ها باید چگونگی همکاری بهتر به‌منظور تبادل اطلاعات، کمک به یکدیگر، تعقیب استفاده جنایی و تروریستی از فناوری‌های اطلاعات و ارتباطات و اجرای سایر اقدامات مشترک جهت مقابله با چنین تهدیداتی را در نظر بگیرند. دولت‌ها ممکن است اتخاذ اقدامات جدید دیگری در این رابطه را در نظر بگیرند؛

۵-۱- دولت‌ها، در تضمین استفاده ایمن از فناوری‌های اطلاعات و ارتباطات، باید به قطعنامه‌های شورای حقوق بشر (به شماره‌های { ۲۰/۸ مورخ ۵ جولای ۲۰۱۵ و ۲۶/۱۳ مورخ ۲۶ ژوئن ۲۰۱۴ در خصوص ارتقای، حفاظت و بهره‌مندی از حقوق بشر در اینترنت، و نیز قطعنامه‌های مجمع عمومی (به شماره‌های { ۶۸/۱۶۷ مورخ ۱۸ دسامبر ۲۰۱۳ و ۶۹/۱۶۶ مورخ ۱۸ دسامبر ۲۰۱۴ در خصوص حق حریم خصوصی در عصر دیجیتال احترام بگذارند و احترام کامل به حقوق بشر از جمله حق آزادی بیان را ضمانت نمایند؛

۶-۱- یک دولت نباید با فعالیت فناوری اطلاعات و ارتباطات که به صورت بالقوه به زیرساخت‌های حیاتی خسارت می‌زند یا به طریق دیگری استفاده و بهره‌گیری از زیرساخت‌های حیاتی جهت ارائه خدمات به عموم را مختل می‌کند و مغایر با تعهداتش ذیل حقوق بین‌الملل است، همکاری یا آگاهانه از این فعالیت‌ها حمایت کند؛

۷-۱- دولت‌ها باید با در نظر گرفتن قطعنامه مجمع عمومی { به شماره { ۵۸/۱۹۹ مورخ ۲۳ دسامبر ۲۰۰۳ درباره ایجاد فرهنگ جهانی امنیت سایبری و حفاظت از زیرساخت‌های حیاتی اطلاعات و دیگر قطعنامه‌های مرتبط، به منظور حفاظت از زیرساخت‌های حیاتی خود در مقابل تهدیدات فناوری اطلاعات و ارتباطات، اقدامات مناسبی را اتخاذ نمایند؛

۸-۱- دولت‌ها باید به درخواست‌های مقتضی کمک دیگر دولت‌ها که زیرساخت‌های حیاتی آن‌ها در معرض اقدامات مخرب فناوری اطلاعات و ارتباطات قرار گرفته است پاسخ دهند، دولت‌ها همچنین باید به درخواست‌های مقتضی جهت تقلیل فعالیت مخرب فناوری اطلاعات و ارتباطات ناشی از سرزمین آن‌ها که زیرساخت‌های حیاتی دیگر دولت‌ها را هدف قرار داده است، پاسخ دهند؛

۹-۱- دولت‌ها باید به منظور تضمین تمامیت زنجیره تأمین که در نتیجه آن، کاربران نهایی بتوانند از امنیت محصولات فناوری اطلاعات و ارتباطات اطمینان حاصل نمایند، گام‌های مناسب بردارند.

۱۰-۱- دولت‌ها باید پیشگیری از اشاعه ابزار و فناوری‌های مخرب (بدافزارها) و استفاده از کارکردهای مخرب مخفی را پیگیری نمایند؛

۱۱-۱- دولت‌ها باید گزارش‌دهی مسئولانه آسیب‌پذیری‌های فناوری اطلاعات و ارتباطات را تشویق نمایند و اطلاعات تجمیعی از راه‌حل‌های موجود را جهت محدود کردن چنین آسیب‌پذیری‌هایی به اشتراک گذارند و در حد امکان تهدیدات بالقوه فناوری‌های اطلاعات و ارتباطات و زیرساخت وابسته به آن‌ها را از بین ببرند؛

۱۲-۱- دولت‌ها نباید فعالیت‌هایی را که به سیستم‌های اطلاعاتی تیم‌های مجاز پاسخ سریع کشورهای دیگر (که گاهی تحت عنوان تیم‌های پاسخ سریع رایانه‌ای یا تیم‌های پاسخ حوادث امنیت سایبری شناخته می‌شوند) آسیب وارد می‌نماید، انجام دهند یا آگاهانه از این فعالیت‌ها حمایت نمایند. یک دولت نباید از تیم‌های مجاز پاسخ سریع جهت درگیری در فعالیت‌های بین‌المللی مخرب استفاده نمایند.

۱۳-۱- دولت‌ها باید بخش خصوصی و جامعه مدنی را جهت ایفای نقش مناسب در بهبود امنیت و استفاده از فناوری‌های اطلاعات و ارتباطات از جمله امنیت زنجیره تأمین برای محصولات و خدمات فناوری‌های اطلاعات و ارتباطات تشویق نمایند، دولت‌ها باید با عنایت به نقش بالقوه بخش‌های خصوصی و سازمان‌های جامعه مدنی در حوزه به‌کارگیری قواعد رفتارمسئولانه در فضای اطلاعات با آن‌ها همکاری نمایند؛

۲- از دولت‌های عضو، ارتقای بیشتر در سطوح چندجانبه، لحاظ تهدیدات موجود و بالقوه در حوزه امنیت اطلاعات و نیز راهبردهای محتمل جهت مقابله با تهدیدات نوظهور در این زمینه، سازگار با ضرورت حفظ جریان آزاد اطلاعات را خواستار است؛

۳- با ملاحظه اینکه هدف چنین اقداماتی می‌تواند از طریق اجرای آزمایشی بیشتر طرح‌های مرتبط بین‌المللی معطوف به تقویت امنیت سیستم‌های اطلاعات و ارتباطات از راه دور (مخابرات) تحقق یابد را مورد نظر قرار می‌دهد؛

۴- از تمامی دولت‌های عضو دعوت می‌نماید، با در نظر گرفتن ارزیابی‌ها و توصیه‌های مندرج در گزارش‌های گروه کارشناسان دولتی در خصوص تحولات حوزه اطلاعات و ارتباطات از راه دور در چارچوبی امنیت بین‌المللی، جهت ادامه اطلاع‌رسانی به دبیرکل از دیدگاه و ارزیابی‌های خود، در مورد سؤالات ذیل اقدام نمایند:

الف - فهم عمومی از موضوعات امنیت اطلاعات؛

ب- تلاش‌های صورت گرفته در سطوح ملی جهت تقویت امنیت اطلاعات و ارتقای همکاری‌های بین‌المللی در این حوزه؛

ج- محتوای مفاهیم مذکور در پارگراف ۳؛

۵- اقدامات محتمل که می‌تواند توسط جامعه بین‌المللی جهت تقویت امنیت اطلاعات در سطح جهانی صورت پذیرد؛

۶- جهت { موارد ذیل } تصمیم‌گیری می‌نماید:

برپایی اجلاسی در سال ۲۰۱۹، با نگاهی بر ایجاد فرایند (فرایندسازی) مذاکره دموکراتیک‌تر، فراگیرتر و شفاف‌تر در سازمان ملل متحد، درباره امنیت در استفاده از فناوری اطلاعات و ارتباطات؛ تشکیل گروه کاری بازی با عملکرد مبتنی بر اجماع، به‌عنوان یک اولویت، جهت ادامه توسعه بیشتر قواعد، هنجارها و اصول رفتار مسئولانه دولت‌ها که در بند ۱ فهرست شده است و طرق اجرای آن‌ها؛

در صورت لزوم، جهت اعمال تغییرات در { قواعد، هنجارها و اصول } یا ایجاد قواعد مکمل رفتاری؛

جهت بررسی امکان برقراری گفتگوی منظم نهادی با مشارکت وسیع تحت نظارت سازمان ملل متحد؛

و ادامه بررسی، با نگاهی بر ارتقای درک عمومی، تهدیدات بالقوه و موجود در حوزه امنیت اطلاعات و اقدامات همکاری جویانه احتمالی جهت مقابله با آن‌ها، چگونگی اعمال حقوق بین‌الملل در استفاده از فناوری اطلاعات و ارتباطات توسط دولت‌ها و نیز اقدامات اطمینان‌ساز و ظرفیت‌سازی و مفاهیم مطرح در بند ۳؛

و تسلیم گزارشی از نتایج بررسی به اجلاس هفتاد و پنجم مجمع عمومی؛
و فراهم کردن امکان برگزاری نشست‌های مشورتی در فاصله زمانی بین اجلاس‌ها، از بین شرکت‌کنندگان داوطلب، با حضور بخش‌های علاقه‌مند از جمله مشاغل (کسب‌وکار)، سازمان‌های غیردولتی و دانشگاهی جهت به اشتراک گذاشتن دیدگاه‌های خود در مورد موضوعات مندرج در دستور کار گروه کارشناسان دولتی؛

۷- همچنین در مورد بایستگی برگزاری اجلاس سازمانی گروه کاری باز در ژوئن ۲۰۱۹، به‌منظور توافق درباره ترتیبات سازمانی مرتبط با گروه، تصمیم می‌گیرد؛

۸- در خصوص درج موضوعی با عنوان «تحولات در حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌الملل» در دستورکار موقت خود در اجلاس هفتاد و چهارم تصمیم می‌گیرد.

بندپنج: قطعنامه پیشرفت رفتار مسئولانه دولت

درباره فضای سایبر در چارچوب امنیت بین‌المللی سال ۲۰۱۸

ترجمه سند



تاریخ انتشار: ۲ ژانویه ۲۰۱۹

شماره قطعنامه: A/RES/ 73/266

توزیع: عمومی

اجلاس هفتادوسوم

دستور کار ۹۶

قطعنامه مصوب مجمع عمومی مورخ ۲۲ دسامبر ۲۰۱۸

بر اساس گزارش ارائه شده از سوی کمیته اول؛ شماره گزارش (A/72/505)

۶۱/۵۴. پیشرفت رفتار مسئولانه دولت درباره فضای سایبر در چارچوب امنیت بین‌المللی^۲

مجمع عمومی؛

با یادآوری قطعنامه‌های خود { به شماره‌های } ۵۳/۷۰ مورخ ۴ دسامبر ۱۹۹۸، ۵۴/۴۹ مورخ اول دسامبر ۱۹۹۹، ۵۵/۲۸ مورخ ۲۰ نوامبر ۲۰۰۰، ۵۶/۱۹ مورخ ۲۹ نوامبر ۲۰۰۱، ۵۷/۵۳ مورخ ۲۲ نوامبر ۲۰۰۲، ۵۸/۳۲ مورخ ۸ دسامبر ۲۰۰۳،

۵۹/۶۱ مورخ ۳ دسامبر ۲۰۰۴، ۶۰/۴۵ مورخ ۸ دسامبر ۲۰۰۵، ۶۱/۵۴ مورخ ۶ دسامبر ۲۰۰۶، ۶۲/۱۷ مورخ ۵ دسامبر ۲۰۰۷، ۶۳/۳۷ مورخ ۲ دسامبر ۲۰۰۸، ۶۴/۲۵ مورخ ۲ دسامبر ۲۰۰۹، ۶۵/۴۱ مورخ ۸ دسامبر ۲۰۱۰، ۶۶/۲۴ مورخ ۲ دسامبر ۲۰۱۱، ۶۷/۲۷ مورخ ۳ دسامبر ۲۰۱۲، ۶۸/۲۴۳ مورخ ۲۷ دسامبر ۲۰۱۳، ۶۹/۲۸ مورخ ۲ دسامبر ۲۰۱۴، ۷۰/۲۳۷ مورخ ۲۳ دسامبر ۲۰۱۵ و ۷۱/۲۸ مورخ ۵ دسامبر ۲۰۱۶ و نیز تصمیم خود به شماره ۷۲/۵۱۲ مورخ ۴ دسامبر ۲۰۱۷،

باتوجه به رشد چشمگیری که در توسعه و به‌کارگیری آخرین فناوری‌های اطلاعاتی و تجهیزات مخابراتی به‌دست آمده است، با تأیید اینکه به موازات این پیشرفت‌های فناورانه ما شاهد گسترده‌ترین فرصت‌های مثبت در {موارد ذیل} هستیم: توسعه بیشتر تمدن، توسعه فرصت‌ها

۱. بررسی این سند به بند شش همین میحث تحت عنوان «مقایسه و بررسی محتوایی، تاریخی و تطبیقی...» موکول شده است.

2. Advancing responsible State behaviour in cyberspace in the context of international security

جهت همکاری حول منافع مشترک تمامی دولت‌ها، ارتقای قابلیت خلاقانه بشری و افزایش پیشرفت در گردش اطلاعات در جامعه جهانی؛

باتوجه به اینکه انتشار و استفاده از فناوری‌ها و ابزار اطلاعاتی، منافع کل جامعه بین‌المللی را تحت تأثیر قرار می‌دهد و اثربخشی بهینه به واسطه همکاری‌های وسیع بین‌المللی ترقی می‌یابد؛ با تأیید اینکه فناوری‌های اطلاعات و ارتباطات، فناوری‌هایی با کاربرد دوگانه می‌باشند و می‌توانند {توآمان} برای اهداف قانونی و مخرب به کار روند، با تأکید بر منفعت دولت‌ها در ارتقای استفاده از فناوری‌های اطلاعات و ارتباطات برای اهداف مسالمت‌آمیز و پیشگیری از مخاصمات ناشی از کاربرد فناوری‌های اطلاعات و ارتباطات؛

ضمن ابراز نگرانی از استفاده بالقوه فناوری‌ها و تجهیزات {با قابلیت کاربرد دوگانه} برای مقاصد ناسازگار با اهداف معطوف به حفظ ثبات و امنیت بین‌المللی و اینکه این فناوری‌ها ممکن است به شکل خصمانه‌ای با ایراد صدمه توآمان به امنیت نظامی و غیرنظامی، تمامیت زیرساخت آن‌ها را تحت تأثیر قرار دهد؛

با تأکید بر ضرورت ارتقای هماهنگی و همکاری میان دولت‌ها در خصوص مبارزه با سوءاستفاده مجرمانه از فناوری‌های اطلاعات، با تأکید بر اهمیت احترام به حقوق بشر و آزادی‌های اساسی در استفاده از فناوری‌های اطلاعات و ارتباطات؛

با استقبال از عملکرد مؤثر گروه کارشناسان دولتی در خصوص تحولات در حوزه اطلاعات و ارتباطات راه دور در چارچوب امنیت بین‌الملل و گزارش‌های ارائه شده توسط دبیرکل؛

با تأکید بر اهمیت ارزیابی‌ها و توصیه‌های مندرج در گزارش‌های گروه کارشناسان دولتی؛ با تأیید نتایج مندرج در گزارش‌های گروه کارشناسان دولتی در سال‌های ۲۰۱۳ و ۲۰۱۵، در خصوص اینکه:

✓ جهت حفظ صلح و امنیت و ارتقای یک محیط فناورانه اطلاعات و ارتباطات آزاد، ایمن، پایدار، قابل دسترس و مسالمت‌آمیز، حقوق بین‌الملل به‌ویژه منشور ملل متحد، ضروری و قابل اعمال می‌باشند؛

✓ هنجارها، قواعد و اصول داوطلبانه و غیرالزام‌آور در رفتار مسئولانه دولت‌ها جهت استفاده از

فناوری‌های اطلاعات و ارتباطات می‌تواند مخاطرات صلح، امنیت و پایداری بین‌المللی را کاهش دهد. ✓
باتوجه به ویژگی‌های منحصربه‌فرد چنین فناوری‌هایی، هنجارهای مکمل می‌تواند در طول زمان ایجاد شوند.

همچنین با تأیید نتایج گروه کارشناسان دولتی مبنی بر اینکه اقدامات اعتمادساز داوطلبانه می‌توانند اعتماد و اطمینان را میان دولت‌ها ارتقای دهند و از طریق افزایش پیش‌بینی‌پذیری و کاهش سوءتفاهمات می‌توانند به کاهش خطر مخاصمات کمک نمایند و بدین وسیله می‌توانند جهت مقابله با نگرانی‌های دولت‌ها درباره استفاده کشورها از فناوری‌های اطلاعات و ارتباطات، مشارکت و همکاری مهمی را ایجاد نمایند و می‌تواند گام مهمی به سوی امنیت بیشتر در محیط بین‌المللی باشد؛ به‌علاوه با تأیید نتایج گروه کارشناسان دولتی که ضرورت مساعدت برای ظرفیت‌سازی در حوزه امنیت فناوری اطلاعات و ارتباطات در جهت امنیت بین‌المللی را خاطر نشان می‌سازد، که از طریق ارتقای ظرفیت دولت‌ها با هدف همکاری اقدامات مشترک و ارتقای استفاده از چنین فناوری‌هایی در جهت اهداف مسالمت‌آمیز، قابل حصول است؛

با تأکید بر اینکه مسئولیت اولیه و اصلی دولت‌ها در قبال حفظ محیط فناوری اطلاعات و ارتباطات ایمن و مسالمت‌آمیز، همکاری بین‌المللی مؤثر برای شناسایی سازوکارهای مشارکت بخش خصوصی، دانشگاهی و سازمان‌های جامعه مدنی، عندالاقضاء، مفید خواهد بود:

۱- از دولت‌های عضو درخواست می‌نماید:

الف- گزارش‌های سال‌های ۲۰۱۰، ۲۰۱۳، ۲۰۱۵ گروه کارشناسان دولتی درباره تحولات در حوزه اطلاعات و ارتباطات راه دور در چارچوب امنیت بین‌المللی را به‌عنوان راهنمایی جهت استفاده خود از فناوری اطلاعات و ارتباطات قرار دهند؛

ب- همان‌طور که در گزارش‌های گروه کارشناسان دولتی تعیین گردیده است، از اجرای اقدامات همکاری جویانه، جهت مقابله با تهدیدات نوظهور در این حوزه پشتیبانی نمایند و اطمینان حاصل نمایند که محیط فناوری اطلاعات و ارتباطات آزاد، با قابلیت تبادل اطلاعات، قابلیت اعتماد و ایمن مطابق با ضرورت حفظ جریان آزاد اطلاعات سازگار می‌باشد؛

۲- از تمامی دولت‌های عضو دعوت می‌نماید، با در نظر گرفتن ارزیابی‌ها و توصیه‌های مندرج در گزارش‌های گروه کارشناسان دولتی، جهت ادامه اطلاع‌رسانی به دبیرکل از دیدگاه و ارزیابی‌های خود، در مورد سؤالات ذیل اقدام نمایند:

الف - تلاش‌های صورت گرفته در سطوح ملی جهت تقویت امنیت اطلاعات و ارتقای همکاری‌های بین‌المللی

ب- محتوای مفاهیم و طرح‌های مذکور در گزارش‌های گروه کارشناسان دولتی.

۳- از دبیرکل درخواست می‌نماید که با مساعدت گروه کارشناسان دولتی که در سال ۲۰۱۹ و بر مبنای توزیع جغرافیایی عادلانه تشکیل می‌گردد، ضمن اجرا و پیشبرد ارزیابی‌ها و توصیه‌های مندرج در گزارش‌های فوق‌الذکر، با نگاهی به ارتقای درک عمومی و اجرای مؤثر به بررسی {مقولات ذیل} ادامه دهند: اقدامات همکاری‌جویانه احتمالی جهت مقابله با تهدیدات موجود و بالقوه در حوزه امنیت اطلاعات از جمله هنجارها، قوانین و اصول رفتار مسئولانه دولت‌ها، اقدامات اطمینان‌ساز و ظرفیت‌ساز و نحوه اعمال حقوق بین‌الملل در استفاده از فناوری‌های اطلاعات و ارتباطات توسط دولت‌ها، {و در نهایت} در اجلاس هفتادوششم مجمع عمومی، گزارشی از نتایج این بررسی‌ها را به انضمام ضمیمه‌ای شامل مشارکت‌های ملی کارشناسان دولتی شرکت‌کننده درباره نحوه اعمال حقوق بین‌الملل در استفاده از فناوری اطلاعات و ارتباطات ارائه نمایند؛

۴- از اداره امور خلع سلاح دبیرخانه سازمان ملل درخواست می‌نماید، با استفاده از منابع موجود و مشارکت‌های داوطلبانه به نمایندگی از اعضای گروه کارشناسان دولتی، {و} با همکاری سازمان‌های منطقه‌ای مربوط همانند اتحادیه آفریقا، اتحادیه اروپا، سازمان دولت‌های آمریکایی، سازمان امنیت و همکاری اروپا و مجمع منطقه‌ای جنوب شرق آسیا (آسی-آن)، مجموعه جلسات و نشست‌های مستشاری را جهت به اشتراک‌گذاری دیدگاه‌ها درباره موضوعات مندرج در دستورکار و در راستای پیشبرد اجلاس‌های گروه کارشناسان دولتی {برگزار نمایند؛

۵- از ریاست گروه کارشناسان دولتی درخواست می‌نماید دو نشست مشورتی غیررسمی دوازده روزه را به شکل باز به گونه‌ای سازماندهی نماید که {اولاً} تمامی دولت‌های عضو بتوانند در مباحث تعاملی درگیر شوند و نگاه‌های خود را به اشتراک بگذارند و {ثانیاً} ریاست گروه ملزم گردد تا {مباحث و دیدگاه‌های مطرح شده را} جهت بررسی به گروه کارشناسان دولتی انتقال دهد؛

۶- در خصوص درج موضوعی با عنوان «تحوالات در حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌الملل» در دستور کار موقت خود در اجلاس هفتاد و چهارم تصمیم می‌گیرد؛

نشست عمومی ۶۵ - ۲۲ (دسامبر ۲۰۱۸)

گفتار دو: گزارش‌های گروه کارشناسان دولتی

بندیک: گزارش اولین گروه کارشناسان دولتی ۲۰۰۵

ترجمه سند



مجمع عمومی

تاریخ انتشار: ۵ آگوست ۲۰۰۵

شماره قطعنامه: A/60/202

توزیع: عمومی

زبان: انگلیسی

اجلاس شصتم

دستور کار ۸۷

تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌الملل

گروه کارشناسان دولتی راجع به تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌الملل^۱

گزارش دبیرکل

فهرست مطالب:

۱- مقدمه

۲- مسائل سازمانی

پیوست: فهرست اعضای گروه کارشناسان دولتی راجع به تحولات حوزه اطلاعات و ارتباطات در

چارچوب امنیت بین‌الملل

مقدمه:

در قطعنامه ۵۸/۳۲ کمیته اول مورخ ۸ دسامبر ۲۰۰۳ با عنوان «تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌الملل» مجمع عمومی از دبیرکل درخواست کرد که تهدیدات بالفعل و بالقوه در حوزه امنیت اطلاعات و هرگونه امکان اقدامات همکاری جویانه برای مقابله با آن تهدیدات را در دستور کار قرار دهد. مجمع عمومی همچنین از دبیرکل درخواست کرد که با کمک گروه کارشناسان دولتی، مطالعه ای در مورد طرح‌های مرتبط بین‌المللی با هدف

1. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

تقویت امنیت سامانه‌های اطلاعاتی و ارتباطی جهانی انجام دهد. این گروه کارشناسی توسط دبیرکل سازمان ملل و بر اساس توزیع عادلانه جغرافیایی تعیین خواهند شد و نتایج مطالعات خود را در اجلاس شصتم مجمع عمومی ارائه خواهند کرد.

مسائل سازمانی:

مطابق با شرایط مندرج در قطعنامه، دبیرکل، گروه کارشناسان دولتی را از ۱۵ کشور عضو انتخاب کرد: بلاروس، برزیل، چین، فرانسه، آلمان، هند، اردن، مالزی، مالی، مکزیک، جمهوری کره، فدراسیون روسیه، آفریقای جنوبی، بریتانیای کبیر انگلستان و ایرلند شمالی و ایالات متحده آمریکا. فهرست کارشناسان در ضمیمه آمده است.

۳. گروه کارشناسان دولتی در سه جلسه حضور یافتند: نخستین جلسه از ۱۲ تا ۱۶ ژوئیه ۲۰۰۴ در مقر سازمان ملل متحد، دوم از ۲۸ مارس تا ۱ آوریل ۲۰۰۵ در ژنو و سوم از ۱۱ تا ۲۲ ژوئیه ۲۰۰۵ در مقر سازمان ملل متحد. گروه در اولین جلسه خود، به اتفاق آراء، آندری-وی کروتسیخ از فدراسیون روسیه را به‌عنوان رئیس انتخاب کرد.

۴. بخش پایش، پایگاه داده و اطلاعات دپارتمان امور خلع سلاح به‌عنوان دبیرخانه به گروه خدمت کرد.

۵. گروه طبق دستورالعمل ابلاغی خود بر اساس قطعنامه ۵۸/۳۲ دیدگاه‌ها را به شکل جامع و عمیق در زمینه تحولات در حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌المللی تبادل نمود. علاوه بر این، نظرها و دیدگاه‌های اخذ شده از سوی کشورهای عضو که در پاسخ به قطعنامه ۵۳/۷۰ مجمع عمومی مورخ ۴ دسامبر ۱۹۹۸، قطعنامه ۵۴/۴۹ مورخ ۱ دسامبر ۱۹۹۹، قطعنامه ۵۵/۲۸ مورخ ۲۰ نوامبر ۲۰۰۰، قطعنامه ۵۶/۱۹ مورخ ۲۹ نوامبر ۲۰۰۱، قطعنامه ۵۷/۵۳ مورخ ۲۲ نوامبر ۲۰۰۲، قطعنامه ۵۸/۳۲ مورخ ۸ دسامبر ۲۰۰۳ و قطعنامه ۵۹/۶۱ مورخ ۳ دسامبر ۲۰۰۴ بود، به ترتیب تحت عنوان «تحولات حوزه اطلاعات و ارتباطات راه دور در چارچوب امنیت بین‌المللی»، و همچنین مشارکت‌ها و یادداشت‌هایی در دسترس اعضای گروه قرار گرفت. با این حال، با توجه به پیچیدگی مسائل، هیچ توافق اجماعی در مورد

تهیه گزارش نهایی صورت نگرفت.

پیوست؛

فهرست اعضای گروه کارشناسان دولتی در حوزه تحولات اطلاعات و ارتباطات در چارچوب امنیت بین‌المللی:

۱. آقای والری وی. دیسپکالو: دستیار رئیس جمهوری بلاروس؛
۲. آقای مواریلو مارکز باربوزا: مشاور ویژه وزیر دفاع برزیل؛
۳. آقای وانگ قون: معاون مدیر کل، دپارتمان کنترل تسلیحات و خلع سلاح وزارت امور خارجه چین؛
۴. آقای وو هیتائو (جلسه اول): مشاور، دپارتمان کنترل تسلیحات و خلع سلاح وزارت امور خارجه چین؛
۵. خانم استفانی شوئر: دبیرخانه عمومی دفاع ملی فرانسه؛
۶. آقای توماس اسپهافر: مشاور اول، رئیس بخش کنترل تسلیحات متعارف دفتر امور خارجه فدرال آلمان؛
۷. آقای آرویند گوپتا: دبیرمشارکت؛ دبیرخانه شورای امنیت ملی هندوستان؛
۸. آقای سنجیان رنجان (جلسه اول): دبیر اول، نماینده دائمی هند در سازمان ملل متحد؛
۹. آقای بیرهر الخاصون (جلسه اول): دبیر اول، نماینده دائمی اردن در سازمان ملل متحد؛
۱۰. آقای عزام المدین: دبیر دوم، نماینده دائمی اردن در دفتر سازمان ملل متحد در ژنو؛
۱۱. آقای شاهنوری بن معین زین: مدیر، اداره توسعه فنی و فناوری اطلاعات بخش امنیت ملی، دفتر نخست وزیر مالزی؛
۱۲. آقای محد الاسان زاهدین: دستیار مدیر، اداره توسعه فنی و فناوری اطلاعات بخش امنیت ملی، دفتر نخست وزیر مالزی؛
۱۳. آقای چیکنا کیتا (جلسه اول): مشاور اول، نماینده دائمی مالی در سازمان ملل متحد؛
۱۴. آقای کالیو دومبیا: مشاور اول، نماینده دائمی مالی در سازمان ملل متحد؛

۱۵. آقای جورج آنتونیو اسپینوزا دوران: مدیر امنیت اطلاعات، پلیس پیشگیری فدرال مکزیک؛
۱۶. آقای لو کووان چول: مشاور وزیر، نماینده دائمی جمهوری کره در سازمان ملل؛
۱۷. آقای آندری وی کروتسکیخ: معاون مدیر. دپارتمان خلع سلاح و امور امنیتی وزارت امور خارجه. فدراسیون روسیه؛
۱۸. سرلشکر عاشوین سی. هوریوبنس: رئیس بخش فرماندهی و مدیریت سیستم‌های اطلاعات وزارت دفاع. آفریقای جنوبی؛
۱۹. آقای جیف اسمیت: رئیس تیم سیاستگذاری امنیت اطلاعات، وزارت تجارت و صنعت. پادشاهی بریتانیا و ایرلند شمالی؛
۲۰. خانم میشل مارکف: هماهنگ کننده ارشد حفاظت از زیرساخت‌های حیاتی بین‌المللی، دفتر امور سیاسی وزارت امور سیاسی نظامی. وزارت امور خارجه ایالات متحده آمریکا؛

بند دو: گزارش دومین گروه کارشناسان دولتی سال ۲۰۱۰

ترجمه سند



مجمع عمومی

تاریخ انتشار: ۳۰ جولای ۲۰۱۰

شماره قطعنامه: A/65/201

توزیع: عمومی

زبان: انگلیسی

اجلاس شصت و پنج

دستور کار ۹۴

تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین الملل
گروه کارشناسان دولتی راجع به تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین الملل

یادداشت دبیرکل؛

دبیرکل افتخار دارد که گزارش گروه کارشناسان دولتی را درباره تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین الملل تقدیم نماید. این گروه به موجب بند ۴ قطعنامه شماره ۶۰/۴۵ مجمع عمومی تأسیس شده است.

گزارش گروه کارشناسان دولتی درباره تحولات حوزه اطلاعات و ارتباطات در چارچوب

امنیت بین الملل

چکیده گزارش:

تهدیدات بالقوه و بالفعل در حوزه امنیت اطلاعات از جدی ترین چالش های قرن بیست و یکم به شمار می رود. این تهدیدات که از طیف گسترده ای از منابع ناشی می شوند و حضور خود را در فعالیت های مخرب نمایان می کنند، افراد، شرکت ها، زیرساخت های ملی و دولت ها را بی هیچ تمایزی مورد هدف قرار می دهند.

آثار مخرب و قابل توجه این تهدیدات، علیه امنیت عمومی، امنیت ملت ها و ثبات جهانی است که به جامعه بین المللی به عنوان یک کل به هم پیوسته وابسته می باشد.

این افزایش استفاده از فناوری‌های اطلاعات و ارتباطات (ICTs) در زیرساخت‌های حیاتی، آسیب‌پذیری‌ها و فرصت‌های جدیدی را برای تخریب ایجاد کرده است. به خاطر پیچیدگی به‌هم‌پیوسته ارتباطات و اینترنت، هر وسیله‌ای که از فناوری اطلاعات و ارتباطات استفاده می‌کند، به‌صورت فزاینده‌ای این قابلیت را دارد که هم به‌عنوان منبع و هم به‌عنوان هدف، به طرز ماهرانه‌ای، مورد سوءاستفاده قرار گیرد. از آنجایی که فناوری‌های اطلاعات و ارتباطات، ماهیت ذاتاً دوگانه‌ای دارند، استفاده گسترده از چنین فناوری‌هایی در تجارت الکترونیک، می‌تواند به‌عنوان تهدیدی علیه صلح بین‌الملل و امنیت ملی، مورد استفاده قرار گیرد.

پی بردن به منشأ اختلال و تعیین هویت عاملان یا انگیزه آن‌ها، می‌تواند دشوار باشد. عاملان این فعالیت‌ها را اغلب از روی اهداف، آثار یا دیگر مدارک و شواهد فرعی، می‌توان حدس زد. آن‌ها تقریباً در هر گوشه‌ای از جهان امکان فعالیت دارند. این ویژگی‌ها، امکان استفاده از فناوری اطلاعات برای فعالیت‌های تخریبی را تسهیل می‌کند. تردید و عدم اطمینان در نسبت دادن این فعالیت‌ها به عاملان آن‌ها و فقدان یک درک مشترک، خطر بی‌ثباتی و سوءبرداشت‌ها را به همراه داشته است. گزارش‌های فزاینده‌ای وجود دارد که نشان می‌دهد، دولت‌ها در حال توسعه فناوری‌های اطلاعاتی و ارتباطی هستند تا از آن به‌عنوان ابزار جنگی یا اطلاعاتی و یا برای اهداف سیاسی استفاده کنند. نگرانی در مورد افراد و سازمان‌ها نیز رو به افزایش است. مخصوصاً سازمان‌های جنایی که به‌عنوان پروکسی در فعالیت‌های برخاسته از طرف دیگران، فعالیت‌های مخرب دارند. رشد مهارت در فعالیت‌های مجرمانه و افزایش میزان این فعالیت‌ها، به‌صورت بالقوه باعث افزایش اقدامات مضر می‌شود. این در حالی است که نشانه‌هایی از استفاده تروریست‌ها از فناوری‌های اطلاعاتی و ارتباطاتی برای اجرای عملیات‌های خرابه‌کارانه وجود دارد که این امر ممکن است در آینده تشدید شود.

مقابله با چالش‌های قرن بیست‌ویکم به همکاری موفقیت‌آمیز بین شرکای همفکر آن بستگی دارد. در این خصوص، همکاری دوجانبه و چندجانبه میان دولت‌ها و همکاری بین بخش خصوصی و جامعه مدنی بسیار مهم است و تدابیر و اقدامات لازم برای ارتقای امنیت اطلاعات نیازمند همکاری گسترده بین‌المللی است تا بتواند مؤثر واقع شود. گزارش گروه کارشناسان

دولتی حامل توصیه‌هایی برای مذاکره بیشتر بین دولت‌ها در راستای کاهش خطرها و محافظت از زیرساخت‌های حیاتی در سطح ملی و بین‌المللی است.

فهرست مطالب:

پیشگفتار دبیرکل

معرفی نامه رئیس گروه

الف. مقدمه گزارش

ب. تهدیدات - خطرها و آسیب‌پذیری‌ها

ج. اقدامات همکاری جویانه

د. توصیه‌ها

پیوست

پیشگفتار دبیرکل

یک دهه پیش ما نمی‌توانستیم پیش‌بینی کنیم که فناوری اطلاعات و ارتباطات چگونه عمیقاً با زندگی روزمره ما عجین خواهد شد یا اینکه چقدر به آن‌ها وابسته می‌شویم. این فناوری‌ها یک جامعه بین‌المللی به هم پیوسته را در سطح جهانی ایجاد کرده‌اند و در حالی که این درهم‌تنیدگی و پیوستگی، منافع فراوانی به ارمغان می‌آورد، در عین حال آسیب‌پذیری‌ها و خطرهایی نیز به همراه خواهد داشت. پیشرفت قابل توجه در زمینه مقابله با کاربرد فناوری‌های جدید حاصل شده است. اما وظیفه ما سنگین است و ما فقط برای ایجاد هنجارها، قوانین و روش‌های همکاری‌های موردنیاز برای این محیط جدید اطلاعاتی شروع به اقدام کرده ایم. (مترجم: و این کار کافی نیست.)

با در نظر گرفتن این موضوع، من گروه کارشناسان دولتی را از ۱۵ کشور انتخاب کردم تا در زمینه تهدیدات بالفعل در این فضا مطالعه کنند و توصیه‌هایی برای مقابله با آن‌ها ارائه نمایند. من از رئیس گروه و کارشناسان به خاطر کار سخت و با دقت تشکر می‌کنم که توانسته‌اند این گزارش را تولید کنند که یک بیانیه کوتاه در مورد مشکلات و گام‌های ممکن بعدی است.

مجمع عمومی نقش مهمی در روند ارتقای امنیت فناوری‌های اطلاعاتی و ارتباطی در هر دو بعد ملی و بین‌المللی ایفا کرده است. گفتگو بین دولت‌های عضو، یک ضرورت برای ایجاد چشم‌انداز مشترک خواهد بود. همکاری‌های عملی نیز حیاتی است برای به اشتراک گذاشتن بهترین شیوه‌ها، تبادل اطلاعات و ظرفیت‌سازی در کشورهای در حال توسعه و کاهش خطر سوء تفاهم، که می‌تواند مانع توانایی جامعه بین‌المللی برای مدیریت رویدادهای مهم در فضای سایبر شود. این یک دستورکار غنی برای کارهای آتی است. گزارش حاضر در صدد برداشتن یک گام ابتکاری برای ایجاد یک چارچوب بین‌المللی برای امنیت و ثبات است که این فناوری‌های جدید نیاز دارند. من از تجزیه و تحلیل و توصیه‌های آن خطاب به کشورهای عضو و طیف گسترده مخاطبان در سراسر جهان تشکر می‌کنم.

معرفی نامه رئیس گروه

افتخار دارم که گزارش گروه کارشناسان دولتی را درباره تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌الملل را تقدیم نمایم. این گروه در سال ۲۰۰۹ به موجب بند ۴ قطعنامه شماره ۶۰/۴۵ مجمع عمومی تأسیس شده است. من به‌عنوان رئیس گروه خوشوقتم به اطلاع شما برسانم که اجماع در مورد این گزارش حاصل شده است.

در آن قطعنامه تحت عنوان «تحولات حوزه ارتباطات و اطلاعات در چارچوب امنیت بین‌الملل» مجمع عمومی درخواست کرده بود که گروه کارشناسان دولتی در سال ۲۰۰۹ بر اساس توزیع عادلانه جغرافیایی تشکیل شود تا به مطالعه در زمینه تهدیدات بالقوه و بالفعل در فضای امنیت اطلاعات و هر گونه اقدام ممکن همکاری‌جویانه جهت مقابله با این تهدیدات ادامه دهد. همچنین مطالعه در زمینه ایده‌های معطوف به تقویت امنیت سیستم‌های جهانی اطلاعات و ارتباطات نیز ادامه یابد. از دبیرکل خواسته شده بود که گزارش نتایج این مطالعه را در شصت‌وپنجمین اجلاس مجمع عمومی ارائه نماید.

مطابق مفاد قطعنامه، کارشناسان از ۱۵ کشور جهان انتخاب شدند: آمریکا، بلاروس، برزیل، چین، فرانسه، آلمان، هند، جمهوری کره، روسیه، آفریقای جنوبی، انگلیس، ایتالیا، قطر، اسرائیل

(رژیم صهیونیستی) و استونی. گروه طی دو سال، چهار جلسه تشکیل داد. جلسه اول از ۲۴ لغایت ۲۶ نوامبر ۲۰۰۹ در ژنو، جلسه دوم از ۱۱ لغایت ۱۵ ژانویه در نیویورک، جلسه سوم از ۲۱ تا ۲۵ ژوئن ۲۰۱۰ در ژنو و چهارمین جلسه از ۱۲ تا ۱۶ جولای در نیویورک برگزار شد. گروه، یک تبادل جامع و کامل دیدگاه ها در مورد تحولات حوزه ارتباطات و اطلاعات در چارچوب امنیت بین الملل را انجام داد. علاوه بر این، گروه، دیدگاه‌هایی را که در پاسخ‌های دریافتی از دولت‌های عضو اظهار شده بود مورد توجه قرار داد. این دیدگاه‌ها به ترتیب در پاسخ به قطعنامه‌های شماره ۶۰/۴۵، ۶۱/۵۴، ۶۲/۱۷ و ۶۳/۳۷ تحت عنوان «تحولات حوزه ارتباطات و اطلاعات در چارچوب امنیت بین الملل» اظهار شده بود. همچنین مشارکت‌ها و نظرهای مرتبط با موضوع که توسط خود اعضای گروه در دسترس قرار گرفته بود، مورد توجه قرار گرفت. گروه لازم می داند مراتب قدردانی خود را از مشارکت مؤسسه خلع سلاح سازمان ملل و دو نماینده آن جیمز لوئیس و کرسستین وینگارد که به‌عنوان مشاور در خدمت گروه بودند اعلام نماید. گروه همچنین مایل است مراتب قدردانی خود را از ایون بوچانان، افسر اطلاعات بخش اطلاع رسانی و تبلیغات اداره امور خلع سلاح دبیرخانه اعلام نماید که به‌عنوان دبیر در خدمت گروه بود. همچنین مراتب تشکر از دیگر مقامات دبیرخانه که به گروه کمک کردند.

امضاء اندری وی. کروتسکخ. رئیس گروه

الف. مقدمه

۱. تهدیدات بالقوه و بالفعل در حوزه امنیت اطلاعات یکی از جدی‌ترین چالش‌های قرن بیست‌ویکم به شمار می‌رود. این تهدیدها ممکن است باعث خسارات توجه‌پذیری به اقتصاد و امنیت ملی و بین‌المللی شود. تهدیدات از طیف متنوع و گسترده‌ای از منابع نشئت می‌گیرند و در فعالیت‌های غیرقانونی و مخرب که اشخاص، مشاغل، زیرساخت‌های ملی و موارد مشابه دولتی را هدف قرار می‌دهند، خود را نمایان می‌کنند. آن‌ها حامل خطرهای مهمی برای ایمنی عمومی، امنیت ملتها و ثبات کل جامعه بین‌المللی در سطح جهانی هستند.

۲. فناوری‌های اطلاعاتی و ارتباطی دارای ویژگی‌های منحصر به فردی هستند و این امر، مقابله با تهدیدات ناشی از آن را برای دولت‌ها و دیگر کاربران درگیر با آن، مشکل کرد. فناوری‌های اطلاعاتی، جهانی است و دسترسی گسترده‌ای درخصوص آن وجود دارد. آن‌ها اساساً دارای ماهیت نظامی و غیرنظامی به صورت توأمان هستند و اهدافی که مورد هدف آن‌ها قرار می‌گیرد تا حد زیادی به نیت کاربران آن بستگی دارد. در موارد متعددی، شبکه‌ها توسط مالکیت یا تصدی‌گری بخش خصوصی یا اشخاص اداره می‌شود. به خاطر پیچیدگی به هم پیوسته ارتباطات و اینترنت، هر گونه ابزار فناوری اطلاعات و ارتباطات به صورت فزاینده‌ای می‌تواند هم به‌عنوان ابزار و هم به‌عنوان هدف، مورد سوءاستفاده ماهرانه و پیچیده قرار گیرد. استفاده مخرب از فناوری‌های اطلاعاتی و ارتباطی به راحتی می‌تواند مخفی شود. اثبات و تعیین منشأ اختلال، هویت مرتکبان یا انگیزه آن‌ها می‌تواند مشکل باشد.

اغلب عوامل چنین فعالیت‌هایی تنها می‌توانند از هدف، اثر یا سایر شواهد حقیقی حدس زده شوند. عاملان تهدید می‌توانند با مصونیت قابل توجه از مجازات تقریباً در هر جایی عملیات کنند. این ویژگی‌ها استفاده از فناوری اطلاعات و ارتباطات را برای فعالیت‌های خرابه‌کارانه تسهیل می‌کند.

۳. با توجه به تبعات این تحولات بر امنیت بین‌الملل، مجمع عمومی سازمان ملل از دبیرکل درخواست کرد که با کمک گروه کارشناسان دولتی به مطالعه و بررسی در هر دو زمینه تهدیدات حوزه امنیت اطلاعات و مفاهیم بین‌المللی مربوط بپردازد و اقدامات همکاری‌جویانه احتمالی را که می‌تواند به تقویت امنیت جهانی اطلاعات و سیستم‌های ارتباطی منجر شود پیشنهاد نماید.

ب. تهدیدات، خطر ها و آسیب پذیری ها

۴. شبکه جهانی فناوری اطلاعات و ارتباطات (ICT) به عرصه فعالیت های مخرب تبدیل شده است. انگیزه این اقدامات خرابه کارانه می تواند طیف گسترده ای را شامل شود. از نمایش یک خودنمایی فنی گرفته تا سرقت پول و اطلاعات و حتی درگیری یک دولت. منبع این تهدیدات از بازیگران غیردولتی مثل مجرمان و به صورت بالقوه تروریست ها گرفته تا خود دولت ها را دربرمی گیرد. فناوری های اطلاعاتی و ارتباطی می توانند برای نابود کردن منابع اطلاعاتی و زیرساخت ها به کار روند. زیرا آن ها ذاتاً ماهیت دوگانه دارند. همان فناوری اطلاعات و ارتباطات که از تجارت الکترونیک قوی پشتیبانی می کند می تواند برای تهدید صلح بین المللی و امنیت ملی استفاده شود. ۵. بسیاری از ابزارها و روش های مخرب، ریشه در تلاش های مجرمانه و هکرها دارند. افزایش پیچیدگی و سطح فعالیت های مجرمانه موجب افزایش بالقوه اقدامات زیان آور شده است.

۶. تاکنون چند نشانه از تلاش تروریست ها برای به خطر انداختن یا از کار انداختن زیرساخت های اطلاعاتی و ارتباطی یا انجام عملیات هایی با استفاده از فناوری های اطلاعاتی و ارتباطی به دست آمده است که ممکن است این اقدامات را در آینده تشدید کنند. در حال حاضر تروریست ها، اغلب با تکیه بر این فناوری ها، درصد ارتباط گیری و جمع آوری اطلاعات، استخدام، سازماندهی، تبلیغ عقاید و اقدامات و درخواست کمک مالی هستند. اما در نهایت می توانند از فناوری اطلاعات و ارتباطات برای حمله استفاده کنند.

۷. گزارش های رو به افزایش حاکی از آن است که دولت ها در حال توسعه فناوری های اطلاعاتی و ارتباطی به عنوان ابزار جنگ و جاسوسی یا با اهداف سیاسی هستند. عدم اطمینان در خصوص انتساب و فقدان درک مشترک در مورد رفتار قابل قبول دولت می تواند خطر بی ثباتی و سوء تفاهم را ایجاد کند.

۸. افزایش نگرانی در مورد افراد، گروه ها یا سازمان ها و از جمله سازمان های جنایتکاری است که از طرف دیگران به عنوان پروکسی در فعالیت های برخط مخرب فعالیت می کنند. این پروکسی ها چه با انگیزه های مالی و چه غیرمالی می توانند ارائه دهنده یکسری از خدمات مخرب به بازیگران دولتی و غیر دولتی باشند.

۹. استفاده روزافزون از فناوری اطلاعات و ارتباطات در زیرساخت‌های حساس، آسیب‌پذیری‌های جدیدی ایجاد می‌کند و فرصت‌های اختلال جدیدی به وجود می‌آورد، همان‌گونه که استفاده روزافزون از دستگاه‌های ارتباطی همراه (موبایل) و خدمات وب نیز همین وضعیت را بوجود می‌آورد.

۱۰. دولت‌ها همچنین نگران آن هستند که زنجیره تأمین فناوری اطلاعات و ارتباطات می‌تواند متأثر از روش‌ها و راه‌ها دگرگون شوند، به‌نحوی که استفاده عادی، امن و قابل اطمینان از فناوری اطلاعات و ارتباطات (ICT) تحت تأثیر قرار دهد. ورود عملکردها و کارکردهای مخرب پنهانی در فناوری اطلاعات و ارتباطات می‌تواند اعتماد به محصولات و خدمات و اعتماد به تجارت را کاهش دهد و بر امنیت ملی تأثیر گذارد.

۱۱. سطوح مختلف و متفاوت کشورها در برخورداری از امنیت و ظرفیت‌های فناوری اطلاعات و ارتباطات، آسیب‌پذیری شبکه جهانی را افزایش داده است. تفاوت‌های موجود در قوانین ملی و شیوه‌های عملی کشورها، ممکن است موجب ایجاد چالش‌هایی در مسیر دستیابی به یک محیط دیجیتال امن و انعطاف‌پذیر باشند.

ج. اقدامات همکاری جویانه

۱۲. خطرهای مرتبط با شبکه به‌هم پیوسته جهانی، نیازمند پاسخی هماهنگ است. کشورهای عضو، طی یک دهه گذشته، نیاز به همکاری بین‌المللی در مقابل تهدیدات در حوزه امنیت فناوری اطلاعات و ارتباطات به‌منظور مبارزه با سوءاستفاده مجرمانه از فناوری اطلاعات، ایجاد یک فرهنگ جهانی امنیت سایبری و اتخاذ اقدام‌های ضروری دیگر که بتواند خطرها را کاهش دهد، مکرراً مورد تأیید قرار داده‌اند.

۱۳. در طول دهه گذشته، تلاش‌هایی برای مبارزه با تهدیدات سایبری در سطح بین‌المللی انجام شده است، به‌ویژه در سازمان همکاری شانگ‌های، سازمان کشورهای آمریکایی، مجمع همکاری‌های اقتصادی آسیا - اقیانوسیه، مجمع منطقه‌ای جنوب شرق آسیا (ASEAN) (جامعه اقتصادی کشورهای غرب آفریقا، اتحادیه آفریقا، اتحادیه اروپا، سازمان امنیت و همکاری در اروپا و شورای اروپا و همچنین تلاش‌های دوجانبه بین کشورها.

۱۴. ابعاد غیرمجرمانه نگرانی بین‌المللی نیز باید به شکل مناسب مورد توجه قرار گیرند. این موارد شامل خطر سوءبرداشت ناشی از فقدان درک مشترک در مورد هنجارهای بین‌المللی مربوط به استفاده دولت از فناوری اطلاعات و ارتباطات (ICT) است که می‌تواند بر مدیریت بحران در مواقع بروز حوادث عمده تأثیر بگذارد. این مباحث به خاطر پیچیدگی اقدامات طراحی شده برای ارتقای همکاری‌های بین‌المللی است، آن‌هم در جایی که امکان آن وجود دارد. چنین اقداماتی همچنین می‌تواند برای به اشتراک گذاشتن بهترین شیوه‌ها، مدیریت حوادث، اعتمادسازی، کاهش خطر و افزایش شفاف‌سازی و پایداری باشد.

۱۵. از آنجا که فعالیت‌های مخرب با استفاده از فناوری‌های اطلاعاتی و ارتباطی در حال پیچیده‌تر شدن و خطرناک‌تر شدن هستند، واضح است که هیچ دولتی به تنهایی قادر به مقابله با این تهدیدات نیست. مواجهه با چالش‌های قرن بیست‌ویکم به همکاری موفقیت‌آمیز بین شرکای همفکر بستگی دارد. همکاری بین خود دولت‌ها و بین دولت‌ها و بخش خصوصی و جامعه مدنی مهم است و اقدامات لازم جهت ارتقای امنیت اطلاعات نیازمند همکاری گسترده بین‌المللی است تا بتواند مؤثر باشد. بنابراین، جامعه بین‌المللی باید موضوع نیاز به اقدامات و سازوکارهای همکاری‌جویانه را بررسی کند.

۱۶. توافقنامه‌های موجود حاوی هنجارهای مربوط به استفاده از فناوری اطلاعات و ارتباطات توسط دولت‌هاست. با توجه به ویژگی‌های منحصر به فرد ICT ها، هنجارهای جدید در طول زمان می‌توانند توسعه یابند.

۱۷. ظرفیت‌سازی برای دستیابی به موفقیت در تضمین امنیت فناوری اطلاعات و ارتباطات جهانی و در کمک به کشورهای در حال توسعه در راستای تلاششان برای تقویت امنیت زیرساخت‌های اطلاعاتی حیاتی ملی آن‌ها و پر کردن شکاف فعلی در امنیت فناوری اطلاعاتی و ارتباطی اهمیت حیاتی دارد. همکاری نزدیک بین‌المللی نیازمند ظرفیت‌سازی در کشورهای است که ممکن است نیازمند کمک جهت پرداختن به امنیت فناوری اطلاعات و ارتباطات خود باشند.

د. توصیه‌ها

۱۸. با در نظر گرفتن تهدیدات موجود و بالقوه، خطرها و آسیب‌پذیری‌ها در حوزه امنیت اطلاعات، آن مفید می‌داند توصیه کند که قدم‌های بیشتری برای توسعه اعتمادسازی و سایر اقدامات لازم جهت کاهش خطر سوء برداشت ناشی اختلالات فناوری اطلاعات و ارتباطات برداشته شود:

- * گفتگوهای بیشتر میان کشورها درباره هنجارهای مرتبط با استفاده کشورها از فناوری اطلاعات و ارتباطات، به منظور کاهش خطر جمعی و حفاظت از زیرساخت‌های مهم ملی و بین‌المللی؛
- * اقدامات اعتمادساز و اقدامات در جهت ایجاد ثبات و کاهش خطر برای مقابله با پیامدهای استفاده دولت از فناوری اطلاعات و ارتباطات، از جمله تبادل دیدگاه‌های ملی در مورد استفاده از فناوری اطلاعات و ارتباطات در جنگ؛

- * تبادل اطلاعات در ارتباط با قانون ملی، اطلاعات ملی و راهبردهای امنیتی فناوری‌های ارتباطی، سیاست‌ها و اتخاذ بهترین شیوه‌های عملی؛

- * شناسایی اقدامات برای حمایت از ظرفیت‌سازی در کشورهای کمتر توسعه‌یافته؛

- * یافتن امکانات و راه‌حلی برای تشریح دقیق واژگان و تعاریف مشترک مربوط به قطعنامه ۶۴/۲۵ مجمع عمومی سازمان ملل.

فهرست اعضای گروه کارشناسان دولتی در زمینه تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌المللی

۱- آقای ولادیمیران. گراسیمویچ. رئیس گروه امنیت بین‌المللی و کنترل تسلیحات وزارت امور خارجه بلاروس؛

۲- آقای الکساندر پونومارو (جلسه سوم). مشاور نماینده دائمی جمهوری بلاروس در دفتر سازمان ملل متحد در ژنو؛

۳- آقای الکساندر ماریانو فیتوسا. فرمانده در نیروی دریایی برزیل، دبیرخانه سیاستگذاری، راهبرد و امور بین‌الملل وزارت دفاع برزیل؛

۴- آقای لی سونگ (جلسات اول و دوم). معاون مدیر کل دپارتمان کنترل تسلیحات و خلع

- سلاح وزارت امور خارجه چین؛
- ۵- آقای کان یانگ (جلسات سوم و چهارم). معاون مدیر کل دپارتمان کنترل تسلیحات و خلع سلاح وزارت امور خارجه چین؛
- ۶- آقای لینار ویک استاد کالج فناوری اطلاعات استونی؛
- ۷- آقای ایمر سایمون.فرانسه؛
- ۸- آقای گرگور کوبل. رئیس بخش کنترل تسلیحات متعارف دفتر امور خارجه فدرال آلمان؛
- ۹- آقای بی.جی.سرینات. مدیر ارشد تیم واکنش اضطراری کامپیوتر هند گروه فناوری اطلاعات هندوستان؛
- ۱۰- خانم رادیکا رادیان گوردون. مدیر دپارتمان کنترل تسلیحات وزارت امور خارجه رژیم صهیونیستی؛
- ۱۱- آقای وینچنزو دلا کورت (جلسات اول و سوم). مدیر بخش امنیت ارتباطات شورای وزیران ایتالیا؛
- ۱۲- آقای والتر مککیا (جلسات دوم و چهارم). امنیت ارتباطات شورای وزیران ایتالیا؛
- ۱۳- آقای رشید المحمدی (اولین جلسه) نیروی زمینی قطر؛
- ۱۴- آقای سعدام. آر.الکعبی سرهنگ دوم (مهندس) وزارت دفاع قطر؛
- ۱۵- آقای لو کووان چول. سفیر. وزارت امور خارجه و بازرگانی جمهوری کره؛
- ۱۶- آقای آندری وی. کروتسکیخ. معاون مدیر دپارتمان چالش‌ها و تهدیدات جدید. وزارت امور خارجه. فدراسیون روسیه؛
- ۱۷- خانم پالزا باندا (جلسه اول). معاون مدیر، بخش مدیریت ارتباطات اینترنتی. آفریقای جنوبی؛
- ۱۸- ژنرال ماریو سیلویینو برازلی. افسر فناوری اطلاعات دولت. وزارت دفاع آفریقای جنوبی؛
- ۱۹- آقای گاوین ویلیس. تیم روابط بین‌الملل. نهاد ملی فنی بیمه اطلاعات (CESG) بریتانیا و ایرلند شمالی؛
- ۲۰- خانم میشل گ. مارکوف. مشاور ارشد سابق اداره امور سایبر وزارت امور خارجه ایالات متحده آمریکا.

بند سه: گزارش سومین گروه کارشناسان دولتی سال ۲۰۱۳

ترجمه سند



مجمع عمومی

تاریخ انتشار: ۲۴ ژوئن ۲۰۱۳

شماره قطعنامه: A/68/98

توزیع: عمومی

زبان: انگلیسی

اجلاس شصت و هشت

دستور کار ۹۴

تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین الملل
گروه کارشناسان دولتی درباره تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین الملل

یادداشت دبیرکل؛

دبیرکل افتخار دارد که گزارش گروه کارشناسان دولتی را درباره تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین الملل را تقدیم نماید. این گروه به موجب بند ۴ قطعنامه شماره ۶۶/۲۴ مجمع عمومی تأسیس شده است.

چکیده گزارش:

فناوری‌های اطلاعات و ارتباطات (ICTs) محیط امنیت بین المللی را تغییر داده است. این فناوری‌ها منافع اقتصادی و اجتماعی بسیار زیادی را به همراه می‌آورد. همچنین فناوری‌های اطلاعاتی و ارتباطی می‌توانند برای اهدافی به کار روند که مغایر با صلح و امنیت بین المللی هستند و موجب ایجاد یک روند افزایشی در بروز خطرها در سال‌های اخیر شده‌اند. این فناوری‌ها همچنین می‌توانند برای ارتکاب جرم و سایر فعالیت‌های مخرب مورد استفاده قرار گیرند. سوءاستفاده از فناوری‌های اطلاعاتی و ارتباطی توسط عواملی صورت می‌گیرد که در اقدامات خود، اغلب از مصونیت برخوردارند و می‌توانند به راحتی پنهان شوند، بنابراین نسبت دادن یک جرم به مرتکب آن، می‌تواند امر دشواری باشد. این امر محیطی را ایجاد می‌کند که اتخاذ رفتارهای پیچیده با استفاده از فناوری‌های اطلاعاتی و ارتباطی را به صورت فزاینده‌ای تسهیل می‌نماید.

کشورهای عضو، نیاز به اقدامات مشترک جمعی در مقابل تهدیدات ناشی از سوءاستفاده از فناوری‌های اطلاعاتی و ارتباطی را بارها مورد تأیید قرار داده‌اند. همکاری بین‌المللی برای کاهش خطرها و افزایش امنیت ضروری است. پیشرفت بیشتر همکاری در سطح بین‌المللی، مستلزم اقداماتی برای فراهم آوردن یک محیط صلح‌آمیز، امن، آزاد و در دسترس برای فناوری‌های اطلاعاتی و ارتباطی است. اقدامات همکاری جویانه که می‌تواند ثبات و امنیت را افزایش دهد شامل هنجارها، قوانین و اصول مربوط به رفتار مسئولانه توسط دولت‌ها، اقدامات داوطلبانه برای افزایش شفاف‌سازی و اقدامات مربوط به اعتمادسازی، مسئولیت‌پذیری و ظرفیت‌سازی میان کشورها می‌باشد. دولت‌ها باید رهبری و هدایت این تلاش‌ها را بر عهده داشته باشند، اما همکاری مؤثرتر، زمانی حاصل خواهد شد که بخش خصوصی و جامعه مدنی نیز در این روند مشارکت نمایند. باتوجه به جامعیت چالش، با در نظر گرفتن تهدیدات موجود و بالقوه و با مبنا قرار دادن توصیه‌های مندرج در گزارش گروه کارشناسان دولتی [منظور دومین گروه کارشناسان دولتی است.]، در ارتباط با تحولات در زمینه اطلاعات و مخابرات در چارچوب امنیت بین‌المللی مربوط به در ژوئیه ۲۰۱۰ (۲۰۱/۶۵/A) گروه کارشناسان دولتی [منظور سومین گروه کارشناسان دولتی است.] در گزارش حاضر، توصیه‌های خود را برای ایجاد صلح و ثبات در استفاده دولت‌ها از فناوری‌های اطلاعاتی و ارتباطی ارائه می‌نماید.

این گزارش حاکی از آن است که به‌کارگیری هنجارهای حاصل از حقوق بین‌الملل موجود که مرتبط با استفاده دولت‌ها از فناوری‌های اطلاعاتی و ارتباطی است، امری ضروری در راستای کاهش خطرهایی است که متوجه صلح، امنیت و ثبات بین‌المللی است. این گزارش، مطالعات بیشتری را توصیه می‌کند تا درک مشترکی در ارتباط با چگونگی کاربست این قواعد در رفتار دولت‌ها و نحوه استفاده آن‌ها از فناوری‌های اطلاعاتی و ارتباطی به‌دست آید. این گزارش باتوجه به ویژگی‌های منحصر به فرد فناوری‌های اطلاعاتی و ارتباطی بیان می‌کند که هنجارهای مکمل را می‌توان در طول زمان ایجاد نمود.

نتایج گزارش گروه، منعکس‌کننده آن است که برای ایجاد محیط آزاد، امن، صلح‌آمیز و دسترس‌پذیر، در حوزه فناوری اطلاعات و ارتباطات، اعمال حقوق بین‌الملل مخصوصاً منشور

ملل متحد نه تنها لازم است بلکه برای حفظ صلح و ثبات در این حوزه، امری ضروری می‌باشد. همچنین این گروه به این نتیجه رسیدند که مباحث مربوط به استقلال و حاکمیت کشورها و هنجارها و اصول بین‌المللی ناشی از آن، در فضای فناوری‌های اطلاعاتی و ارتباطی نیز قابل اعمال است.

این مباحث بر رفتار و عملکرد دولت‌ها در حوزه فناوری اطلاعات و ارتباطات اعم از فعالیت دولت‌ها و صلاحیت آن‌ها بر زیرساخت‌های این فناوری در قلمرو این دولت‌ها نیز اعمال می‌شود. بنابراین دولت‌ها باید به تعهدات بین‌المللی خود درخصوص اقدامات غیرقانونی که در عرصه بین‌المللی به آن‌ها منتسب می‌شود، عمل نمایند. [منظور این است که حقوق و تکالیفی که دولت‌ها در جهان واقعی و در عرصه بین‌الملل دارای آن هستند، در فضای سایبر نیز دارای همان حقوق و تکالیف می‌باشند.] این گزارش برای ایجاد مسئولیت‌پذیری، شفاف‌سازی و اعتمادسازی و همچنین همکاری‌های بین‌المللی، توصیه‌هایی را در قالب اقدامات داوطلبانه ارائه می‌دهد که در راستای ظرفیت‌سازی برای امنیت فناوری اطلاعات و ارتباطات مخصوصاً در کشورهای در حال توسعه می‌باشد.

این گروه به‌منظور پیشبرد این اقدامات، برگزاری منظم گفتگوهای سازمانی درباره این مسائل تحت نظر و حمایت سازمان ملل متحد یا سایر مجامع را توصیه می‌نماید. دولت‌های عضو باید توجه فعالانه‌ای به این گزارش داشته باشند و چگونگی پیگیری و دنبال کردن این توصیه‌ها در راستای توسعه بیشتر و اجرای آن‌ها را مورد نظر قرار دهند.

فهرست مطالب:

پیشگفتار دبیرکل

معرفی نامه رئیس گروه

الف. مقدمه گزارش؛

ب. همکای برای ایجاد محیط صلح‌آمیز، امن، انعطاف‌پذیر و باز برای محیط فناوری اطلاعات و ارتباطات؛

ج. توصیه‌هایی در زمینه هنجارها، قوانین و اصول رفتار مسئولانه دولت‌ها؛

د. توصیه‌هایی در زمینه اقدامات اعتمادساز و تبادل اطلاعات؛

ه. توصیه‌هایی در زمینه اقدامات ظرفیت‌ساز؛

و. نتیجه؛

پیوست

پیشگفتار دبیر کل

فناوری اطلاعات و ارتباطات در تاروپود زندگی روزمره مردم تنیده شده است. در حالی که همه کشورها مزایای فراوان فناوری اطلاعات و ارتباطات (ICT) را درک و احساس می‌کنند، این تشخیص نیز به صورت گسترده‌ای وجود دارد که سوءاستفاده از آن موجب به خطر افتادن صلح و امنیت بین‌المللی می‌شود.

این گزارش حاوی توصیه‌هایی است که توسط گروهی از کارشناسان دولتی متشکل از ۱۵ کشور تهیه شده است تا به تهدیدات موجود و بالقوه که از طریق استفاده از فناوری اطلاعات و ارتباطات (ICT) متوجه کشورها، پروکسی‌های آن‌ها یا بازیگران غیر دولتی است بپردازد. این گزارش بر اساس توصیه‌های سال ۲۰۱۰ گروه کارشناسان دولتی پیشین تنظیم شده است که نیاز به کار بیشتر در مورد هنجارها، راه‌های افزایش اعتماد و اقدامات مربوط به ظرفیت‌سازی را مورد تأکید قرار داده بود.

من فکر می‌کنم که تمرکز گزارش روی محوریت منشور سازمان ملل و حقوق بین‌الملل و همچنین اهمیت عملکرد مسئولانه دولت‌هاست. توصیه‌ها راه پیش رو برای تحکیم امنیت چهارچوب فعلی حقوق بین‌الملل را نشان می‌دهد.

و مفاهمه‌ای است که روابط دولت‌ها را راهبری می‌کند و برای صلح و امنیت بین‌الملل زیربنایی ایجاد می‌کند.

همان‌طور که این گروه اشاره می‌کند، سازمان ملل متحد نقش مهمی را در ارتقای گفتگو بین کشورهای عضو پیرامون موضوع امنیت در استفاده از فناوری اطلاعات و ارتباطات و در توسعه بیشتر همکاری‌های بین‌المللی در این زمینه ایفا می‌کند.

من از رئیس گروه و کارشناسان برای انجام کار دشوار تشکر می‌کنم. این گزارش پایه‌ای قوی برای تلاش‌های آینده جهت افزایش امنیت و ثبات در استفاده از فناوری اطلاعات و ارتباطات فراهم می‌کند. من توصیه‌های گروه به مجمع عمومی را به‌عنوان گامی مهم در تلاش جهانی برای به حداقل رساندن خطرهای مرتبط با فناوری اطلاعات و ارتباطات در عین بهینه‌سازی ارزش آن‌ها می‌ستایم.

معرفی نامه رئیس گروه: ۷ ژوئن ۲۰۱۳

مفتخرم که گزارش گروه کارشناسان دولتی را در مورد تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌الملل تقدیم کنم. گروه با استناد به بند ۴ قطعنامه ۶۶/۲۴ مجمع عمومی تعیین شد. من به‌عنوان رئیس گروه خرسندم که به اطلاع شما برسانم که این گزارش با اجماع نظر اعضاء تهیه شده است.

مجمع عمومی در قطعنامه خود تحت‌عنوان تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌الملل درخواست نمود که یک گروه از کارشناسان دولتی براساس توزیع عادلانه جغرافیایی در سال ۲۰۱۲ تشکیل شود تا به مطالعه در زمینه تهدیدات موجود و بالقوه در حوزه امنیت اطلاعات و ارتباطات و اقدامات همکاری‌جویانه ممکن برای مقابله با آن‌ها ادامه دهد که شامل هنجارها، قوانین و اصول رفتار مسئولانه دولت‌ها و اقدامات اعتمادساز باتوجه‌به فضای اطلاعات می‌باشد. همچنین شامل طرح‌هایی با هدف تقویت امنیت سیستم‌های جهانی مندرج در قطعنامه، کارشناسان از ۱۵ کشور انتخاب شدند: آرژانتین، استرالیا، بلاروس، کانادا، چین، مصر، استونی، فرانسه، آلمان، هندوستان، اندونزی، ژاپن، فدراسیون روسیه، انگلیس و ایالات متحده آمریکا. اسامی کارشناسان در ضمیمه گزارش آمده است.

گروه کارشناسان دولتی یک تبادل نظر جامع و عمیق در مورد تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌الملل انجام داد. این گروه سه جلسه برگزار کرد: اولین جلسه از ۶ تا ۱۰ آگوست ۲۰۱۲ در مقر سازمان ملل متحد در نیویورک، جلسه دوم از ۱۴ تا ۱۸ ژانویه ۲۰۱۳ در ژنو و جلسه سوم از ۳ تا ۷ ژوئن ۲۰۱۳ در مقر سازمان ملل متحد برگزار شد. گروه لازم می‌داند مراتب قدردانی خود را از مؤسسه تحقیقات خلع سلاح سازمان ملل که به

عنوان مشاور به گروه خدمت رسانی کرد ابراز نماید که توسط جیمز لوئیس و کرسستین ویگنارد (جلسات دوم و سوم) نمایندگی شد. گروه همچنین مراتب قدردانی خود را از ایون بوچانان از دفتر امور خلع سلاح سازمان ملل ابراز می دارد که به عنوان دبیر گروه خدمت رسانی کرد.

امضاء دبورا استوکس رئیس گروه

الف. مقدمه:

۱. استفاده از فناوری‌های اطلاعات و ارتباطات (ICT) محیط امنیتی بین‌المللی را تغییر داده است. این فناوری‌ها مزایای اقتصادی و اجتماعی فراوانی را به همراه می‌آورد؛ آن‌ها همچنین می‌توانند برای مقاصدی که با صلح و امنیت بین‌المللی سازگار نیستند استفاده شوند. در سال‌های اخیر افزایش فزاینده خطر به چشم می‌خورد؛ زیرا فناوری اطلاعات و ارتباطات برای جرایم و انجام فعالیت‌های مخرب و غیر قانونی مورد استفاده قرار می‌گیرد.

۲. همکاری بین‌المللی برای کاهش خطر و افزایش امنیت ضروری است. به همین علت مجمع عمومی، از دبیرکل درخواست نمود با کمک گروه از کارشناسان دولتی با ادامه بررسی اقدامات ممکن جهت همکاری برای حل تهدیدات موجود و بالقوه (قطعه‌نامه ۶۶/۲۴) برای ارائه گزارش به جلسه شصت و هشتم مجمع عمومی اقدام نماید. گزارش حاضر بر اساس گزارش سال ۲۰۱۰ (A/۶۵/۲۰۱) گروه قبلی کارشناسان دولتی بنا شده است که این موضوع را بررسی کرده است و توصیه‌هایی را برای کارهای آینده ارائه می‌دهد.

۳. گزارش سال ۲۰۱۰، گفتگوهای بیشتر بین کشورها در مورد هنجارهای مربوط به استفاده دولت از فناوری اطلاعات و ارتباطات برای کاهش خطر جمعی و حفاظت از زیرساخت‌های حساس ملی و بین‌المللی را توصیه کرده است. این گزارش خواستار اقدامات لازم برای ایجاد اعتمادسازی، ثبات و کاهش خطر شده است؛ از جمله مبادله دیدگاه‌های ملی در مورد استفاده از

فناوری اطلاعات و ارتباطات در جنگ، تبادل اطلاعات در مورد قوانین ملی، راهبردها، سیاست‌ها، فناوری‌ها و بهترین شیوه‌های مربوط به امنیت ICT. گزارش سال ۲۰۱۰ بر اهمیت ظرفیت‌سازی در کشورهایی که ممکن است برای ایجاد امنیت فناوری اطلاعات و ارتباطات خود به کمک نیاز داشته باشند، تأکید کرده، پیشنهاد می‌کند که کار بیشتری برای ایجاد واژگان و تعاریف مشترک صورت پذیرد.

۴. طرح‌های متعدد دوجانبه، منطقه‌ای و چندجانبه از سال ۲۰۱۰ اهمیت فزاینده امنیت بیشتر فناوری اطلاعات و ارتباطات، کاهش خطرهای امنیتی عمومی، بهبود امنیت کشورها و افزایش ثبات جهانی را به صورت روزافزونی برجسته کرده‌اند. به نفع همه کشورهاست که از فناوری اطلاعات و ارتباطات برای اهداف صلح‌آمیز استفاده کنند. کشورها همچنین منافع مشترک در پیشگیری از مناقشات ناشی از استفاده از فناوری اطلاعات و ارتباطات دارند. درک مشترک در مورد هنجارها، قواعد و اصول قابل اعمال بر استفاده از فناوری اطلاعات و ارتباطات توسط دولت و اقدامات داوطلبانه اعتمادساز می‌تواند نقش مهمی در پیشبرد صلح و امنیت داشته باشد. فعالیت جامعه بین‌المللی برای حل این چالش که متوجه صلح و امنیت بین‌المللی است، گام اول در این مسیر محسوب می‌شود، اما تعدادی از اقدامات مربوط به هنجارها، قواعد و اصول رفتار مسئولانه دولت‌ها نیز می‌توانند مورد توجه بیشتری قرار گیرند.

تهدیدات، خطرها و آسیب‌پذیری‌ها

۵. فناوری‌های اطلاعاتی و ارتباطی، فناوری‌های دارای کاربرد دوگانه ای هستند که می‌توانند برای هر دو نوع هدف مشروع و مخرب به کار روند. هر گونه وسیله مربوط به فناوری اطلاعات و ارتباطات می‌تواند منبع یا هدف استفاده سوء قرار گیرد. استفاده مخرب از فناوری اطلاعات و ارتباطات به راحتی می‌تواند پنهان شود و انتساب به یک عامل و مرتکب می‌تواند سخت باشد. همین امر باعث افزایش استثمار پیچیده و زیرکانه توسط بازیگرانی شده است که اغلب با برخورداری از مصونیت، عملیات می‌کنند.

۶. تهدید علیه اشخاص، مشاغل، زیرساخت‌های ملی و دولت‌ها، حادثه و حوادث نیز مخرب‌تر شده است. منابع این تهدیدات شامل بازیگران دولتی و غیردولتی است. علاوه بر آن، اشخاص، گروه‌ها یا سازمان‌ها از جمله سازمان‌های جنایی می‌توانند به نمایندگی از دولت‌ها و در قالب پروکسی به اقدامات مخرب در حوزه فناوری اطلاعات و ارتباطات مبادرت کنند. قابلیت توسعه و گسترش ابزارها و تکنیک‌های مخرب پیچیده، مانند بات‌نت‌ها، توسط بازیگران دولتی و غیر دولتی، ممکن است باعث افزایش خطر ارتکاب اشتباه و سهو در انتساب گردد. فقدان درک مشترک در مورد رفتار قابل قبول دولت‌ها در ارتباط با استفاده از فناوری اطلاعات و ارتباطات موجب افزایش خطر علیه صلح و امنیت بین‌المللی شده است.

۷. گروه‌های تروریستی از فناوری‌های اطلاعات و ارتباطات برای اهداف ذیل استفاده می‌کنند: ارتباط‌گیری، جمع‌آوری اطلاعات، استخدام، سازمان‌دهی، برنامه‌ریزی و هماهنگی حملات، ترویج عقاید و اقدامات و درخواست کمک. اگر چنین گروه‌هایی به ابزارهای حمله دسترسی پیدا کنند، می‌توانند فعالیت‌های مخرب در حوزه فناوری اطلاعات و ارتباطات داشته باشند.

۸. دولت‌ها نگران‌اند که قرار دادن امکانات مضر به صورت مخفی روی فناوری‌های اطلاعاتی و ارتباطی می‌تواند استفاده امن و مطمئن از این فناوری‌ها و زنجیره تأمین فناوری برای تولیدات و خدمات را تحت تأثیر قرار دهد و موجب کاهش اعتماد در تجارت و تخریب امنیت ملی شود.

۹. توسعه استفاده از فناوری‌هایی اطلاعاتی و ارتباطی در زیرساخت‌های حساس و سامانه‌های کنترل صنعتی، امکانات جدیدی را برای ایجاد اختلال مهیا کرده است. رشد سریع در استفاده از ابزارهای ارتباطی موبایل، خدمات وب، شبکه‌های اجتماعی و خدمات رایانش ابری موجب افزایش چالش‌های امنیتی شده است.

۱۰. دارا بودن سطوح مختلف ظرفیت امنیت فناوری اطلاعات و ارتباطات بین کشورهای

مختلف، می‌تواند موجب افزایش آسیب‌پذیری در دنیای به هم پیوسته شود. بازیگران مخرب و مضر بدون توجه به جایی که در آن قرار دارند از شبکه‌ها بهره‌برداری می‌کنند. اختلاف در قوانین ملی، مقررات و شیوه‌های مربوط به استفاده از فناوری اطلاعات و ارتباطات موجب تشدید این آسیب‌پذیری‌ها می‌شوند.

ب. همکاری برای ایجاد محیط صلح‌آمیز، امن، منعطف و باز برای فناوری اطلاعات و ارتباطات

۱۱. دولت‌های عضو، نیاز به اقدامات همکاری جویانه علیه تهدیدات حاصل از استفاده مخرب از فناوری‌های اطلاعاتی و ارتباطی را مکرراً مورد تأیید قرار دادند. پیشرفت بیشتر در خصوص همکاری در سطح بین‌المللی نیازمند یک سری اقدامات برای ایجاد محیط صلح‌آمیز، امن، باز و همکاری جویانه برای فناوری اطلاعات و ارتباطات خواهد بود. توجهات باید به سمت اقدامات همکاری جویانه‌ای معطوف شود که بتواند صلح، ثبات و امنیت بین‌المللی را ارتقای دهد. این موارد شامل درک مشترک در زمینه اعمال حقوق بین‌الملل مربوط و هنجارها، قوانین و اصول برخاسته از رفتار مسئولانه دولت‌هاست.

۱۲. دولت‌ها باید مقابله با این چالش‌ها را رهبری کنند اما مشارکت مناسب بخش خصوصی و جامعه مدنی برای این همکاری‌ها مؤثر و مفید خواهد بود.

۱۳. سازمان ملل باید نقش رهبری را در ارتقای گفتگو بین دولت‌های عضو در راستای ایجاد درک مشترک پیرامون امنیت فناوری اطلاعات و استفاده از آن، تشویق تلاش‌های منطقه‌ای، فراهم نمودن اقدامات اعتمادساز و شفاف‌ساز و حمایت از ظرفیت‌سازی و ترویج بهترین شیوه‌ها ایفا نماید.

۱۴. در کنار فعالیت‌های صورت گرفته در مجموعه سازمان ملل، تلاش‌های ارزشمندی توسط سازمان‌های بین‌المللی و نهادهای منطقه‌ای در حال انجام است. مثل: اتحادیه آفریقایی، مجمع ملت‌های جنوب شرق آسیا (ASEAN)، مجمع همکاری‌های اقتصادی آسیا پاسیفیک، شورای

اروپا، جامعه اقتصادی دولت‌های غرب آفریقا، اتحادیه اروپایی، اتحادیه عرب، سازمان دولت‌های امریکایی، سازمان امنیت و همکاری اروپا (OSCE) و سازمان همکاری شانگهای. فعالیت‌های آتی در زمینه امنیت در استفاده از فناوری‌های اطلاعاتی و ارتباطی باید این تلاش‌ها را مورد نظر قرار دهد.

۱۵. برای درک جامع چالش‌ها با در نظر گرفتن تهدیدات موجود و بالقوه، خطرها و آسیب‌پذیری‌ها و بر اساس ارزیابی‌ها و توصیه‌های مندرج در گزارش سال ۲۰۱۰ گروه کارشناسان دولتی در زمینه امنیت اطلاعات و ارتباطات در چارچوب امنیت بین‌الملل (۲۰۱/۶۵/A)، این گروه توصیه‌های زیر را ارائه می‌دهد:

ج. توصیه‌هایی در مورد هنجارها، قوانین و اصول رفتار مسئولانه دولت‌ها

۱۶. اعمال هنجارهای منبعث از حقوق بین‌الملل موجود مرتبط با استفاده دولت‌ها از فناوری‌های اطلاعاتی و ارتباطی، یک اقدام ضروری برای کاهش خطرهای مربوط به صلح، امنیت و ثبات بین‌المللی است. درک مشترک در مورد چگونگی اعمال این هنجارها بر رفتار مسئولانه دولت‌ها و استفاده از فناوری‌های اطلاعاتی و ارتباطی توسط دولت‌ها نیازمند مطالعه بیشتر است. با توجه به ویژگی‌های منحصر به فرد فناوری‌های اطلاعاتی و ارتباطی، سایر هنجارها در طول زمان می‌توانند ایجاد شوند.

۱۷. گروه، دیدگاه‌ها و ارزیابی‌های دولت‌های عضو در زمینه تحولات حوزه فناوری اطلاعات و ارتباطات در چارچوب امنیت بین‌الملل را مورد نظر قرار داد. این دیدگاه‌ها در پاسخ به دعوت مجمع عمومی در قطعنامه‌های ۲۵/۶۴، ۴۱/۶۵ و ۲۴/۶۶ و دیگر اقدامات خواسته شده در قطعنامه‌های ۶۳/۵۵، ۱۲۱/۵۶، ۲۳۹/۵۷، ۱۹۹/۵۸ و ۲۱/۶۴ ارائه گردید.

۱۸. گروه، سند شماره ۳۵۹/۶۶/A را که توسط مجمع عمومی و بنا به درخواست نمایندگان دائم چین، فدراسیون روسیه، تاجیکستان و ازبکستان منتشر شده بود، مورد توجه قرار داد. این سند شامل پیش‌نویس یک کردارنامه بین‌المللی برای امنیت اطلاعات است که متعاقباً از سوی

قزاقستان و قرقیزستان مورد حمایت قرار گرفت.

۱۹. حقوق بین‌الملل، مخصوصاً منشور سازمان ملل، نه تنها قابلیت اعمال بر فضای سایبر را دارند، بلکه تحقق این امر در راستای حفظ صلح، ثبات و فراهم نمودن یک محیط باز، امن، صلح‌آمیز و در دسترس برای فناوری اطلاعات و ارتباطات یک ضرورت است.

۲۰. حاکمیت دولت و هنجارها و اصولی که از حاکمیت دولت سرچشمه می‌گیرند، به رفتار دولت در فعالیت‌های مرتبط با فناوری اطلاعات و ارتباطات، قابل اعمال می‌باشند. این امر به صلاحیت دولت بر زیرساخت‌های فناوری اطلاعات و ارتباطات واقع در قلمرو آن نیز مصداق دارد.

۲۱. تلاش‌های دولتی برای پرداختن به امنیت فناوری‌های اطلاعاتی و ارتباطی باید دوشادوش احترام به حقوق بشر و آزادی‌های اساسی مطرح شده در اعلامیه جهانی حقوق بشر و دیگر اسناد بین‌المللی صورت گیرد.

۲۲. دولت‌ها باید همکاری علیه استفاده تروریستی و مجرمانه از فناوری‌های اطلاعاتی و ارتباطی را تقویت نمایند. رویکردهای قانونی را به صورت مناسب هماهنگ و همکاری عملی بین اجرای قانون‌های مربوط و سازمان‌های قضایی را تقویت کنند.

۲۳. دولت‌ها باید به تعهدات بین‌المللی خود در رابطه با اعمال غیرقانونی بین‌المللی که به آن‌ها نسبت داده می‌شود انجام دهند. دولت‌ها نباید از پروکسی‌ها برای انجام اقدامات نادرست بین‌المللی استفاده کنند. کشورها باید به دنبال تضمین این باشند که قلمرو آن‌ها توسط عوامل غیر دولتی برای استفاده غیرقانونی از فناوری اطلاعاتی و ارتباطی مورد استفاده قرار نمی‌گیرد.

۲۴. کشورها باید بخش خصوصی و جامعه مدنی را تشویق کند تا نقش مناسبی در بهبود

امنیت و استفاده از فناوری اطلاعاتی و ارتباطی از جمله تأمین امنیت زنجیره تأمین برای محصولات و خدمات ICT ایفا کند.

۲۵. کشورهای عضو باید در نظر داشته باشند که چگونه در اجرای هنجارها و اصول رفتار مسئولانه فوق بهترین همکاری را داشته باشند. از جمله نقشی که ممکن است توسط بخش خصوصی و سازمان‌های جامعه مدنی ایفا شود. این معیارها و اصول مکمل کار سازمان ملل و گروه‌های منطقه‌ای هستند و اساس کار بیشتر برای ایجاد اعتماد و اطمینان هستند.

د. توصیه‌هایی در مورد اقدامات اعتمادساز و تبادل اطلاعات

۲۶. اقدامات اعتمادساز داوطلبانه می‌تواند اعتماد و اطمینان را در بین کشورها افزایش دهد و به کاهش خطر درگیری از طریق افزایش پیش‌بینی‌پذیری و کاهش سوء تفاهات کمک کند. این اقدامات می‌توانند نقش مهمی در مقابله با نگرانی‌های دولت‌ها در مورد استفاده از فناوری اطلاعاتی و ارتباطی توسط دولت‌ها داشته باشند و می‌توانند گامی مهم در جهت امنیت بیشتر بین‌المللی باشد. دولت‌ها باید توسعه اقدامات عملی اعتمادسازی را مورد نظر قرار دهند تا به افزایش شفافیت، پیش‌بینی‌پذیری و همکاری کمک کنند. از جمله:

(a) تبادل دیدگاه‌ها و اطلاعات به صورت داوطلبانه در مورد راهبردها و سیاست‌های ملی، بهترین روش‌ها، فرایندهای تصمیم‌گیری، سازمان‌های ملی مربوط و تدابیر و اقداماتی برای بهبود همکاری بین‌المللی. میزان این اطلاعات توسط کشورهای ارائه‌کننده تعیین خواهد شد. این اطلاعات می‌تواند به صورت دو جانبه یا در قالب گروه‌های منطقه‌ای یا در دیگر مجامع بین‌المللی به اشتراک گذاشته شود.

(b) ایجاد چارچوب‌های مشاوره‌ای دوجانبه، منطقه‌ای و چندجانبه برای اعتمادسازی که می‌تواند شامل کارگاه‌ها، سمینارها و تمرین‌ها باشد تا به تصحیح تحقیقات ملی در مورد چگونگی پیشگیری از حوادث مخرب ناشی از استفاده دولتی از فناوری اطلاعاتی و ارتباطی و اینکه چگونه این حوادث ممکن است ایجاد و مدیریت شوند منجر شود.

(c) اشتراک گذاری گسترده اطلاعات بین دولت‌ها در مورد حوادث مربوط به امنیت فناوری اطلاعات و ارتباطات شامل افزایش استفاده مؤثر از کانال‌های موجود یا ایجاد کانال‌ها و سازوکارهای جدید مناسب برای واکنش بموقع، جمع‌آوری، تحلیل و بهبود اقدامات. دولت‌ها به‌منظور گسترش و ارتقای کانال‌های موجود ارتباطی برای مدیریت بحران‌ها و حمایت از ایجاد سازوکارهای هشدار دهنده سریع، باید نقاط تماس ملی برای به اشتراک گذاری اطلاعات در نظر بگیرند.

(d) تبادل اطلاعات و ارتباطات بین تیم‌های واکنش سریع کامپیوتری ملی (CERTs) به‌صورت دوجانبه یا چندجانبه یا دیگر مجامع به‌منظور حمایت از مذاکره در سطوح سیاست‌گذاری و تصمیم‌گیری.

(e) همکاری گسترده برای مقابله با حوادثی که می‌توانند فناوری اطلاعات و ارتباطات یا زیرساخت‌های حساس را که برسیستم‌های کنترل صنعتی فناوری اطلاعات و ارتباطات تکیه دارند، تأثیر بگذارد. این امر شامل دستورالعمل‌ها و بهترین عملکردها بین دولت‌ها علیه اقدامات مخرب و غیرقانونی است که بازیگران غیردولتی مرتکب می‌شوند.

(f) سازوکارهای گسترده برای همکاری انتظامی در جهت کاهش حوادثی که در غیر این صورت می‌توانند به غلط به‌عنوان عمل خصمانه دولت تفسیر شود. افزایش این سازوکارهای همکاری موجب ارتقای امنیت بین‌المللی می‌شود.

۲۷. این تلاش‌های اولیه در مورد اعتمادسازی می‌تواند تجربه ای عملی و راهنمایی مفید برای فعالیت‌های آینده باشد. کشورها باید پیشرفت‌هایی را که به‌صورت دو و چندجانبه حاصل شده تشویق و تقویت نمایند؛ از جمله در گروه‌های منطقه‌ای مانند اتحادیه آفریقا، مجمع منطقه‌ای سه‌آن، اتحادیه اروپا، اتحادیه کشورهای آمریکایی، سازمان امنیت و همکاری اروپا، سازمان همکاری شانگ‌های و سایر موارد. در راستای تکمیل این تلاش‌ها، دولت‌ها باید هم‌افزایی اقدامات و ترویج بهترین شیوه‌ها را ضمن توجه به تفاوت‌های بین کشورها و مناطق گسترش دهند.

۲۸. دولت‌ها باید ایجاد اقدامات اعتمادساز را مدیریت کنند، اما مشارکت بخش خصوصی و

جامعه مدنی در این خصوص مفید خواهد بود.

۲۹. باتوجه به سرعت توسعه فناوری اطلاعات و ارتباطات و ابعاد تهدید، گروه کارشناسان دولتی معتقد به نیاز به افزایش درک مشترک و همکاری عملی است. در این راستا، گروه مذاکرات منظم سازمانی را با مشارکت گسترده، تحت حمایت سازمان ملل متحد و نیز گفتگوهای منظم از طریق مجامع دوجانبه، منطقه‌ای، چندجانبه و سایر سازمان‌های بین‌المللی توصیه می‌کند.

ه. توصیه‌هایی در زمینه اقدامات ظرفیت‌ساز

۳۰. ظرفیت‌سازی برای یک تلاش مؤثر و همکاری‌جویانه جهانی در زمینه تأمین امنیت فناوری اطلاعات و ارتباطات و استفاده از آن‌ها اهمیت حیاتی دارد. بعضی از کشورها ممکن است در تلاش‌هایشان برای انجام مسئولیت‌های خود در موارد زیر نیازمند کمک باشند: بهبود و ارتقای امنیت زیرساخت‌های حساس فناوری اطلاعات و ارتباطات خود، توسعه مهارت‌های فنی و قانون‌گذاری مناسب، راهبردها و چارچوب‌های رگولاتوری (تنظیم مقررات) و پر کردن و از بین بردن شکاف موجود در امنیت فناوری‌های اطلاعاتی و ارتباطی و استفاده از آن‌ها.

۳۱. در این راستا، دولت‌هایی که با سازمان‌های بین‌المللی شامل کارگزاری‌ها و نهادهای سازمان ملل و بخش خصوصی تعامل می‌کنند، باید در نظر داشته باشند که چگونه کمک‌های فنی و سایر کمک‌ها را برای ظرفیت‌سازی در زمینه امنیت ICT و استفاده از آن‌ها در کشورهای نیازمند کمک به‌ویژه کشورهای در حال توسعه به بهترین شکل ممکن ارائه نمایند.

۳۲. براساس نتایج قطعنامه و گزارش‌ها سازمان ملل متحد، از جمله قطعنامه ۶۴/۲۱۱ در زمینه ظرفیت‌سازی، دولت‌ها باید اقدامات زیر را در نظر بگیرند:

الف) حمایت از تلاش‌های دوجانبه، منطقه‌ای، چندجانبه و بین‌المللی در زمینه ظرفیت‌سازی برای تأمین امنیت استفاده از فناوری اطلاعات و ارتباطات و زیرساخت‌های فناوری اطلاعات و

ارتباطات، برای تقویت چارچوب‌های قانونی ملی، ظرفیت‌های انتظامی و راهبردها، برای مقابله استفاده از فناوری‌های اطلاعاتی و ارتباطی برای اهداف مجرمانه و تروریستی؛
 (ب) ایجاد و تقویت ظرفیت‌های واکنشی در مقابل حوادث شامل ایجاد CERT و تقویت همکاری‌های CERT با CERT؛

(همکاری بین‌سرتها)

(ج) حمایت از ایجاد، توسعه و استفاده از آموزش الکترونیک، افزایش فراگیری و آگاهی در کنار احترام به امنیت فناوری اطلاعات و ارتباطات برای کمک به غلبه بر شکاف دیجیتالی و کمک به کشورهای در حال توسعه همگام با پیشرفت‌های سیاست بین‌المللی؛
 (د) افزایش همکاری و انتقال دانش و فناوری برای مدیریت حوادث مربوط به فناوری اطلاعات و ارتباطات، مخصوصاً برای کشورهای در حال توسعه؛
 (ه) تشویق به مطالعه و تجزیه و تحلیل بیشتر توسط مؤسسات تحقیقاتی و دانشگاه‌ها در مورد موضوعات مربوط به امنیت فناوری اطلاعات و ارتباطات. با توجه به دستور کار و مأموریت‌های ویژه مؤسسات آموزشی و تحقیقاتی سازمان ملل مبنی بر حمایت از دولت‌های عضو سازمان ملل و جامعه بین‌المللی، دولت‌ها باید در نظر بگیرند که این مؤسسات چگونه می‌توانند در این زمینه ایفای نقش کنند.

۳۳. این گروه تأکید می‌کند که پیشرفت در تأمین امنیت فناوری اطلاعات و ارتباطات، از جمله از طریق ظرفیت‌سازی، در دستیابی به بند ۸ اهداف توسعه هزاره با عنوان «توسعه مشارکت جهانی برای پیشرفت» نیز کمک خواهد کرد.

و. نتیجه:

۳۴. پیشرفت در امنیت بین‌المللی در استفاده از فناوری اطلاعات و ارتباطات توسط دولت‌ها، با قراردان هر قدم روی قدم قبلی، تکرارپذیر خواهد شد. یک محیط فناورانه شکل گرفته از تغییر

و افزایش مداوم تعداد کاربران جدید ICT این رویکرد تکرارشونده را ضروری می‌سازد. این گزارش حاوی توصیه‌هایی است که روی فعالیت‌های قبلی استوار شده و بنا گردیده است. کاربرد و پالایش آن‌ها به افزایش اعتماد بین همه ذی‌نفعان کمک خواهد کرد. گروه توصیه می‌کند که کشورهای عضو به بررسی فعالانه این گزارش و ارزیابی اینکه آن‌ها چگونه می‌توانند این توصیه‌ها را برای توسعه و کاربرد بیشتر مورد استفاده قرار دهند، همت گمارند.

فهرست اعضای گروه کارشناسان دولتی در مورد تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌المللی:

- ۱- آرژانتین. سفیر آلفردو مورلی. هماهنگ کننده، واحد انرژی و فناوری، وزارت امور خارجه؛
- ۲- استرالیا. خانم دبورا استوکس. دستیار اول دبیر-وزارت امور خارجه و بازرگانی؛
- ۳- بلاروس. آقای ولادیمیر ان. گراسیمویچ. رئیس، دپارتمان امنیت بین‌الملل و کنترل تسلیحات، وزارت امور خارجه؛
- ۴- کانادا. آقای مایکل والما. مدیر بخش برنامه‌ریزی سیاست، وزارت امور خارجه و تجارت بین‌المللی؛
- ۵- چین. آقای لی وانگ (جلسات اول و دوم). مدیر دپارتمان کنترل تسلیحات و خلع سلاح وزارت امور خارجه؛ و چین. خانم زیهوا دونگ (جلسه سوم) مشاور، دپارتمان کنترل تسلیحات و خلع سلاح، وزارت امور خارجه؛
- ۶- مصر دکتر شریف هاشم. مشاور ارشد امنیت اطلاعات وزیر ارتباطات و فناوری اطلاعات وزارت ارتباطات و فناوری اطلاعات؛
- ۷- استونی. آقای لینر ویک. مدیر اجرایی، کالج IT استونی؛
- ۸- فرانسه. آقای ژان فرنچوئیس بلارل. معاون مدیر کل، هماهنگ کننده امور سایبر، وزارت امور خارجه؛
- ۹- آلمان. آقای دتلو ولتر. مدیر اداره کنترل سلاح‌های متعارف و اقدامات امنیت‌ساز و اعتمادساز دفتر امور خارجه فدرال؛
- ۱۰- هندوستان. آقای هاراش. کی. جین. دبیر مشترک و رئیس-بخش راهبری الکترونیک و

فناوری اطلاعات-وزارت امور خارجه؛

۱۱- اندونزی. آقای فبرینا آ. رودیاری (جلسه اول). مدیر امنیت بین‌الملل و خلع سلاح، وزارت امور خارجه و آقای اندی راجمینتو (جلسه سوم). وزیر مشاور نماینده دائمی اندونزی در سازمان ملل، نیویورک؛

۱۲- ژاپن. سفیر تامتوسو شینتسوکا (جلسه اول). سفیر، همکاری بین‌المللی برای مقابله با تروریسم، جرایم سازمان یافته بین‌المللی و سیاست سایبر، وزارت امور خارجه و سفیر اسوشامای ایماهی (جلسات دوم و سوم). سفیر، همکاری بین‌المللی برای مقابله با تروریسم، جرایم سازمان یافته بین‌المللی و سیاست سایبر، وزارت امور خارجه؛

۱۳- فدراسیون روسیه. آندری وی. کروتسکیخ. هماهنگ کننده ویژه امور سیاسی در استفاده از فناوری اطلاعات و ارتباطات، سفیر کبیر، وزارت امور خارجه؛

۱۴- بریتانیا ایرلند شمالی. آقای نیکلاس هاوکک دستیار مدیر امنیت بین‌المللی، دفتر امنیت سایبری و تضمین اطلاعات دفتر کابینه؛

۱۵- ایالات متحده آمریکا. خانم مایکل جی مارکف معاون هماهنگ کننده مسائل سایبری، دفتر وزیر امور خارجه ایالات متحده.

بند چهار: گزارش چهارمین گروه کارشناسان دولتی سال ۲۰۱۵

ترجمه سند



مجمع عمومی

تاریخ انتشار: ۲۲ جولای ۲۰۱۵

شماره قطعنامه: A/70/174

توزیع: عمومی

زبان: انگلیسی

اجلاس هفتادم

دستور کار ۹۳

تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین الملل
گروه کارشناسان دولتی درباره تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین الملل

یادداشت دبیرکل؛

دبیرکل افتخار دارد که گزارش گروه کارشناسان دولتی را درباره تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین الملل تقدیم نماید. این گروه به موجب بند ۴ قطعنامه شماره ۶۸/۲۴۳ مجمع عمومی تأسیس شده است. گزارش گروه کارشناسان دولتی درباره تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین الملل.

چکیده گزارش:

فناوری‌های اطلاعاتی و ارتباطی، فرصت‌های بسیار خوبی برای جامعه بین الملل ایجاد کرد و اهمیت آن به صورت روزافزونی افزایش پیدا کرد. هر چند روندهای مخربی وجود دارند که برای صلح و امنیت بین المللی، ایجاد خطر می‌کنند. همکاری‌های مؤثر بین دولتی برای کاهش این خطرها، امری ضروری است.

گروه کارشناسان دولتی مربوط به سال ۲۰۱۵ {که} در مورد تحولات حوزه فناوری اطلاعات و ارتباطات در چارچوب امنیت بین الملل {فعال‌اند} تهدیدات بالقوه و بالفعل ناشی از کاربرد

فناوری اطلاعات و ارتباطات توسط دولت‌ها را بررسی کرده و اقدامات مربوط به مقابله با آن‌ها را توجه کرده، این اقدامات شامل هنجارها، قوانین، اصول و اقدامات مربوط به اعتمادسازی است. ضمن اینکه گروه کارشناسان دولتی، چگونگی اعمال حقوق بین‌الملل بر استفاده دولت‌ها از فناوری اطلاعات و ارتباطات را نیز بررسی قرار کرده، با مبنا قرار دادن فعالیت گروه‌های قبلی، این گروه توانسته است به پیشرفت‌های مهمی در این حوزه‌ها نایل آید.

گزارش حاضر، پیشرفت توجه‌پذیری در مباحث مربوط به هنجارها ایجاد کرد. گروه توصیه می‌کند که دولت‌ها برای پیشگیری از انجام اعمال زیان‌آور در حوزه فناوری اطلاعات و ارتباطات، با یکدیگر همکاری نمایند و به‌صورت آگاهانه، اجازه ندهند که قلمرو آن‌ها برای اقدامات نادرست بین‌المللی در حوزه فناوری اطلاعات و ارتباطات مورد استفاده قرار گیرد. این گزارش از دولت‌ها می‌خواهد که تبادل اطلاعات را افزایش دهند و استفاده تروریستی و مجرمانه از فناوری اطلاعات و ارتباطات را تحت تعقیب قرار دهند. در این راستا، گروه تأکید می‌کند که دولت‌ها باید احترام به حقوق بشر اعم از حریم خصوصی و آزادی بیان را کاملاً تضمین نمایند. یکی از مهم‌ترین توصیه‌ها این است که دولت‌ها نباید از فناوری اطلاعات و ارتباطات به‌صورت عمدی برای تخریب یا زیان رساندن به زیرساخت‌های حساس دیگر دولت‌ها استفاده کنند. ضمن اینکه نباید چنین فعالیت‌های مخربی را مورد حمایت قرار دهند. همچنین دولت‌ها باید برای حفاظت از زیرساخت‌های حساس خود در برابر تهدیدات ناشی از فناوری اطلاعات و ارتباطات، اقدامات مناسب اتخاذ نمایند. دولت‌ها نباید به سیستم‌های اطلاعاتی مربوط به تیم‌های مجاز واکنش سریع سایر دولت‌ها آسیب برسانند یا این گروه‌ها را در فعالیت‌های سوء بین‌المللی به‌کار گیرند. دولت‌ها باید گزارش‌های مسئولانه در خصوص آسیب‌پذیری‌های حوزه فناوری اطلاعات و ارتباطات را تشویق کنند و گام‌های معقولی جهت حصول اطمینان از استحکام و یکپارچگی زنجیره تأمین و پیشگیری از گسترش بدافزارها، تکنیک‌ها یا اقدامات مخفی زیان‌آور در حوزه فناوری اطلاعات و ارتباطات بردارند.

اقدامات اعتمادساز موجب افزایش همکاری‌ها، شفاف‌سازی و کاهش خطر برخورد {جنگ} می‌شود. این گروه تعدادی از اقدامات داوطلبانه اعتمادساز را جهت افزایش شفاف‌سازی، شناسایی

کرده است و پیشنهاد می‌کند که دولت‌ها اقدامات دیگری را نیز به‌منظور تقویت همکاری‌ها در پیش گیرند. گروه خواستار مشارکت گسترده اعضاء، جهت انجام مذاکرات منظم تحت حمایت سازمان ملل یا دیگر مجامع دوجانبه، چندجانبه یا منطقه‌ای است. دولت‌ها مسئول اصلی حفظ امنیت و صلح در فضای فناوری اطلاعات و ارتباطات می‌باشند، اما مشارکت مناسب بخش خصوصی، دانشگاهی و جامعه مدنی در جهت تقویت همکاری‌های بین‌المللی، مفید خواهد بود. ظرفیت‌سازی جهت توسعه همکاری‌ها و افزایش اعتمادسازی، یک امر ضروری است.

گزارش سال ۲۰۱۳ گروه کارشناسان (۹۸/۶۸/A) از جامعه بین‌الملل می‌خواهد که در جهت ارتقای امنیت زیرساخت‌های حساس حوزه فناوری اطلاعات و ارتباطات، تشریک مساعی کنند، برای پیشرفت مهارت‌های فنی مساعدت نمایند و توصیه می‌کند که راهبرد، قانون و مقررات مناسب اتخاذ نمایند. این گروه نتایج گروه قبلی را مکرراً مورد تأیید قرار می‌دهد و تأکید می‌کند که کشورها می‌توانند درخصوص تهدیدات و واکنش مناسب در مقابل آن‌ها از یکدیگر علم‌آموزی داشته باشند. گروه، اهمیت حقوق بین‌الملل، منشور ملل متحد و اصول حاکمیت را به‌عنوان مبانی افزایش امنیت در استفاده دولت‌ها از فناوری اطلاعات و ارتباطات، مورد تأکید قرار می‌دهد. با علم به ضرورت مطالعه بیشتر، گروه، حق ذاتی دولت‌ها در اتخاذ اقداماتی که مطابق با حقوق بین‌الملل است و توسط منشور به رسمیت شناخته شده باشند را مورد توجه قرار می‌دهد. گروه همچنین تأسیس اصول حقوق بین‌الملل اعم از محل اجراء، اصول انسان‌دوستانه، ضرورت، تناسب و تمایز آن را مورد توجه قرار می‌دهد.

برای فعالیت‌های آتی، گروه پیشنهاد می‌کند که مجمع عمومی تشکیل یک گروه جدید از کارشناسان دولتی در سال ۲۰۱۶ را مورد توجه قرار دهد.

گروه از دولت‌های عضو می‌خواهد که توصیه‌های آن را به‌صورت فعالانه‌ای مورد توجه قرار دهند و نحوه پیگیری موضوع جهت پیشرفت و اجرای آن توسط خود اعضاء را بررسی و پیگیری کنند.

فهرست مطالب:

پیشگفتار دبیر کل

معرفی نامه رئیس گروه

الف. مقدمه گزارش

ب. تهدیدات موجود و در حال ظهور

ج. هنجارها، قوانین و اصول رفتار مسئولانه دولت‌ها

د. اقدامات اعتمادساز

هـ. همکاری بین‌المللی و کمک در زمینه امنیت فناوری اطلاعات و ارتباطات و ظرفیت‌سازی

و. چگونگی اعمال حقوق بین‌الملل در استفاده از فناوری‌های اطلاعاتی و ارتباطی

ز. نتایج و توصیه‌هایی برای فعالیت آینده

ضمیمه

پیشگفتار دبیر کل

معدود فناوری‌هایی به اندازه فناوری اطلاعات و ارتباطات در تغییر شکل دادن به اقتصادها، جوامع و روابط بین‌الملل، قدرتمند بوده‌اند. فضای سایبری تمام جنبه‌های زندگی ما را تحت تأثیر قرار می‌دهد. در کنار مزایای بسیار دارای خطرهایی نیز است. ایجاد فضای سایبری پایدار و امن تنها از طریق همکاری بین‌المللی امکان‌پذیر است و پایه و اساس این همکاری باید قوانین بین‌المللی و اصول منشور سازمان ملل متحد باشد.

این گزارش که توسط کارشناسان دولتی از ۲۰ کشور ارائه شده حاوی توصیه‌هایی است تا تهدیدات موجود و در حال ظهوری را بیان کند که به طور یکسان ممکن است توسط دولت‌ها و بازیگران غیر دولتی، صلح و امنیت بین‌المللی را به خطر اندازد. کارشناسان بر اساس گزارش‌های اجماعی که در سال‌های ۲۰۱۰ و ۲۰۱۳ منتشر شده‌اند، دیدگاه‌های مربوط به تنظیم هنجارها، اعتمادسازی، ظرفیت‌سازی و کاربست حقوق بین‌المللی را ارائه می‌دهند.

از جمله مسائل پیچیده نو ظهور، استفاده مخرب از فناوری اطلاعات و ارتباطات توسط افراط‌گرایان، تروریست‌ها و گروه‌های سازمان‌یافته جنایی است. گزارش حاضر پیشنهادهایی را ارائه می‌دهد که

می‌تواند جهت مقابله با این روند نگران‌کننده کمک کند و در شکل‌دهی و قاعده‌مندسازی طرح اقدام در مورد پیشگیری از افراط‌گرایی خشونت بار مشارکت نماید.

همه کشورها در ایجاد فضای سایبری امن‌تر سهیم هستند. تلاش‌های ما در این زمینه باید تعهد جهانی را برای ایجاد یک اینترنت آزاد، امن و صلح‌آمیز تقویت نماید. در چنین فضایی، من گزارش حاضر را به مجمع عمومی و مخاطبان گسترده جهانی به‌عنوان یک مشارکت مهم در تلاشی اساسی برای تأمین امنیت فضای فناوری اطلاعات تقدیم می‌کنم.

معرفی نامه رئیس گروه ۲۶ ژوئن ۲۰۱۵

من این افتخار را دارم که همراه با این نامه گزارش گروه کارشناسان دولتی را ارائه نمایم که درباره پیشرفت‌ها در زمینه اطلاعات و ارتباطات در حوزه امنیت بین‌المللی است. این گروه در سال ۲۰۱۴ به موجب بند ۴ قطعنامه ۶۸/۲۴۳ مجمع عمومی در رابطه با تحولات در زمینه اطلاعات و ارتباطات راه دور در حوزه امنیت بین‌المللی تأسیس شد. به‌عنوان رئیس گروه، خوشحالم که به اطلاع شما برسانم که در این گزارش اجماع وجود دارد.

مجمع عمومی در قطعنامه خود خواستار تشکیل گروه کارشناسان دولتی در سال ۲۰۱۴ بر اساس توزیع جغرافیایی عادلانه گردید تا با چشم‌انداز حصول به یک درک مشترک، به مطالعه و بررسی در زمینه تهدیدات موجود و بالقوه در حوزه امنیت اطلاعات و اقدامات همکاری‌جویانه ممکن برای مقابله با آن‌ها از جمله هنجارها، قواعد و یا اصول رفتار مسئولانه دولت‌ها و اقدامات اعتمادساز، موضوعات مربوط به استفاده از فناوری اطلاعات و ارتباطات در مخاصمات و نحوه اعمال حقوق بین‌الملل بر استفاده دولت‌ها از فناوری اطلاعات و ارتباطات، و نیز طرح‌هایی که با هدف تقویت امنیت سیستم‌های اطلاعاتی و ارتباطات جهانی مورد استفاده قرار می‌گیرند، ادامه دهد. از گروه همچنین خواسته شد تا ارزیابی‌ها و توصیه‌های گروه قبلی را مورد نظر قرار دهند (نگاه کنید به ۹۸/۶۸/A). از دبیرکل درخواست شد تا گزارشی در زمینه نتایج مطالعات به هفتادمین جلسه مجمع ارائه دهد.

طبق قطعنامه، کارشناسان از ۲۰ کشور انتخاب شدند: بلاروس، برزیل، چین، کلمبیا، مصر،

استونی، فرانسه، آلمان، غنا، (رژیم جعلی) اسرائیل، ژاپن، کنیا، مالزی، مکزیک، پاکستان، جمهوری کره، فدراسیون روسیه، اسپانیا، انگلستان بریتانیای کبیر و ایرلند شمالی و ایالات متحده آمریکا. فهرست کارشناسان در ضمیمه آمده است.

این گروه دارای تبادل نظرهای جامع و عمیق مربوط به تحولات در زمینه اطلاعات و ارتباط از راه دور (مخابرات) در زمینه امنیت بین‌المللی بود. این جلسات در چهار نوبت برگزار شد: اولین جلسه از ۲۱ تا ۲۵ ژوئیه ۲۰۱۴ در مقر سازمان ملل متحد، دومین جلسه از ۱۲ تا ۱۶ ژانویه ۲۰۱۴ در ژنو و جلسه سوم از ۱۳ تا ۱۷ فوریه ۲۰۱۵ و چهارم از ۲۲ تا ۲۶ ژوئن ۲۰۱۵. هر دو در مقر سازمان ملل متحد.

گروه مایل است از کارشناسانی که به‌عنوان تسهیلگر در مباحث پیش‌نویس گزارش خدمت کرده‌اند تشکر کند: فلورانس منگین (فرانسه)، کاترین گتائو (کنیا)، آصف علی (پاکستان)، ریکاردو مور (اسپانیا) و اولیویا پرستون (بریتانیا).

گروه تمایل دارد تا از کمک مؤسسه تحقیقات خلع سلاح سازمان ملل متحد تشکر کند، که به‌عنوان یک مشاور به گروه خدمت کرده است و توسط جیمز لوئیس و کرسستین وینگارد نمایندگی شد تشکر کند. گروه همچنین مایل است تا از ایوان بوچانان از اداره امور خلع سلاح سازمان ملل متح که به‌عنوان دبیر گروه و همچنین دیگر مقامات دبیرخانه که به گروه کمک کرده بودند، قدردانی کند

امضاء کارلوس لوئیس دانت کووتینیو پرز رئیس گروه

الف. مقدمه گزارش

۱. پیرو قطعنامه ۶۸/۲۴۳ مجمع عمومی درباره تحولات در زمینه اطلاعات و ارتباطات راه دور در حوزه امنیت بین‌المللی، دبیرکل بر اساس توزیع جغرافیایی عادلانه، گروه کارشناسان دولتی را تشکیل داد تا با چشم‌انداز حصول یک درک مشترک، در زمینه تهدیدات موجود و بالقوه در حوزه امنیت اطلاعات و اقدامات همکاری‌جویانه ممکن برای مقابله با آن‌ها مطالعه و بررسی کند. این مهم از طریق از جمله هنجارها، قواعد و یا اصول رفتار مسئولانه دولت‌ها و اقدامات

اعتمادساز، موضوعات مربوط به استفاده از فناوری اطلاعات و ارتباطات در مخاصمات و نحوه اعمال حقوق بین‌الملل بر استفاده دولت‌ها از فناوری اطلاعات و ارتباطات، و نیز طرح‌هایی که با هدف تقویت امنیت سیستم‌های اطلاعاتی و ارتباطات جهانی مورد استفاده قرار می‌گیرند، میسر خواهد بود.

۲. یک محیط باز، امن، پایدار، در دسترس و صلح‌آمیز فناوری اطلاعات و ارتباطات برای همه ضروری است و نیازمند همکاری مؤثر بین دولت‌ها برای کاهش خطرهایی است که متوجه صلح و امنیت بین‌المللی است. این گزارش، توصیه‌های گروه کارشناسان دولتی را منعکس می‌کند که درباره تحولات در زمینه اطلاعات و ارتباطات راه دور در عرصه امنیت بین‌المللی است و بر کارگروه‌های قبلی تکیه کرده و بنا شده است (نگاه کنید به ۲۰۱/۶۵/A و ۹۸/۶۸/A). این گروه طرح‌های بین‌المللی مرتبط و اقدامات همکاری‌جویانه ممکن را که مربوط به وظایف خود باشد، بررسی کرد. این نکته که فراهم نمودن زمینه استفاده از فناوری اطلاعات و ارتباطات برای اهداف صلح‌آمیز و پیشگیری از مخاصمه ناشی از استفاده از آن، در راستای منافع همه دولت‌هاست، مورد تأیید مجدد قرار گرفت.

ب. تهدیدات موجود و در حال ظهور

۳. فناوری اطلاعات و ارتباطات فرصت‌های زیادی برای توسعه اجتماعی و اقتصادی فراهم می‌کند و برای جامعه جهانی اهمیت بیشتری پیدا می‌کند. با این حال، روند نگران‌کننده‌ای در محیط فناوری اطلاعات و ارتباطات جهانی وجود دارد، از جمله افزایش چشمگیر حوادثی که ناشی از استفاده مخرب از فناوری اطلاعات و ارتباطات توسط بازیگران دولتی و غیردولتی است. این روند باعث ایجاد خطرهایی برای همه کشورها می‌شود و سوءاستفاده از فناوری اطلاعات و ارتباطات می‌تواند به صلح و امنیت بین‌المللی آسیب برساند.

۴. تعدادی از کشورها در حال توسعه قابلیت‌های فناوری اطلاعات و ارتباطات برای اهداف

نظامی هستند. احتمال استفاده از فناوری اطلاعات و ارتباطات در مخاصمات آینده بین دولت‌ها در حال افزایش است.

۵. مضرترین حملاتی که با استفاده از فناوری اطلاعات و ارتباطات می‌تواند صورت گیرد، حملاتی هستند که زیرساخت‌های حیاتی و سیستم‌های اطلاعاتی مربوط به یک کشور را هدف قرار می‌دهند. خطر چنین حملاتی که با استفاده زیان آور از فناوری اطلاعات و ارتباطات علیه زیرساخت‌های حیاتی صورت می‌گیرد، واقعی و جدی است.

۶. استفاده از فناوری اطلاعات و ارتباطات برای اهداف تروریستی، فراتر از استخدام، تأمین مالی، آموزش، تحریک و ایجاد انگیزه است، از جمله حملات تروریستی علیه فناوری اطلاعات و ارتباطات یا زیرساخت‌های وابسته به فناوری اطلاعات و ارتباطات، احتمال بیشتری را به وجود می‌آورد که اگر با آن مقابله نشود ممکن است صلح و امنیت بین‌المللی را تهدید کند.

۷. تنوع بازیگران غیردولتی مخرب، از جمله گروه‌های جنایتکار و تروریست‌ها، انگیزه‌های متفاوت آن‌ها، سرعت اجرای اقدامات خرابه‌کارانه با استفاده از فناوری اطلاعات و ارتباطات و مشکل تعیین منبع حادثه‌ای که با استفاده از این فناوری صورت گرفته، باعث افزایش خطر می‌شود. دولت‌ها در مورد خطر بی‌ثبات‌سازی ناشی از سوء تفاهمات، قابلیت وقوع مخاصمات و احتمال آسیب رساندن به شهروندان، اموال و اقتصاد خود کاملاً نگران هستند.

۸. سطوح مختلف ظرفیت برای امنیت فناوری اطلاعات و ارتباطات در بین کشورها می‌تواند آسیب‌پذیری در یک جهان به هم پیوسته را افزایش دهد.

ج. هنجارها، قوانین و اصول رفتار مسئولانه دولت‌ها

۹. چگونگی و نحوه تعیین هنجارها، قواعد و اصولی که دولت‌ها می‌توانند در فعالیت‌های مرتبط

با فناوری اطلاعات و ارتباطات به انجام رسانند موجب می‌شود که محیط فناوری اطلاعات و ارتباطات، فرصت‌ها و چالش‌هایی را به صورت توأمان برای جامعه بین‌المللی فراهم کند. یک هدف این است که هنجارهای داوطلبانه و غیرالزام‌آور بیشتری را برای رفتار مسئولانه دولت را شناسایی و به تقویت درک مشترک به منظور افزایش ثبات و امنیت در محیط فناوری اطلاعات و ارتباطات اقدام کنیم.

۱۰. هنجارهای داوطلبانه و غیرالزام‌آور رفتار دولت مسئول می‌تواند خطرهای مربوط به صلح، امنیت و ثبات بین‌المللی را کاهش دهد. بر این اساس، هنجارها به دنبال محدود کردن یا ممنوعیت اقدام مغایر با حقوق بین‌الملل نیستند. هنجارها منعکس کننده انتظارات جامعه بین‌الملل، تنظیم استانداردهای رفتار دولت مسئول و اجازه دادن به جامعه بین‌المللی برای ارزیابی فعالیت‌ها و مقاصد دولت‌هاست. هنجارها می‌توانند به پیشگیری از درگیری در محیط فناوری اطلاعات و ارتباطات کمک کنند و در استفاده صلح‌آمیز از آن مشارکت نمایند تا امکان تحقق کامل افزایش توسعه اجتماعی و اقتصادی جهانی توسط فناوری‌های اطلاعات و ارتباطات فراهم شود.

۱۱. گزارش‌های قبلی گروه نشان داد که یک اجماع در حال ظهور در زمینه رفتار دولت مسئول در امنیت و استفاده از فناوری اطلاعات و ارتباطات از هنجارها و تعهدات بین‌المللی موجود نشئت گرفته است. وظیفه گروه قبلی، ادامه مطالعات با چشم‌اندازی به ارتقای درک مشترک، هنجارهای رفتاری دولت مسئول، تعیین اینکه کدام بخش از هنجارهای موجود ممکن است برای کاربرد در محیط فناوری اطلاعات و ارتباطات قابل تنظیم باشد، تشویق به پذیرش هنجارهای بیشتر و تشخیص و شناسایی اینکه کدام یک از هنجارهای دیگر مربوط به ویژگی‌های پیچیده و منحصر به فرد فناوری اطلاعات و ارتباطات را باید مورد توجه قرار داد که ممکن است نیاز به توسعه داشته باشد.

۱۲. این گروه پیشنهاد چین، قزاقستان، قرقیزستان، فدراسیون روسیه، تاجیکستان و ازبکستان

را برای یک کردارنامه در زمینه امنیت اطلاعات مورد توجه قرار داد (نگاه کنید به ۷۲۳/۶۹/A).

۱۳. باتوجه به تهدیدات، خطرها و آسیب‌پذیری‌های موجود و در حال ظهور و بر اساس ارزیابی‌ها و توصیه‌های مندرج در گزارش‌های ۲۰۱۰ و ۲۰۱۳ گروه‌های قبلی، گروه کنونی توصیه‌های زیر را برای ملاحظه توسط دولت‌ها در زمینه هنجارهای داوطلبانه و غیرالزام‌آور، قواعد یا اصول مسئولیت‌پذیری دولت‌ها با هدف ارتقای یک محیط باز، امن، پایدار، در دسترس و صلح‌آمیز فناوری اطلاعات و ارتباطات ارائه می‌دهد:

(الف) مطابق با اهداف سازمان ملل متحد، از جمله حفظ صلح و امنیت بین‌المللی، دولت‌ها باید در توسعه و به‌کارگیری اقدامات برای افزایش ثبات و امنیت در استفاده از فناوری اطلاعات و ارتباطات و پیشگیری از اقدامات مضر در عرصه فناوری اطلاعات و ارتباطات یا اقداماتی که ممکن است تهدید صلح و امنیت بین‌المللی باشند همکاری کنند؛

(ب) در مورد حوادث فناوری اطلاعات و ارتباطات، دولت‌ها باید تمام اطلاعات مربوط را در نظر بگیرند، از جمله حوزه بزرگ‌تر رویداد، چالش‌های انتساب در محیط فناوری اطلاعات و ارتباطات، ماهیت و گستره پیامدهای آن؛

(ج) دولت‌ها نباید آگاهانه اجازه دهند که قلمرو آن‌ها برای اقدامات غیرقانونی بین‌المللی با استفاده از فناوری اطلاعات و ارتباطات مورد استفاده قرار گیرد؛

(د) کشورها باید چگونگی همکاری بهتر برای تبادل اطلاعات، کمک به یکدیگر، تعقیب استفاده تروریستی و جنایتکارانه از فناوری اطلاعات و ارتباطات و اقدامات دیگر جهت همکاری برای مقابله با چنین تهدیداتی را در نظر بگیرند. ممکن است نیاز باشد دولت‌ها چگونگی انجام اقدامات جدید در این زمینه را در نظر بگیرند؛

(ه) کشورها در حصول اطمینان از استفاده ایمن از فناوری اطلاعات و ارتباطات، باید قطعنامه‌های ۲۰/۸ و ۲۶/۱۳ شورای حقوق بشر در مورد ارتقای، حفاظت و برخورداری از حقوق بشر در اینترنت و نیز قطعنامه‌های ۶۸/۱۶۷ و ۶۹/۱۶۶ مجمع عمومی در حق حفظ حریم خصوصی در عصر دیجیتال، برای تضمین کامل احترام به حقوق بشر، از جمله حق آزادی بیان را محترم بشمارند؛

و) یک دولت نباید فعالیت یا حمایتی آگاهانه را مغایر با تعهدات خود تحت قوانین بین‌المللی انجام دهد که عمداً به زیرساخت‌های حیاتی آسیب می‌رساند یا به طریقی دیگر استفاده و بهره‌برداری از زیرساخت‌های حیاتی را برای ارائه خدمات به عموم کاهش دهد؛

ز) کشورها باید اقدامات لازم را برای محافظت از زیرساخت‌های حیاتی خود در مقابل تهدیدات فناوری اطلاعات و ارتباطات باتوجه به قطعنامه ۵۸/۱۹۹ مجمع عمومی اتخاذ کنند که در مورد ایجاد یک فرهنگ جهانی امنیت سایبری و حفاظت از زیرساخت‌های اطلاعات حیاتی و سایر قطعنامه‌های مربوط است؛

ح) دولت‌ها باید به درخواست‌های کمک متعارف از سوی دولتی دیگر که زیرساخت‌های حیاتی آن مورد تهدیدات مخرب در حوزه فناوری اطلاعات و ارتباطات قرار گرفته پاسخ دهند. دولت‌ها همچنین باید به درخواست‌های مناسب برای کاهش فعالیت‌های مخرب در حوزه فناوری اطلاعات و ارتباطات با هدف زیرساخت‌های حیاتی دولت دیگری که از سرزمین آن‌ها نشئت گرفته است، باتوجه به حق حاکمیت، پاسخ دهد؛

ط) دولت‌ها باید گام‌های مسئولانه برای اطمینان از یکپارچگی زنجیره تأمین انجام دهند تا کاربران نهایی بتوانند به امنیت محصولات حوزه فناوری اطلاعات و ارتباطات اطمینان داشته باشند. دولت‌ها باید به دنبال پیشگیری از گسترش ابزارهای مخرب در حوزه فناوری اطلاعات و ارتباطات و تکنیک‌ها و استفاده از کاربردهای پنهان مضر باشند؛

ی) دولت‌ها باید گزارش‌های مسئولانه از آسیب‌پذیری‌های فناوری اطلاعات و ارتباطات و به اشتراک‌گذاری اطلاعات مرتبط در راه‌حل‌های ممکن درباره این آسیب‌پذیری را تشویق کنند تا به محدود کردن و حتی از بین بردن تهدیدات بالقوه در عرصه فناوری اطلاعات و ارتباطات و زیرساخت‌های وابسته به فناوری اطلاعات و ارتباطات منجر شود؛

ک) کشورها نباید فعالیت یا حمایتی آگاهانه از فعالیت‌های مربوط به آسیب‌رساندن به سیستم‌های اطلاعاتی واحدهای مجاز واکنش اضطراری (گاهی اوقات به‌عنوان گروه‌های واکنش اضطراری رایانه‌ای یا تیم واکنش امنیت سایبری) یکی از کشورهای دیگر انجام دهند. یک دولت نباید از تیم‌های مجاز واکنش اضطراری برای مشارکت در فعالیت‌های بین‌المللی مخرب

۱۴. گروه مشاهده کرد که اگر چه چنین اقداماتی ممکن است برای ارتقای یک محیط آزاد، امن، پایدار، قابل دسترس و صلح‌آمیز از فناوری اطلاعات و ارتباطات، ضروری باشد، امکان دارد این اقدامات به صورت فوری مخصوصاً برای کشورهای در حال توسعه امکان‌پذیر نباشد تا زمانی که بتوانند ظرفیت مناسب را به دست آورند.

۱۵. باتوجه به ویژگی‌های منحصربه‌فرد فناوری‌های اطلاعات و ارتباطات، هنجارهای دیگر در طول زمان می‌توانند ایجاد شوند.

د. اقدامات اعتمادساز

۱۶. اقدامات اعتمادساز، تقویت‌کننده صلح و امنیت بین‌المللی است. آن‌ها می‌توانند همکاری میان کشورها، شفافیت، قابل پیش‌بینی بودن و ثبات را افزایش دهند. در تلاش برای ایجاد اعتماد برای حصول اطمینان از یک محیط فناوری اطلاعات و ارتباطات صلح‌آمیز، کشورها باید دستورالعمل‌هایی برای اقدامات اعتمادسازی که توسط کمیسیون خلع سلاح در سال ۱۹۸۸ تصویب شده و با تصویب قطعنامه توسط مجمع عمومی تأیید شده است را در نظر بگیرند (H) ۴۳/۷۸. برای افزایش اعتماد و همکاری و کاهش خطر درگیری، گروه توصیه می‌کند که دولت‌ها اقدامات داوطلبانه اعتمادساز زیر را در نظر بگیرند:

(الف) تعیین نقاط مناسب تماس در سطوح سیاستگذاری و فنی برای مقابله با حوادث جدی در حیطه فناوری اطلاعات و ارتباطات و ایجاد فهرستی از این نقاط تماس؛

(ب) ایجاد و حمایت از سازوکارها و فرایندها برای مشاوره‌های دوجانبه، منطقه‌ای، درون منطقه‌ای و چندجانبه به منظور افزایش اعتمادسازی بین کشورها و کاهش خطر سوء تفاهم، و درگیری‌هایی که ممکن است از حوادث فناوری اطلاعات و ارتباطات ناشی شود؛

(ج) تشویق اقدامات شفاف‌ساز بر مبنای داوطلبانه، در سطوح دوجانبه، منطقه‌ای، درون منطقه‌ای

و چندجانبه به طور مناسب، برای ارتقای اعتمادسازی و اطلاع‌رسانی درباره کارهای آینده. این می‌تواند شامل به اشتراک‌گذاری داوطلبانه دیدگاه‌های ملی و اطلاعات در مورد جنبه‌های مختلف تهدیدات ملی و بین‌المللی برای استفاده از فناوری اطلاعات و ارتباطات باشد. در رابطه با آسیب‌پذیری و کارکردهای پنهان مضر در محصولات فناوری اطلاعات و ارتباطات؛ بهترین شیوه برای امنیت فناوری اطلاعات و ارتباطات؛ اقدامات اعتمادساز انجام شده منطقه‌ای و چندجانبه بین کشورها؛ و سازمان‌های ملی، راهبردها، سیاست‌ها و برنامه‌های مرتبط با امنیت فناوری اطلاعات و ارتباطات است؛

(د) ارائه داوطلبانه دیدگاه‌های ملی توسط دولت‌ها در مورد قالبها و رده‌های زیرساخت‌هایی که از سوی آن‌ها زیرساخت‌های حساس و حیاتی قلمداد می‌شوند، شامل اطلاعات در مورد قوانین و سیاست‌های ملی برای حفاظت از داده‌ها و زیرساخت‌های مبتنی بر فناوری اطلاعات و ارتباطات است. کشورها باید به دنبال تسهیل همکاری فرامرزی برای مقابله با آسیب‌پذیری‌های زیرساخت‌های حساس خود باشند، آسیب‌پذیری‌هایی که مرزهای ملی را در می‌نوردند. این اقدامات می‌تواند شامل موارد زیر باشد:

۱. تجمیع قوانین و سیاست‌های ملی مربوط به حفاظت از داده‌ها و زیرساخت‌های مبتنی بر فناوری اطلاعات و ارتباطات و انتشار مفادی که برای توزیع در زمینه قوانین و سیاست‌های ملی مناسب به نظر می‌رسند؛

۲. توسعه سازوکارها و فرایندها برای مذاکرات و رایزنی‌های دوجانبه، منطقه‌ای، درون منطقه‌ای و چندجانبه در زمینه حفاظت از زیرساخت‌های حیاتی مبتنی بر فناوری اطلاعات و ارتباطات؛

۳. ایجاد و توسعه سازوکارهای فنی، حقوقی و دیپلماتیک دو جانبه، منطقه‌ای، درون منطقه‌ای

و چندجانبه برای رسیدگی به درخواست‌های مربوط به حوزه فناوری اطلاعات و ارتباطات؛

۴. تصویب توافقنامه‌های ملی داوطلبانه برای طبقه‌بندی حوادث مربوط به حوزه فناوری اطلاعات و ارتباطات از لحاظ میزان و شدت حادثه، به منظور تسهیل تبادل اطلاعات در حوادث.

۱۷. دولت‌ها باید اقدامات اعتمادساز بیشتری را برای تقویت همکاری‌های دوجانبه، درون منطقه‌ای، منطقه‌ای و چندجانبه در نظر بگیرند. این می‌تواند شامل توافقات داوطلبانه‌ای از سوی دولت‌ها برای:

(الف) تقویت سازوکارهای همکاری بین سازمان‌های مربوط برای مقابله با حوادث امنیتی فناوری اطلاعات و ارتباطات و ایجاد سایر سازوکارهای فنی، قانونی و دیپلماتیک برای رسیدگی به درخواست‌های مرتبط با زیرساخت‌های فناوری اطلاعات و ارتباطات، از جمله در نظر گرفتن تبادل کارکنان در زمینه‌هایی مانند رسیدگی به حوادث و امور انتظامی، به صورت مناسب و تشویق برای انجام مبادلات بین مؤسسات تحقیقاتی و دانشگاهی؛

(ب) ارتقای همکاری، از جمله توسعه کانون‌های ارتباطی برای تبادل اطلاعات در مورد استفاده از بدافزارها در حوزه فناوری اطلاعات و ارتباطات و آمادگی کمک در تحقیقات؛

(ج) ایجاد یک تیم واکنش اضطراری (سریع) ملی رایانه‌ای و یا تیم واکنش به حادثه امنیت سایبری یا تعیین یک سازمان به صورت رسمی که عهده‌دار چنین نقشی باشد. دولت‌ها ممکن است بخواهند چنین نهادهایی را در چارچوب تعریف خود از زیرساخت‌های حیاتی نظر بگیرند. دولت‌ها باید عملکرد و همکاری میان چنین تیم‌های واکنش اضطراری (سریع) ملی و سایر نهادهای مجاز را حمایت و تسهیل کنند؛

(د) گسترش دادن و حمایت کردن از اقدامات تیم پاسخ اضطراری رایانه‌ای و همکاری تیم واکنش به حوادث امنیت سایبری، به صورت مناسب، از قبیل تبادل اطلاعات در مورد آسیب‌پذیری‌ها، الگوهای حمله و مناسب‌ترین روش‌ها برای کاهش حملات، از جمله هماهنگ کردن پاسخ‌ها، سازماندهی تمرینات، پشتیبانی از رسیدگی به حوادث مربوط به فناوری اطلاعات و ارتباطات و تقویت همکاری‌های منطقه‌ای و همکاری بخش خصوصی؛

(ز) همکاری به شیوه‌ای سازگار و مطابق با قوانین ملی و بین‌المللی، با درخواست کشورهای دیگر در تحقیق جرایم مرتبط با فناوری اطلاعات و ارتباطات یا استفاده از فناوری اطلاعات و ارتباطات برای اهداف تروریستی یا برای کاهش فعالیت‌های مخرب حوزه فناوری اطلاعات و ارتباطات که نشأت گرفته از قلمرو خودشان است.

۱۸. گروه تأکید می‌کند که باتوجه به سرعت توسعه فناوری اطلاعات و ارتباطات و دامنه تهدیدات، نیاز به افزایش درک مشترک و همکاری بیشتر است. در این راستا، گروه مذاکرات سازمانی منظمی را با مشارکت گسترده تحت حمایت سازمان ملل متحد و نیز گفتگوهای منظم از طریق مجامع دوجانبه، منطقه‌ای و چندجانبه و سایر سازمان‌های بین‌المللی توصیه می‌کند.

هـ. همکاری و مساعدت بین‌المللی در امنیت و ظرفیت‌سازی در حوزه فناوری اطلاعات و ارتباطات

۱۹. دولت‌ها مسئولیت اصلی امنیت ملی و ایمنی شهروندان، از جمله در حوزه فناوری اطلاعات و ارتباطات را بر عهده دارند، اما بعضی از آن‌ها ممکن است از ظرفیت و توانایی کافی برای حمایت از شبکه‌های فناوری اطلاعات و ارتباطات خود برخوردار نباشند. فقدان ظرفیت می‌تواند شهروندان و زیرساخت‌های حیاتی یک کشور را آسیب‌پذیر سازد یا آن را به یک پناهگاه غیرمجاز برای بازیگران مخرب تبدیل کند. همکاری و مشارکت بین‌المللی می‌تواند نقش مهمی را در توانمند ساختن دولت‌ها برای ایمن‌سازی فناوری اطلاعات و ارتباطات (ICT) و اطمینان از استفاده صلح‌آمیز آن‌ها داشته باشد. کمک به ایجاد ظرفیت در زمینه امنیت فناوری اطلاعات و ارتباطات برای امنیت بین‌المللی، با افزایش توانایی دولت‌ها برای همکاری و اقدام جمعی ضروری است. این گروه موافقت کرد که اقدامات ظرفیت‌ساز باید به دنبال فراهم نمودن زمینه استفاده از فناوری اطلاعات و ارتباطات برای اهداف صلح‌آمیز باشد.

۲۰. این گروه توصیه‌های مربوط به ظرفیت‌سازی در گزارش‌های ۲۰۱۰ و ۲۰۱۳ را تأیید کرد. گزارش سال ۲۰۱۰ توصیه می‌کند که دولت‌ها اقداماتی را در جهت حمایت از ظرفیت‌سازی در کشورهای کمتر توسعه‌یافته معین کنند. گزارش سال ۲۰۱۳ از جامعه بین‌المللی خواست تا با همکاری در ارائه کمک به بهبود امنیت زیرساخت‌های حیاتی در حوزه فناوری اطلاعات و ارتباطات؛ توسعه مهارت‌های فنی و تدوین قوانین مناسب، راهبردها و چارچوب‌های قانونی برای انجام مسئولیت‌های خود؛ شکاف در امنیت در حوزه فناوری اطلاعات ارتباطات و استفاده

از آن‌ها را از بین ببرند. گروه فعلی همچنین تأکید دارد که ظرفیت‌سازی، چیزی بیش از انتقال محض دانش و مهارت‌ها از کشورهای توسعه یافته به کشورهای در حال توسعه می‌باشد، زیرا همه کشورها می‌توانند از یکدیگر در مورد تهدیداتی که با آن‌ها روبرو هستند و پاسخ‌های مؤثر برای مقابله با آن تهدیدات را بیاموزند.

۲۱. ادامه کار از طریق قطعنامه‌های پیشین و گزارش‌های قبلی سازمان ملل متحد آغاز شد، از جمله قطعنامه ۶۴/۲۱ مجمع عمومی تحت عنوان «ایجاد فرهنگ جهانی امنیت سایبری و ارزیابی تلاش‌های ملی برای حفاظت از زیرساخت‌های اطلاعات حیاتی»، کشورها باید اقدامات داوطلبانه زیر را برای ارائه کمک‌های فنی و دیگر همکاری‌ها برای ایجاد ظرفیت در ایمنی فناوری‌های اطلاعاتی و ارتباطی در کشورهایی که نیاز به کمک و درخواست کمک دارند در نظر بگیرند:

(الف) کمک به تقویت سازوکارهای همکاری با تیم‌های ملی واکنش سریع رایانه‌ای و سایر نهادهای مجاز؛

(ب) ارائه کمک و آموزش برای کشورهای در حال توسعه برای بهبود امنیت در استفاده از فناوری اطلاعات و ارتباطات، از جمله زیرساخت‌های حیاتی، و تبادل بهترین شیوه‌های قانونی و اداری؛

(ج) کمک برای دسترسی به فناوری‌های مورد نیاز برای امنیت در حوزه‌ی فناوری اطلاعات ارتباطات؛

(د) ایجاد رویه برای کمک و همکاری متقابل در پاسخ دادن به حوادث و مقابله با مشکلات کوتاه‌مدت در امنیت شبکه‌ها، از جمله اتخاذ رویه‌هایی برای کمک سریع؛

(ه) تسهیل همکاری‌های فرامرزی برای مقابله با آسیب‌پذیری‌هایی که مرزهای ملی را در می‌نوردند؛

(و) توسعه راهبردهایی برای پایداری تلاش‌های مربوط به ظرفیت‌سازی در حوزه امنیت فناوری اطلاعات و ارتباطات؛

(ز) اولویت‌دادن به آگاهی و ظرفیت‌سازی برای امنیت فناوری اطلاعات و ارتباطات در برنامه‌ها و بودجه‌های ملی و اختصاص جایگاه مناسب برای آن در برنامه‌ریزی‌های توسعه و کمک‌رسانی. این امر می‌تواند شامل برنامه‌های آگاه‌سازی در حوزه امنیت فناوری اطلاعات و ارتباطات باشد که برای آموزش و اطلاع‌رسانی به نهادها و شهروندان عادی طراحی شده است. چنین برنامه‌هایی می‌تواند به همراه تلاش‌های سازمان‌های بین‌المللی، از جمله سازمان ملل متحد و سازمان‌های تابعه آن، بخش خصوصی، دانشگاه‌ها و سازمان‌های جامعه مدنی انجام شود.

(ح) تشویق به فعالیت بیشتر در زمینه ظرفیت‌سازی، مانند جرم‌یابی یا همکاری مشترک برای مقابله با استفاده از فناوری اطلاعات و ارتباطات برای مقاصد جنایی یا تروریستی.

۲۲. توسعه رویکردهای منطقه‌ای برای ظرفیت‌سازی می‌تواند سودمند باشد، زیرا می‌تواند جنبه‌های فرهنگی، جغرافیایی، سیاسی، اقتصادی و اجتماعی خاصی را در نظر بگیرد و به یک رویکرد مناسب دست یابد.

۲۳. در راستای ایجاد ظرفیت‌سازی در زمینه امنیت فناوری اطلاعات و ارتباطات، کشورها می‌توانند همکاری دوجانبه و چندجانبه انجام دهند که مبتنی بر روابط همکاری‌جویانه باشد. چنین ابتکاراتی به بهبود شرایط برای کمک متقابل مؤثر بین کشورها در پاسخگویی به حوادث مربوط به حوزه فناوری اطلاعات و ارتباطات کمک می‌کند و می‌تواند توسط سازمان‌های بین‌المللی ذی‌صلاح، از جمله سازمان ملل متحد و سازمان‌های تابعه آن، بخش خصوصی، دانشگاه‌ها و سازمان‌های جامعه مدنی توسعه یابد.

این تعهدات به منزله نقاط کانونی و اصلی آزمون اعمال حقوق بین‌الملل در استفاده از فناوری اطلاعات و ارتباطات می‌باشند.

و. چگونگی اعمال حقوق بین‌الملل بر استفاده از فناوری‌های اطلاعات و ارتباطات

۲۴. گزارش سال ۲۰۱۳ نشان می‌دهد که حقوق بین‌الملل و به‌ویژه منشور سازمان ملل متحد، قابل اجرا است و برای حفظ صلح و ثبات و فراهم نمودن یک محیط باز، امن، پایدار، قابل دسترس و صلح‌آمیز ضروری است. پیرو همان دستورکار، گروه فعلی، نحوه اعمال حقوق بین‌الملل در مورد استفاده از فناوری اطلاعات و ارتباطات در کشورها را مورد بررسی قرار داد.

۲۵. تبعیت کشورها از حقوق بین‌الملل، به‌ویژه تعهدات آن‌ها در قبال منشور، یک چارچوب ضروری برای اقدامات آن‌ها در استفاده از فناوری اطلاعات و ارتباطات و ارتقای یک محیط باز، امن، پایدار، در دسترس و صلح‌آمیز از فناوری اطلاعات و ارتباطات است.

۲۶. با در نظر گرفتن اعمال حقوق بین‌الملل بر استفاده دولت‌ها از فناوری اطلاعات و ارتباطات این گروه، اصول مندرج در منشور و سایر قوانین بین‌المللی را به‌عنوان اساسی‌ترین تعهد دولت‌ها تعیین کرد: برابری حاکمیتی؛ حل و فصل اختلافات بین‌المللی با استفاده از روش‌های مسالمت‌آمیز به طوری که صلح و امنیت و عدالت بین‌المللی در معرض خطر قرار نگیرد؛ خودداری از استفاده از زور یا تهدید در روابط بین‌المللی علیه یکپارچگی ارضی یا استقلال سیاسی هر دولتی و یا به هر نحو دیگری که متناقض با اهداف سازمان ملل است؛ احترام به حقوق بشر و آزادی‌های اساسی؛ و عدم مداخله در امور داخلی کشورهای دیگر.

۲۷. حاکمیت دولتی و هنجارها و اصول بین‌المللی که از حاکمیت ناشی می‌شوند، به رفتار دولت‌ها در فعالیت‌های مرتبط با فناوری اطلاعات و ارتباطات اعمال می‌شود و همچنین به حوزه صلاحیت آن‌ها درباره زیرساخت‌های فناوری اطلاعات و ارتباطات در داخل قلمرو آن‌ها اعمال می‌شود.

۲۸. بر اساس کار گروه‌های قبلی و تحت هدایت منشور و دستور کار مندرج در قطعنامه ۶۸/۲۴۳ مجمع عمومی، گروه کنونی دیدگاه‌های زیر را در مورد نحوه اعمال حقوق بین‌الملل در استفاده

از فناوری اطلاعات و ارتباطات توسط کشورها ارائه می‌دهد که البته جامع و کامل نیستند:
(الف) کشورها در مورد زیرساخت‌های مربوط به فناوری اطلاعات و ارتباطات واقع در قلمرو خود صلاحیت دارند؛

(ب) در استفاده از فناوری‌های اطلاعات و ارتباطات، دولت‌ها باید در کنار سایر اصول حقوق بین‌الملل، حاکمیت دولت، برابری حاکمیتی، حل اختلافات با استفاده از ابزارهای صلح‌آمیز و عدم مداخله در امور داخلی کشورهای دیگر را رعایت کنند. تعهدات موجود تحت حقوق بین‌الملل برای استفاده دولت از فناوری اطلاعات و ارتباطات قابلیت اجرا دارد. کشورها باید از تعهدات خود در قبال حقوق بین‌الملل تبعیت کنند و از حقوق بشر و آزادی‌های اساسی حمایت و حفاظت کنند؛

(ج) با تأکید بر آرمان‌های جامعه بین‌المللی برای استفاده صلح‌آمیز از فناوری اطلاعات و ارتباطات برای منافع مشترک بشری و با یادآوری اینکه منشور به طور کامل قابل اعمال است، گروه متذکر می‌شود که انجام اقدامات مطابق با قوانین بین‌المللی و به رسمیت شناخته شده در منشور، حقوق ذاتی کشورها است. گروه نیاز به مطالعه بیشتر در مورد این موضوع را تأیید کرد؛
(د) این گروه اصول قانونی بین‌المللی تأسیس شده از جمله در مواردی که امکان اعمال وجود دارد، اصول بشریت، ضرورت، تناسب و تمایز (تفکیک) را مورد توجه قرار می‌دهد؛

(ه) دولت‌ها نباید از پروکسی برای اعمال اقدامات غیرقانونی بین‌المللی با استفاده از فناوری‌های اطلاعاتی استفاده کنند و باید اطمینان حاصل کنند که قلمرو آن‌ها توسط بازیگران غیر دولتی برای انجام چنین اعمالی مورد استفاده قرار نمی‌گیرد؛

(و) کشورها باید تعهدات بین‌المللی خود را در مورد اقدامات غیرقانونی بین‌المللی که تحت موازین حقوق بین‌الملل به آن‌ها منتسب می‌شود ایفا نمایند. با این حال ممکن است قرائنی که مؤید این باشد که فعالیت صورت گرفته در زمینه فناوری اطلاعات و ارتباطات توسط یک کشور مشخص انجام شده یا به نحو دیگری از قلمرو آن کشور شروع (ناشی) شده یا توسط زیرساخت‌های فناوری اطلاعات و ارتباطات واقع در آن کشور انجام شده باشد، ناکافی باشد. این گروه خاطرنشان می‌کند که اتهامات مربوط به سازمان‌دهی و اجرای اقدامات غیرقانونی که علیه

دولت‌ها اقامه می‌شود، باید با دلیل و مدرک اثبات شود.

۲۹. این گروه خاطرنشان ساخت که درک مشترک درباره چگونگی اعمال قوانین بین‌المللی برای استفاده دولت‌ها از فناوری اطلاعات و ارتباطات برای ارتقای یک محیط باز، امن، پایدار، در دسترس و صلح‌آمیز فناوری اطلاعات و ارتباطات مهم است.

ز. نتیجه‌گیری و توصیه‌هایی برای کارهای آتی

۳۰. پیشرفت توجه‌پذیری در شناخت خطرهای برای صلح و امنیت بین‌المللی در استفاده مخرب از فناوری اطلاعات و ارتباطات صورت گرفته است. با تشخیص اینکه فناوری اطلاعات و ارتباطات می‌تواند یک نیروی محرک در تسریع پیشرفت در جهت توسعه و سازگار با نیاز به حفظ ارتباطات جهانی و جریان آزاد و امن اطلاعات باشد، گروه، تعیین اقدامات ممکن برای کارهای آتی را که می‌تواند مؤثر واقع شود، مورد نظر قرار داد که البته محدود به موارد زیر نیست: (الف) توسعه بیشتر طرح‌های مربوط به صلح و امنیت بین‌المللی در استفاده از فناوری اطلاعات و ارتباطات در سطوح قانونگذاری، فنی و سیاستگذاری توسط کشورها به صورت جمعی و منفرد؛

(ب) افزایش همکاری در سطوح منطقه‌ای و چندجانبه برای تقویت درک مشترک در مورد خطرهای بالقوه علیه صلح و امنیت بین‌المللی ناشی از استفاده مخرب از فناوری اطلاعات و ارتباطات (ICT) و امنیت زیرساخت‌های حیاتی مبتنی بر فناوری اطلاعات و ارتباطات. (توضیح مترجم: زیرساخت‌های دانش بنیان، البته دانشی که مبتنی بر فناوری اطلاعات و ارتباطات باشد.)

۳۱. در حالی که کشورها مسئولیت اصلی حفظ محیط امن و صلح‌آمیز فناوری اطلاعات و ارتباطات را بر عهده دارند، همکاری مؤثر بین‌المللی از شناسایی سازوکارهای لازم برای مشارکت بخش خصوصی، دانشگاه‌ها و تشکل‌های جامعه مدنی سود خواهند برد.

۳۲. طرح‌های مربوط به استفاده دولت از فناوری اطلاعات و ارتباطات از جمله بخش‌هایی است که تحقیق و مطالعه بیشتر در آن می‌تواند مفید باشد. مؤسسه تحقیقات خلع سلاح سازمان ملل متحد که در همه کشورهای عضو خدمت می‌کند، یکی از نهادهایی است که می‌تواند بنا به درخواست، مطالعات مربوط را انجام دهد، مانند دیگر مؤسسات تحقیقاتی مربوط و سازمان‌های تحقیقاتی.

۳۳. سازمان ملل متحد باید نقش برجسته‌ای در ارتقای گفتمان در مورد امنیت فناوری اطلاعات و ارتباطات داشته باشد و همچنین در استفاده آن‌ها از سوی کشورها و ایجاد درک مشترک در مورد اجرای قوانین بین‌المللی و هنجارها، قواعد و اصول رفتار مسئولانه دولت‌ها. کار بیشتر می‌تواند در زمینه در نظر گرفتن ابتکارات برای گفت‌وگو و تبادل نظر بین‌المللی در زمینه مسائل امنیتی در حوزه فناوری اطلاعات و ارتباطات باشد. این تلاش‌ها نباید کارهای جاری سایر سازمان‌های بین‌المللی و انجمن‌هایی را که مسائلی مانند استفاده جنایی و تروریستی از فناوری اطلاعات و ارتباطات، حقوق بشر و حکومت اینترنتی را در دستور کار خود دارند، تکرار کند.

۳۴. این گروه اهمیت بررسی توسط مجمع عمومی برای تشکیل یک گروه جدید از کارشناسان دولتی در مورد تحولات در زمینه اطلاعات و ارتباطات از راه دور در زمینه امنیت بین‌المللی را مورد توجه قرار داد و در سال ۲۰۱۶ برای ادامه مطالعات به منظور ترویج درک مشترک در مورد تهدیدات موجود و بالقوه در حوزه امنیت اطلاعات و اقدامات ممکن همکاری برای رسیدگی به آن‌ها، و همچنین چگونگی اعمال قوانین بین‌المللی در مورد استفاده از فناوری اطلاعات و ارتباطات توسط کشورها، از جمله هنجارها، قوانین و اصول رفتار مسئولانه دولت‌ها، ایجاد اقدامات اعتمادساز و ظرفیت‌سازی را مورد توجه قرار داد.

۳۵. این گروه از تلاش‌های ارزشمندی که در زمینه امنیت فناوری اطلاعات و ارتباطات توسط

سازمان‌های بین‌المللی و گروه‌های منطقه‌ای انجام شده قدردانی می‌کند. باید تلاش‌های انجام شده در میان کشورها در مورد امنیت در استفاده از فناوری اطلاعات و ارتباطات در نظر گرفته شود و کشورهای عضو باید، در زمان مناسب، برای ایجاد سیستم‌های جدید دوجانبه، منطقه‌ای و چندجانبه برای گفتگو، مشاوره و ظرفیت‌سازی ترغیب شوند.

۳۶. گروه توصیه می‌کند که کشورهای عضو به توصیه‌های مندرج در این گزارش در مورد چگونگی کمک به ایجاد یک محیط باز، امن، پایدار، در دسترس و صلح‌آمیز فناوری اطلاعات و ارتباطات در سطح فعلی توجه داشته باشند و ارزیابی کنند که چگونه ممکن است برای توسعه و پیاده‌سازی بیشتر مورد استفاده قرار گیرند.

پیوست:

فهرست اعضای گروه کارشناسان دولتی در مورد تحولات عرصه اطلاعات و ارتباطات در چهارچوب امنیت بین‌المللی؛

۱. بلاروس. آیسنا سناتور چسنوسکی (جلسات سوم و چهارم). معاون دپارتمان امنیت بین‌الملل و کنترل تسلیحات، وزارت امور خارجه و سفیر ولادیمیر ان. گرامویچ (جلسه اول). رئیس دپارتمان امنیت بین‌الملل و کنترل تسلیحات، وزارت امور خارجه؛ و ایوان گرینویچ (جلسه دوم). مشاور نماینده دائمی بلاروس در سازمان ملل متحد در ژنو؛

۲. برزیل. کارلوس لونیس دانت کووتینیو پرز، وزیر، رئیس کارکنان معاون وزیر امور سیاسی، وزارت روابط خارجی؛

۳. چین. هایتاوو (جلسات سوم و چهارم). هماهنگ کننده امور سایبری وزارت امور خارجه و کانگ فو (جلسات اول و دوم) هماهنگ کننده امور سایبری وزارت امور خارجه؛

۴. کلمبیا. جورج فرناندو بیجارنو. مدیر استاندارد و معماری فناوری اطلاعات وزارت فناوری ارتباطات اطلاعات؛

۵. مصر. سم ابول العین. سفیر، معاون وزیر امور خارجه برای خلع سلاح، امنیت بین‌المللی و

استفاده صلح‌آمیز از انرژی هسته‌ای، وزارت امور خارجه و عمرو الجوابلی (جلسه سوم). وزیر، نماینده دائمی مصر در سازمان ملل متحد؛

۶. استونی. مارینا کالجوران. معاون وزیر امور خارجه و مشاور حقوقی وزارت امور خارجه؛
۷. فرانسه. فلورانس مانینگ. سفیر، هماهنگ‌کننده امنیت سایبری، وزارت امور خارجه و لئونارد رولان (جلسه اول). دپارتمان امور راهبردی، امنیتی و خلع سلاح، وزارت امور خارجه؛
۸. آلمان. کارستن جییر. رئیس، اداره هماهنگی سیاست سایبر، اداره امور خارجه فدرال؛
۹. غنا. مارک الیور کوور. عضو هیئت مدیره نهاد ملی ارتباطات؛
۱۰. رژیم صهیونیستی [اسرائیل. ایدو مد. هماهنگ‌کننده امنیت سایبری، وزارت امور خارجه]
۱۱. ژاپن. تاکشی اوکادا (جلسات سوم و چهارم). سفیر در سازمان ملل متحد، معاون مدیرکل سیاست خارجی، وزارت امور خارجه و آکیرا کنو (جلسه دوم). تاکائو ایمافوکو (جلسه اول). مذاکره‌کننده ارشد امور امنیت بین‌المللی، اداره سیاست خارجی، وزارت امور خارجه؛
۱۲. کنیا. کترین گیتائو. دبیر ICT وزارت اطلاعات، ارتباطات و فناوری اطلاعات؛
۱۳. مالزی. نور حایان عبد کریم (جلسه چهارم). معاون وزیر؛ بخش امنیت فضایی و سایبری، شورای امنیت ملی و محمد شاه نوری بن معین زین (جلسات اول، دوم و سوم). معاون وزیر، بخش امنیت فضایی و سایبری، شورای امنیت ملی؛
۱۴. مکزیک. ادگار زوریاتا. وابسته در ایالات متحده آمریکا و کانادا، کمیسیون امنیت ملی مکزیک - پلیس فدرال؛
۱۵. پاکستان. آصف علی (جلسات اول، دوم و چهارم). مدیر کل، شعبه فنی، بخش برنامه‌ریزی راهبردی، ستاد مشترک مرکز فرماندهی؛
- خلیل هاشمی (جلسه سوم). وزیر، نماینده دائمی پاکستان در سازمان ملل؛
۱۶. جمهوری کره. چول لی (جلسات دوم و چهارم). مدیر بخش امنیت بین‌المللی، وزارت امور خارجه و هیونچول جانگ (جلسات اول و سوم). مشاور، سفارت جمهوری کره در پادشاهی بلژیک و اتحادیه اروپا؛
۱۷. فدراسیون روسیه. آندری وی کروتسکیخ. نماینده ویژه رئیس جمهور فدراسیون روسیه برای



همکاری بین‌المللی در زمینه امنیت اطلاعات، سفیر کبیر؛

۱۸. اسپانیا. ریکاردو مور (جلسه چهارم). سفیر در امور امنیت سایبری، وزارت امور خارجه و همکاری و آلیسا مورال (جلسات اول، دوم و سوم). سفیر در امور امنیت سایبری، وزارت امور خارجه و همکاری؛

۱۹. بریتانیا و ایرلند شمالی. اولیویا پرستون. دستیار مدیر، دفتر امنیت سایبری و تضمین اطمینان، دفتر کابینه؛

۲۰. ایالات متحده آمریکا. میشل مارکف. معاون هماهنگ کننده مسائل مربوط به سایبر، دفتر هماهنگ کننده امور سایبر، دفتر وزیر امور خارجه، وزارت امور خارجه ایالات متحده؛

بند پنجم: گزارش پنجمین گروه کارشناسان دولتی سال ۲۰۱۷



مجمع عمومی
کمیته اول

ترجمه سند

تاریخ انتشار: ۱۴ آگوست ۲۰۱۷

شماره قطعنامه: A/72/327

توزیع: عمومی

زبان: انگلیسی

اجلاس هفتاد و دوم

دستور کار ۹۵

تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین الملل
گروه کارشناسان دولتی در زمینه تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین الملل

یادداشت دبیر کل:

گزارش حاضر پیرو قطعنامه مجمع عمومی به شماره ۷۰/۲۳۷ در باره تحولات در حوزه اطلاعات و ارتباطات در چارچوب امنیت بین الملل ارائه گردیده است.

مقدمه:

۱. مجمع عمومی در قطعنامه خود {به شماره} ۷۰/۲۳۷ مورخ ۲۳ دسامبر ۲۰۱۵، درباره تحولات در حوزه اطلاعات و ارتباطات در چارچوب امنیت بین الملل، از دبیر کل درخواست نمود، با کمک گروه کارشناسان دولتی که در سال ۲۰۱۶ بر اساس توزیع عادلانه جغرافیایی تشکیل می شود، با در نظر گرفتن ارزیابی ها و توصیه های مندرج در گزارش فوق الذکر به مطالعه در باب {موضوعات زیر} ادامه دهند و گزارشی از نتایج این مطالعات را در اجلاس هفتاد و دوم مجمع عمومی ارائه نمایند:

✓ ارتقای درک مشترک؛

✓ تهدیدات موجود و بالقوه در حوزه امنیت اطلاعات؛

✓ اقدامات همکاری جویانه ممکن جهت مقابله با آن ها؛

- ✓ چگونگی اعمال حقوق بین‌الملل بر استفاده از فناوری اطلاعات و ارتباطات توسط دولت‌ها؛
- ✓ اقدامات اعتمادساز و ظرفیت‌ساز؛
- ✓ و مفاهیم فهرست شده در بند ۳ {قطعنامه فوق}.

مسائل سازمانی:

۲. مطابق با شرایط مندرج در قطعنامه، دبیرکل، گروه کارشناسان دولتی را از ۲۵ کشور عضو انتخاب نمود: استرالیا، بوتسوانا، برزیل، کانادا، چین، کوبا، مصر، استونی، فنلاند، فرانسه، آلمان، هند، اندونزی، ژاپن، قزاقستان، کنیا، مکزیک، هلند، جمهوری کره (کره جنوبی)، روسیه، سنگال، صربستان، سوئیس، بریتانیا و ایرلند شمالی، آمریکا. فهرست کارشناسان در ضمیمه آمده است.

۳. گروه کارشناسان دولتی، در چهارجلسه حضور یافتند. نخستین جلسه از ۲۹ آگوست تا ۲ سپتامبر ۲۰۱۶ در مقر سازمان ملل متحد در نیویورک، جلسه دوم از ۲۵ نوامبر تا ۲ دسامبر ۲۰۱۶ در دفتر سازمان ملل متحد در ژنو {مقر اروپایی سازمان ملل}، جلسه سوم از ۲۰ تا ۲۴ فوریه ۲۰۱۷ در دفتر سازمان ملل متحد در ژنو و جلسه چهارم از ۱۹ تا ۲۳ ژوئن ۲۰۱۷ در مقر سازمان ملل متحد در نیویورک. در نخستین نشست، گروه، به اتفاق آراء، کارستن‌گی‌یر از آلمان را به‌عنوان رئیس انتخاب کرد.

۴. بخش توسعه و اطلاعات دفتر امور خلع سلاح به‌عنوان دبیرخانه به گروه خدمت کرد. مؤسسه تحقیقات خلع سلاح سازمان ملل به‌عنوان مشاور با گروه همکاری نمود.

۵. گروه طبق دستورالعمل ابلاغی خود بر اساس قطعنامه ۷۰/۲۳۷، اقدام به تبادل دیدگاه‌ها به شکل جامع و عمیق درباره تحولات در حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌المللی نمود. علاوه بر این، گروه گزارش‌های قبلی گروه کارشناسان دولتی درباره تحولات در حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌المللی و مشارکت‌ها و {نیز} یادداشت‌هایی

که در دسترس اعضای گروه قرار گرفت را مورد نظر قرار داد. از جمله در آخرین روز اختتامیه نشست‌های رسمی، چندین گزارش پیش‌نویس محتوایی درباب موضوعات زیر، توسط گروه مورد ملاحظه قرار گرفت.

۶. تهدیدات موجود و نوظهور، ظرفیت‌سازی، اعتمادسازی، توصیه‌هایی درباره اجرای هنجارها، قوانین و اصول درباره رفتار مسئولانه دولت‌ها، اعمال حقوق بین‌الملل در استفاده از فناوری‌های اطلاعات و ارتباطات، نتایج و توصیه‌ها برای فعالیت آینده، هیچ اجماعی روی گزارش نهایی حاصل نگردید.

ضمیمه:

فهرست اعضای گروه کارشناسان دولتی در زمینه تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌المللی:

۱. استرالیا. هنری فاکس. مدیر بخش سیاست سایبری، امنیت بین‌المللی دپارتمان بازرگانی و امور خارجه؛
۲. بوتسوانا. سسیل آتوکیل ماسیگا (اجلاس سوم). مدیر دپارتمان فناوری اطلاعات وزارت حمل و نقل و ارتباطات؛
۳. بوتسوانا. جان ال. واسیلیادیس (اجلاس دوم). نماینده ناظر دولت الکترونیک - امنیت وزارت حمل و نقل و ارتباطات؛
۴. برزیل. مارسلو پازساریا و کامارا. مشاور، رئیس بخش خلع سلاح و فناوری‌های حساس وزارت امور خارجه؛
۵. کانادا. میخیایل والما. هماهنگی سیاست خارجی سایبر در امور جهانی و لانگ ژو. هماهنگی امور سایبری وزارت امور خارجه؛
۶. کوبا. مگل گوتریز رودریگز. مدیر کل وزارت ارتباطات؛
۷. مصر. محمد ابوالخیر. سفیر و نماینده معاون وزیر خارجه برای سازمان‌های تخصصی؛
۸. استونی. مارینا کالجوراند. مشاور وزیر امور خارجه؛
۹. فنلاند. ماریا لتو. سفیر و کارشناس ارشد خدمات حقوقی وزارت امور خارجه؛

۱۰. فرانسه. دیوید مارتینون. سفیر در امور دیپلماسی سایبری و اقتصاد دیجیتال؛
۱۱. آلمان. رئیس ستاد هماهنگی سیاست سایبری، دفتر امور خارجه فدرال؛
۱۲. هند. سانتوش جها. دبیر مشترک. وزارت امور خارجه؛
۱۳. اندونزی. موناوار احمد. کارشناس ارشد میز ملی برای هماهنگی امنیت سایبر و اطلاعات نرم. وزارت سیاست‌ها، قوانین و امنیت؛
۱۴. ژاپن. کوچی میزوشیما. سفیر متصدی در امور سازمان ملل متحد و سفیر سیاست سایبری.
۱۵. قزاقستان. دیمتری گل بوردا. نماینده وزیر دفاع و صنعت هوافضا؛
۱۶. کنیا. کاترین . و. گتوآ. دبیر وزارت اطلاعات ارتباطات و فناوری؛
۱۷. مکزیک. جراردو عیسی مورالز تناریو. نماینده مدیر کل برای امنیت چندجانبه وزارت امور خارجه؛
۱۸. هلند. کارمن گونسالوز. رئیس سیاست سایبر بین‌المللی وزارت امور خارجه؛
۱۹. کره جنوبی. شین ماینگ هو. سفیر امور امنیت بین‌الملل وزارت امور خارجه؛
۲۰. روسیه. آندری وی. کروتسکیخ. نماینده ویژه رئیس جمهور روسیه برای همکاری در امنیت اطلاعات در سطح بین‌المللی، سفیر کبیر، وزارت امور خارجه؛
۲۱. سنگال. چریف دیالو. مدیر فناوری اطلاعات و ارتباطات. وزارت خدمات پستی و مخابراتی
۲۲. صربستان. دارگان مالدینویچ. سرهنگ دوم دپارتمان انفورماتیک و مخابرات ستاد مشترک ارتش صربستان. وزارت دفاع؛
۲۳. سوئیس. برانک گروته. سفیر و رئیس بخش سیاست امنیت وزارت امور خارجه سوئیس؛
۲۴. بریتانیا و ایرلند شمالی. سارا تیلور. مدیر، سیاست سایبر، دفتر امور خارجه و کشورهای مشترک المنافع؛
۲۵. آمریکا. خانم مایکل جی مارکف. معاون هماهنگ‌کننده مسائل سایبری، دفتر وزیر امور خارجه ایالات متحده.

بند شش: تشکیل اولین گروه کاری باز (O.E.W.G) در سال ۲۰۱۹



مجمع عمومی

ترجمه سند

تاریخ انتشار: ۲۲ می ۲۰۱۹

شماره قطعنامه: A/AC.1/2019/290

توزیع: عمومی

زبان: انگلیسی

گروه کاری باز درباره تحولات حوزه اطلاعات و ارتباطات راه دو در چارچوب امنیت بین‌المللی

دستور کار موقت و یادداشت‌ها

۱. انتخاب عوامل مسئول
۲. تصویب دستور کار
۳. سازمان کاری
۴. تبادل نظرهای عمومی
۵. بحث درباره موضوعات محتوایی مندرج در بند ۵ قطعنامه مجمع عمومی به شماره ۷۳/۲۷

برای توسعه بیشتر قواعد، هنجارها و اصول رفتار مسئولانه دولت‌ها که در بند ۱ قطعنامه ۷۳/۲۷ فهرست گردیده است و طرق اجرای آن‌ها و عنداللزوم ایجاد تغییرات در آن‌ها و وضع قوانین تکمیلی درباره این رفتار مسئولانه؛

برای بررسی امکان برقراری گفتگوی منظم نهادی با مشارکت وسیع تحت نظارت سازمان ملل متحد؛ ادامه بررسی با نگاهی به ارتقای درک مشترک، تهدیدات بالقوه و موجود در حوزه امنیت اطلاعات و اقدامات همکاری جویانه ممکن جهت مقابله با آن‌ها؛

چگونگی اعمال حقوق بین‌الملل در استفاده از فناوری اطلاعات و ارتباطات توسط دولت‌ها، اقدامات اطمینان‌ساز؛

ظرفیت‌سازی و مفاهیم اشاره شده در بند ۳ قطعنامه مجمع عمومی به شماره ۷۳/۲۷.

سایر مطالب

تصویب گزارش نهایی

یادداشت‌ها: پیرو قطعنامه مجمع عمومی به شماره ۷۳/۲۷، گروه کاری باز، اجلاس سازمانی خود را در سوم و چهارم جولای ۲۰۱۹ و اجلاس محتوایی خود را در تاریخ‌های زیر برگزار خواهد نمود:

۹ تا ۱۳ سپتامبر ۲۰۱۹، ۱۰ تا ۱۴ فوریه ۲۰۲۰ و ۶ تا ۱۰ جولای ۲۰۲۰.

تمامی این نشست‌ها در نیویورک برگزار خواهد گردید.

انتخاب عوامل مسئول: دبیرکل یا نماینده او تا زمان انتخاب رئیس، به‌عنوان رئیس موقت اجلاس را افتتاح خواهد نمود. از گروه کاری باز جهت انتخاب رئیس، دعوت به عمل خواهد آمد.

سازمان کاری: پیرو قطعنامه مجمع عمومی به شماره ۷۳/۲۷، گروه، در اجلاس سازمانی خود، باید درباره ترتیبات سازمانی خود در ارتباط با گروه، موافقت نماید. از گروه جهت تصمیم‌گیری درباره {موضوعات زیر} دعوت به عمل خواهد آمد:

- برنامه‌های کاری خود در هر اجلاس محتوایی؛

- قواعد خود درباره رویه‌ها؛

- مشارکت دولت‌های ناظر، سازمان‌های بین‌دولتی، سازمان‌های نظام ملل متحد، جامعه

مدنی و سایر بخش‌های علاقه‌مند جهت فعالیت در کار گروه.

تبادل نظرهای عمومی: مشارکت‌کنندگان در گروه کاری، نظرهای خود را درباره تحول در

حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌المللی مبادله خواهند نمود.

گفتگو و بحث درباره موضوعات محتوایی مندرج در بند ۵ قطعنامه مجمع عمومی به شماره

۷۳/۲۷

از مشارکت‌کنندگان در گروه کاری، جهت پیشنهاد عناصری درباره موضوعات محتوایی برای

توصیه‌های نهایی گروه، دعوت به عمل خواهد آمد (اعضای مشارکت‌کننده توصیه‌های خود را

ارائه خواهند نمود و توصیه‌های نهایی توسط کارگروه از بین آن‌ها انتخاب خواهد شد).

سایر مطالب: گروه سایر مطالب را در دست خواهد گرفت (ادامه خواهد داد).

تصویب گزارش نهایی: پیرو قطعنامه مجمع عمومی به شماره ۷۳/۲۳ گروه باید گزارش خود را به اجلاس هفتاد و پنجم مجمع عمومی ارائه نماید. گروه گزارش خود را زیر این بخش (تصویب گزارش نهایی) در آخرین اجلاس محتوایی خود که از ۶ تا ۱۰ جولای ۲۰۲۰ برگزار می شود، تصویب خواهد نمود.

گفتار سه: کردار نامه ها و کنوانسیون ها

بند یک: کردار نامه بین المللی امنیت اطلاعات سال ۲۰۱۱

ترجمه سند



مجمع عمومی

تاریخ انتشار: ۱۴ سپتامبر ۲۰۱۱

شماره قطعنامه: A/66/359

توزیع: عمومی

زبان: انگلیسی

اجلاس شصت و هشتم

بخش ۹۳ از دستور کار موقت (A/66/150)

تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین الملل.

نامه مورخ ۱۲ سپتامبر ۲۰۱۱ از طرف نمایندگان چین، فدراسیون روسیه، تاجیکستان، ازبکستان خطاب به دبیرکل سازمان ملل.

سال های اخیر شاهد پیشرفت توجه پذیری در دستیابی به توسعه و کاربرد آخرین فناوری های مخابراتی و اطلاعاتی بوده است که این فناوری ها به طور بالقوه می توانند برای مقاصد مغایر با اهداف مربوط به حفظ ثبات و امنیت بین المللی استفاده شوند. بسیار مهم است که به چالش های مشترک در حوزه امنیت اطلاعات کاملاً باید با همکاری بین المللی و روح احترام متقابل پرداخته شود. بدین منظور، چین، روسیه، تاجیکستان و ازبکستان به طور مشترک در قالب قطعنامه مجمع عمومی، یک کردار نامه بین المللی در مورد امنیت اطلاعات را ارائه داده اند و مستلزم هم اندیشی های بین المللی در چارچوب ملل متحد روی چنین کردار نامه بین المللی با هدف دستیابی به نخستین اجماع ممکن در مورد هنجارها و قوانین بین المللی که رفتار دولت ها را در فضای سایبری هدایت می کند، می باشد.

اگر این نامه و ضمیمه آن را به عنوان یکی از اسناد نشست شصت و هشتم مجمع عمومی تحت بخش ۹۳ این دستور کار موقت قرار دهید، بسیار مایه سپاسگزاری خواهد بود.

امضاء: لیو بودونگ: نماینده دائمی جمهوری خلق چین در سازمان ملل متحد، ویتالی چورکین

نماینده دائمی فدراسیون روسیه در سازمان ملل متحد، سراج‌الدین اسلاو: نماینده دائمی جمهوری تاجیکستان در سازمان ملل متحد، مراد عکسراف: نماینده دائمی جمهوری ازبکستان در سازمان ملل متحد

پیوست: نامه مورخ ۱۲ سپتامبر ۲۰۱۱ از طرف نمایندگان دائم چین، فدراسیون روسیه، تاجیکستان و ازبکستان خطاب به دبیر کل سازمان ملل متحد. (اصل به زبان: چینی، انگلیسی و روسی)^۱
کردارنامه بین‌المللی امنیت اطلاعات

مجمع عمومی

با یادآوری قطعنامه‌های خود در مورد نقش علم و فناوری در چارچوب امنیت بین‌المللی که در آن، در کنار موارد دیگر، این امر نیز به رسمیت شناخته شد که پیشرفت‌های علمی و فنی می‌تواند کاربردهای غیر نظامی و نظامی داشته باشد و پیشرفت در علم و فناوری برای برنامه‌های غیر نظامی نیازمند حفظ و تشویق هستند.

باتوجه به اینکه پیشرفت قابل توجهی در توسعه و استفاده از آخرین فناوری‌های اطلاعات و ابزار ارتباطات به دست آمده است؛

با به رسمیت شناختن نیاز به پیشگیری از استفاده بالقوه از فناوری‌های اطلاعات و ارتباطات برای مقاصد ناسازگار با اهداف حفظ ثبات و امنیت بین‌المللی و اینکه ممکن است {این فناوری‌ها} به صورت مخصصانه بر یکپارچگی زیرساخت‌های درون دولت‌ها اثر بگذارد، به امنیت آن‌ها ضرر برساند؛

با تأکید بر نیاز به هماهنگی و همکاری بیشتر بین دولت‌ها در مبارزه با سوءاستفاده مجرمانه از فناوری‌های اطلاعاتی، و در این زمینه، با تأکید بر نقشی که می‌تواند توسط سازمان متحد ملل و دیگر سازمان‌های بین‌المللی و منطقه‌ای ایفا شود؛

با تأکید بر اهمیت امنیت، تداوم و ثبات اینترنت و نیاز به حفاظت از اینترنت و شبکه‌های فناوری اطلاعات و ارتباطات از تهدیدات و آسیب‌پذیری‌ها و با تأیید مجدد نیاز به یک درک

مشترک از مسائل {موضوعات} امنیتی اینترنت و همکاری بیشتر در سطوح ملی و بین‌المللی با تأیید مجدد اینکه اقتدار و نهاد سیاسی مربوط به مسائل عمومی حوزه اینترنت حق حاکمیتی دولت‌هایی است که دارای حقوق و مسئولیت‌های بین‌المللی در زمینه مسائل مربوط به سیاست‌گذاری عمومی اینترنت می‌باشند؛

با به رسمیت شناختن اینکه اعتماد و امنیت در استفاده از فناوری‌های اطلاعات و ارتباطات از ستون‌های اصلی جامعه اطلاعاتی هستند و اینکه یک فرهنگ جهانی مستحکم دیگر امنیت سایبری نیاز به تشویق، ترویج، توسعه و اجرای قوی دارد

بر اساس قطعنامه ۶۴/۲۱۱ مورخ ۲۱ دسامبر ۲۰۰۹ مجمع عمومی تحت عنوان «ایجاد یک فرهنگ جهانی امنیت سایبری و ارزیابی تلاش‌های ملی برای حفاظت از زیرساخت‌های اطلاعات حساس»،

با تأکید بر نیاز به تلاش‌های بیشتر برای از بین بردن شکاف دیجیتالی با تسهیل انتقال فناوری اطلاعات و ظرفیت‌سازی به کشورهای در حال توسعه در حوزه‌های امنیت سایبری، با بهترین شیوه‌ها و آموزش، مطابق با قطعنامه ۶۴/۲۱۱، کردارنامه امنیت بین‌الملل اطلاعات به شکل زیر مورد پذیرش قرار می‌گیرد:

ابعاد و اهداف

هدف از کردارنامه حاضر شناسایی و تعیین حقوق و مسئولیت‌های دولت‌ها در فضای اطلاعات است، ارتقای رفتار سازنده و مسئولانه و افزایش همکاری آن‌ها در مقابله با تهدیدات و چالش‌های مشترک در فضای اطلاعات به‌منظور حصول اطمینان از اینکه فناوری‌های اطلاعات و ارتباطات از جمله شبکه‌ها، با هدف حفظ امنیت و ثبات بین‌المللی، منحصراً برای توسعه و رفاه اقتصادی و اجتماعی و رفاه مردم استفاده می‌شود.

پیوستن به کردارنامه، داوطلبانه و برای همه کشورها مفتوح است.

کردارنامه

هر کشوری که به طور داوطلبانه این کردارنامه را تصویب می‌کند متعهد می‌شود:

الف) مطابق با منشور ملل متحد و هنجارهای شناخته شده جهانی که روابط بین‌الملل را راهبری می‌کنند، از جمله احترام به حاکمیت، تمامیت ارضی و استقلال سیاسی همه دولت‌ها، احترام به حقوق بشر و آزادی‌های اساسی و احترام به تنوع تاریخی، فرهنگ و نظام‌های اجتماعی همه کشورها؛

ب) عدم استفاده از فناوری‌های اطلاعات و ارتباطات، از جمله شبکه‌ها، برای انجام فعالیت‌های خصمانه یا اقدامات تجاوزکارانه، {فعالیت‌هایی که باعث} اعمال تهدیدات علیه امنیت و صلح بین‌المللی یا اشاعه سلاح‌های اطلاعاتی یا فناوری‌های مرتبط {می‌شوند}؛

ج) همکاری در مقابله با اقدامات مجرمانه و تروریستی که از فناوری‌های اطلاعات و ارتباطات از جمله شبکه‌ها، استفاده می‌کنند و {همکاری} در محدود کردن انتشار اطلاعاتی که باعث ایجاد تروریسم، تجزیه‌طلبی یا افراطی‌گرایی یا تضعیف ثبات سیاسی، اقتصادی و اجتماعی و نیز محیط فرهنگی و معنوی سایر کشورها می‌شود؛

د) تلاش جهت حصول اطمینان از امنیت زنجیره تأمین محصولات و خدمات فناوری اطلاعات و ارتباطات، به‌منظور محافظت در برابر استفاده سایر دولت‌ها از منابع، زیرساخت‌های حیاتی، فناوری‌های اصلی و سایر پیشرفت‌های خود برای تضعیف حقوق کشورهایی که کردارنامه را پذیرفته‌اند، تلاش جهت کنترل مستقل فناوری‌های اطلاعات و ارتباطات یا {کنترل} تهدید امنیت سیاسی، اقتصادی و اجتماعی سایر کشورها؛

ه) برای تأیید مجدد کلیه حقوق و مسئولیت‌های دولت‌ها در خصوص حفاظت از فضای اطلاعاتی و زیرساخت‌های حساس اطلاعاتی خود {در برابر} تهدیدات، حمله و خرابه‌کاری مطابق با قوانین و مقررات مرتبط؛

و) برای احترام کامل به حقوق و آزادی فضای اطلاعات، از جمله حقوق و آزادی در جستجو، دریافت و انتشار اطلاعات با فرض پیروی از قوانین و مقررات ملی مرتبط؛

ز) برای ارتقای ایجاد {استقرار} یک سیستم مدیریت چندجانبه، شفاف دموکراتیک و بین‌المللی

اینترنت جهت حصول اطمینان و تضمین توزیع عادلانه منابع، تسهیل دسترسی برای همه و اطمینان از عملکرد ایمن و پایدار اینترنت؛

ج) برای هدایت تمامی عناصر جامعه از جمله شرکای اطلاعات و ارتباطات خود در بخش خصوصی، جهت درک نقش و مسئولیتشان در خصوص امنیت اطلاعات به منظور تسهیل ایجاد یک فرهنگ امنیت اطلاعات و حفاظت از زیرساخت‌های اطلاعات حساس؛

ط) برای کمک به کشورهای در حال توسعه در تلاش‌های خود جهت ارتقای ظرفیت‌سازی در امنیت اطلاعات و از بین بردن شکاف دیجیتال؛

ی) برای تقویت همکاری دوجانبه، منطقه‌ای و بین‌المللی، ارتقای نقش مهم سازمان ملل متحد در تدوین و شکل‌دهی به هنجارهای بین‌المللی، حل و فصل‌های صلح‌آمیز اختلافات بین‌المللی و بهبود همکاری‌های بین‌المللی در حوزه امنیت اطلاعات و ارتقای هماهنگی میان سازمان‌های بین‌المللی؛

ک) برای حل و فصل اختلافات ناشی از به کار بردن این کردارنامه از طریق ابزار صلح‌آمیز و پرهیز از تهدید یا استفاده از زور.

بند دو: کردار نامه بین‌المللی امنیت اطلاعات سال ۲۰۱۵

ترجمه سند



مجمع عمومی

تاریخ انتشار: ۱۳ ژانویه ۲۰۱۵

شماره قطعنامه: A/69/273

زبان: انگلیسی

اجلاس شصت و نهم

دستور کار ۹۱

تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌الملل

نامه مورخ ۹ ژانویه ۲۰۱۵ از طرف نمایندگان دائم چین، قزاقستان، قرقیزستان، فدراسیون روسیه، تاجیکستان و ازبکستان خطاب به دبیرکل سازمان ملل متحد.

سال‌های اخیر شاهد پیشرفت توجه‌پذیری در توسعه و کاربرد فناوری اطلاعات و ارتباطات جدید بوده است که این فناوری‌ها به طور بالقوه می‌تواند برای مقاصد مغایر با اهداف مربوط به حفظ ثبات و امنیت بین‌المللی استفاده شود. در حال حاضر در مورد نیاز به تقویت همکاری بین‌المللی و تدوین هنجارهای بین‌المللی مربوط، به منظور حل چالش‌های مشترک در زمینه امنیت اطلاعات، یک اجماع بین‌المللی در حال شکل‌گیری است. به همین منظور، چین، روسیه، تاجیکستان و ازبکستان در نشست شصت و ششم جلسات مشترک خود در سال ۲۰۱۱ به مجمع عمومی سازمان ملل متحد کردارنامه بین‌المللی مربوط به امنیت اطلاعات را ارائه دادند که متعاقباً توسط قرقیزستان و قزاقستان مورد حمایت واقع شد.

کردارنامه باعث جلب توجه بین‌المللی گسترده‌ای گردید و بحث‌های متعاقب آن به‌عنوان سند عمومی منتشر گردید. (A/69/66/35) در نتیجه، ما با در نظر گرفتن نظرها و پیشنهادهای همه کشورهای کردارنامه را اصلاح کردیم. اکنون ما افتخار داریم که به همراه این نامه، نسخه‌های چینی، روسی و انگلیسی کردارنامه تجدید نظر شده را پیوست کنیم (به ضمیمه مراجعه کنید). با این کار، ما امیدواریم که بحث‌های بین‌المللی در مورد هنجارهای بین‌المللی امنیت اطلاعات را پیش ببریم و به ایجاد توافق اولیه در مورد این موضوع کمک کنیم.

اگر این نامه و ضمیمه آن را به‌عنوان یکی از اسناد جلسه شصت‌ونهم مجمع عمومی تحت ماده ۹۱ این دستورالعمل قرار دهید، بسیار مایه سپاسگزاری خواهد بود.

امضاء

لیوجیوی: نماینده دائمی جمهوری خلق چین در سازمان ملل متحد؛
 کایرات عبدالرحمان اف: نماینده دائمی جمهوری قزاقستان در سازمان ملل متحد؛
 تالابگ کیدیوروف: نماینده دائم جمهوری قرقیزستان در سازمان ملل متحد؛
 ویتالی چورکین: نماینده دائمی فدراسیون روسیه در سازمان ملل متحد؛
 محمدمین محمدمینوف: نماینده دائمی جمهوری تاجیکستان در سازمان ملل متحد؛
 مظفریگ ماداراخیمف: نماینده دائمی جمهوری ازبکستان در سازمان ملل متحد؛
 پیوست: نامه مورخ ۹ ژانویه ۲۰۱۵ از طرف نمایندگان دائم چین، قزاقستان، قرقیزستان؛
 فدراسیون روسیه، تاجیکستان و ازبکستان خطاب به دبیرکل سازمان ملل متحد (اصل به زبان: چینی و روسی).

کردار نامه بین‌المللی امنیت اطلاعات

مجمع عمومی،

با یادآوری قطعنامه‌های خود در مورد نقش علم و فناوری در زمینه امنیت بین‌المللی که علاوه بر آن، این امر نیز به رسمیت شناخته شده است که پیشرفت‌های علمی و فناورانه می‌تواند کاربردهای غیر نظامی و نظامی داشته باشد و پیشرفت در علم و فناوری برای برنامه‌های غیر نظامی نیازمند حفظ و تشویق هستند.

با یادآوری قطعنامه‌های ۵۳/۷۰ مورخ ۴ دسامبر ۱۹۹۸، ۵۴/۴۹ مورخ ۱ دسامبر ۱۹۹۹، ۵۵/۲۸ مورخ ۲۰ نوامبر ۲۰۰۰، ۵۶/۱۹ مورخ ۲۹ نوامبر ۲۰۰۱، ۵۷/۵۳ مورخ ۲۲ نوامبر ۲۰۰۲، ۵۸/۳۲ مورخ ۸ دسامبر ۲۰۰۳، ۵۹/۶۱ مورخ ۳ دسامبر ۲۰۰۴، ۶۰/۴۵ مورخ ۸ دسامبر ۲۰۰۵، ۶۱/۵۴ مورخ ۶ دسامبر ۲۰۰۶، ۶۲/۱۷ مورخ ۵ دسامبر ۲۰۰۷، ۶۳/۳۷ مورخ ۲ دسامبر

۲۰۰۸، ۶۴/۲۵ مورخ ۲ دسامبر ۲۰۰۹، ۶۵/۴۱ مورخ ۸ دسامبر ۲۰۱۰، ۶۶/۲۴ مورخ ۲ دسامبر ۲۰۱۱، ۶۷/۲۷ مورخ ۳ دسامبر ۲۰۱۲ و ۶۸/۲۴۳ مورخ ۲۷ دسامبر ۲۰۱۳ در مورد تحولات در حوزه اطلاعات و ارتباطات راه دور در چارچوب امنیت بین‌المللی،
باتوجه به اینکه پیشرفت قابل توجهی در توسعه و استفاده از آخرین فناوری‌های اطلاعات و ابزار ارتباطات به دست آمده است؛

با به رسمیت شناختن نیاز به پیشگیری از استفاده بالقوه از فناوری اطلاعات و ارتباطات برای مقاصد ناسازگار با اهداف حفظ ثبات و امنیت بین‌المللی و اینکه ممکن است به صورت مخربی بر یکپارچگی زیرساخت‌های درون دولت‌ها اثر بگذارد، به امنیت آن‌ها ضرر برساند؛
با تأکید بر نیاز به هماهنگی و همکاری بیشتر بین کشورها در مبارزه با سوءاستفاده مجرمانه از فناوری‌های اطلاعاتی، و در این بین، تأکید بر نقش‌هایی که می‌تواند توسط سازمان متحد ملل و دیگر سازمان‌های بین‌المللی و منطقه‌ای ایفا شود؛

با تأکید بر اهمیت امنیت، تداوم و ثبات اینترنت و نیاز به حفاظت از اینترنت و دیگر شبکه‌های فناوری اطلاعات و ارتباطات از تهدیدات و آسیب‌پذیری‌ها و تأیید نیاز به یک درک مشترک از مسائل امنیتی اینترنت و همکاری بیشتر در سطوح ملی و بین‌المللی؛
با تأیید اینکه اقتدار سیاسی مربوط به مسائل عمومی حوزه اینترنت حق حاکمیت دولتی است که دارای حقوق و مسئولیت‌های بین‌المللی در زمینه مسائل مربوط به سیاست‌گذاری عمومی اینترنت می‌باشند؛

با در نظر گرفتن ارزیابی‌ها و توصیه‌های مندرج در گزارش گروه کارشناسان دولتی که در سال ۲۰۱۲ براساس توزیع عادلانه جغرافیایی در اجرای قطعنامه ۶۶/۲۴ تشکیل شده بود و مطابق با دستورالعمل آن، تهدیدات موجود و بالقوه در حوزه امنیت اطلاعات و اقدامات همکاری‌جویانه ممکن برای مقابله با آن‌ها، از جمله هنجارها، قواعد و اصول رفتار مسئولانه دولت و اقدامات اعتمادساز در فضای اطلاعات و مطالعه‌ای در مورد طرح‌های بین‌المللی مربوط با هدف تقویت امنیت جهانی سیستم‌های اطلاعاتی و مخابراتی مورد توجه قرار گرفت؛

با تأکید بر اینکه نیاز به توسعه یک درک مشترک از اینکه چگونه هنجارهای مربوط به استفاده دولت‌ها از فناوری اطلاعات و ارتباطات از حقوق بین‌الملل موجود سرچشمه می‌گیرند، یک اقدام ضروری برای کاهش خطرهای صلح، امنیت و ثبات بین‌المللی است و در رفتار دولت‌ها و استفاده آن‌ها از فناوری‌های اطلاعاتی و ارتباطات مطابق با بند ۱۶ گزارش گروه کارشناسان دولتی (A) ۹۸/۶۸ مورخ ۲۴ ژوئن ۲۰۱۳، به کار خواهد رفت؛

باتوجه به ویژگی‌های منحصر بفرد فناوری اطلاعات و ارتباطات، هنجارهای تکمیلی می‌توانند در طول زمان، باتوجه به بند ۱۶ گزارش گروه کارشناسان دولتی توسعه یابند؛

با به رسمیت شناختن اینکه اعتماد و امنیت در استفاده از فناوری اطلاعات و ارتباطات از ستون‌های اصلی جامعه اطلاعاتی هستند و بنابراین یک فرهنگ جهانی امنیت سایبری نیاز به تشویق، ترویج، توسعه و اجرای قوی دارد بر اساس قطعنامه ۶۴/۲۱۱ مجمع عمومی تحت عنوان «ایجاد یک فرهنگ جهانی امنیت سایبری و ارزیابی تلاش‌های ملی برای حفاظت از زیرساخت‌های اطلاعات حساس»؛

با تأکید بر نیاز به تلاش‌های بیشتر برای از بین بردن شکاف دیجیتالی با تسهیل انتقال فناوری اطلاعات و ظرفیت‌سازی به کشورهای در حال توسعه در حوزه‌های امنیت سایبری، با بهترین شیوه‌ها و آموزش، مطابق با قطعنامه مجمع عمومی؛
 کردارنامه زیر مورد پذیرش قرار می‌گیرد:

ابعاد و اهداف

هدف از کردارنامه حاضر شناسایی و تعیین حقوق و مسئولیت‌های دولت‌ها در فضای اطلاعات است، ارتقای رفتار سازنده و مسئولانه در بخش آن‌ها و افزایش همکاری آن‌ها در مقابله با تهدیدات و چالش‌های مشترک در فضای اطلاعات، به‌منظور ایجاد یک محیط اطلاعاتی که صلح‌آمیز، امن، باز و بر پایه همکاری متکی باشد و اطمینان حاصل شود که استفاده از فناوری اطلاعات و ارتباطات و شبکه‌های اطلاعاتی و ارتباطی، توسعه و رفاه اقتصادی و اجتماعی و رفاه مردم را تسهیل می‌کند و در جهت مقابله با اهداف همسو با صلح و امنیت بین‌المللی حرکت نمی‌کند.

پیوستن به کردارنامه، داوطلبانه و برای همه کشورها مفتوح است.

هر کشوری که به طور داوطلبانه این کردارنامه را تصویب می‌کند متعهد می‌شود:

(۱) عمل مطابق با منشور ملل متحد و هنجارهای شناخته شده جهانی که روابط بین‌الملل را تضمین می‌کنند، از جمله احترام به حاکمیت، تمامیت ارضی و استقلال سیاسی همه کشورها، احترام به حقوق بشر و آزادی‌های اساسی و احترام به تنوع تاریخ، فرهنگ و نظام‌های اجتماعی همه کشورها؛

(۲) عدم استفاده از فناوری اطلاعات و ارتباطات و شبکه‌های اطلاعاتی و ارتباطی برای انجام فعالیت‌هایی که مغایر با وظیفه حفظ صلح و امنیت بین‌المللی هستند؛

(۳) عدم استفاده از فناوری اطلاعات و ارتباطات و شبکه‌های اطلاعاتی و ارتباطی برای دخالت در امور داخلی کشورهای دیگر یا با هدف تضعیف ثبات سیاسی، اقتصادی و اجتماعی آن‌ها؛

(۴) همکاری در مبارزه با فعالیت‌های جنایی و تروریستی که از فناوری‌های اطلاعات و ارتباطات و شبکه‌های اطلاعاتی و ارتباطی استفاده می‌کنند و همکاری در محدود کردن انتشار اطلاعاتی که باعث تروریسم، جدایی طلبی و افراط‌گرایی می‌شود، و یا باعث انزجار نفرت بر اساس قومیت، نژاد و مذهب می‌شود؛

(۵) تلاش برای اطمینان از امنیت زنجیره تأمین کالاها و خدمات فناوری اطلاعات و ارتباطات، برای پیشگیری از استفاده سایر کشورها از موقعیت غالب خود در فناوری اطلاعات و ارتباطات، از جمله تسلط بر منابع، زیرساخت‌های حیاتی، فناوری‌های اصلی، اطلاعات و کالاها و خدمات فناوری ارتباطات و خدمات و شبکه‌های اطلاعاتی و ارتباطی به منظور تضعیف حق کشورها در کنترل مستقل کالاها و خدمات فناوری اطلاعات و ارتباطات و یا تهدید امنیت سیاسی، اقتصادی و اجتماعی آن‌ها؛

(۶) تأیید حقوق و مسئولیت‌های همه کشورها، مطابق با هنجارها و قوانین مربوط، دایر بر حفاظت قانونی از فضای اطلاعاتی و زیرساخت‌های حساس اطلاعاتی خود در مقابل آسیب ناشی از تهدیدها، نفوذ، حمله و خرابه‌کاری؛

(۷) به رسمیت شناختن اینکه حقوق یک فرد در محیط غیربرخط باید در محیط برخط نیز

محافظة شود؛ برای احترام کامل به حقوق و آزادی‌های فضای اطلاعات، از جمله حق آزادی جستجو، دریافت و انتقال اطلاعات، با عنایت به این واقعیت که میثاق بین‌المللی حقوق مدنی و سیاسی (ماده ۱۹) به این حق، وظایف و مسئولیت‌های ویژه مربوط می‌شود. این امر ممکن است معلول محدودیت‌های خاصی شود (محدودیت‌های خاصی اعمال شود)، اما این باید فقط در قالب قانونی و لازم‌الرعایه باشند:

(الف) برای احترام به حقوق یا اعتبار دیگران؛

(ب) برای حفاظت از امنیت ملی یا نظم عمومی (ordre public)، یا بهداشت عمومی یا

اخلاق.

(۸) همه کشورها باید نقش یکسان و مسئولیت مساوی در حکمرانی بین‌المللی بر اینترنت، امنیت، تداوم و ثبات آن، و توسعه آن را به نحوی ایفا کنند که به ایجاد و استقرار سازوکارهای حکمرانی بین‌المللی چندجانبه، شفاف و دموکراتیک منجر شود تا از توزیع عادلانه منابع، تسهیل دسترسی برای همه و اطمینان از عملکرد پایدار و ایمن اینترنت اطمینان حاصل شود؛

(۹) همه کشورها باید به طور کامل با سایر طرف‌های ذی‌نفع در تشویق درک عمیق‌تر از همه عناصر در جامعه همکاری کنند، از جمله بخش خصوصی و مؤسسات جامعه مدنی، از مسئولیتشان برای اطمینان از امنیت اطلاعات، توسط ابزارهایی مثل ایجاد یک فرهنگ امنیت اطلاعات و تدارک حمایت از تلاش برای حفاظت از زیرساخت‌های اطلاعاتی حساس؛

(۱۰) برای ایجاد اقدامات اعتمادساز با هدف افزایش پیش‌بینی و کاهش احتمال سوء تفاهم و خطر درگیری. چنین اقداماتی عبارت‌اند از، تبادل داوطلبانه اطلاعات مربوط به راهبردهای ملی و ساختار سازمانی برای اطمینان از امنیت اطلاعات دولت، انتشار کتاب سفید و تبادل بهترین شیوه، هر جا که عملی و قابل توصیه باشد؛

(۱۱) برای کمک به کشورهای در حال توسعه در تلاش برای ارتقای ظرفیت‌سازی در زمینه

امنیت اطلاعات و از بین بردن شکاف دیجیتالی؛

(۱۲) برای تقویت همکاری دوجانبه منطقه‌ای و بین‌المللی، نقش برجسته‌ای به سازمان ملل

متحد در زمینه‌هایی؛ مانند تشویق توسعه استانداردهای حقوقی بین‌المللی برای امنیت اطلاعات

حل مسالمت‌آمیز اختلافات بین‌المللی، بهبود کیفی در همکاری‌های بین‌المللی در زمینه امنیت اطلاعات؛ و تقویت هماهنگی بین سازمان‌های بین‌المللی مربوط؛ اعطا می‌شود.

(۱۳) حل و فصل اختلافات ناشی از استفاده از این کردارنامه از طرق صلح‌آمیز و پرهیز از تهدید یا استفاده از زور.

بند سه: پیش نویس کنوانسیون امنیت بین‌المللی اطلاعات سال ۲۰۱۱

ترجمه سند

تاریخ انتشار: سال ۲۰۱۱

زبان: انگلیسی

اجلاس امنیتی
ایکاترینبورگ روسیه^۱

مقدمه:

دولت‌های عضو کنوانسیون^۲؛

- با عنایت به پیشرفت‌های شایان توجه در گسترش دسترسی به فناوری اطلاعات و ارتباطات و ابزاری که فضای اطلاعات (فضای تبادل اطلاعات) را می‌سازد؛

با ابراز نگرانی‌های خود از تهدیدات مرتبط با کاربردهای احتمالی این فناوری‌ها و ابزارها برای اهدافی که با تمهیدات تدارک دیده شده برای حفظ امنیت و ثبات بین‌المللی در عرصه نظامی و غیر نظامی ناسازگار است؛

با درک اهمیت امنیت بین‌المللی اطلاعات به‌عنوان یکی از عناصر کلیدی سیستم امنیت بین‌الملل؛

با ابراز اطمینان از اینکه که رشد بیشتر اعتماد و توسعه همکاری بین دولت‌های عضو در خصوص مسائل امنیت بین‌المللی اطلاعات برای اعضا ضروری و مفید است؛

با در نظر گرفتن نقش مهمی که امنیت اطلاعات در تضمین حقوق اساسی بشر و آزادی‌ها ایفا می‌کند؛

با در نظر گرفتن قطعنامه شماره ۴۱/۶۵/A/RES مورخ ۸ دسامبر ۲۰۱۰ مجمع عمومی سازمان ملل تحت عنوان «توسعه در حوزه اطلاعات و ارتباطات راه دور در چارچوب امنیت بین‌المللی»؛
با تلاش به‌منظور محدود سازی تهدیدات بین‌المللی اطلاعات، تحقق امنیت اطلاعات دولت‌های عضو و خلق فضای اطلاعاتی با ویژگی صلح، همکاری و هماهنگی؛

با ابراز تمایل به ایجاد مبنای حقوقی و سازمانی برای همکاری بین دولت‌های عضو در فضای امنیت بین‌المللی اطلاعات، با اشاره به قطعنامه شماره ۲۹/۵۵/A/RES مورخ ۲۰ نوامبر ۲۰۰۰

1 . INTERNATIONAL MEETING of HIGH-RANKING OFFICIALS RESPONSIBLE for SECURITY MATTERS

2 . CONVENTION on INTERNATIONAL INFORMATION SECURITY (CONCEPT)

تحت عنوان «نقش علم و فناوری در بستر امنیت بین‌الملل و خلع سلاح» که در بخشی از آن تصریح شده است که دستاوردهای علم و فناوری می‌تواند کاربردهای غیرنظامی و نظامی داشته باشد و اینکه لازم است برای توسعه علم و فناوری برای کاربردهای غیرنظامی حمایت صورت گیرد؛ - با اذعان به ضرورت جلوگیری از کاربردهای احتمالی فناوری اطلاعات و ارتباطات برای مقاصدی که با تحقق ثبات و امنیت بین‌المللی سازگار نیستند و قادرند اثر منفی بر یکپارچگی زیرساخت‌های دولتی بر جای گذاشته و باعث آسیب به امنیت آن‌ها گردند؛ - با تأکید بر ضرورت افزایش و تقویت هماهنگی بین دولت‌ها در مبارزه علیه کاربرد مجرمانه فناوری اطلاعات و با لحاظ نقشی که سازمان ملل متحد و دیگر سازمان‌های بین‌المللی می‌توانند ایفا کنند؛ با تأکید بر اهمیت عملکرد امن، بدون وقفه و پایدار اینترنت و ضرورت حفاظت از اینترنت و دیگر شبکه‌های اطلاعاتی و ارتباطاتی از اقدامات مضر و تهدیدات آسیب رسان احتمالی؛ با تأیید ضرورت درک مشترک از مسائل امنیت اینترنت و همکاری بیشتر در سطح ملی و بین‌المللی؛

با تأیید دوباره اینکه مرجع سیاسی در ارتباط با موضوعات سیاست دولتی مرتبط با اینترنت حق حاکمیتی دولت‌هاست و دولت‌های کشورهای عضو در ارتباط با مسائل سیاست‌گذاری مرتبط با اینترنت حق و مسئولیت دارند؛

با اذعان به ضرورت اطمینان و امنیت در هنگام استفاده از فناوری اطلاعات و ارتباطات که به مثابه یک بنیان اساسی برای جامعه اطلاعاتی است و وجود آن برای ایجاد انگیزه، شکل‌دهی، توسعه و تشریک مساعی فعالانه جهت ایجاد فرهنگ پایدار جهانی امنیت سایبری لازم است. همچنین باتوجه به قطعنامه شماره ۲۱۱/۶۴/A/RES مورخ ۲۱ دسامبر ۲۰۰۹ تحت عنوان «فرهنگ سازی جهانی در مورد امنیت سایبری و کمک گرفتن (استفاده) از تلاش‌های ملی برای حفاظت از زیرساخت‌های حساس اطلاعاتی»؛

- باتوجه به ضرورت تلاش‌ها برای غلبه بر «شکاف دیجیتالی» به وسیله افزایش سهولت در عرضه فناوری اطلاعات و ارتباطات به کشورهای در حال توسعه و توانمندی‌های آن‌ها در ارتباط با روش‌های پیشرفته و آموزش حرفه‌ای در زمینه امنیت سایبری، همچنین باتوجه به قطعنامه

شماره ۲۱/۶۴/A/RES مورخ ۲۱ دسامبر ۲۰۰۹ تحت عنوان «فرهنگ جهانی امنیت سایبری و کمک گرفتن (استفاده) از تلاش‌های ملی برای حفاظت از زیرساخت‌های حساس اطلاعاتی»؛

- با اعتقاد به ضرورت در اولویت قرار دادن ایجاد یک خط‌مشی عمومی در جهت حمایت اجتماعی علیه اقدامات خلاف قانون در فضای اطلاعات، که شامل تدوین قوانین مربوط و تقویت همکاری‌های بین‌المللی خواهد شد؛

- با به رسمیت شناختن تغییرات جدی ایجاد شده به‌وسیله گسترش فناوری دیجیتال، یکسان‌سازی و تداوم جهانی‌سازی شبکه‌های رایانه‌ها؛

- با ابراز نگرانی از تهدیدات ناشی از کاربرد شبکه‌های کامپیوتری که ممکن است در ارتکاب اقدامات مجرمانه مورد استفاده قرار گیرند و اسناد این جرایم ممکن است در این شبکه‌ها نگهداری شوند و در داخل آن منتشر شوند؛

- با اذعان به ضرورت همکاری بین بخش‌های دولتی و غیردولتی در مبارزه علیه اقدامات غیرقانونی در فضای اطلاعات و ضرورت حفاظت از منافع قانونی اعضا در استفاده و توسعه فناوری اطلاعات و ارتباطات؛

- با اعتقاد به اینکه در مبارزه با اقدامات غیرقانونی در فضای اطلاعات به‌صورت مؤثر به همکاری‌های بین‌المللی که وسیع، پویا و بسیار کارآمد باشند، نیاز است؛

- با اعتقاد به اینکه در زمینه وجود این کنوانسیون برای مبارزه علیه نقض محرمانگی (افشای اسناد محرمانه)، نقض یکپارچگی و نقض قابلیت دسترسی به سیستم‌ها، شبکه‌ها و اطلاعات کامپیوترها و همچنین سواستفاده از سیستم‌ها، شبکه‌ها و اطلاعات به‌وسیله تعیین مجازات چنین اقداماتی که جزئیات آن در این کنوانسیون آمده و تضمین اختیار و صلاحیت لازم و مؤثر در مبارزه با چنین جرایمی از طریق رهگیری، شناسایی و کشف در مورد این جرایم در سطح داخلی و بین‌المللی و از طریق توسعه توافقنامه‌ها به‌منظور همکاری بین‌المللی کارآمد و قابل اعتماد، ضروری است؛

- با در نظر داشتن ضرورت تضمین تعادل مناسب بین حفظ نظم و قانون و حفاظت از حقوق اساسی بشر، همچنان که در میثاق بین‌المللی ۱۹۶۶ حقوق سیاسی و مدنی پیش‌بینی شده است، همچنین در دیگر توافقنامه‌های بین‌المللی در زمینه حقوق بشر که از حقوق افراد و آزادی

عقیده، آزادی بیان که شامل آزادی تحقیق، دریافت کردن و توزیع هر نوع اطلاعات و عقاید، صرف‌نظر از مرزهای ملی، دفاع می‌کند؛

با در نظر داشتن حق زندگی خصوصی (حریم شخصی) و حفاظت از اطلاعات شخصی؛
- باتوجه به کنوانسیون ۱۹۸۹ ملل متحد در زمینه حقوق کودک و کنوانسیون ممنوعیت و اقدام فوری برای از بین بردن بدترین اشکال کار کودکان، مصوب کنفرانس عمومی سازمان جهانی کار به تاریخ ۱۹۹۹؛

با استقبال از وقایع اخیر که رشد بیشتر درک مسائل بین‌المللی و همکاری در باب تقویت مبارزه با اقدامات غیرقانونی در فضای اطلاعات را ممکن ساخته‌اند که شامل اقدامات صورت پذیرفته توسط سازمان ملل، سازمان همکاری‌های شانگهای، اتحادیه اروپا، سازمان همکاری‌های اقتصادی آسیا-اقیانوسیه، سازمان دولت‌های آمریکایی، گروه 8G و دیگر سازمان‌ها و نشست‌ها، بر موارد زیر توافق کردند:

فصل ۱: مفاد اصلی

ماده ۱: موضوع و هدف کنوانسیون

موضوعی که این کنوانسیون می‌خواهد آن را به نظم در آورد فعالیت دولت‌ها به‌منظور تضمین امنیت بین‌المللی اطلاعات است.

هدف این کنوانسیون اقدام علیه استفاده از فناوری اطلاعات و ارتباطات به‌منظور نقض صلح و امنیت بین‌المللی است و نیز تنظیم اقداماتی برای حصول اطمینان از اینکه فعالیت‌های دولت‌ها در فضای اطلاعات دارای شرایط زیر خواهد بود:

۱. توسعه کلی اقتصادی و اجتماعی
۲. به گونه‌ای اجرا شود که با تلاش‌ها برای حمایت از صلح و امنیت بین‌المللی سازگار باشد؛
۳. مطابقت کلی با اصول و هنجارهای پذیرفته شده حقوق بین‌الملل از جمله اصول مسالمت‌آمیز تنظیم‌کننده کشمکش‌ها و اختلافات، پرهیز از استفاده از زور، عدم دخالت در موضوعات داخلی و احترام به حقوق و آزادی‌های بنیادی بشر؛

۴. موافقت با حق هر فرد در جستجو، دریافت و انتقال اطلاعات و عقاید، همچنان که در اسناد سازمان ملل متذکر شده است، با در نظر داشتن اینکه این حق ممکن است به وسیله قوانین (حفاظت) ملی برای حفاظت از امنیت ملی و اجتماعی هر دولت محدود گردد، و همچنین برای پیشگیری از استفاده نادرست و دخالت غیرمجاز در منابع اطلاعات؛

۵. تضمین تبادل آزاد فناوری و اطلاعات، ضمن حفظ احترام به استقلال دولت‌ها و ویژگی‌های سیاسی، تاریخی و فرهنگی موجود آن‌ها.

ماده ۲: اصطلاحات و تعاریف

اصطلاحات و تعاریف زیر که در این کنوانسیون استفاده می‌شود:

دسترسی به اطلاعات: امکان دریافت و استفاده از اطلاعات

امنیت اطلاعات: حفاظت از منافع اشخاص، جامعه و دولت در یک کشور در برابر اقدامات مخرب و دیگر فعالیت‌های مضر در فضای اطلاعات.

جنگ اطلاعات: درگیری بین دو یا چند دولت در فضای اطلاعات با هدف وارد کردن ضربه مخرب به سیستم اطلاعات، فرایندها و منابع و همچنین ساختارهای مهم حیاتی و دیگر ساختارها؛ تضعیف سیستم‌های اجتماعی، اقتصادی و سیاسی؛ ایجاد کمپین‌های جمعی علیه جمعیت یک دولت به طوری که حکومت و جامعه را بی‌ثبات سازد؛ و نیز مجبور کردن دولت برای تصمیم‌گیری به نفع مخالفان خود.

زیرساخت اطلاعات: مجموعه پیچیده‌ای از ابزارهای فنی و سیستم‌های شکل‌دهی، تبدیل، انتقال، استفاده و ذخیره‌سازی اطلاعات.

سیستم اطلاعات: میزان کل اطلاعات ذخیره شده در یک پایگاه داده و فناوری مورد استفاده برای پشتیبانی از پردازش این اطلاعات.

سلاح اطلاعات (اطلاعاتی): فناوری، ابزارها و روش‌های اطلاعات با هدف استفاده در جنگ اطلاعات

فضای اطلاعات: فضای فعالیت‌های مرتبط با شکل‌گیری، ایجاد، تبدیل، انتقال، استفاده و

ذخیره‌سازی اطلاعات است که تأثیراتی بر آگاهی اجتماعی و فردی، زیرساخت‌های اطلاعاتی و خود اطلاعات دارد.

فناوری اطلاعات و ارتباطات: میزان کل روش‌ها، فرایندهای تولید و برنامه‌ریزی و عناصر فنی که با دارا بودن مجموعه‌ای از اهداف شامل تشکیل، تبدیل، انتقال، استفاده و ذخیره‌سازی اطلاعات، انسجام یافته‌اند.

منابع اطلاعات: یک زیرساخت اطلاعات همچنین خود اطلاعات و جریان آن اطلاعات. محرمانگی اطلاعات: تعهد اجباری یک عضو که اجازه دسترسی به اطلاعات را دارد این اطلاعات بدون اجازه مالک به عضو دیگری منتقل نخواهد شد.

بخش بسیار حساس زیرساخت‌های اطلاعات: یک قسمت (یا عنصر) از زیرساخت‌های اطلاعات که هر گونه اقدامی علیه آن بخش، آثار و پیامدهای مستقیم بر امنیت ملی خواهد داشت که شامل امنیت اشخاص، جامعه و دولت خواهد بود.

امنیت بین‌المللی اطلاعات: وضعیتی از روابط بین‌المللی است که موانع احتمالی در ثبات جهانی یا عوامل موجد تهدیدات امنیتی حکومت‌ها و جامعه جهانی در فضای اطلاعات را از بین ببرد. سوءاستفاده از منابع اطلاعات: استفاده از منابع اطلاعات بدون حقوق لازمه (بدون حق

استفاده) یا نقض قوانین موجود، قوانین ملی یا هنجارهای قانون بین‌الملل؛

اخلال منع نشده در منابع اطلاعات: اقدام غیر قانونی که فرایند شکل‌گیری، پردازش، تبدیل، انتقال، استفاده و ذخیره اطلاعات را تحت تأثیر قرار می‌دهد.

اپراتور سیستم اطلاعات: یک شهروند (به‌صورت انفرادی) یا شرکت که مجری یک سیستم اطلاعاتی است، از جمله پردازش اطلاعات موجود در پایگاه داده آن.

اقدامات غیر قانونی در فضای اطلاعات: استفاده از منابع اطلاعات و/یا فعالیتی که آن‌ها را در فضای اطلاعات برای اهداف غیر قانونی تحت تأثیر قرار می‌دهد.

ارائه اطلاعات: اقداماتی با هدف دریافت اطلاعات به‌وسیله گروهی مشخص یا انتقال اطلاعات به گروهی مشخص.

انتشار اطلاعات: اقداماتی با هدف دریافت اطلاعات به‌وسیله گروهی نامشخص یا انتقال اطلاعات

به گروهی نامشخص.

تروریسم در فضای اطلاعات: استفاده از منابع اطلاعات و /یا فعالیتی که آن‌ها را در فضای اطلاعات برای اهداف تروریستی تحت تأثیر قرار می‌دهد.

تهدید در فضای اطلاعات: عواملی که خطرهایی را برای افراد، اجتماع و دولت و نیز منافع آن‌ها در فضای اطلاعات تحمیل می‌کند.

ماده ۳: استثنائات در اجرای کنوانسیون

این کنوانسیون در موارد زیر به اجرا در نخواهد آمد:

هنگامی که فعالیت‌های مورد نظر در حوزه زیرساخت‌های اطلاعاتی یک دولت، شهروندان یا شرکت‌های تحت صلاحیت آن دولت صورت پذیرد و تأثیر آن اقدامات تنها توسط شهروندان و شرکت‌های تحت قلمرو حاکمیتی آن دولت احساس شود و هیچ دولت دیگری، مدارک مشته ای دال بر صلاحیتش اقامه ننماید.

ماده ۴: تهدیدات اصلی علیه صلح و امنیت بین‌المللی در فضای اطلاعات

موارد زیر به‌عنوان تهدیدات اصلی در فضای اطلاعات به نظر می‌رسند که می‌توانند به صلح و ثبات بین‌المللی آسیب برسانند:

۱. استفاده از فناوری اطلاعات و ابزارهای ذخیره‌سازی و انتقال اطلاعات برای مشارکت در فعالیت‌ها و اقدامات خصمانه و تجاوز کارانه؛
۲. اتخاذ رفتار مخرب و هدفمند در فضای اطلاعات علیه ساختارهای مهم و حساس دولت دیگر؛
۳. استفاده غیرقانونی از منابع اطلاعات دیگر حکومت‌ها بدون اجازه از آن حکومت، در فضای اطلاعات جایی که آن منابع موقعیت مکانی دارند؛
۴. فعالیت در فضای اطلاعات در جهت تخریب نظام اجتماعی، اقتصادی و سیاسی دیگر دولت‌ها و به راه انداختن تبلیغات روانی بر علیه جمعیت (اتباع) یک دولت با هدف بی‌ثبات‌سازی اجتماعی؛
۵. استفاده از فضای بین‌المللی اطلاعات توسط ساختارهای دولتی و غیر دولتی، سازمان‌ها،

- گروه‌ها و افراد برای مقاصد تروریستی، افراط‌گری یا دیگر اهداف مجرمانه؛
۶. انتشار اطلاعات به خارج از مرزهای ملی به روشی مغایر با اصول و هنجارهای حقوق بین‌الملل و همچنین قوانین ملی دولت مربوط؛
۷. استفاده از زیرساخت‌های اطلاعات به منظور انتشار اطلاعات به قصد ایجاد التهاب و کشمکش ملی، قومی یا درگیری مذهبی، محتواهای مکتوب با مضامین نژادپرستانه و هراس‌آلود، تصاویر یا دیگر شیوه‌های بیان عقاید و نظرها که موجب ترویج، توانمندی یا تحریک تنفر، تبعیض یا خشونت علیه هر فرد یا گروه باشد، اگر دلایل حمایت بر اساس نژاد، رنگ پوست، منشأ ملی یا قومی یا مذهبی باشند؛
۸. دستکاری جریان اطلاعات در فضای اطلاعات دیگر دولت‌ها، نشر اکاذیب یا پنهان‌سازی اطلاعات با هدف تأثیر منفی بر روح و روان جامعه یا تخریب ارزش‌های فرهنگی سنتی، اخلاقی، رفتاری و زیبایی شناختی و علمی؛
۹. استفاده از فضای اطلاعات و اقدام در آن-ذیل فناوری اطلاعات و ارتباطات و ارتباطات و ابزارهای آن- به منظور آسیب رساندن به حقوق و آزادی‌های اساسی انسان؛
۱۰. ممانعت از دسترسی به فناوری اطلاعات و ارتباطات جدید، ایجاد یک فناوری وابسته دولتی در عصر اطلاعات و در تعارض با منافع دولت دیگر؛
۱۱. توسعه قلمرو اطلاعات و به دست آوردن کنترل بر منابع اطلاعات ملی دیگر دولت‌ها.
- عوامل دیگری که خطر تهدیدات فوق را زیادتر می‌کنند، عبارت‌اند از:
۱. سختی در شناسایی و تشخیص منابع اقدامات خصمانه، مخصوصاً با توجه به رشد فعالیت افراد، گروه‌ها و سازمان‌ها از جمله سازمان‌های جنایتکار که خدمات واسط ارائه می‌دهند، فعالیت‌هایی را به نام دیگران انجام می‌دهند
 ۲. خطر بالقوه‌ای که شامل گنجاندن ظرفیت‌های مخرب اظهارنشده در فناوری اطلاعات و ارتباطات می‌باشد؛
 ۳. سطوح متفاوت استفاده از فناوری اطلاعات و ارتباطات و امنیت آن‌ها، در دولت‌های مختلف (ناابرابری دیجیتال)؛

۴. تفاوت در قوانین و رویه‌های ملی در مورد تأسیس یک زیرساخت امن با قابلیت بازیافت سریع اطلاعات.

ماده ۵. اصول اصلی تضمین امنیت بین‌المللی اطلاعات

فضای اطلاعات به‌طور کلی به انسان تعلق دارد. امنیت آن در تضمین توسعه پایدار تمدن جهانی نقش مهمی دارد.

برای ایجاد و تقویت جو اطمینان در فضای اطلاعات، دولت‌های عضو باید اصول زیر را رعایت نمایند:

۱. فعالیت‌های هر دولت عضو در فضای اطلاعات باید توسعه اقتصادی و اجتماعی را ارتقای دهد و باید با اهداف حفظ صلح و امنیت جهانی سازگار باشد و با اصول به رسمیت شناخته شده جهانی و هنجارهای حقوق بین‌الملل مطابقت داشته باشد از جمله اصول حل و فصل صلح‌آمیز کشمکش و درگیری، عدم استفاده از زور در روابط بین‌الملل، عدم دخالت در سیاست خارجی دیگر اعضا و احترام به حاکمیت دولت‌ها و حقوق و آزادی‌های اساسی بشر؛

۲. در عین حال که آن‌ها سیستم امنیت بین‌المللی اطلاعات را شکل می‌دهند، دولت‌های عضو باید بر اساس اصول غیر قابل تقسیم امنیت راهنمایی شوند، این امر بدان معناست که امنیت هر دولت با امنیت همه دولت‌های دیگر و کل جامعه بین‌المللی به شکل جدایی‌ناپذیری در هم تنیده است و امنیت آن‌ها به هزینه امنیت کشورهای دیگر تقویت نخواهد شد؛

۳. هر دولت عضو باید برای غلبه بر اختلاف در سطح تجهیزات سیستم‌های ملی اطلاعات به‌وسیله فناوری اطلاعات و ارتباطات مدرن و برای کاهش شکاف دیجیتالی با هدف کاهش سطح تهدیدات عمومی در فضای اطلاعات، تلاش نماید؛

۴. همه دولت‌های عضو در فضای اطلاعات از حاکمیت برابر برخوردارند، حقوق و وظایف برابر دارند و دارای حقوق برابر به‌عنوان ذی‌نفعان در فضای اطلاعات صرف نظر از تفاوت‌های اقتصادی، سیاسی، اجتماعی و دیگر تفاوت‌هایشان دارند؛

۵. هر کشور عضو حق دارد هنجارهای حاکم را ایجاد کند و فضای اطلاعاتی خود را طبق قوانین ملی خود حکمرانی کند حاکمیت و قوانین دولت بر زیرساخت‌های اطلاعات واقع در

محدوده قلمرو آن دولت و یا در محدوده تحت صلاحیت آن اعمال و اجرا می‌شود. دولت‌های عضو باید در جهت هماهنگی قوانین ملی تلاش نمایند؛ تفاوت‌ها نباید موانعی در مسیر ایجاد یک فضای اطلاعات امن و قابل اطمینان باشند؛

۶. هر دولت عضو باید اصل مسئولیت در قبال فضای اطلاعاتی خود را مورد نظر قرار دهد از جمله مسئولیت امنیت فضای اطلاعات و ماهیت اطلاعاتی که در آن برقرار است؛

۷. هر دولت عضو حق توسعه فضای اطلاعاتش بدون دخالت خارجی را دارد و هر دولت دیگر باید به آن حق مطابق با اصل تساوی حقوق و تعیین سرنوشت مردم که در منشور سازمان ملل نیز تصریح شده است احترام بگذارد؛

۸. هر دولت عضو، با لحاظ منافع قانونی در امنیت دیگر دولت‌ها، می‌تواند آزادانه و مستقل منافعی را در حمایت از امنیت اطلاعات، بر اساس حاکمیت برابر و همچنین انتخاب آزادانه روش‌ها تعیین کند تا از این طریق درباره تأمین امنیت اطلاعات خود مطابق با حقوق بین‌الملل اطمینان حاصل کند.

۹. هر دولت عضو تصدیق می‌کند که متجاوز «جنگ اطلاعاتی» یک جرم علیه صلح و امنیت بین‌المللی است؛

۱۰. فضای اطلاعات دولت‌های عضو نباید در نتیجه تهدید به زور یا استفاده از زور باشد، تحت تملک دیگر اعضا قرار گیرد؛

۱۱. هر دولت عضو حق لاینفکی درباره دفاع از خود در مقابل اقدامات تهاجمی که علیه فضای اطلاعاتش صورت می‌گیرد؛ را دارد، این در صورتی است که منبع تجاوز را به‌طور قابل اعتمادی بتوان تعیین کرد. ضمن اینکه اقدامات تلافی‌جویانه نیز باید متناسب باشد.

۱۲. هر دولت عضو ظرفیت نظامی خود در فضای اطلاعات را از طریق روش‌های ملی و با لحاظ منافع قانونی در امنیت دیگر دولت‌ها و همچنین لحاظ ضرورت تلاش برای تقویت امنیت و صلح بین‌المللی تعیین خواهد کرد، هیچ یک از دولت‌های عضو برای تسلط‌یافتن بر فضای اطلاعات دیگر اعضا، تلاش نخواهد کرد؛

۱۳. یک دولت عضو می‌تواند در چارچوب یک توافق‌نامه، نیروها و ادوات خود را برای تضمین

- امنیت اطلاعات در قلمرو دولت دیگری مستقر کند. این امر بر اساس مذاکرات داوطلبانه از طرف هر دو عضو و نیز در چارچوب حقوق بین‌الملل صورت می‌پذیرد؛
۱۴. هر دولت عضو اتخاذ اقدامات ضروری به‌منظور حصول اطمینان از اینکه فعالیت‌های سیستم بین‌المللی اطلاعات، ابزارهای تبادل بین‌المللی اطلاعات از جمله تبادل اطلاعات با اهداف علمی و آموزشی بدون دخالت ادامه خواهد یافت اتخاذ خواهد کرد. بر اساس درک این موضوع که چنین دخالتی می‌تواند تأثیرات منفی بر کل فضای اطلاعات داشته باشد.
۱۵. دولت‌های عضو باید از توسعه فنی و علمی مرتبط با اکتشافات در فضای اطلاعات، همچنین فعالیت‌های آموزشی، در جهت شکل‌دهی فرهنگ جهانی امنیت سایبری حمایت و تشویق نمایند؛
۱۶. هر دولت عضو، در حد توانایی و امکانات خود، تضمین خواهد کرد که از حقوق و آزادی‌های ابتدایی بشر، حقوق و آزادی‌های شهروندی و حقوق مالکیت معنوی (شامل اختراعات، فناوری‌ها، اسرار تجاری، علائم تجاری و کپی‌رایت) در فضای اطلاعاتشان حمایت می‌کنند؛
۱۷. هر دولت عضو آزادی بیان و اظهار عقیده و همچنین حفاظت در مقابل مداخلات غیرقانونی در زندگی خصوصی شهروندان را تضمین می‌نماید؛
۱۸. هر دولت عضو ایجاد توازن بین حقوق اساسی بشری و اقدامات مؤثر به‌منظور مقابله با استفاده تروریستی از فضای اطلاعات را هدف خود قرار می‌دهد؛ {مترجم: به بهانه مبارزه با تروریسم، حقوق اساسی افراد را تضییع نکند.}؛
۱۹. دولت‌های عضو به‌جز در موارد اقدام برای حفاظت از امنیت ملی و اجتماعی یا پیشگیری از استفاده غیرقانونی اخلاص منع نشده در زیرساخت‌های اطلاعات ملی خود، حق محدودسازی یا قطع دسترسی شهروندان به فضای اطلاعات را ندارند؛
۲۰. دولت‌های عضو مشارکت بین مشاغل و جامعه مدنی در فضای اطلاعات را تشویق می‌کنند.
۲۱. دولت‌های عضو به مسئولیت خود برای حصول اطمینان از اطلاع و آگاهی شهروندان، نهادهای عمومی و دولتی، دیگر دولت‌ها و جامعه جهانی در مورد تهدیدات جدید فضای اطلاعات و روش‌های شناخته شده افزایش سطح امنیت آن‌ها، واقف‌اند.

فصل ۲: اقدامات اصلی برای جلوگیری یا حل و فصل درگیری‌های نظامی در فضای اطلاعات

ماده ۶: اقدامات اصلی برای جلوگیری از درگیری نظامی در فضای اطلاعات

به موجب اصول مندرج در ماده ۵، دولت‌های عضو باید اقداماتی را برای پیش‌بینی و ترسیم درگیری‌های بالقوه در فضای اطلاعات و اتخاذ اقدامات مشترک صلح‌آمیز برای جلوگیری از آن‌ها و حل مسالمت‌آمیز بحران‌ها و اختلافات به انجام رسانند.

بدین منظور، دولت‌های عضو باید:

۱. برای تضمین امنیت بین‌المللی اطلاعات برای حفاظت از صلح و امنیت جهانی و مشارکت در پیشرفت و ثبات اقتصاد جهانی، رفاه عمومی مردم جهان و همکاری‌های غیر تبعیض‌آمیز بین‌المللی همکاری کنند؛

۲. تمامی گام‌های ضروری را برای پیشگیری از هرگونه فعالیت اطلاعاتی مخرب، بردارند که از قلمرو آن‌ها ناشی شده یا از استفاده از زیرساخت‌های اطلاعات در حوزه صلاحیت آن‌ها سرچشمه گرفته باشد، همچنین در شناسایی محل سیستم‌های مهاجم که در حوزه قلمرو سرزمینی آنان قرار گرفته‌اند، در دفع این حملات و رفع نتایج آن‌ها همکاری کنند؛

۳. از توسعه و پذیرش طرح‌ها و دکترین‌هایی که قادر به افزایش تهدیدات در فضای اطلاعات، اختلال در رابطه بین دولت‌ها یا محرک و دامن‌زننده جنگ اطلاعات هستند، خودداری کنند؛

۴. از هرگونه فعالیت در جهت نقض کلی یا جزئی تمامیت و یکپارچگی فضای اطلاعات دیگر دولت‌ها، خودداری کنند؛

۵. از استفاده از فناوری اطلاعات و ارتباطات برای مداخله در امور داخلی دیگر دولت‌ها، خودداری کنند؛

۶. از تهدید به استفاده از زور یا نفس استفاده از زور در روابط بین‌الملل علیه فضای اطلاعات هر کشور دیگر، با هدف نقض حریم اطلاعات آن کشور یا تحت عنوان ابزار حل مناقشه، خودداری کنند؛

۷. از سازماندهی یا تشویق هر نیروی بی‌ضابطه که برای فعالیت‌های دارای اهداف غیر قانونی در فضای اطلاعات دیگر کشورها سازمان دهی شده‌اند، خودداری کنند؛

۸. از تهمت همچنین عدم استفاده از توهین یا تبلیغات خصمانه برای مداخله در امور داخلی دیگر دولت‌ها، خودداری کنند؛
۹. در خصوص اقدام علیه اشاعه و نشر اکاذیب یا پیام‌های تحریف شده که می‌توانند همانند یک ابزار برای دخالت در امور داخلی دیگر دولت‌ها یا تخریب صلح و امنیت جهان مورد توجه قرار گیرند، حق و وظیفه دارند؛
۱۰. به منظور محدودسازی اشاعه «تسلیحات اطلاعات» و فناوری تولید آن، اقداماتی انجام دهند.

ماده ۷: اقدامات برای حل درگیری‌های نظامی در فضای اطلاعات

۱. دولت‌های عضو باید درگیری‌هایشان در فضای اطلاعات را ابتدائاً به‌وسیله مذاکره، تحقیق و بررسی، میانجی‌گری، مصالحه، داور، دادرسی، تجدید نظر، مراجعه به نهادها یا موافقت‌نامه‌ها منطقه‌ای یا به‌وسیله دیگر ابزارهای صلح‌آمیز که آن‌ها انتخاب نمایند تا بدینوسیله صلح و امنیت جهانی در مخاطره قرار نگیرد؛
۲. در هر درگیری بین‌المللی، حق دولت‌های عضو که درگیر جنگ هستند برای انتخاب ابزارهای «جنگ اطلاعات» توسط هنجارهای قابل اجرای حقوق بین‌الملل بشردوستانه محدود گشته است.

فصل ۳: اقدامات اصلی برای جلوگیری از استفاده از فضای اطلاعات برای اهداف تروریستی

ماده ۸: استفاده از فضای اطلاعات برای اهداف تروریستی

دولت‌های عضو به امکان استفاده از فضای اطلاعات برای فعالیت‌های تروریستی اذعان دارند.

ماده ۹: اقدامات اصلی برای جلوگیری از استفاده از فضای اطلاعات برای اهداف تروریستی

برای جلوگیری از استفاده از فضای اطلاعات برای مقاصد تروریستی، دولت‌های عضو باید:

۱. برای جلوگیری از استفاده از فضای اطلاعات برای مقاصد تروریستی و اذعان به ضرورت تلاش‌های مشترک و قاطع برای نیل به این هدف؛ اقداماتی انجام دهند.

۲. برای اتخاذ رویکردهای یکسان به منظور از کار انداختن منابع اینترنتی یک ماهیت؛ تروریستی، تلاش کنند.

۳. نیاز به تأسیس و توسعه تبادل اطلاعات در مورد امکان حملات کامپیوتری، علائم، واقعیت ها، روش ها و ابزار استفاده از اینترنت برای اهداف تروریستی و همچنین در مورد مقاصد و فعالیت‌های سازمان‌های تروریستی در فضای اطلاعات، همچنین نیاز به تبادل تجارب و بهترین نحوه اقدام برای پایش منابع اینترنت، پیدا کردن و پایش محتوای وب را تأیید کنند و به ضرورت تلاش‌های مشترک وقاطع برای نیل به این هدف؛ سایت‌های دارای ماهیت تروریستی، انجام تحقیقات جنایی توسط کارشناسان این فضا و تدوین مقررات قانونی و تأسیس سازمان‌هایی که محور فعالیت آن‌ها جلوگیری از استفاده از فضای اطلاعات برای اهداف تروریستی است، اذعان کنند؛

۴. رویه‌ها و مراحل قانونی یا سایر اقداماتی که ممکن است برای صدور مجوز به نهادهای اجرای قانون جهت انجام تحقیقات و دیگر فعالیت‌های مرتبط در جهت جلوگیری و سرکوب اقدامات تروریستی در فضای اطلاعات و از بین بردن عواقب آن‌ها، ضرورت داشته باشد را انجام دهند، همچنین برای مجازات افراد و سازمان‌های مجرمی که این اقدامات را مرتکب می‌شوند؛
۵. برداشتن گام‌های لازم برای قانونگذاری و سایر اقداماتی که دسترسی قانونی به بخش‌های خاصی از زیرساخت‌های اطلاعاتی و ارتباطی در قلمرو کشورهای عضو که به صورت قانونی در فعالیت‌های تروریستی در فضای اطلاعات به کار رفته را تضمین خواهد کرد. همچنین اگر در جهت ارتکاب فعالیت‌های تروریستی در سایر جاها به کار گرفته شده اند که این امر در راستای ارتکاب اقدامات تروریستی بوده یا در خدمت سازمان‌ها یا گروه‌های تروریستی یا اشکال انفرادی تروریسم بوده است را نیز شامل می‌شود.

فصل ۴: اقدامات اصلی برای مقابله با فعالیت‌های غیر قانونی در فضای اطلاعات

ماده ۱۰: اقدامات اصلی برای مقابله با فعالیت‌های غیر قانونی در فضای اطلاعات

برای مقابله با فعالیت‌های غیر قانونی در فضای اطلاعات دولت‌های عضو باید:

۱. برای جرم‌انگاری استفاده از منابع اطلاعات و/یا دستکاری کردن آن‌ها در فضای اطلاعات برای اهداف غیر قانونی که شامل انتشار غیر مجاز اطلاعات، نقض محرمانگی و تخریب انسجام اطلاعات یا از بین بردن امکان دسترسی به اطلاعات تلاش کنند و همچنین جهت تصریح مسئولیت و جلوگیری افراد از ارتکاب، تلاش، مشارکت یا تحریک به اقدامات مجرمانه و اقدامات خطرناک اجتماعی در فضای اطلاعات گام‌های قانونی یا دیگر اقدامات لازم را بردارند؛
۲. تدابیر قانونی یا دیگر اقدامات را به‌منظور تضمین اینکه متجاوزان در فضای اطلاعات به کیفی مؤثر، بازدارنده و متناسب خواهند رسید انجام دهند.

ماده ۱۱: اقدامات ناظر بر سازمان‌دهی رویه‌های مربوط به جرم

برای سازمان‌دهی رویه‌های مربوط به جرم، دولت‌ها باید:

۱. برای تعیین ضوابط و رویه‌هایی به‌منظور انجام بازجویی و تحقیقات فردی یا آیین دادرسی در مورد ارتکاب جرائم و فعالیت‌های مخرب اجتماعی در فضای اطلاعات، تدابیر قانونی یا دیگر اقدامات اتخاذ کنند؛
۲. اطمینان از تصریح، اجرا و اعمال ضوابط و رویه‌های لازم در انجام بازجویی و تحقیقات راجع به جرایم فردی یا آیین دادرسی مربوط به ارتکاب جرائم و فعالیت‌های مخرب اجتماعی در فضای اطلاعات مطابق با مقررات و ضمانت‌های مندرج قوانین دولت و حصول اطمینان از سطح مناسب حفاظت از حقوق و آزادی‌های بشری، و همچنین اصل تناسب {جنایت و مجازات}، داشته باشند؛
۳. برای توانمندسازی مراجع انتظامی دولت در جهت اقدام سریع به‌منظور حفاظت از اطلاعات معین و خاص، از جمله جریان اطلاعات ذخیره شده در زیرساخت‌های اطلاعاتی و ارتباطی، وقتی دلایل قانع‌کننده‌ای وجود دارد که این اطلاعات به‌صورت ویژه‌ای در معرض آسیب‌پذیری در جهت از بین رفتن و دستکاری می‌باشند، تدابیر قانونی یا دیگر اقدامات اتخاذ کنند؛
۴. برای تضمین دسترسی بموقع مراجع انتظامی دولت یا اشخاص تعیین شده توسط این نهادها به میزان کافی از داده‌ها در جریان اطلاعات برای شناسایی ارائه‌کنندگان خدمات و مسیر یک پیام خاص در فضای اطلاعات مربوط به خود؛ تدابیر قانونی یا دیگر اقدامات اتخاذ کنند؛

۵. لازم جهت توانمندسازی نهادهای انتظامی دولت جهت انجام بررسی‌های لازم یا اخذ مجوز دسترسی های مشابه به سیستم‌های اطلاعاتی و ارتباطی و همچنین اجزا و داده‌های ذخیره شده در این سیستم‌ها، همچنین دسترسی به رسانه‌های ذخیره سازی که ممکن است حاوی داده‌های مورد درخواست باشد، اقدامات قانونی یا دیگر اقدامات لازم اتخاذ کنند. این موارد می‌تواند در قلمرو حاکمیتی یک دولت عضو باشد. ضمن اینکه سایر داده‌ها و سیستم‌های اطلاعاتی و ارتباطی فضای اطلاعاتی که به طور منطقی در ذخیره داده‌های مورد نظر دخیل هستند؛ ممکن است مورد سؤال و درخواست قرار گیرد.

۶. لازم جهت توانمندسازی نهادهای انتظامی دولت جهت درخواست از اشخاص موجود در قلمرو آن کشور و داشتن اطلاعات در مورد عملکرد سیستم های اطلاعاتی و ارتباطی مربوط، ابزارهای حفاظتی و ذخیره‌سازی داده‌ها در این سیستم‌ها، انتشار اطلاعات که به مقامات مربوط، این اجازه را بدهد که در حیطه اختیارات خود به منظور انجام تحقیقات جنایی فردی یا آیین دادرسی محاکمات در موارد ارتکاب جنایت و اقدامات اجتماعی خطرناک در فضای اطلاعات وارد عمل شوند، اقدامات قانونی یا دیگر اقدامات لازم اتخاذ کنند؛

۷. جهت توانمندسازی نهادهای انتظامی دولت برای جمع‌آوری و ثبت اطلاعات با ابزارهای تکنولوژیک در قلمرو دولت مربوط و همچنین درخواست اقدام مشابه از ارائه دهندگان این خدمات تا به صورت مداوم با مقامات مجری قانون در کشور عضو همکاری نمایند، اقدامات قانونی یا دیگر اقدامات لازم اتخاذ کنند.

۸. لازم جهت تعریف و ایجاد صلاحیت برای دولت جهت رسیدگی به هر گونه جنایت و اقدام خطرناک اجتماعی در فضای اطلاعات قلمرو حاکمیتی خود در پهنه کشتی حامل پرچم دولت و پهنه هواپیما یا هر پرنده دیگری که تحت قوانین آن کشور به ثبت رسیده باشد، اقدامات قانونی یا دیگر اقدامات لازم اتخاذ کنند.

اگر اعمال صلاحیت حاکمیتی بر یک جرم اتهامی از سوی بیش از یک دولت عضو مورد درخواست واقع شود دولت‌های ذی‌نفع در این خصوص مشاوره و مذاکره می‌کنند تا در مورد مناسب‌ترین روش اعمال صلاحیت جهت پیگیری جرم اتهامی تصمیم‌گیری شود

فصل ۵: همکاری های بین‌المللی در فضای امنیت اطلاعات بین‌المللی

ماده ۱۲: همکاری بین دولت‌های عضو

۱. دولت‌های عضو طبق مفاد این کنوانسیون یا از طریق دیگر توافقات بین‌المللی با یکدیگر همکاری می‌کنند.

۲. دولت‌های عضو باید بر مبنای داوطلبانه یا براساس عمل متقابل، بهترین روش را در خصوص پیشگیری، تحقیق قانونی و از بین بردن آثار و تبعات جرایم از جمله مواردی که مربوط به تروریسم در فضای اطلاعات می‌شود اتخاذ و مبادله نمایند. کشورهای عضو حق دارند که درخواست نمایند اطلاعاتی را که تهیه و تبادل کرده‌اند به صورت محرمانه نگهداری شود. دولتی که اطلاعات را دریافت می‌کند حق مراجعه به این اطلاعات در مباحث مربوط به همکاری‌های دو جانبه با دولت فراهم کننده را دارد.

ماده ۱۳: اقدامات اعتمادساز در زمینه استفاده نظامی از فضای سایبر

هر دولت عضو باید برای ارتقای اقدامات اعتمادساز در زمینه استفاده نظامی از فضای سایبر تلاش نماید. که شامل اقدامات زیر می‌باشد:

۱. تبادل طرح های امنیت ملی در فضای اطلاعات؛
۲. تبادل بموقع اطلاعات در مورد بحران ها و تهدیدات در فضای اطلاعات و در گام های بعد تشریک مساعی با یکدیگر در خصوص اتخاذ اقداماتی برای مقابله با آنها؛
۳. مشاوره در مورد فعالیت‌های موجود در فضای اطلاعات که ممکن است نگرانی های دولت‌های عضو را افزایش دهد و نیز همکاری بمنظور حل و فصل کشمکش‌هایی که ماهیت نظامی دارند.

ماده ۱۴: مساعدت مشاوره‌ای

دولت‌های عضو باید در هر موضوع مرتبط با اهداف، اجرا و پیاده‌سازی مفاد این کنوانسیون با یکدیگر همکاری و مشاوره داشته باشند.

ماده ۱۵: امضای کنوانسیون

این کنوانسیون باید برای امضای تمامی دولت‌ها مفتوح باشد.

ماده ۱۶: تصویب کنوانسیون

این کنوانسیون برای تصویب عرضه خواهد شد. اسناد تصویب نزد دبیرکل سازمان ملل تودیع خواهد شد.

ماده ۱۷: الحاق به کنوانسیون‌های کنوانسیون

باید برای الحاق دیگر دولت‌ها مفتوح بماند. اسناد الحاق باید به دبیرکل سازمان ملل ارائه گردند.

ماده ۱۸: لازم‌الاجرا شدن

۱. این کنوانسیون باید بعد از سی‌امین روز از تاریخ تودیع بیستمین سند تصویب یا الحاق به دبیرکل سازمان ملل لازم‌الاجرا شود.

۲. هر دولتی که بعد از اجرایی شدن این کنوانسیون، آن را تصویب یا به آن ملحق شود، این کنوانسیون سی‌روز بعد از تصویب یا الحاق توسط آن دولت برای دولت مذکور لازم‌الاجرا خواهد شد.

ماده ۱۹: اصلاح کنوانسیون

۱. هر دولت عضو می‌تواند اصلاحیه مورد نظر خود را به دبیرکل سازمان ملل ارائه نماید. سپس دبیرکل، اصلاحیه پیشنهادی را بین کشورهای عضو توزیع خواهد کرد. ضمن اینکه از آن‌ها خواهد خواست که مشخص کنند آیا موافق برگزاری کنفرانس اعضا برای بررسی و رأی‌گیری در مورد اصلاحات پیشنهادی هستند. کنفرانس اصلاحیه در صورتی تشکیل می‌شود که حداقل یک‌سوم از دولت‌های عضو در مدت ۴ ماه از تاریخ توزیع اصلاحیه ابراز تمایل نمایند. در این صورت دبیرکل موظف است آن کنفرانس را تحت نظر سازمان ملل برگزار کند. هر اصلاحیه‌ای که به‌وسیله

اکثریت نمایندگان حاضر در کنفرانس و شرکت‌کنندگان در رأی‌گیری پذیرفته شود باید برای تصویب به مجمع عمومی ارسال شود.

۲. هر اصلاحیه‌ای وفق بند اول این ماده، بعد از تصویب توسط مجمع عمومی سازمان ملل و رأی مثبت اکثریت دو سوم اعضای کنوانسیون، لازم‌الاجرا خواهد شد.

۳. اصلاحیه‌های لازم‌الاجرا شده، برای دولت‌هایی که آن را پذیرفته‌اند جاری شده و الزام‌آور می‌باشد. حال آنکه دیگر دولت‌های عضو فقط موظف به اجرای مفاد این کنوانسیون یا دیگر اصلاحیه‌هایی که قبلاً توسط این دولت‌ها پذیرفته شده است می‌باشند. (اصلاحیه برای آن‌ها الزام‌آور نیست).

ماده ۲۰: حق شرط بر کنوانسیون

۱. دبیرکل سازمان ملل متون حق شرط‌ها را که به وسیله دولت‌ها در زمان الحاق و تصویب صادر شده‌اند، دریافت و به دیگر اعضا ابلاغ می‌کند.

۲. حق شرطی که با اهداف و مقاصد کنوانسیون ناسازگار باشد، قابل قبول نیست.

۳. حق شرط ممکن است در هر زمان توسط یک اعلامیه به دبیرکل سازمان ملل که توسط وی به دیگر دولت‌ها نیز ابلاغ می‌شود، پس گرفته شود. این اعلامیه از زمانی که توسط دبیرکل اعلام وصول می‌شود قابل اجرا است.

ماده ۲۱: اعلان خاتمه کنوانسیون

هر دولت عضوی می‌تواند با نامه کتبی اعلان خاتمه کنوانسیون را به دبیرکل سازمان ملل اطلاع دهد. درخواست اعلان خاتمه یک سال بعد از تاریخ وصول آن توسط دبیرکل سازمان ملل قابل اجرا می‌باشد.

ماده ۲۲: امین کنوانسیون

دبیرکل سازمان ملل به‌عنوان امین کنوانسیون منصوب می‌شود.

ماده ۲۳: زبان اصلی کنوانسیون به عربی، چینی، انگلیسی، فرانسه، روسی و اسپانیولی است که همه آنها اعتبار برابر دارند که نزد دبیرکل سازمان ملل سپرده خواهد شد. در گواهی موارد مذکور امضاکنندگان ذیل حسب وظیفه و اختیار از جانب دولت متبوع خود این کنوانسیون را امضا می نمایند.

با آگاهی از اینکه امنیت سایبری مؤثر صرفاً یک موضوع دولتی یا روش های اجرای قانون {انتظامی} نیست و باید از طریق پیشگیری با آن مقابله شود و از طریق تمام جامعه پشتیبانی گردد؛ همچنین با آگاهی از اینکه فناوری به تنهایی نمی تواند امنیت سایبری را تضمین کند و اینکه اولویت باید به برنامه ریزی و مدیریت امنیت سایبری در سرتاسر جامعه داده شود؛

با به رسمیت شناختن اینکه دولت، مشاغل، سایر سازمان ها و کاربران و مالکان خصوصی فناوری های اطلاعات، به نحوی متناسب با نقش خود، باید از خطر ها و اقدامات پیشگیری مرتبط با امنیت سایبری آگاه شوند و باید مسئولیتی را برای اتخاذ {برداشتن} گام هایی جهت افزایش امنیت این فناوری های اطلاعاتی به عهده بگیرند؛

همچنین با به رسمیت شناختن اینکه شکاف های موجود در دسترسی و استفاده از فناوری اطلاعات توسط دولت ها می تواند موجب کاهش اثربخشی همکاری بین المللی در خصوص مبارزه علیه سوءاستفاده مجرمانه از فناوری اطلاعات و ایجاد جهانی امنیت اطلاعات گردد و باتوجه به نیاز به انتقال فناوری اطلاعات مخصوصاً به کشورهای در حال توسعه؛

با به رسمیت شناختن بیشتر اهمیت همکاری بین المللی در دستیابی به امنیت سایبری از طریق پشتیبانی از تلاش های ملی با هدف افزایش ظرفیت انسانی، آموزش فزاینده و فرصت های استخدامی {شغلی}، خدمات عمومی بهبود یافته و کیفیت بهتر زندگی با بهره گیری از شبکه ها و فناوری های اطلاعات و ارتباطات پیشرفته، قابل اطمینان و امن و ارتقای دسترسی جهانی؛ باتوجه به اینکه در نتیجه افزایش اتصالات و ارتباطات به هم پیوسته داخلی، در حال حاضر شبکه ها و سیستم های اطلاعاتی، در معرض رشد تهدیدات و آسیب پذیری های متعدد و متنوع تری هستند که موضوعات امنیتی جدیدی را برای همه ایجاد می نماید؛

همچنین باتوجه به عملکرد سازمان های بین المللی و منطقه ای مرتبط، در افزایش امنیت سایبری و امنیت فناوری های اطلاعات،

۱. باتوجه به عوامل و عناصر پیوست در قطعنامه حاضر، با نگاهی بر ایجاد فرهنگ جهانی

امنیت سایبری؛

۲. از تمامی سازمان های بین المللی مرتبط دعوت می شود، در کنار موارد دیگر، این عوامل را

جهت ایجاد چنین فرهنگی در هر یک از عملکردهای آتی در خصوص امنیت سایبری ملاحظه نمایند؛
 ۳. از دولت‌های عضو دعوت می‌شود تا در تلاش‌هایشان در توسعه سراسری جوامع خود، این عوامل فرهنگ امنیت سایبر را، در کنار موارد دیگر، در کاربرد و استفاده از فناوری‌های اطلاعات در نظر بگیرند؛

۴. از دولت‌های عضو و کلیه سازمان‌های بین‌المللی مرتبط دعوت می‌شود، تا در کنار موارد دیگر، این عوامل و نیاز به یک فرهنگ جهانی امنیت سایبری را در دستور کار خود برای اجلاس سران درباره جامعه اطلاعاتی که از ۱۰ تا ۱۲ دسامبر ۲۰۰۳ در ژنو و در سال ۲۰۰۵ در تونس برگزار می‌شود، در نظر بگیرند؛

۵. بر ضرورت تسهیل فناوری انتقال اطلاعات و ظرفیت‌سازی به کشورهای در حال توسعه، به‌منظور کمک به آن‌ها، جهت انجام اقدامات در امنیت سایبری تأکید می‌نماید؛

نشست عمومی ۷۸ (۲۰ دسامبر ۲۰۰۲)

پیوست: عوامل برای ایجاد یک فرهنگ جهانی امنیت سایبری

پیشرفت سریع فناوری اطلاعات مسیر دولت‌ها، مشاغل و سایر سازمان‌ها و کاربران خصوصی را که شبکه‌ها و سیستم‌های اطلاعات را توسعه می‌دهند، فراهم می‌کند، خدمات ارائه می‌دهند، مالک آن‌ها هستند، آن‌ها را مدیریت می‌نمایند و {کسانی که از این سیستم‌ها و شبکه‌ها} استفاده می‌نمایند، {از این به بعد مشارکت کنندگان نامیده می‌شوند} را تغییر داده است. مشارکت کنندگان باید رویکرد امنیت سایبری داشته باشند. یک فرهنگ جهانی امنیت سایبری نیازمند آن خواهد بود که تمامی مشارکت کنندگان به ۹ موضوع مکمل ذیل بپردازند:
 ا. آگاهی: مشارکت کنندگان باید از نیازمندی امنیت شبکه‌ها و سیستم‌های اطلاعاتی آگاه باشند و اینکه آن‌ها برای ارتقای امنیت چه اقداماتی می‌توانند انجام دهند؛

ب. مسئولیت‌پذیری: مشارکت کنندگان مسئول امنیت شبکه‌ها و سیستم‌های اطلاعاتی در یک روشی مناسب با نقش‌های مخصوص به خودشان می‌باشند. آن‌ها باید سیاست‌ها، روش‌ها، اقدامات و رویه‌های جاری خود را بازنگری نمایند و ارزیابی نمایند که آیا آن‌ها برای محیط

خودشان مناسب هستند یا نه؟

ج. پاسخگویی: مشارکت کنندگان جهت پیشگیری، کشف و پاسخگویی به حوادث امنیتی باید با یک شیوه همکاری جویانه و بموقع اقدام نمایند. آن‌ها باید اطلاعات مربوط به خطرها و آسیب‌پذیری‌ها را به شکل مناسب به اشتراک گذارند و رویه‌هایی را برای همکاری مؤثر و سریع جهت پیشگیری، کشف و پاسخ به حوادث امنیتی اجرا نمایند. این رویه‌ها ممکن است شامل همکاری و اشتراک‌گذاری فرارمزی اطلاعات {این همکاری و اشتراک‌گذاری باید مرزها را درنوردند} باشند؛

د. اخلاقیات: باتوجه به فراگیری شبکه‌ها و سیستم‌های اطلاعاتی در جوامع مدرن، مشارکت کنندگان نیاز به احترام به منافع مشروع دیگران و به رسمیت شناختن اینکه اقدامات یا عدم اقدامات آن‌ها ممکن است به دیگران آسیب وارد نماید، را دارند؛

ه. دموکراسی: امنیت باید در روشی سازگار با ارزش‌هایی که توسط جوامع دموکراتیک به رسمیت شناخته شده است اجرا شود، از جمله آزادی تبادل اندیشه‌ها و ایده‌ها، جریان آزاد اطلاعات، محرمانگی اطلاعات و ارتباطات، حفاظت مناسب از اطلاعات شخصی، آزادی، شفافیت؛ و ارزیابی خطر: کلیه مشارکت‌کنندگان باید ارزیابی‌های خطر جهت شناسایی تهدیدات و آسیب‌پذیری‌ها را به شکل دوره‌ای {متناوب} انجام دهند. {این ارزیابی‌ها} به قدر کافی برای دربرگرفتن عوامل کلیدی داخلی و خارجی مانند فناوری، عوامل فیزیکی و انسانی، سیاست‌ها و خدمات به کشور ثالث با مفاهیم امنیتی، قوی هستند. {این ارزیابی‌ها} اجازه تعیین سطح قابل پذیرش (سطح قابل قبول) خطر، ارزیابی انتخاب کنترل‌های مناسب جهت مدیریت آسیب بالقوه خطر در شبکه‌ها و سیستم‌های اطلاعاتی را در پرتوی ماهیت و اهمیت اطلاعات محافظت شده می‌دهند؛

ز. طراحی و اجرای امنیت: مشارکت کنندگان باید امنیت را به‌عنوان موضوع ضروری در برنامه‌ریزی و طراحی، عملکرد (عملیات) و استفاده از شبکه‌ها و سیستم‌های اطلاعاتی وارد نمایند؛ ح. مدیریت امنیت: مشارکت‌کنندگان باید رویکردی جامع به مدیریت امنیت بر اساس ارزیابی خطر اتخاذ نمایند که پویا، مشتمل بر تمامی سطوح فعالیت‌های مشارکت‌کنندگان و



جنبه‌های عملیاتی آن‌ها باشد؛

ط. ارزیابی مجدد: مشارکت کنندگان باید امنیت شبکه‌ها و سیستم‌های اطلاعاتی را بازنگری و ارزیابی مجدد نمایند و باید اصلاحاتی را در سیاست‌ها، روش‌ها {متدها}، اقدامات و رویه انجام دهد تا با اعمال این اصلاحات بتوانند با تهدیدات جدید و تغییر یافته و آسیب‌پذیری‌های نوظهور مقابله نمایند و آن‌ها را تحت پوشش قرار دهند.

بند دو: قطعنامه ایجاد فرهنگ جهانی امنیت سایبری و احصاء تلاش‌های ملی برای حفاظت

از زیرساخت‌های حساس اطلاعاتی سال ۲۰۰۳

ترجمه سند

تاریخ انتشار: ۳۰ ژانویه ۲۰۰۴

شماره قطعنامه: A/RES/58/199

توزیع: عمومی



مجمع عمومی
کمیته دوم

اجلاس پنجاه و هشتم

دستور کار ۹۱

قطعنامه مصوب مجمع عمومی (بر اساس گزارش کمیته دوم (A/51/481/Add.2))

۵۸/۱۹۹ ایجاد فرهنگ جهانی امنیت سایبری و احصاء تلاش‌های ملی

برای حفاظت از زیرساخت‌های اطلاعاتی حیاتی

مجمع عمومی؛

با یادآوری قطعنامه‌های خود {به شماره‌های} ۵۷/۲۳۹ مورخ دسامبر ۲۰۰۲ درباره ایجاد فرهنگ جهانی امنیت سایبری، ۵۵/۶۳ مورخ ۴ دسامبر ۲۰۰۰ و ۵۶/۱۲۱ مورخ ۱۹ دسامبر ۲۰۰۱ در زمینه ایجاد مبنای قانونی برای مبارزه با سوءاستفاده مجرمانه از فناوری‌های اطلاعات، و ۵۳/۷۰ مورخ ۴ دسامبر ۱۹۹۸، ۵۴/۴۹ مورخ ۱ دسامبر ۱۹۹۹ و ۵۵/۲۸ مورخ ۲۰ نوامبر ۲۰۰۰، ۵۶/۱۹ مورخ ۲۹ نوامبر ۲۰۰۱ و ۵۷/۵۳ مورخ ۲۲ نوامبر ۲۰۰۲ در خصوص تحولات در حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌المللی؛

با به رسمیت شناختن، افزایش اهمیت فناوری اطلاعات، برای دولت‌ها، مشاغل و سایر سازمان‌ها و کاربران شخصی، جهت ارتقای توسعه اجتماعی-اقتصادی و تهیه کالاها و خدمات ضروری، انجام تجارت و تبادل اطلاعات؛

باتوجه به افزایش پیوندها، اتصالات و ارتباطات میان زیرساخت‌های حیاتی اکثر کشورها، -مانند آنچه، در میان موارد دیگر، جهت تولید، انتقال و انتشار انرژی، حمل و نقل هوایی و دریایی، خدمات بانکی و مالی، تجارت الکترونیکی، تأمین آب، توزیع غذا و سلامت عمومی استفاده شده

است- }رو باتوجه به افزایش پیوند میان { زیرساخت‌های اطلاعات حساس که به طور فزاینده‌ای عملکرد آن‌ها را به هم مرتبط نموده و تحت تأثیر قرار داده است؛

با به رسمیت شناختن اینکه هر کشوری زیرساخت‌های اطلاعات حساس خود را، خود تعیین خواهد کرد، همچنین با به رسمیت شناختن اینکه این رشد وابستگی فنی، روی شبکه پیچیده‌ای از مولفه‌ها و اجزای زیرساخت اطلاعات حساس تکیه می‌کند، باتوجه به اینکه، در نتیجه افزایش اتصالات و ارتباطات به هم پیوسته داخلی، در حال حاضر زیرساخت‌های اطلاعات حساس، در معرض رشد تهدیدات و آسیب‌پذیری‌های متعدد و متنوع‌تری هستند که نگرانی‌های امنیتی جدیدی را ایجاد می‌نماید؛

همچنین باتوجه به اینکه حفاظت مؤثر از زیرساخت حیاتی، از جمله، در میان موارد دیگر، {سبب} شناسایی تهدیدات و کاهش آسیب‌پذیری زیرساخت‌های اطلاعات حساس، به حداقل رساندن خسارت و زمان بازیابی در حادثه خسارت یا حمله، و شناسایی علت تخریب یا ایراد خسارات یا منبع حمله، {می‌گردد}؛

با به رسمیت شناختن اینکه، حفاظت مؤثر، نیازمند همکاری و ارتباط ملی و بین‌المللی میان تمامی ذی‌نفعان می‌باشد و اینکه تلاش‌های ملی باید از طریق همکاری مؤثر و واقعی بین‌المللی و منطقه‌ای میان ذی‌نفعان پشتیبانی گردد؛

همچنین با به رسمیت شناختن اینکه شکاف‌های موجود در دسترسی و استفاده از فناوری‌های اطلاعات توسط دولت‌ها، می‌تواند موجب کاهش اثربخشی همکاری در خصوص مبارزه علیه سوءاستفاده مجرمانه از فناوری اطلاعات و ایجاد یک فرهنگ جهانی امنیت سایبری گردد باتوجه به نیاز به تسهیل و انتقال فناوری اطلاعات مخصوصاً به کشورهای در حال توسعه؛

با به رسمیت شناختن بیشتر اهمیت همکاری بین‌المللی در دستیابی به امنیت سایبری و حفاظت از زیرساخت‌های اطلاعات حساس از طریق پشتیبانی از تلاش‌های ملی با هدف افزایش ظرفیت انسانی، آموزش فزاینده و فرصت‌های استخدامی {شغلی}، خدمات عمومی بهبودیافته و کیفیت بهتر زندگی با بهره‌گیری از شبکه‌ها و فناوری‌های اطلاعات و ارتباطات پیشرفته، قابل اطمینان و امن و ارتقای دسترسی جهانی؛

باتوجه به عملکرد سازمان‌های منطقه‌ای و ملی مرتبط، در افزایش امنیت زیرساخت‌های با به رسمیت شناختن اینکه تلاش‌ها جهت حفاظت از زیرساخت‌های اطلاعات حساس باید کاملاً با رعایت قوانین ملی قابل اعمال در باب حفاظت از حریم خصوصی و سایر قوانین مرتبط انجام گیرد}:

۱. باتوجه به عوامل و عناصر تنظیم شده در پیوست قطعنامه حاضر، جهت حفاظت از زیرساخت‌های اطلاعات حساس؛

۲. از سازمان‌های بین‌المللی مرتبط، از جمله نهادهای مرتبط در سازمان ملل متحد، دعوت می‌شود تا به شکل مناسب، در کنار موارد دیگر، این عوامل را برای حفاظت از زیرساخت‌های اطلاعات حساس و عملکرد آتی در زمینه امنیت سایبری یا حفاظت از زیرساخت‌های حیاتی مورد ملاحظه قرار دهند؛

۳. از دولت‌های عضو دعوت می‌شود، در کنار موارد دیگر، این عوامل را در ایجاد و توسعه راهبردهای خود در خصوص کاهش خطرهای زیرساخت‌های اطلاعات حساس، مطابق با قوانین و مقررات ملی، مورد ملاحظه قرار دهند؛

۴. از دولت‌های عضو و کلیه سازمان‌های بین‌المللی مرتبط، دعوت می‌شود تا در کنار موارد دیگر، این عوامل و نیاز به حفاظت از زیرساخت اطلاعات حساس را در دستور کار خود برای مرحله دوم اجلاس سران درباره جامعه اطلاعاتی که از ۱۶ تا ۱۸ نوامبر در تونس برگزار می‌شود، در نظر بگیرند؛

۵. دولت‌های عضو و سازمان‌های منطقه‌ای و بین‌المللی مرتبط که راهبردهایی را جهت رسیدگی به امنیت سایبری و حفاظت از زیرساخت‌های اطلاعات حساس و همچنین جهت رسیدگی به اشتراک‌گذاری روش‌ها {متدها} و اقدامات خود توسعه داده‌اند، را تشویق می‌نماید، {روش‌ها و متدهایی که توسط آن‌ها} سایر دولت‌های عضو را در تلاش‌هایشان جهت تسهیل و دستیابی به امنیت سایبری مساعدت کردند؛

۶. بر نیاز به افزایش تلاش جهت از بین بردن شکاف دیجیتالی، حصول به دسترسی جهانی به فناوری‌های اطلاعات و ارتباطات و حفاظت از زیرساخت‌های اطلاعات حساس از طریق تسهیل

انتقال فناوری اطلاعات و ظرفیت‌سازی، به‌ویژه به کشورهای در حال توسعه، علی‌الخصوص کشورهای کمتر توسعه یافته تأکید می‌کند. به طوری که کلیه دولت‌ها به طور کامل توانایی بهره‌مندی از فناوری‌های اطلاعات و ارتباطات برای توسعه اجتماعی و اقتصادی خود را داشته باشند. نشست عمومی ۷۸ (۲۳ دسامبر ۲۰۰۳)

پیوست: عوامل برای حفاظت از زیرساخت‌های اطلاعات حساس

۱. داشتن شبکه‌های اخطار سریع در رابطه با آسیب‌پذیری‌های سایبری، تهدیدات و حوادث.
۲. بالابردن آگاهی جهت تسهیل درک ذی‌نفعان از ماهیت و وسعت زیرساخت‌های اطلاعات حساس خود و نقشی که هر یک باید در حفاظت از آن‌ها ایفا نمایند؛
۳. بررسی و بازدید زیرساخت‌ها و شناسایی وابستگی‌های موجود در آن‌ها، {و} به موجب آن افزایش حفاظت از چنین زیرساخت‌هایی؛
۴. ارتقای مشارکت میان ذی‌نفعان خصوصی و عمومی، جهت اشتراک‌گذاری و تحلیل اطلاعات {مربوط به} زیرساخت‌های حیاتی به منظور حفاظت، تحقیق و پاسخ‌گویی به تخریب یا حملات به چنین زیرساخت‌هایی؛
۵. ایجاد و حفظ شبکه‌های ارتباطات بحرانی و آزمایش آن‌ها جهت حصول اطمینان از اینکه آن‌ها در وضعیت‌های غیرمترقبه ایمن و پایدار خواهند بود؛
۶. اطمینان از اینکه سیاست‌های مربوط به دسترس‌پذیری داده‌ها نیاز به حفاظت از زیرساخت‌های اطلاعات حیاتی را در نظر می‌گیرد؛
۷. تسهیل ردیابی حملات علیه زیرساخت‌های اطلاعات حیاتی و در صورت صلاحدید افشا و انتقال اطلاعات ردیابی شده به دولت‌های دیگر؛
۸. اقدام به یادگیری و تمرین‌هایی جهت افزایش ظرفیت‌های پاسخگویی و آزمایش طرح‌های مربوط به هر دو نوع دامنه‌دار و موردی در رویداد حمله به زیرساخت‌های اطلاعاتی و تشویق ذی‌نفعان به تعامل با چنین فعالیت‌هایی؛
۹. داشتن قوانین شکلی و محتوایی مناسب و کارکنان آموزش دیده به منظور توانمند کردن

دولت‌ها برای تحقیق و تعقیب و پیگرد حملات روی زیرساخت‌های اطلاعاتی حساس و در صورت صلاحدید هماهنگی با سایر دولت‌ها {جهت انجام} چنین تحقیقاتی؛

۱۰. تعامل در همکاری بین‌المللی، در زمان مقتضی، جهت ایمن‌سازی زیرساخت‌های اطلاعات حساس، از جمله، از طریق توسعه و هماهنگی سیستم‌های اخطار سریع، اشتراک‌گذاری و تحلیل اطلاعات در رابطه با آسیب‌پذیری‌ها، تهدیدات و حوادث و هماهنگی تحقیقات در مورد حملات روی چنین زیرساخت‌هایی مطابق با قوانین داخلی؛

۱۱. ارتقای پژوهش‌های ملی و بین‌المللی، توسعه و تشویق کاربرد فناوری‌های امنیتی مناسب با استانداردهای بین‌المللی.

بند سه: قطعنامه ایجاد فرهنگ جهانی امنیت سایبری و احصاء تلاش‌های ملی برای حفاظت

از زیرساخت‌های حساس اطلاعاتی سال ۲۰۰۹

ترجمه سند



مجمع عمومی
کمیته دوم

تاریخ انتشار: ۱۷ مارس ۲۰۱۰

ماره قطعنامه: A/RES/ 64/211

توزیع: عمومی

اجلاس شصت و چهارم

دستور کار ۵۵

قطعنامه پذیرفته شده توسط مجمع عمومی در ۲۱ دسامبر ۲۰۰۹

بر اساس گزارش کمیته دوم (A/64/422/Add.3)

۶۴/۲۱۱ ایجاد فرهنگ جهانی امنیت سایبری و شناسایی تلاش‌های ملی برای حفاظت از زیرساخت‌های حساس اطلاعاتی

مجمع عمومی^۱

با یادآوری قطعنامه‌های خود شامل قطعنامه ۵۵/۶۳ مورخ ۴ دسامبر ۲۰۰۰ و قطعنامه ۵۶/۱۲۱ مورخ ۱۹ دسامبر ۲۰۰۱ در زمینه مبارزه با سوءاستفاده مجرمانه از فناوری اطلاعات، قطعنامه ۵۷/۲۳۹ مورخ ۲۰ دسامبر ۲۰۰۲ در زمینه ایجاد فرهنگ جهانی امنیت سایبری و قطعنامه ۵۸/۱۹۹ مورخ ۲۳ دسامبر ۲۰۰۳ در زمینه ایجاد فرهنگ جهانی امنیت سایبری و احصاء تلاش‌های ملی برای حفاظت از زیرساخت‌های اطلاعاتی حساس؛

با یادآوری بیشتر نتایج اجلاس سران در مورد جامعه اطلاعاتی که مرحله نخست آن در تاریخ ۱۰ الی ۱۲ دسامبر ۲۰۰۳ در ژنو و مرحله دوم آن در تاریخ ۱۶ الی ۱۸ نوامبر ۲۰۰۵ در تونس برگزار شد؛

با به رسمیت شناختن اینکه اعتماد و امنیت در استفاده از فناوری اطلاعات و ارتباطات جزء ارکان اصلی جامعه اطلاعاتی است و بنابراین داشتن یک فرهنگ جهانی قوی در امنیت سایبری نیازمند تشویق، فراهم سازی، توسعه و اجرای قدرتمندانه می‌باشد؛

1. Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures

همچنین با به رسمیت شناختن افزایش مشارکت و نقش ایجاد شده توسط فناوری اطلاعات و ارتباطات در بیشتر وظایف ضروری زندگی روزانه، تجارت، شرایط اموال و خدمات، تحقیق، نوآوری و تأسیس و جریان آزاد اطلاعات بین اشخاص و سازمان‌ها، دولت‌ها، مشاغل و جامعه مدنی؛

با یادآوری بیشتر اینکه در یک روش مناسب برای نقش آن‌ها، دولت‌ها، مشاغل، سازمان‌ها و مالکان خصوصی و کاربران فناوری اطلاعات باید مسئولیت برداشتن گام‌هایی جهت ارتقای امنیت این فناوری‌های اطلاعاتی را بر عهده بگیرند؛

با به رسمیت شناختن اهمیت دستور کار مجمع راهبری اینترنت به‌عنوان مذاکرات چنددلی نفعی برای بحث پیرامون موضوعات مختلف از جمله موضوعات سیاستگذاری عمومی مرتبط با عناصر اصلی حکمرانی اینترنت به‌منظور تقویت پایداری، توانمندی، امنیت، ثبات و توسعه اینترنت و با تکرار اینکه همه دولت‌ها باید نقش و مسئولیت برابر در حکمرانی جهانی اینترنت و تضمین ثبات، امنیت و تداوم اینترنت داشته باشند؛

با تأیید مجدد اینکه این تداوم، نیازمند ارتقای همکاری، توانمندسازی دولت‌ها در یک موقعیت برابر جهت ایفای نقش و مسئولیتشان در موضوعات حوزه سیاستگذاری عمومی بین‌المللی مربوط به اینترنت می‌باشد، اما نه موضوعات فنی و عملیاتی روزمره که موضوعات سیاستگذاری عمومی بین‌المللی را تحت تأثیر قرار نمی‌دهند؛

با به رسمیت شناختن اینکه هر کشور زیرساخت‌های اطلاعاتی حساس متعلق به خود را تعیین خواهد کرد؛

با تأیید مجدد نیاز به مهار و کنترل ظرفیت‌های مخفی فناوری‌های اطلاعات و ارتباطات برای فراهم کردن زمینه دستیابی به اهداف توسعه‌ای یک توافق بین‌المللی، از جمله اهداف توسعه هزاره؛ با به رسمیت شناختن اینکه وجود شکاف‌هایی در دسترسی و استفاده از فناوری‌های اطلاعاتی توسط دولت‌ها می‌تواند موجب کاهش بالندگی اقتصادی آن‌ها شود و همچنین با تأیید تأثیر و کارایی همکاری در زمینه مبارزه با سوءاستفاده مجرمانه از فناوری اطلاعات و ایجاد فرهنگ جهانی امنیت سایبری؛

با تأکید بر افزایش تلاش‌ها جهت از بین بردن شکاف دیجیتالی به منظور دستیابی به دسترسی جهانی به فناوری‌های اطلاعاتی و ارتباطی و برای حفاظت از زیرساخت‌های حساس فناوری اطلاعات از طریق تسهیل انتقال فناوری اطلاعات و ظرفیت‌سازی برای توسعه کشورها مخصوصاً کشورهای کمتر توسعه‌یافته، در حوزه‌های امنیت سایبری با بهترین روش و آموزش؛

با اظهار نگرانی در مورد اینکه تهدیدات در برابر عملکرد مطمئن زیرساخت‌های حساس اطلاعاتی و کارایی بی‌عیب اطلاعات در شبکه‌های خود، در هر دو بعد کمیت و کیفیت در حال افزایش است و این امر آرامش بومی، ملی و بین‌المللی را تحت تأثیر قرار می‌دهد؛

با تأیید اینکه تأمین امنیت زیرساخت‌های حساس اطلاعاتی مسئولیت دولت‌هاست که باید به‌صورت نظام‌مند به آن بپردازند و حوزه‌ای است که آن‌ها باید ضمن همکاری با ذی‌نفعان مربوط در سطح ملی راهبری کنند. دولت‌ها باید در برابر خطرهای مربوط آگاه‌سازی کنند و با اتخاذ یک روش مناسب در وظایف مربوط به خود، اقدامات پیشگیرانه و پاسخ‌های مؤثر داشته باشند؛

با به رسمیت شناختن اینکه تلاش‌های ملی باید از طریق همکاری بین‌المللی و به اشتراک گذاشتن بین‌المللی اطلاعات، مورد حمایت قرار گیرد تا با افزایش تهدیداتی که ماهیت فراملی دارند، مواجهه مؤثر داشته باشد؛

باتوجه به فعالیت سازمان‌های منطقه‌ای و بین‌المللی در مورد ارتقای امنیت سایبری و تکرار نقش آن‌ها در تشویق تلاش‌های ملی و تقویت همکاری‌های بین‌المللی؛

با به رسمیت شناختن اینکه یک ارزیابی دوره‌ای از پیشرفت زیرساخت‌های حساس اطلاعاتی می‌تواند در تلاش‌های ملی برای حفاظت از آن‌ها مؤثر واقع شود:

۱. از دولت‌های عضو دعوت می‌شود ابزار خود ارزیابی پیوست را در صورتی که آن را مناسب تشخیص دهند در راستای تلاش‌های ملی برای حفاظت از زیرساخت‌های حساس اطلاعاتی به‌کار گیرند تا بتوانند تلاش‌های خود در این حوزه را برای تقویت امنیت سایبریشان ارزیابی کنند و همچنین مواردی را که نیاز به اقدامات بیشتری دارد، برجسته کنند. این امور با هدف ارتقای فرهنگ جهانی امنیت سایبری صورت می‌گیرد؛

۲. تشویق دولت‌های عضو و سازمان‌های منطقه‌ای و بین‌المللی مرتبط که راهبردهای خود را

در تعامل با امنیت سایبری و حفاظت از زیرساخت‌های حساس اطلاعاتی به اینکه اقدامات و تجارب خود را به بهترین نحو ممکن به اشتراک بگذارند تا به دیگر کشورها جهت دستیابی به امنیت سایبری مساعدت شود. این اطلاعات باید به دبیرکل ارائه شده و توسط ایشان، تجمیع و سپس بین دولت‌های عضو توزیع شود.

۲۱ دسامبر ۲۰۰۹

شصت و ششمین اجلاس عمومی

پیوست

ابزار خودارزیابی داوطلبانه برای تلاش‌های ملی در جهت حفاظت از زیرساخت‌های حساس اطلاعاتی شناسایی نیازمندی‌های امنیت سایبری و راهبردها

۱. ارزیابی نقش فناوری اطلاعات و ارتباطات در اقتصاد ملی، امنیت ملی و زیرساخت‌های حساس شما (مثل حمل و نقل، تأمین آب و غذا، سلامت عمومی، انرژی، مالی و فوریت‌های خدماتی) و جامعه مدنی؛

۲. تعیین مخاطرات حفاظت از امنیت سایبری و زیرساخت‌های حساس اطلاعاتی بر اقتصاد، امنیت ملی، زیرساخت‌های حساس و جامعه مدنی شما که باید مدیریت شود؛

۳. درک آسیب‌پذیری‌های شبکه‌ها در حین استفاده، سطوح نسبی تهدید که هر بخش در طرح‌های مدیریتی حال حاضر و طرح‌های جاری با آن روبروست. توجه به چگونگی تغییر در محیط اقتصاد، اولویت‌های امنیت ملی و نیازهای جامعه مدنی که این محاسبات را تحت تأثیر قرار می‌دهد؛

۴. تعیین اهداف امنیت سایبری ملی و راهبردهای حفاظت از زیرساخت‌های اطلاعاتی حساس، تشریح اهداف آن‌ها، سطح فعلی کاربرد آن‌ها، اقدامات موجود برای اندازه‌گیری میزان پیشرفت آن‌ها، ارتباط آن‌ها با دیگر اهداف سیاست ملی و چگونگی تطبیق چنین راهبرد با طرح‌های منطقه‌ای و بین‌المللی؛

نقش ها و مسئولیت‌های ذی‌نفعان

۵. شناسایی و تعیین ذی‌نفعان اصلی با نقش آن‌ها در حفاظت از امنیت سایبری و زیرساخت‌های حساس اطلاعاتی و تشریح نقش هر کدام از آن‌ها در توسعه سیاست‌ها و اقدامات مربوط از جمله:

- وزارتخانه‌ها و سازمان‌های ملی دولت، توجه به نقاط اصلی تماس و مسئولیت‌های هر کدام از آن‌ها؛
- سایر شرکای دولتی (محلی و منطقه‌ای)؛
- بخش‌های غیر دولتی از جمله جامعه مدنی و دانشگاهی؛
- شهروندان عادی، توجه به متوسط کاربران اینترنت که به آموزش‌های پایه جهت اجتناب از تهدیدهای برخط دسترسی دارند و میزان کمپین‌های مربوط به ارتقای آگاهی ملی درباره امنیت سایبر؛

روندها و مشارکت‌های سیاسی

۶. شناسایی و تعیین مبادی رسمی و غیررسمی که در حال حاضر برای همکاری در سیاست‌گذاری و عملیات‌ها با صنایع دولت جهت توسعه امنیت سایبری و حفاظت از زیرساخت‌های حساس اطلاعاتی وجود دارند؛

۷. شناسایی و تعیین دیگر مجامع و ساختارها که ممکن است برای تکامل چشم‌انداز و نیازدانشی دولتی و غیر دولتی در راستای تحقق اهداف امنیت سایبری و زیرساخت‌های حساس اطلاعاتی مورد نیاز باشد.

همکاری بخش عمومی و خصوصی

۸. تجمع تمام اقدامات صورت گرفته و طرح‌های موجود برای توسعه همکاری بین دولت و بخش خصوصی از جمله هر گونه توافق برای به اشتراک گذاری اطلاعات و مدیریت حوادث؛

۹. تجمع کلیه ابتکارات جاری و طراحی شده (آتی) برای افزایش منافع مشترک و مقابله با چالش‌های مشترک میان شرکای زیرساخت‌های حیاتی و بازیگران بخش خصوصی که به طور متقابل وابسته به یک زیرساخت حساس می‌باشند؛

مدیریت بحران و بهبود {شرایط}

۱۰. تعیین سازمان دولتی که به‌عنوان هماهنگ کننده برای مدیریت حوادث، از جمله توانمندی برای وظایف دیده‌بانی، هشدار، پاسخ و بهبود، عمل کند؛ هماهنگی ادارات دولتی؛ هماهنگی مشارکت کنندگان غیر دولتی، از جمله صنعت و شرکای دیگر؛ و هر ترتیبی که برای همکاری و اشتراک اطلاعات مورد اعتماد قرار گیرد؛

۱۱. به طور جداگانه، تعیین توانمندی و ظرفیت پاسخگویی در سطح ملی در مورد حوادث کامپیوتری از جمله هر تیم پاسخگویی در مورد حوادث کامپیوتری با مسئولیت های ملی و نقش ها و مسئولیت های آن، از جمله ابزار و رویه های موجود برای حفاظت از شبکه های کامپیوتری دولتی، و ابزار و روش های موجود برای انتشار اطلاعات مربوط به مدیریت حادثه؛

۱۲. تعیین شبکه ها و فرایندهای همکاری بین‌المللی که ممکن است واکنش‌ها در مقابل حوادث و برنامه‌ریزی برای موارد احتمالی را بهبود ببخشد، شناسایی شرکا و ترتیبات مقتضی برای همکاری‌های دوجانبه و چندجانبه.

چهارچوبهای قانونی

۱۳. بازنگری و بروزرسانی نهادهای قانونی (از جمله موارد مرتبط با جرایم اینترنتی، حفظ حریم خصوصی، حفاظت از داده‌ها، قانون تجارت، امضای دیجیتال و رمزنگاری) که ممکن است قدیمی شود یا در نتیجه پذیرش سریع و وابستگی به فناوری اطلاعات و ارتباطات جدید و استفاده از کنوانسیون‌های منطقه‌ای و بین‌المللی و ترتیبات والگوهای جدید موجب متروک آن نهاد های قانونی گردد. حصول اطمینان از اینکه آیا کشور شما قوانین لازم را برای تحقیق و تعقیب قانونی جرایم اینترنتی تدوین کرده است، باتوجه‌به چارچوبهای موجود، به‌عنوان مثال، قطعنامه ۵۵/۶۳ و ۵۶/۱۲۱ مجمع عمومی در زمینه مبارزه با سوءاستفاده مجرمانه از فناوری‌های اطلاعات و ابتکارات منطقه‌ای، از جمله کنوانسیون جرایم اینترنتی شورای اروپا؛

۱۴. تعیین وضعیت فعلی نهادها و رویه‌های ملی مربوط به جرایم سایبری از جمله نهادهای قانونی حقوقی و واحدهای ملی جرایم سایبری، و سطح درک در میان دادستانها، قضات و

قانونگذاران مسائل مربوط به جرایم سایبری؛

۱۵. ارزیابی میزان کفایت و بسندگی شاخص‌های قانونی جاری و مقامات فعلی در مقابله با چالش‌های موجود و آینده جرایم اینترنتی و فضای سایبری در شکل عام آن؛
۱۶. بررسی مشارکت ملی در تلاش‌های بین‌المللی برای مبارزه با جرایم اینترنتی، مانند راه‌اندازی نقطه تماس ۲۴ ساعته شبکه جرایم سایبری؛
۱۷. تعیین الزامات سازمان‌های اجرای قانون ملی برای همکاری با هم‌تایان بین‌المللی جهت تحقیق در مورد جرایم سایبری فراملی در مواردی که زیرساخت‌ها در آن قرار دارد یا مرتکبان در قلمرو ملی زندگی می‌کنند، اما قربانیان در سایر نقاط ساکن هستند.

ایجاد فرهنگ جهانی امنیت سایبری

۱۸. تلخیص اقدامات انجام شده و برنامه‌های مربوط به توسعه یک فرهنگ ملی امنیت سایبری با الهام از قطعنامه‌های ۵۷/۲۳۹ و ۵۸/۱۹۹ مجمع عمومی، از جمله اجرای طرح امنیت سایبری برای سیستم‌های اپراتوری دولتی، برنامه‌های مربوط به افزایش آگاهی ملی، توسعه برنامه‌هایی برای کودکان و کاربران فردی و دیگران، و الزامات آموزشی در مورد امنیت ملی سایبری و حفاظت از زیرساخت‌های حساس اطلاعاتی.

بند چهار: قطعنامه فناوری های اطلاعات و ارتباطات برای توسعه سال ۲۰۰۲

ترجمه سند



مجمع عمومی
کمیته دوم

تاریخ انتشار: ۴ مارس ۲۰۰۳

شماره قطعنامه: A/RES/57/295

توزیع: عمومی

اجلاس پنجاه و هفتم

دستور کار ۳۲

قطعنامه مصوب مجمع عمومی (بدون ارجاع به کمیته اصلی براساس گزارش (A/57/L.71))

فناوری های اطلاعات و ارتباطات برای توسعه^۱

مجمع عمومی؛

با یادآوری اعلامیه هزاره سازمان ملل متحد مصوب سران دولت ها و کشورهای عضو سازمان ملل، مورخ ۸ دسامبر ۲۰۰۰، که در آن کشورهای عضو، به حصول اطمینان از اینکه منافع حاصل از فناوری های جدید، علی الخصوص فناوری های فناوری اطلاعات و ارتباطات در دسترس همگان قرار گیرد، رای دادند. {این موضوع} منطبق با توصیه های مندرج در اعلامیه اجرایی شورای اقتصادی و اجتماعی، مصوب اجلاس محتوایی سطح بالا، مورخ ۷ جولای ۲۰۰۰، می باشد؛

همچنین با یادآوری {این نکته} که اعلامیه اجرایی، راهبردی منسجم در گستره سیستم فناوری اطلاعات و ارتباطات را تقاضا می نماید که متضمن هماهنگی و همکاری میان برنامه ها و اقدامات نظام سازمان های خصوصی و تبدیل آن ها به سازمان هایی با سیستم های دانش محور باشد. ضمن یادآوری قطعنامه {مجمع عمومی با شماره} ۵۷/۲۳۸، مورخ ۲۰ دسامبر ۲۰۰۲، درخصوص اجلاس سران درباره جامعه اطلاعاتی که تمامی نهادهای سازمان ملل متحد و سایر سازمان های بین دولتی از جمله مؤسسات منطقه ای و بین المللی را تشویق نمود تا همکاری های خود را در حمایت از فرایند مقدماتی اجلاس سران افزایش دهند.

1 . Information and communications technologies for development

باتوجه به اینکه فناوری‌های اطلاعات و ارتباطات برای توسعه در خروجی‌های کنفرانس‌ها و اجلاس‌های سازمان ملل متحد، به‌عنوان عنصری مهم به رسمیت شناخته شده است:

۱. نیاز به استفاده از فناوری‌های اطلاعات و ارتباطات را به‌عنوان ابزار راهبردی برای ارتقای کارایی، اثربخشی و تأثیر برنامه‌های توسعه و اقدامات {مربوط به} همکاری فنی در نظام سازمان ملل متحد، تأیید می‌نماید؛

۲. به ضرورت هماهنگی و همکاری بین برنامه‌ها و اقدامات نظام سازمان ملل متحد و نقش قاطعی که فناوری اطلاعات و ارتباطات می‌تواند در تسهیل چنین هماهنگی‌هایی ایفا نماید تأکید می‌کند؛

۳. از دبیرکل به‌عنوان ریاست نظام سازمان ملل متحد و رئیس شورای اجرایی برای هماهنگی، درخواست می‌نماید در راستای توسعه یک راهبرد جامع در فناوری اطلاعات و ارتباطات برای نظام ملل متحد، همکاری نزدیکی با سازمان‌های نظام ملل متحد و گروه اقدام {مرتبط با} فناوری‌های اطلاعات و ارتباطات داشته باشد و {در این راستا} اصول زیر را مورد نظر قرار دهد:

ا. تشویق در به‌کارگیری و استفاده از گستره سیستم فناوری اطلاعات و ارتباطات جهت تقویت ظرفیت ملل متحد در تولید، به اشتراک‌گذاری و نشر دانش و کمک به ایجاد ملل متحدی با کارایی و اثربخشی بیشتر در ارائه خدمات به دولت‌های عضو؛

ب. جریان‌شناسی کامل‌تر و تکمیل فناوری اطلاعات و ارتباطات به سوی توسعه و اقدامات همکاری فنی در سازمان‌های نظام {ملل متحد}؛

ج. ایجاد شبکه‌ها و جوامعی برای تشریک مساعی عملی میان سازمان‌های نظام؛ {ملل متحد} د. عندالاقضاء توسعه بسترهای عمومی برای خدماتی مانند پایگاه اطلاعاتی، مستندسازی و برگزاری نشست‌ها؛

ه. تشویق جهت استفاده از فناوری‌های اطلاعات و ارتباطات به‌منظور ارتقای تبادل تجربیات و به اشتراک‌گذاری اطلاعات میان سازمان‌های نظام ملل متحد و بین {این} سازمان‌ها و دولت‌های عضو؛ و. توسعه برنامه‌های آموزش نظام گستر با هدف ظرفیت‌سازی سیستم جهت اتخاذ {بهره‌مندی} کامل از مزایای فناوری اطلاعات و ارتباطات؛



۴. همچنین از دبیرکل درخواست می‌نماید تا گزارش پیشرفت اجرای قطعنامه حاضر را در اجلاس پنجاه‌وهشتم مجمع عمومی، تحت بخشی با عنوان «فناوری اطلاعات و ارتباطات برای توسعه» ارائه نماید.

نشست عمومی ۷۹- مورخ ۲۰ دسامبر

بند پنجم: قطعنامه فناوری‌های اطلاعات و ارتباطات برای توسعه سال ۲۰۰۷

ترجمه سند



مجمع عمومی
کمیته دوم

تاریخ انتشار: ۳۱ ژانویه ۲۰۰۸

شماره قطعنامه: A/RES/62/182

توزیع: عمومی

اجلاس شصت و دوم

دستور کار ۵۱

قطعنامه مصوب مجمع عمومی (بر اساس گزارش کمیته دوم (A/62/416))

فناوری‌های اطلاعات و ارتباطات برای توسعه

مجمع عمومی

با یادآوری قطعنامه‌های خود {به شماره‌های} ۵۶/۱۸۳ مورخ ۲۱ دسامبر ۲۰۰۱، ۵۷/۲۳۸ مورخ ۲۰ دسامبر ۲۰۰۲، ۵۷/۲۷۰B مورخ ۲۳ ژوئن ۲۰۰۳، ۵۹/۲۲۰ مورخ ۲۲ دسامبر ۲۰۰۴ و ۶۰/۲۵۲ مورخ ۲۷ مارس ۲۰۰۶؛

همچنین با یادآوری اعلامیه اصول و طرح اقدام {ژنو} مصوب اولین اجلاس سران درباره جامعه اطلاعاتی که در تاریخ ۱۰ تا ۱۲ دسامبر ۲۰۰۳ در ژنو برگزار {و سپس} توسط مجمع عمومی تأیید گردید، {همچنین با یادآوری} تعهدات و دستورکار تونس برای جامعه اطلاعاتی مصوب دومین اجلاس سران که در تاریخ ۱۸ نوامبر ۲۰۰۵ در تونس برگزار و به تأیید مجمع عمومی رسید: با یادآوری بیشتر خروجی اجلاس سران در سال ۲۰۰۵؛

۱. مجدداً، وضعیت پیشرفت جدی {احصاء شده} در خروجی‌های اجلاس سران درباره جامعه اطلاعاتی در هر دو فاز {مرحله} ژنو و تونس را تأیید می‌نماید و بر اجرای کامل این خروجی‌ها مصر می‌باشد.

۲. همچنین مجدداً درخواست خود از شورای اقتصادی اجتماعی {مبنی بر} بازنگری گستره سیستم پیگیری خروجی‌های اجلاس سران را تأیید می‌نماید.

۳. از دبیرکل درخواست می‌نماید تا گزارشی درباره وضعیت اجرا و پیگیری خروجی اجلاس سران که توسط شورای اقتصادی و اجتماعی برای کمیسیون علم و فناوری آماده می‌شود را در شصت‌وسومین اجلاس مجمع عمومی ارائه نماید. شورای اقتصادی و اجتماعی این گزارش را مطابق دستورکار مندرج در قطعنامه خود به شماره ۲۰۰۶/۴۶ مورخ ۲۸ جولای ۲۰۰۶ برای کمیسیون علم و فناوری تهیه می‌نماید.

نشست عمومی ۷۸، مورخ ۱۹ دسامبر ۲۰۰۷

بند شش: قطعنامه فناوری اطلاعات و ارتباطات برای توسعه سال ۲۰۱۵

ترجمه سند



مجمع عمومی
کمیته دوم

تاریخ انتشار: ۴ فوریه ۲۰۱۶

شماره قطعنامه: A/RES/70/184

توزیع: عمومی

اجلاس هفتادم

دستور کار ۱۷

قطعنامه مصوب مجمع عمومی مورخ ۲۲ دسامبر ۲۰۱۵ بر اساس گزارش کمیته دوم (A/70/469)

فناوری اطلاعات و ارتباطات برای توسعه

مجمع عمومی

با یادآوری قطعنامه‌های خود {به شماره} ۵۶/۱۸۳ مورخ ۲۱ دسامبر ۲۰۰۱، ۵۷/۲۳۸ مورخ ۲۰ دسامبر ۲۰۰۲، B270/57 مورخ ژوئن ۲۰۰۳، ۵۹/۲۲۰ مورخ ۲۲ دسامبر ۲۰۰۴، ۶۰/۲۵۲ مورخ ۲۷ مارس ۲۰۰۶، ۶۲/۱۸۲ مورخ ۱۹ دسامبر ۲۰۰۷، ۶۳/۲۰۲ مورخ دسامبر ۲۰۰۸، ۶۴/۱۸۷ مورخ ۲۱ دسامبر ۲۰۰۹، ۶۵/۱۴۱ مورخ ۲۰ دسامبر ۲۰۱۰، ۶۶/۱۸۴ مورخ ۲۲ دسامبر ۲۰۱۱، ۶۷/۱۹۵ مورخ ۲۱ دسامبر ۲۰۱۲، ۶۸/۱۹۸ مورخ ۲۰ دسامبر ۲۰۱۳ و ۶۹/۲۰۴ مورخ ۱۹ دسامبر ۲۰۱۴؛

با یادآوری قطعنامه‌های شورای اقتصادی و اجتماعی {به شماره} ۲۰۰۶/۴۶ مورخ ۲۸ جولای ۲۰۰۶، ۲۰۰۸/۳ مورخ ۱۸ جولای ۲۰۰۸، ۲۰۰۹/۷ مورخ ۲۴ جولای ۲۰۰۹، ۲۰۱۰/۲ مورخ ۱۹ جولای ۲۰۱۰، ۲۰۱۱/۱۶ مورخ ۲۶ جولای ۲۰۱۱، ۲۰۱۲/۵ مورخ ۲۴ جولای ۲۰۱۲، ۲۰۱۳/۹ مورخ ۲۲ جولای ۲۰۱۳ و ۲۰۱۴/۲۷ مورخ ۱۶ جولای ۲۰۱۴ و باتوجه به قطعنامه شورا {به شماره} ۲۰۱۵/۲۶ مورخ ۲۲ جولای ۲۰۱۵، در خصوص ارزیابی پیشرفت ایجاد شده در اجرا و پیگیری نتایج اجلاس جهانی سران درباره جامعه اطلاعاتی؛

با تأیید مجدد قطعنامه خود {به شماره} ۷۰/۱ مورخ ۲۵ سپتامبر ۲۰۱۵ با عنوان «تبدیل دنیای ما: دستورکار توسعه پایدار» که در آن مجموعه‌ای جامع، گسترده، مردم‌محور از اهداف

و مقاصد تحول‌آمیز و جهانی توسعه پایدار تصویب شد، تعهدات خود جهت کار خستگی ناپذیر برای اجرای کامل دستور کار؛

با به رسمیت شناختن اینکه ریشه‌کن کردن فقر در تمامی اشکال و ابعاد آن، از جمله فقر شدید، بزرگ‌ترین چالش جهانی و یک الزام ضروری برای توسعه پایدار است و به رسمیت شناختن تعهد خود جهت دستیابی به توسعه پایدار در سه بعد - اقتصادی، اجتماعی و زیست محیطی - به نحو متعادل و یکپارچه، و بر اساس دستاوردهای اهداف توسعه هزاره و تلاش برای پرداختن به کارهای ناتمام آن‌ها؛

با یادآوری بیشتر قطعنامه خود {به شماره} ۶۸/۳۰۲ مورخ ۳۱ جولای ۲۰۱۴ در خصوص شرایط بازنگری کلی مجمع عمومی از اجرای نتایج اجلاس جهانی سران درباره جامعه اطلاعاتی و با استقبال از جلسه سطح بالای مجمع در خصوص بازنگری کلی که در دسامبر ۲۰۱۵ برگزار شد؛

با یادآوری اعلامیه اصول و برنامه اقدام مصوب اولین مرحله اجلاس جهانی سران در مورد جامعه اطلاعاتی که از ۱۰ تا ۱۲ دسامبر ۲۰۰۳ در ژنو برگزار گردید و توسط مجمع عمومی تأیید شد و تعهد تونس و دستور کار تونس برای جامعه اطلاعاتی، مصوب دومین مرحله اجلاس جهانی سران که از ۱۶ تا ۱۸ نوامبر ۲۰۰۵ در تونس برگزار و توسط مجمع عمومی تأیید شد؛ باتوجه به گزارش دبیرکل درباره پیشرفت ایجاد شده در پیگیری و اجرای نتایج اجلاس جهانی سران درباره جامعه اطلاعاتی در سطوح بین‌المللی و منطقه‌ای؛

باتوجه به برگزاری مجمع سالیانه اجلاس جهانی سران در مورد جامعه اطلاعاتی، که به‌طور مشترک توسط اتحادیه بین‌المللی مخابرات، کنفرانس تجارت و توسعه سازمان ملل، سازمان آموزشی، علمی و فرهنگی سازمان ملل و برنامه توسعه سازمان ملل برگزار می‌شود، اولین بازنگری ۱۰ ساله رویداد اجلاس جهانی سران درباره جامعه اطلاعاتی که توسط سازمان آموزشی، علمی و فرهنگی سازمان ملل در پاریس از ۲۵ تا ۲۷ فوریه ۲۰۱۳ هماهنگ شد و باتوجه به رویداد سطح بالا در بازنگری ده ساله اجلاس جهانی سران که توسط اتحادیه بین‌المللی مخابرات از ۱۰ تا ۱۳ ژوئن ۲۰۱۴ در ژنو هماهنگ شد؛

همچنین باتوجه به تأسیس کمیسیون پهنای باند جهت توسعه دیجیتال به دعوت دبیرکل اتحادیه بین‌المللی مخابرات و مدیرکل سازمان آموزشی، علمی و فرهنگی سازمان ملل؛ باتوجه به «اهداف پهنای باند برای سال ۲۰۱۵» که اهدافی را برای ایجاد سیاست پهنای باند جهانی و افزایش توانایی و بالابردن استطاعت مالی در پشتیبانی از اهداف توسعه بین‌المللی توافق شده، از جمله اهداف توسعه هزاره تعیین می‌کند، همچنین باتوجه به گزارش کمیسیون باند پهن با عنوان وضعیت پهنای باند سال ۲۰۱۵: پهنای باند به‌عنوان یک رکن برای توسعه پایدار، که یک ارزیابی کشور به کشور از آن اهداف (اهداف پهنای باند در سال ۲۰۱۵) و وضعیت توسعه پهنای باند جهانی را تهیه کرد؛

با توجه بیشتر به برگزاری هجدهمین اجلاس کمیسیون علم و فناوری برای توسعه مورخ ۴ تا ۸ می ۲۰۱۵ در ژنو و باتوجه به گزارش کمیسیون در هجدهمین اجلاس خود، از جمله خلاصه‌ای از بحث اساسی در خصوص بازنگری ۱۰ ساله اجرای نتایج اجلاس جهانی سران همراه با پیوستی از مداخلات شکل گرفته در آن رابطه و گزارش آماده شده توسط دبیرخانه کنفرانس تجارت و توسعه سازمان ملل با عنوان «اجرای نتایج اجلاس جهانی سران درباره جامعه اطلاعاتی: بازنگری ۱۰ ساله» که مبنایی برای بحث اساسی بود و جهت بررسی فرایند مقدماتی مذاکرات نشست سطح بالای مجمع عمومی، ارسال شده بود؛

باتوجه به مراجع فناوری‌های اطلاعات و ارتباطات که در دستور کار توسعه پایدار و دستور کار اقدام آدیس آبابا گنجانده شده است؛

با به رسمیت شناختن این حقیقت که فناوری‌های اطلاعات و ارتباطات توانمندسازهای حیاتی برای سرمایه‌گذاری و توسعه اقتصادی با مزایای تبعی برای استخدام و رفاه اجتماعی هستند و اینکه فراگیری فزاینده تکنولوژی اطلاعات و ارتباطات داخل جامعه تأثیر عمیقی بر راه‌هایی که در آن‌ها دولت‌ها، خدمات، کسب‌وکارهای مربوط به مشارکت مشتریان و شهروندان در زندگی خصوصی و عمومی را ارائه می‌نمایند، داشته است؛

با استقبال از تلاش‌هایی که کشورهای میزبان در سازماندهی نشست‌های مجمع حکمرانی اینترنت، متقبل شده‌اند، نشست‌های برگزار شده در آتن در سال ۲۰۰۶، ریودوژانیرو برزیل در

سال ۲۰۰۷، حیدرآباد هند در سال ۲۰۰۸، شرم الشیخ مصر در سال ۲۰۰۹، ویلنیوس پایتخت لیتوانی در سال ۲۰۱۰، نایروبی در سال ۲۰۱۱، باکو در سال ۲۰۱۲، بالی هندوستان در سال ۲۰۱۳، استانبول ترکیه در سال ۲۰۱۴ و جوآن پوزا برزیل از ۱۰ تا ۱۳ نوامبر سال ۲۰۱۵؛

۱. به رسمیت می‌شناسد که فناوری‌های اطلاعات و ارتباطات قابلیت ارائه راه‌حل‌های جدید برای چالش‌های توسعه، به‌ویژه در چارچوب جهانی‌سازی را دارند و می‌تواند رشد اقتصادی دائمی، فراگیر و برابر و یکسان و توسعه پایدار، رقابتی، دسترسی به دانش و اطلاعات، ریشه‌کنی فقر و جامعه شمولی را تقویت کند که این امر به تسریع در پیوستن تمامی کشورها، به‌ویژه کشورهای در حال توسعه به خصوص کشورهای کمتر توسعه‌یافته به اقتصاد جهانی کمک خواهد کرد؛

۲. تشویق می‌کند تقویت و تداوم همکاری بین ذی‌نفعان جهت حصول اطمینان از اجرای مؤثر نتایج اجلاس جهانی سران درباره جامعه اطلاعاتی ژنو و تونس، در کنار موارد دیگر، از طریق ارتقای مشارکت چندذی‌نفعی ملی، منطقه‌ای و بین‌المللی، از جمله مشارکت بخش‌های خصوصی - عمومی و ارتقای بسترهای موضوعی چندذی‌نفعی ملی، منطقه‌ای درباره تلاش و گفتگوی مشترک با کشورهای در حال توسعه از جمله کشورهای کمتر توسعه‌یافته، توسعه شرکا و بازیگران در بخش فناوری‌های اطلاعات و ارتباطات؛

۳. به پیشرفتی که توسط نهادهای سازمان ملل در همکاری با دولت‌های ملی، کمیسیون‌های منطقه‌ای و سایر ذی‌نفعان از جمله سازمان‌های غیردولتی و بخش خصوصی در اجرای خطوط اقدام گنجانده شده در اسناد منتج از اجلاس جهانی سران درباره جامعه اطلاعاتی حاصل شده است توجه می‌کند و به استفاده از آن خطوط اقدام جهت دستیابی به اهداف توسعه هزاره جهت توسعه پایدار تشویق می‌کند؛

۴. بر اهمیت نقش ایفا شده توسط بخش خصوصی، جامعه مدنی و جوامع فنی در فناوری‌های اطلاعات و ارتباطات تأکید می‌کند؛

۵. رشد سریع در شبکه‌های دسترسی پهنای باند، به‌ویژه در کشورهای توسعه‌یافته را به رسمیت می‌شناسد و در خصوص رشد شکاف دیجیتال در میزان دسترسی (دسترس پذیری)،

استطاعت مالی (به صرفه بودن)، کیفیت دسترسی و استفاده از پهنای باند بین کشورهای پردرآمد و سایر نواحی با کشورهای کمتر توسعه یافته و آفریقا، به عنوان یک قاره که از بقیه کشورهای دنیا عقب مانده است، ابراز نگرانی می کند؛

۶. ابراز نگرانی راجع به شکاف دیجیتالی بین کشورها در سطوح مختلف دسترسی به فناوری های اطلاعات و ارتباطات و اتصال پهنای باند که بر بسیاری از کاربردهای اقتصادی و اجتماعی مرتبط از قبیل حوزه های دولتی، تجارت، سلامت، آموزش، تأثیر می گذارد. و همچنین در ارتباط با چالش های ویژه که کشورهای در حال توسعه از جمله کشورهای کمتر توسعه یافته، دولت های جزیره ای کوچک در حال توسعه و کشورهای در حال توسعه محصور در خشکی، در حوزه اتصال پهنای باند با آن مواجه شده اند، ابراز نگرانی می کند؛

۷. از آنجایی که در گزارش دبیرکل در خصوص پیشرفت ایجاد شده در اجرا و پیگیری نتایج اجلاس جهانی سران در سطوح منطقه ای و بین المللی دیده شده است، به اجرای نتایج اجلاس جهانی سران درباره جامعه اطلاعاتی در سطح منطقه ای که توسط کمیسیون های منطقه ای تسهیل شده است، توجه می کند؛

۸. صندوق ها و برنامه های سازمان ملل و سازمان های تخصصی را جهت مشارکت برای اجرای نتایج اجلاس جهانی سران درباره جامعه اطلاعاتی، مطابق با (در محدوده) دستور کارهای مربوط و طرح های راهبردی خودشان تشویق می کند و بر اهمیت تخصیص منابع کافی در این موضوع تأکید می کند؛

۹. ضمن استقبال توأم با قدردانی از پیشنهاد توسط مکزیک برای میزبانی نشست مجمع حکمرانی اینترنت در سال ۲۰۱۶، توصیه می کند که گسترش دستور کار مجمع در چارچوب بازنگری کلی سال ۲۰۱۵ در نظر گرفته شود؛

۱۰. بر نیاز به مشارکت بیشتر تمامی کشورهای در حال توسعه به ویژه کشورهای کمتر توسعه یافته، در کلیه نشست های مجمع حکمرانی اینترنت تأکید می کند و در این رابطه از دولت های عضو و نیز سایر ذی نفعان دعوت می کند تا از مشارکت دولت ها و سایر ذی نفعان از کشورهای در حال توسعه در مجمع خود و نیز نشست های مقدماتی پشتیبانی نمایند؛

۱۱. نیاز به تحت کنترل درآوردن قابلیت های فناوری اطلاعات و ارتباطات به عنوان توانمندساز حیاتی برای توسعه پایدار و غلبه بر شکاف دیجیتالی را به رسمیت می شناسد و بر مورد نظر قرار دادن ظرفیت سازی جهت استفاده مولد از چنین فناوری هایی بر اجرای دستور کار توسعه پایدار و دستور کار اقدام آدیس آبابا در سومین کنفرانس بین المللی درباره تأمین مالی توسعه تأکید می کند؛

۱۲. از دبیر کل می خواهد تا از طریق کمیسیون علم و فناوری برای توسعه و شورای اقتصادی و اجتماعی، گزارشی به مجمع عمومی در اجلاس هفتادویکم خود در خصوص وضعیت اجرا و پیگیری قطعنامه موجود، در نظر گرفتن دستور کار توسعه پایدار، دستور کار اقدام آدیس آبابا، فرایند بازنگری اجلاس جهانی سران درباره جامعه اطلاعاتی و سایر فرایندهای مرتبط - به عنوان بخشی از گزارش سالانه خود درباره پیشرفت ایجاد شده در اجرا و پیگیری نتایج اجلاس جهانی سران در سطوح منطقه ای و بین المللی - ارائه کند و جهت گنجاندن بخش «فناوری های اطلاعات و ارتباطات برای توسعه» در دستور کار موقت اجلاس هفتادویکم خود، تصمیم می گیرد مگر اینکه در بحث های مربوط به تجدید فعالیت کمیته دوم به نحو دیگری توافق شود.

نشست عمومی ۸۱ مورخ ۲۲ دسامبر ۲۰۱۵

بند هفت: فناوری اطلاعات و ارتباطات برای توسعه سال ۲۰۱۸

ترجمه سند



مجمع عمومی
کمیته دوم

تاریخ انتشار: ۸ ژانویه ۲۰۱۹

شماره قطعنامه: A/RES/73/218

توزیع: عمومی

اجلاس هفتادوسوم

دستور کار ۱۷

قطعنامه مصوب مجمع عمومی مورخ ۲۰ دسامبر ۲۰۱۸ بر اساس گزارش کمیته دوم (A/73/535)

فناوری اطلاعات و ارتباطات برای توسعه

با یادآوری قطعنامه‌های خود {به شماره} ۵۶/۱۸۳ مورخ ۲۱ دسامبر ۲۰۰۱، ۵۷/۲۳۸ مورخ ۲۰ دسامبر ۲۰۰۲، قطعنامه ۵۷/۲۷۰ مورخ ۲۳ ژوئن ۲۰۰۳، ۵۹/۲۲۰ مورخ ۲۲ دسامبر ۲۰۰۴، ۶۰/۲۵۲ مورخ ۲۷ مارس ۲۰۰۶، ۶۲/۱۸۲ مورخ ۱۹ دسامبر ۲۰۰۷، ۶۳/۲۰۲ مورخ دسامبر ۲۰۰۸، ۶۴/۱۸۷ مورخ ۲۱ دسامبر ۲۰۰۹، ۶۵/۱۴۱ مورخ ۲۰ دسامبر ۲۰۱۰، ۶۶/۱۸۴ مورخ ۲۲ دسامبر ۲۰۱۱، ۶۷/۱۹۵ مورخ ۲۱ دسامبر ۲۰۱۲، ۶۸/۱۹۸ مورخ ۲۰ دسامبر ۲۰۱۳ و ۶۹/۲۰۴ مورخ ۱۹ دسامبر ۲۰۱۴، ۷۰/۲۰۱۴، ۷۱/۲۱۲ مورخ ۲۱ دسامبر ۲۰۱۶ و ۷۲/۲۰۰ مورخ ۲۰ دسامبر ۲۰۱۷؛

با یادآوری قطعنامه‌های شورای اقتصادی و اجتماعی {به شماره} ۲۰۰۶/۴۶ مورخ ۲۸ جولای ۲۰۰۶، ۲۰۰۸/۳ مورخ ۱۸ جولای ۲۰۰۸، ۲۰۰۹/۷ مورخ ۲۴ جولای ۲۰۰۹، ۲۰۱۰/۲ مورخ ۱۹ جولای ۲۰۱۰، ۲۰۱۱/۱۶ مورخ ۲۶ جولای ۲۰۱۱، ۲۰۱۲/۵ مورخ ۲۴ جولای ۲۰۱۲، ۲۰۱۳/۹ مورخ ۲۲ جولای ۲۰۱۳ و ۲۰۱۴/۲۷ مورخ ۱۶ جولای ۲۰۱۴، ۲۰۱۵/۲۶ مورخ ۲۲ جولای ۲۰۱۵، ۲۰۱۶/۲۲ مورخ ۲۷ جولای ۲۰۱۶ و ۲۰۱۸/۲۸ مورخ ۲۴ جولای ۲۰۱۸، و با توجه به قطعنامه شورا {به شماره} ۲۰۱۷/۲۱ مورخ ۶ جولای ۲۰۱۷، در خصوص ارزیابی پیشرفت ایجاد شده در اجرا و پیگیری نتایج اجلاس جهانی سران درباره جامعه اطلاعاتی؛

با تأیید مجدد قطعنامه خود {به شماره} ۷۰/۱ مورخ ۲۵ سپتامبر ۲۰۱۵ با عنوان «تبدیل دنیای ما: دستور کار توسعه پایدار» که در آن مجموعه‌ای جامع، گسترده، مردم‌محور از اهداف و مقاصد تحول آمیز و جهانی توسعه پایدار تصویب شد، تعهدات خود جهت کار خستگی‌ناپذیر برای اجرای کامل دستور کار،

با به رسمیت شناختن اینکه ریشه‌کن کردن فقر در تمامی اشکال و ابعاد آن، از جمله فقر شدید، بزرگ‌ترین چالش جهانی و یک الزام ضروری برای توسعه پایدار است؛ و به رسمیت شناختن تعهد خود جهت دستیابی به توسعه پایدار در سه بعد - اقتصادی، اجتماعی و زیست محیطی - به نحو متعادل و یکپارچه و بر اساس دستاوردهای اهداف توسعه هزاره و تلاش برای پرداختن به کارهای ناتمام آن‌ها؛ با یادآوری قطعنامه خود {به شماره} ۷۰/۲۹۹ مورخ ۲۹ جولای ۲۰۱۶ درباره پیگیری و بررسی دستور کار توسعه پایدار در سطح جهانی؛

با تأیید مجدد، قطعنامه خود {به شماره} ۶۹/۳۱۳ مورخ ۲۷ جولای ۲۰۱۵ درباره دستور کار اقدام آدیس آبابا در سومین کنفرانس بین‌المللی تأمین مالی توسعه، که بخش جداناپذیری از دستور کار توسعه پایدار می‌باشد، ضمن حمایت و تکمیل آن، با خط‌مشی و اقدامات قوی، به مفهوم سازی ابزار آن جهت اجرای اهداف کمک می‌نماید و مجدداً، تعهد (الزام) سیاسی قوی جهت مقابله با چالش‌های تأمین مالی و ایجاد محیط توانمندساز در تمامی سطوح توسعه پایدار با روحیه مشارکت و اتحاد جهانی را تأیید می‌نماید؛

همچنین با تأیید مجدد دستور کار مدنی جدید مصوب کنفرانس ملل متحد درباره مسکن و توسعه پایدار شهری (محل سکونت) که در شهر کیوتو اکوادور مورخ ۱۷ تا ۲۰ اکتبر ۲۰۱۶ برگزار گردید،

با به رسمیت شناختن نقش کمیسیون علم و فناوری برای توسعه به‌عنوان نقطه کانونی ملل متحد درباره علم، فناوری و نوآوری برای توسعه پایدار و {همچنین} به‌عنوان مجمعی درباره رسیدگی به سؤالات علم و فناوری، {همچنین} ضمن به رسمیت شناختن نقش علم و فناوری به‌عنوان توانمندساز برای دستیابی به دستور کار توسعه پایدار، پیشرفت در درک خط‌مشی‌های علم و فناوری علی‌الخصوص در رابطه با کشورهای در حال توسعه و قاعده مند کردن توصیه‌ها و

خطوط راهنما درباره موضوعات علم و فناوری برای توسعه در نظام ملل متحد؛

همچنین ضمن به رسمیت شناختن کمیسیون علم و فناوری برای توسعه به عنوان نقطه کانونی ملل متحد با سیستم گسترده پیگیری در خروجی اجلاس سران درباره جامعه اطلاعاتی؛ با به رسمیت شناختن بیشتر نقش سازوکار (مکانیزم) تسهیل فناوری از جمله:

مجمع چنددی‌نفعی درباره علم، فناوری و نوآوری برای اهداف توسعه پایدار، تیم اقدام بین‌سازمانی درباره علم، فناوری و نوآوری برای اهداف توسعه پایدار و بستر برخط به عنوان ابزاری برای تسهیل همکاری چنددی‌نفعی و مشارکت میان دولت‌های عضو، جامعه مدنی، بخش خصوصی، جامعه علمی، نهادهای نظام بین‌الملل و سایر ذی‌نفعان جهت حمایت از اجرای اهداف توسعه پایدار؛

با یادآوری اعلامیه اصول و برنامه اقدام مصوب اولین مرحله اجلاس جهانی سران در مورد جامعه اطلاعاتی که از ۱۰ تا ۱۲ دسامبر ۲۰۰۳ در ژنو برگزار گردید و توسط مجمع عمومی تأیید شد و تعهد تونس و دستور کار تونس برای جامعه اطلاعاتی، مصوب دومین مرحله اجلاس جهانی سران که از ۱۶ تا ۱۸ نوامبر ۲۰۰۵ در تونس برگزار گردید و توسط مجمع عمومی تأیید شد، با توجه به منابع مندرج در دستور کار توسعه پایدار و دستور کار اقدام آدیس آبابا برای فناوری‌های اطلاعات و ارتباطات، و با تکرار تقاضا جهت هماهنگی نزدیک بین روند اجلاس سران درباره جامعه اطلاعات و دستور کار توسعه پایدار و همچنین سایر خروجی‌های بین‌دولتی مرتبط؛

با یادآوری سند خروجی نشست سطح بالای مجمع عمومی درباره بازنگری کلی اجرای خروجی‌های اجلاس سران درباره جامعه اطلاعاتی که مورخ ۱۵ و ۱۶ دسامبر ۲۰۱۵ در نیویورک برگزار گردید که در آن فرایند اجرای خروجی اجلاس سران به دقت مورد بررسی قرار گرفت {و} به شکاف‌های بالقوه در فناوری اطلاعات و ارتباطات پرداخته شد و حوزه‌هایی جهت تمرکز پیوسته {دائم} معین گردید؛

با تأیید مجدد آمال و تعهد مشترک خود درباره نگاه اجلاس سران درباره جامعه اطلاعاتی همان‌طور که در اعلامیه اصول ژنو مطرح گردید؛

با به رسمیت شناختن اینکه فناوری‌های اطلاعات و ارتباطات فرصت‌ها و چالش‌های جدیدی را ایجاد می‌نماید و نیاز مبرم به مقابله با موانع اصلی که کشورهای در حال توسعه جهت دسترسی

به این فناوری‌های جدید با آن‌ها روبه‌رو هستند وجود دارد؛

با تأکید بر ضرورت مقابله با چالش‌های متداول در رفع شکاف‌های دیجیتال بین مناطق مختلف داخل یک کشور و شکاف‌های دیجیتال بین کشورها (شکاف درون کشوری و شکاف بین کشوری) و {با تأکید بر ضرورت} تحت کنترل درآوردن فناوری اطلاعات و ارتباطات برای توسعه؛ و یادآوری نیاز به اهمیت کیفیت دسترسی جهت رفع شکاف‌های دیجیتال و شکاف‌های دانشی، استفاده از رویکردهای چند بُعدی برای اشخاص معلول جسمی، از جمله سرعت، ثبات، به صرفه بودن، زبان، کارآموزی، ظرفیت‌سازی، محتوای محلی و دسترس‌پذیری؛

باتوجه به گزارش دبیرکل، درباره پیشرفت ایجاد شده در پیگیری و اجرای نتایج اجلاس جهانی سران درباره جامعه اطلاعاتی در سطوح بین‌المللی و منطقه‌ای؛

باتوجه به درخواست از کمیسیون علم و فناوری برای توسعه جهت تداوم در ارائه گزارش سالانه به شورای اقتصادی و اجتماعی، در خصوص اجرای خروجی اجلاس سران درباره جامعه اطلاعاتی و با تأیید مجدد نقش کمیسیون، به‌عنوان نقطه کانونی در سیستم گسترده پیگیری جهت مساعدت شورا علی‌الخصوص در بررسی و ارزیابی پیشرفت حاصل در اجرای خروجی اجلاس سران. {این نقش} در قطعنامه شورای {اقتصادی اجتماعی} به شماره ۲۰۰۶/۴۶ تعیین گردید؛ همچنین باتوجه به برگزاری بیست‌ویکمین اجلاس کمیسیون علم و فناوری برای توسعه مورخ ۱۴ تا ۱۸ می ۲۰۱۸ در ژنو، و ضمن انتظار جهت برگزاری اجلاس بیست‌ودوم با اولویت در موضوعات «تأثیر تغییر سریع فنی روی توسعه پایدار» و «نقش علم، فناوری و نوآوری در ایجاد جوامع انعطاف‌پذیر از جمله از طریق مشارکت دانش شهروندی»، {و} بدینسان، تهیه بستری برای تمامی ذی‌نفعان جهت به اشتراک گذاری تجربیات و پیگیری مشارکت جهت ظرفیت‌سازی؛

با استقبال از آغاز میزگرد سطح بالا درباره همکاری دیجیتالی در سال ۲۰۱۹، که در آن دبیرکل توصیه‌های خود را در خصوص نظام‌های اثربخش و فراگیر در همکاری دیجیتالی میان تمامی بازیگران مرتبط در فضای دیجیتال ارائه خواهد داد؛

باتوجه به برگزاری مجمع سالیانه اجلاس جهانی سران در مورد جامعه اطلاعاتی که به‌طور مشترک توسط اتحادیه بین‌المللی مخابرات، کنفرانس تجارت و توسعه سازمان ملل، سازمان آموزشی،

علمی و فرهنگی سازمان ملل و برنامه توسعه سازمان ملل برگزار می‌شود؛

باتوجه به گزارش کمیسیون پهنای باند برای توسعه پایدار با عنوان «وضعیت پهنای باند ۲۰۱۸: پهنای باند، تسریع کننده توسعه پایدار» که ارزیابی از پیشرفت به سوی دستیابی به اهداف حمایتی کمیسیون درخصوص پهنای باند و وضعیت توسعه پهنای باند در گستره جهانی را ارائه می‌دهد؛

باتوجه به نیاز به رفع شکاف‌های دیجیتالی و توجه به گزارش اجلاس ویژه کمیسیون با عنوان «همکاری جهت اتصال نزدیک به یک‌ونیم میلیارد نفر به اینترنت تا سال ۲۰۲۰» که در آن کمیسیون اشاره نمود که در حال حاضر کمتر از نیمی از جمعیت جهان در و تعداد کمتر از یک دهم جمعیت در کشورهای کمتر توسعه یافته به اینترنت متصل می‌باشند؛

با به رسمیت شناختن، این حقیقت که فناوری‌های اطلاعات و ارتباطات، در کنار موانع قانون گذاری در مشارکت اقتصادی، توانمندسازی‌های حیاتی برای سرمایه گذاری و توسعه اقتصادی با مزایای تبعی برای استخدام و رفاه اجتماعی هستند و اینکه فراگیری فزاینده تکنولوژی اطلاعات و ارتباطات داخل جامعه تأثیر عمیقی بر راه‌هایی که در آن‌ها دولت‌ها، خدمات، کسب و کارهای مربوط به مشارکت مشتریان و شهروندان در زندگی خصوصی و عمومی را ارائه می‌نمایند، داشته است؛ با تأکید بر اینکه، باوجود پیشرفت اخیر، اهمیت و رشد شکاف‌های دیجیتال بین کشورهای در حال توسعه و بین آن‌ها در موضوعات زیر همچنان باقی است دسترسی پذیری، به صرفه بودن، استفاده از فناوری اطلاعات و ارتباطات و دسترسی به پهنای باند؛

همچنین با تأکید بر نیاز مبرم به رفع شکاف دیجیتالی از جمله در باب موضوعاتی مانند به صرفه بودن اینترنت و {همچنین با تأکید بر نیاز به} حصول اطمینان از اینکه منافع فناوری‌های اطلاعات و ارتباطات از جمله فناوری‌های نوین، برای همه دسترس پذیر می‌باشد، {و} در این رابطه با تأیید مجدد تعهد خود جهت افزایش قابل توجه دسترسی به اینترنت در کشورهای کمتر توسعه یافته تا سال ۲۰۲۰، و باتوجه به تلاش‌های فراوان در کمک به رفع شکاف‌های دیجیتالی و توسعه دسترسی به انضمام دستور کار اتصال ۲۰۲۰ برای توسعه فناوری‌های اطلاعات و ارتباطات/ مخابرات جهانی؛

باتوجه به گروه کاری کمیسیون پهنای باند در خصوص توسعه پایدار درباره شکاف دیجیتالی و توصیه‌های مندرج در گزارش پیشرفت خود درباره اقدام در رفع این شکاف‌ها، برای مثال: مقابله با موانع از جمله موانع مربوط به دسترسی، به صرفه‌بودن، ایمنی، مهارت‌های دیجیتال، ارتباط و همکاری، به اشتراک‌گذاری رویه‌های برتر؛

و با توجه بیشتر به گزارش گروه کاری کمیسیون پهنای باند درباره آموزش با عنوان «مهارت‌های دیجیتال برای زندگی و کار» که ظهور شکاف‌های مهارتی جدید در سطح جهان را برجسته می‌نماید و ارائه راهبردهایی جهت تضمین توانایی تمامی گروه‌های مردمی در توسعه مهارت‌ها داشته باشد، ضمن به رسمیت شناختن نیاز جهت تمرکز روی خط‌مشی‌های توسعه ظرفیت و حمایت پایدار برای ارتقای بیشتر تأثیر فعالیت‌ها و ابتکارات در سطوح ملی و محلی با هدف تهیه تجهیزات، خدمات و پشتیبانی، با نگاهی به ایجاد جامعه اطلاعاتی فراگیر، مردم‌محور و توسعه‌مدار؛ باتوجه به تداوم ظهور مجموعه‌ای از موضوعات در بحث‌های مرتبط با دسترسی، استفاده و کاربرد فناوری جامعه اطلاعاتی و ارتباطی و تأثیر آن‌ها روی ابعاد اقتصادی، اجتماعی و محیطی توسعه پایدار؛

ضمن تأیید مجدد بر {این موضوع} که مشابه حقوقی که مردم در فضای غیربرخط دارند باید در فضای برخط نیز حفظ گردد و با تأکید بر اینکه پیشرفت به سوی چشم‌انداز ترسیمی اجلاس سران درباره جامعه اطلاعاتی نه تنها به‌عنوان تابعی از توسعه اقتصادی و گسترش فناوری اطلاعات و ارتباطات بلکه باید به‌عنوان تابعی از پیشرفت در ارتباط با تحقق حقوق بشر و آزادی‌های اساسی مورد نظر باشد؛

همچنین با تأیید مجدد اینکه حکمرانی اینترنت از جمله فرایند همکاری‌های ارتقای یافته و گردهمایی مجمع حکمرانی اینترنت، جهت پیگیری مفاد تعیین شده در خروجی اجلاس سران در ژنو و تونس باید تداوم داشته باشد؛

با استقبال از تلاش‌های کشورهای میزبان که سازماندهی نشست‌های مجمع حکمرانی اینترنت را به عهده داشتند: ۲۰۰۶ آتن {یونان}، ۲۰۰۷ ریودوژانیرو برزیل، ۲۰۰۸ حیدرآباد

هند، ۲۰۰۹ شرم الشيخ مصر، ۲۰۱۰ ویلنس {لیتوانی}، ۲۰۱۱ نایروبی {کنیا}، ۲۰۱۲ باکو {آذربایجان}، ۲۰۱۳ بالی اندونزی، ۲۰۱۴ استانبول ترکیه، ۲۰۱۵ جوآ پوسا برزیل، ۲۰۱۶ گوآداجرا مکزیک، ۲۰۱۷ ژنو، ۲۰۱۸ پاریس و انتظار جهت برگزاری نشست مجمع حکمرانی اینترنت در برلین {آلمان} در سال ۲۰۱۹، همچنین با استقبال از بیانیه گروه کاری درباره همکاری ارتقاء یافته، بر اساس پیشنهاد رئیس کمیسیون علم و فناوری برای توسعه در رابطه با ساختار و ترکیب گروه کاری، همان طور که مجمع عمومی در قطعنامه خود {به شماره} ۷۰/۱۲۵ مورخ ۱۶ دسامبر ۲۰۱۵ درخواست نمود و در قطعنامه شورای اقتصادی اجتماعی {به شماره} ۲۰۱۷/۲۱ تأیید گردید؛ با توجه به اینکه فناوری‌های اطلاعات و ارتباطات می‌توانند به تسریع پیشرفت به سوی اهداف توسعه پایدار کمک نمایند و همچنین با توجه به اهمیت نقش اتحادیه بین‌المللی مخابرات {در میان موارد دیگر} در پشتیبانی دولتهای عضو جهت اجرای اهداف توسعه پایدار،

همچنین با توجه به تشکیل جلسه کنفرانس جهانی توسعه مخابرات، مورخ ۹ تا ۲۰ اکتبر ۲۰۱۷ در بوینس آیرس {آرژانتین}، تحت موضوع «فناوری اطلاعات و ارتباطات برای اهداف توسعه پایدار» که توسط اتحادیه بین‌المللی مخابرات، {برگزار گردید}؛

با توجه بیشتر به اینکه تغییر فنی شامل {ایجاد} ابزار جدید و قدرتمند برای توسعه می‌باشد و {همچنین با توجه به} آگاهی از تأثیرات آن (تغییر فنی)، فرصت‌ها و چالش‌ها و اینکه دولت‌ها، بخش خصوصی، سازمان‌های بین‌المللی، جامعه مدنی، جوامع فنی و دانشگاهی باید موضوعات اجتماعی، اقتصادی، اخلاقی، فرهنگی و فنی مرتبط با پیشرفت‌های فنی سریع را به منظور درک عمیق از چگونگی تحت کنترل درآوردن قابلیت آن‌ها برای پشتیبانی از دستورکار توسعه پایدار را مورد نظر قرار دهند؛

با تأیید مجدد ارزش و اصول همکاری چندذی‌نفعی و تعاملی که از زمان شروع فرایند اجلاس سران درباره جامعه اطلاعاتی توصیف گردیده است و با به رسمیت شناختن اینکه نقش اثربخش، مشارکت و همکاری دولت‌ها، بخش خصوصی، جامعه مدنی، سازمان‌های بین‌المللی، جوامع فنی و دانشگاهی و تمامی ذی‌نفعان مرتبط دیگر، در چارچوب و حیطه مسئولیت‌ها و نقش‌های مربوط خود، در توسعه جامعه اطلاعاتی حیاتی است و همچنان حیاتی هستند، به‌ویژه

{مشارکت و همکاری} متوازن نمایندگان کشورهای در حال توسعه؛

با آگاهی از چالش‌های پیش روی دولت‌ها درباره پیشگیری و مبارزه با استفاده از فناوری‌های اطلاعات و ارتباطات برای اهداف مجرمانه، از جمله توسط تروریست‌ها، و با تأکید بر ضرورت ادامه همکاری بین‌المللی در این رابطه و تقویت مساعدت فنی و اقدامات ظرفیت‌سازی و {ضرورت} درخواست دولت‌ها جهت پیشگیری، تعقیب و مجازات چنین استفاده‌هایی مطابق با حقوق ملی و بین‌المللی؛ با تصریح مجدد {این تعهد} که هیچ کسی از این پس کنار گذاشته نخواهد شد {فرد فرد شهروندان جهان مخاطب ما هستند}؛

با تأیید مجدد اینکه شأن و کرامت فرد انسان (نوع بشر) به‌عنوان امری اساسی به رسمیت شناخته شده است، و آرزو جهت حصول اهداف و مقاصد شایسته و مناسب برای تمامی ملل و افراد و برای تمامی بخش‌های اجتماع و با توصیه مجدد جهت تلاش برای رسیدن عقب‌مانده‌ترین ملل؛ با توصیه مجدد جهت تضمین اینکه هیچ کشور و یا شخصی کنار گذاشته نخواهد شد و تضمین اینکه تلاش ما روی {کشورهایی} است که درگیر بزرگ‌ترین چالش می‌باشند از جمله از طریق تضمین حضور و مشارکت آن‌هایی که دچار بیشترین عقب ماندگی هستند؛

۱. به رسمیت می‌شناسد که فناوری‌های اطلاعات و ارتباطات قابلیت ارائه راه‌حل‌های جدید برای چالش‌های توسعه، به‌ویژه در چارچوب جهانی سازی را دارند و می‌تواند رشد اقتصادی دائمی، فراگیر و برابر و یکسان و توسعه پایدار، رقابتی، دسترسی به دانش و اطلاعات، تجارت و توسعه، ریشه‌کنی فقر و جامعه شمولی را تقویت کند که این امر به تسریع در پیوستن تمامی کشورها، به‌ویژه کشورهای در حال توسعه به خصوص کشورهای کمتر توسعه‌یافته به اقتصاد جهانی کمک خواهد کرد؛

۲. از تکامل و گسترش قابل ملاحظه فناوری‌های اطلاعاتی و ارتباطی استقبال می‌کند که:

✓ نتیجه مشارکت هر دو بخش عمومی و خصوصی است؛

✓ گستره نفوذ این فناوری در هر گوشه‌ای از جهان قابل رویت است؛

✓ فرصت‌های جدید را برای تعاملات اجتماعی ایجاد کرده است؛

✓ الگوی کسب و کار جدیدی را فعال و توانمند نموده است؛

✓ به رشد و توسعه اقتصادی سایر بخش‌ها کمک کرده است

ضمن توجه به این نکته که تکامل و گسترش فناوری با چالش‌های منحصربه‌فرد و نوپدید نیز همراه می‌باشد.

۳. قابلیت فناوری‌های اطلاعات و ارتباطات را جهت دستیابی به دستور کار توسعه پایدار، و سایر اهداف توسعه‌ای مورد وفاق بین‌المللی به رسمیت می‌شناسد، ضمن توجه به اینکه این فناوری‌ها می‌توانند پیشرفت تمامی اهداف هفده‌گانه توسعه پایدار را تسریع نمایند از این رو، درخواست می‌نماید تا تمامی دولت‌ها، بخش خصوصی، جامعه مدنی، سازمان‌های بین‌المللی، جوامع فنی و دانشگاهی و تمامی ذی‌نفعان مرتبط، فناوری‌های اطلاعات و ارتباطات را در رویکردهای خود جهت اجرای این اهداف یکپارچه نمایند و از نهادهای نظام ملل متحد درخواست می‌نماید تا خطوط اقدام اجلاس سران درباره جامعه اطلاعاتی را جهت بررسی گزارش‌دهی و برنامه‌های کاری خود برای پشتیبانی از اجرای دستور کار توسعه پایدار تسهیل نمایند.

۴. تعهدات خود مبنی بر از بین بردن شکاف‌های دیجیتالی و دانشی را تأیید می‌کند. اینکه رویکرد سازمان ملل باید چند بعدی و شامل یک فهم منطقی از عناصر و منابع در دسترس با تأکید بر کیفیت دسترسی باشد را به رسمیت شناخته و بر عناصر اصلی کیفیت در عصر حاضر {مانند} سرعت، ثبات، به صرفه بودن، زبان، محتوای منطقه‌ای و قابلیت دسترس‌پذیری برای اشخاص معلول و نیز ضرورت پهنای باند با سرعت بالا به‌عنوان عنصری توانمند برای توسعه پایدار تأکید می‌نماید؛

۵. بر اهمیت ایفای نقش بخش خصوصی، جامعه مدنی و جوامع فنی در فناوری‌های اطلاعات و ارتباطات تأکید می‌نماید.

۶. تقویت و تداوم همکاری بین ذی‌نفعان کشورهای توسعه‌یافته و در حال توسعه را، در راستای ایفای نقش و مسئولیت‌های مربوط به خود، جهت حصول اطمینان از {مورد زیر} تشویق می‌نماید: اجرای مؤثر نتایج اجلاس جهانی سران درباره جامعه اطلاعاتی ژنو و تونس، در کنار موارد دیگر، از طریق ارتقای مشارکت چندذی‌نفعی ملی، منطقه‌ای و بین‌المللی، از جمله مشارکت خصوصی - عمومی و ارتقای بسترهای موضوعی چندذی‌نفعی ملی، منطقه‌ای

درباره تلاش و گفتگوی مشترک با کشورهای در حال توسعه از جمله کشورهای کمتر توسعه یافته، توسعه شرکا و بازیگران در بخش فناوری‌های اطلاعات و ارتباطات؛

۷. به پیشرفتی که توسط نهادهای نظام سازمان ملل در همکاری با دولت‌های ملی، کمیسیون‌های منطقه‌ای و سایر ذی‌نفعان از جمله سازمان‌های غیر دولتی و بخش خصوصی در اجرای خطوط اقدام گنجانده شده در اسناد منتج از اجلاس جهانی سران درباره جامعه اطلاعاتی حاصل شده است توجه می‌کند و به استفاده از آن خطوط اقدام جهت اجرای دستور کار توسعه پایدار تشویق می‌کند؛

۸. همچنین به این نکته توجه می‌نماید که اقتصاد دیجیتال یک بخش مهم و در حال رشدی از اقتصاد جهانی می‌باشد و این هم‌افزایی و اتصال {به اقتصاد جهانی} با افزایش تولید ناخالص داخلی ارتباط دارد و اهمیت حیاتی توسعه مشارکت تمامی کشورها علی‌الخصوص کشورهای در حال توسعه در اقتصاد جهانی را به رسمیت می‌شناسد؛

۹. درخواست می‌نماید تا از طریق ابتکاراتی مانند تجارت الکترونیکی برای همه، که در چهاردهمین اجلاس کنفرانس تجارت و توسعه ملل متحد راه اندازی شد، در راستای {اجلاس مذکور} که مورخ ۱۷ تا ۲۲ جولای ۲۰۱۶ در نیروبی برگزار گردید، در کسب دستاوردهای حداکثری توسعه از تجارت الکترونیک، تمرکز مستمری داشته باشند که رویکرد جدیدی برای توسعه و تجارت از طریق تبادل الکترونیک فراهم می‌آورد. رویکرد جدید برای کشورهای در حال توسعه این امکان را فراهم می‌کند که راحت تر به هدایت کمک‌های فنی در راستای ظرفیت‌سازی در کسب آمادگی‌های مربوط به تجارت الکترونیک اقدام کنند. این رویکرد همچنین به داوطلبان مالی کمک می‌کند تا تصویری واضح و روشن از برنامه‌هایی داشته باشند که باید در آن‌ها سرمایه‌گذاری کنند؛

۱۰. در این رابطه {ابتکار و اقدام} کنفرانس ملل متحد درباره تجارت و توسعه ارزیابی‌های آمادگی سریع تجارت الکترونیکی در کشورهای کمتر توسعه یافته را به رسمیت می‌شناسد که با همکاری حامیان مالی داوطلبانه و سازمان‌ها به منظور بالابردن آگاهی از فرصت‌ها و چالش‌های مرتبط با نفوذ تجارت الکترونیکی در کشورهای کمتر توسعه یافته شروع و تکمیل نموده است؛

۱۱. از برگزاری دومین نشست گروه کارشناسان بین دولتی درباره تجارت الکترونیک و اقتصاد دیجیتال، و توصیه‌های سیاستی و تصمیمات آن مبنی بر تأسیس گروه کاری درباره اقدامات تجارت الکترونیکی و اقتصاد دیجیتال که جهت پیشنهاد به شورای تجارت و توسعه کنفرانس تجارت و توسعه سازمان ملل {آماده گردید} استقبال می‌نماید؛

۱۲. همچنین از برگزاری هفته تجارت الکترونیک از ۱۶ تا ۲۰ آوریل ۲۰۱۸، با موضوع «ابعاد توسعه در بستر های دیجیتال» و {برگزاری} اولین هفته تجارت الکترونیکی آفریقا مورخ ۱۰ تا ۱۴ دسامبر ۲۰۱۸ در نایروبی استقبال می‌نماید؛

۱۳. ضمن استقبال بیشتر از عملکرد سازمان یونسکو {در خصوص} «اطلاعات برای تمامی برنامه ها» جهت مساعدت دولت‌های عضو در قاعده‌مهندسازی خط‌مشی‌ها برای رفع شکاف‌های دیجیتالی و تضمین جوامع دانشی برابر، همچنین از برگزاری هفته سواد رسانه و اطلاعات مورخ ۲۴ تا ۳۱ اکتبر ۲۰۱۸ استقبال می‌نماید؛

۱۴. باوجود پیشرفت‌ها و دستاوردهای قابل توجه که اخیراً حاصل شده است، وجود رشد نابرابر در دسترسی و استفاده از فناوری اطلاعات و ارتباطات را به رسمیت می‌شناسد و درباره شکاف اساسی دامنه‌دار دیجیتال و شکاف در پهنای باند بین کشورهای توسعه‌یافته و در حال توسعه و داخل آن‌ها ابراز نگرانی می‌نماید. از جمله درخصوص این حقیقت که ۹۷ درصد از مشترکان تلفن‌های همراه در کشورهای توسعه‌یافته از پهنای باند استفاده می‌نمایند و در مقایسه با آن این میزان در کشورهای در حال توسعه ۴۸ درصد و در کشورهای کمتر توسعه‌یافته ۲۲ درصد می‌باشد. و {همچنین اینکه} هزینه دسترسی به {پهنای باند} در مقایسه با میانگین درآمد خانوادگی، در کشورهای در حال توسعه بالاتر می‌باشد و در نتیجه فقدان دسترسی کم‌هزینه به فناوری اطلاعات و ارتباطات وجود دارد.

۱۵. ضمن تشویق به تحقیق و توسعه، توسعه راهبردهای قابل اجرا که منتج به رقابت، سرمایه‌گذاری بیشتر و کاهش سریع هزینه فناوری اطلاعات و ارتباطات می‌شود، از تمامی ذی‌نفعان مرتبط درخواست می‌نماید تا در کنار سایر موارد از {طرق زیر} با رشد شکاف دیجیتال میان کشورها و همچنین درون آن‌ها مقابله نمایند: محیط‌های سیاسی تقویت‌شده توانمندساز در تمامی سطوح،

چارچوب‌های قانونی و تنظیم مقررات که به افزایش سرمایه‌گذاری و نوآوری منجر می‌شود، مشارکت بخش‌های خصوصی - عمومی، راهبردهای دسترسی جهانی و همکاری بین‌المللی جهت بهبود سودآوری، آموزش، ظرفیت‌سازی، چندزبانی، صیانت فرهنگی، سرمایه‌گذاری و انتقال فناوری بر اساس شرایط مورد توافق طرفین (متقابل)

۱۶. از آنجایی که در گزارش دبیرکل در خصوص پیشرفت ایجاد شده در اجرا و پیگیری نتایج اجلاس جهانی سران در سطوح منطقه‌ای و بین‌المللی دیده شده است، به اجرای نتایج اجلاس جهانی سران درباره جامعه اطلاعاتی در سطح منطقه‌ای، که توسط کمیسیون‌های منطقه‌ای تسهیل شده است، توجه می‌کند؛

۱۷. صندوق‌ها و برنامه‌های سازمان ملل و سازمان‌های تخصصی را جهت مشارکت برای اجرای نتایج اجلاس جهانی سران درباره جامعه اطلاعاتی، مطابق با (در حدود) دستور کارهای مربوط و طرح‌های راهبردی خودشان، تشویق می‌کند، و بر اهمیت تخصیص منابع کافی در این موضوع تأکید می‌کند؛

۱۸. همان‌گونه که در سند خروجی نشست سطح بالای مجمع عمومی درباره بازنگری کلی اجرای خروجی‌های اجلاس سران درباره جامعه اطلاعاتی تنظیم گردید، به توسعه دستورکار مجمع حکمرانی اینترنت در سال ۲۰۲۵، اذعان داریم؛

۱۹. اهمیت مجمع حکمرانی اینترنت و دستور کار آن را به‌عنوان یک مجمع برای گفتگوی چند ذی‌نفعی درباره موضوعات مختلف، همان‌گونه که در بند ۷۲ دستورکار تونس منعکس گردیده است، از جمله بحث درباره موضوعات سیاست عمومی مرتبط با عناصر کلیدی حکمرانی اینترنت، به رسمیت می‌شناسد و از دبیرکل درخواست می‌نماید تا به‌عنوان بخشی از گزارش سالانه خود، {گزارشی} درباره پیشرفت اجرا و تعقیب نتایج اجلاس سران درباره جامعه اطلاعاتی در سطوح منطقه‌ای و بین‌المللی، اطلاعاتی درباره پیشرفت اجرای توصیه‌های مندرج در گزارش گروه کاری درباره اصلاحات مجمع حکمرانی اینترنت را ارائه نماید به‌ویژه توصیه‌هایی که مشارکت کشورهای در حال توسعه را ارتقای می‌بخشد؛

۲۰. بر نیاز به مشارکت بیشتر تمامی دولت‌ها و ذی‌نفعان از کشورهای در حال توسعه به‌ویژه کشورهای

کومتر توسعه یافته، در کلیه نشست‌های مجمع حکمرانی اینترنت تأکید می‌کند و در این رابطه از دولت‌های عضو و نیز سایر ذی‌نفعان مرتبط دعوت می‌کند تا از مشارکت دولت‌ها و سایر ذی‌نفعان از کشورهای در حال توسعه در مجمع خود و نیز نشست‌های مقدماتی پشتیبانی نمایند.

۲۱. به عملکرد گروه کاری در زمینه همکاری ارتقای یافته توجه می‌نماید، که این گروه کاری توسط رئیس کمیسیون علم و فناوری برای توسعه و بنا به درخواست مجمع عمومی در قطعنامه خود {به شماره} ۷۰/۱۲۵، با هدف تهیه توصیه‌نامه‌هایی در خصوص چگونگی اجرای همکاری ارتقای یافته همان‌گونه که در دستور کار تونس دیده شده، ایجاد گردیده است، همچنین {به این موضوع} توجه نماید که گروه کاری تعامل کامل دولت‌ها و سایر ذی‌نفعان مرتبط به‌ویژه از کشورهای در حال توسعه، {و} در نظر گرفتن تمامی دیدگاه‌های گوناگون و تخصص خود، را تضمین خواهد کرد.

۲۲. همچنین به ۵ نشست گروه کاری که بین سپتامبر ۲۰۱۶ تا ژانویه ۲۰۱۸ برگزار گردید {و} در آن همان‌گونه که در قطعنامه مجمع عمومی {به شماره} ۷۰/۱۲۵ تصریح شد، درباره نظرهای دولت‌های عضو و سایر ذی‌نفعان بحث گردید توجه می‌نماید.

۲۳. باتوجه به گزارش رئیس گروه کاری که شامل ارجاعاتی به متن‌های کامل تمامی پیشنهادها و همکاری‌ها می‌باشد، سپاسگزاری خود را از رئیس و تمامی مشارکت‌کنندگانی که نظرهای خود را ارائه دادند و در عملکرد گروه کاری همکاری داشتند بیان می‌نماید.

۲۴. ضمن استقبال از پیشرفت خوب گروه کاری در بسیاری از حوزه‌ها و اموری که {درباره} نوظهور بودن {آن‌ها} در برخی موضوعات اجماع وجود دارد، در رابطه با تداوم واگرایی قابل توجه در نگاه به تعدادی از موضوعات دیگر، از اینکه گروه کاری نتوانست توافقی درباره پیشنهادها در خصوص چگونگی اجرای همکاری ارتقای یافته وفق دستور کار تونس پیدا نماید، متاثر است.

۲۵. تقاضا می‌نماید تا گفتگو و کار درباره انجام همکاری سازمان یافته همان‌گونه که در دستور کار تونس دیده شده ادامه یابد.

۲۶. {موضوعات زیر را} به رسمیت می‌شناسد:

– باقی ماندن فقدان دسترسی به فناوری‌ها و خدمات کم‌هزینه و قابل اعتماد به‌عنوان یک چالش حیاتی در بسیاری از کشورهای در حال توسعه علی‌الخصوص کشورهای آفریقایی، کشورهای کمتر توسعه‌یافته، کشورهایی در حال توسعه محصور در خشکی و دولت‌های جزیره‌ای کوچک در حال توسعه و کشورهایی با درآمد متوسط و نیز کشورها و سرزمین‌های تحت اشغال عوامل بیگانه، کشورهایی در شرایط مخاصمه، کشورهای پساتخاصم و کشورهای متأثر از بلایای طبیعی؛

– ضرورت به‌کارگیری تمامی تلاش‌ها جهت کاهش هزینه و بهای فناوری اطلاعات و ارتباطات و دسترسی به پهنای باند

– یادآوری این موضوع که وفق تحقیقات پیش‌بینی شده از جمله از طریق تحقیق و توسعه و انتقال فناوری در موضوعات مورد توافق متقابل این امکان وجود دارد که در خصوص انتخابهای مربوط به اتصالات {اینترنتو...} گزینه‌هایی با هزینه‌های کمتر وجود داشته باشد.

۲۷. اینکه فناوری اطلاعات و ارتباطات فرصت‌ها و چالش‌های جدیدی را ارائه می‌نماید {ایجاد می‌نماید} و اینکه نیاز مبرم به مقابله با موانع عمده‌ای که کشورهای در حال توسعه در دسترسی به فناوری‌های جدید با آن‌ها مواجه هستند را به رسمیت می‌شناسد، {مقابله با موانع با اقداماتی از قبیل ایجاد} محیط توانمندساز مناسب، منابع کافی، زیرساخت، آموزش، ظرفیت، سرمایه‌گذاری، و اتصالات {اینترنتی} و نیز موضوعات مرتبط با مالکیت فناوری، تنظیم استانداردها و جریان فناوری، و در این رابطه از تمامی ذی‌نفعان درخواست می‌نماید تا منابع دستورکار کافی، ظرفیت‌سازی ارتقای‌یافته و انتقال دانش و فناوری به کشورهای در حال توسعه، به‌ویژه کشورهای کمتر توسعه‌یافته، {را جهت حرکت} به سوی یک جامعه توانمند شده دیجیتالی و اقتصاد دانش بنیان فراهم نمایند.

۲۸. نیاز به تحت کنترل درآوردن قابلیت‌های فناوری اطلاعات و ارتباطات به‌عنوان توانمندساز حیاتی برای توسعه پایدار و غلبه بر شکاف‌های دیجیتالی را بیشتر به رسمیت می‌شناسد و بر مورد نظر قرار دادن ظرفیت‌سازی جهت استفاده مولد از چنین فناوری‌هایی بر اجرای توسعه پایدار و دستور کار اقدام آدیس آبابا در سومین کنفرانس بین‌المللی درباره تأمین مالی توسعه، تأکید می‌کند؛

۲۹. به این نکته توجه می‌نماید، که با وجود اینکه بنیاد و زیربنای محکم (و قوی) برای ظرفیت‌سازی در فناوری اطلاعات و ارتباطات در بسیاری از حوزه‌ها در رابطه با ایجاد جامعه اطلاعاتی گذاشته شده است، اما هنوز نیاز به ادامه تلاش‌ها برای مقابله با چالش‌های مداوم و دامنه‌دار، بویژه برای کشورهای در حال توسعه و کشورهای کمتر توسعه یافته وجود دارد، و توجه‌ها را به تأثیر مثبت توسعه عرضی ظرفیت جلب می‌نماید که، مؤسسات، سازمان‌ها و نهادهایی که با فناوری‌های اطلاعات و ارتباطات و موضوعات حکمرانی اینترنت سروکار دارند را وارد عرصه و تعامل می‌کنند؛

۳۰. اهمیت کمک به کشورهای در حال توسعه علی‌الخصوص کشورهای کمتر توسعه یافته را جهت پرداختن به چالش‌ها و فرصت‌های مرتبط با استفاده از اینترنت، تجارت الکترونیکی، در کنار سایر موارد برای توسعه ظرفیتهای تجارت بین‌المللی خود به رسمیت می‌شناسد؛

۳۱. اهمیت جریان آزاد اطلاعات و دانش را به رسمیت می‌شناسد. همانگونه که میزان توزیع اطلاعات در جهان افزایش یافت و نقش ارتباطات بیش از پیش مهم‌تر گردید. بر تسهیل دستاوردهای قابل توجه در اتصالات اینترنتی و توسعه پایدار در بسیاری از کشورها از طریق موارد زیر { اذعان دارد: جریان‌شناسی و تبیین مسیر اصلی فناوری‌های اطلاعات و ارتباطات در برنامه‌های تحصیلی مدارس، دسترسی آزاد به داده‌ها، تقویت رقابت، ایجاد نظام‌های قانونی و مقررات شفاف، قابل پیش‌بینی، مستقل و غیر تبعیض‌آمیز، همکاری چنددلی‌نفعی، راهبردهای پهنای باند ملی و منطقه‌ای، تخصیص مؤثر طیف‌های فرکانس رادیویی، مدل‌های اشتراک‌گذاری زیرساخت، رویکردهای جامعه محور و تسهیلات دسترسی عمومی؛

۳۲. از تمامی ذی‌نفعان درخواست می‌نماید تا اهداف مرتبط با رفع شکاف‌های دیجیتالی در اشکال مختلف آن را { جهت احصاء موارد زیر { به‌عنوان یک اولویت ذهنی در راهبردهای جامع خود قرار دهند؛

✓ مشارکت در توسعه دولت الکترونیک

۳۳. با نگاهی به کاهش شکاف‌های دیجیتالی میان کشورها و داخل آن‌ها و در نتیجه ایجاد جوامع دانشی و اطلاعاتی، تمرکز مداوم روی خط‌مشی‌ها و کاربردهای فناوری اطلاعات و ارتباطات به نفع افراد کم برخوردار از جمله دسترسی به پهنای باند در سطوح اجتماعات محلی {داشته باشند}؛

۳۴. ضمن توجه به تعهدات ایجاد شده {موجود} در دستور کار اقدام آدیس آبابا، مساعدت رسمی در توسعه و سایر جریان‌های مالی داوطلبانه (اعطایی و غیررسمی) برای فناوری اطلاعات و ارتباطات، که می‌تواند به طور قابل توجهی در ایجاد (شکل‌گیری) خروجی‌های توسعه همکاری نمایند را به رسمیت می‌شناسد، به‌ویژه جایی که آن‌ها می‌توانند خطرهای مربوط به سرمایه‌گذاری عمومی و خصوصی را کاهش دهند و استفاده از فناوری‌های اطلاعات و ارتباطات را برای حکمرانی شایسته و جمع‌آوری مالیات افزایش دهند؛

۳۵. ضمن به رسمیت شناختن اهمیت حیاتی سرمایه‌گذاری بخش خصوصی در زیرساخت فناوری اطلاعات و ارتباطات، محتوا و خدمات و در انتها، اهمیت مشارکت {توأمان} بخش‌های خصوصی و عمومی، راهبردهای دسترسی جهانی و سایر رویکردها، دولت‌ها را جهت ایجاد چارچوب‌های قانونی و تنظیم مقررات که به نوآوری و سرمایه‌گذاری فزاینده منجر خواهد شد تشویق می‌نماید؛

۳۶. ضمن استقبال از برگزاری سه‌سالانه مجمع شورای اقتصادی اجتماعی درباره تأمین مالی برای توسعه، به نتایج و توصیه‌های مورد توافق آن در سطح بین‌دولتی توجه می‌نماید، و منتظر پیشرفت بیشتر در روند پیگیری می‌باشد و {همچنین} از {موضوعات زیر} استقبال می‌نماید:

- عملکرد گروه اقدام بین‌سازمانی درباره تأمین مالی برای توسعه؛

- پیشرفت در عملیاتی کردن مؤلفه‌های سه‌گانه سازوکار تسهیل فناوری؛

- برگزاری سه‌سالانه مجمع چندذی‌نفعی درباره علم، فناوری و نوآوری برای اهداف توسعه پایدار.

۳۷. از سازمان‌های مربوط در نظام سازمان ملل متحد، درخواست می‌نماید تا در دستور کار و منابع مربوط خود، درباره اینکه هیچ شخص و هیچ کشوری در اجرای قطعنامه حاضر رها نمی‌گردد {کنار گذاشته نمی‌شود}، اطمینان حاصل نمایند؛

۳۸. از دبیرکل می‌خواهد تا از طریق کمیسیون علم و فناوری برای توسعه و شورای اقتصادی و اجتماعی، گزارشی به مجمع عمومی در اجلاس هفتادوچهارم خود در خصوص وضعیت اجرا و پیگیری قطعنامه موجود، در نظر گرفتن دستور کار توسعه پایدار، دستور کار اقدام آدیس آبابا، فرایند بازنگری اجلاس جهانی سران درباره جامعه اطلاعاتی، خلاصه‌ای از نشست مجمع چند ذی‌نفعی

درباره علم، فناوری و نوآوری برای اهداف توسعه پایدار سایر فرایندهای مرتبط - به عنوان بخشی از گزارش سالانه خود درباره پیشرفت ایجاد شده در اجرا و پیگیری نتایج اجلاس جهانی سران در سطوح منطقه‌ای و بین‌المللی - ارائه کند؛

۳۹. در خصوص درج بخشی تحت عنوان «فناوری اطلاعات و ارتباطات برای توسعه پایدار»، در دستور کار موقت خود در اجلاس هفتاد و چهارم تصمیم می‌گیرد مگر اینکه به نحو دیگری توافق گردد.

نشست عمومی ۶۲ مورخ ۲۰ دسامبر ۲۰۱۸

جدول ۳: مشخصات قطعنامه‌های «فناوری‌های اطلاعاتی و ارتباطی برای توسعه» ۲۰۰۲ تا ۲۰۱۸

سال صدور قطعنامه	تاریخ انتشار قطعنامه	شماره قطعنامه	شماره اجلاس	شماره دستورکار	شماره گزارش	شماره پیش‌نویس قطعنامه	نماینده گروه ۷۷ جهت ارائه قطعنامه
۲۰۰۲	۴ مارس ۲۰۰۳	A/RES/295/57	۵۷	۳۲	A/57/L.71	A/57/L.71	شلی، چین، کوبا، گواتمالا، هندلسوتو، نیجریه، پاکستان، کره جنوبی، برومبی، سنگال، آفریقای جنوبی و زامبیا
۲۰۰۷	۳۱ ژانویه ۲۰۰۸	A/RES/182/62	۶۲	۵۱	A/62/416	A/C.62/2/L.28	پاکستان
۲۰۰۸	۲۸ ژانویه ۲۰۰۹	A/RES/202/63	۶۳	۴۶	A/63/411	A/C.63/2/L.10	آنتیگوا و باربودا
۲۰۰۹	۹ فوریه ۲۰۱۰	A/RES/187/64	۶۴	۵۰	A/417/64	A/C.64/2/L.26	سودان
۲۰۱۰	۲ فوریه ۲۰۱۱	A/RES/141/65	۶۵	۱۷	A/65/433	A/C.65/2/L.22	یمن
۲۰۱۱	۶ فوریه ۲۰۱۲	A/RES/184/66	۶۶	۱۶	A/66/437	A/C.66/2/L.21	آرژانتین
۲۰۱۲	۵ فوریه ۲۰۱۳	A/RES/195/67	۶۷	۱۷	A/67/434	A/C.67/2/L.36	الجزایر
۲۰۱۳	۱۵ ژانویه ۲۰۱۴	A/RES/198/68	۶۸	۱۶	A/68/435	A/C.68/2/L.18	فیجی
۲۰۱۴	۲۱ فوریه ۲۰۱۵	A/RES/204/69	۶۹	۱۶	A/69/465	A/C.2/69/L.11	بولیوی
۲۰۱۵	۴ فوریه ۲۰۱۶	A/RES/184/70	۷۰	۱۷	A/70/469	A/C.2/70/L.23	آفریقای جنوبی
۲۰۱۶	۱۸ ژانویه ۲۰۱۷	A/RES/71/212	۷۱	۱۶	A/71/460	A/C.2/71/L.15	تایلند
۲۰۱۷	۱۷ ژانویه ۲۰۱۸	A/RES/72/200	۷۲	۱۶	A/72/417	A/C.2/72/L.5	اکوادور
۲۰۱۸	۸ ژانویه ۲۰۱۹	A/RES/73/218	۷۳	۱۷	A/73/523	A/C.2/73/L.29	مصر

بند هشت: قطعنامه اجلاس سران در مورد جامعه اطلاعاتی سال ۲۰۰۴

ترجمه سند



مجمع عمومی
کمیته دوم

تاریخ انتشار: ۱۱ فوریه ۲۰۰۵

شماره قطعنامه: A/RES/59/220

توزیع: عمومی

اجلاس پنجاه و نهم

دستور کار ۴۴

قطعنامه مصوب مجمع عمومی مورخ ۲۲ دسامبر ۲۰۰۴ براساس گزارش کمیته دوم (A/59/480)

اجلاس سران درباره جامعه اطلاعاتی^۱

مجمع عمومی:

با یادآوری قطعنامه‌های خود {به شماره‌های} ۵۶/۱۸۳ مورخ ۲۱ دسامبر ۲۰۰۱، ۵۷/۲۳۸ مورخ ۲۰ دسامبر ۲۰۰۲

با تأیید مجدد قابلیت فناوری‌های اطلاعات و ارتباطات به عنوان ابزاری قدرتمند جهت تقویت توسعه اجتماعی-اقتصادی و مشارکت در تحقق اهداف توسعه مورد وفاق بین‌المللی از جمله اهدافی که در اعلامیه توسعه هزاره سازمان ملل متحد درج گردیده است:

۱. قدردانی خود را از دولت سوئیس درخصوص موارد زیر بیان می‌دارد: میزبانی مرحله اول اجلاس سران درباره جامعه اطلاعاتی در ژنو مورخ ۱۰ تا ۱۲ دسامبر ۲۰۰۳، پشتیبانی و مقدماتی که در اختیار اجلاس قرار دادند؛

۲. ضمن تصدیق تلاش‌های دولت تونس درخصوص میزبانی مرحله دوم اجلاس سران که مورخ ۱۶ تا ۱۸ نوامبر ۲۰۰۵ در این کشور برگزار خواهد شد، قدردانی خود را تکرار می‌نماید؛

۳. به یادداشت {نقطه نظرها} دبیرکل درمورد گزارش ارسالی دبیرکل اتحادیه بین‌المللی مخابرات درباره مرحله اول اجلاس سران درباره جامعه اطلاعاتی و پیشرفت در آمادگی جهت

1. World Summit on the Information Society

برگزاری مرحله دوم این اجلاس توجه می‌نماید؛

۴. ضمن تأیید اعلامیه اصول و طرح اقدام {ژنو}، مصوبه اجلاس سران در تاریخ ۱۲ دسامبر ۲۰۰۳، در این رابطه:

- از وضعیت پیشرفت جدی {شناسایی شده} در هر دو سند {فوق} استقبال می‌نماید؛
- مشارکت پیوسته کشورهای در حال توسعه و توسعه‌یافته را جهت تعیین اینکه فناوری اطلاعات چگونه می‌تواند در حصول {تحقق} اهداف توسعه مورد وفاق بین‌المللی سهم بیشتری داشته باشد. از جمله اهداف مندرج در اعلامیه هزاره سازمان ملل متحد؛
- بر اهمیت اجرای مؤثر و بموقع طرح اقدام تأکید می‌نماید.

۵. از همکاری دولت‌های عضو، نهادهای مرتبط در سازمان ملل، از جمله گروه اقدام فناوری‌های اطلاعات و ارتباطات، و سایر سازمان‌های بین‌دولتی، سازمان‌های غیردولتی، جامعه مدنی و بخش خصوصی در کسب موفقیت اجلاس سران در ژنو استقبال می‌نماید؛

۶. از دولت‌های عضو، نهادهای مرتبط در سازمان ملل متحد از جمله گروه اقدام فناوری‌های اطلاعات و ارتباطات و دیگر سازمان‌های بین‌دولتی، سازمان‌های غیردولتی، جامعه مدنی و بخش خصوصی، درخواست می‌نماید تا خروجی اجلاس سران در ژنو را جهت فرایند مقدماتی مرحله دوم اجلاس {در تونس} اجرا نمایند و نیز این درخواست را از خود اجلاس سران و به‌منظور تضمین موفقیت کامل خود {در اجلاس تونس} دارد؛

۷. به نتایج تصمیمات اولین نشست کمیته مقدماتی در باب ساختار و خروجی مرحله دوم اجلاس سران توجه می‌نماید. این نشست در تاریخ ۲۴ تا ۲۶ ژوئن ۲۰۰۴ در شهر حمامه کشور تونس برگزار گردید؛

۸. از تشکیل گروه کاری درباره حکمرانی اینترنت و تشکیل گروه اقدام درباره سازوکار تأمین مالی، مطابق تصمیمات اتخاذ شده در مرحله اولی اجلاس سران، استقبال می‌کند؛

۹. از کشورها دعوت می‌نماید تا حد ممکن نمایندگان از بالاترین سطح سیاسی خود در مرحله دوم اجلاس سران سال ۲۰۰۵ در تونس داشته باشند؛

۱۰. فراخوان خود را در سطح جامعه بین‌الملل جهت مشارکت داوطلبانه در صندوق ویژه {مالی}



تکرار می‌نماید. این صندوق توسط اتحادیه بین‌المللی مخابرات به‌منظور پشتیبانی از آماده‌سازی و برگزاری اجلاس سران تأسیس گردید؛

۱۱. از دبیرکل اتحادیه بین‌المللی مخابرات دعوت می‌نماید گزارش اجلاس سران درباره جامعه اطلاعاتی را به محض {آماده شدن} برای مجمع عمومی ارسال نماید.

نشست عمومی ۷۵- مورخ ۲۲ دسامبر ۲۰۰۴

بند نه: قطعنامه اجلاس سران در مورد جامعه اطلاعاتی سال ۲۰۰۶

ترجمه سند



مجمع عمومی
کمیته دوم

تاریخ انتشار: ۲۷ آوریل ۲۰۰۶

شماره قطعنامه: A/RES/60/252

توزیع: عمومی

اجلاس شصتم.

دستور کار ۴۹

قطعنامه مصوب مجمع عمومی مورخ ۲۷ مارس ۲۰۰۶ بدون ارجاع به کمیته اصلی A/60/L.50 and Add.1

اجلاس سران درباره جامعه اطلاعاتی^۱

مجمع عمومی

با یادآوری قطعنامه‌های خود (به شماره‌های { ۵۶/۱۸۳ مورخ ۲۱ دسامبر ۲۰۰۱، ۵۷/۲۳۸ مورخ ۲۰ دسامبر ۲۰۰۲، ۵۷/۲۷۰B مورخ ۲۳ ژوئن ۲۰۰۳ و ۵۹/۲۲۰ مورخ ۲۲ دسامبر ۲۰۰۴؛ با یادآوری اعلامیه اصول و طرح اقدام (ژنو) که در مرحله اول اجلاس سران درباره جامعه اطلاعاتی در ژنو مورخ ۱۰ تا ۱۲ دسامبر ۲۰۰۳ تصویب و توسط مجمع عمومی تأیید گردید؛ با یادآوری بیشتر خروجی اجلاس سران در سال ۲۰۰۵ ضمن به رسمیت شناختن اینکه اجرا و پیگیری اجلاس سران:

باید بخش جداناپذیری از پیگیری‌های یکپارچه اجلاس‌ها و کنفرانس‌های تخصصی سازمان‌های ملل متحد در حوزه‌های اقتصادی، اجتماعی و حوزه‌های مرتبط باشد و باید در حصول اهداف توسعه مورد توافق بین‌المللی از جمله اهداف هزاره توسعه سهیم باشد و نباید مستلزم ایجاد هیچ نهاد عملیاتی جدیدی باشد؛

ضمن اذعان به نیاز ضروری جهت رفع شکاف دیجیتالی و مساعدت به کشورهای در حال توسعه با تأکید بر اهمیت همکاری اجلاس در ایجاد جامعه اطلاعاتی مردم‌محور، فراگیر و توسعه مدار از جمله کشورهای کمتر توسعه یافته، کشورهای در حال توسعه محصور در خشکی و جزایر کوچک،

1. World Summit on the Information Society

و {نیاز ضروری به} بهره‌مندی کامل کشورهایی با اقتصاد در حال گذار از قابلیت‌های فناوری اطلاعات و ارتباطات؛

با تأیید مجدد قابلیت فناوری‌های اطلاعات و ارتباطات به‌عنوان ابزاری قدرتمند جهت تقویت توسعه اجتماعی- اقتصادی و مشارکت در تحقق اهداف توسعه مورد وفاق بین‌المللی از جمله اهداف توسعه هزاره برای ارتقای فرصت‌های دیجیتالی برای تمامی مردم به‌منظور کمک به رفع شکاف‌های دیجیتالی؛

با اذعان توأم با قدردانی از نقشی که اتحادیه بین‌المللی مخابرات در سازماندهی هر دو مرحله اجلاس سران ایفا نمود:

۱. قدردانی خود را از دولت تونس جهت میزبانی مرحله دوم اجلاس سران درباره جامعه اطلاعاتی مورخ ۱۶ تا ۱۸ نوامبر ۲۰۰۵ را بیان می‌دارد؛

۲. به یادداشت {نقطه نظرهای} دبیرکل درمورد گزارش ارسالی دبیرکل اتحادیه بین‌المللی مخابرات درباره مرحله دوم اجلاس سران توجه می‌نماید؛

۳. تعهدات و دستور کار تونس برای جامعه اطلاعاتی مصوب مرحله دوم اجلاس سران را تأیید می‌نماید؛

۴. از همکاری دولت‌های عضو، نهادهای مرتبط در سازمان ملل و سایر سازمان‌های بین دولتی، سازمان‌های غیردولتی، جامعه مدنی و بخش خصوصی در کسب موفقیت اجلاس سران در تونس استقبال می‌نماید؛

۵. همچنین از وضعیت پیشرفت جدی {شناسایی شده} در خروجی‌های اجلاس سران درباره جامعه اطلاعاتی در هر دو فاز {مرحله} ژنو و تونس استقبال می‌نماید؛

۶. از پیشرفت شناسایی شده اجلاس سران در پیشبرد رویکرد چنددلی نفعی در ایجاد جامعه اطلاعاتی مردم‌محور، فراگیر و توسعه محور استقبال مضاعفی می‌نماید و بر توان دولت‌ها در ایفای نقشی مهم در این پیشرفت‌ها اذعان دارد؛

۷. از صندوق همکاری دیجیتال که در ژنو به‌عنوان سازوکار مالی نوآورانه ایجاد شد استقبال می‌نماید، این صندوق با ماهیت داوطلبانه و آزاد برای ذی‌نفعان علاقه‌مند، هدف زیر را دنبال می‌نماید: تبدیل شکاف‌های دیجیتال به فرصت برای دنیای در حال توسعه از طریق تمرکز اساسی

روی نیازهای ویژه و مبرم در سطح ناحیه‌ای و جستجوی منابع داوطلبانه جهت همکاری مالی؛
 ۸. تصریح می‌نماید که تمامی سازمان‌های مربوط و ذی‌نفعان، متناسب با نقش‌های خود، در فرایند همکاری‌های ارتقای یافته که توسط دبیرکل شروع گردید، تعامل خواهند داشت. همانگونه که این {موضوع} در بند ۷۱ دستورکار تونس ذکر شد؛

۹. از دبیرکل دعوت می‌نماید تا مطابق با تصمیمات اتخاذ شده در اجلاس سران تونس، در یک فرایند آزاد و فراگیر، {شکل‌گیری} مجمع جدیدی جهت گفتگو {درباره} خط‌مشی چندذی‌نفعی فراخوانده شده در مجمع حکمرانی اینترنتی را هماهنگ نماید؛

۱۰. از اهمیتی که اجلاس سران، بر اساس آنچه در دستور کار تونس منعکس گردیده، به اجرای چندذی‌نفعی در سطح بین‌المللی اختصاص داده است، استقبال می‌نماید که {اجرای چندذی‌نفعی}، عندالاقضاء، با در نظر گرفتن موضوعات و خطوط اقدام {مندرج در} طرح اقدام ژنو، باید توسط سازمان‌های {ذی‌ربط} سازمان ملل متحد سازماندهی، تعدیل یا تسهیل گردد.
 ۱۱. از دولت‌های عضو، نهادهای مرتبط در سازمان ملل متحد و دیگر سازمان‌های بین‌دولتی و نیز سازمان‌های غیردولتی، جامعه مدنی و بخش خصوصی، درخواست می‌نماید تا در صورت مقتضی، در کنار سایر اقدامات آغازگر {خود}، همکاری فعالانه‌ای را جهت اجرا و پیگیری خروجی‌های اجلاس سران در ژنو و تونس داشته باشند؛

۱۲. از شورای اقتصادی و اجتماعی دعوت می‌نماید تا گستره سیستم پیگیری خروجی‌های اجلاس سران در ژنو و تونس را اداره نماید و در خاتمه از شورا درخواست می‌نماید تا وظایف، دستورکار و ترکیب کمیسیون علم و فناوری برای توسعه را در اجلاس محتوایی خود در سال ۲۰۰۶ بررسی نماید و در این بررسی، از جمله تقویت کمیسیون را با در نظر گرفتن رویکرد چندذی‌نفعی، مورد ملاحظه قرار دهد؛

۱۳. تصمیم می‌گیرد که ۱۷ تاریخ می را به‌عنوان روز جهانی جامعه اطلاعاتی با هدف زیر اعلام نماید: کمک به ارتقای سطح آگاهی از اینکه استفاده از اینترنت و سایر فناوری‌های اطلاعات و ارتباطات می‌تواند در {حوزه‌های} اجتماعی و اقتصادی وارد شود و راهی است جهت رفع شکاف دیجیتالی؛

۱۴. همچنین درخصوص انجام بازنگری کلی جهت اجرای نتایج اجلاس سران در سال ۲۰۱۵ تصمیم می‌گیرند. از دبیرکل درخواست می‌نماید تا از طریق شورای شورای اقتصادی اجتماعی گزارشی را تا جولای ۲۰۰۶ درباره موضوع زیر به مجمع عمومی ارائه نماید: شرایط و نحوه هماهنگی درون سازمانی درباره اجرای خروجی‌های اجلاس سران از جمله توصیه‌ها و پیشنهادهای مربوط به فرایند پیگیری جهت ملاحظه در اجلاس محتوایی شورا.

نشست عمومی ۷۴ مورخ ۲۷ مارس ۲۰۰۶

جدول ۴: مشخصات قطعنامه‌های اجلاس سران در مورد جامعه اطلاعاتی سال ۲۰۰۱ تا ۲۰۰۶

سال صدور قطعنامه	تاریخ انتشار قطعنامه	شماره قطعنامه	شماره اجلاس	شماره دستورکار	شماره گزارش	شماره پیش‌نویس قطعنامه	نماینده گروه ۷۷ جهت ارائه قطعنامه
۲۰۰۱	۳۱ ژانویه ۲۰۰۲	A/RES/183/56	۵۶	۹۵	A/56/558/Add.3	A/C.56/2/L.3	تونس
۲۰۰۲	۳۱ ژانویه ۲۰۰۳	A/RES/238/57	۵۷	۸۴	A/57/529/Add.3	A/C.57/2/L.7	تونس و سوییس
۲۰۰۳	۱۱ فوریه ۲۰۰۵	A/RES/220/59	۵۹	۴۴	A/59/480	A/C.59/2/L.18	تونس و سوییس
۲۰۰۴	۲۷ آوریل ۲۰۰۶	A/RES/252/60	۶۰	۴۹	A/60/L.50 and Add.1	A/60/L.50	چین، آفریقای جنوبی، سوییس، تونس و ترکیه

مجمع عمومی

مبحث سه: کمیته سوم مجمع عمومی

بندیک: قطعنامه مبارزه با سوءاستفاده مجرمانه از فناوری‌های اطلاعاتی ۲۰۰۱

ترجمه سند



مجمع عمومی
کمیته سوم

تاریخ انتشار: ۲۳ ژانویه ۲۰۰۲

شماره قطعنامه: A/RES/56/121

توزیع: عمومی

اجلاس پنجاه و ششم

دستور کار ۱۱۰

قطعنامه مصوب مجمع عمومی بر اساس گزارش کمیته سوم A/56/574

مبارزه با سوءاستفاده مجرمانه از فناوری‌های اطلاعاتی^۱

مجمع عمومی:

با یادآوری اعلامیه هزاره ملل متحد^۲ که در آن دولت‌های عضو تصمیم گرفتند تا تضمین نمایند که مزایای فناوری‌های جدید، به‌ویژه فناوری‌های اطلاعات و ارتباطات، مطابق با توصیه‌های موجود در اعلامیه وزیران بخش سطح بالای اجلاس اصلی سال ۲۰۰۰ شورای اقتصادی و اجتماعی^۳، در دسترس همگان قرار گیرد و {بایادآوری} قطعنامه خود {به شماره} ۵۵/۶۳ مورخ ۴ دسامبر ۲۰۰۰ که در آن قطعنامه از کشورهای عضو دعوت شده تا اقداماتی برای مبارزه با سوءاستفاده مجرمانه از فناوری‌های اطلاعات را مورد نظر قرار دهند؛

با به رسمیت شناختن اینکه جریان آزاد اطلاعات می‌تواند توسعه اقتصادی و اجتماعی، آموزش و حکمرانی دموکراتیک را ارتقای دهد؛

باتوجه به پیشرفت‌های مهم در توسعه و کاربرد تکنولوژی‌های اطلاعات و ابزار مخابراتی؛
با ابراز نگرانی از پیشرفت‌های فنی که امکانات جدیدی را برای فعالیت‌های مجرمانه به‌ویژه

1. Combating the criminal misuse of information technologies

2. See resolution +2/55

3. See Official Records of the General Assembly, Fifty-fifth Session, Supplement No.3 (A/3/55/Rev.1), chap. III, para. 17.

سوءاستفاده مجرمانه از فناوری‌های اطلاعات را ایجاد کرده‌اند؛
 باتوجه‌به اینکه وابستگی به فناوری‌های اطلاعات، هر چند ممکن است میزان این وابستگی از
 دولتی به دولت دیگر متفاوت باشد، موجب افزایش چشمگیر همکاری و هماهنگی جهانی شده
 است، به همین دلیل سوءاستفاده مجرمانه از فناوری اطلاعات ممکن است تأثیر عمیقی بر کلیه
 کشورها داشته باشد؛

با به رسمیت شناختن اینکه شکاف‌های موجود در خصوص دسترسی و استفاده از فناوری‌های
 اطلاعات از سوی کشورها می‌تواند اثربخشی همکاری‌های بین‌المللی در مبارزه با سوءاستفاده
 مجرمانه از فناوری اطلاعات را کاهش دهد، و همچنین با به رسمیت شناختن نیاز به تسهیل
 انتقال فناوری اطلاعات، به‌ویژه به کشورهای در حال توسعه؛

باتوجه‌به ضرورت پیشگیری از سوءاستفاده مجرمانه از فناوری‌های اطلاعات؛
 با به رسمیت شناختن نیاز به همکاری بین دولت‌ها و بخش خصوصی جهت مبارزه علیه
 سوءاستفاده مجرمانه از فناوری اطلاعات؛

با تأکید بر نیاز به همکاری و هماهنگی بیشتر میان دولت‌ها در زمینه مبارزه با سوءاستفاده
 مجرمانه از فناوری‌های اطلاعات و در این چارچوب، با تأکید بر نقشی که سازمان ملل و سایر
 سازمان‌های منطقه‌ای و بین‌المللی می‌توانند ایفا نمایند؛

با استقبال از عملکرد دهمین کنگره سازمان ملل در خصوص پیشگیری از جرم و رفتار با مجرمان؛
 با به رسمیت شناختن توأم با قدردانی از عملکرد کمیسیون پیشگیری از جرم و عدالت
 کیفری در نهمین و دهمین اجلاس خود و متعاقب آن آماده‌سازی برنامه اقدام علیه جرائم مرتبط
 با کامپیوتر و فناوری برتر که در کنار موارد دیگر، به رسمیت شناختن نیاز به قانون اجرایی مؤثر،
 نیاز به حفظ حمایت‌های مؤثر از حریم شخصی و سایر حقوق اساسی مرتبط و نیز نیاز به در نظر
 گرفتن عملکرد جاری سایر مجامع؛

باتوجه‌به عملکرد سازمان‌های منطقه‌ای و بین‌المللی در خصوص مقابله با جرائم مرتبط
 با فناوری‌های برتر، از جمله عملکرد شورای اروپا گسترش کنوانسیون جرائم سایبری^۱ و نیز

عملکرد آن سازمان‌ها {سازمان‌های منطقه‌ای و بین‌المللی} در ارتقای و ترویج گفتگو بین دولت و بخش خصوصی در خصوص ایمنی و اعتماد در فضای سایبر:

۱. از کشورهای عضو دعوت می‌کند هنگام تدوین قانون ملی، سیاستگذاری یا اتخاذ اقداماتی جهت مقابله با سوءاستفاده مجرمانه از فناوری‌های اطلاعات، عملکرد و دستاوردهای کمیسیون پیشگیری از جرم و عدالت کیفری و سایر سازمان‌های منطقه‌ای و بین‌المللی را در صورتی که مناسب برای خود تشخیص دهند، در نظر بگیرند؛

۲. به ارزش و اهمیت مجموعه اقدامات که در قطعنامه خود {به شماره ۵۵/۶۳} مندرج است، توجه می‌نماید، و دوباره از کشورهای عضو جهت در نظر گرفتن آن‌ها {مجموعه اقدامات} در تلاش‌های خود در خصوص مقابله با سوءاستفاده مجرمانه از فناوری‌های اطلاعاتی، دعوت می‌کند؛

۳. تصمیم می‌گیرد تا بررسی موضوع را تا اتمام زمان پیش‌بینی شده برای فعالیت در برنامه اقدام علیه جرائم مرتبط با رایانه و فناوری برتر کمیسیون پیشگیری جرم و عدالت کیفری دیده شده به تعویق اندازد.

نشست عمومی ۸۸ (۱۹ دسامبر ۲۰۰۱)

بند دو: قطعنامه حق حریم خصوصی در عصر دیجیتال سال ۲۰۱۳

ترجمه سند



مجمع عمومی
کمیته دوم

تاریخ انتشار: ۲۱ ژانویه ۲۰۱۴

شماره قطعنامه: A/RES/68/167

توزیع: عمومی

اجلاس شصت و هشتم

دستور کار ۶۹

قطعنامه مصوب مجموع عمومی مورخ ۱۸ دسامبر ۲۰۱۳ بر اساس گزارش کمیته سوم A/68/456/Add.2

حق حریم خصوصی در عصر دیجیتال^۱

مجمع عمومی:

با تأیید دوباره اهداف و اصول منشور ملل متحد؛

همچنین با تأیید دوباره حقوق بشر و آزادیهای اساسی مورد احترام در اعلامیه جهانی حقوق

بشر و معاهدات بین‌المللی حقوق بشری مربوط، از جمله میثاق حقوق مدنی و سیاسی و میثاق

بین‌المللی حقوق اقتصادی، اجتماعی و فرهنگی؛

با تأیید دوباره اعلامیه وین و برنامه اقدام؛

باتوجه به اینکه حرکت سریع توسعه فنی، افراد را در سراسر جهان قادر می‌سازد تا از فناوری‌های

جدید ارتباطی و اطلاعاتی استفاده کنند و در عین حال ظرفیت حکومت‌ها، شرکت‌ها و اشخاص

برای نظارت، اختلال و جمع‌آوری اطلاعات را افزایش می‌دهد که این امر می‌تواند حقوق بشر،

مخصوصاً حق حریم خصوصی، را نقض یا مورد تجاوز قرار دهد، موضوعی که در ماده ۱۲ اعلامیه

جهانی حقوق بشر و ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی آمده است و بنابراین این

موضوع یک نگرانی فزاینده است؛

با تأیید دوباره حق حریم خصوصی انسان، که طبق آن، خود فرد، حریم خصوصی، خانواده، منزل

1 . The right to privacy in the digital age

و مکاتبات، هیچکس نباید مورد مداخله غیرقانونی یا خودسرانه قرار گیرد و حق حفاظت قانون {مورد حمایت قانون بودن} در مقابل این مداخلات وجود داشته باشد و با به رسمیت شناختن اینکه اعمال حق حریم خصوصی برای تحقق حق آزادی بیان و داشتن عقیده ای مصون از مداخلات امری مهم است و حق آزادی مجامع و انجمن‌ها یکی از ارکان یک جامعه دموکراتیک است؛ با تأکید بر اهمیت احترام کامل به آزادی در جستجو، دریافت و انتقال اطلاعات، از جمله اهمیت اساسی دسترسی به اطلاعات و مشارکت دموکراتیک؛

با استقبال از گزارش گزارشگر ویژه درباره ارتقای و حفاظت از حق آزادی عقیده و بیان درخصوص {موارد زیر} که در اجلاس بیست‌وسوم شورای حقوق بشر {به آن شورا} ارائه گردید: ✓ نظارت دولت بر ارتباطات در راستای رعایت حقوق بشر مرتبط با حق حریم خصوصی با تأکید بر اینکه نظارت یا رهگیری غیرقانونی ارتباطات و نیز جمع‌آوری داده‌ها به شکل غیرقانونی یا خودسرانه، به‌عنوان اقدامات مداخله‌گرایانه، حقوق حریم خصوصی و آزادی بیان را نقض نماید و ممکن است با اصول جامعه دموکراتیک تناقض داشته باشد؛

باتوجه به این موضوع که نگرانی‌ها درباره امنیت عمومی، ممکن است گردآوری و حفاظت از اطلاعات حساس معین را توجیه نماید، دولت‌ها باید تضمین نمایند که تعهدات خود تحت حقوق بین‌المللی بشر را کاملاً رعایت نمایند؛

با نگرانی عمیق از امکان تأثیر منفی نظارت و یا رهگیری ارتباطات، از جمله نظارت و یا رهگیری ارتباطات فراسرزمینی، در به‌کارگیری و بهره‌مندی از حقوق بشر، و نیز جمع‌آوری داده‌های شخصی به‌ویژه در مقیاس وسیع، با تأیید مجدد اینکه دولت‌ها باید تضمین نمایند که هر اقدامی را که جهت مبارزه با تروریسم اتخاذ می‌نمایند باید مطابق با تعهدات خود تحت حقوق بین‌الملل باشد به‌ویژه حقوق بشر، حقوق پناهندگان و حقوق بشردوستانه:

۱. مجدداً حق حریم خصوصی را تأیید می‌نماید مطابق {با این موضوع} که حریم خصوصی، خانوادگی، منزل یا مکاتبات هیچ کس نباید دستخوش مداخله خودسرانه یا غیرقانونی قرار گیرد، و {همچنین مجدداً} حقوق مربوط به حفاظت قانون (مورد حمایت قانون بودن) در مقابله با چنین مداخله‌ای را {تأیید می‌نماید} وفق حقوق مصرحه در ماده ۱۲ اعلامیه جهانی حقوق

بشر و ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی؛
۲. ماهیت جهانی و آزاد اینترنت و پیشرفت سریع فناوری اطلاعات و ارتباطات به‌عنوان نیروی پیشران جهت تسریع پیشرفت به سوی اشکال مختلف توسعه را به رسمیت می‌شناسد؛
۳. تأیید می‌کند که همان حقوقی که مردم در فضای غیربرخط دارند باید در فضای برخط نیز محافظت گردد از جمله حقوق مربوط به حریم خصوصی؛
۴. از تمامی دولت‌ها درخواست می‌نماید:
أ. به حقوق حریم خصوصی، از جمله در زمینه ارتباطات دیجیتالی، احترام بگذارند و از آن حفاظت نمایند.

ب. اقداماتی را جهت پایان دادن به نقض حقوق حریم خصوصی و ایجاد شرایطی برای پیشگیری از چنین نقض‌هایی اتخاذ نمایند از جمله از طریق حصول اطمینان از تطابق قانون ملی مربوط با تعهدات خود زیر قوانین بین‌المللی حقوق بشر؛
ج. رویکردها، رویه‌ها و قوانین خود را در ارتباط با موضوعات زیر بررسی و مورد بازنگری قرار دهند:

✓ نظارت، رهگیری و جمع‌آوری { داده‌ها } ارتباطات از جمله نظارت همگانی (نظارت جمعی)؛

✓ مداخله؛

✓ جمع‌آوری داده‌های شخصی؛

{ و این بررسی }، با نگاهی بر اصرار روی حق حریم خصوصی، از طریق حصول اطمینان از اجرای کامل و اثر بخش تمامی تعهدات زیر قوانین بین‌المللی حقوق بشر { انجام گردد }
د. سازوکارهایی که می‌توانند متضمن شفافیت و عندالاقضاء پاسخگویی دولت‌ها درباره نظارت و رهگیری ارتباطات و جمع‌آوری داده‌های شخصی باشند را ایجاد نمایند و یا { در صورت وجود چنین سازوکارهایی } آن‌ها را حفظ کنند؛

۵. از کمیساری عالی حقوق بشر سازمان ملل متحد درخواست می‌نماید تا گزارشی را از نظرها و توصیه‌های دولت‌های عضو در بیست‌وهفتمین اجلاس شورای حقوق بشر و شصت‌ونهمین اجلاس مجمع عمومی را درباره { موضوع زیر } ارائه نماید: حفاظت و ارتقای حق حریم



خصوصی در چارچوب نظارت. و همچنین حفاظت و ارتقای این حقوق در رهگیری ارتباطات داخلی و فراسرزمینی و جمع آوری داده‌های شخصی به‌ویژه در مقیاس وسیع؛

۶. تصمیم می‌گیرد تا در اجلاس شصت‌ونهم خود، درخواست‌ها زیر را بررسی کند:

- بخش فرعی با عنوان «مطالبات حقوق بشری از جمله رویکردهای دیگر برای بهبود بهره‌مندی مؤثر حقوق بشر و آزادی‌های اساسی»؛

- بخشی تحت عنوان «ارتقای و حفاظت از حقوق بشر».

نشست عمومی ۷۰ - مورخ ۱۸ دسامبر ۲۰۱۳

بند سه: قطعنامه حق حریم خصوصی در عصر دیجیتال سال ۲۰۱۴

ترجمه سند



مجمع عمومی
کمیته سوم

تاریخ انتشار: ۱۰ فوریه ۲۰۱۵

شماره قطعنامه: A/RES/69/166

توزیع: عمومی

اجلاس شصت و هشتم

دستور کار ۶۹

قطعنامه مصوب مجموع عمومی مورخ ۱۸ دسامبر ۲۰۱۴ بر اساس گزارش کمیته سوم A/69/488/Add.2

حق حریم خصوصی در عصر دیجیتال

مجمع عمومی:

با تأیید دوباره اهداف و اصول منشور ملل متحد؛

همچنین با تأیید دوباره حقوق بشر و آزادیهای اساسی مورد احترام در اعلامیه جهانی حقوق بشر و معاهدات بین‌المللی حقوق بشری مربوط، از جمله میثاق حقوق مدنی و سیاسی و میثاق بین‌المللی حقوق اقتصادی، اجتماعی و فرهنگی؛

با تأیید دوباره اعلامیه وین و برنامه اقدام؛

با یادآوری قطعنامه خود {به شماره} ۶۸/۱۶۷ مورخ ۱۸ دسامبر ۲۰۱۳ درباره حق حریم

خصوصی در عصر دیجیتال؛

با استقبال از تصیب قطعنامه شورای حقوق بشر {به شماره} ۲۶/۱۳ مورخ ۲۶ ژوئن ۲۰۱۴

درباره ارتقای، حفاظت و بهره‌مندی از حقوق بشر در اینترنت؛

با استقبال از عملکرد دفتر کمیساریای عالی ملل متحد برای حقوق بشر در زمینه حق حریم

خصوصی در عصر دیجیتال و توجه توأم با علاقه به گزارش این دفتر در موضوع حاضر، و با یادآوری جلسه مباحثه و مناظره که در مورد حق حریم خصوصی در عصر دیجیتال در خلال

بیست و هفتمین جلسه شورای حقوق بشر برگزار شد؛

باتوجه به گزارش گزارشگر ویژه شورای حقوق بشر درباره ارتقای و حفاظت از حقوق بشر و آزادی‌های اساسی در کنار مقابله با تروریسم و گزارش‌های گزارشگر ویژه شورای حقوق بشر درباره ارتقای و حفاظت از حق آزادی بیان و اندیشه؛

با توجه توأم با قدردانی به نظر عمومی شماره ۱۶ کمیته حقوق بشر در خصوص حق احترام به حریم خصوصی، خانواده، منزل و مکاتبات و حفظ حیثیت و حرمت افراد، در عین توجه به جهش‌های فناورانه گسترده ای که از زمان تصویب آن اتفاق افتاده است؛

با به رسمیت شناختن نیاز به بحث و تجزیه و تحلیل بیشتر بر اساس حقوق بشر بین‌المللی، موضوعات مرتبط با ارتقا و حفاظت از حریم خصوصی در عصر دیجیتال، پادمان‌های رویه‌ای نظارت و راه‌حل‌های مؤثر محلی، تأثیر نظارت بر حق حریم خصوصی و سایر حقوق بشری و همچنین نیاز به بررسی اصول غیرخودسرانگی و قانونی و مرتبط بودن ضرورت و تناسب ارزیابی‌ها در رابطه با شیوه‌های نظارت؛

باتوجه به برگزاری نشست جهانی چند ذی نفعی در زمینه آینده حکمرانی اینترنت (در نت موندیال)، در سائوپائولوی برزیل در آوریل ۲۰۱۴، و با به رسمیت شناختن اینکه مقابله مؤثر با چالش‌های مرتبط با حق حریم خصوصی در چارچوب فناوری ارتباطاتی مدرن، نیازمند یک مشارکت، مداومت و تعهد چندذی‌نفعی است؛

باتوجه به اینکه حرکت سریع توسعه فنی، افراد را در سراسر جهان قادر می‌سازد تا از فناوری‌های جدید ارتباطی و اطلاعاتی استفاده کنند و در عین حال ظرفیت حکومت‌ها، شرکت‌ها و اشخاص برای نظارت، اختلال و جمع‌آوری اطلاعات را افزایش می‌دهد که این امر می‌تواند حقوق بشر، مخصوصاً حق حریم خصوصی را نقض یا مورد تجاوز قرار دهد، موضوعی که در ماده ۱۲ اعلامیه جهانی حقوق بشر و ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی آمده است و بنابراین این موضوع یک نگرانی فزاینده است؛

با تأیید دوباره حق حریم خصوصی انسان، که طبق آن، خود فرد، حریم خصوصی، خانواده، منزل و مکاتبات، هیچکس نباید مورد مداخله غیرقانونی یا خودسرانه قرار گیرد و حق حفاظت قانون {مورد حمایت قانون بودن} در مقابل این مداخلات وجود داشته باشد و با به به رسمیت

شناختن اینکه اعمال حق حریم خصوصی برای تحقق حق آزادی بیان و داشتن عقیده‌ای مصون از مداخلات، امری مهم است و حق آزادی مجامع و انجمن‌ها یکی از ارکان یک جامعه دموکراتیک است؛

با تأکید بر اهمیت احترام کامل به آزادی در جستجو، دریافت و انتقال اطلاعات، از جمله اهمیت اساسی دسترسی به اطلاعات و مشارکت دموکراتیک؛

باتوجه به اینکه، باوجود مزایایی که ابرداها می‌توانند فراهم کنند، انواع خاصی از ابرداها، زمانی که جمع می‌شوند، می‌توانند اطلاعات شخصی افراد را فاش کنند و همچنین می‌توانند رفتار افراد، روابط اجتماعی، اولویت‌های خصوصی و هویت فرد را ادراک کنند؛

با تأکید بر اینکه نظارت یا رهگیری غیرقانونی ارتباطات و نیز جمع‌آوری داده‌ها به شکل غیرقانونی یا خودسرانه (اختیاری)، به‌عنوان اقدامات مداخله‌گرایانه، حقوق حریم خصوصی را نقض می‌کند، می‌تواند با حقوق آزادی بیان تداخل یابد و ممکن است با اصول جامعه دموکراتیک تناقض داشته باشد از جمله وقتی که {این اقدامات} در مقیاس وسیعی به‌کار گرفته شود.

با توجه ویژه بر اینکه نظارت بر ارتباطات دیجیتال باید:

- مطابق با تعهدات بین‌المللی حقوق بشری باشد،

- مبتنی بر چارچوب قانونی انجام گیرد که {این چارچوب قانونی} لزوماً باید قابل دسترسی

برای عموم، شفاف، دقیق، جامع و غیرتبعیض‌آمیز باشد؛

و {باتوجه به اینکه} هیچ مداخله‌ای نباید به شکل خودسرانه و غیرقانونی در حقوق حریم خصوصی انجام گیرد، با در نظر داشتن آنچه که در جهت تحقق اهداف مشروع، قابل قبول است و با یادآوری مجدد اینکه دولت‌های عضو که در میثاق بین‌المللی مدنی و سیاسی باید گام‌های لازم جهت تصویب قوانین یا سایر اقدامات لازم برای تأمین حقوق مصرح در میثاق را اتخاذ نمایند.

با تأکید بر اینکه دولت‌ها باید به تعهدات بین‌المللی حقوق بشری در رابطه با حق حریم خصوصی احترام بگذارند:

✓ هنگامی که آن‌ها ارتباطات دیجیتالی اشخاص را رصد می‌کنند؛

✓ هنگام گردآوری داده‌های شخصی؛

✓ هنگام نیاز به افشای داده‌های شخصی از اشخاص ثالث از جمله داده‌های مربوط به شرکت‌های

خصوصی

با یادآوری اینکه مؤسسات تجاری در احترام به حقوق بشر، قوانین حاکم، اصول و استانداردهای بین‌المللی مسئول می‌باشند؛

در راستای احترام به حقوق بشر وفق اصول راهنما درباره مسائل و حقوق بشر واقف باشند؛ به چارچوب سند سازمان ملل تحت عنوان «حفاظت، احترام و اصلاح و جبران» عامل باشند. با نگرانی عمیق از امکان تأثیر منفی نظارت و یا رهگیری ارتباطات، از جمله نظارت و یا رهگیری ارتباطات فراسرزمینی، در به‌کارگیری و بهره‌مندی از حقوق بشر، و نیز جمع‌آوری داده‌های شخصی به‌ویژه در مقیاس وسیع؛

ضمن توجه توأم با نگرانی عمیق {در خصوص} اینکه در بسیاری از کشورها، اشخاص و سازمان‌های درگیر در {موضوع} ارتقای و دفاع از حقوق بشر و آزادی‌های بنیادین {اساسی} در نتیجه فعالیت‌های خود، مکرراً با تهدیدات و آزار و اذیت، رنج از ناامنی و نیز مداخله خودسرانه و غیرقانونی در خصوص حقوق حریم خصوصی خود روبه‌رو هستند؛

باتوجه به این موضوع که نگرانی‌ها درباره امنیت عمومی، ممکن است گردآوری و حفاظت از اطلاعات حساس معین را توجیه نماید، دولت‌ها باید تضمین نمایند که تعهدات خود تحت حقوق بین‌المللی بشر را کاملاً رعایت نمایند؛

در ارتباط با {موضوع قبل} ضمن توجه بیشتر به اینکه پیشگیری و سرکوب تروریسم یک منفعت عمومی با {درجه} اهمیت زیاد می‌باشد، در عین حال مجدداً تأیید می‌نماییم که دولت‌ها باید تضمین نمایند که هر اقدامی را جهت مبارزه با تروریسم اتخاذ می‌نمایند باید مطابق با تعهدات خود تحت حقوق بین‌الملل باشد به‌ویژه حقوق بشر، حقوق پناهندگان و حقوق بشر دوستانه.

۷. مجدداً حق حریم خصوصی را تأیید می‌نماید مطابق {با این موضوع} که حریم خصوصی خانوادگی، منزل یا مکاتبات هیچکس نباید دستخوش مداخله خودسرانه یا غیرقانونی قرار گیرد، و {همچنین مجدداً} حقوق مربوط به حفاظت قانون (مورد حمایت قانون بودن) در مقابله با چنین مداخله‌ای را {تأیید می‌نماید} وفق حقوق مصرحه در ماده ۱۲ اعلامیه جهانی حقوق

بشر و ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی؛

۸. ماهیت جهانی و آزاد اینترنت به‌عنوان نیروی پیشران جهت تسریع پیشرفت به سوی آشکال مختلف توسعه از جمله حصول اهداف توسعه پایدار را به رسمیت می‌شناسد؛

۹. تأیید می‌کند که همان حقوقی که مردم در فضای غیربرخط دارند باید در فضای برخط نیز محافظت گردد از جمله حقوق مربوط به حریم خصوصی؛

۱۰. از تمامی دولت‌ها درخواست می‌نماید:

ا. به حقوق حریم خصوصی، از جمله در زمینه ارتباطات دیجیتالی، احترام گذاشته و از آن حفاظت نمایند؛

ب. اقداماتی را جهت پایان دادن به نقض آن حقوق ها و ایجاد شرایطی برای پیشگیری از چنین نقض‌هایی اتخاذ نمایند از جمله از طریق حصول اطمینان از تطابق قانون ملی مربوط با تعهدات خود ذیل قوانین بین‌المللی حقوق بشر؛

ج. رویکردها، رویه‌ها و قوانین خود را در ارتباط با موضوعات زیر بررسی و مورد بازنگری قرار دهند:

✓ نظارت، رهگیری و جمع‌آوری {داده‌ها} ارتباطات از جمله نظارت همگانی (نظارت جمعی)؛

✓ مداخله؛

✓ جمع‌آوری داده‌های شخصی؛

{و این بررسی}، با نگاهی بر اصرار روی حق حریم خصوصی، از طریق حصول اطمینان از اجرای کامل و اثر بخش تمامی تعهدات ذیل قوانین بین‌المللی حقوق بشر {انجام گردد}

د. سازوکارهایی که می‌توانند متضمن شفافیت و عندالافتضاء پاسخگویی دولت‌ها درباره نظارت و رهگیری ارتباطات و جمع‌آوری داده‌های شخصی باشند را ایجاد نمایند و یا {در صورت وجود چنین سازوکارهایی} آن‌ها را حفظ کنند. سازوکارهای اجرایی و پارلمانی داخلی مستقل، مؤثر، با منابع کافی و بسنده و منصفانه از نظر قضایی؛

ه. حصول یک راه‌حل مؤثر و سازگار با تعهدات بین‌المللی حقوق بشر را برای اشخاصی که حق حریم خصوصی آن‌ها از طریق نظارت‌های غیرقانونی و خودسرانه نقض گردیده است، مهیا نمایند.



۱۱. شورای حقوق بشر را تشویق می‌نماید تا: برگزاری فعالانه مباحثه با هدف زیر را حفظ نماید: تعیین و شفاف‌سازی اصول، استانداردها، رویه‌های برتر در رابطه با ارتقای و محافظت از حق حریم خصوصی و مورد نظر قرار دادن امکان ایجاد یک رویه خاص برای نیل به هدف فوق؛

۱۲. در خصوص حفظ برگزاری این مباحثه تصمیم می‌گیرد.

نشست عمومی ۷۳- مورخ ۱۸ دسامبر ۲۰۱۴

بند چهار: قطعنامه حق حریم خصوصی در عصر دیجیتال سال ۲۰۱۶

ترجمه سند



مجمع عمومی
کمیته دوم

تاریخ انتشار: ۲۵ ژانویه ۲۰۱۷

شماره قطعنامه: A/RES/71/199

توزیع: عمومی

اجلاس هفتاد و یک

دستور کار ۶۸(b)

قطعنامه پذیرفته شده توسط مجمع عمومی در ۱۹ دسامبر ۲۰۱۶ براساس گزارش کمیته سوم A/71/484/Add.2

۷۱/۱۹۹. حق حریم خصوصی در عصر دیجیتال^۱

مجمع عمومی:

با تأیید دوباره اهداف و اصول منشور ملل متحد؛

همچنین با تأیید دوباره حقوق بشر و آزادی‌های اساسی مورد احترام در اعلامیه جهانی حقوق بشر و معاهدات بین‌المللی حقوق بشری مربوط، از جمله میثاق حقوق مدنی و سیاسی و میثاق بین‌المللی حقوق اقتصادی، اجتماعی و فرهنگی،

با تأیید دوباره اعلامیه وین و برنامه اقدام؛

با یادآوری قطعنامه‌های مجمع عمومی ۱۶۷/۶۸ در تاریخ ۱۸ دسامبر ۲۰۱۳ و ۱۶۶/۶۹ در ۱۸ دسامبر ۲۰۱۴، همچنین قطعنامه‌های شورای حقوق بشر ۱۶/۲۸ در ۲۶ مارس ۲۰۱۵ درباره حق حریم خصوصی در عصر دیجیتال و قطعنامه ۱۳/۲۳ در تاریخ ۱ جولای ۲۰۱۶ درباره ارتقای، محافظت و برخورداری از حقوق بشر در اینترنت و با استقبال از انتصاب گزارشگر ویژه شورای حقوق بشر در مورد حق حفظ حریم خصوصی؛

با استقبال از سند مربوط به نتیجه جلسه سطح بالای مجمع عمومی درباره بازنگری کلی اعمال نتایج اجلاس سران در مورد جامعه اطلاعاتی، با توجه به گزارش‌های گزارشگر ویژه درباره

1 . The right to privacy in the digital age

حق حریم خصوصی و گزارش‌های گزارشگر ویژه شورای حقوق بشر درباره ارتقای و حفاظت از حق آزادی بیان و اندیشه؛

با استقبال از عملکرد دفتر کمیساریای عالی ملل متحد برای حقوق بشر در زمینه حق حریم خصوصی در عصر دیجیتال و توجه توأم با علاقه به گزارش این دفتر در مانحن فیه، و با یادآوری جلسه مباحثه و مناظره که در مورد حق حریم خصوصی در عصر دیجیتال در خلال بیست و هفتمین جلسه شورای حقوق بشر برگزار شد؛

باتوجه‌به اینکه حرکت سریع توسعه فنی، افراد را در سراسر جهان قادر می‌سازد تا از فناوری‌های جدید ارتباطی و اطلاعاتی استفاده کنند و در عین حال ظرفیت حکومت‌ها، شرکت‌ها و اشخاص برای نظارت، اختلال و جمع‌آوری اطلاعات را افزایش می‌دهد که این امر می‌تواند حقوق بشر، مخصوصاً حق حریم خصوصی، را نقض یا مورد تجاوز قرار دهد، موضوعی که در ماده ۱۲ اعلامیه جهانی حقوق بشر و ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی آمده است و بنابراین این موضوع یک نگرانی فزاینده است، همچنین باتوجه‌به اینکه نقض و سوءاستفاده از حق حریم خصوصی در عصر دیجیتال می‌تواند بر تمام اشخاص و به‌صورت ویژه بر زنان و همچنین کودکان و کسانی که آسیب‌پذیر هستند یا در حاشیه قرار گرفته‌اند اثر بگذارد؛

با تأیید دوباره حق حریم خصوصی انسان، که طبق آن، خود فرد، حریم خصوصی، خانواده، منزل و مکاتبات هیچکس نباید مورد مداخله غیر قانونی یا خودسرانه قرار گیرد و حق حفاظت قانون {مورد حمایت قانون بودن} در مقابل این مداخلات وجود داشته باشد و با به رسمیت شناختن اینکه اعمال حق حریم خصوصی برای تحقق حق آزادی بیان و داشتن عقیده‌ای مصون از مداخلات امری مهم است و حق آزادی مجامع و انجمن‌ها یکی از ارکان یک جامعه دموکراتیک است؛ با توجه و قدردانی از نظریه عمومی شماره ۱۶ کمیته حقوق بشر درباره ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی، در مورد حق احترام به حریم خصوصی، خانواده، خانه و مکاتبات، و حفظ حیثیت و شهرت افراد، در عین توجه به جهش‌های فناورانه گسترده‌ای که از زمان تصویب آن اتفاق افتاده است و نیاز به بحث در مورد حق حریم خصوصی با در نظر گرفتن چالش‌های عصر دیجیتال وجود دارد؛

با به رسمیت شناختن نیاز به بحث و تجزیه و تحلیل بیشتر بر اساس حقوق بشر بین‌المللی، موضوعات مرتبط با ارتقا و حفاظت از حریم خصوصی در عصر دیجیتال، پادمان‌های رویه‌ای، نظارت و راه‌حلهای مؤثر محلی، تأثیر نظارت بر حق حریم خصوصی و سایر حقوق بشری، و همچنین نیاز به بررسی اصول غیرخودسرانگی و قانونی، و مرتبط بودن ضرورت و تناسب ارزیابی‌ها در رابطه با شیوه‌های نظارت؛

باتوجه به برگزاری نشست جهانی چنددلی‌نفعی در زمینه آینده حکمرانی اینترنت (در نت موندیال) و بحثهای چنددلی‌نفعی که هر ساله در مجمع راهبری اینترنت برگزار می‌شود، که یک مجمع چنددلی‌نفعی برای بحثهایی درباره موضوعات مربوط به راهبری اینترنت است و مأموریت آن توسط مجمع عمومی در سال ۲۰۱۵ برای ۱۰ سال دیگر تمدید شد، و با به رسمیت شناختن اینکه مقابله مؤثر با چالش‌های مرتبط با حق حریم خصوصی در چارچوب فناوری ارتباطاتی مدرن، نیازمند یک مشارکت، مداومت و تعهد چنددلی‌نفعی است، با تأیید اینکه این مشارکت به‌طور گسترده‌ای توسط گفتگوهای غیررسمی در مورد حق حریم خصوصی در میان همه ذی‌نفعان مرتبط تسهیل می‌شود؛

با به رسمیت شناختن اینکه بحث در مورد حق حریم خصوصی باید بر اساس تعهدات قانونی داخلی و بین‌المللی، از جمله قانون بین‌الملل حقوق بشر، و نیز تعهدات مربوط باشد، و نیز، نباید منجر به باز شدن راهی برای دخالت بی‌مورد در حقوق بشر فردی شود؛

با تأکید بر اهمیت احترام کامل به آزادی در جستجو، دریافت و انتقال اطلاعات، از جمله اهمیت اساسی دسترسی به اطلاعات و مشارکت دموکراتیک؛

با یادآوری اینکه حق حریم خصوصی برای استفاده از آزادی بیان، از جمله حق درخواست، دریافت و انتقال اطلاعات مهم است و همکاری در توسعه توانایی فردی برای مشارکت در امور سیاسی، اقتصادی، اجتماعی و فرهنگی حایز اهمیت است و همچنین یادآوری اینکه استفاده از فناوری دیجیتال تأثیر قابل ملاحظه‌ای بر برخورداری از این حقوق دارد؛

باتوجه به اینکه، باوجود مزایایی که ابردادها می‌توانند فراهم کنند، انواع خاصی از ابردادها، زمانی که جمع می‌شوند، می‌توانند اطلاعات شخصی افراد را فاش کنند و همچنین می‌توانند

رفتار افراد، روابط اجتماعی، اولویتهای خصوصی و هویت فرد را ادراک کنند، با ابراز نگرانی از اینکه اغلب آزادی اشخاص تأمین نمی‌گردد، زیرا در عصر دیجیتال به طور قابل توجهی { موارد زیر} افزایش یافته است: موافقت صریح و آگاهانه جهت فروش یا فروش مجدد و متعدد داده‌های شخصی خود، جمع‌آوری، پردازش و به اشتراک‌گذاری داده‌ها از جمله داده‌های حساس؛ با تأکید بر اینکه نظارت یا رهگیری غیرقانونی ارتباطات و نیز جمع‌آوری داده‌ها به شکل غیرقانونی یا خودسرانه (اختیاری)، به‌عنوان اقدامات مداخله‌گراییانه، حقوق حریم خصوصی را نقض می‌کند، می‌تواند با حقوق آزادی بیان تداخل یابد و ممکن است با اصول جامعه دموکراتیک تناقض داشته باشد از جمله وقتی که {این اقدامات} در مقیاس وسیعی به‌کار گرفته شود؛

با به رسمیت شناختن اینکه از حقوق مردم در فضای برخط باید مشابه حقوق فضای غیربرخط محافظت گردد از جمله حقوق حریم شخص؛

با توجه ویژه بر اینکه نظارت بر ارتباطات دیجیتال باید مطابق با تعهدات بین‌المللی حقوق بشری باشد و مبتنی بر چارچوب قانونی انجام گیرد که {این چارچوب قانونی} لزوماً باید قابل دسترس برای عموم، شفاف، دقیق، جامع و غیرتبعیض‌آمیز باشد و {باتوجه به اینکه} هیچ مداخله‌ای نباید به شکل خودسرانه و غیرقانونی در حقوق حریم خصوصی انجام گیرد، با در نظر داشتن آنچه که در جهت تحقق اهداف مشروع، قابل قبول است و با یادآوری مجدد اینکه دولت‌های عضو در میثاق بین‌المللی مدنی و سیاسی باید گام‌های لازم جهت تصویب قوانین و یا سایر اقدامات لازم برای تأمین حقوق مصرحه در میثاق را اتخاذ نمایند.

با تأکید بر اینکه دولت‌ها باید به تعهدات بین‌المللی حقوق بشری در رابطه با حق حریم خصوصی احترام بگذارند :

- ✓ هنگامی که آن‌ها ارتباطات دیجیتالی اشخاص را رصد می‌کنند،
 - ✓ هنگام گردآوری داده‌های شخصی؛
 - ✓ هنگام نیاز به افشای داده‌های شخصی از اشخاص ثالث از جمله داده‌های مربوط به شرکت‌های خصوصی؛
- ضمن به رسمیت شناختن ماهیت جهانی و باز اینترنت به‌عنوان نیروی محرک در تسریع پیشرفت به سوی اشکال مختلف توسعه از جمله حصول اهداف توسعه پایدار؛

باتوجه به نظر عمومی شماره ۱۶ که توصیه نمود دولت‌ها اقدامات مؤثری برای پیشگیری از نگهداری، پردازش و استفاده غیرقانونی از داده‌های شخصی ذخیره شده توسط نهادهای عمومی و مؤسسات تجاری (کسب‌وکار) اتخاذ نمایند؛

همچنین باتوجه به اینکه رشد قابلیت مؤسسات تجاری در زمینه جمع‌آوری، پردازش و استفاده از داده‌های شخصی، می‌تواند {در رابطه با} برخورداری از حق حریم خصوصی در عصر دیجیتال، خطرآفرین باشد؛

ضمن استقبال از اقدامات داوطلبانه مؤسسات تجاری جهت ایجاد شفافیت برای کاربران خود در خصوص خط‌مشی‌های خود درباره درخواست‌های مراجع دولتی جهت دسترسی به داده‌ها و اطلاعات کاربران؛

با یادآوری اینکه مؤسسات تجاری در قبال احترام به حقوق بشر، قوانین حاکم، اصول و استانداردهای بین‌المللی مسئول می‌باشند؛

با نگرانی عمیق از امکان تأثیر منفی نظارت و یا رهگیری ارتباطات، از جمله نظارت و یا رهگیری ارتباطات فراسرزمینی، در به‌کارگیری و بهره‌مندی از حقوق بشر، و نیز جمع‌آوری داده‌های شخصی به‌ویژه در مقیاس وسیع، ضمن توجه توأم با نگرانی عمیق {در خصوص} اینکه در بسیاری از کشورها، اشخاص و سازمان‌های درگیر در {موضوع} ارتقای و دفاع از حقوق بشر و آزادی‌های بنیادین {اساسی}، در نتیجه فعالیت‌های خود، مکرراً با تهدیدات و آزار و اذیت، رنج از ناامنی و نیز مداخله خودسرانه و غیرقانونی درباره حقوق حریم خصوصی خود روبه‌رو هستند؛ باتوجه به این موضوع که نگرانی‌ها درباره امنیت عمومی، ممکن است گردآوری و حفاظت از اطلاعات حساس معین را توجیه نماید، دولت‌ها باید تضمین نمایند که تعهدات خود تحت حقوق بین‌المللی بشر را کاملاً رعایت نمایند؛

در ارتباط با {موضوع قبل} ضمن توجه بیشتر به اینکه پیشگیری و سرکوب تروریسم یک منفعت عمومی با {درجه} اهمیت زیاد می‌باشد، در عین حال مجدداً تأیید می‌نماییم که دولت‌ها باید تضمین نمایند که هر اقدامی را جهت مبارزه با تروریسم اتخاذ می‌نمایند باید مطابق با تعهدات خود تحت حقوق بین‌الملل باشد به‌ویژه حقوق بشر، حقوق پناهندگان و حقوق بشر دوستانه باشد؛

ضمن به رسمیت شناختن اینکه وجود یک محیط آزاد، ایمن، پایدار، دسترس پذیر و صلح آمیز برای فناوری اطلاعات و ارتباطات در راستای تحقق، حق حریم خصوصی در عصر دیجیتال امری مهم است؛

۱۳. مجدداً حق حریم خصوصی را تأیید می‌نماید مطابق {با این موضوع} که حریم خصوصی، خانوادگی، منزل یا مکاتبات هیچ کس نباید دستخوش مداخله خودسرانه یا غیرقانونی قرار گیرد، و {همچنین مجدداً} حقوق مربوط به حفاظت قانون در مقابله با چنین مداخله ای را {تأیید می‌نماید} وفق حقوق مصرحه در ماده ۱۲ اعلامیه جهانی حقوق بشر و ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی؛

۱۴. ماهیت جهانی و آزاد اینترنت به‌عنوان نیروی پیشران جهت تسریع پیشرفت به سوی اشکال مختلف توسعه از جمله حصول اهداف توسعه پایدار را به رسمیت می‌شناسد؛

۱۵. تأیید می‌کند که همان حقوقی که مردم در فضای غیربرخط دارند باید در فضای برخط نیز محافظت گردد از جمله حقوق مربوط به حریم خصوصی؛

۱۶. تمامی کشورهای عضو را تشویق می‌نماید تا یک محیط فناوری اطلاعات و ارتباطات آزاد، ایمن، پایدار، قابل دسترس و صلح آمیز را بر مبنای احترام به حقوق بین‌المللی ارتقای دهند، از جمله حقوقی که در منشور ملل متحد و اسناد حقوق بشر گرامی داشته شده است؛

۱۷. از تمامی دولت‌ها درخواست می‌نماید:

ه. به حقوق حریم خصوصی، از جمله در زمینه ارتباطات دیجیتالی، احترام گذاشته و از آن حفاظت نمایند؛

و. اقداماتی را جهت پایان دادن به نقض حقوق حریم خصوصی و ایجاد شرایطی برای پیشگیری از چنین نقض‌هایی اتخاذ نمایند از جمله از طریق حصول اطمینان از تطابق قانون ملی مربوط با تعهدات خود زیر قوانین بین‌المللی حقوق بشر؛

ز. رویکردها، رویه‌ها و قوانین خود را در ارتباط با موضوعات زیر بررسی و مورد بازنگری قرار دهند: نظارت، رهگیری و جمع‌آوری {داده‌ها} ارتباطات از جمله نظارت همگانی (نظارت جمعی)، مداخله جمع‌آوری داده‌های شخصی؛

{و این بررسی}، با نگاهی بر اصرار روی حق حریم خصوصی، از طریق حصول اطمینان از اجرای کامل و اثر بخش تمامی تعهدات زیر قوانین بین‌المللی حقوق بشر {انجام گردد}؛

ح. سازوکارهایی که می‌توانند متضمن شفافیت و عندالاقضاء پاسخگویی دولت‌ها در برابر نظارت و رهگیری ارتباطات و جمع‌آوری داده‌های شخصی باشند را ایجاد نمایند و یا {در صورت وجود چنین سازوکارهایی} آن‌ها را حفظ کنند. سازوکارهای اجرایی و پارلمانی {قانونگذاری} داخلی مستقل، مؤثر، با منابع کافی و بسنده و منصفانه از نظر قضایی؛

ط. حصول یک راه‌حل مؤثر و سازگار با تعهدات بین‌المللی حقوق بشر را برای اشخاصی که حق حریم خصوصی آن‌ها از طریق نظارت‌های غیرقانونی و خودسرانه نقض گردیده است، مهیا نمایند. ی. قوانین مناسب با ضمانت‌های اجرایی و جبرانی مؤثر در جهت محافظت شخص در برابر نقض و سوءاستفاده از حق حریم خصوصی را توسعه دهند یا حفظ نمایند و اجرا کنند، برای مثال نقض و سوءاستفاده از حقوق حریم خصوصی {می‌تواند} از طریق جمع‌آوری، پردازش و نگهداری و یا استفاده از اطلاعات شخصی توسط اشخاص دیگر، دولت‌ها، مؤسسات تجاری و سازمان‌های خصوصی {انجام گیرد}؛

ک. در این رابطه، اقدامات پیشگیرانه و اصلاحات {قانونی در خصوص} نقض و سوءاستفاده از حقوق حریم خصوصی در عصر دیجیتال را بیشتر گسترش دهند و یا حفظ نمایند. اقدامات و اصلاحاتی که ممکن است برای تمامی اشخاص مؤثر باشد از جمله تأثیرات ویژه برای زنان، کودکان و {گروه‌های} حساس و مهاجر {داشته باشد}

ل. فرصت‌های آموزش کیفی در طول زندگی، برای تمامی افراد را ارتقای دهند، این ارتقای در میان سایر موارد {شامل} تقویت سواد دیجیتال و مهارت‌های فنی لازم برای حفاظت مؤثر از حریم خصوصی خود می‌باشد.

م. مانع دخالت {مداخله} خودسرانه یا غیرقانونی مؤسسات تجاری درخواست‌کننده به حق حریم خصوصی شوند.

ن. اقدامات مناسبی را در نظر بگیرند که به واسطه آن‌ها مؤسسات تجاری {کسب‌وکار} را قادر سازند تا اقدامات داوطلبانه شفافیت را در رابطه با درخواست دسترسی به اطلاعات و داده‌های

کاربر خصوصی از مراجع دولتی، اتخاذ نمایند.

س. قوانین و اقدامات پیشگیرانه جهت مقابله با آسیب ناشی از { موارد زیر } را توسعه دهند یا حفظ و اصلاح نمایند: فروش، فروش متعدد یا اشتراک گذاری های داده‌های شخصی بدون رضایت اختیاری، آگاهانه و صریح شخص

۱۸. از مؤسسات تجاری { کسب‌وکار } درخواست می‌نماید تا:

أ. به مسئولیت خود در راستای احترام به حقوق بشر وفق اصول راهنما درباره مسائل و حقوق بشر واقف باشند. به چارچوب سند سازمان ملل تحت عنوان « حفاظت، احترام و اصلاح » عامل باشند از جمله در حوزه حق حریم خصوصی در عصر دیجیتال

ب. کاربران را در خصوص جمع‌آوری، استفاده، به اشتراک گذاری و نگهداری اطلاعات خود و امکان تأثیر { آن‌ها } بر حقوق حریم خصوصی خود آگاه سازند و در صورت مقتضی، خط‌مشی‌های شفاف‌تری را ایجاد نمایند.

۱۹. مؤسسات تجاری { کسب‌وکار } را تشویق می‌نماید، از جمله از طریق توسعه راه‌حل‌های فنی، در جهت حرکت به سوی توانمندسازی ارتباطات ایمن و حفاظت کاربران شخصی در مقابل مداخله‌های خودسرانه و غیرقانونی به حریم خصوصی آن‌ها عمل نمایند

۲۰. تمامی ذی‌نفعان مرتبط را تشویق می‌نماید تا در گفتگوهای غیر رسمی درباره حق حریم خصوصی شرکت نمایند و از همکاری گزارشگر ویژه شورای حقوق بشر در خصوص حق حریم خصوصی در این فرایند استقبال می‌نماید.

۲۱. شورای حقوق بشر را تشویق می‌نماید تا:

- برگزاری فعالانه مباحثه با هدف زیر را حفظ نماید: تعیین و شفاف‌سازی اصول، استانداردها، رویه‌های برتر در رابطه با ارتقای و محافظت از حق حریم خصوصی

- در راستای همکاری برای گزارش آتی کمیساری عالی سازمان ملل درباره حقوق بشر در خصوص این موضوع، برگزاری کارگاه کارشناسی را مورد نظر قرار دهد.

۲۲. تصمیم می‌گیرد تارسیدگی به مسائل و استفهامات را در اجلاس هفتاد و سوم خود ادامه دهد.

بند پنجم: قطعنامه بر نامه تقویت پیشگیری از جرم و عدالت کیفری سازمان ملل

به ویژه ظرفیت همکاری فنی خود سال ۲۰۱۷



مجمع عمومی
کمیته سوم

ترجمه سند

تاریخ انتشار: ۲۵ ژانویه ۲۰۱۸

شماره قطعنامه: A/RES/72/196

توزیع: عمومی

اجلاس هفتاد و دوم

دستور کار ۱۰۷

قطعنامه مصوب مجمع عمومی مورخ ۱۹ دسامبر ۲۰۱۷ (بر اساس گزارش کمیته سوم)^۱
برنامه تقویت پیشگیری از جرم و عدالت کیفری سازمان ملل به ویژه ظرفیت همکاری فنی خود
مجمع عمومی؛

با تأیید مجدد قطعنامه‌های خود به {شماره‌های} ۴۶/۱۵۲ مورخ ۱۸ دسامبر ۱۹۹۱، ۶۰/۱ مورخ ۱۶ سپتامبر ۲۰۰۵، ۶۷/۱ مورخ ۱۹ سپتامبر ۲۰۱۲، ۶۹/۱۹۳ و ۶۹/۱۹۶ مورخ ۱۸ دسامبر ۲۰۱۴، ۷۰/۱۷۸ و ۷۰/۱۸۲ مورخ ۱۷ دسامبر ۲۰۱۵ و ۷۱/۲۰۹ مورخ ۱۹ دسامبر ۲۰۱۶، با نگرانی در خصوص روند رو به رشد جرائم سایبری و سوءاستفاه از فناوری‌های اطلاعات و مخابرات در اشکال مختلف جرم،

۱. در این رابطه، با استقبال از قطعنامه ۲۶/۴ کمیسیون پیشگیری از جرم و عدالت کیفری مورخ ۲۶ می ۲۰۱۷ در خصوص تقویت همکاری بین‌المللی جهت مبارزه با جرائم سایبری، که در آن از گروه کارشناسان بین‌دولتی با بازه زمانی نامحدود که با هدف مطالعه ای جامع در خصوص جرائم سایبری تشکیل شده است، درخواست می‌شود که به فعالیت‌های خود و تبادل اطلاعات در زمینه تدوین قانون ملی، اتخاذ بهترین شیوه‌ها، مساعدت فنی و همکاری بین‌المللی ادامه دهد و در این راستا، بررسی گزینه‌هایی به منظور تقویت پاسخ‌های موجود و پیشنهاد قانونی ملی و بین‌المللی یا سایر پاسخها به جرائم سایبری را مورد نظر قرار دهد. و {گروه کارشناسان بین‌دولتی باز} در خصوص توسعه نتایج و توصیه‌های ممکن جهت ارسال به کمیسیون تشویق می‌شود؛

۱. فقط بندها و مباحث مرتبط با فضای سایبر و جرائم سایبری ترجمه شده است. قابل متن کامل سند در بانک اسناد الکترونیکی ارائه شده است.

2. Strengthening the United Nations crime prevention and criminal justice programme, in particular its technical cooperation capacity

۲. با تأیید مجدد اهمیت برنامه پیشگیری از جرم و عدالت کیفری سازمان ملل در ارتقای اقدام مؤثر برای تقویت همکاری بین‌المللی در پیشگیری از جرم و عدالت کیفری، و نیز عملکرد دفتر مبارزه با مواد مخدر و جرم سازمان ملل در اجرای دستور کار خود دایر بر پیشگیری از جرم و عدالت کیفری، از جمله، تدارک براساس درخواست دولت‌های عضو، به‌عنوان موضوعی با اولویت بالا، همکاری فنی، خدمات مشاوره‌ای و سایر اشکال مساعدت، هماهنگی و تکمیل عملکرد تمامی نهادها و دفترهای ذی‌صلاح و مرتبط سازمان ملل در خصوص کلیه جرائم سازمان‌یافته، از جمله جرائم ارتكابی در دریا، جرم سایبری، استفاده از فناوری‌های اطلاعاتی جدید جهت سوءاستفاده و استثمار کودکان، و نیز جرائم مرتبط با هویت، قاچاق محصولات و مالکیت فرهنگی، جریانهای مالی غیرمجاز، جرائم مالی و اقتصادی، از جمله کلاهبرداری و نیز جرائم مالیاتی و صنفی، قاچاق سنگ و فلزات گرانبها، جعل و تقلب در علامت تجاری کالاها، جرائم مؤثر بر محیط زیست و قاچاق غیرمجاز گونه‌های گیاهی و جانوری وحشی، قاچاق مواد مخدر، قاچاق انسان، قاچاق مهاجران و ساخت غیرمجاز و قاچاق جنگ افزارهای گرم، تجارت مستقیم و غیرمستقیم نفت و محصولات نفتی پالایش شده با گروه‌های مجرمان سازمان یافته و تروریست و نیز فساد و تروریسم؛

۳. توجه توأم با قدردانی از سومین نشست گروه کارشناسان بین‌دولتی باز (نامحدود زمانی) جهت انجام مطالعه‌ای جامع در خصوص جرائم سایبری و پاسخ به جرائم سایبری توسط دولت‌های عضو، جامعه بین‌المللی و بخش خصوصی و درخواست از دولت‌های عضو برای پشتیبانی از عملکرد گروه کارشناسان جهت کشف اقدامات ویژه و توسعه نتایج و توصیه‌های ممکن که برای ایجاد محیط سایبری امن و انعطاف پذیر برای پیشگیری و مقابله مؤثر با فعالیت‌های مجرمانه که در بستر اینترنت انجام شده است، طراحی گردیده اند. با توجه خاص به سرقت هویت، استخدام با هدف قاچاق انسان، و محافظت از کودکان در مقابل سوءاستفاده و استثمار برخط، تقویت همکاری پلیسی در سطوح ملی و بین‌المللی، از جمله با هدف تعیین هویت و محافظت از قربانیان، در کنار موارد دیگر، از طریق رفع {حذف} پورنوگرافی کودک از بستر اینترنت، به‌ویژه تصویرسازی سوءاستفاده جنسی از کودک، جهت افزایش امنیت شبکه‌های کامپیوتری و محافظت از یکپارچگی زیرساخت‌های مربوط و تلاش برای فراهم نمودن مساعدت فنی درازمدت

و ظرفیت‌سازی به‌منظور تقویت توانمندی نهادهای ملی برای مقابله با جرم سایبری، از جمله پیشگیری، کشف، تحقیق و تعقیب چنین جرائمی در کلیه اشکال آن؛

۴. دولت‌های عضو را جهت تقویت تلاش‌های خود در مبارزه علیه جرائم سایبری و کلیه اشکال سوءاستفاده مجرمانه از فناوری‌های اطلاعات و مخابرات و افزایش همکاری‌های بین‌المللی در این رابطه تشویق می‌کند.

بند شش: قطعنامه مقابله با استفاده از فناوری اطلاعات و ارتباطات برای اهداف مجرمانه سال ۲۰۱۸



مجمع عمومی
کمیته سوم

ترجمه سند

تاریخ انتشار: ۱۴ ژانویه ۲۰۱۹

شماره قطعنامه: A/RES/73/187

توزیع: عمومی

اجلاس هفتاد و سوم

دستور کار ۱۰۹

قطعنامه مصوب مجمع عمومی مورخ ۱۷ دسامبر ۲۰۱۸ بر اساس گزارش کمیته سوم (A/73/590)

مقابله با استفاده از فناوری اطلاعات و ارتباطات برای اهداف مجرمانه^۱

مجمع عمومی؛

با عنایت به این که فناوری های اطلاعات و ارتباطات به موازات قابلیت های متعددی که در توسعه کشورها دارند، فرصت های جدیدی را برای مجرمان و افزایش ارتکاب جرائم ایجاد می نمایند؛ همچنین با توجه به قابلیت فناوری های نوظهور، از جمله هوش مصنوعی، در پیشگیری و مبارزه علیه استفاده از فناوری های اطلاعات و ارتباطات برای اهداف مجرمانه؛

با ابراز نگرانی از افزایش میزان و تنوع جرائم ارتكابی در دنیای دیجیتال و تأثیر آن ها روی ثبات زیرساخت های حیاتی دولت ها و مؤسسات و رفاه اشخاص، با به رسمیت شناختن اینکه مجرمان مختلف از جمله مرتکبان به قاچاق انسان، که از مزایای فناوری اطلاعات و ارتباطات جهت انجام اقدامات مجرمانه استفاده می نمایند؛

با تأکید بر ضرورت ارتقای هماهنگی و همکاری میان دولت ها جهت مبارزه علیه استفاده از فناوری های اطلاعات و ارتباطات برای اهداف مجرمانه، از جمله از طریق کمک فنی به کشورهای در حال توسعه بر اساس درخواست آن ها، بهبود تدوین قانون ملی، ایجاد ظرفیت در نهادهای ملی جهت اقدام علیه تمامی اشکال استفاده مجرمانه از جمله پیشگیری، کشف، تحقیق و پیگردهای قانونی و با تأکید بر ایفای نقش سازمان ملل متحد به ویژه کمیسیون پیشگیری از جرم و عدالت کیفری در این چارچوب؛

1. . Countering the use of information and communications technologies for criminal purposes

با یادآوری قطعنامه کمیسیون پیشگیری از جرم و عدالت کیفری سازمان ملل {به شماره} ۲۲/۸ مورخ ۲۶ آوریل ۲۰۱۳، {مبنی بر} استقبال کمیسیون از تلاش‌های دفتر مقابله با جرم و مواد مخدر سازمان ملل جهت اجرای دستورکار خود در مساعدت فنی و ظرفیت‌سازی درباره مقابله با جرم سایبری؛

عملکرد کمیسیون پیشگیری از جرم و عدالت کیفری ملل متحد قابل توجه است. چرا که گروه کارشناسان دولتی باز، جهت مقابله با استفاده از فناوری‌های اطلاعات و ارتباطات برای اهداف مجرمانه، تحت حمایت این کمیسیون تأسیس گردید؛

با یادآوری قطعنامه {شماره} ۶۵/۲۳۰ مورخ ۲۱ دسامبر ۲۰۱۰ مجمع عمومی سازمان ملل که اعلامیه السالوادور با عنوان زیر را تأیید کرد: «راهبردهای جامع برای چالش‌های جهانی: سیستم‌های پیشگیری از جرم و عدالت کیفری و توسعه آن‌ها در یک جهان در حال تغییر»؛
با لحاظ مباحث مطرح شده پیرامون نیاز به ارتقای بیشتر مذاکرات بین‌المللی درخصوص همکاری علیه جرم سایبری که در طول چهار نشست گروه کارشناسان دولتی باز در تاریخ‌های ۱۷ تا ۲۱ ژانویه ۲۰۱۱، ۲۵ تا ۲۸ فوریه ۲۰۱۳، ۱۰ تا ۱۳ آوریل ۲۰۱۷ و ۳ تا ۵ آوریل ۲۰۱۸ برگزار گردید،

باتوجه به اهمیت اسناد بین‌المللی و منطقه‌ای در مبارزه علیه جرم سایبری و تلاش‌های دامنه‌دار جهت بررسی گزینه‌ها به منظور تقویت قوانین موجود و پیشنهاد قوانین جدید در سطوح ملی و بین‌المللی {تقویت} سایر پاسخها و واکنشها درباره استفاده از فناوری‌های اطلاعات و ارتباطات برای اهداف مجرمانه؛

با یادآوری قطعنامه خود {به شماره‌های} ۵۳/۷۰ مورخ ۴ دسامبر ۱۹۹۸، ۵۴/۴۹ مورخ ۱ دسامبر ۱۹۹۹، ۵۵/۲۸ مورخ ۲۰ نوامبر ۲۰۰۰، ۵۶/۱۹ مورخ ۲۹ نوامبر ۲۰۰۱، ۵۷/۵۳ مورخ ۲۲ نوامبر ۲۰۰۲، ۵۸/۳۲ مورخ ۸ دسامبر ۲۰۰۳، ۵۹/۶۱ مورخ ۳ دسامبر ۲۰۰۴، ۶۰/۴۵ مورخ ۸ دسامبر ۲۰۰۵، ۶۱/۵۴ مورخ ۶ دسامبر ۲۰۰۶، ۶۲/۱۷ مورخ ۵ دسامبر ۲۰۰۷، ۶۳/۳۷ مورخ ۲ دسامبر ۲۰۰۸، ۶۴/۲۵ مورخ ۲ دسامبر ۲۰۰۹، ۶۵/۴۱ مورخ ۸ دسامبر ۲۰۱۰، ۶۶/۲۴ مورخ ۲ دسامبر ۲۰۱۱، ۶۶/۱۸۱ مورخ ۱۹ دسامبر ۲۰۱۱، ۶۷/۲۷ مورخ ۳ دسامبر ۲۰۱۲، ۶۸/۱۹۳

مورخ ۱۸ دسامبر ۲۰۱۳، ۶۸/۲۴۳ مورخ ۲۷ دسامبر ۲۰۱۳، ۶۹/۲۸ مورخ ۲ دسامبر ۲۰۱۴، ۷۰/۲۳۷ مورخ ۲۳ دسامبر ۲۰۱۵، ۷۱/۲۸ مورخ ۵ دسامبر ۲۰۱۶ و ۷۲/۱۹۶ مورخ ۱۹ دسامبر ۲۰۱۷، باتوجه به گزارش‌های گروه کارشناسان دولتی درباره توسعه در حوزه اطلاعات و ارتباطات راه دور در چارچوب امنیت بین‌المللی، همچنین باتوجه به قطعنامه شماره ۲۶/۴ مورخ ۲۶ می ۲۰۱۷ کمیسیون پیشگیری از جرم و عدالت کیفری ملل متحد، که در آن، کمیسیون ضمن ابراز خرسندی از عملکرد گروه کارشناسان در انجام بررسی جامع درباره جرم سایبری، از آن گروه درخواست نمود تا کار خود را با نگاهی به بررسی گزینه‌هایی جهت تقویت پاسخ‌ها و واکنش‌های موجود و پیشنهاد قوانین جدید در سطوح ملی و بین‌المللی و سایر پاسخ‌ها درباره جرم سایبری ادامه دهد.

با تأیید مجدد اهمیت احترام به حقوق بشر و آزادی‌های اساسی در استفاده از فناوری‌های اطلاعات و ارتباطات:

۱. از دبیر کل درخواست می‌نماید تا نظرهای دولت‌های عضو درباره چالش‌های پیش روی آن‌ها در مقابله علیه استفاده از فناوری‌های اطلاعات و ارتباطات برای اهداف مجرمانه را پیگیری نماید و گزارشی را بر مبنای آن نظرها جهت رسیدگی به هفتاد و چهارمین اجلاس مجمع عمومی، ارائه نماید؛

۲. تصمیم می‌گیرد که هزینه‌های مازاد ناشی از اجرای بند ۱ قطعنامه حاضر، باید توسط مشارکت کنندگان داوطلب {مشارکت داوطلبانه در تأمین هزینه} تأمین گردد؛

۳. همچنین تصمیم می‌گیرد آیتی تحت عنوان «اقدام علیه استفاده از فناوری‌های اطلاعات و ارتباطات برای اهداف مجرمانه» در دستور کار موقت خود مربوط به اجلاس هفتاد و چهارم درج گردد؛

نشست عمومی ۵۶ (۱۷ دسامبر ۲۰۱۸)

بند هفت: قطعنامه مقابله با استفاده از فناوری اطلاعات و ارتباطات برای اهداف مجرمانه سال ۲۰۱۹



مجمع عمومی
کمیته سوم

ترجمه سند

تاریخ انتشار: ۲۷ نوامبر ۲۰۱۹

شماره قطعنامه: A/RES/74/401

توزیع: عمومی

اجلاس هفتاد و چهارم

دستورکار ۱۰۷

مقابله با استفاده از فناوری‌های اطلاعات و ارتباطات برای اهداف مجرمانه

مجمع عمومی؛

با عنایت به اینکه فناوری‌های اطلاعات و ارتباطات به موازات قابلیت‌های متعددی که در توسعه کشورها دارند، فرصت‌های جدیدی را برای مجرمان و افزایش ارتکاب جرائم ایجاد می‌نمایند، و ممکن است در بالابردن سطوح و پیچیدگی جرم مؤثر شود؛ همچنین با توجه به قابلیت خطر سوءاستفاده از فناوری‌های نوظهور، از جمله هوش مصنوعی، ضمن به رسمیت شناختن قابلیت آن‌ها {این فناوری‌ها} در پیشگیری و مبارزه با استفاده از فناوری‌های اطلاعات و ارتباطات برای اهداف مجرمانه؛ با ابراز نگرانی از افزایش میزان و تنوع جرائم ارتكابی در دنیای دیجیتال و تأثیر آن‌ها روی ثبات زیرساخت‌های حیاتی دولت‌ها و مؤسسات و رفاه اشخاص؛ با به رسمیت شناختن اینکه مجرمان مختلف از جمله مرتکبان به قاچاق انسان، که از مزایای فناوری اطلاعات و ارتباطات جهت انجام اقدامات مجرمانه استفاده می‌نمایند؛ با تأکید بر ضرورت ارتقای هماهنگی و همکاری میان دولت‌ها جهت مبارزه علیه استفاده از فناوری‌های اطلاعات و ارتباطات برای اهداف مجرمانه، از جمله از طریق کمک فنی به کشورهای در حال توسعه بر اساس درخواست آن‌ها، بهبود تدوین قانون ملی، ایجاد ظرفیت در نهادهای ملی جهت اقدام علیه تمامی اشکال استفاده مجرمانه از جمله پیشگیری، کشف، تحقیق و پیگردهای

قانونی و با تأکید بر ایفای نقش سازمان ملل متحد به‌ویژه کمیسیون پیشگیری از جرم و عدالت کیفری در این چارچوب، و با تأکید بر نقشی که سازمان ملل متحد به‌ویژه کمیسیون پیشگیری از جرم و عدالت کیفری در این زمینه ایفا می‌نماید؛

با یادآوری قطعنامه کمیسیون پیشگیری از جرم و عدالت کیفری سازمان ملل {به شماره} ۲۲/۸ مورخ ۲۶ آوریل ۲۰۱۳، {مبنی بر} استقبال کمیسیون از تلاش‌های دفتر مقابله با جرم و مواد مخدر سازمان ملل جهت اجرای دستورکار خود در مساعدت فنی و ظرفیت‌سازی درباره مقابله با جرم سایبری؛

به عملکرد کمیسیون پیشگیری از جرم و عدالت کیفری ملل متحد توجه می‌نماید. چرا که گروه کارشناسان دولتی باز، جهت مقابله با استفاده از فناوری‌های اطلاعات و ارتباطات برای اهداف مجرمانه و واکنش‌های دولت‌ها، جامعه بین‌الملل و بخش خصوصی به این {موضوع} تحت حمایت این کمیسیون تأسیس گردید؛

با یادآوری قطعنامه {شماره} ۶۵/۲۳۰ مورخ ۲۱ دسامبر ۲۰۱۰، مجمع عمومی سازمان ملل که اعلامیه السالوادور با عنوان زیر را تأیید کرد: «راهبردهای جامع برای چالش‌های جهانی: سیستم‌های پیشگیری از جرم و عدالت کیفری و توسعه آن‌ها در یک جهان در حال تغییر»؛

همچنین با یادآوری اعلامیه دوحه درباره «گنجاندن {موضوع} پیشگیری از جرم و عدالت کیفری در دستورکار گسترده تر ملل متحد جهت مقابله با چالش‌های اقتصادی و اجتماعی و فراهم نمودن حاکمیت قانون در سطوح ملی و بین‌المللی و مشارکت عمومی» {که این اعلامیه} در سیزدهمین کنگره ملل متحد درباره پیشگیری از جرم و عدالت کیفری مورخ ۱۲ تا ۱۹ آوریل ۲۰۱۵ در دوحه به تصویب رسید؛

با لحاظ مباحث مطرح‌شده پیرامون نیاز به ارتقای بیشتر مذاکرات بین‌المللی درخصوص همکاری علیه جرم سایبری که در طول چهار نشست گروه کارشناسان بین دولتی باز در تاریخ‌های ۱۷ تا ۲۱ ژانویه ۲۰۱۱، ۲۵ تا ۲۸ فوریه ۲۰۱۳، ۱۰ تا ۱۳ آوریل ۲۰۱۷ و ۳ تا ۵ آوریل و ۲۷ تا ۲۹ مارس ۲۰۱۹ تا ۲۰۱۸ برگزار گردید، {و} با تأیید مجدد اهمیت بررسی و ضرورت ارتقای بیشتر گفتگو درباره جرم سایبری و ارتقای همکاری علیه آن؛

باتوجه به اهمیت اسناد بین‌المللی و منطقه‌ای در مبارزه علیه جرم سایبری و تلاش‌های دامنه‌دار جهت بررسی گزینه‌ها به‌منظور تقویت قوانین موجود و پیشنهاد قوانین جدید در سطوح ملی و بین‌المللی یا {تقویت} سایر پاسخ‌ها و واکنش‌ها درباره استفاده از فناوری‌های اطلاعات و ارتباطات برای اهداف مجرمانه؛

با یادآوری قطعنامه خود {به شماره‌های} ۵۳/۷۰ مورخ ۴ دسامبر ۱۹۹۸، ۵۴/۴۹ مورخ ۱ دسامبر ۱۹۹۹، ۵۵/۲۸ مورخ ۲۰ نوامبر ۲۰۰۰، ۵۶/۱۹ مورخ ۲۹ نوامبر ۲۰۰۱، ۵۷/۵۳ مورخ ۲۲ نوامبر ۲۰۰۲، ۵۸/۳۲ مورخ ۸ دسامبر ۲۰۰۳، ۵۹/۶۱ مورخ ۳ دسامبر ۲۰۰۴، ۶۰/۴۵ مورخ ۸ دسامبر ۲۰۰۵، ۶۱/۵۴ مورخ ۶ دسامبر ۲۰۰۶، ۶۲/۱۷ مورخ ۵ دسامبر ۲۰۰۷، ۶۳/۳۷ مورخ ۲ دسامبر ۲۰۰۸، ۶۴/۲۵ مورخ ۲ دسامبر ۲۰۰۹، ۶۵/۴۱ مورخ ۸ دسامبر ۲۰۱۰، ۶۶/۲۴ مورخ ۲ دسامبر ۲۰۱۱، ۶۶/۱۸۱ مورخ ۱۹ دسامبر ۲۰۱۱، ۶۷/۲۷ مورخ ۳ دسامبر ۲۰۱۲، ۶۸/۱۹۳ مورخ ۱۸ دسامبر ۲۰۱۳، ۶۸/۲۴۳ مورخ ۲۷ دسامبر ۲۰۱۳، ۶۹/۲۸ مورخ ۲ دسامبر ۲۰۱۴، ۷۰/۲۳۷ مورخ ۲۳ دسامبر ۲۰۱۵، ۷۱/۲۸ مورخ ۵ دسامبر ۲۰۱۶ و ۷۲/۱۹۶ مورخ ۱۹ دسامبر ۲۰۱۷ و ۷۳/۱۸۷ مورخ ۱۷ دسامبر ۲۰۱۸؛

باتوجه به گزارش‌های گروه کارشناسان دولتی درباره توسعه در حوزه اطلاعات و ارتباطات راه دور در چارچوب امنیت بین‌المللی که در آن بیان شده است دولت‌ها باید بهترین همکاری را برای تعقیب قانونی استفاده مجرمانه از فناوری‌های اطلاعات و ارتباطات در نظر بگیرند؛

باتوجه به قطعنامه شماره ۲۶/۴ مورخ ۲۶ می ۲۰۱۷ کمیسیون پیشگیری از جرم و عدالت کیفری ملل متحد، که در آن، کمیسیون ضمن ابراز خرسندی از عملکرد گروه کارشناسان درانجام بررسی جامع درباره جرم سایبری، از آن گروه درخواست نمود تا کار خود را با نگاهی به بررسی گزینه‌هایی جهت تقویت پاسخ‌ها و واکنش‌های موجود و پیشنهاد قوانین جدید در سطوح ملی و بین‌المللی و سایر پاسخ‌ها درباره جرم سایبری ادامه دهد. و در این رابطه مجدداً بر نقش دفتر مقابله با مواد مخدر و جرم ملل متحد تأکید می‌نماید؛

همچنین باتوجه به قطعنامه شورای اقتصادی اجتماعی {به شماره} ۲۰۱۹/۱۹ مورخ ۲۳ جولای ۲۰۱۹ با عنوان «ارتقای مساعفت فنی و ظرفیت‌سازی جهت تقویت اقدامات ملی و همکاری

بین‌المللی برای مبارزه با جرم سایبری از جمله به اشتراک‌گذاری اطلاعات» { که } بر مبنای توصیه‌های کمیسیون پیشگیری از جرم و عدالت کیفری مصوب گردیده است؛

با به رسمیت شناختن نقش گروه کارشناسان بین‌دولتی باز در انجام بررسی جامع درباره جرم سایبری به‌عنوان یک بستر جهت تبادل اطلاعات درباره تدوین قوانین ملی، رویه‌های برتر، مساعدت فنی و همکاری بین‌المللی با نگاهی به بررسی گزینه‌ها به‌منظور تقویت قوانین موجود و پیشنهاد قوانین جدید در سطوح ملی و بین‌المللی یا { تقویت } سایر پاسخ‌ها و واکنش‌ها درباره جرم سایبری؛

با تأیید مجدد اهمیت احترام به حقوق بشر و آزادی‌های اساسی در استفاده از فناوری‌های اطلاعات و ارتباطات؛

۱. به گزارش دبیرکل که پیرو قطعنامه ۷۳/۱۸۷ تهیه گردیده بود توجه می‌نماید؛

۲. { درباره } تأسیس کمیته کارشناسان بین‌دولتی باز ویژه، با نمایندگانی از تمامی مناطق، تصمیم‌گیری می‌نماید. { این کمیته } با ملاحظه { و بررسی } کامل اسناد بین‌المللی و تلاش‌های موجود در سطح ملی و بین‌المللی در راستای مبارزه با استفاده از فناوری‌های اطلاعات و ارتباطات برای اهداف مجرمانه، به‌منظور ایجاد { توسعه } کنوانسیون جامع بین‌المللی جهت مقابله با استفاده از فناوری اطلاعات و ارتباطات برای اهداف مجرمانه تأسیس می‌گردد، به‌ویژه { ملاحظه } عملکرد و خروجی‌های گروه کارشناسان بین‌دولتی برای انجام بررسی جامع جرم سایبری؛

۳. همچنین تصمیم می‌گیرد که به‌منظور توافق روی طرح کلی و چگونگی و کیفیت فعالیت‌های بعدی خود، این کمیته ویژه باید نشست سازمانی سه روزه‌ای را در ماه اگوست سال ۲۰۲۰ در نیویورک برگزار کند { و این طرح کلی را } جهت بررسی و تصویب در هفتادوپنجمین اجلاس مجمع عمومی به این مجمع ارائه نماید؛

۴. از دبیرکل درخواست می‌نماید تا به‌منظور سازمان‌دهی و حمایت از کار کمیته ویژه، منابع { مالی } لازم را از { محل } برنامه بودجه سازمان ملل متحد { به این امر } اختصاص دهد؛

۵. از کشورهای حامی مالی داوطلب دعوت می‌نماید تا سازمان ملل را در راستای تضمین

تعامل فعال کشورهای در حال توسعه در کار گروه کمیته ویژه یاری نمایند از جمله از طریق {تأمین} هزینه‌های سفر و اسکان؛

۶. تصمیم می‌گیرد در هفتاد و پنجمین اجلاس خود، تحت گزینه ای با عنوان «مبارزه با استفاده از فناوری‌های اطلاعات و ارتباطات برای اهداف مجرمانه» موضوع را بررسی نماید؛

نامه سرگشاده به مجمع عمومی سازمان ملل متحد

نامه سرگشاده^۱ به مجمع عمومی سازمان ملل متحد: کنوانسیون بین‌المللی پیشنهادی درباره جرم سایبری تهدیدی برای حقوق بشر در فضای برخط را مطرح می‌نماید.^۲

عالی جنابان

مقابله با جرم سایبری چالش اصلی است که نیازمند همکاری بین‌المللی می‌باشد. به هر حال، رویکرد اتخاذی در قطعنامه کمیته سوم مجمع عمومی سازمان ملل با عنوان «مقابله با استفاده از فناوری‌های اطلاعات و ارتباطات برای اهداف مجرمانه» {A/C.3/74/L.11/Rev.1} اساساً به حقوق بشر و توسعه اجتماعی و اقتصادی خدشه وارد نموده است و استفاده از اینترنت را برای این اهداف محدود می‌نماید.

این قطعنامه تمایل دارد تا «کمیته کارشناسان بین دولتی باز ویژه، با نمایندگانی از تمامی مناطق را تأسیس نماید. {این کمیته به منظور بررسی} جزئیات کنوانسیون جامع بین‌المللی جهت مقابله با استفاده از فناوری اطلاعات و ارتباطات برای اهداف مجرمانه تأسیس می‌گردد». ما درباره ضرورت کنوانسیون جدید بین‌المللی درباره جرم سایبری قانع نشدیم. ما در خصوص رویکرد فعالیت سازمان ملل در این حوزه که در پیش‌نویس کنوانسیون ملل متحد برای همکاری جهت مقابله با جرم سایبری (A/C.3/72/12)، پیشنهاد شده است و توسط روسیه به جریان افتاد، شدیداً نگران هستیم. زیرا این می‌تواند استفاه از اینترنت برای بهره‌مندی حقوق بشر و تسهیل توسعه اجتماعی و اقتصادی را تضعیف نماید.

نگرانی‌های مادر باره این قطعنامه و فرایندی که این قطعنامه آغاز نموده است به شکل زیر می‌باشد:
 اولاً: استفاده از فناوری‌های اطلاعات و ارتباطات برای اهداف مجرمانه، در این قطعنامه تعریف نشده است. متن شامل دو موضوع زیر می‌باشد:

✓ امنیت سایبری (جرائمی که بر روی ثبات و زیرساخت‌های حیاتی دولت‌ها و مؤسسات تأثیر می‌گذارد)؛

✓ اقدامات مجرمانه‌ای که از طریق فناوری‌های اطلاعات و ارتباطات توأمند می‌شوند {به‌عنوان مثال در متن قطعنامه آمده است که «مجرمان مختلف از جمله مرتکبان به قاچاق انسان، که از مزایای فناوری اطلاعات و ارتباطات جهت انجام اقدامات مجرمانه استفاده می‌نمایند»}.
 عام بودن {تعاریف} نه تنها باعث نگرانی در خصوص صحت دیدگاه‌ها می‌شود بلکه این عبارات تعریف نشده، دری را باز می‌نماید تا رفتارهای معمولی در فضای برخط که تحت حقوق بشر حفاظت می‌گردند نیز جرم‌انگاری شوند.^۱

ثانیاً: جرم‌انگاری فعالیت‌های معمولی اشخاص و سازمان‌ها در فضای برخط از طریق اعمال حقوق جرم سایبری یک روند رو به رشدی را در بسیاری از کشورهای جهان شکل می‌دهد. گزارشگر ویژه سازمان ملل درباره حقوق آزادی تجمع و انجمن مسالمت آمیز، عنوان نموده است که: « جریان موجود در قانون‌گذاری و خط‌مشی‌ها به‌منظور مقابله با جرم سایبری دری به سوی مجازات معترضان و نظارت بر فعالیت‌ها را در بسیاری از کشورهای جهان باز نموده است.^۲
 در این گزارش ذکر می‌گردد که، چنین حقوقی میتواند:

✓ {برای جرم‌انگاری} دسترسی و استفاده از ارتباطات دیجیتالی ایمنی (به‌عنوان مثال استفاده از رمزنگاری) استفاده شود که این ارتباطات دیجیتالی ایمن برای کارهای جامعه مدنی، مدافعان حقوق بشر^۱ و روزنامه‌نگاران و همچنین مؤسسات دولتی و خصوصی که به اینترنتی پایدار و ایمن اعتماد دارند، حیاتی می‌باشند؛

✓ {به دولت‌ها} اجازه می‌دهد خودسرانه یا {به شکل} صلاح‌دیدگی از عبارات مبهم و نامعلوم در جرم‌انگاری اشکال قانونی بیان، تجمع و انجمن در فضای برخط استفاده کنند {که این امر}

1. "opens the door to criminalizing ordinary online behavior that is protected under international human rights law"
 2. 2019 Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association (A/HRC/41/4)

منتج به عدم قطعیت و عدم اطمینان قانونی می شود؛

✓ به حکومت‌ها قدرت گسترده ای می‌دهد تا وبسایت‌هایی را که از نگاه حاکمیت، حساس می‌باشند و حتی تمامی شبکه‌ها، برنامه‌ها و خدمات کاربردی که دسترسی و تبادل اطلاعات در فضای برخط تسهیل می‌نمایند را مسدود نمایند؛

✓ از آنجایی که قانونگذاری با هدف مقابله با جرم سایبری می‌تواند ضروری باشد و سبب تقویت سازمان‌ها و نهادهای دموکراتیک گردد، اما هنگام استفاده سوء از قوانین، حقوق جرم سایبری می‌تواند یک تأثیر دلسردکننده‌ای را ایجاد نماید و مانع توانمندی افراد جهت استفاده از اینترنت در راستای بهره‌مندی از حقوق خود در فضای برخط و غیربرخط گردد؛

✓ از آنجایی که رویه‌های ویژه و گوناگون ملل متحد در ارتباط با دولت‌ها شکل گرفته است، حقوق سایبری می‌تواند منتج به بازداشت، حبس خودسرانه، مستبدانه افراد و حتی مرگ آن‌ها از طرف دولت‌ها شود؛

ثالثاً، «پیش‌نویس کنوانسیون سازمان ملل متحد درباره همکاری در مقابله با جرم سایبری» که به‌عنوان یک مبنایی برای توسعه کنوانسیون جامع بین‌المللی هدفمند گردیده است، میزان نگرانی‌ها را افزایش می‌دهد. مخصوصاً اینکه پیش‌نویس این کنوانسیون به دنبال کنوانسیون بوداپست پیشنهاد گردید.

کنوانسیون‌هایی که اجازه دسترسی خارج از مرز به داده‌ها را می‌دهد، از جمله توانایی دولت‌امضاءکننده این کنوانسیون در خصوص نپذیرفتن یا عدم تأمین دسترسی به داده‌های مورد نیاز را محدود می‌کند.^۲

پیش‌نویس کنوانسیون تمایل دارد تا از طریق ایجاد کمیسیون فنی بین‌المللی جهت مبارزه علیه جرم فناوری اطلاعات و ارتباطات، درمیان سایر سازوکارهای اجرایی، سازمان ملل متحد را به‌عنوان یک نهاد، برای گزینه اجرایی تصدیق نماید.

برخی از مفاد پیش‌نویس کنوانسیون منعکس‌کننده کنوانسیون بوداپست است، اما منابعی جهت تعادل بین منافع حاکمیت قانون و احترام به حقوق آزادی اساسی بشر در این کنوانسیون وجود ندارد، تلاش‌های مسلم روسیه جهت توسعه کنترل حکومت روی اینترنت تحت اصطلاح حقوق

1. human rights defenders (HRDs)

2. (3) Articles 51-56 of the Draft Convention establish conditions for the availability of data from other states.

«حاکمیت اینترنت» مؤثر است، رهبری روسیه در توسعه معاهده الزام آور بین‌المللی در خصوص جرم سایبری، سطوح بالای امنیت را تضمین می‌کند.

رایعاً؛ ما در خصوص نیاز به کنوانسیون بین‌المللی جدید درباره جرم سایبری قانع نشدیم. تقویت و ارتقای اسناد موجود پسندیده‌تر و عملیاتی‌تر است در مقایسه با اینکه منابع قلیلی که از گذشته وجود داشته است را متوجه پیگیری چارچوب بین‌المللی جدید نماییم. زیرا این کار به طور قطع سال‌های زیادی طول می‌کشد و بعید است که نتایج آن به اجماع برسد.

پیش از این نیز در بخش‌های مختلف سازمان ملل متحد جهت مقابل با جرم سایبری کارهایی در دست اقدام می‌باشد. از جمله اقداماتی که توسط دفتر مقابل با مواد مخدر و جرم سازمان ملل در سطوح ملی و منطقه‌ای انجام می‌شود. مطابق با بانک اطلاعاتی این دفتر درباره تدوین قانون جرم سایبری، بیشتر از ۱۸۰ کشور قانونگذاری ماهوی و رویه‌ای را درباره جرم سایبری و ادله الکترونیکی دارند. از گذشته فرایندی جهت مقابل با چالش‌های ناشی از تنوع توانایی قوانین ملی و ظرفیت حکومت‌ها جهت اجرای آن‌ها، در سازمان ملل در حال اجرا می‌باشد اما به‌طور قطع این چالش‌ها وجود دارند. انتظار می‌رود که گروه کارشناسان بین‌دولتی باز سازمان ملل متحد در خصوص اجرای بررسی جامع جرم سایبری، گزارش خود را در سال ۲۰۲۱ منتشر نماید، گزارشی که باید شامل یافته‌ها و توصیه‌هایی در خصوص تدوین قانون ملی، رویه‌های برتر، مساعدت فنی و همکاری بین‌المللی باشد. در حال حاضر فرایندی جهت توسعه دومین پروتکل الحاقی به کنوانسیون بوداپست در جریان است که به شکل گسترده‌ای اسناد بین‌المللی درباره جرم سایبری را تأیید و تصدیق نموده است.

در خاتمه، جهت مقابل با جرم سایبری، مجاهدت و تلاش چنددینفعی ضروری می‌باشد و این موضوع نیازمند {همکاری} مقامات عالی رتبه و کارشناسان دولتی، اعضای جامعه فنی، جامعه مدنی، بخش خصوصی و نهادهای علمی تحقیقاتی است.

ایجاد یک کمیته کارشناسی ویژه جهت پرداختن به موضوعات جرم سایبری، ذی‌نفعان اصلی را مستثنی می‌کند. ذی‌نفعانی که تجربیات و چشم‌اندازهای با ارزشی را در خصوص موارد زیر دارند: مقابل مؤثر با استفاده از فناوری‌های اطلاعات و ارتباطات با اهداف مجرمانه و تضمین

اینکه چنین تلاش‌هایی حقوق بشر در بهره‌مندی از استفاده از فناوری اطلاعات و ارتباطات و همچنین توسعه اجتماعی و اقتصادی را تضعیف نمی‌نماید. ما قویاً بر رای منفی، نماینده شما به قطعنامه A/C.3/74/L/11/Rev.1 {با عنوان} «مقابله با استفاده از فناوری اطلاعات و ارتباطات برای اهداف مجرمانه» اصرار داریم و {همچنین} برای کار جهت تضمین اینکه ابتکارات جهت مقابله با جرم سایبری برای تمامی ذی‌نفعان فراگیر می‌باشد اصرار داریم.

اجلاس هفدهم، شورای حقوق بشر و اجلاس شصت و هشتم مجمع عمومی در خصوص آزادی بیان در اینترنت، ارائه شده است:

۱. تأیید می‌کند که همان حقوقی که مردم در حالت غیربرخط دارند باید در حالت برخط نیز محافظت شود، به‌ویژه آزادی بیان، که مطابق با ماده ۱۹ اعلامیه جهانی حقوق بشر و میثاق بین‌المللی حقوق سیاسی و مدنی، قطع نظر از مرزها و از طریق هر نوع رسانه به انتخاب خود فرد، قابل اجراست؛

۲. ماهیت باز و جهانی اینترنت را به‌عنوان یک نیروی محرکه و پیشران جهت تسریع پیشرفت به سوی توسعه اینترنت در شکل‌های مختلف، به رسمیت می‌شناسد؛

۳. از تمامی دولت‌ها، درخواست می‌کند که دسترسی به اینترنت و همکاری بین‌المللی خود را با هدف توسعه رسانه و فناوری و امکانات اطلاعاتی و ارتباطاتی در تمامی کشورها ارتقای دهند و تسهیل نمایند؛

۴. تشویق می‌کند رویه‌های ویژه را برای این موضوعات در احکام موجود خود به‌صورت کاربردی در نظر بگیرند؛

۵. مطابق برنامه کاری خود، برای ادامه ملاحظاته‌اش در ارتقای، حفاظت و برخورداری از حقوق بشر، از جمله حق آزادی بیان، در اینترنت و سایر فناوری اطلاعات و ارتباطات و ادامه ملاحظاته‌اش در اینکه چگونه اینترنت می‌تواند ابزار مهمی برای تحقق توسعه و به‌رمندی حقوق بشر، در هر جامعه باشد، تصمیم می‌گیرد؛

مصوب بدون رأی‌گیری (اجماع) نشست ۳۱ (۵ جولای ۲۰۱۲)

بند دو: قطعنامه ارتقای، حفاظت و برخورداری از حقوق بشر در اینترنت سال ۲۰۱۴



مجمع عمومی
شورای حقوق بشر

ترجمه سند

تاریخ انتشار: ۱۴ جولای ۲۰۱۴

شماره قطعنامه: A/HRC/RES/26/13

زبان: انگلیسی

اجلاس بیست و هشتم

دستور کار ۳

ارتقای، حفاظت تمامی حقوق بشر، حقوق مدنی، سیاسی، اقتصادی، اجتماعی و فرهنگی از جمله حق توسعه قطعنامه مصوب شورای حقوق بشر
ارتقای، حفاظت و برخورداری از حقوق بشر در اینترنت

شورای حقوق بشر؛

با هدایت منشور ملل متحد؛

با تأیید مجدد حقوق بشر و آزادی‌های اساسی ارج نهاده شده در اعلامیه جهانی حقوق بشر و معاهدات بین‌المللی مرتبط با حقوق بشری از جمله میثاق بین‌المللی حقوق مدنی و سیاسی و میثاق بین‌المللی حقوق اقتصادی، اجتماعی و فرهنگی؛
با یادآوری تمامی قطعنامه‌های مربوط به کمیسیون و شورای حقوق بشر در خصوص حق آزادی عقیده و بیان، به‌ویژه قطعنامه‌های شورا {رُبه شماره} ۲۰/۸ مورخ ۵ جولای ۲۰۱۲ درباره ارتقای، حفاظت و برخورداری از حقوق بشر در اینترنت و قطعنامه‌های ۱۲/۱۶ مورخ ۲ اکتبر ۲۰۰۹ در مورد آزادی عقیده و بیان، ۲۳/۲ مورخ ۱۳ ژوئن ۲۰۱۳ درباره نقش آزادی عقیده و بیان در توانمندسازی زنان و همچنین با یادآوری قطعنامه‌های مجمع عمومی {رُبه شماره} ۶۸/۱۶۷ مورخ ۱۸ دسامبر ۲۰۱۳ در خصوص حق حریم خصوصی در عصر دیجیتال، و ۶۸/۱۹۸ مورخ ۲۰ دسامبر ۲۰۱۳ درباره فناوری‌های اطلاعات و ارتباطات برای توسعه و تصمیم شورای حقوق بشر {رُبه شماره} ۲۵/۱۱۷ مورخ ۲۷ مارس ۲۰۱۴ در خصوص میزگردی درباره حقوق حریم خصوصی در عصر دیجیتال؛

باتوجه به نشست چندذی‌نفعی جهانی در خصوص آینده حکمرانی بر اینترنت، در سائوپائولو مورخ ۲۳ و ۲۴ آوریل ۲۰۱۴ که در میان موارد دیگر، بر نیاز به {رعایت} حقوق بشر در حکمرانی اینترنت اذعان داشت و اینکه حقوقی که مردم در فضای غیربرخط دارند باید از همان حقوق در فضای برخط نیز حفاظت شود. {همان حقوق را باید داشته باشند}؛

باتوجه به اینکه بهره‌مندی از حقوق بشر، به‌ویژه حق آزادی بیان، در اینترنت موضوعی مهم و منافع‌فزاینده می‌باشد، از آنجایی که گام سریع توسعه فنی، اشخاص را در سراسر دنیا در استفاده از فناوری جدید اطلاعات و ارتباطات توانمند می‌کند؛

همچنین باتوجه به اهمیت اعتمادسازی و اطمینان‌سازی در اینترنت - که اهمیت آن کمتر از آزادی بیان، حریم خصوصی و سایر حقوق بشر در اینترنت نیست - به طوری که قابلیت‌های اینترنت به‌عنوان یک توانمندساز در حوزه نوآوری و توسعه، در کنار موارد دیگر، می‌تواند تحقق یابد. با تأکید بر اینکه دسترسی به اطلاعات در اینترنت فرصت‌های زیادی برای آموزش فراگیر و کم‌هزینه در سطح جهانی را تسهیل می‌نماید، در نتیجه، ابزار مهمی برای تسهیل ارتقای حق آموزش می‌باشد، ضمن تأکید بر نیاز به پرداختن به مقوله سواد دیجیتالی و شکاف دیجیتالی، چرا که این امر، برخورداری از حق آموزش را تحت تأثیر قرار می‌دهد؛

با به رسمیت شناختن اینکه، به‌منظور باقیماندن اینترنت با قابلیت تعامل متقابل، باز و جهانی، الزامی است که دولت‌ها، مطابق با تعهدات حقوق بشر بین‌المللی خودشان، با نگرانی‌های امنیتی به‌ویژه در مورد آزادی بیان، آزادی حریم خصوصی و تشکل‌ها، مقابله نمایند؛

با توجه توأم با قدردانی از گزارش‌های گزارشگر ویژه در مورد ارتقای و حفاظت از حق آزادی عقیده و بیان که در اجلاس‌های ۱۷ و ۲۳ شورای حقوق بشر و اجلاس ۶۶ مجمع عمومی در خصوص آزادی بیان در اینترنت، ارائه شده است؛

با در نظر گرفتن اهمیت کلیدی تعامل دولت با تمامی ذی‌نفعان مرتبط، از جمله جامعه مدنی، بخش خصوصی، جامعه فنی و دانشگاهی، در خصوص ارتقای و حفاظت از حقوق بشر و آزادی‌های اساسی برخط؛

۱. تأیید می‌کند که همان حقوقی که مردم در حالت غیربرخط دارند باید در حالت برخط،

نیز محافظت شود، به‌ویژه آزادی بیان که مطابق با ماده ۱۹ اعلامیه جهانی حقوق بشر و میثاق بین‌المللی حقوق سیاسی و مدنی، قطع نظر از مرزها و از طریق هر نوع رسانه به انتخاب خود فرد، قابل اجراست؛

۲. ماهیت باز و جهانی اینترنت را به‌عنوان یک نیروی محرکه و پیشران جهت تسریع پیشرفت به سوی توسعه اینترنت در شکل‌های مختلف، به رسمیت می‌شناسد؛

۳. از تمامی دولت‌ها، درخواست می‌کند که دسترسی به اینترنت و همکاری بین‌المللی خود را با هدف توسعه رسانه و فناوری و امکانات اطلاعاتی و ارتباطاتی در تمامی کشورها ارتقای دهند و تسهیل نمایند؛

۴. تأیید می‌کند که کیفیت آموزش نقش قاطع و تعیین‌کننده‌ای در توسعه ایفا می‌کند و از این رو از تمامی دولت‌ها می‌خواهد که سواد دیجیتالی را ارتقای دهند و دسترسی به اطلاعات در اینترنت را که می‌تواند ابزار مهمی در تسهیل ارتقای حق آموزش باشد، تسهیل نماید آموزش باشد، تسهیل نماید؛

۵. از تمامی دولت‌ها می‌خواهد که با نگرانی‌های امنیتی مربوط به اینترنت مطابق با تعهدات بین‌المللی حقوق بشری خود مقابله نمایند تا در خصوص از حفاظت آزادی بیان، آزادی تجمع، حریم خصوصی و سایر حقوق بشر برخط، اطمینان حاصل شود، از جمله از طریق مؤسسات ملی دموکراتیک، شفاف، مبتنی بر حاکمیت قانون، به‌نحوی که آزادی و امنیت اینترنت را تضمین کند به‌طوری که اینترنت بتواند به‌عنوان یک نیروی پویا به توسعه فرهنگی، اجتماعی و اقتصادی ادامه دهد؛

۶. بر اهمیت مبارزه با کینه‌ورزی (نفرت پراکنی)، که باعث انگیزه تبعیض یا خشونت در

اینترنت می‌شود، از جمله از طریق ارتقای آستانه تحمل و ترویج گفتگو، تأکید می‌کند؛

۷. از همه دولت‌ها می‌خواهد تا از طریق فرایندهای شفاف و فراگیر با همه ذی‌نفعان، تدوین و تصویب سیاست‌های عمومی مرتبط با اینترنت ملی را در نظر بگیرند. سیاست‌هایی که اهدافی مثل دسترسی جهانی و برخورداری از حقوق بشر را در درون خود دارند؛

۸. تشویق می‌کند رویه‌های ویژه را برای این موضوعات در احکام موجود خود به‌صورت کاربردی در نظر بگیرند؛

۹. مطابق برنامه‌کاری خود، برای ادامه ملاحظاته‌ش در ارتقای، حفاظت و برخورداری از حقوق بشر، از جمله حق آزادی بیان، در اینترنت و سایر فناوری اطلاعات و ارتباطات و ادامه ملاحظاته‌ش در اینکه چگونه اینترنت می‌تواند ابزار مهمی برای تحقق توسعه و بهره‌مندی حقوق بشر، در هر جامعه باشد، تصمیم می‌گیرد؛

نشست ۳۸ (۲۶ ژوئن ۲۰۱۴)

مصوب بدون رأی‌گیری (اجماع)

بند سه: قطعنامه ارتقای، حفاظت و برخورداری از حقوق بشر در اینترنت سال ۲۰۱۶

ترجمه سند



مجمع عمومی
شورای حقوق بشر

تاریخ انتشار: ۱ جولای ۲۰۱۶

شماره قطعنامه: A/HRC/RES/32/13

زبان: انگلیسی

اجلاس سی و دوم

دستور کار ۳

قطعنامه مصوب شورای حقوق بشر مورخ اول جولای ۲۰۱۶
ارتقای، حفاظت و برخورداری از حقوق بشر در اینترنت

شورای حقوق بشر؛

با هدایت منشور ملل متحد؛

با تأیید مجدد حقوق بشر و آزادی‌های اساسی ارج نهاده شده در اعلامیه جهانی حقوق بشر و معاهدات بین‌المللی مرتبط حقوق بشری از جمله میثاق بین‌المللی حقوق مدنی و سیاسی و میثاق بین‌المللی حقوق اقتصادی، اجتماعی و فرهنگی؛

با یادآوری تمامی قطعنامه‌های مربوط به کمیسیون و شورای حقوق بشر در خصوص حق آزادی عقیده و بیان، به‌ویژه قطعنامه‌های شورا {به شماره} ۲۰/۸ مورخ ۵ جولای ۲۰۱۲ و ۲۶/۱۳ مورخ ۲۶ ژوئن ۲۰۱۴ درباره ارتقای، حفاظت و برخورداری از حقوق بشر در اینترنت و قطعنامه‌های ۱۲/۱۶ مورخ ۲ اکتبر ۲۰۰۹ در مورد آزادی عقیده و بیان، ۲۸/۱۶ مورخ ۲۴ مارس ۲۰۱۵ در خصوص حق حریم خصوصی در عصر دیجیتال و ۲۳/۲ مورخ ۱۳ ژوئن ۲۰۱۳ درباره نقش آزادی عقیده و بیان در توانمندسازی زنان و ۳۱/۷ مورخ ۲۳ مارس ۲۰۱۶ در مورد حقوق کودک: فناوری‌های اطلاعات و ارتباطات و استثمار جنسی کودک و همچنین با یادآوری قطعنامه‌های مجمع عمومی {به شماره} ۶۸/۱۶۷ مورخ ۱۸ دسامبر ۲۰۱۳ و ۶۹/۱۶۶ مورخ ۱۸ دسامبر ۲۰۱۴ در خصوص حق حریم خصوصی در عصر دیجیتال، ۷۰/۱۸۴ مورخ ۲۲ دسامبر ۲۰۱۵ درباره فناوری‌های اطلاعات و ارتباطات برای توسعه و ۷۰/۱۲۵ مورخ ۱۶ دسامبر ۲۰۱۵، شامل سند

منتج از نشست سطح بالای مجمع عمومی در مورد بازنگری کلی اجرای نتایج اجلاس سران درباره جامعه اطلاعاتی؛

با استقبال از تصویب دستور کار توسعه پایدار و با به رسمیت شناختن اینکه گسترش فناوری اطلاعات و ارتباطات و همبستگی جهانی پتانسیل عظیمی در تسریع پیشرفت انسانی برای رفع و از بین بردن شکاف دیجیتالی و توسعه جوامع علمی دارد؛

باتوجه به نشست چندذی‌نفعی جهانی در خصوص آینده حکمرانی بر اینترنت، در سائوپائولو مورخ ۲۳ و ۲۴ آوریل ۲۰۱۴، که در میان موارد دیگر، بر نیاز به {رعایت} حقوق بشر در حکمرانی اینترنت اذعان داشت و اینکه حقوقی که مردم در فضای غیربرخط دارند باید از همان حقوق در فضای برخط نیز حفاظت شود. {همان حقوق را باید داشته باشند}؛

همچنین باتوجه به اجلاس‌های قبلی مجمع راهبری اینترنت، از جمله آخرین نشست که از ۱۰ تا ۱۳ نوامبر ۲۰۱۵ در سائوپائولو برگزار شد؛

باتوجه به اینکه بهره‌مندی از حقوق بشر، به‌ویژه حق آزادی بیان، در اینترنت موضوعی دارای اهمیت و منافع فزاینده می‌باشد، از آنجایی که گام سریع توسعه فنی، اشخاص را در سراسر دنیا در استفاده از فناوری جدید اطلاعات و ارتباطات توانمند می‌کند؛

همچنین باتوجه به اهمیت اعتمادسازی و اطمینان‌سازی در اینترنت - که اهمیت آن کمتر از آزادی بیان، حریم خصوصی و سایر حقوق بشر در اینترنت نیست - به طوری که قابلیت‌های اینترنت به‌عنوان یک توانمندساز در حوزه نوآوری و توسعه، در کنار موارد دیگر، با همکاری کامل بین دولت‌ها، جامعه مدنی، بخش خصوصی، جامعه فنی و دانشگاهی می‌تواند تحقق یابد و جامعه عمل ببوشد؛ با به رسمیت شناختن اینکه حریم خصوصی برخط برای تحقق حق آزادی بیان و داشتن عقاید بدون مداخله و حق آزادی مجامع و تشکل‌های صلح‌آمیز، مهم می‌باشد؛

با تأکید بر اینکه دسترسی به اطلاعات در اینترنت فرصت‌های زیادی برای آموزش فراگیر و کم‌هزینه در سطح جهانی را تسهیل می‌نماید، در نتیجه، ابزار مهمی برای تسهیل ارتقای حق آموزش می‌باشد، ضمن تأکید بر نیاز به پرداختن به مقوله سواد دیجیتالی و شکاف دیجیتالی، چرا که این امر، برخورداری از حق آموزش را تحت تأثیر قرار می‌دهد؛

با ابراز نگرانی از اینکه بسیاری از اشکال شکاف های دیجیتالی بین کشورها و درون آنها و بین زنان و مردان، پسرها و دخترها باقی می ماند و با به رسمیت شناختن نیاز به از بین بردن این شکافها؛ با تأکید بر اهمیت توانمندسازی تمامی زنان و دختران از طریق دسترسی بیشتر آنها به فناوری اطلاعات و ارتباطات، ارتقای سواد دیجیتالی و مشارکت زنان و دختران در آموزش و یادگیری فناوری اطلاعات و ارتباطات و با تشویق زنان و دختران به مبادرت به شغل هایی در علوم و فناوری اطلاعات و ارتباطات؛

با یادآوری مجدد مواد ۹ و ۲۱ کنوانسیون حقوق اشخاص ناتوان، که در میان موارد دیگر، از دولت های عضو درخواست می کند اقدامات مناسب جهت ارتقای دسترسی افراد ناتوان به سیستمها و فناوری اطلاعات و ارتباطات از جمله اینترنت را اتخاذ نمایند؛

با به رسمیت شناختن اینکه، به منظور باقی ماندن اینترنت با قابلیت تعامل متقابل، باز و جهانی الزامی است که دولت ها، مطابق با تعهدات حقوق بشر بین المللی خودشان، با نگرانی های امنیتی به ویژه در مورد آزادی بیان، آزادی حریم خصوصی و تشکلهای، مقابله نمایند؛

با ابراز نگرانی عمیق از ارتکاب به سوءاستفاده و نقض حقوق بشر و مصونیت از مجازات ناشی این سوءاستفاده ها و نقضها که علیه افراد در حال بهره مندی از حقوق بشر و آزادی های اساسی آنها در اینترنت رخ می دهد؛

همچنین با نگرانی عمیق از اقدامات عمدی در نقض قانون بین المللی حقوق بشر، با هدف جلوگیری یا مختل کردن دسترسی و یا انتشار اطلاعات برخط؛

با تأکید بر اهمیت به کارگیری یک رویکرد مبتنی بر حقوق بشر جامع، که دسترسی به اینترنت و اینترنتی باز، قابل دسترسی و رشد یافته توسط مشارکت چنددی نفعی رامهیا می کند و توسعه می دهد، با توجه توأم با قدردانی از گزارش های گزارشگر ویژه در مورد ارتقای و حفاظت از حق آزادی عقیده و بیان که در اجلاس های هفدهم، بیست و سوم، بیست و نهم و سی و دوم شورای حقوق بشر و اجلاس شصت و ششم مجمع عمومی در خصوص آزادی بیان در اینترنت، ارائه شده است و باتوجه به گزارش گزارشگر ویژه در خصوص حق حریم خصوصی که در اجلاس سی و یکم حقوق بشر ارائه گردیده است؛

با در نظر گرفتن اهمیت کلیدی تعامل دولت با تمامی ذی‌نفعان مرتبط، از جمله جامعه مدنی، بخش خصوصی، جامعه فنی و دانشگاهی، در خصوص ارتقای و حفاظت حقوق بشر و آزادی‌های اساسی برخط؛

۱. تأیید می‌کند که همان حقوقی که مردم در حالت غیربرخط دارند باید در حالت برخط نیز محافظت شود، به‌ویژه آزادی بیان، که مطابق با ماده ۱۹ اعلامیه جهانی حقوق بشر و میثاق بین‌المللی حقوق سیاسی و مدنی، قطع نظر از مرزها و از طریق هر نوع رسانه به انتخاب خود فرد، قابل اجراست؛

۲. ماهیت باز و جهانی اینترنت را به‌عنوان یک نیروی محرکه و پیشران جهت تسریع پیشرفت به سوی توسعه اینترنت در شکل‌های مختلف، از جمله اتخاذ اهداف توسعه پایدار، به رسمیت می‌شناسد؛
۳. از تمامی دولت‌ها، درخواست می‌کند که همکاری بین‌المللی خود را با هدف توسعه رسانه و فناوری و امکانات اطلاعاتی و ارتباطاتی در تمامی کشورها ارتقای دهند و تسهیل نمایند

۴. تأیید می‌کند که کیفیت آموزش نقش قاطع و تعیین‌کننده‌ای در توسعه ایفا می‌کند و از این رو از تمامی دولت‌ها می‌خواهد که سواد دیجیتالی را ارتقای دهند و دسترسی به اطلاعات در اینترنت را که می‌تواند ابزار مهمی در تسهیل ارتقای حق آموزش باشد،

۵. همچنین اهمیت کاربرد رویکرد مبتنی بر حقوق بشر جامع در تأمین و توسعه دسترسی به اینترنت را تأیید می‌کند و از تمامی دولت‌ها می‌خواهد به‌منظور پر کردن و از بین بسیاری از اشکال شکاف دیجیتال تلاش نمایند؛

۶. از تمامی دولت‌ها می‌خواهد که شکاف دیجیتالی جنسیتی را از بین ببرند و استفاده از فناوری توانمندساز، به‌ویژه فناوری اطلاعات و ارتباطات را جهت ارتقای توانمندی تمامی زنان و دختران، افزایش دهد؛

۷. تمامی دولت‌ها را تشویق می‌کند که اقدامات مناسب برای ترویج مشارکت اشخاص ناتوان (معلول)، طراحی، توسعه، تولید و توزیع سیستم‌ها و فناوری اطلاعات و ارتباطات از جمله فناوری‌های کمک‌کننده (مفید) و سازگار که برای افراد ناتوان قابل دسترسی هستند، اتخاذ نمایند؛

۸. از تمامی دولت‌ها می‌خواهد که با نگرانی‌های امنیتی مربوط به اینترنت مطابق با تعهدات بین‌المللی حقوق بشری خود مقابله نمایند تا در خصوص از حفاظت از آزادی بیان، آزادی تجمع حریم خصوصی و سایر حقوق بشر برخط، اطمینان حاصل شود، از جمله از طریق مؤسسات ملی دموکراتیک، شفاف، مبتنی بر حاکمیت قانون، به نحوی که آزادی و امنیت اینترنت را تضمین کند به طوری که اینترنت بتواند به‌عنوان یک نیروی پویا به توسعه فرهنگی، اجتماعی و اقتصادی ادامه دهد؛

۹. با صراحت، کلیه موارد نقض و سوءاستفاده از حقوق بشر مثل شکنجه، اعدام‌های خارج از چارچوب قضایی، ناپدید شدن اجباری، بازداشت خودسرانه، تبعید، آزار و اذیت و ارباب، و نیز خشونت جنسیتی، ارتکاب علیه اشخاصی که از آزادی‌های اساسی و حقوق بشر خود در اینترنت استفاده می‌کنند را محکوم می‌کند. و از تمامی دولت‌ها تضمین جوابگویی و مسئولیت در این خصوص را درخواست می‌کند؛

۱۰. همچنین به‌طور صریح اقدامات عمدی در نقض قانون بین‌المللی حقوق بشر از طریق پیشگیری و یا مختل کردن دسترسی یا پخش اطلاعات برخط را محکوم می‌کند و از تمامی دولت‌ها درخواست می‌نماید که از چنین اقداماتی خودداری نمایند و آن را متوقف کنند؛

۱۱. بر اهمیت مبارزه با کینه‌ورزی (نفرت‌پراکنی)، که باعث انگیزه تبعیض یا خشونت در اینترنت می‌شود، از جمله از طریق ارتقای آستانه تحمل و ترویج گفتگو، تأکید می‌کند؛

۱۲. از همه دولت‌ها می‌خواهد تا از طریق فرایندهای شفاف و فراگیر با همه ذی‌نفعان، تدوین و تصویب سیاست‌های عمومی مرتبط با اینترنت ملی را در نظر بگیرند. سیاست‌هایی که اهدافی مثل دسترسی جهانی و برخورداری از حقوق بشر را در درون خود دارند؛

۱۳. از کمیساریای عالی حقوق بشر سازمان ملل تقاضا می‌کند، تا گزارشی در خصوص راه‌های رفع شکاف دیجیتالی جنسیتی با چشم‌انداز حقوق بشری در مشاوره با دولت‌ها، رویکردهای ویژه شورای حقوق بشر، سازمان‌های بین‌المللی، مؤسسات ملی حقوق بشر، جامعه مدنی، صنعت، دانشگاه‌ها و جامعه فنی و سایر ذی‌نفعان جهت ارائه در اجلاس سی‌وپنجم شورای حقوق بشر آماده کند؛

۱۴. تشویق می‌کند رویه‌های ویژه را برای این موضوعات در احکام موجود خود به صورت کاربردی در نظر بگیرند؛

۱۵. مطابق برنامه کاری خود، برای ادامه ملاحظاته‌ش در ارتقای، حفاظت و برخورداری از حقوق بشر، از جمله حق آزادی بیان، در اینترنت و سایر فناوری اطلاعات و ارتباطات و ادامه ملاحظاته‌ش در اینکه چگونه اینترنت می‌تواند ابزار مهمی برای پرورش شهروند و مشارکت جامعه مدنی جهت تحقق توسعه و بهرمندی حقوق بشر، در هر جامعه باشد، تصمیم می‌گیرد؛
نشست ۴۳ (۱ جولای ۲۰۱۶)
مصوب بدون رای گیری (اجماع)

بند چهار: قطعنامه حق حریم خصوصی در عصر دیجیتال ۲۰۱۵

ترجمه سند



مجمع عمومی
شورای حقوق بشر

تاریخ انتشار: ۱ آوریل ۲۰۱۵

شماره قطعنامه: A/HRC/RES/28/16

زبان: انگلیسی

شورای حقوق بشر

اجلاس بیست‌وهشتم

دستور کار ۳: ارتقای و حفاظت از تمامی حقوق بشر، حقوق مدنی، سیاسی، اقتصادی، اجتماعی و فرهنگی
از جمله حق توسعه قطعنامه مصوب شورای حقوق بشر
حق حریم خصوصی در عصر دیجیتال

شورای حقوق بشر؛

با هدایت اهداف و اصول منشور ملل متحد؛

با تأیید دوباره حقوق بشر و آزادی‌های اساسی مورد احترام در اعلامیه جهانی حقوق بشر و معاهدات بین‌المللی حقوق بشری مربوط، از جمله میثاق حقوق مدنی و سیاسی و میثاق بین‌المللی حقوق اقتصادی، اجتماعی و فرهنگی؛
با یادآوری اینکه تمامی ابعاد حقوق بشر و آزادی‌های اساسی، جهان‌شمول، تقسیم‌ناپذیر، وابسته به هم و دارای مناسبات مشترک می‌باشند؛
با تأیید دوباره اعلامیه وین و برنامه اقدام؛

با یادآوری قطعنامه‌های خود {به شماره‌های} ۵/۱ درباره تأسیس شورای حقوق بشر و ۵/۲ مورخ ۱۸ جولای ۲۰۰۷ در خصوص کردارنامه برای رویه‌های ویژه دارندگان حکم مأموریت شورا و با تأکید بر اینکه لغو و انفعال حکم دارنده مأموریت باید مطابق با آن قطعنامه‌ها و ضمیمه‌های آن باشند؛

همچنین با یادآوری قطعنامه‌های مجمع {به شماره‌های} ۶۸/۱۶۷ مورخ ۱۸ دسامبر ۲۰۱۳ و ۶۹/۱۶۶ مورخ ۱۸ دسامبر ۲۰۱۴ درباره حق حریم خصوصی در عصر دیجیتال و {با یادآوری}

تصمیم شورای حقوق بشر {به شماره} ۲۵/۱۱۷ مورخ ۲۷ مارس ۲۰۱۴ در خصوص پنل حق حریم خصوصی در عصر دیجیتال؛

با یادآوری بیشتر قطعنامه‌های خود {به شماره‌های} ۲۰/۸ مورخ ۵ جولای ۲۰۱۲ و ۲۶/۱۳ مورخ ۲۶ ژوئن ۲۰۱۴ درباره ارتقای، حفاظت و بهره‌مندی از حقوق بشر در اینترنت؛
با استقبال از عملکرد دفتر کمیساریای عالی ملل متحد برای حقوق بشر در زمینه حق حریم خصوصی در عصر دیجیتال و توجه توأم با علاقه به گزارش این دفتر در موضوع جاری (حاضر)، و با یادآوری جلسه مباحثه و مناظره که در مورد حق حریم خصوصی در عصر دیجیتال در خلال بیست و هفتمین جلسه شورای حقوق بشر برگزار شد؛

باتوجه به گزارش‌های گزارشگران ویژه درباره ارتقای و حفاظت از حقوق بشر و آزادی‌های اساسی در کنار مقابله با تروریسم و گزارش گزارشگر ویژه درباره ارتقای و حفاظت از حقوق بشر و حق آزادی عقیده و بیان؛

با توجه و قدردانی از نظریه عمومی شماره ۱۶ کمیته حقوق بشر درباره در مورد حق احترام به حریم خصوصی، خانواده، خانه و مکاتبات و حفظ حیثیت و شهرت افراد، در عین حال همچنین باتوجه به جهش‌های فناورانه گسترده‌ای که از زمان تصویب آن اتفاق افتاده است.

با یادآوری اینکه مجمع عمومی در قطعنامه خود به شماره ۶۹/۱۶۶، شورای حقوق بشر را تشویق نمود تا به‌طور فعال، برگزاری مباحثه درباره حق حریم خصوصی در عصر دیجیتال را با هدف شناسایی و شفاف‌سازی اصول، استانداردها و رویه‌های برتر درباره ارتقای و حفاظت حق حریم خصوصی حفظ نماید و در نظر گرفتن امکان ایجاد روشی ویژه برای نیل به این هدف؛

با به رسمیت شناختن نیاز به بحث و تجزیه و تحلیل بیشتر بر اساس حقوق بشر بین‌المللی موضوعات مرتبط با ارتقا و حفاظت از حریم خصوصی در عصر دیجیتال، پادمان‌های رویه‌ای نظارت و راه‌حل‌های مؤثر محلی، تأثیر نظارت بر حق حریم خصوصی و سایر حقوق بشری و همچنین نیاز به بررسی اصول غیر خودسرانگی و قانونی و مرتبط بودن ضرورت و تناسب ارزیابی‌ها در رابطه با شیوه‌های نظارت؛

با تأیید مجدد حق حریم خصوصی بشر {که} مطابق با {آن} حریم خصوصی، خانواده، خانه

و مکاتبات هیچ شخصی نباید در معرض مداخله خودسرانه یا غیرقانونی قرار گیرد، حق حفاظت قانونی در برابر چنین مداخله‌هایی {تأیید می‌شود} و با به رسمیت شناختن اینکه به‌کارگیری حق حریم خصوصی برای تحقق حق آزادی بیان و عقاید بدون مداخله و حق تجمع و اجتماع مسالمت‌آمیز مهم است و یکی از پایه‌های جامعه دموکراتیک می‌باشد؛

باتوجه به اینکه حرکت سریع توسعه فنی، افراد را در سراسر جهان قادر می‌سازد تا از فناوری‌های جدید ارتباطی و اطلاعاتی استفاده کنند و در عین حال ظرفیت حکومت‌ها، شرکت‌ها و اشخاص را برای نظارت، اختلال و جمع‌آوری اطلاعات افزایش می‌دهد که این امر می‌تواند حقوق بشر، مخصوصاً حق حریم خصوصی، را نقض یا مورد تعدی قرار دهد، موضوعی که در ماده ۱۲ اعلامیه حقوق بشر و ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی آمده است و بنابراین این موضوع یک نگرانی فزاینده است؛

همچنین باتوجه به اینکه، باوجود مزایایی که ابر داده‌ها می‌توانند فراهم کنند، انواع خاصی از ابر داده‌ها، زمانی که جمع می‌شوند، می‌توانند اطلاعات شخصی افراد را فاش کنند و همچنین می‌توانند رفتار افراد، روابط اجتماعی، اولویت‌های خصوصی و هویت فرد را ادراک کنند؛

با تأکید به اینکه دولت‌ها باید به تعهدات بین‌الملل حقوق بشری در رابطه با حق حریم خصوصی احترام بگذارند: هنگامی که آن‌ها ارتباطات دیجیتالی اشخاص را رصد می‌کنند، هنگام گردآوری داده‌های شخصی هنگام نیاز به افشای داده‌های شخصی از اشخاص ثالث از جمله داده‌های مربوط به شرکت‌های خصوصی؛

با یادآوری مسئولیت مؤسسات تجاری کسب‌وکار جهت احترام به حقوق بشر، موضوعی که در اصول راهنمای کسب‌وکار و حقوق بشر: اجرای چارچوب حفاظت، احترام و جبران ملل متحد آمده است؛

با نگرانی عمیق از امکان تأثیر منفی نظارت یا رهگیری ارتباطات، از جمله نظارت یا رهگیری ارتباطات فراسرزمینی، در به‌کارگیری و بهره‌مندی از حقوق بشر، و نیز جمع‌آوری داده‌های شخصی به‌ویژه در مقیاس وسیع؛

ضمن توجه توأم بانگرانی عمیق {در خصوص} اینکه در بسیاری از کشورها، اشخاص و سازمان‌های

درگیر در {موضوع} ارتقای و دفاع از حقوق بشر و آزادی‌های بنیادین {اساسی}، در نتیجه فعالیت‌های خود، مکرراً با تهدیدات و آزار و اذیت، رنج از ناامنی و نیز مداخله خودسرانه و غیر قانونی درباره حقوق حریم خصوصی خود روبه‌رو هستند؛

باتوجه به این موضوع که نگرانی‌ها درباره امنیت عمومی، ممکن است گردآوری و حفاظت از اطلاعات حساس خاصی را توجیه نماید، دولت‌ها باید تضمین نمایند که تعهدات خود تحت حقوق بین‌المللی بشر را کاملاً رعایت نمایند؛

در ارتباط با {موضوع قبل} ضمن توجه بیشتر به اینکه پیشگیری و سرکوب تروریسم یک منفعت عمومی با {درجه} اهمیت زیاد می‌باشد، در عین حال مجدداً تأیید می‌نماییم که دولت‌ها باید تضمین نمایند که هر اقدامی را جهت مبارزه با تروریسم اتخاذ می‌نمایند باید مطابق با تعهدات خود تحت حقوق بین‌الملل باشد به‌ویژه حقوق بشر، حقوق پناهندگان و حقوق بشر دوستانه .
۱. مجدداً حق حریم خصوصی را تأیید می‌نماید {باین موضوع} که حریم خصوصی، خانوادگی، منزل یا مکاتبات هیچکس نباید دستخوش مداخله خودسرانه یا غیرقانونی قرار گیرد، و {همچنین مجدداً} حقوق مربوط به حفاظت قانون در مقابله با چنین مداخله‌ای را {تأیید می‌نماید} وفق حقوق مصرح که در ماده ۱۲ اعلامیه جهانی حقوق بشر و ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی؛

۲. ماهیت جهانی و آزاد اینترنت به‌عنوان نیروی پیشران در فناوری اطلاعات و ارتباطات، جهت تسریع پیشرفت به سوی اشکال مختلف توسعه را به رسمیت می‌شناسد؛

۳. تأیید می‌کند که همان حقوقی که مردم در فضای غیربرخط دارند باید در فضای برخط نیز محافظت گردد از جمله حقوق مربوط به حریم خصوصی؛

۴. تصمیم می‌گیرد برای دوره سه ساله، گزارشگر ویژه‌ای را درباره حق حریم خصوصی با وظایف {زیر} منصوب نماید؛

أ. گردآوری اطلاعات مرتبط از جمله {اطلاعاتی} درباره چارچوب‌های ملی و بین‌المللی، رویه‌ها و تجارب ملی جهت بررسی روندها، تحولات و چالش‌ها در رابطه با حق حریم خصوصی و طرح پیشنهادهایی برای تضمین ارتقای و حفاظت از آن، از جمله در رابطه با چالش‌های ناشی

از فناوری‌های جدید؛

ب. ضمن اجتناب از دوباره کاری، جستجو، دریافت و پاسخ {واکنش} به اطلاعات، از: دولت‌ها، سازمان ملل و سازمان‌های {مرتبط با} آن، برنامه‌ها، هزینه‌ها، سازوکارهای منطقه‌ای درباره حقوق بشر، مؤسسات ملی حقوق بشر، سازمان‌های جامعه مدنی، بخش خصوصی از جمله مؤسسات تجاری کسب‌وکار و سایر بخشها و ذی‌نفعان مرتبط؛

ج. شناسایی موانع احتمالی در زمینه ارتقای و حفاظت از حق حریم خصوصی، شناسایی، تبادل و ارتقای اصول و رویه‌های برتر در سطوح ملی، منطقه‌ای و بین‌المللی و ارائه پیشنهادها و توصیه‌ها به شورای حقوق بشر در این رابطه، از جمله با نگاهی به چالش‌های ویژه ناشی از عصر دیجیتال؛
د. مشارکت و همکاری در کنفرانس‌های بین‌المللی مرتبط و رخدادهایی {که} با هدف ارتقای رویکردهای نظام‌مند و منسجم درباره موضوعات مندرج در حکم {خود بر گزار می‌گردد}؛

ه. رشد و بالا بردن آگاهی در باب اهمیت ارتقای و حفاظت از حق حریم خصوصی از جمله با نگاهی به چالش‌های ویژه ناشی عصر دیجیتال، اهمیت تأمین دسترسی به جبران مؤثر در خصوص اشخاصی که حق حریم خصوصی آن‌ها نقض گردیده است وفق تعهدات حقوق بین‌المللی بشر؛
و. توأم نمودن منظر و نگاه جنسیتی در سراسر عملکرد حکم و تعهد {خود}؛

ز. ارائه گزارشی از تخلفات ادعایی در خصوص نقض حریم خصوصی که ممکن است در هر کجای دنیا رخ دهند، همانگونه که در ماده ۱۲ اعلامیه جهانی حقوق بشر و ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی آمده است، از جمله {نقض حریم خصوصی} در ارتباط با چالش‌های ناشی از فناوری‌های جدید، {هدف از ارائه این گزارش} جلب توجه و نظر شورا و کمیساریای عالی حقوق بشر سازمان ملل به وضعیت‌های ویژه و جدی مرتبط با موضوع می‌باشد؛

ح. آغاز ارائه گزارش سالانه در سی‌ویکمین نشست شورای حقوق بشر و هفتادویکمین

نشست مجمع عمومی؛

۵. از گزارشگر ویژه دعوت می‌نماید تا در اولین گزارش خود، جهت پرداختن به حق حریم

خصوصی در عصر دیجیتال، ملاحظاتی را در باب یافته‌های مرتبط با مأموریت بگنجاند؛

۶. از تمامی دولت‌ها دعوت می‌نماید که همکاری کاملی با گزارشگر ویژه در خصوص انجام

مأموریتش داشته باشند و او را یاری نمایند از جمله از طریق تأمین تمامی نیازهای اطلاعاتی مورد درخواست او، به درخواست‌ها و سایر ارتباطات مبرم او پاسخ فوری دهند. به درخواست‌های مأمور (گزارشگر ویژه) جهت بازدید از کشورها به طور مطلوب رسیدگی نمایند. به اجرای توصیه‌ها (پیشنهادها) ارائه شده در گزارش گزارشگر ویژه توجه نمایند؛

۷. تمامی ذی نفعان مرتبط از جمله سازمان ملل متحد و سازمان‌های آن، برنامه‌ها، تأمین مالی، سازوکارهای منطقه‌ای درباره حقوق بشر، مؤسسات ملی حقوق بشر، سازمان‌های جامعه مدنی و بخش خصوصی را تشویق می‌نماید تا به طور کامل با گزارشگر ویژه جهت انجام مأموریت خود همکاری نمایند؛

۸. از دبیرکل و کمیساری عالی {حقوق بشر} می‌خواهد تا تمامی منابع مالی لازم را برای گزارشگر ویژه جهت انجام {و تکمیل} مأموریت {خود} مهیا نماید؛

۹. تصمیم می‌گیرد ملاحظاته‌اش راجع به موضوع را زیر همان عنوان دستور کار ادامه دهد.

بند پنجم: قطعنامه نقش آزادی عقیده و بیان در توانمندسازی زنان سال ۲۰۱۳

ترجمه سند



مجمع عمومی
شورای حقوق بشر

تاریخ انتشار: ۲۴ ژوئن ۲۰۱۳

شماره قطعنامه: A/HRC/RES/ 23/2

زبان: انگلیسی

توزیع: عمومی

اجلاس بیست و سوم

دستور کار ۳

ارتقای و حفاظت از کلیه حقوق بشر، حقوق مدنی، سیاسی، اقتصادی، اجتماعی و فرهنگی از جمله حق توسعه قطعنامه مصوب شورای حقوق بشر ۲۳/۲. نقش آزادی عقیده و بیان در توانمندسازی زنان

شورای حقوق بشر

با یادآوری اعلامیه جهانی حقوق بشر و معاهدات بین‌المللی مرتبط با حقوق بشر، از جمله میثاق بین‌المللی حقوق مدنی و سیاسی، میثاق بین‌المللی حقوق اقتصادی، اجتماعی و فرهنگی و کنوانسیون رفع تمام اشکال تبعیض علیه زنان؛

همچنین با یادآوری اعلامیه وین و برنامه اقدام مصوب ۲۵ ژوئن ۱۹۹۳ توسط کنفرانس جهانی حقوق بشر و اعلامیه پکن و خط‌مشی اقدام مصوب ۱۵ سپتامبر ۱۹۹۵ توسط چهارمین کنفرانس جهانی زن و بازنگریهای بعدی آن؛

با در نظر داشتن اینکه کنوانسیون رفع تمام اشکال تبعیض علیه زنان، حقوق بشر و آزادی‌های اساسی و برابری زنان در سراسر جهان را تأیید می‌کند، دولت‌ها، از جمله دولت‌های عضو باید کلیه اقدامات مناسب جهت رفع تبعیض علیه زنان را در حیات عمومی و سیاسی کشور اتخاذ کند، با یادآوری قطعنامه شورای حقوق بشر (۱۲/۱۶) به تاریخ ۲ اکتبر ۲۰۰۹؛

همچنین با یادآوری قطعنامه شورای حقوق بشر (۱۶/۴) به تاریخ ۲۴ مارس ۲۰۱۱ و کلیه قطعنامه‌های قبلی کمیسیون حقوق بشر و شورا درباره حق آزادی عقیده و بیان، از جمله قطعنامه ۲۰/۸ به تاریخ ۵ جولای ۲۰۱۲ درباره ارتقای، حفاظت و برخورداری از حقوق بشر در اینترنت؛

با یادآوری بیشتر قطعنامه‌های مجمع عمومی در ارتباط با موضوع توانمندسازی زنان، از جمله قطعنامه ۶۶/۱۳۰ به تاریخ ۱۹ دسامبر ۲۰۱۱ در زمینه زنان و مشارکت سیاسی و قطعنامه ۶۶/۲۱۶ به تاریخ ۲۲ دسامبر ۲۰۱۱ در زمینه زنان در توسعه و نتایج توافق شده در کمیسیون جایگاه زنان؛

با تأیید مجدد مفاد ۱۹ اعلامیه جهانی حقوق بشر و میثاق بین‌المللی حقوق مدنی و سیاسی، همچنین با تأیید مجدد اینکه زنان و مردان بر پایه مساوات حق برخورداری از کلیه حقوق بشر و آزادی‌های اساسی خود را دارند؛

با به رسمیت شناختن اینکه بهره‌مند شدن مؤثر از حق آزادی عقیده و بیان که در میثاق بین‌المللی حقوق مدنی و سیاسی و اعلامیه جهانی حقوق بشر گرامی داشته شده است، جهت برخورداری از سایر حقوق و آزادی‌های بشر ضروری می‌باشد و یک رکن بنیادین برای ساختن جامعه دموکراتیک و تقویت‌کننده دموکراسی می‌باشد، با در نظر گرفتن اینکه کلیه حقوق بشر جهانی، تقسیم‌ناپذیر، به هم وابسته و دارای روابط متقابل هستند؛

همچنین با به رسمیت شناختن اینکه چگونه پیشرفت‌ها در فناوری‌های اطلاعات و ارتباطات، زنان را برای شروع یا گسترش مشارکتشان در حیات سیاسی، اقتصادی، فرهنگی و اجتماعی توانمند کرده است؛

علاوه بر این با به رسمیت شناختن همکاری‌های مهم که زنان در راستای نیل به برقراری یک دولت نماینده‌محور، شفاف و پاسخگو در بسیاری از کشورها انجام داده‌اند؛

با اذعان به نقش مهم روزنامه نگاران زن و زنان مدافع حقوق بشر در بهرمنند شدن، ارتقای و حفاظت از حق آزادی عقیده و بیان و در این چارچوب، ابراز نگرانی در مورد خطرهایی که این زنان در انجام کارهای خود با آن‌ها مواجه می‌شوند؛

با تأکید بر اهمیت حیاتی مشارکت سیاسی زنان در تمامی زمینه‌ها، از جمله زمان صلح و جنگ و در کلیه مراحل انتقال سیاسی، نگرانی در مورد اینکه هنوز موانع بسیاری از شرکت زنان دارای شرایط مساوی با مردان در حیات سیاسی جلوگیری می‌کند و باتوجه به این نکته که شرایط انتقال سیاسی ممکن است یک فرصت منحصر به فرد برای مقابله با چنین موانعی فراهم کند؛

با به رسمیت شناختن ادامه همکاری ضروری که زنان سرتاسر جهان در دستیابی و حفظ صلح و امنیت بین‌المللی و تحقق کامل حقوق بشر، برای ارتقای دموکراسی، توسعه پایدار و رشد اقتصادی و ریشه‌کن کردن فقر، گرسنگی و بیماری انجام می‌دهند؛

با نگرانی شدید در خصوص اینکه که زنان در جهان، از جمله زنان متعلق به اقلیت‌های نژادی، قومی، مذهبی یا زبانی و زنان بومی، اغلب در نتیجه تبعیض، دسترسی نابرابر به آموزش، فقدان دسترسی به خدمات درمانی، تأثیر نامتناسب فقر روی زنان و خشونت علیه زنان و دختران همچنان از حوزه‌های سیاسی، اقتصادی، فرهنگی و اجتماعی به حاشیه رانده می‌شوند:

۱. با تأیید نقش اساسی که آزادی عقیده و بیان در توانمندی زنان در تعامل با کل جامعه ایفا می‌کند، به‌ویژه در مشارکت در حوزه‌های اقتصادی و سیاسی و با تأیید مجدد اینکه مشارکت فعال زنان با شرایط مساوی با مردان، در تمامی سطوح تصمیم‌سازی، جهت دستیابی به برابری، توسعه پایدار، صلح و دموکراسی ضروری می‌باشد؛

۲. با ابراز نگرانی عمیق از تبعیض، ارباب، آزار و خشونت، از جمله در فضاهای سیاسی، اغلب زنان و دختران را از برخورداری کامل از حقوق بشر و آزادی‌های اساسی‌شان، از جمله حق آزادی آن‌ها در عقیده و بیان، باز می‌دارد که این امر از مشارکت کامل آن‌ها در امور اقتصادی، اجتماعی، فرهنگی، سیاسی ممانعت به‌عمل می‌آورد؛

۳. از تمامی دولت‌ها درخواست می‌کند:

أ. ارتقای احترام و اطمینان از برخورداری زنان از آزادی عقیده و بیان، در هر دو حالت

برخط و غیربرخط، از جمله به‌عنوان اعضای سازمان‌های غیردولتی و سایر انجمن‌ها؛

ب. اطمینان از اینکه زنان و دختران در برخورداری از حق آزادی عقیده و بیان مورد تبعیض

واقع نشده‌اند، به‌ویژه در استخدام، مسکن، سیستم دادگستری، خدمات اجتماعی و آموزش؛

ج. تسهیل مشارکت کامل، برابر و مؤثر و ارتباط آزاد کلیه زنان در تمامی سطوح تصمیم

سازی در جوامعشان و در نهادهای ملی، منطقه‌ای و بین‌المللی از جمله در سازوکارهایی جهت پیشگیری، مدیریت و حل و فصل درگیری‌ها (مخاصمات)؛

د. تسهیل مشارکت برابر در دسترسی و استفاده از اطلاعات و فناوری‌های ارتباطات مانند

اینترنت، به کارگیری دیدگاه جنسیتی و تشویق همکاری‌های بین‌المللی با هدف توسعه رسانه و تجهیزات اطلاعات و ارتباطات در تمامی کشورها؛

هـ تأمین دسترسی زنان و دختران به دادرسی مؤثر در قبال نقض حقوق آن‌ها در آزادی عقیده و بیان و اطمینان از اینکه هیچ مصونیتی برای خشونت بر مبنای جنسیت وجود ندارد، از جمله استفاده از خشونت جنسی برای مرعوب کردن زنان و دخترانی که در حال استفاده از حق آزادی عقیده و بیان هستند؛

۴. از گزارشگر ویژه در امور ارتقای و حفاظت از حق آزادی عقیده و بیان دعوت می‌شود تحلیلی از نقش آزادی عقیده و بیان در بهبود مشارکت زنان در حیات سیاسی، اجتماعی، فرهنگی و اقتصادی و در پیشبرد برابری جنسیتی و نیز تحلیل چالش‌هایی که زنان در به کارگیری آزادی عقیده و بیانشان با آن‌ها مواجه هستند در گزارش‌های خود قرار دهد.

مصوب بدون رای مخالف (اجماع)

نشست سی‌وهشتم (۱۳ ژوئن ۲۰۱۳)

بندش: قطعنامه حقوق کودک؛ فناوری اطلاعات و ارتباطات و استثمار جنسی کودکان سال ۲۰۱۶

ترجمه سند



مجمع عمومی
شورای حقوق بشر

تاریخ انتشار: ۲۶ آوریل ۲۰۱۶

شماره قطعنامه: A/HRC/RES/ 31/7

زبان: انگلیسی

توزیع: عمومی

اجلاس سی و یکم

دستور کار ۳

قطعنامه مصوب شورای حقوق بشر در ۲۳ مارس ۲۰۱۶
حقوق کودک: فناوری‌های اطلاعات و ارتباطات و استثمار جنسی کودک

شورای حقوق بشر؛

با تأکید بر اینکه کنوانسیون حقوق کودک، استاندارد در ارتقای و حفاظت از حقوق کودک را تأسیس کرد، با در نظر داشتن اهمیت پروتکل‌های اختیاری در کنوانسیون و تقاضا جهت تصویب جهانی و اجرای مؤثر آن‌ها و سایر اسناد مربوط به حقوق بشر؛

با یادآوری تمامی قطعنامه‌های پیشین حقوق کودک، مصوب کمیسیون حقوق بشر، شورای حقوق بشر و مجمع عمومی، آخرین قطعنامه موجود شورا ۲۸/۱۹ به تاریخ ۲۷ مارس ۲۰۱۵ و قطعنامه مجمع ۷۰/۱۳۷ تاریخ ۱۷ دسامبر ۲۰۱۵؛

با استقبال از عملکرد کمیته حقوق کودک در موضوع فناوری‌های اطلاعات و ارتباطات و استثمار جنسی کودک، از جمله در محتوای نظرهای عمومی اش، به‌ویژه نظرهای عمومی شماره ۱۳ (۲۰۱۱) درباره حق کودک در آزادی از تمامی اشکال خشونت و شماره ۱۶ (۲۰۱۳) درباره تعهدات دولت در خصوص تأثیر بخش تجارت روی حقوق کودکان؛

همچنین با استقبال از عملکرد گزارشگر ویژه درباره فروش کودکان، فحشاء و پورنوگرافی (جنسی اینترنتی) کودک و عملکرد نماینده ویژه دبیرکل در خصوص خشونت علیه کودکان، در فرصت‌ها و خطرهای مرتبط با استفاده از فناوری اطلاعات و ارتباطات و حفاظت کودکان از سوءاستفاده و استثمار جنسی و عملکرد (نماینده ویژه دبیرکل) در خصوص کودکان و مخاصمات

مسلحانه و توجه توأم با قدردانی از گزارش‌های اخیر آن‌ها؛

علاوه بر این با استقبال از تصویب دستورکار توسعه پایدار توسط مجمع عمومی؛
با تأکید بر اهمیت اجرای اطمینان بخش آن در برخورداری حقوق کودک، و با یادآوری اینکه
هدف قطعنامه ۵,۲ رفع تمامی اشکال خشونت علیه کلیه زنان و دختران در حوزه‌های عمومی و
خصوصی، از جمله قاچاق و استثمار جنسی و انواع دیگر را شامل می‌شود، و هدف ۱۶,۲ پایان یافتن
سوءاستفاده، استثمار، قاچاق و تمامی اشکال خشونت علیه کودکان و شکنجه آن‌ها را در بر می‌گیرد؛
با به رسمیت شناختن اهمیت فناوری‌های اطلاعات و ارتباطات در زندگی‌های کودکان
به‌عنوان یک ابزار جدید جهت یادگیری، اجتماعی شدن، بیان، شمولیت و تکامل حقوق کودک
و آزادی‌های اساسی از قبیل حق آموزش، حق آزادی بیان، آزادی جستجو، دریافت و ارسال
اطلاعات و حق بیان آزادانه دیدگاه‌های خود؛

با تأیید مجدد مسئولیت‌ها، حقوق و وظایف والدین، سرپرست‌های قانونی یا سایر اشخاصی
که مسئولیت قانونی تأمین و تدارک کودک، متناسب با ظرفیت‌های در حال رشد و نمو او را بر
عهده دارند، هدایت و راهنمایی مناسب در بهره‌مندی کودک از حقوق خود؛
با به رسمیت شناختن اینکه کودکان از جمله فعال‌ترین مشارکت‌کنندگان بر خط می‌باشند
و والدین، سرپرستان، آموزش‌دهندگان که مسئولتی در قبال فعالیت‌های کودکان دارند ممکن
است جهت حفاظت از کودکان بر خط به راهنمایی نیاز داشته باشند؛

با تأیید مجدد اینکه دولت‌ها باید جهت حفاظت کودک از تمامی اشکال استثمار و سوءاستفاده
جنسی متعهد شوند و بدین منظور، به‌ویژه، اتخاذ کلیه اقدامات ملی، دوجانبه و چندجانبه مناسب
جهت جلوگیری از جذب یا اجبار کودک برای به‌کارگیری در هرگونه فعالیت جنسی غیرقانونی،
استفاده استثماری از کودکان در فحشاء یا سایر شیوه‌های جنسی غیرقانونی و استفاده استثماری
از کودکان در انجام پورنوگرافی و ابزار و امور آن؛

با به رسمیت شناختن اینکه فناوری‌های اطلاعات و ارتباطات می‌تواند ارتکاب فعالیت‌های
مجرمانه همراه با مصنویت را در خصوص فروش، سوءاستفاده جنسی و استثمار کودکان، از جمله
در پورنوگرافی، مواد سوءاستفاده جنسی از کودک و فحشاء تسهیل نماید، تهدیدات یا اشکال جدید

سوءاستفاده جنسی و استثمار، از قبیل درخواست از کودکان جهت اهداف جنسی باعنوان واداشتن کودک به اعمال جنسی «اغفال جنسی یا گرومینگ کودکان»، اخاذی جنسی، سوءاستفاده کودک در برنامه زنده، مالکیت، توزیع، دسترسی، مبادله، تولید یا پرداخت مواد سوءاستفاده جنسی کودک، و تماشا، هدایت یا تسهیل مشارکت کودکان در سوءاستفاده‌های جنسی زنده - در میان انواع دیگر - شناخته شدند؛

با ابراز نگرانی عمیق از خطرهایی همچون میزان پیامک‌های جنسی و ارسال تصاویر برهنه به وسیله تلفن همراه (سکستینگ) و میزان موالید نامشروع به واسطه اشکال جدید و منتج از خشونت علیه کودکان، به‌ویژه سوءاستفاده جنسی و استثمار کودک و از طریق زورگویی سایبری (قدری اینترنتی) که به استفاده از فناوری‌های اطلاعات و ارتباطات مرتبط می‌باشند؛ با اذعان به نقشی که فناوری‌های اطلاعات و ارتباطات در کاهش خطر استثمار و سوءاستفاده جنسی از جمله از طریق توانمندسازی کودکان جهت ارائه گزارش چنین سوءاستفاده‌هایی بازی می‌کنند؛

با به رسمیت شناختن اینکه دولت‌ها باید دسترسی به رسانه دیجیتال و فناوری‌های ارتباطات و اطلاعات را ضمن حفاظت کودکان از آسیب ارتقای دهند؛ با تأکید بر اینکه دولت‌ها مسئولیت عمده‌ای در احترام، پاسداشت و اجرای کامل حقوق کودک، از جمله از طریق پیشگیری از نقض‌ها، حفاظت و فراهم کردن درمان‌های مؤثر برای قربانیان و مقابله با تمامی اشکال خشونت و سوءاستفاده علیه کودکان، از جمله سوءاستفاده و استثمار جنسی، در هر زمان و در تمام زمینه‌ها را دارند؛

با تأکید بر اینکه سوءاستفاده و استثمار جنسی کودک از طریق فناوری‌های اطلاعات و ارتباطات - از جمله برخط - شامل تولید، فروش، انتشار یا مالکیت مواد سوءاستفاده و استثمار جنسی کودک - از جمله پورنوگرافی کودک - می‌شود خشونت یا سوءاستفاده جدی از کل وجود جسمی و روانی کودک و شأن انسانی و استفاده غیرقانونی از داده شخصی کودک قربانی را باعث می‌شود و اینکه می‌تواند یک تأثیر منفی روی برخورداری حق کودک از محافظت قانونی در مقابل مداخله غیرقانونی یا خودسرانه در ارتباط با حریم خصوصی خود داشته باشد؛

با تأیید مجدد اینکه کودک جهت توسعه کامل و هماهنگ شخصیت خود باید در محیط خانواده رشد کند، بهترین منافع کودک باید اصول راهنمایی باشد برای کسانی که مسئولان تربیت کودکان و حفاظت از آنها هستند و اینکه باید توانایی‌های خانواده‌ها و سرپرستان جهت تأمین مراقبت و محیط ایمن برای کودک ارتقای داده شود؛

با به رسمیت شناختن اینکه گاهی اوقات مرتکبان سوءاستفاده و استثمار جنسی کودک به شکل برخط مراقبان مستقیم کودک هستند و اینکه اعضاء خانواده، جوامع و همسایگان ممکن است در عرضه کودکان به منظور سوءاستفاده و استثمار جنسی از طریق فناوری‌های اطلاعات و ارتباطات درگیر شوند؛

با یادآوری این نکته که کشورها باید تمامی اقدامات قانونگذاری، اجرایی، اجتماعی و آموزشی مناسب جهت حفاظت کودک از تمامی اشکال خشونت روحی و فیزیکی، آسیب یا سوءاستفاده، رفتار بی دقت و غفلت، بدرفتاری، استثمار و سوءاستفاده جنسی را به کار گیرند تا مادامی که تحت مراقبت خانواده‌های خود، قیم قانونی یا شخص دیگری که مراقب کودک است، می‌باشند؛ با به رسمیت شناختن اینکه مسئولیت برای احترام به حقوق کودک همچنین شامل بازیگران و عوامل خصوصی و شرکت‌های تجاری و به‌ویژه بازیگران خصوصی در صنعت اینترنت که خدمات را در سرتاسر حوزه‌های داخلی فراهم می‌کنند، می‌باشد، باید به سهیم شدن در تلاش‌های بین‌المللی مشترک جهت بالا بردن آگاهی و قدرت کودکان درباره خطرهای برخط و برای پیشگیری و مقابله با سوءاستفاده و استثمار جنسی کودک به شکل برخط و غیربرخط ادامه دهند؛

با عنایت به تلاش‌های انجام شده توسط بازیگران خصوصی در چارچوب مسئولیت اجتماعی همگانی برای حصول اطمینان از اینکه زیرساخت‌ها و خدمات آنها برای اهداف مجرمانه استفاده نمی‌شود و همکاری کامل در تلاش‌های مرتبط با شناسایی، گزارش، تحقیق، پیگرد قانونی و پیشگیری از سوءاستفاده و استثمار جنسی کودک به شکل برخط و غیربرخط؛

با به رسمیت شناختن اهمیت پیشگیری در تضمین یک محیط ایمن برخط و فناوری‌های اطلاعات و ارتباطات برای کودکان در عین حفاظت از حقوق کودک از طریق مورد حمایت قانون

بودن کودک در مقابل مداخله خودسرانه یا غیرقانونی به حریم خصوصی او، جستجو، دریافت یا افشای اطلاعات، آموزش، آزادی بیان و مشارکت و همچنین با به رسمیت شناختن اینکه اقدامات و رویکردهای پیشگیرانه باید شامل عوامل و بازیگران اصلی و کلیدی از جمله دولت‌ها، جامعه مدنی، صنعت، والدین، مدارس، کودکان و کل اجتماع باشد؛

با ابراز نگرانی در ارتباط با وضعیت ناشی از امتناع بازیگران خصوصی از انجام اقدامات مورد نیاز تحت قانون ملی و بین‌المللی جهت فراهم نمودن پادمان‌های کافی به منظور پیشگیری از سوءاستفاده و استثمار جنسی کودک، و در این راستا با تأکید بر بیشترین اهمیت به اقامه و اجرای عدالت در مورد همه کسانی که در استثمار یا سوءاستفاده جنسی کودکان در فضای برخط درگیر بوده‌اند یا آن را تسهیل کرده‌اند، باید به پیشگاه عدالت یا همان دادگاه آورده شوند؛

با به رسمیت شناختن ماهیت چند صلاحیتی و فراملی سوءاستفاده و استثمار جنسی کودک به صورت برخط و از طریق فناوری‌های اطلاعات و ارتباطات، ضعف و عدم بسندگی مدارک الکترونیکی چنین جرائمی و بروزسانی پیوسته فناوری توسط مرتکبان جهت جلوگیری از تشخیص و تحقیق که مشکلات متعددی را برای مساعدت حقوقی متقابل در شکل سنتی و مرسوم آن و کانال‌های همکاری ایجاد کرده است و نیازمند به همکاری بین‌المللی فعال بین بازیگران مختلف، از جمله دولت‌ها و نیروی پلیس و نهادهای قضایی و بازیگران خصوصی، از جمله در مورد تشخیص جرائم، گزارش‌دهی آن‌ها به مراجع ذیصلاح جهت تحقیق، حفاظت از مدارک الکترونیکی جرائم و تحویل بموقع آن به مقامات می‌باشند؛

با استقبال از حرکت مجدد در مبارزه جهانی علیه سوءاستفاده و استثمار کودک که توسط ابتکارات بین‌المللی چندذی‌نفعی مربوط، با مشارکت دولت‌ها ایجاد گردید، از جمله نیروی پلیس و مراجع قضایی، بازیگران خصوصی، مؤسسات تجاری و جامعه مدنی - همانند برنامه جهانی مقابله با جرم سایبری دفتر مبارزه با جرم و مواد مخدر سازمان ملل، ابتکار حفاظت برخط کودک در اتحادیه بین‌المللی مخابرات، اتحاد جهانی علیه سوءاستفاده جنسی برخط کودک، اتحادیه جهانی «ما محافظت می‌کنیم»، و گروه اقدام دنیای مجازی و جلسه سطح بالا مجمع عمومی درخصوص بازنگری کلی اجرای نتایج اجلاس سران درباره جامعه اطلاعاتی ترویج کرده است

و با تشویق بیشتر هماهنگی میان ابتکارات آن‌ها و انتشار اطلاعات مربوط به فعالیت آن‌ها؛ با قدردانی از ابتکارات بین‌المللی، منطقه‌ای و محلی و تلاش‌های انجام شده جهت پیشگیری و مقابله با تهدید سوءاستفاده و استثمار جنسی برخط کودک و پیامدهای مؤثر وابسته به آن در برخورداری کامل کودکان از حقوق بشر و ستودن نقش اتحادیه بین‌المللی مخابرات و گروه کاری آن در زمینه حفاظت برخط کودک در مبارزه با استثمار و سوءاستفاده جنسی برخط کودکان: ۱. با توجه توأم با قدردانی از گزارش نماینده کمیساریای عالی حقوق بشر سازمان ملل با عنوان «فناوری اطلاعات و ارتباطات و استثمار جنسی کودک»؛

۲. پافشاری دولت‌ها در برداشتن تمامی گام‌های لازم جهت حصول اطمینان از دسترسی کامل، برابر، فراگیر و ایمن بدون هیچ نوع تبعیض تمامی کودکان به فناوری‌های اطلاعات و ارتباطات و تأمین حفاظت کودکان برخط و غیربرخط از طریق یک رویکرد یکپارچه و چندوجهی برمبنای حقوق و رفاه کودکان؛

۳. با قوی‌ترین عبارات ممکن تمام اشکال خشونت علیه کودکان، از جمله خشونت جنسی و جنسیتی را محکوم می‌کند از جمله در مواردی که ارتکاب از طریق یا در نتیجه سوءاستفاده مجرمانه از وسیله فناوری‌های اطلاعات و ارتباطات موجود در اینترنت و استثمار برخط جنسی برخط کودکان صورت گرفته باشد؛

۴. از همه دولت‌ها می‌خواهد تا از حفاظت قانونی کودکان از سوءاستفاده و استثمار برخط اطمینان حاصل کنند و یک تعریف قانونی مطابق با حقوق و تعهدات بین‌المللی حقوق بشر ارائه کنند، تمامی رفتارهای مرتبط با استثمار جنسی برخط و غیربرخط کودکان را جرم‌انگاری کنند. از جمله - اما به جدیدترین اشکال محدود نمی‌شود- از قبیل درخواست از کودکان برای اهداف جنسی و اغفال جنسی آن‌ها که به گرومینگ کودکان موسوم است، اخاذی جنسی، جریان‌سازی برای سوءاستفاده از کودکان و مالکیت یا توزیع، دسترسی یا تبادل یا تولید یا پرداخت برای مواد سوءاستفاده جنسی کودک و تماشای آن، هدایت یا تسهیل مشارکت کودکان در سوءاستفاده‌های جنسی زنده که از طریق فناوری‌های ارتباطات و اطلاعات ارسال می‌شود. در حین حصول اطمینان از اینکه قانونگذاری آن‌ها، تحولات و پیشرفت‌های احتمالی آتی در شیوه عمل مربوط به

۵. سوءاستفاده و استثمار جنسی برخط کودک را در نظر می‌گیرد؛ {آینده نگری در تدوین قانون}؛ همچنین از دولت‌ها می‌خواهد تا اطمینان یابند که زنجیره کامل از کسانی که در ارتکاب به چنین فعالیت‌های مجرمانه درگیرند یا در صدد ارتکاب به چنین جرائمی هستند، جوابگو و مسئول هستند و به‌منظور مقابله با اعطای مصونیت به آن‌ها، به پیشگاه عدالت آورده می‌شوند، با در نظر گرفتن ماهیت چند صلاحیتی و فراملی استثمار و سوءاستفاده جنسی برخط کودک از طریق فناوری‌های اطلاعات و ارتباطات؛

۶. علاوه بر این از دولت‌ها می‌خواهد تا اطمینان حاصل کنند از اینکه تدوین قانون داخلی درباره حریم خصوصی و حفاظت داده‌ها مطابق با قانون بین‌الملل حقوق بشر است و اجازه اجرای قانون، رفاه اجتماعی، انجام تحقیقات مؤثر و مناسب توسط مراجع ذی‌صلاح قضایی جهت مبارزه با نقض‌های حق کودک قربانی در حریم خصوصی را می‌دهد، بر طبق آن هیچ‌کس نباید در معرض مداخله غیرقانونی یا خودسرانه درباره حریم خصوصی، خانواده، خانه یا مکاتباتش باشد و حق حفاظت از قانون علیه چنین مداخله‌هایی را همانند آنچه در ماده ۱۲ اعلامیه جهانی حقوق بشر و ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی درباره استثمار جنسی برخط و غیربرخط کودک و جهت بالابردن آگاهی درباره اهمیت فعالیت‌ها و تبعیت از قانون توسط بازیگران خصوصی، به‌طور برجسته بازیگران خصوصی صنعت اینترنت برای تقویت تلاش‌های خود نشان می‌دهد، را می‌دهد؛

۷. از دولت‌ها می‌خواهد از طریق همکاری فزاینده بین سازمان‌های دولتی مرتبط، در خصوص رفع موانع تحقیقات و پیگردهای قانونی مؤثر مربوط به استثمار و سوءاستفاده جنسی از کودکان برخط و غیربرخط توسط نیروی پلیس و مقامات قضایی ذی‌صلاح از طریق تسهیل دسترسی به مدارک جرائم ارتكابی در داخل مرزها اقدام کند، از جمله شهادت شهود و اطلاعات الکترونیکی که توسط تأمین‌کنندگان خدمات اینترنت و بسترهای برخط ذخیره شده است و تأکید می‌کند که بازیگران خصوصی باید از اقدامات نیروی پلیس در این ارتباط پیروی و تبعیت کنند؛

۸. همچنین از دولت‌ها خواستار تضمین یک محیط حقوقی و مقرراتی شفاف و قابل پیش‌بینی است که برای احترام گذاشتن به فناوری اطلاعات و ارتباطات و سایر صنایع مرتبط به حقوق کودک

مورد نیاز است و اینکه سازمان‌های مربوط به تنظیم مقررات که در خصوص توسعه استانداردهایی برای حفاظت از حقوق کودک مسئولیت دارند را تقویت نماید؛

۹. ضمناً از دولت‌ها می‌خواهد تا رویه‌های مؤثر و سریع جهت رفع یا انسداد سوءاستفاده جنسی کودک یا مواد پورنوگرافی که کودکان را گرفتار می‌کنند را اتخاذ نمایند. از جمله از طریق تصویب قانون و ارتقای چارچوبهای خودتضمینی مشاغل مطابق با قوانین و تعهدات ملی و بین‌المللی در زمینه حقوق بشر جهت کمک به کشف جرائم برخط، گزارش مدارک متعلق به آن و پیشگیری از پخش مواد سوءاستفاده جنسی کودک که کودکان را گرفتار می‌کند، واداشتن کودک به اعمال جنسی و اغفال جنسی کودک موسوم به گرومینگ کودک و سایر اشکال سوءاستفاده و استثمار برخط کودک؛

۱۰. پافشاری می‌کند که خدمات نیروی پلیس دولت‌ها، همکاری منطقه‌ای و بین‌المللی بین خود را تقویت نمایند. از جمله در کنار اقدامات دیگر از طریق چارچوب‌های مساعدت حقوقی متقابل در مسائل جزایی و سازمان بین‌المللی پلیس جنایی و برای اطمینان از اجرای مؤثر استانداردهای بین‌المللی مرتبط با آن و اجرای چارچوب قانونی قابل اعمال در موضوعات مرتبط با سوءاستفاده و استثمار جنسی برخط و غیربرخط کودک؛

۱۱. درخواست می‌کند دولت‌ها همکاری فنی و مالی بین‌المللی را در این حوزه جهت تبادل بهترین شیوه‌ها، روش‌های تحقیق، آموزش و ظرفیت‌سازی به‌منظور پیشگیری، ریشه‌کنی و کاهش سوءاستفاده و استثمار جنسی برخط کودک و بهبود جسمی و روانی و بازگشت اجتماعی دوباره قربانیان ترویج دهند؛

۱۲. پافشاری می‌کند دولت‌ها واحدهای مستقل تحقیقی نیروی پلیس که به خوبی آموزش دیده و مهارت یافته‌اند را مسئول تحقیق، تعقیب و مبارزه با ارتکاب خشونت جنسی و جنسیتی علیه کودکان و استثمار جنسی برخط کودک، با استفاده از فناوری‌های اطلاعات و ارتباطات، کنند یا اگر چنین واحدهایی از قبل موجود می‌باشند با تأمین پشتیبانی مالی کافی و ظرفیت‌سازی و فرصت‌های آموزشی ویژه آن‌ها را تقویت نمایند؛

۱۳. از دولت‌ها درخواست می‌کند رویکردی جامع، ایمن، فراگیر و قدرتمند را جهت محافظت

از کودکان برخط ایجاد نمایند که هم راستا با کنوانسیون حقوق کودک باشد. با اطمینان از اینکه اصول گرامی داشته شده در کنوانسیون از جمله اصول عدم تبعیض، بهترین منافع کودک، بقاء و توسعه و حق کودکان در بیان نظریاتشان درباره موضوعاتی که آن‌ها را تحت تأثیر قرار می‌دهد، به‌طور کاملاً معناداری اجرا می‌شوند؛

۱۴. پافشاری می‌کند دولت‌ها از جمله از طریق سازوکارهای گزارش‌دهی، خدمات و برنامه‌ها و دادخواهی‌های یکپارچه و حساس درباره کودک و جنسیت و مشی کودک‌دوستانه جهت درمان و بهبودی مؤثر و بازگشت مجدد کودکان قربانی سوءاستفاده و استثمار جنسی برای تسکین صدمات وارد شده به آن‌ها و پیشگیری از قربانی شدن ثانویه آن‌ها اقدام کنند. در عین اینکه تضمین شود حق کودک از جمله در هر اقدام اداری یا قضایی که برای او مؤثر است؛ با یک روش مطابق با قواعد رویه‌ای قانون ملی استماع خواهد شد؛

۱۵. دولت‌ها را تشویق می‌کند که جمع‌آوری، تحلیل و انتشار داده به شکل مناسب در مورد سوءاستفاده و استثمار جنسی برخط و غیربرخط را با صرف‌نظر از سن، جنسیت، درآمد خانواده و سایر عوامل مرتبط به‌عنوان یک بخش لاینفک از تلاش‌های دولت جهت پیشگیری و پاسخ به این سوءاستفاده، توسعه دهد و تقویت نماید؛

۱۶. درخواست می‌کند دولت‌ها کلیه اقدامات اجرایی و قانونی لازم جهت تضمین حقوق حریم خصوصی، تأمین، حفاظت، ایمنی و اطلاعات کافی کلیه کودکان درگیر در تحقیقات جاری جزایی و یا دادرسی‌های قضایی را قبل، حین و بعد از چنین تحقیقات و دادرسی‌هایی اتخاذ و فراهم نمایند؛

۱۷. همچنین از دولت‌ها درخواست می‌کند تا برنامه‌های آموزشی مستمر و فراگیر برای توانمندسازی کودک به شکل رسمی و غیررسمی را اتخاذ و اجرا کنند. مهارت‌های پایه‌ای مرتبط با رسانه و سوادآموزی اطلاعاتی، به‌طور برجسته اطلاعات و آموزش درمورد محیط برخط، استفاده ایمن، مزایا و خطرهای آن را به‌منظور افزایش آگاهی و توانایی کودکان، خانواده‌ها، قلم‌های قانونی، معلمان و سایر افراد حرفه‌ای که با کودکان کار می‌کنند جهت اتخاذ راهبرد (تدابیر) مواجهه با محیط برخط را تأمین کنند و حمایت از برگشت‌پذیری کودکان از جمله از طریق وارد کردن و

درگیر کردن کودکان، قربانیان سابق، سازمان‌های غیردولتی و صنایع مرتبط به موضوع؛
۱۸. به‌علاوه از دولت‌ها درخواست می‌کنند که برنامه‌ها و ابتکارات استفاده از فناوری‌های اطلاعات و ارتباطات از جمله تلفن همراه و رسانه اجتماعی را جهت مطلع کردن کودکان از حقوقشان، خطرهای سوءاستفاده و استثمار جنسی و اتخاذ راهبرد از جمله اجرای سازوکارهای هشدار بموقع را توسعه دهند در عین حال که چالش‌های پیش روی کودکان و فقدان توانمندی‌های آنان در رابطه با این چالش‌ها را در نظر می‌گیرند؛

۱۹. پافشاری به دولت‌ها جهت تاسیس سازوکارهای مشاوره، گزارش‌دهی و دادخواهی برای کودکان که این سازوکارها به‌صورت گسترده در دسترس، به راحتی قابل حصول، حساس درباره کودک و جنسیت و محرمانه باشند. مثل خطوط تلفنی امداد کودک جهت گزارش تعاملات نامناسب و مواجهه با خشونت برخط و همچنین استفاده از این خطوط برای محافظت از کودکان؛
۲۰. تشویق می‌کنند مشارکت کودکان را در توسعه و اجرای سیاست‌ها، برنامه‌ها و سایر ابتکارات با هدف ارتقای (ترویج) حقوق کودک، به‌ویژه حقوقی که از سوءاستفاه و استثمار جنسی برخط و غیربرخط کودک پیشگیری و یا با آن مبارزه می‌کنند؛

۲۱. تشویق دولت‌ها به ایجاد و تقویت بسترهای چندذی‌نفعی با مشارکت دولت‌ها، جامعه مدنی و نمایندگان صنعت، به‌ویژه بخش فناوری اطلاعات و ارتباطات، صنعت گردشگری و بخش‌های مالی و بانکداری با نگاهی به ارتقای مشارکت شرکای خصوصی در بسط و اجرای سیاست‌های توانمندسازی و آگاه‌سازی کودکان، پیشگیری از سوءاستفاده و استثمار جنسی برخط و غیربرخط کودک که شامل اقدامات مربوط به ایمنی پیشگیرانه و هشدار کیفیت می‌باشد؛

۲۲. تصمیم می‌گیرد برای ادامه ملاحظاته‌اش در مسئله حقوق کودک مطابق با برنامه کاری خود و قطعنامه‌های ۷/۲۹ به تاریخ ۲۸ مارس ۲۰۰۸ و ۱۹/۳۷ به تاریخ ۲۳ مارس ۲۰۱۲ و با تمرکز مباحث سال آتی درباره موضوع «حفاظت از حقوق کودک در اجرای دستورکار توسعه پایدار»؛

۲۳. از کمیساری عالی حقوق بشر سازمان ملل می‌خواهد، گزارشی درخصوص آن موضوع (موضوع بند قبل) را با همکاری نزدیک با تمامی ذی‌نفعان مرتبط، از جمله دولت‌ها، صندوق



کودکان سازمان ملل، سایر نهادها و سازمان‌های مرتبط سازمان ملل، دارندگان دستورالعمل ویژه روند کار {صاحبان ایده و فکر}، سازمان‌های منطقه‌ای و نهادهای حقوق بشری، مؤسسات ملی حقوق بشری و جامعه مدنی، از جمله خود کودکان، جهت ارائه در اجلاس سی و چهارم شورای حقوق بشر با نگاهی بر تأمین اطلاعات برای مباحث سال آتی در مورد حقوق کودک آماده نماید.

مصوب بدون رأی‌گیری (کنسانسوس)

نشست ۶۲ (۲۳ مارس ۲۰۱۶)

مجمع عمومی

مبحث پنجم: کنفرانس توسعه و تجارت ملل متحد (آنکتاد)

بند یک: گزارش گروه کارشناسان بین دولتی درباره تجارت الکترونیک و اقتصاد دیجیتال - سال ۲۰۱۷

ترجمه سند



مجمع عمومی
آنکتاد

تاریخ انتشار: ۳۱ اکتبر ۲۰۱۷

شماره قطعنامه: TD/B/EDE/1/3

زبان: انگلیسی

کنفرانس تجارت و توسعه ملل متحد

اجلاس یکم - ژنو، مورخ ۴ تا ۱۶ اکتبر ۲۰۱۷

گزارش کارشناسان بین دولتی درباره تجارت الکترونیک و اقتصاد دیجیتال

گروه کارشناسان بین دولتی درباره تجارت الکترونیک و اقتصاد دیجیتال

با یادآوری مجدد قطعنامه مجمع عمومی ۷۰/۱ مورخ ۲۵ دسامبر ۲۰۱۵ با عنوان «تبدیل دنیای ما: دستور کار توسعه پایدار»؛

با یادآوری مجدد قطعنامه مجمع عمومی {به شماره} ۷۰/۱۲۵ مورخ ۱۶ دسامبر ۲۰۱۵ با عنوان «سند منتج از نشست سطح بالای مجمع عمومی در مورد بازنگری کلی اجرای نتایج اجلاس سران در باره جامعه اطلاعاتی» که در آن مجمع هماهنگی نزدیک بین فرایند اجلاس سران درباره جامعه اطلاعاتی و دستور کار توسعه پایدار را تقاضا می نماید، {همچنین} با برجسته نمودن نقش میان بر به فناوری اطلاعات و ارتباطات در اهداف توسعه پایدار و ریشه کنی فقر؛

با ابراز نگرانی مشترک درباره اینکه شکاف های دیجیتالی مهمی همچنان بین کشورها و درون آن ها و بین زنان و مردان وجود دارد که نیاز به مقابله با آن ها، در کنار سایر اقدامات، از طریق تقویت توانمندسازی محیط های سیاسی و همکاری های بین المللی وجود دارد تا {مباحث مربوط به} کم هزینه بودن، دسترسی، آموزش، ظرفیت سازی، چندزبانی، صیانت فرهنگی و حمایت مالی مناسب را بهبود بخشد؛

با یادآوری مقررات مربوط به تجارت الکترونیک و اقتصاد دیجیتالی مصوب چهاردهمین اجلاس کنفرانس تجارت و توسعه سازمان ملل متحد (جولای ۲۰۱۶، نایروبی)، از جمله بند U و ۵۵۷، با یادآوری بند ۲۱۰۰ از سند نایروبی مبنی بر درخواست تشکیل گروه‌های کارشناسی بین دولتی درباره تجارت الکترونیکی و اقتصاد دیجیتال؛

با یادآوری تمرکز سیاستی خود روی منافع توسعه حداکثری از طریق تجارت الکترونیکی و اقتصاد دیجیتالی و مقابله با چالش‌های مرتبط و تقویت ابعاد توسعه آن، با تأکید بر اینکه فناوری اطلاعات و ارتباطات و اقتصاد دیجیتال از جمله تجارت الکترونیک تأثیر فزاینده‌ای روی توسعه و تجارت جهانی از جمله سامان بخشی و سازمان دهی به کار و استخدام و تولید دارد؛

ضمن به رسمیت شناختن اینکه رشد اقتصاد دیجیتال می‌تواند فرصت‌ها و چالش‌هایی را برای کشورهای در حال توسعه از جمله در خصوص شرایط رقابت، ایجاد زنجیره‌های قیمت جدید کارآفرینی و وابستگی اقتصادی ایجاد نماید؛

ضمن به رسمیت شناختن بیشتر نیاز به تقویت عملکرد آنکتابد درباره فناوری‌های اطلاعات و ارتباطات، تجارت الکترونیک و اقتصاد دیجیتال برای توسعه، به‌منظور افزایش توانایی خود در حمایت از کشورهای در حال توسعه در تعامل جهت رشد اقتصاد دیجیتالی و بهره‌مندی از آن و کاهش شکاف دیجیتالی، ایجاد جوامع دانشی فراگیر؛

ضمن توجه توأم با نگرانی {درباره} کاهش و افول کمک به {بخش} فناوری اطلاعات و ارتباطات، در مقایسه با مجموع کمک‌هایی که برای {عرصه} تجارت صورت می‌گیرد؛

باتوجه به اینکه تنها ۱۶ درصد از جمعیت بالغ جهان از اینترنت جهت پرداخت صورت حساب یا خرید استفاده می‌کند و در حالی که بیش از ۷۰ درصد از جمعیت برخی از کشورهای توسعه‌یافته، در حال حاضر کالا و خدمات را به‌صورت برخط خریداری می‌کنند و در بیشتر کشورهای کمتر توسعه‌یافته سهم معادل آن {خرید و دریافت کالا و خدمات از طریق برخط} کمتر از ۲ درصد می‌باشد؛

ضمن استقبال از مشارکت شرکت‌کنندگان چه در ارائه مقاله مکتوب و چه ارائه شفاهی که سبب غنای بحث در طول اولین اجلاس گردید؛

ضمن توجه توأم با قدردانی درباره مستنداتی که توسط دبیرخانه آنکتابد برای اولین اجلاس آماده گردید؛

با استقبال از گزارش تحلیل اطلاعات اقتصادی در سال ۲۰۱۷ با عنوان «دیجیتالی کردن، تجارت و توسعه» ضمن تأکید بر ضرورت زیرساخت‌های ارتقای یافته، منعطف و گسترده جهت اتصال دیجیتال وسیع‌تر و باتوجه‌به اینکه به‌منظور دستیابی به این نتایج گسترش وسیع دیجیتال { به منابع متنوع عمومی و خصوصی جهت تأمین مالی نیاز خواهد شد؛ باتوجه‌به تعهدات مندرج در هدف ۴,۴ توسعه پایدار (۲۰۳۰) تعداد جوانان و بالغانی که جهت استخدام، کار و کارآفرینی دارای مهارت‌های فنی و شغلی مرتبط می‌باشند، اساساً افزایش داشته است:

۱. دولت‌های عضو را تشویق می‌نماید تا به نحو مقتضی، دستور کار دیجیتال را در دستور کار توسعه ملی خود (در داخل و در کلیه رده‌ها) به‌صورت کامل بگنجانند و از آنکتابد می‌خواهد همکاری‌های خود را با سایر ذی‌نفعان مربوط افزایش دهد و به‌منظور آماده‌سازی کشورها به وسیله الگوهای عملی و رویه‌های معتبر و از این تلاش‌ها پشتیبانی نماید؛

۲. باتوجه‌به ابزارها و سازوکارهای ایجاد شده توسط آنکتابد مانند شاخص تجارت الکترونیکی مشاغل با مشتری^۱، بازنگری‌های مربوط به سیاست‌گذاری در حوزه فناوری اطلاعات و ارتباطات، {سامانه} پیگیری قوانین سایبری در جهان^۲، ارزیابی‌های آمادگی سریع تجارت الکترونیکی و مشارکت آن‌ها در جمع‌آوری و تحلیل داده‌های مربوط به وضعیت ملی درباره تجارت الکترونیکی و دیجیتالی کردن، از دبیرخانه درخواست می‌نماید تا این ارزیابی‌ها را در مورد کشورهای کمتر توسعه‌یافته ادامه دهد و قلمرو این تحقیقات را به کشورهای در حال توسعه گسترش دهند و از شرکای توسعه‌یافته، برای تأمین هزینه‌های لازم برای آنکتابد به‌منظور پوشش چنین مساعدت‌های فنی به هر نحو مقتضی دعوت می‌نماید؛

۳. ضمن توجه توأم با نگرانی درباره ماهیت نامتقارن اقتصاد دیجیتال جهانی، از جمله دسترسی

1. Business-to-Consumer E-commerce Index

مدل تجارت الکترونیکی کسبوکار با مصرف‌کننده رایج‌ترین نوع تجارت الکترونیکی است که به خرید کالا و خدمات بین‌بنگاه تجاری و یک مشتری اطلاق می‌شود. در واقع معاملات الکترونیکی بین شخص حقیقی (مصرف‌کننده یا مشتری) با یک شخص حقوقی (شرکت یا مؤسسه تجاری) صورت می‌گیرد. در این روش خریدار و فروشنده مسقیماً و بدون واسطه از طریق اینترنت با هم ارتباط برقرار می‌کنند. (منبع: آژانس دیجیتال مارکتینگ آویژه www.e-avijeh.ir)

2. Global Cyber law Tracker

نامتوازن جاری به بسترهای تجارت الکترونیکی در سطح بین‌المللی که به طور مستقیم تشکیلات اقتصادی خیلی کوچک (میکرو)، کوچک و متوسط را مخصوصاً در کشورهای در حال توسعه تحت تأثیر قرار می‌دهد، از دبیرخانه درخواست می‌نماید تا تحلیل‌های خود را درباره چالش‌های کشورهای در حال توسعه در اقتصاد دیجیتال، به‌ویژه تجارت الکترونیکی که نخستین قدم (درباره این چالش‌ها) در گزارش اطلاعات اقتصادی مربوط به سال ۲۰۱۵ برداشته شده است ادامه دهند: {طبق این گزارش} آشکار شدن قابلیت تجارت الکترونیک برای کشورهای در حال توسعه و مطرح شدن توصیه‌های سیاستی برای اعضا جهت بحث در نشست آتی با در نظر گرفتن چالش‌های پیش روی کشورهای در حال توسعه؛

۴. ضمن توجه توأم با قدردانی در مورد آمادگی الکترونیکی، از اینکه اغلب کشورهای در حال توسعه هنوز نیازمند زیرساخت، سیستم‌های پرداخت الکترونیکی و سایر ترتیبات آمادی برای اجرای تجارت الکترونیکی هستند، ابراز نگرانی می‌نماید؛

۵. از دولت‌های عضو دعوت می‌نماید تا اطلاعات مندرج در {سامانه} پیگیری قوانین سایبری در جهان - متعلق به آنکتاد- را در مورد کشورهای خود بررسی کنند و به نحو مقتضی اطلاعات به‌روز شده را در دسترس دبیرخانه آنکتاد قرار دهند؛

۶. اهمیت جریانهای مربوط به داده‌های فرامرزی در اقتصاد دیجیتال را به رسمیت می‌شناسد و دبیرخانه را جهت تداوم عملکرد خود درباره مفاهیم ضمنی {جریان داده‌ها} برای کشورهای در حال توسعه تشویق می‌نماید؛

۷. ضمن اذعان به اینکه در بسیاری از کشورهای در حال توسعه، تدارکات ضعیف و ناچیز به‌عنوان یک مانع برای تجارت الکترونیک محسوب می‌شود، دبیرخانه را جهت تداوم همکاری خود با اتحادیه جهانی پست در حمایت از تجارت الکترونیکی به انضمام به‌کارگیری امکاناتی جهت مشارکت بین بخش خصوصی و ادارات پست محلی، مطابق با خط‌مشی‌ها و اولویت‌های آن‌ها، تشویق می‌نماید؛

۸. توأم با نگرانی به وجود شکاف دیجیتال و آمادگی ضعیف در تجارت الکترونیک در کشورهای در حال توسعه به‌ویژه کشورهای کمتر توسعه‌یافته توجه می‌نماید که می‌تواند به تقسیم ناعادلانه

در کسب منفعت از تجارت الکترونیک و اقتصاد دیجیتال منجر شوند و از دبیرخانه درخواست می‌کند تا تحلیلی از نخستین مجموعه ارزیابی‌های مربوط به آمادگی سریع تجارت الکترونیک مربوط به کشورهای کمتر توسعه‌یافته را ارائه دهد. این مهم از جمله با هدف بحث درباره راه‌های حصول اطمینان از پیگیری مؤثر توصیه‌های مندرج در ارزیابی‌ها و ابعاد رو به گسترش شکاف دیجیتال و تدوین شاخص‌های مرتبط‌تر برای ارزیابی آمادگی دیجیتال صورت گیرد تا این موضوع بیشتر مورد بحث قرار گیرد؛

۹. نیاز به تعامل مؤثر بین گروه‌های زیر را با نگاهی بر ایجاد هم‌افزایی و اجتناب از موازی‌کاری، تأکید می‌نماید: کارشناسان بین دولتی درباره تجارت الکترونیک و اقتصاد دیجیتالی، گروه کارشناسان بین دولتی درباره سیاست و قانون حمایت از مصرف‌کننده و گروه کارشناسان بین دولتی درباره سیاست و قانون رقابت؛

۱۰. ضمن توجه به اینکه میان برنامه‌های تعداد بیشماری از شرکای توسعه، گسست و عدم انسجام وجود دارد، بنگاه‌های اقتصادی و بازیگران بخش خصوصی، الگوهایی را برای تسهیل اتصالات وسیع‌تر، کاهش هزینه‌ها و پرداختن به موضوعات تنظیم مقررات پیشنهاد می‌دهند و از شرکای توسعه در هر موقعیتی دعوت می‌کند که پشتیبانی مالی از تجارت الکترونیک برای تمامی برنامه‌های مرتبط را به‌عمل آورند. استفاده از تجارت الکترونیک و کاربرد آن در تمام بسترها را به‌منظور ارتقای هماهنگی مورد تشویق قرار می‌دهد؛

۱۱. به‌کارگیری ابتکاراتی جهت ارتقای دسترس‌پذیری به آمارها برای کشورهای در حال توسعه را تشویق می‌نماید. از جمله ابتکار مشترک آنکتاد، کمیسیون‌های منطقه‌ای سازمان ملل متحد، سازمان همکاری و توسعه اقتصادی^۱، اتحادیه جهانی پست، بانک جهانی، سازمان گمرکات جهانی و سازمان تجارت جهانی که با هدف ارتقای اقدامات مربوط به تجارت الکترونیکی در سطح فرامرزی صورت پذیرفت و از شرکای توسعه دعوت می‌نماید تا در این حوزه‌ها از طریق پشتیبانی از ظرفیت‌سازی همکاری نمایند؛

۱۲. ایجاد گروه کاری برای سنجش تجارت الکترونیک و اقتصاد دیجیتالی در قالبی منطبق

با منابع دسترس‌پذیر را توصیه می‌نماید و دبیرخانه را درباره آماده‌سازی یادداشت مفهومی و طرحی درباره گروه کاری و کشف علائق و منافع میان شرکای توسعه جهت پشتیبانی مالی از عملکردهای خود دعوت می‌نماید؛

۱۳. بر نیاز به تعامل بین ذی‌نفعان برای اجرای دستورکار توسعه پایدار ۲۰۳۰ تأکید می‌نماید مخصوصاً در ارتباط با دستیابی به منافع تجارت الکترونیکی و توسعه فراگیر ناشی از دیجیتالی کردن. و از مشارکت جامعه مدنی، نمایندگان کسب‌وکار و نمایندگان دانشگاهی جهت مشاوره در اجلاس‌های گروه کارشناسان بین‌دولتی درباره تجارت الکترونیک و اقتصاد دیجیتالی استقبال می‌نماید؛

۱۴. تصمیم می‌گیرد که درخصوص موضوعات محتوایی مورد توجه در برنامه کاری گروه کارشناسان بین‌دولتی درباره تجارت الکترونیک و اقتصاد پایدار به‌صورت اجلاس سالانه و در هر اجلاس تصمیم‌گیری خواهد شد؛

۱۵. تصمیم می‌گیرد که دومین اجلاس به موضوع تقویت منافع توسعه‌ای کشورهای در حال توسعه از تجارت الکترونیکی بومی و فرامرزی اختصاص یابد؛

۱۶. تصمیم می‌گیرد که دومین اجلاس خود باید روی سؤالات زیر متمرکز باشد:

أ. کشورهای در حال توسعه چگونه می‌توانند بسترهای محلی را برای تجارت الکترونیکی بومی و فرامرزی تقویت نمایند؟

ب. در ارتباط با بسترهای تجارت الکترونیکی در سطح بین‌المللی، کشورهای در حال توسعه از جمله کشورهای کمتر توسعه‌یافته، با چه موانعی روبرو می‌باشند و چگونه می‌توانند از این موانع عبور نمایند؟

ج. کسب‌وکارهای کوچک و متوسط در کشورهای در حال توسعه در هنگام تجارت برخط با چه محدودیت‌های عملیاتی روبرو هستند و این کشورها چگونه می‌توانند بر محدودیت‌های موجود فائق آیند؟

د. کشورهای توسعه‌یافته و در حال توسعه، از جمله کشورهای کمتر توسعه‌یافته چه رویه‌های معتبری را می‌توانند از یکدیگر فراگیرند؟

بند دو: گزارش گروه کارشناسان بین دولتی درباره تجارت الکترونیک و اقتصاد دیجیتال – سال ۲۰۱۸

ترجمه سند

تاریخ انتشار: ۲۲ می ۲۰۱۸

پشماره قطعنامه: TD/B/EDE/2/4 تا ۶ اکتبر ۲۰۱۷

زبان: انگلیسی



مجمع عمومی
آنکتاد

کنفرانس تجارت و توسعه ملل متحد

اجلاس یکم - ژنو، مورخ ۴ تا ۶ اکتبر ۲۰۱۷

گزارش کارشناسان بین دولتی درباره تجارت الکترونیک و اقتصاد دیجیتال

الف: تقویت دستاوردهای توسعه تجارت الکترونیکی بومی و فرامرزی در کشورهای در حال توسعه - توصیه‌های مرتبط با خط‌مشی‌های مورد توافق

گروه کارشناسان بین دولتی درباره تجارت الکترونیک و اقتصاد دیجیتال؛ ضمن استقبال از همکاری مشارکت‌کنندگان به شکل مکتوب و شفاهی که سبب غنای بحث در باره موضوعات مورد انتخاب جهت گفتگو گردید و با تأکید بر اهمیت تجارت الکترونیک و اقتصاد دیجیتال برای توسعه پایدار و فراگیر؛

ضمن به رسمیت شناختن شکاف موجود در {سطح} آمادگی تجارت الکترونیک بین کشورهای توسعه‌یافته و در حال توسعه و {همچنین شکاف موجود} در داخل کشورها، {و این موضوع} دلالت دارد بر اینکه منافع حاصل از تجارت الکترونیکی عادلانه توزیع نگردیده و به خط‌مشی‌های مناسبی جهت پاسخگویی در این زمینه نیاز می‌باشد؛

باتوجه به اینکه بسترهای اقتصادی و تجارت الکترونیک می‌توانند برای کشورهای در حال توسعه {توأم} فرصت و چالش‌هایی را ایجاد نمایند؛

با به رسمیت شناختن نیاز به بررسی امکان تقویت بسترهای تجارت الکترونیکی در سطح محلی در کشورهای در حال توسعه؛

ضمن توجه توأم با نگرانی از اینکه دسترسی و استفاده مؤثر از بسترهای تجارت الکترونیکی

بین‌المللی توسط تشکیلات اقتصادی در اندازه‌های میکرو (ریز)، کوچک و متوسط در کشورهای در حال توسعه، به صورت یک چالش همچنان باقی است؛

ضمن به رسمیت شناختن اینکه تشکلات اقتصادی در اندازه‌های میکرو (ریز)، کوچک و متوسط در کشورهای در حال توسعه برای تحقق تجارت برخط با بسیاری از مشکلات از جمله محدودیت‌های عملیاتی روبه‌رو می‌باشند:

۱. اذعان می‌دارد که تحصیل منافع حداکثری و مقابله با چالش‌های تجارت الکترونیک و اقتصاد دیجیتال امری ضروری می‌باشد و اینکه سیاستگذاران نیازمند اتخاذ سیاست‌های چندگانه در ابعاد کلان موضوع می‌باشند، از جمله حوزه‌های مرتبط با زیرساخت‌های دیجیتال، تجارت، رقابت، محتوای محلی، حمایت از مصرف‌کننده، حفاظت داده، تراکنش‌های الکترونیک، امنیت سایبری، حل و فصل دعاوی برخط، وضع مالیات، تنوع زبانی، آموزش، مهارت‌ها، توسعه و کار؛

۲. دولت‌ها را تشویق می‌نماید، تا در زمان تدوین سیاست‌ها و تنظیم مقررات برای تعامل با سایر ذی‌نفعان به نحو مقتضی و در زمان مقتضی وارد مذاکره شوند تا به تضمین منافع بالقوه توسعه ناشی از رشد استفاده از بسترهای دیجیتال کمک شود؛

۳. کشورهای در حال توسعه را تشویق می‌نماید تا برای یادگیری از تجارب اقتصادی دولت‌های دیگر جهت مقابله با چالش‌های ناشی از سیاستگذاری، اجتناب از تکرار خطاها و بهره‌مندی از رویه‌های برتر تلاش نمایند؛

۴. ضمن توجه به اهمیت ایفای نقش بسترهای محلی جهت پرداختن به تقاضا و پاسخگویی به شرایط (پیشامدهای) محلی، همکاری بین دولت‌ها و سایر ذی‌نفعان مرتبط را تشویق می‌نماید تا به سوی (موارد زیر) حرکت کنند:

- ایجاد یک محیط توانمند برای کارآفرینی و ابتکار و فراهم کردن دسترسی به سرمایه‌گذاری و فناوری برای استارت‌آپ‌های دیجیتال،

- آگاهی بخشی، اعتمادسازی، تقویت و توانمندسازی محیط سیاسی، قانونی،

۵. با نگاهی به ایجاد بسترهای محلی قویتر و رقابت پذیرتر در کشورهای کمتر توسعه‌یافته، به امکان استفاده از این زمینه‌های همکاری دیجیتال که از منابع محدودی برخوردارند در راستای

توسعه راه‌حل‌های دیجیتالی توجه می‌نمایند. از جمله پشتیبانی از تجارت الکترونیکی جهت ظرفیت‌سازی برای تمامی شرکاء؛

۶. ضمن توجه به دسترسی عوامل ناهمگون در استفاده مؤثر از بسترهای تجارت الکترونیک بین‌المللی، که ممکن است ناشی از عوامل مختلفی باشد (عواملی همانند مقررات کشور مبدأ یا مقصد^۱، محدودیت‌های جغرافیایی، راهبردهای مربوط به حوزه اصناف و محیط‌های کسب‌وکار)، دولت‌ها و سایر ذی‌نفعان را تشویق می‌نمایند تا موانعی که علی‌الخصوص در این ارتباط کشورهای در حال توسعه با آن‌ها روبه‌رو می‌شوند را رفع نمایند؛

۷. بر اهمیت مباحث بین‌المللی درباره {موضوعات زیر} ضمن حفظ پادمانهای ضد پول‌شویی اذعان می‌دارد:

✓ چگونگی ارتقای دسترس‌پذیری جهانی به سیستم‌های پرداختی قابل تعمیم که محدوده عمل داخلی دارند

✓ محیط‌های کسب‌وکار شفاف و قابل پیش‌بینی برای تعامل بین بسترها و مشاغل
۸. استفاده مؤثر از راه‌حل‌های نهادی و فنی ابتکاری را با هدف رفع مشکلات مرتبط با پرداخت‌ها، سیستم‌های پرداخت فیزیکی، ارتقای صادرات و آمادگی (لجستیک) تجاری تشویق می‌نماید؛

۹. ضمن توجه به نگرانی‌ها در خصوص برخی مشکلات موجود در استفاده از تجارت الکترونیک و اقتصاد دیجیتالی، بر این موضوع اصرار دارد که تمامی ذی‌نفعان توجهات کافی را جهت مقابله با چالش‌های ویژه و تقویت فرصت‌ها برای کسب‌وکارهایی با محوریت زنان در فضای برخط مبذول دارند؛
۱۰. با تأکید بر تفاوت در {سطح} آمادگی تجارت الکترونیک بین نواحی شهری و روستایی، دولت و سایر مشارکت‌کنندگان در امر گردشگری را تشویق می‌نمایند تا تلاش {خود را} جهت ایجاد تجارت الکترونیک با ثبات در نواحی روستایی در کشورهای در حال توسعه، افزایش دهند. {تلاش‌هایی که} به‌طور قابل ملاحظه‌ای دسترس‌پذیری به برق، اتصالات سیال، مسیر زیرساخت‌ها و سیستم‌های نشانه‌یابی را تضمین نماید.

۱. به‌عنوان مثال گوگل که یک شرکت آمریکایی است و در ایران فعالیت می‌کند ممکن است همزمان درگیر مقررات ایران یا آمریکا شود. امریکا محل ثبت شرکت است و ایران محل فعالیت آن.

۱۱. از دولت‌ها و سایر مشارکت‌کنندگان در امر توسعه درخواست می‌نماید تا تلاش‌های خود را در راستای ظرفیت‌سازی برای تولیدکنندگان کوچک در کشورهای در حال توسعه افزایش دهند تا {آن‌ها} توسط تجارت برخط در بازار صادرات رقابت نمایند؛

۱۲. نیاز به تعاملات مؤثر بین گروه کارشناسان دولتی زیر را با رویکرد هم‌افزایی و پرهیز از موازی کاری تصریح می‌نماید:

✓ گروه کارشناسان بین دولتی درباره تجارت الکترونیک و اقتصاد دیجیتالی؛

✓ گروه کارشناسان بین دولتی درباره خط‌مشی و قانون حمایت از مصرف‌کننده؛

✓ گروه کارشناسان بین دولتی درباره قانون و خط‌مشی رقابت؛

۱۳. دبیرخانه آنکتاد را تشویق می‌نماید تا فرصت‌هایی را برای همکاری با بانک فناوری در رابطه با حوزه‌های زیر شناسایی نماید: تقویت سطح آمادگی تجارت الکترونیک در کشورهای کمتر توسعه‌یافته و تلاش برای توسعه ارزیابی‌های سطح آمادگی تجارت الکترونیک برای سایر کشورهای در حال توسعه

نشست اختتامیه عمومی مورخ ۲۰ آوریل ۲۰۱۸

ب: گروه کاری درباره سنجش تجارت الکترونیک و اقتصاد دیجیتال - تصمیم‌ها

گروه کارشناسان بین دولتی درباره تجارت الکترونیک و اقتصاد دیجیتالی، با نگاهی بر ضرورت ارتقای دسترسی پذیری آمارهای رسمی تجارت الکترونیک و اقتصاد دیجیتالی مخصوصاً در کشورهای در حال توسعه جهت پشتیبانی از سیاست‌گذاری‌های مبتنی بر ادله به شورای تجارت و توسعه توصیه می‌نماید تا گروه کاری درباره سنجش تجارت الکترونیکی و اقتصاد دیجیتالی را همان‌طور که در سند شرح داده شد، ایجاد نماید. درخواست می‌نماید که دبیرخانه آنکتاد شرح وظایف گروه کاری جدید را بر مبنای اطلاعات مندرج در سند TD/B/EDE/2/3 آماده سازد و شفاف نماید که اهداف آن مشارکت و همکاری پیشرفته درباره سنجش تجارت الکترونیکی و اقتصاد دیجیتال است و اینکه این گروه کاری از موازی کاری با سایر کارهای مرتبط در حال فعالیت اجتناب می‌نماید.

نشست عمومی مورخ ۲۰ آوریل ۲۰۱۸

بند سه: گزارش گروه کارشناسان بین دولتی درباره تجارت الکترونیک و اقتصاد دیجیتال – سال ۲۰۱۹

ترجمه سند



مجمع عمومی
آنکتاد

تاریخ انتشار: ۲۲ می ۲۰۱۹

پشماره قطعنامه: TD/B/EDE/3/3

زبان: انگلیسی

کنفرانس تجارت و توسعه ملل متحد

اجلاس سوم - ژنو مورخ ۳ تا ۵ آوریل ۲۰۱۹

گزارش کارشناسان بین دولتی درباره تجارت الکترونیک و اقتصاد دیجیتال

اول. اقدامات صورت گرفته توسط گروه کارشناس‌های بین دولتی درباره تجارت الکترونیک و اقتصاد دیجیتال

الف. گروه کاری درباره سنجش تجارت الکترونیک و اقتصاد دیجیتال (بخش ۴ دستور کار موقت)

۱. در نشست مورخ ۵ آوریل ۲۰۱۹، گروه کارشناسان بین دولتی درباره تجارت الکترونیک و اقتصاد دیجیتال، شرح وظایف گروه کاری درباره اقدامات مربوط به تجارت الکترونیک و تجارت دیجیتال را تصویب نمودند در اولین نشست گروه کاری درباره موضوعات زیر توافق کردند:

- بازنگری دستورالعمل آنکتاد در راستای تولید آمار درباره اطلاعات اقتصادی؛

- سنجش ملی و فراملی تجارت الکترونیکی.

ب. دستور کار موقت چهارمین اجلاس گروه کارشناسان بین دولتی درباره تجارت الکترونیکی و

اقتصاد دیجیتالی (بخش ۵ دستور کار)

۲. در نشست عمومی اختتامیه مورخ ۵ آوریل ۲۰۱۹ گروه کارشناسان بین دولتی توافق

شد که تصمیم‌گیری درباره این بخش در دستور کار شورای تجارت و توسعه به تعویق انداخته شود. دبیرخانه آنکتاد پیشنهادهای رسیده از کشورهای عضو درباره دستور کار و سؤالات راهنما را گردآوری خواهد کرد و جهت ملاحظه به شورا ارائه و نسخه (متن) نهایی دستور کار موقت پنج میزگرد مباحثه ای را {در خصوص موضوعات زیر} برگزار نمود؛

✓ نقش فزاینده داده‌های دیجیتال در دنیای اقتصاد؛

✓ داده‌های دیجیتال و کاربردهای آن در تجارت و توسعه فراگیر؛

✓ فرصت‌ها و چالش‌های مرتبط با داده‌ها و جریان داده‌ها؛

✓ موضوعات مربوط به تنظیم مقررات و چالش‌های آن؛

✓ ظرفیت‌سازی برای تحلیل داده‌ها و هوش مصنوعی؛

✓ بحث در زمینه وی توصیه‌های پیشنهادی مربوط به حوزه سیاستگذاری؛

ج. کارگروه سنجش تجارت الکترونیک و اقتصاد دیجیتال (دستور کار ۴)

۳. شورای تجارت و توسعه در بخش اول اجلاس شصت‌وپنجم خود، مبنی بر ایجاد گروه کاری درباره سنجش تجارت الکترونیک و اقتصاد دیجیتال تصمیم‌گیری نمود. از این رو از گروه کارشناسان بین دولتی درباره تجارت الکترونیک و اقتصاد دیجیتال دعوت شد تا شرح وظایف و موضوعات پیشنهادی برای اولین نشست {این} گروه کاری را تصویب نماید. - به‌عنوان مثال، بازبینی دستورالعمل آنکتاد برای تولید آمار درباره اطلاعات اقتصادی و سنجش تجارت الکترونیک در سطح بومی و فرامرزی - . این دستورالعمل در نظام ملل متحد {به‌عنوان} ابزار مرجع اصلی، برای کارمندان سازمان‌های آمار ملی {مطرح} و برای متخصصان آمار در کشورهای در حال توسعه به‌عنوان یک {سند} راهنما تعیین گردید. {تا از آن} در تمامی مراحل تولید و توزیع آمارهای فناوری اطلاعات و ارتباطات مرتبط با فضای کسب‌وکار (تجارت) استفاده گردد؛
 ✓ متن جاری {این سند} که در سال ۲۰۰۹ منتشر گردید، جهت حصول اطمینان از {موارد زیر} نیازمند تجدید نظر می‌باشد؛

درج آخرین تعاریف و رده بندی‌ها در آن؛

✓ معرفی تحولات جدید در حوزه سنجش تجارت الکترونیک و اقتصاد دیجیتال.

دبیر خانه آنکتاد پیشنهاد نمود که کارشناسان آمار از کشورهای عضو در اولین نشست گروه کاری، بازخورد و نظرهای خود در خصوص پیش‌نویس تجدید نظر شده این دستورالعمل را ارائه نمایند. {این امر} به مراجع آماری ملی مرتبط {کشورها} اجازه اعمال نظر قوی‌تری را می‌دهد. دومین موضوع، در پی پاسخ به افزایش تقاضای دولت‌های عضو مبنی بر اصلاح سنجش تجارت

الکترونیک در سطح بومی و فرامرزی، پیشنهاد گردید. گروه کاری در اولین نشست خود، توانست تحولات روش شناختی اخیر را بررسی نماید و دولت‌های عضو جهت به اشتراک گذاری تجربیات و رویه‌های برتر در این حوزه دعوت شدند. در رابطه با این موضوع، هنوز کمبود آماری در تجارت الکترونیک در کشورهای در حال توسعه و توسعه‌یافته وجود داشت، به‌ویژه در کشورهای در حال توسعه؛

۴. کارشناسان ضمن بیان حمایت از گروه کاری، شرح وظایف و توافق خود در خصوص دو موضوع مطرح شده برای اولین نشست گروه کاری را تصویب کردند. دو نماینده به ارائه {ترجمه} واضح مفاد گروه کاری به تمامی زبانهای رسمی توسط دبیر خانه آنکتاد اشاره کردند. یک نماینده پیشنهاد نمود که گروه کاری در اولین نشست خود، در کنار سایر موضوعات مورد بحث، {موضوع} تلاش جهت سنجش ارزش تجارت الکترونیکی مخصوصاً تجارت الکترونیکی را مورد نظر قرار دهد. سودان و تایلند علاقه کشور خود را جهت میزبانی نشست‌های آتی گروه کاری ابراز نمودند.



فصل دوم

شورای اقتصادی و اجتماعی سازمان ملل (اکوسوک)

مبحث یک: مصوبات اکوسوک

بند یک: قطعنامه پیشگیری، حفاظت و همکاری بین‌المللی علیه استفاده از فناوری‌های نوین اطلاعاتی در جهت سوءاستفاده یا استثمار کودکان سال ۲۰۱۱

ترجمه سند

تاریخ انتشار: ۲۰۱۱

شماره قطعنامه: ۲۰۱۱/۳۳

زبان: انگلیسی

توزیع: عمومی



شورای اقتصادی و اجتماعی

پیشگیری، حفاظت و همکاری بین‌المللی علیه کاربرد فناوری‌های نوین اطلاعاتی

در جهت سوءاستفاده یا استثمار کودکان

شورای اقتصادی و اجتماعی؛

با یادآوری قطعنامه‌های مجمع عمومی {به شماره‌های} ۵۵/۶۳ مورخ ۴ دسامبر ۲۰۰۰، ۵۶/۱۲۱، مورخ ۱۹ دسامبر ۲۰۰۱ و ۶۴/۲۱۱ مورخ ۲۱ دسامبر ۲۰۰۹ در باب مبارزه علیه سوءاستفاده، مجرمانه از فناوری اطلاعات و نیز {با یادآوری} سایر قطعنامه‌های مرتبط سازمان ملل متحد، با تأیید مجدد قطعنامه خود {به شماره} ۲۰۰۴/۲۶ مورخ ۲۱ جولای ۲۰۰۴ با عنوان «همکاری»،

بین‌المللی در زمینه پیشگیری، تحقیق، پیگرد و مجازات کلاهبرداری، سوءاستفاده مجرمانه و جعل هویت و جرائم مرتبط» و قطعنامه ۲۰۰۷/۲۰ مورخ ۲۶ جولای ۲۰۰۷ با عنوان «همکاری بین‌المللی جهت پیشگیری، تحقیق، پیگرد و مجازات کلاهبرداری اقتصادی و جرم مرتبط با هویت» همچنین با تأیید مجدد قطعنامه کمیسیون پیشگیری از جرم و عدالت کیفری (به شماره { ۱۶/۲ مورخ ۲۷ آوریل ۲۰۰۷ با عنوان «واکنش‌های مؤثر جهت پیشگیری از جرم و عدالت کیفری با هدف مبارزه با استثمار جنسی کودکان»؛

باتوجه به قطعنامه شماره ۹، در خصوص جرائم مرتبط با کامپیوتر، مصوب هشتمین کنگره تحت عنوان «پیشگیری از جرم و رفتار با مجرمان سازمان ملل متحد»، که در آن قطعنامه از دولت‌ها درخواست شده است که تلاش‌های خود را به‌منظور مبارزه مؤثرتر علیه سوءاستفاده‌های مرتبط با کامپیوتر تشدید نمایند؛

با درنظر گرفتن نتایج دهمین کنگره پیشگیری از جرم و رفتار با مجرمان سازمان ملل متحد در راستای مواجهه با چالش‌های قرن بیست و یکم با هدف مبارزه علیه جرم و ارتقای عدالت؛ با تأکید بر اهمیت بند ۴۲ اعلامیه السالوادور در خصوص راهبردهای جامع برای چالش‌های جهانی: سیستم‌های پیشگیری از جرم و عدالت کیفری و تحول آن‌ها در یک جهان در حال تغییر، مصوب دوازدهمین کنگره پیشگیری از جرم و عدالت کیفری سازمان ملل، که در آن کنگره از کمیسیون پیشگیری از جرم و عدالت کیفری دعوت شد که تشکیل گروه کارشناسان بین‌دولتی باز به‌منظور انجام یک مطالعه جامع درباره معضل جرم سایبری و پاسخگویی به آن توسط دولت‌های عضو، جامعه بین‌المللی و بخش خصوصی را مورد نظر قرار دهد و با استقبال از نشست گروه کارشناسان که از ۱۷ تا ۲۱ ژانویه ۲۰۱۱ در وین برگزار شد؛

با به رسمیت شناختن عملکرد کمیسیون مبارزه علیه جرم سایبری، و با در نظر داشتن اینکه کنواسیون سازمان ملل متحد علیه جرائم سازمان یافته فراملی نشانگر یک گام اصلی در راستای مبارزه با جرائم مربوط به استفاده از فناوری‌های نوین اطلاعاتی و ارتباطاتی می‌باشد؛ با ابراز نگرانی از اینکه پیشرفت‌های سریع فنی به شکل فزاینده، امکانات جدیدی را برای سوءاستفاده مجرمانه از فناوری‌های نوین اطلاعات و ارتباطات ایجاد کرده است؛

با یادآوری کنوانسیون حقوق کودک و پروتکل اختیاری در کنوانسیون حقوق کودک در خصوص فروش کودکان، فحشاء و پورنوگرافی کودک؛

با تأیید مجدد اینکه وفق کنوانسیون بدترین اشکال کار کودک مصوب سازمان بین‌المللی کار (شماره ۱۸۲ سال ۱۹۹۹)، ضروری است که دولت‌های عضو، اقدامات فوری و مؤثری را جهت تضمین ممنوعیت و عدم استفاده، واسطه‌گری جهت عرضه کودک برای فحشاء، تولید یا انجام پورنوگرافی، اتخاذ نمایند؛

همچنین با تأیید مجدد قطعنامه ۱۹/۱ کمیسیون پیشگیری از جرم و عدالت کیفری مورخ می ۲۰۱۰ با عنوان «تقویت مشارکت‌های عمومی و خصوصی برای مقابله با جرم در تمامی اشکال و مظاهر آن» و با ملاحظه نتایج همایش دفتر جرم و مواد مخدر سازمان ملل در خصوص مشارکت‌ها در هر دو بخش عمومی و خصوصی علیه جرایم سازمان یافته فراملی که در تاریخ ۸ آوریل ۲۰۱۱ در وین برگزار گردید که در آن از دولت‌ها تقاضا گردید به منظور مبارزه با استثمار جنسی کودکان در عصر دیجیتال، همکاری‌های مؤثری با بخش خصوصی {داشته باشند}؛

با در نظر گرفتن این حقیقت که فضاهای اجتماعی که با استفاده از فناوری‌های نوین اطلاعات و ارتباطات ایجاد شده‌اند، به شکل گسترده‌ای توسط کودکان در تعاملات اجتماعی استفاده می‌شوند؛ با تأکید بر اینکه فناوری‌های نوین اطلاعات و ارتباطات و برنامه‌های کاربردی (اپلیکیشن‌ها)، با هدف ارتکاب جرائم استثمار جنسی کودک، مورد سوءاستفاده قرار می‌گیرند و {همچنین با تأکید} بر اینکه پیشرفت‌های فناورانه موجب ظهور جرائمی مانند تولید، توزیع و مالکیت تصاویر، صدا یا ویدئو از سوءاستفاده‌های جنسی از کودک، در معرض قرار گرفتن کودکان {در برابر} محتوای مضر، گرومینگ {اغفال جنسی}، آزار و اذیت و سوءاستفاده جنسی از کودکان و زورگویی سایبری (قلدری سایبری) شده است؛

با در نظر داشتن مخاطرات احتمالی مربوط به یک محتوای خاص موجود در اینترنت و شبکه‌های اجتماعی مجازی و {همچنین با در نظر داشتن} اینکه تماس آسان با مجرمان برخط ممکن است رشد و نمو صحیح کودکان را تحت تأثیر قرار دهد؛

باتوجه به اینکه، در نتیجه پیشرفت‌های فنی سال‌های اخیر، دسترسی افراد به مواردی که

اصالت و انسجام شخصیتی و حقوق کودکان را نقض می‌کند، به شکل روزافزونی در حال افزایش می‌باشد؛

با ابراز نگرانی از اینکه فناوری‌های نوین اطلاعات و ارتباطات برای مجرمان امکان تماس آسان با کودکان را ایجاد نموده است که این امکان و سهولت، سابقه ندارد؛

با آگاهی از اینکه فناوری‌های نوین اطلاعات و ارتباطات، امکان ساختن هویت های جعلی را فراهم می‌نماید، این امر موجب تسهیل سوءاستفاده یا استثمار جنسی کودکان توسط مجرمان می‌گردد؛

با تأیید مجدد اینکه از کودکان باید در دنیای مجازی همانند دنیای فیزیکی حفاظت شود، با تأکید بر اهمیت همکاری بین دولت‌ها و بخش خصوصی، در مبارزه علیه استفاده از فناوری‌های نوین اطلاعات و ارتباطات به منظور سوءاستفاده یا استثمار کودکان؛

همچنین با تأکید بر اهمیت همکاری و هماهنگی بین‌المللی در مبارزه مؤثر علیه سوءاستفاده مجرمانه از فناوری‌های نوین اطلاعاتی و ارتباطات با هدف سوءاستفاده یا استثمار کودکان، با به رسمیت شناختن اینکه شکاف‌های {موجود} در دسترسی و استفاده از فناوری‌های نوین اطلاعات و ارتباطات توسط دولت‌ها، می‌تواند اثربخشی همکاری بین‌المللی در مبارزه علیه استفاده از آن فناوری‌ها برای سوءاستفاده یا استثمار کودکان را کاهش دهد؛

باتوجه به مباحث موضوعی با عنوان «حفاظت از کودکان در عصر دیجیتال: سوءاستفاده از فناوری جهت استفاده نادرست و استثمار کودک» که توسط کمیسیون پیشگیری از جرم و عدالت کیفری در بیستمین اجلاس خود برگزار شد:

۱. پافشاری می‌نماید تا آن دسته از دولت‌هایی که هنوز کنوانسیون حقوق کودک و پروتکل اختیاری حقوق کودک در خصوص فروش کودکان، فحشا و پورنوگرافی کودک، کنوانسیون بدترین اشکال کار کودک {مربوط به} سازمان بین‌المللی کار (شماره ۱۸۲ سال ۱۹۹۹)، کنوانسیون علیه جرم سازمان یافته فراملی و پروتکل پیشگیری، توقیف و مجازات قاچاق اشخاص به‌ویژه زنان و کودکان، الحاقیه کنوانسیون سازمان ملل علیه جرم سازمان یافته فراملی را تصویب نکرده اند، {برای تصویب کنوانسیون‌های فوق‌الذکر} اقدام نمایند؛

۲. مصرانه از دولت‌های عضو می‌خواهد برای ایجاد، توسعه و اجرای سیاست‌های عمومی و روش‌های مفید به‌منظور حفاظت و دفاع از حقوق کودک، در مقوله‌های امنیت، حریم خصوصی و صمیمیت در فضاهایی که با استفاده از فناوری‌های نوین اطلاعات و ارتباطات ایجاد شده‌اند، اقدام نماید؛

۳. دولت‌های عضو را جهت ورود وزارتخانه‌های مسئول {در امر} مخابرات (ارتباطات از راه دور)، سازمان‌های مسئول در حفاظت داده و نمایندگان صنعت فناوری اطلاعات و ارتباطات، به سازوکارهای بین‌بخشی و فعال شدن آن‌ها جهت مقابله با سوءاستفاده از فناوری‌های نوین اطلاعات و ارتباطات در تجاوز یا استثمار کودکان با نگاهی بر ارائه راه‌حل‌های پیشنهادی جامع برای مقابله با چنین سوءاستفاده‌ها و {همچنین پیشنهاد راه‌حل برای} ممانعت و اجتناب از نقض حقوق کودک، تشویق می‌کند؛

۴. مصرانه از دولت‌های عضو می‌خواهد تا، در صورت لزوم، اقدامات مناسبی از جمله: طرح‌های تقنینی برای جرم‌انگاری کلیه وجوه سوءاستفاده از فناوری جهت ارتکاب به جرم‌های استثمار جنسی کودک، را مصوب نماید و {همچنین مصرانه از دولت‌های عضو می‌خواهد}، که وفق قوانین ملی و حقوق بین‌الملل، اقدامات مناسبی را جهت کشف و حذف تصاویر شناخته شده مربوط به سوءاستفاده جنسی از کودک در فضای اینترنت را مورد نظر قرار دهند و شناسایی مرتکبان به سوءاستفاده و استثمار جنسی کودکان را تسهیل نمایند؛

۵. دولت‌های عضو را جهت ایجاد و کاربرد اقدامات راستی‌آزمایی کافی و ارتقای آن برای محافظت برخط کودکان تشویق می‌نماید؛

۶. پافشاری می‌نماید تا دولت‌های عضو تولید، توزیع، انتشار، دریافت و مالکیت داوطلبانه تصاویر سوءاستفاده و استثمار جنسی کودک، همراه با دسترسی عمده و مکرر به تارنماها (وبسایت) حاوی چنین تصاویری و مشاهده محتواهای ذخیره شده برخط را به‌عنوان جرائم کیفری در نظام‌های حقوقی خود تعیین نمایند؛

۷. همچنین پافشاری می‌نماید تا دولت‌های عضو، وفق چارچوب‌های قانونی ملی خود با تأمین کنندگان خدمات اینترنتی، شرکت‌های تلفن همراه و سایر بازیگران کلیدی به‌منظور

تشکیل سازوکارهای مناسب و کارآمد، همکاری نزدیک داشته باشند، از جمله در صورت امکان، تدوین قانون در مورد ارائه گزارش مربوط به تصاویر و مواد سوءاستفاده جنسی از کودک به مراجع مرتبط جهت مسدود نمودن تار نماها {وبسایت‌های حاوی} تصاویر سوءاستفاده جنسی کودک و {همچنین سازوکارهای} همکاری با نیروی پلیس در تحقیق و پیگرد مجرمان مسئول؛ ۸. دولت‌های عضو را تشویق می‌نماید تا در قانون ملی خود، مطابق با نظام‌های حقوقی خویش، اقدامات لازم را جهت ذخیره و تضمین دسترسی سریع به داده الکترونیکی در خلال تحقیقات کیفری {جنایی} مربوط به استفاده از فناوری‌های نوین اطلاعات و ارتباطات در سوءاستفاده و استثمار کودکان پیش‌بینی نمایند؛

۹. مصرانه می‌خواهد تا دولت‌های عضو، منابع کافی برای انجام مؤثرتر وظایف خود در دفترهای {ادارات} مسئول تحقیق و تعقیب مجرمانی که مرتکب جرائم مربوط به استفاده از فناوری‌های نوین اطلاعات و ارتباطات برای نقض حقوق کودک شده‌اند، را فراهم نمایند؛ ۱۰. دولت‌های عضو را تشویق می‌کند که فعالیت‌های مربوط به آگاهی بخشی را خطاب به کودکان درگیر با فضای اطلاعات افزایش دهند تا کودکان با فراگیری این سازوکارها بتوانند در موارد لازم، درخواست محافظت یا حمایت یا مساعدت نمایند و حتی یاد بگیرند موارد سوءاستفاده یا استثمار را گزارش دهند و نیز {دولت‌های عضو را بر انجام} فعالیت‌هایی به منظور بالا بردن سطح آگاهی والدین و آموزش دهندگان، جهت پیشگیری از چنین جرائمی {تشویق می‌نماید}؛

۱۱. از کشورهای عضو جهت اجرای سازوکارهای گزارش‌دهی مؤثر دعوت می‌نماید تا شهروندان آن کشور از طریق آن سازوکارهای مقرر بتوانند فعالیت‌های مربوط به تارنماها {وبسایت‌های غیرقانونی} و فعالیت‌های مجازی مرتبط با جرائم استثمار جنسی کودکان را گزارش دهند؛

۱۲. پافشاری می‌نماید تا دولت‌های عضو، کمپین‌هایی را به منظور بالا بردن سطح آگاهی عموم مردم از خطرهای سوءاستفاده از فناوری‌های نوین اطلاعات و ارتباطات ایجاد و راهبری کنند؛

۱۳. دولت‌های عضو را در خصوص ایجاد و اجرای سازوکارهایی برای نهادهای ذی‌صلاح به منظور شناسایی کودکانی که از طریق فناوری‌های نوین اطلاعات و ارتباطات مورد سوءاستفاده و استثمار

- قرار گرفته اند و {همچنین} تشکیل رویه‌هایی جهت محافظت از آن‌ها تشویق می‌نماید؛
۱۴. پافشاری می‌نماید تا دولت‌های عضو، تدوین (تهیه پیش نویس) و تصویب کردارنامه‌ها و سایر سازوکارهای مربوط به مسئولیت مشترک اجتماعی را برای شرکت‌های ارائه دهنده خدمات اینترنت، شرکت‌های تلفن همراه، کافی نت‌ها و سایر بازیگران کلیدی مرتبط ارتقای دهند؛
۱۵. از دفتر مبارزه با مواد مخدر و جرم سازمان ملل درخواست می‌کند که عندالاقضاء داده‌های مرتبط که توسط گروه موسوم به «گروه کارشناسان بین‌دولتی مأمور انجام مطالعه جامع راجع به جرم سایبری» جمع‌آوری شده است را جهت انجام مطالعه جامع در خصوص تسهیل شناسایی، تشریح و ارزیابی {سنجش} تأثیرات فناوری‌های جدید اطلاعاتی روی سوءاستفاده و استثمار کودکان، در نظر بگیرد. ضمن اینکه {از این دفتر درخواست می‌کند که} مطالعات انجام شده مرتبط توسط سازمان‌های منطقه‌ای و سایر سازمان‌های داخل سیستم سازمان ملل مانند صندوق کودکان ملل متحد، اتحادیه بین‌المللی مخابرات، «دفتر کمیساریای عالی حقوق بشر سازمان ملل» را با رویکرد ارتقای تبادل تجربه و متدهای مفید {در نظر بگیرند}؛
۱۶. همچنین از دفتر مبارزه با مواد مخدر و جرم سازمان ملل درخواست می‌کند که به صورت مقتضی، جهت طراحی و انجام یک ارزیابی در مورد نیازهای آموزشی دولت‌ها در زمینه تحقیق جرائم علیه کودکان با استفاده از فناوری‌های نوین اطلاعات و ارتباطات، داده مرتبط را که توسط گروه کارشناسان جمع‌آوری شده در نظر بگیرند، {و همچنین از این دفتر درخواست می‌کند که} بر مبنای نتایج این بررسی، یک برنامه مساعدت فنی و آموزشی را جهت کمک به کشورهای عضو در زمینه مبارزه مؤثرتر علیه چنین جرائمی باتوجه به منابع {مالی} در دسترس طراحی کند، مشروط به اینکه با تلاش‌های سازمان پلیس جنایی (اینترپل) موازی کاری نگردد؛
۱۷. پافشاری می‌نماید تا دولت‌های عضو، هماهنگی و همکاری، تبادل اطلاعات درباره روش‌های مفید و تجربیات موفق خود را در زمینه مبارزه علیه استفاده از فناوری‌های نوین اطلاعات و ارتباطات برای سوءاستفاده و استثمار کودکان افزایش دهند؛
۱۸. دولت‌های عضو را تشویق می‌نماید تا از تلاش‌ها و دانش پیشرفته و نیز ابتکارات پیشگیرانه مربوط به سازمان ملل و سایر سازمان‌های بین‌المللی، سازمان‌های منطقه‌ای، جامعه مدنی و

بخش خصوصی، جهت مبارزه با سوءاستفاده مجرمانه از فناوری‌های نوین اطلاعات و ارتباطات بهره برداری نمایند؛

۱۹. پافشار می‌نماید تا دولت‌های عضو اطمینان حاصل نمایند که نظام‌های مساعدت متقابل، تبادل بموقع مدارک در موارد مرتبط با استفاده از فناوری‌های نوین اطلاعات و ارتباطات در سوءاستفاده و استعمار کودکان را تضمین می‌نماید؛

۲۰. از دولت‌های عضو دعوت می‌نماید تا مساعدت فنی و انتقال فناوری از جمله آموزش ابزار تحقیقی را به‌ویژه برای استفاده و بهره‌مندی کشورهای در حال توسعه مهیا نمایند. (این مساعدت فنی و انتقال فناوری را) با رویکرد توانمندسازی آن دسته از کشورهایی که ظرفیت ملی خود را جهت مبارزه مؤثر علیه فعالیت‌های مجرمانه‌ای که از فناوری‌های نوین اطلاعات و ارتباطات جهت نقض حقوق کودک استفاده می‌نمایند انجام دهند {انتقال و بومی سازی دانش فنی}؛

۲۱. از دبیرکل درخواست می‌نماید تا گزارشی در خصوص اجرای قطعنامه حاضر را به بیست و سومین نشست کمیسیون پیشگیری از جرم و عدالت کیفری، ارائه نماید؛

۲۲. از کشورهای عضو و سایر حامیان مالی داوطلبانه خارج از بودجه دعوت می‌نماید تا منابع مالی (بودجه‌ای) فوق‌العاده را برای اجرای بندهای مرتبط در قطعنامه حاضر مطابق با قوانین و رویه‌های سازمان ملل فراهم نمایند.

نشست عمومی ۴۸ - (مورخ ۲۸ جولای ۲۰۱۱)

بند دو: خلاصه ای از قطعنامه‌های شورای اقتصادی اجتماعی

ترجمه سند

«همکاری بین‌المللی در پیشگیری، تحقیق، تعقیب و مجازات کلاهبرداری اقتصادی و جرائم مرتبط با هویت»^۱

شماره قطعنامه و سال صدور	محتوا
۲۰۰۴/۲۶ سال ۲۰۰۴	<p>✓ شورای اقتصادی و اجتماعی سازمان ملل متحد در قطعنامه خود { به شماره } ۲۰۰۴/۲۶ تحت عنوان همکاری بین‌المللی در پیشگیری، تحقیق، پیگرد و مجازات کلاهبرداری، سوءاستفاده مجرمانه و جعل هویت و جرائم مرتبط:</p> <p>✓ درباره اشاعه مواردی از کلاهبرداری و جرائم اقتصادی مرتبط در سطح ملی و فراملی و درگیری گروه‌های جنایی سازمان یافته، فناوری‌های نوین و سوءاستفاده مجرمانه و جعل هویت در چنین مواردی ابراز نگرانی نمود.</p> <p>✓ { این شورا همچنین } درباره گسترش فناوری‌های نوین اطلاعاتی و ارتباطاتی که یک دامنه وسیعی از فرصت‌های جدید را برای کلاهبرداری و سوءاستفاده مجرمانه و جعل هویت ایجاد می‌کند، به شکل متوالی استفاده قانونی از چنین فناوری‌هایی را به خطر می‌اندازد و موجب ایجاد تهدید برای کشورهای می‌شود که درصدد استفاده از چنین فناوری‌هایی برای توسعه هستند، ابراز نگرانی کرد.</p>
۲۰۰۷/۲۰ سال ۲۰۰۷	<p>✓ همچنین این شورا در قطعنامه خود با شماره ۲۰۰۷/۲۰، تحت عنوان مشابه با قطعنامه قبل، درباره نقشی که توسط فناوری‌های اطلاعات، ارتباطات و کامپیوتر در تحول کلاهبرداری اقتصادی و جرائم مرتبط با هویت ایفا شده است، ابراز نگرانی کرد.</p>
۲۰۰۹/۲۲ سال ۲۰۰۹	<p>✓ باتوجه به کنوانسیون جرم سایبری (کنوانسیون بوداپست)، { که } در حال حاضر تنها معاهده بین‌المللی می‌باشد که به طور ویژه به مقابله با کلاهبرداری، جعل مرتبط با کامپیوتر و سایر اشکال جرم سایبری می‌پردازد که ممکن است در ارتکاب کلاهبرداری اقتصادی، جرائم مرتبط با تعیین هویت، پول شویی و سایر فعالیت‌های غیر مجاز مربوط دارای نقش باشند.</p> <p>✓ همچنین با ابراز نگرانی درباره بهره برداری از فناوری‌های جدید اطلاعاتی، ارتباطاتی و تجاری توسط مرتکبان کلاهبرداری اقتصادی و جرائم مرتبط با تعیین هویت، و { با ابراز نگرانی } از تهدیداتی که اینگونه بهره برداری { مجرمانه } برای تجارت، خود فناوری‌ها و کاربران آن‌ها ایجاد می‌نماید { شورا } به { لزوم داشتن توانمندی‌های بومی مؤثر و مناسب در داخل کشور جهت کشف و تحقیق، پیگرد و مجازات کلاهبرداری اقتصادی و جرائم مرتبط با تعیین هویت و نیز { لزوم داشتن } سازو کارهایی برای ارتقای همکاری بین‌المللی جهت پیشگیری و مبارزه علیه چنین اشکالی از جرم مجاب شده است و ارتباط نزدیک { تنگاتنگ } بین جرائم مرتبط با هویت و فناوری‌های اطلاعات و ارتباطات را به رسمیت می‌شناسد. شورا دولت‌های عضو را تشویق می‌نماید تا توصیه‌های گروه کارشناسی بین دولتی جهت بررسی کلاهبرداری و سوءاستفاده مجرمانه و هویت جعلی بر اساس آنچه در قطعنامه شورای اجتماعی و اقتصادی { به شماره } ۲۰۰۴/۲۶ مورخ ۲۱ جولای ۲۰۰۴، درخواست شده است را مورد نظر قرار دهند: { از جمله } توسعه و حفظ ظرفیت کافی نیروی پلیس و ظرفیت تحقیق جهت حفظ برابری برای مقابله با تحولات جدید در بهره برداری از فناوری‌های تجاری و اطلاعات در راستای کلاهبرداری‌های اقتصادی و جرائم مرتبط با تعیین هویت و ارتباطات از جمله تارنماها و سایر مجامع برخط که به‌منظور تسهیل قاچاق { و تبادل } اطلاعات یا اسنادی مانند گذرنامه‌ها، گواهینامه رانندگی و کارت‌های شناسایی ملی</p>
۲۰۱۱/۳۵ سال ۲۰۱۱	<p>✓ { مجدداً این شورا } در قطعنامه خود با شماره ۲۰۱۱/۳۵، تحت عنوان مشابه با قطعنامه قبل، درباره نقشی که توسط فناوری‌های اطلاعات، ارتباطات و کامپیوتر در تحول کلاهبرداری اقتصادی و جرائم مرتبط با هویت ایفا شده است ابراز نگرانی کرد.</p>

۱. این قطعنامه‌ها دارای محتوای مفصلی درباره همکاری بین‌المللی در پیشگیری، تحقیق، تعقیب و مجازات کلاهبرداری اقتصادی و جرائم مرتبط با هویت می‌باشند و تنها بخش‌هایی از آن‌ها که در ارتباط با فضای سایبر هستند، ترجمه گردیده‌اند جهت دستیابی به متون اصلی قطعنامه‌ها به بانک الکترونیکی بیوست کتاب مراجعه گردد.



محتوا	شماره قطعنامه و سال صدور
<p>۷ شورای اقتصادی و اجتماعی سازمان ملل متحد در قطعنامه خود { به شماره } ۲۰۱۳/۳۹ مورخ ۲۵ جولای ۲۰۱۳، همکاری بین‌المللی در پیشگیری، تحقیق، تعقیب و مجازات کلاهبرداری اقتصادی و جرائم مرتبط با هویت. درباره انتفاع (بهره برداری) مرتکبان کلاهبرداری اقتصادی و جرائم مرتبط با تعیین هویت از فناوری‌های اطلاعاتی، ارتباطاتی و تجاری جدید و همچنین درخصوص تهدیدات ناشی از چنین بهره برداری‌هایی که بر تجارت و فناوری‌ها و کاربران آن‌ها تهدید تخمیل می‌شود ابراز نگرانی نمود. { همچنین این شورا } به فعالیتهای گروه کارشناسان بین دولتی باز درخصوص انجام بررسی جامع درباره مشکل جرم سایبری در حوزه‌سهای وابسته به جرائم مرتبط با تعیین هویت که پیرو قطعنامه مجمع عمومی { به شماره } ۶۵/۲۳۰ ایجاد شد توجه می‌نماید.</p>	<p>۲۰۱۳/۳۹ سال ۲۰۱۳</p>

بند سه: قطعنامه ارتقای مساعدت فنی و ظرفیت‌سازی برای تقویت اقدامات ملی و همکاری‌های بین‌المللی جهت مبارزه با جرم سایبری از جمله به اشتراک گذاری اطلاعات ۲۰۱۹

ترجمه سند



شورای اقتصادی و اجتماعی

تاریخ انتشار: ۳۱ جولای ۲۰۱۹

شماره قطعنامه: E/RES/29/19

زبان: انگلیسی

توزیع: عمومی

اجلاس ۲۰۱۹

دستور کار ۱۹

قطعنامه مصوب شورای اقتصادی اجتماعی مورخ ۲۳ جولای ۲۰۱۹
بر اساس توصیه‌های کمیسیون پیشگیری از جرم و عدالت کیفری (E/30/2019)

ارتقای مساعدت فنی و ظرفیت‌سازی برای تقویت اقدامات ملی و همکاری‌های بین‌المللی جهت مبارزه با جرم سایبری از جمله به اشتراک گذاری اطلاعات

شورای اقتصادی اجتماعی به مجمع عمومی درباره تصویب پیش‌نویس قطعنامه زیر توصیه نمود.

مجمع عمومی

با یادآوری قطعنامه خود {به شماره} ۶۵/۲۳۲ مورخ ۲۱ دسامبر ۲۰۱۰ که در آن {مجمع} اعلامیه السالوادور {با عنوان} درباره راهبردهای جامع برای چالش‌های جهانی: سیستم‌های پیشگیری از جرم و عدالت کیفری و توسعه آن در یک جهان در حال تغییر، را تأیید نمود. اعلامیه ای که در دوازدهمین کنگره پیشگیری از جرم و عدالت کیفری سازمان ملل تصویب شده بود {و در آن} کنگره از کمیسیون پیشگیری از جرم و عدالت کیفری درخواست کرد تا در راستای بند ۴۲ اعلامیه السالوادور، یک گروه کارشناسان بین دولتی باز را جهت انجام بررسی جامع درباره مسئله جرم سایبری و پاسخگویی به آن توسط دولت‌ها، جامعه بین‌الملل و بخش خصوصی به آن را تأسیس نماید. از جمله {اهداف این گروه موارد زیر می‌باشد}: تبادل اطلاعات درباره تدوین قانون ملی، رویه‌های برتر، مساعدت فنی و همکاری بین‌المللی با نگاهی به بررسی گزینه‌ها جهت تقویت قانون ملی و حقوق بین‌المللی موجود و پیشنهاد قانون ملی و حقوق بین‌المللی

جدید و سایر پاسخگویی‌ها به جرم سایبری؛

با یادآوری قطعنامه‌های خود {به شماره‌های} ۴۶/۱۵۲ مورخ ۱۸ دسامبر ۱۹۹۱، ۶۰/۱ مورخ ۱۶ سپتامبر ۲۰۰۵، ۶۷/۱ مورخ ۲۴ سپتامبر ۲۰۱۲، ۶۹/۱۹۳ و ۶۹/۱۹۶ مورخ ۱۸ دسامبر ۲۰۱۴، ۷۰/۱۷۸ و ۷۱/۲۰۹ مورخ ۱۹ دسامبر ۲۰۱۶ و ۷۲/۱۹۶ مورخ ۱۹ دسامبر ۲۰۱۷ و ۷۳/۱۸۶ مورخ ۱۷ دسامبر ۲۰۱۸، ۷۳/۱۸۷ مورخ ۱۷ دسامبر ۲۰۱۸، با یادآوری قطعنامه خود {به شماره} ۷۰/۱۷۴ مورخ ۱۷ دسامبر ۲۰۱۵ که در آن مجمع عمومی، به‌منظور مقابله با چالش‌های اجتماعی اقتصادی و ارتقای حاکمیت قانون در سطوح ملی و بین‌المللی و مشارکت عمومی، {قرار گرفتن} اعلامیه دوحه درباره پیشگیری یکپارچه از جرم و عدالت کیفری در دستور کار گسترده تر سازمان ملل را تأیید کرد؛

با استقبال از قطعنامه کمیسیون پیشگیری از جرم و عدالت کیفری {به شماره} ۲۶/۴ مورخ ۲۶ می ۲۰۱۷، که در آن کمیسیون تصمیم گرفت گروه کارشناسان بین دولتی باز بررسی جامعی درباره جرم سایبری را انجام دهد، نشست‌های آتی خود را با شیوه‌ای ساختاریافته، به رسیدگی به هریک از موضوعات اصلی موجود در پیش‌نویس مطالعه جامع درباره جرم سایبری اختصاص دهد، گروه کارشناسان را به توسعه نتایج و توصیه‌های ممکن جهت ارائه آن به کمیسیون تشویق نماید، از دفتر درخواست کرد که به شکل دوره ای اطلاعاتی درخصوص تحولات جدید، پیشرفت‌های ایجاد شده و رویه‌های برتر شناخته شده را جمع‌آوری نماید؛ همچنین ضمن استقبال از طرح کار گروه کارشناسان برای دوره زمانی ۲۰۱۸ تا ۲۰۲۰ که در چهارمین نشست گروه کارشناسان بین دولتی باز مورخ ۳ تا ۵ آوریل ۲۰۱۸ در وین به تصویب رسید. ضمن توجه به اینکه گروه کارشناسان نشست آتی خود را {با در نظر گرفتن موارد زیر} به همکاری و پیشگیری بین‌المللی اختصاص دادند:

- اطلاعات درباره موضوعات موجود در پیش‌نویس بررسی جامع جرم سایبری؛

- تفاسیر ارائه شده توسط دولت‌های عضو و تحولات اخیر در سطوح ملی و بین‌المللی؛

با یادآوری قطعنامه خود {به شماره} ۷۳/۱۸۶ که در آن {مجمع}، در کنار سایر موضوعات، ضمن توجه توأم با قدردانی درباره چهارمین نشست گروه کارشناسان، از دولت‌های عضو

درخواست نمود تا از طرح کار گروه کارشناسان حمایت نمایند؛ با یادآوری قطعنامه خود {به شماره} ۷۳/۱۸۷، که در آن از دبیرکل درخواست نمود تا نظرهای دولت‌های عضو را درباره چالش‌هایی که آن‌ها در خصوص مقابله با استفاده از فناوری‌های اطلاعات و ارتباطات با اهداف مجرمانه با آن مواجه هستند را پیگیری نماید و در اجلاس هفتادوچهارم {مجمع عمومی} گزارشی را از ملاحظات خود بر مبنای این نظرها ارائه نماید؛ با یادآوری بیشتر قطعنامه خود به شماره ۷۳/۱۸۷ که در آن {مجمع عمومی} تصمیم گرفت گزینه ای تحت عنوان «مقابله با استفاده از فناوری‌های اطلاعات و ارتباطات برای اهداف مجرمانه» را در دستور کار موقت خود در اجلاس هفتادوچهارم بگنجاند؛

ضمن تأکید بر نیاز به ارتقای هماهنگی و همکاری میان دولت‌های عضو درباره مبارزه با جرم سایبری از جمله از طریق تأمین مساعدت فنی کشورهای در حال توسعه - بنا به درخواست آن‌ها - در راستای بهبود تدوین قانون ملی و ارتقای ظرفیت مراجع ملی که با تمامی اشکال جرائم سایبری سروکار دارند از جمله پیشگیری، ردیابی، تحقیق و تعقیب قانونی، و در این چارچوب با تأکید بر نقش ملل متحد مخصوصاً نقشی که کمیسیون پیشگیری از جرم و عدالت کیفری ایفا می‌کند و با تأیید مجدد اهمیت احترام به حقوق بشر و آزادی‌های اساسی در استفاده از فناوری‌های اطلاعات و ارتباطات؛

با استقبال توأم با قدردانی از عملکرد گروه کارشناسان و تمرکز {این گروه} بر گفتگو و مباحثه محتوایی میان کارشناسان و صاحبان مشاغل از کشورهای عضو؛

باتوجه به اینکه کنوانسیون ملل متحد علیه جرم سازمان‌یافته فراملی ابزاری است که ممکن است دولت‌های عضو به منظور ایجاد همکاری بین‌المللی جهت پیشگیری و مبارزه با جرم سازمان یافته فراملی از آن استفاده نمایند، ابزاری که ممکن است برای بعضی از دولت‌های عضو در برخی موارد مربوط به جرم سایبری از آن استفاده شود؛

با آگاهی از چالش‌های پیش روی تمامی دولت‌ها در مبارزه با جرم سایبری و با تأکید بر نیاز به تقویت مساعدت فنی و اقدامات ظرفیت‌ساز {دولت‌ها} بنا به درخواست و بر مبنای نیازهای ملی {آن‌ها}، و با در نظر گرفتن چالش‌های ویژه که در این رابطه پیش روی کشورهای در حال توسعه قرار دارد؛

با انتظار از پرداختن به مباحثاتی با موضوعاتی وابسته به جرم سایبری از جمله ادله الکترونیکی در خلال برگزاری چهاردهمین کنگره ملل متحد درباره پیشگیری از جرم و عدالت کیفری؛

با استقبال توأم با قدردانی از تلاش‌های دفتر مقابله با مواد مخدر و جرم سازمان ملل در پیشرفت اجرای برنامه جهانی درباره جرم سایبری با هدف اجرای دستور کار خود در راستای تأمین مساعدتهای فنی و ظرفیت‌سازی درباره جرم سایبری؛

۱. ضمن قدردانی، از نتایج پنجمین نشست گروه کارشناسان بین دولتی باز جهت انجام بررسی جامع جرم سایبری که مورخ ۲۷ تا ۲۹ مارس ۲۰۱۹ در وین برگزار گردید، استقبال می‌نماید؛
 ۲. بر اهمیت کار گروه کارشناسان، جهت تداوم تبادل اطلاعات درباره موارد زیر اذعان می‌دارد: قانون ملی، رویه‌های برتر، مساعدتهای فنی همکاری بین‌المللی با نگاهی بر بررسی گزینه‌ها جهت تقویت پاسخ‌های (واکنش‌های) موجود و پیشنهاد قانون ملی و حقوق بین‌المللی جدید یا سایر پاسخ‌ها (واکنش‌ها) به جرم سایبری؛

۳. ضمن قدردانی، به این موضوع توجه می‌نماید که مطابق با طرح کار گروه کارشناسان برای دوره زمانی ۲۰۱۸ تا ۲۰۲۱ و نتایج و توصیه‌های ممکن جهت ارائه به کمیسیون {آن}، گروه کارشناسان توسعه خواهد یافت؛

۴. گروه کارشناسان برای انجام بررسی جامع درباره جرم سایبری را به‌عنوان یک بستر مهم جهت تبادل اطلاعات {در خصوص موارد زیر} به رسمیت می‌شناسد: تدوین قانون ملی، رویه‌های برتر، مساعدت فنی و همکاری بین‌المللی با نگاهی به بررسی گزینه‌هایی جهت تقویت {پاسخ‌ها} واکنش‌های موجود و پیشنهاد قانون ملی و حقوق بین‌الملل جدید یا سایر پاسخ‌ها برای جرم سایبری؛

۵. دولت‌های عضو را تشویق می‌نماید تا اقداماتی را توسعه دهند و اجرا نمایند که بتوانند متضمن {امور زیر} باشند:

- ادله الکترونیکی مرتبط با جرائم و جرم سایبری به طور مؤثری در سطح ملی تحقیق و

پیگیری شود؛

- همکاری بین‌المللی در این حوزه می‌تواند مطابق با قانون داخلی و سازگار با حقوق بین‌الملل مربوط و قابل اعمال – از جمله اسناد قابل اعمال حقوق بین‌المللی بشر – حاصل گردد.
۶. همچنین مصرانه دولت‌های عضو را تشویق کند تا مأموران انتظامی، مراجع تحقیقی، دادستان‌ها و قضات را در حوزه جرم سایبری از جمله مهارت‌های گردآوری و فناوری اطلاعات تعلیم دهند و آن‌ها را {برای} ایفای مؤثر نقش‌های مربوط خود در تحقیق، پیگرد و قضاوت جرائم سایبری مجهز نمایند؛
۷. دولت‌های عضو را تشویق می‌نماید تا بنا به درخواست و مبتنی بر نیازهای ملی {دولت‌ها}، تلاش نمایند تا مساعدت فنی مناسب و ظرفیت‌سازی تاب‌آوری را {برای آن‌ها} مهیا نمایند، توانمندی مراجع ملی که با جرم سایبر سروکار دارند را تقویت کنند و به تبادل نظرهای {خود} درخصوص تجربیات کاربردی و سایر وجوه فنی مربوط ادامه دهند؛
۸. مجدداً، پیرو قطعنامه کمیسیون پیشگیری از جرم و عدالت کیفری {شماره} ۲۲/۸ مورخ ۲۶ آوریل ۲۰۱۳، نقش دفتر مقابله با مواد مخدر و جرم ملل متحد به‌عنوان منبع مرکزی از حقوق و دروس آموخته شده جرم سایبری را تأیید می‌نماید، با نگاه به ارزیابی مداوم نیازها و قابلیت‌های عدالت کیفری، ارائه و هماهنگی مساعدت‌های فنی .
۹. از دفتر مقابله با مواد مخدر و جرم ملل متحد درخواست می‌نماید تا به‌صورت دوره‌ای اطلاعاتی را درباره تحولات جدید، پیشرفت‌های حاصل‌شده و رویه‌های برتر شناخته شده را جمع‌آوری کند و به شکل دوره‌ای گزارشی از این اطلاعات را به گروه کارشناسان و {همچنین} کمیسیون پیشگیری از جرم و عدالت کیفری ارائه نماید.
۱۰. از گروه کارشناسان دعوت می‌نماید تا مبتنی بر کار خود، با دفتر مقابله با مواد مخدر و جرم ملل متحد مشاوره نماید از جمله درباب برنامه جهانی جرم سایبری به‌منظور ارزیابی، بدون آنکه در سایر موضوعات مندرج در دستور کار گروه کارشناسان تأثیرگذار باشد و شناسایی اولویت‌های کلان در نیازهای ظرفیت‌سازی و پاسخ‌های مؤثر، بدون آنکه در موقعیت کمیسیون به‌عنوان نهاد حاکم بر برنامه جرم این دفتر تأثیرگذار باشد؛
۱۱. از دفتر مقابله با مواد مخدر و جرم ملل متحد درخواست می‌نماید تا از طریق برنامه جهانی

جرم سایبری و در میان سایر موارد از طریق دفترهای منطقه‌ای خود {و} مبتنی بر نیازهای ملی دولت‌های عضو که با جرم سایبری سروکار دارند، به تأمین تقاضای آن‌ها { در راستای مساعدت فنی و ظرفیت‌سازی تاب آور در ارتباط با پیشگیری، شناسایی، تحقیق و تعقیب قانونی جرم سایبری در تمامی اشکال آن ادامه دهد، همکاری با دولت‌های عضو، سازمان‌های منطقه‌ای و بین‌المللی، بخش خصوصی، جامعه مدنی و سایر ذی‌نفعان مربوط را تسهیل نمایند را به رسمیت بشناسد؛

۱۲. از دولت‌های عضو دعوت می‌نماید تا در صورت مقتضی ادامه همکاری با بخش خصوصی و جامعه مدنی جهت توسعه اقدامات مربوط به مبارزه با جرم سایبری را در شیوه‌ای شفاف و پاسخگو مورد ملاحظه قرار دهند؛

۱۳. از دولت‌های عضو و سایر حامیان مالی داوطلبانه دعوت می‌نماید تا مطابق با قواعد و رویه‌های سازمان ملل، منابع مالی (بودجه‌ای) فوق‌العاده را برای اهداف مشروح فوق، تأمین نمایند؛

۱۴. از دبیرکل تقاضا می‌نماید تا در اجلاس بیست و نهم کمیسیون پیشگیری از جرم و عدالت کیفری، گزارشی را در خصوص اجرای قطعنامه حاضر به آن کمیسیون ارائه نماید.

شورای اقتصادی و اجتماعی سازمان ملل (اکوسوک)
مبحث دو: کمیسیون علم و فناوری برای توسعه
بند یک: قطعنامه علم، فناوری و نوآوری برای توسعه سال ۲۰۱۸

ترجمه سند



شورای اقتصادی و اجتماعی
کمیسیون علم و فناوری برای توسعه

تاریخ انتشار: ۶ آگوست ۲۰۱۸

شماره قطعنامه: E/RES/29/2018

زبان: انگلیسی

توزیع: عمومی

قطعنامه مصوب شورای اقتصادی و اجتماعی مورخ ۲۴ جولای ۲۰۱۸
بر اساس توصیه کمیسیون علم و فناوری برای توسعه (E/31/2018)
علم، فناوری و نوآوری برای توسعه^۱

شورای اقتصادی و اجتماعی؛

با به رسمیت شناختن بیشتر نقش اصلی که فناوری اطلاعات و ارتباطات در ارتقای و توانمندسازی علم، فناوری و نوآوری به عنوان توانمندساز توسعه ایفا می نماید؛

با یادآوری نتایج اجلاس سران و قطعنامه مجمع عمومی (به شماره { ۷۰/۱۲۵ مورخ ۱۶ دسامبر ۲۰۱۵، با عنوان «سند نتیجه نشست سطح بالای مجمع عمومی در خصوص بررسی کلی اجرای نتایج اجلاس سران درباره جامعه اطلاعاتی» که در آن نقش حیاتی فناوری و اطلاعات از جمله فناوری های اطلاعات و ارتباطات جهت دستیابی به اهداف توسعه مورد توافق در سطح بین الملل به رسمیت شناخته شد، و با تأیید مجدد تعهدات مندرج در آن؛

با به رسمیت شناختن نقش ابزاری علم، فناوری و نوآوری و فناوری های اطلاعات و ارتباطات در دستیابی به تعدادی از اهداف توسعه پایدار، و با تأکید بر نقش علم، فناوری و نوآوری هم راستا با فناوری های اطلاعات و ارتباطات به عنوان توانمندساز؛

باتوجه به اینکه فناوری های جدید، مشاغل جدیدی را ایجاد می نمایند و فرصت ها را توسعه

۱. این قطعنامهها دارای محتوای مفصلی است و تنها بخش هایی از آن ها که در ارتباط با فضای سایبر هستند، ترجمه گردیده اند. جهت دستیابی به متون اصلی قطعنامهها به بانک الکترونیکی پیوست کتاب مراجعه گردد.

می دهند، بدین گونه که تقاضا جهت مهارت‌ها و صلاحیت‌های دیجیتال افزایش می‌یابد و با تأکید بر اهمیت ایجاد مهارت‌ها و صلاحیت‌های دیجیتال، تا آنجا که جوامع بتوانند به‌روز رسانی شوند و از تغییرات فنی بهره‌مند گردند؛

با به رسمیت شناختن نیاز به رویکردهای نوآورانه که پاسخگوی نیازهای جوامع فقیر، محلی و به حاشیه رانده شده در کشورهای در حال توسعه و توسعه‌یافته باشند و آن‌ها را در فرایندهای نوآوری درگیر نمایند و {با به رسمیت شناختن} درج و لحاظ ظرفیت‌سازی در حوزه‌های علم، فناوری و نوآوری به‌عنوان یک جزء قاطع، در کنار سایر موارد، در برنامه‌های توسعه ملی از با به رسمیت شناختن اینکه نوآوری به خوبی توسعه‌یافته وزیست بوم‌های (اکوسیستم‌های) دیجیتال نقشی اساسی را در توسعه دیجیتال مؤثر و تسهیل علم، فناوری و نوآوری ایفا می‌نمایند، با توجه دستاوردهای مهم و تداوم سهم بالقوه علم، فناوری و نوآوری و فناوری‌های اطلاعات و ارتباطات در به‌کارگیری رفاه بشر و رونق اقتصاد،

به دولت‌های ملی، کمیسیون علم و فناوری برای توسعه و کنفرانس تجارت و توسعه ملل متحد ملاحظات زیر را توصیه می‌نماید:

۱. دولت‌ها، به شکل انفرادی و جمعی، تشویق شوند تا یافته‌های کمیسیون را در نظر بگیرند و اقدامات زیر را مورد ملاحظه قرار دهند:

أ. پیوند دقیق علم، فناوری، نوآوری و راهبردهای توسعه پایدار از طریق ظرفیت‌سازی برجسته در زمینه فناوری اطلاعات و ارتباطات، علم، فناوری و نوآوری در برنامه ریزی توسعه ملی؛
 ب. تشویق و پشتیبانی از تلاش‌های علم، فناوری و نوآوری جهت هدایت {آن‌ها} به سمت توسعه زیرساخت‌ها و سیاست‌هایی که از گسترش جهانی زیرساخت‌های فناوری اطلاعات و ارتباطات، تولید و خدمات پشتیبانی می‌نماید، از جمله {خدمات مربوط به} دسترسی به پهنای باند اینترنت، توسط تمامی مردم، و افرادی با نیازهای ویژه از جوامع دور و روستایی، تسریع در تلاش‌های چند ذی‌نفعی جهت رساندن {تعداد} کاربران جدید اینترنت برخط به ۱/۵ طریق همکاری بین وزارت‌های مربوط و نهادهای تنظیم مقررات، به حاشیه رانده شده در میلیارد نفر تا سال ۲۰۲۰ و تلاش جهت بهبود کم‌هزینه بودن چنین تولیدات و خدماتی؛

ج. تعهد جهت {انجام} تحقیقات سیستمی از جمله {تحقیق در} جنبه‌های جنسیتی، حساس، جهت آینده نگاری درباره روندهای جدید در علم، فناوری و نوآوری و فناوری‌های اطلاعات و ارتباطات و تأثیر آن‌ها بر توسعه؛

د. پرداختن به الزامات تغییرات اساسی در اقتصاد دیجیتال برای بازارهای کار؛
هـ. ارزیابی سیستم‌های نوآوری ملی از جمله زیست بوم‌های (اکوسیستم‌های) دیجیتال در فواصل زمانی معین، که از تمرین‌های آینده نگاری استخراج شده اند، {با هدف} شناسایی نقاط ضعف این سیستم‌ها و مداخلات سیاسی مؤثر در تقویت اجزای ضعیف‌تر و اشتراک گذاری نتایج با سایر دولت‌ها، از جمله {ارزیابی} جنبه‌های حساسیت جنسی {این سیستم‌ها}؛
و. به رسمیت شناختن نیاز به ارتقای محرک‌های اساسی سیستم‌های نوآوری و سایر روش‌های مربوط مبتنی بر ابزار سیاسی گوناگون، جهت پشتیبانی از اولویت‌های توسعه علم، فناوری و نوآوری، به‌منظور تقویت همبستگی چنین سیستم‌هایی برای توسعه؛
ز. پیشنهاد سیاست‌های مناسب که از توسعه زیست بوم‌های دیجیتال حمایت می‌کنند، در نظر گرفتن قابلیت فناوری‌های دیجیتال نوظهور در به حرکت درآوردن فناوری‌های فراگیر موجود جهت توسعه، در نظر گرفتن چارچوب اجتماعی-اقتصادی و سیاسی کشورها و جذب و پشتیبانی از سرمایه گذاری و نوآوری خصوصی به‌ویژه تشویق توسعه محتوا و کارآفرینی محلی؛
ح. اجرای برنامه‌ها و ابتکاراتی که سرمایه گذاری و مشارکت در اقتصاد دیجیتال را تشویق و تسهیل می‌نماید؛

ط. همکاری با تمامی ذی‌نفعان مربوط، ارتقای به‌کارگیری فناوری‌های اطلاعات و ارتباطات در تمام بخش‌ها، بهبود پایدارپذیری محیطی؛

ی. پشتیبانی از اقدامات و سیاست‌های کشورهای در حال توسعه در زمینه علم و فناوری از طریق همکاری شمال-جنوب و جنوب-جنوب، ضمن توجه به تکمیل {سیاست‌ها} نه جایگزینی آن‌ها، تشویق مساعدت‌های مالی و فنی، ظرفیت‌سازی، انتقال فنی در زمینه موضوعات، ملاحظات، برنامه‌ها یا دوره‌های آموزشی مورد توافق متقابل؛

۲. کمیسیون تشویق می‌شود تا:

ا. نقش خود را به‌عنوان پیشگام علم، فناوری و نوآوری ادامه دهد و مشورت سطح بالایی را در خصوص موضوعات مرتبط با علم، فناوری، مهندسی و نوآوری، به شورای اقتصادی و اجتماعی و مجمع عمومی ارائه نماید؛

ب. از طریق اقدام در قالب مجمعی برای برنامه ریزی راهبردی، آینده نگاری در خصوص روندهای حیاتی در علم، فناوری و نوآوری در بخش‌های کلیدی اقتصاد، توجه به فناوری‌های جدید و نوظهور، به شفاف‌سازی نقش مهم فناوری‌های اطلاعات و ارتباطات و علم، فناوری و نوآوری به‌عنوان یک توانمندساز کمک نماید؛

ج. آگاهی و تسهیل شبکه سازی و مشارکت میان سازمان‌ها و شبکه‌های آینده نگاری فناوری در همکاری با سایر ذی‌نفعان را ارتقای دهد؛

د. از تلاش جهت ظرفیت‌سازی برای توسعه، استفاده و به‌کارگیری فناوری‌های جدید و موجود در کشورهای در حال توسعه به‌ویژه کشورهای کمتر توسعه‌یافته، دولت‌های جزیره‌ای کوچک در حال توسعه و کشورهای در حال توسعه محاط در خشکی، پشتیبانی نماید؛

هـ. مشارکت‌های جهانی علم، فناوری و نوآوری برای توسعه پایدار به شکل فعال را تجدید و تقویت نماید. {این کار} مستلزم تعامل کمیسیون در {حوزه‌های زیر} می‌باشد:

- انتقال {موضوع} آینده نگاری فناوری به طرف بسط قلمرو پروژه‌های ویژه بین‌المللی با هدف تحقیق، توسعه و به‌کارگیری فناوری و ابتکارات جهت ظرفیت‌سازی منابع انسانی برای علم، فناوری و نوآوری؛

- یافتن مدل‌های ابتکاری تأمین مالی و {تحقیق} سایر منابعی که ظرفیت‌های کشورهای در حال توسعه در زمینه همکاری در پروژه‌ها و ابتکارات تشریک مساعی در {حوزه} علم، فناوری و نوآوری را ارتقای می‌دهد؛

و. از تلاش کشورها در خصوص شناسایی بیشتر روندهای {مربوط به} موضوعاتی درباره نیازهای ظرفیت‌سازی، از جمله از طریق آینده نگاری، پشتیبانی نماید؛

ز. ظرفیت‌سازی و همکاری با مؤسسات مرتبط با تحقیق و توسعه از جمله سازمان‌های تخصصی ملل متحد، و فعالیت در زمینه تسهیل تقویت سیستم‌های نوآوری را ارتقای دهد،

از جمله سیستم هایی که از تقویت تلاش های نوآوران جهت همکاری در دستیابی به توسعه پایدار، به ویژه در کشورهای در حال توسعه، پشتیبانی می نماید؛

ح. بر اهمیت همکاری کمیسیون در ارتباط با اجرا و تعقیب حوزه های فناوری اطلاعات و ارتباطات و علم، فناوری و نوآوری مرتبط با اهداف توسعه پایدار، با رئیس کمیسیون تأکید کند، { این همکاری } در خصوص ارائه گزارش از بررسی ها و نشست های شورای اقتصادی اجتماعی، مجمع سیاسی سطح بالا درباره توسعه پایدار و سایر مجامع مربوط { می باشد }؛

۳. کنفرانس سازمان ملل برای تجارت و توسعه تشویق می شود تا:

أ. به شکل فعال و به نحو مقتضی، در خصوص همکاری نزدیک با سازمان های ملل متحد و سازمان های بین المللی، جهت تأمین مالی به منظور گسترش بازنگری های خط مشی علم، فناوری و توسعه تلاش نماید، { خط مشی هایی که در آن } بر نقش حیاتی فناوری های اطلاعات و ارتباطات در توانمندسازی علم، فناوری و نوآوری، مهندسی ظرفیت سازی، به کارگیری و اجرای توصیه های منتج از این بازنگری ها تأکید می گردد؛

ب. در بازنگری های خط مشی های علم، فناوری و نوآوری و فناوری های اطلاعات و ارتباطات، تسهیل مولفه های مشمول در آینده نگاری راهبردی و ارزیابی زیست بوم دیجیتال را بررسی و تحقیق نماید، و در صورت امکان فصلی از این خط مشی ها را به این موضوعات اختصاص دهد؛ ج. برای به روزرسانی دوره ای پیشرفت های حاصل شده در بازنگری های خط مشی علمی، فناوری و نوآوری در کشورهایی که { این بازنگری ها } در آن ها اجرا شده است، برنامه ریزی نماید و از این کشورها جهت ارائه گزارش به کمیسیون علم و فناوری برای توسعه در خصوص پیشرفته های حاصل شده، دروس آموخته شده و چالش های پیش رو در اجرای توصیه ها دعوت نماید.



جدول ۶: مشخصات سایر قطعنامه‌های علم، فناوری و نوآوری برای توسعه ۲۰۰۹ تا ۲۰۱۸

شماره اجلاس	شماره قطعنامه	سال صدور قطعنامه
۲۰۰۹	E/RES/2009/8	۲۰۰۹
۲۰۱۰	E/RES/2010/3	۲۰۱۰
۲۰۱۱	E/RES/2011/17	۲۰۱۱
۲۰۱۲	E/RES/6/2012	۲۰۱۲
۲۰۱۳	E/RES/10/2013	۲۰۱۳
۲۰۱۴	E/RES/28/2014	۲۰۱۴
۲۰۱۵	E/RES/27/2015	۲۰۱۵
۲۰۱۶	E/RES/23/2016	۲۰۱۶
۲۰۱۷	E/RES/22/2017	۲۰۱۷
۲۰۱۸	E/RES/29/2018	۲۰۱۸

بند دو: قطعنامه ارزیابی پیشرفت های صورت گرفته در اجرا و تعقیب نتایج اجلاس سران درباره جامعه اطلاعاتی سال ۲۰۱۸



شورای اقتصادی و اجتماعی
کمیسیون علم و فناوری برای توسعه

ترجمه سند

تاریخ انتشار: ۷ آگوست ۲۰۱۸

شماره قطعنامه: E/RES/2018/28

زبان: انگلیسی

توزیع: عمومی

اجلاس ۲۰۱۸

دستور کار ۱۸

قطعنامه مصوب شورای اقتصادی و اجتماعی مورخ ۲۴ جولای ۲۰۱۸

بر اساس توصیه کمیسیون علم و فناوری برای توسعه (E/2018/31)

ارزیابی پیشرفت های صورت گرفته در اجرا و تعقیب نتایج اجلاس سران درباره جامعه اطلاعاتی

شورای اقتصادی و اجتماعی؛

با یادآوری اسناد {مربوط به} نتایج اجلاس سران درباره جامعه اطلاعاتی، همچنین با یادآوری قطعنامه خود {به شماره} ۲۰۰۶/۴۶ مورخ ۲۸ جولای ۲۰۰۶ درباره تعقیب اجلاس سران و بررسی کمیسیون علم و فناوری برای توسعه و {بازنگری} دستور کاری که {شورای اقتصادی و اجتماعی} به کمیسیون واگذار کرده است؛

با یادآوری بیشتر قطعنامه خود {به شماره} ۲۰۱۷/۲۱ مورخ ۱۶ جولای ۲۰۱۷ درخصوص ارزیابی پیشرفت در اجرا و تعقیب نتایج اجلاس سران، با یادآوری قطعنامه مجمع عمومی {به شماره} ۷۰/۱ مورخ ۲۵ سپتامبر ۲۰۱۵ با عنوان «تبدیل دنیای ما: دستور کار توسعه پایدار» همچنین با یادآوری قطعنامه مجمع عمومی {به شماره} ۷۰/۱۲۵ مورخ ۱۶ دسامبر ۲۰۱۵، با عنوان «سند نتایج نشست سطح بالای مجمع عمومی درخصوص بازنگری کلی اجرای نتایج اجلاس سران درباره جامعه اطلاعاتی» که در آن سند، مجمع عمومی، نگرش و دیدگاه اجلاس سران برای {ایجاد} یک جامعه اطلاعاتی مردم محور، فراگیر و توسعه محور را تأیید می نماید که در آن همه بتوانند اطلاعات و دانش تولید کنند، {به آنها} دسترسی داشته باشند و از آن بهره مند شوند و به اشتراک گذارند، {و همچنین اینکه} اشخاص توانمند، جوامع و مردم

با مبنا قرار دادن اهداف و اصول منشور ملل متحد و احترام کامل و حمایت از اعلامیه جهانی حقوق بشر {توانند} به قابلیت‌های کامل خود در زمینه ارتقای توسعه پایدار و بهبود کیفیت زندگی خود دست یابند؛

با یادآوری بیشتر قطعنامه مجمع عمومی {به شماره} ۷۲/۲۰۰ مورخ ۲۰ دسامبر ۲۰۱۷ درباره فناوری اطلاعات و ارتباطات برای توسعه، با توجه توأم با خرسندی از گزارش دبیرکل درخصوص پیشرفت در اجرا و تعقیب نتایج اجلاس سران در سطوح منطقه‌ای و بین‌المللی، با ابراز قدردانی خود از دبیرکل کنفرانس تجارت و توسعه سازمان ملل، به جهت ایفای نقش در کمک حصول اطمینان از تکمیل بموقع گزارش فوق؛

با توجه توأم با قدردانی از برگزاری چهاردهمین اجلاس کنفرانس تجارت و توسعه سازمان ملل متحد در نایروبی از ۱۷ تا ۲۲ جولای ۲۰۱۶، و سند خروجی آن با عنوان «نتیجه و خروجی نایروبی: از تصمیم تا اقدام: حرکت به سوی محیط اقتصادی فراگیر و عادلانه جهانی برای توسعه و تجارت»،

بررسی: بازنگری اجرای نتایج اجلاس سران درباره جامعه اطلاعاتی؛

۱. از اجرای کامل قطعنامه مجمع عمومی {با شماره} ۷۰/۱۲۵ استقبال می‌نماید و بر {آن} پافشاری می‌نماید؛

۲. از (نظرهای) مختلف و سازنده تمام ذی‌نفعان در بررسی کلی پیشرفت اجرای نتایج اجلاس سران درباره جامعه اطلاعاتی استقبال می‌نماید؛

۳. مجدداً تعهد خود را بر اجرای کامل نتایج و نظر بازنگری ده ساله اجلاس سران بعد از ۲۰۱۵ تأیید می‌نماید؛

۴. مجدداً تعهدات ایجاد شده در قطعنامه مجمع عمومی {به شماره} ۷۰/۱۲۵ جهت از بین بردن شکاف‌های دیجیتال از جمله رفع شکاف دیجیتالی جنسیتی بین مناطق مختلف یک کشور و همچنین بین کشورهای مختلف را تأیید می‌نماید که از طریق تلاش در بهبود اتصالات، کم‌هزینه بودن، دسترسی به اطلاعات و دانش، محتوای چندزبانی، مهارت‌ها و سواد دیجیتال قابل حصول است. با اذعان به چالش‌های خاص پیش رو و نیازهای ویژه که افراد معلول و گروه‌های آسیب‌پذیر با آن مواجه هستند؛

۵. هماهنگی نزدیک بین فرایند اجلاس سران و دستور کار توسعه پایدار را بنا بر تقاضای قطعنامه مجمع عمومی {به شماره} ۷۰/۱۲۵ مورد تشویق قرار می‌دهد {همچنین} سهم میان بر فناوری اطلاعات و ارتباطات را در اهداف توسعه پایدار و ریشه‌کنی فقر برجسته می‌نماید، و اینکه دسترسی به فناوری‌های اطلاعات و ارتباطات یک شاخص برای توسعه و فی‌نفسه (به خودی خود) به یک آرزو بدل شده است را مورد توجه و اشاره قرار می‌دهد؛

۶. از تکامل و گسترش قابل توجه فناوری‌های اطلاعات و ارتباطات که توسط همکاری‌های بخش‌های عمومی و خصوصی پایه‌ریزی شده است، که به نظر می‌رسد تقریباً در هر گوشه جهان ورود و نفوذ کرده است، استقبال می‌نماید، {همچنین} ضمن توجه به چالش‌های نوظهور و منحصر به فرد مرتبط با تکامل و گسترش {این فناوری‌ها}، از ایجاد فرصت‌های جدیدی برای تعامل اجتماعی، توانمندسازی الگوهای نوین تجارت، مشارکت در رشد و توسعه اقتصادی در کل بخش‌های دیگر {توسط این فناوری‌ها} استقبال می‌نماید؛

۷. توجه توأم با نگرانی از اینکه هنوز شکاف‌های دیجیتالی قابل توجهی از قبیل شکاف بین کشورها و همچنین شکاف بین مناطق مختلف در داخل یک کشور و بین زنان و مردان وجود دارد، که برای مقابله با آن‌ها لازم است در کنار اقدامات دیگر، برای تقویت توانمندی‌های محیط‌های سیاسی و همکاری‌های بین‌المللی با هدف بهبود کم‌هزینه کردن، دسترسی، آموزش، ظرفیت‌سازی، چندزبانی، صیانت فرهنگی، سرمایه‌گذاری و تأمین مالی مناسب اقدام شود، {همچنین} بر وجود تقسیم جنسیتی به‌عنوان بخشی از شکاف‌های دیجیتالی اذعان می‌دارد و تمامی ذی‌نفعان را جهت حصول اطمینان از مشارکت کامل دختران و زنان در جامعه اطلاعاتی و دسترسی زنان به فناوری‌های جدید، به‌ویژه فناوری‌های اطلاعات و ارتباطات برای توسعه، تشویق می‌نماید؛

۸. کمیسیون علم و فناوری برای توسعه را تشویق می‌نماید تا مطابق قطعنامه مجمع عمومی {به شماره} ۷۲/۲۴۲ سال ۲۰۱۷، تأثیر تغییرات کلیدی سریع فناورانه روی دستیابی به اهداف توسعه پایدار را در محدوده دستور کارهای مربوط و منابع موجود، مورد نظر قرار دهند؛

۹. همچنین از برگزاری جشن سالانه روز جهانی جامعه مخابرات و اطلاعات در هفدهم می تحت مدیریت اتحادیه بین‌المللی مخابرات استقبال می‌نماید؛

۱۰. به تداوم اجرای نتایج اجلاس سران توجه می‌نماید، {همچنین} با تأکید ویژه بر ماهیت چنددلی‌نفعی خود، نقش‌هایی که در این رابطه توسط سازمان‌های برجسته به‌عنوان تسهیل‌کنندگان خط اقدام ایفا می‌شود، و نقش‌های کمیسیون‌های منطقه‌ای و گروه‌های سازمان ملل متحد درباره جامعه اطلاعاتی {توجه می‌نماید} و قدردانی خود را از نقش کمیسیون علم و فناوری برای توسعه به خاطر مساعدت به شورای اقتصادی و اجتماعی که به‌عنوان نقطه کانونی در سیستم عریض و گسترده که به دنبال تحقق نتایج اجلاس سران هستند، بیان می‌نماید؛

۱۱. ارزش و اصل همکاری چنددلی‌نفعی و تعاملاتی که فرایند اجلاس سران از بدو امر، آن را ترسیم کرده و به وضوح در دستور کار توسعه پایدار شناخته شده است را به رسمیت می‌شناسد و به فعالیت‌هایی که اهداف اجلاس سران و توسعه پایدار را مورد حمایت قرار داده و توسط دولت‌ها، سازمان‌های بین‌المللی، بخش خصوصی، جامعه مدنی، جوامع دانشگاهی و فنی و مشارکت‌کنندگان چنددلی‌نفعی، در نقشها و مسؤلیتهای مربوط خود، به کار گرفته می‌شوند، توجه می‌نماید؛

۱۲. بر اهمیت همکاری میان فرایند پیگرد و بازنگری اجلاس سران و سازوکار تسهیل فناوری برای اهداف توسعه پایدار ۱۲. بر اهمیت همکاری میان فرایند پیگرد و بازنگری اجلاس سران و سازوکار تسهیل فناوری برای اهداف توسعه پایدار تأکید می‌کند و ادامه این روند را مورد تشویق قرار می‌دهد. از جمله مجمع چنددلی‌نفعی درباره علم، فناوری و نوآوری را که در راستای اهداف توسعه پایدار فعالیت می‌کند؛

۱۳. به گزارش‌های بسیاری از نهادهای سازمان ملل که به‌عنوان ورودی اطلاعات اولیه برای تهیه جزئیات گزارش سالانه دبیرکل سازمان ملل متحد به «کمیسیون علم و فناوری برای توسعه» ارائه شده است و در تارنمای (وبسایت) کمیسیون به‌عنوان دستور کار شورا (اقتصادی و اجتماعی) در قطعنامه {به شماره} ۲۰۰۷/۸ مورخ ۲۵ جولای ۲۰۰۷ منتشر گردیده است، توجه می‌نماید، و اهمیت هماهنگی نزدیک میان تسهیل‌کنندگان برجسته خط اقدام و {همکاری با} دبیر کمیسیون را یادآوری می‌نماید؛

۱۴. همان‌گونه که در گزارش دبیرکل در خصوص پیشرفت اجرا و تعقیب نتایج گزارش اجلاس سران در سطوح منطقه‌ای و بین‌المللی دیده شده است، به اجرای نتایج اجلاس سران در سطح

منطقه‌ای که توسط کمیسیون های منطقه‌ای تسهیل گردیده است، توجه می‌نماید، از جمله موارد مندرج در این گزارش می‌توان به گام های برداشته شده در این رابطه {اشاره نمود}؛ و تأکید بر نیاز به ادامه پرداختن به مسائل خاص مورد علاقه هر منطقه، تمرکز بر چالش‌ها و موانعی که ممکن است در رابطه با اجرای کلیه اهداف و اصول ایجاد شده توسط اجلاس سران با آن مواجه شد، با توجه ویژه به فناوری اطلاعات و ارتباطات اشاره نمود؛

۱۵. اهمیت حفظ فرایند هماهنگی چنددلی‌نفعی در اجرای نتایج اجلاس سران از طریق ابزار مؤثر، با هدف تشویق همکاری و مشارکت میان تمام ذی‌نفعان، از جمله سازمان‌های بین‌المللی، {و اهمیت} تبادل اطلاعات میان تسهیل‌کنندگان خط اقدام و سایر ذی‌نفعان، شناسایی موضوعاتی که نیاز به بهبود {اصلاح} و بحث در خصوص چگونگی گزارش دهی در سراسر فرایند اجرا دارد را تکرار می‌نماید {تصریح می‌نماید}؛

۱۶. تمام ذی‌نفعان را به تداوم همکاری اطلاعاتی برای پایگاه داده‌های موجود که توسط اتحادیه بین‌المللی مخابرات برای اجرای اهداف اتخاذ شده توسط اجلاس سران دایر شده، تشویق می‌نماید و از نهادهای سازمان ملل جهت به‌روزرسانی اطلاعات در مورد طرح‌های خود در پایگاه داده‌های موجود دعوت می‌نماید؛

۱۷. بر نیاز ضروری به الحاق توصیه‌های مندرج در اسناد نتایج اجلاس سران در دستورالعمل‌های تجدید نظر شده {توسط این اجلاس} برای تیم های کشورهای عضو سازمان ملل در خصوص مهیا کردن ارزیابی‌های مشترک کشوری و چارچوب‌های مساعدت توسعه سازمان ملل تأکید می‌نماید، از جمله {توصیه‌هایی مبتنی بر مساعدت اجلاس سران جهت} افزودن فناوری اطلاعات و ارتباطات برای بخش توسعه که برای گروه جامعه اطلاعاتی سازمان ملل پیشنهاد کرده است؛

۱۸. قطعنامه مجمع عمومی {به شماره} ۶۰/۲۵۶ مورخ ۲۷ مارس ۲۰۰۶ را یاد آوری می‌نماید که در آن، مجمع از شورای اکوسوک درخواست کرده است که بر سیستم باز پیگیری نتایج مراحل اجلاس سران در ژنو و تونس نظارت نماید؛

۱۹. همچنین یاد آوری می‌نماید که مجمع عمومی در قطعنامه خود {به شماره} ۷۰/۱۲۵ تداوم ارائه گزارش‌های سالانه به شورا {شورای اقتصادی و اجتماعی} در خصوص اجرای نتایج

اجلاس سران را از طریق کمیسیون علم و فناوری برای توسعه، تقاضا کرده است و مجدداً نقش کمیسیون، در خصوص مساعدت به شورا به عنوان نقطه کانونی در سیستم باز پیگیری، به ویژه بررسی و ارزیابی پیشرفت‌های ایجاد شده در اجرای نتایج اجلاس سران، همان گونه که در قطعنامه شورا {به شماره} ۲۰۰۶/۴۶ معین شده است را تأیید می‌نماید؛

۲۰. از تمامی دولت‌ها درخواست می‌نماید در راستای ایجاد جامعه اطلاعاتی، گام‌هایی را جهت اجتناب و خودداری از اتخاذ اقدام یک جانبه‌ای که مطابق با قانون بین‌المللی و منشور سازمان ملل نیستند اتخاذ نماید، {اقدامات یک جانبه‌ای که} مانع دستیابی کامل توسعه اقتصادی و اجتماعی جمعیت کشورهای تحت تأثیر می‌شود و رفاه آن‌ها را به تعویق می‌اندازد؛

۲۱. از این واقعیت استقبال می‌نماید که رشد سریع در دسترسی به تلفنهای سیار {موبایل} و پهنای باند پس از سال ۲۰۰۵ به وقوع پیوست. این امر بدین معناست که در راستای اهداف اجلاس سران، حدود دو سوم از ساکنان دنیا به فناوری اطلاعات و ارتباطات دسترسی دارند، ۹۵ درصد از جمعیت جهان به شبکه‌های سیار با ۷/۴ میلیارد مشترک دسترسی دارند و ۴۸ درصد از جمعیت جهان از اینترنت استفاده می‌نمایند

۲۲. توأم با نگرانی زیاد به این {موضوعات} توجه می‌نماید که تعداد زیادی از کشورهای در حال توسعه فاقد دسترسی کم‌هزینه به فناوری‌های اطلاعات و ارتباطات هستند و اینکه برای اکثریت {کشورهای} فقیر، نوید و انتظار از علم و فناوری، از جمله فناوری‌های اطلاعات و ارتباطات محقق نشده، و بر نیاز به تهیه فناوری به شکل اثربخش، از جمله فناوری‌های اطلاعات و ارتباطات و ارتقای سواد دیجیتال جهت پرکردن شکاف‌های دیجیتالی و دانشی تأکید می‌نماید؛

۲۳. اینکه فناوری اطلاعات و ارتباطات فرصت‌ها و چالش‌های جدیدی را ارائه می‌نماید {ایجاد می‌نماید} و اینکه نیاز مبرم به مقابله با موانع عمده‌ای که کشورهای در حال توسعه در دسترسی به فناوری‌های جدید با آن‌ها مواجه هستند، را به رسمیت می‌شناسد، {مقابله با موانع با اقداماتی از قبیل ایجاد} محیط توانمندساز مناسب، منابع کافی، زیرساخت، آموزش، ظرفیت، سرمایه، و اتصالات {اینترنتی} و نیز موضوعات مرتبط با مالکیت فناوری، استانداردها و جریانها، و در این رابطه

از تمامی ذی‌نفعان درخواست می‌نماید تا منابع کافی، ظرفیت‌سازی ارتقای یافته و انتقال دانش و فناوری به کشورهای در حال توسعه، به‌ویژه کشورهای کمتر توسعه‌یافته، (را جهت حرکت به سوی یک جامعه توانمند شده دیجیتالی و اقتصاد دانش بنیان فراهم نمایند؛

۲۴. همچنین رشد سریع در شبکه‌های دسترسی به پهنای باند، به‌ویژه در کشورهای توسعه یافته را به رسمیت می‌شناسد و بر نیاز به مقابله فوری علیه شکاف‌های دیجیتالی در (موضوعات) دسترسی پذیری، کم‌هزینه بودن، کیفیت دسترسی و استفاده از پهنای باند- بین کشورهای با درآمد بالا، متوسط و پایین و سایر مناطق تأکید می‌نماید، با تمرکز ویژه بر پشتیبانی از کشورهای کمتر توسعه‌یافته، دولت‌های کوچک جزیره‌ای در حال توسعه و قاره آفریقا؛ ۲۵. همچنین این امر که گذار به محیط ارتباطات سیار منجر به تغییرات قابل توجهی در الگوهای شغلی و تجاری اپراتورها می‌شود را به رسمیت می‌شناسد و بنابراین این موضوع نیازمند بازاندیشی (بازنگری) قابل توجهی است که باید در خصوص راه‌های استفاده اشخاص و جوامع از شبکه‌ها و تجهیزات، راهبردهای دولتی و راه‌هایی که شبکه‌های ارتباطاتی بتوانند جهت دستیابی به اهداف توسعه استفاده شوند، صورت گیرد؛

۲۶. (این موضوع را) به رسمیت می‌شناسد که باوجود کلیه تحولات و پیشرفت‌هایی که در برخی موارد مشاهده می‌شود، در تعداد کثیری از کشورهای در حال توسعه، فناوری‌های اطلاعات و ارتباطات و کاربردهای آن‌ها، هنوز برای اکثر مردم مخصوصاً آن‌هایی که در نواحی روستایی زندگی می‌کنند، دسترس پذیر و کم‌هزینه نیست؛

۲۷. همچنین (این موضوع را) به رسمیت می‌شناسد که تعداد کاربران اینترنت در حال رشد است و در برخی موارد، ماهیت شکاف دیجیتالی و علمی، از شکاف مبتنی بر فراهم بودن دسترسی به شکاف مبتنی بر کیفیت دسترسی و کیفیت اطلاعات و مهارت‌هایی که کاربران می‌توانند (در محیط اینترنت) کسب نمایند و ارزشی که آن‌ها می‌توانند از آن استنتاج نمایند، در حال تغییر می‌باشد؛ و در این رابطه، نیاز به اولویت بندی استفاده از فناوری‌های اطلاعات و ارتباطات از طریق رویکردهای ابتکاری، از جمله رویکردهای چندذی‌نفعی در راهبردهای توسعه ملی و منطقه‌ای را به رسمیت می‌شناسد؛

۲۸. در این رابطه، بر اهمیت حیاتی محتوی چندزبانی و محلی در جامعه اطلاعاتی تأکید می‌کند و بر تشویق کلیه ذی‌نفعان در ایجاد، دسترسی برخط به محتوای آموزشی، فرهنگی و علمی جهت ارتقای کیفیت دسترسی و تضمین امکان عرضه کلیه اقوام و فرهنگ‌ها و همچنین تضمین دسترسی به اینترنتی با کلیه زبان‌ها از جمله زبان‌های بومی، اصرار می‌نماید؛
۲۹. اهمیت ظرفیت‌سازی انسانی، محیطی توانمند و زیرساختی پویا در فناوری اطلاعات و ارتباطات را به رسمیت می‌شناسد، همچنین {اهمیت} ارتقای مشارکت‌های چندذی‌نفعی و مساعدت کشورها در تلاش جهت تقویت توانمندسازی نقش فناوری اطلاعات و ارتباطات برای حصول اهداف توسعه پایدار را {به رسمیت می‌شناسد} و به برگزاری کنفرانس جهانی توسعه مخابرات تحت عنوان کلی «فناوری اطلاعات و ارتباطات برای اهداف توسعه پایدار» توجه می‌نماید؛
۳۰. مصرانه تمرکز مستمر بر منافع توسعه حداکثری از طریق تجارت الکترونیکی، تجارت اینترنتی برای تمامی نوآوری‌هایی {ابتکاراتی} که رویکرد جدیدی را برای توسعه تجارت از طریق تبادلات الکترونیکی فراهم می‌نماید تأکید می‌نماید که طریق آن {رویکرد} به کشورهای در حال توسعه اجازه می‌دهد پشتیبانی از مساعدت فنی برای ظرفیت‌سازی در آمادگی تجارت الکترونیکی را آسان‌تر هدایت نمایند و اهدا کنندگان مالی را در داشتن تصویری شفاف از برنامه‌هایی که آن‌ها توانستند تأمین مالی نمایند، توانمند می‌سازند، اصرار می‌نماید؛
۳۱. در این رابطه، طرح ابتکاری کنفرانس تجارت و توسعه سازمان ملل (آنکتاد) در اجرای تحقیقات مربوط به آمادگی تجارت الکترونیکی سریع در کشورهای کمتر توسعه یافته را به رسمیت می‌شناسد که با مشارکت دیگر حامیان داوطلب مالی و سایر سازمان‌ها به منظور ارتقای آگاهی از فرصت‌ها و چالش‌های مرتبط با قدرت تجارت در کشورهای کمتر توسعه یافته صورت گرفت؛
۳۲. از برگزاری اولین و دومین اجلاس گروه کارشناسان بین‌دولتی درباره تجارت الکترونیکی و اقتصاد دیجیتالی استقبال می‌نماید و به توصیه‌های مربوط به سیاست‌ها و خط‌مشی‌های مورد وفاق که توسط این گروه‌ها در طول این دو اجلاس تصویب شده است توجه می‌نماید؛
۳۳. به گزارش جهانی کمیسیون پهنای باند برای توسعه پایدار با عنوان «وضعیت پهنای باند ۲۰۱۷»: پهنای باند تسریع کننده توسعه پایدار» توجه می‌نماید و به تلاش‌های مداوم کمیسیون

پهنای باند در زمینه ارتقای حمایت به بالاترین سطح ممکن جهت ایجاد محیطی توانمندساز برای اتصالات پهنای باند، به‌ویژه از طریق طرح‌های پهنای باند ملی، {همچنین} مشارکت بخش‌های عمومی و خصوصی جهت حصول اطمینان از اینکه چالش‌های دستورکار توسعه با ملحق شدن تمامی ذینفان با تأثیر مناسبی مواجه می‌شوند توجه می‌نماید؛

۳۴. به اقدام کمیسیون پهنای باند مربوط به اهداف ۲۰۲۵ در حمایت از «اتصال نیمه دیگر» و تلاش {آن کمیسیون} جهت برخط نمودن ۳/۸ میلیارد نفر از جمعیت جهان که به اینترنت متصل نیستند توجه می‌نماید؛

۳۵. قابلیت‌های متعدد اقتصاد دیجیتال در منافع اجتماعی، اجرای نتایج اجلاس سران و دستیابی به اهداف توسعه پایدار را به رسمیت می‌شناسد؛

۳۶. از بسیاری از ابتکارات سازمان‌های ملل متحد که از اجرای خطوط اقدام اجلاس سران پشتیبانی می‌کنند استقبال می‌نماید و تمامی تسهیل‌کنندگان خطوط اقدام را برای تداوم عملکرد به سوی اجرای خطوط اقدام تشویق می‌نماید؛

۳۷. همچنین از تأثیر اطلاعات در تمامی برنامه‌های سازمان آموزشی، علمی و فرهنگی ملل متحد {یونسکو} به‌منظور مساعدت کشورهای عضو در تدوین سیاست‌ها جهت از بین بردن شکاف دیجیتالی و {همچنین جهت} تضمین {ایجاد} جوامع دانشی عادلانه استقبال می‌نماید (تضمین دسترسی یکسان و عادلانه جوامع به دانش)؛

۳۸. همچنین از عملکرد اتحادیه بین‌المللی مخابرات در پشتیبانی از به‌کارگیری شبکه‌های پهنای باند بی‌سیم در کشورهای در حال توسعه از جمله {پشتیبانی از} آموزش کارشناسان محلی بیشتر استقبال می‌نماید؛

۳۹. عملکرد سازمان خواروبار و کشاورزی ملل متحد (فائو) در ارتقای دیجیتال فراگیر در آفریقا و سایر مناطق به‌منظور پشتیبانی از کاهش فقر و امنیت غذایی را به رسمیت می‌شناسد؛

۴۰. همچنین سازمان بین‌المللی کار را که در خصوص تأثیر تغییرات فناورانه روی مشاغل کار می‌کنند مورد تشویق قرار می‌دهد؛

۴۱. توجه توأم با قدردانی درباره عملکرد سازمان بهداشت جهانی در رصد جهانی بهداشت

الکترونیکی از جمله رسیدگی به چگونگی ثبت اطلاعات مربوط به سلامت، بهداشت ارتباطات راه دور، بهداشت الکترونیکی و {همچنین رسیدگی به} آموزش الکترونیکی که می‌تواند در اهداف مربوط به پوشش بهداشت در سطح جهانی مفید واقع شود؛

۴۲. توأم با نگرانی زیاد به این حقیقت که شرایط مشابه استفاده زنان از اینترنت ۱۲ درصد کمتر از مردان می‌باشد و در کشورهای کمتر توسعه یافته این نسبت ۳۱ درصد است، توجه می‌کند، {و} توجه‌ها را به سمت شکاف جنسیتی دیجیتال جلب می‌نماید، که به دسترسی و استفاده زنان از فناوری‌های اطلاعات و ارتباطات از جمله در آموزش، استخدام و سایر حوزه‌های توسعه اقتصادی و اجتماعی در راستای هدف {شماره ۵} توسعه پایدار در خصوص دستیابی به عدالت جنسی و توانمندسازی تمامی زنان و دختران پافشاری می‌نماید، از دولت‌های عضو درخواست می‌نماید تا تمامی اقدامات مناسب را به‌ویژه از طریق ارتقای قابل توجه آموزش و مشارکت زنان و دختران در فناوری‌های اطلاعات و ارتباطات، به‌عنوان کاربران، تولید کنندگان محتوا، کارمندان، مؤسسان شرکت‌ها، مبتکران و رهبران اتخاذ نمایند؛

۴۳. به بسیاری از ابتکارات هدفمند در پر کردن شکاف جنسیتی دیجیتال توجه می‌نماید، از جمله ابتکارات اتحادیه بین‌المللی مخابرات و سازمان آموزشی، علمی و فرهنگی ملل متحد (یونسکو)؛

۴۴. مجدداً تعهدات مربوط به توجه ویژه به چالش‌های منحصربه‌فرد و نوظهور فناوری اطلاعات و ارتباطات که تمامی کشورها مخصوصاً کشورهای در حال توسعه با آن روبرو هستند را تأیید نماید، همان‌گونه که بندهای مرتبط در قطعنامه مجمع عمومی {به شماره ۷۰/۱۲۵} نیز آمده است؛

۴۵. توجه می‌نماید، ضمن اینکه بنیاد محکم (و قوی) برای ظرفیت‌سازی در فناوری اطلاعات و ارتباطات در بسیاری از حوزه‌ها در رابطه با ایجاد جامعه اطلاعاتی گذاشته شده است، اما هنوز نیاز به ادامه تلاش‌ها برای مقابله با چالش‌های مداوم، به‌ویژه برای کشورهای در حال توسعه و کشورهای کمتر توسعه یافته وجود دارد، و توجه‌ها را به تأثیر مثبت توسعه عرضی ظرفیت جلب می‌نماید که، مؤسسات، سازمان‌ها و نهادهایی که با فناوری‌های اطلاعات و ارتباطات و موضوعات حکمرانی اینترنت سروکار دارند را درگیر می‌کنند؛

۴۶. نیاز به تمرکز روی سیاست های توسعه ظرفیت و پشتیبانی پایدار جهت ارتقای بیشتر تأثیر فعالیتها و ابتکارات در سطوح ملی و منطقه‌ای به منظور ارائه مشاوره، خدمات و پشتیبانی با نگاهی به ایجاد یک جامعه اطلاعاتی فراگیر، مردم‌محور و توسعه مدار را به رسمیت می‌شناسد؛

۴۷. با توجه به اینکه بروز و ظهور موضوعات ادامه می‌یابند، {موضوعاتی} مانند اپلیکیشن‌های (برنامه‌های کاربردی) مربوط به محیط الکترونیکی، میزان سهم و مشارکت فناوری‌های اطلاعات و ارتباطات برای هشدار سریع، کاهش تغییرات هوایی (اقلیمی)، شبکه‌های اجتماعی، مجازی سازی و پردازش ابری و خدمات، اینترنت هم‌زمان و خدمات مبتنی بر موبایل، امنیت سایبری، شکاف جنسیتی، حفاظت از حریم خصوصی برخط و توانمندسازی و حفاظت، به‌ویژه علیه استثمار و سوءاستفاده سایبری از گروه‌های آسیب‌پذیر جامعه، مخصوصاً کودکان و افراد جوان؛

۴۸. مجدداً تأیید می‌نماید که در سند صادر شده مربوط به بازنگری کلی اجرای خطوط اقدام اجلاس سران، مجمع عمومی سازمان ملل درخواست نمود تا مجمع مربوط به اجلاس سران درباره مجمع جامعه اطلاعاتی به صورت سالانه برگزار گردد، ارزش مجمع در ارتقای همکاری، مشارکت، نوآوری، تبادل تجربیات و روش‌های سودمند توسط تمامی ذی‌نفعان در زمینه فناوری‌های اطلاعات و ارتباطات برای توسعه پایدار را به رسمیت می‌شناسد.

۴۹. به برگزاری مجمع سران جهان درباره جامعه اطلاعاتی ۲۰۱۸ که تحت عنوان «قدرت نفوذ فناوری‌های اطلاعات و ارتباطات در ایجاد جوامع دانشی و اطلاعات جهتی دستیابی به اهداف توسعه پایدار» به میزبانی اتحادیه مخابرات بین‌المللی و سازماندهی مشترک اتحادیه، یونسکو، برنامه توسعه و کنفرانس توسعه و تجارت سازمان ملل متحد، در تاریخ ۱۹ تا ۲۳ مارس ۲۰۱۸ برگزار گردید توجه می‌نماید، {همچنین} از برگزاری مجمع سران جهان درباره جامعه اطلاعاتی ۲۰۱۹، مورخ ۸ تا ۱۲ آوریل ۲۰۱۹ در ژنو استقبال می‌نماید و به فرایند رایزنی باز به منظور تضمین مشارکت و شمولیت وسیع و گسترده مجمع توجه می‌نماید؛

۵۰. با عنایت به ماتریس اهداف توسعه پایدار اجلاس سران درباره جامعه اطلاعاتی که توسط کارگزاری‌های تخصصی سازمان‌های ملل متحد تعریف و ایجاد شده است، تسهیل کنندگان خط اقدام را به استفاده از طرح اقدام ژنو به عنوان چارچوبی برای شناسایی و تعیین اقدامات عملی به

منظور استفاده از فناوری‌های اطلاعات و ارتباطات با هدف کمک به حصول دستور کار توسعه پایدار تشویق می‌نماید؛

۵۱. تسهیل کنندگان خط اقدام اجلاس سران را برای تضمین هماهنگی با دستور کار توسعه پایدار تشویق می‌نماید. این امر باتوجه به کار جدید در خصوص اجرای نتایج اجلاس سران، مطابق با منابع و دستور کارهای موجود، صورت می‌گیرد؛

۵۲. اهمیت فراخوان مجمع عمومی از تمامی ذی‌نفعان برای تکامل فناوری‌های اطلاعات و ارتباطات، با حرکت به سمت رویکردهایی جهت اجرای اهداف توسعه پایدار را تصریح می‌نماید و {همچنین} درخواست خود {شورای اقتصادی و اجتماعی} از نهادهای سازمان ملل که خطوط اقدام اجلاس سران را تسهیل می‌نمایند جهت بررسی گزارش‌دهی و برنامه‌های کاری خود در پشتیبانی از دستور کار توسعه پایدار را تکرار می‌نماید.

حکمرانی اینترنت

۵۳. مجدداً نتایج اجلاس سران در ارتباط با حکمرانی اینترنت را تأیید می‌نماید، از قبیل فرایند همکاری ارتقای یافته و برگزاری مجمع حکمرانی اینترنت که توسط مجمع عمومی از طریق دو فرایند مجزا دنبال می‌شوند و اینکه دو فرایند ممکن است مکمل هم باشند را به رسمیت می‌شناسد؛

۵۴. همچنین بندهای ۳۴ تا ۳۷ و ۶۲ تا ۷۲ از دستور کار تونس را برای جامعه اطلاعاتی تأیید می‌نماید؛

۵۵. علاوه بر این بندهای ۵۵ تا ۶۵ قطعنامه مجمع عمومی {به شماره} ۷۰/۱۲۵ را تأیید می‌نماید؛ همکاری ارتقای یافته؛

۵۶. اهمیت همکاری ارتقای یافته آتی جهت توانمندسازی دولت‌ها، در یک موقعیت عادلانه، به منظور ایفای نقشها و مسئولیت‌های خود در موضوعات سیاست بین‌الملل عمومی وابسته به اینترنت را به رسمیت می‌شناسد، اما نه در موضوعات عملیاتی و فنی روزانه که تأثیری روی موضوعات سیاست بین‌الملل عمومی ندارند؛

۵۷. به تداوم عملکرد گروه کاری در زمینه همکاری ارتقای یافته توجه می‌نماید، که {این گروه کاری} توسط رئیس کمیسیون علم و فناوری برای توسعه و بنا به درخواست مجمع عمومی در قطعنامه خود {به شماره} ۷۰/۱۲۵، با هدف تهیه توصیه نامه هایی در خصوص چگونگی اجرای همکاری ارتقای یافته همان‌گونه که در دستور کار تونس دیده شده، ایجاد گردیده است، همچنین {به این موضوع} توجه نماید که گروه کاری درگیری کامل دولت‌ها و سایر ذی‌نفعان مرتبط به‌ویژه از کشورهای در حال توسعه و در نظر گرفتن تمامی دیدگاه‌های گوناگون و تخصص خود را تضمین خواهد کرد و {همچنین} مشارکت کنندگان در گروه کاری را جهت پیشبرد تلاش‌های آن‌ها در خصوص انجام دستور کار خود {دستور کار شورای اقتصادی و اجتماعی} تشویق می‌نماید؛

۵۸. همچنین به برگزاری ۵ نشست {توسط} کارگروه در فواصل سپتامبر ۲۰۱۶ تا ژانویه ۲۰۱۸، توجه می‌نماید، {این نشست‌ها} طبق آنچه در قطعنامه ۷۰/۱۲۵ مجمع عمومی مطرح شده است، در خصوص بحث درباره نظرهای ارسالی از جانب دولت‌های عضو و سایر ذی‌نفعان {بر گزار گردید}؛ ۵۹. گزارش رئیس کارگروه را که شامل مراجعی از متن کامل تمامی پیشنهادها و همکاری‌ها می‌باشد را مورد توجه قرار می‌دهد و سپاسگزاری خود را از رئیس و کلیه مشارکت کنندگان در خصوص ارائه نظرها و همکاری در عملکرد کارگروه بیان می‌نماید؛

۶۰. از پیشرفت مطلوب ایجاد شده در بسیاری از زمینه‌ها و اجماع {شکل گرفته} در خصوص ظهور برخی موضوعات توسط کارگروه، استقبال می‌نماید، ضمن اینکه {معتقد است هنوز} در خصوص تعدادی از موضوعات، واگرایی دیدگاه وجود دارد و در این رابطه از اینکه کارگروه نتوانسته است مطابق با آنچه در دستور کار تونس ترسیم شده بود، به توافقی جهت {ارائه} توصیه‌هایی درباره چگونگی اجرای بیشتر همکاری‌های ارتقای یافته دست یابد، ابراز تأثر می‌نماید؛

مجمع حکمرانی اینترنت

۶۱. اهمیت مجمع حکمرانی اینترنت و دستور کار آن را به‌عنوان یک مجمع برای گفتگوی چندذی‌نفعی درباره موضوعات مختلف، همان‌گونه که در بند ۷۲ دستور کار تونس منعکس؛

گردیده است، از جمله بحث درباره موضوعات سیاست عمومی مرتبط با عناصر کلیدی حکمرانی اینترنت، به رسمیت می‌شناسد؛

۶۲. تصمیم مجمع عمومی در قطعنامه خود {به شماره} ۷۰/۱۲۵ در خصوص تمدید وظایف مجمع حاکمیت اینترنت برای ده سال آتی، را یاد آوری می‌نماید که در طی این مدت مجمع باید ارائه پیشرفت در کیفیت های عملکردی و مشارکت ذی‌نفعان مرتبط از کشورهای در حال توسعه را دنبال نماید؛

۶۳. ظهور ابتکارات مجمع حکمرانی اینترنت در سطوح ملی و منطقه‌ای را به رسمیت می‌شناسد، رخ دادن {آن‌ها} در تمامی مناطق و پرداختن به رابطه و اولویت موضوعات حکمرانی اینترنت در مناطق یا کشور سازماندهی شده را به رسمیت می‌شناسد؛

۶۴. قطعنامه مجمع عمومی {به شماره} ۷۰/۱۲۵ را یاد آوری می‌نماید که در آن، مجمع عمومی سازمان ملل از «کمیسیون علم و فناوری برای توسعه» درخواست کرد که در گزارش‌دهی منظم خود، ملاحظات مقتضی را جهت تکمیل توصیه‌های مندرج در گزارش گروه کاری در خصوص اصلاحات مجمع حکمرانی اینترنت درباره کمیسیون مورد نظر قرار دهد؛

۶۵. به برگزاری یازدهمین نشست مجمع حکمرانی اینترنت به میزبانی دولت سوئیس در ژنو مورخ ۱۸ تا ۲۱ دسامبر ۲۰۱۷ تحت موضوع «شکل‌دهی آینده دیجیتالی خود» توجه می‌نماید؛

۶۶. از برگزاری سیزدهمین نشست مجمع حکمرانی اینترنت که در سه ماه آخر سال ۲۰۱۸ برگزار گردید، استقبال می‌نماید و {به این نکته} که در فرایند آماده‌سازی جلسه، توصیه‌های مندرج در گزارش گروه کاری درباره اصلاحات در خصوص مجمع حکمرانی اینترنتی تحت ملاحظه قرار می‌گیرند، توجه می‌نماید؛

۶۷. در آن زمینه، همچنین از پیشرفت مداوم حاصل از فعالیت صورت گرفته بین دو اجلاس مجمع حکمرانی اینترنت در خصوص شرایط مختلف اتصال میلیاردها کاربر برخط و توانمندسازی ائتلاف‌های پویا و بهترین انجمن‌های علمی و نیز همکاری‌های ایجاد شده توسط دو کشور و مجامع حکمرانی اینترنت منطقه‌ای استقبال می‌نماید؛

مسیر روبه جلو

۶۸. از نهادهای سازمان ملل متحد درخواست می‌نماید تا به همکاری فعالانه در زمینه اجرا و تعقیب نتایج اجلاس سران در سرتاسر سیستم سازمان ملل متحد ادامه دهند، {همچنین} گام‌های ضروری را بردارند و به یک جامعه اطلاعاتی مردم‌محور، فراگیر و توسعه‌مدار متعهد شوند و دستیابی به اهداف توسعه مورد قبول در سطح بین‌المللی از جمله {اهداف} مندرج دستورکار توسعه پایدار را تسریع نمایند؛

۶۹. از تمامی ذی‌نفعان درخواست می‌نماید تا به هدف مربوط به پر کردن شکاف‌های دیجیتالی، در اَشکال مختلف آن به‌عنوان یک حوزه نگرانی در اولویت توجه خود قرار دهد؛ همچنین درخواست می‌نماید تا راهبردهای کاملاً مفید و صحیحی به کارگیرند که به توسعه دولت الکترونیک کمک نمایند و {درخواست می‌نماید تا} به تمرکز روی سیاست‌ها و اپلیکیشن‌ها (برنامه‌های کاربردی) فناوری اطلاعات و ارتباطات با رویکرد توجه به قشر فقیر و ضعیف ادامه دهند، از جمله دسترسی به پهنای باند در سطح اجتماع محلی، با نگاهی به محدود کردن شکاف‌های دیجیتالی میان بخش‌ها و مناطق مختلف یک کشور و همچنین میان کشورهای مختلف (شکاف دیجیتالی فرمولیو فراملی) که به سوی ایجاد جوامع اطلاعاتی و دانشی پیش می‌روند؛ ۷۰. پافشاری می‌نماید تا تمامی ذی‌نفعان ایجاد و اتخاذ رویکردهای ابتکاری و نوآورانه را اولویت بندی نمایند، {رویکردهایی} که تدارک دسترسی جهانی به زیرساخت پهنای باند کم‌هزینه در کشورهای در حال توسعه و استفاده از خدمات پهنای باند مرتبط را به‌منظور تضمین توسعه فراگیر، جامعه اطلاعاتی توسعه‌مدار، مردم‌محور و حداقل کردن شکاف‌های دیجیتالی تهییج و تشویق خواهد کرد؛

۷۱. از سازمان‌های بین‌المللی و منطقه‌ای درخواست می‌نماید تا به ارزیابی و ارائه گزارش منظم در خصوص دسترس‌پذیری جهانی به فناوری‌های اطلاعات و ارتباطات با هدف ایجاد فرصت‌های عادلانه جهت رشد بخش‌های فناوری اطلاعات و ارتباطات در کشورهای در حال توسعه ادامه دهند؛

۷۲. پافشاری می‌نماید تا کلیه کشورها برای انجام تعهدات خود تحت دستورکار اقدام آدیس

آبابا در سومین کنفرانس بین‌المللی درباره تأمین مالی توسعه تلاش نمایند؛

۷۳. اهمیت شاخص‌های فناوری اطلاعات و ارتباطات در قالب داده‌های باز را به‌عنوان ابزار پایش و ارزیابی جهت سنجش شکاف دیجیتال میان کشورها و درون جوامع تصریح می‌نماید، {همچنین اهمیت این شاخص‌ها} را در آگاه‌سازی تصمیم‌سازی که سیاست‌ها و راهبردها را برای توسعه اجتماعی، فرهنگی و اقتصادی تدوین می‌نمایند، {تصریح می‌نماید} و بر اهمیت استانداردهای و هماهنگ‌سازی شاخص‌های قابل اطمینان و به‌طور مرتب و مداوم به‌روز رسانی شده تأکید می‌نماید؛

۷۴. اهمیت ابزار پایش دیجیتال که از گسترش و سنجش اهداف توسعه پایدار پشتیبانی می‌نماید را تأیید می‌نماید.

۷۵. اهمیت اشتراک‌گذاری رویه‌های برتر در تمامی سطوح را تصریح می‌نماید، و ضمن به رسمیت شناختن مزیت به‌کارگیری پروژه‌ها و ابتکاراتی که علاوه بر اهداف اجلاس سران، تمامی ذی‌نفعان را جهت معرفی و کاندیداتوری پروژه‌های خود برای اخذ جوایز پروژه سالانه اجلاس سران به‌عنوان بخش جداناپذیری از فرایند بررسی اجلاس سران، ضمن توجه به گزارش مربوط به تشریح توفیقات اجلاس سران تشویق می‌نماید؛

۷۶. از سازمان‌های ملل متحد و سایر سازمان‌ها و مجامع مرتبط درخواست می‌نماید، مطابق با نتایج اجلاس سران در بازنگری دوره‌ای روش‌شناسی‌ها برای شاخص‌های فناوری اطلاعات و ارتباطات، سطوح مختلفی از توسعه و اوضاع ملی را در نظر بگیرند و بدین منظور:

ا. دولت‌های عضو را تشویق می‌نماید تا داده‌های مرتبط با فناوری‌های اطلاعات و ارتباطات در سطح ملی را جمع‌آوری کنند و اطلاعات مربوط به مطالعات موردی کشور را به اشتراک گذارند و با سایر کشورها در خصوص برنامه‌های تبادل ظرفیت‌سازی همکاری نمایند؛

ب. کارگزاری‌های تخصصی ملل متحد و سایر سازمان‌ها و مجامع مرتبط را جهت ارتقای ارزیابی تأثیر فناوری‌های اطلاعات و ارتباطات روی توسعه پایدار، تشویق می‌نماید؛

ج. توجه توأم با قدردانی، به فعالیت موسوم به «مشارکت در سنجش فناوری اطلاعات و ارتباطات برای توسعه و گزارش سالانه سنجش جامعه اطلاعاتی» که جدیدترین روندها و آمارها

را در خصوص دسترسی و کم‌هزینه بودن فناوری‌های اطلاعات و ارتباطات و ارزیابی جهانی جوامع دانش و اطلاعات، از جمله شاخص توسعه فناوری اطلاعات و اطلاعات را فراهم می‌نماید؛ د. برنامه موسوم به «مشارکت در سنجش فناوری اطلاعات و ارتباطات» را به خاطر پیگیری

تصمیم ۴۰/۱۱۰ کمیسیون آمار مورخ ۱۱ مارس ۲۰۱۶، مورد تشویق قرار می‌دهد و در این زمینه توصیه می‌نماید که مشارکت کنندگان دستورالعملی را جهت بهبود همکاری با ذی‌نفعان مختلف در خصوص اهداف تولید موقوع و با کیفیت بالا آمار فناوری اطلاعات و ارتباطات و فواید بالقوه استفاده از داده‌های بزرگ برای آمارهای رسمی توسعه دهد؛

ه. به برگزاری پانزدهمین همایش مخابرات جهانی/شاخصهای فناوری اطلاعات و ارتباطات در تونس مورخ ۱۴ تا ۱۶ نوامبر ۲۰۱۷ توجه می‌نماید، همچنین به شانزدهمین {دوره این} همایش که از ۱۰ تا ۱۲ دسامبر ۲۰۱۸ برگزار خواهد شد توجه می‌نماید؛

۷۷. ضمن تأیید توأم با قدردانی از پشتیبانی مالی صندوق ویژه تونس توسط دولت‌های فنلاند، سوئیس و ایالات متحده آمریکا، جامعه بین‌الملل را برای همکاری‌های داوطلبانه در {این} صندوق دعوت می‌نماید، {این صندوق} توسط کنفرانس تجارت و توسعه سازمان ملل (آنکتاد) به منظور پشتیبانی از بررسی و ارزیابی عملکرد کمیسیون علم و فناوری برای توسعه در موضوع تعقیب اجلاس سران تشکیل گردیده است؛

۷۸. پیشنهاد مجمع عمومی در قطعنامه {شماره} ۷۰/۱۲۵ {مبنی بر} برگزاری نشست سطح بالایی درباره بازنگری کلی اجرای نتایج اجلاس سران در سال ۲۰۲۵ را یادآوری می‌نماید؛ ۷۹. توأم با قدردانی، به گزارش دبیرکل و بحث مرتبط در «کمیسیون علم و فناوری برای توسعه» در بیست‌ویکمین اجلاس خود، توجه می‌نماید؛

۸۰. بر اهمیت ارتقای جامعه اطلاعاتی فراگیر، با توجه ویژه به ازبین بردن شکاف‌های دیجیتال و پهنای باند، {و} در نظر گرفتن ملاحظات کشورهای در حال توسعه، جنسیت، فرهنگ و نیز جوانان و گروه‌های فاقد نماینده تأکید می‌نماید؛

۸۱. گفتگو و کار مداوم جهت اجرای همکاری ارتقای یافته، مورد تقاضاست همان‌گونه که مورد انتظار دستور کار تونس نیز می‌باشد؛

۸۲. از دبیرکل درخواست می‌نماید تا گزارشی سالیانه از اجرای توصیه‌های مندرج در قطعنامه حاضر و نیز سایر قطعنامه‌های شورا در خصوص ارزیابی کمی و کیفی فرایند اجرا و تعقیب نتایج اجلاس سران، را به « کمیسیون علم و فناوری برای توسعه»، ارائه نماید؛
نشست عمومی ۵۱ (۲۴ جولای ۲۰۱۸)

جدول ۶: مشخصات قطعنامه‌های ارزیابی پیشرفت‌های صورت گرفته در اجرا و تعقیب نتایج اجلاس سران درباره جامعه اطلاعاتی ۲۰۰۶ تا ۲۰۱۸

شماره اجلاس	شماره قطعنامه	سال صدور قطعنامه
۲۰۰۶	E/RES/2006/46	۲۰۰۶
۲۰۰۷	E/RES/2007/8	۲۰۰۷
۲۰۰۸	E/RES/2008/3	۲۰۰۸
۲۰۰۹	E/RES/ 2009/7	۲۰۰۹
۲۰۱۱	E/RES/2011/16	۲۰۱۱
۲۰۱۲	E/RES/2012/5	۲۰۱۲
۲۰۱۳	E/RES/2013/9	۲۰۱۳
۲۰۱۴	E/RES/2014/27	۲۰۱۴
۲۰۱۵	E/RES/2015/26	۲۰۱۵
۲۰۱۶	E/RES/2016/22	۲۰۱۶
۲۰۱۷	E/RES/2017/21	۲۰۱۷
۲۰۱۸	E/RES/2018/28	۲۰۱۸

شورای اقتصادی و اجتماعی سازمان ملل مبحث سه: کمیسیون پیشگیری از جرم و عدالت کیفری



شورای اقتصادی و اجتماعی

تاریخ: ۲۰۱۱

شماره قطعنامه: ۲۰/۷

زبان: انگلیسی

توزیع: عمومی

با یادآوری مجدد قطعنامه‌های مجمع عمومی {به شماره‌های} ۵۵/۵۹ مورخ ۴ دسامبر ۲۰۰۰، ۵۵/۶۳ مورخ ۴ دسامبر ۲۰۰۰، ۵۶/۱۲۱ مورخ ۱۹ دسامبر ۲۰۰۱، ۶۳/۱۹۵ مورخ ۱۸ دسامبر ۲۰۰۸، ۶۴/۱۷۹ مورخ ۱۸ دسامبر ۲۰۰۹ و ۶۵/۲۳۲ مورخ ۲۱ دسامبر ۲۰۱۰؛

همچنین با یادآوری مجدد قطعنامه شورای اقتصادی و اجتماعی ملل متحد {به شماره‌های} ۲۰۰۹/۲۲ مورخ ۳۰ جولای ۲۰۰۹، و نیز قطعنامه‌های شورا {به شماره‌های} ۲۰۰۷/۱۲ مورخ ۲۵ جولای ۲۰۰۷ و ۲۰۰۷/۱۹ مورخ ۲۶ جولای ۲۰۰۷ درباره راهبرد دفتر مقابله با مواد مخدر و جرم ملل متحد برای دوره زمانی ۲۰۰۸-۲۰۱۱؛

با در نظر گرفتن اعلامیه السالوادور مصوب دوازدهمین کنگره پیشگیری از جرم و عدالت کیفری ملل متحد، با عنوان «راهبردهای جامع برای چالش‌های جهانی: سیستم‌های پیشگیری از جرم و عدالت کیفری و توسعه آن در جهان در حال تغییر» که در آن به نقش {توسعه فناوری‌های اطلاعات و ارتباطات و استفاده فزاینده از اینترنت در ایجاد فرصت‌های جدیدی برای مجرمان، تسهیل در رشد جرم توجه گردید؛

ضمن آگاهی از چالش‌های پیش روی دولت‌ها در مبارزه با جرائم سایبری و با تأکید بر ضرورت تقویت مساعدت فنی و اقدامات ظرفیت‌ساز، بر اساس نیازهای ملی، جهت محافظت، پیگرد و مجازات استفاده از فناوری‌های اطلاعاتی برای اهداف مجرمانه؛

با اذعان بر اهمیت اقدام برای همکاری بین‌المللی به منظور تسهیل حفاظت، تحقیق، پیگرد و مجازات جرم سایبری از جمله از طریق مساعدت‌های فنی برای تصویب و اصلاح قانون ملی

ضمن استقبال از قطعنامه مجمع عمومی {به شماره} ۶۵/۲۳۰ مورخ ۲۱ دسامبر ۲۰۱۰ {مصوب} دوازدهمین کنگره پیشگیری از جرم و عدالت کیفری ملل متحد، و با توجه به اعلامیه السالوادور، که در آن دولت‌های عضو به دفتر مقابله با مواد مخدر و جرم ملل متحد توصیه کردند که باید، بنا به درخواست، در همکاری با دولت‌های عضو، سازمان‌های بین‌المللی مرتبط و بخش خصوصی، {زمینه} مساعدت‌های فنی و آموزشی به دولت‌ها جهت اصلاح تدوین قانون ملی و ظرفیت‌سازی مراجع ملی {در باب موضوعات مرتبط} با جرم سایبری را فراهم نمایند از جمله پیشگیری، کشف، تحقیق و پیگرد جرائم سایبری در تمامی اشکال آن و ارتقای امنیت شبکه‌های کامپیوتری؛ با برجسته نمودن کاربری (کاربردپذیری) کنوانسیون ملل متحد علیه جرائم سازمان‌یافته فراملی در تقویت همکاری‌های بین‌المللی برای محافظت، تحقیق و پیگرد جرائم سایبری با ماهیت جرائم سازمان یافته فراملی؛

با یادآوری مجدد (این موضوع که) مبارزه علیه سوءاستفاده مجرمانه از فناوری‌های اطلاعات، نیازمند توسعه راه‌حلی می‌باشد که توأمان محافظت از آزادی‌های شخصی و حریم خصوصی و ظرفیت حکومت‌ها برای مبارزه علیه چنین سوءاستفاده‌هایی را مورد نظر قرار می‌دهند. ضمن به رسمیت شناختن نقش دفتر مقابله با مواد مخدر و جرم ملل متحد در زمینه ایجاد مساعدت فنی از طریق برنامه‌های منطقه‌ای و موضوعی خود، و یادآوری اینکه {این دفتر} در توسعه و اجرای برنامه‌های مساعدت فنی خود باید {رسیدن به} نتایج پایدار و مداوم در محافظت، پیگرد و مجازات مجرمان مخصوصاً از طریق ایجاد، به‌روزرسانی و تقویت نظام‌های عدالت کیفری و نیز ارتقای حاکمیت قانون را هدف‌گیری نماید، و نیز {این دفتر} باید در یک مسیر یکپارچه و چشم‌اندازی دائم، چنین برنامه‌هایی را برای دستیابی به آن اهداف در تمامی اجزای نظام عدالت کیفری طراحی نماید، که به موجب {این برنامه‌ها} ظرفیت دولت‌های درخواست‌کننده برای ممانعت و توقف انواع مختلف جرم، از جمله جرائم سازمان یافته و جرم سایبری، که جوامع را تحت تأثیر قرار می‌دهد افزایش می‌یابد.

۱. از دفتر مقابله با مواد مخدر و جرم ملل متحد درخواست می‌نماید به همکاری خود با دولت‌های عضو، سازمان‌های منطقه‌ای و بین‌المللی مرتبط و عندالاقضاء، بخش‌های خصوصی {در زمینه}

مساعدت های فنی و آموزشی بر مبنای نیازهای ملی دولت های درخواست کننده ادامه دهند، به ویژه نیازهای مربوط به حفاظت، کشف تحقیق و پیگرد تمامی اشکال جرم سایبری بدون صدمه به عملکرد و نتایج نشست های گروه کارشناسان بین دولتی درباره مطالعه جامع راجع به مشکل جرم سایبری و پاسخگویی به آن توسط دولت ها، جامعه بین الملل و بخش خصوصی؛

۲. به نتایج و خروجی اولین اجلاس گروه کارشناسان درباره مطالعه جامع راجع به جرم

سایبری توجه می نماید؛

۳. از گروه کارشناسان درباره مطالعه جامع درباره جرم سایبری دعوت می نماید تا گزارش بررسی نشست اول خود را نهایی کند و از دبیرخانه { کمیسیون } درخواست می نماید که این گزارش ها را به شش زبان رسمی سازمان ملل برای دولت های عضو منتشر نماید و همچنین به پشتیبانی از نشست های گروه کارشناسان ادامه دهد.

۴. از دفتر مقابله با مواد مخدر و جرم ملل متحد درخواست می نماید، در زمینه مبارزه با جرم سایبری، همکاری { خود را } با دولت های عضو، سازمان های مرتبط مانند پلیس بین المللی (اینترپل)، اداره پلیس اروپا، اتحادیه بین المللی مخابرات، کمیسیون اروپا، شورای اروپا، سازمان همکاری های شانگهای و دولت های مستقل مشترک المنافع و نیز بخش خصوصی از جمله شرکت های کامپیوتری و خدمات دهندگان اینترنتی، تقویت نماید.

۵. دولت های عضو را دعوت می نماید تا به تبادل نظر در خصوص مسیرها و منابع جهت حصول بهتر مساعدت فنی، به ویژه چالش های احتمالی پیش روی دولت ها برای اهداف همکاری های بین المللی ادامه دهند، { همچنین } از گروه کارشناسان برای مطالعه جامعه درباره مشکل جرم سایبری دعوت می نماید تا این تبادل نظرها را در کار خود و در زمان مقتضی مورد ملاحظه قرار دهند.

۶. از دولت های عضو و سایر حامیان مالی داوطلبانه خارج از بودجه، دعوت می نماید تا در صورت لزوم و مطابق با قوانین و رویه های ملل متحد، بندهای مرتبط از قطعنامه حاضر را اجرا نمایند؛

۷. از دبیرکل درخواست می نماید تا گزارشی از اجرای قطعنامه حاضر را آماده و آن را در بیست و دومین نشست کمیسیون پیشگیری از جرم و عدالت کیفری، ارائه نماید.

مساعادت فنی و ظرفیت‌سازی برای تقویت اقدامات ملی و همکاری‌های بین‌المللی علیه باند دو: قطعنامه ارتقا
جرم سایبری سال ۲۰۱۳



شورای اقتصادی و اجتماعی
کمیسیون پیشگیری از جرم و عدالت کیفری

ترجمه سند

تاریخ انتشار: ۲۰۱۳

شماره قطعنامه: ۲۲/۸

زبان: انگلیسی

توزیع: عمومی

ارتقای مساعادت فنی و ظرفیت‌سازی برای تقویت اقدامات ملی و همکاری‌های بین‌المللی علیه جرم سایبری
کمیسیون پیشگیری از جرم و عدالت کیفری

با یادآوری قطعنامه‌های مجمع عمومی {به شماره‌های} ۵۵/۵۹ مورخ ۴ دسامبر ۲۰۰۰، ۵۵/۶۳ مورخ ۴ دسامبر ۲۰۰۰، ۵۶/۱۲۱ مورخ ۱۹ دسامبر ۲۰۰۱، ۶۳/۱۹۵ مورخ ۱۸ دسامبر ۲۰۰۸، ۶۴/۱۷۹ مورخ ۱۸ دسامبر ۲۰۰۹، ۶۵/۲۳۲ مورخ ۲۱ دسامبر ۲۰۱۰، ۶۶/۱۷۹ مورخ ۱۹ دسامبر ۲۰۱۱، ۶۶/۱۸۱ مورخ ۱۹ دسامبر ۲۰۱۱، ۶۷/۱۸۴ مورخ ۲۰ دسامبر ۲۰۱۲ و ۶۷/۱۸۹ مورخ ۲۰ دسامبر ۲۰۱۲؛

همچنین با یادآوری قطعنامه‌های شورای اقتصادی و اجتماعی {با شماره‌های} ۲۰۱۱/۳۳ مورخ ۲۸ جولای ۲۰۱۱ درباره پیشگیری، حفاظت و همکاری بین‌المللی علیه استفاده از فناوری‌های جدید اطلاعات در سوءاستفاده و استثمار کودکان و ۲۰۱۲/۱۹ مورخ ۲۷ دسامبر ۲۰۱۲ درباره تقویت همکاری بین‌المللی در مبارزه علیه جرم سازمان یافته فراملی در تمامی اشکال و مظاهر آن؛

با استقبال از قطعنامه مجمع عمومی {به شماره} ۶۵/۲۳۰ مورخ ۴ دسامبر ۲۰۱۰، درخصوص دوازدهمین کنگره سازمان ملل درباره پیشگیری از جرم و عدالت کیفری و باتوجه به توصیه دولت‌های عضو در اعلامیه سالوادور {با عنوان} «درباره راهبردهای جامع برای چالش‌های جهانی: سیستم‌های پیشگیری از جرم و عدالت کیفری و توسعه آن در یک جهان در حال تغییر» مبنی بر اینکه دفتر مقابله با مواد مخدر و جرم ملل متحد باید، بنا به درخواست، در همکاری با دولت‌های عضو،

سازمان‌های بین‌المللی مربوط و بخش خصوصی، {شرایط} مساعدت فنی و آموزشی به دولت‌ها را در امور زیر مهیا نماید:

اصلاح {بهبود} قانونگذاری ملی و ظرفیت‌سازی مراجع ملی به‌منظور رسیدگی به جرم سایبری، از جمله پیشگیری، کشف، تحقیق و پیگرد چنین جرائمی در کلیه اشکال خود و {همچنین} بالابردن امنیت شبکه‌های کامپیوتری.

باتوجه به قطعنامه شورای اقتصادی و اجتماعی {به شماره} ۲۰۰۵/۱۵ مورخ ۲۲ جولای ۲۰۰۵ که در آن شورا، اعلامیه بانکوک {با عنوان} «همکاری مشترک و مسئولیتها: اتحادهای راهبردی در زمینه پیشگیری از جرم و عدالت کیفری»، مصوب در یازدهمین کنگره سازمان ملل متحد در خصوص پیشگیری از جرم و عدالت کیفری، را امضاء کرد {و در آن} اهمیت اساسی اجرای اسناد موجود و توسعه بیشتر اقدامات ملی و همکاری‌های بین‌المللی در مسائل جزایی (کیفری)، از جمله جرم سایبر مجدداً توسط دولت‌های عضو تأیید شد و از کمیسیون پیشگیری از جرم و عدالت کیفری، دعوت گردید تا امکان همکاری بیشتر و مشارکت با سایر سازمان‌های تمرکز یافته، تحت پر توی سازمان ملل متحد، در حوزه‌های جزایی را بررسی نمایند.

با برجسته نمودن کاربری (کاربردپذیری) کنوانسیون ملل متحد علیه جرائم سازمان یافته فراملی در تقویت همکاری‌های بین‌المللی برای محافظت، تحقیق و پیگرد جرائم سایبری با ماهیت جرائم سازمان یافته فراملی، ضمن آگاهی از چالش‌های پیش روی دولت‌ها در مبارزه با جرائم سایبری و تأکید بر ضرورت تقویت مساعدت فنی و اقدامات ظرفیت‌ساز، بر اساس نیازهای ملی، جهت محافظت، پیگرد و مجازات استفاده از فناوری‌های اطلاعاتی برای اهداف مجرمانه، با استقبال از تلاش اخیر دفتر مقابله با مواد مخدر و جرم ملل متحد در تهیه {نسخه} نهایی برنامه جهانی درباره جرم سایبری در راستای اجرای دستور کار خود برای تأمین همکاری فنی و ظرفیت‌سازی درباره جرم سایبری، با در نظر گرفتن اینکه مساعدت‌های فنی که به‌منظور تقویت ظرفیت‌های پیشگیری از جرم و عدالت کیفری برای مقابله با جرم سایبری، صورت می‌گیرد منفعت و تأثیری مستقیم در این خصوص داشته و به تأمین نیازها با هدف ظرفیت‌سازی، کمک خواهد کرد.

از این رو، مخصوصاً با یادآوری مجدد قطعنامه خود {به شماره} ۲۰/۷ مورخ ۱۵ آوریل ۲۰۱۱ درباره ارتقای اقدامات مربوط به مبارزه با جرائم سایبری از جمله مساعدت‌های فنی و ظرفیت‌سازی:

۱. به خروجی {نتایج} دومین نشست گروه کارشناسان درباره اجرای مطالعه جامع درباره جرائم سایبری که در تاریخ ۲۵ تا ۲۸ فوریه ۲۰۱۳ در وین برگزار شد توجه می‌نماید، به‌ویژه مباحث مربوط به مطالعه و توجه به حمایت گسترده از ظرفیت‌سازی و مساعدت فنی و {همچنین} نقش دفتر مقابله با مواد مخدر و جرم ملل متحد در رابطه با این مباحث؛

۲. از دفتر مقابله با مواد مخدر و جرم ملل متحد دعوت می‌نماید تا با همکاری نزدیک با دولت‌های عضو، اجرای برنامه جهانی درباره جرم سایبری را پیش ببرند؛

۳. از دفتر مقابله با مواد مخدر و جرم ملل متحد درخواست می‌نماید تا در موعد مقرر، برنامه جهانی گروه کاری بین دولتی دائمی باز درباره جرم سایبری را در زمینه بهبود حاکمیت و وضعیت مالی آن دفتر ارائه نماید؛

۴. همچنین از دفتر مقابله با مواد مخدر و جرم ملل متحد درخواست می‌نماید تا بر مبنای نیازهای کشورهای متقاضی، همکاری {خود} با دولت‌های عضو، سازمان‌های مرتبط، بخش خصوصی و جامعه مدنی را در زمینه مساعدت فنی و ظرفیت‌سازی علیه جرم سایبری تقویت نمایند؛

۵. به‌علاوه از دفتر مقابله با مواد مخدر و جرم ملل متحد درخواست می‌نماید تا به‌عنوان مرکز ذخیره داده‌های مربوط به قوانین حوزه جرائم سایبری و دروس آموخته شده در زمینه جرائم سایبری، با نگاهی بر تسهیل {روند} ارزیابی مداوم نیازها و ظرفیت‌های عدالت کیفری و دریافت و همکاری در مساعدت‌های فنی عمل نمایند؛

۶. از دولت‌های عضو و سایر حامیان مالی داوطلبانه خارج از بودجه، دعوت می‌نماید تا در صورت لزوم و مطابق با قوانین و رویه‌های ملل متحد، قطعنامه حاضر را اجرا نمایند؛

۷. از مدیر اجرایی درخواست می‌نماید تا گزارشی در خصوص اجرای قطعنامه حاضر و عملکرد برنامه جهانی درباره جرم سایبری را آماده و آن را در بیست‌وسومین نشست کمیسیون پیشگیری از جرم و عدالت کیفری، ارائه نماید.

بند سه: قطعنامه تقویت همکاری بین‌المللی جهت مبارزه با جرم سایبری سال ۲۰۱۳



شورای اقتصادی و اجتماعی
کمیسیون پیشگیری از جرم و عدالت کیفری

ترجمه سند

تاریخ انتشار: ۲۰۱۳

شماره قطعنامه: ۲۲/۷

زبان: انگلیسی

توزیع: عمومی

تقویت همکاری بین‌المللی جهت مبارزه با جرم سایبری
کمیسیون پیشگیری از جرم و عدالت کیفری

با یادآوری مجدد قطعنامه مجمع عمومی (به شماره) ۶۵/۲۳۰ مورخ ۲۱ دسامبر ۲۰۱۰، که در آن مجمع با حمایت از اعلامیه السالوادور درباره «راهبردهای جامع برای مقابله با چالش‌های جهانی: سیستم‌های پیشگیری از جرم و عدالت کیفری و توسعه آن در جهان در حال تغییر» از کمیسیون پیشگیری از جرم و عدالت کیفری درخواست کرد تا: در راستای بند ۴۲ اعلامیه السالوادور، یک گروه کارشناسان بین‌دولتی باز توسط دولت‌های عضو، جامعه بین‌الملل و بخش خصوصی را به منظور انجام بررسی جامع درباره مسئله جرم سایبری و پاسخگویی به آن از جمله تبادل اطلاعات درباره {این موضوعات} تأسیس نماید: تدوین و تصویب قانون ملی، رویه‌های برتر، مساعدت فنی و همکاری بین‌المللی با نگاهی به بررسی گزینه‌ها جهت تقویت حقوق بین‌الملل موجود و ارائه حقوق بین‌الملل جدید یا سایر پاسخگویی‌ها به جرم سایبری؛

همچنین با یادآوری قطعنامه مجمع عمومی {به شماره} ۶۷/۱۸۹ مورخ ۲۰ دسامبر ۲۰۱۲ که در آن مجمع عمومی ضمن توجه توأم با قدردانی از عملکرد گروه کارشناسان بین‌دولتی باز جهت انجام مطالعه جامع درباره مسئله جرم سایبری، {این گروه} را جهت ارتقای تلاش‌هایش در خصوص تکمیل کار و ارائه نتیجه مطالعات خود به کمیسیون پیشگیری از جرم و عدالت کیفری در موعد مقرر تشویق نمود؛

ضمن در نظر گرفتن اعلامیه السالوادور، دولت‌های عضو به نقش {توسعه فناوری‌های اطلاعات

و ارتباطات و استفاده فزاینده از اینترنت در ایجاد فرصت‌های جدیدی برای مجرمان، تسهیل در رشد جرم توجه نمودند،

ضمن تأکید بر هماهنگی و همکاری‌های ارتقای یافته میان دولت‌ها جهت مبارزه با جرم سایبری، بر نقش ایفا شده توسط ملل متحد مخصوصاً کمیسیون پیشگیری از جرم و عدالت کیفری در این موضوع تأکید می‌نماید؛

با به رسمیت شناختن توأم با خرسندی از کار انجام شده در حوزه مبارزه با جرم سایبری توسط کمیسیون پیشگیری از جرم و عدالت کیفری در پرتو گروه کارشناسی بین دولتی باز که جهت مطالعه جامع درباره جرم سایبری تأسیس شده بود؛

۱. به مطالعه جامع درباره جرم سایبری که توسط دفتر مقابله با مواد مخدر و جرم ملل متحد و تحت گروه کارشناسان بین دولتی باز برای بررسی جامع درباره جرم سایبری انجام شده بود توجه می‌نماید و {همچنین} به بحث درباره محتوای دومین نشست این گروه که در تاریخ ۲۵ تا ۲۸ فوریه ۲۰۱۳ در وین برگزار گردید و در آن نگاه‌های مختلفی در رابطه با محتوا، یافته‌ها و انتخاب‌های موجود در این مطالعه بیان گردید نیز توجه می‌نماید؛

۲. خرسندی خود را از عملکرد گروه کارشناسان بین دولتی باز، تا کنون، بیان می‌دارد؛

۳. از دولت‌های عضو دعوت می‌نماید تا تحت پرتو کمیسیون پیشگیری از جرم و عدالت کیفری به رسیدگی درخصوص {این موارد} ادامه دهند: مسئله جرم سایبری، مبنای عملکرد گروه کارشناسان بین دولتی باز درباره انجام مطالعه جامع جرم سایبری که توسط این کمیسیون تشکیل شده است؛

۴. از دبیرخانه {کمیسیون} درخواست می‌نماید تا {سند} بررسی جامع درباره جرم با سایبری را به شش زبان رسمی سازمان ملل متحد ترجمه کند و آن را جهت تفسیر و به‌منظور ارزیابی گروه کارشناسان بین دولتی باز در اجرای دستور کار خود، در زمان مقتضی برای دولت‌های عضو منتشر نماید؛

۵. از گروه کارشناسان بین دولتی باز درخواست می‌نماید، تا به‌صورت مقتضی، با مساعدت دبیرخانه {کمیسیون} کار خود را به سوی اجرای دستور کار گروه ادامه دهند؛

۶. از گروه کارشناسان بین دولتی باز دعوت می‌نماید تا خلاصه‌ای از گزارش‌های بررسی نشست‌های اول و دوم خود را نهایی کند و از دبیرخانه { کمیسیون } درخواست می‌نماید که تصویب گروه کارشناسی، این گزارش‌ها را به شش زبان رسمی سازمان ملل برای دولت‌های عضو منتشر نماید؛

۷. به‌منظور تسهیل عملکرد گروه کارشناسان بین دولتی باز، مطابق با قوانین و رویه‌های ملل متحد، از دولت‌های عضو و سایر حامیان مالی داوطلبانه خارج از بودجه، دعوت می‌کند؛

۸. از گروه کارشناسان بین دولتی باز درخواست می‌نماید تا گزارشی را درباره پیشرفت عملکرد خود به کمیسیون پیشگیری از جرم و جرائم کیفری ارائه نماید.

بند چهار: قطعنامه تقویت همکاری بین‌المللی برای مبارزه با جرم سایبری سال ۲۰۱۷



شورای اقتصادی و اجتماعی
کمیسیون پیشگیری از جرم و عدالت کیفری

ترجمه سند

تاریخ انتشار: ۲۰۱۷

شماره قطعنامه: ۲۶/۴

زبان: انگلیسی

توزیع: عمومی

تقویت همکاری بین‌المللی برای مبارزه با جرم سایبری
کمیسیون پیشگیری از جرم و عدالت کیفری

با یادآوری قطعنامه مجمع عمومی {به شماره} ۶۵/۲۳۰ مورخ ۲۱ دسامبر ۲۰۱۰ که اعلامیه السالوادور در خصوص راهبردهای جامع برای چالش‌های جهانی: نظام‌های پیشگیری از جرم و عدالت کیفری و توسعه آن در جهان در حال تغییر را تأیید نمود و از کمیسیون پیشگیری از جرم و عدالت کیفری درخواست کرد تا در راستای بند ۴۲ اعلامیه السالوادور، یک گروه کارشناسی بین‌دولتی باز را جهت بررسی جامع مشکلات جرم سایبری و مسئولیت‌های دولت‌های عضو، جامعه بین‌المللی و بخش خصوصی در قبال (موضوعات مربوط از جمله این موارد) تشکیل دهد: تبادل اطلاعات در تدوین قانون ملی، رویه‌های برتر، مساعدت‌های فنی و همکاری بین‌المللی با نگاهی به تحلیل گزینه‌هایی به‌منظور تقویت قانون بین‌المللی یا ملی موجود و پیشنهاد قوانین جدید یا سایر مسئولیت‌ها در زمینه جرم سایبری؛

همچنین با یادآوری قطعنامه مجمع عمومی به شماره ۷۰/۱۷۴ مورخ ۱۷ دسامبر ۲۰۱۵ که در آن: اعلامیه دوحه را در خصوص گنجاندن {موضوع} پیشگیری از جرم و عدالت کیفری در دستور کار گسترده‌تر ملل متحد جهت مقابله با چالش‌های اقتصادی و اجتماعی و فراهم نمودن حاکمیت قانون در سطوح ملی و بین‌المللی و مشارکت عمومی تأیید نمود:

- توجه سران دولت‌ها و کشورها درباره فعالیت‌های گروه کارشناسان بین‌دولتی باز جهت انجام بررسی جامع مشکل جرائم سایبری و مسئولیت دولت‌های عضو، جامعه بین‌المللی و بخش

خصوصی جلب گردید؛

- از کمیسیون پیشگیری از جرم و عدالت کیفری دعوت نمود تا به پیشنهادهای مربوط به تداوم فعالیت گروه کارشناسان در خصوص {موضوع زیر} رسیدگی نماید:

تبادل اطلاعات درباره تدوین قانون ملی، رویه های برتر، مساعدت فنی و همکاری بین‌المللی با نگاهی به تحلیل گزینه‌هایی به منظور تقویت قانون بین‌المللی یا ملی موجود و پیشنهاد قوانین جدید یا سایر مسئولیت‌ها در زمینه جرم سایبری،

با یادآوری مجدد قطعنامه خود که در آن به موارد زیر توجه شده است:

- بررسی جامع درباره جرم سایبری که توسط دفتر مقابله با جرم و مواد مخدر سازمان ملل متحد و تحت حمایت گروه کارشناسان جهت انجام بررسی جامع جرم سایبری آماده گردید؛

- مباحث مطرح‌شده در محتوای مطالعه صورت‌گرفته (گزارش تحقیقی) در دومین نشست گروه کارشناسان در وین، که از تاریخ ۲۵ تا ۲۸ فوریه ۲۰۱۳ برگزار گردید و در آن نگاه‌های گوناگونی در رابطه با مفاد، یافته‌ها و گزینه‌های ارائه شده بیان گردیده است؛

از گروه کارشناسان درخواست گردید تا با همکاری دبیرخانه به فعالیت خود جهت تکمیل دستور کار خود ادامه دهد.

با یادآوری قطعنامه خود {به شماره} ۲۲/۸ مورخ ۲۶ آوریل ۲۰۱۳ که در آن کمیسیون به خروجی دومین نشست گروه کارشناسان توجه نمود، مخصوصاً در مباحثی که به بررسی‌های گسترده در مورد ظرفیت‌سازی، مساعدت فنی و نقش دفتر مقابله با جرم و مواد مخدر سازمان ملل در این باره توجه نموده است؛

با استقبال از تلاش‌های دفتر مقابله با جرم و مواد مخدر سازمان ملل متحد در ارتقای پاسخگویی مؤثر به تهدیدات جرم سایبری از جمله از طریق برنامه جهانی درباره جرم سایبری، همچنین با استقبال از خروجی سومین نشست گروه کارشناسان و توصیه‌های آن و ضمن اظهار قدردانی از کارهایی که تاکنون توسط گروه کارشناسان صورت گرفته:

- از گروه کارشناسان بین‌دولتی باز با مأموریت انجام یک مطالعه جامع در مورد جرم سایبری درخواست می‌نماید؛

- پذیرش مسئولیت و انجام یک مطالعه جامع درباره جرم سایبری، {به‌عنوان} مسئول مطالعه جامع درباره مشکل جرم سایبری و نحوه واکنش در برابر آن توسط دولت‌های عضو، جامعه بین‌المللی و بخش خصوصی؛

- تداوم کارهای در حال انجام جهت برگزاری نشست‌های دوره ای و مأموریتی به‌عنوان بستری جهت بحث بیشتر درباره موضوعات محتوایی درباب جرم سایبری، اقدام وفق مأموریت‌های خود، و هم راستا با اعلامیه السالوادور در خصوص راهبردهای جامع برای مقابله با چالش‌های جهانی: نظام‌های پیشگیری از جرم و عدالت کیفری و توسعه آن در جهان در حال تغییر، {و همسو با} اعلامیه دوحه در خصوص گنجاندن موضوع پیشگیری از جرم و عدالت کیفری در دستور کار گسترده تر ملل متحد جهت مقابله با چالش‌های اقتصادی و اجتماعی و حاکمیت قانون در سطوح ملی و بین‌المللی و مشارکت عمومی؛

همچنین از گروه کارشناسان دولتی درخواست می‌نماید تا تبادل اطلاعات درباره تدوین قانون ملی، رویه‌های برتر، مساعدت فنی و همکاری بین‌المللی را با نگاهی به تحلیل گزینه‌هایی به‌منظور تقویت قانون بین‌المللی یا ملی موجود و پیشنهاد قوانین جدید یا سایر واکنش‌ها و پاسخ‌ها در برابر جرم سایبری؛

- تصمیم می‌گیرد که گروه کارشناسان، نشست آتی خود را در یک الگوی ساختاری، بدون آنکه موضوعات مشمول در دستور کار گروه تحت تأثیر قرار گیرد، به بررسی هریک از موضوعات اصلی فصل‌های سه تا هشت (فصل ۳: تدوین قوانین و چارچوب‌ها، فصل ۴: جرم انگاری، فصل ۵: تحقیقات و اجرای قانون، فصل ۶: مدارک الکترونیکی و عدالت کیفری، فصل ۷: همکاری بین‌المللی فصل ۸: پیشگیری) برنامه جامع اقدام کند و در صورت مقتضی، با در نظر گرفتن همکاری‌های دریافتی پیرو قطعنامه کمیسیون {به شماره} ۲۲/۷، نشست‌های قبلی گروه کارشناسی را بررسی نمایند؛

- گروه کارشناسان را تشویق می‌نماید تا نتایج و توصیه‌ها را جهت ارائه به کمیسیون آماده نماید؛
- از دفتر مقابله با جرم و مواد مخدر سازمان ملل درخواست می‌کند تا به شکل دوره‌ای اطلاعاتی را از تحولات جدید، پیشرفته‌های ایجاد شده و رویه‌های برتر شناخته شده جمع‌آوری نماید؛

از گروه کارشناسان دعوت می‌نماید، با هدف مساعدت و بر اساس مأموریت محوله، مشورت‌هایی را به دفتر مقابله با جرم و مواد مخدر سازمان ملل در ارتباط با برنامه جهانی جرم سایبری {همانند} شناسایی نیازهای ظرفیت‌سازی با اولویت بالا و واکنش‌های مؤثر ارائه نماید، بدون اینکه سایر موضوعات مندرج در دستور کار گروه کارشناسی را تحت تأثیر قرار دهد و بموقعیت کمیسیون به‌عنوان نهاد حاکم در برنامه جرم لطمه ای وارد شود؛

- جهت برگزاری اجلاس های آتی گروه کارشناسان در حدود منابع موجود و بدون لطمه به سایر اقدامات دستور کار کمیسیون تصمیم می‌گیرد و از کشورهای عضو و سایر حامیان مالی داوطلبانه خارج از بودجه، دعوت می‌نماید تا منابع مالی بودجه ای فوق‌العاده را برای اهداف قطعنامه حاضر مطابق با نقش و رویه های سازمان ملل متحد، فراهم نمایند، از جمله {اهدافی} در ارتباط با عملکرد گروه کارشناسان و برنامه جهانی جرم سایبری؛

از گروه کارشناسان می‌خواهد تا در اجلاس بعدی گزارشی را از پیشرفت عملکرد خود به کمیسیون ارائه نمایند.

بند پنج: قطعنامه روندهای جهانی جرم و موضوعات نو ظهور و واکنش هادر حوزه پیشگیری از جرم و عدالت کیفری، مقابله با سوءاستفاده و استثمار جنسی برخط از کودکان سال ۲۰۱۹



شورای اقتصادی و اجتماعی

ترجمه سند

تاریخ انتشار: ۲۴ می ۲۰۱۹

شماره قطعنامه: E/CN.15/2019/L.3/Rev.1

زبان: انگلیسی

توزیع: محدود

کمیسیون پیشگیری از جرم و عدالت کیفری

اجلاس بیست و هشتم، وین، ۲۰ الی ۲۴ می ۲۰۱۹ دستور کار ۸

روندهای جهانی جرم و موضوعات نو ظهور و واکنش ها در حوزه پیشگیری از جرم و عدالت کیفری

آندورا، استرالیا، هندوراس، مکزیک، عربستان سعودی، پرو و فیلیپین پیش نویس قطعنامه را مجدداً بررسی نمودند.

کمیسیون پیشگیری از جرم و عدالت کیفری، به شورای اقتصادی اجتماعی توصیه نمود {تا} پیش نویس قطعنامه زیر را جهت تصویب در مجمع عمومی تأیید و تنفیذ نماید.

قطعنامه مقابله با سوءاستفاده و استثمار جنسی برخط از کودکان

مجمع عمومی

ضمن به رسمیت شناختن عامل بالقوه {منفی} برای قربانیان کودک {که مورد} استثمار و سوءاستفاده جنسی برخط قرار گرفته و ضربه روحی که موجب تغییر زندگی آنها می شود را تجربه کرده اند، از جمله مسیرهای رشد منفی؛

ضمن اذعان به این موضوع که پیشرفت های {موجود} در فناوری های اطلاعات و ارتباطات {موجب} پیشرفت های قابل توجهی در {عرصه های} اقتصادی و اجتماعی کشورها، جوامع و کودکان آنها و حمایت از توسعه اقتصادی شده است و با به رسمیت شناختن کیفیت اتصال {کشورها و جوامع} از طریق اشتراک گذاری ایده ها و تجربیات، اما چنین پیشرفت هایی فرصت های

جدید و بی سابقه ای برای مجرمان روابط جنسی با کودکان {در رابطه با} دسترسی، تولید و توزیع مواد سوءاستفاده جنسی از کودکان را فراهم می‌نماید تا تمامیت حقوق کودکان را نقض نمایند و آن‌ها را جهت تماس مضر برخط با کودکان صرف نظر از موقعیت فیزیکی و ملیت {آن‌ها} توانمند می‌سازد؛

با ابراز نگرانی از اینکه فناوری‌های اطلاعات و ارتباطات جدید و توسعه یافته از جمله قابلیت رمزنگاری و ابزار گمنام‌سازی، جهت ارتکاب به جرائم مرتبط با سوءاستفاده و استثمار جنسی کودکان مورد استفاده سوء قرار می‌گیرند؛

باتوجه به اینکه سوءاستفاده و استثمار جنسی کودکان ممکن است اشکال بسیاری داشته باشد مانند {موارد زیر هر چند که} محدود به این موارد نمی‌شود: جرایم تماس {جنسی} یا غیرتماسی، جرایم برخط، قاچاق کودکان جهت اهداف استثمار جنسی، اغفال جنسی یا گرومینگ کودکان، سوءاستفاده جنسی از تصاویر کودکان جهت تهدید، اخاذی و مالکیت، تولید، توزیع و دسترس پذیری، فروش، کپی و تصرف دسترسی به مواد سوءاستفاده جنسی از کودک، سوءاستفاده کودک در برنامه زنده و تمامی اشکال استثمار مضر است و تأثیر منفی در رشد و رفاه بلندمدت کودکان و همبستگی خانوادگی و ثبات اجتماعی {آن‌ها} دارد؛

با تأکید به اینکه، افزایش راه‌هایی که مواد سوءاستفاده و استثمار جنسی کودک {از طریق آن‌ها} می‌تواند تولید یا توزیع گردد، به فروش برسد، کپی شود، جمع آوری شود و به شکل برخط دیده شود و همچنین قابلیت اشخاص برای تجمع برخط و سوءاستفاده و استثمار جنسی کودک ارتقای یابد، خطرهایی را برای کودکان افزایش داده است. از جمله هنجارسازی سوءاستفاده و استثمار جنسی کودک، به رسمیت شناختن ارتباط مضر با کودکان، باتوجه به اینکه ارتباط {مضر}، تمامیت حقوق و ایمنی کودکان را نقض و دچار تهدید می‌نماید؛

باتوجه به اینکه کنوانسیون ملل متحد علیه جرائم سازمان یافته فراملی ابزاری است که دولت‌های عضو می‌توانند از آن جهت ایجاد همکاری بین‌المللی به منظور پیشگیری و مبارزه با جرائم سازمان یافته فراملی استفاده کنند، برخی از دولت‌های عضو ممکن است از آن علیه برخی موارد مرتبط با سوءاستفاده و استثمار جنسی کودکان به شکل برخط استفاده نمایند؛

با تأکید بر اهمیت ارتقای هماهنگی و همکاری میان دولت‌های عضو در زمینه: پیشگیری و مبارزه با سوءاستفاده و استثمار جنسی کودکان به شکل برخط، شناسایی کودکان قربانی، اجرای عدالت در مورد مرتکبان، تقویت مساعدت‌های فنی برای دولت‌های درخواست کننده در راستای بهبود تدوین قانون ملی و ارتقای ظرفیت مراجع ملی که با تمامی اشکال استثمار جنسی کودک سروکار دارند از جمله در طول فرایند پیشگیری، کشف، تحقیق و تعقیب قانونی، احیای جسمی و روانی و همبستگی اجتماعی کودکان قربانی؛

با یادآوری کنوانسیون حقوق کودک و پروتکل اختیاری این کنوانسیون درباره فروش کودکان، فحشاء و پورنوگرافی کودک؛

با ذکر این نکته که اصطلاح پورنوگرافی کودک، در برخی از کشورهای عضو به طور فزاینده‌ای به‌عنوان استثمار جنسی کودک یا مواد آزار جنسی در کودکان مورد استفاده قرار می‌گیرد تا بهتر منعکس کننده ماهیت چنین مطالبی و جدی بودن آسیب‌های کودک در این زمینه باشد؛ با تأیید مجدد اهمیت اسناد حقوق بین‌الملل موجود که در مبارزه علیه سوءاستفاده و استثمار جنسی کودک مشارکت دارند و توافق بین‌المللی بر روی تعاریف، ضمن به رسمیت شناختن اهمیت استفاده از واژگان و اصطلاحات که منعکس کننده شدت آسیب وارد شده به کودکان توسط چنین اقداماتی می‌باشد؛

باتوجه به پروتکل اختیاری کنوانسیون حقوق کودک درباره فروش کودکان، فحشاء و پورنوگرافی کودک؛

با اذعان به اهمیت اسناد حقوقی موجود که لازم می‌داند دولت‌ها سوءاستفاده و استثمار جنسی کودکان را جرم انگاری نمایند و همکاری اثربخش بین‌المللی در چارچوب مبارزه با سوءاستفاده و استثمار جنسی کودکان را توانمند می‌سازد؛

با یادآوری قطعنامه‌های خود (به شماره‌های) ۷۳/۱۵۴ مورخ ۱۷ دسامبر ۲۰۱۸ درباره حفاظت از کودکان در برابر زورگویی، ۷۳/۱۴۸ مورخ ۱۷ دسامبر ۲۰۱۸ درباره افزایش تلاش‌ها جهت پیشگیری و رفع کلیه اشکال خشونت علیه زنان و دختران: آزار و اذیت جنسی، ۶۹/۱۹۴ مورخ ۱۸ دسامبر ۲۰۱۴ درباره راهبردهای نمونه و اقدامات کاربردی درباره رفع خشونت علیه

کودکان در زمینه پیشگیری از جرم و عدالت کیفری، ۷۲/۱۹۵ مورخ ۱۹ دسامبر ۲۰۱۷ درباره اصلاح {و بهبود} هماهنگی در تلاش‌ها علیه قاچاق افراد؛

{با یادآوری} قطعنامه‌های شورای اقتصادی اجتماعی {به شماره‌های} ۲۰۱۱/۳۳ مورخ ۲۸ جولای ۲۰۱۱ درباره ممانعت، حفاظت و همکاری بین‌المللی علیه استفاده از فناوری‌های اطلاعاتی جدید برای سوءاستفاده یا استثمار کودکان، ۲۰۰۴/۲۷ مورخ ۲۱ جولای ۲۰۰۴ درباره راهنماهای عدالت برای کودکان قربانی و شهود جرم؛

{با یادآوری} قطعنامه کمیسیون پیشگیری از جرم و عدالت کیفری {به شماره} ۱۶/۲ مورخ ۲۷ آوریل ۲۰۰۷ درباره پیشگیری مؤثر از جرم و پاسخ عدالت کیفری در مبارزه با استثمار جنسی کودکان؛

با اذعان به نقش‌های مهم و متمایزی که خانواده‌ها، قلم‌های قانونی، مدارس، جامعه مدنی، انجمن‌های ورزشی، جوامع، مؤسسات دولتی و رسانه‌ها در ایمن نمودن حفاظت از کودکان در مقابل سوءاستفاده و استثمار جنسی از طریق برخط و در پیشگیری از کلیه اشکال خشونت ایفا می‌کنند از جمله از ارتقای ایمنی کودکان در فضای برخط؛

با تأیید مجدد اهمیت برنامه پیشگیری از جرم و عدالت کیفری ملل متحد در ارتقای اقدام اثر بخش جهت تقویت همکاری بین‌المللی در پیشگیری از جرم و عدالت کیفری؛

با تأیید اهمیت کار گروه کارشناسان بین دولتی باز در بررسی جامع مسئله جرم سایبری و همکاری در درک تهدید جرم سایبری؛

باتوجه به اهمیت دفتر مقابله با موادمخدر و جرم ملل متحد و برنامه‌های جهانی آن درباره قاچاق اشخاص، خشونت علیه کودکان، جرم سایبری، که ظرفیت‌سازی و مساعدت فنی برای کشورهای تقاضاکننده را، علاوه بر موارد دیگر، برای مبارزه با سوءاستفاده و استثمار جنسی کودکان تأمین می‌نماید، از جمله سوءاستفاده و استثمار جنسی کودک در فضای برخط؛

با به رسمیت شناختن اهمیت مشارکت‌ها و ابتکارات چندذی‌نفعی دوجانبه، منطقه‌ای و بین‌المللی که {موجب} پیشرفت حفاظت مؤثر و ارتقای حقوق کودک و رفع سوءاستفاده و استثمار جنسی کودک در فضای برخط می‌گردد. همچنین انجام تحقیقات با هدف ایجاد یک

پایگاه شواهد دقیق در مورد استفاده کودکان از اینترنت را میسر می‌سازد و در این راستا، در کنار سایر تلاش‌ها، به تلاش‌های اتحادیه جهانی «ما حمایت می‌کنیم» و «کودکان جهان برخط» توجه می‌نماید؛

با یادآوری قطعنامه کمیسیون پیشگیری از جرم و عدالت کیفری {به شماره ۲۷/۳} مورخ ۱۸ می ۲۰۱۸، که در آن کمیسیون ضمن ابراز نگرانی خود از سوءاستفاده مجرمانه از فناوری‌های اطلاعات و ارتباطات بیان می‌نماید که این امکان وجود دارد مجرمان {از طریق این فناوری‌ها} مرتکب اقدامات غیرقانونی مانند {موارد زیر} شوند:

به‌کارگیری {استخدام}، کنترل و پناه دادن به کودکانی که در معرض خطر قاچاق اشخاص قرار دارند و تبلیغ قاچاق چنین کودکانی و همچنین ایجاد هویت‌های جعلی که سوءاستفاده یا استثمار کودکان، گرومینگ و سوءاستفاده از کودک در برنامه زنده و سایر مواد سوءاستفاده از کودک را تقویت می‌کند؛

با یادآوری قطعنامه کمیسیون پیشگیری از جرم و عدالت کیفری {به شماره ۲۶/۳} مورخ ۲۶ می ۲۰۱۷ درباره جریان سازی یک چشم‌انداز کلان به سیاست‌ها و برنامه‌های پیشگیری از جرم و عدالت کیفری و تلاش‌ها جهت پیشگیری و مبارزه با جرائم سازمان یافته فراملی:

۱. مصرانه از دولت‌های عضو می‌خواهد تا:

سوءاستفاده و استثمار جنسی کودک را جرم‌انگاری نمایند از جمله سوءاستفاده و استثمار جنسی کودک در فضای برخط، اجازه تعقیب قانونی مرتکبان را صادر نمایند. در صورت مقتضی به سازمان‌های نیروی انتظامی قدرت اعطاء نموده و ابزاری را جهت شناسایی مرتکبان و قربانیان فراهم نمایند و به شکل اثربخشی با سوءاستفاده و استثمار جنسی کودک مبارزه نمایند؛

۲. همچنین پافشاری (اصرار) می‌نماید تا دولت‌ها تلاش‌های خود را جهت مبارزه با جرم سایبری در رابطه با سوءاستفاده و استثمار جنسی کودک به شکل برخط، سازگار با چارچوب قانون داخلی خود، تقویت نمایند؛

۳. از دولت‌های عضو {ملل متحد} که عضو پروتکل اختیاری کنوانسیون حقوق کودک درباره فروش کودکان، فحشا و پورنوگرافی کودک می‌باشند، درخواست می‌نماید که به تعهدات قانونی

خود عمل نمایند؛

۴. مصرانه از دولت‌های عضو می‌خواهد تا آگاهی عمومی {خود} را درباره {موارد زیر} ارتقای دهند: ماهیت جدی و مهم مواد سوءاستفاده و استثمار جنسی کودکان، چگونگی استفاده از این مواد در تعرض‌های جنسی علیه کودکان، چگونگی تولید، توزیع و مصرف {این مواد} که بیشتر کودکان را در معرض سوءاستفاده و استثمار جنسی قرار می‌دهد از جمله از طریق هنجارسازی نمایش و حمایت از مطالبه چنین موادی؛

۵. مصرانه از کشورهای عضو می‌خواهد اقدامات قانونی یا سایر اقدامات مطابق با قانون داخلی را برای تسهیل شناسایی موارد استثمار جنسی کودکان و مواد سوءاستفاده جنسی را از طریق خدمات اینترنتی و ارائه دهندگان دسترسی یا سایر نهادهای ذی‌ربط اتخاذ کنند و مطابق با قوانین داخلی موارد زیر را تضمین نمایند:

ارائه گزارش از چنین موادی به مقامات ذی‌صلاح، حذف آن‌ها از طریق خدمات اینترنتی و ارائه‌دهندگان دسترسی یا سایر نهادهای مربوط از جمله در تعامل با نیروی انتظامی؛

۶. دولت‌های عضو را تشویق می‌نماید تا مطابق با حقوق داخلی {خود} به کفایت و بسندگی منابع مربوط به تحقیقات و تعقیب قانونی جرائم از جمله سوءاستفاده و استثمار جنسی کودکان به شکل برخط اطمینان حاصل نمایند؛

۷. دولت‌های عضو را تشویق می‌نماید تا اطلاعاتی را در خصوص رویه‌های برتر به اشتراک گذارند و اقدامات سازگار با حقوق داخلی جهت مبارزه با سوءاستفاده و استثمار جنسی کودک از جمله مصادره و از بین بردن، بهبود زمان نابودی مواد سوءاستفاده و استثمار جنسی کودک به شکل برخط را به انجام رسانند.

۸. دولت‌های عضو را تشویق می‌نماید تا جهت تقویت هماهنگی ملی جهت مقابله با سوءاستفاده و استثمار جنسی کودک در فضای برخط، مؤسسات دولتی مسئول برای {تدوین} خط‌مشی‌های حفاظت داده و ارتباطات راه دور، صنعت فناوری اطلاعات و ارتباطات را وارد میدان نمایند

۹. دولت‌های عضو را تشویق می‌نماید تا مؤسسات دولتی و بخش خصوصی مربوط را در راستای تلاش‌های خود جهت تسهیل گزارش‌دهی و ردیابی انتقالات مالی مشکوک با هدف کشف،

ممانعت (بازداشت) و مبارزه علیه سوءاستفاده و استثمار جنسی کودکان در فضای برخط وارد میدان نمایند.

۱۰. دولت‌های عضو را تشویق می‌نماید تا موازنه مناسبی بین توسعه و اجرای خط‌مشی‌های حریم خصوصی و تلاش جهت شناسایی و گزارش مواد سوءاستفاده جنسی کودک یا جرائم استثمار کودک در فضای برخط برقرار نمایند.

۱۱. کشورهای عضو را ترغیب کنید تدابیر مؤثر پیشگیری از وقوع جرم مبتنی بر شواهد اتخاذ نمایند. از جمله مواردی که به صورت بالقوه می‌تواند موجب کاهش آزار کودکان شود. ضمناً با هدف کاهش خطر {ناشی} از قرار گرفتن {کودکان} در معرض سوءاستفاده و استثمار جنسی در فضای برخط، دولت‌ها چنین اقداماتی را به‌عنوان بخشی از راهبردهای کلی پیشگیری از جرم قرار دهند.

۱۲. همچنین دولت‌های عضو را تشویق می‌نماید تا به نحو مقتضی: اطلاعات و تحلیل‌هایی را برای اطلاع رسانی از ارزیابی خطرهای مرتبط با سوءاستفاده و استثمار کودکان در فضای برخط را تولید کنند {ارائه دهند}، اقدامات مؤثر جهت کاهش این خطرهای را از طریق جمع‌آوری کیفی و کمی داده‌های مربوط به تفکیک سن، جنسیت و سایر عوامل مربوط توسعه دهند، چشم‌انداز تحقیقات و تحلیل‌های خود درباره جرائم سوءاستفاده و استثمار جنسی کودکان را جریان‌سازی کنند.

۱۳. پافشاری بیشتری می‌نماید تا به‌منظور حفاظت و حمایت {دفاع} از کودکان در مقابل سوءاستفاده و استثمار جنسی از جمله در فضای برخط و عدم رضایت و بهره‌کشی از انتشار نمایش قربانیان، دولت‌های عضو خط‌مشی‌های عمومی {ملی} را ایجاد و به انجام برسانند و نیز به شکل فعالانه اطلاعاتی را درباره رویه‌های برتر از جمله برنامه‌های حمایتی از قربانیان و جریان‌سازی چشم‌انداز فعالیت خود را به اشتراک گذارند.

۱۴. دولت‌های عضو را تشویق می‌نماید تا: قربانیان سوءاستفاده و استثمار جنسی کودک را با برنامه‌های کیفی و مبتنی بر ادله، شناسایی و حمایت نمایند. {از منظر} جسمی از آن‌ها مراقبت نمایند و {از بُعد} روانشناختی به آن‌ها مشاوره دهند. {از نگاه} اجتماعی آن‌ها را احیاء نمایند.

همچنین مراقبت‌های روانشناختی، مشاوره جهت آسیب‌های روانی، توانبخشی و احیای مجدد آن‌ها در جامعه {را انجام دهند}، با مساعدت کلیه ذی‌نفعان مرتبط، حفاظت از حقوق کودکان {متأثر از این اتفاق}، حقوق حریم‌خصوصی قربانیان و رازداری گزارش‌های مربوط به آن‌ها را تضمین و حفظ نمایند؛

۱۵. از دفتر مقابله با مواد مخدر و جرم ملل متحد درخواست می‌نماید تا دولت‌های عضو را بنا به درخواست {آن‌ها} در خصوص {موارد زیر} مساعدت و یاری رسانند: توسعه و اجرای اقداماتی جهت افزایش دسترسی به عدالت و حفاظت از جمله از طریق قانون‌گذاری داخلی و توسعه و اجرای سایر اقدامات برای قربانیان سوءاستفاده و استثمار جنسی کودکان در فضای برخط، همچنین با یادآوری رویکردهای حساس {در مقوله‌های} جنسیتی و کودک، راه‌حل بموقع و منصفانه‌ای را برابر نقض حقوق آن‌ها بیابد؛

۱۶. از دولت‌های عضو دعوت می‌نماید، رویه‌های برتر در خصوص گزارش‌دهی از سوءاستفاده و استثمار جنسی کودکان در فضای برخط را {با هم} تبادل نمایند از جمله گزارشی از شاخص‌ها، راه‌ها و ابزاری که آگاهی عمومی درباره این سازوکارهای گزارش‌دهی را ارتقای می‌دهد؛

۱۷. از آن دسته از دولت‌هایی که با کنوانسیون ملل متحد علیه جرائم سازمان یافته فراملی و پروتکل حفاظت، منع و مجازات قاچاق انسان، به‌ویژه زنان و کودکان موافقت ننموده‌اند و یا {آن‌ها} را تصویب ننموده‌اند درخواست می‌نماید تا با در نظر گرفتن نقش آن اسناد در مبارزه علیه قاچاق کودکان که از جمله با هدف استثمار جنسی صورت می‌گیرد، به کنوانسیون ملل متحد علیه جرائم سازمان یافته فراملی ملحق شوند؛

۱۸. به‌منظور مقابله با چنین جرائمی و اطمینان از اینکه ضمن احترام به حقوق حریم خصوصی کودکان، قربانیان شناسایی شده و مرتکبان به محاکم عدالت سپرده می‌شوند، از دولت‌های عضو درخواست می‌نماید، مطابق با چارچوب‌های قانون داخلی {خود} و قابلیت اعمال حقوق بین‌المللی، همکاری‌های بین‌المللی جهت مبارزه با استثمار و سوءاستفاده جنسی کودک در فضای برخط را به نحو مقضی از طرق {زیر} تقویت نمایند: مساعدت متقابل قانونی، استرداد مجرمان و نیز همکاری فی مابین نیروهای پلیس و سازمان‌ها با یکدیگر؛

۱۹. به دولت‌ها اصرار می‌ورزد تا کار و تلاش مداوم خود برای تقویت بیشتر همکاری بین‌المللی در زمینه مبارزه علیه سوءاستفاده و استثمار جنسی کودک در فضای برخط را اثبات نمایند. از جمله از طریق تضمین این موضوع که، سوءاستفاده و استثمار جنسی کودک در فضای برخط، به شکل جامعی در چارچوب و طرح کاری گروه کارشناسان بین‌دولتی باز برای انجام بررسی جامع درباره جرم سایبری مورد ملاحظه قرار گرفته است. این گروه، یک مجمع با ارزشی جهت مباحث جرم سایبری را میسر می‌سازد؛

۲۰. دولت‌های عضو را تشویق می‌نماید تا به‌منظور مقابله با سوءاستفاده و استثمار جنسی کودک در فضای برخط، در {ایجاد} منابع دفتر مقابله با مواد مخدر و جرم ملل متحد از جمله برنامه جهانی درباره جرم سایبری همکاری کنند؛

۲۱. از دولت‌های عضو و سایر حامیان مالی داوطلبانه دعوت می‌نماید تا، مطابق با قواعد و رویه‌های سازمان ملل، منابع مالی (بودجه ای) فوق‌العاده را برای اجرای بندهای ذی‌ربط در قطعنامه‌های حاضر تأمین نمایند.

بند شش: قطعنامه روندهای جهانی جرم و موضوعات نو ظهور و واکنش ها در حوزه پیشگیری از جرم و عدالت کیفری ۲۰۱۹، ارتقای مساعدت فنی و ظرفیت سازی برای تقویت اقدامات ملی و همکاری بین المللی برای مبارزه با جرم سایبری از جمله اشتراک گذاری اطلاعات

ترجمه سند

تاریخ انتشار: ۲۴ می ۲۰۱۹

شماره قطعنامه: E/CN.15/2019/L.6/Rev.1

زبان: انگلیسی

توزیع: محدود



شورای اقتصادی و اجتماعی

کمیسیون پیشگیری از جرم و عدالت کیفری

اجلاس بیست و هشتم، وین، ۲۰ الی ۲۴ می ۲۰۱۹ دستور کار ۸

روندهای جهانی جرم و موضوعات نو ظهور و واکنش ها در حوزه پیشگیری از جرم و عدالت کیفری

استرالیا، بلاروس، کانادا، کلمبیا، هندوراس، مکزیک، پرو، فیلیپین، پرتغال و عربستان سعودی پیش نویس قطعنامه را مورد بررسی مجدد قرار دادند. کمیسیون پیشگیری از جرم و عدالت کیفری، به شورای اقتصادی اجتماعی توصیه نمود {تا} پیش نویس قطعنامه زیر را جهت تصویب در مجمع عمومی تأیید و تنفیذ نماید.

ارتقای مساعدت فنی و ظرفیت سازی برای تقویت اقدامات ملی و همکاری بین المللی برای مبارزه با جرم سایبری از جمله اشتراک گذاری اطلاعات

مجمع عمومی

با یادآوری قطعنامه خود {به شماره} ۶۲/۲۳۰ مورخ ۲۱ دسامبر ۲۰۱۰، که در آن اعلامیه السالوادور درباره «راهبردهای جامع برای چالش های جهانی: نظام های پیشگیری از جرم و عدالت کیفری و توسعه آن ها در یک جهان در حال تغییر» را تأیید نمود، این اعلامیه در دوازدهمین کنگره ملل متحد درباره پیشگیری از جرم و عدالت کیفری تصویب شد. تأسیس کمیسیون پیشگیری از جرم و عدالت کیفری درخواست گردید. در راستای بند ۴۲ اعلامیه {السالوادور}، {تشکیل}

یک گروه کارشناسان بین دولتی باز جهت اجرای بررسی جامع مسئله جرم سایبری و پاسخگویی به آن توسط دولت‌های عضو، جامعه بین‌الملل و بخش خصوصی {درخواست گردید}. {هدف از این گروه موارد زیر می‌باشد}: تبادل اطلاعات درباره تدوین قانون ملی، رویه‌های برتر، مساعدت فنی و همکاری بین‌المللی با نگاهی بر بررسی گزینه‌ها جهت تقویت قانون ملی و حقوق بین‌المللی موجود و پیشنهاد قانون ملی و حقوق بین‌المللی جدید و سایر پاسخگویی‌ها به جرم سایبری؛ با یادآوری قطعنامه‌های خود {به شماره‌های} ۴۶/۱۵۲ مورخ ۱۸ دسامبر ۱۹۹۱، ۶۰/۱ مورخ ۱۶ سپتامبر ۲۰۰۵، ۶۷/۱ مورخ ۲۴ سپتامبر ۲۰۱۲، ۶۹/۱۹۳ و ۶۹/۱۹۶ مورخ ۱۸ دسامبر ۲۰۱۴، ۷۰/۱۷۸ و ۷۱/۲۰۹ مورخ ۱۹ دسامبر ۲۰۱۶ و ۷۲/۱۹۶ مورخ ۱۹ دسامبر ۲۰۱۷ و ۷۳/۱۸۶ مورخ ۱۷ دسامبر ۲۰۱۸، ۷۳/۱۸۷ مورخ ۱۷ دسامبر ۲۰۱۸، با یادآوری قطعنامه خود {به شماره} ۷۰/۱۷۴ مورخ ۱۷ دسامبر ۲۰۱۵، که در آن مجمع عمومی، به‌منظور مقابله با چالش‌های اجتماعی اقتصادی و ارتقای حاکمیت قانون در سطوح ملی و بین‌المللی و مشارکت عمومی، {قرار گرفتن} اعلامیه دوحه درباره پیشگیری یکپارچه از جرم و عدالت کیفری در دستورکار گسترده‌تر سازمان ملل را تأیید کرد؛

با استقبال از قطعنامه کمیسیون پیشگیری از جرم و عدالت کیفری {به شماره} ۲۶/۴ مورخ ۲۶ می ۲۰۱۷، که در آن کمیسیون تصمیم گرفت: گروه کارشناسان بین دولتی باز، بررسی جامعی درباره جرم سایبری را انجام دهد، نشست‌های آتی خود را با شیوه‌ای ساختاریافته، به رسیدگی به هریک از موضوعات اصلی موجود در پیش‌نویس مطالعه جامع درباره جرم سایبری اختصاص داد این قطعنامه گروه کارشناسان را به توسعه نتایج و توصیه‌های ممکن جهت ارائه آن به کمیسیون تشویق نمود و از دفتر درخواست کرد که به شکل دوره‌ای اطلاعاتی درخصوص تحولات جدید، پیشرفت‌های ایجاد شده و رویه‌های برتر شناخته شده را جمع‌آوری نماید؛ همچنین ضمن استقبال از طرح کار گروه کارشناسان برای دوره زمانی ۲۰۱۸ تا ۲۰۲۰ که در چهارمین نشست گروه کارشناسان بین دولتی باز مورخ ۳ آوریل ۲۰۱۸ و به‌منظور انجام مطالعه جامع درباره جرم سایبری به تصویب رسید.

ضمن توجه به اینکه گروه کارشناسان نشست آتی خود را {با در نظر گرفتن موارد زیر} به

همکاری و پیشگیری بین‌المللی اختصاص دادند: اطلاعات درباره موضوعات موجود در پیش نویس بررسی جامع جرم سایبری، تفاسیر ارائه شده توسط دولت‌های عضو و تحولات اخیر در سطوح ملی و بین‌المللی؛

با یادآوری قطعنامه خود {به شماره} ۷۳/۱۸۶ مورخ ۱۷ دسامبر ۲۰۱۸ که در آن {مجمع}، در کنار سایر موضوعات، ضمن توجه توأم با قدردانی درباره چهارمین نشست گروه کارشناسان بین دولتی باز برای انجام بررسی جامع درباره جرم سایبری از دولت‌های عضو درخواست نمود تا از طرح کار گروه کارشناسان حمایت نمایند؛

با یادآوری قطعنامه خود {به شماره} ۷۳/۱۸۷ مورخ ۱۷ دسامبر ۲۰۱۸، که در آن از دبیرکل درخواست نمود تا نظرهای دولت‌های عضو را درباره چالش‌هایی که آن‌ها درخصوص مقابله با استفاده از فناوری‌های اطلاعات و ارتباطات با اهداف مجرمانه با آن مواجه هستند را پیگیری نماید و در اجلاس هفتاد و چهارم {مجمع عمومی} گزارشی را از ملاحظات خود بر مبنای این نظرها ارائه نماید؛

با یادآوری قطعنامه خود به شماره ۷۳/۱۸۷ مورخ ۱۷ دسامبر ۲۰۱۸ که در آن {مجمع عمومی} تصمیم گرفت گزینه‌ای تحت عنوان «مقابله با استفاده از فناوری‌های اطلاعات و ارتباطات برای اهداف مجرمانه» را در دستورکار موقت خود در اجلاس هفتاد و چهارم، بگنجاند. ضمن تأکید بر نیاز به ارتقای هماهنگی و همکاری میان دولت‌های عضو درباره مبارزه با جرم سایبری از جمله از طریق تأمین مساعدت فنی کشورهای در حال توسعه - بنا به درخواست آن‌ها - در راستای بهبود تدوین قانون ملی و ارتقای ظرفیت مراجع ملی که با تمامی اشکال جرائم سایبری سروکار دارند از جمله پیشگیری، ردیابی، تحقیق و تعقیب قانونی؛

و در این چارچوب با تأکید بر نقش ملل متحد علی‌الخصوص نقشی که کمیسیون پیشگیری از جرم و عدالت کیفری ایفا می‌کند و با تأیید مجدد اهمیت احترام به حقوق بشر و آزادی‌های اساسی در استفاده از فناوری‌های اطلاعات و ارتباطات؛

با استقبال توأم با قدردانی از عملکرد گروه کارشناسان بین دولتی باز جهت انجام بررسی جامع درباره جرم سایبری و تمرکز {این گروه} بر گفتگو و مباحثه محتوایی میان کارشناسان و صاحبان

مشاغل از کشورهای عضو؛

باتوجه به اینکه کنوانسیون ملل متحد درباره جرم سازمان‌یافته فراملی ابزاری است که ممکن است دولت‌های عضو به منظور ایجاد همکاری بین‌المللی جهت پیشگیری و مبارزه با جرم سازمان‌یافته فراملی از آن استفاده نمایند، ابزاری که ممکن است برای بعضی از دولت‌های عضو در برخی موارد مربوط به جرم سایبری از آن استفاده شود؛

با آگاهی از چالش‌های پیش روی تمامی دولت‌ها در مبارزه با جرم سایبری و با تأکید بر نیاز به تقویت مساعدت فنی و اقدامات ظرفیت‌ساز {دولت‌ها} بنا به درخواست و بر مبنای نیازهای ملی {آن‌ها}، و با در نظر گرفتن چالش‌های ویژه که در این رابطه پیش روی کشورهای در حال توسعه قرار دارد، انتظار از پرداختن به مباحثاتی با موضوعاتی وابسته به جرم سایبری از جمله ادله الکترونیکی در خلال برگزاری چهاردهمین کنگره ملل متحد درباره پیشگیری از جرم و عدالت کیفری؛

با استقبال توأم با قدردانی از تلاش‌های دفتر مقابله با مواد مخدر و جرم سازمان ملل در پیشرفت اجرای برنامه جهانی درباره جرم سایبری با هدف اجرای دستورکار خود در راستای تأمین مساعدت‌های فنی و ظرفیت‌سازی درباره جرم سایبری؛

ضمن قدردانی، از نتایج پنجمین نشست گروه کارشناسان بین‌دولتی باز جهت انجام بررسی جامع جرم سایبری که مورخ ۲۷ تا ۲۹ مارس ۲۰۱۹ در وین برگزار گردید، استقبال می‌نماید. بر اهمیت کار گروه کارشناسان بین‌دولتی باز در بررسی جامع درباره جرم سایبری، جهت تداوم تبادل اطلاعات درباره موارد زیر اذعان می‌دارد: قانون ملی، رویه‌های برتر، مساعدت‌های فنی همکاری بین‌المللی با نگاهی بر بررسی گزینه‌ها جهت تقویت پاسخ‌های موجود و پیشنهاد قانون ملی و حقوق بین‌المللی جدید یا سایر پاسخ‌ها (واکنش‌ها) به جرم سایبری؛

ضمن قدردانی، به این موضوع توجه می‌نماید که مطابق با طرح کار گروه کارشناسان برای دوره زمانی ۲۰۱۸ تا ۲۰۲۱ و نتایج و توصیه‌های ممکن جهت ارائه به کمیسیون؛

گروه کارشناسان بین‌دولتی باز برای انجام بررسی جامع درباره جرم سایبری را به‌عنوان یک بستر مهم جهت تبادل اطلاعات درباره موارد رسمیت می‌شناسد: تدوین قانون ملی، رویه‌های برتر،

مساعادت فنی و همکاری بین‌المللی با نگاهی به بررسی گزینه‌هایی جهت تقویت واکنش‌های موجود و پیشنهاد قانون ملی و حقوق بین‌الملل جدید یا سایر پاسخ‌ها برای جرم سایبری؛ دولت‌های عضو را تشویق می‌نماید تا اقداماتی را توسعه دهند و اجرا نمایند که بتوانند متضمن {این امور زیر} باشند: ادله الکترونیکی مرتبط با جرائم و جرم سایبری به طور مؤثری در سطح ملی تحقیق و پیگیری شود، همکاری بین‌المللی در این حوزه می‌تواند مطابق با قانون داخلی و سازگار با حقوق بین‌الملل مربوط و قابل اعمال - از جمله اسناد قابل اعمال حقوق بین‌المللی بشر - حاصل گردد؛

همچنین مصرانه دولت‌های عضو را تشویق کند تا: مأموران انتظامی، مراجع تحقیقی، دادستان‌ها و قضات را در حوزه جرم سایبری از جمله مهارت‌های گردآوری و فناوری اطلاعات تعلیم دهند. آن‌ها را {برای} ایفای مؤثر نقش‌های مربوط خود در تحقیق، پیگرد و قضاوت جرائم سایبری مجهز نمایند. علاوه بر این دولت‌های عضو را تشویق می‌نماید تا: بنا به درخواست و مبتنی بر نیازهای ملی {دولت‌ها}، تلاش نمایند تا مساعادت فنی مناسب و ظرفیت‌سازی تاب‌آوری را {برای آن‌ها} ایجاد نمایند. توانمندی مراجع ملی که با جرم سایبر سروکار دارند را تقویت کنند و به تبادل نظرها {خود} در خصوص تجربیات کاربردی و سایر وجوه فنی مربوط ادامه دهند؛

مجدداً، پیرو قطعنامه کمیسیون پیشگیری از جرم و عدالت کیفری {به شماره} ۲۲/۸ مورخ ۲۶ آوریل ۲۰۱۳، نقش دفتر مقابله با مواد مخدر و جرم ملل متحد به‌عنوان منبع مرکزی از حقوق و دروس آموخته شده جرم سایبری را با نگاهی به تسهیل {موارد زیر} تأیید می‌نماید. ارزیابی مداوم نیازها و قابلیت‌های عدالت کیفری، ارائه و هماهنگی مساعادت‌های فنی؛

از دفتر مقابله با مواد مخدر و جرم ملل متحد درخواست می‌نماید تا به‌صورت دوره‌ای اطلاعاتی را درباره تحولات جدید، پیشرفت‌های حاصل شده و رویه‌های برتر شناخته شده را جمع‌آوری کنند و به شکل دوره‌ای گزارشی از این اطلاعات را به گروه کارشناسان بین‌دولتی برای انجام بررسی جامع درباره جرم سایبری و کمیسیون پیشگیری از جرم و عدالت کیفری ارائه نماید.

از گروه کارشناسان بین‌دولتی برای انجام بررسی جامع درباره جرم سایبری دعوت می‌نماید تا مبتنی بر کار خود، با دفتر مقابله با مواد مخدر و جرم ملل متحد مشاوره نماید از جمله درباب

{این موضوعات زیر}: برنامه جهانی جرم سایبری به منظور ارزیابی، بدون آنکه در سایر موضوعات مندرج در دستور کار گروه کارشناسان تأثیرگذار باشد، شناسایی اولویت‌های کلان بدون آنکه در موقعیت کمیسیون به‌عنوان نهاد حاکم بر برنامه جرم این دفتر تأثیرگذار باشد؛

از دفتر مقابله با مواد مخدر و جرم ملل متحد درخواست می‌نماید تا: از طریق برنامه جهانی جرم سایبری و در میان سایر موارد از طریق دفترهای منطقه‌ای خود {و} مبتنی بر نیازهای ملی دولت‌های عضو که با جرم سایبری سروکار دارند، به تأمین تقاضای {آن‌ها} در راستای مساعدت فنی و ظرفیت‌سازی تاب‌آور در ارتباط با {این مسائل} ادامه دهد: پیشگیری، شناسایی، تحقیق و تعقیب قانونی جرم سایبری در تمامی اشکال آن، همکاری با دولت‌های عضو، سازمان‌های منطقه‌ای و بین‌المللی، بخش خصوصی، جامعه مدنی و سایر ذی‌نفعان مربوط که می‌توانند این اقدام را تسهیل نمایند. از دولت‌های عضو دعوت می‌نماید تا در صورت مقتضی ادامه همکاری با بخش خصوصی و جامعه مدنی جهت توسعه اقدامات مربوط به مبارزه با جرم سایبری را در شیوه‌ای شفاف و پاسخگو مورد ملاحظه قرار دهند. از دولت‌های عضو و سایر حامیان مالی داوطلبانه دعوت می‌نماید تا مطابق با قواعد و رویه‌های سازمان ملل، منابع مالی فوق‌العاده را برای اهداف مشروح فوق، تأمین نمایند. از دبیرکل تقاضا می‌نماید تا در اجلاس بیست‌ونهم کمیسیون گزارشی را در خصوص اجرای قطعنامه حاضر به آن کمیسیون ارائه نماید.

بند هفت: گزارش گروه کارشناسان بین دولتی با راجع به موضوع جرم سایبری ۲۰۱۸

ترجمه سند

تاریخ انتشار: ۱۳ آوریل ۲۰۱۸

شماره قطعنامه: E/CN.15/2018/12

زبان: انگلیسی



شورای اقتصادی و اجتماعی

کمیسیون پیشگیری از جرم و عدالت کیفری

اجلاس بیست و هفتم

وین، ۱۴ تا ۱۸ می ۲۰۱۸

دستور کار ۸

روندهای جهانی جرم و موضوعات نو ظهور و واکنش‌ها در حوزه پیشگیری از جرم و عدالت کیفری گزارش اجلاس گروه کارشناسان برای انجام بررسی جامع درباره جرم سایبری که مورخ ۳ تا ۵ آوریل ۲۰۱۸ در وین برگزار گردید:

موضوع اصلی این نشست درباره تدوین قانون، چارچوب‌ها و جرم‌انگاری بود:

تدوین قانون، چارچوب‌ها

در اولین نشست این اجلاس مورخ ۳ آوریل ۲۰۱۸، دستور کار یک با عنوان پیشنهاد رئیس برای طرح کاری گروه کارشناسی برای دوره زمانی ۲۰۱۸ تا ۲۰۲۱ را مورد ملاحظه قرار دادند. در دومین، سومین و چهارمین نشست این اجلاس مورخ ۳ و ۴ آوریل ۲۰۱۸، گروه کارشناسان دستور کار ۲ را تحت عنوان تدوین قانون و چارچوب‌ها مورد ملاحظه قرار دادند. در خلال بحث‌های متوالی، بسیاری از نمایندگان {کشورهای عضو} به پیشرفت‌های ملی خود در حوزه خط‌مشی گذاری و تدوین قانون راجع به موضوعات مرتبط با جرم سایبری و امنیت سایبری اشاره نمودند. آن‌ها به نقش اصلی برنامه‌های مربوط به ظرفیت‌سازی و مساعدت فنی در پشتیبانی از اجرای موفق تدوین قانون و ظرفیت‌سازی ملی جهت تحقیق، تعقیب قانونی و قضاوت تأکید نمودند. ضمن اینکه نیاز به رویکردهای چند منظمی^۱ در جامعه مدنی و بخش خصوصی مورد تأکید قرار گرفت.

جرم انگاری

در چهارمین و پنجمین نشست‌های این اجلاس، مورخ ۴ و ۵ آوریل ۲۰۱۸، گروه کارشناسان دستورکار ۳ تحت عنوان جرم انگاری را بررسی کردند. بسیاری از سخنرانان اطلاعاتی را درخصوص راه‌هایی که از طریق آن‌ها، جرم سایبری در کشورشان جرم‌انگاری می‌شود ارائه نمودند. ادامه این گزارش حاوی مطالبی در خصوص نشست سازمانی این اجلاس بود. از جمله:

- نشست افتتاحیه؛

- بیانیه‌هایی که توسط کارشناسان کشورهای مختلف از جمله آلبانی، الجزایر، آرژانتین، استرالیا، بلاروس، بوسنی و هرزگوین، برزیل، بلغارستان، کانادا، شیلی، چین، کلمبیا، کاستاریکا، جمهوری چک، جمهوری دومینیک، اکوادور، یونان، السالوادور، استونی، گرجستان، غنا، گواتمالا، هند، اندونزی، جمهوری اسلامی ایران، ایتالیا، ژاپن، اردن، قزاقستان، کویت، لیختن اشتاین، مالزی، موریتانی، مکزیک، مونته نگرو، هلند، نیجریه، نروژ، پاراگوئه، فیلیپین، پرتغال، جمهوری مولداوی، رومانی، روسیه، صربستان، آفریقای جنوبی، سریلانکا، تایلند، مقدونیه، تونس، ترکیه، اکراین، انگلستان، آمریکا و ویتنام و نیز توسط نمایندگان سازمان‌های بین‌دولتی زیر ارائه گردید:

شورای اروپا، اتحادیه اروپا، سازمان همکاری شانگهای؛

- تصویب دستور کار و موضوعات سازمانی؛

- حاضران در نشست شامل نمایندگانی از ۹۸ کشورهای عضو، نماینده‌ای از عضو ناظر، نماینده‌ای از دبیرخانه سازمان ملل متحد، نمایندگانی از ۴ سازمان بین‌دولتی و ۹ نماینده از مؤسسات دانشگاهی و بخش خصوصی بودند؛

- مستندات.

بند هشت: گزارش گروه کارشناسان بین دولتی باز راجع به موضوع جرم سایبری ۲۰۱۹



دبیرخانه

ترجمه سند

تاریخ انتشار: ۱۲ آوریل ۲۰۱۹

شماره قطعنامه: UNODC/CCPCJ/EG.4/2019/2

زبان: انگلیسی

گزارش نشست گروه کارشناسان درباره انجام بررسی جامع جرم سایبری مورخ ۲۷ تا ۲۹ مارس ۲۰۱۹ در وین

مقدمه

مجمع عمومی در قطعنامه خود {به شماره} ۶۲/۲۳۰، از کمیسیون پیشگیری از جرم و عدالت کیفری درخواست نمود تا در راستای بند ۴۲ اعلامیه السالوادور درباره «راهبردهای جامع برای چالش‌های جهانی: نظام‌های پیشگیری از جرم و عدالت کیفری و توسعه آن‌ها در یک جهان در حال تغییر» یک گروه کارشناسان بین دولتی باز را تأسیس نماید {و این گروه} قبل از اجلاس بیستم کمیسیون، تشکیل جلسه دهند: مطالعه جامع مسئله جرم سایبری و پاسخگویی به آن توسط دولت‌های عضو جامعه بین‌الملل و بخش خصوصی از جمله تبادل اطلاعات درباره تدوین قانون ملی، رویه‌های برتر، مساعدت فنی و همکاری بین‌المللی با نگاهی به بررسی گزینه‌ها جهت تقویت قانون ملی و حقوق بین‌المللی موجود و پیشنهاد قانون ملی و حقوق بین‌المللی جدید و سایر واکنش‌ها درباره جرم سایبری به‌عنوان دستور کار مطرح گردید.

اولین نشست گروه کارشناسان مورخ ۱۷ الی ۲۱ ژانویه ۲۰۱۱ در وین برگزار گردید. در این نشست، گروه کارشناسان مجموعه‌ای از موضوعات و روش‌هایی را برای بررسی {جامع مسئله جرم سایبری} مرور و تصویب کردند.

دومین نشست گروه کارشناسان مورخ ۲۵ تا ۲۸ فوریه ۲۰۱۳ برگزار گردید. در این نشست گروه کارشناسان، {موضوعات زیر} را مورد توجه و ملاحظه قرار دادند:

- پیش‌نویس «بررسی جامع درباره مسئله جرم سایبری» و پاسخگویی به آن توسط دولت‌ها

جامعه بین‌الملل و بخش خصوصی که به موجب قطعنامه مجمع عمومی به شماره ۶۵/۲۳۰ توسط دفتر مقابله با مواد مخدر و جرم سازمان ملل و با راهنمایی گروه کارشناسان تهیه شده بود. - مجموعه موضوعات مصوب در اولین نشست گروه کارشناسان درباره بررسی جامع در خصوص اثر جرم سایبری و پاسخگویی {به آن} و روش‌های مورد بررسی.

در اعلامیه دوحه، دولت‌های عضو به اقدامات گروه کارشناسان، جامعه مدنی و بخش خصوصی درباره پیشگیری یکپارچه از جرم و عدالت کیفری جهت مقابله با چالش‌های اقتصادی و اجتماعی و تقویت حاکمیت قانون در سطوح ملی و بین‌المللی و مشارکت عمومی، توجه نمودند.

{این اعلامیه} در سیزدهمین کنگره ملل متحد درباره پیشگیری از جرم و عدالت کیفری مصوب شد و مجمع عمومی آن را در قطعنامه خود {به شماره} ۷۰/۱۷۴ تأیید نمود؛

سومین نشست گروه کارشناسان مورخ ۱۰ تا ۱۳ آوریل ۲۰۱۷ برگزار گردید. در این نشست گروه کارشناسان خلاصه‌ای از بررسی‌های اولین و دومین نشست گروه کارشناسان را که توسط گزارشگر {ویژه کمیسیون پیشگیری از جرم و عدالت کیفری} ارائه شد، مورد ملاحظه قرار داد و در میان سایر موضوعات، علاوه بر پیش‌نویس بررسی جامع درباره مسئله جرم سایبری، این موضوعات زیر را مورد ملاحظه قرار داد: تفسیر پیش‌نویس، راه‌های پیش روی مبتنی بر این پیش‌نویس، تبادل اطلاعات درباره قانون‌گذاری ملی، رویه‌های برتر، مساعدت فنی و همکاری بین‌المللی. کمیسیون پیشگیری از جرم و عدالت کیفری، در قطعنامه‌ای {به شماره} ۲۶/۴ مصوب بیست و ششمین اجلاس {خود} مورخ می ۲۰۱۷، از گروه کارشناسان درخواست نمود تا: اولاً به کار خود به همان رویه ادامه دهد ثانیاً با هدف {ایجاد} بستری جهت مباحثه بیشتر در خصوص موضوعات محتوایی مربوط به جرم سایبری، نشست‌های دوره‌ای را با حفظ توسعه روندهای خود و در راستای اعلامیه‌های السالوادور و دوحه برگزار نماید. ثالثاً به تبادل اطلاعات در خصوص تدوین قانون ملی، رویه‌های برتر، مساعدت فنی و همکاری بین‌المللی با نگاهی به بررسی گزینه‌ها جهت تقویت قانون ملی و حقوق بین‌المللی موجود و پیشنهاد قانون ملی و حقوق بین‌المللی جدید و سایر پاسخگویی‌ها به جرم سایبری ادامه دهد.

چهارمین نشست گروه کارشناسان در تاریخ ۳ الی ۵ آوریل ۲۰۱۸ در وین برگزار گردید. در

این نشست، گروه کارشناسان روی تدوین قانون و چارچوب‌ها و {همچنین} جرم‌انگاری جرائم سایبری متمرکز شد.

تحولات قانون‌گذاری و خط‌مشی‌ها در رابطه با مقابله با جرم سایبری در سطوح ملی و بین‌المللی مورد بحث بود و ملاحظات دیگری درباره راه‌هایی که در آن جرم سایبری در سطح ملی جرم‌انگاری می‌شود نیز تعیین شد.

همچنین گروه کارشناسان پیشنهاد رئیس برای طرح کار گروه کارشناسان در دوره زمانی ۲۰۱۸ تا ۲۰۲۱ را تصویب کرد.

فهرست توصیه‌ها و نتایج مقدماتی:

در راستای برنامه کاری گروه کارشناسان برای دوره زمانی ۲۰۱۸ تا ۲۰۲۱ {مقرر گردید که}: گزارشگر در هر یک از نشست‌های گروه کاری در سال‌های ۲۰۱۹ و ۲۰۲۰، با مساعدت دبیرخانه و بر مبنای مباحثات و بررسی‌های گروه کارشناسی فهرستی از نتایج مقدماتی و توصیه‌های پیشنهادی دولت‌های عضو مهیا خواهد نمود. این گزارش باید دقیق و مختصر باشد و بر تقویت واکنش‌های کاربردی در خصوص جرم سایبری تمرکز نماید.

همچنین مطابق با طرح کاری، گروه کارشناسان به منظور ایجاد فهرستی جامع و یکپارچه از نتایج و توصیه‌های مصوب و ارائه آن به کمیسیون پیشگیری از جرم و عدالت کیفری، نتایج و توصیه‌های مقدماتی تجمیع شده را بررسی خواهند کرد.

پیش از نشست بررسی، نتایج و توصیه‌های مقدماتی که توسط دولت‌های عضو پیشنهاد گردیده، بین تمامی دولت‌ها عضو، ناظران و سایر ذی‌نفعان منتشر و سپس جهت ملاحظه و بررسی توسط نمایندگان، به شکل برخط به نشست بررسی پیشرفته ارسال خواهد شد. در ادامه این گزارش حاوی مطالبی در این موضوعات زیر می‌باشد: ۱. اجرای قانون و تحقیقات و ۲. ادله الکترونیکی و عدالت کیفری.

این گزارش همچنین حاوی مطالبی در خصوص نشست سازمانی این اجلاس بود. از جمله:

- نشست افتتاحیه؛

- بیانیه‌هایی که توسط کارشناسان کشورهای مختلف ارائه گردید: از جمله الجزایر، آرژانتین،



ارمنستان، استرالیا، بلاروس، برزیل، بورکینا فاسو، کانادا، شیلی، چین، کلمبیا، هند، اندونزی، جمهوری اسلامی ایران، ایتالیا، ژاپن، اردن، کویت، مالزی، موریتانی، مکزیک، مراکش، هلند، نیجر، نیجریه، نروژ، پرو، پاراگوئه، فیلیپین، روسیه، صربستان، اسلواکی، آفریقای جنوبی، اسپانیا، سریلانکا، تایلند، امارات متحده عربی، انگلستان، آمریکا و ویتنام. بیانیه هایی نیز توسط نمایندگان دو سازمان بین دولتی شورای اروپا و اتحادیه اروپا ارائه گردید؛

- تصویب دستور کار و موضوعات سازمانی و مستندات

شورای اقتصادی و اجتماعی سازمان ملل مبحث چهار: کمیسیون مبارزه با مواد مخدر

بند یک: قطعنامه اینترنت سال ۲۰۰۰

ترجمه سند



شورای اقتصادی و اجتماعی
کمیسیون مبارزه با مواد مخدر

تاریخ انتشار: ۱۵ مارس ۲۰۰۰

شماره قطعنامه:

زبان: انگلیسی

توزیع: عمومی

قطعنامه اینترنت

کمیسیون مبارزه با مواد مخدر

با به رسمیت شناختن تبلیغات و فروش پیوسته داروها و مواد پیش‌سازهای شیمیایی تحت کنترل {که} در اکثر کشورها از طریق وب جهان گستر (اینترنت) مورد قاچاق قرار می‌گیرند؛ با ابراز نگرانی عمیق درباره اینکه آگهی، تبلیغ و فروش داروها و مواد پیش‌ساز شیمیایی تحت کنترل با اهداف غیرقانونی به‌عنوان یک فعالیت در سطح بین‌الملل مطرح است که باید زدوده شود و از بین برود تا از آثار زیان‌بار آن روی جامعه، اقتصاد و مؤسسات اجتماعی و سیاسی پیشگیری شود؛

باتوجه به طرح اقدام علیه تولید غیرقانونی، قاچاق و سوءاستفاده از محرک‌های نوع آمفتامین و پیش‌سازهای آن‌ها و باتوجه به سایر قطعنامه‌های مصوب مجمع عمومی در اجلاس بیستم، از جمله اقدامات مقابله‌ای با سوءاستفاده از فناوری‌های جدید به‌ویژه اینترنت توسط سازمان‌های جنایی در زمینه استفاده غیرمجاز و سوءاستفاده از داروها و پیش‌سازهای شیمیایی تحت کنترل با تصمیم بر منع استفاده از وب جهان گستر (اینترنت) جهت اشاعه قاچاق مواد مخدر و سوءاستفاده از آن؛ و با تصمیم بر قطع دسترس‌پذیری داروها و پیش‌سازهای شیمیایی تحت کنترل برای اهداف غیرقانونی از طریق سوء استفاده از اینترنت؛

دولت‌های عضو را تشویق می‌نماید تا اقدامات زیر را جهت ممانعت از استفاده غیرمجاز از

داروهای تحت کنترل و پیش سازهای شیمیایی فراهم شده غیرمجاز از طریق فناوری‌های مبتنی بر وب جهان گستر (اینترنت) مورد نظر قرار دهند:

ا. همکاری دولت‌ها با یکدیگر و تبادل سریع‌تر اطلاعات و تجربیات مرتبط با فروش داروها و پیش سازهای شیمیایی تحت کنترل که از طریق اینترنت در مسیر شبکه‌های غیرقانونی توزیع قرار می‌گیرند؛

ب. ارزیابی مقررات و کنترل‌های قانونی خود درباره تبلیغ و فروش داروها و پیش‌سازهای شیمیایی تحت کنترل از طریق اینترنت در صورت ضرورت، ایجاد یا افزایش سطح کنترل و پایش سایت‌های تارنمایی (اینترنتی) مربوط به داروها و پیش‌سازهای شیمیایی تحت کنترل، به انضمام مجازات‌های کیفری، مدنی و اداری ممکن مطابق با حقوق ملی (داخلی)؛

ج. افزایش سطح همکاری میان پلیس، گمرک‌ها، سایر سازمان‌های مجری قانون و سازمان‌های تنظیم مقررات جهت افزایش کنترل و پایش تلاش‌های برنامه ریزی شده برای محدود نمودن قاچاق داروها و پیش سازهای شیمیایی تحت کنترل از طریق اینترنت همکاری نزدیک با تأمین‌کنندگان خدمات اینترنت و صنایع شیمیایی و دارویی جهت خنثی نمودن سوءاستفاده از این فناوری‌های ارتباطی نوظهور جهت اشاعه سوءاستفاده داروهای مخدر. ارتقای همکاری با تأمین‌کنندگان خدمات اینترنتی، انتشار اطلاعات به‌منظور ممانعت استفاده از داروهای مخدر غیر مجاز.

نشست ۱۱۹۳ (۱۵ مارس ۲۰۰۰)

بند دو: قطعنامه همکاری بین‌المللی در پیشگیری از توزیع غیرقانونی مواد مجاز تحت کنترل در سطح بین‌الملل از طریق اینترنت سال ۲۰۰۷



شورای اقتصادی و اجتماعی
کمیسیون مبارزه با مواد مخدر

ترجمه سند

تاریخ انتشار: ۱۶ جولای ۲۰۰۷

شماره قطعنامه: ۱۱/۵۰

زبان: انگلیسی

توزیع: عمومی

همکاری بین‌المللی در پیشگیری از توزیع غیرقانونی مواد مجاز تحت کنترل در سطح بین‌الملل از طریق اینترنت کمیسیون مبارزه با مواد مخدر

با به رسمیت شناختن اینکه توزیع غیرقانونی مواد مجاز تحت کنترل در سطح بین‌الملل از طریق اینترنت مشکلی فزاینده می‌باشد و اینکه استفاده بدون نظارت از چنین موادی که از طریق اینترنت توسط عموم مردم، مخصوصاً افراد نابالغ خریداری می‌شود، ایجاد خطر جدی برای سلامت جهانی را ایجاد می‌نماید؛

با یادآوری مجدد اینکه، {این کمیسیون} در قطعنامه خود {به شماره} ۴۳/۸، دولت‌های عضو را برای انجام اقدامات همکاری با نگاهی بر ممانعت از استفاده غیرمجاز داروها و پیش‌سازهای شیمیایی تحت کنترل از طریق اینترنت تشویق نمود؛

باتوجه به اینکه شورای بین‌المللی کنترل مواد مخدر در گزارش خود در سال ۲۰۰۶، در میان موارد دیگر، توزیع غیرقانونی مواد مجاز تحت کنترل در سطح بین‌الملل از طریق اینترنت را برجسته نموده است؛

ضمن به رسمیت شناختن اینکه تهیه مواد مجاز تحت کنترل در سطح بین‌المللی از طریق اینترنت، هرگاه معاهده بین‌المللی و حقوق ملی را نقض نماید غیرقانونی می‌باشد؛

با یادآوری اقدامات صورت گرفته در سطوح ملی و بین‌المللی جهت کنترل استفاده غیرمجاز از مواد مجاز تحت کنترل در سطح بین‌المللی، از طریق اجرای مفاد تنها کنوانسیون مواد مخدر مربوط به سال ۱۹۶۱ که توسط پروتکل ۱۹۷۲ اصلاح گردید، {همچنین} کنوانسیون مواد غیر

روان گردان مربوط به سال ۱۹۷۱ و کنوانسیون مقابله با قاچاق غیرمجاز مواد مخدر و روان گردان سازمان ملل متحد مربوط به سال ۱۹۸۸؛

باتوجه به دستور کار تونس برای فاز دوم اجلاس سران درباره جامعه اطلاعاتی که در تاریخ ۱۶ الی ۱۸ نوامبر ۲۰۰۵ در تونس برگزار گردید؛

با اظهار اینکه کمیسیون سازمان دولت‌های آمریکایی در امور کنترل سوءاستفاده از مواد مخدر میان کشورهای آمریکایی، در چهلمین اجلاس مقرر خود که در نوامبر ۲۰۰۶ در سانتاکروز بولیوی برگزار گردید، رهنمودی با عنوان «مواد مخدر در فضای سایبر: درک و تحقیق استفاده مجاز و توزیع مواد تحت کنترل از طریق اینترنت» را تصویب نمود؛

با به رسمیت شناختن اینکه رهنمود فوق، قلمرو موضوعات، عناصر و ابزار برای دولت‌های عضو جهت پاسخگویی به موضوعات از جمله نیاز به تدوین قانون مناسب را طرح ریزی می‌نماید:

۱. به تلاش‌های صورت گرفت توسط سازمان‌های منطقه‌ای و بین‌المللی و نیز دولت‌های عضو، در تصویب اقداماتی جهت مبارزه با توزیع غیر قانونی داروهای مجاز تحت کنترل در سطح بین‌المللی از طریق اینترنت اذعان می‌دارد؛

۲. دولت‌های عضو را دعوت می‌نماید تا تلاش‌های سازمان‌های منطقه‌ای و بین‌المللی را در هنگام بررسی اینکه آیا اقدامات کافی جهت کنترل، تحقیق و پیگرد توزیع غیر قانونی مواد مجاز تحت کنترل بین‌المللی را وجود دارد یا نه، مورد نظر قرار دهند. {اقداماتی} مانند رهنمودی تحت عنوان «داروها در فضای سایبری: درک و تحقیق استفاده غیر مجاز و توزیع مواد تحت کنترل از طریق اینترنت»؛

۳. دولت‌های عضو را تشویق می‌نماید به منظور ارزیابی کامل روندهای مرتبط با موضوع مواد مخدر و مواد مجاز تحت کنترل در سطح بین‌الملل، به اندازه امکان، به شیوه ای استاندارد و منظم، شورای بین‌المللی کنترل مواد مخدر را درباره سفارش و تحویل {این مواد} از طریق اینترنت و ایمیل مطلع نمایند؛

۴. شورای بین‌المللی کنترل مواد مخدر را تشویق می‌نماید تا به فعالیت‌های خود با نگاهی بر بالابردن آگاهی و ممانعت از سوءاستفاده از اینترنت جهت تأمین، فروش و توزیع غیر قانونی



مواد مجاز تحت کنترل در سطح بین‌الملل را ادامه دهد؛

۵. دولت‌های عضوی را که در امر تحقیق در مورد جرائم مرتبط با دارو (جرائم دارویی) در بستر اینترنت دارای تجربه می‌باشند را دعوت می‌نماید تا تجهیزات لازم، آموزش و مساعدت برای سایر دولت‌های عضو، بر اساس درخواست {آن‌ها}، تأمین نمایند، {همچنین از این دولت‌ها درخواست می‌نماید تا} در موقعیتی مناسب با دفتر جرم و مواد مخدر سازمان ملل متحد، جهت افزایش منابع بودجه همکاری نمایند؛

۶. بر تداوم بحث درباره این موضوعات مهم در اجلاس چهل‌ویکم خود تصمیم می‌گیرد؛

۷. از مدیر اجرایی دفتر جرم و مواد مخدر ملل متحد درخواست می‌نماید تا متن قطعنامه موجود را به تمامی کشورهای عضو ارسال نماید.

بند سه: قطعنامه تقویت همکاری بین‌المللی به منظور پیشگیری از استفاده از اینترنت در ارتکاب مرتبط با مواد مخدر سال ۲۰۰۵



شورای اقتصادی و اجتماعی
کمیسیون مبارزه با مواد مخدر

ترجمه سند

تاریخ انتشار: ۱۱ مارس ۲۰۰۵

شماره قطعنامه:

زبان: انگلیسی

توزیع: عمومی

تقویت همکاری بین‌المللی به منظور پیشگیری از استفاده از اینترنت در ارتکاب مرتبط با مواد مخدر
- کمیسیون مبارزه با مواد مخدر

با یادآوری کنوانسیون مقابله با قاچاق غیرقانونی مواد مخدر و روانگردان سازمان ملل متحد
مربوط به سال ۱۹۸۸

با در نظر گرفتن اینکه در مبارزه علیه قاچاق غیرقانونی مواد مخدر می توان جهت مقابله با اشکال جدید جرائم سازمان یافته فراملی از فناوری‌های نوآورانه بهره جست؛
با آگاهی از اهمیتی اشکال جدید جرائم سازمان یافته فراملی از فناوری‌های نوآورانه بهره جست؛
با آگاهی از اهمیتی که شورای بین‌المللی کنترل مواد مخدر به تلاش‌های دولت‌ها جهت پیشگیری از استفاده اینترنت جهت ترویج سوءاستفاده و قاچاق مواد مخدر و روان گردان قائل است،
مصرانه از دولت‌های عضو می خواهد، مطابق با نظام‌های قانونی خود، با نگاهی بر تقویت اثربخشی اقدام نیروی پلیس با استفاده از اینترنت جهت مبارزه با جرم مرتبط با مواد مخدر همکاری نمایند؛
- دولت‌های عضو را فرا می خواند تا مطابق با نظام‌های قانونی خود، به اندازه نیاز، از فناوری‌های نوین اجرای قانون جهت ممانعت از استفاده اینترنت برای ارتکاب جرائم مرتبط با مواد مخدر استفاده نمایند؛

- دولت‌های عضو دارای مهارت‌های مناسب را دعوت می‌نماید تا سایر دولت‌ها را در زمینه طرح‌ریزی و اجرای برنامه‌های آموزشی، جهت اشتراک‌گذاری مهارت‌ها در زمینه پیشگیری از استفاده اینترنت جهت ارتکاب جرائم مرتبط با مواد مخدر مساعدت نمایند.

بند یک: بازنگری ده ساله اجلاس سران درباره جامعه اطلاعاتی ۲۰۱۵
(WSIS+10)



ترجمه سند

تاریخ انتشار: ۱ فوریه ۲۰۱۶

شماره قطعنامه: A/RES/70/125

توزیع: عمومی

اجلاس هفتادم

دستورکار ۱۷

قطعنامه مصوب مجمع عمومی مورخ ۱۶ دسامبر ۲۰۱۵

مجمع عمومی

سند خروجی نشست سطح بالای مجمع عمومی در خصوص بازنگری کلی اجرای نتایج اجلاس سران درباره جامعه اطلاعاتی را در اجلاس هفتادم خود تصویب نمود.

سند خروجی نشست سطح بالای مجمع عمومی در خصوص بازنگری کلی اجرای نتایج اجلاس سران درباره جامعه اطلاعاتی:

ماء، وزرا و روسای هیئت نمایندگان شرکت کننده در نشست سطح بالای عمومی مجمع عمومی در خصوص بازنگری کلی اجرای خروجی های اجلاس سران درباره جامعه اطلاعاتی که در ۱۵ و ۱۶ دسامبر ۲۰۱۵ در نیویورک برگزار گردید:

با یادآوری درخواست مندرج در بند ۱۱۱ دستورکار تونس درباره جامعه اطلاعاتی که در آن، مجمع عمومی متعهد به اجرای بازنگری کلی در خصوص انجام نتایج اجلاس سران درباره جامعه اطلاعاتی در سال ۲۰۱۵ گردید و در این رابطه ضمن تأیید مجدد نقش مجمع عمومی در این فرایند، و همچنین با تأیید مجدد تصمیم مجمع در قطعنامه خود به شماره ۶۸/۳۰۲ مورخ ۳۱ جولای ۲۰۱۴ مبنی بر برگزاری نشست دو روزه سطح بالا توسط مجمع که با وجود برجسته بودن نقش دولت ها در فرایند مقدماتی این نشست، نظرهای تمامی ذی نفعان مرتبط مورد نظر قرار گرفت.

با استقبال از نظرهای سازنده و مختلف دولت‌ها، بخش‌های خصوصی، جامعه مدنی، سازمان‌های بین‌المللی، جوامع فنی و دانشگاهی و تمامی ذی‌نفعان مرتبط در بررسی پیشرفت اجرای نتایج اجلاس سران درباره جامعه اطلاعاتی و با پرداختن به حوزه‌ها و شکاف‌های بالقوه فناوری اطلاعات و ارتباطات جهت تمرکز دامنه‌دار و نیز پرداختن به چالش‌ها از جمله از بین بردن شکاف‌ها و هدایت فناوری‌های اطلاعات و ارتباطات را راستای توسعه؛

در کنار سایر نظرهای مربوط، با مبنا قرار دادن {رویداد و اسناد زیر}؛ بازنگری ۱۰ ساله اجلاس سران درباره جامعه اطلاعاتی که توسط کمیسیون علم و فناوری برای توسعه در می سال ۲۰۱۵ برگزار گردید و سند خروجی آن تحت عنوان «اجرای نتایج اجلاس سران درباره جامعه اطلاعاتی: بازنگری ۱۰ ساله»؛ رویداد بازنگری ۱۰ ساله چند ذی‌نفعی با عنوان «به سوی جوامع اطلاعاتی برای صلح و توسعه پایدار» که توسط سازمان یونسکو در فوریه ۲۰۱۳ برگزار گردید و بیانیه نهایی آن با عنوان «دانش و اطلاعات برای همه: نظر(نگاه) توسعه‌یافته و تعهد بازنگری شده»؛ رویداد چندذی‌نفعی سطح بالا جهت بازنگری اجلاس سران که توسط اتحادیه بین‌المللی مخابرات در جولای ۲۰۱۴ هماهنگ و برگزار گردید و توسط این اتحادیه، «کنفرانس تجارت و توسعه سازمان ملل» و «برنامه توسعه سازمان ملل» سازماندهی گردید و خروجی‌های آن و {در نهایت} رویکرد یا منویات بازنگری ۱۰ ساله اجلاس سران پیش از ۲۰۱۵، که هر دو بازنگری از طریق اجماع تصویب گردید،

ضمن تأیید مجدد قطعنامه مجمع عمومی {به شماره} ۷۰/۱ مورخ ۲۵ سپتامبر ۲۰۱۵ تحت عنوان «تبدیل دنیا ما: دستور کار توسعه پایدار» که در آن مجموعه‌ای جامع، گسترده، مردم‌محور از اهداف و مقاصد تحول محور و جهانی توسعه پایدار تصویب شد، تعهدات خود جهت کار خستگی‌ناپذیر برای اجرای کامل دستور کار توسعه پایدار، با به رسمیت شناختن اینکه ریشه کن کردن فقر در تمامی اشکال و ابعاد آن، از جمله فقر شدید، بزرگ‌ترین چالش جهانی و یک نیاز ضروری برای توسعه پایدار است و به رسمیت شناختن تعهد خود جهت دستیابی به توسعه پایدار در سه بعد اقتصادی، اجتماعی و زیست محیطی به نحو متعادل و یکپارچه، و بر اساس دستاوردهای اهداف توسعه هزاره و تلاش برای پرداختن به کارهای ناتمام آن‌ها،

همچنین با تأیید مجدد قطعنامه خود {به شماره} ۶۹/۳۱۳ مورخ ۲۷ جولای ۲۰۱۵ در خصوص دستور کار اقدام آدیس آبابا در سومین کنفرانس بین‌المللی تأمین مالی توسعه که بخش جداناپذیری از دستورکار توسعه پایدار برای توسعه پایدار می‌باشد، از این دستورکار پشتیبانی می‌کند و آن را تکمیل می‌نماید، و با اقدامات و سیاست‌های ملموس (عینی) جهت تحقق بخشیدن به اهداف خود در اجرای مقاصد کمک می‌کند و مجدداً تعهد سیاسی قوی جهت مقابله با چالش‌های مالی و ایجاد محیطی توانمند با روحیه همبستگی و مشارکت جهانی در کلیه سطوح توسعه پایدار را تأیید می‌کند:

۱. ما مجدداً آرزو و تعهد مشترک خود را درباره نظر رویکرد اجلاس سران درباره جامعه اطلاعاتی به‌منظور ایجاد جامعه اطلاعاتی مردم‌محور، فراگیر و توسعه محور تأیید می‌نماییم، {جامعه اطلاعاتی} که در آن هر شخصی بتواند اطلاعات و دانش را تولید نماید، به آن‌ها دسترسی داشته باشد از آن‌ها استفاده نماید و آن‌ها را به اشتراک بگذارد، {جامعه اطلاعاتی} که در آن اشخاص، جوامع و مردم ضمن مبنا قرار دادن اهداف، اصول منشور سازمان ملل و احترام کامل و تأیید اعلامیه جهانی حقوق بشر، بتوانند قابلیت‌های کامل خود را در ارتقای توسعه پایدار و بهبود کیفیت زندگی خود کسب نمایند؛

۲. علاوه بر اینکه ما مجدداً تعهدات خود را درباره اعلامیه اصول ژنو، طرح و خطوط اقدام ژنو، تعهد و دستورکار تونس درباره جامعه اطلاعاتی تأیید می‌نماییم، ما نیاز دولت‌ها، بخش‌های خصوصی، جامعه مدنی، سازمان‌های بین‌المللی، جوامع فنی و دانشگاهی و تمامی ذی‌نفعان مربوط جهت تداوم همکاری در اجرای منویات اجلاس سران درباره جامعه اطلاعاتی پس از سال ۲۰۱۵ را به رسمیت می‌شناسیم؛

۳. علاوه بر این، ما مجدداً {این موارد} را تأیید می‌نماییم، ارزش و اصل همکاری چند ذی‌نفعی و تعاملاتی که فرایند اجلاس سران از بدو امر، آن را ترسیم کرده است، در نظر گرفتن {اهمیت} همکاری و مشارکت مؤثر دولت‌ها، بخش‌های خصوصی، جامعه مدنی، سازمان‌های بین‌المللی، جوامع فنی و دانشگاهی و کلیه ذی‌نفعان مربوط، مخصوصاً {همکاری متوازن نمایندگان کشورهای در حال توسعه} در نقش‌ها و مسئولیت‌های مربوط خود در توسعه جامعه اطلاعاتی

و ضرورت تداوم {این همکاری‌ها}؛

۴. ما از تکامل و افزایش قابل توجه سطح پوشش فناوری‌های اطلاعات و ارتباطات که توسط همکاری‌های بخش‌های عمومی و خصوصی پایه‌ریزی شده است، و به نظر می‌رسد تقریباً در هر گوشه جهان ورود و نفوذ کرده است، استقبال می‌نماییم، {همچنین} ضمن توجه به چالش‌های نوظهور و منحصر به فرد مرتبط با تکامل و گسترش {این فناوری‌ها}، از ایجاد فرصت‌های جدیدی برای تعامل اجتماعی، توانمندسازی الگوهای نوین تجارت، مشارکت در رشد و توسعه اقتصادی در کل بخش‌های دیگر {توسط این فناوری‌ها} استقبال می‌نماییم؛

۵. ما ایفای نقش حیاتی افزایش دسترسی، نوآوری، اتصالات {اینترنتی} در پیشرفت توانمندی در اهداف توسعه هزاره را به رسمیت می‌شناسیم و هماهنگی نزدیک بین فرایند اجلاس سران درباره جامعه اطلاعاتی را تقاضا می‌کنیم، {همچنین} نقش میان بر فناوری اطلاعات و ارتباطات را در اهداف توسعه پایدار و ریشه کنی فقر برجسته می‌نماییم، و اینکه دسترسی به فناوری‌های اطلاعات و ارتباطات یک شاخص برای توسعه و فی نفسه به یک آرزو بدل شده است را مورد توجه و اشاره قرار می‌دهیم؛

۶. ما نگرانی خود را از اینکه هنوز شکاف‌های دیجیتالی قابل توجهی از قبیل شکاف بین کشورها و همچنین شکاف بین مناطق مختلف در داخل یک کشور وجود دارد بیان می‌نماییم که برای مقابله با آن‌ها لازم است در کنار اقدامات دیگر، درباره تقویت توانمندی‌های محیط‌های سیاسی و همکاری‌های بین‌المللی با هدف بهبود کم‌هزینه کردن، دسترسی، آموزش، ظرفیت‌سازی، چندزبانی، صیانت فرهنگی، سرمایه‌گذاری و تأمین مالی مناسب اقدام شود؛

۷. ما اذعان می‌نماییم که جهت مقابله با چالش‌های منحصر به فرد و نوظهور در فناوری اطلاعات و ارتباطات که تمامی کشورها با آن مواجه شده‌اند، باید تلاش‌های ویژه‌ای صورت پذیرد، مخصوصاً کشورهای در حال توسعه آفریقایی، کشورهای کمتر توسعه یافته، کشورهایی در حال توسعه محصور در خشکی و دولت‌های جزیره‌ای کوچک در حال توسعه و کشورهایی با درآمد متوسط و نیز کشورها و سرزمین‌های تحت اشغال عوامل بیگانه، کشورهای در شرایط تخصم، کشورهای پسا تخصم و کشورهای متأثر از بلایای طبیعی. همچنین اذعان می‌نماییم که جهت مقابله با چالش‌های

مربوط به فناوری و ارتباطات که کودکان، جوانان، افراد معلول، افراد مسن، مردم بومی، پناهندگان سیاسی و تبعیدشدگان داخلی، مهاجران و جوامع دوردست و روستایی با آن‌ها مواجه می‌باشند، باید تلاش‌های ویژه‌ای صورت پذیرد؛

۸. ما ضرورت تداوم پیگیری مفاد تعیین شده در خروجی اجلاس ژنو و تونس را تأیید می‌نماییم؛
۹. علاوه بر این ما مجدداً تأیید می‌نماییم که حقوق مردم در فضای برخط باید مشابه فضای غیربرخط مورد حفاظت و حمایت قرار گیرد. ما تأکید می‌کنیم که حرکت و پیشروی به سوی آمل و اهداف اجلاس سران درباره جامعه اطلاعاتی نه تنها باید به‌عنوان تابعی از توسعه اقتصادی و گسترش فناوری‌های اطلاعات و ارتباطات مورد نظر قرار گیرد بلکه باید با ارتقای احترام به تحقق حقوق بشر و آزادی‌های اساسی همراه باشد؛

۱۰. به‌ویژه با توجه به رشد چالش‌ها، از جمله سوءاستفاده از فناوری‌های اطلاعات و ارتباطات جهت انجام اقدامات مضر از آزار و اذیت گرفته تا جرائم تروریستی، اطمینان‌سازی و امنیت در استفاده از چنین فناوری‌هایی برای توسعه پایدار باید در اولویت قرار گیرد؛

۱۱. ما بر تعهدات خود در استفاده مثبت از اینترنت و سایر فناوری‌های اطلاعات و ارتباطات و همچنین بر { اتخاذ اقدامات مناسب و پیشگیرانه قانونی {حقوقی}، علیه سوءاستفاده از آن فناوری‌ها، مطابق ابعاد اخلاقی جامعه اطلاعاتی مذکور در اعلامیه اصول و طرح اقدام ژنو تأکید می‌نماییم؛

۱. فناوری اطلاعات و ارتباطات برای توسعه

۱۲. ضمن توجه به توانایی فناوری اطلاعات و ارتباطات جهت شتاب بخشی در پیشبرد تمامی ۱۷ هدف توسعه پایدار، ما متعهد هستیم تا قابلیت این فناوری‌ها در دستیابی به دستورکار توسعه پایدار و سایر اهداف توسعه مورد توافق در فضای بین‌المللی را فراهم نماییم. از این رو ما از تمامی دولت‌ها، بخش‌های خصوصی، جامعه مدنی، سازمان‌های بین‌المللی، جوامع فنی و دانشگاهی و تمامی ذی‌نفعان مربوط درخواست می‌نماییم تا فناوری‌های اطلاعات و ارتباطات را در رویکردهای خود جهت اجرای این اهداف یکپارچه نمایند و از نهادهای سازمان ملل درخواست می‌نماییم تا خطوط اقدام اجلاس سران درباره جامعه اطلاعاتی را جهت بررسی

گزارش‌دهی و برنامه‌های کاری خود برای پشتیبانی از اجرای دستورکار توسعه پایدار تسهیل نمایند؛

۱۳. ما ضمن ابراز خرسندی از رشد قابل ملاحظه در گسترش اینترنت، استفاده، ایجاد و نوآوری در دهه‌های گذشته، {آن‌ها را به‌عنوان} ابزار جدیدی جهت ریشه‌کنی فقر و ایجاد بهبود در {شرایط} اقتصادی، اجتماعی و محیطی به رسمیت می‌شناسیم. به‌عنوان مثال در زمان تصویب دستور کار تونس، اینترنت ثابت با پهنای باند بی‌سیم، اینترنت سیار، تبلت‌ها و تلفن‌های هوشمند، پردازش ابری، داده‌های باز، رسانه اجتماعی و کلان داده در مراحل اولیه {رشد} خود بودند و در حال حاضر {این ابزار} توانمندسازهای قابل توجهی برای توسعه به حساب می‌آیند؛

۱۴. ما مجدداً تأیید می‌نماییم که در فرایند اجلاس سران درباره جامعه اطلاعاتی، {موضوع} توسعه و استفاده از فناوری‌های اطلاعات و ارتباطات باید به‌عنوان کانون و خروجی اصلی تداوم یابد. ما از تخمین به‌دست آمده درخصوص ارتقای تعداد مشترکان تلفن‌های همراه از ۲/۲ میلیارد در سال ۲۰۰۵ به ۷/۱ میلیارد در سال ۲۰۱۵ و {همچنین از اینکه} انتظار می‌رود تا پایان سال ۲۰۱۵، ۳/۲ میلیارد نفر (۴۳ درصد از جمعیت کل جهان) برخط باشند و اینکه ۲ میلیارد نفر از آن‌ها متعلق به کشورهای در حال توسعه هستند دلگرم شدیم. همچنین ما به این موضوع توجه می‌نماییم که نرخ نفوذ مشترکان پهنای باند ثابت در مقایسه با سال ۲۰۰۵ از ۳/۴ درصد به ۱۰ درصد {در سال ۲۰۱۵} رسیده است و پهنای باند سیار در بازار با نرخ رشد دو رقمی {معادل} ۴۷ درصد در سال ۲۰۱۵ (افزایش ۱۲ برابری از سال ۲۰۰۷) سریع‌ترین رشد را دارد؛

۱۵. ما بر این نکته توجه می‌نماییم که اقتصاد دیجیتالی بخش مهم و در حال رشدی از اقتصاد جهانی می‌باشد و اتصالات اینترنتی به افزایش تولید ناخالص داخلی وابسته می‌باشد. فناوری‌های اطلاعات و ارتباطات نسل جدیدی از کسب‌وکار (تجارت)، مبتکران و مشاغل را ایجاد کرده‌اند، ضمن اینکه {کسب‌وکار و مشاغل} دیگر تغییر کرده و در حال منسوخ شدن می‌باشند. ما اهمیت حیاتی توسعه مشارکت تمامی کشورها مخصوصاً کشورهای در حال توسعه را در اقتصاد دیجیتال به رسمیت می‌شناسیم؛

۱۶. ما همچنین مشارکت و همکاری فناوری‌های اطلاعات و ارتباطات را در این امور به رسمیت می‌شناسیم: مزایا و مشمولیت‌های اجتماعی در سطوح بالاتر، فراهم سازی شبکه‌هایی میان شهروندان، شاغلان و تشکیلات دولتی جهت به اشتراک‌گذاری و تقویت دانش و نیز مشارکت در تصمیم‌هایی که زندگی و کار شهروندان و شاغلان را تأثیر تحت تأثیر قرار می‌دهد؛

۱۷. ما همزمان با این موضوع که فناوری اطلاعات و ارتباطات به شکل اساسی تعاملات فردی و اجتماعی و زمان صرف شده برای این تعاملات را تغییر می‌دهد، پیامدهای بهداشتی و اجتماعی پیش‌بینی نشده ناشی از این فناوری‌ها را که بسیاری از آن‌ها مثبت و برخی دیگر باعث بروز نگرانی می‌شوند را تصدیق می‌نماییم؛

۱۸. ما اهمیت فناوری اطلاعات و ارتباطات را در پاسخگویی در برابر سوانح و پاسخ‌های بشر دوستانه تصدیق می‌نماییم و علاوه بر این مجدداً نقش این فناوری‌ها را در ارتقای و توسعه سیستم‌های هشدار چند مخاطره‌ای سریع، آمادگی، پاسخ‌گویی، بهبود، نوسازی و بازسازی تأیید می‌نماییم. همچنین ما سرمایه‌گذاری‌های بیشتر را در نوآوری و توسعه فناوری {همچنین} برای تحقیقات درازمدت، چند مخاطره‌ای و چاره‌ساز در حوزه مدیریت خطر سوانح تشویق می‌نماییم.

۱۹. ما همچنین {نقش} فزاینده فناوری‌های اطلاعات و ارتباطات را {به‌عنوان} حامی و پشتیبان از تفاوت موجود در تجلی و رشد سریع فرهنگ و صنایع خلاق، تصدیق می‌نماییم و ما مجدداً نیاز به راهبردهای جامع و دیجیتال عملی جهت محافظت از میراث فرهنگی و دسترسی به تمامی اشکال اطلاعات ثبت شده در محیط دیجیتالی را تأیید می‌نماییم؛

۲۰. به‌علاوه، ما مزایا و مضرات محیطی ناشی از افزایش استفاده از فناوری اطلاعات و ارتباطات و هدف خود مبنی بر کاهش این هزینه‌ها را به رسمیت می‌شناسیم.

۱.۱. از بین بردن شکاف‌های دیجیتالی

۲۱. باوجود دستاوردهای دهه‌های قبل در زمینه اتصالات فناوری اطلاعات و ارتباطات، منگرانی خود را مبنی بر باقی ماندن اشکال متعدد شکاف‌های دیجیتالی بین کشورها و در داخل یک کشور ابراز می‌داریم. ما {این موضوع که} شکاف‌های دیجیتالی اغلب به سطوح آموزشی و عدم کیفیت

{آموزشی} مرتبط می‌باشد را مورد توجه قرار می‌دهیم و اینکه تا زمانی که توسعه پایدار به کندی پیش رود، شکاف‌های بیشتری در آینده می‌توانند ظهور یابند را مورد تصدیق قرار می‌دهیم. {همچنین} ما اذعان می‌داریم که تا سال ۲۰۱۵، تنها حدود ۴۳ درصد مردم جهان به اینترنت دسترسی داشتند و مطابق یک ارزیابی حدود ۸۰ درصد محتوای آن لاین به ۱۰ زبان در دسترس بود؛

۲۲. علاوه بر این ما از شکاف دیجیتال موجود بین کشورهای توسعه‌یافته و کشورهای در حال توسعه {و از} عدم دسترسی کم‌هزینه بودن به فناوری‌های اطلاعات و ارتباطات در بسیاری از کشورهای در حال توسعه ابراز نگرانی می‌نماییم. تا سال ۲۰۱۵، تنها ۳۴ درصد از خانوارها در کشورهای در حال توسعه، با اختلاف قابل توجهی در مقایسه با خانوارها در کشورهای توسعه‌یافته (۸۰ درصد) به اینترنت دسترسی داشتند و این بدان معناست که دو سوم خانوارها در کشورهای در حال توسعه به اینترنت دسترسی ندارند.

۲۳. ما تعهدات خود مبنی بر از بین بردن شکاف‌های دیجیتالی و دانشی را تأیید می‌کنیم. ما بر این باوریم که رویکرد ما باید چند بعدی و شامل یک فهم منطقی از عناصر و منابع در دسترس با تأکید بر کیفیت دسترسی باشد ما ضمن اذعان بر عناصر اصلی کیفیت در عصر حاضر {مانند} سرعت، ثبات، کم‌هزینه بودن، زبان، محتوای منطقه‌ای و قابلیت دسترس‌پذیری برای اشخاص معلول و نیز ضرورت پهنای باند با سرعت بالا به‌عنوان عنصری توانمند برای توسعه پایدار که از گذشته‌ها مطرح شده است، وجود تفاوت در قابلیت فردی در دو زمینه استفاده و ایجاد فناوری‌های اطلاعات و ارتباطات را که معرف شکاف دانشی می‌باشد و دائماً عدم تساوی و نابرابری را به دنبال دارد اعلام می‌داریم. به‌علاوه ما به آرزوی گذر از جوامع اطلاعاتی به سمت جوامع دانشی توجه می‌نماییم، آرزویی که در آن اطلاعات نه تنها ایجاد شده و منتشر می‌گردند بلکه در راستای توسعه منافع انسانی به کار برده می‌شوند. ما چنین شکاف‌هایی را که ممکن است با نوآوری فنی و خدماتی تغییر یابند را تصدیق می‌کنیم و نیز از تمامی ذی‌نفعان به‌ویژه نهادهای تخصصی سازمان ملل متحد که {روند} خطوط اقدام اجلاس سران درباره جامعه اطلاعاتی را تسهیل می‌نمایند، درخواست می‌کنیم در دستور کار و منابع موجود، ماهیت شکاف‌های دیجیتالی

را تحلیل و راهبردهای {موجود} را برای از بین بردن آن‌ها بررسی نمایند و یافته‌های خود را در اختیار جامعه بین‌المللی قرار دهند؛

۲۴. ما بر ضرورت توسعه بیشتر خدمات و محتوای محلی قابل دسترس برای تمامی مردم به زبان‌ها و قالب‌بندی‌های (فرمت‌های) مختلف و {همچنین} ضرورت قابلیت‌ها و ظرفیت‌ها از جمله {در حوزه} رسانه، اطلاعات و مهارت سواد دیجیتالی به‌منظور بهره‌برداری و توسعه بیشتر از فناوری‌های اطلاعات و ارتباطات، را تأکید می‌نماییم؛

۲۵. علاوه بر این ما افزایش قابل توجه در دسترسی به فناوری‌های اطلاعات و ارتباطات را خواستاریم؛

۲۶. همچنین ما {وجود} شکاف‌های دیجیتالی در کاربرد و سواد دیجیتالی و نیاز جهت از بین بردن آن‌ها را به رسمیت می‌شناسیم؛

۱.۲. محیط توانمندساز

۲۷. ما خطوط مشی قطعی در از بین بردن شکاف‌های دیجیتالی و {همچنین} ارزش فناوری‌های اطلاعات و ارتباطات که برای توسعه پایدار مشارکت و همکاری داشته‌اند را به رسمیت می‌شناسیم و بر تداوم شناسایی و اجرای رویه‌های برتر و نوظهور در تشکیل و اعمال چارچوب‌های آموزش، نوآوری و سرمایه‌گذاری در فناوری‌های اطلاعات و ارتباطات تعهد می‌نماییم؛

۲۸. ما اهمیت جریان آزاد اطلاعات و دانش را به رسمیت می‌شناسیم. همان‌گونه که میزان توزیع اطلاعات در جهان افزایش یافت و نقش ارتباطات بیش از پیش مهم‌تر گردید. بر تسهیل منافع قابل توجه در اتصالات اینترنتی و توسعه پایدار در بسیاری از کشورها {از طریق این موارد} اذعان داریم: مسیر اصلی فناوری‌های اطلاعات و ارتباطات در برنامه‌های تحصیلی مدارس، دسترسی آزاد به داده‌ها، تقویت رقابت، ایجاد نظام‌های قانونی و مقررات شفاف، قابل پیش‌بینی، مستقل و غیرتبعیض‌آمیز، همکاری چندذی‌نفعی، راهبردهای پهنای باند ملی و منطقه‌ای، تخصیص مؤثر طیف‌های فرکانس رادیویی، مدل‌های اشتراک‌گذاری زیرساخت، رویکردهای جامعه محور و تسهیلات دسترسی عمومی؛

۲۹. ما فقدان دسترسی به فناوری و خدمات کم‌هزینه و قابل اعتماد را به‌عنوان یک چالش حیاتی در کشورهای در حال توسعه به‌ویژه کشورهای آفریقایی، کشورهای کمتر توسعه‌یافته، کشورهای در حال توسعه محصور در خشکی و دولت‌های جزیره‌ای کوچک در حال توسعه و کشورهای با درآمد متوسط به رسمیت می‌شناسیم. تمامی تلاش‌ها باید در جهت کاهش قیمت فناوری اطلاعات و ارتباطات و دسترسی پهنای باند صورت پذیرد؛

۳۰. دولت‌ها مُصر گردیده اند، ضمن اجتناب از اقدامات یک طرفه و مغایر با حقوق بین‌الملل و منشور ملل متحد که مانع دستیابی کامل به توسعه اقتصادی و اجتماعی و {همچنین} سبب بروز عقب ماندگی در رفاه عمومی مردم در کشورهای تحت تأثیر می‌باشد، جهت تشکیل یک جامعه اطلاعاتی، گام‌هایی را اتخاذ نمایند؛

۳۱. ما ضرورت مدیریت طیف فرکانس رادیویی در راستای منافع عمومی و وفق اصول قانونی و ضمن رعایت کامل حقوق و مقررات ملی و توافقات بین‌المللی مربوط را به رسمیت می‌شناسیم.

۳۲. ما تقاضای نماییم جهت بهبود و (پیشرفت) محیطی توانمندساز برای فناوری‌های اطلاعات و ارتباطات و توسعه آموزش مرتبط و فرصت‌های ظرفیت‌ساز، اقدامات متمرکز ویژه ای انجام گیرد همچنین ما از کمیسیون علم و فناوری برای توسعه، درخواست می‌نماییم تا در دستور کار خود مربوط به پیگیری اجلاس سران درباره جامعه اطلاعات و تمامی تسهیل‌کنندگان خطوط اقدام، {و همچنین} در دستور کارهای مربوط به خود و منابع موجود، با تمامی ذی‌نفعان جهت {این امور} همکاری نمایند: شناسایی منظم و ارتقای اقدامات ویژه تفصیلی جهت حمایت از محیطی توانمند برای فناوری‌های اطلاعات و ارتباطات؛

۱.۳ سازوکارهای مالی

۳۳. ما از این حقیقت استقبال می‌نماییم که مجموع {منابع مالی} خصوصی و عمومی که صرف فناوری‌های اطلاعات و ارتباطات می‌شود اساساً در دهه گذشته افزایش یافته و در حال حاضر سالانه به چندین تریلیون دلار رسیده است و گسترش و توسعه سازوکارهای جدید مالی منتج به پیشرفت در دو بند ۲۳ و ۲۷ دستور کار تونس شده است؛

۳۴. به هر حال ما به رسمیت می‌شناسیم که کنترل توسعه فناوری اطلاعات و ارتباطات و از بین بردن شکاف‌های دیجیتالی نیازمند سازوکارهای سرمایه‌گذاری پایدار و گسترده‌تری در زیرساخت‌ها و خدمات، ظرفیت‌سازی، ارتقای تحقیق و توسعه مشترک و انتقال فناوری به شکل متقابل و طی دوره‌های مورد توافق خواهد بود. با ذکر این نکته که اولویت تمرکز این سازوکارها بر مردم و کشورهای در حال توسعه می‌باشد؛

۳۵. ما متعهد هستیم {ضمن} تصدیق نیاز به تأمین بودجه برای فناوری اطلاعات و ارتباطات در تمامی بخش‌ها مخصوصاً آموزش، منابع عمومی مؤثری را جهت به‌کارگیری و توسعه فناوری اطلاعات و ارتباطات اختصاص دهیم، ما بر {عامل} ظرفیت به‌عنوان یک مانع اصلی جهت از بین بردن شکاف‌های دیجیتالی تأکید می‌کنیم و بر اهمیت توسعه ظرفیت از جمله در نوآوری، در تقویت کارشناسان و جوامع محلی جهت بهره‌مندی کامل و همکاری در کاربردهای فناوری اطلاعات و ارتباطات برای توسعه، توصیه می‌نماییم. ما قابلیت پیشرفت و بهبود اتصالات اینترنت به‌ویژه در نواحی دور و روستایی را در میان سایر ابزار، از طریق تأمین مالی خدمات جهانی و زیرساخت‌های شبکه‌های سرمایه‌گذاری عمومی مخصوصاً در مناطقی که در شرایط بازار جهت سرمایه‌گذاری مشکل می‌باشد، به رسمیت می‌شناسیم؛

۳۶. ما ضمن توجه به تعهدات ایجاد شده در دستورکار اقدام آدیس آبابا در سومین کنفرانس تأمین مالی توسعه، مساعدت رسمی در توسعه و سایر جریان‌های مالی انحصاری برای فناوری اطلاعات و ارتباطات، که می‌تواند به طور قابل توجهی در ایجاد (شکل‌گیری) خروجی‌های توسعه همکاری نمایند را به رسمیت می‌شناسیم، به‌ویژه جایی که آن‌ها می‌توانند خطر سرمایه‌گذاری عمومی و خصوصی را کاهش دهند و استفاده از فناوری‌های اطلاعات و ارتباطات را برای حکمرانی شایسته و جمع‌آوری مالیات افزایش دهند؛

۳۷. ما ضمن به رسمیت شناختن اهمیت حیاتی سرمایه‌گذاری بخش خصوصی در زیرساخت فناوری اطلاعات و ارتباطات، محتوا و خدمات و درانته‌ها، اهمیت مشارکت {توآمان} بخش‌های خصوصی و عمومی، راهبردهای دسترسی جهانی و سایر رویکرد‌ها، دولت‌ها را جهت ایجاد چارچوب‌های قانونی و تنظیم مقررات که منجر به نوآوری و سرمایه‌گذاری فزاینده خواهد شد تشویق می‌نماییم.

۳۸. ما خصوصیات برجسته اتخاذ شده در سازوکار تسهیل فناوری جدید در دستورکار اقدام آدیس آبابا درباره فناوری‌های اطلاعات و ارتباطات و توجه به چگونگی توانایی آن در کمک به اجرای خطوط اقدام اجلاس سران درباره جامعه اطلاعاتی را تشویق می‌نماییم؛

۳۹. ضمن نگرانی از چالش‌های موجود در اجرای {فرایند} تأمین مالی مشترک دیجیتال که در دستورکار تونس به‌عنوان سازوکار مالی ابتکاری با ماهیتی داوطلبانه قید شد، ما ارزیابی {وضعیت} پیشرفت گزینه‌های مالی ابتکاری را در بازنگری سالانه خروجی نتایج اجلاس سران را خواستاریم.

۲. حقوق بشر در جامعه اطلاعاتی

۴۰. ضمن تأیید مجدد تعهدات تنظیم شده در اعلامیه اصول ژنو و تعهدات تونس درباره تمامی {ابعد} حقوق بشر و آزادی‌های اساسی، از جمله حق توسعه، به شکل فراگیر، تقسیم‌ناپذیری، همبستگی و رابطه متقابل، همان‌گونه که به‌صورت مشترک در اعلامیه وین و برنامه اقدام کنفرانس جهانی حقوق بشر بیان شده است، ما همچنین مجدداً تأیید می‌نماییم که دموکراسی، توسعه پایدار و احترام به حقوق بشر و آزادی‌های اساسی و نیز حکمرانی شایسته در تمامی سطوح متکی به یکدیگر هستند و متقابلاً همدیگر را تقویت می‌نمایند؛

۴۱. ما حقوق بشر را به‌عنوان {عنصر} محوری در رویکردهای اجلاس سران درباره جامعه اطلاعاتی و قابلیت‌های فناوری‌های اطلاعات و ارتباطات را در تقویت بهره‌مندی از حقوق بشر، توانمندسازی دسترسی به اطلاعات، آزادی بیان و آزادی تشکیل مجامع و مؤسسات به رسمیت می‌شناسیم؛

۴۲. به‌علاوه ما مجدداً ضرورت حمایت از حقوق مردم در فضای برخط مشابه فضای غیر برخط را به‌عنوان بنیاد اصلی جامعه اطلاعاتی تأیید می‌کنیم، همان‌گونه که {این ضرورت} در قطعنامه شورای حقوق بشر {به شماره} ۲۶/۱۳، مورخ ۲۶ جولای ۲۰۱۴، و قطعنامه مجمع عمومی {به شماره} ۶۹/۱۶۶ مورخ ۱۸ دسامبر ۲۰۱۴ به رسمیت شناخته شده است؛

۴۳. و در این چارچوب، ما با یادآوری قطعنامه مجمع عمومی به شماره ۶۹/۱۶۶، تأکید می‌نماییم که وفق الزامات کشوری و تحت قوانین بین‌المللی حقوق بشر، حریم خصوصی،

خانوادگی، باید رعایت گردد؛

۴۴. ما مجدداً تعهدات خود در خصوص مفاد مندرج در ماده ۲۹ اعلامیه جهانی حقوق بشر را تأیید می‌نماییم که در آن: هر شخصی در قبال آن جامعه‌ای که رشد آزاد و کامل شخصیت او را میسر می‌سازد و او را از حقوق و آزادی‌ها خود بهره‌مند می‌سازد وظیفه‌ای دارد، {و اینکه} هر شخصی در اجرای حقوق و استفاده از آزادی‌های خود، فقط تابع محدودیت‌هایی است که توسط قانون وضع گردیده است.

۳. اعتمادسازی و امنیت در استفاده از فناوری‌های اطلاعات و ارتباطات

۴۵. ما تأیید می‌نماییم که تقویت اعتماد و امنیت در استفاده از فناوری اطلاعات و ارتباطات برای توسعه جامعه اطلاعاتی و موفقیت در چنین فناوری‌هایی به‌عنوان یک پیشران جهت نوآوری اقتصادی و اجتماعی مطرح می‌باشد؛

۴۶. ما در میان سایر تلاش‌ها در سطوح بین‌المللی، منطقه‌ای و ملی، از تلاش‌های قابل توجه دولت‌ها، بخش خصوصی، جامعه مدنی، جامعه فنی و دانشگاهی جهت اعتمادسازی و ایجاد امنیت در استفاده از فناوری اطلاعات و ارتباطات {که از طریق نهادهای زیر صورت گرفته است} استقبال می‌نماییم. از جمله اتحادیه بین‌المللی مخابرات، کمیسیون پیشگیری از جرم و عدالت کیفری، دفتر مقابله با مواد مخدر و جرم ملل متحد، گروه کارشناسان بین‌دولتی باز برای انجام بررسی جامع مشکلات جرائم سایبری و گروه کارشناسان دولتی درباره تحول در حوزه اطلاعات و مخابرات در چارچوب امنیت ملی؛

۴۷. ما ضمن به رسمیت شناختن، نقش محوری دولت‌ها در موضوعات امنیت سایبری در حوزه امنیت ملی، اهمیت نقش و همکاری تمامی ذی‌نفعان در حیطة مسئولیت‌ها و نقش‌های مرتبط خود را به رسمیت می‌شناسیم. ما مجدداً ضرورت سازگاری و وفاق {موضوعات} اعتمادسازی و امنیت در استفاده از فناوری‌های اطلاعات و ارتباطات، با حقوق بشر را تأیید می‌نماییم؛

۴۸. ما ضمن به رسمیت شناختن اهمیت نقش حقوق بین‌الملل مخصوصاً منشور ملل متحد در {موضوع} اعتمادسازی و امنیت در استفاده از فناوری‌های اطلاعات و ارتباطات توسط دولت‌ها،

از گزارش‌های سال‌های ۲۰۱۳ و ۲۰۱۵ گروه کارشناسان دولتی درباره تحول در حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌الملل استقبال می‌نماییم؛

۴۹. ما در خصوص رشد قطعی در استفاده از فناوری‌های اطلاعات و ارتباطات از جمله فناوری‌هایی با اهداف تروریستی و جرائم سایبری که منافع امنیت و توسعه را به مخاطره می‌اندازند نگرانیم. ما ضمن ابراز ضرورت وجود چارچوب‌های قانونی و اجرایی جهت نگه داشتن حفظ {کنترل} سرعت تغییر فناوریانه و اپلیکیشن‌های آن، توأم با نگرانی به اقدام حملات علیه دولت‌ها، مؤسسات، شرکت‌ها و سایر نهادها و اشخاص از طریق ابزار دیجیتالی توجه می‌نماییم. ما عقیده و باور خود را تکرار می‌نماییم که فرهنگ جهانی امنیت سایبری نیازمند ارتقا و گسترش می‌باشد و اقدامات امنیت سایبری، به‌منظور تقویت اعتماد و امنیت در جامعه اطلاعاتی، باید در قالب همکاری با تمامی ذی‌نفعان و نهادهای کارشناسی بین‌المللی انجام پذیرد؛

۵۰. ما از دولت‌های عضو درخواست می‌نماییم ضمن تشدید تلاش در راستای تقویت امنیت داخلی در {حوزه} فناوری اطلاعات و ارتباطات و استفاده از آن‌ها، وفق تعهدات بین‌المللی و حقوق داخلی خود، در موضوعات فراملی فناوری اطلاعات و ارتباطات و استفاده از آن‌ها نیز همکاری نمایند از جمله در {حوزه‌های} ظرفیت‌سازی و همکاری در مبارزه علیه سوءاستفاده‌های مجرمانه از فناوری‌ها و ممانعت در استفاده از فناوری، ارتباطات و منابع جهت اهداف مجرمانه و تروریستی؛

۵۱. ما ضمن به رسمیت شناختن چالش‌های پیش روی دولت‌ها از جمله کشورهای در حال توسعه در {موضوع} اعتمادسازی و امنیت، استفاده از فناوری‌های اطلاعات و ارتباطات، تمرکز مکرر روی این موضوعات زیر را تقاضا می‌نماییم: ظرفیت‌سازی، آموزش، اشتراک‌گذاری دانش و تمرینات منظم و ارتقای همکاری چند ذی‌نفعی در تمامی سطوح و بالابردن آگاهی میان کاربران فناوری اطلاعات و ارتباطات مخصوصاً فقیرترین و آسیب پذیرترین کاربران؛

۴. حکمرانی اینترنت

۵۲. ما با تأیید مجدد بند ۵۵ دستورکار تونس، در این رابطه ضمن به رسمیت شناختن عملکرد مؤثر ترتیبات موجود بر روی ایجاد اینترنتی بسیار قوی، پویا با بستر جغرافیایی متنوع

{ به شکل امروزی خود}، نوآوری و تولید ارزش در کنار افزایش روز افزون نقش محوری بخش خصوصی را رسمیت می‌شناسیم. به‌رحال تقریباً ۴ میلیارد نفر از جمعیت که تقریباً نماینده دو سوم مردم مقیم در کشورهای در حال توسعه می‌باشند غیربرخط باقی مانده‌اند {به اینترنت دسترسی ندارند}.

۵۳. ما وجود بسیاری از خطوط شکاف در موضوعات سیاست بین‌الملل عمومی را که نیازمند تلاش می‌باشند و به قدر کفایت به آن‌ها پرداخته نشده است را به رسمیت می‌شناسیم؛

۵۴. ما باتوجه‌به بند ۲۹ دستور کار تونس مدیریت اینترنت شامل فرایندهای چندجانبه، شفاف، دموکراتیک و چند ذی‌نفعی با مشارکت کامل دولت‌ها، بخش‌های خصوصی، جامعه مدنی، سازمان‌های بین‌المللی، جوامع فنی و دانشگاهی و سایر ذی‌نفعان مربوط با نقش‌ها و مسئولیت‌های متناسب خود را به‌عنوان یک وسیله {امکان} جهانی به رسمیت می‌شناسیم؛

۵۵. ما تعریف جاری حکمرانی اینترنت را بنا بر بند ۳۴ دستور کار تونس تصریح می‌نماییم: توسعه و کاربرد نقش‌های مربوط، اصول مشترک، هنجارها، قواعد، رویه‌های تصمیم‌سازی و برنامه‌هایی که توسط دولت‌ها، بخش خصوصی و جامعه مدنی به‌منظور شکل‌دهی به تکامل و استفاده از اینترنت صورت می‌گیرد.

۵۶. ما اصول مورد قبول در اعلامیه اصول ژنو را مجدداً تأیید می‌نماییم که در آن مدیریت اینترنت دربرگیرنده توأمان موضوعات سیاست عمومی و فنی می‌باشد و مطابق آنچه در بند ۳۵ دستور کار تونس تنظیم شده است تمامی ذی‌نفعان و سازمان‌های بین‌المللی و بین‌دولتی مربوط با نقش‌ها و مسئولیت‌های متناسب خود باید {در مدیریت اینترنت} درگیر شوند؛

۵۷. ما به نشست چندذینفعی جهانی نت موندیال درباره آینده حکمرانی اینترنت که به میزبانی برزیل در شهر سائوپائولو مورخ ۲۳ و ۲۴ آوریل ۲۰۱۴ برگزار گردید توجه می‌نماییم.

۵۸. ما ضمن به رسمیت شناختن ضرورت ارتقای مشارکت و تعامل بیشتر دولت‌ها، بخش‌های خصوصی، جامعه مدنی، سازمان‌های بین‌المللی، جوامع فنی و دانشگاهی و تمامی ذی‌نفعان مربوط از کشورهای در حال توسعه، خاصه کشورهای آفریقایی، کشورهای کمتر توسعه‌یافته، کشورهای در حال توسعه محصور در خشکی و دولت‌های جزیره‌ای کوچک در حال توسعه و

کشورهایی با درآمد متوسط و نیز کشورهای در شرایط مخاصمه، کشورهای پسا تخاصم (پس از جنگ) و کشورهای متأثر از بلایای طبیعی در مباحث حکمرانی اینترنت، در انتها سازوکارهای تأمین مالی قوی، پایدار، شفاف و داوطلبانه را تقاضا می نماییم؛

۵۹. ما ضمن توجه به روندها مهم تنظیم و تدوین قانون در برخی کشورهای عضو درباره اینترنت باز در چارچوب جامعه اطلاعاتی و محرک های اساسی آن، درخواست می نماییم تا در سطح بین المللی اطلاعات درباره فرصت ها و چالش ها بیشتر به اشتراک گذارده شود؛

۶۰. ما ضمن اذعان به نقش مجمع حکمرانی اینترنت به عنوان بستری چنددلی نفعی برای بحث درباره موضوعات حکمرانی اینترنت، از توصیه های مندرج در گزارش گروه کاری درخصوص اصلاحات مجمع حکمرانی اینترنت درباره کمیسیون علم و فناوری برای توسعه که مجمع عمومی آن را در قطعنامه خود {به شماره} ۶۸/۱۹۸ مورخ ۲۰ دسامبر ۲۰۱۳ مورد توجه قرار داد، حمایت کرده و شتاب در اجرای آن را تقاضا می نماییم. ما وظایف حال حاضر مجمع حکمرانی اینترنت را همانگونه که در بندهای ۷۲ تا ۷۸ دستور کار تونس تنظیم گردیده است به مدت ۱۰ سال دیگر تمدید می کنیم. در طی این مدت مجمع ملزم به تداوم در ارائه پیشرفت در کیفیت های عملکردی و مشارکت ذی نفعان مرتبط از کشورهای در حال توسعه می باشد. ما از کمیسیون درخواست می نماییم تا در گزارش دهی منظم خود، ملاحظات مقتضی را جهت تکمیل توصیه های مندرج در گزارش گروه کاری درخصوص اصلاحات مجمع حکمرانی اینترنت درباره کمیسیون مورد نظر قرار دهد؛

۴.۱. همکاری ارتقای یافته

۶۱. ما بر اجرای ابتکارات مختلف و برخی از پیشرفت های ایجاد شده در رابطه با فرایند «به سوی همکاری های ارتقای یافته» که در بند ۶۹ تا ۷۱ دستور کار تونس به تفصیل آمده است، اذعان داریم.

۶۲. به هر حال، ما ضمن توجه به نظرهای کشورهای عضو درباره فرایند «به سوی اجرای همکاری ارتقای یافته» همان گونه که در دستور کار تونس دیده شده است، تداوم گفتگو و کار بر روی اجرای همکاری های ارتقای یافته را تقاضا می نماییم و از این رو از رئیس کمیسیون علم و

فناوری برای توسعه درخواست می‌نماییم تا از طریق شورای اقتصادی و اجتماعی ملل متحد، کار گروهی را ایجاد نمایند تا ضمن در نظر گرفتن کارهای انجام شده تا امروز در خصوص چگونگی اجرای همکاری ارتقای یافته، همان‌گونه که در دستور کار تونس دیده شده، توصیه‌نامه‌هایی را در این خصوص تهیه نمایند.

۵. پیگیری و بازنگری

۶۳. ما مجدداً تأیید می‌نماییم که جهت پیشرفت اجرای خروجی‌های اجلاس سران درباره جامعه اطلاعاتی، به تداوم تعهدات و اقدامات ذی‌نفعان از جمله دولت‌ها، بخش خصوصی، جامعه مدنی، سازمان‌های بین‌المللی و جوامع فنی و دانشگاهی نیاز خواهیم داشت و بازنگری منظم پیشرفت مجموعه کامل خطوط اقدام جهت دستیابی به نظر اجلاس سران ضروری می‌باشد؛

۶۴. ما از کمیسیون علم و فناوری برای توسعه تقاضا می‌نماییم تا بر تداوم گزارش‌دهی سالانه خود به شورای اقتصادی و اجتماعی، درباره اجرای نتایج اجلاس سران درباره جامعه اطلاعاتی {و} با در نظر گرفتن پیگیری و بازنگری دستور کار توسعه پایدار، اهتمام ورزند. و در این رابطه ضمن تشویق اعضای گروه ملل متحد درباره جامعه اطلاعاتی در خصوص تهیه این گزارش‌ها، از مجمع سیاسی سطح بالا درباره توسعه پایدار دعوت می‌نماییم تا گزارش‌های سالانه کمیسیون علم و فناوری را در راستای توسعه بررسی قرار کنند؛

۶۵. همچون ما از کار گروه ملل متحد درباره جامعه اطلاعاتی تقاضا می‌نماییم مطابق با وظایف {دستور کار} و صلاحیت خود و در هماهنگی با عملکرد کارگزاری‌های تخصصی ملل متحد کار خود را ادامه دهند و از کمیسیون‌های منطقه‌ای جهت تداوم عملکرد خود در اجرای خطوط اقدام اجلاس سران درباره جامعه اطلاعاتی و همکاری در بازنگری آن‌ها، از جمله از طریق بررسی‌های منطقه‌ای، دعوت می‌کنیم؛

۶۶. ما مجمع اجلاس سران درباره جامعه اطلاعاتی را به‌عنوان بستری برای بحث و به اشتراک‌گذاری رویه‌های برتر در خصوص اجرای خروجی‌های اجلاس سران توسط تمامی ذی‌نفعان و {همچنین} ضرورت تداوم برگزاری {این مجمع} به‌صورت سالانه را به رسمیت می‌شناسیم؛

۶۷. ما ضمن اذعان بر اهمیت آمارها و داده‌ها جهت پشتیبانی از فناوری اطلاعات و ارتباطات برای توسعه، داده‌های کیفی بیشتری را برای {این موارد} تقاضا می‌نماییم: حمایت از تصمیم‌سازی‌های مبتنی بر شواهد، استفاده از آمارهای فناوری اطلاعات و ارتباطات در راهبردهای ملی، برای توسعه سرشماری‌ها و برنامه‌های عملکرد آماری منطقه‌ای، تقویت ظرفیت آماری محلی، آموزش هدفمند دولت‌ها و تمامی ذی‌نفعان مرتبط. فعالیت‌های مشارکت در سنجش فناوری اطلاعات و ارتباطات برای توسعه که سهم‌گران‌بهایی را در جمع‌آوری و انتشار داده‌ها دارد باید تداوم داشته باشد.

ما در طی اقدامات مقدماتی برای این بازنگری، {وجود} تعدادی از چالش‌ها و فرصت‌های شناسایی شده، نیازه‌های مشاوره‌های طولانی مدت جهت تعیین پاسخ‌های مناسب و ضرورت رسیدگی به پیشرفت‌های کسب شده در سطح بالاتر و اقدامات بیشتر جهت حرکت به سمت توسعه فناوری‌های اطلاعات و ارتباطات را به رسمیت می‌شناسیم.

بنابراین ما از مجمع عمومی را درخواست می‌نماییم:

برگزاری نشست سطح بالا درباره بازنگری کلی اجرای نتایج اجلاس سران درباره جامعه اطلاعاتی در سال ۲۰۲۵، درگیر کردن نظرها و مشارکت تمامی ذی‌نفعان از جمله در فرایند مقدماتی {بازنگری}،

بررسی پیشرفت نتایج اجلاس سران و شناسایی توأمان حوزه‌های تمرکز پیوسته و چالش‌ها. ما توصیه می‌نماییم که نتایج نشست سطح بالا به‌عنوان یک ورودی در فرایند بازنگری دستورکار توسعه پایدار وارد گردد.

نشست عمومی ۷۹ (۱۶ دسامبر ۲۰۱۵)



شورای اقتصادی اجتماعی (اکوسوک) مبحث شش: سازمان آموزشی علمی فرهنگی سازمان ملل متحد (یونسکو)

بند یک: سند پیش نویس ضوابط اخلاقی برای جامعه اطلاعاتی سال ۲۰۱۱



سازمان آموزشی علمی فرهنگی
ملل متحد (یونسکو)

ترجمه سند

تاریخ انتشار: ۱ فوریه ۲۰۱۱

شماره قطعنامه: IFAP-2011/Bureau.XVIII/4

زبان: انگلیسی

برخی از محورهای سند پیش نویس ضوابط اخلاقی برای جامعه اطلاعاتی^۱ شورای بین دولتی اطلاعات برای تمامی برنامه‌های سازمان یونسکو: ضمن تعهد بر اجرای کامل حقوق بشر و آزادی‌های اساسی اظهار شده در اعلامیه جهانی حقوق بشر و سایر اسناد حقوقی سازمان یافته جهانی؛ با یادآوری مقدمه اساسنامه سازمان یونسکو که درباره نیاز به احترام جهانی بیشتری به عدالت حاکمیت قانون و حقوق بشر و آزادی‌های اساسی برای مردم در سراسر جهان بدون برتری جنسیتی، نژادی، زبانی و مذهبی تأکید دارد؛ ضمن به رسمیت شناختن نقش محوری سازمان یونسکو در:

- ✓ پیشرفت و ارتقای جوامع دانشی مردم محور، فراگیر، توسعه مدار، مورد توافق در فرایند جامعه اطلاعاتی درباره جامعه اطلاعاتی؛
- ✓ احترام به صلح و حمایت از ارزش‌های بنیادین آزادی، تساوی، همبستگی، تاب آوری و مسئولیت مشترک؛

با اذعان به ماهیت چند وجهی جامعه اطلاعاتی، به ویژه در خصوص گستره، دسترس پذیری، ارتقای مصالح عامه مردم، حفاظت از داده‌های شخصی و حریم خصوصی و با اذعان به ضرورت

۱. اصل سند دارای محتویات مفصل تری می‌باشد و باتوجه به اهداف و رسالت پیش روی این کتاب، تنها برخی از محورهای این سند قید گردیده است.

اتخاذ اقدامات مناسب و پیشگیرانه مقرر در قانون جهت مقابله با استفاده زیان بار (سوءاستفاده) از فناوری‌های اطلاعات و ارتباطات مانند افعال غیرقانونی که سبب تحریک نژاد پرستی، تبعیض نژادی و بیگانه‌هراسی می‌شود و همچنین افعال غیرقانونی مرتبط با عدم تاب‌آوری، تنفر، خشونت، تمامی اشکال سوءاستفاده از کودکان، از جمله کودک آزاری و پورنوگرافی کودکان، قاچاق و استثمار انسان؛

با تأکید بر اینکه اصول اخلاقی شامل تمامی ذی‌نفعان جامعه اطلاعاتی، (اعم از شخصی یا جمعی) می‌باشد و اینکه وجود و اجرای این اصول اخلاقی در تمامی سطوح برای مراقبت از تمامی جامعه اطلاعاتی ضروری می‌باشد؛

توافقاتی درباره مجموعه‌ای از ارزش‌ها، حقوق بنیادین و تعهدات مربوط به جامعه اطلاعاتی حاصل گردید. مجموعه‌ای که باید اقدامات را هدایت نماید و توسط اعضای جامعه اطلاعاتی رعایت شود ۱. اینترنت باید به‌عنوان یک خدمت عمومی کلیدی جهت ایجاد جامعه دانشی مردم‌محور، فراگیر و توسعه‌مدار به رسمیت شناخته شود و {همچنین} اینترنت در ارتقای به‌کارگیری و بهره‌مندی جهانی از حقوق بشر و آزادی‌های بنیادین که به رسمیت شناخته شده‌اند باید نقشی تعیین‌کننده داشته باشد.

۲. هر شخصی صرف‌نظر از محل زندگی، جنسیت، وضعیت آموزشی، مذهبی و اجتماعی خود، باید توانایی بهره‌مندی از اینترنت و توانایی اتصال، دسترسی، انتخاب، گفتگو، تولید، ابداع و به اشتراک‌گذاری اطلاعات و دانش از طریق اینترنت را داشته باشد؛

۳. باید دسترسی کم‌هزینه به اینترنت به‌عنوان ابزاری جهت توسعه، پیوستگی اجتماعی و توانمندسازی قابلیت‌های افراد فراهم شده و مشارکت اجتماعی فعال در زندگی عمومی از طریق استفاده از اینترنت و بر مبنای غیرتبعیض‌آمیز مهیا گردد؛

۴. اطلاعات باید به شکل قابل دسترس، قابل وصول، کم‌هزینه، برای تمامی گروه‌های اجتماعی، فرهنگی و زبانی و جنسیتی تهیه گردد، از جمله برای افراد ناتوان فیزیکی و حسی یا شناختی و افرادی که به زبان‌های اقلیت‌ها صحبت می‌نمایند. {و} فناوری‌های اطلاعات و ارتباطات باید جهت کاهش شکاف‌های دیجیتالی و گسترش فناوری و اپلیکیشن‌ها برای تضمین

پوشش تمامی افراد به کار گرفته شود؛

۵. ایجاد محتوای علمی، فرهنگی و آموزشی در شکل دیجیتال و حفاظت، پیشرفت و دسترسی {به آن‌ها} باید تقویت گردد تا جایی که اطمینان حاصل گردد تمامی فرهنگ‌ها می‌توانند خود را در فضای اینترنت اظهار نمایند و در بستر اینترنت به تمامی زبان‌ها از جمله زبان‌های بومی و زبان‌های اقلیت دسترسی دارند؛

۶. دولت‌های عضو و ذی‌نفعان مربوط باید تمامی گام‌های لازم را جهت توسعه اینترنت قابل اعتماد، متضمن امنیت، دارای اعتبار و ثبات خدمات و اپلیکیشن‌های فراگیر و حیاتی اتخاذ نمایند.

۷. سواد رسانه‌ای و اطلاعاتی، پیش‌نیازی اساسی برای دسترسی به اطلاعات، بهره‌مندی حقوق فرهنگی و حق آموزش از طریق فناوری‌های اطلاعات و ارتباطات می‌باشد. برای اینکه گروه‌های کاربر بتوانند اعضای پاسخگوی جامعه اطلاعاتی باشند، داشتن اطمینان از دانش و مهارت‌های آن‌ها جهت انتخاب‌هایی آگاه، شفاف و مبتنی بر رضایت در به کار بردن فناوری‌های اطلاعات و ارتباطات و اینترنت، ضروری می‌باشد؛

۸. هر فردی دارای حق مشارکت و تعامل در فضای اینترنت می‌باشد؛

۹. هر فردی دارای حق حفاظت از داده‌های شخصی و زندگی خصوصی در محیط اینترنت می‌باشد. کاربران باید در مقابل ذخیره‌سازی‌های غیرقانونی، سوءاستفاده یا افشای غیرمجاز داده‌های شخصی و تجاوز به حریم خصوصی‌شان حفاظت گردند؛

۱۰. تمامی ذی‌نفعان باید از طریق مجموعه اقدامات قانونی در زمینه آموزش کاربران از جمله به‌کارگیری مهارت‌های سواد اطلاعات و رسانه، و راه‌حل‌های فنی، جهت مقابله با موارد زیر با همدیگر همکاری نمایند :

✓ سوءاستفاده از فناوری‌های اطلاعات و ارتباطات؛

✓ حفاظت داده‌ها و حریم خصوصی؛

۱۱. دولت‌های عضو باید اقدامات پیشگیرانه و راهبردهای هماهنگی را جهت حصول اطمینان از امنیت اینترنت و حفاظت جامعه در برابر جرائم سایبری از جمله جرائم زیر به‌کارگیرند:

✓ اقداماتی جهت تحریک نژادپرستی، تبعیض نژادی، بیگانه‌هراسی و مانند آن؛

✓ خصومت و دشمنی و خشونت؛

✓ تمامی اشکال سوءاستفاده از کودکان؛

✓ قاچاق و استثمار انسانی.

۱۲. دولت‌های عضو باید استفاده از اینترنت درخصوص موارد زیر را حمایت نمایند:

✓ ارتقای اثربخشی؛

✓ تهیه فرصت‌های همگانی برای مشاوره و مشارکت عمومی؛

✓ ارتقای و تقویت شفافیت، پاسخ‌گویی، مسئولیت‌پذیری، تعاملات، جامعیت، دسترس

پذیری، مشارکت و همبستگی‌های اجتماعی.

۱۳. تمامی اعضای جامعه اطلاعاتی به‌صورت فردی یا جمعی باید جهت توسعه و توزیع

اپلیکیشن‌های جدید برای محیط اینترنت آزاد باشند.

۱۴. مالکیت فکری مربوط به خلاقیت‌ها در محیط دیجیتال باید موضوعی مورد مطالعه باشد

و تحت حقوق مالکیت فکری حفاظت گردد. از کپی و توزیع غیر مجاز اسناد نباید چشم‌پوشی

نمود. کاربرد کنوانسیون‌های بین‌المللی مالکیت فکری باید مبتنی بر تعادل بی‌طرفانه بین منافع

حقوق دارندگان حق و حقوق عمومی باشد.



بخش دوم :
بررسی و ارزیابی



مبحث یک: اقدامات مبتکرانه روسیه در کمیته‌های سه گانه مجمع عمومی

گفتار یک: ارائه اولین قطعنامه امنیت بین‌الملل سایبری در سال ۱۹۹۸

اگر زادگاه و خاستگاه فنی فضای سایبر، ایالات متحده و به طور مشخص، وزارت دفاع این کشور باشد، روسیه را شاید بتوانیم فعال‌ترین کشور در حوزه قاعده‌مند سازی فضای سایبر تلقی کنیم. یعنی همان‌گونه که اینترنت در کشور آمریکا، طراحی و به‌کارگیری شده است، دولت روسیه ابتکار عمل عرصه بین‌المللی سایبر را در ابعاد مختلف آن از جمله امنیت سایبری و جرایم سایبری، به‌دست گرفته است.

در تاریخ ۲۳ سپتامبر ۱۹۹۸، ایگور ایوانف، وزیر دفاع وقت روسیه، طی نامه‌ای از دبیرکل سازمان ملل متحد درخواست کرد که پیش‌نویس یک قطعنامه جدید درباره «تحولات عرصه اطلاعات و ارتباطات در چهارچوب امنیت»^۱ را در مجمع عمومی سازمان ملل تصویب کند.^۲ پیش‌نویس قطعنامه ۱۹۹۸ روسیه به کمیته اول، در قالب قطعنامه ۵۳/۷۰ در ۴ ژانویه ۱۹۹۹ در مجمع عمومی با اجماع و بدون رأی مخالف تصویب شد.^۳ این روند تا سال ۲۰۰۴ به همین شکل ادامه داشت.^۴ قطعنامه ۵۴/۴۹ در ۱۱ دسامبر ۱۹۹۹، قطعنامه ۵۵/۲۸ در ۲۰ نوامبر ۲۰۰۰،

1. Developments in the field of information and telecommunications in the context of international security

2. Anatolij A. Streltsov, International information security: description and legal aspects, United Nations Institute for Disarmament Research (UNIDIR), Geneva 2007.

3. UN General Assembly A/576/53. Consideration of draft resolution A/C.53/1/L.17 and Rev.1

4. UN General Assembly A/558/54. Consideration of draft resolution A/C.54/1/L.4

UN General Assembly A/554/55. Consideration of draft resolution A/C.55/1/L.6

قطعنامه ۵۶/۱۹ در ۲۹ نوامبر ۲۰۰۱، قطعنامه ۵۷/۵۳ در ۲۲ نوامبر ۲۰۰۲، قطعنامه ۵۸/۳۲ در ۸ دسامبر ۲۰۰۳ و قطعنامه ۵۹/۶۱ در ۳ دسامبر ۲۰۰۴ بعد از طی پروسه در کمیته اول، با اجماع در مجمع عمومی تصویب شدند.^۱ تا سال ۲۰۰۴، روسیه تنها بانی و ارائه‌کننده پیش‌نویس قطعنامه بود.^۲ و این قطعنامه‌ها به شیوه اجماع (کنسانسوس) و بدون رأی‌گیری تصویب می‌شد. تعارض منافع ایالات متحده در روند قطعنامه سایبری برای اولین بار در سال ۲۰۰۵ خود را نشان داد. در این سال ما شاهد اتفاق غیرمنتظره‌ای در کمیته اول مجمع عمومی هستیم. پیش‌نویس تقدیمی روسیه، طبق روال سابق در کمیته اول تصویب شد، اما برای اولین بار در تاریخ خود، به رأی گذاشته شد. رأی‌گیری در سال ۲۰۰۵ از طرف آمریکا مورد درخواست واقع شد و آمریکا در ۲۸ اکتبر ۲۰۰۵ به این قطعنامه، رأی منفی داد.^۳ قطعنامه پیشنهادی روسیه^۴، با وجود رأی منفی آمریکا، هم در کمیته اول^۵ و هم در مجمع عمومی (۸ دسامبر ۲۰۰۵) تصویب شد.^۶ برای درک علل رأی منفی آمریکا به این قطعنامه، که در دوره دوم ریاست جمهوری بوش اتفاق افتاد باید گفت: اتحادیه بین‌المللی مخابرات در اجلاس ۲۰۰۵ تونس به حکمرانی چند ذی‌نفعی اینترنت رأی داد و از عملکرد شرکت آی‌کان آمریکایی انتقاد و بر مشارکت بیشتر و جدی‌تر کشورها در امور مربوط به حکمرانی اینترنت تأکید کرد. این امر به هیچ وجه خوشایند آمریکا نبود. بنابراین تقابل بین آی‌کان و اتحادیه بین‌المللی مخابرات به تقابل سایبری بین روسیه و آمریکا انجامید. رأی منفی آمریکا به قطعنامه پیشنهادی روسیه در کمیته اول و مجمع عمومی را می‌توان اولین و فوری‌ترین واکنش آمریکا در قبال شکست در اجلاس تونس تلقی کرد.

این تقابل در سال‌های بعد، ابعاد جدیدی به خود گرفت. بنابراین روسیه در سال ۲۰۰۶ با یارگیری قبلی به میدان آمد. همان‌گونه که ذکر شد تا سال ۲۰۰۵، روسیه تنها بانی قطعنامه پیشنهادی به کمیته اول بود. بعد از رأی منفی آمریکا در سال ۲۰۰۵، قطعنامه پیشنهادی روسیه در سال

1 . resolutions A/RES/ 54/49 of 1 December 1999, A/RES/ 55/28 of 20 November 2000, A/RES/ 56/19 of 29 November 2001, A/RES/ 57/53 of 22 November 2002, A/RES/ 58/32 of 8 December 2003. A/RES/ 59/61 of 3 December 2004

2 . UN General Assembly A/59/454. Consideration of draft resolution A/C.1/59/L.2 and Rev.1

3 . UN General Assembly. A/60/452

4 . UN. General Assembly A/C.1/60/L.29

5 . UN. General Assembly A/60/452

6 . UN General Assembly A/RES/60/45

۲۰۰۶ با حمایت ۱۴ کشور به عنوان هم بانى به کمیته اول ارائه شد.^۱ رأی منفی آمریکا به این قطعنامه در سال‌های ۲۰۰۷ و ۲۰۰۸ نیز ادامه پیدا کرد. به موازات آن، روسیه نیز به تعداد هم بانیان قطعنامه پیشنهادی خود افزود. در سال ۲۰۰۷، تعداد هم بانیان قطعنامه به ۱۷ کشور^۲ و در سال ۲۰۰۸ به ۲۸ کشور^۳ افزایش پیدا کرد. این روند تا روی کار آمدن اوباما در سال ۲۰۰۹ ادامه داشت و مانع تکامل هنجارهای سایبری شد.

به دنبال اتمام دوره دولت بوش و روی کار آمدن اوباما، تاکتیک بازنگری در ارتباط با روسیه و سازمان ملل اعمال شد. بنابراین در سال ۲۰۰۹، پیش نویس قطعنامه روسیه در کمیته اول دوباره به روش اجماع تصویب شد. اما روسیه هر سال بر تعداد هم بانیان قطعنامه افزود. در سال ۲۰۰۹ تعداد ۳۰ کشور از قطعنامه حمایت کردند.^۴ این رقم در سال ۲۰۱۰ به ۳۶ کشور افزایش پیدا کرد.^۵ آمریکا که در سال ۲۰۰۹ با پرهیز از رأی منفی به قطعنامه روسیه، همگرایی نسبی با روسیه را اعلام کرده بود، در سال ۲۰۱۰ یک گام نیز جلوتر نهاد و به جرگه هم بانیان قطعنامه پیشنهادی روسیه پیوست.^۶ اما آمریکا در سال ۲۰۱۱ نام خود را از فهرست هم بانیان قطعنامه خارج کرد^۷ و تا سال ۲۰۱۵ دیگر به عنوان هم بانى به آن فهرست نپیوست و به عدم مخالفت خود به قطعنامه پیشنهادی، اکتفا کرد.^۸

به دنبال خروج ایالات متحده در سال ۲۰۱۱، سایر متحدان آمریکا از جمله، آلمان، استرالیا، کانادا و ژاپن که در سال ۲۰۱۰ که به عنوان هم بانى به این فهرست پیوسته بودند، از آن خارج شدند.^۹ بنابراین تعداد هم بانیان قطعنامه روسیه که در سال ۲۰۱۰ به ۳۶ کشور افزایش پیدا کرده بود، به خاطر خروج آمریکا و متحدانش از این فهرست، در سال ۲۰۱۱ به ۳۳ کشور کاهش یافت.^{۱۰} اما در سال‌های ۲۰۱۲ تا ۲۰۱۴ با وجود حضور نیافتن کشورهای قدرتمند سایبری در قطعنامه روسیه، تعداد هم بانیان آن در سال ۲۰۱۲ به ۳۸ کشور^{۱۱}، در سال ۲۰۱۳ به ۴۱ کشور^{۱۲} و در

1 . UN. General Assembly . A/61/389

2 . UN. General Assembly A/62/386

3 . UN. General Assembly A/63/385.

4 . UN. General Assembly A/64/386:

5 . UN. General Assembly. A/65/405: Armenia, ... Ukraine, the United States of America and Viet Nam, ...

6 . A/65/405 Consideration of draft resolution A/C.1/65/L.37

7 . A/66/407 Consideration of draft resolution A/C.1/66/L.30

8 . A/70/455. Consideration of draft resolution A/C.1/70/L.45

9 . A/66/407. Consideration of draft resolution A/C.1/66/L.30

10 . A/66/407:

11 . A/67/40:

12 . A/68/406:

سال ۲۰۱۴ به ۶۱ کشور^۱ افزایش پیدا کرد.

آمریکا در سال ۲۰۱۵ دوباره به جرگه هم‌بانیان قطعنامه پیوست و به دنبال آن، دیگر هم‌پیمانان آمریکا از جمله انگلیس، فرانسه، آلمان، ژاپن و استرالیا نیز به این فهرست پیوستند. حتی رژیم صهیونیستی نیز که در فهرست هم‌بانیان قطعنامه در سال ۲۰۱۰ غایب بود، در سال ۲۰۱۵ به این فهرست پیوست. به دنبال تغییر رفتار آمریکا، دیگر کشورهای متأثر از رفتار این کشور نیز به هم‌بانیان این قطعنامه پیوستند. به طوری که شمار هم‌بانیان قطعنامه از ۶۱ کشور در سال ۲۰۱۴ به ۸۴ کشور در سال ۲۰۱۵ افزایش پیدا کرد.^۲ در مورد اتفاق سال ۲۰۱۵ باید گفت که آمریکا نگران افزایش تعداد هم‌بانیان قطعنامه پیشنهادی روسیه در خلال سال‌های ۲۰۱۱ تا ۲۰۱۴ بود. آمریکا تصور می‌کرد با خروجش در سال ۲۰۱۱، روسیه نیز در یارگیری شکست خواهد خورد و آن را ادامه نخواهد داد.

حمایت ۶۱ کشور در سال ۲۰۱۴ از قطعنامه روسیه، موجب نگرانی آمریکا گردید. زیرا این خطر وجود داشت که در ادامه ممکن است هنجارهای بین‌المللی حوزه سایبری در غیاب آمریکا شکل گیرد. بنابراین آمریکا تصمیم گرفت با مشارکت در این روند، ملاحظات و منافع خود را بگنجانند. این دلیل زمانی تقویت می‌شود که بدانیم، آمریکا به تنهایی وارد فهرست نشد بلکه با تمام متحدان و حتی متأثران خود به این فهرست پیوست. به طوری که ۲۳ کشور به تعداد هم‌بانیان قطعنامه در سال ۲۰۱۵، افزوده شد. آمدن آمریکا با تمام قدرت به فهرست هم‌بانیان قطعنامه، به این جهت بود که بتواند بیشترین تأثیر را در تدوین و اصلاح قطعنامه پیشنهادی روسیه داشته باشد و اجازه ندهد که روسیه آن را یکسویه و صرفاً در راستای منافع خود، پیش ببرد. اقدامات واکنشی آمریکا به موارد فوق محدود نمی‌شود. آمریکا طی این سال‌ها جهت جلوگیری از اینکه روسیه تنها بازیگر عرصه امنیت سایبری در کمیته اول نباشد، یک سری قطعنامه در سال‌های ۲۰۰۲، ۲۰۰۳، ۲۰۰۹ را تحت عنوان قطعنامه «فرهنگ جهانی امنیت سایبری» در کمیته دوم به جریان انداخت. به عبارت دیگر، قطعنامه‌های کمیته دوم که به پیشنهاد آمریکا تصویب می‌شد باید نوعی توازن با روسیه در اداره جریان امنیت سایبری در سازمان ملل ایجاد می‌کرد که البته چنین نشد. روسیه که اولین

1 . Federation, on behalf of

2 . A/70/455 Consideration of draft resolution A/C.1/70/L.45.

قطعنامه موسوم به امنیت سایبری را در سال ۱۹۹۸ به کمیته اول ارائه نموده بود، توانست این جریان را در کمیته اول نهادینه کند و بنابراین آمریکا امکان بازیگری در این کمیته را از دست داد و سعی کرد با به راه انداختن جریان موسوم به «ایجاد فرهنگ جهانی امنیت سایبری»^۱ در کمیته دوم این عقب ماندگی را جبران نماید.

اقدامات تقابلی آمریکا به کمیته دوم محدود نمی شود. دو سال پس از اینکه فدراسیون روسیه قطعنامه موسوم به قطعنامه امنیت سایبری را به کمیته اول ارائه نمود، کمیته سوم - کمیته اجتماعی، بشر دوستانه و فرهنگی - به عنوان بخشی از کار خود در ارتباط با پیشگیری از جرم و عدالت کیفری، به بحث درباره یک پیش نویس قطعنامه تحت عنوان «مبارزه با سوءاستفاده مجرمانه از فناوری های اطلاعات»^۲ پرداخت. ^۳ پیش نویس این قطعنامه توسط ایالات متحده ارائه گردید و ۳۸ کشور دیگر از جمله فرانسه، رژیم صهیونیستی و انگلستان از آن حمایت کردند. متعاقباً ۱۹ کشور دیگر به هم بانیان این قطعنامه پیوستند. جمهوری خلق چین از این قطعنامه حمایت نکرد.^۴ پیش نویس قطعنامه بدون رأی گیری (آیین کنسانسوس) در تاریخ ۲۲ ژانویه ۲۰۰۱ در مجمع عمومی به تصویب رسید.

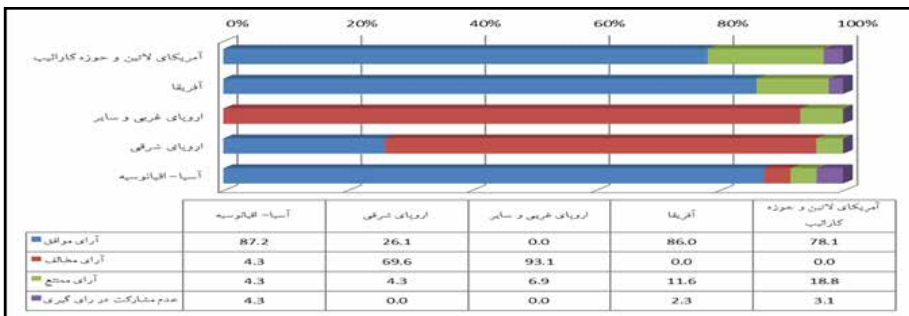
هدف اصلی قطعنامه ۵۵/۶۳ تأسیس یک «مبنای قانونی برای مبارزه با استفاده مجرمانه از فناوری های اطلاعات» عنوان شده است.^۵ این قطعنامه به سابقه این موضوع در سال ۱۹۹۰ اشاره می کند^۶ که هشتمین کنگره سازمان ملل متحد در ارتباط با پیشگیری از جرم و رفتار با مجرمان، قطعنامه ای را در ارتباط با جرائم مرتبط با کامپیوتر تصویب کرد. این قطعنامه همچنین به فعالیت شورای اروپا در ارتباط با تصویب کنوانسیون جرائم سایبری بوداپست اشاره می کند. اگر دوباره به کمیته اول برگردیم باید گفت که آمریکا در سال ۲۰۱۶ دوباره از فهرست هم بانیان قطعنامه روسیه خارج شد. در سال ۲۰۱۷ به جهت شکست گروه کارشناسان دولتی، قطعنامه ای نیز صادر نشد.

در مجموع می توان گفت که از زمان ارائه اولین قطعنامه در حوزه امنیت سایبری در سال ۱۹۹۸

1 . creation of a global culture of cyber-security
2 . Combating the criminal misuse of information technologies
3 . A/55/59, 16 November 2000
4 . UN General Assembly A/55/593
5 . UN General Assembly A/57/529/Add. 3 .
6 . resolution 45/121 of 14 December 1990,

توسط روسیه به مجمع عمومی سازمان ملل و تصویب آن، روند تعامل و تقابل آمریکا با این قطعنامه طی ۲۰ سال گذشته از بُعد راهبردی فقط شامل مهار و مقابله بوده و از بُعد تاکتیکی از رأی منفی گرفته تا حمایت از قطعنامه به عنوان هم بان^۱ را شامل شده است.

سال ۲۰۱۸ نقطه عطفی در روند قطعنامه‌ها در کمیته اول محسوب می شود. در این سال روسیه قطعنامه خود را در که با حمایت ۳۴ کشور به عنوان هم بان^۲ تهیه نموده بود در مجمع عمومی تصویب نمود. اما در این سال آمریکا بعد از ۲۰ سال کارشکنی، توانست رأساً به ارائه قطعنامه ای تحت عنوان «پیشرفت رفتار مسئولانه دولت درباره فضای سایبر در چارچوب امنیت بین‌المللی»^۳ از طرف خود به کمیته اول اقدام نماید. آمریکا در این سال قطعنامه خود را که با حمایت ۵۱ کشور به عنوان هم بان^۴ تهیه نموده بود در مجمع عمومی تصویب نمود. بنابراین در این سال، آرایش موافقان و مخالفان هر دو قطعنامه شکل جدی تری به خود گرفت. در ادامه به بررسی مواضع کشورهای مختلف به دو قطعنامه امنیت سایبری روسیه و آمریکا خواهیم پرداخت.



شکل ۱: توزیع آراء و مواضع کشورها درباره قطعنامه امنیت سایبری روسیه در سال ۲۰۱۸

نتایج:

۱. بیش از ۹۳ درصد از کشورهای اروپای غربی به تبعیت از آمریکا، به قطعنامه پیشنهادی روسیه رأی منفی داده‌اند که حاکی از عدم استقلال سایبری این قاره و پیروی از سیاست‌های سایبری دولت ایالات متحده آمریکاست. می توان نتیجه گرفت که در سایر حوزه‌ها نیز نمی توان از اروپا

1. co- sponsor

2. On 8 November, the representative of the Russian Federation, on behalf of Algeria, ...” (A/C.1/73/L.27/Rev.1). Subsequently, Guinea, Kyrgyzstan and Myanmar joined in sponsoring the draft resolution.

3 . Advancing responsible State behaviour in cyberspace in the context of international security

4. On 18 October, the representative of the United States of America, on behalf of Australia,...” (A/C.1/73/L.37). Subsequently, Albania, ...

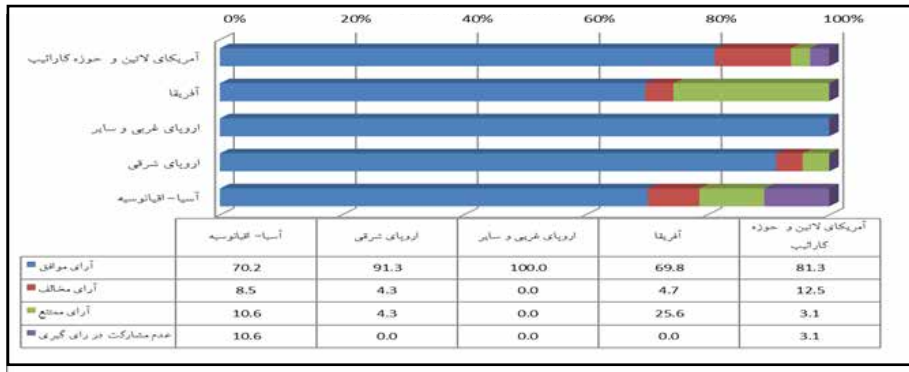
انتظار سیاستی مستقل از امریکا داشت. البته این امر نوعی پاسخ مقابله‌ای به روسیه نیز محسوب می‌شد که در سال ۲۰۱۷ با ارائه پیش‌نویس کنوانسیون جرایم سایبری توانست کنوانسیون بوداپست را با چالش جدی مواجه سازد. (کنوانسیون بوداپست با موضوع جرایم سایبری ریشه در شورای اروپا دارد.) در واقع کل اروپا به استثنای سوئیس و ترکیه (که به این قطعنامه رأی ممتنع داده‌اند.) به قطعنامه روسیه رأی منفی داده‌اند.

۲. در اروپای شرقی که از سمت غرب، ادامه اروپا و از سمت شرق، ادامه روسیه است این یکپارچگی در وابستگی به آمریکا، روند کاهشی دارد. نزدیک ۳۰ درصد از کشورهای این منطقه به قطعنامه روسیه رأی مثبت داده‌اند. کشورهایی مثل بوسنی و هرزگوین، بلاروس، صربستان، ارمنستان و آذربایجان به قطعنامه روسیه رأی مثبت داده‌اند. البته برخی کشورهای این منطقه که تحت نفوذ غرب قرار گرفته‌اند. مثل گرجستان که عضو ناتو شده و تالین (پایتخت استونی) که مقر سایبری ناتو می‌باشد به قطعنامه روسیه رأی منفی داده‌اند.

۳. کشورهای آسیایی و آفریقایی بیشترین میزان موافقت با قطعنامه روسیه را داشته‌اند. این کشورها به صورت سنتی از سال ۲۰۰۶ شروع به حمایت از این قطعنامه کرده‌اند. این حمایت در سال ۲۰۱۸ نزدیک به ۹۰ درصد بوده است. این موضوع زمانی جالب می‌شود که بدانیم در آسیا فقط رژیم صهیونیستی و ژاپن به قطعنامه روسیه رأی منفی داده‌اند. جالب است بدانیم در قاره آفریقا هیچ کشوری به قطعنامه روسیه رأی منفی نداده است و فقط دو کشور بوتسوانا و ساحل عاج رأی ممتنع داده‌اند. کنگو نیز در جلسه نبوده است.

۴. رأی مثبت حدود ۸۰ درصدی قاره آمریکا و حوزه کارائیب به قطعنامه روسیه حاکی از عدم محبوبیت دولت آمریکا در قاره متبوع خودش است که این امر ناشی از مداخلات تاریخی و فعلی آمریکا در کشورهای مختلف این منطقه و انزجار افکار عمومی آن از آمریکاست. همان‌طور که در حال حاضر نیز شاهد دخالت آمریکا در امور داخلی برخی از کشورهای غیرهمسو در این منطقه هستیم. این موضوع زمانی جالب‌تر می‌شود که بدانیم هیچ یک از کشورهای این منطقه به قطعنامه روسیه رأی منفی نداده‌اند و فقط دو کشور مثل برزیل و شیلی و چند کشور ذره‌ای (میکرواستیت) به این قطعنامه رأی ممتنع داده‌اند. کشور ۶۰ هزار نفری مارشال نیز غایب بوده

است! این در حالی است که در همین قاره (آمریکا)، چند کشور مهم مثل بولیوی، ونزوئلا، کوبا و نیکاراگوئه به قطعنامه آمریکا رأی منفی داده‌اند. در مجموع به علت ادامه رقابت و کارشنکنی آمریکا، این کشور در سال ۲۰۱۸ به قطعنامه روسیه رأی منفی داد متحدان آمریکا در اروپای غربی و شرقی و همچنین آسیا (رژیم صهیونیستی اسرائیل و ژاپن) نیز به قطعنامه روسیه رأی منفی دادند.



شکل ۲: توزیع آرا و مواضع کشورها درباره قطعنامه امنیت سایبری آمریکا در سال ۲۰۱۸ بر اساس مناطق جغرافیایی

نتایج

۱. کل اروپای غربی به قطعنامه پیشنهادی آمریکا رأی مثبت داده است. در اروپای شرقی نیز فقط خود روسیه به قطعنامه آمریکا رأی منفی داده و بلاروس هم به این قطعنامه رأی ممتنع داده است.

۲. همان‌گونه که گفته شد: در قاره آمریکا چند کشور مهم مثل بولیوی، ونزوئلا، کوبا و نیکاراگوئه به قطعنامه آمریکا رأی منفی داده‌اند.

۳. در آسیا ۴ کشور شامل جمهوری خلق چین، کره شمالی، ج.ا.ایران و سوریه به قطعنامه آمریکا رأی منفی داده‌اند. انتظار می‌رفت که عراق نیز به این قطعنامه رأی منفی دهد.

۴. در قاره آفریقا دو کشور مصر و زیمبابوه به قطعنامه آمریکا رأی منفی داده‌اند.

بخش دوم: بررسی و ارزیابی ۳۹۳

جدول ۸: خلاصه ای از وضعیت و آمار آرا و مواضع کشورهای مختلف درباره قطعه نامه روسیه و آمریکا در سال ۲۰۱۸

روسیه										
	درصد فراوانی	تعداد	درصد فراوانی	تعداد	درصد فراوانی	تعداد	درصد فراوانی	تعداد	درصد فراوانی	تعداد
	آمریکای لاتین و حوزه کارائیب	آمریکای لاتین و حوزه کارائیب	آفریقا	آفریقا	اروپای غربی و سایر	اروپای غربی و سایر	اروپای شرقی	اروپای شرقی	آسیا - اقیانوسیه	آسیا - اقیانوسیه
آرای موافق	۷۸,۱	۲۵,۰	۸۶,۰	۳۷,۰	۰,۰	۰,۰	۲۶,۱	۶,۰	۸۷,۲	۴۱
آرای مخالف	۰,۰	۰,۰	۰,۰	۰,۰	۹۳,۱	۲۷,۰	۶۹,۶	۱۶,۰	۴,۳	۲
آرای ممتنع	۱۸,۸	۶,۰	۱۱,۶	۵,۰	۶,۹	۲,۰	۴,۳	۱,۰	۴,۳	۲
عدم مشارکت در رای گیری	۳,۱	۱,۰	۲,۳	۱,۰	۰,۰	۰,۰	۰,۰	۰,۰	۴,۳	۲
آمریکا										
	درصد فراوانی	تعداد	درصد فراوانی	تعداد	درصد فراوانی	تعداد	درصد فراوانی	تعداد	درصد فراوانی	تعداد
	آمریکای لاتین و حوزه کارائیب	آمریکای لاتین و حوزه کارائیب	آفریقا	آفریقا	اروپای غربی و سایر	اروپای غربی و سایر	اروپای شرقی	اروپای شرقی	آسیا - اقیانوسیه	آسیا - اقیانوسیه
آرای موافق	۸۱,۳	۲۶,۰	۶۹,۸	۳۰,۰	۱۰۰,۰	۲۹,۰	۹۱,۳	۲۱,۰	۷۰,۲	۳۳
آرای مخالف	۱۲,۵	۴,۰	۴,۷	۲,۰	۰,۰	۰,۰	۴,۳	۱,۰	۸,۵	۴
آرای ممتنع	۳,۱	۱,۰	۲۵,۶	۱۱,۰	۰,۰	۰,۰	۴,۳	۱,۰	۱۰,۶	۵
عدم مشارکت در رای گیری	۳,۱	۱,۰	۰,۰	۰,۰	۰,۰	۰,۰	۰,۰	۰,۰	۱۰,۶	۵

گفتار دو: پیشنهاد تشکیل اولین گروه کارشناسان دولتی (G.G.E) در سال ۲۰۰۱

تشکیل نخستین گروه کارشناسان دولتی^۱ اولین بار در قطعنامه پیشنهادی روسیه، مصوب سال ۲۰۰۱ مجمع عمومی، مورد درخواست واقع شد.^۲ در بند ۴ این قطعنامه، مجمع عمومی از دبیرکل سازمان ملل خواسته است که «تهدیدات بالقوه و بالفعل موجود در فضای امنیت اطلاعات را مورد توجه قرار داده و هر گونه اقدام ممکن در راستای همکاری برای مقابله با این تهدیدات را مورد نظر قرار دهد. دبیرکل برای مطالعه در این خصوص، از کمک گروه کارشناسان دولتی، که در سال ۲۰۰۴ تشکیل خواهد شد، استفاده خواهد کرد...»^۳

تشکیل گروه کارشناسان دولتی که اولین بار در سال ۲۰۰۱ از دبیرکل خواسته شده بود، در قطعنامه‌های سایبری سال ۲۰۰۲ و سال ۲۰۰۳ نیز عیناً مورد درخواست و تأکید قرار گرفت. این گروه در سال ۲۰۰۴ فعالیت خود را شروع کرد و در سال ۲۰۰۵ به خاطر کارشکنی‌های آمریکا با اذعان به شکست، بدون هیچ دستاوردی به کار خود پایان داد.^۴

برای درک علل عدم توفیق نخستین گروه کارشناسان دولتی، که در دوره دوم ریاست جمهوری بوش اتفاق افتاد مجبوریم دوباره به اجلاس تونس در سال ۲۰۰۵ اشاره می‌کنیم. همزمان با تشکیل گروه کارشناسان در سال ۲۰۰۴، در گوشه دیگری از سازمان ملل به نام اتحادیه بین‌المللی ارتباطات راه دور (مخابرات)^۵، موضوع حکمرانی سایبری پیگیری می‌شد. آمریکا در صدد بود تمام فعالیت‌های سایبری سازمان ملل از جمله فعالیت گروه کارشناسان دولتی را به تلافی شکست خود در جریان حکمرانی سایبری (اجلاس تونس در سال ۲۰۰۵)، با شکست مواجه سازد. عملکرد منفی آمریکا در این گروه را می‌توان واکنش آمریکا در قبال شکست در اجلاس ژنو و تونس تلقی کرد. بنابراین اولین گروه کارشناسان دولتی در حوزه سایبر را که به موجب قطعنامه سازمان ملل^۶ در سال ۲۰۰۴ تشکیل شده بود به خاطر کارشکنی آمریکا بی‌هیچ نتیجه‌ای در

1 . group of governmental experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security

2 . UN General Assembly A/RES/56/19. 29 November 2001

3 . A/RES/56/19.paragraph 4. Requests the Secretary-General to consider...group of governmental experts, to be established in 2004...

4 . UN General Assembly A/RES/57/53. 22 November 2002 & A/RES/58/32. 8 December 2003

5 . International Telecommunication Union (ITU)

6 . UN. General Assembly A/RES/58/32

سال ۲۰۰۵ به فعالیت خود خاتمه داد.^۱

قطعهنامه امنیت سایبری سال ۲۰۰۵ مجمع عمومی^۲ بدون اشاره به شکست گروه اول کارشناسان، به راحتی از کنار آن گذشت و از دبیرکل خواست که گروه دوم کارشناسان را در سال ۲۰۰۹ تشکیل دهد.^۳

به باور نویسنده، فاصله زمانی چهارساله (۲۰۰۵ تا ۲۰۰۹) تا تشکیل گروه دوم کارشناسان دولتی، خود اشاره‌ای ضمنی به شکست گروه اول کارشناسان دولتی است. زیرا مجمع عمومی می‌توانست تشکیل گروه دوم کارشناسان را در سال ۲۰۰۶ خواستار شود، اما چنین نکرد. مجمع عمومی برای اینکه گروه دوم کارشناسان به سرنوشت گروه اول دچار نشود، اقدام به اتخاذ سیاست ابن‌الوقتی نمود تا حداقل همگرایی بین بازیگران اصلی این عرصه در این فاصله زمانی فراهم شود.

باتوجه به اینکه، سرنوشت گروه کارشناسان تا حد زیادی به مواضع آمریکا و روسیه بستگی داشت، شاید قطعهنامه سایبری، نیم‌نگاهی هم به نتایج انتخابات آمریکا در سال ۲۰۰۹ داشت و امیدوار بود که جانشین بوش، سیاست تعاملی بهتری با روسیه و جامعه بین‌المللی داشته باشد که البته همین‌طور هم شد.

در سال ۲۰۰۹ با همگرایی نسبی قدرت‌های اصلی سایبری، گروه دوم کارشناسان دولتی، با یک گزارش اجماعی، گام مهمی به سمت جلو بردارد که پیشرفت بزرگی برای این گروه محسوب می‌شود.^۴ تشکیل سومین گروه سایبری در قطعهنامه سایبری ۲۰۱۰ مورد درخواست واقع شد و مجمع عمومی از دبیرکل خواست که سومین گروه کارشناسان دولتی در حوزه امنیت سایبری را در سال ۲۰۱۲ تشکیل دهد. این درخواست در بند ۴ قطعهنامه سایبری سال ۲۰۱۱ نیز مورد تأکید قرار گرفت.^۵ این گروه در سال ۲۰۱۳ گزارش خود را منتشر کرد. مهم‌ترین دستاورد گزارش ۲۰۱۳ گروه کارشناسان دولتی، توافق حول این مهم بود که حقوق بین‌الملل، قابل اعمال بر فضای سایبر می‌باشد.

1 . UN. General Assembly A/60/202

2 . A/RES/60/45, 8 December 2005

3 . [paragraph4. Requests the Secretary-General, with the assistance of a group of governmental experts, to be established in 2009 on ...]

4 . UN. General Assembly. A/65/201

5 . UN General Assembly .A/RES/66/24 .

چهارمین گروه کارشناسان دولتی به موجب قطعنامه ۶۸/۲۴۳ مصوب ۲۷ دسامبر ۲۰۱۳ در سال ۲۰۱۴ تشکیل شد.^۳ تمرکز گزارش چهارمین گروه کارشناسان دولتی، مطالعه روی چگونگی اعمال حقوق بین‌الملل بر فضای سایبر بود. این مهم نیز بعد از آنی حاصل شد که گروه قبلی کارشناسان دولتی، حول این موضوع توافق کردند که حقوق بین‌الملل اصولاً قابل اعمال بر فضای سایبر است. بنابراین مطالعه روی چگونگی اعمال، قدم دوم بود.

پنجمین گروه کارشناسان دولتی در سال ۲۰۱۶ و به موجب قطعنامه سایبری سال ۲۰۱۵ مجمع عمومی، تشکیل شد.^۴ مقرر شد بعد از یک سال گزارش خود را در سال ۲۰۱۷ ارائه نماید. تعداد کشورها عضو گروه نیز به ۲۵ کشور افزایش یافت. گروه همچنین مأموریت داشت در مورد چگونگی اعمال حقوق بین‌الملل بر استفاده دولت‌ها از فناوری اطلاعات و ارتباطات نیز تحقیق نماید. دقیقاً همین موضوع (حقوق بین‌الملل و اعمال آن) نقطه آغازین بحرانی بود که در نهایت به شکست مأموریت گروه انجامید.

مارکوف نماینده آمریکا از شاخه‌های مختلف حقوق بین‌الملل، فقط اصرار بر اعمال ابعاد نظامی آن داشت و با تفسیر موسع از حقوق مخاصمات مسلحانه، سعی در اعمال این حقوق بر فضای سایبر داشت. همان کاری که در سند تالین توسط ناتو به رهبری حقوق دانان آمریکایی انجام شده است. نماینده آمریکا اصرار داشت که حقوق بشر دوستانه، حق دفاع مشروع و اقدامات تلافی جویانه عیناً در فضای سایبر اعمال شود. اما سایر کشورها که از نیات دولت ایالات متحده اطلاع داشتند با این پیشنهادات مخالفت کردند. نماینده کوبا در رأس مخالفین قرار داشت. وی اعلام کرد که این امر به اقدامات تنبیهی یکجانبه از جمله اعمال تحریمها و حتی اقدام نظامی توسط دولتهایی که مدعی قربانی سوءاستفاده از فناوری‌های اطلاعاتی و ارتباطی شده اند مشروعیت می‌بخشید. در عوض، گروه بر حل مسالمت‌آمیز اختلافات و پیشگیری از درگیری تأکید داشت. هر چند فقط بیانیه کوبا در مخالفت با مواضع آمریکا در دسترس عموم است، اما قطعاً روسیه و چین نیز چنین نظرهای داشته و از آن حمایت کرده و این نظر را در بین اعضای گروه ترویج کرده اند. چرا که اعلام این نظرها از سوی دو کشور اخیر نیز مسبوق

1 . UN Doc. A/70/174, 22 July 2015p.5.

2 . UN Doc. A/RES/70/237, 23 December 2015

به سابقه است.^۱ گفته شده است که مفاد ماده ۳۴ پیش نویس نیز مورد اختلاف بوده است. در این ماده اعمال منشور ملل متحد بر فضای سایبر باید مورد تأیید قرار می گرفت. از جمله مفاد منشور که مورد اختلاف واقع شد همان مباحث مربوط به استفاده از زور و حقوق بشر دوستانه بین‌المللی بود. مخالفین استدلال می کردند که به رسمیت شناختن این مفاد موجب نظامی شدن هر چه بیشتر فضای سایبر می شود.^۲ کوبا اعلام کرد که مخالف هم تراز قرار گرفتن و تلقی یکسان درباره استفاده غیرقانونی از فضای سایبری با مفهوم حمله سایبری است. البته محافل غربی در توجیه سیاست‌های آمریکا مدعی شده اند که علت مخالفت کوبا این است که نمی خواهد از مزایای نسبی نامتقارن بودن^۳ فضای سایبر محروم شود. زیرا اگر قرار باشد جواب حمله سایبری با سلاح های متعارف داده شود، نتیجه تقابل کشوری مثل کوبا با ایالات متحد آمریکا مشخص است. بنابراین در خصوص برتری در سلاح های متعارف^۴ کشوری مثل کوبا هیچ گونه مزیتی ندارد. البته اینجا باید دو وضعیت مختلف را از هم جدا کرد. مخالفت کوبا با حمله ای (سایبری) نیست که به آستانه حمله متعارف رسیده است. در اینجا حق دفاع مشروع وفق ماده ۵۱ منشور، محرز است.^۵ محل بحث درحالی است که حمله سایبری به آستانه حمله متعارف نرسیده است.^۶ بنابراین نمی توان از سلاح های متعارف به عنوان دفاع مشروع استفاده کرد.

به نظر می رسد شکست مأموریت پنجمین گروه کارشناسان دولتی از شکست گروه اول نیز سنگین تر است. زیرا شکاف در پنجمین گروه کارشناسان دولتی به حدی بود که این گروه اساساً نتوانست به شکل سابق به فعالیت خود ادامه دهد و سال بعد دچار دو دستگی شد.^۷ یعنی از سال ۲۰۱۹ عملاً گروه کارشناسان دولتی و گروه کاری باز به موازات هم تشکیل شدند. تشکیل گروه کارشناسان دولتی که تا کنون ریشه در قطعنامه پیشنهادی روسیه داشت^۸ برای اولین بار در

1 . <https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/> UN GGE on Cybersecurity: The End of an Era? By Elaine Korzak July 31, 2017

2 . <https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well>

3 . asymmetric advantages

4 . conventional superiority

5 . in response to cyber operations that meet the threshold of an "armed attack" under Article 51 of the UN Charter

6 . in scenarios that fell below the threshold of the 'use of force' in cyberspace,

7 . For lack of consensus, the GGE will not submit a report of its recommendations to the UN General Assembly. <https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well>. By Arun M. Sukumar

Tuesday, July 4, 2017, 1:51 PM

۸ . روسیه برای اولین بار تشکیل گروه کارشناسان دولتی را در ماده ۴ قطعنامه سال ۲۰۰۱ به شماره A/RES/۵۶/۱۹ عنوان نمود که این بند در قطعنامه سال‌های بعد روسیه نیز تکرار گردید.

قطعه‌نامه پیشنهادی آمریکا مورد مطالبه واقع شد و تشکیل گروه کاری باز در قطعه‌نامه پیشنهادی روسیه مورد تقاضا واقع شد. بنابراین تشکیل ششمین گروه کارشناسان دولتی^۱ درباره پیشرفت رفتار مسئولانه دولت درباره فضای سایبر در چارچوب امنیت بین‌المللی سال ۲۰۱۹ از سری رویدادی مهم در این روند محسوب می‌شود.

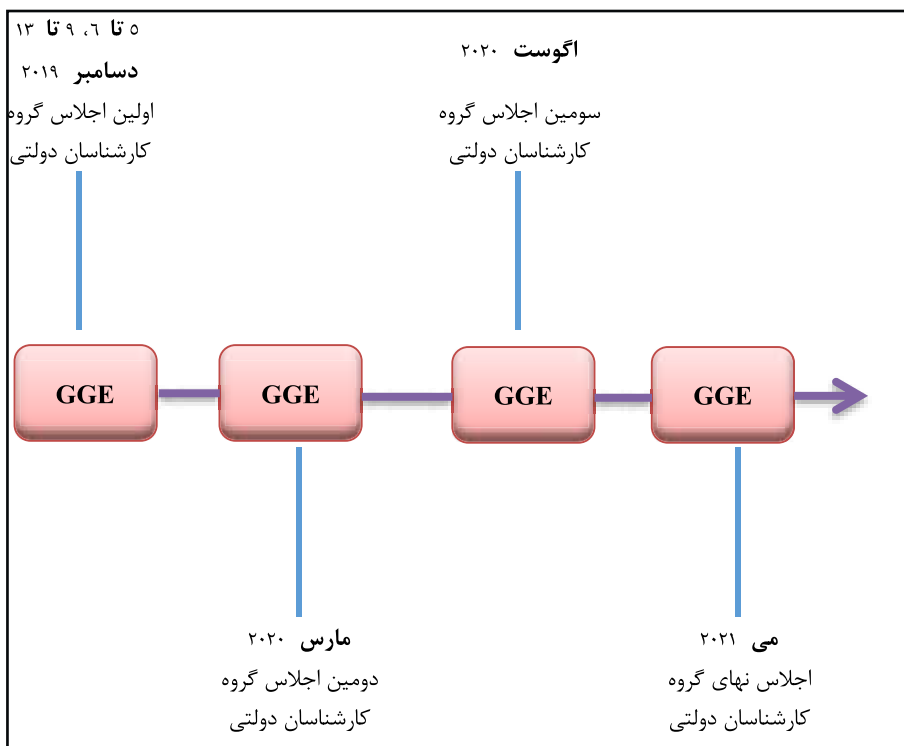
جدول ۹: خلاصه عملکرد تشکیل ۵ گروه کارشناسان دولتی (GGE)

تاریخ صدور و شماره قطعه‌نامه	شماره سند گزارش	تعداد اعضا	تاریخ تشکیل گروه کارشناسان دولتی	نتایج عمده
قطعه‌نامه سال ۲۰۰۳ به شماره A/RES/58/32	A/60/202	۱۵ نفر	تشکیل گروه کارشناسان دولتی در سال ۲۰۰۴، ارائه گزارش سال ۲۰۰۵	شکست گروه کارشناسان دولتی
قطعه‌نامه سال ۲۰۰۵ به شماره A/RES/60/45	A/65/201	۱۵ نفر	تشکیل گروه کارشناسان دولتی در سال ۲۰۰۹ و ارائه گزارش در سال ۲۰۱۰	توافق حول تهدیدات بالفعل و بالقوه در حوزه امنیت اطلاعات به‌عنوان یکی از جدیدترین چالش‌های قرن بیست و یکم
قطعه‌نامه سال ۲۰۱۱ به شماره A/RES/66/24	A/68/98	۱۵ نفر	تشکیل گروه کارشناسان دولتی در سال ۲۰۱۲ و ارائه گزارش در سال ۲۰۱۳	توافق حول این نکته اساسی که حقوق بین‌الملل مخصوصاً منشور ملل متحد قابل اعمال بر فضای سایبری است
قطعه‌نامه سال ۲۰۱۳ به شماره A/RES/68/243	A/70/174	۲۰ نفر	تشکیل گروه کارشناسان دولتی در سال ۲۰۱۴ و ارائه گزارش در سال ۲۰۱۵	مسئولیت دولت‌ها در نظارت بر استفاده از فناوری اطلاعات و ارتباطات
قطعه‌نامه سال ۲۰۱۵ به شماره A/RES/70/237	A/72/327	۲۵ نفر	تشکیل گروه کارشناسان دولتی در سال ۲۰۱۶ و ارائه گزارش در سال ۲۰۱۷	شکست گروه کارشناسان دولتی

ماده سه قطعه‌نامه آمریکا بر ادامه روند تشکیل گروه کارشناسان دولتی تأکید نموده است^۲ و خطوط زمانی ترسیم شده برای تشکیل این گروه، در طی دو سال چهار نشست برگزار خواهد شد که اولین نشست آن در سال ۲۰۱۹ در تاریخ ۵ تا ۶ و ۹ تا ۱۳ دسامبر خواهد بود و پس از پایان دو سال گزارش نهایی آن در می ۲۰۲۱ ارائه می‌گردد.

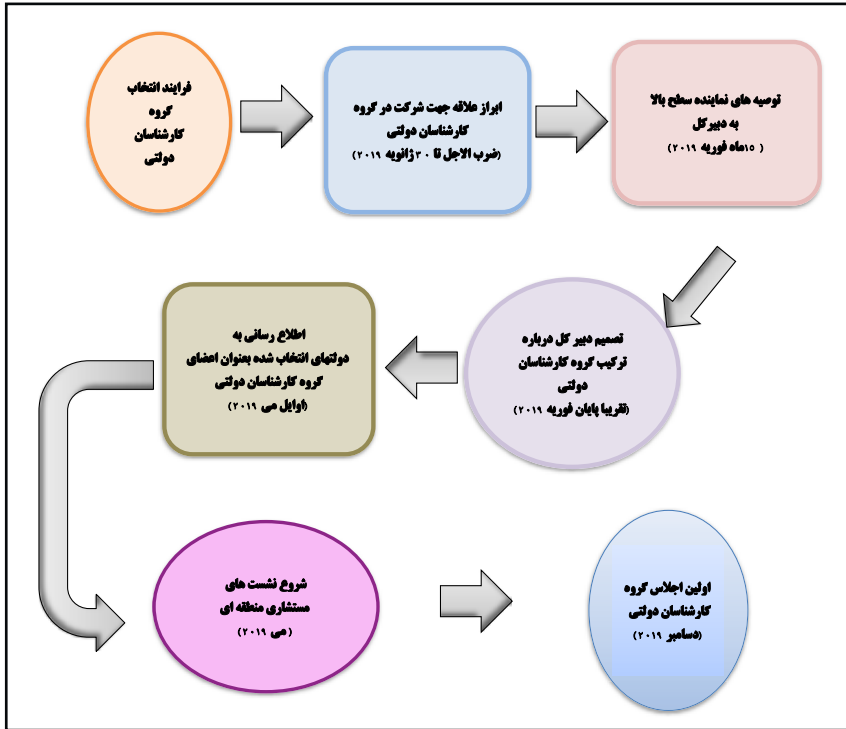
۱. انتشار گزارش در سال ۲۰۲۱.

۲. از دبیرکل درخواست می‌نماید، که با مساعدت گروه کارشناسان دولتی که در سال ۲۰۱۹ و بر مبنای توزیع جغرافیایی عادلانه تشکیل می‌گردد، ضمن اجرا و پیشبرد ارزیابی‌ها و توصیه‌های مندرج در گزارش‌های فوق‌الذکر، با نگاهی به ارتقای درک عمومی و اجرای مؤثر به بررسی (مقولات ذیل) ادامه دهند: اقدامات همکاری‌جویانه احتمالی جهت مقابله با تهدیدات موجود و بالقوه در حوزه امنیت اطلاعات از جمله هنجارها، قوانین و اصول رفتار مسئولانه دولت‌ها، اقدامات اطمینان‌ساز و ظرفیت‌ساز و نحوه اعمال حقوق بین‌الملل در استفاده از فناوری‌های اطلاعات و ارتباطات توسط دولت‌ها، (و در نهایت) در اجلاس هفتاد و ششم مجمع عمومی، گزارشی از نتایج این بررسی‌ها را به انضمام ضمیمه‌ای شامل مشارکت‌های ملی کارشناسان دولتی شرکت‌کننده درباره نحوه اعمال حقوق بین‌الملل در استفاده از فناوری اطلاعات و ارتباطات ارائه نمایند؛



شکل ۳: روند شکل‌گیری گروه کارشناسان دولتی (GGE)

روند شکل‌گیری این گروه نیز مانند سایر گروه‌های کارشناسان دولت می‌باشد شکل بالا توصیف نسبتاً کاملی از زمان بندی فرایند انتخاب گروه کارشناسان و تشکیل اولین اجلاس گروه کارشناسان دولتی را ارائه می‌دهد.



شکل ۴: فرایند انتخاب گروه کارشناسان و تشکیل دومین اجلاس (GGE)

بخش دوم : بررسی و ارزیابی ۴۰۱

جدول ۱۰: شرکت کشورها در گروه‌های کارشناسان دولتی (GGE)

کشور	اولین گروه کارشناسان دولتی ۲۰۰۵	دومین گروه کارشناسان دولتی ۲۰۱۰	سومین گروه کارشناسان دولتی ۲۰۱۳	چهارمین گروه کارشناسان دولتی ۲۰۱۵	پنجمین گروه کارشناسان دولتی ۲۰۱۷	ششمین گروه کارشناسان دولتی ۲۰۲۱-۲۰۱۹
اردن						
اروگوئه						
اسپانیا						
استرالیا						
استونی						
اندونزی						
انگلستان						
ایتالیا						
آرژانتین						
آفریقای جنوبی						
آلمان						
آمریکا						
برزیل						
بلاروس						
بوتسوانا						
پاکستان						
چین						
رژیم صهیونیستی						
روسیه						
رومانی						
ژاپن						
سنگاپور						



گروه کشور	اولین گروه کارشناسان دولتی ۲۰۰۵	دومین گروه کارشناسان دولتی ۲۰۱۰	سومین گروه کارشناسان دولتی ۲۰۱۳	چهارمین گروه کارشناسان دولتی ۲۰۱۵	پنجمین گروه کارشناسان دولتی ۲۰۱۷	ششمین گروه کارشناسان دولتی ۲۰۲۱-۲۰۱۹
سنگال						
سوئیس						
صربستان						
غنا						
فرانسه						
فنلاند						
قزاقستان						
قطر						
کانادا						
کره جنوبی						
کلمبیا						
کنیا						
کوبا						
مالزی						
مالی						
مراکش						
مصر						
مکزیک						
موریتانی						
نروژ						
هلند						
هند						

گفتار سه: پیشنهاد تشکیل اولین گروه کاری باز (O.E.W.G) در سال ۲۰۱۹

پس از شکست گروه کارشناسان دولتی در سال ۲۰۱۷، روسیه در سال ۲۰۱۸ قطعنامه «تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌الملل» را از طریق کمیته اول، به مجمع عمومی سازمان ملل ارائه نمود. در این قطعنامه نیز روسیه ضمن تأیید گزارش گروه کارشناسان دولتی در سال ۲۰۱۵، پیشنهاد جدیدی را مبنی بر تشکیل گروه کاری با علامت اختصاری^۱ OEWG - در ماده ۵ - مطرح کرد^۲ روسیه در این ماده خواهان تشکیل گروه کاری بازی بود که در راستای ادامه توسعه بیشتر قواعد، هنجارها و اصول رفتار مسئولانه دولت‌ها زیر مفاد سیزده گانه که در بند ۱ همین قطعنامه به آن‌ها اشاره گردیده است، گام بردارد و شیوه رأی‌گیری در جلسات آن به شکل اجماع صورت پذیرد؛

➤ حفظ امنیت و صلح بین‌المللی؛

➤ تعهد بین‌المللی دولت‌ها در ارتباط با اقدامات غیرقانونی خود؛

➤ جلوگیری دولت‌ها از اجازه آگاهانه جهت استفاده از سرزمین‌شان جهت اقدامات بین‌المللی غیرقانونی؛

➤ همکاری بهتر دولت‌ها به منظور تبادل اطلاعات و کمک به یکدیگر؛

➤ تضمین استفاده ایمن از فناوری اطلاعات و ارتباطات؛

➤ جلوگیری از همکاری آگاهانه در خسارت به زیرساخت‌های حیاتی جهت مختل نمودن ارائه خدمات به عموم از طریق فعالیت‌های فناوری اطلاعات و ارتباطات؛

➤ اقدامات مناسب جهت حفاظت از زیرساخت‌های حیاتی خود در برابر تهدیدات فناوری اطلاعات و ارتباطات؛

➤ پاسخ به کمک و درخواست مقتضی دولت‌های دیگر که زیرساخت‌های حیاتی آن‌ها در معرض اقدامات مخرب فناوری اطلاعات و ارتباطات قرار دارد؛

➤ تضمین تمامیت زنجیره تأمین جهت اطمینان کاربران نهایی از امنیت محصولات فناوری اطلاعات و ارتباطات؛

1. Open - ended Working Group

2. an open-ended working group acting on a consensus basis, to continue, as a priority, to further develop the rules, norms and principles of responsible behaviour of States listed in paragraph 1 above, and the ways for their implementation;

➤ پیشگیری از اشاعه ابزار و فناوری‌های مخرب؛

➤ گزارش‌دهی مسئولانه آسیب‌پذیری‌های فناوری اطلاعات و ارتباطات؛

➤ ممانعت از انجام و حمایت از فعالیت‌های آگاهانه جهت آسیب به سیستم اطلاعاتی تیم‌های مجاز پاسخ سریع کشورهای دیگر،

➤ تشویق بخش خصوصی و جامعه مدنی در ایفای نقش مناسب در بهبود امنیت و استفاده از فناوری اطلاعات و ارتباطات.

به دلیل عدم محدودیت در تعداد شرکت‌کنندگان در این گروه کاری و عدم محدودیت زمانی آن، روسیه با پیشنهاد تشکیل این گروه، سعی کرد مشارکت گسترده‌تر و دمکراتیک‌تر ذی‌نفعان فراهم آورد.

به علت محدودیت تعداد کشورها در گروه کارشناسان دولتی و همچنین باوجود سازوکارهای انتخاب کشورهای عضو این گروه بر اساس توزیع عادلانه جغرافیایی توسط دبیرکل، در عمل کشورها شاهد عدم برقراری عدالت در این انتخاب می‌باشند: بنابراین گروه کاری باز که به موازات گروه کارشناسان دولتی تشکیل شد موقعیت خوبی جهت گردهمایی تمامی کشورها و رایزنی بین کشورها درباره مسائل مختلف حوزه سایبری خواهد بود.

یکی دیگر از مزایای تشکیل گروه کاری باز، شیوه تصمیم‌گیری در آن می‌باشد که مبتنی بر اجماع در نظر گرفته شده است. این امر نیز می‌تواند به جلوگیری از تصمیم‌گیری‌های مغرضانه توسط برخی کشورهای صاحب قدرت در حوزه سایبری کمک شایانی نماید. هر چند تحقق اجماع بین‌المللی در موضوعات مختلف نیز امری صعب و مشکل است.

نکته حائز اهمیت دیگر در قطعنامه روسیه، ایجاد فرصت و بهره‌مندی از نظرهای بخش صنعت، سازمان‌های مردم‌نهاد و دانشگاهی از طریق تشکیل نشست‌های مشورتی در فاصله زمانی بین اجلاس‌ها می‌باشد این در حالی است که آمریکا در قطعنامه خود تنها به نشست‌های مستشاری منطقه‌ای از جمله نشست‌هایی با اتحادیه آفریقا، اتحادیه اروپا، سازمان دولت‌های آمریکایی، سازمان امنیت و همکاری اروپا و مجمع منطقه‌ای جنوب شرق آسیا (آس‌آن)^۱، و

1. Requests the Office for Disarmament Affairs of the Secretariat, through existing resources and voluntary contributions, on behalf of the members of the group of governmental experts, to collaborate with relevant regional organizations, such as the African Union, the European Union, the Organization of American States, the Organization for Security and Cooperation in Europe and the Regional Forum of the Association of Southeast Asian Nations, to convene a series of consultations to share views on the issues within the mandate of the group in advance of its sessions;

بخش دوم: بررسی و ارزیابی ۴۰۵

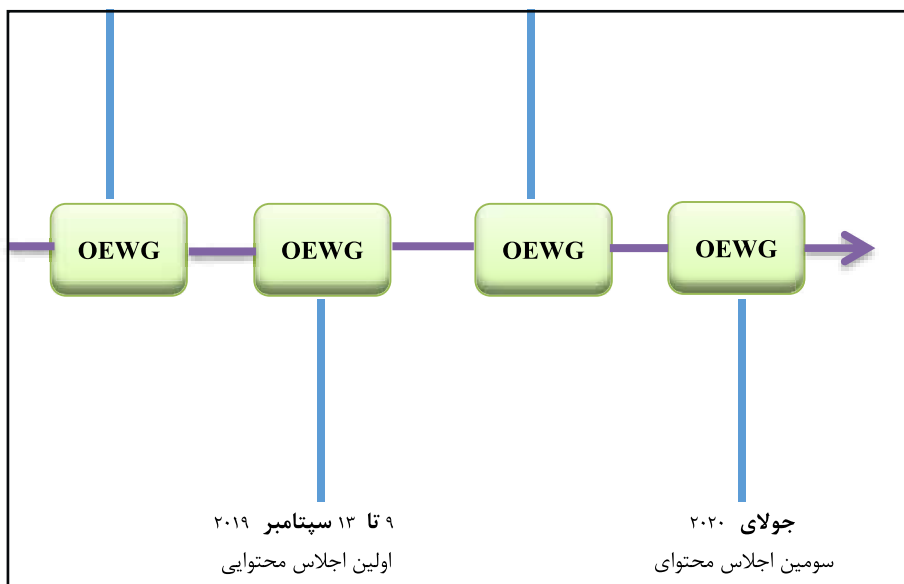
همچنین نشست‌های مستشاری با تمامی دولت‌های عضو سازمان ملل متحد اشاره نموده است. خطوط زمانی تشکیل اجلاس‌های مختلف گروه کاری باز (۲۰۱۹ تا ۲۰۲۱) در شکل زیر به خوبی مشهود می‌باشد.

۳ تا ۴ ژوئن ۲۰۱۹

نشست سازمانی

۱۰ تا ۱۴ فوریه ۲۰۲۰

دومین اجلاس محتوایی



شکل ۵: فرایند شکل‌گیری اولین گروه کاری باز (O.E.W.G)

طبق شکل فوق و پیرو تصویب قطعنامه روسیه، مجمع عمومی در تاریخ ۲۲ می ۲۰۱۹ در سند شماره A/AC.290/2019/1، دستور کار مربوط به این گروه کاری را ابلاغ نمود و نشست سازمانی آن در سوم تا چهارم ژوئن سال ۲۰۱۹ در نیویورک برگزار گردید. در این نشست کشور سوئیس به‌عنوان رئیس این گروه کاری انتخاب گردید. بندهای سوم، چهارم و پنجم این دستور کار به تمامی دولت‌های عضو اجازه ارائه نظرها و پیشنهادهای خود و همچنین تبادل نظرهای عمومی در زمینه موضوعات محتوایی مربوط به فضای سایبر را می‌دهد.

گفتار چهار: ارائه اولین کردارنامه امنیت بین الملل سایبری در سال ۲۰۱۱

اقدام دیگر روسیه در حوزه امنیت سایبری، تدوین و ارائه پیش نویس « کردارنامه بین المللی امنیت اطلاعات»^۱ است. این پیش نویس با نامه مشترک روسیه، چین، ازبکستان و تاجیکستان به دبیرکل سازمان ملل ارسال شد که به عنوان سند سازمان در سال ۲۰۱۱ منتشر گردید.^۲ گفته می شود این کردارنامه، بیشتر با تشریح مساعی چین در سازمان همکاری شانگهای تهیه و تدوین گردیده بود.^۳

در سال ۲۰۱۵، روسیه اقدام به بازنگری و به روزرسانی کردارنامه بین المللی امنیت اطلاعات نمود و به مجمع عمومی سازمان ملل ارائه کرد^۴ و بر هم بانیان آن نیز افزوده شد. قرقیزستان و قزاقستان به فهرست حمایت کنندگان از پیش نویس، اضافه شدند.^۵ این سند، حمایت چین را نیز پشت سر خود دارد و از جایگاهی مثل سازمان شانگهای برخاسته است. نسخه اصلاحی کردارنامه بین المللی امنیت اطلاعات^۶ مربوط به سال ۲۰۱۵ و در ۶ صفحه تنظیم شده است.

1 . International code of conduct for information security.

2 . A/66/359. Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary General

3. Tim Maurer . Cybersecurity in a Complex Environment.2/2016. p.7.

4. A/69/723 .13 January 2015

5 A/69/723. Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General

6 A/69/723, 13 January 2015

گفتار پنجم: ارائه پیش‌نویس اولین کنوانسیون امنیت بین‌الملل سایبری در سال ۲۰۱۱

بعد از قطعنامه و کردارنامه امنیت سایبری، ابتکار دیگر روسیه در حوزه فضای سایبر، ارائه پیش‌نویس کنوانسیون امنیت بین‌المللی اطلاعات است. روسیه پس از یک دهه فعالیت در زمینه امنیت سایبری، به جهان اعلام کرد که منتظر یک معاهده در زمینه امنیت سایبری باشند. این پیش‌نویس با عنوان «کنوانسیون امنیت بین‌المللی اطلاعات»^۱ در اجلاس یکاترین‌بورگ (اکاترینبورگ یا ایکاترینبورگ)^۲ روسیه رونمایی شد.^۳

طی دو روز در ۲۱ و ۲۲ سپتامبر ۲۰۱۱^۴ (۲۹ و ۳۰ شهریور ۱۳۹۰) یکاترین‌بورگ روسیه در منطقه اورال، میزبان دبیران شورای امنیت، معاونان رئیس‌جمهور، نخست‌وزیران و مدیران نهادهای اجرای قانون بیش از ۶۰ کشور جهان از جمله ایران و همین‌طور نمایندگان از سازمان ملل بود. این کنفرانس دومین کنفرانس امنیتی در سطح بین‌المللی بود که به ابتکار روسیه و با هدف بسط و گسترش همکاری‌های چندجانبه در زمینه مبارزه با چالش‌ها و تهدیدات جهانی از جمله تهدیدات سایبری برگزار شد.^۵ اقدام روسیه در ارائه کنوانسیون سایبری، باعث تعجب و حتی شک و تردید آمریکا گردید. بنابراین غرب به‌ویژه آمریکا از این کنوانسیون حمایت نکرد.

1. Convention On International Information Security

2. Ekaterinburg

3. International Meeting Of High-Ranking Officials Responsible For Security Matters (Concept)

4. EKATERINBURG, RUSSIA, 21-22 SEPTEMBER 2011

۵. اولین کنفرانس بین‌المللی امنیتی از این دست در اکتبر سال ۲۰۱۰ (۱۳۸۹) در شهر سوچی روسیه، با دعوت از نمایندگان نهادهای امنیتی ۴۰ کشور برگزار شد، با این تفاوت که در کنفرانس ۲۰۱۰ از نماینده جمهوری اسلامی ایران دعوت به عمل نیامده بود و بسیاری از کارشناسان این عدم حضور ایران را نشانه‌ای مبنی بر فاصله گرفتن روسیه از ایران می‌دانستند. سال ۲۰۱۰ دقیقاً همان سالی است که آمریکا به هم‌پاتیان قطعنامه روسیه در کمیته اول پیوست.

گفتار شش: ارائه اولین پیش‌نویس کنوانسیون مقابله با جرایم سایبری در سال ۲۰۱۷

ارائه «پیش‌نویس کنوانسیون ملل متحد برای همکاری در مبارزه با جرایم سایبری»^۱ از جانب روسیه^۲ در سال ۲۰۱۷، اقدامی مهم برای مقابله با جرایم سایبری محسوب می‌شود. این کشور مدعی است که کنوانسیون جدید این ویژگی را دارد که استقلال کشورها را مورد تهدید قرار ندهد. وزارت خارجه روسیه این پیش‌نویس را آماده و ارائه کرده است. این پیش‌نویس به کارشناسان سازمان ملل در وین اتریش ارائه شده است. مسکو این پیش‌نویس جدید را به‌عنوان یک جایگزین ضروری برای کنوانسیون بوداپست می‌داند.

کنوانسیون جرایم سایبری^۳ موسوم به کنوانسیون بوداپست^۴، یک کنوانسیون بین‌دولتی خارج از سازمان ملل است که در چارچوب شورای اروپا^۵، تدوین، امضاء، تصویب و اجرا شده است. این کنوانسیون در سال ۲۰۰۱ در بوداپست، پایتخت مجارستان بین اعضای شورای اروپا امضاء شد و در سال ۲۰۰۴ اجرایی شد.^۶

کنوانسیون بوداپست، نخستین معاهده الزام‌آور بین‌المللی (خارج از سازمان ملل) در زمینه مقابله با جرایم کامپیوتری و اینترنتی است.

روسیه تنها عضو شورای اروپاست که کنوانسیون بوداپست را امضاء نکرده است و اقدام غافلگیرکننده روسیه در ارتباط با این کنوانسیون در سال ۲۰۱۷ نیز از همین جانشی می‌شود. روس‌ها مدعی هستند که به خاطر ماده ۳۲ مندرج در این کنوانسیون، از امضای آن خودداری می‌کنند. ماده ۳۲ کنوانسیون بوداپست اشعار می‌دارد:

«هر عضو می‌تواند بدون اخذ مجوز از اعضای دیگر و صرف نظر از موقعیت جغرافیایی، با مراجعه به منابع عمومی در دسترس (منبع باز^۱) به داده‌های ذخیره شده دست یابد.»

این ماده به سرویس‌های ویژه کشورهای خارجی، این اجازه را می‌دهد که در حین رسیدگی به جرایم سایبری، به داده‌های ذخیره شده در کامپیوترهای مورد نظر، دسترسی فرا سرزمینی داشته باشند. مقامات روس بر این باورند که اعطای چنین اختیارات گسترده‌ای به سرویس‌های

1. Draft United Nations Convention on Cooperation in Combating Cybercrime

2. A/C.3/72/12. 16 October 2017

3. convention on cybercrime

4. Budapest

5. council of Europe

۶. خود شورای اروپا در سال ۱۹۴۹ ایجاد شد و روسیه در سال ۱۹۹۶ به آن ملحق شد.

ویژه خارجی می‌تواند موجب تضعیف امنیت و حاکمیت ملی و استقلال کشورها شود. پیش‌نویس کنوانسیون پیشنهادی روسیه تحت عنوان «پیش‌نویس کنوانسیون سازمان ملل راجع به همکاری در زمینه مقابله با جرایم اطلاعاتی» {جرایم مرتبط با فناوری اطلاعات و ارتباطات} شامل یک مقدمه، ۶ فصل و یک ضمیمه (غیر از ضمیمه فنی) می‌باشد. در مجموع این پیش‌نویس دارای ۷۲ ماده می‌باشد.

در مقدمه پیش‌نویس کنوانسیون آمده است:

«دولت‌های عضو این کنوانسیون، (که پس از این دولت‌های عضو نامیده خواهند شد)، نگران مسائل و تهدیدات جدی ناشی از جرایم تحمیلی به فضای فناوری اطلاعات و ارتباطات (که پس از این ICT نامیده خواهد شد) هستند که متوجه ثبات و امنیت جامعه هستند، موجب تضعیف نهادها و ارزش‌های دمکراتیک، ارزش‌های اخلاقی و عدالت می‌شوند و موجبات شکست توسعه پایدار و همچنین زوال حاکمیت قانون را فراهم می‌آورند.

همچنین نگرانی درباره اینکه سوءاستفاده مجرمانه از فناوری اطلاعات و ارتباطات، فرصت‌های گسترده‌ای را برای انجام اشکال دیگری از فعالیت‌های مجرمانه فراهم می‌آورد که پولشویی یکی از آنهاست.

نگرانی عمیق‌تر در باره موارد و مصادیق جرایم مرتبط با فناوری اطلاعات و ارتباطات می‌باشد که می‌تواند سرمایه‌های هنگفتی را گرفتار خود سازد. سرمایه‌هایی که ممکن است بخش قابل توجهی از منابع یک دولت را به خود اختصاص داده باشد و در نتیجه ثبات سیاسی و توسعه پایدار این کشورها را با تهدید مواجه سازد.

دولت‌ها بر این باورند که جرایم حوزه فناوری اطلاعات و ارتباطات، یک پدیده فراملی است که بر همه جوامع و اقتصادها تأثیر می‌گذارد و معتقدند که ایجاد همکاری‌های بین‌المللی برای پیشگیری و مقابله با این جرایم، یک ضرورت است.

همچنین معتقدند که سطوح فناورانه (تکنولوژیکی) سیستم‌های اطلاعاتی و مخابراتی کشورهای عضو بایستی از طریق ارائه کمک‌های فنی، هم تراز گردند. چرا که این امر نقش مهمی

در افزایش ظرفیت‌های کشورها در زمینه پیشگیری مؤثر و کارآمد از جرایم و ارتقای سطح امنیت اطلاعات ایفا می‌کند.

مصمم شدن دولت‌ها جهت پیشگیری، کشف و شناسایی و ممانعت مؤثر از نقل و انتقال بین‌المللی دارایی‌هایی که به صورت نامشروع تحصیل شده‌اند، این امر می‌تواند نتیجه مقابله با جرایم سایبری و تقویت همکاری‌های بین‌المللی در راستای احیای دارایی‌ها تلقی شود.

دولت‌ها بر این امر واقف‌اند که پیشگیری و ریشه کن کردن جرایم مربوط به فناوری اطلاعات و ارتباطات، مسئولیت همه دولت‌هاست و آن‌ها باید از طریق همکاری با یکدیگر، از مؤثر بودن تلاش‌هایشان در این حوزه اطمینان حاصل کنند. این امر از طریق حمایت از اشخاص و گروه‌های خارج از بخش عمومی {دولتی} مثل جامعه مدنی و مشارکت آن‌ها حاصل می‌شود. چرا که امنیت همه جانبه محیط اطلاعاتی به تلاش همه کشورها بستگی دارد.

دولت‌ها بر این باورند که محیط اطلاعاتی باید دقیقاً براساس اصول پذیرفته شده جهانی و هنجارهای حقوق بین‌الملل ایجاد شود.

با وقوف بر اینکه تمام دولت‌ها دارای استقلال هستند و هر کشوری باتوجه به محیط اطلاعاتی قلمرو خود، طبق قوانین ملی، اعمال صلاحیت می‌کند.

همچنین دولت‌ها اصول بی‌طرفی، مسئولیت و برابری درمقابل قانون و ترویج فرهنگ عدم پذیرش جرایم حوزه فناوری اطلاعات و ارتباطات را مورد نظر قرار می‌دهند.»

عناوین ۶ فصل این پیش‌نویس عبارت‌اند از:

فصل اول: مفاد عمومی^۱

در این فصل مواردی مثل اهداف کنوانسیون، ابعاد کاربست آن، حفاظت از استقلال و تعاریف و اصطلاحات لازم ارائه شده است. هدف اصلی کنوانسیون طبق ماده ۱ این فصل، اشاعه و تقویت اقدامات لازم با هدف پیشگیری و مقابله مؤثر با جرایم و سایر اقدامات غیر قانونی در حوزه فناوری اطلاعات و ارتباطات ذکر شده است.^۲

فصل دوم: جرم‌انگاری و اجرای قانون^۳

در این فصل به جرایم عمده سایبری مثل سرقت، استراق سمع، استفاده از بدافزار، دسترسی غیرمجاز به داده‌ها، قاچاق، جرایم مرتبط با پورنوگرافی کودکان و... اشاره و راه‌های مقابله و برخورد قانونی با این جرایم را ذکر شده است.

فصل سوم: اقدامات برای پیشگیری و مقابله با جرایم و دیگر اقدامات غیر قانونی در فضای

اطلاعات^۴

در این فصل، سیاست‌ها و شیوه‌های پیشگیری از جرایم و نهادهای مسئول در این زمینه تشریح شده است.

فصل چهارم: همکاری بین‌المللی^۵

قواعد عمومی همکاری‌های بین‌المللی و کمک‌های متقابل، استرداد مجرمان فضای سایبر و انتقال افراد محکوم شده، همکاری مراجع قضایی، همکاری‌های آموزشی و کمک‌های فنی، عمده مباحث این فصل می‌باشد.

فصل پنجم: سازوکارهای اجرا^۶

پیش‌بینی یک کمیسیون بین‌المللی و استفاده از ابزارهای سازمان ملل، عمده مطالب این فصل است.

فصل ششم: مفاد {مقررات} پایانی^۷

1. Chapter I.General provisions

2. To promote and strengthen measures aimed at effectively preventing and combating crimes and other unlawful acts in the field of ICT...

3. Chapter II. Criminalization and law enforcement

4. Chapter III.Measures to prevent and combat offences and other unlawful acts in cyberspace

5. Chapter IV.International cooperation

6. Chapter V.Mechanisms for implementation

7. Chapter VI.Final provisions

در فصل پایانی به مواردی مثل حل و فصل اختلافات، نحوه امضا، تصویب و پذیرش کنوانسیون، شرایط لازم الاجرا شدن آن، اصلاحات و بازنگری در کنوانسیون و موارد اعمال حق شرط پرداخته شده است.

روس‌ها مدعی هستند که پیش‌نویس ارائه شده توسط آن‌ها، اجازه دسترسی فراسرزمینی برای دستیابی به اطلاعات ذخیره شده را نمی‌دهد و آن را به اجازه آژانس‌های امنیت ملی کشورها منوط نموده است. در پیش‌نویس روسیه، یک بند اختصاصی برای حفاظت از استقلال ملی کشورهای امضاءکننده در نظر گرفته شده است. در این پیش‌نویس همچنین جزئیات سناریوهای مختلف برای همکاری و تشریک مساعی بین کشورها جهت مقابله با جرایم کامپیوتری مورد اشاره واقع شده است. مواردی از قبیل: تحقیقات و بازجویی‌های مشترک، تبادل اطلاعات درباره فعالیت‌های مجرمانه و بازداشت و تحویل مظنونان.

این پیش‌نویس پیشنهاد می‌کند که یک مرکز تماس ویژه تشکیل شود که قابلیت فعالیت ۲۴ ساعته در تمام ایام هفته را داشته باشد. همچنین پیشنهاد می‌کند که از طریق این مرکز، کمک‌های فوری برای بررسی جرایم کامپیوتری، بازداشت و تحویل مظنونان و ایجاد رویه‌های دادگاهی در مورد جرایم کامپیوتری صورت گیرد. روس‌ها در این پیش‌نویس همچنین پیشنهاد برگزاری کنفرانس‌های منظم تحت نظارت سازمان ملل، با مشارکت اعضای کنوانسیون را ارائه کرده‌اند. آخرین پیشنهاد روسیه، ایجاد یک کمیسیون دائمی بین‌المللی راجع به ابزارهای فنی جهت مقابله با جرایم سایبری می‌باشد.

باید گفت که نگرانی روسیه راجع به ماده ۳۲ کنوانسیون بوداپست یک نگرانی روسیه واقعی است. با توجه به اینکه جاسوسی، خلاف روح کنوانسیون وین (روابط دیپلماتیک) می‌باشد، اما بین دولت‌ها رایج است. فضای سایبر نیز قابلیت‌های گسترده‌ای برای جاسوسی دارد. از طرف دیگر با عنایت به پیشرفت‌های شگفت‌انگیز فناوری سایبری مخصوصاً در اروپا و آمریکا می‌توان درک کرد که چرا روسیه کنوانسیون بوداپست را امضا نمی‌کند. این نگرانی روسیه بعد از افشاگری‌های اسنودن، طبیعی است که دو چندان شود، زیرا انگلیس و چند کشور دیگر نیز در کنار آمریکا جاسوسی سایبری کرده‌اند. برخورد ضعیف بین‌المللی با آمریکا در این قضیه موجب شد که

روسیه خود به فکر تأمین امنیت زیرساخت‌های سایبری خود باشد و پرواضح است که کنوانسیون بوداپست را در این روند، یک مخاطره و تهدید بدانند. زیرا طبق ماده ۳۲، غربی‌ها می‌توانند جاسوسی سایبری نمایند.

از طرف دیگر نویسندگان غربی در مقالات خود می‌نویسند که روسیه، غرب را عامل انقلابات رنگی و مخملین در حوزه دربارهی خود می‌داند و در حال حاضر نگران است که غربی‌ها از فضای سایبر نیز برای شکل‌دهی انقلاب‌های رنگین استفاده کنند. بنابراین طبیعی است که روسیه مانع دست‌اندازی سایبری اروپا از طریق کنوانسیون بوداپست به قلمرو خود شود.

گفتار هفت: پیشنهاد تشکیل اولین کمیته باز برای تدوین کنوانسیون جرایم سایبری ۲۰۱۹

قدم‌های روسیه جهت تدوین کنوانسیون مقابله با جرایم سایبری در سازمان ملل از سال ۲۰۱۹ شتاب معناداری گرفته است. واکنش‌های هیجانی و غیر حقوقی غرب در مقابل اقدامات و ابتکارات حقوقی و دیپلماتیک روسیه حاکی از تشدید نگرانی آن‌هاست. اروپا و آمریکا نگران‌اند که قواعد مربوط به مبارزه با جرایم سایبری و تدوین کنوانسیون در این حوزه با ابتکار روسیه و حمایت جامعه جهانی منهای اروپا و آمریکا تدوین و توسعه یابد. مخصوصاً اروپا به خاطر پیدا شدن یک رقیب برای کنوانسیون جرایم سایبری (بوداپست) به شدت خشمگین است. روسیه در سال ۲۰۱۷ پیش‌نویس کنوانسیون جرایم سایبری را با هدف مقابله با کنوانسیون بوداپست به سازمان ملل ارائه کرد. اخیراً نیز در سال ۲۰۱۹ زیر قطعنامه مقابله با جرایم سایبری در سازمان ملل، تشکیل یک کمیته باز برای تدوین کنوانسیون جرایم سایبری را با وجود رأی منفی اروپا و آمریکا از تصویب گذراند. همه این اقدامات بر خلاف میل آمریکا و اروپا پیش می‌رود. همان‌گونه که گفته شد آخرین پیشنهاد روسیه در این پیش‌نویس، ایجاد یک کمیسیون دائمی بین‌المللی راجع به ابزارهای فنی جهت مقابله با جرایم سایبری می‌باشد.

مجمع عمومی در دومین نشست عمومی خود، که مورخ ۲۰ سپتامبر ۲۰۱۹ برگزار گردید، تصمیم گرفت تا در دستور کار اجلاس هفتادوچهارم مجمع، موضوعی تحت عنوان زیر را بگنجانند و {بررسی} آن را به کمیته سوم اختصاص دهد:

مقابله با استفاده از فناوری‌های اطلاعات و ارتباطات برای اهداف مجرمانه

کمیته سوم نیز در پنجمین و ششمین نشست خود در ۳ اکتبر ۲۰۱۹، یک بحث عمومی را {جهت بررسی} این گزینه برگزار نمود. برای بررسی این دستورکار، کمیته، گزارش دبیرکل درخصوص مقابله با استفاده از فناوری اطلاعات و ارتباطات برای اهداف مجرمانه^۱ را در اختیار داشت.

در چهل‌وچهارمین نشست کمیته سوم در ۷ نوامبر ۲۰۱۹، نماینده روسیه از طرف بلاروس، کامبوج، چین، کره شمالی، میانمار، نیکاراگوئه، ونزوئلا پیش‌نویس قطعنامه ای را با عنوان «مقابله با استفاده از فناوری اطلاعات و ارتباطات برای اهداف مجرمانه» ارائه نمود.^۲

در پنجاهمین نشست کمیته سوم که در ۱۸ نوامبر برگزار گردید، کمیته نسخه تجدید نظر شده این پیش‌نویس^۳ را مورد بررسی قرار داد در این پیش‌نویس علاوه بر هم‌بنیان پیش‌نویس اول، کشورهای زیر نیز هم‌بانی این پیش‌نویس گردیدند:

الجزایر، اوگاندا، آذربایجان، بولیوی، برونئی، کوبا، مصر، اریتره، ایران، قزاقستان، جمهوری دموکراتیک لائوس، ماداگاسکار، سودان، سورینام، سوریه، تاجیکستان، ازبکستان و زیمبابوه.

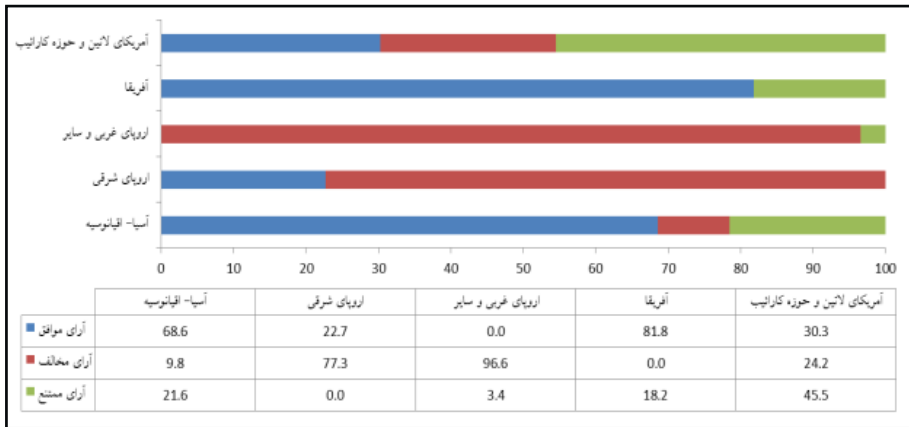
متعاقباً کشورهای زیر به هم‌بنیان پیش‌نویس این قطعنامه پیوستند:

آنگوا باربادوس، ارمنستان، بنین، کامرون، آفریقای مرکزی، کنگو، گینه استوایی، سوازیلند، گینه، هند، اندونزی، جامائیکا، قرقیزستان، نائرو، نیجریه، سنت ونسنت و گرنادا و آفریقای جنوبی، توگو، ترکمنستان، اوگاندا.

در همین نشست کمیته سوم، نسخه تجدید شده پیش‌نویس قطعنامه اخیر را با ۸۸ رای موافق، ۵۸ رای مخالف و ۳۴ رای ممتنع به تصویب کرد.

در ادامه مواضع کشورها در برابر قطعنامه روسیه در سال ۲۰۱۹ را بررسی می‌نماییم. قطعنامه‌ای که در آن تشکیل یک کمیته برای تدوین کنوانسیون جرایم سایبری پیش‌بینی شده است. مواضع اروپای غربی و شرقی و آمریکا محل تأمل است.

1. A/74/130
2. A/C.3/74/L.11
3. A/C.3/74/L.11/Rev.1



شکل ۶: توزیع آرا و مواضع کشورها درباره قطعنامه روسیه در سال ۲۰۱۹ براساس مناطق جغرافیایی

طبق نمودار بالا می‌توان گفت:

۱. بیش از ۹۶ درصد از کشورهای اروپای غربی به تبعیت از آمریکا، به قطعنامه پیشنهادی روسیه رأی منفی داده اند البته این امر نوعی پاسخ مقابله‌ای به روسیه محسوب می‌شد که در سال ۲۰۱۷ با ارائه پیش‌نویس کنوانسیون جرایم سایبری توانست کنوانسیون بوداپست را با چالش جدی مواجه سازد. در واقع کل اروپا به استثنای ترکیه (که به این قطعنامه رأی ممتنع داده است) به قطعنامه روسیه رأی منفی داده اند. بنابراین رأی ممتنع ترکیه خللی به یکپارچگی اروپا در وابستگی به آمریکا وارد نمی‌کند؛

۲. در اروپای شرقی که از سمت غرب، ادامه اروپا و از سمت شرق، ادامه روسیه است این یکپارچگی در وابستگی به آمریکا، دچار چالش است. نزدیک به ۲۳ درصد از کشورهای این منطقه به قطعنامه روسیه رأی مثبت داده اند. چهار کشور، بلاروس، صربستان، ارمنستان و آذربایجان به قطعنامه روسیه رأی مثبت داده اند. البته برخی کشورهای این منطقه مثل گرجستان و استونی به قطعنامه رأی منفی داده اند؛

۳. کشورهای آسیا و آفریقا بیشترین میزان موافقت با قطعنامه روسیه را داشته اند. حدود ۶۸٪ در آسیا و بالای ۸۱٪ در آفریقا با این قطعنامه همراه بودند. در آسیا فقط رژیم صهیونیستی، ژاپن و کره جنوبی به قطعنامه روسیه رأی منفی داده اند؛

۴. رأی مثبت حدود ۳۰ درصدی قاره آمریکا و حوزه کارائیب به قطعنامه روسیه حاکی از بلاتکلیفی این قاره است. آرای ممتنع این قاره از آرای موافق و مخالف بیشتر است.

بررسی سایر واکنش‌های مربوط به مخالفان اقدامات روسیه

در ادامه به بیان برخی نظرها درباره این قطعنامه و پیش‌نویس معاهده جرم سایبری از طرف مخالفان پرداخته می‌شود:

- روسیه به شکل پنهان تلاش می‌نماید تا هنجارهای جهانی را ایجاد نماید که از طریق این هنجارها دولت‌ها {می‌توانند} اینترنت را کنترل نمایند. هدف روسیه در طول دو دهه اخیر، دستیابی به یک معاهده جهانی است که اصولی را برای حاکمیت در فضای سایبری ایجاد نماید. در طول این ماه و به دنبال اجازه روسیه مبنی بر مسدود نمودن ترافیک اینترنت از خارج روسیه در شرایط اضطرار و اجازه به تأمین‌کنندگان خدمات اینترنتی جهت نصب نرم‌افزارهایی برای فیلتر کردن و برگرداندن مسیبر ترافیک‌های اینترنت^۱ که یکی از صاحب‌منصبان آمریکایی از آن به‌عنوان مانع آهنی دیجیتال^۲ نام می‌برند، حقوق حاکمیت اینترنت اجرا یافته است.^۳

- بحث حاکمیت در قلمرو امنیت ملی عامل مهمی شده است. به‌طوری که دولت‌های عضو سازمان ملل، سال‌هاست که در خصوص هنجارهایی که جنگ سایبری و جاسوسی سایبری را کنترل می‌کند بحث می‌نمایند. از طرفی طبق نظر استادیار دانشگاه نوادا «مدت‌های طولانی است که مفاهیمی در خصوص آزادی بیان و دموکراسی وجود دارد اگر مدل روسی - چینی در بحث اینترنت غالب شود، می‌تواند در آینده به رژیم‌های قدرت طلب کمک نماید.» به نظر برخی کارشناسان، غربی‌ها در جلوگیری از غلبه رویکرد چینی و روسی در این فضا موفق بوده‌اند.

- به نظر مخالفان، این قطعنامه برای تهدیدات جهانی درباره جرم سایبری مسیری را هموار می‌نماید. خود قطعنامه این عبارات را بیان نمی‌کند، اما این قطعنامه فرصتی برای کشورهایی مانند چین و روسیه مهیا می‌نماید که یک استاندارد مصوب در سازمان ملل را ایجاد کنند، {استانداردی که} به دولت‌ها اجازه می‌دهد وب‌سایت‌هایی را مسدود نمایند که از

1. government to block internet traffic from outside Russia "in an emergency" and to require internet service providers to install software that can filter and reroute traffic

2. "digital Iron Curtain."

3. "sovereign internet" law took effect

نگاه مراجع حکومتی حساس می‌باشند و همچنین اجازه می‌دهد که از فناوری‌های اطلاعات و ارتباطات جهت پایش مخالفان حکومت استفاده کنند. بنابراین اگرچه معاهده سازمان ملل متحد برای اعضای که آن را امضاء و به تصویب نکرده‌اند الزام‌آور نیست، اما مقامات عالی رتبه دولت‌ها از ایجاد استانداردهای جهانی با تأیید سازمان ملل توسط کشورهای روسیه و چین وحشت دارند. -تصویر کلی از این قطعنامه چنین است که روسیه و چین در تلاش‌اند تا مجموعه‌ای از هنجارهای جهانی را در خصوص چگونگی و حمایت از کنترل اینترنت و اطلاعات ایجاد نمایند. یکی از صاحب‌منصبان اروپایی عنوان نمود که، آن‌ها {روس‌ها} از هر وسیله‌ای که می‌توانند در سازمان ملل و محل‌های دیگر استفاده می‌کنند تا {این موضوع} را تقویت کنند. این موضوع درباره جرم سایبری نیست این درباره کسی است که اینترنت را کنترل می‌کند.»^۱

- به دنبال مخالفت روسیه با کنوانسیون بوداپست بر مبنای این اعتقاد که کنوانسیون بوداپست به حاکمیت {کشورها} تجاوز می‌نماید، روسیه، پیش‌نویس این معاهده را به شکلی تنظیم نموده است که جایگزین کنوانسیون بوداپست شود.

طبق نظر مخالفان، کنوانسیون بوداپست با هدف تقویت همکاری بین‌المللی در موضوعات جرم سایبری مطرح شده است و حاوی موضوع حاکمیت قانون و پادمان‌های حقوق بشر نیز می‌باشد. به نظر مخالفان که عموماً از طرف محافل غربی عنوان می‌شود تلاش‌های صورت گرفته توسط چین و روسیه نه تنها تهدیدی است برای با لکانیزه کردن (تجزیه کردن) فضای سایبری بلکه پوششی را برای مجرمان فراهم می‌کند که می‌توانند از هر مخفیگاهی به ما و به هر کسی برسند.^۲ -این قطعنامه در سازمان ملل متحد از طرف روسیه، چین، کره شمالی، میانمار، نیکاراگوئه، سوریه، کامبوج، ونزوئلا و بولیوی حمایت شد. محافل غربی تحت عنوان گروه‌های حقوق بشری، به شکل ائتلاف، نامه‌ای به مجمع عمومی نوشتند و عنوان کردند که:

«این قطعنامه دری را باز می‌نماید تا رفتارهای معمولی در فضای برخط که تحت حقوق بشر حفاظت می‌گردند جرم‌انگاری شوند.»^۳

1. "They're using every means they can in the U.N. and elsewhere to promote that. This is not about cybercrime. This is about who controls the internet."
 2. "can reach us — can reach everyone — from positions of sanctuary."
 3. "opens the door to criminalizing ordinary online behavior that is protected under international human rights law."

مبحث دوم

عملکرد حقوق بشری غرب در کمیته سوم و شورای حقوق بشر مجمع عمومی

گفتار اول: قطعنامه «حق حریم خصوصی در عصر دیجیتال»

«حق حریم خصوصی در عصر دیجیتال»^۱ عنوان اولین قطعنامه‌ای است که آلمان و برزیل این قطعنامه را در پی افشای برنامه‌های جاسوسی آمریکا از سوی ادوارد اسنودن، پیمانکار سابق آژانس امنیت ملی آمریکا ارائه کردند. بنا بر افشاگری‌های اسنودن، آژانس امنیت ملی آمریکا، مکالمات رهبران خارجی از جمله دیلما روسف رئیس جمهور برزیل و آنگلا مرکل صدر اعظم آلمان را استراق سمع کرده بود. این قطعنامه با هدف حفاظت از حریم شخصی افراد در برابر نظارت غیرقانونی در سال ۲۰۱۳ به تصویب رسید.^۲ تصویب این قطعنامه یکی از شدیدترین مظاهر اعتراضات بین‌المللی علیه اقدامات مربوط به جاسوسی آمریکا، از سوی جامعه بین‌المللی بود که در مجمع عمومی سازمان ملل به وقوع پیوست.

این قطعنامه از میان ۶۵ قطعنامه توصیه شده از کمیته سوم به مجمع عمومی بود که راجع به این موضوع از سوی کشورهای مختلف برای تصویب به سازمان ملل ارائه شده بود.^۳ این قطعنامه از اعضای سازمان ملل می‌خواهد تا درباره حفاظت از حریم شخصی کاربران اینترنتی و دیگر اشکال ارتباطات الکترونیکی اطمینان دهند.

در این قطعنامه آمده است: «حقوق افراد از جمله حریم شخصی آن‌ها؛ چه در محیط برخط و چه در محیط غیربرخط باید حفظ شود.»^۴ این برای نخستین بار بود که ضرورت تعمیم همه حقوق مربوط به حریم خصوصی زندگی مردم را در رابطه با استفاده از وسایل ارتباط جمعی و اینترنتی مورد تأکید قرار داده بود.

قطعنامه در پایان از کمیسر عالی حقوق بشر سازمان ملل می‌خواهد که گزارشی در خصوص ارتقای و حفاظت از حق حریم خصوصی در فضای سایبر را به مجمع عمومی سازمان ملل ارائه دهد.

1. The Right to Privacy in the Digital Age

2. UN Doc A/RES/68/167. 18 December 2013

3. <http://www.un.org/apps/news/story.asp?NewsID=46780#WPIimg3k2zIU> "General Assembly backs right to privacy in digital age"

4. Affirms that the same rights that people have offline must also be protected online, including the right to privacy;

این قطعنامه در سال ۲۰۱۴ نیز با اعمال تغییرات لازم و روزآمد کردن پیش‌نویس در مجمع عمومی سازمان ملل به تصویب رسید.^۱ در سال ۲۰۱۶ نیز این قطعنامه با پوشش تحولات جدید در مجمع عمومی سازمان ملل دوباره به تصویب رسید.^۲ این سه قطعنامه از مجاری کمیته سوم پیش رفتند. اما شورای حقوق بشر سازمان ملل^۳ در سال ۲۰۱۵ قطعنامه «حق حریم خصوصی در عصر اطلاعات»^۴ را تصویب کرد. تصویب قطعنامه با این عنوان در شورای حقوق بشر سازمان ملل، سابقه نداشته است و معلول افشاگری‌های اسنودن در خصوص شنودها و جاسوسی‌های فراگیر ایالات متحده در فضای فناوری اطلاعات و ارتباطات می‌باشد. البته اولین قطعنامه تحت این عنوان توسط مجمع عمومی در سال ۲۰۱۳ صادر شد. مجمع عمومی تعداد سه قطعنامه با این عنوان در سال‌های ۲۰۱۳، ۲۰۱۴ و ۲۰۱۶ صادر کرد. شورای حقوق بشر نیز در سال ۲۰۱۵ قطعنامه‌ای تحت این عنوان صادر کرد.

اگر دقیق شویم، متوجه می‌شویم که در سال ۲۰۱۵ که مجمع عمومی، قطعنامه «حق حریم خصوصی در عصر اطلاعات» را صادر نکرده، شورای حقوق بشر مبادرت به این اقدام کرده است. به نظر می‌رسد که نوعی هماهنگی بین ارکان و بخش‌های سازمان ملل وجود داشته که اولاً هر سال قطعنامه‌ای تحت این عنوان صادر شود و ثانیاً موازی‌کاری صورت نگیرد، به‌طوری که هم‌زمان مجمع عمومی و شورای حقوق بشر، قطعنامه‌ای تحت یک عنوان و موضوع صادر نمایند. این هماهنگی زمانی بیشتر خود را نشان می‌دهد که محتوای قطعنامه شورای حقوق بشر را با قطعنامه‌های مجمع عمومی مقایسه کنیم. در قطعنامه شورای حقوق بشر از مضامین، مفاهیم و حتی جملات قطعنامه‌های دو سال قبل مجمع عمومی استفاده شده و تنها تفاوتی که می‌توان یافت، تأکید بیشتر قطعنامه شورای حقوق بشر بر مباحث، اعلامیه‌ها، قطعنامه‌ها، میثاق‌ها و... حقوق بشری است که درصد فراوانی آن در مقایسه با قطعنامه‌های مجمع بیشتر است که البته این موضوع نیز کاملاً بجا و طبیعی است.

1. UN Doc A/RES/69/166 of 18 December 2014

2. UN Doc A/RES/71/199. 25 January 2017

3. Human Rights Council

4. UN Doc A/HRC/RES/28/16 - 1 April 2015

گفتار دو: قطعنامه «ارتقای، حفاظت و برخورداری از حقوق بشر در اینترنت»

شورای حقوق بشر سازمان ملل متحد به‌عنوان یک سازمان بین‌الدولی در ۱۵ مارس ۲۰۰۶ پایه‌ریزی شد. کوفی عنان، درست زمانی که دستور کار خود برای اصلاحات گسترده در سازمان ملل را مطرح کرد، ایجاد یک نهاد حقوق بشری جدید با اعتبار بیشتر را به‌عنوان اولویت مهم معرفی نمود. نهایتاً رهبران جهان از درخواست وی برای یک شورای حقوق بشر مؤثرتر و پاسخگوتر در سند نهایی اجلاس سران ۲۰۰۵ حمایت نمودند و یک سال بعد، این شورا تشکیل شد. وظیفه شورای حقوق بشر سازمان ملل متحد، نظارت بر اجرای مفاد منشور حقوق بشر در کشورهای عضو سازمان ملل متحد است. مقر این شورا در ژنو قرار دارد.^۱ در این مجمع ۴۷ کشور عضویت دارند. هر ساله یک‌سوم اعضای جدید این شورا به مدت سه سال دیگر انتخاب می‌شوند. مسئله سخت‌گیری در عضویت شورا، یکی از مهم‌ترین مباحثی بود که در جایگزینی نهادی جدید به جای کمیسیون مورد توجه قرار گرفت. در آخرین سند هم در چندین مورد تدابیری برای تضمین این مسئله لحاظ شده است، ولی باید در نظر داشت که در نهایت ضوابط و معیارهای دقیقی برای عضویت تعریف نشد و روند عضویت بر اساس توزیع متناسب جغرافیایی مورد پذیرش قرار گرفت، اما انتخاب اعضاء توسط مجمع عمومی به یک انتخاب سیاسی تبدیل شد که نتیجه آن را در برخوردهای دوگانه این شورا شاهدیم. کوفی عنان، دبیرکل وقت سازمان ملل معتقد بود که کمیسیون حقوق بشر سازمان ملل راه خود را گم کرده، خیلی سیاسی شده و به مجمعی تبدیل شده بود که در آن نقض‌کنندگان حقوق بشر با توطئه بر کار یکدیگر سرپوش می‌گذاشتند و برای کاری که به آن محول شده بود کوچک بود.^۲ اما امروز شاهدیم که شورا نیز به همان سرنوشت کمیسیون دچار شده است.

شورای حقوق بشر سازمان ملل متحد، به‌عنوان جانشین کمیسیون حقوق بشر، عمل می‌کند. شورای جدید، نهاد فرعی مجمع عمومی است و انتخاب اعضای شورای حقوق بشر به مجمع عمومی واگذار شده است. در حالی که کمیسیون حقوق بشر تابع شورای اقتصادی و اجتماعی بود و اعضای آن توسط شورای اقتصادی - اجتماعی تعیین می‌شدند. بنابراین در نظر داشته

1. <http://hamshahrionline.ir/details/81342>

2. <http://www.asibha.com/tab-248/index.aspx?nid=150&mId=2508>

باشیم که شورای حقوق بشر به مجمع عمومی گزارش می‌دهد و نهاد تابع مجمع عمومی محسوب می‌شود و ارتباط مستقیمی با شورای امنیت ندارد. هر چند که گفته می‌شود شورای امنیت، طبق روالی که به خصوص پس از جنگ سرد در پیش گرفت می‌تواند در موارد نقض گسترده و سیستماتیک حقوق بشر، وضعیت را تهدید به صلح، نقض صلح یا تجاوز قلمداد کند و از سازوکارهای تنبیهی فصل هفتم استفاده نماید. دادن ضمانت اجرایی قوی‌تر به شورای حقوق بشر از جمله مباحث اولیه بود. اما در آخرین سند، برایندهایی چون ارائه «توصیه» به چشم می‌خورد که در مقایسه با انتظارات و پیشنهادهای اولیه مبنی بر دادن ضمانت‌ها و ابزارهای اجرایی، ضعیف‌تر به نظر می‌رسد، به هر حال هیچ سازوکار مستقیم اجرایی برای شورای حقوق بشر مورد توافق واقع نشده است.

این مقدمه را باید گفت که قطعنامه «ارتقای، حفاظت و برخورداری از حقوق بشر در اینترنت»^۱ اولین بار در سال ۲۰۱۲ از سوی شورای حقوق بشر صادر شد^۲ که متن آن حدود یک صفحه بود. این قطعنامه در سال‌های ۲۰۱۴ و ۲۰۱۶ نیز در شورای حقوق بشر تصویب شد. افشاگری اسنودن، تأثیر خود را بر کم و کیف قطعنامه در سال‌های بعد گذاشته و محتوای آن را با تحولات جدید عجین کرد. این قطعنامه با تأکید بر اسناد بین‌المللی حقوق بشری شروع می‌شود و در بندهای بعدی به موضوع حقوق بشر از جمله اهمیت آزادی بیان در اینترنت می‌پردازد. این قطعنامه تصریح می‌کند همان حقوقی که مردم به صورت غیر برخط دارند را باید در فضای برخط نیز داشته باشند که از جمله آن‌ها حق آزادی بیان می‌باشد.

قطعنامه سال ۲۰۱۴ تحت تأثیر افشاگری اسنودن، طیف گسترده‌تری از مسائل را پوشش داده است.^۳ اولین مسئله‌ای که در قطعنامه ۲۰۱۴ تازگی دارد تأکید بر اهمیت اعتمادسازی در اینترنت^۴ است که قطعنامه سال ۲۰۱۲ فاقد آن است. این موضوع به جهت موج فزاینده بی‌اعتمادی به فضای سایبر در بین کشورها و ملت‌ها، در قطعنامه گنجانده شده است که معلول افشاگری اسنودن از اقدامات غیرقانونی آمریکا در فضای سایبر می‌باشد. مسئله بعدی که در این

1. The promotion, protection and enjoyment of human rights on the Internet

2. A/HRC/RES/20/8 - 16 July 2012

3. A/HRC/RES/26/13- 14 July 2014

4. importance of building confidence and trust in the Internet

قطعنامه، نوظهور است تأکید بر اهمیت کلیدی مشارکت همه ذی‌نفعان فضای سایبر اعم از جامعه مدنی، بخش خصوصی و جامعه فنی و دانشگاهی در کنار دولت برای حفاظت از حقوق بشر و آزادی‌های اساسی در فضای سایبر است^۱ که واکنشی به انحصارگرایی آمریکا در فضای فناوری اطلاعات است.

رعایت حریم خصوصی و حاکمیت قانون، دو موردی هستند که ردپای افشاگری اسنودن در این قطعنامه را به وضوح نشان می‌دهد.

قطعنامه سال ۲۰۱۶ شورای حقوق بشر با عنوان ارتقای، حفاظت و برخورداری از حقوق بشر در اینترنت^۲ باز در مقایسه با دو قطعنامه قبلی مفصل‌تر است. بحث عدم مداخله^۳ در این قطعنامه مطرح شده که در مقایسه با دو قطعنامه قبلی، سابقه ندارد. در صفحه دوم این قطعنامه آمده است:

«نگرانی عمیق به دلیل نقض هر یک از ابعاد حقوق بشر و اقدام غیرمجاز علیه حقوق اساسی افراد در اینترنت و نگرانی عمیق بابت اینکه این تخلفات از مصونیت (حاشیه امن) نیز برخوردار باشند {و مجازات نشوند}»^۴

این قطعنامه پا را از این هم فراتر نهاده و برای اولین بار چنین اقداماتی را محکوم^۵ می‌کند. قبلاً توضیح دادیم که در هیچ یک از سه قطعنامه مجمع عمومی که بعد از افشاگری اسنودن علیه آمریکا صادر شدند از عبارت محکومیت استفاده نشده و صرفاً به انتقاد از این اقدامات پرداخته‌اند. این موضوع نشان می‌دهد که تا سال ۲۰۱۶ ابعاد بیشتری از اقدامات غیر قانونی دولت ایالات متحده، برای جهانیان آشکارسازی شده است.

بند ۸ از صفحه سوم قطعنامه بیان می‌دارد:

«محکومیت جهانی همه موارد نقض حقوق بشر یا سوءاستفاده از آن مثل شکنجه و... علیه حقوق اساسی افراد در اینترنت...»^۶.

1. Considering the key importance of government engagement with all relevant stakeholders, including civil society, private sector, the technical community and academia, in protecting and promoting human rights and fundamental freedoms online,
2. A/HRC/RES/32/13- 18July 2016
3. interference
4. Deeply concerned by all human rights violations and abuses committed against persons for exercising
5. Condemns
6. Condemns unequivocally all human rights violations and abuses, such as torture...



در مجموع می‌توان گفت که به موازات روشن شدن ابعاد جدیدی از اقدامات غیرقانونی آمریکا در فضای سایبر، متن و محتوای قطعنامه‌های شورای حقوق بشر سازمان ملل نیز پررنگ‌تر و شدیدالحن‌تر شده است. در نظر داشته باشیم که این همه با وجود فشارهای پیدا و پنهان آمریکا و نفوذ این کشور بر ارکان و اجزای سازمان ملل حاصل شده است و گرنه می‌توانستیم شاهد اقدامات به واقع شدیدتری علیه آمریکا باشیم.

مبحث سوم عملکرد گروه ۷۷ در کمیته دوم

گفتار اول: ارائه پیش‌نویس قطعنامه «فناوری‌های اطلاعات و ارتباطات برای توسعه»

پیش‌نویس «قطعنامه فناوری‌های اطلاعات و ارتباطات برای توسعه» در سال ۲۰۰۲ به ابتکار این گروه تهیه شد. سابقه این قطعنامه به سال ۲۰۰۱ برمی‌گردد و پیش‌نویس آن، اولین بار توسط گروه موسوم به گروه ۷۷ ارائه شد. گروه ۷۷ در راستای مأموریتی که برای خود دارد، سعی می‌کند شکاف موجود بین کشورهای توسعه‌یافته و در حال توسعه را کاهش دهد. یکی از این شکاف‌ها، شکاف علمی و فناورانه است. در سال ۲۰۰۱، گروه ۷۷ و چین، پیش‌نویس قطعنامه‌ای تحت عنوان «علم و فناوری برای توسعه»^۱ را به کمیته دوم ارائه کردند.^۲

این پیش‌نویس با اعمال تغییرات مربوط به تحولات جدید و تقریباً با همان محتوا در سال ۲۰۰۲ ارائه شد^۳ و در سال ۲۰۰۳ نیز این روند ادامه یافت.^۴

در سال ۲۰۰۴، این روند ضمن تداوم، با تغییراتی همراه شد. در این سال، نماینده سوئیس به نمایندگی از کشور خود و تونس، پیش‌نویس قطعنامه دیگری^۵ را به کمیته دوم ارائه کرد که به تصویب مجمع عمومی سازمان ملل رسید.^۶

در سال ۲۰۰۵ به واسطه اینکه کشورها درگیر اجلاس تونس و اسناد آن بودند، قطعنامه‌ای از کانال کمیته دوم در ارتباط با موضوع به مجمع عمومی ارائه نشد. در عوض، اسناد تونس توانست تا حدی به نفع کشورهای در حال توسعه تنظیم و تصویب شود.

در سال ۲۰۰۶ قطعنامه «اجلاس جهانی سران در مورد جامعه اطلاعاتی» دوباره تصویب شد که به دستاوردهای اجلاس سران در ژنو و تونس اختصاص داشت.^۷

در این قطعنامه، نقش محوری و اصلی فناوری اطلاعات و ارتباطات در ایجاد اقتصاد دانش‌بنیان،

1. science and technology for development

2. A/56/558/Add.3- 13 December 2001

3. A/57/529/Add.3 -12 December 2002

4. UN DOC - A/57/48

5. "World Summit on the Information Society" «اجلاس جهانی سران در مورد جامعه اطلاعاتی»

6. A/RES/59/220 -11 February 2005

7. A/RES/60/252 - 27 April 2006

مورد تأکید قرار گرفته است. در بند دیگری از این پیش‌نویس از ایجاد نیروی اقدام^۱ در زمینه فناوری اطلاعات و ارتباطات استقبال شده است.

این قطعنامه از کشورهای توسعه‌یافته می‌خواهد که درباره کاهش محدودیت‌های اعمال شده برای انتقال فناوری به کشورهای در حال توسعه اقدام کنند. همچنین از سیستم سازمان ملل می‌خواهد که برای تقویت فعالیت‌ها در قالب همکاری‌های جنوب - جنوب اقدام نماید.

هفتادونهمین نشست عمومی اجلاس ۵۷ مجمع عمومی در ۲۰ دسامبر ۲۰۰۲ در نیویورک و به ریاست آقای کاوان^۲ از جمهوری چک برگزار گردید، دستور کار شماره ۳۲ این نشست، به بررسی پیش‌نویس قطعنامه شماره A/57/L.71 تحت عنوان «فناوری اطلاعات و ارتباطات برای توسعه» اختصاص یافت.

در ادامه برگردان اظهارات نماینده پاکستان در خصوص قطعنامه ارائه می‌گردد:

در این نشست آقای کاوان ضمن یادآوری بحث‌هایی که درباره این موضوع در نشست‌های عمومی ۴۳ و ۴۴ این اجلاس {اجلاس ۵۷}^۳ انجام شده بود، از نماینده پاکستان در خواست نمود تا قطعنامه شماره A/57/L.71 را برای اعضا تشریح نماید.^۴

آقای حسن، نماینده پاکستان ضمن ابراز خرسندی از مجالی که برای تشریح این قطعنامه در اختیار وی قرار داده شد، مطالبی را در خصوص پیش‌نویس این قطعنامه درباره فناوری اطلاعات و ارتباطات برای توسعه ارائه نمود. به ادعای ایشان:

«اهمیت فناوری اطلاعات و ارتباطات برای توسعه» به قدری مهم است که جای هیچ مبالغه‌ای درباره آن وجود ندارد. با اذعان به اهمیت این موضوع بود که:

- رهبران گروه جنوب (کشورهای در حال توسعه)، در نشست هاوانا در آوریل ۲۰۰۰، به اتفاق آرا تصمیم گرفتند تا دانش و فناوری را در مرکز خط‌مشی‌های توسعه در کشورهای خود قرار دهند؛

- رهبران ما {اعضای گروه ۷۷} در اعلامیه هزاره، تصمیم گرفتند تا تضمین نمایند که منافع حاصل از فناوری‌های جدید مخصوصاً فناوری‌های اطلاعات ارتباطات در دسترس همگان

1. Task Force

2. Mr. Kavan

4. A/57/PV.79

۳. این دو نشست عمومی به ترتیب در چهارم و هشتم نوامبر سال ۲۰۰۲ برگزار گردیدند.

قرار گیرد؛^۱

- اعلامیه اجرایی شورای اقتصادی و اجتماعی مربوط به سال ۲۰۰۰، خواهان راهبردی منسجم در گستره سیستم فناوری اطلاعات و ارتباطات می‌باشد که هماهنگی و همکاری میان برنامه‌ها و اقدامات سازمان‌های منحصربه‌فرد (خصوصی) در نظام فناوری و اطلاعات و تبدیل آن به سازمان‌هایی با سیستم دانش‌محور^۲ را تضمین نماید؛

- مجمع عمومی در اجلاس پنجاه و هفتم خود یک اجلاس ویژه دو روزه به موضوع فناوری اطلاعات برای توسعه اختصاص داد؛

- علاوه بر این، مقدماتی جهت تشکیل اجلاس سران درباره جامعه اطلاعاتی در سال‌های ۲۰۰۳ و ۲۰۰۵ در دست اقدام می‌باشد و انتظار می‌رود که این اجلاس یک فرصت بزرگی را برای بررسی قابلیت‌های فناوری اطلاعات و ارتباطات برای توسعه مهیا می‌نماید. پیش‌نویس این قطعنامه بر اساس اعلامیه هزاره سوم و اعلامیه شورای اقتصادی و اجتماعی بنا شده است و بر موضوعات زیر تأکید دارد:

- استفاده از فناوری اطلاعات و ارتباطات به‌عنوان یک ابزار راهبردی جهت ارتقای کارایی، اثربخشی و تأثیر برنامه‌های توسعه و اقدامات نظام سازمان ملل متحد در همکاری‌های فنی. - نقش قاطع و محکمی که فناوری اطلاعات و ارتباطات می‌تواند در تسهیل هماهنگی و مساعدت بین برنامه‌ها و اقدامات نظام سازمان ملل متحد ایفا نماید.

{از آنجایی که} این پیش‌نویس، گامی مهم به سوی توسعه راهبردی جامع برای فناوری‌های اطلاعات و ارتباطات می‌باشد. من باید به طور مختصر برخی از عناصری که ضروری است تا در توسعه این راهبرد مورد نظر قرار گیرد را برجسته نمایم:

اولاً: ما به‌کارگیری و استفاده از گستره سیستم فناوری اطلاعات و ارتباطات جهت تقویت ظرفیت ملل متحد در تولید، به اشتراک‌گذاری و نشر دانش و کمک به ایجاد ملل متحدی

۱. اهداف توسعه هزاره شامل ۸ مورد است که ۱۹۱ کشور عضو سازمان ملل متحد، در سپتامبر ۲۰۰۰ متعهد شدند تا بدان دست یابند: مورد هشتم آن در باب مشارکت گسترده جهانی در برابر توسعه، در کنار موارد دیگر، با هدف رسیدگی به نیازهای ویژه و خاص کشورهای با کمترین میزان توسعه و کشورهای در حال توسعه محصور در خشکی و نیز جزایر کوچک می‌باشد.

2. Providing global leadership in bridging the digital divide and promoting digital opportunity, and adopting, in order to enhance the capacity of the United Nations system to achieve these goals, a coherent system-wide ICT strategy that would ensure coordination and synergy among programmes and activities of individual organizations of the system and transform it into a knowledge-based system of organizations;

با کارایی، اثربخشی بیشتر در ارائه خدمات به دولت‌های عضو، را مورد تشویق قرار می‌دهیم؛
ثانیاً: ما باید فناوری‌های اطلاعات و ارتباطات را به‌صورت کامل در فعالیت‌های مربوط به
همکاری‌های فنی - توسعه‌ای سازمان‌های وابسته به نظام ملل متحد، جریان‌سازی و نهادینه
نماییم؛

ثالثاً: ما باید شبکه‌های همکاری و جوامع عملی را میان سازمان‌های {متعلق به} نظام ملل
متحد ایجاد نماییم؛

رابعاً: ما باید تشویق نماییم تا از فناوری اطلاعات و ارتباطات در راستای ارتقای تبادل تجربیات
و به اشتراک‌گذاری اطلاعات میان سازمان‌های {متعلق به} نظام سازمان ملل و بین {این}
سازمان‌ها و کشورهای عضو استفاده گردد؛

و در آخر: توسعه راهبرد جامع فناوری اطلاعات و ارتباطات برای نظام سازمان ملل متحد،
تمامی نهادهای مرتبط در سازمان ملل و سایر سازمان‌های بین‌دولتی را جهت همکاری بیشتر و
حمایت از آماده‌سازی فرایند اجلاس سران درباره جامعه اطلاعاتی را تشویق خواهد نمود.
بر اساس خروجی {جلسات} مستشاری که به شکل غیر رسمی {برگزار گردیده است}، من
بسیار خرسندم تا مجمع عمومی را در خصوص این نکته آگاه سازم که پیش‌نویس قطعنامه،
مورد حمایت تمامی دولت‌های عضو سازمان ملل متحد قرار گرفته است و امیدوارم که مجمع
این پیش‌نویس را از طریق اجماع تصویب کند.

بعد از سخنرانی نماینده پاکستان، آقای کاوان اعلام نمود که در این اجلاس، مجمع عمومی
در خصوص این قطعنامه تصمیم‌گیری خواهد کرد.

و نهایتاً پیش‌نویس این قطعنامه تحت شماره ۵۷/۲۹۵ در سال ۲۰۰۲ تصویب شد. این روند
تا کنون ادامه داشته و ترجمه سه عنوان قطعنامه به فاصله زمانی مناسب، انتخاب و ترجمه شده
است. مشخصات کامل سایر قطعنامه‌ها ارائه شده و متن آن‌ها در لوح الکترونیکی پیوست کتاب،
ارائه شده است.

سال ۲۰۰۷ دوباره قطعنامه‌ای تحت عنوان «فناوری اطلاعات و ارتباطات برای توسعه»^۱ از

طرف گروه ۷۷ به کمیته دوم ارائه شد^۱ و در مجمع عمومی به تصویب رسید.^۲ تا سال ۲۰۰۷ قطعنامه‌ها به صورت عام به نقش علم و فناوری برای توسعه پرداخته و در ضمن آن به نقش فناوری‌های اطلاعاتی و ارتباطی اشاره می‌شد. اما از سال ۲۰۰۷ به صورت متمرکز به موضوع فناوری اطلاعاتی و ارتباطی پرداخته شد.

قطعنامه سال ۲۰۰۷ بسیار مختصر بود و به چند بند محدود شده بود که باز به اجلاس سران اختصاص داشت. اما قطعنامه سال ۲۰۰۸ مشتمل بر چهار صفحه، مطالب متنوعی را در ارتباط با موضوع مورد اشاره قرار داده بود.^۳

این قطعنامه بر کاهش شکاف دیجیتالی^۴ و بهره‌مندی همگان از دسترسی به فناوری‌های جدید مخصوصاً فناوری اطلاعات و ارتباطات تأکید کرده و معتقد است که فناوری‌های اطلاعاتی و ارتباطی می‌تواند راه‌حل‌های جدیدی را پیش روی چالش‌های توسعه قرار دهد. این موضوع مخصوصاً در قالب جهانی‌سازی، تسریع رشد اقتصادی، دسترسی به اطلاعات و دانش قابل بررسی است. بر این نکته نیز تصریح شد که فناوری اطلاعات و ارتباطات، کاربرد دوگانه دارد و به صورت توأمان می‌تواند فرصت‌ها و چالش‌هایی را ایجاد کند.

همچنین تأکید دوباره بر اینکه همکاری‌های جنوب- جنوب می‌تواند به عنوان ابزاری مؤثر به توسعه فناوری اطلاعاتی و ارتباطی کمک نماید صورت گرفت.

قطعنامه «فناوری اطلاعات و ارتباطات برای توسعه» از سال ۲۰۰۷ تا کنون از طرف گروه ۷۷ به کمیته دوم ارائه شده و پس از طی مراحل به تصویب مجمع عمومی رسیده است.^۵ محتوای همه قطعنامه‌ها مثل هم است و فقط تحولات جدید به متن قطعنامه‌ها اضافه شده است. این قطعنامه‌ها نوعاً ایجابی است و به نقش فناوری اطلاعات و ارتباطات در توسعه اقتصادی و حتی اجتماعی پرداخته‌اند و نگاه توسعه‌ای و ابزار محور به فناوری اطلاعات و ارتباطات، ویژگی مشترک این قطعنامه‌هاست.

1. A/62/416- 19 November 2007
2. A/RES/62/182- 31 January 2008
3. A/RES/63/202 - 28 January 2009
4. digital divide
5. A/RES/70/184- 4 February 2016

گفتار دو: حمایت از قطعنامه «اجلاس سران در مورد جامعه اطلاعاتی»

در سال ۲۰۰۴، نماینده سوئیس به نمایندگی از کشور خود و تونس، پیش‌نویس قطعنامه‌ای تحت عنوان «اجلاس جهانی سران در مورد جامعه اطلاعاتی»^۱ را به کمیته دوم ارائه کرد که مورد حمایت گروه ۷۷ و کشورهایی مثل کانادا، فنلاند، فرانسه، آلمان، ژاپن، پرتغال، اسپانیا، سوئد و ترکیه قرار گرفت.^۲ البته تونس که از سال ۲۰۰۱ به‌عنوان میزبان اجلاس جهانی سران درباره جامعه اطلاعاتی در سال ۲۰۰۵ تعیین شده بود، هر سال پیش‌نویس‌هایی تحت همین عنوان به کمیته دوم ارائه می‌کرد. سوئیس نیز میزبان اجلاس سال ۲۰۰۳ بود.

قطعنامه تحت عنوان «اجلاس جهانی سران در مورد جامعه اطلاعاتی»^۳ در سال ۲۰۰۴ به تصویب مجمع عمومی سازمان ملل رسید.^۴

در ابتدای این قطعنامه نقش بالقوه فناوری اطلاعات و ارتباطات به‌عنوان ابزاری قدرتمند برای تقویت توسعه اجتماعی و اقتصادی مورد تأکید قرار گرفته است. عمده محتوای این قطعنامه به اجلاس ژنو و تونس اختصاص یافته است.

در سال ۲۰۰۵ به واسطه اینکه کشورها درگیر اجلاس تونس و اسناد آن بودند، قطعنامه‌ای از کانال کمیته دوم در ارتباط با موضوع به مجمع عمومی ارائه نشد. در عوض، اسناد تونس توانست تا حدی به نفع کشورهای در حال توسعه تنظیم و تصویب شود.

در سال ۲۰۰۶ قطعنامه «اجلاس جهانی سران در مورد جامعه اطلاعاتی» دوباره تصویب شد که به‌دستاوردهای اجلاس سران در ژنو و تونس اختصاص داشت.^۵

درباره قطعنامه شماره A/60/L.50 تحت عنوان «اجلاس سران درباره جامعه اطلاعاتی» در سال ۲۰۰۶ باید گفت که هفتادوچهارمین نشست عمومی تحت اجلاس ۶۰ مجمع عمومی در ۲۷ مارس ۲۰۰۶ در نیویورک برگزار گردید، این نشست با غیبت آقای الیسون^۶ (رئیس مجمع عمومی وقت) از کشور سوئد، توسط جانشین وی خانم باهاموکا^۷ از کشور کنیا اداره شد.

1. "World Summit on the Information Society"

2. Draft resolutions A/C.2/59/L.18 and A/C.2/59/L.32

3. "World Summit on the Information Society"

4. A/RES/59/220 - 11 February 2005

5. A/RES/60/252 - 27 April 2006

6. Eliasson

7. Bahemuka

دستورکار ۴۹ این نشست، به بررسی پیش‌نویس قطعنامه شماره A/60/L.50 تحت عنوان «اجلاس سران درباره جامعه اطلاعاتی» اختصاص یافت.

در این نشست خانم باهاموکا مطالبی را به شرح زیر عنوان داشتند:

«اعضای تصمیم شماره ۵۸/۵۶۹ مجمع عمومی مورخ ۱ جولای ۲۰۰۴ را به یاد خواهند آورد مبنی بر اینکه، گزارش اجلاس سران درباره جامعه اطلاعاتی، بدون در نظر گرفتن این حقیقت که این موضوع مختص به کمیته دوم می‌باشد مستقیماً در نشست عمومی اجلاس شصتم ملاحظه گردید. در این ارتباط یادداشتی از طرف دبیرکل در خصوص گزارش ارسالی اجلاس سران درباره جامعه اطلاعاتی در سندی با شماره A/60/687 منتشر گردیده است.»

وی در ادامه ضمن یادآوری نقش کلیدی علم و فناوری مخصوصاً اهمیت فناوری اطلاعات و ارتباطات به‌عنوان ابزار حیاتی جهت دستیابی به اهداف توسعه پایدار، عنوان نمودند: «همانگونه که اعضا آگاه هستند، دو سال بعد از طرح و دستور کار ژنو که در آن اهداف دقیقی برای اتصالات {اینترنت} جهانی تا سال ۲۰۱۵ ترسیم شد، مرحله دوم اجلاس سران درباره جامعه اطلاعاتی در تاریخ ۱۶ تا ۱۸ نوامبر سال ۲۰۰۵ در تونس برگزار گردید. در این اجلاس، اساساً به موضوع تقویت نگاه مشترک به جامعه اطلاعاتی مردم‌محور، فراگیر و توسعه مدار پرداخته شد^۴ و دستورکار این اجلاس در میان سایر موارد موضوعات زیر را در بر گرفت:

✓ اتخاذ گام‌های ویژه جهت رفع شکاف دیجیتالی؛

✓ اصولی برای اقدام و تنظیم سازوکارهای مالی؛

✓ پیگیری تصمیمات اتخاذ شده در ژنو و تونس.

به طور شفاف، نشست امروز می‌تواند گامی پیشرفته در اقدامات جمعی قلمداد شود که در راستای اجرای خروجی اجلاس سران در سال ۲۰۰۵ در زمینه توسعه تشکیل گردیده است. «وی در ادامه ضمن بیان توضیحاتی در خصوص ضرورت و اهمیت اینترنت در زندگی شخصی و کسب‌وکار افراد بیان نمودند:

«جهان نیازمند تضمینی است مبنی بر اینکه تمامی منافی که اینترنت به همراه دارد برای

4. contributed substantially to the strengthening of our common vision of an information society that is people-centred, inclusive and development-oriented

اکثریت مردم مخصوصاً در کشورهای در حال توسعه قابل دسترس باشد. همچنین ضمن اطمینان از اینکه اینترنت به طریقی مدیریتی می شود که متضمن آزادی دسترسی به اطلاعات باشد، ما نیازمند یافتن راهی هستیم برای حفاظت از مردم در مقابل ابعاد و جنبه های مضر اینترنت. ما چنانچه بخواهیم مردم در همه جای دنیا از بیشترین منافع فناوری اطلاعات و ارتباطات بهره مند گردند راهی نداریم جز اینکه با هم در سطوح ملی و بین المللی همکاری نماییم.» در ادامه وزیر فناوری ارتباطات کشور تونس، آقای Montasser Ouaili (به نمایندگی از گروه ۷۷) به تشریح پیش نویس قطعنامه شماره A/60/L.50 پرداخت:

«من باید در ابتدا از خانم رئیس به خاطر تشکیل این نشست عمومی و همچنین بابت بیانیه مقدماتی {ایشان} که منعکس کننده اهمیت {این موضوع} می باشد تشکر نمایم. اهمیت این موضوع باعث گردیده { که شما و مجمع عمومی این بخش را ضمیمه دستور کار خود قرار دهد. همچنین از این فرصت استفاده می نمایم تا از دبیرکل بابت علاقه همیشگی شان به اجلاس سران درباره جامعه اطلاعاتی و مشارکت ایشان در مرحله دوم این اجلاس که مورخ ۱۶ تا ۱۸ نوامبر ۲۰۰۵ در تونس برگزار گردید تشکر نمایم.

- رهبر تونس آقای زین العابدین بن علی و نیز دولت و مردم ما، از میزبانی اجلاس سران خرسند گردیدند و از هیچ تلاشی جهت برگزاری موفق این اجلاس کوتاهی ننمودند. این مرحله از اجلاس سران درباره جامعه اطلاعاتی به خاطر حضور تعداد شرکت کنندگان برجسته گردید. شرکت کنندگانی که نماینده دولت ها، سازمان های بین المللی، سازمان های بین دولتی، بخش خصوصی، جامعه مدنی و رسانه بودند. ما امیدواریم که آن ها خاطره خوبی از تونس به عنوان یک کشور آزاد و مهمان نواز داشته باشند.

هشت سال پیش، رئیس جمهور تونس پیشنهادی جهت برگزاری کنفرانس اتحادیه بین المللی مخابرات- در سطح بالای بین المللی- در شهر مینیاپولیس^۱ ارائه نمود. در آن زمان دنیا هنوز در مرحله شروع انقلاب دیجیتالی بود.

در خلال مرحله اول، اجلاس سران درباره جامعه اطلاعاتی تأثیر انقلاب دیجیتال بر روی

اختلاف های اقتصادی، اجتماعی و فرهنگی را تأیید نمود در مرحله بعدی راه حل های امیدبخشی را برای آینده کشورهای ما ایجاد کرد.

توسعه فناوری های اطلاعات و ارتباطات که به عنوان عاملی برای رشد مطرح است همیشه به شکل عادلانه به اشتراک گذارده نشده است. درست هنگامی که فناوری اطلاعات و ارتباطات باید به عنوان عاملی جهت یکپارچگی به کار آید و در حصول اهداف توسعه پایدار هزاره مشارکت فعال داشته باشد، شکاف دیجیتالی بین کشورها، نواحی و طبقه های اجتماعی در طول این سال ها رشد یافته است.

امروزه بیشتر از گذشته، یکپارچگی فناوری های اطلاعات و ارتباطات به عنوان یک ابزار راهبردی توسعه، امری ضروری می باشد. بنابراین جامعه بین المللی باید تلاش خود را جهت توانمندسازی تمامی کشورها مخصوصاً کشورهای کمتر توسعه یافته جهت بهره مندی از انقلاب دیجیتالی، تشدید نماید. جامعه بین المللی باید درباره شرایطی که باعث ایجاد یک مشارکت دیجیتالی در سطح بین الملل و مبتنی بر نگاه عمومی به توسعه همکاری مشترک می شود اطمینان حاصل نماید.

برگزاری اجلاس سران درباره جامعه اطلاعاتی در دو مرحله در ژنو (به عنوان نماینده کشورهای توسعه یافته (شمال)) و تونس (به عنوان کشورهای در حال توسعه و کمتر توسعه یافته (جنوب)) حاوی این پیام بود که این اجلاس خواهان ایجاد پلی بین سطوح مختلف توسعه و واقعیت های مختلف دیجیتالی می باشد.

اسناد خروجی اجلاس سران در این دو مرحله، مخصوصاً اجلاس تونس، حد اعلاای فرایند مقدماتی بود که در آن تمامی کشورهای عضو با نگاهی به حصول نتایج واقعی در راستای منافع تمامی مردم دنیا درگیر بودند.

من از این فرصت استفاده می نمایم تا قدردانی تونس از تمامی مشارکت کنندگان فعال در طول این اجلاس را به خاطر تلاش های وافرشان در رسیدن به اجماع درباره مجموعه ای از اهداف مشترکمان تکرار نمایم.

همچنین اجازه دهید که من نقش مهمی که اتحادیه بین‌المللی مخابرات و دبیرکل این اتحادیه، آقای یوشیو اوتسومی^۱ در امور مربوط به سازمان‌دهی این اجلاس ایفا نمودند تقدیر نمایم. مرحله دوم اجلاس سران این امکان را فراهم آورد که چالش‌های پیش‌رو مشخص گردد و مجموعه‌ای از نتایج در خصوص اجرا و پیگیری توسط ذی‌نفعان از جمله دولت‌ها، سازمان‌های بین‌المللی و سازمان‌های بین‌دولتی، جامعه مدنی و بخش خصوصی حاصل گردد.

سال ۲۰۱۵ که برای حصول اهداف توسعه هزاره تعیین گردیده است، به‌عنوان تاریخ مرجع جهت بررسی اجرای کلی نتایج اجلاس سران درباره جامعه اطلاعاتی تصویب شده است. تعهدات تونس بیانگر سیاستی است جهت اجرای تعهدات تعیین شده در طول این دو اجلاس توسط جامعه بین‌المللی. این تعهدات در خصوص رفع شکاف دیجیتالی و ایجاد یک جامعه اطلاعاتی توسعه‌محور و متعادل می‌باشد.

دستور کار تونس سه حوزه اصلی را تحت پوشش قرار می‌دهد:

- ✓ سازوکار مالی برای رفع شکاف دیجیتال؛
- ✓ حکمرانی اینترنت؛
- ✓ اجرا و پیگیری خروجی اجلاس سران.

ما در حال حاضر در مرحله بعد از اجلاس تونس قرار داریم و تمامی ذی‌نفعان از جمله دولت‌ها، سازمان‌های بین‌المللی و بین‌دولتی، جامعه مدنی و بخش خصوصی، باید برحسب اولویت‌ها و حوزه‌های مورد علاقه (مورد منفعت) خود، در خصوص همکاری مؤثر جهت اجرای نتایج اجلاس سران در هر دو مرحله، {در چارچوب} تعهدات خود رفتار نمایند. این تعهدات در زمینه آگاهی بین‌المللی در رابطه با ایجاد جامعه اطلاعاتی متعادل، هماهنگ و یکپارچه تر می‌باشد. با پشتیبانی بسیاری از کشورهای عضو، کشور من مبتکر ارائه پیش‌نویس قطعنامه‌ای به شماره A/60/L.50 به مجمع عمومی می‌باشد که امروز من متعهد به شرح آن هستم.

قطعنامه حاضر با عنوان «اجلاس سران درباره جامعه اطلاعاتی»، نتیجه مشاوره با کشورهای می‌باشد: آفریقای جنوبی به نمایندگی از گروه ۷۷، سوئد، چین، ترکیه، بلاروس، نروژ و کانادا نیز به

است هم بانیان این قطعنامه پیوستند. که این مشاوره‌های گسترده به صورت اجماع و مشارکت سازنده رخ داد.

من دوست دارم از این فرصت جهت بیان قدردانی از تمامی نمایندگان استفاده نمایم این قدردانی به خاطر علاقه‌مندی آن‌ها در نهایی سازی پیش‌نویس قطعنامه در یک دوره زمانی کوتاه می‌باشد. پیش‌نویس این قطعنامه خواستار:

✓ اجرا و پیگیری نتایج هر دو مرحله اجلاس سران (ژنو و تونس) توسط تمامی بازیگران مرتبط از جمله دولت‌ها، سازمان‌های بین‌المللی و بین دولتی، نمایندگان بخش خصوصی و جامعه مدنی می‌باشد؛

✓ از شورای اقتصادی اجتماعی درخواست می‌نماید تا مدیریت پیگیری نتایج مراحل اجلاس سران درباره جامعه اطلاعاتی در ژنو و تونس را به عهده بگیرد. و در اجلاس محتوایی خود در سال ۲۰۰۶، تعهدات، دستور کار و ترکیب کمیسیون علم و فناوری برای توسعه را بررسی نماید؛
✓ و در آخر از مجمع عمومی می‌خواهد تا بازنگری کلی در سال ۲۰۱۵ در باره اجرای نتایج اجلاس سران را انجام دهد و نیز تاریخ ۱۷ می را به‌عنوان روز جهانی جامعه اطلاعاتی اعلام نماید. من، از طرف هیئت نمایندگان تونس و سایر هم‌بانیان این پیش‌نویس، امیدوارم که پیش‌نویس این قطعنامه از پشتیبانی مجمع عمومی به شکل اجماعی بهره‌مند گردد. در این صورت {این پشتیبانی} نه تنها ممکن است که نتایج اجلاس سران را مستحکم نماید بلکه بارقه‌های نور در مینیاپولیس^۱ را زنده نگه می‌دارد. {نشست سران اتحادیه جهانی مخابرات در این پشتیبانی} مسیری که انسان در آینده در ارتباط با انقلاب دیجیتالی طی خواهد کرد و ما در حال حاضر شاهد آن هستیم را روشن خواهد کرد.

مبحث چهارم عملکرد کنفرانس توسعه و تجارت ملل متحد (آنکتاد)

گفتار یک: آنکتاد و فضای سایبر

کنفرانس تجارت و توسعه سازمان ملل متحد با علامت اختصاری آنکتاد^۱ در سال ۱۹۶۴ میلادی با هدف پیوستن کشورهای در حال توسعه به اقتصاد جهانی تأسیس گردید. در ابتدا این نهاد از سوی ۷۷ کشور کمتر توسعه یافته (گروه ۷۷) با هدف تحت فشار قرار دادن کشورهای توسعه یافته جهت آزادسازی بیشتر تجارت تشکیل شد. سال ها بعد آنکتاد بر مبنای قطعنامه مجمع عمومی تأسیس گردیده است. هدف اصلی آنکتاد کمک در راستای برگزاری مباحث توسعه می باشد و تأکید آن بر همگرایی سیاست های داخلی و اقدامات بین المللی می باشد.

به گفته برخی کارشناسان داخلی و خارجی آنکتاد تنها محفل بین المللی اقتصادی می باشد که برخلاف صندوق بین المللی پول، بانک جهانی و مؤسسات مالی منطقه ای، کشورهای صنعتی در آن در اقلیت محض قرار دارند. به همین دلیل موضع گیری های آنکتاد و کلیه مسائل مربوط به کمیته های آن عمدتاً به سود کشورهای در حال توسعه و کمتر توسعه یافته می باشد.

در ادامه در خصوص عملکرد کنفرانس تجارت و توسعه ملل متحد (آنکتاد) در حوزه فضای سایبر باید گفت: فناوری های اطلاعات و ارتباطات نقش مهم و فزاینده ای در اجرای دستور کار سند توسعه پایدار ایفا می نمایند. اقدامات مرتبط با اقتصاد و تجارت دیجیتال رابطه مستقیمی با برخی اهداف سند توسعه پایدار دارند از جمله:

✓ هدف 5b: تجارت الکترونیک و کاربردهای مختلف دیجیتال می تواند به عنوان اهرمی جهت ارتقای توانمندی زنان کارآفرین و شاغل به کار گرفته شود؛

✓ هدف 8.3: آن ها می توانند فعالیت های تولیدی، اشتغال زایی، کارآفرینی، خلاقیت و نوآوری را حمایت کنند و تشکل های اقتصادی بسیار کوچک، کوچک و متوسط را از طریق دسترسی به خدمات مالی که توسط فناوری اطلاعات و ارتباطات توانمند شده اند، تقویت کنند و سبب

1. UNCTAD (United Nations Conference for Trade and Development)

2. E-commerce and various digital applications can be leveraged to promote the empowerment of women as entrepreneurs and traders (Goal 5.b).

رسمیت یافتن و رشد فعالیت آن‌ها شوند؛

✓ هدف ۹،۳: راه‌حل‌های دیجیتالی می‌توانند به‌عنوان اهرمی جهت افزایش دسترسی تشکیلات اقتصادی موجود در کشورهای در حال توسعه به خدمات مالی و بازارها و یکپارچگی آن‌ها در زنجیره‌های ارزشی^۲ گردند.

علاوه بر این، تجارت الکترونیک اهمیت فزاینده‌ای در دستیابی به هدف ۱۷،۱۱ این سند و به‌طور ویژه در افزایش صادرات کشورهای در حال توسعه و همچنین افزایش دوبرابری سهم کشورهای کمتر توسعه‌یافته در صادرات جهانی تا سال ۲۰۲۰^۳ خواهد داشت. فرصت‌های ناشی از تجارت الکترونیکی برای کشورهای در حال توسعه شامل موارد زیر می‌باشد:

- کاهش هزینه‌های معاملات و دسترسی بهتر به مشتری‌های بومی و فرامرزی؛
 - مشارکت در زنجیره‌های قیمت جهانی^۴، بهره‌وری ارتقای یافته^۵؛
 - کارآفرینی، ابتکار و ایجاد شغل در بخش دیجیتال؛
 - برقراری امکاناتی برای اتصال بازارهای روستایی و شهری، منفعت برای مشتریان؛
 - راه‌جدیدی جهت فائق آمدن بر موانع توسعه کسب‌وکار.
- چالش‌ها و موانعی نیز پیش‌روی کشورهای در حال توسعه می‌باشد و این چالش‌ها به‌طور ویژه برای تشکیلات اقتصادی کوچک و متوسط شدیدتر است به‌طوری‌جهت پشتیبانی در ظرفیت‌سازی برای غلبه بر این چالش‌ها، نیاز به مساعدت جامعی می‌باشد و در این رابطه تجارت الکترونیک باید نقش مهمی را ایفا نماید. این چالش‌ها شامل موارد زیر می‌باشد:
- عدم کفایت فناوری‌های اطلاعات و ارتباطات و زیرساخت‌های صنعتی؛
 - محدودیت دسترسی به انرژی، پرهزینه و غیرقابل اعتماد بودن منبع تغذیه و همچنین محدودیت اعتبار؛
 - فقدان راه‌حل‌های پرداختی مناسب و تحدید دسترسی به فناوری، فقدان قدرت خرید؛

1. They can support productive activities, decent job creation, entrepreneurship, creativity and innovation, and encourage the formalization and growth of micro, small and medium-sized enterprises, including through access to ICT-enabled financial services (Goal 8.3).

2. Value chine

طیف کاملی از فعالیتها شامل مراحل طراحی، تولید، بازاریابی و توزیع را در بر می‌گیرد که کسب‌وکارها برای تبدیل محصول یا خدمات از طرح تا تحویل به مشتری آن را طی می‌کنند.

3. Moreover, e-commerce will become increasingly important in achieving Goal 17.11, to significantly increase the exports of developing countries and double the share of global exports of the least developed countries (LDCs) by 2020.

4. global value chains,

5. enhanced productivity

سیستم های مالی توسعه نیافت؛

- نگرانی بابت از دست دادن شغل به علت رشد جمعیت و همچنین ماشینی و اتوماتیک شدن بسیاری از مشاغل؛

- از بین رفتن تعادل تجاری و بازرگانی و خطر سلطه و نفوذ برخی تجارتخانه ها در بازار؛
- کم شدن سود سهام؛

- افزایش شکاف های دیجیتالی از جمله در اقتصاد دیجیتال؛

- عدم کفایت و بسندگی چارچوب های تنظیم مقررات و قانون و اتکا به پول نقد در جامعه؛

- پایین بودن سطح سواد فناوری اطلاعات و ارتباطات و آگاهی و دانش مربوط به تجارت

الکترونیکی میان مشتریان، تشکیلات اقتصادی و دولت ها.

گفتار دو: گروه کارشناسان بین دولتی درباره تجارت الکترونیک و اقتصاد دیجیتال - سال ۲۰۱۷

وفق زیر بندهای (I) ۱۰۰ و S از سند نایروبی، شورای تجارت و توسعه^۱، دو گروه کارشناسان با موضوعات تجارت الکترونیکی و اقتصاد دیجیتال^۲ و سرمایه گذاری برای توسعه را تشکیل داد. شورای تجارت و توسعه در سی و یکمین اجلاس ویژه خود که در تاریخ ۵ آوریل ۲۰۱۷ در ژنو برگزار گردید - مطابق دستورکار شماره ۵ این اجلاس - شرح وظایفی^۳ را برای هر دو گروه کارشناسان بین دولتی به تصویب رساند.^۴ به طوری جهت شناسایی مسیرها و اقدامات لازم برای ارتقای منافع توسعه از طریق اقتصاد دیجیتال، خط مشی گروه کارشناسان بین دولتی درباره تجارت الکترونیکی و اقتصاد دیجیتالی، بر تقویت ابعاد توسعه تجارت الکترونیک و اقتصاد دیجیتالی متمرکز گردید. مباحث مطرح در جلسات این گروه، در خصوص امکان بروز فرصت های ناشی از تجارت الکترونیک و اقتصاد دیجیتال و نیز چگونگی رویارویی و برخورد با خطرها و چالش های مرتبط می باشد.

1. Trade and Development Board (TDB)

2. Intergovernmental Group of Experts on E-commerce and the Digital Economy

3. terms of reference

4. TD/B(S-XXXI)/2, Report of the Trade and Development Board on its thirty-first special session, 26 May 2017

می توان گفت گروه کارشناسان بین دولتی، فرصتی را برای تقویت مساعدت فنی آنکتاد در امر تحقیق و تحلیل فراهم می نماید. این گروه، مجمعی از سیاست گذاران اقتصاد دیجیتال را بین کشورهای در حال توسعه و کشورهای توسعه یافته ایجاد نمود که مرکزی جهت اشتراک گذاری تجربیات میان سیاست گذاران و سایر ذی نفعان در این چارچوب می باشد. بحث در مورد نتایج حاصل از بررسی خط مشی فناوری اطلاعات و ارتباطات ملی داده های باارزشی خواهند بود. همچنین در این اجلاس ملاحظات سازمانی خاصی در خصوص تشکیل گروه کارشناسان بین دولتی تصویب گردید در این ملاحظات سازمانی قید گردیده است که گروه کارشناسان بین دولتی درباره تجارت الکترونیک و اقتصاد دیجیتال به صورت سالانه مقارن با هفته تجارت الکترونیکی کنفرانس تجارت و توسعه ملل متحد (آنکتاد) و با حضور شرکت کنندگانی از بخش های دولتی، جامعه مدنی، بخش خصوصی و دانشگاهی که دارای تجربیات مناسب و مرتبط با موضوعات ویژه و خاص برگزار می شود. پیشنهاد می شود که گروه کارشناسان بین دولتی، رویه ها و روش های استاندارد کاری را برای نشست های بین دولتی در آنکتاد دنبال نماید. گروه کارشناسان درباره الگوها و اشکال عملکردی و سازمانی مناسب تصمیم گیری خواهد نمود. با هدف تأثیر و مشارکت حداکثری در بررسی های گروه، لازم است ترتیباتی جهت مشارکت از راه دور برای نشست های مکمل اتخاذ گردد. هدایت و کنترل بخش ارائه کننده خدمات گروه کارشناسان (بخش فناوری و تدارکاتی)، مطابق با قواعد رویه شورای تجارت و توسعه، توسط دفتر دبیر کل آنکتاد و با هماهنگی سایر بخش های مربوط در آنکتاد، پایش می شود. مستندسازی برای هر یک از نشست های گروه کارشناسی بین دولتی شامل مجموعه ای از اسناد زیر خواهد بود:

۱. دستور کار مقدماتی ۲. یادداشت های موضوعی ۱:

یادداشت های موضوعی که قبل از هر اجلاس سالانه تولید خواهند شد باید {شامل} چکیده ای از موضوعات کلیدی باشد که بتواند پاسخگوی سؤالات روشنگری باشد که برای هر اجلاس مطرح می گردد. این یادداشت های موضوعی که توسط کارشناسان مورد تحقیق و بررسی قرار می گیرد باید شامل حداکثر ۱ یادداشت برای هر بخش محتوایی دستور کار باشد.

- گزارش اجلاس: تا سال ۲۰۱۹ تعداد سه اجلاس گروه کارشناسان بین دولتی درباره تجارت الکترونیکی و اقتصاد دیجیتال در ژنو به تاریخ های زیر تشکیل و گزارش آن به شورای تجارت و توسعه ارائه گردیده است:

۱. اجلاس اول مورخ ۴ تا ۶ اکتبر ۲۰۱۷ ، ۲. اجلاس دوم مورخ ۱۸ تا ۲۰ آوریل ۲۰۱۸ ۳. اجلاس سوم مورخ ۳ تا ۵ آوریل ۲۰۱۹. در بخش شماره ۳ دستور کار موقت اجلاس اول گروه کارشناسان بین دولتی درباره تجارت الکترونیکی و اقتصاد دیجیتال با عنوان «بحث درباره ابعاد توسعه تجارت الکترونیکی و اقتصاد دیجیتال، پرداختن به فرصت ها و چالش های مرتبط» که مورخ ۲۶ جولای ۲۰۱۷ توسط کنفرانس تجارت و توسعه ملل متحد منتشر گردید^۱، گروه کارشناسان بین دولتی پنج میزگرد مباحثه ای در موضوعات زیر برگزار نمودند:

✓ مفاهیم توسعه در اقتصاد دیجیتال^۲

✓ مزایای ایجاد رقابت از طریق تجارت الکترونیک و اقتصاد دیجیتال در کشورهای در حال توسعه^۳

✓ تقویت زیرساخت های فنی و فیزیکی در کشورهای در حال توسعه^۴

✓ مشارکت های مؤثر بین کشورهای توسعه یافته و در حال توسعه جهت حداکثر نمودن

فرصت ها و مقابله با چالش های مرتبط با تجارت الکترونیک و اقتصاد دیجیتال^۵

✓ مسیر بعدی (تعیین برنامه کاری اجلاس بعدی گروه کارشناسان)

یکی از توصیه های مورد توافق در اولین اجلاس گروه کارشناسان بین دولتی درباره تجارت

الکترونیکی و اقتصاد دیجیتالی^۶ تأسیس گروه کاری درباره اقدامات تجارت الکترونیکی و اقتصاد دیجیتالی بود. مخصوصاً توصیه های شماره ۱۱ و ۱۲ این سند.

1. TD/B/EDE/1/1

2. Development implications of the digital economy

3. Building competitive advantages through e-commerce and the digital economy in developing countries

4. Strengthening physical and technology infrastructure in developing countries

5. Impactful partnerships between developed and developing countries to maximize opportunities and address challenges relating to e-commerce and the digital economy

6. (TD/B/EDE/1/3)

گفتار سه: خلاصه‌ای از وضعیت قوانین تصویب شده در ۱۹۳ کشور عضو آنکتاد درباره تجارت الکترونیک

در ماده دو گزارش اولین اجلاس گروه کارشناسان بین دولتی به ابزارهای توسعه یافته توسط آنکتاد مانند شاخص تجارت الکترونیکی کسب و کار با مصرف کننده ، بازنگری های خط مشی فناوری اطلاعات و ارتباطات، {سامانه} پیگیری قوانین سایبری در جهان^۱، اشاره گردید که به معرفی اجمالی این دو ابزار پرداخته می شود؛

در خصوص سامانه پیگیری قانون سایبری جهانی آنکتاد^(۱) اولین نقشه جهانی در خصوص قوانین سایبری می باشد. این سامانه وضع قانونگذاری ۱۹۳ کشور عضو آنکتاد را در خصوص تجارت الکترونیک در چهار حوزه زیر دنبال می کند. خلاصه‌ای از وضعیت قانونگذاری در این چهار حوزه در دو جدول درج گردیده است؛

✓ تراکنش (معامله) الکترونیکی^۲؛

✓ حمایت از مشتری (مصرف کننده)^۳؛

✓ حفاظت از داده ها / حریم خصوصی^۴؛

✓ جرائم سایبری؛

وضعیت وجود قوانین در چهار حوزه مختلف تجارت الکترونیکی در کشورهای عضو آنکتاد	
حوزه	درصد کشورها
قوانین در زمینه معاملات الکترونیکی	۷۹
قوانین در زمینه حمایت از مصرف کننده	۵۲
قوانین در زمینه حفاظت از داده ها و حریم خصوصی	۵۸
قوانین در زمینه جرائم سایبری	۷۲

1. Global Cyber law Tracker
 2. e-transactions
 3. , consumer protection
 4. data protection/privacy

وضعیت کشورهای عضو آنکتاد درباره تدوین قانون در هر یک از چهار حوزه تجارت الکترونیک		
حوزه	وضعیت تدوین قانون	درصد کشورها
قوانین در زمینه معاملات الکترونیکی	قانون تدوین شده	۷۹
	قانون در حد پیش نویس	۹
	فاقد قانون	۵
	اطلاعاتی موجود نیست	۷
قوانین در زمینه حمایت از مصرف کننده	قانون تدوین شده	۵۲
	قانون در حد پیش نویس	۶
	فاقد قانون	۱۰
	اطلاعاتی موجود نیست	۳۲
قوانین در زمینه حفاظت از داده ها و حریم خصوصی	قانون تدوین شده	۵۸
	قانون در حد پیش نویس	۱۰
	فاقد قانون	۲۱
	اطلاعاتی موجود نیست	۱۲
قوانین در زمینه جرائم سایبری	قانون تدوین شده	۷۲
	قانون در حد پیش نویس	۹
	فاقد قانون	۱۸
	اطلاعاتی موجود نیست	۱

آخرین شاخص تجارت الکترونیکی کسبوکار به مشتری که در سال ۲۰۱۸ توسط آنکتاد منتشر گردیده است به رتبه بندی ۱۵۱ کشور جهان در خصوص آمادگی و ظرفیت آن‌ها جهت پشتیبانی از تجارت برخط بر اساس چهار عامل می‌باشد که هر یک از این چهار عامل دارای وزن برابر در محاسبات می‌باشند. شایان ذکر است که این رتبه‌بندی بر اساس آخرین داده‌های موجود در سال ۲۰۱۷ انجام گرفته است.

گفتار چهار: کار گروه اقدام تجارت الکترونیکی و اقتصاد دیجیتال

در ماده ۱۱ و ۱۲ گزارش اولین اجلاس گروه کارشناسان بین دولتی در زمینه تجارت الکترونیک و اقتصاد دیجیتال به نکاتی در خصوص تشکیل گروه کاری درباره اقدامات تجارت الکترونیکی و اقتصاد دیجیتالی اشاره گردیده است.

در بخش ۴ دستور کار موقت دومین اجلاس گروه کارشناسان بین دولتی درباره تجارت الکترونیکی و اقتصاد دیجیتال با عنوان «گروه کاری درباره اقدامات تجارت الکترونیک و اقتصاد دیجیتال» مورخ ۲۱ فوریه ۲۰۱۸ عنوان گردید که^۱: گروه کارشناسان بین دولتی درباره تجارت الکترونیک و اقتصاد دیجیتالی، با نگاهی بر ضرورت ارتقای دسترسی به آمار رسمی در خصوص تجارت الکترونیکی و اقتصاد دیجیتالی، مخصوصاً آمار مربوط به کشورهای در حال توسعه، جهت پشتیبانی از سیاست‌گذاری‌های مبتنی بر سند و مدرک^۲:

۱. به شورای تجارت و توسعه توصیه می‌نماید که گروه کارشناسانی را در خصوص اقدامات تجارت الکترونیکی و اقتصاد دیجیتالی همان‌گونه که در سند TD/B/EDE/2/3 شرح داده شده است ایجاد نمایند؛

۲. درخواست می‌نماید که دبیرخانه آنکتاد شرح وظایفی را بر مبنای اطلاعات مندرج در سند TD/B/EDE/2/3 برای گروه کاری جدید آماده نماید، همچنین درخواست می‌نماید تا دبیرخانه آنکتاد شفاف‌سازی نماید که هدف، مشارکت و پیشرفت همکاری در اقدامات تجارت الکترونیک و اقتصاد دیجیتال می‌باشد و اینکه این هدف از تکرار (موازی کاری) با سایر عملکردهای مربوط و در جریان اجتناب می‌نماید؛

بخش ۴ دستور کار موقت سومین اجلاس گروه کارشناسان بین دولتی درباره تجارت الکترونیکی و اقتصاد دیجیتال با عنوان «گروه کاری درباره اقدامات تجارت الکترونیک و اقتصاد دیجیتال» سند حاضر طرح کلی از شرح وظایف مورد درخواست برای گروه کاری درباره اقدامات تجارت الکترونیکی و اقتصاد دیجیتالی (که از این پس تحت عنوان گروه کاری خوانده می‌شود) ارائه می‌دهد.^۳

1. (TD/B/EDE/2/1)
3. TD/B/EDE/2/3

2. evidence-based policymaking

این طرح طبق بخش چهار دستور کار موقت دومین اجلاس گروه کارشناسی بین دولتی درباره‌ی تجارت الکترونیکی و اقتصاد دیجیتال ارائه گردید.

✓ هدف گروه کاری: هدف تشکیل گروه کاری، مشارکت و پیشرفت همکاری درباره اقدامات مربوط به:

- تجارت الکترونیک و اقتصاد دیجیتال؛

- ارتقای دسترسی، کیفیت، قابلیت قیاس، قابلیت استفاده و ارتباط آماری در باب تجارت

الکترونیکی و اقتصاد دیجیتال؛

- و با نگاهی به پشتیبانی از سیاست‌گذاری‌های مستند محور مخصوصاً در کشورهای در حال

توسعه گروه کاری باید از کارهایی که موازی با سایر کارهای مربوط و در حال جریان می‌باشد اجتناب نماید.

✓ شرکت‌کنندگان در گروه کاری به منظور حصول اطمینان از اینکه:

- عملکرد گروه کاری منتج از نیازهای کشورهای عضو می‌باشد؛

- گروه کاری در ارتقای همکاری درباره اقدامات مربوط به تجارت الکترونیک و اقتصاد

دیجیتال اثربخش می‌باشد؛

- گروه کاری از موازی کاری با سایر کارهای مرتبط و در جریان اجتناب می‌نماید.

این گروه از مشارکت گروه‌های زیر استقبال خواهد نمود:

- نمایندگان دولتی، با تخصص‌های مرتبط (به‌عنوان مثال نمایندگانی از دفترهای آمار ملی،

وزارتخانه‌های دولتی)

سازمان‌های بین‌المللی مرتبط که باید جهت مشارکت دعوت گردند از جمله سازمان بین‌المللی

کار^۱، صندوق بین‌المللی پول^۲، اتحادیه بین‌المللی مخابرات، سازمان توسعه و همکاری اقتصادی^۳،

دفتر همکاری جنوبگان سازمان ملل متحد^۴، کمیسیون‌های منطقه‌ای سازمان ملل متحد، بخش

آمار سازمان ملل متحد^۵، سازمان جهانی گمرک^۶، بانک جهانی و سازمان تجارت جهانی^۷

1. international labour organization (ILO)
 2. International Monetary Fund (IMF)
 3. Organization for Economic Cooperation and Development (OECD)
 4. United nations office for south- south cooperation(UNOSSC)
 5. United nations statistis division (UNSD)
 6. World customs organization (WCO)
 7. World Trade Organization(WTO)

- سازمان‌های تخصصی مربوط و شبکه‌های تحقیقاتی، مرکز تحقیقات فناوری اطلاعات و ارتباطات آفریقا؛

- متخصصان از جامعه مدنی، بخش خصوصی و دانشگاهی در صورت مقتضی ممکن است جهت اهداف مستشاری و مطابق با موضوعات ویژه‌ای دعوت شوند.

✓ فعالیت‌ها: گروه کاری باید مجمعی را تشکیل دهد که از تبادل تجربیات و همکاری‌های مؤسسه‌ای^۱ میان مشارکت‌کنندگان خود پشتیبانی نماید؛

- توسعه‌های جدید مربوط در حوزه آماری (مانند تولیدات آماری از طریق روش‌های نوآورانه، استفاده از فناوری‌ها و منابع جدید) را به نمایش گذارد؛

- دولت‌های عضو را جهت تولید آمارهای مربوط و در صورت نیاز ارائه توصیه‌هایی در باب انتشار آن‌ها تشویق نماید؛

- تعاریف آماری، روش‌های شناختی و خطوط راهنمای مربوط و در صورت ضرورت ارائه و پیشنهاد روش‌ها، تعاریف و خطوط راهنمای جدید را بررسی نماید؛

- نواحی و حوزه‌هایی که اصلاحات روش شناختی باید در آن به کار گرفته شود را شناسایی نماید.^۲

- در خصوص مسیرهای جدید جهت همکاری‌های جنوبگان^۳ از جمله در زمینه اشتراک‌گذاری دانش و دروس آموخته شده درباره اقدامات تجارت الکترونیکی و اقتصاد دیجیتال تحقیق نماید؛

- در قبال فعالیت‌های آتی در باب اقدامات مربوط به تجارت الکترونیکی و اقتصاد دیجیتالی مطابق آنچه گروه کارشناسان بین‌دولتی درخواست می‌نماید متعهد می‌باشند؛

✓ ملاحظات سازمان:

➤ تکرار پذیری، زمانبندی و تنظیم طول مدت^۴:

- گروه کاری سالی یک بار به مدت ۲ الی ۳ روز گردهم جمع خواهند شد، شروع این گردهمایی در پاییز سال ۲۰۱۹ خواهد بود. زمان مناسب جهت ارائه گزارش این گروه کاری به گروه کارشناسان بین‌دولتی، در نشست بعدی گروه کارشناسان بین‌دولتی در پاییز هر سال

1. Institutional cooperation
2. Identifies areas where methodological improvement should be undertaken
3. South-South cooperation
4. Frequency, length and timing

- ماه مارس و آوریل - خواهد بود.^۱

- جهت مشارکت حداکثری کارشناسان کشورهای در حال توسعه، باید به خاطر سپرد که در صورت امکان تاریخ‌های این گروه کاری مقارن با زمان‌بندی سایر نشست‌های اماری مرتبط انتخاب خواهد شد مخصوصاً متناسب با زمان‌بندی: گروه کار OECD درباره اقدامات و تحلیل اقتصاد دیجیتال^۲، نشست‌های گروه کارشناسان اتحادیه بین‌المللی مخابرات درباره شاخص‌های خانواده فناوری اطلاعات و ارتباطات^۳، گروه کارشناسی درباره شاخص‌های مخابرات؛
- فناوری‌های اطلاعات و ارتباطات^۴.

✓ مستند سازی: مستندسازی برای هر یک از نشست‌های گروه کاری شامل مجموعه‌ای از اسناد زیر خواهد بود که توسط دبیرخانه آماده می‌شود:
- دستور کار مقدماتی،

- یادداشت‌های موضوعی^۵: یادداشت‌های موضوعی که قبل از هر اجلاس سالانه تولید خواهند شد باید {شامل} اختصاری از موضوعات کلیدی باشد که بتواند پاسخگوی سؤالات راهنمایی باشد که برای هر اجلاس مطرح می‌شود. این یادداشت‌های موضوعی که توسط کارشناسان مورد تحقیق و بررسی قرار گیرد باید شامل حداکثر ۱ یادداشت برای هر بخش محتوایی دستور کار باشد.
- گزارش اجلاس.

✓ فرم عملکرد و ارائه خدمات گروه کاری:

از هر یک از کشور عضو درخواست می‌گردد تا یک {نهادی} را به عنوان نقطه تماس جهت ارتباط با دبیرخانه معرفی نماید (برای مثال، اداره ملی آمار یا هر یک از وزارتخانه‌هایی که پاسخگوی ارائه آمارهای مرتبط با تجارت الکترونیک و اقتصاد دیجیتال می‌باشد). دبیرخانه باید به طور مسقیم با این نقاط مرکزی در خصوص با مشارکت در گروه کاری و عملکرد آن ارتباط پیدا نماید. برنامه عملکرد هر اجلاس از گروه کاری توسط رئیس گروه کارشناسان بین‌دولتی^۶ تعیین خواهد شد گروه کارشناسان بین‌دولتی سابقاً وظیفه‌ای را به گروه کاری، ارجاع داده است. دبیرخانه باید برای

۱. تاریخ مقارن با هفته تجارت الکترونیک در آنکتاد

2. Working Party on Measurement and Analysis in the Digital Economy (WP-MADE),

3. ICT Household Indicators (EGH)

4. Expert Group on Telecommunication/ICT Indicators (EGTI)

5. issues notes

6. preceding IGE

تقویت بررسی {موضوعات} در گروه کاری و نیز شناسایی کارشناسانی که ممکن است {به واسطه} دانش‌های مکملی در بررسی این موضوعات اثربخشی داشته باشند، یادداشت موضوعاتی را آماده سازد. در شروع هر نشست، گروه کاری یک رئیس و یک نایب رئیس را برای آن نشست انتخاب خواهد نمود. گروه کاری در خصوص شکل سازمانی و شیوه عملکرد مناسب و نیازهای بعد از آن، در اولین نشست خود تصمیم‌گیری خواهد نمود.

گروه کاری موارد زیر را به منظور حصول اطمینان از هماهنگی فعالیت‌های خود با سایر سازمان‌ها و اجتناب از تلاش‌های تکراری (موازی کاری) مورد بررسی قرار خواهد داد: برنامه کاری خود، هر گونه موفقیت و مشکلاتی که در نشست پیشین با آن مواجه شده بود و سایر فعالیت‌های بین‌المللی مرتبط. گروه کاری جهت ارائه توصیه و پیشنهادهایی در خصوص ملاحظات مورد نظر گروه کارشناسان بین‌دولتی در نشست بعدی آن گروه، تلاش خواهد کرد. این توصیه و پیشنهادهای باید بر روی وظایف و تکالیفی متمرکز باشد که گروه کاری توسط گروه کارشناسان بین‌دولتی به آن مأمور گردیده است. اما ممکن است این توصیه و پیشنهادهای عندالاقضاء حاوی جنبه‌های دیگری از اقدامات تجارت الکترونیکی و اقتصاد دیجیتال از جمله پیشنهادهایی برای موضوعاتی که می‌تواند در نشست‌های آینده گروه کاری مورد نظر قرار گیرد، باشد.

نشست‌های گروه کاری به طور مشترک توسط بخش‌های زیر و از طریق پشتیبانی و حمایت تدارکاتی و آماده‌سازی مستندات مرتبط کمک خواهد شد. بخش‌های فناوری و لجستیک (تدارکاتی) و بخش‌های راهبردی توسعه و جهانی‌سازی کمک خواهد شد.

خروجی‌ها:

خروجی هر نشست گروه کاری باید شامل پیشنهادهای و توصیه‌های زیر به گروه کارشناسان بین‌دولتی باشد:

- پیشنهادهای و توصیه‌ها برای ملاحظات مورد نظر و موضوعات شناسایی شده توسط گروه کارشناسان بین‌دولتی.

مبحث پنجم

مؤسسه تحقیقات خلع سلاح ملل متحد (یونیدیر)

گفتار یک: یونیدیر و فضای سایبر

امروزه ما شاهد رشد کاربردهای فضای سایبری در فعالیت‌های دولت‌ها، برنامه ریزی‌های نظامی و عملیاتی، فرایندهای مرتبط با زیرساخت‌های صنعتی و مدنی و نظام‌های مالی هستیم. این امر همان‌طور که می‌تواند به‌عنوان یک فرصت تلقی گردد می‌تواند به‌طور همزمان، خطرهای فزاینده‌ای را برای دولت‌ها، بخش‌های نظامی و کسب‌وکارها ایجاد نماید.

جهت حصول منافع حداکثری برای یک جهان به هم پیوسته که از طریق فضای سایبری ایجاد شده است، دولت‌ها و سایر ذی‌نفعان جهت مدیریت و استفاده از ابزار سایبری، در جستجوی انجام بحث و مذاکراتی در یک رویکرد متقابل، پایدار و هماهنگ می‌باشند.

مؤسسه تحقیقاتی خلع سلاح ملل متحد^۱ که پس از این، تحت عنوان یونیدیر معرفی می‌گردد، به‌عنوان یک مؤسسه مستقل در چارچوب سازمان ملل متحد، تحقیقاتی را در باب موضوعات خلع سلاح و امنیت انجام می‌دهد. مرکز این مؤسسه در شهر ژنو واقع است و در حقیقت مرکزی برای مذاکرات دوجانبه و چندجانبه در خصوص خلع سلاح و عدم اشاعه می‌باشد. این مؤسسه موضوعات جاری مختلف در خصوص وضعیت فعلی و آینده سلاح‌ها و نیز دیپلماسی جهانی و تنش‌ها و مخاصمات محلی را بررسی می‌کند. این مؤسسه با هدف همکاری با محققان، دیپلمات‌ها، دفترهای دولتی، سازمان‌های مردم‌نهاد و سایر مؤسسات کار خود را از سال ۱۹۸۰ آغاز نمود. در اصل می‌توان عنوان کرد که عملکرد یونیدیر پلی است بین جامعه محققان و دولت‌ها. اقدامات این مؤسسه توسط دولت‌ها و سایر داوطلبان تأمین مالی می‌گردد. این مؤسسه فعالیت‌های سایبری خود را در راستای اهداف زیر انجام می‌دهد:

- ظرفیت‌سازی متمرکز بر سیاستگذاری‌ها^۲ در سطوح ملی، منطقه‌ای و چندجانبه، تحقیق و تحلیل، آگاه‌سازی در خصوص نوآوری‌های مرتبط با سایبر جهت تضمین رشد و توسعه پایدار

1. United Nations Institute for Disarmament Research (UNIDIR)
2. policy-focused capacity-building

برای موضوع سایبری.

پروژه‌های در حال جریان در این مؤسسه به چند بخش زیر تقسیم می‌گردد: مجموعه کارگاه‌هایی با موضوعات امنیت بین‌المللی سایبری^۱، مجموع کنفرانس‌های پایداری سایبری^۲ و پشتیبانی از {تشکیل} گروه‌های کارشناسان دولتی سازمان ملل متحد (در فضا و سایبر)، نشست‌های مرتبط با حقوق بین‌الملل و رفتار دولت در فضای سایبر. پروژه‌های خاتمه‌یافته شامل: قابلیت‌های ملی، دکترین، سازمان‌ها و شفاف‌سازی و اعتمادسازی برای امنیت سایبری^۳، چشم‌انداز جنگ سایبری: چارچوب‌های قانونی و شفافیت‌سازی و اعتمادسازی^۴، ابزار شاخص سایبری^۵.

گفتار دو: برگزاری کارگاه‌هایی با موضوعات امنیت بین‌المللی سایبری

پروژه کارگاه‌هایی با موضوعات امنیت بین‌المللی سایبری، چالش‌ها و فرصت‌های فناوری‌های دیجیتال و چگونگی تأثیر آن بر سیاست، امنیت بین‌المللی و نوآوری‌ها را مورد رصد قرار می‌دهد. این کارگاه‌ها در قالب دو فاز در سال ۲۰۱۶ و ۲۰۱۹ برگزار گردیده است.

مجموعه‌ای از کارگاه‌ها با موضوعات امنیت بین‌المللی سایبری (فاز اول)^۶ سال ۲۰۱۶. این فاز در سال ۲۰۱۶ برگزار گردید، حمایت مالی از این کارگاه‌ها از طرف دولت‌های هلند و ایالات متحده آمریکا صورت گرفت. مرکز مطالعات راهبردی بین‌المللی^۷ ایالات متحده آمریکا که برنامه فناوری‌های راهبردی را بر اساس تحلیل مبتنی بر واقعیات و داده‌ها تهیه می‌نماید معتقد است برنامه‌های کاری درباره امنیت سایبری علاوه بر اینکه به شکل‌گیری سیاست‌ها و رویه‌ها در کشورهای سرتاسر جهان کمک می‌کند بلکه می‌تواند به تعریف دستورکار جهانی از جمله در کمیسیون امنیت سایبری منجر شود.

اداره امور خلع سلاح ملل متحد^۸ به‌عنوان دبیر گروه کارشناسان دولتی خدماتی رادر باب اداره امور

1. International Security Cyber Issues Workshop Series
2. Cyber Stability Conference Series
3. National Capabilities, Doctrine, Organization and Building Transparency and Confidence for Cyber Security: An Assessment
4. Perspectives on Cyber War: Legal Frameworks and Transparency and Confidence-Building
5. The Cyber Index Tool
6. International Security Cyber Issues Workshop Series (Phase I)
7. Center for Strategic International Studies (CSIS)
8. UN Office for Disarmament Affairs

به این گروه ارائه می‌نماید. یونیدیر نیز در این امر در تمامی دوره‌های برگزار شده گروه کارشناسان، به‌جز سال ۲۰۰۵، به‌عنوان مشاور جهت هماهنگی مباحث مطرح در گروه، آماده‌سازی پیش‌نویس گزارش‌ها و ارائه آن به رئیس گروه به ارائه خدمات مشغول بوده است. نماینده سطح بالای اداره خلع سلاح^۱ و وظیفه پیشنهاد ترکیب گروه کارشناسان به دبیرکل را دارد. این کار نه تنها با در نظر گرفتن تعادل سیاسی و جغرافیایی انجام می‌گردد بلکه، اقتضائات موضوعی^۲ و تعداد دفعاتی که کشور در سایر گروه‌های کاری حضور داشته است مورد نظر قرار می‌گیرد.

رئیس گروه کارشناسان دولتی از میان اعضای شرکت کننده انتخاب می‌گردد. روسیه در سال‌های ۲۰۰۵ و ۲۰۱۰، استرالیا در سال ۲۰۱۳ و برزیل در سال ۲۰۱۵ ریاست این گروه کارشناسان را به عهده داشته است.

در خصوص کمک به آماده‌سازی گروه کارشناسان دولتی و شناسایی حوزه‌های درک مشترک و واگرایی در موضوعات سایبری، CSIS و یونیدیر سه کارگاه آزاد در خصوص مباحث مرتبط با امنیت بین‌المللی سایبر را با ترکیبی از دیپلمات‌ها، محققان و کارشناسان فنی برگزار کردند. این سه کارگاه در ژنو و به ترتیب زمانی روی موضوعات زیر تمرکز داشت:

کارگاه اول: مورخ ۹ تا ۱۰ فوریه ۲۰۱۶ در خصوص هنجارهای آتی جهت حفظ و ارتقای امنیت سایبری در سطح بین‌المللی^۳ برگزار گردید. کارگاه دوم: مورخ ۱۹ تا ۲۱ آوریل ۲۰۱۶ در خصوص کاربرد حقوق بین‌الملل در چارچوب امنیت بین‌المللی^۴ برگزار گردید. کارگاه سوم: مورخ ۱۵ الی ۱۶ ژوئن ۲۰۱۶ در خصوص مدیریت توسعه ابزار سایبری که می‌تواند جهت مقابله با اهداف غیرقانونی یا اهدافی با سوء نیت استفاده گردد^۵، برگزار گردید.

انتظار می‌رود که در این کارگاه‌ها، ملل غیر غربی^۶ از جمله اعضای گروه ۷۷ و اعضای جنبش عدم تعهد^۷ نقش بیشتری را ایفا نمایند و نظرهای متفاوتی را در باب موضوعات حاکمیت، حقوق بین‌المللی و کنترل تسلیحات در این کارگروه مورد بحث قرار دهند. بیانیه‌های گروه نم در

1. office of the High Representative for Disarmament

2. demonstrated interest in the topic

3. International security cyber issues workshop series: future of norms to preserve and enhance international cyber stability

4. The Application of International Law in the Context of International Cybersecurity

5. Managing the Spread of Cyber Tools that can be used for Malicious or Unlawful Purposes

6. Non-Western nations

7. Non-Aligned Movement(NAM)

مجمع عمومی درخواست می‌نماید برای تشدید تلاش برای «حراست از فضای سایبری جهت جلوگیری از تبدیل آن به یک عرصه مخاصمه»^۱ و تضمین استفاده صلح آمیز در مشارکت جهت توسعه اجتماعی و اقتصادی^۲ اقداماتی صورت گیرد.

کارگاه اول: هنجارهای آتی جهت حفظ و ارتقای امنیت سایبری در سطح بین‌المللی، مورخ ۹ تا ۱۰ فوریه ۲۰۱۶:

در این کارگاه کارشناسان پیشرفت در توسعه هنجارها، رفتار مسئولانه دولت‌ها در فضای سایبر را مورد بررسی قرار دادند. همچنین تمایل اصلی این کارگاه روی موضوعات زیر متمرکز بود:

✓ توسعه ایده‌های جدید برای هنجارها؛

✓ شناسایی هنجارهایی که از نظر فنی سودمند و امکان‌پذیر می‌باشد^۳؛

✓ کمک جهت آماده سازی پایه و اساس گروه کارشناسان بعدی^۴؛

خروجی‌های این کارگاه را می‌توان بر اساس نظرهای مختلف مشارکت‌کنندگان در چند جمله زیر خلاصه نمود:

موضوعات خلع سلاح، استفاده صلح‌آمیز از فضای سایبری، حاکمیت و توسعه اقتصادی اولویت بالایی را در مباحث بین‌المللی خواهد داشت. بیشتر کشورها در خصوص امنیت سایبری اظهار نگرانی می‌کنند این موضوع مثبت است. برخی ملل ترجیح می‌دهند رویکردی را بر اساس خلع سلاح و اجتناب از مسابقات تسلیحاتی یا نظامی‌گری اتخاذ نمایند و بنابراین تلاش می‌نمایند حقوق مخاصمات مسلحانه را در فضای سایبری توسعه دهند.

رویکردی برای هنجارها بر مبنای کنترل تسلیحات و عدم اشاعه یک نقطه شروع ارزشمند برای مباحث امنیت سایبری خواهد بود اما این موضوع نیازمند درگیر شدن فناوری‌های جدید همساز^۵ و گروه ذی‌نفعان بین‌المللی می‌باشد.

کنترل بیشتر دولت‌ها روی اینترنت پیشنهاد برخی ملل خواهد بود. اگر گروه کارشناسان دولتی

1. safeguard cyberspace from becoming 'an arena of conflict' and ensure its peaceful use to contribute to social and economic development

2. "Cyber Warfare, unchecked, could topple entire edifice of international security, says speaker in First Committee at conclusion of thematic debate segment", General Assembly Meetings Coverage, 29 October 2014, <http://www.un.org/press/en/2014/gadis3512.doc.htm>

3. identify what is technologically feasible and useful

4. help lay the groundwork for the next GGE

5. accommodate new technologies

را یک نقطه کانونی در خصوص پیشرفت در هنجارهای جهانی امنیت سایبری در نظر بگیریم همان طور که :

✓ در گزارش سال ۲۰۱۰ مشخص شد که پیشنهاد جامعه بین‌الملل روی هنجارها، اقدامات اعتمادساز و ظرفیت‌سازی متمرکز است؛

✓ در گزارش سال ۲۰۱۳ مشخص گردید که دورنمای سیاسی مرتبط با فضای سایبری توسط تأیید کاربرد حقوق بین‌الملل، منشور سازمان ملل، اصل حاکمیت دولت‌ها در فضای سایبر تغییر شکل داد. ✓ مجموعه موضوعات مهم در گزارش سال ۲۰۱۵ از جمله مجموعه مهمی از هنجارها و اقدامات اعتمادساز داوطلبانه از جمله موافقت درباره عدم حمله به زیرساخت‌های حیاتی در زمان صلح، ارتقای زنجیره تأمین یکپارچه و پاسخ به درخواست دولت‌ها برای کمک و مساعدت، حق کشورها در اتخاذ اقدامات سازگار با منشور سازمان ملل و حقوق بین‌الملل از جمله حق ذاتی دفاع از خود.

برخی از کارشناسان خارج از گروه کارشناسان دولتی پیشنهاد دادند که گروه کارشناسان دولتی بعدی، باید هنجارهای جدید را مورد نظر قرار دهند از جمله تعهد جهت حفاظت از زیرساخت‌های حیاتی و مراکز عمومی^۱ اینترنت، توسعه بیشتر و وضوح کاربرد حقوق بین‌الملل موجود، و توافق ممکن روی توقف و محدودیت جاسوسی تجاری^۲ در فضای سایبری.

ضمن اینکه هنجارهای ویژه که توسط جوامع دانشگاهی، بخش‌های خصوصی پیشنهاد گردیده است و ابتکارات بین‌المللی رهبری شده توسط دولت‌های هم فکر^۳ باید مورد نظر قرار گیرد.

در نخستین کارگاه، فرایند پیشرفت هنجارها در خصوص رفتار مسئولانه دولت‌ها در فضای سایبری بررسی گردید. هنجارهای ارائه شده در گزارش گروه کارشناسان دولتی قبلی مشخص گردید و در این گروه کاری در خصوص هنجارهای مکمل که ممکن است برای موارد زیر مورد نیاز باشد بحث گردید:

- هنجارهایی در خصوص محدود کردن خطر ناشی از پیامدهای غیر عامدانه در زمان صلح^۴،

1. public core

2. constrain commercial espionage

3. like-minded states

4. limit the risk of unintended consequences in peacetime

- هنجارهای دیگری که متضمن حفاظت از زیرساخت‌های اینترنت می‌باشد. اولین پنل در خصوص توسعه هنجارهای بین‌المللی درباره رفتار در فضای سایبری با بررسی چشم‌اندازهای بین‌المللی درباره هنجارهایی که از قبل موجود بوده‌اند و یا ممکن است وجود داشته باشند شروع شد. نتایج حاصل از این پنل شامل موارد زیر است:

- افزایش علاقه بخش وسیعی از کشورها امید بخش بود اما نیازمند تجدید تلاش‌ها در خصوص ارتقای آگاهی از خط‌مشی امنیت سایبری کشورها و ظرفیت فناوری به‌منظور اجتناب از احساس خطر بین کشورها با ظرفیت‌های مختلف می‌باشد؛

- کشورهای در حال توسعه می‌توانند در فرایند بین‌المللی وارد شوند و احساس نمایند که سهم و نقشی در شکل‌دهی به هنجارها دارند؛

- اقبال بزرگ‌تر و مهم‌تر اینکه پیشنهادها و توصیه‌های گروه کارشناسان دولتی تصویب خواهد شد؛

- به‌رغم تداوم بحث در خصوص موضوع حاکمیت، احتمال اینکه اغلب کشورها برای رسیدن به یک

زمینه مشترک در باب هنجارها در خصوص چگونگی همکاری جهت حفاظت از زیرساخت‌های حیاتی

در هر کشور و زیرساخت‌های حیاتی اینترنت به شکل کلی به یک توانمندی خواهند رسید، وجود دارد؛

- بحث درباره هنجارها همان‌طور که برای کشورهای توسعه‌یافته مهم است، برای کشورهای

در حال توسعه نیز مهم خواهد بود زیرا کشورهای در حال توسعه برای رشد خود به میزان برابر

با کشورهای توسعه‌یافته، وابسته به فناوری‌های اطلاعات و ارتباطات و اینترنت خواهند بود. این

کشورها نه تنها حاکمیت را در موضوعات عدم مداخله می‌بینند بلکه به حاکمیت به‌عنوان یک

وظیفه برای حمایت از آنچه در فضای داخلی کشور خود دارند می‌نگرند؛

- تجربیات کشورهای در حال توسعه آن‌ها را از اهمیت فضای سایبری آگاه ساخته است اما

در خصوص درک مشترک از موضوعات، این کشورها در سطوح بسیار متفاوتی از هم قرار دارند.

بنابراین هنجارهای مطرح در گزارش‌های گروه کارشناسان دولتی می‌تواند در سطح منطقه‌ای

تکمیل شوند جایی که تفاوت‌ها در ظرفیت‌سازی، سرمایه‌گذاری و حساسیت‌های سیاسی به

سهولت همسان‌سازی شوند.^۱

1. GGE norms are and can be supplemented at the regional level, where differences in capacity, investment, and political sensitivities are more readily accommodated.

دومین پنل در خصوص چشم‌اندازهای آینده فناوری‌ها^۱ و بررسی امکان ایجاد هنجارهای فنی برگزار شد. این پنل بر روی موضوع زیر متمرکز گردید. چگونگی عمیق‌تر شدن و تصریح هنجارهای توسعه‌یافته توسط گروه کارشناسان دولتی در خصوص ممنوعیت هدف‌گیری زیرساخت‌های حیاتی.

یکی از نگرانی‌های اصلی، آسیب‌پذیری معماری اینترنت با مورد هدف واقع شدن سرورهای اصلی اینترنت بود و باعث شد اعضای پنل بر روی واژه حمله به شرح زیر به توافق برسند:

✓ قطع زیرساخت‌های حیاتی؛

✓ آسیب‌پذیری‌های سیستم نام دامنه^۲ و پروتکل‌ها؛

در این خصوص اعضای پنل متذکر شدند که خط‌مشی دولت‌ها برای ارتقای حاکمیت فناوریانه و داده سبب بروز مشکلاتی می‌شود. مشکلاتی مانند انجام مداخله در امور مختلف کشورها از طریق پروتکل‌های مسیریابی مداخله، اثر متقابل بین فناوری‌ها، پیشامدهای پیش‌بینی نشده برای منافع تجاری و امنیت.

هنجارهای مبسوط در گزارش گروه کارشناسان دولتی در سال ۲۰۱۵، مخصوصاً هنجارهایی که هدف‌گیری زیرساخت‌های حیاتی را ممنوع می‌کند می‌تواند برای اجتناب از این مشکلات بیشتر توسعه یابد.

همچنین متخصصان فنی بر اهمیت حفظ اعتماد و ایجاد هنجارهایی که می‌تواند دولت‌ها را در مقابل اقدامات بی‌ثبات‌کننده حفاظت می‌کند تأکید دارند. اعتماد، نقطه اصلی در خصوص چگونگی عملکردهای اینترنت می‌باشد و چنانچه ضعف و نقصانی در پروتکل اصلی رخ دهد از دست می‌رود. بنابراین اعضای پنل بر روی توافقی درباب هنجارهای مربوط به حفاظت از مرکز (هسته) عمومی اینترنت در مقابله مداخله‌های غیرآگاهانه توسط دولت‌ها بحث نمودند.

سومین پنل در این کارگروه به این نکته توجه داشت که چارچوب گروه کارشناسان دولتی طوری نیست که بتواند برای هم‌ساز سازی منافع جامعه بین‌المللی کافی باشد و ممکن است به سازوکار رسمی بیشتری برای بحث در خصوص موضوعاتی که فضای سایبری برای امنیت

1. featured technologists' perspectives
2. Domain Name System (DNS)

بین‌الملل ایجاد می‌کند نیاز باشد سازوکاری که علاوه بر وابستگی به سیستم ملل متحد، باید فراگیرتر و شفاف‌تر باشد. چگونگی کاربردهای حاکمیت در فضای سایبری یک موضوع مهم در این پنل بود که مورد بحث قرار گرفت. دولت‌ها در خصوص اجرا و تکمیل مسئولیت‌های خود در این حوزه (از بعد تعاملات داخلی و بین‌المللی) مشتاق هستند و در پی تصویب مقررات و فناوری‌هایی هستند که آن‌ها را برای کنترل بیشتری تأمین نماید.

آنچه ما حالا مشاهده می‌کنیم توسعه حاکمیت در فضای سایبری است. این توسعه در حال حاضر اجتناب‌ناپذیر است، زیرا خطرهای ایجاد شده توسط اینترنت برای منافع عمومی توسط بسیاری از کشورها حس شده است و این امر نیازمند مداخله آن‌ها در بحث حاکمیت فضای مجازی گردیده است.

در آخرین پنل که در این کارگاه برگزار گردید تلاش‌های بیشتر جهت ایجاد هنجارهای سایبری در سطح بین‌المللی مورد ملاحظه قرار گرفت و نتایج مهمی که از خروجی‌های گروه کارشناسان دولتی می‌تواند کسب گردد در خصوص ارتقای ظرفیت‌سازی، ایجاد سازوکارهایی برای حفاظت از ثبات و محدود کردن تهدیدات خواهد بود.

اعضای پنل به ملاحظات و توصیه‌هایی که گروه کارشناسان دولتی بر موضوعات زیر داشته‌اند تأکید کردند:

- چگونگی توسعه کنترل ملی بر این فضا جهت حفاظت از ماهیت جهانی و اتصالات جهانی فضای سایبر؛

- راه‌هایی برای ارتقای و پشتیبانی از امنیت و پایداری جهانی این فضا؛

- تعریف رفتار مسئولانه دولت‌ها در فضای سایبری؛

- کاربرد تعهدات بین‌المللی موجود در زمینه حقوق محاصمات و حقوق بشر؛

- توافق درباره ممنوع کردن توسل به زور علیه زیرساخت‌هایی که پیامدهای آن‌ها می‌تواند

به‌ویژه فضای سایبر را ویران کند.

همچنین برخی از اعضای پنل موکداً بر روی موضوعات زیر اشاره کردند:

۱. ضرورت تعامل بخش خصوصی در توسعه هنجارهای سایبری؛

۲. اهمیت تفکر وسیع درباره هنجارها و اجتناب از تمرکز روی برخی از هنجارهای ویژه که تنها مختص زمان صلح است؛

۳. رویکردهای جدید برای امنیت سایبری در سطح بین‌الملل که می‌توانند سازوکارهایی را برای پایش و به اشتراک‌گذاری اطلاعات در خصوص چشم‌انداز تهدیدات را پیشنهاد دهند؛

۴. ظرفیت‌سازی جهت توان‌مندسازی کشورها جهت اجرای هنجارها مخصوصاً هنجارهای مرتبط با مقابله با خطرها و ایجاد ثبات و صلح ناشی از اقدامات مربوط به پایین آستانه مخاصمات مسلحانه در فضای سایبری^۱ و در نهایت بحث در مورد انتساب.

کارگاه دوم: کاربرد حقوق بین‌الملل در چارچوب امنیت بین‌المللی مورخ ۱۹ تا ۲۱ آوریل ۲۰۱۶

پس از برگزاری موفق سری اول کارگروه در خصوص موضوع امنیت سایبری در سال ۲۰۱۶، سری دوم آن نیز جهت کمک به شناسایی حوزه‌های درک مشترک در خصوص موضوعات سایبری برگزار شد. این کارگاه با حضور کارشناسان حقوقی و سیاسی از بخش‌های دولتی و دانشگاهی به‌منظور تقویت فهم بهتر از چگونگی کاربرد حقوق بین‌الملل در فضای سایبر برگزار گردید. این رخداد فرصت مناسبی جهت پرداختن به موضوعات زیر ارزیابی گردید:

تبادل نقطه نظرها با نگاهی به تسهیل پیشرفت در مباحث آتی و ارائه نظر در خصوص چگونگی عملیاتی‌سازی این هنجارها و اتخاذ گام‌های بعدی جهت ارتقای ثبات سایبری در سطوح منطقه‌ای و بین‌المللی.

یکی دیگر از اهداف کارگاه تقویت درک مشترک میان دولت‌ها، جوامع دانشگاهی و فنی در خصوص ارائه درک مشترکی از مشکلات موجود برای امنیت و ثبات در فضای سایبر و دامنه راه‌حل‌های ممکن در سطوح منطقه‌ای و چندجانبه^۲ بود.

از موضوعات مهم و برجسته که در این کارگاه و با هدف ارائه نقطه نظرهای کارشناسان غیردولتی در خصوص آن بحث شد، کاربرد حقوق بین‌الملل برای امنیت سایبری و پاسخ‌گویی دولت‌ها در چارچوب خلع سلاح و امنیت بین‌الملل بود به‌طوری‌که مباحث مطرح شده در این کارگاه

1. actions below the level of armed conflict in cyberspace

2. range of possible solutions at the regional and multilateral levels

روشن نمود که به کارگیری حقوق بین‌الملل در فضای سایبر یک انتخاب درست و بی‌پرده‌ای نیست و دلیل آن پیچیدگی در تصمیم‌گیری درباب موضوعاتی مثل چگونگی استفاده نامطلوب از اقدامات سایبری در رابطه با مفاهیم زور و حمله، امنیت سایبری وفق حقوق بشر، ماهیت حاکمیت، چگونگی مقابله با تروریسم در استفاده از اینترنت می‌باشد.

{در این کارگاه به گزارش‌های گروه کارشناسان دولتی اشارات فراوانی گردیده است.} در گزارش گروه کارشناسان دولتی در سال ۲۰۱۳، بر اهمیت حقوق بین‌الملل از جمله منشور سازمان ملل متحد و اصل حاکمیت دولت‌ها {به‌عنوان موارد مهم} برای قرار دادن امنیت سایبری در چارچوب حقوق موجود و درک رابطه بین دولت‌های حاکم تأکید شده است. در این گزارش، کارهای بیشتری درخصوص توسعه درک مشترک از کاربرد حقوق و هنجارها، قواعد و اصول بین‌الملل موجود برای رفتار مسئولانه دولت‌ها درخواست شده است. این موضوعات در دستورکار گروه کارشناسان دولتی در سال ۲۰۱۵ منعکس گردید که در آن درخواست گردید تا دبیرخانه و گروه کارشناسان دولتی در کنار سایر موضوعات به بررسی چگونگی اعمال حقوق بین‌الملل در استفاده از فناوری‌های اطلاعات و ارتباطات توسط دولت‌ها ادامه دهند.

{از نگاه این کارگاه} نحوه اعمال حقوق بین‌الملل یکی از سخت‌ترین موضوعاتی است که جامعه ملل به طور مداوم بدان می‌پردازد. برخی ملل بحث می‌کنند که حقوق بین‌الملل موجود کفایت و بسندگی لازم را ندارد و حقوق جدید باید توسعه یابند. نگاه‌های متفاوتی درباره ماهیت مخاصمات مسلحانه در فضای سایبری، بهترین راه جهت پیشگیری از آن و کاربرد اصول مندرج در کنوانسیون‌های لاهه و ژنو وجود دارد. سایر موضوعاتی که در مباحث و گفتگوها دوباره ظهور یافته‌اند از جمله: اعمال ماده ۴ بخش ۲ و همچنین ماده ۵۱ منشور سازمان ملل متحد در فضای سایبری، سطح ادله و انتساب جهت پاسخگویی دولت‌ها، کاربرد حق دفاع مشروع یا اقدامات متقابل از طریق دولت‌های صدمه دیده، حوزه‌های دیگر درگیری شامل نقش بی‌طرفی و نقض حاکمیت دولت ثالث، حملات سایبری توسط بازیگران غیر دولتی، استنباطها و مفاهیم شکل گرفته از حاکمیت دولت‌ها در امنیت سایبری و رفتار مسئولانه دولت‌ها.

دقیقاً چگونگی انتخاب دولت‌ها در پاسخ به حوادث سایبری، یک تصمیم سیاسی می‌باشد اما

چنین تصمیماتی توسط توافقات و حقوق بین‌المللی هدایت می‌شوند. عملکرد گروه کارشناسان دولتی درباره کاربرد حقوق بین‌الملل، الزام‌آور نیست اما اساس و بنیانی سودمند برای مباحث آتی و گفتگو درباره چگونگی ارتقای امنیت و ثبات در فضای سایبری خواهند بود. در اولین پنل مربوط به این کارگاه، به این نکته توجه شد که در عمل تفاوت‌هایی در تفسیر و کاربرد حقوق بین‌الملل موجود مانده است مخصوصاً در خصوص اقداماتی که در پایین آستانه استفاده از زور می‌باشد.^۱ این می‌تواند اقداماتی باشد که سبب خسارات فیزیکی یا تلفات انسانی نمی‌شود. اقدامات سایبری که ممکن است بزرگ‌ترین خطر را برای ثبات ایجاد نماید، خطرهایی مانند تخریب داده‌ها، در ناحیه خاکستری قرار می‌گیرد در این زمان کاربرد حقوق بین‌الملل بشر دوستانه به‌عنوان شاخه‌ای از حقوق بین‌الملل که با جنگ سروکار دارد، مطرح می‌گردد. این‌ها اقدامات قهری هستند که تخریب می‌کنند یا به اهداف ناملموس صدمه وارد می‌کنند اما به‌طور شفاف به استفاده از زور یا حمله مسلحانه وابسته نیستند.^۲

«دولت‌ها نباید آگاهانه اجازه دهند که از سرزمین آن‌ها جهت اقدامات غیرقانونی در سطح بین‌المللی با استفاده از فناوری‌های اطلاعات و ارتباطات استفاده شود.»^۳ «این عبارت در متن گزارش ۲۰۱۵ (گروه کارشناسان دولتی) قید شده است. اعضای پنل روی اصولی که ناشی از تلاش مقتضی (مکفی)^۴ بحث کردند. این قاعده از دولت‌ها درخواست می‌نماید تا تضمین نمایند که از سرزمین آن‌ها برای اقدامات سوء به شکل مستقیم علیه کشورهای دیگر استفاده نشود.^۵

و جهت این تضمین یک دولت متعهد می‌شود تا در رویدادهای مهم:

- تمامی اقدامات موجود را اتخاذ نماید^۶؛

- تمامی مسئولیت‌های قابل انتظار را انجام دهد.^۷

چنانچه دولتی تمامی اقدامات مسئولانه و امکان‌پذیری را اتخاذ نماید اما در پیشگیری از یک اقدام غیر قانونی در سطح بین‌المللی ناتوان باشد، پس در این صورت از اصول تخطی نموده

1. actions that fall below the threshold of force

2. but are not regarded as a clear use of force or an "armed attack".

3. "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs".

4. due diligence

5. Due diligence requires States to ensure that their territory is not used for harmful actions directed against other States

6. "take all available measures"

7. "do all that could be reasonably expected of it"--

اما ممکن است هنوز متعهد به اخطار (آگاهی‌رسانی) و همکاری باشد.

از آنجایی که دولت‌ها نمی‌توانند به شکل مطلق از تمامی آنچه در سرزمین آن‌ها اتفاق می‌افتد، آگاه باشند، استانداردهای قبلی‌ای وجود دارد مبتنی بر اینکه آیا دولتی در خصوص اقدامات و فعالیت‌های ویژه در سرزمین‌های خود اطلاع داشته یا باید اطلاع داشته باشد.^۱ همچنین برای دولت‌ها در خصوص اتخاذ اقدامات پیشگیرانه، مسئولیتی وجود دارد که این مسئولیت مطابق با تعهدات آن‌ها در سطح بین‌المللی در خصوص حفاظت از زیرساخت‌های حیاتی و سایبری می‌باشد.

در این پنل چالش‌هایی که بر سر راه گروه کارشناسان دولتی در سال ۲۰۱۷ متصور می‌شود ضربه‌ای است که چنانچه هنجارهای مربوط به قاعده تلاش مقتضی، بیشتر توسعه یابد، تعادل درباره مسئولیت دولت‌ها برقرار می‌شود.^۲

مباحثه و مجادله‌ای در خصوص میزان و اندازه به‌کارگیری اصل تلاش مقتضی در فضای سایبر وجود داشت. برخی مشارکت‌کنندگان اشاره کردند که تلاش مقتضی تنها در قواعد اقدام متقابل مهم می‌باشد.

احساس دیگری که دولت‌ها از قبل دارند «تعهد به اتخاذ تمامی اقدامات در دسترس»^۳ از جمله تجهیزات و ادوات سایبری برای حفاظت پیش‌دستانه از زیرساخت‌های سایبری و حیاتی می‌باشد.^۴ در خلال بحث، نمایندگان برخی کشورهای در حال توسعه استدلال کردند که حقوق بین‌الملل «به طرفداری از ما کار نمی‌کند»^۵ در این پنل، اعضای پنل بر روی آنچه آن‌ها به‌عنوان موضوعات اصلی و ضروری درباب ادله و انتساب تعیین شده است، متمرکز شدند و مخصوصاً این موضوع چگونه یک کشور خود را آماده خواهد ساخت تا یک پاسخ روشنی را ارائه و شواهد خود را در شورای امنیت، جامعه بین‌المللی یا در جمع دوجانبه مطرح نماید. زمانی که دولت‌ها از نظر فنی و سیاسی آمادگی این کارها را ندارند. شواهد و ادله شامل، شناسایی و تعیین هویت،

1. there are precedential standards based on whether a State knew or ought to have known about a particular activity or action on its territory

2. will be to strike the right balance on State responsibilities if it is to further develop norms on due diligence

3. "take all available measures"

4. others felt that States already have the obligation to "take all available measures", including cyber means to pre-emptively protect cyber and critical infrastructure

5. "does not work in our favour",

حقیقی است که حقوق بین‌الملل بر آن اعمال می‌گردد. انتساب به مبدأ یک اقدام ضد حقوق بین‌الملل و ضد تعهدات دولت‌ها، اغلب برای امنیت بین‌الملل مشکلاتی را رقم می‌زند. دومین پنل، گزارش سال ۲۰۱۵ گروه کارشناسان دولتی را برجسته نمود. گزارشی که باوجود اینکه هنوز برای ایجاد اجماع روی اعمال حقوق بین‌الملل در زمان جنگ مشکلاتی وجود دارد، اما پیشرفت چشمگیری در نگاه‌های مشترک ملی روی قواعد در زمان صلح ایجاد کرده است. این پنل به موضوعاتی محدود شد که گروه کارشناسان دولتی بر اساس دستور کار خود آن را پوشش داده‌اند.

در پنل سوم، حقوق مخاصمات مسلحانه و کاربرد زور و حمله مسلحانه در فضای سایبر مورد بحث قرار گرفت. نتیجه اجماع روی اعمال حقوق بین‌الملل در زمان جنگ مشکلاتی وجود دارد، اما پیشرفت چشمگیری در نگاه‌های مشترک ملی روی قواعد در زمان صلح ایجاد کرده است. این پنل به موضوعاتی محدود شد که گروه کارشناسان دولتی بر اساس دستور کار خود آن را پوشش داده‌اند.

در پنل سوم، حقوق مخاصمات مسلحانه و کاربرد زور و حمله مسلحانه در فضای سایبر مورد بحث قرار گرفت. نتیجه این مباحث به شکل زیر بود:

- تعاریفی از حقوق بشردوستانه^۱: حقوق بشردوستانه بر فضای جنگ سایبری اعمال می‌شود جایی که این حقوق تلاش می‌کند تا از افراد غیرنظامی حفاظت نماید.^۲ حقوق بشردوستانه رفتار دولت‌های درگیر در مخاصمات سایبری را تنظیم می‌کند. حقوق بشر دوستانه ممنوعیت و محدودیت‌هایی را بیان می‌کند. این حقوق در خصوص مشروعیت بخشی به کاربرد زور نمی‌باشد.^۳ حقوق بشردوستانه در مخاصمات بین‌المللی و غیر بین‌المللی اعمال می‌گردد. این حقوق تلاش می‌نماید تا غیرنظامیان را حفاظت نماید. براساس ماده ۳۶ پروتکل الحاقی کنوانسیون‌های ژنو،^۴ حقوق بشردوستانه برای سلاح‌های جدید، روش‌ها و ادوات جنگی جدید اعمال می‌شود.^۵
- چگونگی اعمال حقوق بشردوستانه بر عملیات‌های سایبری هنگامی که در خلال مخاصمات

1. International humanitarian law(IHL)

2. IHL "regulates the conduct of parties engaged in an armed conflict"

3. IHL sets forth prohibitions and limitations—it is not about legitimization of the use of force.

4. 18 Article 36 of Additional Protocol I of the Geneva Conventions.

5. IHL applies to new weapons, methods and means of warfare

مسلحانه رخ می دهند..

• بخش وسیعی از تعهدات حقوق بشردوستانه نسبتاً به راحتی می‌تواند به مقوله امنیت سایبری منتقل گردد. اما لازم است هنگام کاربرد حقوق بشردوستانه در فضای سایبر، برخی موضوعات شفاف گردد از جمله چگونگی اعمال این حقوق در مواقعی که اثر حرکتی وجود ندارد^۱ و تغییر فیزیکی انجام نمی‌شود یا مواردی که حمله تنها روی داده‌ها تأثیرگذار بوده است. در این پند، این موضوع مورد بحث قرار گرفت که حقوق بین‌الملل از پیش برای پرداختن به فعالیت دولت‌ها در چارچوب جنگ وجود دارد در خصوص {حقوق} مربوط به کاربرد زور مربوط به اقدامات و فعالیت‌های زیر سطح آستانه (که هنوز ضمنی می‌باشد و به شکل رسمی تعریف نشده است) نیاز به توافق بین کشورها دارد.

• توجه به توافق صریح و روشن بین دولت‌ها که در آن، دولت‌ها نباید عملیات‌های سایبری را علیه غیرنظامیان یا زیرساخت‌های اصلی که برای اهداف غیرنظامی قابل کاربرد است، به کارگیرند.^۲
- بحث انتساب، اصلی برای اعمال حقوق بشردوستانه می‌باشد اما اشکال ناشی از این بحث وجود تفاوت بین کشورها در خصوص قابلیت‌ها و استانداردهای {لازم جهت شناسایی و بحث انتساب} می‌باشد.^۳

- آیا حملات سایبری که منجر به ایجاد صدمات فیزیکی نشده اند {می‌تواند} به منزله کاربرد زور باشد {تلقی گردد}.^۴

- اقدامات متقابل به‌عنوان یک عنصر از حقوق بین‌الملل هنوز در گزارش گروه کارشناسان دولتی نقش دارد. به این صورت که در نشست آتی گروه کارشناسان دولتی باید هنجارهایی را مورد نظر قرار دهد در آن «دولت قربانی ممکن است اقداماتی را در پاسخ یا تلافی در برابر کشور دیگری که اقدامات سایبری سوء {را انجام داده اند} اتخاذ نماید، {اقداماتی} که شامل کاربرد زور نباشد.»^۵ یک اقدام متقابل می‌تواند به‌عنوان مثال شامل {در قالب} تحریم‌های اعمالی شورای

1. without kinetic impact

2. States should not engage in cyber operations against civilians or essential civilian infrastructure could be useful

3. attribution was paramount for the application of IHL, but difficulties arise given the varying capabilities and standards of proof among different States

4. whether cyberattacks constituted "use of force" when they did not lead to physical damage.

5. "the victim State may take actions not involving the use of force in response (or retaliation) to a malicious cyber action by another State".

امنیت علیه کشور حمله کننده و به منظور تقویت و حفظ صلح و امنیت بین‌المللی باشد.^۱

کارگاه سوم: مدیریت گسترش ابزار سایبری که می‌توانند جهت اهداف سوء و غیرقانونی به کار روند مورخ ۱۵ الی ۱۶ ژوئن ۲۰۱۶

باتوجه به اینکه گزارش گروه کارشناسان دولتی در سال ۲۰۱۵ شامل توصیه ای است مبنی بر اینکه دولت‌ها باید پیشگیری از اشاعه ابزار و فناوری‌های مخرب (بدافزارها) و استفاده از کارکرد های مخرب مخفی را پیگیری نمایند، این کارگاه سوابقی از عدم اشاعه برای ایجاد هنجارها و سازو کارهایی به منظور جلوگیری از استفاده ابزار سایبری برای اهداف سوء و غیرقانونی را بررسی کرد. فناوری اطلاعات و ارتباطات دارای ویژگی و خصوصیتی هستند که چالش‌های حاصل مبین ضرورت تلاش جهت کنترل گسترش این ابزار به منظور استفاده در خصوص اهداف سوء می‌باشد. خصوصیتی مانند سرعت انتقال قابلیت‌ها، ماهیت کاربرد دوگانه این ابزار. کارشناسان صنعتی و جامعه تحقیقاتی در این کارگروه، در خصوص مسائل مختلفی از جمله موارد زیر به بحث و گفتگو پرداختند:

۱. روندهای جاری در گسترش قابلیت‌های سایبری که می‌تواند برای اهداف سوء به کار گرفته شود. زیرا توسعه و گسترش این قابلیت‌ها سبب بروز چالش‌ها و نیاز به تلاش جهت کنترل آن‌ها می‌گردد. این گفتگوها دامنه وسیعی از دیدگاه‌ها را در خصوص اینکه چگونه قابلیت‌های سایبری گسترش می‌یابند و راه‌حل‌های ممکن جهت مقابله با چالش‌های حاصل از آن‌ها را در بر گرفت؛

۲. رویکرد کنترل صادرات/عدم اشاعه^۲ در مقابل رویکرد کنترل تسلیحات^۳؛

۳. کنترل توسعه ابزاری که می‌تواند برای اهداف سوء استفاده گردد. کنترل استفاده سوء از ابزار سایبری با استفاده از رویکردهای سنتی عدم اشاعه شدیداً چالش‌آفرین است. به‌عنوان مثال بسیاری از تجهیزات سایبری که می‌توانند برای اهداف سوء استفاده گردند در این گروه کاری توافق کلی بر روی این موضوع صورت گرفت که جامعه بین‌الملل باید برخی راه‌ها را برای کنترل

1. A countermeasure could, for example, entail the Security Council imposing sanctions on the attacking State in order to strengthen and maintain international peace and security.

2. export control/non-proliferation approach

3. arms control approach

توسعه سوءاستفاده از ابزار و نرم افزارها بیاید؛

۴. در بحث امنیت سایبر ممکن است نیاز به تمرکز روی نیت حمله وجود داشته باشد تا آثار (حمله)¹.

این کارگروه همچنین فرصتی بود جهت تبادل نظر و بحث در خصوص:

- وجوه توسعه ابزار سایبری که مهم‌ترین تهدیدات را برای ثبات سایبری در سطح بین‌الملل را ایجاد می‌نماید؛

- شناسایی اهداف کلیدی برای مدیریت گسترش چنین قابلیت‌هایی؛

- تلاش جهت ارتقای ثبات در فضای سایبری از جمله قابلیت کاربرد حقوق بین‌الملل در

فضای سایبر، که گروه کارشناسان دولتی از طریق اجماع بدان رسیده‌اند؛

- تلاش‌های دوجانبه و چندجانبه در خصوص گسترش اقدامات اعتمادساز؛

- در نظر گرفتن چالش‌های منحصربه‌فرد مترتب بر تلاش‌ها به مدیریت گسترش

قابلیت‌های فضای سایبری توسط دولت‌ها. از جمله چالش‌های مربوط به ماهیت کاربرد دو گانه فناوری‌ها است که تعیین اینکه آیا انتقال این فناوری‌ها برای اهداف مضر صورت می‌گیرد یا

اهداف سودمند را دشوار می‌نماید؛

- بحث در خصوص سازوکارهای موجود که درس‌های مفیدی را ارائه نماید. سازوکارهایی مانند:

• ابتکار جهانی جهت مبارزه با تروریسم هسته‌ای^۲ که رژیم داوطلبانه ای می‌باشد که در

خصوص ظرفیت‌سازی و همکاری میان دولت‌ها جهت مبارزه با تروریسم هسته‌ای عمل می‌نماید.

• ابتکار اشاعه امنیت^۳ که یک چارچوب جهانی است و در آن دولت‌ها متعهد شدند تا انتقال سلاح‌های کشتار جمعی^۴، سیستم‌های پرتاب^۵ و سایر ادوات مربوط از طرف بازیگران دولتی و غیردولتی را مختل نمایند؛

• همکاری‌های دولتی با بخش خصوصی جهت ایمنی مواد خطرناک و داده‌های حساس.

طبق نظر کارشناسان این گروه کاری، شاید تنها سازوکار موجود که می‌تواند خیلی مرتبط

1. There was also discussion of how cyberattacks are often highly tailored, designed for a specific target, and thus limit the potential for indiscriminate effect. Since indiscriminate effect is a characteristic of weapons of mass destruction and other banned weapons, the question for cybersecurity may need to focus more on the intent of attacks rather than their effects.

2. Global Initiative to Combat Nuclear Terrorism (GICNT)

3. Proliferation Security Initiative (PSI)

4. weapons of mass destruction

5. delivery systems

با امنیت سایبری باشد رژیم کنترل صادرات و اسنار^۱ می‌باشد. ژریمی که در سال ۱۹۹۶ بر پایه یک توافقنامه چندجانبه در خصوص ارتقای امنیت بین‌المللی از طریق تنظیم انتقال سلاح‌های متعارف و کالاها و فناوری‌های دومنظوره (دارای کاربرد دوگانه) بنا گردید. دولت‌های شرکت‌کننده {این رژیم کنترل صادرات} اخیراً توافق کردند که «رژیم» کنترل استفاده سوء از ابزار سایبری را نیز ایجاد نمایند هرچند که هنوز این «رژیم‌های» کنترل به دلیل مسائل تعریفی جای بحث و جدل می‌باشد. توافقنامه «واسنار» تقریباً انواع زیادی از نرم افزارها را کنترل می‌کند اما کنترل آن برای نرم افزارهای مرتبط با تجهیزات نظامی یا فناوری‌های تولید کنترل شده تعریف شده است. از جمله نرم افزارهایی که با سخت افزارهای نظامی یا کاربرد دوگانه پیوند دارند. {نرم افزارهایی مانند} آن‌هایی که برای راه‌اندازی ادوات مورد نیاز برای بخش‌های مختلف هواپیماهای نظامی به کار می‌روند. حدود و حیطه کنترل این توافقنامه در خصوص نرم افزارها کاملاً مشخص است اما ممکن است واسنار به‌عنوان یک ابزار کنترل و مدیریت دسترسی به محصولات نرم‌افزاری که با سخت افزارهای نظامی پیوند می‌خورند، مفید نباشد. در نهایت مشارکت‌کنندگان در این کارگروه به این نتیجه رسیدند که احتمالاً به دو دلیل مدل‌های کنترل صادرات یا عدم اشاعه، برای کنترل دسترسی به فناوری‌های امنیت سایبری حاضر مفید نیستند:

- موضوعات تعریفی: به این معنی که خطر واقعی وجود دارد که یک تعریفی که می‌توانند بدافزارها را در بر بگیرد، ممکن است محصولات {نرم‌افزاری} قانونی را در بگیرد و ممکن است نوآوری‌ها را محدود نماید؛

- به دلیل تعداد بی‌شمار محصولات و شکل‌گیری آسان بدافزارها اجرای یک رژیم کنترل مشکل است و می‌تواند به راحتی محصولات را به سمت بازارهای سیاه و یا بازارهایی که کمتر تنظیم مقررات شده اند جهت دهی نماید؛

- سازوکارهای مبتنی بر بازار مانند برنامه‌هایی که تعداد آسیب‌پذیری‌های شناخته نشده که توسط برخی بازیگران سایبری و از روی عناد انجام می‌شود را شناسایی و کاهش می‌دهند.

1. Wassenaar
 2. market-based mechanisms
 3. undiscovered vulnerabilities

مجموعه‌ای از کارگاه با موضوعات امنیت بین‌المللی سایبری (فاز دوم)^۱ سال ۲۰۱۹ به دنبال موفقیت در فاز اول پروژه «کارگاه‌هایی با موضوعات امنیت بین‌المللی سایبری» در سال ۲۰۱۶، فاز دوم این پروژه با همکاری مرکز مطالعات راهبردی و بین‌المللی (CSIS) و حمایت یونیدیر و حمایت مالی آلمان و هلند شروع گردید. یکی از اهداف مهم این فاز، ارتقای درک مشترک میان دولت‌ها، جوامع فنی و دانشگاهی در خصوص مشکلات مرتبط با صلح و امنیت فضای سایبری و راه‌حل‌های ممکن در سطوح منطقه‌ای و چندجانبه بود. اگرچه گروه کارشناسان دولتی در سال ۲۰۱۷ موفق به تصویب گزارش اجماعی نگردید اما گزارش این گروه در سال ۲۰۱۵، دستور کار هنجاری^۲ و همچنین مرحله‌بندی‌های^۳ مهمی را جهت همکاری بین‌المللی درباره امنیت سایبری تنظیم نمود. مجموعه گروه‌کاری در فاز دوم این پروژه یک فرصت مناسب جهت بررسی^۴ چگونگی عملیات سازی این هنجارها و بررسی قدمهای بعدی جهت ارتقای ثبات سایبری در سطوح منطقه‌ای و بین‌المللی می‌باشد.

✓ دومین مجموعه از کارگاه‌های موضوعات امنیت بین‌المللی سایبری: نقش سازمان‌های منطقه‌ای در تقویت ثبات و امنیت سایبری^۵ مورخ ۲۴ ژانویه ۲۰۱۹ در ژنو (سوئیس) این کارگاه در موضوعات مهم زیر برگزار گردید:

چشم‌اندازهای منطقه‌ای درباره امنیت سایبری^۶، همکاری بین منطقه‌ای و رویه‌های برتر^۷، بررسی فرایندهای گروه کارشناسان دولتی و گروه‌کاری باز^۸، چشم‌اندازهای بین‌المللی در خصوص همکاری منطقه‌ای^۹، موضوعاتی برای گفتگوهای بین‌المللی^{۱۰}.

دومین مجموعه از کارگاه‌های موضوعات امنیت بین‌المللی سایبری: رویکردهای منطقه‌ای^{۱۱} سازمان دولت‌های آمریکا، واشنگتن (ایالات متحده آمریکا).

1. International Security Cyber Issues Workshop Series (Phase II)

2. normative agenda

3. milestones

4. take stock

5. The 2nd international security cyber issues workshop series: the Role of Regional Organizations in strengthening Cyber-security and Stability

6. Regional Perspectives on Cybersecurity

7. Inter-Regional Cooperation and Best Practices

8. Overview of the GGE and OEWG processes

9. International Perspectives on Regional Cooperation

10. Issues for International Dialogue

11. The 2nd international security cyber issues workshop series: Regional Approaches

دومین مجموعه از کارگاه‌های موضوعات امنیت بین‌المللی سایبری «حفظ و ارتقای ثبات سایبری در سطح بین‌الملل: رویکردها و واقعیت‌های منطقه‌ای: مرکز^۱ (سنگاپور).

گفتار سه: برگزاری کنفرانس‌های سالانه ثبات سایبر

کنفرانس سالانه ثبات سایبری فرصت مداومی را برای ذی‌نفعان جهت بحث در خصوص چگونگی اتخاذ گام‌های عملگرایانه به سمت {ایجاد} زیست‌بوم امنیت سایبری با ثبات و قابل پیش‌بینی با تمرکز بر موضوعات ویژه زیر را مهیا می‌نماید:

- خطرناک‌ناشی از افزایش تدریجی شدت و وسعت جنگ در زمان مخاصمات؛
- اجرای اقدامات اعتمادساز و شفاف:

از سال ۲۰۱۲ تا کنون (۲۰۱۹) شش کنفرانس با عناوین مختلف برگزار گردیده است:

- ثبات سایبری: تقویت تعامل جهانی^۳ ۶ ژوئن ۲۰۱۹ نیویورک، آمریکا؛
- نقش سازمان‌های منطقه‌ای در تقویت امنیت و ثبات سایبری^۴ در ۲۴ ژانویه ۲۰۱۹ در ژنو سوئیس؛
- ثبات سایبری: پیشگیری و کاهش {احتمال بروز} مخاصمات^۵، ۲۶ سپتامبر ۲۰۱۸، ژنو، سوئیس؛
- واقعیت‌ها و رویکردها منطقه‌ای: حفظ و تقویت ثبات سایبری در سطح بین‌المللی^۶، در ۲۷ فوریه ۲۰۱۸؛

- فناوری‌های اطلاعات و ارتباطات در چارچوب امنیت و صلح بین‌المللی (وضعیت حاضر و رویکردهای آتی)، ۱۱ اکتبر ۲۰۱۷، نیویورک، آمریکا؛

- سمینار ثبات سایبری ۲۰۱۶: پیشبرد امنیت بر اساس گزارش سال ۲۰۱۵ گروه کارشناسان دولتی^۷ ۱۷ ژوئن ۲۰۱۶، ژنو سوئیس؛

- سمینار ثبات سایبری ۲۰۱۵، انسجام نظام^۸، ۹ جولای ۲۰۱۵ ژنو سوئیس؛

- سمینار ثبات سایبری ۲۰۱۴، پیشگیری از مخاصمات سایبری، ۱۰ فوریه ۲۰۱۴، ژنو سوئیس؛

1. suntec city convention
 2. risks of escalation in times of conflict
 3. Strengthening global engagement
 4. Role of regional organizations in strengthening cybersecurity and stability
 5. Preventing and mitigation conflict
 6. Preserving and enhancing international cyber stability: regional realities and approaches
 7. Cyber Stability seminar 2016: Taking security forward-building on the 2015 report of the GGE
 8. Cyber Stability seminar 2015: Regime Coherence

۸ تا ۹ نوامبر ۲۰۱۲، ژنو، سوئیس.^۲

کنفرانس امنیت سایبری ۲۰۱۲: نقش اقدامات اعتمادساز در تضمین ثبات سایبری^۱، ۸ تا

گفتار چهار: مجموعه نشست‌هایی در خصوص حقوق بین‌الملل و رفتار دولت در فضای سایبری

با به‌کارگیری فضای سایبری در فعالیت‌های دولتی مانند برنامه‌ریزی و عملیات نظامی، فرایندها و زیرساخت‌های صنعتی و شهری و سازوکارهای مالی با رشد قابل توجهی روبه‌رو گردید. به این دلیل بود که نیاز مبرم به تعیین چگونگی اعمال اسناد حقوقی و هنجارهای بین‌المللی در فضای پویا و بدون مرز سایبری مطرح شد. بر مبنای اعلام یونیدیر، بر اساس بررسی‌های صورت گرفته توسط بخش‌های دولتی و جامعه مدنی، یک اجماع عمومی روی این قضیه وجود دارد که حقوق بین‌الملل {در قلمرو سایبری} به‌کار گرفته می‌شود اما سؤال اساسی این است که از چه طریقی این حقوق اعمال می‌گردد.^۳

به نظر می‌آید که گروه کارشناسان دولتی در سال ۲۰۱۳ که به قابلیت اعمال حقوق بین‌الملل پرداخته است، فرصت خوبی برای بررسی و گفتگو در خصوص این سؤال بود. گسترش درک مشترک درباره چنین موضوعی می‌توانست از طریق ایجاد مجمعی شکل گیرد که در آن بازیگرانی که فضای سایبر را ایجاد می‌کنند و بازیگرانی که این فضا را توسعه می‌دهند حضور داشته باشند تا در آن روی موضوعات دیگر تعامل نمایند. در این خصوص در یونیدیر با پشتیبانی کشورهای آلمان، هلند و سوئیس پروژه‌ای مطرح گردید که طی آن از اکتبر ۲۰۱۴ تا ژوئن ۲۰۱۵ مجموعاً سه نشست جهت پوشش موضوعاتی در خصوص همکاری منطقه‌ای و قابلیت کاربرد حقوق بین‌الملل در فضای سایبر برگزار گردید:

✓ نشست در خصوص حقوق بین‌الملل و رفتار دولت‌ها در فضای سایبری، سمینار منطقه‌ای اوراسیا، ۳ تا ۴ ژوئن ۲۰۱۵، مسقط (عمان)؛

1. Cyber security conference 2012: the role of confidence-Building measures in Assuring cyber stability

۲. به جهت حجم بالا، محتوای کنفرانس‌ها و سمینارها و ترجمه آن‌ها در فایل الکترونیکی ارائه شده است.

3. As academia and government explore these questions, there is general consensus that international law does apply; however the conversation becomes: in what ways does it apply?

✓ نشست‌های در خصوص حقوق بین‌الملل و رفتار دولت‌ها در فضای سایبری، سمینار منطقه‌ای آفریقا، ۳ تا ۴ مارس ۲۰۱۵، نایروبی (کنیا)؛

✓ نشست‌های در خصوص حقوق بین‌الملل و رفتار دولت‌ها در فضای سایبری، سمینار منطقه‌ای آسیا - اقیانوسیه، ۹ تا ۱۰ دسامبر ۲۰۱۴، سئول (کره جنوبی).

قابلیت‌های ملی، دکترین، سازمان‌ها و شفاف‌سازی و اعتمادسازی برای امنیت سایبری
یونیدیر با کمک مالی کشور آلمان، تحت پروژه «قابلیت‌های ملی، دکترین، سازمان‌ها و شفاف‌سازی و اعتمادسازی برای امنیت سایبری»، کنفرانسی را با عنوان «تهدیدات سایبری، اطلاعات به‌عنوان سلاح»^۱ در تاریخ ۹ اکتبر ۲۰۱۳ در نیویورک آمریکا برگزار نمود. این کنفرانس فرصت خوبی را ایجاد نمود تا در خصوص اینکه استفاده از اطلاعات ممکن است به‌عنوان یک سلاح در نظر گرفته شود، بحث و بررسی گردد. بررسی موضوعات زیر در دستور کار این کنفرانس قرار داشت:

- سلاح سایبری چیست؟ نظرها و استدلال‌های مقدماتی^۲؛

- جنگ سایبری از منظر آلمان^۳؛

- مخاصمات سایبری: چارچوب راهبردی^۴؛

چشم‌انداز جنگ سایبری: چارچوب‌های قانونی و شفاف‌سازی و اعتمادسازی؛

✓ کنفرانس آماده شدن برای جنگ سایبری^۵.

یونیدیر با کمک مالی کشور آلمان، در قالب پروژه چشم‌انداز جنگ سایبری: چارچوب‌های قانونی و شفاف‌سازی و اعتمادسازی، کنفرانسی را با عنوان «آماده شدن برای جنگ سایبری» در تاریخ ۲۴ آگوست ۲۰۱۱ در ژنو کشور سوئیس برگزار نمود. هدف از این کنفرانس درک بیشتر از این موضوع بود که دولت‌ها به مسئله جنگ سایبری چگونه می‌پردازند و چگونه امنیت سایبری را استدلال می‌نمایند. بررسی موضوعات زیر در دستور کار این کنفرانس قرار داشت:

1. Cyber Threats: Information as a Weapon?
2. What is a Cyber Weapon: Some Preliminary Thoughts
3. Cyber Warfare - The German Perspective
4. Cyber Conflict: The Strategic Context
5. Gearing Up for Cyberwar?

- فضای سایبری - مرز جدیدی برای جنگ؛

- ناتو و دفاع سایبری. {دفاع} متکی به هم یا {دفاع} جداگانه؟^۲.

کنفرانس چالش‌های امنیت سایبری - خطرها، راهبردها و اعتمادسازی^۳:

یونیدیر به میزبانی کشور آلمان در تاریخ ۱۳ تا ۱۴ دسامبر ۲۰۱۱، کنفرانسی را تحت عنوان «کنفرانس چالش‌های امنیت سایبری - خطرها، راهبردها و اعتمادسازی» در محل وزارت خارجه آلمان در برلین برگزار نمود. این کنفرانس روی مقابله با چالش‌ها و موضوعاتی درباره حوزه‌های نوظهور امنیت سایبری از منظر ذی‌نفعان اصلی، تصمیم سازان جامعه مدنی، صنعتی، دولت‌ها و حوزه‌های بین رشته ای دانشگاهی متمرکز بود. این کنفرانس به بررسی و بحث عمیق در خصوص مشکلات اساسی، آینده رژیم‌های تنظیم مقررات ملی و بین‌المللی، رویکردهای فنی و غیرفنی در خصوص امنیت سایبری پرداخت. با هدف بررسی نظرها در خصوص اقدامات اعتمادساز و شفاف‌ساز در فضای سایبری، مقاصد اصلی این نشست دو روزه را می توان به شکل زیر خلاصه نمود: -توسعه رویکردهای مشترک جهت حفظ اینترنت به‌عنوان یک {ابزار} مشترک و بدون انحصار و محلی برای مذاکره و تجارت آزاد؛

- درک راهبردها، اقدامات و رویکردهای موجود و برنامه‌ریزی شده جهت حفاظت از فضای سایبر؛ -شناسایی خطرها و آسیب‌پذیری‌های نوظهور در فضای سایبر، دامنه اختلال زیرساخت‌های حیاتی در برابر جاسوسی اقتصادی و نظامی و خرابه‌کاری عمدی^۴ و مقابله فنی و اتخاذ گام‌هایی جهت تنظیم مقررات برای روبه‌رو شدن با این خطرها؛

- بررسی و کشف بهترین راه‌ها به‌منظور توسعه اصول، هنجارها و قواعد جهت رفتار مناسب و مسئولانه دولت‌ها در فضای سایبر از جمله توسعه هنجارها و حقوق موجود و آتی و اقداماتی جهت تنظیم رفتار دولت‌ها در زمان مخاصمات؛

- بررسی نیاز به تصویب حقوق بین‌الملل بشر دوستانه جهت به‌کاربردن آن بویژه در جنگ سایبری؛

1. Cyber Space—New Frontier for Warfare

2. NATO and Cyber Defence: Hanging Together or Hanging Separately?

3. Challenges in Cybersecurity - Risks, Strategies, and Confidence-Building

4. ranging from disruptions of critical infrastructures to economical and military espionage and sabotage

- تقویت تلاش‌های بین‌المللی جهت حفظ فضای سایبری باز، ایمن از طریق ارتقای اقدامات اعتمادساز، اقدامات شفاف‌ساز، و امنیت، از جمله توسط سازمان امنیت و همکاری اروپا^۱، مجمع منطقه‌ای جنوب شرق آسیا (آس آن)^۲ و سازمان ملل متحد.

ابزار شاخص سایبری

توسعه خط‌مشی سایبری در نزد تمامی دولت‌های عضو سازمان ملل متحد به شکل فزاینده‌ای شروع شده است. طی دهه گذشته یونیدیر بر روی سیاست‌های سایبری در قلمرو امنیت بین‌الملل متمرکز شد و از سال ۲۰۱۲ پروژه‌ای را آغاز کرد که می‌توانست به‌عنوان یک ابزار کاربرمحور^۳ برای سیاست‌گذاران فضای سایبری مفید باشد. این پروژه تحقیقاتی در راستای فاز اول پروژه قابلیت‌های ملی، دکترین، سازمان‌ها و شفاف‌سازی و اعتمادسازی برای امنیت سایبری در حواصل ماه می سال ۲۰۱۲ تا ماه آوریل سال ۲۰۱۵ انجام گرفت و در سال ۲۰۱۳ اولین شاخص سایبری: روندها و واقعیت‌های امنیت بین‌المللی^۴ ارزیابی و منتشر گردید. هدف از این مطالعه به‌کارگیری یک تصویر فوری از اقدامات امنیت سایبری در سطوح ملی، منطقه‌ای و بین‌المللی^۵ با هدف کمک به سیاست‌گذاران و دیپلمات‌ها جهت درک پیچیدگی عرصه {سایبر}^۶ بود. در حال حاضر، برنامه تهدیدات نوظهور امنیت یونیدیر^۷ عهده دار انجام فاز دوم این پروژه می‌باشد و بر روی جنبه‌های بین‌المللی مرتبط با خط‌مشی ظرفیت‌سازی سایبری متمرکز است. یونیدیر طرح اولیه‌ای را برای دسترسی به این منابع به شکل برخط مهیا کرده است که قابلیت استفاده از این اطلاعات حیاتی را ارتقای می‌دهد.^۸

1. Organization for Security and Co-operation in Europe (OSCE)

2. Association of Southeast Asian Nations (ASEAN)

3. A User-Centred Tool

4. Cyber Index: International Security Trends and Realities

5. serve as a snapshot of [then] current cybersecurity activities at the national, regional, and international levels

6. help policymakers and diplomats understand the complexity of the arena

7. UNIDIR's Emerging Security Threats programme

8. support and improve capacity for informed participation in key dialogue and policy processes

مبحث ششم

عملکرد کمیسیون‌های تخصصی مجمع عمومی

گفتار یک: کمیسیون حقوق بین‌الملل

تدوین و توسعه، نقش اصلی را در توسعه و تحول حقوق بین‌الملل ایفا می‌کنند. در حقوق بین‌الملل، مانند سایر رشته‌های حقوقی، تدوین عبارت است از تبدیل و برگرداندن علمی قواعد عرفی به مجموعه‌ای از قواعد نوشته که به صورت منظم دسته‌بندی شده‌اند و توسعه حقوق، عمل و علمی است که قواعد جدید را بر مبنای حقوق موجود تأیید می‌کند یا تخصیص می‌دهد.

ماده ۱۵ اساسنامه کمیسیون حقوق بین‌الملل، سعی بر تفکیک صریح تدوین از توسعه تدریجی حقوق بین‌الملل دارد: اصطلاح «توسعه مترقیانه حقوق بین‌الملل» به معنی تهیه و آماده‌سازی پیش‌نویس یا طرح عهدنامه‌هایی در زمینه موضوعاتی است که هنوز در حقوق بین‌الملل قاعده‌مند نشده‌اند یا در آن موارد، حقوق هنوز به حد کافی در رویه کشورها توسعه نیافته است و اصطلاح تدوین حقوق بین‌الملل به معنی قاعده‌مند کردن بسیار صریح و منظم قواعد حقوق بین‌الملل در زمینه‌هایی است که قبلاً در آن‌ها رویه منطقی با سابقه و آموزه وجود داشته باشد. اکثر حقوق‌دانان امتیازات زیادی برای تدوین قائل‌اند که فهرست‌وار به ذکر اهم آن‌ها می‌پردازیم:

- تدوین، عامل توسعه حقوق بین‌الملل؛

- تدوین، عامل رفع ابهام از حقوق بین‌الملل؛

- تدوین، عامل انتشار و اشاعه حقوق بین‌الملل در افکار عمومی؛

- تدوین، عامل تشویق و برانگیختن فعالیت علمی.

در منشور ملل متحد، بر خلاف میثاق جامعه ملل، مقررات صریحی در مورد تدوین و توسعه حقوق بین‌الملل وجود دارد که در ماه ۱۳ آن منعکس است. مجمع عمومی برای امور زیر موجبات انجام مطالعات و صدور توصیه‌هایی را فراهم می‌کند:

ترویج همکاری بین‌المللی در امور سیاسی و ایجاد زمینه‌های مناسب برای توسعه تدریجی حقوق بین‌الملل و تدوین آن.

در اجرای مقررات مذکور، مجمع عمومی در ۲۱ نوامبر ۱۹۴۷، قطعنامه تشکیل کمیسیون دائمی حقوقدانان را به نام «کمیسیون حقوق بین‌الملل» صادر کرد.

طبق آخرین اصلاحیه اساسنامه کمیسیون، تعداد اعضای کمیسیون ۳۴ حقوقدان بین‌المللی هستند که به مدت پنج سال انتخاب می‌شوند و تجدید انتخاب آنان منعی ندارد. انتخاب به گونه‌ای انجام می‌شود که کمیسیون بتواند نماینده تمدن‌های اصلی و نظام‌های حقوقی مناطق عمده جغرافیایی جهان باشد.

اعضای کمیسیون از میان شخصیت‌های صاحب‌نظر در حقوق بین‌الملل انتخاب می‌شوند. نحوه انتخاب آنان به این صورت است که کشورهای عضو سازمان ملل متحد می‌توانند قبل از خاتمه مأموریت هر یک از اعضاء، اشخاص واجد صلاحیت را از میان اتباع خود، به دبیرکل سازمان معرفی نمایند. دبیرکل از بین افراد مذکور، اشخاص اصلاح را (به تعداد کرسی‌های لازم) به مجمع پیشنهاد می‌نماید. انتخاب قطعی و نهایی اعضا با مجمع عمومی است.

اعضای کمیسیون، هر چند توسط کشورهای متبوع خویش معرفی می‌شوند، اما در صورت انتخاب، به هیچ وجه نماینده آن‌ها محسوب نمی‌شوند، بلکه از استقلال عمل کامل برخوردارند. ضمناً در کمیسیون نباید بیش از یک عضو از اتباع هر کشور باشد.

اولین جلسه کمیسیون حقوق بین‌الملل در سال ۱۹۴۹ تشکیل شد و از آن پس، همه ساله به مدت دو تا سه ماه در ژنو، دوره اجلاسیه دارد و موضوعات مختلفی را برای تدوین و توسعه حقوق بین‌الملل مطالعه می‌کند و نتیجه آن را طی گزارشی به مجمع عمومی توصیه می‌نماید. مجمع عمومی در صورتی که طرح‌های پیشنهادی کمیسیون را قابل تصویب بداند، از کشورهای مختلف دعوت می‌کند تا در کنفرانسی که به این منظور تشکیل می‌شود، شرکت نمایند و تصمیم نهایی را اتخاذ کنند. برای نمونه می‌توان از کنفرانس وین ۱۹۶۹ در زمینه حقوق معاهدات نام برد.

طرز کار کمیسیون: هنگامی که کمیسیون موضوع خاصی را برای کار انتخاب و آن را برای تصویب مجمع عمومی به مجمع گزارش می‌کند. موقعی که مجمع عمومی از کمیسیون درخواست می‌نماید که درباره موضوعی کار کند، شیوه معمول از این قرار است که یکی از یک

اعضای خورا به‌عنوان «مخبر ویژه»^۱ کمیسیون انتخاب می‌کند و او نیز پیش‌نویسی را که معمولاً به شکل پیش‌نویس مواد و همراه نظریات تفسیری است برای مباحثه و تصویب توسط کمیسیون تهیه می‌کند. کمیسیون پس از اینکه به طور موقت، تعدادی از مواد مندرج در پیش‌نویس را تصویب کرد، آن‌ها را به کشورهای عضو تسلیم می‌نماید تا نظرهای خود را ابراز دارند. از آن پس، کمیسیون پیش‌نویس مواد و تفسیرها را با توجه به نظریاتی که کتباً ابراز یا شفاهاً در مباحثات مجمع عمومی بیان می‌شود، تجدید نظر و تکمیل می‌کند. هنگامی که بررسی مواد مندرج در پیش‌نویس تکمیل شد، تسلیم مجمع عمومی می‌شود و مجمع ممکن است کنفرانس بین‌المللی برای انعقاد یک معاهده درباره آن موضوع تشکیل دهد یا به شیوه دیگری عمل کند. قسمت اعظم کار کمیسیون، توسط مجمع عمومی به کنفرانس‌های تدوین ارجاع می‌شود و این کنفرانس‌ها، معاهدات چندجانبه ای تصویب می‌کنند و برای امضاء تصویب یا پذیرش کشورها مفتوح می‌گذارند.

در خصوص موضوع سایبر باید گفت: عدم دستیابی به اجماع در گزارش نهایی گروه کارشناسان دولتی در زمینه اطلاعات و ارتباطات در چارچوب امنیت بین‌الملل (GGE) در ژوئن ۲۰۱۷، آینده مباحث چندجانبه در مورد امنیت سایبری و دفاع سایبری مخصوصاً قابلیت اعمال حقوق بین‌الملل بر فضای سایبر مورد سؤال است. این امر ما را به این سمت رهنمون می‌سازد که دولت‌ها باید مذاکرات مربوط به قابلیت اعمال هنجارهای حقوق بین‌الملل را از مذاکرات سیاسی و راهبردی که در مورد هنجارهای مربوط به رفتار دولت‌ها و اقدامات اعتمادساز است تفکیک نمایند. به نظر می‌رسد که بحث‌های سیاسی و راهبردی باید به‌عنوان یک رویه دیپلماتیک بین دولتی باقی بماند. در حالی که مباحث در چارچوب حقوقی باید به یک نهاد بین‌المللی متشکل از کارشناسان حقوقی سپرده شود و نه دیپلمات‌ها و نمایندگان دولت‌ها. این نهاد بین‌المللی همان کمیسیون حقوق بین‌الملل است. شایان ذکر است که قابلیت اعمال حقوق بین‌الملل و منشور سازمان ملل در گزارش اجماعی گروه کارشناسان دولتی در سال ۲۰۱۳ و ۲۰۱۵ به رسمیت شناخته شده است. تعدادی از کشورها این موضع را در اظهار نظرهای خود و همچنین

1. Reporter ad hoc

در راهبردهای دفاع سایبری و امنیت سایبری به رسمیت شناخته اند.

اعمال حقوق بین‌الملل بر عملیات‌های سایبری عموماً در ادبیات مربوط مورد اعتراض واقع نشده است. بنابراین سؤال این نیست که آیا حقوق بین‌الملل قابل اعمال بر فضای سایبر است یا خیر. بلکه سؤال مورد چگونگی اعمال هنجارهای حقوق بین‌الملل بر این فضا می‌باشد.

البته باید گفت که ارجاع قانون‌گذاری بر فضای سایبر به کمیسیون حقوق بین‌الملل نه معجزه می‌کند و نه به فعالیت‌های خصمانه توسط بازیگران و کنشگران این فضا خاتمه می‌دهد. ضمن اینکه ورود این کمیسیون به فضای سایبر، ورودی دیر هنگام است و باید تاکنون شاهد اقداماتی از این کمیسیون می‌بودیم. به هر حال انتظار می‌رود کمیسیون کم‌کاری خود در این عرصه را جبران نماید و نقش برجسته خود را در قاعده‌مند کردن این فضا ایفا نماید.

کمیسیون حقوق بین‌الملل که از جانب مجمع عمومی به منظور تدوین و توسعه تدریجی حقوق بین‌الملل مأموریت یافت است، اگر چه تا سال ۲۰۱۹ مستقیماً به موضوعات فناوری‌های اطلاعات و ارتباطات و امنیت بین‌الملل ورود ننموده است اما این کمیسیون در اجلاس هفتادویکم خود در سال ۲۰۱۹، موضوعی تحت عنوان «حفاظت از داده‌های شخصی در جریان فرامرزی اطلاعات»^۱ را به برنامه کاری این کمیسیون اضافه نمود. در خصوص موضوعات جدید اضافه شده به برنامه کاری، این کمیسیون از معیارهای زیر استفاده می‌نماید:^۲

۱. موضوع باید منعکس‌کننده نیاز دولت‌ها در احترام به تدوین و توسعه تدریجی حقوق بین‌الملل باشد؛

۲. موضوع از جهت عملکرد دولت‌ها باید از پیشرفت کافی برخوردار باشد تا امکان تدوین و توسعه تدریجی آن میسر شود؛

۳. موضوع جهت تدوین و توسعه تدریجی باید محکم باشد؛

۴. کمیسیون نباید خود را فقط به موضوعات سنتی محدود کند، بلکه باید موضوعاتی را که منعکس‌کننده تحولات جدید در حقوق بین‌الملل بوده و بیانگر کلیت نگرانی‌های منطقی جامعه بین‌الملل باشد را مورد نظر قرار دهد.

1. "Protection of personal data in trans border flow of information"

2. <https://legal.un.org/ilc/> <https://legal.un.org/ilc/programme.shtml#a53>

گفتار دو: کمیسیون خلع سلاح ملل متحد

کمیسیون خلع سلاح ملل متحد^۱ یک نهاد مشورتی است که درباره موضوعات مرتبط با خلع سلاح، پیشنهادها را مورد در نظر قرار می‌گیرد و توصیه‌هایی را ارائه می‌دهد. دستور کار نشست‌های سه هفته‌ای این کمیسیون که در هر سال برگزار می‌شود دو بخش محتوایی را شامل می‌شود که این دو بخش برای سه سال متوالی مورد بحث قرار می‌گیرد. خروجی‌های {نشست‌های} این کمیسیون شامل اصول، خطوط راهنما و توصیه‌های اجماعی هستند که به مجمع عمومی فرستاده می‌شود. {در مجمع} موضوعات توسط دولت‌های عضو تعیین می‌شوند و از طریق قطعنامه در کمیته اول مورد توافق قرار می‌گیرند. برابر بررسی به عمل آمده، این کمیسیون هنوز به موضوعات فناوری‌های اطلاعات و ارتباطات و امنیت بین‌المللی ورود ننموده است.^۲

نتیجه‌گیری فصل اول

حقوق بین‌الملل فضای سایبر در مقایسه با سایر حوزه‌های حقوق بین‌الملل (از جمله حوزه‌های معاصر مثل حقوق فضای ماورای جو) از توسعه و تکامل اندکی برخوردار بوده است. بنابراین این حوزه فاقد یک معاهده یا کنوانسیون در حال اجرا و یا حتی در حال شکل‌گیری در سطح بین‌الملل می‌باشد. فقط فعالیت‌هایی در سطوح منطقه‌ای صورت گرفته است. فقر و ضعف حقوق بین‌الملل فضای سایبر عمدتاً ناشی از عملکرد غیر سازنده دولت ایالات متحده و همچنین متأثر از ویژگی‌های منحصر به فرد این فضا می‌باشد و سبب بروز مشکلاتی در مقوله انتساب گردیده که شکل‌گیری مسئولیت برای بازیگران را مشکل می‌سازد. در سطح سازمان ملل تنها دورکن مجمع عمومی و شورای اقتصادی و اجتماعی (اکوسوک) در زمینه سایبری فعالیت در خوری داشته‌اند. شاید مهم‌ترین بخش سازمان ملل که در حوزه فضای سایبر ورود کرده است، کمیته اول مجمع عمومی باشد که مأموریت خلع سلاح و امنیت بین‌الملل را یدک می‌کشد. عملکرد این کمیته موجب شکل‌گیری جریانی شده است که می‌توان آن را جریان امنیتی فضای سایبر نامید. منظور از جریان سایبری این است که جهان و مخصوصاً دولت‌ها چه نگاهی به خطرهای و مضرات

1. United Nations Disarmament Commission (UNDC)

۲. مدارک و مستندات در فایل الکترونیکی موجود می‌باشد.

فضای سایبر دارند و آن را بستر چه تهدیداتی می‌دانند و به تبع آن چه سیاست‌ها، راهبردها و راهکارهایی برای مقابله با این خطرها و تهدیدات اتخاذ و اجرا می‌کنند. جریان امنیتی مؤید این است که فضای سایبر این قابلیت را دارد که صلح و امنیت جهان را به مخاطره اندازد. بنابراین این نگاه بر این باور است که فضای سایبر می‌تواند در جهت مخالف اهداف مربوط به تقویت ثبات و امنیت بین‌المللی باشد. از این منظر، تأمین امنیت فضای سایبر در چهارچوب امنیت بین‌المللی تعریف می‌شود. یعنی امنیت فضای سایبر جزء جداناپذیر امنیت بین‌المللی است.

دولت روسیه در سال ۱۹۹۸ اولین قطعنامه را در ارتباط با تأمین امنیت فضای سایبر به کمیته اول مجمع عمومی ارائه کرد. عنوان کمیته اول یعنی کمیته خلع سلاح و امنیت بین‌الملل، خود مؤید آن است که این قطعنامه چه دیدگاهی به فضای سایبر دارد. ضمن اینکه محتوای قطعنامه نیز این دیدگاه را تأیید می‌کند. زیرا در این قطعنامه به قابلیت کاربرد نظامی فضای سایبر تصریح شده است.

این قطعنامه از سال ۱۹۹۸ تا کنون، هر سال به کمیته اول ارائه شده و پس از طی تشریفات خاص، به تصویب مجمع عمومی رسیده است. روند تصویب این قطعنامه و واکنش آمریکا به آن، طول این سال‌ها، تاریخ پرفراز و نشیبی داشته است. تغییرات تاکتیکی آمریکا در اتخاذ موضع درباره این قطعنامه در خلال این سال‌ها به خوبی نشان می‌دهد که این قطعنامه‌ها به جای اینکه به تأمین امنیت فضای سایبر کمک کند به تابعی از رقابت‌های پیدا و پنهان قدرت‌های سایبری تبدیل شده است. به خاطر ناکارآمدی همین قطعنامه‌هاست که امنیت فضای سایبر از سال ۱۹۹۸ تا کنون هر سال در مقایسه با سال قبل وخیم‌تر شده است. رأی مخالف آمریکا به قطعنامه روسیه در برخی سال‌ها و بارگیری روسیه در ارائه قطعنامه در این سال‌ها، ورود و خروج‌های آمریکا در حمایت یا عدم حمایت از این قطعنامه، همه گواه آن است که موضع آمریکا همیشه تابعی از منافع این کشور است که در بعضی سال‌ها ایجاب می‌کرده است که از قطعنامه حمایت کند و در برخی سال‌ها مقابل قطعنامه سنگ‌اندازی کند. این روند همچنان ادامه دارد و بعید به نظر می‌رسد که در آینده نیز چشم‌انداز روشنی برای تأمین امنیت فضای سایبر از قبیل قطعنامه‌های کمیته اول بتوان تصویر کرد. چیزی که در عمل شاهد آن هستیم حرکت

روزافزون غرب به تدوین قواعد جنگی فضای سایبر است که حاکی از عدم توفیق فعالیت‌های کمیته اول در این خصوص می‌باشد.

آنچه در سطور بالا ذکر شد مربوط به روند قطعنامه موسوم به قطعنامه امنیت سایبری است که روسیه از بدو امر پرچمدار آن در کمیته اول بوده است. نفس این امر، هرگز خوشایند آمریکا نبوده است؛ چرا که از دید آن‌ها، قطعنامه فضای سایبر که طراحی این فضا ریشه در این کشور دارد، نباید در دست دولت دیگری باشد. یکی دیگر از دلایل کارشکنی آمریکا در قبال این قطعنامه نیز همین امر بوده است. اما روس‌ها همیشه ابتکار عمل را در دست داشتند. همین امر باعث گردید که روس‌ها با رونمایی از پیش‌نویس کنوانسیون امنیت سایبری در سال ۲۰۱۱، آمریکا را بهت‌زده کنند. شگفتی آمریکایی‌ها با رونمایی روس‌ها از کردارنامه امنیت سایبری تکمیل شد. هر چند کنوانسیون پیشنهادی روسیه به خاطر مشکلاتش نتوانست توفیقی در عرصه بین‌المللی به‌دست آورد، اما روس‌ها توانستند کردارنامه خود را در سال ۲۰۱۵ به‌روزرسانی کنند. یکی از اقدامات آمریکا در سازمان ملل در جهت مقابله با اقدامات دیپلماتیک روسیه، ارائه قطعنامه فرهنگ سایبری به کمیته دوم بود که چندان توفیقی نیز به‌دست نیاورد.

یکی دیگر از عرصه‌های تقابل منافع قدرت‌های سایبری، گروه کارشناسان دولتی می‌باشد. تاریخ تحولات این گروه دقیقاً مثل قطعنامه روسیه از رقابت‌های قدرت‌های عمده سایبری شکل گرفته است. از ناکامی گروه اول گرفته تا اقدامات گروه‌های بعدی که توفیقات اندکی داشته‌اند، انعکاسی از رقابت‌های سایبری صاحبان اصلی آن را به نمایش می‌گذارد. دستاوردهای این گروه هیچ‌سختی با اوضاع رو به وخامت فضای سایبر ندارد. تشکیل گروه‌های مختلف و متوالی، بدون یک دستاورد مشخص و قابل توجه، موجب شده است که در سال ۲۰۱۷ ادامه فعالیت این گروه‌ها با شکست مواجه گردد.

کوچ گروه کارشناسان دولتی (G.G.E) از قطعنامه روسیه به قطعنامه آمریکا و تشکیل اولین گروه کاری باز (O.E.W.G) تحت قطعنامه روسیه در سال ۲۰۱۸ تعامل بین صاحبان قدرت سایبری را پیچیده تر کرد. آنچه تا سال ۲۰۲۰ شاهد آن هستیم این است که به جای اینکه شاهد هم‌افزایی بین این دو گروه باشیم شاهد رقابت بین آن‌ها هستیم و مباحثی مانند اینکه اصالت

و اهمیت با کدام گروه است.

در مجموع به نظر می‌رسد که هیچ تناسبی بین وخامت امنیتی روزافزون فضای سایبر و فعالیت‌های صورت گرفته برای تأمین امنیت آن وجود ندارد و انتظار می‌رود که این شکاف در آینده نیز بیشتر شود؛ چرا که تداخل و تضاد منافع قدرت‌های عمده سایبری مانع از همگرایی واقعی آن‌ها برای تأمین امنیت فضای سایبر شده است و چشم‌انداز روشنی نیز برای رفع این تضادها دیده نمی‌شود.

همان‌گونه که توضیح داده شد منظور از جریان امنیتی این است که فضای سایبر قابلیت اختلال در امنیت بین‌الملل را دارد و بستری برای جنگ محسوب می‌شود. اما جریان اقتصادی، فضای سایبر را دارای قابلیت جرایم اقتصادی می‌داند. نگاه جریان اقتصادی به فضای سایبر همان‌گونه که از عنوانش پیداست، اقتصادمحور است نه امنیت‌محور. جریان اقتصادی نگران تخلفات و جرایم مالی و اقتصادی در بستر فضای سایبر است. بنابراین اقدامات این جریان نیز درصدد مقابله با این نوع جرایم و تخلفات است. سکاندار این جریان که در کمیته سوم مجمع عمومی متمرکز است، دولت آمریکا است. دو سال بعد از اینکه روسیه ابتکار عمل را در کمیته اول به‌دست گرفت، ایالات متحده نیز سعی کرد این عقب‌ماندگی حقوقی دیپلماتیک را در کمیته سوم با ارائه قطعنامه مقابله با جرایم اقتصادی سایبری جبران نماید.

در کمیته دوم نیز تحرکاتی از طرف گروه ۷۷ با ارائه قطعنامه‌ای تحت عنوان فناوری اطلاعات و ارتباطات صورت گرفت که نوعاً مطالبه‌گر بود و هدف آن رفع شکاف دیجیتالی بین کشورهای پیشرو و در حال توسعه بود.

اما مهم‌ترین نکته در حوزه جرایم سایبری این است که تنها کنوانسیون حوزه سایبر با محوریت جرایم سایبری در قالب شورای اروپا در حال اجراست. هر چند این کنوانسیون خارج از سازمان ملل تصویب و اجرا شده ولی به خاطر همین ویژگی‌های انحصاری، حائز اهمیت فراوان است. به طوری که حتی برخی کشورها خارج از قلمرو شورای اروپا نیز به این کنوانسیون ملحق شده‌اند. البته عکس این موضوع نیز صادق است. به طوری که روسیه با وجود عضویت در شورای اروپا، تنها کشوری است که این کنوانسیون را امضاء نکرده است که دلایل آن نیز بررسی گردید.

اما آنچه اروپا را در سال ۲۰۱۷ دچار بهت و حیرت کرد، رونمایی روسیه از پیش‌نویس کنوانسیون جرایم سایبری می‌باشد. روسیه که در سال ۲۰۱۱ با رونمایی از پیش‌نویس کنوانسیون امنیت سایبری، آمریکا را دچار شگفتی کرده بود، در سال ۲۰۱۷ نیز با رونمایی از پیش‌نویس کنوانسیون جرایم سایبری، اروپا را شگفت‌زده کرد. روسیه که تا دیروز برای امضای کنوانسیون بوداپست تحت فشار بود، امروز پیش‌نویس خود را مطرح کرده و همه کشورها را برای حمایت از آن فرا می‌خواند. پیش‌نویس روسیه، فرصتی برای سایر کشورها نیز تلقی می‌گردد؛ چرا که قدرت چانه‌زنی آن‌ها را برای الحاق به هر یک از دو کنوانسیون بوداپست یا روسیه یا حتی ابتکار ارائه پیش‌نویس کنوانسیون سوم افزایش داده است. بی‌جهت نیست که کشورهای اروپایی که تا دیروز حاضر نبودند بعد از ۱۵ سال، کنوانسیون خود را بازنگری کنند، امروزه صحبت از این موضوع به میان می‌آورد و ادبیات تحکم‌آمیز دیروز برای الحاق به کنوانسیون را به ادبیات نرم خواهش و تمنا تبدیل کرده‌اند. روسیه در قطعنامه ۲۰۱۹ کمیته سوم با پیشنهاد تشکیل کمیته کارشناسان برای شکل‌گیری کنوانسیون جرایم سایبری، اقدام بلندی برداشت که بر خلاف خوشایند شورای اروپا بود. واکنش‌های هیجانی و غیر حقوقی غرب در مقابل اقدامات و ابتکارات حقوقی و دیپلماتیک روسیه حاکی از تشدید نگرانی آن‌هاست. شایسته است از فرصت به‌وجود آمده، در راستای گنجانیدن ملاحظات سایبری کشورمان، حداکثر استفاده را به عمل آورد.

در خصوص عملکرد شورای حقوق بشر و سایر قطعنامه‌های حقوق بشری نیز باید گفت: حقوق بشر که فی‌نفسه، ترکیبی زیبا برای شأن‌الای انسانی محسوب می‌شود به خاطر استفاده‌های ابزاری از سوی جوامع غربی، به عبارتی اشمئزاز‌آور بدل شده است که از آن به‌عنوان اهرمی علیه دولت‌ها و ملت‌های مستقل استفاده می‌شود. فضای سایبر نیز از این دوگانگی غربی‌ها مصون نمانده است. افشاگری‌های اسنودن از سال ۲۰۱۳ به بعد نشان داد که دولت آمریکا برای هیچ یک از موازین حقوق بشری در فضای سایبر احترام و تعهدی قائل نیست.



فصل دوم: سایر ارکان مبحث اول: شورای اقتصادی و اجتماعی سازمان ملل (اکوسوک)

گفتار یک: اکوسوک و فضای سایر

شورای اقتصادی و اجتماعی (اکوسوک)^۱ یکی از ارکان اصلی سازمان ملل است، اما تحت امر مجمع عمومی فعالیت می‌کند. اعضای این شورا در بدو تأسیس ۱۸ دولت بودند. سپس به ۲۷ دولت افزایش پیدا کرد. آخرین تغییر در سال ۱۹۷۴ صورت گرفت و اعضای آن به ۵۴ دولت رسید. این اعضا بر اساس توزیع عادلانه جغرافیایی انتخاب می‌شوند. هر دولت در شورا برای سه سال انتخاب می‌شود. اکوسوک از طریق کمیسیون‌های فرعی، به انجام وظایف خود می‌پردازد. قطعنامه‌های اکوسوک، جنبه توصیه دارند و الزامی نیستند. اکوسوک قطعنامه‌های خود را در اجلاس مجمع عمومی سازمان ملل مطرح می‌کند و سپس در مورد آن تصمیم‌گیری می‌کند. در حال حاضر بیش از ۲۰۰۰ سازمان غیر دولتی با اکوسوک طرف مشورت هستند. بر اساس ماده ۷۱ منشور ملل متحد، اکوسوک می‌تواند از سازمان‌های غیردولتی در مقام مشاوره استفاده کند.^۲ شورای اقتصادی و اجتماعی (اکوسوک) برای اولین بار در سال ۲۰۰۴ قطعنامه‌ای درباره جرایم مرتبط با هویت تصویب کرد. قطعنامه ۲۰۰۴/۲۶ درباره «همکاری بین‌المللی در پیشگیری، تحقیق، تعقیب و مجازات کلاهبرداری، سوءاستفاده مجرمانه و جعل هویت و جرایم مرتبط^۳

1. Economic and Social Council. (ECOSOC)

۲. برای اطلاعات بیشتر رک: تقریرات درس حقوق سازمان‌های بین‌المللی، دکتر ابراهیم بیگزاده

3. International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes

در بین کشورهای عضو تمرکز نمود و درباره گسترش فناوری‌های اطلاعاتی و ارتباطاتی مدرن که طیف گسترده‌ای از فرصت‌های جدید را برای کلاهبرداری و سوءاستفاده مجرمانه و جعل هویت ایجاد نموده، ابراز نگرانی کرد.^۱ این قطعنامه همچنین از دبیرکل درخواست کرد. تا یک گروه از کارشناس بین دولتی جهت مطالعه درباره کلاهبرداری و سوءاستفاده مجرمانه و جعل هویت در فضای سایبر تشکیل دهد. دولت‌های کانادا و انگلستان برای حمایت و پشتیبانی از این گروه اعلام آمادگی کردند.^۲

قطعنامه بعدی یعنی قطعنامه ۲۰۰۷/۲۰ مربوط به سال ۲۰۰۷ بیان می‌کند که کنوانسیون شورای اروپا در ارتباط با جرایم سایبری (کنوانسیون بوداپست) که یک سند قانونی بین‌المللی است، برای تصویب یا الحاق از سوی کشورهای غیرعضو شورا باز می‌باشد. این قطعنامه، کشورهای غیرعضو را ترغیب می‌نماید تا الحاق به آن را مورد توجه قرار دهند. نفود اروپا در تنظیم محتوای قطعنامه را از اینجا می‌توان درک کرد. این قطعنامه همچنین از «دفتر سازمان ملل متحد در ارتباط با مواد مخدر و جرایم»^۳ می‌خواهد تا در صورت درخواست کشورهای عضو و منوط به دسترسی بودن منابع و بودجه لازم، زمینه کمک‌های کارشناسی در زمینه قانون و همچنین سایر اشکال کمک‌های فنی برای کشورهای عضو را مهیا سازد.

قطعنامه ۲۰۰۹/۲۲ به تشریح درخواست خود از UNODC می‌پردازد و به گزارش این گروه کارشناس اشاره می‌نماید.

گفتار دو: کمیسیون پیشگیری از جرم و عدالت کیفری

کمیسیون پیشگیری از جرم و عدالت کیفری^۴، به موجب قطعنامه شماره ۱۹۹۲/۱ شورای اقتصادی، اجتماعی (اکوسوک) و به درخواست مجمع عمومی^۵ به‌عنوان یک کمیسیون کارکردی تأسیس شد. این کمیسیون به‌عنوان یک نهاد ارشد سیاستگذار سازمان ملل در زمینه پیشگیری از جرم و عدالت کیفری زیر نظر اکوسوک فعالیت می‌کند. اکوسوک طی قطعنامه شماره ۱۹۹۲/۲۲،

1. UN ECOSOC resolution 2004/26

2. UN ECOSOC resolution 2009/22; UN ECOSOC E/CN.15/2009/2 and Corr.1

3. United Nations Office on Drugs and Crime

4. Commission on Crime Prevention and Criminal Justice (CCPCJ)

5. General Assembly (GA) resolution 46/152

دستور کار و اولویت‌های این کمیسیون را مشخص کرده است که شامل ارتقای اقدامات بین‌المللی برای مبارزه با جرایم ملی و فراملی و افزایش کارایی و عدالت‌محوری سیستم‌های دولتی در برخورد با مجرمان است. این کمیسیون همچنین به دولت‌ها پیشنهاد داده است که جهت تبادلات کارشناسی، تجربیات و اطلاعات، اقدام به تشکیل مجمعی بین خود نمایند تا راهبردهای ملی و بین‌المللی را توسعه دهند و اولویت‌های خود برای مبارزه با جرم را تعیین کنند. این کمیسیون در مجموعه سازمان ملل به‌عنوان نهاد هماهنگ‌کننده بین همه اجزای این سازمان که در زمینه پیشگیری از جرم فعالیت می‌کنند، عمل می‌کند. مسئولیت برگزاری کنگره‌های سازمان ملل نیز برعهده همین کمیسیون است. اعلامیه‌های کنگره از طریق این کمیسیون و اکوسوک برای تأیید به مجمع عمومی ارسال می‌شود.^۱

اولین جلسه «کمیسیون پیشگیری از جرم و عدالت کیفری» در سال ۱۹۹۲ تشکیل شد. اما اولین بار در سال ۲۰۱۰ بود که جرائم سایبری به‌صورت یک موضوع برجسته در گزارش‌های سالانه آن ظهور پیدا کرد. در گزارش سومین جلسه کمیسیون در سال ۱۹۹۴ برای اولین بار، همکاری‌های فنی در ارتباط با جرایم کامپیوتری مورد توجه قرار می‌گیرد و از نهمین کنگره سازمان ملل^۲ (سال ۱۹۹۵) می‌خواهد که این موضوع را مورد نظر قرار دهد.^۴ این درخواست به این خاطر صورت گرفت که هشتمین کنگره سازمان ملل^۵ در سال ۱۹۹۰ به این موضوع ورود کرده و پیشگیری از جرم و رفتار با مجرمان^۶ را در دستور کار خود قرار داده بود و قطعنامه‌ای در ارتباط با جرایم کامپیوتر صادر کرده بود. در نهایت، کمیسیون در سال ۱۹۹۸ از مجمع عمومی می‌خواهد تا کارگاهی در ارتباط با جرائم مرتبط با شبکه کامپیوتری را در دستور کار دهمین کنگره سازمان ملل (سال ۲۰۰۰) قرار دهد. کمیسیون در سال ۱۹۹۹ پیش‌نویس قطعنامه‌ای را به شورای اقتصادی و اجتماعی سازمان ملل^۷ در ارتباط با «کار برنامه پیشگیری از جرم و عدالت کیفری سازمان ملل متحد» ارائه می‌دهد و از دبیرکل می‌خواهد تا مطالعه‌ای را در ارتباط با جرائم مرتبط

1. <http://www.unodc.org/unodc/commissions/CCPCJ/>

3. Ninth United Nations Congress

4. UN ECOSOC E/1994/31: 65

5. Eighth United Nations Congress

6. Prevention of Crime and the Treatment of Offenders

7. ECOSOC

۲. کنگره‌های سازمان ملل هر پنج سال یک بار برگزار می‌شود.

با کامپیوتر انجام دهد و نتایج آن را به دهمین جلسه کمیسیون (۲۰۰۱) گزارش دهد. این پیش‌نویس همچنین به جلسه تخصصی که در ارتباط با جرائم مرتبط با شبکه‌های کامپیوتری در سال ۱۹۹۸ در ژاپن برگزار شده بود، اشاره می‌کند. در گزارش سال ۲۰۰۰ کمیسیون به عباراتی مثل «سایبری»، «اینترنت» و «هویت» اشاره نشده و تنها یک بار به «فناوری» و سه بار نیز به «کامپیوتر» اشاره شده است. همین‌الگو در گزارش سال ۲۰۰۱ کمیسیون نیز تکرار شد.

گزارش سال ۲۰۰۲ کمیسیون، برای اولین بار به عبارت «سایبری» اشاره نمود و آن را دو مرتبه به کار برد و همچنین به کنوانسیون جرائم سایبری^۱ اشاره کرد. در گزارش سال ۲۰۰۲ کمیسیون با هدف ارائه پیشنهادی مبنی بر برگزاری کارگاهی درباره «اقدامات علیه جرائم مرتبط با فناوری برتر و کامپیوتر»^۲ مربوط به یازدهمین کنگره سازمان، عبارت «اینترنت» سه مرتبه و «کامپیوتر» تنها یک مرتبه مورد اشاره واقع شد. مجدداً در گزارش سال ۲۰۰۳ هیچ اشاره‌ای به «سایبری» و «فناوری» و «هویت» صورت نگرفت. اولین بار در گزارش سال ۲۰۰۴ کمیسیون است که «کنوانسیون سازمان ملل متحد علیه جرائم سایبری»^۳ مورد درخواست قرار می‌گیرد. این گزارش همچنین اولین پیش‌نویس قطعنامه برای ECOSOC در ارتباط با «همکاری بین‌المللی در پیشگیری، رسیدگی، تعقیب و مجازات کلاهبرداری، سوءاستفاده مجرمانه و جعل هویت و جرائم مربوط»^۴ را در بر دارد. گزارش سال‌های ۲۰۰۵ و ۲۰۰۶ اشاره متعددی به عبارت یادشده داشته‌اند اما بدون اینکه اقدامات بیشتری را در پیش گیرند. گزارش سال مجدداً پیش‌نویس قطعنامه از طرف ECOSOC در ارتباط با «همکاری بین‌المللی در پیشگیری، تحقیق، تعقیب و مجازات کلاهبرداری، سوءاستفاده مجرمانه و جعل هویت مربوط» همانند سال ۲۰۰۴ در بردارد. در سال ۲۰۰۸ کمیسیون تصمیم می‌گیرد تا «کلاهبرداری اقتصادی و جرائم مرتبط با هویت» به‌عنوان یکی از دو مبحث موضوعی دوازدهمین کنگره سازمان ملل در دستور کار قرار گیرد.

در سال ۲۰۰۹، کمیسیون مباحث موضوعی در ارتباط با کلاهبرداری اقتصادی و جرائم مرتبط

1. Convention on Cybercrime

2. measures against high-technology and computer-related crime

3. United Nations Convention against cybercrime

4. "International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes"

با هویت را برگزار نمود و پیش‌نویس قطعنامه‌ای را برای تصویب از سوی ECOSOC در ارتباط با « همکاری بین‌المللی در پیشگیری، تحقیق، تعقیب و مجازات کلاهبرداری اقتصادی و جرائم مرتبط با هویت» آماده کرد.^۱

گزارش سال ۲۰۱۰ مجدداً ضرورت یک کنوانسیون جهانی علیه جرائم سایبری را مطرح ساخت. این گزارش همچنین درخواست تشکیل یک گروه کارشناسان دولتی با دوره فعالیت زمانی نامحدود را ارائه کرده تا مطالعه‌ای جامع درباره مشکل جرائم سایبری و واکنش‌های کشورهای عضو جامعه بین‌الملل و بخش خصوصی در زمینه‌هایی مثل تبادل اطلاعات در ارتباط با قوانین ملی کشورهای عضو و همکاری بین‌المللی انجام دهد.^۲

در مورد گزارش سال ۲۰۱۱ باید گفت که این گزارش بیشترین اشاره به «سایبر» را داشته است. این گزارش، قطعنامه ۲۰/۷ با عنوان «ارتقای فعالیت‌های مرتبط با مبارزه با جرائم سایبری شامل کمک‌های فنی و ظرفیت‌سازی» را شامل می‌شود. این گزارش تأکید می‌کند که «کنوانسیون علیه جرائم سازمان یافته فراملی»^۳ را می‌توان در خصوص جرائم سایبری در چهارچوب جرائم سازمان یافته اعمال کرد. این گزارش همچنین شامل پیش‌نویس قطعنامه‌ای تحت عنوان تحت عنوان «پیشگیری و حفاظت و همکاری بین‌المللی علیه استفاده از فناوری‌های اطلاعاتی جدید در جهت سوءاستفاده و بهره‌کشی از کودکان»^۴ را در بر می‌گیرد که برای اولین بار به مزاحمت سایبری اشاره شده است.

گفتار سه: کمیسیون مبارزه با مواد مخدر

این کمیسیون^۵ در سی‌ونهمین جلسه خود در سال ۱۹۹۶ بر نقش اینترنت در خصوص جرائم مرتبط با قاچاق مواد مخدر تمرکز کرد.^۶ جالب توجه است که یکی از اسناد قبلی عمدتاً بر قابلیت‌ها و کاربرد بالقوه مثبت اینترنت در کنترل مواد مخدر تمرکز کرده بود. در سال ۱۹۹۹، گزارش مربوط به جلسه سالانه کمیسیون، فصل مستقلی را به «تأثیر شبکه‌های ارتباطی مانند

1. UN ECOSOC E/2009/30

2. UN ECOSOC E/2010/30; UN ECOSOC resolution 2010/18; UN General Assembly A/RES/65/230

3. Convention against Transnational Organized Crime

4. Prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children

5. The Commission on Narcotic Drugs on the Internet and drug trafficking

6. UN ECOSOC E/1999/28/Rev.1: p. 45

اینترنت بر معضل مواد مخدر^۱ اختصاص داده بود.^۲ در سال ۲۰۰۰، در نهایت کمیسیون، قطعنامه‌ای را تصویب کرد که صرفاً بر عنوان «اینترنت» تمرکز داشت و توجه اکوسوک را به خود جلب نمود. برخلاف اسناد قبلی، این قطعنامه بر چگونگی سوءاستفاده از «تارنمای جهان گستر»^۳ برای تبلیغات و فروش داروهای غیرقانونی تأکید کرده بود. این موضوع از سوی ایالات متحده مورد حمایت قرار گرفت، اما چین و روسیه از آن حمایت نکردند.^۴ پس از سال ۲۰۰۰، هیچ قطعنامه‌ای به صورت خاص به اینترنت نپرداخت، اما به عنوان بخشی از مباحث کمیسیون مکرراً به آن اشاره شده است. کمیسیون در سال ۲۰۰۴ با اشاره به قطعنامه سال ۲۰۰۰، پیش‌نویس قطعنامه‌ای را برای ارائه به ECOSOC آماده نمود که تحت عنوان قطعنامه شماره ۲۰۴/۴۲ ECOSOC راجع به «فروش کنترل شده داروهای قانونی به صورت بین‌المللی به افراد از طریق اینترنت»^۵ به تصویب رسید.^۶ این پیش‌نویس از سوی ایالات متحده مورد حمایت قرار گرفت، اما روسیه و چین از آن حمایت نکردند. در سال ۲۰۰۵، کمیسیون قطعنامه جدیدی را این بار تحت عنوان «تقویت همکاری بین‌المللی به منظور پیشگیری از استفاده از اینترنت در ارتکاب جرائم مرتبط با مواد مخدر»^۷ به تصویب رساند.^۸ کمیسیون همچنان در این زمینه فعال است.

گفتار چهار: اتحادیه بین‌المللی مخابرات

بند یک: اسناد اجلاس ژنو ۲۰۰۳

مرحله اول اجلاس جهانی سران درباره جامعه اطلاعاتی در تاریخ ۱۰ تا ۱۲ دسامبر ۲۰۰۳ در ژنو برگزار گردید و بعد از سه روز فعالیت نفس گیر، با تجمیع نتایج اجلاس‌های مقدماتی، نظرهای کارشناسی و سایر جوانب و با وجود کارشکنی‌های آمریکا، با صدور دو سند مهم به کار خود پایان داد:

۱. اعلامیه اصول؛ ۲. طرح اقدام.

عنوان کامل اعلامیه اصول عبارت بود از: «اعلامیه اصول، ایجاد و ساخت جامعه اطلاعاتی: چالش

1. the impact of communication networks, such as the Internet, on the drug problem

2. UN ECOSOC E/1999/28/Rev.1

3. World Wide Web

4. UN ECOSOC resolution 43/8 in E/2000/28

5. Sale of internationally controlled licit drugs to individuals via the Internet.

6. UN ECOSOC E/2004/28

7. Strengthening international cooperation in order to prevent the use of the Internet to commit drug-related crim

8. UN ECOSOC resolution 48/5 in E/2005/28

جهانی در هزاره جدید» که از سه بخش و ۶۷ ماده تشکیل می‌شد:

بخش اول تحت عنوان «نظر مشترک ما درباره جامعه اطلاعاتی» مواد ۱ تا ۱۸ اعلامیه اصول را به خود اختصاص داده است در این بخش جامعه اطلاعاتی چنین تعریف شد:

«ما نمایندگان مردم جهان، گرد آمده در ژنو از ۱۰ تا ۱۲ دسامبر ۲۰۰۳ برای برگزاری دور اول نشست جهانی جامعه اطلاعاتی، میل و تعهد مشترک خود به ایجاد جامعه اطلاعاتی مردم‌محور، همه‌شمول و توسعه‌مدار را اعلام می‌داریم؛ جامعه‌ای که در آن همگان بتوانند اطلاعات و دانش خلق کنند، به آن دسترسی داشته باشند، آن را به کار گیرند و به اشتراک بگذارند، تا افراد، اجتماعات و مردمان قادر شوند بر پایه اهداف و اصول منشور ملل متحد و احترام کامل و پاسداشت بیانیه جهانی حقوق بشر، در ارتقای توسعه پایدار و بهبود کیفیت زندگی خویش، به طور کامل استعدادهای خود را محقق سازند.»

بخش دوم اعلامیه اصول تحت عنوان «جامعه اطلاعاتی برای همه: اصول کلیدی» مواد ۱۹ تا ۶۴ اعلامیه را شامل می‌شود. بخش سوم اعلامیه نیز تحت عنوان «به سوی جامعه اطلاعاتی برای همه بر اساس به اشتراک گذاری دانش» مواد ۶۵ تا ۶۷ اعلامیه اصول را به خود اختصاص داده است. طرح اقدام ژنو از ۲۹ ماده تشکیل شده است. اگر ما، اعلامیه اصول را دیدگاه و بینش اجلاس سران جهان درباره جامعه اطلاعاتی تلقی کنیم می‌توان گفت که طرح اقدام ۲۹ ماده‌ای، سازوکار و نقشه راه رسیدن به آن بینش است. به عبارت دیگر، اعلامیه اصول، تصویری از جامعه اطلاعاتی ارائه می‌دهد و طرح اقدام، تکلیف دولت‌ها و سایر ذی‌نفعان را در این جامعه مشخص می‌کند.^۱

بند دو: اسناد اجلاس تونس ۲۰۰۵

اجلاس جهانی سران درباره جامعه اطلاعاتی در تاریخ ۱۶ تا ۱۸ نوامبر ۲۰۰۵ در تونس برگزار گردید. اجلاس تونس هم دو سند به نام‌های تعهد تونس و دستور جلسه تونس برای جامعه اطلاعاتی به تصویب رساند. تعهد تونس ۴۰ ماده داشت که همان اعلامیه اصول و در واقع بینش اجلاس بود، مثل ژنو.

۱. باتوجه به اینکه آقای دکتر کاظم معتمد نژاد در کتاب «اجلاس جهانی سران در باره جامعه اطلاعاتی» به صورت کامل و مفصل به این موضوع پرداخته است جهت پرهیز از تکرار ترجمه این اسناد، علاقمندان محترم را جهت اطلاعات بیشتر به این کتاب که توسط نشر شهر منتشر شده است راهنمایی می‌کنیم. تحلیل کامل تر این اسناد را نیز می‌توانید در کتاب «به سوی کنوانسیون سایبری» تألیف آقای نصراله سلطانی مطالعه نمایید.

دستور جلسه تونس برای جامعه اطلاعاتی هم ۱۲۲ ماده داشت که همان طرح اقدام و در واقع نقشه عملیاتی در راستای تحقق بینش بود. مواد دستور جلسه تونس برای جامعه اطلاعاتی به این شکل تنظیم شده بود:

مواد ۱ و ۲ به مقدمه اختصاص یافته است.

مواد ۳ تا ۲۸ به سازوکارهای مالی برای مواجهه با چالش‌های ICT برای توسعه پرداخته است. مواد ۲۹ تا ۸۲ به موضوع حاکمیت اینترنت پرداخته است. (اختصاص بیش از ۵۰ ماده به بحث حاکمیت اینترنت به جهت اهمیت فوق‌العاده این موضوع).

مواد ۸۳ تا ۱۲۲ مربوط به اجرا و تعقیب مسائل است.

دستور جلسه تونس برای جامعه اطلاعاتی یک ضمیمه ۱۱ ماده‌ای هم داشت که به ۱۱ خط عمل جامعه اطلاعاتی معروف شد و همچنان دنبال می‌شود.

مواد ۲۹ تا ۸۲ دستور جلسه تونس مربوط به حاکمیت اینترنت بود. یعنی اختصاص بیش از ۵۰ ماده به بحث حاکمیت اینترنت به لحاظ اهمیت فوق‌العاده آن. تشکیل مجمع راهبری (حاکمیت) اینترنت تحت ماده ۷۲ دستور جلسه تونس به یکی از مهم‌ترین نتایج اجلاس جهانی سران درباره جامعه اطلاعاتی تبدیل شد که هدف اصلی آن بحث بر سر مسائل مرتبط با حاکمیت اینترنت و ارائه توصیه برای جامعه جهانی در این زمینه بود.

تعهدات مجمع راهبری اینترنت در بند ۷۲ دستور جلسه تونس آمده است:

ما از دبیرکل سازمان ملل می‌خواهیم: در پایان سال ۲۰۰۶ اجلاسی برای تعیین سیاست‌های حاکمیت بر اینترنت برپا شود. وظایف این اجلاس به قرار زیر می‌باشد:

الف - بحث بر سر سیاست‌های عمومی مرتبط با عناصر اصلی حاکمیت اینترنت به‌منظور تداوم، امنیت، ثبات و گسترش اینترنت؛

ب - تسهیل مباحثه بین سازمان‌هایی که درگیر با سیاست‌های عمومی بین‌المللی در خصوص اینترنت و مباحث مرتبط با آن هستند و همچنین مسائلی که هیچ سازمان خاصی وظیفه انجام آن را بر عهده ندارد؛

پ - ارتباط با سازمان‌های دولتی و سایر مؤسسات در خصوص قلمرو اجرایی‌شان؛

ت - تسهیل مبادله اطلاعات و استفاده کامل از تخصص علمی، آکادمیک و فنی کشورها؛
ث - سفارش به تمامی کشورها برای ارائه راهکارها و ابزاری برای شتاب بخشیدن به قابلیت دسترسی و امکان استفاده از اینترنت در کشورهای در حال توسعه؛

ج - تقویت به‌کارگیری فعالان در ساز و کار فعلی یا آینده حاکمیت اینترنت به‌ویژه کسانی که در کشورهای در حال توسعه هستند؛

چ - تشخیص مباحث جدید و جلب توجه سایر سازمان‌ها و حتی مردم و در صورت لزوم ارائه توصیه‌های لازم؛

ح - مشارکت در ایجاد ظرفیت برای حاکمیت اینترنت در کشورهای در حال توسعه؛

خ - ارزیابی و پیشبرد مستمر اصول اجلاس جهانی سران درباره جامعه اطلاعاتی در فرایند حاکمیت اینترنت؛

د - بحث در خصوص منابع حیاتی اینترنت در میان موضوعات مختلف؛

ذ - کمک به یافتن راه‌حلهایی درباره مسائل ناشی از استفاده درست و نادرست از اینترنت.
ر - انتشار فعالیت‌های انجام گرفته.

این مجمع در سال ۲۰۰۶ رسماً تشکیل شد و در همین سال، اولین جلسه خود را برگزار کرد. در اسناد تونس نیز همانند اسناد ژنو، بحث مشارکت همه ذی‌نفعان در حاکمیت بر فضای سایبر مورد تأکید قرار گرفت. اما در دستور کار تونس برای جامعه اطلاعاتی که ۱۲۰ ماده می‌باشد، بیش از ۴۰ ماده (یک‌سوم مفاد سند) به این موضوع پرداخته است. اما ابتکاری که در این سند برای اولین بار شاهد آن هستیم، کاربرد عبارت «چندذی‌نفعی» است.

واژگان "Multistakeholder" و "Multistakeholderism" در لغتنامه‌های مشهوری چون وبستر یا آکسفورد یافت نمی‌شوند و این بدین معنی است که این مفاهیم و کاربرد آن‌ها تاریخچه طولانی‌ای ندارد.

مدل راهبری چندذی‌نفعی که گاهی تحت عنوان ابتکار چندذی‌نفعی شناخته می‌شود، یک ساختار راهبری است برای جمع کردن ذی‌نفعان جهت مشارکت در گفت‌وگو، تصمیم‌گیری و خلق راهکار برای مشکلات یا اهداف عمومی.

بند سه: بازنگری ۱۰ ساله اجلاس سران درباره جامعه اطلاعاتی (WSIS+10) ۲۰۱۵

در تاریخ ۱۶ دسامبر ۲۰۱۵، یک نشست دو روزه سطح بالا در خصوص بازنگری ۱۰ ساله نتایج اجلاس سران درباره جامعه اطلاعاتی، در محل مجمع عمومی سازمان ملل با حضور نمایندگان سطح بالای تمام اعضاء و دولت‌ها و سایر اعضای ناظر و نمایندگان تمامی ذی‌نفعان مرتبط در اجلاس سران درباره جامعه اطلاعاتی، به ریاست آقای موگنس لیکتوف^۱ رئیس مجمع عمومی برگزار گردید و مجمع در پایان این نشست، سند خروجی بازنگری کلی اجرای نتایج اجلاس سران درباره جامعه اطلاعاتی را در قطعنامه‌ای با همین عنوان و با شماره ۷۰/۱۲۵ تصویب نمود.^۲ طبق توافق صورت گرفته توسط کشورهای عضو سازمان ملل متحد، مجمع عمومی یک نشست سطح بالا دیگر را برای بازنگری کلی اجرای نتایج اجلاس سران در سال ۲۰۲۵ برگزار خواهد کرد. نقاط تمرکز در سند نتایج این نشست دو روزه را می‌توان در حوزه‌های زیر مورد بررسی قرار داد: از بین بردن شکاف‌های دیجیتالی^۳، چالش‌ها و شکاف‌ها^۴، حکمرانی اینترنت^۵، فناوری‌های اطلاعات و ارتباطات برای توسعه پایدار^۶.

در سند نتایج اجلاس سران، بر اهمیت شکاف‌های دیجیتالی و ضرورت مقابله با آن‌ها، همکاری‌های بین‌المللی در ارتقای حوزه‌های زیر اشاره شده است: مقرون به صرفه‌گی، دسترسی، آموزش، ظرفیت‌سازی، چندزبانی، حفظ فرهنگ، سرمایه‌گذاری و عندالاقضاء تأمین مالی. آقای بانکی مون دبیر کل وقت سازمان ملل متحد، در طول این نشست در خصوص شکاف‌های دیجیتالی موجود در سطح جهان عنوان نمود: «در حالیکه در کشورهای در حال توسعه دوسوم خانواده‌ها به اینترنت دسترسی ندارند، امروزه بیش از ۸۰ درصد از خانواده‌ها در کشورهای توسعه یافته به اینترنت دسترسی دارند. ما باید این شکاف‌های دیجیتالی را از بین ببریم»^۷.

در سند خروجی این نشست، کشورها ضمن پرداختن به فرصت‌ها و چالش‌های این حوزه نوظهور، از تکامل و گسترش قابل توجه فناوری‌های اطلاعات و ارتباطات در هر گوشه از جهان،

1. Lykketoft Mogens

2. Resolution adopted by the General Assembly on 16 December 2015

3. Bridging the Digital Divide

4. Challenges and Gaps

5. Internet Governance

6. ICTs for Sustainable Development

7. "Today, more than 80% of households in developed countries have internet access. Meanwhile, two out of three households in developing countries do not. Women are half the global population – yet 200 million fewer women than men have access to the Internet. We must bridge these divides."

توانمندسازی در اشتراک گذاری دانش، رشد اقتصادی و توانمندسازی توسعه پایدار استقبال نمودند. این سند، به طور مهم، به چالش‌های جدید و نوظهور از جمله در زمینه‌های جرائم سایبری، حملات سایبری و استفاده از فناوری‌های اطلاعات و ارتباطات برای اهداف تروریستی پرداخته است. در این رابطه نقش محوری دولت‌ها در موضوعات امنیت سایبری مربوط به امنیت ملی را به تصدیق نموده و اهمیت نقش حقوق بین‌الملل مخصوصاً منشور سازمان ملل را در اعتمادسازی و امنیت در استفاده از فناوری‌های اطلاعات و ارتباطات توسط دولت‌ها به رسمیت شناخته است. همچنین سند نتایج خروجی اجلاس سران ۲۰۱۵ بر ضرورت ارتقای مشارکت و تعامل بیشتر دولت‌ها و بخش‌های خصوصی، جامعه مدنی، سازمان‌های بین‌المللی، جوامع فنی و دانشگاهی و تمامی ذی‌نفعان مرتبط در زمینه مباحث حکمرانی اینترنت اصرار دارد و از این لحاظ عنوان می‌دارد که مجمع حکمرانی اینترنت نقش بستر چندذی‌نفعی را برای مباحثه در موضوعات حکمرانی اینترنت ایفا کرده است.

در یک تصمیم ویژه مندرج در این سند، مجمع عمومی دستور کار {وظایف} مجمع حکمرانی اینترنت را به مدت ۱۰ سال دیگر تمدید نمود. ضمن اینکه در طی این مدت مجمع باید ارائه پیشرفت در کیفیت‌های عملکردی و مشارکت ذی‌نفعان مرتبط از کشورهای در حال توسعه را دنبال نماید و در انتها و به شکل برجسته‌تری به استفاده از فناوری‌های اطلاعات و ارتباطات برای دستیابی به توسعه پایدار پرداخته شده است.

کشورها، مجدداً تعهدات خود را در قبال استفاده از فناوری‌های اطلاعات و ارتباطات به‌عنوان ابزاری ضروری برای دستیابی دستور کار تونس برای جامعه اطلاعاتی حاوی. به اهداف توسعه پایدار جدید تأیید نموده و طرح و برنامه جدیدی را جهت استفاده از اینترنت و فناوری‌های اطلاعات برای اجرای دستور کار توسعه پایدار جدیدی تصویب نمودند.

در این نشست آقای لیکتوف در خصوص نقش فناوری اطلاعات و ارتباطات در توسعه اظهار نمود: «فناوری اطلاعات و ارتباطات به طور فزاینده‌ای نقش مهمی را در ارتقای توسعه اقتصادی و اجتماعی همانند ارتقای تولیدات، تسهیل تجارت و بازرگانی، ایجاد مشاغل باکیفیت، خدمات مبتنی بر فناوری اطلاعات و ارتباطات، سلامت و آموزش اینترنتی و اصلاح حکمرانی ایفا نموده است»^۱.

1. "ICT has played an increasingly important role in promoting economic and social development, such as enhancing productivity, facilitating trade, creating quality jobs, providing ICT-based services such as e-health and e-learning, and improving governance."

آقای بانکی مون، بیان نمود: « فناوری‌های اطلاعات و ارتباطات می‌توانند به‌عنوان موتور برای دستیابی به اهداف توسعه پایدار عمل نمایند آن‌ها می‌توانند این اهداف را تقویت نمایند»^۱ در خاتمه، کشورهای عضو سازمان ملل متحد در یک تصمیم کلیدی با نگاه رو به جلو درباره سند توسعه، با برجسته سازی نقش میان بر فناوری اطلاعات و ارتباطات در ریشه‌کنی فقر، ایجاد هماهنگی نزدیک بین فرایند اجلاس سران درباره جامعه اطلاعاتی را تقاضا کردند.

متأسفانه در گزارش ۲۰۱۵ ما شاهد آن هستیم که آمال و اهداف دولت‌ها برای مشارکت در حکمرانی چنددی‌نفعی فضای سایبر رنگ باخته است. اهداف انقلابی که در اسناد ۲۰۰۳ ژنو و ۲۰۰۵ تونس شاهد آن بودیم جایی در سند خروجی سال ۲۰۱۵ ندارد. بیش از ۵۰ ماده از ۱۲۲ ماده دستور کار تونس در سال ۲۰۰۵ (مفاد ۲۹ تا ۸۲) به بحث حکمرانی اینترنت پرداخته است. اما در گزارش سال ۲۰۱۵ این موضوع کاملاً کم رنگ می‌باشد. ارائه آمار و ارقام گسترش اینترنت و فناوری اطلاعات و ارتباطات در کشورهای مختلف جهان بدون اشاره به حکمرانی این فضا و ابزار خرسندی صرفاً به جهت گسترش آن، نمی‌تواند پوششی برای فاصله گرفتن اجلاس سران از اهداف انقلابی خود در اجلاس تونس باشد. سال ۲۰۰۵ اوج فعالیت انقلابی اجلاس سران بود. از آن تاریخ به بعد با اقدامات مخرب پیدا و پنهان آمریکا، شاهد رکود و افول فعالیت اجلاس سران هستیم که مدام در حال فاصله و زاویه گرفتن از اهداف اصلی خود می‌باشد.

بند چهار: مجمع حکمرانی اینترنت

اجلاس سران در مورد جامعه اطلاعاتی (WSIS)^۲ توسط اتحادیه بین‌المللی مخابرات^۳ در دو مرحله در ژنو ۲۰۰۳ و تونس ۲۰۰۵ برگزار گردید. اجلاس تونس^۴ دو سند خروجی داشت:

الف: تعهد تونس

ب: دستور کار تونس برای جامعه اطلاعاتی دستور کار تونس برای جامعه اطلاعاتی^۵ حاوی ۱۲۲

1. "This High-Level review is timely coming just three months after the adoption of the 2030 Agenda for Sustainable Development. ICTs can be an engine for achieving the Sustainable Development Goals. They can power this global undertaking."

2. World Summit on the Information Society

3. International Telecommunication Union (ITU)

4. TUNIS COMMITMENT

5. TUNIS AGENDA FOR THE INFORMATION SOCIETY

ماده است که ماده ۷۲ از این سند^۱ در خصوص تشکیل مجمع حکمرانی اینترنت (IGF)^۲ می‌باشد این مجمع در اجلاس تونس (۲۰۰۵) و با هزاران امید و آرزو علیه آیکان عَلم شد، در عمل نتوانست کارایی مؤثری داشته باشد. اعلام رسمی تأسیس آن توسط مجمع عمومی سازمان ملل در جولای ۲۰۰۶ صورت گرفت و اولین اجلاس خود را اکتبر و نوامبر ۲۰۰۶ برگزار کرد.^۳ این اجلاس جهانی در آتن برگزار شد.

اجلاس یونان، باتوجه به پیشنهاد گروه مشورتی مجمع راهبری اینترنت حول چهار محور برگزار شد:

۱. گشودگی: آزادی بیان، جریان آزاد اطلاعات، اندیشه‌ها و معرفت‌ها؛

۲. امنیت: ایجاد اعتماد و اطمینان در کاربرد اینترنت از طریق توسعه همکاری‌ها؛

۳. تنوع: پیشبرد چندزبانی‌گرایی و محتوای محلی؛

۴. دسترسی: اتصال اینترنتی، سیاست‌ها و قیمت‌ها.

دومین اجلاس مجمع راهبری اینترنت در نوامبر ۲۰۰۷ در ریودوژانیروی برزیل (۱۲ تا ۱۵ نوامبر) برگزار شد.

سومین اجلاس مجمع در دسامبر ۲۰۰۸ در حیدرآباد هند (۳ تا ۶ دسامبر) برگزار شد.

چهارمین اجلاس مجمع در نوامبر ۲۰۰۹ در شرم‌الشیخ مصر (۱۵ تا ۱۸ نوامبر) برگزار شد.

1. We ask the UN Secretary-General, in an open and inclusive process, to convene, by the second quarter of 2006, a meeting of the new forum for multi-stakeholder policy dialogue—called the Internet Governance Forum (IGF). The mandate of the Forum is to:

- Discuss public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet.
- Facilitate discourse between bodies dealing with different cross-cutting international public policies regarding the Internet and discuss issues that do not fall within the scope of any existing body.
- Interface with appropriate intergovernmental organizations and other institutions on matters under their purview.
- Facilitate the exchange of information and best practices, and in this regard make full use of the expertise of the academic, scientific and technical communities.
- Advise all stakeholders in proposing ways and means to accelerate the availability and affordability of the Internet in the developing world.
- Strengthen and enhance the engagement of stakeholders in existing and/or future Internet governance mechanisms, particularly those from developing countries.
- Identify emerging issues, bring them to the attention of the relevant bodies and the general public, and, where appropriate, make recommendations.
- Contribute to capacity building for Internet governance in developing countries, drawing fully on local sources of knowledge and expertise.
- Promote and assess, on an ongoing basis, the embodiment of WSIS principles in Internet governance processes.
- Discuss, inter alia, issues relating to critical Internet resources.
- Help to find solutions to the issues arising from the use and misuse of the Internet, of particular concern to everyday users.
 - Publish its proceedings.

2. Internet Governance Forum

3. <http://www.intgovforum.org/multilingual/content/about-igf-faq>

اجلاس پنجم در سال ۲۰۱۰ در ویلینیوس، اجلاس ششم در سال ۲۰۱۱ در نایروبی، اجلاس ۲۰۱۲ در باکو، اجلاس ۲۰۱۳ در بالی، اجلاس ۲۰۱۴ در استانبول، اجلاس سال ۲۰۱۵ در برزیل و اجلاس سال ۲۰۱۶ در مکزیک برگزار گردید.^۱

کشور ما تاکنون میزبانی هیچ اجلاسی را در این زمینه بر عهده نداشته است. در بین همسایگان ما، ترکیه و جمهوری آذربایجان، هر کدام یک بار میزبان این کنفرانس جهانی بوده‌اند. سایت رسمی مجمع راهبری اینترنت، اهداف زیر را برای این مجمع ترسیم کرده است:

«هدف مجمع راهبری اینترنت، ایجاد فرصت حداکثری برای مذاکره آزاد و جامع و تبادل نظر در زمینه همه موضوعات مرتبط با حاکمیت بر اینترنت است تا بهترین اقدامات و تجارب ممکن، بین اعضاء مبادله شود. موضوعات نوظهور، شناسایی شوند تا توجه نهادهای مرتبط و عامه مردم، به این موضوعات جلب شود. بنابراین هدف اصلی مجمع راهبری اینترنت، تسهیل مذاکرات است. مذاکراتی که جامع، شامل و مولد باشد. مذاکراتی که یک چشم‌انداز کلی از موضوعات مرتبط با سیاستگذاری عمومی درباره اینترنت را ایجاد کند و نظر تمام ذی‌نفعان این حوزه را پوشش دهد.»^۲

اما باید توجه داشت که این مجمع برای نیل به اهداف اشاره شده، دارای مشکلاتی است. از جمله اینکه مجمع راهبری اینترنت فاقد قدرت تصمیم‌گیری است و صرفاً محلی برای مذاکره بین اعضاست که البته به کشورهای در حال توسعه این امکان را می‌دهد که با کشورهای توسعه‌یافته درباره موضوع حاکمیت بر اینترنت صرفاً مذاکره کنند.^۳

بنابراین هدف مجمع راهبری اینترنت این است که بستری فراهم کند تا موضوعات دامنهدار و مسائل نوظهور راجع به حاکمیت بر اینترنت بتواند از سوی ذی‌نفعان این حوزه اعم از جامعه مدنی، مشاغل، بخش‌های فنی، دولت‌ها و محافل دانشگاهی مورد بحث و بررسی قرار گیرد. شرکت در جلسات مجمع راهبری اینترنت برای عموم علاقه‌مندان آزاد است. در این مجمع حدود ۱۵۰۰ تا ۲۲۰۰ نفر از گروه‌های مختلف ذی نفع در حوزه اینترنت گرد هم می‌آیند تا

1. ... Rio (2007), Hyderabad (2008), Sharm El Sheikh (2009), Vilnius (2010), Nairobi (2011), Baku (2012), Bali (2013), Istanbul (2014) and João Pessoa (2015).... <http://www.intgovforum.org>
2. <http://www.intgovforum.org>

. باید خاطر نشان کرد که اجلاس جهانی مخابرات موسوم به سران مختار، نهاد اصلی تصمیم‌گیرنده و سیاست‌گذار در اتحادیه بین‌المللی مخابرات (ITU) است که هر چهار سال یک بار برگزار می‌شود. مجمع سران مختار، عالی‌ترین مرجع بین‌المللی در حوزه مخابرات می‌باشد. بنابراین مجمع راهبری اینترنت که توسط اتحادیه یادشده تأسیس شده، فاقد قدرت تصمیم‌گیری است.

درباره موضوعات این حوزه اعم از ایجاد ظرفیت حداکثری برای استفاده از فرصت‌های ایجاد شده به واسطه اینترنت و مقابله با خطرهای و چالش‌های برخاسته از این حوزه بحث و مذاکره کنند. مجمع راهبری اینترنت، اجلاس‌های سالانه‌ای دارد که معمولاً در پاییز هر سال برگزار می‌شود.^۱ در این مجمع، فراخ‌تر از کمیته مشورتی دولتی است. اگر در کمیته مشورتی به روی همه دولت‌ها باز است، در مجمع راهبری به روی همه باز است. اعم از دولت‌ها، بخش عمومی، بخش دانشگاهی، صنعت، جامعه مدنی و بخش خصوصی. وجه مشترک مجمع راهبری اینترنت و کمیته مشورتی دولتی، فقدان ضمانت اجرا برای تصمیمات آن‌هاست و به عبارت دیگر، هیچ سازوکار الزام‌آوری برای کاربرست تصمیمات این دو نهاد پیش‌بینی نشده است. همان‌گونه که ذکر شد، کارویژه اصلی چنین نهادهایی، مشروعیت‌زایی برای حکمرانان اصلی فضای سایبر است.

رکود مجمع راهبری اینترنت به حدی بود که در سال ۲۰۱۰ دبیرکل ضمن تمدید فعالیت مجمع برای ۵ سال دیگر، کمیسیون علم و فناوری برای توسعه^۲ را مأمور کرد که یک گزارش و توصیه‌هایی در ارتباط با چگونگی ارتقای جایگاه مجمع راهبری اینترنت ارائه دهد. متعاقب آن، یک کارگروه برای توسعه و پیشرفت مجمع راهبری اینترنت^۳ توسط سازمان ملل تشکیل شد که متشکل از ۲۲ دولت از جمله آمریکا و سایر گروه‌های ذی‌نفع در مقوله حاکمیت بر اینترنت بود.^۴ در خصوص توفیقات این کارگروه، همین بس که آمریکا که اساساً مخالف تشکیل مجمع راهبری اینترنت بود، حالا به عضویت کارگروهی در آمده است که مأموریت ارائه راهکار برای پیشرفت مجمع را بر عهده دارد!

در دسامبر ۲۰۱۵ مجمع عمومی سازمان ملل، فعالیت مجمع راهبری اینترنت را تا سال ۲۰۲۵ تمدید کرد. اما هیچ گشایشی جهت بهبود کارایی آن، صورت نگرفت.

1. <http://www.ifla.org/node/7406>

2. [... the IGF serves as an open discussion forum and does not have negotiated outcomes, nor does it make formal recommendations to the U.N....] Internet Governance and the Domain Name System.p2.

3. the U.N.'s Commission on Science and Technology for Development (CSTD)

4. A Working Group on Improvements to the Internet Governance Forum

5. Internet Governance and the Domain Name System.ibid

اجلاس ۲۰۱۸ مجمع حکمرانی اینترنت در پاریس برگزار شد و «مکرون» موضوع اینترنت اروپا را با نفی اینترنت آمریکا و چین مطرح کرد. برخی از موضعات مطرح شده در این اجلاس عبارت‌اند از: حفاظت از داده، آینده هویت دیجیتال و حقوق بشر، حقوق در حال ظهور فناوری‌های نسل آتی، سنجش فعالیت‌های تبعیض آمیز، حق حریم خصوصی در دوران دیجیتال، اشاعه، ثبات سایبری و مسئولیت دولت‌ها، اینترنت آزاد و رایگان برای تمامی ذی‌نفعان، به سوی یک نظام اینترنت غیرمتمرکز، هوش مصنوعی و آینده دیپلماسی، بهبود قوانین ملی برای حکمرانی اینترنت، تقویت مباحثات چندذی‌نفعی در خصوص اینترنت و انتخابات، مشارکت دولتی - خصوصی - مدنی در ایجاد ظرفیت سایبری، گذشته، حال و آینده چندذی‌نفعی، نوآوری فناوریانه و قوانین حکمرانی اینترنت، تعهد شرقی-غربی در قالب چندذی‌نفعی، بلاک چین برای کاربردهای اجتماعی و انسانی، بی‌طرفی شبکه و فراتر از آن: تضمین آزادی انتخاب برخط، بهبود دسترسی: ایجاد جوامع فراگیر توسط هوش مصنوعی، حقوق بشر، جنسیت و جوانان، توسعه مشارکت جوانان در IGF.

اجلاس ۲۰۱۹ نیز در برلین آلمان برگزار گردید.

اگر مقوله حکمرانی اینترنت را به یک اتوبوس در حال حرکت تشبیه نماییم می‌توان گفت: راننده و راهبر آن، آیکن است، اتوبوس متعلق به آیکن می‌باشد و جاده نیز متعلق به آیکن است. اعضای IGF فقط در حکم مسافران این اتوبوس هستند که قرار است در مسیر حرکت در خصوص مالکیت اتوبوس، راهبری آن و موضوعات این چنینی حرف بزنند. طبیعی است که کسی مالکیت خود بر چیزی را به بحث نمی‌گذارد مگر اینکه برای سرگرمی باشد و IGF محل همین سرگرمی می‌باشد.

اگر امروزه ما اینترنت چین، اینترنت روسیه، و اخیراً اینترنت اروپا را از زبان مکرون شنیدیم به این خاطر است که بالکانیزه شدن (تجزیه اینترنت) به خاطر عملکرد بسته، غیر منعطف و انحصارطلبانه شرکت‌های آمریکایی از جمله آیکن به یک امر بسیار جدی تبدیل شده است و دولت‌ها از اینکه در آیکن تحول مثبتی روی دهد کاملاً سرخورده و ناامید شده‌اند و منطقه‌گرایی در مقابله جهان‌شمولی اینترنت کاملاً در حال رشد می‌باشد. چند روز پیش نیز روسیه از افتتاح

شبکه ملی اینترنت خود خبر داد.

عجیب نیست که کشوری مثل روسیه که در همه حوزه‌های حقوقی و دیپلماتیک سایبری حضور فعال دارد و از سال ۱۹۹۸ در کمیته اول پرچمدار تنها قطعنامه سایبری است، کردارنامه و پیش‌نویس کنوانسیون در حوزه‌های مختلف سایبری مثل امنیت سایبری، جرائم سایبری، تروریسم سایبری و... را ارائه نموده، حضور در خوری در IGF نداشته و ندارد.

شرکت در جلسات مجمع راهبری اینترنت برای عموم علاقه‌مندان آزاد و در آن به روی همه باز است. در این مجمع حدود دو سه هزار نفر گردهم می‌آیند. صدها موضوع گسترده می‌شود و هزاران نفر حضور دارند. مکان خوبی برای گفتن و شنیدن است. اما اعتبار حقوقی برای هیچ گونه اظهار نظری متصور نیست. کسانی که به موضوعات علاقه‌مند هستند و فرصت و فراغ بال دارند می‌توانند با هزینه شخصی و ظرفیت حقیقی خود در این اجتماع شرکت نمایند.

مواردی مثل اعلام موضع یا انتشار بیانیه در این اجتماع مفهوم حقوقی ندارد. چرا که اجلاس اساساً بین دولتی نیست. اجتماع I.G.F صرفاً بستری برای مذاکره است و آن‌هم مذاکره کارشناسی غیررسمی. غیر از گفتگو هیچ مأموریتی برای IGF تعریف نشده است. مصوبه یا معاهده‌ای در بستر IGF قابل تصور نیست.

هیچ خروجی ملموس و غیرملموسی از سال ۲۰۰۶ - که اولین نشست IGF تشکیل شده است - تاکنون، از این مجمع ثبت نشده است. حضور برخی مقامات کشورهای میزبان یا مهمان کاملاً جنبه تشریفاتی دارد و چیزی فراتر از یک دوره‌می سایبری یا یک شو سایبری نمی‌باشد. اما بهتر است بخش خصوصی و افراد حقیقی با تخصص‌های مرتبط برای حضور در اجلاس تشویق شوند تا با مباحث و موضوعات جدیدی آشنا شوند و بدهستان‌های گفتمانی داشته باشند.

گفتار پنج: سازمان آموزشی علمی فرهنگی سازمان ملل متحد (یونسکو)

بند یک: یونسکو و فضای سایبر

اساسنامه یونسکو در تاریخ ۱۶ نوامبر سال ۱۹۴۵ میلادی به تصویب رسید و در تاریخ ۴ نوامبر ۱۹۴۶ با امضا و تصویب ۲۰ کشور از جمله استرالیا، برزیل، کانادا، چین، دانمارک، فرانسه،

یونان، هند و ... لازم‌الاجراء شد. ایران در سال ۱۹۴۸ میلادی مصادف با سال ۱۳۲۷ شمسی به این اساسنامه (بدون اعمال حق شرط) پیوست.

سازمان آموزشی علمی فرهنگی سازمان ملل متحد (یونسکو)^۱ سیاست اعلامی مفصلی در خصوص تقویت بنیان‌های صلح و توسعه پایدار دارد. از طرف دیگر همکاری‌های فزاینده این سازمان در زمینه‌های آموزشی، علمی، فرهنگی ارتباطات و اطلاعات، می‌تواند در برخی جوامع راهگشا باشد. مخصوصاً هنگامی که جوامع در سرتاسر جهان با افزایش فشار ناشی از تغییر دست به گریبان هستند و جوامع بین‌المللی نیز با چالش‌های جدیدی روبه‌رو می‌باشند. سازمان یونسکو نقش برجسته‌ای در مراحل مختلف اجلاس سران درباره جامعه اطلاعاتی (طی سال‌های ۲۰۰۳ و ۲۰۰۵)، مجمع حکمرانی اینترنت (IGF)، کمیسیون پهنای باند برای توسعه پایدار و سایر مجامع مرتبط با اینترنت و تأثیرات آن ایفا نموده است.

به‌طور کلی اسناد مهمی که در زمینه فضای سایبر توسط سازمان یونسکو منتشر گردیده است شامل موارد زیر می‌باشد:

- ✓ توصیه در خصوص ارتقای و استفاده چندزبانی و دسترسی به فضای مجازی^۲؛
- ✓ دیدگاه اندیشه‌ای و تحلیل یونسکو درباره اینترنت، یونسکو و استفاده از اینترنت در قلمرو صلاحیت خود^۳؛
- ✓ ضوابط اخلاقی برای جامعه اطلاعاتی^۴؛
- ✓ اصول و شاخص میزان پوشش جهانی یا جهان‌شمولی (جهان‌گستری) اینترنت^۵.

بند دو: توصیه در خصوص ارتقای و استفاده چندزبانی و دسترسی به فضای مجازی
یونسکو از اواسط سال ۱۹۹۰ مجموعه‌ای از جلسات کارشناسان بین‌المللی را برگزار کرد که به تولید سند «توصیه در خصوص ارتقای و استفاده چندزبانی و دسترسی به فضای مجازی» منجر شد.

1. United Nations Educational, Scientific and Cultural Organization (UNESCO)
2. RECOMMENDATION CONCERNING THE PROMOTION AND USE OF MULTILINGUALISM AND UNIVERSAL ACCESS TO CYBERSPACE
3. REFLECTION AND ANALYSIS BY UNESCO ON THE INTERNET ,UNESCO and the use of the Internet in its domains of competence 186 EX/INF.11 PARIS, 29 April 2011
4. Code of ethics for information
5. Internet Universality

این سند که در ۱۵ اکتبر ۲۰۰۳ توسط کنفرانس عمومی یونسکو تصویب گردید، یونسکو و دولت‌های عضو را دعوت می‌نماید تا در بررسی‌های خود روی چهار حوزه زیر متمرکز گردند: ۱. توسعه سیستم‌ها و محتوای چندزبانی. ۲. تسهیل دسترسی به شبکه و سیستم‌ها. ۳. توسعه محتوای نظرها عمومی. ۴. تأیید مجدد تعادل عادلانه بین منافع ذی‌حقان (ذی‌نفعان) و منافع عمومی. در این سند کنفرانس عمومی یونسکو توصیه نمود که:

❖ دولت‌های عضو جهت تأثیرپذیری قلمروهای فضایی^۱ و سرزمینی خود، توصیه‌های مندرج، هنجارها و اصول این سند را از طریق مراجع قانونگذار یا سایر سطوح به‌کارگیرند؛

❖ دولت‌های عضو جهت توجه مراجع مسئول در عملکرد خط‌مشی‌ها، راهبردها و زیرساخت‌های عمومی و خصوصی فناوری اطلاعات و ارتباطات از جمله در خصوص موارد زیر، این توصیه‌ها را به‌کارگیرند:

✓ اپلیکیشن‌های (برنامه‌های کاربردی) چندزبانی در اینترنت؛

✓ توسعه شبکه‌ها و ارائه خدمات؛

✓ گسترش اطلاعات مربوط به دامنه عمومی^۲ در اینترنت؛

✓ موضوعات شفاف در زمینه حقوق مالکیت فکری (مالکیت معنوی).

❖ دولت‌های عضو باید در خصوص اقدامات صورت گرفته جهت اجرای این توصیه‌ها در سطح کشوری، هر چهار سال یکبار گزارشی را به یونسکو ارائه دهند و یونسکو باید بر اساس گزارش‌های دریافتی از دولت‌ها، گزارشی منسجم برای شورای اجرایی و کنفرانس عمومی تهیه نماید. گزارش‌های مختلف در طول این مدت و با فاصله زمانی چهارسال توسط دولت‌ها به دبیرخانه سازمان یونسکو ارائه گردید و این سازمان گزارش منسجم خود را در خصوص اقدامات دولت‌ها جهت به‌کارگیری توصیه‌ها در باب ارتقای دسترسی فراگیر به فضای سایبری و استفاده چندزبانی در فضای سایبری را ارائه نمود و این گزارش در اجلاس‌های شورای اجرایی و کنفرانس عمومی یونسکو مورد بررسی قرار گرفت. مشخصات چهار گزارش ارائه شده در اجلاس کنفرانس عمومی یونسکو در جدول زیر مشهود می‌باشد:

1. territories and jurisdictions
2. public domain information

جدول ۱۱: مشخصات چهارگزارش ارائه شده در اجلاس کنفرانس عمومی یونسکو

شماره گزارش	اجلاس شورای اجرایی	اجلاس کنفرانس عمومی یونسکو	سال	فهرست کشورهای که بر اساس گزارش آنها گزارش تهیه گردید
یک	۱۷۶	۳۹	۲۰۰۷	الجزایر، استرالیا، بلژیک، بونان، بولیوی، کانادا، کلمبیا، ساحل عاج، دانمارک، مصر، فنلاند، فرانسه، آلمان، گرجستان، لهستان، هند، رژیم صهیونیستی، ژاپن، لیتوانی، لیتوانی-ماریتوس، مالدیو، مکزیک، ناسیونال، روسیه، سنگال، صربستان، اسلوواکی، اسپانیا، ترکیه، زیمبابوه
دو	۱۸۶	۳۹	۲۰۱۱	آذربایجان، کانادا، کلمبیا، جمهوری چک، دانمارک، جمهوری دومینیک، مصر، فنلاند، آلمان، گینه، لهستان، رژیم صهیونیستی، ژاپن، اردن، فرانسه، لیتوانی، مالتی، مکزیک، موناکو، نیجریه، جمهوری مولداوی، رومانی، رواندا، پرو، اسپانیا، جمهوری عربی سوریه، جمهوری مقدونیه یوگسلاوی سابق
سه	۱۹۶	-	۲۰۱۵	الجزایر، بلژیک، بلغارستان، بروندی، کانادا، جمهوری آفریقای مرکزی، مصر، فنلاند، فرانسه، آلمان، لهستان، عراق، ژاپن، اردن، لیتوانی، مکزیک، موناکو، مولدووا، نیجریه، رومانی، اسلوواکی، اسپانیا، سوئد
چهار	۲۰۶	-	۲۰۱۹	الجزایر، برزیل، بلغارستان، کانادا، دانمارک، فنلاند، آلمان، لهستان، ژاپن،

همچنین در سال ۲۰۰۵ یونسکو گزارش جهانی درباره جوامع دانش محور برای همه را تحت عنوان به سوی جوامع دانش محور^۱ منتشر نمود. این سند در خصوص تکامل یا تحول جوامع اطلاعاتی به سوی جوامع دانش محور می‌باشد.^۲

بند سه: دیدگاه اندیشه‌ای و تحلیل یونسکو درباره اینترنت، یونسکو و استفاده از اینترنت در قلمرو صلاحیت خود

در ۲۹ آوریل سال ۲۰۱۱، کشورهای عضو یونسکو سندی را تحت عنوان «دیدگاه اندیشه‌ای و تحلیل یونسکو درباره اینترنت، یونسکو و استفاده از اینترنت در قلمرو صلاحیت خود» را مصوب نمودند. در خلاصه این سند آمده است:

پیرو تصمیم شماره چهل و دو اجلاس صد و هشتاد و پنجم شورای اجرایی، این سند شامل اطلاعات و تحلیل‌های تفصیلی درباره استفاده سازمان یونسکو از اینترنت جهت انجام تعهدات خود می‌باشد. این سند خلاصه‌ای است از:

- ✓ بررسی وضعیت جاری و روند توسعه در حوزه اینترنت؛
- ✓ ایجاد مرجعی برای تعریف نقش سازمان یونسکو در حکمرانی اینترنت؛
- ✓ تأکید بر شناسایی اقدامات ویژه برای مسیر آینده جهت توانمندسازی حداکثری قابلیت

1. Towards Knowledge Societies

۲. این سند توسط دکتر محمدرضا سعید آبادی استادیار دانشگاه تهران ترجمه گردیده است.

اینترنت در سازمان جهت دستیابی به اهداف ارتقای صلح و توسعه پایدار. در خصوص نقش یونسکو در حکمرانی اینترنت در این سند آمده است که: موضوع حکمرانی اینترنت شامل دامنه وسیعی از موضوعات از جمله زیرساخت، استانداردهای فنی، حقوق و محتوا می‌باشد و هیچ مؤسسه منفردی نمی‌تواند متصدی حکمرانی اینترنت باشد. به‌طور جاری بازیگران اصلی درگیر (ذی‌مدخلان) در مبحث حکمرانی اینترنت شامل موارد زیر می‌باشند:

- ❖ بازیگران بین‌الدولی که در راستای خطوط اقدام اجلاس سران در حوزه صلاحیت خود عهده‌دار مسئولیت می‌باشند برای مثال:
 - ✓ دپارتمان امور اقتصادی - اجتماعی سازمان ملل متحد^۱ مسئول مباحث مرتبط با توسعه، دولت الکترونیک، همکاری‌های بین‌المللی؛
 - ✓ اتحادیه بین‌المللی مخابرات (آی تی یو) مسئول مباحث مرتبط با زیرساخت‌ها، ظرفیت‌سازی، امنیت، محیط توانمندساز^۲؛
 - ✓ یونسکو مسئول مباحث مرتبط با دسترسی، علوم الکترونیکی^۳، آموزش الکترونیکی، تنوع فرهنگی و زبانی، رسانه و اخلاق اطلاعاتی^۴؛
 - ✓ سازمان همکاری‌های اقتصادی و توسعه^۵ مسئول مباحث مرتبط با اقتصاد اینترنتی؛
 - ✓ سازمان جهانی مالکیت فکری^۶ مسئول مباحث مرتبط با حق کپی (کپی رایت).
- ❖ آیکان (شرکت اینترنتی برای تعیین و اختصاص نام‌ها و شماره‌ها): مسئول هماهنگی جهانی درباره شناسه‌های منحصربه‌فرد اینترنت (نام‌های دامنه و آدرس‌های پروتکل اینترنت)؛
- ❖ نیروی ضربتی مهندسی اینترنت^۷ مسئول توسعه فنی استانداردها برای اینترنت؛
- ❖ مجمع حکمرانی اینترنت مسئول گفتگو درباره تمامی موضوعات مرتبط با حکمرانی اینترنت. یونسکو تبدیل به یک توسعه‌دهنده فعال^۸ در مجمع حکمرانی اینترنت شده است و این مجمع

1. United nations department of economic and social affairs(UNDESA)

2. enabling environment

3. e-science

4. information ethics

5. The Organisation for Economic Co-operation and Development (OECD)

6. The World Intellectual Property Organization (WIPO)

7. Internet Engineering Task Force (IETF)

8. active contributor

را در قالب یک بستر اساسی برای تبادل نظر و تبادل ایده چنددلی‌نفعی و تبادل نگرانی‌ها، حمایت نموده است. این سازمان کارگاه‌هایی را در خصوص موضوعات مختلفی مانند آزادی بیان در اینترنت، شبکه‌های خصوصی و اجتماعی و... در تمامی نشست‌های مجمع حکمرانی اینترنت راه‌اندازی نموده است و همچنین در گروه‌های مشورتی چنددلی‌نفعی، جهت برجسته نمودن اهمیت اصول اصلی جوامع دانشی فراگیر، به‌عنوان یک عضو ناظر شرکت نموده است. این سازمان جهت برقراری همکاری بین دولت‌ها، جوامع مدنی، بخش خصوصی و جوامع دانشگاهی و هم‌افزایی بین‌دلی‌نفعان، فعال می‌باشد. برخی از این تعاملات به شکل غیررسمی برگزار گردیده اند اما برخی از آن‌ها هم در قالب تعاملات رسمی بوده‌اند: مانند ایجاد یک ائتلاف پویا در خصوص آزادی بیان و آزادی رسانه در اینترنت، توافق همکاری بین یونسکو و آی‌کان جهت تقویت چندزبانی در فضای سایبر در سال ۲۰۰۹. همچنین این سند حاوی مطالبی در خصوص عملکرد سازمان یونسکو در رابطه با چالش‌ها و فرصت‌های اینترنت در حوزه‌های اصلی زیر می‌باشد: آموزش (سیاست‌گذاری، کیفیت آموزش الکترونیکی، آموزش معلمان با فناوری دیجیتال، فناوری سیار،^۱ نوآوری، سواد اطلاعاتی و رسانه، منابع آموزشی آزاد^۲)، علوم طبیعی، علوم اجتماعی و انسانی، فرهنگ، دسترسی به اطلاعات و دانش، آزادی بیان، دموکراسی و صلح، حفاظت و صیانت از محصولات دیجیتالی^۳ (متن، بانک داده‌ها، فیلم، تصاویر، صدا و...).

بند چهارم: سند پیش‌نویس ضوابط اخلاقی برای جامعه اطلاعاتی سال ۲۰۱۱

یونسکو در هجدهمین نشست شورای بین‌دولتی درباره اطلاعات برای تمامی برنامه‌ها^۴ در سال ۲۰۱۱، پیش‌نویس سندی^۵ را تحت عنوان «ضوابط اخلاقی برای جامعه اطلاعاتی» ارائه نمود. سند توسعه ضوابط اخلاقی بر مبنای تعهدات زیر شکل گرفت:

✓ تعهدات تعریف شده در اساسنامه یونسکو؛

✓ تعهدات تعیین شده توسط اجلاس سران درباره جامعه اطلاعاتی برای سازمان یونسکو در

1. Mobile technologies

2. Open Educational Resources (OERs)

3. Digital Heritage

4. Intergovernmental Council for Information for all program-

5. IFAP- 2011/Bureau.XVIII/4 Paris, 1st February 2011

در این سند به مفاد ۵۶ تا ۵۹ ابعاد اخلاقی جامعه اطلاعاتی در اعلامیه اصول ژنو و همچنین ماده ۲۵ طرح اقدام ژنو در سال ۲۰۰۳ اشاره گردیده است.

اعلامیه اصول ژنو و خطوط اقدام ژنو در سال ۲۰۰۳.

آنچه در مورد عملکرد سایبری سازمان یونسکو ذکر می شود، مختصری از انبوه اسناد و مدارکی است که هم به جهت محدودیت حجم کتاب و هم به جهت مغایرت برخی مطالب با فرهنگ عامه و ارزشهای حاکم بر جامعه از ذکر آنها معذوریم. محققان و علاقه‌مندان با عنایت به منابع ارائه شده و پانویس‌های این بخش می توانند به تکمیل تحقیقات خود اقدام کنند.

برخی از محورهای اسناد یونسکو با اسناد بالادستی کشورمان از جمله قانونی اساسی و قوانین و مقررات داخلی مغایرت دارد که لازم است مورد نظر قرار گیرد. تأمل موشکافانه و دقیق در برخی محورهای اسناد یونسکو، نواقص و مغایرت‌های آن را آشکار می کند. به‌عنوان مثال تساوی جنسیتی و توانمندسازی زنان و دختران را می توان در نظر گرفت. در ابتدا این عناوین بسیار متعالی و ارزشمند و انسانی اند. اما هنگامی که به توضیحات مراجعه می کنیم با عباراتی مواجه می شویم که با منظومه شرعی و قانونی ما پذیرفته نیست.

سؤالی که در اینجا مطرح می شود این است؛ اسنادی مثل سند توسعه پایدار و ضوابط اخلاقی برای جامعه اطلاعاتی عملاً از چه ماهیت حقوقی برخوردارند؟ آیا اسنادی الزام‌آورند و یا غیر الزام‌آور؟

در پاسخ باید اذعان نمود که باوجود کاربرد اصطلاحاتی چون «باید»، «متعهد می شوند» و نظایر آن در متن این اسناد باید گفت که این گونه اسناد که خارج از چارچوب معاهده و با قصد عدم ایجاد تعهد سخت بین‌المللی شکل گرفته اند، الزام حقوقی معاهدات و عرف حقوقی بین‌المللی را ندارند. بلکه اسنادی بالادستی و توصیه ای در قالب حقوق نرم تلقی می گردند. البته این بیان باوجود درست بودن، تا حد زیادی فریبنده است. زیرا این اسناد توصیه ای با گذشت زمان و ایجاد اجماع جهانی قابلیت تبدیل به معاهده و کنوانسیون‌های بین‌المللی را دارند. این مسئله در خصوص اعلامیه جهانی حقوق بشر نیز محقق شده است. در واقع در سال ۱۹۴۷ میلادی هنگامی که دولت‌های جهان گرد هم آمدند و در مورد اعلامیه جهانی حقوق بشر و اهداف و مفاد مشترک آن به اجماع رسیدند تنها در پی ایجاد گفتمانی مشترک در حوزه حقوق بشر بودند، اما بعد از سپری شدن دوده با تنظیم و تصویب جهانی دو میثاق بین‌المللی حقوق مدنی، سیاسی

و حقوق اقتصادی و اجتماعی و فرهنگی جامعه الزام بر تن اعلامیه جهانی حقوق بشر نمودند. بنابراین تبدیل اسناد یونسکو در حوزه جامعه اطلاعاتی و سایبر به معاهدات الزام آور حقوقی دور از حقیقت نخواهد بود. زیرا تمام اقدامات داوطلبانه و توصیه‌ای نرم در گذر زمان طی یک فرایند پویا به حقوق سخت الزام آور تبدیل می‌شوند.

علاوه بر این سند یونسکو در تشریح جایگاه خود متذکر می‌شود که تمام اصول یاد شده برای فضای برخط برگرفته از اسناد زیر و دیگر قطعنامه مرتبط سازمان ملل می‌باشد:

✓ اعلامیه جهانی حقوق بشر؛

✓ میثاق بین‌المللی حقوق مدنی و سیاسی؛

✓ میثاق بین‌المللی حقوق اقتصادی، اجتماعی و فرهنگی؛

✓ کنوانسیون رفع تمامی هنجارهای تبعیض نژادی؛

✓ کنوانسیون رفع تبعیض علیه زنان؛

✓ کنوانسیون حقوق کودک.

این مسئله بدان معناست که سند یونسکو در مقام بیان قواعد معاهداتی و عرفی الزام آور است. در مجموع باید به محتوای این اسناد با دقت و احتیاط نگریست و بیان به ظاهر متعالی این اسناد نباید موجب اغفال تصمیم‌سازان و تصمیم‌گیران در کشور شود.

بند پنج: اصول و شاخصه‌های پوشش اینترنت

باتوجه به درک و ارزیابی پیچیدگی توسعه اینترنت و تأثیر آن، ضرورت پرداختن به موضوع مشارکت بهینه اینترنت در اهداف توسعه پایدار تعیین کننده می‌باشد. یونسکو نیز در دستور کار خود، موضوعاتی را با تأکید بر قابلیت های اینترنت در توسعه و تحول جوامع اطلاعاتی مندرج نمود که این سازمان را در برابر انجام اقداماتی بر مبنای دسترسی جهانی به اطلاعات و دانش، احترام به فرهنگ و تنوع زبان، کیفیت آموزش برای همه متعهد می‌نمود.

یونسکو سال‌های متمادی است که به‌عنوان بخش مهمی در {ترسیم} خطوط اقدام جامع اجلاس سران و مجمع سالانه اجلاس سران ایفا نقش می‌نماید.

یونسکو در سال ۲۰۱۳، جهت شناسایی ویژگی‌ها و تکمیل قابلیت‌های اینترنت که در ایجاد جامعه اطلاعاتی و تحقق توسعه پایدار، ضروری می‌باشد و همچنین جهت شناسایی و تولید شاخص‌های اینترنت جهانی (فراگیری یا جهان‌شمولی/ جهان‌گستری اینترنت) فعالیت‌های خود را آغاز نموده نمود.

سازمان یونسکو این فعالیت را از طریق برنامه‌های گسترده‌ای شامل تحقیق، تحلیل، مشاوره‌های برخط و مباحثه‌های رودررو با نمایندگان کشورهای عضو و جامعه ذی‌نفعان اینترنت (از جمله جامعه مدنی و سازمان‌های مردم‌نهاد، بخش‌های خصوصی، کارشناسان حقوقی، سیاسی، روزنامه‌نگاران و کارشناسان فضای رسانه) در سطوح مختلف ملی، منطقه‌ای و بین‌المللی انجام داد. اولین مطالعات مفهومی در این زمینه در سال ۲۰۱۳ انجام گرفت و در ژوئن ۲۰۱۴ پس از ماه‌ها مشورت چندجانبه با کشورهای عضو و مشارکت گروه‌های بین‌دولتی مانند گروه ۷۷ و اتحادیه اروپا، اولین پیش‌نویس سند فراگیری اینترنت تهیه شد و این سند توسط شورای عمومی یونسکو در سال ۲۰۱۵ به تأیید رسید.

سپس به دنبال شناخت شاخصه‌های اینترنت جهانی، فرایندی از تحقیقات کتابخانه‌ای^۱ رایزنی و مشاوره‌های کارشناسان در سطح بین‌المللی، آزمایش‌های میدانی در تعدادی از کشورها صورت گرفت. این عملیات توسط سازمان یونسکو و با پشتیبانی کنسرسیومی^۲ به رهبری انجمن ارتباطات پیشرفته^۳ در سال ۲۰۱۷ در طی سه دوره انجام گرفت. فاز اول و فاز دوم شامل جلسات همفکری بودند که جهت توسعه شاخصه‌هایی برای فراگیری اینترنت هم در بستر برخط و هم جلسات رودررو انجام گرفت و فاز سوم جهت فقط شامل نشست‌های غیربرخط بود.

در فاز اول این پروژه از ۱۴ ژوئن تا ۳۱ اکتبر سال ۲۰۱۷، جلسات مشاوره‌ای در بستر برخط و به شش زبان رسمی انجام گرفت این جلسات در خصوص آماده‌سازی پیش‌نویسی درباره فراگیری اینترنت و نحوه تجمع این موضوعات در یک چارچوب مشخص بود. همچنین در همین راستا، بین ماه‌های مارس تا اکتبر همین سال، ۲۶ نشست مشاوره‌ای و گارگاهی

1. desk research

2. Consortium

3. Association for Progressive Communications (APC)

در سطوح ملی، منطقه‌ای و بین‌المللی در کشورهای زیر برگزار گردید: آرژانتین، اتریش، بلژیک، چین، کلمبیا، استونی، فرانسه، آلمان، اندونزی، جامائیکا، اردن، کنیا، پاناما، پرو، پرتغال، روسیه، آفریقای جنوبی، سوئد، سوئیس، تایلند، امارات متحده عربی و ویتنام.

فاز دوم این پروژه با هدف تهیه پیش‌نویس چارچوب شاخصه‌ها از اول دسامبر ۲۰۱۷ تا ۱۵ مارس ۲۰۱۸ در بستر برخط به شش زبان رسمی انجام شد. همچنین ۱۵ رویداد مشاوره‌ای در ۱۳ کشور زیر برگزار گردید: برزیل، کانادا، یونان، فرانسه، غنا، ایتالیا، پرو، سریلانکا، سوئیس، تایلند، تونس، انگلیس و ایالات متحده آمریکا.

در فاز سوم پروژه که از جولای تا سپتامبر ۲۰۱۸ انجام گرفت، شاخص‌هایی که از دو فاز قبلی استخراج شده بودند مورد بررسی و اصلاح بیشتری قرار گرفت و جهت غربالگری علمی در چهار کشور برزیل، اکوادور، نیجریه و پاکستان مورد آزمایش قرار گرفت. در مرحله بعد این شاخصه‌ها طی تمرینات دیگری به شکل تمرینات پایلوت در سه کشور برزیل، سنگال و تایلند تصحیح گردیدند. نتایج این تمرینات توانست سبب اصلاح نهایی این شاخصه‌ها گردد. همچنین این فاز شامل برگزاری ۵ نشست مشاوره‌ای در کشورهای فرانسه، گرجستان، آلمان، غنا و آمریکا بود.

فراگیری اینترنت چهار اصل زیر را دربر می‌گیرد که اساس توسعه اینترنت جهت دستیابی به اهداف توسعه پایدار می‌باشد. این شاخص‌ها بر مبنای چهار اصل مهم زیر تحت عنوان R-O-A-M^۱ شناخته می‌شود:

- ✓ اصل اینترنتی مبتنی بر حقوق بشر؛
- ✓ اصل اینترنت آزاد؛
- ✓ اصل اینترنت دسترس پذیر برای همه؛
- ✓ اصل اینترنت با مشارکت چندذی‌نفعی.

این ساختار، علاوه بر چهار اصل فوق، شاخص دیگری تحت عنوان شاخصه‌های مداخله‌ای

1. R – that the internet be based on human Rights
 O – that it is Open
 A – that it should be Accessible to all, and
 M – that it is nurtured by Multistakeholder participation.

یا متقاطعی^۱ را دارد که چند موضوع زیر را در بر می‌گیرد:

✓ کودکان؛

✓ توسعه پایدار؛

✓ اعتماد و امنیت؛

✓ جنبه های قانونی و اخلاقی اینترنت.

شاخصه های ROAM جهت کمک به دولت‌ها و سایر ذی‌نفعان در امور زیر قابل کاربرد می‌باشد:

✓ ارزیابی محیط‌های اینترنت ملی خود؛

✓ شناسایی و بررسی حوزه‌های مختلف و نحوه هم‌ترازی آن با اصول ROAM و شناسایی

حوزه‌هایی که در آن اصلاحات سیاست و رویه‌ها می‌تواند ارتقای داده شود؛

✓ توسعه مناسب رویکردهای سیاسی و اصلاحات در زمینه اجرای این سیاست‌ها؛

✓ بررسی مقایسه‌ای کشورها باهم در زمینه ارزیابی عملکرد ملی؛

✓ استفاه‌دی‌نفعان ملی مختلف از جمله دولت، سازمان‌ها، جامعه مدنی، صنعتی، دانشگاهی

و سایر گروه‌های چندذی‌نفعی که با توسعه اینترنت، دسترسی و حقوق اینترنت ارتباط دارند.

چارچوب شاخصه های فراگیری اینترنت، علاوه بر چهار اصل فوق، شامل تعداد دیگری از

شاخص های وابسته نیز می‌باشند که اطلاعات زمینه ای را تأمین می‌نمایند که برای تفسیر

یافته های مشتق شده از شاخصه های ROAM مهم می‌باشند. این شاخصه ها در حوزه‌های

زیر قرار دارند:

۱. شاخصه‌های اقتصادی: موضوعات مطرح در این شاخصه‌ها در ارتباط با وضعیت جاری و

کارایی اقتصاد کشورها بحث می‌نماید:

✓ سرانه درآمد ناخالص ملی^۲: که منبع مهم برای این شاخص مجموعه داده‌هایی از تولید

می‌باشد که توسط بانک جهانی نگهداری می‌شود؛

✓ نرخ رشد درآمد ناخالص ملی در ۱۰ سال گذشته؛

1. cross-cutting

شیوه ای برای جداسازی شاخصه ها و بررسی آن‌ها می‌باشد که از دیدگاه ذی‌نفعان مختلف انتخاب می‌گردد. به این شکل که نیازهای هر یک از ذی‌نفعان مشخص شده و نیاز آن‌هایی که نیازهای دیگر را تحت تأثیر قرار می‌دهند مطرح می‌گردند.

2. Gross National Income (GNI)

✓ سهم خدمات از تولید ناخالص ملی^۱ قابل انتساب به خدمات^۲: منبع مهم این شاخصه مجموعه داده‌هایی درباره توزیع بخشی تولید ناخالص داخلی است که توسط بانک جهانی نگهداری می‌گردد.

۲. شاخصه‌های جمعیتی (شاخصه‌های جهت آمارگیری نفوس): موضوعات اصلی در این شاخصه‌ها در ارتباط با وضعیت جمعیت کشورها مورد استفاده قرار می‌گیرد. از قبیل: تعداد و روند رشد جمعیت کشور که منبع مهم برای این شاخص مجموع داده‌هایی از تعداد و میزان رشد جمعیت است که توسط بخش جمعیت در اداره امور اقتصادی اجتماعی سازمان ملل متحد نگهداری می‌گردد: امید به زندگی^۳، مقاطع سنی، تنوع زبانی، رتبه شهرنشینی.

۳. شاخصه‌های توسعه: موضوعات مهم این شاخصه به تحلیل سطح توسعه سرتاسر کشور که شدیداً به دسترسی و استفاده از فناوری اطلاعات و ارتباطات وابسته می‌باشد می‌پردازد.

✓ شاخصه‌های توسعه انسانی در برنامه توسعه سازمان ملل متحد^۴: شاخصه‌ای مرکب از امید به زندگی، آموزش و درآمد ناخالص ملی؛

✓ شاخصه تجربه آموزشی: میانگین سال‌های تحصیلی، تناسب گروه‌های سنی در آموزش مقاطع ابتدایی، دوره‌های دوم و سوم آموزش؛

✓ سطح سواد در ارتباط با قابلیت‌های فردی در استفاده از اینترنت؛

✓ دسترسی به برق که یک زیرساخت متمم و اصلی برای تسهیل استفاده از اینترنت می‌باشد.

۴. شاخصه‌های تساوی و برابری: موضوعات مطرح در این شاخصه در ارتباط با برابری و تساوی در استطاعت دسترسی و استفاده از اینترنت را شامل می‌گردد. ضریب جینی^۵ جهت اندازه‌گیری توزیع ثروت و یا درآمد مطابق با جمعیت که جزء مهم‌ترین شاخصه‌ها برای تعیین بی‌عدالتی اجتماعی می‌باشد.

۵. شاخصه حکمرانی: موضوعات مربوط به این شاخص در ارتباط با جنبه‌های مختلف کیفیت

حکمرانی بر محیط اینترنت می‌باشد:

1. Gross domestic Product
2. Proportion of GDP attributable to services
3. life expectancy
4. UNDP Human Development Index (HDI)
5. Gini coefficient

شاخصی برای نابرابری درآمد می‌باشد در صورتیکه توزیع درآمد کاملاً برابر باشد این ضریب مساوی صفر و در صورتیکه توزیع درآمد کاملاً نابرابر باشد این ضریب مساوی ۱ است هرچه این ضریب کوچک باشد توزیع درآمد عادلانه‌تر است

✓ شاخص حکمرانی جهانی: منبع مهم برای این شاخص، شش الگویی است که توسط بانک جهانی ایجاد شده است؛

✓ شاخص‌های حاکمیت قانون^۱: منبع مهم این شاخصه توسط پروژه عدالت جهانی^۲ ایجاد شده است؛

✓ شاخص انجام کسب و کار^۳ (که منبع مهم این شاخص توسط بانک جهانی آماده شده است).
۶. شاخص‌های توسعه فناوری اطلاعات و ارتباطات: موضوعات مهم در این شاخصه که در ارتباط با آمادگی و کارایی، ارزیابی محیط فناوری اطلاعات و ارتباطات برای شاخصه‌های فراگیری اینترنت هستند شامل موارد زیر می‌باشند:

✓ شاخص توسعه فناوری اطلاعات و ارتباطات: منبع مهم برای این شاخصه، فهرستی از شاخص‌های توسعه فناوری اطلاعات و ارتباطات می‌باشد که توسط اتحادیه بین‌المللی مخابرات تهیه شده است؛

✓ شاخصه اتصالات سیار^۴: منابع اصلی برای ارزیابی این شاخصه، فهرستی از شاخص‌هایی است که توسط انجمن گروه ویژه موبایل^۵ آماده شده است؛

✓ شاخص آمادگی شبکه‌ای مربوط به مجمع جهانی اقتصاد که اثر فناوری اطلاعات در سطح جهانی را ارزیابی می‌کند و آمادگی کشورها در استفاده از فناوری اطلاعات در اقتصاد خود را نشان می‌دهد.

✓ شاخصه تجارت الکترونیکی کنفرانس تجارت و توسعه ملل متحد (آنکتاد)^۷.

اصل اول: اینترنتی مبتنی بر حقوق بشر

این اصل در ارتباط با چارچوب‌های تنظیم مقررات و حقوقی برای دسترسی جهانی می‌باشد و موضوعات زیر را دربر می‌گیرد:

1. Rule of law index
2. World Justice Project (WJP)
3. Doing Business Index World Bank
4. Mobile Connectivity Index
5. Group Spectioal Mobile Association (GSMA)
6. World Economic Forum Networked Readiness Index
7. United nations conference on trade and development

➤ چارچوب سیاسی، حقوقی و تنظیم مقررات:

باتوجه به اینکه مجمع عمومی و شورای حقوق بین‌الملل سازمان ملل تأیید نموده‌اند که همان حقوقی که افراد در فضای غیربرخط دارند باید در فضای برخط نیز محافظت گردد، علاوه بر تعدادی از اسناد حقوق منطقه‌ای، از سند‌های مورد نیاز جهت بررسی این شاخص در راستای حقوق بشر در چارچوب بین‌الملل می‌توان به موارد زیر اشاره نمود:

- ✓ اعلامیه جهانی حقوق بشر؛
- ✓ میثاق بین‌المللی حقوق مدنی و سیاسی^۱؛
- ✓ میثاق بین‌المللی حقوق اقتصادی، اجتماعی و فرهنگی^۲؛
- ✓ کنوانسیون رفع تمامی اشکال تبعیض نژادی^۳؛
- ✓ کنوانسیون رفع تبعیض علیه زنان^۴؛
- ✓ کنوانسیون حقوق کودک^۵.

➤ آزادی بیان:

یکی از مصادیق حقوق بشر که مطابق اعلامیه جهانی حقوق بشر تحت تأثیر اینترنت به‌عنوان محیط ارتباطی قرار گرفته است حق آزادی بیان می‌باشد. اعمال این حق ممکن است تابع محدودیت‌های معینی قرار گیرد. این محدودیتها باید بنا به ضرورت‌های زیر و بوسیله قانون انجام گیرد:

- الف: برای احترام به حقوق و حیثیت دیگران؛
- ب: برای حفظ امنیت ملی، نظم و سلامت و اخلاق عمومی.

➤ حق دسترسی به اطلاعات:

اسناد تعیین خط‌مشی این مقوله شامل مورد زیر می‌باشد:

✓ مطابق ماده ۳۴ کنوانسیون حقوق کودک جهت استثمار کودکان در موضوع پورنوگرافی^۶ که در آن دولت‌های عضو پیمان، خود را موظف می‌دانند که کودک را در مقابل هرگونه استثمار و سوءاستفاده جنسی حمایت کنند. حکومت‌ها برای این منظور اقداماتی در سطح داخل و خارج

1. the International Covenant on Civil and Political Rights (ICCPR)
 2. the International Covenant on Economic, Social and Cultural Rights (ICESCR)
 3. the Convention on the Elimination of All Forms of Racial Discrimination (ICERD)
 4. the Convention on the Elimination of Discrimination against Women (CEDAW)
 5. the Convention on the Rights of the Child (CRC)
 6. Right of access to information

از کشور انجام می‌دهند تا:

(الف) کودکان به روابط جنسی غیر قانونی یا اجباری کشانده نشوند؛

(ب) کودکان در زمینه فاحشه‌گری مورد استفاده قرار نگیرند؛

(ج) از کودکان در پورنوگرافی و نمایش های جنسی استفاده نشود.

➤ آزادی تجمع و حق مشارکت در انجام امور عمومی:

این مقوله جزء مصادیقی از حقوق بشر می‌باشد که تحت تأثیر اینترنت قرار گرفته است و طبق قوانین و مقررات موجود ماده ۲۱ و ۲۲ میثاق بین‌المللی حقوق مدنی و سیاسی^۲ که مربوط به تجمع صلح آمیز و حقوق آزادی مرتبط با آن می‌باشد مورد بررسی قرار می‌گیرد.^۳

➤ حقوق حریم خصوصی:

از زمانی که آزادی بیان و تجمع و حقوق دسترسی به اطلاعات توسعه یافته اند، نگرانی درباره تهدیدات حریم خصوصی که توسط اینترنت ایجاد می‌شود تشدید شده است. خطمشی‌های این موضوع می‌توانند مطابق با قوانین و مقررات زیر تعیین گردند:

✓ طبق ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی که هیچ شخصی نباید تحت تأثیر مداخله‌های خودسرانه یا نامشروع در حریم خصوصی خود، خانواده، خانه یا مکاتبات خود قرار بگیرد. نباید شرافت و حیثیت هیچ کس او مورد تعرض غیرقانونی واقع گردد. هر کسی این حق را دارد تا در مقابل این تعرضات و دخالت‌ها از حمایت قانون برخوردار گردد؛

1. Freedom of Association and the Right to take part in the Con-duct of Public Affairs
2. International convent on civil and political Rights

۳. ماده بیست و دوم

۱. هر کس حق آزادی (تشکیل) اجتماعات با دیگران را دارد. این حق شامل تشکیل و پیوستن به اتحادیه‌ها و برای حفاظت علاقه مندیها و منافع خود می‌باشد.
۲. اعمال این حق تابع هیچگونه محدودیتی نیست مگر اینکه این محدودیتها مطابق قانون آنهم در یک جامعه دموکراتیک و به‌طور ضروری جهت نفع (مصلحت)، امنیت ملی، ایمنی عمومی، نظم عمومی، حفاظت از سلامت و اخلاق عمومی و یا حفاظت از آزادیهای دیگران باشد. (همچنین) این ماده مانع از آن نمی‌شود که اعضاء نیروهای مسلح و پلیس در اعمال این حق، تابع محدودیت‌های قانونی باشند.
۳. هیچیک از مقررات این ماده، کشورهای عضو مقوله نامه سازمان بین‌المللی کار، مورخ ۱۹۴۸ که مربوط به آزادی (تشکیل) اتحادیه و حمایت از حق متشکل شدن است، مجاز نمی‌شمارد که با اقدامات قانونگذاری و یا با نحوه اجرای قوانین به تضمین های ارائه شده در این مقوله نامه مخالفت کنند و به آن لطمه وارد آورند.
ماده بیست و سوم

۱. خانواده یک واحد گروهی و (جزء عنصر) بنیادین و طبیعی جامعه است و شایسته می‌باشد که بوسیله جامعه و حکومت حفاظت گردد.

۲. حق ازدواج و تشکیل خانواده برای مردان و زنانی که به این سن رسیده اند، برسمیت شناخته میشود.

۳. هیچ ازدواجی بدون رضایت آزادانه و کامل زوجین منعقد نمی‌گردد.

۴. کشورهای عضو این میثاق، باید اقدامات مناسب را بمنظور تأمین تساوی حقوق و مسئولیت‌های زوجین در خلال انعقاد و فسخ ازدواج بعمل آورند. در مورد فسخ ازدواج باید برای حفاظت کودکان پیش‌بینی‌های لازم انجام گیرد.

4. The Right to Privacy

✓ ماده ۱۶ کنوانسیون حقوق کودک به حمایت از این حقوق بیشتر تأکید می‌نماید.
 ✓ علاوه بر این می‌توان به قطعنامه‌های مصوب مجمع عمومی در باب حق حریم خصوصی در عصر دیجیتال نیز اشاره نمود.

➤ حقوق اجتماعی، اقتصادی و فرهنگی:

اینترنت قابلیت عظیمی در اهداف توسعه اقتصادی و اجتماعی مندرج در دستور کار ۲۰۳۰ توسعه پایدار دارد. مفاد ۶ تا ۱۴ سند حقوق اجتماعی اقتصادی و فرهنگی^۳ به موضوعاتی در ارتباط با حقوق استخدام، امنیت اجتماعی، زندگی خانوادگی، استاندارد کافی برای زندگی از جمله رهایی از قحطی، سلامت، آموزش و ماده ۱۵ این سند نیز به حقوق هر شخصی در سهیم شدن در زندگی اجتماعی اشاره می‌نمایند.

اصل دوم: اصل اینترنت آزاد

موضوعات زیر این اصل در ادامه مورد بررسی قرار می‌گیرد.

➤ سیاست کلی، چارچوب حقوقی و تنظیم مقررات:

چارچوب‌های حقوقی و تنظیم مقررات مناسبی جهت پشتیبانی از یک فرایند سیاست‌گذاری شفاف و با نگاهی رو به جلو ضروری است تا از یک منبع آزاد، عمومی و فراگیر مانند اینترنت حمایت نماید. اسناد تعیین خط‌مشی، باید به‌کارگیری اینترنت در بستری ملی و آزاد، تسهیل همکاری و رقابت میان تمامی دستگاه‌ها، با احترام به حقوق بشر، تحویل محتوا و اپلیکیشن‌ها به کاربر در در یک محیط امن را تضمین نماید.

➤ استانداردهای آزاد:

ارزیابی اینترنت، نیازمند رسیدگی و توجه به اجرای استانداردها و پروتکل‌هایی است که رشد و امنیت اینترنت را تسهیل می‌نماید. استانداردهای آزاد یک نقش اساسی در ارتقای قابلیت‌ها، نوآوری‌ها،

۱. محدوده شخصی و خصوصی هیچ کودکی قابل تعرض نیست. این محدوده که شامل همه جوانب مربوط به امور خانوادگی، مسکونی، حیثیتی و مکانیات شخصی است، نباید به‌طور عمد یا غیرقانونی آسیب ببیند.
 ۲. برخورداری از حمایت قانونی در مقابل چنین آسیب‌هایی، حق کودک است.

تأمین خدمات گوناگون در بستر اینترنت را ایفا می‌نماید. علاوه بر این مراجع و مقامات ملی می‌توانند در ارتقای استانداردهای آزاد از طریق تأمین خدمات عمومی نقش مهمی ایفا نمایند.

➤ **بازارهای آزاد:**

بازارهای آزاد برای خدمات شبکه‌ها و ارتباطات، انتخاب مشتریان را تسهیل می‌نماید. نوآوری و تمایل برای پایین آوردن قیمت‌ها، بهبود کیفیت‌ها برای کاربران نهایی را برانگیخته می‌نماید.

➤ **داده‌ها و حاکمیت باز:**

خط‌مشی داده‌های باز و قابل دسترس‌پذیر برای بهره‌مندی عموم است که توسط دولت‌ها و گاهی ذی‌نفعان محقق می‌شود و توسط اشخاص، تجار (در تجارت‌های محلی و خارجی) و سازمان‌های جامعه مدنی استفاده می‌شوند.

اصل سوم: اینترنتی دسترس‌پذیر برای همه

امروزه دسترسی به اینترنت و خدمات مبتنی بر آن سریع‌تر از سایر رسانه‌ای ارتباط جمعی قبلی رشد نموده است به‌ویژه از زمانی که صفحه گسترده جهانی محبوب گردید و اخیراً ظهور دسترسی موبایل (تلفن همراه) به اینترنت و دسترس‌پذیری تلفن‌های هوشمند نیز رشد کرده‌اند. با این حال هنوز دسترسی به اینترنت به شدت غیرمتعادل است. وجود شکاف‌های دیجیتالی بین کشورها و بین مناطق و بین جوامع، بیش از یک دهه است که ذهن نهادهای سازمان ملل متحد و سایر ذی‌نفعان را به خود مشغول نموده است. سابقه این نگرانی به قبل از اجلاس سران درباره جامعه اطلاعاتی برمی‌گردد. اصول دسترس‌پذیری اینترنت برای همه شامل جنبه‌های فنی، اقتصادی و اجتماعی می‌باشد و نیاز به چارچوب‌های قانونی و تنظیم مقررات دارند که توانایی و استطاعت دسترسی را برای تمامی جوامع موجود در یک کشور مطالبه نمایند.

بُعد فنی موضوع شامل دسترس‌پذیری برابر به زیرساخت‌های ارتباطی و ظرفیت تجهیزات استفاده شده جهت قابلیت دسترسی به خدمات مربوط به پهنای باند بالاتر می‌باشد. ابعاد اقتصادی و اجتماعی موضوع شامل موارد زیر می‌باشد: استطاعت مالی، دسترس‌پذیری به محتوا

از جمله محتوای مربوط به زبان^۱، ظرفیت‌های مردم در استفاده مؤثر از اینترنت برای اهداف شخصی خود.

استفاده مؤثر از اینترنت و خدمات مبتنی بر اینترنت نیازمند تأیید قابلیت و صلاحیت از نگاه کاربران می‌باشد. برای اشخاص و مؤسسات بازرگانی و سازمان‌هایی که استفاده از اینترنت را جهت تجارت و یا سایر اهداف خود انتخاب می‌نمایند قابلیت و صلاحیت در ارائه خدمات مهم می‌باشد. اهمیت سواد رسانه‌ای و اطلاعاتی - مانند سوادهای پایه‌ای، قابلیت‌های لازم جهت استفاده مؤثر از خدمات برخط، اپلیکیشن‌ها و شایستگی‌های فنی در سطوح مختلف- جهت اکتساب این هدف، به شکل گسترده‌ای به رسمیت شناخته شده است.

بنابراین می‌توان عنوان نمود که در مقوله اینترنت دسترس‌پذیر، شاخصه‌های زیر باید مورد نظر قرار گیرد:

✓ چارچوب سیاسی، حقوقی و تنظیم مقررات؛

✓ اتصالات و کاربرد؛

✓ استطاعت و توانایی دسترسی؛

✓ محتوا و زبان محلی؛

✓ ظرفیتها / شایستگی‌ها^۲.

اصل چهارم: اینترنت با مشارکت چند ذی‌نفعی

توسعه اینترنت توسط مشارکت ذی‌نفعان ایجاد شده است. دستور کار تونس برای جامعه اطلاعاتی که در فاز دوم اجلاس سران درباره جامعه اطلاعاتی در سال ۲۰۰۵، تصویب گردید، ضمن اذعان به ضرورت مشارکت چندذی‌نفعی جهت ایجاد جامعه اطلاعاتی مردم‌محور، فراگیر و توسعه‌مدار^۳، توسعه فرایندهای چندذی‌نفعی در سطوح ملی، منطقه‌ای و بین‌المللی را تصدیق نمود. این

1. content in relevant languages

2. Capabilities / Competencies

3. multi-stakeholder participation is essential to the successful building of a people-centred, inclusive and development-oriented Information Society

فرایندهای چندذی‌نفعی در زمینه بحث و همکاری در توسعه و گسترش اینترنت می‌باشد که به‌عنوان ابزاری جهت پشتیبانی از تلاش برای کسب توافق بین‌المللی در اهداف و مقاصد توسعه پایدار، از جمله اهداف توسعه هزاره، مطرح است.^۱

مجمع عمومی سازمان ملل نیز در بازنگری ۱۰ ساله نتایج اجلاس سران^۲ در سال ۲۰۱۵ با تأیید ارزش و اصول همکاری و تعاملات چندذینفعی، {نقش حیاتی} مشارکت مؤثر و همکاری دولت‌ها، بخش خصوصی، جامعه مدنی، سازمان‌های بین‌المللی، جوامع فنی و دانشگاهی و تمامی ذی‌نفعان مرتبط را مطابق با مسئولیت‌پذیری و نقش آن‌ها در توسعه جامعه اطلاعاتی به رسمیت می‌شناسد. به‌ویژه نقش این همکاری‌ها در نمایشی متعادل از کشورهای در حال توسعه^۳.

مشارکت چندذی‌نفعی دولت‌ها، سازمان‌های بین‌دولتی و بین‌المللی، بخش خصوصی، جامعه مدنی، جوامع فنی اینترنت، جوامع حرفه‌ای و دانشگاهی در توسعه و حکمرانی اینترنت ترسیم شده است. هدف مشارکت چند ذی‌نفعی، بهبود جامعیت، کیفیت تصمیم‌سازی توسط تمامی کسانی که منافع در اینترنت دارند و اثر این تصمیمات روی توسعه اجتماعی، اقتصادی و فرهنگی، در فرایندهای باز و تصمیم‌سازی شفاف می‌باشد.^۴

طبق دستور کار سازمان ملل متحد درباره توسعه پایدار، مشارکت چند ذی‌نفعی می‌تواند موجب اشتراک‌گذاری دانش، خبرگی، تجهیز منافع فنی و مالی در حمایت از دستاوردهای اهداف توسعه پایدار در تمامی کشورها مخصوصاً کشورهای در حال توسعه گردد. میزان مشارکت تأثیرگذار ذی‌نفعان توسط تعدادی از عوامل مشخص می‌گردد، از جمله گسترش سطح آگاهی

2. the development

of multi-stakeholder processes at the national, regional and international levels to discuss and collaborate on the expansion and diffusion of the Internet as a means to support development efforts to achieve internationally agreed development goals and objectives, including the Millennium Development Goals

3. ten-year review of WSIS outcomes in 2015

4. reaffirmed 'the value and principles of multi-stakeholder cooperation and engagement ... , recognizing that effective participation, partnership and cooperation of Governments, the private sector, civil society, international organizations, the technical and academic communities and all other relevant stakeholders, within their respective roles and responsibilities, especially with balanced representation from developing countries, has been and continues to be vital in developing the information society.

5. Multistakeholder participation in the development and governance of the Internet has drawn together governments, intergovernmental and international organisations, the private sector, civil society and the Internet technical and professional community and academia. The goal of multistakeholder participation is to improve the inclusiveness and quality of decision-making by including all those who have an interest in the Internet and its impact on wider social, economic and cultural development in open and transparent decision-making processes

آن‌ها، منافع، محتوا و دانش، سطح سازمان یا سطح مسئولیت آن‌ها در نتایج مرتبط با اینترنت و ماهیت فرایند مشاوره و تصمیم‌سازی‌ها.

مشارکت چندذی‌نفعی، به اصل محوری مجمع حکمرانی اینترنت تبدیل شده است. شاخصه‌های تقویت و رشد اینترنت توسط مشارکت ذی‌نفعان به سه موضوع زیر تقسیم می‌گردد:

- ✓ چارچوب سیاسی، حقوقی و تنظیم مقررات برای مشارکت در حکمرانی؛
- ✓ حکمرانی اینترنت در سطح ملی (مشارکت گروه‌های مختلف ذی‌نفعان در سیاست‌گذاری‌های مرتبط با اینترنت در سطح ملی)؛
- ✓ حکمرانی اینترنت در سطح منطقه‌ای و بین‌المللی (توسعه مشارکت گروه‌های مختلف ذی‌نفعان داخل کشور در مجمع بین‌المللی با موضوعات حکمرانی اینترنتی).

گفتار شش: سازمان جهانی مالکیت معنوی

حوزه کپی رایت و سایر حقوق مرتبط با آن در چند دهه اخیر به موازات پیشرفت‌های فناورانه، گسترش چشمگیری داشته است. اما انتشار آثار از طریق اینترنت، آخرین تحولی است که سؤالات جدیدی را در ارتباط با کپی رایت ایجاد کرده است. سازمان جهانی مالکیت معنوی (واپو) عمیقاً درگیر مباحث دامن‌داری برای شکل دادن به استانداردهای جدید برای حفاظت از کپی رایت در فضای سایبر است. سازمان معاهدات موسوم به معاهدات اینترنت در صدد تنظیم هنجارهای بین‌المللی با هدف پیشگیری از دسترسی غیر مجاز و استفاده از آثار خلق شده در اینترنت و سایر شبکه‌های دیجیتال می‌باشد. هر دو معاهده در صدد مواجهه و تعامل با فناوری‌های دیجیتال کنونی و مقابله با استفاده‌های سوء از آن است، از جمله مقابله با انتشار محتوای حفاظت شده در شبکه‌های دیجیتال با تمرکز بر اینترنت. به همین خاطر است که به این معاهدات، اغلب معاهدات اینترنت گفته می‌شود. مهم‌ترین نکته در ارتباط با این معاهدات این است که این معاهدات از حقوق مالکان این آثار به صورت بسنده و مؤثر در زمان انتشار از طریق سیستم‌های ارتباطی مثل اینترنت محافظت خواهد کرد. بنابراین این معاهدات تصریح می‌کنند که حقوق موجود، قابل

اعمال و تسری در فضای دیجیتال می‌باشد. ضمن اینکه این دو معاهده حقوق برخطی جدیدی ایجاد می‌کنند. برای حفظ تعادل منصفانه و عادلانه منافع بین مالکان حقوق و عامه مردم، معاهدات تصریح می‌کنند که کشورها منطقیاً در ایجاد استثناها و محدودیتهای مربوط به حقوق محیط دیجیتال دارای انعطاف‌پذیری معقولی می‌باشند. کشورها می‌توانند عندالافتضاء استثنائاتی را برای منافع عمومی مثل اهداف مرتبط با آموزش و پرورش و پژوهش رایگان در نظر گیرند.

معاهدات اینترنت سازمان جهانی مالکیت معنوی

در سال ۱۹۹۶ نگرانی‌های مربوط به امکان فرار از اقدامات حمایتی فناوریانه^۱ بسیاری از اعضای سازمان جهانی مالکیت معنوی را بر آن داشت که دو معاهده را که به معاهدات اینترنت سازمان جهانی مالکیت معنوی^۲ معروف‌اند تصویب نمایند. به موجب این دو معاهده، دولت‌های عضو موظف گردیدند حمایت‌های مناسب و راهکارهای جبران خسارت قانونی مؤثری را در مقابل گریز غیر قانونی از اقدامات حمایتی فناوریانه^۳ پیش گیرند.

اقدامات حمایتی فناوریانه، یک راهکار فنی برای جلوگیری از نقض کپی رایت آثار در محیط‌های الکترونیکی است. مثل کدگذاری و رمزگذاری اطلاعات. این دو معاهده شامل: ۱. معاهده کپی رایت وایپو^۴ و ۲. معاهده اجراها و فنوگرام‌های وایپو^۵. این معاهدات در پاسخ به چالش‌های پدید آمده در زمینه کپی رایت ناشی از فناوری‌های جدید دیجیتال در دسامبر ۱۹۹۶ در ژنو تصویب شدند. معاهده «WCT» در مارس ۲۰۰۲ لازم‌الاجرا گردید. این معاهده، کنوانسیون برن را که مهم‌ترین معاهده بین‌المللی کپی‌رایت در جهان امروز می‌باشد را به‌روز و تکمیل نمود.

مهم‌ترین ویژگی‌های معاهده در زمینه کپی رایت عبارت است از ایجاد حق انتقال دیجیتال. این حق به‌عنوان حق انحصاری مؤلفان آثار ادبی و هنری جهت صدور اجازه‌ی انتشار عمومی آثار آنان از طریق بی‌سیم و با سیم پیش‌بینی شده است تا آثار مؤلفان به نحوی در دسترس عموم

1. Technological Protection Measures (TPMs)

2. WIPO Internet Treaties

3. Unlawful Circumvention of TPMs

4. WIPO Copyright Treaty (WCT)

5. WIPO Performances and Phonograms Treaty (WPPT)

قرار گیرد که افراد جامعه بتوانند در هر زمان و از هر مکانی که بخواهند به این آثار دسترسی پیدا کنند. طرف‌های متعاقد معاهده آزادند که محدودیت‌ها یا استثنائاتی را در مورد حقوق مؤلفان در برخی از موارد پیش‌بینی نمایند مشروط بر اینکه با استفاده‌ی معمول و متعارف از اثر متعارض نباشد و به نحو نامتعارفی به منافع مشروع مؤلف صدمه نزند. طرف‌های متعاقد مکلف به پیش‌بینی حمایت قانونی مناسب و کافی و راه‌های حقوقی جبران خسارت مؤثر در مقابل فرار از فناوری حمایتی کپی رایت می‌باشند.

بر اساس معاهده WCT حق تکثیر به نحوی که در ماده (۹) کنوانسیون برن پیش‌بینی شده، در محیط دیجیتال نیز جهت استفاده از آثار مزبور قابل اعمال است و ذخیره سازی اثر مشمول کپی‌رایت به صورت دیجیتال در یک واسطه‌ی الکترونیکی نیز به منزله‌ی تکثیر و نسخه برداری در مفهوم ماده (۹) کنوانسیون برن تلقی شده است. بر اساس این ماده:

۱. مؤلفان آثار ادبی و هنری تحت حمایت معاهده از حق انحصاری و قانونی تکثیر آثار خود به هر شکل و نوع برخوردارند؛

۲. در کشورهای عضو اتحادیه، اجازه تکثیر این آثار در موارد خاص مشروط بر این خواهد بود که با اصل اثر، مغایر نباشد و به منافع قانونی مؤلف آسیب نرساند؛

۳. طبق مفاد بیانیه هر نوع ضبط یا تهیه تصویر به عنوان تکثیر تلقی می‌شود. بر این اساس، برنامه‌های رایانه‌ای و مجموعه داده‌ها و اطلاعات تهیه شده به هر شکلی و از هر محلی از قبیل سایت‌های رایانه‌ای صراحتاً در زمره آثار تحت حمایت قرار گرفتند.

ماده ۸ معاهده WCT حق عرضه اثر برای مؤلفان در محیط الکترونیکی را تضمین کرده است. بر این اساس برای مؤلفان، حق انحصاری کنترل دسترسی کاربران به آثار آن‌ها در قالب سیستم‌های ارتباطی زنده از جمله سیستم‌های کارتی و اینترنت در نظر گرفته شده است. طرف‌های متعاقد مکلف گردیده‌اند اقدامات قانونی کافی و مؤثری را در مورد حقوق مدیریت اطلاعات^۱ اتخاذ نمایند. ماده ۱۱ معاهده WCT و ماده ۱۸ معاهده WPPT مقرراتی در خصوص تضمین استفاده از انواع ابزار فنی که برای حمایت از اجرای کپی‌رایت در محیط‌های دیجیتال و شبکه‌ای، لازم و ضروری است پیش‌بینی نموده‌اند، به طوری که قانون‌گذاران کشورهای عضو را مکلف کرده‌اند تا

1 . Rights Management Information(RMI)

از یک چارچوب مشخصی که در معاهدات مزبور برای اقدامات حمایتی فناورانه پیش‌بینی شده تبعیت نمایند. باتوجه به مفاد این دو معاهده توازن میان منافع دارندگان کپی‌رایت و مصالح عمومی ضرورت دارد.

گفتار هفت: سازمان بهداشت جهانی

یکی از برنامه‌های سازمان بهداشت جهانی^۱ به بهداشت الکترونیکی^۲ و بهداشت اینترنت^۳ مربوط می‌شود. امروزه بهداشت اینترنت، طیف گسترده‌ای از توصیه‌های سودمند را برای کاربران شخصی و متخصصان امور بهداشت و همچنین سیستم‌های بهداشتی و بهداشت عمومی جهانی ارائه می‌دهد. در بسیاری از کشورها مردم برای اخذ اطلاعات بهداشتی به سراغ اینترنت می‌روند. در مجامع برخط شرکت می‌کنند و محصولات و خدمات بهداشتی و درمانی خریداری می‌کنند. مؤسسات بهداشتی بخشی از این روند هستند. زیرا سوابق بیماران در حال شبکه شدن هستند و تعاملات با سیستم بهداشت به صورت فزاینده‌ای در حال برخط شدن می‌باشد. رشد جهانی بهداشت اینترنت با اشکال جدیدی از خطرهای مواجه شده است. انواع جدیدی از استثمار و کلاهبرداری شامل فروش و استفاده از داده‌های مربوط به سلامت افراد و گروه‌ها در حال شکل‌گیری است. سوء مدیریت مربوط به اطلاعات بهداشتی و ابزارهای بهداشت الکترونیک پیامدهای گسترده‌ای را برای مردم، صنعت و دولت‌ها به بار آورده است. پخش و فروش غیرقانونی داروها شامل داروهای تقلبی و داروهای بدون مجوز و همچنین داروهای تأیید نشده^۴ و سایر محصولات، مخاطرات بهداشتی در پی داشته و تجارت قانونی را تضعیف کرده است. بنابراین نیازمند یک تلاش بین‌المللی برای مقابله و مبارزه با آثار آن می‌باشیم. حکمرانی اینترنت (شامل حوزه‌های حریم خصوصی، محرمانگی، امنیت و رضایت آگاهانه) به یک موضوع تعیین کننده در زمان ما تبدیل شده است. در محیط جهانی، قوانین و مقررات پیچیده که در سطوح ملی تدوین شده اند از بسندگی و کفایت لازم و کافی برای پیشگیری از فروش اطلاعات پایش

1. the World Health Organization(W.H.O)

2. electronic health

3. The Health Internet

4. counterfeits, adulterated or unapproved drugs

سلامت، افشای داده‌های برخط مربوط به سلامت افراد و رفع نگرانی از امنیت تجهیزات پزشکی و تجهیزات و شبکه‌های بیمارستانی برخوردار نیستند.

مثال‌های زیر برخی موضوعات را نشان می‌دهد: مطالعات اخیر نشان می‌دهد که نگرانی‌های امنیتی در مورد اطلاعات حوزه بهداشت باید فراتر از نگرانی‌های سنتی در مورد به اشتراک گذاشتن اطلاعات مربوط به سوابق بهداشتی بیماران برای استفاده از این اطلاعات توسط افراد ثالث باشد. بنابر اعلام وزارت بهداشت، درمان و خدمات انسانی آمریکا^۱، یک شرکت بیمه درمانی در این کشور رقمی در حدود ۱,۷ میلیون دلار جریمه به خاطر افشای سوابق شخصی (از طریق برخط) بیش از ششصد هزار نفر خواهد پرداخت. سازمان غذا و داروی آمریکا نیز اخیراً هشدار داده است که باتوجه به اتصال و درهم‌تنیدگی تجهیزات پزشکی از طریق اینترنت، شبکه‌های بیمارستانی و سایر تجهیزات پزشکی به صورت روزافزونی در معرض رخنه امنیتی قرار دارند که می‌توانند نحوه عملکرد این تجهیزات را تحت تأثیر قرار دهد.

قطعنامه سازمان بهداشت جهانی

اجلاس شصت‌وششم سازمان بهداشت جهانی^۲ که در ماه می ۲۰۱۳ برگزار شد قطعنامه WH660/24 را در ارتباط با بهداشت الکترونیک تصویب نمود. این قطعنامه تأکید می‌نماید. نام دامنه‌های سطح بالای جهانی مرتبط با بهداشت و سلامت^۳ در تمامی زبانها باید به نحوی عمل نمایند که سلامت عمومی حفظ گردد. این مهم باید از طریق مثل پیشگیری از ایجاد فروشگاه‌های قاچاق دارو، تجهیزات پزشکی و محصولات و خدمات غیر مجاز پزشکی^۴ محقق گردد. این قطعنامه از کشورها عضو خواسته است تا راهکارهایی را برای وزارتخانه‌های بهداشت و مقامات بهداشت عمومی کشورها در جهت تعامل با نمایندگان خود در کمیته مشورتی دولتی شرکت آیکن^۵ به منظور هماهنگی مواضع ملی در قبال نمایندگی، حکمرانی و عملکرد نام دامنه‌های واجد کلمه بهداشت و سلامت^۶ به تمامی زبانها ارائه دهند و به نفع بهداشت عمومی وارد عمل

1. the US Department of Health and Human Services

2. The 66th World Health Assembly

3. health-related global top-level domain names

4. illicit markets of medicines, medical devices and unauthorized health products and services

5. ICANN Governmental Advisory Committee (GAC)

6. the delegation, governance and operation of health-related global top-level domain names

شوند. این قطعنامه از دبیرکل می‌خواهد که بر نهادهای مقتضی از جمله کمیته مشورتی دولتی و هیئت مؤسس آیکن تکلیف نماید که در راستای مصالح سلامت عمومی جهان برای پوشش نام دامنه‌های سطح بالای جهان کلمه «بهداشت و سلامت» در تمامی زبانها اقدام نماید. همچنین از دبیرکل می‌خواهد که به تعامل با کمیته مشورتی و شورای آیکن و دیگر سازمان‌های بین‌دولتی در جهت حمایت از نام‌ها و علائم اختصاری سازمان‌های بین‌دولتی از جمله سازمان بهداشت جهانی اقدام نماید.

اصول حاکم بر نام دامنه‌های سطح بالای مربوط به اینترنت در حوزه سلامت^۱

وجود یک محیط قابل اعتماد برای بهداشت اینترنت امری ضروری و قابل دستیابی است. این موضوع در راستای امنیت بهداشتی، بهداشت و آموزش پزشکی، حفظ حریم خصوصی و ارتقای بهداشت عمومی در مقیاس اجتماعی امری بسیار مهم است. بهداشت در بسیاری از کشورها به‌عنوان یک بخش بسیار مهم، تنظیم مقررات^۲ شده است. هر چند به خاطر ماهیت جهانی اینترنت، اجرای قوانین ملی مشکل است. بنابراین ضروری است مدیریت و هماهنگی این نوع دامنه‌ها مطابق با اهداف بهداشت عمومی در جهان باشد تا بتواند در این سطح به مردم، جامعه مدنی، دولت‌ها و صنعت خدمت نماید.

حکمرانی و مدیریت^۳

باید یک الگوی حکمرانی مناسب اتخاذ شود و در آن ضرورت مشارکت جامعه بهداشت جهانی و سایر ذی‌نفعان شامل جامعه مدنی، مؤسسات دانشگاهی، مجامع حرفه‌ای، مشاغل، دولت‌ها و سازمان‌های بین‌المللی^۴ با هدف توسعه مستمر بهداشت اینترنت و استفاده از آن به رسمیت شناخته شود. علاوه بر آن، چارچوب سیاست‌گذاری‌ها، خط‌مشی‌ها و رویه‌ها باید مطابق با چارچوب‌های قانونی و مقرراتی باشد. برای ایجاد اعتماد عمومی، سیاست‌ها و پروتکل‌ها باید

1. Governing principles for a .health top-level domain

2. regulations

3. Governance and management

4. the global health community and stakeholders – including civil society, academic institutions, professional associations, businesses, governments and international organizations

شفافیت، انصاف، پاسخگویی و مسئولیت‌پذیری را تضمین نمایند.

استفاده مفرط از اینترنت^۱، تدوین سیاست‌ها و برنامه‌هایی برای مقابله با این مشکل روبه‌رشد دهه‌های اخیر شاهد انفجار استفاده از دستگاه‌های الکترونیکی، اینترنت و پلت فرم‌های بازی‌ها بوده است. در ارتباط با استفاده مفرط از این وسایل، اغلب عواقب منفی برای سلامتی به ثبت رسیده است. در تعداد روزافزونی از کشورها، این مشکل به یک نگرانی فزاینده در ارتباط با بهداشت عمومی تبدیل شده و موجب تدوین سیاست‌هایی در بخش سلامت برای مقابله با این مشکل شده است. ارتقای سلامت، سیاست‌ها و برنامه‌های پیشگیری و درمان برای کاهش معضلات بهداشت عمومی (از جمله اعتیادهای رفتاری) که به استفاده مفرط مربوط می‌شود در یک نشست ویژه در هنگ کنگ چین مورد بحث قرار گرفت. در این اجلاس که توسط سازمان بهداشت جهانی و با همکاری وزارت بهداشت هنگ کنگ برگزار شد، کارشناسان ۲۰ کشور و مناطق ۵ گانه سازمان بهداشت جهانی شرکت کردند. در سال ۲۰۱۴ نیز نشستی در توکیو و ۲۰۱۵ نشستی در سئول برگزار شد. نتایج این نشست‌ها را به صورت خلاصه به شرح زیر می‌توان بیان کرد:

۱. لزوم به اشتراک گذاری اطلاعات و همکاری‌های فرهنگی متقابل اولویت‌های اصلی آینده برای اطلاع‌رسانی در مورد ابتکارات در سراسر جهان است؛
۲. معبود آزمایش‌های کنترل رندومی و مطالعات طولی در این زمینه وجود دارد؛
۳. لزوم گزارش‌های استاندارد برای تسهیل مقایسه فراملی تحت نظر WHO؛
۴. لزوم شفاف‌سازی این رفتارها و تأثیر اختلالات روانی افراد مبتلا بر بهداشت عمومی جامعه در راستای توسعه برنامه‌های پیشگیری و درمان؛
۵. اهمیت اتخاذ یک رویکرد چندوجهی برای بهبود و ارتقای آموزش در مورد اختلالات برای مربیان، پزشکان و متخصصان بهداشت عمومی^۲.

1. excessive internet use

۲. مطالبی که ذکر شد ترجمه و تلخیص اسنادی است که متن کامل آن‌ها در پیوست الکترونیکی موجود می‌باشد.

گفتار هشت: سازمان جهانی گمرک

تمام گمرک‌های جهان تحت فشار شدیدی برای حرکت به موازات تغییرات هستند. این مهم به طور همزمان در ترخیص کالاها و حفاظت از جامعه در مقابل تجارت غیرقانونی و قاچاق به صورت مؤثری نمود پیدا کرده است. برای مدیریت مؤثر این مسئولیت دوگانه، گمرک به صورت فزاینده‌ای به سیستم‌های شبکه‌های کامپیوتری پیچیده، دارای سرعت بالا و همه‌جاشمول متکی است. از طرف دیگر متاسفانه سهولت استفاده و گمنامی مجرمان در بهره‌برداری از این نوآوری‌های فناورانه زمینه ارتکاب طیف وسیعی از فعالیت‌های مجرمانه را فراهم می‌آورد.

جرایم سایبری^۱ در حال حاضر یکی از سریع‌ترین حوزه‌های رشد را در میان انواع مختلف جرم داراست. جرم سایبری به‌عنوان جرمی تعریف می‌شود که ارتکاب آن از طریق ابزارهایی مثل ذخیره‌های الکترونیکی، سیستم‌های کامپیوتری و شبکه‌ها صورت می‌گیرد.

ادارات گمرک^۲ جهت مقابله با جرایم پیچیده که در فضای سایبر صورت می‌گیرد و چالش‌های زیادی که مخصوصاً در خصوص شناسایی آن‌ها و اختلالاتی ایجاد می‌کنند، باید مجهز باشند. در تأیید این امر سومین کارگاه جرایم سایبری در سال ۲۰۰۰ توصیه نمود که یک گروه کارشناسان خبره جهت بررسی طیف گسترده‌ای از جرایم الکترونیکی تشکیل شود. گروه کارشناسان جرایم الکترونیک^۳ در سال ۲۰۰۱ تشکیل شد و در سال ۲۰۰۲ از سوی سازمان جهانی گمرک مورد تأیید قرار گرفت.

گروه کارشناسان جرایم الکترونیک، منبعی از متخصصان در دسترس^۴ را به سازمان جهانی گمرک^۵ معرفی نمود. متخصصانی که بر جنبه‌های مختلف جرایم الکترونیک متمرکز می‌شوند و توصیه‌های راهبردی و عملیاتی را جهت حمایت از سازمان جهانی گمرک ارائه می‌دهند. این شبکه متخصصان یک بار در سال نشستی را برگزار می‌کنند و اصول راهنمایی را در مورد پیشرفت‌های فنی که مرتبط با ادارات مدرن گمرک و فعالیت‌های عملیاتی آن‌ها می‌شود ارائه می‌دهند. آن‌ها

2. cyber crime

3. Customs administrations

4. The Electronic Crime Expert Group (ECEG)

5. a resource of specialists available to the WCO

6. world customs organization(WCO)

طیف گسترده ای از موضوعات جرم‌یابی کامپیوتری^۱ که پیش شرط تشکیل واحد جرم سایبری است گرفته تا تجزیه و تحلیل نرم‌افزار و محصولات داده‌کاوی را پوشش می‌دهند.^۲

گفتار نه: گروه بانک جهانی

در خصوص امنیت سایبری، ریسک سایبری و تنظیم مقررات و نظارت بر بخش مالی، باید گفت که تهدیدات و تأثیرات ناشی از حملات سایبری بر بخش مالی در حال افزایش است و مسئولان بخش مالی به‌صورت فزاینده ای در صدد مقابله با خطرهای سایبری و ایجاد امنیت سایبری هستند. بانک جهانی یکی از سازمان‌های فعال و گسترده بین‌المللی است که از نظر تشکیلاتی، در زیرمجموعه کمیسیون اقتصادی-اجتماعی سازمان ملل متحد قرار دارد و از جمله سازمان‌های تخصصی این کمیسیون محسوب می‌گردد. بانک جهانی نام دیگر بانک بین‌المللی توسعه و ترمیم^۳ است. همراه با چهار شعبه دیگر خود: مؤسسه بین‌المللی توسعه، مؤسسه مالی بین‌المللی، آژانس تضمین سرمایه‌گذاری چندجانبه‌ای و مرکز بین‌المللی برای حل و فصل منازعات سرمایه‌گذاری، گروه بانک جهانی را تشکیل می‌دهند. بانک جهانی یکی از سه رکن برتون وودز را تشکیل می‌دهد. سازمان صندوق بین‌المللی پول^۴، بانک بین‌المللی ترمیم و توسعه یا بانک جهانی و گات که البته امروزه جای خود را به سازمان تجارت جهانی^۵ داده است، به‌طور جمعی تشکیل‌دهنده سیستم برتون وودز هستند. در پایان جنگ جهانی دوم از طرفی عواقب منفی جنگ جهانی و از طرف دیگر سیاست‌های خودخواهانه تجاری اوایل دهه ۱۹۳۰ منجر به ایجاد مشکلات اقتصادی زیادی برای کشورها شده و توان تولیدی کشورها به‌شدت تقلیل یافته بود. به‌همین دلیل در ۲-۲۱ ژوئیه ۱۹۴۴ (قبل از پایان جنگ)، به پیشنهاد روزولت (رئیس جمهور وقت آمریکا)، کنفرانس پولی و مالی سازمان ملل متحد با شرکت نمایندگان ۴۴ کشور در برتون وودز تشکیل و طی آن موافقت‌نامه‌های تأسیس بانک بین‌المللی ترمیم و توسعه (بانک جهانی) و صندوق بین‌المللی پول تصویب شد. بانک جهانی در دسامبر ۱۹۴۵ تأسیس شد و در

1. computer forensics

۲. مطالبی که ذکر شد ترجمه و تلخیص اسنادی است که متن کامل آن‌ها در پیوست الکترونیکی موجود می‌باشد.

3. IBRD

4. IMF

5. WTO

نوامبر ۱۹۴۷ با تصویب مجمع عمومی سازمان ملل متحد به صورت رسمی در آمد و به جرگه نهادهای تخصصی سازمان ملل متحد پیوست. بانک جهانی ابتدا برای کمک به بازسازی خرابی‌های جنگ جهانی دوم به وجود آمد، ولی در سال ۱۹۴۹، به سمت ارتقای توسعه اقتصادی در کشورهای توسعه‌نیافته معطوف شد. هدف اصلی بانک جهانی اعطای وام برای توسعه و گسترش طرح‌های تولیدی آن دسته از کشورهای در حال توسعه است که عضو بانک هستند. این وام‌ها برای مقاصد ماندگاری پروژه‌های لوله‌کشی آب آشامیدنی، آموزش و پرورش و همچنین اجرای برنامه‌های کلی عمرانی از جمله واردات کالاهای صنعتی است. فقط اعضای صندوق بین‌المللی پول می‌توانند به عضویت بانک جهانی درآیند. از طرف دیگر شرط اولیه عضویت در مؤسسه بین‌المللی توسعه و مؤسسه مالی بین‌المللی، عضویت در بانک جهانی است. در خصوص مخاطرات سایبری مترتب بر فعالیت‌های بانک جهانی باید گفت که بر اساس برآورد گروه بانک جهانی در سال ۲۰۱۶ مشتریان خدمات مالی ۶۵٪ بیش از مشتریان سایر بخش‌ها متحمل حملات سایبری شده‌اند. این رقم در مقایسه سال گذشته افزایش ۲۹٪ را نشان می‌دهد. بهبود و ارتقای هماهنگی بین مسئولان بخش مالی با دیگر آژانس‌های مربوط به مقابله با ریسک سایبری و تأمین امنیت سایبری یک ضرورت است. برای کمک به پیشبرد این مهم، بانک جهانی اقدام به انتشار دو گزارش نموده است:

۱. خلاصه‌ای از مقررات مربوط به تأمین امنیت بخش مالی که شامل مجموعه‌ای از رویه‌های تنظیم مقررات و نظارت اعم از قوانین امنیت سایبری، تنظیم مقررات، اصول راهنما و دیگر اسناد مهم راجع به امنیت سایبری بخش مالی است؛^۱

۲. یادداشتی در مورد مقررات و نظارت بر امنیت بخش مالی؛^۲

برخی کشورها و سازمان‌های پیشرو جهت مقابله با خطرهای سایبری اقدام به تصویب رویه‌های مربوط به تنظیم مقررات و نظارت نموده‌اند. بهترین رویه‌ها در سطح جهان عبارت‌اند از:

1. Financial Sector's Cybersecurity Regulatory Digest, which takes stock of existing regulatory and supervisory practices, including cybersecurity laws, regulations, guidelines and other significant documents on cybersecurity for the financial sector
2. A paper on Financial Sector's Cybersecurity Regulation and Supervision

۱. ایجاد پروتکل های همکاری بین مسئولان بخش مالی با سازمان ها و آژانس های حوزه تنظیم مقررات و نظارت بر خطرهای سایبری در راستای ثبات مالی^۱؛
۲. به اشتراک گذاشتن داوطلبانه اطلاعات از حوادث سایبری بین مشارکت کنندگان در امر دادوستد در بازار^۲؛
۳. تنظیم کنندگان مقررات می توانند خطرها و حوادث را طبقه بندی کنند و به منظور برآورد تأثیرات بالفعل و بالقوه روی تداوم خدمات ضروری جهت تسهیل اشتراک گذاری اطلاعات نیاز به ارائه گزارش های را اجباری نمایند؛
۴. ایجاد یک راهبرد و چارچوب مدیریت خطر. تا بتوانند تصمیمات شغلی لازم را اتخاذ نمایند. این چارچوب شامل طرح های مربوط به واکنش به حوادث با یک زنجیره شفاف فرماندهی است. برخی کشورها نیاز به انتصاب یک افسر امنیت اطلاعات را نیز تجویز می کنند. مؤسسات مالی اقدام به آزمایش های منظم و شبیه سازی ظرفیت های پاسخ به حواث می نمایند.
- در ادامه فعالیت های بانک جهانی باید به برنامه مبارزه با جرایم سایبری اشاره کرد. برنامه ای که به ابتکار بانک جهانی برای کمک به کشورهای در حال توسعه جهت مقابله با جرایم سایبری از طریق مجهز کردن آن ها در راستای پیشبرد سیاست ها، ابعاد قانونی و مجرمانه فناوری اطلاعات و ارتباطات ارائه شده است^۳. بنابراین این برنامه به کشورهای در حال توسعه کمک می نماید تا موانع توسعه تجارت الکترونیک را کاهش دهند. در مرکز این برنامه یک درگاه برخط برای اقتصادهای نوظهور تدارک دیده شده است^۴.

1. Establishing coordination protocols between financial sector authorities...

2. Voluntary and anonymous information-sharing...

3. The World Bank: Combatting Cybercrime - Tools and capacity building to tackle cybercrime. <https://etradeforall.org/development-solution/world-bank-combatting-cybercrime-tools-capacity-building-tackle-cybercrime/>

۴. مطالبی که ذکر شد ترجمه و تلخیص اسنادی است که متن کامل آن ها در بیوست الکترونیکی موجود می باشد.

گفتار ده: سازمان تجارت جهانی

سازمان تجارت جهانی با نام اختصاری WTO سازمانی بین‌المللی و از مؤسسات تخصصی سازمان ملل متحد است.

سازمان تجارت جهانی یا به اصطلاح (WTO)^۱ سازمانی است که برای گسترش تجارت خارجی در سطح بین‌المللی به وجود آمد. ارتقای سطح زندگی، تأمین اشتغال کامل در کشورهای عضو و توسعه تولید و تجارت و بهره‌وری بهینه از منابع جهانی، دستیابی به توسعه پایدار با توجه به بهره‌برداری بهینه از منابع جهانی، حفظ محیط زیست طوری که با سطوح مختلف توسعه اقتصادی جوامع سازگاری داشته باشد و افزایش سهم کشورهای در حال توسعه و کمتر توسعه یافته از رشد تجارت بین‌المللی، جزء هدفهای اصلی سازمان تجارت جهانی است. متناسب با همین اهداف، سازمان تجارت جهانی به مدیریت و تسهیل عملیات اجرایی و توسعه اهداف موافقتنامه سازمان تجارت جهانی و تهیه چارچوب لازم برای اجرای مدیریت موافقتنامه‌های تجاری چندجانبه می‌پردازد.

همچنین وظیفه فراهم کردن امکانات گردهمایی اعضا برای مذاکره و مشورت در زمینه روابط چندجانبه تجاری و اجرا و تدوین مقررات مربوط به روش‌های حل اختلاف میان اعضا را برعهده دارد. سازمان تجارت جهانی همچنین موظف است نظام بررسی و تجدید نظر در سیاست‌های تجاری را برقرار کند، با سازمان‌ها و تشکیلات اقتصادی بین‌المللی همچون صندوق بین‌المللی پول و بانک جهانی همکاری داشته باشد.

راجع به مقوله سایبر در ارتباط با سازمان تجارت جهانی باید گفت که تجارت و امنیت سایبری به صورت روزافزونی به هم تنیده شده‌اند. توسعه جهانی اینترنت و افزایش استفاده از جریان داده‌ها توسط مشاغل و مشتریان (برای ارتباطات، تجارت الکترونیک^۲ و به عنوان منبع اطلاعات و نوآوری) در حال دگرگونی تجارت بین‌المللی است. گسترش هوش مصنوعی و اینترنت اشیاء و رایانش ابری^۳ موجب تسریع به هم پیوستگی و اتصال جهانی دولت‌ها، مشاغل و زنجیره‌های تأمین خواهد شد.

1. WORLD TRADE ORGANIZATION

2. e-commerce

3. artificial intelligence, the "internet of things," (IoT) and cloud computing

با وجود رشد این به‌هم‌تنیدگی، مواجهه ما با خطرهای و حملات سایبری نیز در حال افزایش است. نه تنها اهداف سنتی بلکه اهداف جدید اقتصادی نیز در معرض حملات سایبری قرار دارند. این امر موجب تحلیل رفتن مشاغل و اعتماد مشتریان در اینترنت به‌عنوان پایه‌ای برای تجارت می‌شود. بسیاری از کشورها اقدامات و سیاست‌گذاری‌هایی برای پاسخ به این تهدیدات تدوین کرده‌اند. بر اساس برآوردها حدود ۵۰٪ کشورها سیاستگذاری‌ها و مقررات حوزه امنیت سایبری را تدوین کرده‌اند.^۱

بسیاری از این کشورها نیاز به همکاری بین‌المللی در این زمینه را به رسمیت شناخته‌اند. اتحادیه اروپا نیاز به همکاری نزدیک‌تر در سطح جهانی برای ارتقای استانداردهای امنیتی، بهبود اطلاعات و فراهم کردن یک رویکرد مشترک جهانی برای موضوعات مرتبط با امنیت شبکه و اطلاعات را به رسمیت می‌شناسد.

سیاستگذاری‌های امنیت سایبری به‌صورت فزاینده‌ای مبتنی بر ریسک است. نیاز دولت‌ها، سازمان‌ها و مشاغل برای ارزیابی خطر حمله، تعیین خسارت بالقوه و اتخاذ اقدامات مقتضی برای کاهش خطرهای یا آثار آن هر روز بیشتر می‌شود. برخی اقدامات پیشنهادی احتمالاً ایجاد برخی موانع در مقابل جریان داده و تجارت دیجیتال است. این امر می‌تواند شامل محدودیت‌های مربوط به جریان داده، الزامات مربوط به جانمایی داده و ایجاد محدودیت‌های وارداتی برای محصولات فناوری اطلاعات است، از جمله واردات نرم‌افزارها از کشورهای یا زنجیره تأمین در جایی که میزان خطر بالاست. کشورها همچنین می‌توانند به‌عنوان ابزار مجازات و ممانعت از حملات سایبری به محدودیت‌های وارداتی از جمله اعمال تعرفه‌های بالاتر متوسل شوند. این نحوه تعامل با کالاها، خدمات و داده‌های مربوط به کشورها پرخطر سایبری در مقایسه با کشورهای کم‌خطر سایبری که تحت عنوان اقدامات امنیت‌ساز سایبری صورت می‌گیرد می‌تواند تعهدات مربوط به سازمان تجارت جهانی و موافقت‌نامه تجارت آزاد را به‌صورت جدی نقض نماید. نیاز روزافزون به امنیت سایبری موجب ایجاد چالش برای سیستم‌های تجاری مبتنی بر قانون شده است. چالش این است که هر چه اقتصاد دیجیتالی‌تر و به‌هم پیوسته‌تر باشد احتمال افزایش توسل

^۱. ITU Global Cybersecurity Index 2017.

به محدودیت‌های تجاری برای اهداف مشروع مربوط به امنیت سایبری بیشتر خواهد شد. استثنائات امنیتی مربوط به سازمان تجارت جهانی به منظور مقابله با اقدامات امنیتی سنتی طراحی شده‌اند و بنابراین مناسب برای اتخاذ اقدامات تأمینی برای مقابله با حملات و خطرهای سایبری نیستند. گزینه دیگر برای توسل به استثنائات امنیتی، توجیه مقررات مربوط به امنیت سایبری تحت استثنائات عمومی سازمان تجارت جهانی و موافقتنامه تجارت آزاد است. نتیجه‌ای که حاصل می‌شود این است که درک دقیق‌تری از انواع خطرهای مترتب بر امنیت سایبری مورد نیاز است. باید ایجاد مجموعه جدیدی از قوانین خاص تجارت در امنیت سایبری مورد توجه قرار گیرد.^۱

گفتاریاز ده: سازمان جهانی هواشناسی

کیفیت کار علمی، تحقیقاتی و خدماتی که از سلامتی و ایمنی انسانها پشتیبانی می‌کند به تبادل اطلاعات هواشناسی و داده‌های محیطی^۲ و مباحثی بستگی دارد که در جامعه سازمان هواشناسی^۳ اتفاق می‌افتد.^۴

وجود ارتباطات برای حصول به اهداف شغلی، امری ضروری است و اینترنت یکی از ابزارهای ضروری برای تبادل اطلاعات است.

ابزارهای الکترونیک برای انتقال فایل‌ها، از جمله نامه الکترونیکی، شبکه جهانی وب و شبکه‌های اجتماعی امکان توسعه همزیستی بین دانشمندان و حوزه‌های پیشرفت در پیش‌بینی و توزیع دقیق محصولات هواشناسی را فراهم آورده است. هر چند به موازات این تغییرات مثبت در نحوه عملکرد جامعه سازمان جهانی هواشناسی، میزان روزافزونی از تهدیدات در سراسر اینترنت رایج بوده است. این امر برای سازمان‌ها اجتناب‌ناپذیر می‌باشد که با خطرهای مواجه شده و از سیستم‌های امنیتی خود جهت حفظ پردازش عملیاتی داده‌ها و ارتباطات حفاظت کنند. اینترنت شبکه‌ای از شبکه‌هاست. این شبکه، خدماتی مانند شبکه جهانی وب ارائه می‌دهد که امکان مرور اطلاعات موجود در سرورهای جهان، تبادل ایمیل، فایل و موارد دیگر را فراهم می‌آورد.

۱. مطالبی که ذکر شد ترجمه و تلخیص اسنادی است که متن کامل آن‌ها در پیوست الکترونیکی موجود می‌باشد.

2. exchange of meteorological and environmental data

3. World Meteorological Organization (WMO)

4. Guide to Information Technology Security: WMO-No. 1115

باتوجه به حضور و استفاده گسترده، متأسفانه اینترنت در حال تبدیل شدن به یک رسانه انتخابی برای انتشار ناخواسته اطلاعات و انجام حملات الکترونیکی علیه سازمان‌ها و دارایی‌های اطلاعاتی آن‌هاست. این مسئله بسیار گسترده و غیر قابل اجتناب شده است. به‌عنوان مثال فقط چند دقیقه طول می‌کشد که یک سیستم کامپیوتری تازه خریداری شده، اگر اقدامات امنیتی انجام نشود، بعد از اتصال به اینترنت به اشکال متنوعی از ویروس‌های کامپیوتری آلوده شود.^۱

مبحث دوم شورای امنیت

گفتار یک: شورای امنیت و فضای سایبر

پیرو ماده ۲۹ منشور ملل متحد، شورای امنیت سازمان ملل مبتنی بر نیاز خود جهت انجام وظایفش، دامنه وسیعی از نهادهای فرعی را تأسیس نمود.^۲ این نهادهای فرعی تحت مسئولیت مستقیم^۳ شورای امنیت و از اعضای این شورا تشکیل شده‌اند. نهادهایی مانند: کمیته‌های تحریم‌ها^۴، گروه‌های کاری و سایر کمیته‌هایی که تلاش می‌نمایند تا هنجارهای بین‌المللی در زمینه‌های {مختلف مانند} مقابله با تروریسم، پیشگیری از اشاعه سلاح‌های کشتار جمعی و حفاظت از کودکان در مخاصمات مسلحانه را ارتقای بخشند. کمیته ضد تروریسم^۵ تحت قطعنامه ۱۳۷۳ مورخ ۲۸ سپتامبر ۲۰۰۱ و با دستور کار مقابله با تروریسم تأسیس گردید و به‌منظور پیشگیری از افعال تروریستی که انجام آن‌ها در قطعنامه‌های {شورای امنیت} به شماره‌های ۱۳۷۳ و ۱۶۲۴ مورخ ۱۴ سپتامبر ۲۰۰۵ منع گردیده اند، این کمیته، متعهد به انجام اقدامات {لازم} از سوی کشورهای عضو می‌باشد. بدین صورت که در فاصله کوتاهی بعد از حادثه ۱۱ سپتامبر ۲۰۰۱، شورای امنیت در قطعنامه ۱۳۷۳، از کشورهای عضو درخواست نمود تا برخی از اقدامات مورد انتظار را به‌منظور ارتقای توانمندی قانونی و سازمانی {نهادی}^۶ خود در فعالیت‌های {مرتبط با} مقابله با تروریسم اجرا نماید، از جمله:

۱. مطالبی که ذکر شد ترجمه و تلخیص اسنادی است که متن کامل آن‌ها در پیوست الکترونیکی موجود می‌باشد.
۲. ماده ۲۹: شورای امنیت می‌تواند آنگونه ارکان فرعی را که برای انجام وظایف خود لازم بداند تأسیس نماید.

3. direct authority

4. sanctions committees

5. Counter-Terrorism Committee(CTC)

6. legal and institutional ability

- اتخاذ گام‌هایی جهت جرم‌انگاری تأمین مالی تروریسم؛
 - بلوکه کردن بی‌درنگ هرگونه سرمایه متعلق به افرادی که درگیر اقدامات تروریستی می‌باشند؛
 - اجتناب از تمامی اشکال حمایت مالی از گروه‌های تروریستی؛
 - ممانعت از تأمین پناهگاه و محل امن، معاش یا پشتیبانی از تروریستها؛
 - ممانعت از به اشتراک‌گذاری اطلاعات با سایر حکومت‌ها یا گروه‌هایی که اقدامات تروریستی را برنامه ریزی می‌نمایند یا خود مرتکب اقدامات تروریستی می‌شوند؛
 - همکاری با سایر حکومت‌ها در خصوص تحقیق، ردیابی، توقیف، استرداد مجرمان و پیگرد قانونی کسانی که درگیر چنین اقداماتی می‌باشند؛
 - جرم‌انگاری مساعدت‌های فعال و انفعالی به تروریسم در حقوق داخلی و سپردن ناقضان به عدالت^۴.
- همچنین در این قطعنامه شورای امنیت از تمامی دولت‌ها درخواست می‌کند که در جستجوی راه‌هایی جهت تقویت و شتاب در تبادل اطلاعات عملیاتی در خصوص استفاده از فناوری‌های اطلاعات و ارتباطات توسط گروه‌های تروریستی و محدود نمودن استخدام افراد توسط تروریست‌ها باشند و در قطعنامه ۱۶۲۴، مربوط به تحریک به ارتکاب اقدامات تروریستی^۵، از دولت‌ها درخواست می‌نماید تا از طریق قانون: ۱. ارتکاب به این اقدامات را ممنوع کنند، ۲. از انجام چنین اقداماتی جلوگیری نمایند و ۳. از تأمین محل امن برای هر یک از مقصران چنین تحریکاتی امتناع ورزند.^۶
- همچنین این قطعنامه اهمیت اقدامات همکاری‌جویانه توسط کشورهای عضو به منظور ممانعت از بهره‌مندی تروریستها از فناوری سطح بالا، ارتباطات و منابع پشتیبانی‌کننده از اقدامات مجرمانه را به رسمیت می‌شناسد. در قطعنامه شورای امنیت به شماره ۲۱۷۸ مورخ ۲۴ سپتامبر ۲۰۱۴، { این شورا } افزایش خطرهای ناشی از جنگ طلبان تروریست خارجی^۷ را به‌عنوان یک موضوع نوظهور شناسایی نمود. موضوعی که مورد توجه خاص کمیته ضد تروریسم می‌باشد.
- شورای امنیت در این قطعنامه از این کمیته می‌خواهد تا با حمایت مدیریت اجرایی کمیته

1. criminalize the financing of terrorism
2. freeze without delay any funds related to persons involved in acts of terrorism
3. share information with other governments on any groups practising or planning terrorist acts
4. criminalize active and passive assistance for terrorism in domestic law and bring violators to justice.
5. incitement to commit acts of terrorism
6. Resolution 1624 (2005), relating to incitement to...
7. Foreign terrorist fighters (FTFs)

مقابله با تروریسم^۱ متعهد به انجام اقدامات زیر گردند:

۱. شناسایی شکاف‌های اصلی و عمده در ظرفیت دولت‌های عضو جهت اجرای قطعنامه‌های ۱۳۷۳ و ۱۶۲۴ که {این شکاف‌ها} مانع توانایی دولت‌ها در قطع جریان جنگ طلبان تروریست خارجی می‌شود^۲؛

۲. شناسایی رویه‌های برتر جهت قطع جریان جنگ طلبان تروریست خارجی با اجرای قطعنامه‌های ۱۳۷۳ و ۱۶۲۴؛

۳. تسهیل مساعدت‌های فنی.

ضمن مدیریت اجرایی کمیته ضد تروریسم زیر قطعنامه ۱۵۳۵ مورخ ۲۰۰۴ جهت اجرای موارد زیر تأسیس گردید: ۱. تصمیم‌گیری‌های سیاسی کمیته مقابله با تروریسم، ۲. اجرای ارزیابی‌های کارشناسی هر یک از دولت‌های عضو و ۳. تسهیل مساعدت‌های فنی جهت مقابله با تروریسم برای کشورها. قطعنامه ۲۳۹۵ شورای امنیت مورخ ۲۰۱۷ دستور کار این ساختار را تا ۳۱ دسامبر ۲۰۲۱ تجدید نمود.

در ماه می سال ۲۰۱۶، در یک نشست {جلسه} توجیهی باز شورای امنیت به ریاست وزیر امور خارجه مصر، درباره تهدیدات صلح و امنیت بین‌المللی ناشی از اقدامات تروریستی، شورا یک بیانیه رئیس^۳ را به تصویب رسانید^۴ و در آن از کمیته ضد تروریسم درخواست نمود تا یک طرح پیشنهادی را تا ۳۰ آوریل ۲۰۱۷ با موضوع و هدف زیر به شورا ارائه نماید: «چارچوب بین‌المللی جامع^۵» برای مقابله اثربخش و سازگار با حقوق بین‌الملل، راه‌هایی که گروه تروریستی داعش، القاعده و اشخاص و نهادهای وابسته {به آنها} برای تشویق، تحریک و استخدام دیگران جهت ارتکاب به اقدامات تروریستی استفاده نمودند.

گفتار دو: عملکرد کمیته ضد تروریسم در مباحث فناوری اطلاعات و ارتباطات

تروریست و گروه‌های تروریستی از اینترنت و شبکه‌های اجتماعی نه تنها به منظور ارتکاب

1. Counter-Terrorism Committee Executive Directorate (CTED)

2. identify principal gaps in Member States' capacities to implement resolutions 1373 (2001) and 1624 (2005) which may hinder States' abilities to stem the flow of foreign terrorist fighters

3. presidential statement

4. S/PRST/2016/6

5. "comprehensive international framework"

اقدامات تروریستی استفاده می‌کنند بلکه از آن‌ها برای تسهیل دامنه وسیعی از فعالیت‌های تروریستی خود بهره‌مند می‌شوند. از جمله تحریک^۱ {افکار عمومی} و افراطی‌گری^۲، استخدام^۳، آموزش، برنامه‌ریزی، جمع‌آوری اطلاعات، ارتباطات، آماده‌سازی و تأمین وجوه نیز از اینترنت و شبکه‌های اجتماعی. به جهت سوءاستفاده از فناوری‌های اطلاعات و ارتباطات توسط تروریست‌های و گروه‌های تروریستی، کمیته ضدتروریسم شورای امنیت سازمان ملل توسط چندین قطعنامه از طرف این شورا هدایت شده است.

عملکرد مربوط به مدیریت اجرایی کمیته ضدتروریسم روی چهار رکن متمرکز می‌باشد:

۱- جریان شناسی فناوری اطلاعات و ارتباطات در {طول} ارزیابی خود از اجرای قطعنامه‌های ۱۳۷۳، ۱۶۲۴ و ۲۱۷۸ توسط کشورهای عضو^۴؛

۲- ارتقای خودتنظیمی بخش صنعت^۵؛

۳- تقویت مساعدت حقوقی متقابل در رابطه با محتوای دیجیتال^۶؛

۴- تقویت فناوری‌های مقابله با انتقال پیام از جمله به شکل برخط^۷.

مدیریت اجرایی کمیته ضدتروریسم {علاوه بر} جریان‌سازی فناوری اطلاعات و ارتباطات به طور برجسته روی موضوعات زیر در فعالیت‌های جاری و آتی خود ادامه می‌دهد: تأمین مالی تروریسم، سپردن تروریست‌ها به محکمه عدالت^۸، همکاری ملی و بین‌المللی، حفاظت از زیرساخت‌های حیاتی، مساعدت جهت پایش اجرای قطعنامه‌های مربوط به شورای امنیت. در سال ۲۰۱۳، شورای امنیت سازمان ملل متحد در قطعنامه خود به شماره ۲۱۲۹ به مدیریت اجرایی کمیته ضدتروریسم دستور داد تا:

- ضمن مشورت با دولت‌های عضو، سازمان‌های بین‌المللی، منطقه‌ای و فرو منطقه‌ای، بخش خصوصی، جامعه مدنی به مقابله با استفاده از فناوری اطلاعات و ارتباطات در فعالیت‌های تروریستی ادامه دهد؛

1. incitement

2. radicalization

3. recruitment

4. mainstreaming ICT in its assessment of Member States' implementation of resolutions 1373 (2001), 1624 (2005), and 2178 (2014);

5. the promotion of industry self-regulation

6. strengthening mutual legal assistance regarding digital content

7. promoting counter-messaging techniques, including online

8. bringing terrorists to justice

- در خصوص رویکردهای آتی این کمیته مشورت‌هایی را ارائه نماید.^۱

در سال ۲۰۱۴، شورای امنیت در قطعنامه خود به شماره ۲۱۷۸ درباره جنگ‌طلبان تروریست خارجی، از دولت‌های عضو درخواست می‌نماید تا به شکل همکاری‌جویانه‌ای اقدامات ملی را جهت ممانعت از بهره‌مندی تروریست‌ها از فناوری، ارتباطات و منابع پشتیبانی‌کننده برای برانگیختن اقدامات تروریستی، اتخاذ نمایند.^۲ در ادامه کمیته، دو نشست ویژه را درباره موضوعات زیر ساماندهی نمود:

- نشست دسامبر ۲۰۱۵ با عنوان «ممانعت از بهره‌مندی تروریست‌ها از اینترنت و شبکه‌های اجتماعی جهت استخدام تروریست‌ها و تحریک به اقدام تروریستی ضمن احترام به حقوق بشر و آزادی‌های اساسی»^۳؛

- نشست دسامبر ۲۰۱۶ با عنوان «ممانعت از بهره‌برداری از فناوری اطلاعات و ارتباطات جهت اهداف تروریستی، ضمن احترام به حقوق بشر و آزادی‌های اساسی»^۴.

مدیریت اجرایی کمیته ضدتروریسم جهت درک بیشتر از پاسخ‌ها {واکنش‌های} صنعتی به استفاده از فناوری جدید برای اهداف تروریستی^۵ و شناسایی رویه‌های برتر، مشغول به پیشبرد {طرح} ابتکاری گردید و بر مبنای آن پروژه مشترکی را همراه با بنیاد سوئیسی فناوری اطلاعات و ارتباطات برای صلح^۶ انجام داد.

از سال ۲۰۱۴، مدیریت اجرایی کمیته ضدتروریسم به‌طور فعالانه تعاملات خود با بخش خصوصی را در حوزه فناوری اطلاعات و ارتباطات آغاز نموده است. در سال ۲۰۱۶ این همکاری در قالب مشارکت بخش‌های خصوصی - دولتی قاعده‌مند گردید که اکنون تحت عنوان فناوری علیه تروریسم^۷ نامیده می‌شود. گزارش اولیه این پروژه در نشست ویژه کمیته ضدتروریسم در دسامبر ۲۰۱۶،

1. Security Council resolution 2129 (2013) directs the Counter-Terrorism Committee Executive Directorate (CTED) to continue to address the use of ICT in terrorist activities, in consultation with Member States, international, regional, and subregional organizations, the private sector, and civil society, and to advise the Committee on further approaches.

2. Security Council resolution 2178 (2014), on foreign terrorist fighters, calls on Member States to act cooperatively when taking national measures to prevent terrorists from exploiting technology, communications, and resources to incite support for terrorist acts. In doing so, States should respect human rights and fundamental freedoms and ensure compliance with their obligations under international law.

3. "Preventing terrorists from exploiting the Internet and social media to recruit terrorists and incite terrorist acts, while respecting human rights and fundamental freedoms"

4. "Preventing the exploitation of ICT for terrorist purposes, while respecting human rights and fundamental freedoms."

5. understanding of industry responses to the use of new technology for terrorist purposes

6. ICT for Peace

7. Tech Against Terrorism

ارائه گردید. گزارشی با موضوع «پروژه مشترک درباره تعامل بخش خصوصی در پاسخ به استفاده از اینترنت و فناوری اطلاعات و ارتباطات برای اهداف تروریستی: تقویت گفتگو و اعتمادسازی»^۱ در این طرح ابتکاری که شرکای متعددی از بخش‌های دولتی و خصوصی، مؤسسات تجاری، جامعه مدنی، دانشگاهی و مجامع چندذی‌نفعی در آن درگیرند، هدف اصلی، پشتیبانی از صنعت فناوری جهانی^۲ جهت ممانعت از بهره‌برداری تروریست‌ها از این فناوری‌ها می‌باشد. فناوری علیه تروریسم در همکاری نزدیک با مجمع جهانی اینترنت برای مقابله با تروریسم^۳ می‌باشد که این مجمع توسط شرکت‌های آمریکایی فیس‌بوک، گوگل، مایکروسافت و توییتر در سال ۲۰۱۷ تأمین مالی شد. شورای امنیت در قطعنامه خود به شماره‌های ۲۳۹۵ و ۲۳۹۶ مورخ ۲۰۱۷، ضمن توجه به مجمع جهانی اینترنت برای مقابله با تروریسم، از این مجمع درخواست نمود تا تعامل خود را با شرکت‌های دولتی و فناوری در سطح دنیا افزایش دهد. این دو قطعنامه موارد زیر را رسمیت شناخت: توسعه فناوری علیه تروریسم و تلاش‌های جهت تقویت همکاری با نمایندگان صنعت فناوری به‌منظور اخلال در قابلیت تروریست‌ها در استفاده از اینترنت برای اهداف تروریستی. همچنین قطعنامه ۲۳۹۵، ضمن احترام به حقوق بشر و آزادی‌های اساسی، عملکرد مدیریت اجرایی کمیته ضد تروریسم در مقابله با استفاده از اینترنت و رسانه‌های اجتماعی برای اهداف تروریستی را به رسمیت می‌شناسد این قطعنامه همچنین به ضرورت پایبندی دولت‌ها به تعهداتشان تحت حقوق بین‌الملل و نیاز به حفظ اتصالات جهانی و جریان آزاد و ایمن اطلاعات نیز توجه می‌نماید. این قطعنامه بر اهمیت همکاری با جامعه مدنی و بخش خصوصی در این تلاش‌ها تأکید می‌نماید.

طرح ابتکاری دیگری که مدیریت اجرایی کمیته ضد تروریسم همراه با مجمع دادستان‌های بین‌المللی^۴ و دفتر مقابله با مواد مخدر و جرم ملل متحد انجام داد روی تقویت همکاری بین‌المللی میان دادستان‌های ملی^۵ که با موضوعات مقابله با تروریسم درگیر می‌باشند متمرکز می‌باشد. به طور برجسته، هدف این همکاری ارتقای ظرفیت دادستانها در احراز ادله بموقع می‌باشد.

1. a joint project on "Private Sector Engagement in Responding to the Use of the Internet and ICT for Terrorist Purposes: Strengthening Dialogue and Building Trust."

2. global tech industry

3. Global Internet Forum to Counter Terrorism (GIFCT),

4. International Association of Prosecutors (IAP)

5. national prosecutors

بخش حیاتی از تلاش‌های مقابله با تروریسم، ارتقای واکنش‌های مؤثر در قبال عدالت کیفری مبتنی بر حاکمیت قانون^۱ می‌باشد. در عمل، دولت‌های عضو با چالش‌های مهم و جدی در تلاش‌های خود جهت احراز ادله قابل قبول که بتواند جهت کمک به تعقیب قانونی و مجازات تروریست‌ها^۲ استفاده شود روبه‌رو می‌باشد. وضعیت جنگ‌طلبان تروریست خارجی که به داخل کشوری سفر می‌کنند یا از آن خارج می‌شوند جزء چالش‌های حاد می‌باشد. به دلیل اینکه اطلاعات مرتبط با فعالیت‌های این افراد اغلب در میدان نبرد قرار دارد و این امر سبب می‌شود که اطلاعات قابل دسترس برای محققان و دادستان‌های غیرنظامی فراهم نباشد. بنابراین پیگیری قانونی این افراد ممکن است وابسته به استفاده از شواهد دیجیتال یا مبتنی بر اینترنت باشد و ممکن است نیاز به آشکالی از همکاری‌های قضایی داشته باشد.

برای پرداختن به این چالش‌ها، مدیریت اجرایی کمیته ضدتروریسم همراه با مؤسسه بین‌المللی دادستان‌ها و دفتر مقابله با مواد مخدر و جرم سازمان مللی در سپتامبر ۲۰۱۸ یک راهنمای عملیاتی را تهیه نمود که در آن موارد زیر لحاظ شده است:

- درخواست شواهد و ادله الکترونیکی در مرزهای داخلی^۳؛

- نحوه پاسخ به درخواست مندرج در قطعنامه‌های شورای امنیت به شماره‌های ۲۳۲۲ و ۲۳۳۱ مورخ ۲۰۱۶ و ۲۳۴۱ مورخ ۲۰۱۷ مبنی بر اینکه از دولت‌های عضو درخواست می‌کند تا ادله را برای اهداف تحقیقاتی و پیگرد قانونی جمع‌آوری و حفظ نماید تا توسط این ادله بتوان تروریست‌ها را {مسئول پاسخگویی به حملات تروریستی نمود.

گفتار سه: فرمول آریا

شورای امنیت سازمان ملل در سال ۲۰۱۷ قطعنامه‌ای به شماره ۲۳۴۱ در خصوص حفاظت از زیرساخت‌های حیاتی در برابر حملات تروریستی مصوب نمود که در آن امنیت سایبری به‌عنوان یک عنصر مهم جهت حفاظت به رسمیت شناخته شد. این شورا برای نخستین بار در سال ۲۰۱۶

1. promotion of effective rule of law-based criminal justice responses
2. convictions of terrorist
3. across borders

در نشست تحت عنوان «فرمول آریا»^۱ درباره استفاده از فناوری‌های اطلاعات و ارتباطات و امنیت بین‌المللی توضیح داد.^۲ این نشست، در واقع یک گردهمایی غیررسمی است که اعضای شورای امنیت را قادر می‌سازد تا در یک چارچوب شکلی منعطف، با دعوت شدگان تبادل نظر خصوصی و بی‌پرده داشته باشند.

نشست اول که در سال ۲۰۱۶ با مشارکت نمایندگان دولتی، سازمان‌های منطقه‌ای، بخش خصوصی، جامعه مدنی برگزار شد، ملاحظه و رسیدگی به ظرفیت دولت‌ها در استفاده از فناوری‌های اطلاعات و ارتباطات در تقویت تنش‌های سیاسی و نظامی و اهمیت حفاظت زیرساخت‌های حیاتی وابسته به فناوری اطلاعات و ارتباطات را دنبال نمود. دومین نشست در آوریل ۲۰۱۷ با موضوع جنگ‌های هیبریدی به‌عنوان تهدید صلح و امنیت بین‌المللی^۳ برگزار گردید و روی تغییر ماهیت جنگ که به واسطه افزایش استفاده از فناوری‌ها و راهبردهای جدید راه‌اندازی می‌شود متمرکز شد و در این رابطه به فناوری‌های سایبری، مداخله در فرایندهای سیاسی، انتشار سیستماتیک تبلیغات در داخل و محیط بین‌المللی، از جمله ابزاری‌های مربوط به دستیابی به اهداف سیاسی اشاره نمود.^۴

مبحث سوم: دبیرخانه

گفتار یک: گزارش کلی از عملکرد دبیرکل سازمان ملل متحد در مورد فضای سایبری

بند یک: گزارش سالانه دبیرکل

دبیرکل سازمان ملل متحد^۵ از سال ۱۹۹۸، گزارش‌های سالانه خود را درباره نظرهای دولت‌های عضو در موضوعات مرتبط با «تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌الملل»^۶ به مجمع عمومی سازمان ملل متحد ارائه می‌نماید. در سال ۲۰۱۹، نیز مطابق سنوات پیشین، و مطابق بند ۴ قطعنامه پیشنهادی روسیه^۷ به شماره ۷۳/۲۷ و بند ۲ قطعنامه ۷۳/۲۶۶

1. Arria formula

۲. مترجم: اجلاس‌های «فرمول آریا» که نام خود را از دیگو آریا دیپلمات ونزوئلایی گرفته است، یکی از روش‌هایی است که اعضای شورای امنیت سازمان ملل متحد در سال‌های اخیر به آن توسل می‌جویند.

3. "hybrid wars as a threat to international peace and security"

4. What's in Blue, "Arria-formula Meeting on Hybrid Wars", 30 March 2017,

<http://www.whatsinblue.org/2017/03/arriaformula-meeting-on-hybrid-wars.php>.

5. Secretary-General

۶. عنوان قطعنامه روسیه که از سال ۱۹۹۸ تا کنون هر سال به کمیته اول مجمع عمومی ارائه می‌شود.

۷. شماره همان قطعنامه

که^۱ در سال ۲۰۱۸ توسط مجمع عمومی به تصویب رسید، دبیرکل از دولت‌ها دعوت نمود تا نظرهای ملی خود را در خصوص موضوعات مندرج در این دو بند ارائه دهند؛ تجمیع این نقطه‌نظرها در گزارش مورخ ۲۴ ژوئن ۲۰۱۹ دبیرکل ارائه گردید.^۲ بنابراین، می‌توان گفت که تقریباً دبیرکل هر ساله از تمامی دولت‌های عضو دعوت می‌نماید تا نظرهای خود را در خصوص موضوعات کلی زیر بیان نمایند:

- ✓ فهم عمومی از موضوعات امنیت اطلاعات؛
- ✓ تلاش‌های صورت گرفته در سطوح ملی جهت تقویت امنیت اطلاعات و ارتقای همکاری‌های بین‌المللی در این حوزه؛
- ✓ محتوای مفاهیم و طرح‌های مذکور در گزارش‌های گروه کارشناسان دولتی؛
- ✓ اقدامات ممکن که می‌تواند جهت تقویت امنیت اطلاعات در سطح جهانی توسط جامعه بین‌المللی اتخاذ گردد

جدول زیر مشخصات گزارش‌های سالانه دبیرکل در باب نظرهای کشورها در موضوعات مطرح در زمینه تحولات حوزه اطلاعات و ارتباطات در چارچوب امنیت بین‌الملل را بیان می‌نماید:

جدول ۱۲: مشخصات گزارش‌های سالانه دبیرکل درباره نظر کشورها در زمینه تحولات اطلاعات و ارتباطات

شماره گزارش	تاریخ انتشار	درخواست نظرها بر اساس قطعنامه شماره	کشورهایی که نظرهای خود را ارائه نموده اند
A/71/3/54	۱۰ اگوست ۱۹۹۹	۵۴/۸۰ مصوب سال ۱۹۹۸	استرالیا، بلاروس، برونئی دارالسلام، کوئاب، قطر، روسیه، عربستان سعودی، انگلستان، ایالات متحده آمریکا
A/74/55	۱۰ جولای ۲۰۰۰	۵۴/۸۹ مصوب سال ۱۹۹۹	اردن، قطر، روسیه
A/74/56	۳ جولای ۲۰۰۱	۵۵/۸۸ مصوب سال ۲۰۰۰	بولیوی، مکزیک، فیلیپین، سوئد
A/76/57	۲ جولای ۲۰۰۲	۵۶/۸۹ مصوب سال ۲۰۰۱	گواتمالا
A/77/58	۱۷ سپتامبر ۲۰۰۲	۵۷/۵۲ مصوب سال ۲۰۰۲	بولیوی، کوئاب، السالوادور، گرجستان، روسیه، سنگال، اکراین
A/79/59	۲۳ ژوئن ۲۰۰۴	۵۸/۸۲ مصوب سال ۲۰۰۲	آرژانتین، چین، کاستاریکا، کوئاب، گرجستان، لبنان، انگلستان
A/95/60	۵ جولای ۲۰۰۵	۵۹/۸۱ مصوب سال ۲۰۰۴	شیلی، مکزیک
A/76/61	۱۸ جولای ۲۰۰۶	۶۰/۵۵ مصوب سال ۲۰۰۵	بولیوی، چین، اردن، لبنان، قطر، امارات متحده عربی
A/98/62	۲ جولای ۲۰۰۷	۶۱/۵۶ مصوب سال ۲۰۰۶	برونئی دارالسلام، بوزنیوئینا، کوبا، چین، کوئاب، لبنان، مکزیک
A/139/63	۱۸ جولای ۲۰۰۸	۶۲/۸۷ مصوب سال ۲۰۰۷	چین، کوئاب، اردن، لبنان، نیجریه، قطر
A/149/64	۸ جولای ۲۰۰۹	۶۳/۸۷ مصوب سال ۲۰۰۸	برزیل، قزاقستان، لبنان، لیتوانی، مکزیک، سرستان، تاجیکستان، ناپلند، اکراین
A/154/65	۲۰ جولای ۲۰۱۰	۶۴/۸۵ مصوب سال ۲۰۰۹	کوئاب، یونان، مکزیک، پاناما، قطر، اکراین، انگلیس
A/154/66	۱۵ جولای ۲۰۱۱	۶۵/۸۶ مصوب سال ۲۰۱۰	
A/167/67	۲۳ جولای ۲۰۱۲	۶۶/۸۶ مصوب سال ۲۰۱۱	گنمبیا، کوئاب، پاناما، قطر، ترکیه، اکراین
A/156/68	۱۱ جولای ۲۰۱۳	۶۷/۲۷ مصوب سال ۲۰۱۲	کوئاب، اسپانیا، اکراین، انگلستان

۱. قطعنامه پیشنهادی ایالات متحده آمریکا با عنوان "پیشرفت رفتار مسئولانه دولت درباره فضای سایبر در چارچوب امنیت بین‌الملل"

شماره گزارش	تاریخ انتشار	درخواست نظرها بر اساس قطعنامه شماره	کشورهایی که نظرهای خود را ارائه نموده اند
A/۱۱۲/۶۹	۳۰ ژوئن ۲۰۱۴	۶۸/۲۴۲ مصوب سال ۲۰۱۳	استرالیا، اتریش، کلمبیا، کوپا، السالوادور، گرجستان، آلمان، پرتغال، صربستان، سوئیس، انگلیستان
A/۱۷۲/۷۰	۲۲ جولای ۲۰۱۵	۶۹/۲۸ مصوب سال ۲۰۱۴	کانادا، کوپا، السالوادور، گرجستان، آلمان، هلند، پاناما، پرو، پرتغال، قطر، کره جنوبی، اسپانیا، انگلیس
A/۱۷۲/۷۱	۱۹ اگوست ۲۰۱۶	۷۰/۳۳۷ مصوب سال ۲۰۱۵	آلبانی، استرالیا، کانادا، کلمبیا، کوپا، السالوادور، فنلاند، هند، ژاپن، اردن، آلمان، لهستان، پرتغال، صربستان، اسپانیا، سوئیس، توگو، ترکمنستان، انگلیس
A/۳۱۵/۷۲	۱۱ اگوست ۲۰۱۷	۷۱/۲۸ مصوب سال ۲۰۱۶	افغانستان، ازمنستان، بلاروس، برونی دارالسلام، کانادا، کوپا، اکوادور، السالوادور، استونی، فنلاند، آلمان، یونان، ژاپن، اردن، ماداگاسکار، هلند، نروژ، پاراگوئه، پرتغال، قطر، سنگاپور، ترکیه، انگلیس
A/۱۲۰/۷۴	۲۴ ژوئن ۲۰۱۹	۷۳/۲۷ و ۷۳/۲۶۶ مصوب سال ۲۰۱۸	آرژانتین، کلمبیا، کوپا، مصر، فرانسه، یونان، ژاپن، سنگاپور، ترکیه

بند دو: یادداشت دبیرکل

دبیرکل سازمان ملل بعد از برگزاری هر یک از اجلاس گروه کارشناسان دولتی درباره تحولات در زمینه اطلاعات و ارتباطات راه دور در چارچوب امنیت بین‌الملل، یادداشتی را منتشر می‌نماید. در این یادداشت‌ها ابتدا چکیده ای از گزارش، سپس پیشگفتار دبیرکل و در نهایت گزارش گروه کارشناسان دولتی قید می‌گردد.^۱

بند سه: دستور کار دبیرکل برای خلع سلاح

در گذشته برخی از دولت عضو از امکان سوءاستفاده از {زیرساخت‌های} آن‌ها در یک مخاصمه سایبری ابراز نگرانی کردند. در سال ۲۰۱۸، دبیرکل {وقت} سازمان ملل متحد، آقای آنتونیو گوترش^۲، نگرانی خود را درباره استفاده سوء از فناوری‌های اطلاعات و ارتباطات بیان نمود و ارتقای زیست‌بوم فناوری اطلاعات و ارتباطات صلح‌آمیز را به‌عنوان اولویت‌های اصلی خود قرار داد. بنابراین در ماه می همین سال، ایشان دستورکاری برای خلع سلاح^۳ را آغاز نموده و در آن تصریح کرد که «شدت و فراوانی حملات سایبری به ابزار اتصالات جهانی^۴ می‌تواند به طور فزاینده‌ای

۱. به گفتار دو از فصل یک کتاب مراجعه گردد.

2. António Guterres
3. Secretary-General's Agenda for Disarmament
4. global interconnectivity

گسترده شود و تعداد زیادی از سیستم‌ها و شبکه‌ها را به صورت تصاعدی در زمان واحد تحت تأثیر قرار دهد.^۱ همچنین ایشان بیان کرد که «در این زمینه، اقدامات سوء در فضای سایبری به کم شدن اعتماد میان دولت‌ها کمک می‌نماید».^۲

در همین راستا، به منظور مقابله با این چالش، دبیرکل دو پیشنهاد اقدامی^۳ زیر را درباره امنیت فناوری اطلاعات و ارتباطات در بندهای ۳۰ و ۳۱ طرح اجرایی^۴ مربوط به دستور کار خلع سلاح گنجانده است.

➤ بند ۳۰. دبیرکل باید مساعی جمیله^۵ خود را جهت کمک به پیشگیری از {مخاصمه ناشی از فعالیت سوء در فضای سایبری و حل و فصل مسالمت‌آمیز اختلافات} ناشی از آن فراهم نماید. ضمن تسهیل همکاری جهت کاهش خطر مخاصمات و تشویق به حل اختلاف مسالمت‌آمیز، اقدام بموقع می‌تواند در اعتمادسازی و اطمینان‌سازی متقابل، اثربخشی داشته باشد. در هر نوع از شرایط مخاصمه، مساعی جمیله از طرف دبیرکل می‌تواند نقشی در کاهش، پیشگیری و مدیریت مخاصمه ناشی از استفاده سوء از {فناوری اطلاعات و ارتباطات} از طریق اقدامات سایبری در داخل مرزها یا فراتر از مرزها، ایفا نماید.

اجرای روش مساعی جمیله عبارت است از استفاده از طرف ثالث، اعم از یک دولت یا گروهی از دولت‌ها یا یک سازمان بین‌المللی، جهت تشویق طرفهای متنازع جهت نیل به یک راه‌حل رضایت‌بخش برای دو طرف. این فرایند، برخلاف شیوه داوری و رسیدگی قضایی، تحریض و تشویق طرفهای اختلاف را برای نیل به شرایطی رضایت‌بخش جهت ختم اختلاف در میان خود مورد هدف دراد، ولی مصرحاتی را برای اجرا مقرر نمی‌دارد. از نظر فنی، مساعی جمیله هنگامی به کار می‌رود که یک طرف ثالث می‌کوشد با استفاده از نفوذ خود در طرفهای متنازع، آن‌ها را به مذاکره بکشاند. کنوانسیون‌های لاهه مورخ ۱۸۹۷ و ۱۹۰۷، بسیاری از قواعد ناظر بر این فرایند را وضع کرده است {در این کنوانسیون‌ها} تصریح شده که امضاکنندگان معاهدات حق دارند مساعی

1. "global interconnectivity means that the frequency and impact of cyberattacks could be increasingly widespread, affecting an exponential number of systems or networks at the same time"

2. "in this context, malicious acts in cyberspace are contributing to diminishing trust among States."

3. action points

4. implementation plan

5. good offices

جمیله خود را حتی در خلال جنگها به عمل آورند و اینکه اعمال این حق هرگز نباید از سوی طرفهای متنازع، عملی غیردوستانه تلقی شود.^۱ بر همین اساس در ۳ اکتبر ۲۰۱۸ دو اقدام زیر منتشر و در ۲۸ ژانویه ۲۰۱۹ به تصویب رسید:

۱. ایجاد ظرفیت در دبیرخانه جهت توانمندسازی آن در راستای حمایت بموقع از دبیرکل باهدف انجام مساعی جمیله در زمان درخواست {دولت‌ها}^۲

۲. به‌منظور کاهش هرگونه مخاصمه ناشی از حوادث سایبری و بنا به درخواست {دولت‌ها} و طی هماهنگی با شرکای قابل اطمینان، محتوا (متن) کارشناسی {لازم} در حمایت از مساعی جمیله دبیرکل تهیه گردد.^۳ در این باب، جهت مساعی جمیله دبیرکل در زمینه تقلیل قابلیت بروز مخاصمه ناشی از حوادث سایبری، اداره امور خلع سلاح ملل متحد حمایت محتوایی^۴ را در هماهنگی با همکاری‌های مربوط تأمین خواهد نمود.

در ۵ فوریه ۲۰۱۹ ژاپن و در ۲۰ فوریه همین سال سوئد به‌عنوان کشورهای پشتیبان^۵ این گام‌ها ثبت شدند.

➤ بند ۳۱. دبیرکل جهت کمک به تقویت فرهنگ پذیرش و پاسخگویی به هنجارها، قواعد و اصول درباره رفتار مسئولانه در فضای سایبری، با دولت‌های عضو تعامل خواهد کرد.^۶ گزارش سال ۲۰۱۵ گروه کارشناسان دولتی درباره تحولات در زمینه اطلاعات و ارتباطات راه دور در چارچوب امینیت بین‌الملل تعداد ۱۱ هنجار غیرالزام‌آور داوطلبانه را درباره رفتار مسئولانه دولت‌ها در استفاده از چنین فناوری‌هایی توصیه نمود. متعاقب آن مجمع عمومی در قطعنامه خود به شماره ۷۰/۲۳۷، از تمامی دولت‌های عضو درخواست نمود تا در استفاده از فناوری‌های اطلاعات و ارتباطات راه دور، این ۱۱ توصیه را راهنمای خود قرار دهند.

جهت پیشگیری از مخاصمه در فضای سایبری، اجرای چارچوب‌های هنجاری موجود اهمیت زیادی دارد و می‌تواند از طریق توسعه ابزار کاربردی تسهیل گردد. در این باب و به‌منظور

۱. حقوق بین‌الملل، ملکم شاول، ترجمه محمدحسین وقار، چاپ سوم، ص ۳۷۱

2. Establish a capacity within the Secretariat to enable, upon request, timely support to the good offices of the Secretary-General

3. Provide, upon request, substantive expertise in coordination with trusted partners to support of the good offices of the Secretary-General in mitigating any conflict that may arise from cyber-incidents

4. Substantive support

5. supporter

6. The Secretary-General will engage with Member States to help foster a culture of accountability and adherence to emerging norms, rules and principles on responsible behaviour in cyberspace.

پشتیبانی از ظرفیت‌سازی در دولت‌های عضو طرحی آماده شد و اداره امور خلع سلاح^۱ و مؤسسه پژوهشی خلع سلاح ملل متحد^۲، متعهد { به انجام } چندین اقدام ابتکاری از جمله موارد زیر گشتند:

۱. توسعه دوره آموزشی برخط مبتنی بر گزارش‌های گروه کارشناسان دولتی درباره تحولات در زمینه اطلاعات و ارتباطات راه دور در چارچوب امنیت بین‌الملل^۳ (این اقدام توسط اداره امور خلع سلاح و به‌منظور ارتقای سطح آگاهی و درک توصیه‌های مندرج در گزارش گروه کارشناسان دولتی در بستر آموزش الکترونیکی^۴ انجام می‌شود)؛

۲. ایجاد بسته ابزاری اجرای هنجارها جهت حمایت از دولت‌های عضو در اجرای هنجارهای بازده گانه داوطلبانه^۵ (این اقدام نیز توسط اداره امور خلع سلاح انجام می‌شود)؛

۳. تعامل با سایر ذی‌نفعان از جمله بخش‌های خصوصی، نیروهای انتظامی، سازمان‌های منطقه‌ای و نهادهای فرعی جهت اقدامات کاربردی در عملیاتی نمودن هنجارهای داوطلبانه سایبری و تشویق برای همکاری بیشتر^۶ (این اقدام نیز توسط اداره امور خلع سلاح و مؤسسه پژوهشی خلع سلاح ملل متحد انجام می‌گیرد)؛

۴. علاوه بر این ایجاد پورتال خط‌مشی سایبری یونیدیر با سایر بخش‌ها و منابع در خصوص عملیاتی‌سازی هنجارها^۷ (این پورتال سبب ارتقای شفافیت در اسناد راهبرد سایبری و چارچوب‌های حقوقی می‌شود)؛

۵. مشارکت جهت رفع شکاف دانشی میان دولت‌های عضو از طریق پیش‌بینی سناریوی تمرینی، رخدادهای و کارگاه‌ها^۸. از جمله اقدامات اجرا شده در این زمینه می‌توان به موارد زیر اشاره نمود:

- کنفرانس ثبات سایبری توسط یونیدیر در سال ۲۰۱۹؛

- کارگاه‌هایی با موضوعات امنیت بین‌المللی سایبری توسط یونیدیر؛

1. United Nations Department for Disarmament Affairs
2. The United Nations Institute for Disarmament Research (UNIDIR)
3. Develop an online training course based on the reports of the Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security
4. e-learning platform
5. Develop a norms implementation toolkit to support Member States in their implementation of the 11 voluntary cyber norms
6. Engage with other stakeholders, including the private sector, law enforcement, regional organizations and technical bodies to develop practical measures to operationalize voluntary cyber norms and encourage further collaboration.
7. Further develop UNIDIR's Cyber Policy Portal with additional sections and resources on norms operationalization.
8. Contribute to closing the cyber knowledge gap amongst Member States through workshops, scenario exercises and events

این طرح در تاریخ ۳ اکتبر ۲۰۱۸ منتشر و در تاریخ ۳۱ اکتبر همین سال، اقدامات ۴ و ۵ به‌عنوان اقدامات جدید جهت انعکاس به یونیدیر منتشر شد، اقدام شماره ۳ نیز جهت انعکاس به دامنه کاملی از ذی‌نفعان به‌روزرسانی گردید.

از کشورهای تقویت‌کننده این طرح می‌توان به استرالیا، هلند، کره جنوبی، سنگاپور و از کشورهای حامی این طرح می‌توان به ژاپن و سوئیس اشاره نمود. به‌طوری که کشورهای سنگاپور و هلند در تاریخ ۵ فوریه و کشور کره جنوبی در تاریخ ۱ مارس و استرالیا در تاریخ ۲۵ می ۲۰۱۹ در این کمپین^۱ قرار گرفتند و کشورهای سوئیس در تاریخ ۲۰ فوریه و ژاپن در اول مارس ۲۰۱۹ در لیست کشوران پشتیبانی‌کننده قرار گرفتند.

دولت‌ها و سازمان‌های منطقه‌ای که درباره ایفای نقش راهبری فعال در فعالیتهای مربوط به اقدام مفروض توافق کرده اند، از جمله از طریق تعهدات مالی و سیاسی یا سایر تعاملات فعال تحت عنوان کمپین و پشتیبان شناخته می‌شوند.^۲ اما طبق بررسی‌های به‌عمل آمده تفاوت عمده بین کشورهای کمپین و کشورهای پشتیبان این است که کمپین معمولاً برای اقداماتی جهت تقویت و دفاع از امری استفاده می‌شود در حالی که پشتیبان و حامی به‌عنوان کشوری استفاده می‌شود که مانع خاتمه و شکست امری می‌گردد.^۳

بند چهار: راهبرد دبیرکل درباره فناوری‌های جدید

توسعه سریع فناوری‌های جدید مانند هوش مصنوعی، فناوری‌های زیستی، علوم مواد و رباتیک به طور غیرباورکردنی سبب پیشرفت رفاه بشر می‌شود اما آن‌ها این قابلیت را دارند که سبب عدم تساوی و خشونت بیشتر نیز گردند. در این راستا راهبردی از طرف دبیرکل ملل متحد درباره فناوری‌های جدید^۴ در سال ۲۰۱۸ منتشر گردید در این سند این‌گونه آمده است که: «این راهبرد داخلی با هدف تعریف اینکه نظام ملل متحد چگونه از {موضوع} تحت حمایت خواهد کرد، تعیین گردیده است. «استفاده از فناوری‌های جدید به‌منظور تسریع دستیابی به

1. champion

2. States and regional organizations that have agreed to play to play to an active leadership role in the activities of a given action, including through specific political or financial commitments, or through active engagement, are identified as champions and supporters.

3. champion is (usually) of a cause) to promote, advocate, or act as a champion for while support is to keep from falling

4. SECRETARY-GENERAL'S STRATEGY ON NEW TECHNOLOGIES

دستور کار توسعه پایدار و تسهیل انطباق آن‌ها با ارزش‌های تکریم شده در منشور ملل متحد، اعلامیه جهانی حقوق بشر و هنجارها و استانداردهای حقوق بین‌الملل»^۱.

در اصل می‌توان گفت: این راهبرد توانمندی ملل متحد در استفاده از فناوری‌های جدید برای تحقق اهداف منشور ملل متحد، اعلامیه جهانی حقوق بشر و دستور کار توسعه پایدار را ارتقای خواهد داد. در ادامه در این سند آمده است که:

«جهت غلبه بر چالش‌ها و تطبیق حقوق {در حوزه فناوری‌های جدید} نیاز به کار نزدیک با شرکای جدید و فعلی وجود خواهد داشت. مخصوصاً در حوزه‌های حق حریم خصوصی و حقوق بشر، اخلاقیات، تساوی و انصاف، حاکمیت، مسئولیت‌پذیری و شفافیت و پاسخگویی» بر مبنای مشاوره‌های {انجام شده} در سرتاسر نظام ملل متحد، دبیرکل، به‌عنوان راهنما جهت تعامل ملل متحد با فناوری‌های جدید پنج اصل را شناسایی نموده است:

۱. حفاظت و ارتقای ارزش‌های جهانی^۲: تکیه‌گاه اصلی کار ما باید ارزش‌ها و الزامات مندرج در منشور ملل متحد و اعلامیه جهانی حقوق بشر باشد؛

۲. تقویت شمولیت و شفافیت^۳: ما باید بستری را برای حکومت‌ها، فضای کسب و کار و جامعه مدنی

برای تمامی نسل‌ها ایجاد نماییم تا انتخاب انبوهی در خصوص فناوری‌های جدید داشته باشند؛^۴

۳. کار مشارکتی^۵: ما جهت افزایش دانش جمعی، سنجش ایده‌ها و گسترش گفتگو، باید توسعه مشارکت سرتاسری میان دامنه‌ای از بازیگران را ارتقای دهیم؛

۴. اقدام مبتنی بر ظرفیت‌ها و دستور کارهای موجود^۶: تعامل ما با فناوری‌های جدید نیازمند حفظ

ارزش‌های منشور ملل متحد و اجرای دستور کارهای سازمان ملل متحد {دستور العمل} می‌باشد.

۵. تواضع و تداوم یادگیری^۷: ملل متحد شریک معلوم و مشهودی برای بسیاری از صنایع، گروه‌های

جامعه مدنی و نهادهای حکومتی نیست بنابراین ما نیاز داریم تا با هم تعامل داشته باشیم و از هم

بیاموزیم.

1. facilitate their alignment with the values enshrined in the UN Charter, the Universal Declaration of Human Rights and the norms and standards of International Laws

2. PROTECT AND PROMOTE GLOBAL VALUES

3. FOSTER INCLUSION AND TRANS-PARENCY

4. we must provide a platform for governments, businesses and civil society across generations to make collective choices about new technologies

5. WORK IN PARTNERSHIP

6. BUILD ON EXISTING CAPABILITIES AND MANDATES

7. BE HUMBLE AND CONTINUE TO LEARN

بر اساس این پنج اصل و بر اساس تلاش‌ها و ابتکارات صورت گرفته توسط بخش‌های مختلف سازمان ملل متحد مخصوصاً تلاش‌هایی که در سطح کشورها صورت گرفته است، دبیرکل سازمان ملل چهار تعهد راهبردی {زیر} را برای دبیرخانه و رئیس‌ان سایر بخش‌های نظام ملل متحد اعلام نمود. شایان ذکر است که این چهار تعهد ترکیبی از عناصری است که ناشی از تعاملات خارجی و حمایت توسط اقدامات داخلی سازمان ملل جهت بالابردن دانش و تعامل با فناوری‌های جدید و تقویت یک سیستم آموزشی نوآور و کارآفرین می‌باشد:

۱. تعمیق قابلیت‌های داخلی سازمان ملل متحد و و ارائه آن در قبال فناوری‌های جدید^۱؛
۲. افزایش درک، پشتیبانی و گفتگو {در خصوص فناوری‌های جدیدی}^۲؛
۳. پشتیبانی از گفتگو درباره چارچوب‌های هنجاری {قاعده ای} و همکاری^۳؛
۴. ارتقای پشتیبانی نظام ملل متحد از توسعه ظرفیت حکومت‌ها^۴.

گفتار دو: دفتر مقابله با مواد مخدر و جرم ملل متحد

ماهیت پیچیده جرم سایبری، درنوردیدن مرزهای سنتی جغرافیایی و ایجاد قلمروهای بدون مرز در فضای سایبر و درگیری فزاینده گروه‌های مربوط به جرائم سازمان یافته سبب شده تا نیاز به تدوین و اتخاذ یک برنامه جامع جهانی جهت بالا بردن مسئولیت بین‌المللی، پویا و فوری توسط دولت‌ها، جامعه بین‌المللی و بخش‌های خصوصی بیش از پیش احساس شود.

از طرفی به دلیل اینکه جهان به سمت جامعه ای ابرپیوسته با دسترسی به یک اینترنت جهانی حرکت می‌نماید، شناخت و کشف جرائم کامپیوتری هر روز سخت‌تر می‌شود. مخصوصاً جرائمی که {مستقیماً} با مدارک الکترونیکی مرتبط نباشد، جرائمی که علاوه بر اینکه می‌توانند در دنیای غیربرخط رخ دهند، می‌توانند توسط فناوری اطلاعات و ارتباطات و به شکل برخط تسهیل گردند. جرائمی مانند کلاهبرداری برخط، خرید مواد مخدر به شکل برخط و پول شویی برخط. چنین جرائمی تحت عنوان جرائم دارای امکان ارتکاب در فضای سایبر^۵ اطلاق می‌گردد.

1. Deepening the UN's internal capacities and exposure to new technologies
2. Increasing understanding, advocacy and dialogue
3. Supporting dialogue on normative and cooperation frameworks
4. Enhancing UN system support to government capacity development
5. Cyber-enabled offences

این جرائم فی‌نفسه متعلق به فضای غیربرخط هستند که امکان ارتکاب آن‌ها در فضای برخط نیز وجود دارد. در واقع از فضای غیربرخط به فضای برخط تسری پیدا کرده‌اند. علاوه بر جرائم دارای امکان ارتکاب در فضای سایبری، سوءاستفاده و استثمار جنسی کودکان، اخاذی جنسی در فضای اینترنت نیز بسیار مشهود می‌باشد.

محتوای منافی عرف که اغلب مردم در فضای برخط مشاهده می‌کنند تنها بخش کوچکی از داده‌هایی است که در فضای آشکار اینترنت^۱ وجود دارد. اغلب موتورهای جستجوگر تنها ۴٪ از محتوای موجود در اینترنت را نشان می‌دهند. وب تاریک^۲ یا وب عمیق که به‌عنوان بخشی از تارنمای جهان‌گستر تعریف شده است و نمی‌تواند توسط موتورهای جستجوگر پوشش داده شود، مجموعه‌ای از هزاران تارنمایی است که از ابزارهای خاص و مجهولی برای رمزنویسی مسیر ترافیک و مخفی کردن آدرس IP خود استفاده می‌کنند و وب تاریک با اینکه می‌تواند توسط فعالان حقوق بشر و روزنامه‌نگاران به شکل مثبتی استفاده گردد، اما اغلب توسط مجرمان و بدون اینکه فعالیت‌های آن‌ها آشکار گردد، به راحتی جهت فروش سلاح در بازار سیاه، فروش دارو و سوءاستفاده از کودکان بهره‌برداری می‌شود.

از این رو، چنین تحولاتی نیازمند تغییرات اساسی در رویکردهای مربوط به اجرای قوانین، جمع‌آوری ادله و مدارک و سازوکارهای همکاری بین‌المللی در موضوعات کیفی می‌باشد. تدارک چنین برنامه‌ای می‌تواند تصویری جهانی از جرائم سایبری ترسیم کند، دروس آموخته شده از تلاش‌های جاری و گذشته را برجسته نماید و گزینه‌های ممکن برای مسئولیت‌های آینده را ارائه دهد.

باتوجه به نکات فوق، مجمع عمومی سازمان ملل در قطعنامه خود^۳ {شماره} ۶۵/۲۳۰ مورخ ۲۱ دسامبر ۲۰۱۰ از کمیسیون پیشگیری از جرم و عدالت کیفی درخواست نمود تا در راستای بند ۴۲ اعلامیه سالوادور، یک گروه کارشناسی بین‌دولتی باز^۳ را جهت بررسی جامع مسئله جرم سایبری و مسئولیت‌های دولت‌های عضو، جامعه بین‌المللی و بخش خصوصی در قبال آن، از جمله در موضوعات زیر تشکیل دهد:

1. Clear internet
2. Dark web
3. open-ended intergovernmental expert group (IEG)

تبادل اطلاعات در تدوین قانون ملی و همچنین تبادل رویدر همین راستا، گروه کارشناسان، ۵ نشست را در خصوص اجرای بررسی جامع مسئله جرم سایبری در وین برگزار نمود: نشست اول در تاریخ ۱۷ تا ۲۱ ژانویه ۲۰۱۱، نشست دوم در تاریخ ۲۵ تا ۲۸ فوریه ۲۰۱۳، نشست سوم در تاریخ ۱۰ تا ۱۳ آوریل ۲۰۱۷، نشست چهارم در تاریخ ۳ تا ۵ آوریل ۲۰۱۸ و نشست پنجم در تاریخ ۲۷ تا ۲۹ مارس ۲۰۱۹.

در اولین اجلاس گروه کارشناسان (سال ۲۰۱۱)، این گروه، مجموعه‌ای از موضوعات و روش‌ها را جهت بررسی در حوزه جرم سایبری تصویب نمود. از آنجایی که یک تعریف بین‌المللی از جرم سایبری و از حملات سایبری وجود ندارد، نوع جرائم مرتبط با اینترنت^۱ در مقوله‌های زیر دسته بندی می‌شوند: جرائم علیه محرمانگی، یکپارچگی و دسترس پذیری سیستم‌ها و داده‌های کامپیوتر، جرائم مرتبط با کامپیوتر، جرائم مرتبط با محتوا، جرائم مرتبط با نقض حقوق با تأکید بر حقوق نشر. مجموع موضوعات جهت رسیدگی در این بررسی جامع درباره جرم سایبری شامل موارد زیر می‌باشد: مسئله جرم سایبری، پاسخ‌ها و مسئولیت‌های قانونی در برابر جرم سایبری، قابلیت‌های پیشگیری از جرم و عدالت کیفری و سایر مسئولیت‌ها در برابر جرم سایبری، سازمان‌های بین‌المللی، مساعدت‌های فنی.

در بررسی این موضوعات، عناوین هشتگانه‌ای تحت پوشش قرار گرفت: اتصالات و جرم سایبری^۲، تصویر جهانی^۳، چارچوب‌ها و قانونگذاری (تدوین قوانین)^۴، جرم‌انگاری^۵، تحقیق و اجرای قوانین^۶، مدارک الکترونیکی و عدالت کیفری^۷، همکاری بین‌المللی^۸، پیشگیری^۹. روشی که دفتر مقابله با مواد مخدر و جرم سازمان ملل متحد جهت توسعه بررسی اتخاذ نمود شامل این اقدامات زیر بود: ۱. ایجاد پرسش‌نامه‌هایی با هدف گردآوری اطلاعات، ۲. وصول و تحلیل داده‌ها و ۳. ایجاد یک متن پیش‌نویس بررسی.

1. Types of internet-related crimes
2. Connectivity and cybercrime
3. The global picture
4. Legislation and frameworks
5. Criminalization
6. Law enforcement and investigations
7. Electronic evidence and criminal justice
8. International cooperation
9. Prevention

روش گردآوری اطلاعات شامل پرسشنامه‌هایی بود که توسط دفتر مقابله با مواد مخدر و جرم سازمان ملل از فوریه ۲۰۱۲ تا ژوئن همان سال بین دولت‌های عضو، سازمان‌های بین‌دولتی و نمایندگان بخش خصوصی و مؤسسات دانشگاهی توزیع گردید. اطلاعات از ۶۹ کشور با توزیع جغرافیایی زیر دریافت شد. همچنین بیش از ۵۰۰ سند (منبع باز) توسط دبیرخانه بررسی گردید: قاره آفریقا: ۱۱ کشور، قاره آمریکا: ۱۳ کشور، قاره آسیا: ۱۹ کشور، قاره اروپا: ۲۴ کشور، قاره اقیانوسیه: ۲ کشور و ۴۰ سازمان بخش خصوصی، ۱۶ سازمان دانشگاهی و ۱۱ سازمان بین‌دولتی. مجمع عمومی در قطعنامه خود {به شماره} ۶۷/۱۸۹ مورخ ۲۰ دسامبر ۲۰۱۲، ضمن تقدیر از عملکرد گروه کارشنان بین‌دولتی باز در اولین نشست خود، این گروه را جهت ارتقای تلاش به‌منظور تکمیل عملکرد و ارائه خروجی بررسی‌های خود به کمیسیون پیشگیری از جرم و عدالت کیفری در دوره‌های مقرر تشویق نمود.

بعد از پایان نشست دوم گروه کارشناسان در فوریه ۲۰۱۳، وفق قطعنامه‌های کمیسیون پیشگیری از جرم و عدالت کیفری سازمان ملل {به شماره‌های} ۲۲/۷ مورخ ۲۶ آوریل ۲۰۱۳ و ۲۲/۸ مورخ ۲۶ آوریل ۲۰۱۳، برنامه جهانی درباره جرم سایبری متعهد شد تا با همیاری دولت‌های عضو، از طریق ظرفیت‌سازی و مساعدت‌های فنی، با جرائم مرتبط مقابله نمایند. در این راستا، کمیسیون از دبیرخانه درخواست نمود تا بررسی جامع درباره جرم سایبری را به شش زبان سازمان ملل ترجمه کند و جهت گرفتن نظرهای دولت‌ها، به‌منظور کمک به گروه کارشناسان بین‌دولتی باز، این اسناد را در زمان مقتضی بین اعضاء منتشر نماید.

در راستای این قطعنامه دبیرخانه از دولت‌ها دعوت نمود تا نظرهای خود را درباره بررسی جامع جرم سایبری حداکثر تا تاریخ ۱۳ می ۲۰۱۶ به دبیرخانه ارسال نمایند.^۱ با درخواست دولت‌ها آخرین مهلت ارائه تا ۲۰۱۳ تمدید گردید.^۲ از جمله کشورهایی که به درخواست دبیرخانه پاسخ دادند می‌توان به الجزایر، آرژانتین، استرالیا، برزیل، کانادا، چین، کلمبیا، ساحل عاج، اکوادور، فرانسه، آلمان، ژاپن، مکزیک، مراکش، پاراگوئه، روسیه، عربستان سعودی، سودان، سوریه، انگلیس، آمریکا، اتحادیه اروپا اشاره نمود.

1. CU 2016/50/DTA/OCB/CSS
2. CU 2016/133/DTA/OCB/CSS

در سومین نشست گروه کارشناسان که در تاریخ ۱۰ تا ۱۳ آوریل ۲۰۱۷ برگزار گردید. به منظور پیشگیری و مبارزه علیه جرائم سایبری در یک الگوی کلی، با پشتیبانی دولت‌های عضو یک برنامه جهانی جهت پاسخ به نیازهای شناخته شده در کشورهای در حال توسعه، طراحی گردید. از نظر جغرافیایی، تمرکز اصلی برنامه جرائم سایبری در سال ۲۰۱۷ روی مناطق آمریکای مرکزی، شرق آفریقا، آسیای میانه، جنوب شرق آسیا و اقیانوسیه بود و اهداف زیر را پوشش داد:

✓ افزایش کارایی و اثربخشی در تحقیق، پیگرد و رسیدگی قضایی به جرائم سایبری با تأکید بر سوءاستفاده و استثمار جنسی کودکان از طریق برخط در یک چارچوب حقوق بشری قوی؛
✓ واکنش مؤثر و کارآمد بلندمدت و کامل کشورها در برابر جرم سایبری از جمله {از طریق} همکاری ملی، جمع‌آوری داده‌ها و چارچوب‌های مؤثر قانونی که منتهی به پاسخگویی پایدار و بازدارندگی کامل‌تری می‌شود؛

✓ تقویت ارتباط بین دولت‌ها، نیروی انتظامی (پلیس) و بخش خصوصی در سطح ملی و بین‌المللی، درباره دانش عمومی ارتقای یافته از خطرهای مربوط به جرائم سایبری.

در چهارمین نشست گروه کارشناسان که در تاریخ ۳ تا ۵ آوریل ۲۰۱۸ برگزار گردید، کارشناسان روی تدوین قانون و چارچوب‌ها و جرم‌انگاری‌های سایبری متمرکز شدند. تحولات سیاسی و قانونی جهت مقابله با جرم سایبری در سطوح ملی و بین‌المللی بحث گردید. در ارتباط با اینکه آیا یک سند حقوقی فراگیر و جهانی درباره جرم سایبری در چارچوب سازمان ملل متحد نیاز هست یا خیر؟، دیدگاه‌های متفاوتی مطرح گردید. این گروه همچنین درخصوص چگونگی ارتباط امنیت سایبری و جرم سایبری و همچنین تفاوت بین این دو مقوله بحث نمودند. علاوه بر این، گروه کارشناسان درباره راه‌هایی که از طریق آن جرم سایبری در سطح ملی جرم‌انگاری شده است بحث کردند. در این نشست طرح پیشنهادی مربوط به برنامه کاری گروه کارشناس^۱ برای دوره زمانی ۲۰۱۸ تا ۲۰۲۱ که بر مبنای قطعنامه کمیسیون پیشگیری از جرم و عدالت کیفری به شماره ۲۶/۴ و به‌منظور تسهیل اجرای این برنامه تهیه و توسط ریاست گروه ارائه گردید، مورد تصویب قرار گرفت. ترتیبات و موضوعات اصلی و نتایج و پیشنهادهای مطرح شده

1. workplan of the Expert Group for the period 2018–2021 (UNODC/CCPCJ/EG.4/2018/CRP.1).

در نشست های موقت گروه کارشناسان برای دوره فوق به شکل زیر مطرح شده است:

✓ چهارمین نشست در سال ۲۰۱۸: تدوین قانون، چارچوبها، جرم‌انگاری؛

✓ پنجمین نشست در سال ۲۰۱۹: تحقیق و اجرای قانون، مدارک الکترونیکی و عدالت کیفری؛

✓ ششمین نشست در سال ۲۰۲۰: همکاری بین‌المللی، پیشگیری؛

✓ هفتمین نشست در سال ۲۰۲۱: رسیدگی و بحث در خصوص فعالیت‌های آتی.

البته در این سند عنوان گردیده است که این برنامه کاری مانع امکان ورود موضوعات دیگر به‌دستور کار گروه کارشناسان بین‌دولتی و نیز مانع امکان ارائه تعاریف زیر موضوعات دیگر جهت بحث و گفتگو نخواهد بود. چارچوب زمانی و ترتیبات شرح داده شده در این برنامه کاری ممکن است در زمان لازم توسط گروه کارشناسی تنظیم شود. مطابق با این طرح کاری، دبیرخانه قبل از پنجمین نشست گروه کارشناسان در سال ۲۰۱۹، از دولت‌های عضو دعوت نمود تا نظرها، رویه‌های برتر، اطلاعات جدید، تلاش‌های ملی و پیشنهادها و توصیه‌های مربوط به گردآوری و انتشار بخش های ۲ و ۳ دستور کار نشست ۲۰۱۹ را ارائه نمایند.

در بند ۲۸ گزارش نشست گروه کارشناسان در سال ۲۰۱۸، بر نیاز به تدوین قانون درباره قابلیت طرح مدارک الکترونیکی در تحقیقات و پیگردها جهت مقابله مؤثر با جرم سایبری تأکید نموده است. تقنین در این حوزه باید با آموزش و ظرفیت‌سازی کافی برای مأموران نیروی پلیس، دادستان‌ها و قضات همراه باشد. اهمیت به اشتراک‌گذاری مدارک الکترونیکی میان افراد در حوزه قضایی تأکید گردیده است.

گفتار سه: اداره امور سیاسی و صلح‌سازی

اداره امور سیاسی و صلح‌سازی^۱ در تلاش‌های ملل متحد جهت ممانعت از مخاصمات مرگبار و ایجاد صلح پایدار^۲ در جهان نقش محوری را ایفا می‌نماید. اداره امور سیاسی و ایجاد صلح ملل متحد، اداره‌ای تحت دبیرخانه سازمان ملل است که مسئول پایش و ارزیابی تحولات سیاسی جهان و مشاوره و مساعمت دبیرکل ملل متحد و نمایندگان او در پیشگیری‌های صلح‌آمیز از

1. Department of Political and Peace building Affairs (DPPA)

2. prevent deadly conflict and build sustainable peace

مخاصمات در جهان می‌باشد. این اداره مأموریت‌های سیاسی در آفریقا، آسیای مرکزی و خاورمیانه را مدیریت می‌نماید و در سال‌های اخیر قابلیت‌های خود را در میانجی‌گیری مخاصمات^۱ و دیپلماسی پیشگیرانه^۲ افزایش داده است.

واحد پشتیبانی میانجی‌گری این اداره^۳، گزارش و بسته‌ابزاری درباره «فناوری‌های دیجیتال و میانجی‌گری در مخاصمات مسلحانه» را ایجاد کرده است. جهت شناسایی کاربردهای عملی فناوری در زمینه‌های میانجی‌گری، {این} گزارش و بسته‌ابزاری، چگونگی تأثیر فناوری‌های دیجیتال روی تلاش‌های میانجی‌گرانه را برجسته می‌نماید.^۴ این اداره در حمایت از پیشنهاد دبیرکل در خصوص ایجاد تلاش‌های مطلوب خود جهت پیشگیری {از} مخاصمه ناشی از فعالیت سوء در فضای سایبری و حل و فصل مسالمت‌آمیز {ناشی از آن} نقش راهبری دارد.

گفتار چهار: دفتر هماهنگی امور بشر دوستانه

در سال ۲۰۱۴ دفتر هماهنگی امور بشر دوستانه^۵ مقاله‌ای تحت عنوان «مکتب بشر دوستانه در عصر جنگ سایبری: به سوی استفاده اصولی و ایمن از اطلاعات در مواقع اضطراری بشر دوستانه» را منتشر و دفاع از «فضای سایبر بشر دوستانه» را توصیه نمود. در سال ۲۰۱۷ این دفتر، مرکزی را برای داده‌های بشر دوستانه {با اهداف زیر} تأسیس نمود:

- تضمین اینکه در موقعیت‌های بشر دوستانه، آن‌ها {طرف‌های مخاصمه و سایر نیازمندان} به داده‌های مورد نیاز دسترسی داشته باشند؛

- {مشخص کردن} زمان و چگونگی نیاز آن‌ها به داده‌ها و اتخاذ تصمیمات مسئولانه و

آگاهانه

این مرکز روی این حوزه‌های زیر متمرکز است: خدمات داده، سواد داده، خط‌مشی داده و تعاملات شبکه‌ای.

1. conflict mediation
2. preventive diplomacy
3. The Mediation Support Unit of DPPA
4. (Action 30 of the Secretary-General's Agenda for Disarmament)
5. Office for the Coordination of Humanitarian Affairs (OCHA)

گفتار پنج: کنفرانس خلع سلاح

کنفرانس خلع سلاح^۱ مجمعی چندجانبه است که توسط جامعه بین‌الملل پایه‌گذاری گردیده و دفتر آن در ژنو می‌باشد. این مجمع رسماً از سازمان ملل متحد جدا می‌باشد، اما به روش‌های گوناگون با آن در ارتباط است. مدیر کل دفتر ملل متحد در ژنو به‌عنوان دبیر با این کنفرانس همکاری می‌نماید. مجمع عمومی ملل متحد در قالب قطعنامه‌هایی موضوعاتی را جهت بررسی در این کنفرانس ارائه می‌نماید. کنفرانس، گزارش‌هایی از فعالیت‌های خود را هر ساله به مجمع عمومی سازمان ملل ارائه می‌نماید. این کنفرانس از طریق دفتر امور خلع سلاح ملل متحد^۲ تحت دبیرخانه حمایت می‌گردد.^۳ در سال‌های اخیر اعضای کنفرانس خلع سلاح، موضوعات مرتبط با فناوری اطلاعات و ارتباطات را در مباحث خود با عنوان «انواع جدید سلاح‌های کشتار جمعی و سیستم‌های جدید برای چنین سلاح‌هایی» را مطرح نمودند. در سال ۲۰۱۸ در پنجمین نهاد فرعی {این کنفرانس} مباحث محتوایی در خصوص ابعاد امنیتی فناوری‌های اطلاعات و ارتباطات، هوش مصنوعی و یادگیری ماشین برگزار گردید.

گفتار شش: اداره امور خلع سلاح ملل متحد

اداره امور خلع سلاح ملل متحد^۴، در سال ۱۹۸۲، بر اساس توصیه‌های دومین نشست ویژه مجمع عمومی درباره خلع سلاح^۵ تشکیل شد. در سال ۱۹۹۲ به نام دپارتمان امور خلع سلاح تحت دایره امور سیاسی^۶ تغییر نمود. سپس در ژانویه سال ۱۹۹۸ به‌عنوان دپارتمان امور خلع سلاح^۷ و در نهایت در سال ۲۰۰۷ به نام فعلی خود تغییر کرد.

حکم و وظایف این اداره و برنامه‌های آن از اولویت‌های مندرج در قطعنامه‌ها و تصمیمات مجمع عمومی در زمینه خلع سلاح استخراج گردید؛ از جمله سند نهایی دهمین نشست ویژه مجمع عمومی، اولین نشست ویژه و اختصاصی خلع سلاح^۸.

1. Conference on Disarmament (CD)

2. UNODA

3. wikipedia

4. United Nations Office for Disarmament Affairs

5. General Assembly's second special session on disarmament (SSOD II).

6. Department of Political Affairs

7. Department of Disarmament Affairs

8. first special session devoted to disarmament (resolution S-10/2)

از وظایف اصلی این اداره می‌توان به موارد زیر اشاره نمود:

- حمایت محتوایی و سازمانی جهت تنظیم هنجارها در حوزه‌های خلع سلاح؛
- تقویت اقدامات خلع سلاح از طریق گفتگو، شفاف‌سازی و اعتمادسازی درباره موضوعات نظامی؛^۱
- تشویق تلاش‌های خلع سلاح در سطح منطقه‌ای؛
- تحقیق و آموزش مؤسسات، جامعه مدنی، مخصوصاً سازمان‌های غیردولتی؛
- تأمین اطلاعات معقول، منصفانه (بی‌غرض) و به‌روز^۲ درباره موضوعات زیر:

✓ اقدامات دولت‌های عضو در خصوص خلع سلاح چندجانبه

✓ توافقات چندجانبه بین دولت‌های عضو، سازمان‌های بین‌دولتی، مؤسسات، سازمان‌های

نظام ملل متحد.

جهت انجام این وظایف، اداره امور خلع سلاح در پنج بخش زیر ساختارمند گردیده است:^۳

دبیرخانه کنفرانس خلع سلاح و بخش پشتیبانی کنفرانس^۴ که مقر آن در ژنو می‌باشد. این شاخه، مسئول تأمین خدمات سازمانی و محتوایی برای کنفرانس خلع سلاح، مجمع واحد گفتگوی خلع سلاح چندجانبه برای جامعه بین‌الملل^۵ و کمیته ویژه خلع سلاح می‌باشد.

بخش سلاح‌های کشتار جمعی^۶: این شاخه مسئول تأمین حمایت‌های محتوایی در خصوص خلع سلاح‌های کشتار جمعی (سلاح‌های هسته‌ای، شیمیایی، بیولوژیکی)، ضمن مشارکت مسئول حمایت از تلاش‌های چندجانبه می‌باشد. این شاخه، جهت تقویت عدم اشاعه سلاح‌های کشتار جمعی و در این ارتباط با سازمان‌های بین‌دولتی مرتبط و سازمان‌های تخصصی نظام ملل متحد مخصوصاً آژانس بین‌المللی انرژی اتمی^۷، سازمان منع سلاح‌های شیمیایی^۸ و کمیسیون مقدماتی سازمان معاهده منع جامع آزمایش‌های هسته‌ای^۹.

بخش سلاح‌های متعارف^{۱۰}: تلاش‌های این بخش در خصوص تمامی سلاح‌هایی متمرکز است

1. military matters
2. objective, impartial and up-to-date information
3. Structured in five branches
4. CD secretariat & conference support Branch (CD: conference on Disarmament)
5. Single multilateral disarmament negotiating forum of the international community
6. Weapons of mass destruction (WMD)
7. IAEA
8. OPCW
9. CTBTO PrepCom
10. Conventional Arms Branch(CAB)

که به‌عنوان سلاح کشتار جمعی در نظر گرفته نمی‌شوند. این بخش مسئول حمایت محتوایی از کنفرانس درباره برنامه و اقدام سازمان ملل درباره سلاح‌های کوچک، فرایند پیمان تجارت سلاح‌ها^۱ می‌باشد.

بخش خلع سلاح منطقه‌ای^۲: این بخش مسئول تأمین محتوایی از جمله ارائه خدمات مشاوره ای به دولت‌های عضو و سازمان‌های زیرمنطقه‌ای در خصوص اقدامات خلع سلاحی و موضوعات مرتبط با امنیت می‌باشد. این بخش اقدامات مربوط به سه مرکز منطقه‌ای برای امنیت و خلع سلاح (آفریقا، آسیا و اقیانوسیه و آمریکای لاتین و حوزه کارائیب) را مدیریت و هماهنگ می‌نماید.

بخش اطلاعات و توسعه^۳: این بخش مسئول سازمان‌دهی موارد زیر می‌باشد:

- ✓ رخدادهای برنامه‌های ویژه و متنوع وسیع در زمینه خلع سلاح،
- ✓ محصولات اداره امور خلع سلاح ملل متحد در قالب نشریه‌ها (مانند کتاب سال خلع سلاح) به‌روزرسانی طراحی و محتوای وبسایت اداره امور خلع سلاح ملل متحد
- ✓ حفظ پایگاه داده‌ها برای حوزه‌های خاص (وضعیت و متن تهدیدات خلع سلاح، قطعنامه‌ها و تصمیمات مجمع عمومی و ...)

خط‌مشی سایبری اداره امور خلع سلاح ملل متحد:

حمایت‌هایی سازمانی و محتوایی جهت تنظیم هنجارها^۴ در حوزه خلع سلاح از طریق کمیته یک مجمع عمومی، کمیسیون خلع سلاح، کنفرانس خلع سلاح و سایر نهادها، حمایت از مباحثات چندجانبه از جمله حمایت از گروه کارشناسان دولتی درباره تحولات در زمینه اطلاعات و ارتباطات راه دور در چارچوب امنیت بین‌الملل، دوره‌های آموزشی برخط درباره خط‌مشی سایبری.

بر مبنای ارزیابی‌ها و توصیه‌های مندرج در گزارش‌های گروه کارشناسان دولتی، این اداره با حمایت دولت سنگاپور و همکاری سایر شرکای اصلی، دوره آموزشی برخطی را توسعه داد

1. Arms Trade Treaty Process
 2. Regional Disarmament Branch (RDB)
 3. Information and Outreach Branch (IOB)
 4. norm-setting

که هدف اصلی از این دوره تشویق دولت‌ها جهت درک بیشتر در خصوص استفاده از فناوری‌های اطلاعات و ارتباطات و مفاهیم {مربوط به آن} در حوزه امنیت بین‌الملل می‌باشد. پنج رکن اصلی بر اساس گزارش‌های گروه کارشناسان در این دوره آموزشی مورد بحث قرار می‌گیرد و محتوای آموزشی هر بخش شامل موارد زیر می‌باشد:

تهدیدات موجود و نوظهور: تهدیداتی که امنیت فناوری اطلاعات و ارتباطات را در سطح بین‌الملل به مخاطره می‌اندازد و توسط گروه کارشناسان دولتی شناخته شده است. تحولات قابل پیش‌بینی که می‌تواند تهدیدات موجود را وخیم‌تر نماید؛

حقوق بین‌الملل: چگونگی اعمال حقوق بین‌الملل در استفاده از فناوری‌های اطلاعات و ارتباطات، توصیه‌هایی که گروه کارشناسان دولتی در این حوزه ارائه نموده است؛
هنجارها، قواعد و اصول: این بخش از دوره به معرفی هنجارهای یازده گانه غیرالزام‌آور و داوطلبانه در خصوص رفتار مسئولانه دولت‌ها که توسط گروه کارشناسان دولتی ارائه شده است می‌پردازد.

اقدامات اعتمادساز: اقدامات اعتمادساز چه می‌باشند و چرا ما برای فناوری اطلاعات و ارتباطات نیازمند به این اقدامات می‌باشیم. توصیه‌های کلیدی گروه کارشناسان دولتی در خصوص اقدامات اعتمادساز چیست؟ ابتکارات موجود در اقدامات اعتمادساز چیست؟

همکاری و مساعدت بین‌المللی در {حوزه} ظرفیت‌سازی: دولت‌ها چگونه می‌توانند در خصوص ظرفیت‌سازی خود جهت استفاده مسالمت‌آمیز از فناوری‌های اطلاعات ارتباطات با هم کار کنند ما چگونه می‌توانیم تاب‌آوری در ظرفیت‌سازی را تضمین نماییم؟ از طرفی و با توجه به اینکه قرن بیست و یکم، مخصوصاً با چالش‌های مربوط به جهان برخط روبه‌رو می‌باشد، زیست‌بوم فناوری اطلاعات و ارتباطات جهانی با افزایش استفاده سوء از این فناوری توسط بازیگران دولتی و غیردولتی همراه می‌باشد و ممکن است به امنیت و صلح بین‌المللی لطمه وارد نماید

بنابراین جهت ایجاد امنیت و ثبات بیشتر در فضای سایبری، {جهان} نیازمند ایده‌های متفاوت و جدیدی می‌باشد که ضمن همکاری بین‌رشته‌ای، قابل قیاس با عملکرد سایر حوزه‌های مختصات

ارائه شده باشد. در این خصوص اداره امور خلع سلاح ملل متحد برنامه‌ای را در قالب مسابقه و به‌منظور شبیه‌سازی تفکرات جدید زاینده از ذهن‌های نوآور جوان در سرتاسر جهان آغاز نمود. اداره امور خلع سلاح ملل متحد امیدوار است که در این طی روند، مبتکران جوان و هادیان جامعه فنی و سیاسی به هم کمک نماید تا به عوامل مورد نیاز جهت تقویت امنیت سایبری و کاهش تنش میان ملت‌ها در فضای برخط بپردازند. این اداره هدف اصلی این مسابقه را موارد زیر معرفی می‌نماید:

- ✓ توسعه فناوری‌های بدیع مبتنی بر راه‌حل‌ها؛
- ✓ کمک به محدود کردن اینترنتت به‌عنوان یک قلمرو مخاصمه؛
- ✓ کمک به افزایش و تقویت امنیت و ثبات، ایمنی، آزادی، دسترس‌پذیری و مسالمت‌آمیز بودن زیست‌بوم برخط (سایبر)؛

- ✓ مقابله به تهدیدات سایبری موجود و تهدیدات بالقوه؛
- ✓ تضمین احترام به حقوق بین‌الملل در فضای سایبری؛
- ✓ تضمین احترام به حقوق بشر در فضای سایبری؛
- ✓ پذیرفتن هنجارها، قواعد و اصول داوطلبانه؛
- ✓ تقویت اعتمادسازی؛
- ✓ ظرفیت‌سازی در فضای سایبری.

درخصوص تأثیر فناوری‌های اطلاعات جدید روی سوءاستفاده و استثمار جنسی کودکان، در سال ۲۰۱۵ بخش پشتیبانی کنفرانس این اداره، پیرو قطعنامه اکوسوک {به شماره} ۲۰۱۱/۳۳ درباره پیشگیری، حفاظت و همکاری بین‌المللی علیه استفاده از فناوری‌های اطلاعاتی جدید در سوءاستفاده و استثمار کودکان، گزارشی را آماده نمود. این مبنای تحقیقات این مطالعه موارد زیر می‌باشد:

منابع باز؛

نتایج نشست غیر رسمی گروه کارشناسان درباره تسهیل سوءاستفاده و استثمار جنسی توسط

فناوری اطلاعات و ارتباطات که در تاریخ ۲۳ تا ۲۵ سپتامبر ۲۰۱۳ در وین برگزار گردید؛ بررسی جامع جرم سایبری سال ۲۰۱۳ گروه کارشناسان بین دولتی باز. این اداره در این بررسی از حضور کارشناسان شاغل در حوزه‌های نیروی انتظامی، تعقیب کنندگان قانون، بخش خصوصی و دانشگاهی و جامعه مدنی بهره برد. این اداره در چارچوب برنامه اطلاعات خلع سلاح ملل متحد و به‌منظور بحث و گفتگوی رسمی بیشتر در خصوص موضوعات محدودیت‌های نیروهای مسلح^۱، خلع سلاح و امنیت، سلسله گزارش‌هایی را تحت عنوان جامعه مدنی و خلع سلاح^۲ منتشر می‌نماید. در طی همین روند، گزارشی را در سال ۲۰۱۷ منتشر نمود با عنوان «تفسیری از هنجارهای داوطلبانه و غیرالزام‌آور برای رفتار مسئولانه دولت‌ها در استفاده از فناوری اطلاعات و ارتباطات راه دور»^۳ این گزارش شامل مجموعه تفاسیری است از توصیه‌ها و پیشنهادهای موجود در بند ۱۳ گزارش گروه کارشناسان دولتی در سال ۲۰۱۵ درباره تحولات در زمینه اطلاعات و ارتباطات راه دور در چارچوب امنیت بین‌المللی.

نتیجه‌گیری فصل دوم:

فعالیت‌های شورای اقتصادی و اجتماعی سازمان ملل در حوزه جرایم اقتصادی مثل کلاهبرداری، سوءاستفاده مجرمانه و جعل هویت، حائز اهمیت است. در حوزه حکمرانی نیز نمی‌توان نتایج اجلاس سران راجع به جامعه اطلاعاتی را نادیده گرفت. مفهوم حکمرانی بر اینترنت بین کارشناسان هنوز هم محل چالش است. فارغ از مفاهیم تئوریک، آنچه در عمل دیده می‌شود تسلط کامل دولت ایالات متحده بر تاروپود فضای سایبر در طول تاریخ این فناوری می‌باشد. اگر تعریف حکمرانی بر اینترنت را در مفهوم مضیق آن، به امور فنی محدود کنیم، این حکمرانی از بدو امر در دست شرکت آمریکایی آیکان بوده است. اگر مفهوم موسع را در نظر بگیریم و سیاستگذاری بر اینترنت را تعریف حکمرانی بر اینترنت بدانیم، باید گفت که مشارکت دولت‌های ملی در این امر،

1. arms limitation

2. CIVIL SOCIETY AND DISARMAMENT

3. Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology A Commentary

تا کنون تشریفاتی بوده است و دولت ایالات متحده به اشکال مختلف سعی نموده است مانع مشارکت دولت‌ها در اداره جهانی اینترنت شود. آمریکا با شعار عوام‌فریبانه مبارزه با اعمال دیکتاتوری دولت‌ها بر فضای سایبر، در عمل، انحصار این حکمرانی را برای خود حفظ کرده است. آنچه در تاریخ حکمرانی بر اینترنت شاهدیم، تلاش‌های ملی، منطقه‌ای و بین‌المللی علیه انحصار حکمرانی آمریکا بر فضای سایبر است که این تلاش‌ها به خاطر کارشکنی‌های دولت ایالات متحده، اگر نگوییم به شکست کامل منجر شده، اما به طور حتم می‌توان ادعا کرد که نتایج حداقلی در پی داشته است. مهم‌ترین تلاش‌های صورت گرفته در این خصوص به اجلاس سران جامعه اطلاعاتی بر می‌گردد که طی دو مرحله به این موضوع ورود کرد و با وجود پیشرفت‌های اعلامی، در عمل دستاورد چندانی حاصل نشد. مجمع راهبری اینترنت، مهم‌ترین خروجی این تلاش‌ها بوده است که این مجمع در عمل به یک گردهمایی کم‌اهمیت تبدیل شده است و تلاش‌ها برای کارآمد کردن آن، به نتیجه‌ای نرسیده است، به طوری که ادامه حیات آن با وضعیت فعلی، محل ابهام است و نباید منتظر خروجی توجه‌پذیری از این مجمع بود.

بعد از افشاگری‌های اسنودن در سال ۲۰۱۳ بود که هجمه جهانی علیه انحصار حکمرانی آمریکا دوباره شروع شد، به طوری که این دولت با یک ترفند تاکتیکی و طی یک عقب‌نشینی ظاهری اعلام کرد که به نظارت خود بر آیکان خاتمه خواهد داد و آن را به همه ذی‌نفعان این حوزه خواهد سپرد. بعد از چند سال که روند این انتقال صورت گرفت آنچه در نهایت حاصل شد، مشارکت دولت‌ها نبود، بلکه مشاوره تصنعی و غیرالزام‌آور دولت‌ها خطاب به آیکان بود. در واقع آمریکا از این طریق به حکمرانی باطنی و واقعی خود، تحت پوشش مشارکت دولت‌ها، مشروعیت بخشید و این روند همچنان ادامه دارد.

در خصوص عملکرد سایر سازمان‌های تخصصی اکوسوک نیز باید گفت که این اسناد تولیدی هرچند فی‌نفسه در زمره حقوق نرم قرار دارند، اما در مقام بیان هنجارها، قواعد معاهداتی و عرفی می‌باشند. در مجموع باید به محتوای این اسناد با دقت و احتیاط نگریست و بیان به ظاهر متعالی این اسناد نباید موجب اغفال تصمیم‌سازان و تصمیم‌گیران در کشور شود.

بررسی عملکرد شورای امنیت نشان می‌دهد که این شورا در آینده نزدیک با محوریت و

بهبانۀ مبارزه با تروریسم در فضای سایبر به این موضوع ورود جدی تری خواهد کرد. آنچه تاکنون شورای امنیت را تا حد زیادی از ورود به این مباحث بازداشته است، نبود کنوانسیون های مربوط به تروریسم سایبری، جنگ سایبری و امنیت سایبری است. به عبارت دیگر، عنصر قانونی جهت ورود شورای امنیت وجود ندارد. اما پیشرفت روزافزون سند تالین که در مورد اعمال حقوق جنگ بر جنگهای سایبری است و ساخته و پرداخته سازمان ناتو می باشد و همچنین با عنایت به سایر روندهای بین المللی و دکترین های برخی کشورها از جمله دولت ایالات متحده که فضای سایبر را به عنوان عرصه پنجم نبرد (بعد از زمین، هوا، دریا و فضا) به رسمیت شناخته است، تدوین کنوانسیون جنگ سایبری و سایر کنوانسیون ها در آینده اجتناب ناپذیر است.

بنابراین این احتمال وجود دارد که در آینده از بستر چنین کنوانسیون هایی، کشورهای مستقل، مورد اتهام هایی مثل تهدید صلح و نقض صلح و حمایت از تروریسم در فضای سایبر واقع شده و تدابیر شورای امنیتی علیه آن کشورها اتخاذ گردد. بنابراین شایسته است ضمن تعامل با کشورها و سازمان های همسو، مانع تفسیر موسع کشورهای غربی از حقوق مختصات مسلحانه در فضای سایبر شویم.

موضوع فناوری های اطلاعات و ارتباطات و امنیت بین المللی تاکنون در دیوان بین المللی دادگستری مطرح نشده است. برابر بررسی به عمل آمده تا زمان نگارش کتاب، رد پای موضوعات مرتبط با فضای سایبر در آرای مشورتی و ترافعی دیوان دیده نمی شود.

به باور نویسنده، مشکلات مرتبط با انتساب و صعوبت بار کردن مسئولیت در این فضا به خاطر عدم بسندگی ادله حقوقی و فنی، عامل اصلی در عدم ورود نهاد حقوقی و قضایی ملل متحد به این موضوع بوده است^۱ که این همه ناشی از ویژگی های خاص فضای سایبر است. اما ورود دیوان به این حوزه نوپدید در آینده امر غیرمحمتملی نیست.

۱. منبع در فایل الکترونیک پیوست شده است.

نتیجه‌گیری نهایی

الف. جمع‌بندی تحلیلی مطالب

حقوق بین‌الملل سایبری از شاخه‌های متأخر حقوق بین‌الملل است، اما نباید تصور شود که هیچ اقدامی برای نظام‌مند کردن فعالیت در فضای سایبر در محیط بین‌الملل صورت نگرفته است. همه‌ذی‌نفعان فضای سایبر از جمله دولت‌ها به‌عنوان نخستین تابعان حقوق بین‌الملل، اقدامات متعددی برای تدوین و اجرای حقوق بین‌الملل سایبری صورت داده‌اند. فضای سایبر به‌عنوان یکی از عرصه‌های نوپدید در محیط بین‌الملل به خاطر ویژگی‌های منحصر‌به‌فرد خود، به نگرانی مشترک و درعین حال فزاینده کارشناسان حقوقی، فنی، سیاسی، امنیتی و بازیگران فروملی و فراملی بدل شده و جایگاه مهمی در گفتمان‌های حقوقی داخلی و بین‌المللی پیدا کرده است. با عنایت به ضرورت قاعده‌مند شدن فعالیت در این فضا، شکل‌گیری گفتمان‌های حقوقی هم در حقوق داخلی و هم در حقوق بین‌الملل به سرعت در حال تحقق است. دولت‌ها اقدام به ارائه طرح‌های مختلفی در راستای قاعده‌مند شدن این فضا نموده‌اند. از بین رفتن مرزهای سنتی در فضای سایبر دولت‌ها را به این نتیجه رسانده است که تدوین حقوق داخلی در حوزه سایبر با صرف نظر از تحولات بین‌المللی آن، امر مشکلی است. از طرف دیگر هیچ کنوانسیون مصوب بین‌المللی در حوزه سایبر وجود ندارد اما روندها و جریان‌های بین‌المللی به سمت تدوین چنین کنوانسیون یا کنوانسیون‌ها و معاهدات مربوط در حرکت‌اند. ویژگی‌های خاص فضای سایبر از جمله گمنامی در این فضا که شکل‌گیری مسئولیت را با مشکل مواجه می‌سازد از یک طرف و عملکرد غیرسازنده دولت ایالات متحده آمریکا در تدوین قواعد حوزه سایبر از طرف دیگر موجب ناکارآمدی تلاش‌های جمعی دولت‌ها جهت قاعده‌مندسازی این فضا بوده است. مثال زنده این مدعا، تلاش‌های صورت گرفته در بستر سازمان ملل بوده است که تا کنون به سرانجام قابل قبولی نرسیده است.

اگر خواسته باشیم نتایج فعالیت‌های سازمان ملل برای تأمین امنیت فضای سایبر و به تبع آن، تأمین امنیت بین‌الملل را ارزیابی کنیم، باید اذعان کرد که به موازات فعالیت این سازمان، امنیت فضای سایبر نیز رو به وخامت بوده است. به‌طوری که این سازمان نه‌تنها نتوانسته است

وضعیت بهتری برای امنیت فضای سایبر تأمین و ترسیم نماید، بلکه وضع موجود را نیز نتوانسته است حفظ نماید. افزایش روزافزون حملات سایبری و همچنین افزایش سالانه تعداد کشورهایی که در صدد ایجاد و تقویت زیرساخت‌های نظامی خود در حوزه سایبری هستند، گواه این واقعیت است که تلاش‌های بین‌المللی برای امن‌سازی فضای سایبر، چندان موفقیت‌آمیز نبوده است. برخی کشورها با انگیزه تهاجمی در صدد نظامی‌سازی فضای سایبر هستند، برخی دیگر که پیرامون امنیت سایبری خود بیمناک هستند، انگیزه‌های دفاعی در ایجاد و توسعه زیرساخت‌ها و ساختارهای نظامی سایبری دارند. اهداف و انگیزه‌ها هر چه که باشد، آنچه در عمل شاهد آن هستیم، اوضاع رو به وخامت امنیت فضای سایبر است که ناشی از رقابت‌های پیدا و پنهان بازیگران اصلی این حوزه می‌باشد. رقابت‌هایی که فعالیت‌های بین‌المللی را در مرحله هنجارسازی متوقف کرده است و مانع تدوین و اجرای کنوانسیون‌ها یا معاهداتی در سطح بین‌المللی برای تأمین امنیت عرصه نوظهور سایبری شده است.

در این کتاب، عملکرد سایبری ارکان و اجزای سازمان ملل را بررسی کردیم:

شاید مهم‌ترین بخش سازمان ملل که در حوزه فضای سایبر ورود کرده است، کمیته اول مجمع عمومی باشد که مأموریت خلع سلاح و امنیت بین‌الملل را یدک می‌کشد. عملکرد این کمیته موجب شکل‌گیری جریانی شده است که می‌توان آن را جریان امنیتی فضای سایبر نامید. منظور از جریان سایبری این است که جهان و مخصوصاً دولت‌ها چه نگاهی به خطرها و مضرات فضای سایبر داشته و آن را بستر چه تهدیداتی می‌دانند و به تبع آن، چه سیاست‌ها، راهبردها و راهکارهایی برای مقابله با این خطرها و تهدیدات اتخاذ و اجرا می‌کنند. جریان امنیتی مؤید این است که فضای سایبر این قابلیت را دارد که صلح و امنیت جهان را به مخاطره اندازد. بنابراین این نگاه بر این باور است که فضای سایبر می‌تواند در جهت مخالف اهداف مربوط به تقویت ثبات و امنیت بین‌المللی باشد. از این منظر، تأمین امنیت فضای سایبر در چهارچوب امنیت بین‌المللی تعریف می‌شود. یعنی امنیت فضای سایبر جزء جداناپذیر امنیت بین‌المللی است.

دولت روسیه در سال ۱۹۹۸ اولین قطعنامه را در ارتباط با تأمین امنیت فضای سایبر به کمیته اول مجمع عمومی ارائه کرد. عنوان کمیته اول یعنی کمیته خلع سلاح و امنیت بین‌الملل، خود

مؤید آن است که این قطعنامه چه دیدگاهی به فضای سایبر دارد. ضمن اینکه محتوای قطعنامه نیز این دیدگاه را تأیید می‌کند. زیرا در این قطعنامه به قابلیت کاربرد نظامی فضای سایبر تصریح شده است.

این قطعنامه از سال ۱۹۹۸ تا کنون، هر سال به کمیته اول ارائه شده و پس از طی تشریفات خاص، به تصویب مجمع عمومی رسیده است. روند تصویب این قطعنامه و واکنش آمریکا در برابر آن در طول این سال‌ها، تاریخ پرفراز و نشیبی داشته است. این امر مؤید این واقعیت است که آنچه اولویت اول را برای بازیگر اصلی این حوزه یعنی آمریکا به خود اختصاص داده، منافع این دولت بوده است و نه تأمین امنیت فضای سایبر. تغییرات تاکتیکی آمریکا در اتخاذ موضع در برابر این قطعنامه در خلال این سال‌ها به خوبی نشان می‌دهد که این قطعنامه‌ها به جای اینکه به تأمین امنیت فضای سایبر کمک کند به تابعی از رقابت‌های پیدا و پنهان این کشور تبدیل شده است. به خاطر ناکارآمدی همین قطعنامه‌هاست که امنیت فضای سایبر از سال ۱۹۹۸ تا کنون هر سال در مقایسه با سال قبل وخیم تر شده است. رأی مخالف آمریکا به قطعنامه در برخی سال‌ها و یارگیری روسیه در ارائه قطعنامه در این سال‌ها، ورود و خروج‌های آمریکا در حمایت و یا عدم حمایت از این قطعنامه، همه گواه آن است که موضع آمریکا همیشه تابعی از منافع این کشور بوده که در بعضی سال‌ها ایجاب می‌کرده است که از قطعنامه حمایت کند و در برخی سال‌ها علیه قطعنامه موضع‌گیری کند.

این روند همچنان ادامه دارد و بعید به نظر می‌رسد که در آینده نیز چشم‌انداز روشنی برای تأمین امنیت فضای سایبر از قبل قطعنامه‌های کمیته اول بتوان تصویر کرد. چیزی که در عمل شاهد آن هستیم استقبال آمریکا از حرکت روزافزون فضای سایبر به سمت نظامی‌گری است که حاکی از عدم توفیق فعالیت‌های کمیته اول در این خصوص می‌باشد.

آنچه در سطور بالا ذکر شد مربوط به روند قطعنامه موسوم به قطعنامه امنیت سایبری است که روسیه از بدو امر پرچمدار آن در کمیته اول بوده است. نفس این امر، هرگز خوشایند آمریکا نبوده است؛ چرا که از دید آن‌ها، قطعنامه فضای سایبر که طراحی آن ریشه در این کشور دارد، نباید در دست دولت دیگری باشد. اما روس‌ها همیشه ابتکار عمل را در دست داشتند. همین

امر باعث گردید که روس‌ها با رونمایی از پیش‌نویس کنوانسیون امنیت سایبری در سال ۲۰۱۱، آمریکا را به‌تازده کنند. شگفتی آمریکایی‌ها با رونمایی روس‌ها از کردارنامه امنیت سایبری تکمیل شد. هر چند کنوانسیون پیشنهادی روسیه نتوانست توفیقی در عرصه بین‌المللی به‌دست آورد، اما روس‌ها توانستند کردارنامه خود را در سال ۲۰۱۵ به‌روزرسانی کنند.

یکی از اقدامات آمریکا در سازمان ملل در جهت مقابله با اقدامات دیپلماتیک روسیه، ارائه قطعنامه فرهنگ جهانی امنیت سایبری به کمیته دوم بود که چندان توفیقی نیز به‌دست نیاورد. یکی دیگر از عرصه‌های تقابل منافع قدرت‌های سایبری، گروه کارشناسان دولتی می‌باشد. تاریخ تحولات این گروه دقیقاً مثل قطعنامه روسیه از رقابت‌های قدرت‌های عمده سایبری شکل گرفته است. از ناکامی گروه اول گرفته تا اقدامات گروه‌های بعدی که توفیقات اندکی داشته‌اند، انعکاسی از رقابت‌های سایبری صاحبان اصلی آن را به نمایش می‌گذارد.

دستاوردهای این گروه هیچ‌سختی با اوضاع رو به وخامت فضای سایبر ندارد. تشکیل گروه‌های مختلف و متوالی، بدون یک دستاورد مشخص و قابل توجه، موجب شد که در سال ۲۰۱۷ این گروه‌ها دوباره با شکست مواجه گردد.

کوچ گروه کارشناسان دولتی (G.G.E) از قطعنامه روسیه به قطعنامه آمریکا و تشکیل اولین گروه کاری باز (O.E.W.G) تحت قطعنامه روسیه در سال ۲۰۱۸ رقابت بین صاحبان قدرت سایبری را پیچیده‌تر کرد. آنچه تا سال ۲۰۲۰ شاهد آن هستیم این است که اصالت و اهمیت با کدام گروه است!

بعد از نگاه امنیتی به فضای سایبر، نگاه اقتصادی به فضای سایبر همان‌گونه که از عنوانش پیداست، نگاهی اقتصادمحور است نه امنیت‌محور. جریان اقتصادی نگران تخلفات و جرایم مالی و اقتصادی در بستر فضای سایبر است. بنابراین اقدامات این جریان نیز درصدد مقابله با این نوع جرایم و تخلفات است.

سکاندار این جریان که در کمیته سوم مجمع عمومی متمرکز است، دولت آمریکاست. دو سال بعد از اینکه روسیه ابتکار عمل را در کمیته اول به‌دست گرفت، ایالات متحده نیز سعی کرد این عقب‌ماندگی حقوقی دیپلماتیک را در کمیته سوم با ارائه قطعنامه مقابله با جرایم اقتصادی

سایبری جبران نماید.

در کمیته دوم نیز تحرکاتی از طرف کشورهای در حال توسعه با ارائه قطعنامه‌ای تحت عنوان فناوری اطلاعات و ارتباطات صورت گرفت که نوعاً مطالبه‌گر بود و هدف آن رفع شکاف دیجیتالی بین کشورهای پیشرو و در حال توسعه بود.

اما مهم‌ترین نکته در حوزه جرایم سایبری این است که تنها کنوانسیون حوزه سایبر با محوریت جرایم سایبری در قالب شورای اروپا در حال اجراست. هر چند این کنوانسیون خارج از سازمان ملل تصویب و اجرا شده ولی به خاطر همین ویژگی‌های انحصاری، حائز اهمیت فراوان است. به طوری که حتی برخی کشورها خارج از قلمرو شورای اروپا نیز به این کنوانسیون ملحق شده‌اند. البته عکس این موضوع نیز صادق است. به طوری که روسیه با وجود عضویت در شورای اروپا، تنها کشوری است که این کنوانسیون را امضاء نکرده است که دلایل آن نیز بررسی گردید.

اما آنچه اروپا را در سال ۲۰۱۷ دچار بهت و حیرت کرد، رونمایی روسیه از پیش‌نویس کنوانسیون جرایم سایبری می‌باشد. روسیه که در سال ۲۰۱۱ با رونمایی از پیش‌نویس کنوانسیون امنیت سایبری، آمریکا را دچار شگفتی کرده بود، در سال ۲۰۱۷ نیز با رونمایی از پیش‌نویس کنوانسیون جرایم سایبری، اروپا را شگفت‌زده کرد. روسیه که تا دیروز برای امضای کنوانسیون بوداپست تحت فشار بود، امروز پیش‌نویس خود را مطرح کرده و همه کشورها را برای حمایت از آن فرا می‌خواند. پیش‌نویس روسیه، فرصتی برای سایر کشورها نیز تلقی می‌گردد؛ چرا که قدرت چانه‌زنی آن‌ها را برای الحاق به هر یک از دو کنوانسیون بوداپست یا روسیه یا حتی ابتکار ارائه پیش‌نویس کنوانسیون سوم افزایش داده است. بی‌جهت نیست که کشورهای اروپایی که تا دیروز حاضر نبودند بعد از ۱۵ سال، کنوانسیون خود را بازنگری کنند، امروزه صحبت از این موضوع به میان می‌آورد و ادبیات تحکم‌آمیز دیروز برای الحاق به کنوانسیون را به ادبیات نرم خواهش و تمنا تبدیل کرده‌اند. روسیه در قطعنامه سال ۲۰۱۹ کمیته سوم با پیشنهاد تشکیل کمیته کارشناسان درباره شکل‌گیری کنوانسیون جرایم سایبری، گام بلندی برداشت که بر خلاف خوشایند شورای اروپا بود. واکنش‌های هیجانی و غیر حقوقی غرب در مقابل اقدامات و ابتکارات حقوقی و دیپلماتیک روسیه حاکی از تشدید نگرانی آن‌هاست. شایسته است از فرصت به‌وجود آمده، در راستای گنجاندن

ملاحظات سایبری کشورمان در این پیش‌نویس، حداکثر استفاده را به عمل آورد. در خصوص عملکرد شورای حقوق بشر و سایر قطعنامه‌های حقوق بشری نیز باید گفت: حقوق بشر که فی‌نفسه، ترکیبی زیبا برای شأن والای انسانی محسوب می‌شود به خاطر استفاده‌های ابزاری از سوی جوامع غربی، به عبارتی اشمئزاز‌آور بدل شده است که از آن به‌عنوان اهرمی علیه دولت‌ها و ملت‌های مستقل استفاده می‌شود. فضای سایبر نیز از این دوگانگی غربی‌ها مصون نمانده است.

افشاگری‌های اسنودن از سال ۲۰۱۳ به بعد نشان داد که دولت آمریکا برای هیچ یک از موازین حقوق بشری در فضای سایبر احترام و تعهدی قائل نیست.

فعالیت‌های شورای اقتصادی و اجتماعی سازمان ملل نیز در حوزه جرایم اقتصادی مثل کلاهبرداری، سوءاستفاده مجرمانه و جعل هویت، حائز اهمیت است. در حوزه حکمرانی نیز نمی‌توان نتایج اجلاس سران راجع به جامعه اطلاعاتی را نادیده گرفت.

مفهوم حکمرانی بر اینترنت بین کارشناسان و صاحب‌نظران، هنوز هم محل چالش است. فارغ از مفاهیم تئوریک، آنچه در عمل دیده می‌شود تسلط کامل دولت ایالات متحده بر تار و پود فضای سایبر در طول تاریخ این فناوری می‌باشد. اگر تعریف حکمرانی بر اینترنت را در مفهوم مضیق آن، به امور فنی محدود کنیم، این حکمرانی از بدو امر در دست شرکت آمریکایی آیکان بوده است. اگر مفهوم موسع را در نظر بگیریم و سیاستگذاری بر اینترنت را تعریف حکمرانی بر اینترنت بدانیم، باز باید گفت که مشارکت دولت‌های ملی در این امر، تاکنون تشریفاتی بوده است و دولت ایالات متحده به انحای مختلف سعی نموده است مانع مشارکت دولت‌ها در اداره جهانی اینترنت شود. آمریکا با شعار عوام‌فریبانه مبارزه با اعمال دیکتاتوری دولت‌ها بر فضای سایبر، در عمل، انحصار این حکمرانی را برای خود حفظ کرده است.

آنچه در تاریخ حکمرانی بر اینترنت شاهدیم، تلاش‌های ملی، منطقه‌ای و بین‌المللی علیه انحصار حکمرانی آمریکا بر فضای سایبر است که این تلاش‌ها به خاطر کارشکنی‌های دولت ایالات متحده، اگر نگوییم به شکست کامل منجر شده، اما به طور حتم می‌توان ادعا کرد که نتایج حداقلی در پی داشته است.

مهم‌ترین تلاش‌های صورت گرفته در این خصوص به اجلاس سران جامعه اطلاعاتی برمی‌گردد که طی دو مرحله به این موضوع ورود کرد و باوجود پیشرفت‌های اعلامی، در عمل دستاورد چندانی حاصل نشد. مجمع راهبری اینترنت، مهم‌ترین خروجی این تلاش‌ها بوده است که این مجمع در عمل به یک گردهمایی بی‌مصرف تبدیل شده است و تلاش‌ها برای کارآمد کردن آن، به نتیجه‌ای نرسیده است، به‌طوری که ادامه حیات آن با وضعیت فعلی، محل ابهام است و نباید منتظر خروجی قابل توجهی از این مجمع بود.

بعد از افشاگری‌های اسنودن در سال ۲۰۱۳ بود که هجمه جهانی علیه انحصار حکمرانی آمریکا دوباره شروع شد، به‌طوری که این دولت با یک ترفند تاکتیکی و طی یک عقب‌نشینی ظاهری اعلام کرد که به نظارت خود بر آیکان خاتمه خواهد داد و آن را به همه ذی‌نفعان این حوزه خواهد سپرد. بعد از چند سال که روند این انتقال صورت گرفت آنچه در نهایت حاصل شد، مشارکت دولت‌ها نبود، بلکه مشاوره تصنعی و غیرالزام‌آور دولت‌ها خطاب به آیکان بود. در واقع آمریکا از این طریق به حکمرانی باطنی و واقعی خود، تحت پوشش مشارکت دولت‌ها، مشروعیت بخشید و این روند همچنان ادامه دارد.

عدم ورود دیوان بین‌المللی دادگستری نیز تا حد زیادی ناشی از عدم بسندگی ادله، صعوبت انتساب و نهایتاً سختی بار کردن مسئولیت بر مرتکبان می‌باشد که اینهمه ناشی از ویژگیهای خاص فضای سایبر است. اما ورود دیوان به این حوزه نوپدید در آینده امر غیر محتملی نیست.

ب. آینده‌نگری و پیش‌بینی روندهای آتی

بررسی سیر تاریخی و اوضاع کنونی مؤید این است که در آینده نزدیک نیز چشم‌انداز روشنی برای تأمین امنیت فضای سایبر وجود ندارد. بنابراین باید منتظر افزایش مخاطرات امنیتی در کلیه سطوح آن در آینده باشیم. این سخن بدین معنی است که هر چند تأمین امنیت فضای سایبر باید با مشارکت و تلاش کلیه کشورهای جهان باشد، اما در شرایط فعلی و حتی آتی، باید اقدامات ملی برای تأمین امنیت فضای سایبر در دستور کار قرار گیرد تا امنیت حداقلی در این خصوص محقق شود و نباید به انتظار تلاش‌های بین‌المللی نشست. بسیاری از کشورها نیز با

نامیدی از فعالیت‌های بین‌المللی، رأساً در این خصوص در حال تلاش‌اند. بررسی عملکرد شورای امنیت نشان می‌دهد که این شورا در آینده نزدیک با محوریت و بهانه مبارزه با تروریسم در فضای سایبر به این موضوع ورود جدی‌تری خواهد کرد. آنچه تاکنون شورای امنیت را تا حد زیادی از ورود به این مباحث بازداشته است، نبود کنوانسیون‌های مربوط به تروریسم سایبری، جنگ سایبری یا امنیت سایبری است. به عبارت دیگر، عنصر قانونی جهت ورود شورای امنیت وجود ندارد. اما پیشرفت روزافزون سند تالین که در مورد اعمال حقوق جنگ بر جنگ‌های سایبری است و ساخته و پرداخته سازمان ناتو می‌باشد و همچنین با عنایت به سایر روندهای بین‌المللی و دکترین‌های برخی کشورها از جمله دولت ایالات متحده که فضای سایبر را به‌عنوان عرصه پنجم نبرد (بعد از زمین، هوا، دریا و فضا) به رسمیت شناخته است، تدوین کنوانسیون جنگ سایبری و سایر کنوانسیون‌ها در آینده اجتناب‌ناپذیر است. بنابراین این احتمال وجود دارد که در آینده از بستر چنین کنوانسیون‌هایی، کشورهای مستقل، مورد اتهام‌هایی مثل تهدید صلح و نقض صلح و حمایت از تروریسم در فضای سایبر شوند و تدابیر شورای امنیتی علیه آن کشورها اتخاذ گردد. بنابراین شایسته است ضمن تعامل با کشورها و سازمان‌های همسو، مانع تفسیر موسع کشورهای غربی از حقوق تعامل نماید و در روندهای منطقه‌ای و فرامنطقه‌ای مشارکت مؤثری داشته باشد.

در حوزه جرایم سایبری نیز به نظر می‌رسد اقدامات روسیه در کمیته سوم تا سال ۲۰۳۰ به تدوین کنوانسیون مقابله با جرایم سایبری منجر شود که رقیب جدی برای کنوانسیون بوداپست به شمار خواهد رفت. از هم اکنون باید با دولت روسیه در کمیته مربوط تحت سازمان ملل تعامل جدی داشت و در روند تدوین کنوانسیون حضور مؤثر داشته باشیم، زیرا امکان تعامل ما با کنوانسیون بوداپست از اقبال حداقلی برخوردار است.

نقطه مهمی که دوباره باید بدان توجه کرد اینکه بر خلاف فقدان اراده بین صاحبان قدرت سایبری برای امنیت‌زایی و قاعده‌مندی فضای سایبری آنچه در مجموعه سازمان ملل و خارج از آن شاهدیم این است که دولت ایالات متحده و برخی دولت‌های دیگر به‌شدت در صدد نظامی کردن فضای سایبر می‌باشند. تدوین حقوق جنگ در سازمان ناتو (سند تالین) شروع شده

و آمریکا در صدد آن است که این موضوع را در گروه کارشناسان دولتی بگنجانند. به نظر می‌رسد که تدوین قواعد نظامی فضای سایبر بیش از قواعد سایر حوزه‌های سایبری تدوین شود. این موضوع هر چند جای تأسف دارد ولی یک واقعیت انکارناپذیر است که فضای سایبر به سمت عرصه نبرد در حرکت است.

جدول ۱۳: آینده روندهای حقوقی در محیط بین‌الملل

ادامه روند فعلی ←	عرفی شدن حقوق بین‌الملل سایبری (حقوق عرفی)
حرکت شتابنده به سمت نظام مند شدن ←	تدوین حقوق قراردادی (معاهده ای)
حرکت به سمت حقوق نرم ←	تدوین کردارنامه و عرفی شدن حقوق بین‌الملل سایبری

ج. توصیه‌های کارشناسی و اقدامات پیشنهادی برای:

اول: محیط داخلی

توصیه: تعریف و توسعه گفتمان حقوق بین‌الملل سایبری در داخل کشور
اقدامات: تأسیس، تثبیت و توسعه دانش حقوق بین‌الملل سایبری در داخل کشور در:

الف. جامعه علمی-دانشگاهی

۱. دایر کردن این رشته در دانشکده های حقوق دانشگاههای معتبر کشور؛
۲. راه‌اندازی مراکز پژوهشی و مطالعاتی، آموزشی و تحصیلات تکمیلی، متناسب با نیازهای دانشی در سطح ملی؛
۳. ایجاد وحدت رویه و گفتمان واحد در تعاریف و مفاهیم حقوق سایبری در سطح کلان ملی از طریق تهیه و تدوین دایرة المعارف مشترک بومی با هدف جلوگیری از تشتت و پراکندگی آرا

- و نظرها و تعاریف مربوط به حوزه سایبر و حقوق سایبری؛
۴. استفاده حداکثری از ظرفیت علمی (استادان و محققان) موجود در کشور در جهت تربیت نیروی متخصص جوان؛
۵. حمایت از جامعه علمی در انتشار خروجی علمی این افراد در قالب کتاب، مقاله، مصاحبه و نظایر آن؛
۶. صدور مجوز و راه اندازی نشریه تخصصی مربوط به حقوق بین الملل سایبری با رفع مشکلات مالی، اداری و اجرایی و حاکمیتی در کشور.

ب. بخش خصوصی

۱. بخش خصوصی خود به دو بخش اشخاص حقیقی و اشخاص حقوقی قابل تقسیم است. متأسفانه اشخاص حقوقی اعم از شرکت‌ها و مؤسسات در کشور ما قابل مقایسه با شرکت‌های غربی نیستند و باید تقویت شوند. شرکت‌های فراملی غربی به اندازه‌ای توسعه یافته‌اند که اقدام به تدوین کنوانسیون سایبری می‌نمایند. کنوانسیون دیجیتال ژنو یکی از همین موارد است. این پیش‌نویس توسط ۳۶ شرکت غربی که بیش از ۳۰ شرکت آمریکایی بودند تدوین شد. جالب است بدانیم که در این پیش‌نویس، شرکت‌ها خود را قربانی و دولت‌ها را متهم اعلام کرده‌اند و این یک بدعت و کودتا در حقوق بین‌الملل است؛
۲. شرکت‌های فناورانه ما در حوزه سایبر باید متوجه باشند که حوزه سایبر یکی از گرایش‌های حقوق بین‌الملل است و در حال قانونمند شدن می‌باشد؛
۳. شرکت‌های داخلی باید به اندازه‌ای توسعه یافته و قوی و بزرگ شوند که بتوانند در تدوین حقوق بین‌الملل سایبری در جهان مشارکت نمایند. لازمه این امر توسعه حقوقی شرکت‌ها نیست. بلکه توسعه فنی و افزایش قلمرو فعالیت آن‌ها در بعد فراملی است به نحوی که بتوانند در تراز شرکت‌های غربی عمل نمایند. بنابراین افزایش قدرت فنی شرکت‌های خصوصی به تأثیرگذاری آن‌ها در روند قانونگذاری بین‌المللی منجر می‌شود؛
۴. در مورد اشخاص حقیقی می‌توان به شخصیت‌های علمی داخلی اشاره کرد که وجهه جهانی

دارند. مثل قضاات بین‌المللی ایرانی یا دانشمندان حقوقی کشور در سطح جهان. آرای و نظرهای این اشخاص به‌عنوان منابع فرعی به توسعه حقوق بین‌الملل منجر می‌شود. در این راستا لازم است از استادان بنام کشور حمایت جدی به عمل آورد و مواضع حقوقی کشور را از زبان این افراد به گوش جهان رساند.

ج. دولت

ایجاد نظام جامع، کامل و فراگیر در سطح ملی جهت هم‌افزایی بین متولیان بخش‌های مختلف و تعریف و تعیین ماتریس وظایف مربوط، متناسب با مأموریت‌های ذاتی هر یک از وزارتخانه‌ها، سازمان‌ها و نهادهای ذی‌مدخل جهت مشارکت در روندها و تدوین و توسعه هنجاری سایبری.

دوم: محیط بین‌الملل

توصیه: اشراف دانشی به اسناد بین‌المللی و پایش فعالیت سازمان‌های بین‌المللی حوزه سایبر از منظر تهدید و فرصت اقدامات:

۱. استخراج فرصت‌ها و تهدیدات نهفته در معاهدات و کنوانسیون‌های بین‌المللی و منطقه‌ای موجود در حوزه سایبر و اتخاذ تدابیر لازم جهت بهره‌برداری از فرصت‌ها و رفع و دفع تهدیدات مندرج و مستتر در این اسناد؛

۲. کشور ما اگر در صدد الحاق به هر کنوانسیون یا معاهده سایبری باشد باید ملاحظات و مصالح خود را مورد نظر قرار دهد و عنداللزوم برای برخی مفاد کنوانسیون حق شرط قائل شود؛

۳. باید با کشورهای پیشرو در این حوزه تعامل و ملاحظات خود را مطرح کنیم و مشارکت فعال‌تری در روندهای بین‌المللی، روندسازی بین‌المللی و منطقه‌ای در حوزه سایبر داشته باشیم تا دیگران کنوانسیون را در غیاب ما تدوین نکنند و صرفاً برای امضاء و تصویب، جلوی ما نکنند؛

۴. رصد و پایش اقدامات، روندها، هنجارها و جریاناتی که به سمت تدوین کنوانسیون در حرکت‌اند؛ قدم بعدی، مشارکت مؤثر در این روندهای هنجارساز می‌باشد؛ از جمله این موارد می‌توان به

به روند هنجارسازی حاکم در کمیته اول، دوم و سوم مجمع عمومی سازمان ملل اشاره کرد؛
۵. ارائه پیش‌نویس کنوانسیون و معاهده سایبری به محیط بین‌الملل از طریق هم‌افزایی با کشورهای دوست و همسو. دستور کارسازی پیش‌نویس‌های ارائه شده از طرف ج.ا.ایران در حوزه فضای سایبر برای طرح در سازمان‌هایی مثل سازمان کشورهای اسلامی، اکو، سازمان همکاری شانگهای، و مانند آن در حوزه‌های مختلف سایبری؛

۶. میزبانی اجلاس‌های مهم بین‌المللی و منطقه‌ای در ابعاد مختلف سایبری با هدف تأثیرگذاری حداکثری در موضوعات مطرح شده در این اجلاس‌ها و همایش‌ها مانند (I.G.F) مجمع راهبری اینترنت باید در دستور کار قرر گیرد. عجیب است که کشوری مثل جمهوری آذربایجان که سه دهه از عمر آن می‌گذرد اجلاس (IGF) مجمع راهبری اینترنت را میزبانی کرده است ولی ما چنین اقدامی صورت نداده‌ایم و چنین برنامه‌ای نیز در دستور کار نداریم. مخصوصاً مشارکت بخش خصوصی، جامعه مدنی و جامعه فنی و دانشگاهی در این زمینه‌ها مورد توصیه است. زیرا این مجامع درصدد گفت‌وگو سازی هستند و مشارکت تمام ذی‌نفعان مفید خواهد بود. ظرفیت‌سازی در بخش خصوصی، مهم تر از حضور دولتی‌ها در چنین مجامعی است. این مجامع، بین دولتی و چندجانبه نیستند، بلکه غیر دولتی و چندذی‌نفعی هستند. هر چند ممکن است دولت‌ها هم به‌عنوان ذی‌نفع حضور داشته باشند؛

۷. ایجاد آزمایشگاه‌های جرم‌یابی سایبری (فارن‌زیک) در راستای تأمین منافع امنیتی سایبری کشور با نهادهای ذی‌ربط؛

۸. نقش‌آفرینی در تدوین و شکل‌گیری حقوق نرم سایبری اقدام دیگری است که باید مورد نظر قرار گیرد. نظر به اینکه عرصه بین دولتی در حال فاصله گرفتن از حقوق سخت و حرکت به سمت حقوق نرم است، متولیان امر نیز باید این موضوع را در دستور کار قرار دهند. موج فزاینده کردارنامه‌نویسی از سوی کشورهای مختلف که از مصادیق حقوق نرم است، مؤید این است که باید با کشورهای مختلف در زمینه کردارنامه‌نویسی تعامل کرد. ایجاد اعتمادبه‌نفس برای نگارش کردارنامه و تعامل سازنده برای ارائه بین‌المللی آن، بسیار مهم است. در این خصوص می‌توان

فهرست اهم منابع:

- 1) Anatolij A. Streltsov, International information security: description and legal aspects, United Nations Institute for Disarmament Research (UNIDIR), Geneva 2007.
- 2) Christopher A. Ford, the Trouble with Cyber Arms Control, The New Atlantis. A Journal of Technology & Society. Vol. 2010/29, p. 65
- 3) Christopher A. Ford, the Trouble with Cyber Arms Control, The New Atlantis. A Journal of Technology & Society. Vol. 2010/29, p. 65.
- 4) Clarke, Richard A. and Robert Knake. Cyber War : The Next Threat to National Security and What To Do About It. Ecco, April 2010.
- 5) CONVENTION on INTERNATIONAL INFORMATION SECURITY(CONCEPT) INTERNATIONAL MEETING of HIGH-RANKING OFFICIALS RESPONSIBLE for SECURITY MATTERS EKATERINBURG, RUSSIA, 22-21 SEPTEMBER 2011
- 6) Draft resolutions A/C. 59/2/L. 18 and A/C. 59/2/L. 32
- 7) Finmore and Sikkink, Op. cit. , p. 900-899; and Ann Florini, «The Evlution of International Norms», International Studies Quarterly, Vol. 40. No. 3, September 1996, pp. 389-363.
- 8) Georg Sorensen, Changes in Statehood: The Transformation of International Relations, London: Palgrave, 2001,
- 9) Guest Blogger. The UN GGE on Cybersecurity: What is the UN's role? April 2015 ,15
- 10) Guest Blogger. The UN GGE on Cybersecurity: What is the UN's role? April 2015 ,15
- 11) Hiro Katsumata, «Teaching and Learning of Norms» in, International Conference on Civic Education and Research, New Orleans, November 2003 ,18-16.
- 12) <http://104.129.85.209/search?Q=cache:ouamzp.kmmcj:law.anu.an/cip/lectures%seminars/>
- 13) <http://bcode.ir/post/147>
- 14) http://beta.did.ir/document/index_fa.asp
- 15) <http://blog.internetgovernance.org/pdf/UN-infosec-code.pdf>.
- 16) <http://brazil.usembassy.gov/statementusgdeletionnetmundial.html>.
- 17) <http://donya-e-eqtasad.com/SiteKhan/748655>

- 18) <http://energycommerce.house.gov/hearings/hearingdetail.aspx?NewsID=9543>
- 19) <http://files.wcitleaks.org/public/Merged20%UAE20081212%.pdf>
- 20) <http://hamshahrionline.ir/details/81342>
- 21) <http://igfwatch.org/discussion-board/indias-proposal-for-a-un-committee-for-internet-related-policies-cirp>
- 22) <http://middleeastpress.com/blog>
- 23) <http://netmundial.br/wp-content/uploads/04/2014/NETmundial-Multistakeholder-Document.pdf>
- 24) <http://old.tabrizebidar.ir/news/34323>
- 25) <http://rapporteuronline.com/fa/news-details/3445/>
- 26) <http://regmedia.co.uk/04/02/2015/un-internet-security13-jan15.pdf>
- 27) <http://unpan3.un.org/wsis10/GA-High-Level-Meeting>
- 28) <http://whoswholegal.com/news/features/article/31013>
- 29) <http://workspace.unpan.org/sites/Internet/Documents/UNPAN95318.pdf>
- 30) http://www.bashgah.net/fa/content/print_version/44605 (Tue Feb 2017 04:55:18 14)
- 31) http://www.culturalivre.org.br/artigos/IBSA_recommendations_Internet_Governance.pdf
- 32) <http://www.entekhab.ir/fa/news/172376/>
- 33) <http://www.g-20g8.com/g-8g20/g8/english/live/news/renewed-commitment-for-freedom-and-democracy.1314.html>
- 34) <http://www.icann.org/en/news/announcements/announcement07-oct-13>
- 35) <http://www.ifla.org/node/7406>
- 36) <http://www.intgovforum.org/multilingual/content/about-igf>
- 37) <http://www.itis-ev.de/infosecur>
- 38) http://www.itu.int/dms_pub/itu-s/md/03/wsis/c/S-03WSIS-C0006-!PDF-E.pdf
- 39) <http://www.itu.int/en/wcit12-/Documents/final-acts-wcit12-.pdf>
- 40) <http://www.itu.int/wsis/docs2/pc3/html/off5/index.html>
- 41) <http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions>
- 42) <http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions>
- 43) <http://www.oecd.org/dataoecd/48387430/12/33.pdf>
- 44) <http://www.state.gov/e/rls/rmk/250719.htm>
- 45) <http://www.state.gov/r/pa/prs/ps/202037/12/2012.htm>
- 46) <http://www.state.gov/r/pa/prs/ps/233914/11/2014.htm>
- 47) <http://www.un.org/apps/news/story.asp?NewsID=#46780.WPImg3k2zIU> « General Assembly backs right to privacy in digital age»
- 48) <http://www.un.org/apps/news/story.asp?NewsID=#46780.WPImg3k2zIU> « General Assembly backs right to privacy in digital age»
- 49) <http://www.un.org/pga/16/12/2015/70/press-release-wsis-10outcome/>
- 50) <http://www.unodc.org/unodc/commissions/CCPCJ/>
- 51) http://www3.weforum.org/docs/WEF_1NetmundialInitiativeBrief.pdf
- 52) <https://ccdcoe.org/sites/default/files/documents/OSCE131203->

- 53) <https://ccdcoe.org/un.html>
- 54) <https://www.icann.org/en/system/files/files/iana-stewardship-transition-proposal-resolutions-exceprts10-mar-16en.pdf>.
- 55) <https://www.icann.org/resources/reviews/specific-reviews>.
- 56) <https://www.ip-watch.org/08/01/2014/un-general-assembly-adopts-resolution-on-privacy-and-surveillance/>
- 57) <https://www.ip-watch.org/08/01/2014/un-general-assembly-adopts-resolution-on-privacy-and-surveillance/>
- 58) <https://www.lawfareblog.com/icann-and-iana-transition-proceed-caution>
- 59) https://www.ntia.doc.gov/files/ntia/publications/amendment_33.pdf.
- 60) <https://www.ntia.doc.gov/report/2016/iana-stewardship-transition-proposal-assessment-report>.
- 61) <https://www.rond.ir/News/694/-icann>
- 62) Jeffrey T. Checkel, «Sanctions, Social Learning and Institutions: Explaining State Compliance with the Norms of the European Human Rights Regime», ARENA Working Papers, Series: 1999) ,3 .15).
- 63) Lennard G. Kruger. Specialist in Science and Technology Policy Internet Governance and the Domain Name System: Issues for Congress. . November 2016 ,18. P. 13
- 64) Lennard G. Kruger. Internet Governance and the Domain Name System: Issues for Congress. November 2016 ,18
- 65) Markoff, John and Andrew E. Kramer. In Shift, U. S. Talks to Russia on Internet Security. The New York Times. 13 December 2009.
- 66) Milton Mueller, John Mathiason, and Hans Klein, “The Internet and Global Governance: Principles and Norms for a New Regime,” Global Governance, vol. 2007) 13),
- 67) Mortha Finnemore and Kathryn Sikkink, «International Norms Dynamics and Political Change», International Organizations, Vol. 52, No. 4. Autumn, 1998, pp. 917-887.
- 68) NATIONAL SECURITY STRATEGY. FEBRUARY 5 01 2. THE WHITE HOUSE WASHINGTON
- 69) Nye Jr, Joseph S. Cyberpower. Paper. Cambridge, Mass. : Harvard Belfer Center for Science and International Affairs May 2010.
- 70) Office of the Press Secretary, The White House, “U. S. -Russian Cooperation on Information and Communications Technology Security,” June 2013 ,17. For a discussion of confidence-building measures in cyberspace, see UNIDIR, “Cyber Index,”
- 71) Rajeswari Pillai Rajagopalan and Daniel A. Porras (Editors) . AWAITING LAUNCH: PERSPECTIVES ON THE DRAFT ICOC FOR OUTER SPACE ACTIVITIES) www.orfonline.org/
- 72) Ronald Deibert, Tracking the emerging arms race in cyberspace, Bulletin of the Atomic Scientists, Vol. 67, Issue 2011 ,1, p. 6.
- 73) Shaun Riordan Cyber Diplomacy vs. Digital Diplomacy: A Terminological Distinction May ,12 2016
- 74) Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Armed Services Committee. James R. Clapper Director of National Intelligence February 2015 ,26
- 75) Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Armed Services Committee. James R. Clapper Director of National Intelligence February 2015 ,26
- 76) Streltsov, A. A. International information security: description and legal aspects. Disarmament Forum 2007) 3) Last accessed 12 October 2011. <http://www.unidir.org/pdf/articles/pdf-art2642.pdf>

- 77) The Cyber Index. International Security Trends and Realities. UNIDIR2013
- 78) Tim Maurer. Cyber security in a Complex Environment. 2016/2
- 79) Tim Maurer». Cyber Norm Emergence at the United Nations– An Analysis of the UN’s Activities Regarding Cyber-security. September 80 2011) Touré. Dr Hamadoun I. . Secretary-General of the International Telecommunication Union and the Permanent Monitoring Panel on Information Security World Federation of Scientists January 2011
- 81) Toure, Hamadoun I. Cyberspace and the Threat of Cyberwar, in The Quest for Cyber Peace. International Telecommunication Union and World Federation of Scientists, January 201
- 82) UN General Assembly A/529/57/Add. 3
- 83) UN General Assembly. A/RES/32/58
- 84) UN General Assembly. A/RES/8.45/60 December 2005
- 85) UN General Assembly. A/RES/24/66.
- 86) UN General Assembly A/RES/29.19/56 November 2001
- 87) UN General Assembly A/RES/22.53/57 November 2002 & A/RES/8.32/58 December 2003
- 88) UN General Assembly A/RES/41/65
- 89) UN General Assembly. A/RES/3.61/59 December 2004. paragraph4
- 90) UN Doc 9 November 2006. A/389/61
- 91) UN Doc A /RES/2.37/63 December 2008
- 92) UN Doc A/558/56/Add. 13 -3 December 2001
- 93) UN Doc A/529/57/Add. 12- 3 December 2002
- 94) UN Doc A/385/63
- 95) UN Doc A/386/64
- 96) UN Doc A/201/65
- 97) UN Doc A/405/65
- 98) UN Doc A/359/66. International code of conduct for information security
- 99) UN Doc A/407/66. Consideration of draft resolution A/C. 66/1/L. 30
- 100) UN Doc A/406/68
- 101) UN Doc A/98/68
- 102) UN Doc A/13 723/69 January 2015
- 103) UN Doc A/455/70
- 104) UN Doc A/455/70 Consideration of draft resolution A/C. 70/1/L. 45
- 105) UN Doc A/CONF. 222/L. 13 - 6March 2015
- 106) UN Doc A/HRC/RES/16 - 8/20 July 2012
- 107) UN Doc A/HRC/RES/24 - 2/23 June 2013
- 108) UN Doc A/HRC/RES/14 - 13/26 July 2014
- 109) UN Doc A/HRC/RES/20 -7/31 April 2016
- 110) UN Doc A/RES 166/69 of 18 December 2014
- 111) UN Doc A/RES/ 28/55 of 20 November 2000
- 112) UN Doc A/RES/ 19/56 of 29 November 2001
- 113) UN Doc A/RES/ 53/57 of 22 November 2002
- 114) UN Doc A/RES/ 32/58 of 8 December 2003
- 115) UN Doc A/RES/ 61/59 of 3 December 2004

- 116) UN Doc A/Res/603/55
- 117) UN Doc A/RES/31 -183/56 January 2002
- 118) UN Doc A/RES/11- 220/59 February 2005
- 119) UN Doc A/RES/27 - 252/60 April 120 2006) UN Doc A/RES/8 .45/60 December 2005
- 121) UN Doc A/RES/6 .54/61 December 2006
- 122) UN Doc A/RES/5 . 17/62 December 2007
- 123) UN Doc A/RES/31 -182/62 January 2008
- 124) UN Doc A/RES/28 - 202/63 January 2009
- 125) UN Doc A/RES/23 .232/65 March 2011
- 126) UN Doc A/RES/4 -184/70 February 2016
- 127) UN Doc resolution 121/45 of 14 December 1990,
- 128) UN Doc resolutions A/RES/ 49/54 of 1 December 1999
- 129) UN Doc 6 November 2008. A/385/63
- 130) UN Doc 8 November 2007. A/386/62
- 131) UN Doc A/16 59/55 November 2000
- 132) UN DOC - A/48/57
- 133) UN Doc A/202/60
- 134) UN Doc A/452/60
- 135) UN Doc A/40/67
- 136) UN Doc A/15 -469/70 December 2015
- 137) UN Doc A/C. 60/1/L. 29
- 138) UN Doc A/HRC/RES/1 - 16/28 April 2015
- 139) UN Doc A/HRC/RES/18 -13/32 July 2016
- 140) UN Doc A/RES/32/58
- 141) UN Doc A/RES/45/60
- 142) UN Doc A/RES/18 .167/68 December 2013
- 143) UN Doc 4 December 1998 . A/RES/70/53
- 144) UN Doc A/558/56/Add. 13 -3 December 2001
- 145) UN Doc A/529/57/Add. 12 -3 December 2002
- 146) UN Doc A/16 -480/59 December 2004
- 147) UN Doc A/202/60& A/201/65& A/98/68& A/174/70
- 148) UN Doc A/19 -416/62 November 2007
- 149) UN Doc A/19 -416/62 November 2007
- 150) UN Doc A/2 -411/63 December 2008
- 151) UN Doc A/386/64. Consideration of draft resolution A/C. 64/1/L. 39
- 152) UN Doc A/386/64. Consideration of draft resolution A/C. 64/1/L. 39
- 153) UN Doc A/10 -417/64 December 2009
- 154) UN Doc A/201/65. Letter of transmittal
- 155) UN Doc A/405/65. Consideration of draft resolution A/C. 65/1/L. 37
- 156) UN Doc A/23 -433/65 November 2010
- 157) UN Doc A/35/66
- 158) UN Doc A/13 -437/66 December 2011

- 159) UN Doc A/14 -434/67 December 2012
 160) UN Doc A/13 -435/68 December 2013
 161) UN Doc A/CONF. 222/L. 13- 61March 2015
 162) UN Doc A/RES 166/69 of 18 December 2014
 163) UN Doc A/RES/63/55
 164) UN Doc A/RES/31 -183/56 January 2002
 165) UN Doc A/RES/27 - 252/60 April 2006
 166) UN Doc A/RES/28 - 202/63 January 2009
 167) UN Doc A/RES/2 -141/65 February 2011
 168) UN Doc A/RES/23 .232/65 March 2011
 169) UN Doc A/RES/6 -184/66 February 2012
 170) UN Doc A/RES/5 -195/67 February 2013
 171) UN Doc A/RES/15 -198/68 January 2014
 172) UN Doc A/RES/21 - 204/69 January 2015
 173) UN Doc A/RES/4 -184/70 February 2016
 174) UN Doc A/RES/25 .199/71 January 2017
 175) UN Doc A/576/53. Consideration of draft resolution A/C. 53/1/L. 17 and Rev. 1
 176) UN Doc A/558/54. Consideration of draft resolution A/C. 54/1/L. 4
 177) UN Doc A/558/56/Add. 13 -3 December 2001
 178) UN Doc A/529/57/Add. 12- 3 December 2002
 179) UN Doc A/454/59. Consideration of draft resolution A/C. 59/1/L. 2 and Rev. 1
 180) UN Doc A/RES/11- 220/59 February 2005
 181) UN Doc A/RES/25 .199/71 January 2017
 182) UN Doc, A/RES/23 ,237/70 December 2015
 183) UN Doc. A/22 ,174/70 July 2015
 184) UN DocA/554/55. Consideration of draft resolution A/C. 55/1/L. 6
 185) UN DocA/533/56. Consideration of draft resolution A/C. 56/1/L. 3 and Rev. 1
 186) UN DocA/505/57. Consideration of draft resolution A/C. 57/1/L. 1
 187) UN DocA/457/58. Consideration of draft resolution A/C. 58/1/L. 3
 188) UN ECOSOC E/65 :31/1994
 189) UN ECOSOC E/28/1999/Rev. 1
 190) UN ECOSOC E/28/2004
 191) UN ECOSOC E/30/2009
 192) UN ECOSOC E/30/2011
 193) UN ECOSOC E/CN. 2/2009/15 and Corr. 1
 194) UN ECOSOC resolution 26/2004
 195) UN ECOSOC resolution 22/2009
 196) UN ECOSOC resolution 18/2010
 197) UN ECOSOC resolution 8/43 in E/28/2000
 198) UN ECOSOC resolution 5/48 in E/28/2005
 199) UN General Assembly. A/201/65.
 200) UN General Assembly A/576/53. Consideration of draft resolution A/C. 53/1/L. 17 and Rev. 1

- 201) UN General Assembly A/558/54. Consideration of draft resolution A/C. 54/1/L. 4
- 202) UN General Assembly A/554/55. Consideration of draft resolution A/C. 55/1/L. 6
- 203) UN General Assembly A/593/55
- 204) UN General Assembly A/533/56. Consideration of draft resolution A/C. 56/1/L. 3 and Rev. 1
- 205) UN General Assembly A/574/56
- 206) UN General Assembly A/505/57. Consideration of draft resolution A/C. 57/1/L. 1
- 207) UN General Assembly A/529/57/Add. 3
- 208) UN General Assembly A/457/58. Consideration of draft resolution A/C. 58/1/L. 3
- 209) UN General Assembly A/481/58/Add. 2
- 210) UN General Assembly A/454/59. Consideration of draft resolution A/C. 59/1/L. 2 and Rev. 1
- 211) UN General Assembly A/RES/63/55
- 212) UN General Assembly A/RES/121/56
- 213) UN General Assembly A/RES/239/57
- 214) UN General Assembly A/RES/239/57; A/RES/199/58; A/RES/211/64.
- 215) UN General Assembly A/RES/45/60
- 216) UN General Assembly A/RES/230/65
- 217) UN General Assembly A/RES/S4/20-
- 218) UN General Assembly. A/452/60
- 219) UN General Assembly A/RES/288/60
- 220) UN ITU Global Strategic Report, 95 :2008
- 221) UN. General Assembly A/386/62
- 222) UN. General Assembly A/385/63
- 223) UN. General Assembly. A/389/61
- 224) UN. General Assembly A/202/60
- 225) UN. General Assembly A/452/60
- 226) UN. General Assembly A/C. 60/1/L. 29
- 227) UN. General Assembly A/RES/32/58
- 228) <https://www.un.org/disarmament/sg-agenda/en>
- 229) <https://dppa.un.org/en>
- 230) <https://peacemaker.un.org/digitaltoolkit>
- 231) <https://www.worldbank.org/en/topic/financialsector/brief/cybersecurity-cyber-risk-and-financial-sector-regulation-and-supervision>
- 232) <https://etradeforall.org/development-solution/world-bank-combatting-cybercrime-tools-capacity-building-tackle-cybercrime/>
- 233) (<https://gtldcomment.icann.org/comments-feedback/applicationcomment/login>).
- 234) <https://www.unocha.org/publication/policy-briefs-studies/humanitarianism-age-cyber-warfare>
- 235) <https://centre.humdata.org/>
- 236) [https://www.unog.ch/80256EE600585943/\(httpPages\)/BF18ABFEFE5D344DC1256F3100311CE9?OpenDocument](https://www.unog.ch/80256EE600585943/(httpPages)/BF18ABFEFE5D344DC1256F3100311CE9?OpenDocument)
- 237) <https://www.icj-cij.org/en>

اهم اسناد

1. WSIS. TUNIS COMMITMENT
2. WSIS. TUNIS AGENDA FOR THE INFORMATION SOCIETY
3. Declaration of Principles Building the Information Society: a global challenge in the new Millennium
4. WSIS Action Lines & WSIS Plan of Action
5. I.T.U THE QUEST FOR CYBER PEACE
6. ITU Global Cyber security Agenda (GCA) High-Level Experts Group (HLEG)
7. Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society
8. Countries adopt new plan to utilize Internet and information technologies in implementation of new Sustainable Development Agenda
9. THE ADVANTAGES OF ADHERENCE TO THE WIPO COPYRIGHT TREATY (WCT) AND THE WIPO PERFORMANCES AND PHONOGRAMS TREATY (WPPT)
10. Berne Convention for the Protection of Literary and Artistic Works
11. THE WIPO COPYRIGHT TREATY (WCT) AND THE WIPO PERFORMANCES AND PHONOGRAMS TREATY (WPPT)
12. WIPO Copyright Treaty
13. Resolution 22/2009 International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity related-crime
14. Resolution 26/2004 International cooperation in the prevention ,investigation, prosecution and punishment of fraud ,the criminal misuse and falsification of identity and related crimes
15. Draft resolution II (Adopted by ECOSOC resolution 20/2007) International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime
16. E COSOC r e s o l u t i o n 2 2 / 9 0 2 o f 3 J u l y 9 0 2 International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime
17. ECOSOC resolution 39/2013 of 25 July 2013 International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime
18. ECOSOC Resolution 42/2004 Sale of internationally controlled licit drugs to individuals via the Internet
19. The World Bank Group FINANCE, COMPETITIVENESS & INNOVATION INSIGHT | FINANCIAL STABILITY & INTEGRITY
20. The World Bank Group Cyber security, Cyber Risk and Financial Sector Regulation and Supervision
21. The World Bank: Combatting Cybercrime – Tools and capacity building to tackle cybercrime
22. WORLD HEALTH ORGANIZATION SIXTY-SIXTH WORLD HEALTH ASSEMBLY
23. The Health Internet
24. SIXTY-SIXTH WORLD HEALTH ASSEMBLY WHA66.24 Agenda item 27 17.5 May 2013 eHealth standardization and interoperability
25. Report. Cyber security and digital trade: What role for international trade rules?
26. Cyber security Threats and the WTO National Security Exceptions
26. Guide to Information Technology Security WMO-No. 1115

27. ECOSOC Resolution 46/2006 Follow-up to the World Summit on the Information Society and review of the Commission on Science and Technology for Development
28. ECOSOC Resolution 3/2008 Assessment of the progress made in the implementation of and follow-up to the outcomes of the World Summit on the Information Society
29. draft resolution Promoting technical assistance and capacity-building to strengthen national measures and international cooperation to combat cybercrime including information sharing
30. Draft resolution for adoption by the General Assembly. Countering child sexual exploitation and sexual abuse online
31. Resolution Prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children
32. Resolution 4/26 Strengthening international cooperation to combat cybercrime
33. Resolution 7/20 Promotion of activities relating to combating cybercrime, including technical assistance and capacity-building
34. Resolution 7/22 Strengthening international cooperation to combat cybercrime
35. Resolution 8/22 Promoting technical assistance and capacity-building to strengthen national measures and international cooperation against cybercrime
36. Science, technology and innovation for development 22/2017.
37. Resolution 5/48 Strengthening international cooperation in order to prevent the use of the Internet to commit drug related crime
38. Resolution 11/50 International cooperation in preventing the illegal distribution of internationally controlled licit substances via the Internet
39. RECOMMENDATION CONCERNING THE PROMOTION AND USE OF MULTILINGUALISM AND UNIVERSAL ACCESS TO CYBERSPACE
40. Draft Code of Ethics for the Information Society. UNESCO
41. RECOMMENDATION CONCERNING THE PROMOTION AND USE OF MULTILINGUALISM AND UNIVERSAL ACCESS TO CYBERSPACE . UNESCO
42. SECURING OUR COMMON FUTURE Office for Disarmament Affairs New York, 2018 An Agenda for Disarmament
43. SECRETARY-GENERAL'S STRATEGY ON NEW TECHNOLOGIES
44. Private Sector Engagement in Responding to the Use of the Internet and ICT for Terrorist Purposes
45. UNITED NATIONS SECURITY COUNCIL COUNTER-TERRORISM COMMITTEE EXECUTIVE DIRECTORATE (CTED) INFORMATION AND COMMUNICATIONS TECHNOLOGIES (ICT)
46. The United Nations Global Counter-Terrorism Strategy. Resolution adopted by the General Assembly on 8 September 2006
47. The promotion, protection and enjoyment of human rights on the Internet
48. The role of freedom of opinion and expression in women's empowerment
49. The right to privacy in the digital age
50. Rights of the child: information and communications technologies and child sexual exploitation
51. Advancing responsible State behaviour in cyberspace in the context of international security
52. Developments in the field of information and telecommunications in the context of international security

53. The role of science and technology in the context of international security, disarmament and other related fields
54. International code of conduct for information security
55. CONVENTION on INTERNATIONAL INFORMATION SECURITY (CONCEPT)
56. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security Report of the Secretary-General
57. Science and technology for development
58. Tunisia: draft resolution World Summit on the Information Society Creation of a global culture of cyber security and the protection of critical information infrastructures
59. Modalities for the overall review by the General Assembly of the implementation of the outcomes of the World Summit on the Information Society
60. Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society
61. Strengthening the United Nations Crime Prevention and Criminal Justice Program, in particular its technical cooperation capacity
62. Crime prevention and criminal justice Report of the Third Committee
63. Combating the criminal misuse of information technologies
64. Countering the use of information and communications technologies for criminal purposes
65. Draft United Nations Convention on Cooperation in Combating Cybercrime
66. Responsibility of States for Internationally Wrongful Acts 2001
67. Report of the Intergovernmental Group of Experts on E-commerce and the Digital Economy on its first session
68. Working Group on Measuring E-commerce and the Digital Economy
69. International Law and State Behavior in Cyberspace Series Compendium of Regional Seminars.
- UNIDIR RESOURCES



مرکز ملی فضای مجازی
انتشارات پژوهشگاه فضای مجازی

ماهیت جهان گستر فضای سایبر موجب شده است که تهدیدات، چالش‌ها و مخاطرات آن نیز ماهیت بین‌المللی پیدا کند. در نتیجه طبیعی است که راهکارها و راهبردهای کلان مقابله با معضلات فضای سایبر نیز باید جهانی باشد. سازمان ملل متحد به عنوان سازمانی با مأموریت جهانی و صلاحیت عام الشمول، از دو دهه قبل به این موضوع توجه نموده و ابعاد مختلف فضای سایبر از جمله امنیت، حکمرانی، حقوق بشر، حریم خصوصی و جرم را در دستور کار خود قرار داده است. ویژگی‌های خاص فضای سایبر و رقابت‌های پیدا و پنهان قدرتهای بزرگ سایبری و نفوذ آنها در ارکان مختلف سازمان ملل، مانع از آن شده است که این سازمان در مأموریت جهانی خود برای نظام‌مند کردن فضای سایبر و قاعده‌مند کردن فعالیت در این فضا، توفیق چندانی داشته باشد. تکثر ذی‌نفعان، حکمرانی برخی شرکت‌های داخلی در گستره بین‌المللی، تحدید و تضعیف نقش دولتها و فقدان نقش‌آفرینی واقعی جامعه بین‌دولتی در تدوین و توسعه حقوق بین‌الملل فضای سایبر از دیگر عوامل موثر در توسعه نیافتگی حقوق بین‌الملل فضای سایبر در بستر سازمان ملل می‌باشد.

قیمت: ؟