حکمرانی در عرصه پنجم

CYBERSPACE

گذار به دیپلماسی سایبری

عباس قنبری باغستان
عبدالحسین گلاندخری

حکمرانی در عرصهٔ پنجم: گذار به دیپلماسی سایبری

حکمرانی در عرصهٔ پنجم: گذار به دیپلماسی سایبری

عباس قنبری باغستان
عبدالحسین کلانتری

بهار ۱۴۰۰

سر شناسه	:	قنبری باغستان، عباس، ۱۳۵۷ -
عنوان و نام پدیدآور	:	حکمرانی در عرصه پنجم: گذار به دیپلماسی سایبری / نویسندگان عباس قنبری باغستان، عبدالحسین کلانتری
مشخصات نشر	:	تهران : پژوهشگاه فضای مجازی ، ۱۴۰۰
مشخصات ظاهری	:	۴۵۶ ص. : جدول. ؛ ۱۴×۲۱س م
شابک	:	۹۷۸-۶۲۲-۹۷۷۰۰-۶-۱
وضعیت فهرست نویسی	:	فیپا
یادداشت	:	کتابنامه
یادداشت	:	نمایه.
موضوع	:	فضای مجازی — جنبه های سیاسی
موضوع	:	Cyberspace -- Political aspects
موضوع	:	فضای مجازی — تدابیر ایمنی — سیاست دولت
موضوع	:	Cyberspace -- Security measures -- Government policy
موضوع	:	همکاری های بین المللی -- تدابیر ایمنی-- فضای مجازی
موضوع	:	International cooperation --Cyberspace -- Security measures
شناسه افزوده	:	کلانتری، عبدالحسین، ۱۳۵۶ -
شناسه افزوده	:	پژوهشگاه فضای مجازی
رده بندی کنگره	:	HM۸۵۱
رده بندی دیویی	:	۳۰۳/۴۸۳۴
شماره کتابشناسی ملی	:	۷۶۶۹۴۲۶
اطلاعات رکود کتابشناسی	:	فیپا

حکمرانی در عرصهٔ پنجم: گذار به دیپلماسی سایبری

نویسندگان: عباس قنبری باغستان (عضو هیئت علمی دانشگاه تهران)

و عبدالحسین کلانتری (عضو هیئت علمی دانشگاه تهران)

ویراستاران: فخرالسادات حیدری و راهله میلانی

صفحه‌آرا: سعیده رجبلو

چاپ نخست: ۱۴۰۰

شمارگان: ۱۰۰۰ نسخه

ویرایش، آماده‌سازی و صفحه‌آرایی متن: مژگان مهدوی

لیتوگرافی، چاپ و صحافی: چاپ بلوط

این کتاب با همکاری مرکز ملی فضای مجازی، دانشکدهٔ روابط بین‌الملل وزارت امور خارجه و ادارهٔ هماهنگی امور پژوهشی و نشر وزارت امور خارجه به چاپ رسیده است.

فهرست

پیش‌گفتار

عرصهٔ سایبری جدی‌ترین مسئله و چالش حکمرانی در ابعاد ملی، منطقه‌ای و بین‌المللی است و درست همانند دوران گذارهای حساس تاریخی، همچون تسخیر فضا، ساخت بمب هسته‌ای، جهانی‌سازی و ...، تمامی معادلات در نظم مستقر بین‌الملل را به چالش کشیده است. عرصهٔ سایبری پدیده‌ای چندوجهی است که به دلیل ماهیت پیچیده و شبکه‌ای، خصلت مرکزگریزی و کنترل‌ناپذیری و نیز ظهور بازیگران قدرتمند غیررسمی و بعضاً ناشناخته در آن، مستلزم نگاه حاکمیتی و فراتر رفتن از رویکردهای تک‌بُعدی و کلاسیک است.

در مطالعهٔ اسناد و متون سایبری و نیز تجارب کشورهای مختلف در مواجهه با چالش‌های سایبری، کشورهای مختلف بعضاً سه فاز متفاوت را تجربه کرده‌اند: ۱. فاز دفاعی، ۲. فاز تهاجمی و ۳. فاز دیپلماسی سایبری. عمدهٔ کشورهای جهان در سطوح مختلف، فازهای اول و دوم را تجربه کرده‌اند، با این حال تعداد قلیلی از کشورها توانسته‌اند با تبدیل این عرصه به فرصت، وارد فاز «دیپلماسی سایبری» به معنای استفاده از پتانسیل عرصهٔ سایبری برای ظرفیت‌سازی و اعتمادسازی با هدف پیشبرد اهداف و منافع ملی خود در عرصه‌های منطقه‌ای و بین‌المللی بشوند.

در بین کشورهایی که وارد فاز دیپلماسی سایبری شده‌اند، دو رویکرد عمده قابل شناسایی است: ۱. رویکرد غربی با محوریت آمریکا: ایالات متحده آمریکا اولین کشوری است که دیپلماسی سایبری خود را تدوین و به

عنوان سند ملی اعلام نمود. به دنبال آن بسیاری از کشورهای غربی، از جمله کشورهای اروپایی و نیز استرالیا و نیوزلند به پیروی از این کشور اسناد سایبری ملی خود را تدوین کردند و به تصویب رساندند. ۲. رویکرد شرقی با محوریت کشورهای روسیه و چین که به لحاظ اصول و مبانی تا حد بسیار زیادی در مقابل کشورهای غربی قرار دارد. این رویکرد عمدتاً از سوی کشورهای عضو سازمان همکاری شانگهای دنبال می‌شود. در این بین، برخی از کشورها همچون ژاپن از یک سو به دلیل نزدیکی ایدئولوژیک با کشورهای غربی و از سوی دیگر به دلیل واقع شدن در منطقهٔ شرق آسیا و در مجاورت کشورهایی همچون روسیه و چین، سعی کرده‌اند بر اساس منافع ملی خود رویکرد بینابینی را دنبال کنند.

فراتر از سطوح ملی، در عرصهٔ منطقه‌ای و بین‌المللی نیز موضوع دیپلماسی سایبری از اهمیت خاصی برخوردار بوده است. سازمان ملل متحد و به طور مشخص «گروه کارشناسان دولتی این سازمان» از اوایل سال ۲۰۰۰ میلادی با هدف پیگیری این موضوع تشکیل شده و تا کنون چندین نشست با حضور اکثریت اعضای این سازمان برگزار کرده و اسناد و خروجی‌های آن، در قالب اسناد رسمی، به مجمع عمومی سازمان ملل یا شورای امنیت این سازمان ارجاع شده است. اتحادیهٔ اروپا، سازمان ناتو، سازمان همکاری شانگهای، گروه هفت، گروه بیست، اتحادیهٔ کشورهای جنوب شرق آسیا (آسه‌آن) و ... از دیگر نهادها و سازمان‌های بین‌المللی هستند که در چارچوب منافع کشورهای عضو به این موضوع پرداخته‌اند.

با توجه به چندوجهی و چندذی‌نفعی بودن عرصهٔ سایبری، نکتهٔ حائز اهمیت ظهور بازیگران نوظهور در قالب سازمان‌ها و کمپانی‌های بزرگ آی‌تی و نیز نهادها و سازمان‌های مدنی است که غالباً در انواع دیپلماسی‌های کلاسیک جایگاه چندانی نداشتند. این بازیگران که به ویژه

نمایندگان بخش خصوصی محسوب می‌شوند، به دلیل تضاد منافع با دولت‌ها و منابع رسمی دارای اولویت‌های متفاوتی هستند و به همین دلیل نیز دایرهٔ اثرگذاری و بازیگری دولت‌ها در این عرصه را محدود و بیش از گذشته تنگ کرده‌اند. پلتفرم‌ها و غول‌های آی‌تی همچون گوگل، مایکروسافت، اپل و ... از جمله مهم‌ترین بازیگران قدرتمند عرصهٔ سایبری هستند که دایرهٔ اثرگذاری و قدرت بازیگری آن‌ها بعضاً از مجموع بسیاری از کشورهای کوچک و بزرگ بیشتر می‌باشد.

مطالعهٔ مبانی و اصول دیپلماسی سایبری کشورهایی که دارای اسناد رسمی دیپلماسی سایبری هستند، و نیز برآیند ارزیابی بیش از ۸۰ سند بین‌المللی و منطقه‌ای که در ارتباط با دیپلماسی سایبری تدوین و تصویب شده‌اند، نشان می‌دهد که مدیریت و هدایت این عرصه به سبک و سیاق دیپلماسی‌های کلاسیک امکان‌پذیر نیست. مواجهه با چالش‌های این حوزه و نیز مقابله با بازیگران ناشناسی که عمدتاً از طریق سازماندهی حملات تهاجمی همچون حمله به زیرساخت‌ها، جاسوسی سایبری، سرقت اطلاعات و ... ظهور و بروز می‌یابند، مستلزم حضور کانون‌های قدرتمند نهادی از جمله «استراتژیست‌های سایبری» و «ژنرال‌های سایبری» در کنار «دیپلمات‌های سایبری» است تا بتوانند با هم‌افزایی منابع قدرت داخلی، به بهترین نحو ممکن اهداف و سیاست‌های منطقه‌ای و بین‌المللی مطلوب در این عرصه را پیش ببرند.

در ایران، مرکز ملی فضای مجازی به عنوان نهاد سیاست‌گذار در عرصهٔ سایبری و وزارت امورخارجه به عنوان دستگاه متولی سیاست خارجی کشور دو نهاد اصلی و تأثیرگذار در تدوین، تبیین و پیش‌بینی مسائل، چالش‌ها و فرصت‌های عرصهٔ سایبری و به تبع آن تدوین سیاست‌ها و برنامه‌های اصلی کشور در دو سطح ملی و بین‌المللی محسوب می‌شوند. با توجه به موقعیت ژئوپولیتیک و منحصربه‌فرد کشور از یک سو، و نیز گستردگی دامنهٔ تهدیدات

و فشارهایی که ناحیهٔ سایبری در شرایط نوین بین‌المللی بر کشور وارد می‌شود از سوی دیگر، همکاری، هم‌اندیشی و در نهایت رویکرد بین‌سازمانی با هدف هم‌افزایی منابع دانش و قدرت بیش از پیش ضرورت می‌یابد.

با این نگاه، کتاب *حکمرانی در عرصهٔ پنجم: گذار به دیپلماسی سایبری* به عنوان یکی از طرح‌های مطالعاتی در زمینهٔ دیپلماسی سایبری در ۱۰ فصل تدوین یافته و هم‌اکنون به صورت مشترک از سوی انتشارات پژوهشگاه فضای مجازی، دانشکدهٔ روابط بین‌الملل وزارت امور خارجه و ادارهٔ هماهنگی امور پژوهشی و نشر وزارت امور خارجه در اختیار محققان، پژوهشگران و علاقه‌مندان مسائل دیپلماسی سایبری قرار گرفته است.

مبنای تدوین این کتاب، مطالعهٔ موردی است و به طور خاص مبانی، اصول و راهبردهای دیپلماسی سایبری چند کشور مهم از جمله آمریکا، روسیه، چین، اتحادیهٔ اروپا و مالزی در آن ارزیابی شده است. در کنار مطالعات موردی، بیش از ۸۰ سند منطقه‌ای و بین‌المللی در این حوزه نیز مورد مطالعه قرار گرفته و پس از احصاء اصول اصلی آن‌ها، مهم‌ترین بازیگران این عرصه در سطوح ملی، منطقه‌ای و بین‌المللی، و نیز بازیگران بخش خصوصی معرفی و رویکرد آن‌ها به مقوله سایبری تبیین شده است. همچنین با توجه به اهمیت ظهور بازیگران غیردولتی، یک فصل به طور کامل به ارزیابی و مطالعهٔ این بازیگران پرداخته و به طور خاص گافام، به عنوان بزرگ‌ترین پلتفرم‌های آی‌تی، در چارچوب دیپلماسی شرکتی ارزیابی و تحلیل شده است.

ویژگی متمایز این کتاب، بررسی تطبیقی تمامی مطالعات موردی و نیز رویکردهای مهم منطقه‌ای و بین‌المللی به دیپلماسی سایبری در فصل پایانی می‌باشد. بر مبنای این مقایسهٔ تطبیقی، در نهایت یک الگوی عملیاتی با محوریت ۲۴ مقولهٔ مهم سایبری برای تدوین سند دیپلماسی سایبری در ایران پیشنهاد شده است.

این کتاب در اصل فتح بابی در خصوص مسائل مرتبط با دیپلماسی سایبری کشور در این عرصهٔ چالشی و در عین حال روبه‌توسعه می‌باشد و امید است علاقه‌مندان به این حوزه با مطالعه و نقد این کتاب فضای دیالکتیکی و گفتمانی مناسبی را برای پیشبرد مباحث مربوطه در این حوزه فراهم سازند.

عبدالحسین کلانتری؛ مرکز ملی فضای مجازی
محمدحسن شیخ‌الاسلامی؛ دانشکدهٔ روابط بین‌الملل

مقدمه

زمین، دریا، هوا و فضا؛ و اکنون فضای سایبری، به عنوان عرصهٔ پنجم، حوزه‌ای کاملاً جدید برای بسط قدرت و نفوذ در تعاملات منطقه‌ای و بین‌المللی کشورهاست. به این اعتبار، سازوکار و مکانیسم فعالیت در این عرصه که عموماً «دیپلماسی سایبری» نامیده می‌شود، متأخرترین نوع دیپلماسی در ادبیات روابط بین‌الملل است که عمر آن به کمتر از یک دهه می‌رسد.

اهمیت مقولهٔ «فضای سایبری» در گسترهٔ روابط بین‌الملل به حدی است که برخی از محققان، اهمیت ظهور آن را با اختراع «بمب اتم» مقایسه کرده و تأکید داشته‌اند که عرصهٔ سایبری به همان اندازه مستلزم تکاپوی جدی و بی‌شمارِ دیپلماسی و دیپلمات‌هاست تا بتوان از پیامدها و آسیب‌های ملی، منطقه‌ایِ و بین‌المللیِ به مراتب بیشتر، وسیع‌تر و خطرناک‌ترِ آن (در مقایسه با بمب‌های هسته‌ای) اجتناب کرد. با توجه به نوظهور بودنِ و نیز اهمیت روزافزون آن، با قاطعیت می‌توان گفت که دیپلماسی سایبری در سطوح مختلف ملی، منطقه‌ای و بین‌المللی در صدر توجهات سیاسی ـ حاکمیتی قرار داشته و (گرایش به پرداختن به آن) به عنوان مؤلفهٔ اصلی تعیین‌کنندهٔ قدرت و نفوذ در قرن ۲۱، بیش از پیش افزایش یافته است.

در مطالعه‌ای که در کتب، متون علمی و نیز اسناد ملی و منطقه‌ای کشورهای خارجی صورت گرفت، در مجموع بیش از هشتاد سند یا

اعلامیهٔ تبیین‌کنندهٔ دیپلماسی سایبری کشورها، استراتژی‌های ملی، دوجانبه و چندجانبه و بین‌المللی اتخاذشده در ارتباط با دیپلماسی سایبری و رویکردهای جهانی به این مقوله شناسایی شده است. اگر بنا به اقتضای اشرافیت راهبردی و فنّاورانهٔ کشورهای غربی از پیشگامی آن‌ها در این حوزه صرف‌نظر کنیم، برخی تلاش‌ها و ابتکارات دیپلماتیک در ارتباط با دیپلماسی سایبری به کشورهای حوزهٔ خلیج فارس، آسیای میانه و حتی کشورهای آفریقایی نیز کشیده شده است که نشان از درجه و اهمیت این موضوع در بازیگری منطقه‌ای و بین‌المللی هر یک از کشورها دارد. با توجه به اهمیت این اقدامات و ابتکارات، برخی از مهم‌ترین آن‌ها در این کتاب به صورت «مطالعهٔ جامع اقدامات و سازوکارهای جهانی دیپلماسی سایبری» در فصل ۲ و برخی دیگر نیز به صورت مطالعهٔ موردی (فصول ۴ ــ ۹) در این کتاب مورد مطالعه و ارزیابی قرار گرفته‌اند.

با این حال و به رغم موضوعیت فراوان آن، به مقولهٔ دیپلماسی سایبری در ایران کمتر توجه شده است. در عرصهٔ نظری، هنوز کتابی جامع و مانع در این حوزه که مبیّن مبانی، اصول و مؤلفه‌های دیپلماسی سایبری باشد، وجود ندارد. در عرصهٔ عمل، در حالی که رویکردهای جدید بر گذار به مرحلهٔ شناسایی و ردیابی فعالیت‌های سایبری و نیز اتخاذ استراتژی‌های نفوذ در قلمروهای به دقت طراحی‌شدهٔ سایبری در اقصی نقاط جهان تأکید دارد، عمدهٔ اقدامات و ابتکارات سایبری کشور با رویکرد «دفاعی» تنظیم و سامان یافته که بر اساس شواهد تاریخی، رویکرد بسیار ابتدایی و اولیهٔ تمامی کشورها به مقولهٔ فضای سایبری بوده است. در برخی نظریه‌پردازی‌های پراکندهٔ دیگر نیز مقولهٔ دیپلماسی سایبری با برخی مفاهیم مشابه همچون دیپلماسی دیجیتال، دیپلماسی الکترونیکی، دیپلماسی عمومی و... خلط معنایی پیدا کرده و یا حتی کرانه‌های

آن به حضور چند مقام ارشد کشور در شبکه‌های اجتماعی جهانی، همچون توییتر و اینستاگرام، تقلیل یافته است.

به لحاظ مفهومی، دیپلماسی سایبری را به معنای عامِ آن می‌توان در دو سطح بررسی کرد: نخست، ادامه و تداوم دیپلماسی سنتی در فضا و بستر جدید است که فضای سایبری نامیده می‌شود. به این اعتبار، تمامی فعالیت‌های دیپلماتیک را، که سابقاً به صورت سنتی جاری و ساری بوده است، می‌توان از این طریق و در بستر فضای سایبری نیز دنبال کرد. دوم، که بیشتر و مهم‌تر جلوه یافته، به معنای مدیریت تضادها و اختلافات منطقه‌ای و بین‌المللی مرتبط با فضای سایبری از طریق گفت‌وگو و مذاکره، استفاده از قابلیت‌ها و توانمندی‌های سایبری برای «دفاع» از منافع ملی و در سطح ایدئال آن، پیشبرد منافع ملی از طریق ظرفیت‌سازی سایبری، اعتمادسازی سایبری و اتخاذ استراتژی‌های مؤثر با هدف نفوذ در حوزه‌های قدرت و ثروت در عرصهٔ جهانی است. به این اعتبار، دیپلماسی سایبری از سیاست‌گذاریِ ملی در حوزهٔ فضای سایبری تمایز یافته و از سطح پیشین (تداوم و گسترش دیپلماسی سنتی در فضای سایبری) نیز فراتر می‌رود. سطح دوم از تعریف فوق، در واقع نقطهٔ ایدئال و مطلوبِ دیپلماسی سایبری است که باید به دنبال آن بود.

با توجه به این مقدمه و تعریفی که در بالا در دو سطح از دیپلماسی سایبری ارائه شده، این کتاب تلاشی است در زمینهٔ ۱. مطالعهٔ اصول و مبانی دیپلماسی سایبری برخی کشورهای پیشرو در حوزهٔ سایبری، و ۲. ارائهٔ یک چارچوب مفهومی از مؤلفه‌ها و مقولات مرتبط با دیپلماسی سایبری با هدف پیشنهاد یک الگوی عملی از دیپلماسی سایبری در ایران.

بر اساس این اهداف، کتاب حاضر در مجموع دارای ده فصل است:

۱. دیپلماسی سایبری؛ مسائل، چالش‌ها و رسالت: این فصل ترجمهٔ مقاله‌ای است که به درخواست نویسندهٔ اصلی آن، هلی تییرما کلار،[1] به عنوان مقدمه‌ای بر موضوع دیپلماسی سایبری ترجمه و تلخیص شده است. نویسندهٔ مقاله یکی از پیشگامان مفهوم‌پردازی در حوزهٔ دیپلماسی سایبری است. هلی تییرما کلار از ۲۰۱۳، در اتحادیهٔ اروپا به عنوان دیپلماتی برجسته درگیر موضوعاتِ حوزهٔ سایبری بوده و هم‌اکنون نیز در کسوت سفیر ارشد حوزهٔ سایبری، در وزارت امور خارجهٔ کشور استونی مشغول به فعالیت است. مقالهٔ وی حاوی یکی از جامع‌ترین مفهوم‌پردازی‌های صورت‌گرفته دربارهٔ دیپلماسی سایبری است که تا کنون به رشتهٔ تحریر درآمده است. این مقاله صورت‌بندی کاملی از مسائل، چالش‌ها و دستورالعمل‌های موضوعات سایبری در عرصهٔ بین‌الملل را ارائه می‌دهد.

۲. مطالعهٔ جامع اقدامات و سازوکارهای جهانی دیپلماسی سایبری: در این فصل، مطالعهٔ نسبتاً جامعی دربارهٔ بیش از هشتاد اقدام و سازوکار ملی، منطقه‌ای، بین‌المللی و جهانی که تا کنون در ارتباط با دیپلماسی سایبری به سرانجام رسیده، صورت گرفته است. این فصل از این جهت حائز اهمیت است که در وهلهٔ اول مهم‌ترین بازیگران عرصهٔ دیپلماسی سایبری را در سطوح مختلف (کشورها، سازمان‌های بین‌المللی، مذاکرات دوجانبه، چندجانبه، بخش خصوصی و شرکت‌های فناوری و ...) شناسایی کرده و بر اساس آن می‌توان مهم‌ترین ابتکارات صورت‌گرفته، میزان پیشرفت کشورها، رویکردهای منطقه‌ای و بین‌المللی و نیز مهم‌ترین سازوکارهایی را که در سطح جهان در ارتباط با اقدامات مرتبط با دیپلماسی سایبری تعریف و نهایی شده، به صورت تطبیقی با یکدیگر مقایسه کرد. حضور فعال برخی

1. Heli Tiirmaa-Klaar

کشورها در مناطق مختلف (چه در پلتفرم سازمان‌های منطقه‌ای و بین‌المللی و چه در قالب مذاکرات دوجانبه) در سازوکارهای تعریف‌شدهٔ منطقه‌ای و بین‌المللی حائز اهمیت است.

۳. گذار ژاپن به دیپلماسی سایبری (۲۰۱۸): این فصل مطالعهٔ موردی اقدامات ژاپن دربارهٔ دیپلماسی سایبری، رویکرد اصلی این کشور به این مقوله و اقدامات منطقه‌ای و بین‌المللی این کشور در ارتباط با فضای سایبری است. به لحاظ اصول و مبانی، اگرچه دیپلماسی سایبری ژاپن در سطح بین‌الملل شباهت‌ها و قرابت‌های زیادی با دموکراسی‌های غربی همچون آمریکا و اتحادیهٔ اروپا دارد، اما در سطح داخلی، درست همانند چین و روسیه، مهم‌ترین دغدغهٔ این کشور موضوع «امنیت داخلی» است، به خصوص اینکه اقتصاد این کشور تماماً به زیرساخت‌های اقتصاد دیجیتال وابسته است. شاید بر همین اساس نیز ژاپن در استراتژی‌های عملیاتی برای پیشبرد دیپلماسی سایبری خود، اولویت بیشتری برای همسایگان پیرامونی خود به خصوص در آسیا و اقیانوسیه قائل است. از این رو مطالعهٔ کشور ژاپن، که تلاش می‌کند همسو با اصول و مبانی دموکراسی‌های غربی دغدغه‌ها و چالش‌های شرقی (همچون روسیه و چین) را نیز مدیریت کند، می‌تواند حائز اهمیت باشد.

۴. ظهور و افول دیپلماسی سایبری آمریکا، بازگشت به رویکرد امنیتی ـ تهاجمی: این فصل به مطالعهٔ تاریخچهٔ دیپلماسی سایبری در آمریکا، به عنوان کشوری که در حوزهٔ سایبری به لحاظ فنی از سایر کشورها جلوتر است، بر اساس اسناد تدوین‌شده در دو دههٔ اخیر می‌پردازد. نکتهٔ اصلی و قابل توجه در این مطالعه، افول دیپلماسی سایبری آمریکا از سیاست‌های آرمان‌گرایانهٔ تاریخی و بازگشت این کشور به رویکرد امنیتی ـ نظامی در ارتباط با فضای سایبری به

خصوص پس از انتخاب دونالد ترامپ به ریاست‌جمهوری در ۲۰۱۶ است. با توجه به رویکرد تجاری ـ نظامیِ دولت ترامپ، به نظر می‌رسد دولت فعلی حاکم بر این کشور از بعضی از مهم‌ترین اصول و مؤلفه‌های بنیادینی همچون «حقوق بشر» و «آزادی بیان» و ...، که در دیپلماسی کلاسیک بین‌الملل خود مدعی آن‌ها بود، افول کرده و در چارچوب دیپلماسی سایبری جدید، بیشتر به دنبال تضمین «امنیت سایبری» خود (جلوگیری از حملات سایبری یا جاسوسی سایبری) و نیز کسب بیشترین منافع تجاری و اقتصادی در تمامی استراتژی‌های تعاملی دوجانبه و چندجانبه در عرصهٔ منطقه‌ای و جهانی است. در این فصل، همچنین به مهم‌ترین چالش‌های پیش روی آمریکا در عرصهٔ دیپلماسی سایبری، یعنی چالش مخالفت‌ها با «جریان آزاد و فرامرزی داده‌ها» که در قالب جنبش‌هایی همچون تقاضا برای محلی‌سازی داده‌ها، تدوین استانداردهای ملی امنیت اطلاعات، ارائهٔ الگوهای جایگزین از حکمرانی اینترنت و حکمرانی سایبری و ... از سوی کشورهایی همچون هندوستان، چین، روسیه و حتی اتحادیهٔ اروپا دنبال می‌شود، پرداخته شده است.

۵. چین و گذار به دیپلماسی سایبری مدبرانه: این فصل مطالعهٔ موردی کشور چین به عنوان یک قدرت بزرگ جهانی، در ارتباط با دیپلماسی سایبری است که می‌توان آن را در قالب یک استراتژی سه‌وجهی دنبال کرد: ۱. تهاجمی؛ از طریق نفوذ در زیرساخت‌های اطلاعاتی و ارتباطی کشورهای رقیب، به خصوص آمریکا و اروپا، ۲. تجاری ـ اقتصادی؛ از طریق سرمایه‌گذاری گسترده در زیرساخت‌های کشورها و مناطق هدف به خصوص اروپا، آفریقا، خاورمیانه، آسیای میانه و آمریکای لاتین،۳. استانداردسازی؛ از طریق مشارکت جدی در تعریف پروتکل‌ها و استانداردهای فناوری در نرم‌افزار، سخت‌افزار و شبکه‌های مدرن. گذار

چین از یک موضع تدافعی در ارتباط با دیپلماسی سایبری به یک سیاست مدبرانه با هدف مقابله با نفوذ و اشرافیت راهبردی آمریکا در حوزهٔ سایبری، تثبیت اصل «حاکمیت ملی» در حکمرانی فضای سایبری، صورت‌بندی تهدیدات سایبری، پیشبرد اهداف سایبری از طریق سرمایه‌گذاری‌های تجاری هنگفت منطقه‌ای و بین‌المللی، پیشبرد صلح سایبری از طریق اتخاذ استراتژی‌های تعامل چندجانبه (با سازمان ملل[1]، اتحادیهٔ اروپا و سازمان همکاری شانگهای) و نیز استراتژی تعامل دوجانبه با آمریکا، روسیه و انگلستان از جمله مهم‌ترین محورهایی است که در این فصل به آن پرداخته شده است. الگوی عملیاتی پیاده‌سازی دیپلماسی سایبری در ساختار حاکمیتی این کشور و نقش شرکت‌های فناوری چینی به خصوص هوآوی و زدتی‌ای، در پیشبرد اهداف دیپلماسی سایبری چین نیز در جای خود قابل تأمل است.

۶. دیپلماسی سایبری روسیه، حاکمیت ملی و امنیت اطلاعات: روسیه، همانند چین، به عنوان اصلی‌ترین رقیب آمریکا در عرصهٔ دیپلماسی سایبری، از اهمیت قابل‌توجهی برخوردار است. موضوع مقابلهٔ تاریخی و ایدئولوژیک این کشور با دموکراسی‌های غربی که امروزه به عرصهٔ سایبری نیز کشیده شده، بر اهمیت رویکرد سایبری روسیه می‌افزاید. در این فصل، به طور کلی رویکرد روسیه با تأکید بر دو مؤلفهٔ «حاکمیت ملی» و «امنیت اطلاعات»، که آشکارا مؤلفه‌ها و مبانی اصلی دیپلماسی سایبری غربی را زیر سؤال می‌برد، بررسی شده است. علاوه بر این، استراتژی‌هایی که روسیه برای پیشبرد دیپلماسی سایبری در عرصهٔ جهانی و منطقه‌ای، به خصوص از طریق مکانیسم سازمان ملل، سازمان همکاری شانگهای و ...

1. United Nation Group of Governmental Experts (UNGGE)

در پیش گرفته، همراه با چالش‌های آن نیز با جزئیات بحث و بررسی می‌شود. نکتهٔ قابل تأمل‌تر در ارتباط با دیپلماسی سایبری روسیه این است که روند روزافزون تهدیدات سایبری به طور خودکار برداشت بسیاری از کشورها را، حتی کشورهای غربی، به مبانی فکری روسیه در ارتباط با ماهیت چالش‌های فضای سایبری نزدیک ساخته است.

۷. دیپلماسی سایبری اتحادیهٔ اروپا، از تاب‌آوری سایبری تا بستهٔ دیپلماسی سایبری: این فصل رویکرد کلان اتحادیهٔ اروپا را به دیپلماسی سایبری ارزیابی می‌کند. اگرچه سیاست‌های اتحادیهٔ اروپا در سطح کلان در ارتباط با دیپلماسی سایبری تا حدودی همسو با آمریکاست، اما در مقایسه با آمریکا، کمتر تهاجمی و بیشتر دفاعی و همراه با تلاش برای حل مسائل سایبری از طریق مذاکرات سیاسی است. به طور مثال، بستهٔ دیپلماسی سایبری، که در سال ۲۰۱۷ به تصویب رسید، به عنوان یکی از ابتکارات اتحادیهٔ اروپا، بر اساس محور صلح‌طلبی طیف نسبتاً جامعی از اقدامات سایبری مشترک با هدف پیشبرد اهداف سیاسی این اتحادیه ارائه می‌دهد. با این حال، همان طور که در این فصل به آن پرداخته شده، این بسته نیز در عمل به دلیل دشواری مکانیزم‌های تصمیم‌گیری اشتراکی و دیگر چالش‌هایی که با آن مواجه است، بیشتر شبیه یک مانیفست سیاسی است تا یک برنامهٔ جامع عملیاتی. این فصل در نهایت با ارائهٔ چشم‌اندازی از آیندهٔ بستهٔ دیپلماسی سایبری اتحادیهٔ اروپا و نیز استراتژی‌هایی که به صورت چندجانبه، دوجانبه و نیز از طریق درگیر ساختن تمامی ذی‌نفعان غیردولتی از سوی این اتحادیه در پیش گرفته شده، پایان می‌یابد.

۸. دیپلماسی سایبری مالزی: این فصل به مطالعهٔ کشور مالزی، به عنوان یک کشور اسلامیِ نسبتاً پیشرفته، در ارتباط با مقولهٔ دیپلماسی سایبری

می‌پردازد. اگرچه این کشور به لحاظ زیرساخت، رویکرد و حتی نقشی که در این حوزه دارد، قابل مقایسه با سایر کشورهایی که در این کتاب مورد مطالعه قرار گرفته‌اند نیست، با این حال تاریخچهٔ توسعهٔ فناوری (به خصوص استفاده از فناوری اطلاعات و ارتباطات در حکمرانی ملی و نیز کسب رتبهٔ عالی در دولت الکترونیک) و نیز پرداختن زودهنگام به مقولهٔ سایبری در سیاست‌گذاری و برنامه‌ریزی‌های مختلف که سابقهٔ آن به دههٔ ۱۹۹۰ می‌رسد، حائز اهمیت است. اگر از چالش‌های داخلی مالزی، از جمله دشواری برقراری توازن استراتژیک بین ملاحظات حکمرانی ملی با تأکید بر چندقومی و چندنژادی بودن این کشور و الزامات همراهی آن با جریانات غالب حکمرانی بین‌المللی در عرصهٔ سایبری، صرف‌نظر کنیم؛ نقشی که مالزی در دهه‌های اخیر به عنوان یک کشور اسلامیِ پیشرفته در معادلات منطقه‌ای و بین‌المللی ایفا کرده، به خصوص از منظر همسویی با جامعهٔ جهانی، مورد توجه خاص بسیاری از کشورها واقع شده است.

۹. گافام و دیپلماسی شرکتی: گافام نام یک کشور یا واحد سیاسی با مختصات حکمرانی همراه با قلمرو مشخص و مرزهای جغرافیایی معیّن نیست. بلکه پنج پلتفرم (گوگل، اپل، فیس‌بوک، آمازون و مایکروسافت) پیشتاز در عرصهٔ سایبری هستند که به لحاظ سیاسی به پادشاهان آنلاین، به لحاظ ثروت به امپراتوری‌های تجاری و به لحاظ فناوری به غول‌های آی‌تی مشهور شده‌اند. در واقع ترکیب «ثروت» و «فناوری» در دستان این پلتفرم‌ها، به گافام قدرت بازیگری و اثرگذاری بسیار زیادی در عرصهٔ سیاست و نیز روابط بین‌الملل داده که در هیچ سپهر سیاسی نمی‌توان آن‌ها را نادیده گرفت. در این فصل، گافام در چارچوب مفهوم پلتفرم، دیپلماسی شرکتی، عوامل قدرت‌افزای آن‌ها در حکمرانی شبکه‌ای و نیز چالش‌هایی

که از این ناحیه متوجه دیپلماسی به معنای کلاسیک آن شده، واکاوی شده است. ارزش تجاری گافام در سه ماههٔ اول سال ۲۰۲۰ به بیش از پنج هزار میلیارد دلار (پنج تریلیون دلار) رسید و برای فهم نقش و جایگاه آن‌ها در دنیای سیاست مدرن می‌توان به استعارهٔ «کودکان نابخرد» شرود براون[1] سناتور آمریکایی، اشاره کرد که در اعتراض به عملکرد این پلتفرم‌ها گفت دنیا همانند یک خانه است و این پلتفرم‌ها همچون کودکان نابخرد بارها همه آن را به آتش زده‌اند. با توجه به اهمیت این پلتفرم‌ها و حضور آن‌ها به عنوان بازیگر مستقل در بسیاری از منازعات سیاسی داخلی و خارجی، امروزه بسیاری از کشورها فارغ از تعاملات سیاسی کلاسیک، باب تعامل دیپلماتیک سایبری با این پلتفرم‌ها گشوده‌اند که از جمله می‌توان به انتصاب اولین سفیر در گوگل از سوی کشور دانمارک اشاره کرد.

۱۰. گذار به دیپلماسی سایبری، چارچوب مفهومی و پیشنهاد الگوی عملی دیپلماسی سایبری در ایران: این فصل در مجموع جمع‌بندی تمامی فصل‌های تدوین‌شده در این کتاب است. این فصل افزون بر مقدمهٔ آن، مطالعهٔ سیر تاریخی ظهور مفاهیم مشابه با دیپلماسی سایبری، و مرزبندی و تمایز معنایی و مفهومی که بین آن‌ها صورت پذیرفته، از دو حیث حائز اهمیت است: ۱. جمع‌بندی‌ای را که از گرایش‌های مختلف ملی، منطقه‌ای و جهانی به مقولهٔ دیپلماسی سایبری به دست آمده در قالب دو رویکرد کلان همراه با مبانی و اصول اصلی آن‌ها، که به طور هم‌زمان از سوی دو جبههٔ متفاوت (یکی به رهبری آمریکا در غرب و دیگری به رهبری چین و روسیه در شرق) در سطح جهان دنبال می‌شود، به معرض نمایش می‌گذارد. ۲. مهم‌ترین مقولات یا مفاهیمِ دیپلماسی سایبری را، که از طریق مطالعات

1. Sherrod Brown

موردی و نیز تکنیک هم‌افزایی فکری در جلسات بحث متمرکز احصا شده، در قالب «جدول مقولات سایبری» ارائه و با تعریف دقیق آن‌ها در قالب یک الگو برای تدوین به صورت عملیاتی در ایران پیشنهاد می‌دهد.

با مطالعهٔ عمیق فصول این کتاب می‌توان دریافت که علاوه بر اصول، مبانی و مؤلفه‌های دیپلماسی سایبری در هر یک از این کشورها، صف‌بندی جهانی در ارتباط با دیپلماسی سایبری، رویکرد کشورها به این مقوله و استراتژی‌هایی که گاهی از سوی هر یک از کشورها، چه به صورت دوجانبه یا چندجانبه و یا بین‌المللی، اتخاذ شده نیز روشن و مبرهن است.

با وجود این، در صف‌بندی فعلی از نظام حاکم بر فضای سایبری جهانی، نکته‌ای قابل تأمل دربارهٔ دیپلماسی سایبری وجود دارد و آن اینکه تنها، کشورهایی در این زمینه موفق بوده‌اند که توانسته‌اند دربارهٔ اصول و مؤلفه‌های حاکم بر این نظم، «استانداردسازی» کرده و در قالب دیپلماسی سایبری، این استانداردها را در روابط بین‌الملل به جوامع مختلف تحمیل کنند. در واقع می‌توان گفت تنها ایالات متحده آمریکاست که توانسته استانداردِ مورد نظر خود در این زمینه را به نظام جهانی (جامعهٔ جهانی) تحمیل کند به طوری که بر اساس بررسی‌های انجام‌شده، حداقل ۲۵ کشور جهان که عمدتاً غربی و از کشورهای اروپایی‌اند، عیناً از استراتژی دیپلماسی سایبری این کشور اقتباس کرده و دنباله‌رو آن هستند. در سطوحی پایین‌تر، روسیه و چین نیز تلاش‌هایی در این زمینه کرده‌اند، هرچند هنوز در مراحل اولیه قرار دارند و با چالش‌های اساسی از سوی رقبای غربی خود مواجه‌اند. صرف‌نظر از آمریکا و روسیه و چین، عمدهٔ کشورها (حتی کشورهایی در سطح انگلستان، آلمان، فرانسه و اتحادیهٔ اروپا) عمدتاً در ابعاد امنیت سایبری با تأکید بر ملاحظات داخلی متوقف

مانده و نتوانسته‌اند به راهبردهای دیپلماتیک بـا تأکیـد بـر عرصـهٔ سیاسـت خارجی دست یابند. به عبارت دیگر، به جرئت می‌توان گفت که بـه غیـر از آمریکا و تا حدودی روسیه و چین، عمدهٔ کشورها اغلب در ابعاد داخلـی و امنیتی سایبری متوقف مانده و اگر کمی فراتر رفته‌اند، یا دنباله‌روی کرده‌انـد و یا صرفاً به بیان لزوم دیپلماسی در این حوزهٔ جدید بسنده کرده‌اند.

با توجه به ملاحظهٔ فوق، ادعای اصلی کتاب این است که با توجه به تبـدیل شدن فضای سایبری به منشأ اصلی نبرد و مناقشه بـین کشـورها و قـدرت‌هـای بزرگ در عرصهٔ جهانی، نظام حکمرانی کشور باید هر چه سریع‌تر از لایـه‌هـای دفاعی ـ امنیتی فضای سایبری فراتر رفته و به پشتوانهٔ قابلیت‌هـا و ظرفیـت‌هـای سایبری که تا کنون به دست آورده، در ارتباط با مقولات و مؤلفه‌های دیپلماسـی سایبری (جدول مقولات ارائـه‌شـده در فصـل دهـم) استانداردسـازی کنـد. بـه عبارت روشن‌تر، نظام حکمرانی باید به یـک تعریـف، جمـع‌بنـدی و سیاسـت واحد در ارتباط با هر یک از مقولات حوزهٔ سایبری برسد تا بتواند بـه صـورت منسجم و یکپارچه در قالب الگـویی عملـی[1] و صـاحب‌گفتمـان (و در جایگـاه مدعی) برای پیشبرد منافع ملی کشور در این حـوزه وارد تعامـل اسـتراتژیک بـا طرف‌های خارجی در عرصهٔ منطقه‌ای و بین‌المللی بشود. در غیر ایـن صـورت، همواره باید در چارچوب و استانداردهای دیپلماسی سایبری کشـورهای پیشـرو بازیگری کند و بپذیرد که همواره در موضـع دفـاعی قـرار داشـته و نسـبت بـه مطالبات آن‌ها ــ به خصوص آنچه به طور مشخص می‌توان برنامهٔ هدایت‌شـدهٔ ایران‌هراسی سایبری نامید ــ پاسخگو باشد.

در پایان و به مناسبت چاپ این کتاب بر خود لازم مـی‌دانـیم از تمـامی

---

۱. این الگوی عملی که از آن به عنوان دیپلماسی سایبری یاد می‌شود، بـه تفصـیل در فصل دهم به همراه مقولات پیشنهادی برای تصمیم‌گیـری و سیاسـت‌گـذاری بررسـی می‌گردد.

افرادی که به روش‌های مختلف در به سرانجام رسیدن این مجموعه ما را یاری کرده‌اند، به خصوص دبیر محترم شورای‌عالی و رئیس مرکز ملی فضای مجازی، ریاست محترم دانشکدهٔ روابط بین‌الملل، کارشناسان پژوهشگاه فضای مجازی و همکاران هیئت‌علمی دانشکدهٔ روابط بین‌الملل وزارت امور خارجه، قدردانی نماییم.

همچنین با توجه به قلّت منابع نظری داخلی و خارجی در این زمینه، آشکارا مفروض است که این مجموعه صرفاً فتح بابی در زمینهٔ دیپلماسی سایبری است و لذا مشتاقانه منتظر دریافت نظریات، پیشنهادات و نقد و بررسی‌های مشفقانه و کارشناسانهٔ تمامی کنشگران این عرصه هستیم.

فصل نخست

دیپلماسی سایبری: مسائل، چالش‌ها و اهداف[1]

درآمد

بسیاری از کارشناسان روابط بین‌الملل و دیپلمات‌های حرفه‌ای با موضوع جدیدی به نام مسائل سایبری بین‌المللی یا دیپلماسی سایبری مواجه‌اند. این امر شامل سیاست فناوری اطلاعات و ارتباطات، امنیت سایبری بین‌المللی، گفت‌وشنودهای دوجانبهٔ سایبری، سیاست توسعه، مسائل اینترنتی، حقوق بشر در عصر سایبری، موضوعات تجارت و مالکیت معنوی و بسیاری از مسائل سیاسی دیگر است. این در حالی است که ابعاد و عناصر و مؤلفه‌های دیپلماسی سایبری همواره در حال تغییر بوده و به سرعت نیز در حال توسعه است.

این موضوع در ارتباط با فعالیت‌های دیپلمات‌ها، مسیر کاملاً جدید و تازه‌ای را پیش روی روابط بین دولت‌ها قرار داده است که طیف گسترده‌ای از ابزارهای سیاست خارجی را در بر می‌گیرد و نیز بسیاری از ذی‌نفعان داخلی و خارجی را شامل می‌شود. بنابراین، وظایف هماهنگ‌سازی

---

۱. نویسندهٔ اصلی این مقاله هلی تییرما کلار، اولین دیپلمات امنیت سایبری اتحادیهٔ اروپا و سفیر ارشد حوزهٔ سایبری در وزارت امور خارجهٔ کشور استونی، است. این مقاله به درخواست ایشان به عنوان مقدمه‌ای بر بحث «دیپلماسی سایبری» عیناً ترجمه شده است.

جدیدی برای وزارت‌های امور خارجه مطرح می‌شود که نیازمند دانش جامعی در زمینهٔ فناوری اطلاعات، امنیت رایانه و شبکه، حکمرانی اینترنت، امنیت بین‌المللی، جرایم سایبری، هوش سایبری و غیره است. حال آنکه همواره آکادمی‌های دیپلماتیک یا مدارس امور بین‌الملل به تمام این مباحث نمی‌پردازند. همچنین دیپلمات‌ها باید به سرعت بر اصول و مؤلفه‌های فضای سایبری اشراف یابند، زیرا این فضا به سرعت در حال تغییر و تحول است. این امر در حال حاضر اهمیت ویژه‌ای دارد، به این دلیل که دولت‌ها همواره مقامات ارشدی را به هدایت این روابط بین‌المللی تازه روی‌کارآمده منصوب می‌کنند. در آینده، در اختیار داشتن نسل جدیدی از دیپلمات‌های توانمند و آموزش‌دیده به منظور پیشبرد برنامه‌های بین‌المللی سایبری بسیار حائز اهمیت خواهد بود. در اینجا، به شفاف‌سازی دربارهٔ چالش‌ها و الزامات اصلی این حوزهٔ سیاسی، که به احتمال زیاد دیپلمات‌های آینده در طول فعالیت شغلی خود با آن مواجه خواهند شد، می‌پردازیم.

چنانچه از دست‌اندرکاران این حوزه دربارهٔ ماهیت دیپلماسی سایبری سؤال شود، به احتمال زیاد دیدگاه‌های متفاوتی ارائه خواهند داد. عده‌ای ادعا می‌کنند که عمدتاً آزادیِ بیان از طریق اینترنت است، برخی دیگر اظهار خواهند داشت که باید علیه جرایم سایبری مبارزهٔ جهانی صورت گیرد، حال آنکه برخی دیگر معتقدند که می‌بایست به قوانین جنگ سایبری بپردازیم. حقیقت امر آن است که یک دیپلمات سایبری موفق باید به طور هم‌زمان به بسیاری از موضوعات موازی اشراف داشته باشد، زیرا در موقعیت‌های مختلف کاری، باید با آگاهی از جنبه‌ها و ابعاد مختلف سیاست خارجی تصمیم‌گیری کنند.

از آنجا که در مراحل بسیار اولیهٔ شکل‌گیری سیاست خارجی سایبری به

سر می‌بریم، تنها تعداد محدودی از وزارت‌های امور خارجه دارای یک دفتر سایبری ویژه هستند. در اغلب وزارتخانه‌ها، حتی در صورتی که واحد سایبری ویژه‌ای در آن‌ها تأسیس نشده باشد، به مباحث سایبری در کنار امور روزمرهٔ دیگر، از جمله حقوق بشر، امنیت بین‌المللی، تهدیدات فراملّی و سایر موارد توجه می‌شود. چنانچه دولت‌ها تمایل داشته باشند تمام جنبه‌های حوزهٔ سایبری را تحت پوشش قرار دهند، در اختیار داشتن گروهی از دیپلمات‌های سایبری الزامی است. دارا بودن یک دفتر تخصصی با دانش کافی در زمینهٔ مسائل سایبری یک مزیت محسوب می‌شود، حال آنکه وجود هماهنگی افقی[1] کافی بین دیپلمات‌هایی که در موضوعات خاص و ژئوپلیتیک متبحرند، در حوزهٔ مسائل سایبری نیز حائز اهمیت است. یک ساختار هماهنگی سایبری افقی ایدئال باید شامل حقوق بشر، امنیت بین‌المللی، تجزیه و تحلیل اطلاعات، مسائل مربوط به تهدید جهانی و دیپلمات‌های جغرافیایی و چندجانبه[2] در وزارتخانه‌های امور خارجه باشد.

اولویت‌بندی مسائل مختلف سایبری بین‌المللی کار چندان آسانی نیست. عنصر اصلی سیاست خارجی همواره حمایت از حقوق و آزادی‌های اولیه بوده است و شروع از این نقطه منطقی به نظر می‌رسد. در دموکراسی‌های لیبرال، ترویج فعالیت‌های بین‌المللی یکی از اصلی‌ترین عناصر سیاست خارجی است که به صورت اینترنتی یا غیراینترنتی به دفاع از حقوق بشر کمک می‌کند. تنش ذاتی بین آزادی اینترنتی و الزامات امنیت سایبری موجب شده است که بسیاری از دولت‌ها، از جمله دولت‌های لیبرال دموکرات، دربارهٔ چگونگی استفاده از فناوری اینترنت به منظور به حداکثر رساندن میزان تأثیرگذاری بر رفاه جمعی، همراه با کمترین موارد

1. Horizontal Coordination
2. Geographical and Multilateral Diplomats

نقض حقوق اساسی، تصمیمات دشواری اتخاذ کنند. روند افزایشی سانسور و نظارت گسترده بر اینترنت مستلزم اقدام جمعی برای محکوم کردن رژیم‌های سرکوبگرِ آزادی بیان در رسانه‌های جدید است.

دیپلمات‌ها باید همواره در محافظت از اینترنت کوشاتر باشند. اینترنت آزاد و باز به‌خودی‌خود پدیدهٔ بخصوصی نیست و از ابتدای راه، توجه بسیاری از دست‌اندرکاران را به خود جلب کرده است. شبکهٔ جهانی وب به عنوان سکویی برای ارتباطات، در جوامع مختلف روی کار آمد و به یک زیرساخت مهم و اساسی در سراسر جهان تبدیل گشت که نحوهٔ ارتباط با افراد دیگر و تفکر و انجام امور و فرایندها را تغییر داد. تأثیر اینترنت به عنوان یک فناوری آزادی‌بخش، برای بسیاری از گروه‌های اجتماعی غیرممتاز و دورافتاده و کم‌سواد بسیار چشمگیر است و باید به شکل فعلی آن حفظ شود. اینترنت به دلیل نوآوری و همکاری داوطلبانهٔ نشئت‌گرفته از بخش خصوصی، بین گروه‌های غیردولتی و بخش مدنی بسیار موفقیت‌آمیز عمل کرده است. شرط اصلی تداوم این گونه نوآوری‌ها حفظ تأثیر نوآوری بخش خصوصی و محرک‌های جامعهٔ مدنی در الگوی فعلی حکمرانی اینترنت است. این موضوع نیز باید در سیاست خارجی در نظر گرفته شود.

دیپلمات‌ها هم‌زمان با ترویج اینترنت آزاد و حقوق بشر به صورت اینترنتی، باید به جامعه‌ای بپردازند که به اجرای قانون اهمیت زیادی می‌دهد و به افزایش سریع جرایم سایبری واقف است. مسئلهٔ حائز اهمیت دیگری که می‌تواند نگران‌کننده‌تر نیز باشد، جاسوسی سایبری مخفیانه با اهداف صنعتی است. تمامی این جوانب باید در طراحی گفتمان‌های سایبری و سیاست‌های سایبری بین‌المللی در نظر گرفته شوند؛ برای مثال، یک کشور نمی‌تواند در حوزهٔ امنیت سایبری با شرکای خارجی خود، که به نفوذ مخفیانه به رایانه‌ها و سرقت اسرار تجاری شهرت دارند، مشارکت کند.

همچنین دیپلمات‌ها باید در برنامه‌های اجرایی و عملیاتی خود، کشورهایی که از این ابزار برای سرکوبی آزادی بیان یا دستگیری وبلاگ‌نویسان ضد دولت بهره می‌جویند را مدنظر قرار دهند.

در پایان، تمام دیپلمات‌ها باید به خوبی با قوانین جنگ و درگیری در عرصهٔ جدید سایبری آشنایی داشته باشند. سرمنشأ نگرانی‌های امنیتی بین‌المللی در فضای سایبری این حقیقت است که کشورها همواره در حال تعیین قوانین و هنجارهای رفتاری در فضای سایبری هستند. نخستین چالش سایبری در حوزهٔ امنیت بین‌المللی، دستیابی به درک مشترکی از پارامترهای رفتاری دولت است. برخی طرح‌ها در دستیابی به این هدف همواره نقش مؤثری داشته‌اند، از جمله گزارش‌های گروه متخصصان دولتی سازمان ملل متحد در سال ۲۰۱۰ و ۲۰۱۳ یا کنفرانس جهانی فضای سایبری که از سال ۲۰۱۱ در لندن راه‌اندازی شد. در سازمان امنیت و همکاری اروپا[1] به منظور دستیابی به توافق در حوزهٔ اقدامات اعتمادسازِ مربوط به امنیت سایبری، فعالیت‌هایی در حال انجام است. جامعهٔ علمیِ دراین‌باره داده‌های ارزشمندی را، همچون راهنمای تالین، دربارهٔ کاربرد قوانین بشردوستانهٔ بین‌المللی[2] در جنگ سایبری ارائه کرده است. نخستین گام‌ها در تعیین هنجارها در دورهٔ غرب وحشی[3] فضای سایبری باید در مباحث سیاست‌های امنیتی بین‌المللی گنجانده شود. فعالیت‌های خطیری در راستای توافق دربارهٔ جزئیات نحوهٔ پیاده‌سازی اقدامات اعتمادسازی یا قوانین بشردوستانهٔ بین‌المللی در فضای سایبری صورت گرفته است؛ بنابراین بستر مناسبی برای توسعهٔ این فعالیت‌ها وجود دارد.

---

1. Organization for Security and Co-operation in Europe (OSCE)
2. International Humanitarian Law (IHL)
3. Wild West

یکی از مهم‌ترین اهداف سیاست‌گذاران ملی و بین‌المللی فضای سایبری همواره باید گنجاندن مسائل سایبری در حوزه‌های سیاست‌های موجود، از جمله امنیت داخلی، حفاظت از زیرساخت‌های اساسی، امنیت بین‌المللی و سیاست‌های حقوق بشر باشد. با توجه به تعدد عوامل داخلی و بین‌المللی در این حوزه ممکن است درک و مشارکت در تصمیم‌گیری دربارهٔ سیاست‌های سایبری برای دیپلمات‌ها بسیار چالش‌برانگیز باشد. در این مقاله ابتدا به شرح امنیت سایبری، که امروزه دولت‌ها با آن مواجه‌اند، پرداخته خواهد شد. سپس، پنج حوزهٔ اصلی فعالیت که سیاست‌های بین‌المللی می‌توانند در آنجا در زمینهٔ پاسخگویی به تهدیدات سایبری روزافزون مؤثر واقع شوند مطرح می‌گردد. هدف دیگر این مطالعه اشاره به اهمیت جریان مداوم سیاست‌های سایبری و چگونگی غلبه بر تمایل طبیعی انفکاک پروژه‌های سایبری کشورهاست. برای دستیابی به یک سیاست خارجی موفق در حوزهٔ سایبری، دیپلمات‌ها باید از هماهنگی سایبری ساختاریافته و ملی برخوردار باشند.

چالش‌های سیاست‌گذاری در عرصهٔ سایبری

پس از آنکه ویلیام هرشل[1] نور مادون قرمز را در سال ۱۸۰۰ کشف کرد، اکتشاف امواج الکترومغناطیسی پیشرفت روندهای فناورانه را تسهیل ساخت. توسعهٔ فیبر نوری برای ارتباطات از راه دور و فناوری رایانه‌ای، آغازگر عصر جدیدی بود که اکنون آن را انقلاب فناوری اطلاعات و ارتباطات[2] می‌نامیم. در حال حاضر، در عصری به سر می‌بریم که شاهد تغییر بزرگی در الگوی نگرش به انقلاب فناوری اطلاعات و ارتباطات و مدیریت فناوری در آینده است. در حالی که ابتدا، انقلاب فناوری اطلاعات و ارتباطات به عنوان

1. William Herschel
2. ICT Revolution

حرکتی مثبت و سودمند برای رشد اقتصادی در نظر گرفته می‌شد، در دههٔ ۱۹۹۰ با گسترش بدافزارها به عنوان یک تهدید و چالش جهانی برای صنایع و دولت‌ها، این تغییر الگو صورت گرفت. ممکن است در کتاب‌های تاریخی آینده از دههٔ ۲۰۰۰ ــ ۲۰۱۰ به عنوان یک نقطهٔ عطف تاریخی[1] یاد شود؛ هنگامی که بشر شاهد حملات سایبری حمایتگرانه برای پیشرفت‌های نظامی بود و از ابزارهای سایبری برای نخستین‌بار به منظور ایجاد اختلال و نابودی زیرساخت‌های فیزیکی بهره‌برداری شد.

در سال‌های ابتدایی فناوری اطلاعات و ارتباطات و اینترنت، این حقیقت که این پشتیبانی فنی نوین ممکن است به یک زیرساخت اساسی برای تمام اقتصادها و جوامع تبدیل شود قابل پیش‌بینی نبود. نقاط عطف بخصوصی دربارهٔ چگونگی توسعهٔ اینترنت و فناوری اطلاعات و ارتباطات به یک بستر مهم جهانی در پی معرفی نظام نام‌گذاری دامنه[2] و تجاری‌سازی اینترنت، انفجار محصولات نرم‌افزاری، رشد اقتصاد اینترنتی و سایر رویدادها وجود دارد که تمام این موارد نمایانگر وابستگی روزافزون به فناوری اطلاعات و ارتباطات است. توسعهٔ فناوری اطلاعات و ارتباطات در بخش خصوصی به سوی حمایت از استمرار مشاغل، تضمین دسترسی سریع به اطلاعات و اتصال پرسرعت سوق داده شده بود. با آنکه شرکت‌ها و دولت‌ها در حال توسعهٔ نظام‌های اطلاعاتی پیچیده‌ای بودند، غالباً در ابتدای امر به مسئلهٔ امنیت نمی‌پرداختند. اکنون متخصصان امنیت فناوری اطلاعات و ارتباطات بر این باورند که به دلیل پیچیدگی ساختار فناوری اطلاعات و ارتباطات در اکثر سازمان‌ها، دستیابی به امنیت صددرصد در هر یک از این نظام‌ها غیرممکن است. امروزه بهترین اقدام ممکن، شناسایی سریع بازدیدکنندگان ناخواسته در

---

1. Breaking Point
2. Domain Name System (DNS)

شبکه‌های رایانه‌ای است، زیرا همواره احتمال شکستن کدها و دسترسی غیرمجاز به هر یک از رایانه‌ها وجود دارد. متخصصان معتقدند که پیشگیری و دفاع تا حد زیادی با شکست مواجه شده و اکنون تمرکز اصلی متخصصان امنیت رایانه‌ای ردیابی و تفحص است. با وجود آنکه می‌بایست با پیشرفت‌های جدید فناوری به راه‌حل این مسئله دست یافت و این موضوع را در نشست‌های رمزنگاری و ریاضیات دانشگاهی بررسی کرد، سیاست‌گذاران همواره در شرایط فعلی فعالیت می‌کنند. حال آنکه سطح پایین امنیت فناوری اطلاعات و ارتباطات از ویژگی‌های فزایندهٔ این دامنهٔ ساخت بشر است.

با این حال، این تحولات رخ داده است و هرگز قادر نیستیم به زمان الواح سنگی، طومارهای کاغذی و ماشین‌های تحریر بازگردیم. کماکان کفهٔ رشد اقتصادی نشئت‌گرفته از فضای سایبری سنگین‌تر از کفهٔ نگرانی‌های امنیتی است و سیاست‌های امنیت سایبری به عنوان مسائل و دغدغه‌های اصلی رهبران ارشد ملی یا صنعتی محسوب نشده‌اند. میزان آگاهی عوام نیز از فضای سایبری و میزان وابستگی ما به آن و سیاست‌های داخلیِ به‌کارگرفته‌شده به منظور حفاظت از امنیت نظام‌های اطلاعاتی مهم بسیار ناچیز است.

اینترنت تنها جزء تشکیل‌دهندهٔ فضای سایبری نیست، بلکه از فناوری‌های مختلف، رایانه‌ها، تلفن‌ها، دستگاه‌ها، کابل‌های فیبر نوری، روترها[1]، نرم‌افزارها و ... تشکیل شده است که همگی در چرخهٔ توسعه‌ای ثابت و پرسرعت قرار دارند. دنیای فناوری توانسته است امکان اتصالات پرسرعت و روش‌های نوین دسترسی به اطلاعات و فرصت‌های شغلی زیادی را فراهم کند. فناوری اطلاعات و ارتباطات تمامی خدمات مهم و اساسی جوامع و اقتصاد، از جمله انرژی، ارتباط از راه دور، تأمین آب یا سیستم‌های کنترل هوا را تسهیل

1. Routers

می‌کند. امروزه تقریباً تمام خدمات ضروری به سیستم‌های اطلاعاتی وابسته‌اند و فناوری اطلاعات در همهٔ امور نفوذ یافته است. حتی بایگانی اسناد قرون وسطایی و همچنین پرونده‌های پزشکی و سایر اطلاعات شخصی حساس نیز در عصر حاضر دیجیتالی شده‌اند.

سیاست‌گذاران عمومی، با توجه به پیچیدگی مسائل فناوری، همواره در مرحلهٔ اولیهٔ شناخت نحوهٔ هدایت سیاست‌های امنیت سایبری ملی، محافظت از اسرار صنعتی یا دولتی و کمک به مقامات قانونی در مبارزه با جرایم سایبری به سر می‌برند. از آنجا که اکثریت قریب به اتفاق دارایی‌های مهم سایبری به بخش خصوصی تعلق دارد، هر گونه سیاست سایبری ملی موفقیت‌آمیز باید شامل همکاری تنگاتنگ دولتی ـ خصوصی و هماهنگی افقی بین بخش‌های صنعتی و ادارات دولتی باشد. حال آنکه هماهنگی سیاست سایبری ملی باید شامل مسائل سیاست خارجی و مسائل امنیتی نیز باشد. از آنجایی که سیاست‌های سایبری ملی همواره در حال شکل‌گیری است و دولت‌ها کماکان در جست‌وجوی یک قهرمان ملی برای هدایت فعالیت‌های سایبری هستند، سیاست خارجی به دشواری می‌تواند خود را در این زمینهٔ دشوار تثبیت کند. با توجه به فضای بین‌المللی حاکم که در آن تمامی اعلامیه‌های امنیت سایبری می‌بایست دربارهٔ حقوق بشر و سیاست‌های خارجی دیگر باشد، دیپلمات‌ها باید جزئی از محافل سیاست‌گذاری سایبری کشورها به شمار آیند. به طور کلی، دیپلمات‌ها باید محرک‌های مؤثری در سیاست سایبری باشند که دلایل آن در ادامه توضیح داده خواهد شد.

به احتمال زیاد، هر متخصص سیاست خارجی هنگام مواجهه با سیاست‌گذاران ملی با این بحث روبه‌رو می‌شود که هر حوزهٔ بخصوصی به شاخه‌ای از دانش تخصصی نیاز دارد که دیپلمات‌ها از آن بهره‌مند نیستند.

بنابراین، متخصصان هر حوزه باید تصمیمات لازم را أخذ کنند. این امر ممکن است در مباحث سایبری نیز صادق باشد که در آن همواره کنترل و ادارهٔ این حوزه از سیاست بر عهدهٔ جامعهٔ فنی ملی و وزارتخانه‌های مربوط است. به منظور تسهیل امور برای دیپلمات‌های فعال در این زمینه می‌توان این گونه استدلال کرد که چون عرصهٔ سایبری یک عرصهٔ مهم جهانی برای سایر فعالیت‌های بشری است، سیاست‌های جامع مربوط به مسائل سایبری به مشارکت متخصصان روابط بین‌المللی نیاز دارد. با توجه به اینکه مهندسان هسته‌ای در مذاکرات منع گسترش سلاح‌های هسته‌ای[1] نمایندهٔ دولت نیستند، کارشناسان فناوری نیز نباید به مسئلهٔ دیپلماسی سایبری بپردازند. همانند سیاست‌های سایبری داخلی، که طی آن مسائل سایبری باید در مدیریت بحران و محافظت از خدمات بحرانی مدنظر قرار گیرند، لازم است بنیان‌گذاران سیاست خارجی و دست‌اندرکاران امنیت ملی نیز مسائل سایبری را بیاموزند و آن‌ها را در فعالیت‌های معمول خود به کار گیرند.

به منظور قابل درک ساختن و شفاف‌سازی هر چه بیشتر عرصهٔ سایبری برای سیاست‌گذاران، برنامه‌ریزی سیاست‌های سایبری با در نظر گرفتن پیامدهای اختلال یا تخریب زیرساخت‌های سایبری یا ضرر اقتصادی ناشی از جرایم و جاسوسی سایبری مؤثر خواهد بود. پیشگیری و کاهش میزان خسارات و کاهش خطرات نظام‌مند در عرصهٔ سایبری مستلزم دخالت بنیان‌گذاران سیاست خارجی است. اساسی‌ترین نگرانی دیپلمات‌ها باید جلوگیری از عواقب احتمالی اختلال یا تخریب زیرساخت‌های اطلاعاتی در سطح جهانی و منطقه‌ای باشد. می‌توان انتظار داشت که تمامی عوامل مسئول بین‌المللی به دنبال جلوگیری از وقایع فاجعه‌بار عرصهٔ سایبری

1. Non-Proliferation Negotiations

باشند. با وجود این، از لحاظ نظری، برخی حملات سایبری ممکن است صدمات و آسیب‌هایی برابر با حملات جنبشی[1] به بار آورند. سازمان‌دهی درگیری منطقه‌ای و حملهٔ سیل‌آسا به همراه حملهٔ سایبری نقطه‌ای[2] یا حملهٔ فیزیکی به زیرساخت‌های اطلاعاتی، با هدف متضرر ساختن کشوری دیگر از لحاظ اقتصادی به دلایل سیاسی، قابل تصور است. چنانچه نظام مالی نیز به زیرساخت‌های اطلاعاتیِ حمله‌شده وابسته باشد، ممکن است موجب اختلالی جدی در خدمات مالی یک منطقه نیز بشود.

کشورهایی که از قابلیت دفاع سایبری متوسطی برخوردارند، نگرانی‌های بیشتری را تجربه می‌کنند، زیرا این رویکرد دوگانه سبب افزایش جرم و جنایت و نظامی‌سازی هر چه بیشتر حوزهٔ مربوط می‌شود. عدم تقارن کلی این حوزه، آسیب‌پذیری‌های غیرقابل‌قبولی برای سیستم‌های مهم اطلاعاتی خصوصی و عمومی ایجاد می‌کند. همچنین در درگیری‌های آینده ممکن است طی مبارزات نظامی یا در شرایطی دیگر، علیه زیرساخت‌های مهم یک کشور حملاتی سایبری صورت بگیرد. حملات سایبری‌ای که در جریان درگیری‌های مسلحانهٔ بین‌المللی اتفاق می‌افتند تحت نظارت حقوق بشردوستانهٔ بین‌المللی خواهند بود. در این شرایط، به منظور جلوگیری از تحت تأثیر قرار گرفتن افراد غیرنظامی، یافتن روش‌های مناسب یا محاسبهٔ تأثیرات ثانویهٔ کشورها باید از مقررات مربوط پیروی کنند. در واقع، عرصهٔ سایبری مباحث تازه‌ای را دربارهٔ نحوهٔ اعمال حقوق بشردوستانهٔ بین‌المللی ایجاد کرده است. بسیاری از وکلا بر این باورند که در زمینهٔ نظام‌مندسازی جنبه‌های بشردوستانهٔ یک درگیری، که موجب اختلال و آزار و اذیت افراد

---

1. Kinetic Attacks

۲. Surgical's Cyber Attack، حمله به هدفی مشخص است به طوری که هیچ گونه خسارتی به ساختارهای دیگر وارد نشود.

غیرنظامی در پی حملات سایبری شده، اما درگیری مسلحانه محسوب نمی‌شود، شکافی در حقوق بین‌المللی وجود دارد.

مسئلهٔ حل‌نشدهٔ دیگری نیز رویدادهای سایبری را، هم در زمان جنگ و هم در زمان صلح، پیچیده‌تر می‌کند. حتی در صورت موافقت کشورها با برخی هنجارها و قوانین، سهولت نسبی بهره‌برداری از بازیگران پراکسی[۱] می‌تواند آن‌ها را به انتخاب ابزار سایبری ترغیب کند. تا زمانی که کشورها در زمینهٔ نظارت بر جریان داده‌ها یا مبارزه با جرایم سایبری ضعیف عمل بکنند، چالش همچنان باقی است. به منظور کاهش تعداد پناهگاه‌های امن سایبری[۲] باید به صورت دسته‌جمعی وارد عمل شد.

طراحی سازوکارهای بین‌المللی برای روابط بین کشورها در زمینهٔ مسائل عرصهٔ سایبری عملاً به عهدهٔ عوامل سیاست خارجی خواهد بود. نخستین حرکت دیپلمات‌ها کاهش احتمال سوءتفاهم، سوء تفسیر و عدم اعتماد در روابط سایبری است. دیپلمات‌ها باید همراه با اجتماعات سایبری داخلی با هدف جلوگیری یا کاهش اختلالات سایبری بکوشند.

مسئلهٔ مهم سیاست امنیت ملی حمایت از زیرساخت‌های اساسی غیرنظامی است که احتمال دارد در درگیری‌های آینده بیشترین آسیب را متحمل شوند. در شرایطی که حدود ۸۰ ـ ۹۰ درصد زیرساخت‌های سایبری مهم متعلق به بخش خصوصی است، دولت‌ها باید در نظام‌های تاب‌آوری سایبری ملی[۳] سرمایه‌گذاری کنند. مشارکت‌های عمومی ـ خصوصی و چارچوب‌های مدیریت بحران در زمینهٔ امنیت سایبری باید به

---

۱. Proxy Actors، گروه‌ها و اشخاصی که به نیابت از یک کشور، علیه دولت‌ها اقدامات سایبری مخرب انجام می‌دهند.

2. Cyber Safe Heavens

3. National Cyber Resilience Systems

عنوان پاسخی به چشم‌انداز تهدیدهای تازه توسعه یابند. بخش خصوصی، برخی سازوکارهای مدیریت بحران سایبری را معرفی کرده است که تا کنون موفقیت‌آمیز بوده‌اند و دولت‌هایی که در آن‌ها بخش خصوصی نقش اصلی را به عهده دارد، نباید دخالت زیادی داشته باشند. جامعهٔ سیاست خارجی نیز می‌تواند در زمینهٔ اعتمادسازی بین ملت‌ها، ایجاد کانال‌های ارتباطی، و نشاندن احزاب مختلف بر سر میزهای مذاکره ایفای نقش کند؛ به ویژه جامعهٔ دیپلماتیک باید حساسیت بیشتری به حمایت از زیرساخت‌های مهم غیرنظامی در سراسر جهان داشته باشد. به منظور ایجاد پایگاه گسترده‌ای از قابلیت‌های سایبری غیرنظامی، وجود مکانیسم‌های پیشگیرانه و مدیریت بحران کارآمد، که ارکان یک نظام سایبری ملی را تشکیل می‌دهند، ضروری است. اغلب کشورهای پیشرفتهٔ سایبری پیشاپیش متوجه شده‌اند که تلاش‌های سنتی نظامی در درگیری‌های مدرن، که در آن فعالیت‌های گستردهٔ سایبری نقش اصلی را بازی می‌کنند، کافی نیستند. در مقابل، کشورهایی به دنبال سازوکارهای جدید مدیریت بحران‌های غیرنظامی و روش‌هایی برای سازمان‌دهی عوامل غیردولتی هستند که ممکن است نقش بنیادینی در درگیری‌های سایبری آینده داشته باشند.

عواقب ناشی از فعالیت‌های مخرب سایبری بیشتر از همه متوجه عوامل اقتصادی (شرکت‌ها و صنایع بخش‌های مختلف) است. فواید مالی، مجرمان سایبریِ صنعت بانکداری را به منظور تشکیل مراکز بازنشر اطلاعات امنیت سایبری و سرمایه‌گذاری بیشتر در جنبه‌های اعتباری، برای تأمین هزینه‌های جرایم سایبری، تجهیز کرده است. امروزه بسیاری از بخش‌های دیگر هم نفوذها و حملات مداومی را تجربه می‌کنند، زیرا جرایم سازمان‌یافته نیز به عرصهٔ سایبری راه یافته است. در صورتی که عوامل تحت حمایت دولت، که

دارای منابع اطلاعاتی قابل توجهی هستند، دربارهٔ شرکت‌های فعال در حوزهٔ خدمات‌رسانی تفحص کنند به کمک‌های بیشترِ دولت نیازمندند. به منظور تسهیل جرایم سنتی از ابزارهای سایبری به طور فزاینده‌ای استفاده می‌شود. اکثر شرکت‌های بزرگ در زمینهٔ حمایت سایبری سرمایه‌گذاری‌های گسترده‌ای انجام می‌دهند و خطر بروز جرایم سایبری را پذیرفته‌اند. حال آنکه شرکت‌های معدودی آمادگی افشای خسارات واقعی ناشی از حملات سایبری را دارند. این امر در طولانی‌مدت اثر بومرنگی یا بازگشتی دارد، زیرا در دسترس نبودن اطلاعات معتبر دربارهٔ جرایم سایبری مانع از واکنش سهامداران و سیاست‌گذاران عمومی در مواجهه با این تهدیدات روزافزون می‌شود.

کارشناسان قانونی از نظام سرمایه‌گذاری ناکافی در این حوزه که مبارزه با جرایم سایبری سازمان‌یافته را دشوارتر می‌کند شکایت دارند. از آنجا که «بو کشیدن» یا «لمس کردن» جرایم سایبری که در شبکه‌های رایانه‌ای صورت می‌گیرند دشوار است، مقامات دولتی از تأیید و واکنش به این تهدید جدید عقب مانده‌اند. در بیشتر کشورها، مسئولان اجرای قانون برای ردیابی جرایم سایبری روزافزون سخت در تلاش‌اند. شرکت‌های کوچک‌تر بیشترین خسارت را متحمل می‌شوند، زیرا از منابع کافی برای به‌روزرسانی سامانه‌های دفاع سایبری خود برخوردار نیستند. جنایتکاران با افزایش درآمدهای حاصل از جرایم سایبری جهانی سازمان‌یافته‌تر می‌شوند و ضرر اقتصادی ناشی از آن در طولانی‌مدت تهدیدی جدی برای دولت‌ها خواهد بود. دولت‌ها برای مبارزه با جرایم سایبری که تهدیدی برای امنیت داخلی و ملی و اقتصادی همهٔ کشورها محسوب می‌شوند، نیازمند قابلیت‌های خطیر ملی هستند.

هیچ یک از سازوکارهای ملی دولت‌ها در صورت بروز بحران سایبری گسترده یا در مبارزه با جرایم سایبری سازمان‌یافتهٔ بین‌المللی به تنهایی کافی

نیست. پرداختن به این نوع جرایم سایبری چالشی است که به وضوح به سطح نگران‌کننده‌ای رسیده است و باید جامعهٔ سیاست خارجی به آن توجه کند. به منظور اطمینان یافتن از وجود یک چارچوب قانونی مطلوب برای رسیدگی به جرایم سایبری در خارج از جهانِ توسعه‌یافته باید ارتقای کنوانسیون جرایم سایبری شورای اروپا[1] در فعالیت‌های دیپلماتیک گنجانده شود.

جاسوسی سایبری با اهداف اقتصادی، چالش دیگری را برای دولت‌ها از جمله دیپلمات‌ها به وجود آورده است. انتقال خاموش مالکیت معنوی ممکن است این خطر را در قالب جرایم سایبری ساده متوجه رونق اقتصادی کند. این امر به وضوح زمینهٔ دیگری است که در آن دخالت دیپلماتیک برای تأیید رفتار دولت که موجب تعیین هنجارهای عرصهٔ سایبری می‌شود ضرورت دارد. یقیناً درگیری‌های سایبری و دیگر موضوعات تهدیدآمیز بیشتر متوجه دیپلمات‌هایی است که در زمینهٔ رسیدگی به مسائل سیاستِ امنیتی آموزش دیده‌اند. بنابراین، دیپلمات‌ها نیز باید حمایت از مالکیت معنوی به صورت آنلاین و برخی دیگر از مسائل اقتصادی مرتبط با عرصهٔ سایبری را به خوبی بشناسند. کارشناسان حوزهٔ تجارت به طور فزاینده‌ای با موانع ناعادلانه‌ای در بازار مواجه هستند که برخی کشورها با تعیین استانداردهای محصولات حوزهٔ فناوری اطلاعات و ارتباطات در زمینهٔ امنیت ملی سبب ایجاد آن شده‌اند. این استانداردها برای جلوگیری از دسترسی بازار به تولیدکنندگان خارجی اعمال می‌شوند. در اینجا نیز اطلاع‌رسانی به دیپلمات‌ها از طریق مذاکرات تجاری مربوطه ضرورت دارد.

تحولات سایبری فعلی، عرصهٔ ناشناختهٔ دیگری را برای دیپلمات‌ها مطرح می‌سازند که همان حکمرانی اینترنت است. این حوزهٔ پیچیدهٔ

---

1. Council of Europe (CoE)

نوآوری‌ها و انجمن‌ها عمدتاً متعلق به فناوران است. اما توجه جامعهٔ سیاست خارجی باید هر چه بیشتر به این حوزه معطوف گردد، زیرا چندین کشور الگوی چندذی‌نفعی فعلی حکمرانی اینترنت را تحت فشار قرار داده‌اند. اختلافات دربارهٔ حاکمیت ملی رو به افزایش است و دیپلمات‌ها باید در حل‌وفصل این اختلاف در مجامع بین‌المللی نقش بسزایی داشته باشند.

دیپلمات‌ها همچنین باید به روندهای آتی تحولات سایبری توجه داشته باشند. آمادگی سایبری دولت‌ها در آینده به موضوع اصلی تصمیمات تجاری بدل خواهد شد. قابلیت‌های سایبری قدرتمند ملی عامل بازدارندهٔ مهمی برای مجرمان سایبری خواهد بود و ارائهٔ بسترهای امن به ایجاد یک فضای تجاری مناسب‌تر کمک خواهد کرد. بخش خصوصی ممکن است به دنبال آمادگی ملی امنیت سایبری در زمینهٔ راهبردهای سرمایه‌گذاری آتی باشد. کشورهایی که شاخص سایبری ضعیفی دارند مناسب نخواهند بود. به نوعی، امنیت سایبری می‌تواند به بخشی از سیاست اقتصادی خارجی برای جذب سرمایه و استعداد تبدیل شود. اگرچه دست‌اندرکاران خصوصی باید بیشتر اقداماتِ تاب‌آوری را انجام دهند، اما دولت‌ها بایستی توانایی شایان خود را در واکنش به تهدیدات سایبری نظام‌مند تضمین کنند. توسعهٔ ساختارهای هشدار و مشاورهٔ زودهنگام بین‌المللی و منطقه‌ای در زمینهٔ امنیت سایبری مسئلهٔ درازمدت دیگری است که دولت‌ها با آن روبه‌رو خواهند شد. این امر بدون دخالت جوامع دیپلماتیک سراسر جهان میسر نمی‌شود.

در حال حاضر، تعداد کشورهایی که در آن‌ها هماهنگی سایبری ملی کارآمد بوده است و قادر به ارائهٔ نظر یکپارچه و متحدانهٔ خود در تمامی مجامع بین‌المللی‌اند، بسیار محدود است. چالش‌های معمولی که تمامی دیپلمات‌ها با آن روبه‌رو هستند عبارت‌اند از: چالش ساختاری هماهنگی

سیاست ملی ضعیف، عدم همکاری و ارتباط[1] نهادی سیاست سایبری، سردرگمی و ابهام میان‌بخشی در خصوص رهبری ملی، آژانس‌های قدرتمند داخلی که نظریات سیاست خارجی را مردود شمرده‌اند و مدنظر قرار نمی‌دهند و همچنین نبود ژنرال‌های سایبری که قادر به تفسیر و شفاف‌سازی اصطلاحات فنی برای دیپلمات‌ها هستند. چنانچه دولت دارای راهبرد، سایبری ملی نداشته نباشد و هیچ گونه هماهنگی سایبری ساختاری در آن وجود نداشته نباشد، ارائهٔ گزینه‌های سیاسی آگاهانه برای جامعهٔ سیاسی بسیار دشوار خواهد بود. تدوین یک راهبرد ملی امنیت سایبری و ایجاد چارچوبی برای هماهنگی سایبری که بخش‌های اصلی دولت بتوانند در آن ایفای نقش کنند، فرایندی ضروری برای تمامی ملت‌هاست.

دیپلمات‌ها باید به طور منظم نظریات خود را با سیاست‌گذاران ملی حوزهٔ سایبری، واحدهای جنایی با فناوری پیشرفته، وکلا، آژانس‌های محافظت از زیرساخت‌های اطلاعاتی اساسی، مسئولان پاسخگویی به حوادث سایبری ملی و تحلیلگران اطلاعاتی هماهنگ سازند تا به یک دیدگاه کلی و درک درست از این حوزهٔ درحال‌توسعه دست یابند. همچنین این افراد، جدا از جزئیات عملکرد، به منظور شناسایی و تشخیص استدلال‌های سطحی ارائه‌شدهٔ سایر کشورها در مجامع بین‌المللی باید از نحوهٔ عملکرد فناوری آگاهی پیدا کنند، و نیز باید از روند تنظیم مقررات سایبری ملی و توسعهٔ تهدیدات سایبری در سطح جهان اطلاع داشته باشند. دیپلمات‌های سایبری نیز مانند دیپلمات‌های هسته‌ای باید آثار ابزارهای سایبری مخرب و نحوهٔ استفاده از زیرساخت‌های اساسی را برای فلج کردن و از کار انداختن کشورها در درگیری‌های پیش رو به خوبی بشناسند. کمال مطلوب آن است که جامعهٔ سیاست خارجی بتواند

---

1. Silfication

سالانه در بخشی از فعالیت‌های سایبری ملی مشارکت داشته باشد و از روش‌های حملات سایبری گستردهٔ بین‌المللی آگاهی پیدا کند.

از آنجا که در حال حاضر در جهانی به سر می‌بریم که در آن سیاست‌های سایبری همواره در حال رشدند و اکثریت کشورها تا به حال نتوانسته‌اند به یک راهبرد سایبری ملی جامع دست یابند، ممکن است از نظر جامعهٔ سیاست خارجی، به استحکام رسیدن در این عرصه دشوار باشد. حال آنکه برای آیندهٔ فضای سایبری آزاد و بدون حاشیه، فعالیت هر چه بیشتر دیپلمات‌ها در این زمینه ضرورت دارد. مدت‌زمان مدیدی است که جامعهٔ فنی هدایت تحولات بین‌المللی این حوزه را به عهده دارد. اکنون زمان آن فرارسیده است که هر دو سیاست‌های سایبری داخلی و بین‌المللی را در بستر راهبردی روابط بین‌الملل، تحولات اقتصادی بین‌المللی و امنیت ملی قرار دهیم. بدین منظور به تصمیم‌گیرندگان ارشد ملی، دیپلمات‌ها، وکلا و سایر جوامع غیرفنی نیازمندیم تا هر چه سریع‌تر در این زمینهٔ سیاسی جدید به آگاهی دست یابند و مشارکت در مباحث سایبری را در عرصهٔ جهانی از سر گیرند.

دستور کار فعلی روابط سایبری بین‌المللی

با توجه به آنچه در بالا به آن اشاره شده و نیز چشم‌اندازی که از تحولات مربوط به دنیای سایبری وجود دارد، پنج محور ذیل را می‌توان به عنوان مهم‌ترین دستور کار دیپلماسی سایبری، با تأکید بر نقشی که دیپلمات‌ها باید در آن ایفا کنند، پیشنهاد داد:

- **امنیت بین‌المللی و اعتمادسازی در عرصهٔ سایبری**

اعتماد و اطمینان مقوله‌های کمیابی در عرصهٔ سایبری هستند. در این حوزه

رقابت‌های دیرین و تازه‌ای نیز بین کشورها جریان دارد. درگیری‌های بین‌المللی اخیر شامل ابعاد سایبری بوده‌اند و ما شاهد یک درگیری مسلحانهٔ بین‌المللی بوده‌ایم که طی آن، حملات سایبری با پیشرفت‌های نظامی هماهنگ شده بودند.

برخلاف عقیدهٔ عمومی که جنگ سایبری به تازگی از جنبه‌های تاریک نشئت گرفته است، تاریخِ درگیری‌های فضای سایبری به دههٔ ۱۹۸۰ بازمی‌گردد. دولت‌ها ابزارهای سایبری را برای دست‌کاری در سیستم‌های فناوری اطلاعات و ارتباطات و بازیابی اطلاعات سرّی و حساس دولتی و نظامی، به مدت ۲۵ سال توسعه بخشیدند. از زمان روی کار آمدن سیستم‌های رایانه‌ای، دولت‌ها درحال‌توسعه و دستیابی به ابزارهای پیشرفتهٔ سایبری بودند. کشورهایی که نظامیان قدرتمندی دارند، در زمینهٔ حفاظت از سیستم‌های اطلاعاتی، که از اسرار امنیت ملی و امنیت سلاح‌های هسته‌ای محافظت می‌کنند، سرمایه‌گذاری‌های کلانی انجام داده‌اند. برخی کشورها با استفاده از فناوری اطلاعات و ارتباطات برای مقاصد دفاعی و تهاجمی، قابلیت‌های قابل توجهی را توسعه داده‌اند. تا همین اواخر، معمولاً به خوبی از این ابزارها محافظت می‌شد و فقط برای اهداف دولتی و نظامی مورد استفاده قرار می‌گرفت.

دست‌اندرکارانِ بخش خصوصی به طور فزاینده‌ای متوجه وجود بدافزاری در سیستم‌های خود شده‌اند که سطح پیچیدگی آن ورای توانایی متخلفان است. به عبارت دیگر، وارد دوره‌ای از اختلالات و خرابکاری‌های سایبری شده‌ایم که زیرساخت‌های مهم غیرنظامی، هدف احتمالی خواهند بود. همچنین برخی دولت‌ها از ابزارهای سایبری پیشرفته برای جاسوسی صنعتی استفاده می‌کنند که به خسارات سنگین در مالکیت معنوی شرکت‌ها

منجر می‌شود. بنابراین، دیپلمات‌ها موظف به نظم‌دهی بـه دامنـهٔ سـایبری و توافق بر سر برخی قوانین در خصوص نحوهٔ رفتار عوامل دولتی هستند.

به دلیل پیچیدگی و عدم تقارن در عرصهٔ سایبری، دولت‌ها در شناسـایی بموقع عوامل حملات سایبری با چالش مواجه شده‌انـد. حملـهٔ سـایبری بـا توجه به انگیزه‌های پشت آن می‌تواند جـرم سـایبری، شـورش سـایبری یـا جنگ سایبری تلقی شود. هـر یـک از آن‌هـا مـی‌توانـد بسـیاری از جوامـع سایبری داخلی را به طور هم‌زمان تحت تأثیر قرار دهـد و شناسـایی بموقـع متجاوزان بی‌نام‌ونشان دشوار است. بنابراین، دولـت‌هـا بـرای جلـوگیری از سوء تفسیر احتمالی دربارهٔ حوادث سایبری و همچنین تشدید غیرضـروری اوضاع، به ایجاد اعتمـاد و اطمینـان در روابـط سـایبری سیاسـی ـ نظـامی پرداخته‌اند. در حال حاضر، اقـدامات اعتمـادسـازی در عرصـهٔ سـایبری در سازمان امنیت و همکاری اروپا و در اتحادیهٔ آسه‌آن بررسی می‌شود.

برخی دولت‌ها برای تنظیم رفتار عوامل دولتی در عرصهٔ سایبری خواسـتار معاهدات و کنوانسیون‌های جدید سایبری شده‌اند. این رویکرد ممکـن اسـت برای افراد تازه‌کار در حوزهٔ سیاست سایبری که پیچیدگی‌هـای ایـن مسـئله را بـه درسـتی درک نمـی‌کننـد جالـب توجـه باشـد. متأسـفانه بـه دلیـل تعـدد دست‌اندرکاران و استفادهٔ دوگانه از فناوری اطلاعات و ارتباطات، توسعهٔ یـک کنوانسـیون سـایبری جهـانی تقریبـاً غیـرممکن اسـت. از آنجـا کـه فنـاوری اطلاعات و ارتباطات ماهیتی غیرنظامی دارد، تأیید هر گونه پیمـان تسـلیحاتی سایبری دست‌کم با فناوری قابل دسترس در زمان حـال امکـان‌پـذیر نخواهـد بود، حتی در صورت موافقت، کشورها با خط‌مشی منع انجـام اقـدام نخسـت[1] همواره قادر خواهند بود عاملی نیابتی برای انجام چنـین فعالیـت‌هـایی بیابنـد.

1. Non-First Use Policy

اعلام عرصهٔ سایبری به عنوان میراث جهانی بشریت که اعمال تجاوزگرانـه در آن ممنوع است و تخصیص منابع بیشتر بـه مبـارزه بـا جـرایم سـایبری ایـدهٔ بهتری است. با آنکه ممکن است کمی ایدئال به نظر برسد، این پیش‌فـرض را نیز مطرح می‌کند که عوامل مهم بین‌المللی «پناهگـاه‌هـای امنـی» را در اختیـار مجرمان سایبری قلمرو خودشان قرار نمی‌دهند.

دلیل دیگر عدم پشـتیبانی دموکراسـی‌هـای لیبـرال از توسـعهٔ پیمـان یـا کنوانسیون سایبری مبتنی بر این فرض است که از آن به عنوان یک دستاویز بین‌المللی برای مشروعیت بخشیدن به سانسور در عرصـهٔ سـایبری اسـتفاده خواهد شد. در مقابل، غرب پافشاری خواهد کـرد کـه حقـوق بـین‌المللـی بشردوستانه در عرصهٔ سایبری اعمال شـود. بـه جـای پیمـان، بایـد دربـارهٔ مجموعه‌ای از هنجارها که در آینده به کاهش درگیری‌هـای سـایبری کمـک خواهد کرد تفاهم حاصل شود.

در سـال ۲۰۰۹، مرکـز عـالی دفـاع سـایبری نـاتو[1] بـه منظـور تحلیـل چگونگی اعمال حقوق بین‌المللی بشردوسـتانه در عرصـهٔ سـایبری، گـروه مستقلی از حقوق‌دانان بین‌المللی تشکیل داد. در سـال ۲۰۱۳، فعالیـت‌هـای این گروه متشکل از سی متخصص برجستهٔ حقوق بین‌المللی بـا سرپرسـتی مایکل اشمیت،[2] وکیل ایالات متحده، منتشر شد. این کتابچه بیـانگر نخسـتین گام مؤثر و سودمند در زمینهٔ تحلیل حقوقی گسترده‌تر قوانین اعمال‌شده بـر درگیری‌های احتمالی عرصهٔ سایبری است. فراتر از آن، این کتاب در مسـیر هدف سیاسی کاهش فشار برای توسعهٔ پیمان جهانی جنگ سایبری است.

توسـعهٔ اقـدامات اعتمادسـاز، بـه عنـوان نخسـتین مجموعـهٔ هنجارهـای

1. The NATO Cooperative Cyber Defence Center of Excellence
2. Michael Schmitt

سایبری، نتیجهٔ گفت‌وگوهای سازمان امنیت و همکاری اروپا در حوزهٔ مباحث سایبری است. به احتمال زیاد، مذاکرات ۱۷ مارچ ۲۰۰۹ در وین نقطهٔ عطف دیپلماسی سایبری معاصر بوده است. به دنبال طرح ابتکاری ارائه‌شده توسط استونی در دورانی که این کشور ریاست مجمع همکاری‌های امنیتی سازمان امنیت و همکاری اروپا را به عهده داشت، یک کارگاه امنیت سایبری در سال ۲۰۰۸ تشکیل شد. این کارگاه به خصوص زمانی که رؤسای آژانس‌های سایبری ملی با شرکت در کارگاه سازمان امنیت و همکاری اروپا سعی داشتند اقدامات قابل اجرا در این مجمع را شناسایی کنند، به پیدایش دیپلماسی سایبری اشاره داشت. از آن زمان، توسعهٔ دستور کار دیپلماسی سایبری بین‌المللی آغاز شد. سازمان امنیت و همکاری اروپا در سال‌های ۲۰۰۹ – ۲۰۱۰، چندین نشست مهم دیگر در زمینهٔ امنیت سایبری برگزار کرده‌اند. مضامین اصلی این مباحث شامل آگاهی از امنیت سایبری، تعیین رفتار مسئولانهٔ دولت در فضای سایبری و نیاز به ظرفیت‌های ملی برای مقابله با تهدیدات سایبری بود. پس از سال ۲۰۰۹، هنگامی که دولت اوباما خط‌مشی سایبری جدید بین‌المللی ایالات متحده را اعلام کرد، دولت آمریکا پیشبرد دستور کار سایبری سازمان امنیت و همکاری اروپا را آغاز نمود. نشست مشترک مجمع همکاری‌های امنیتی سازمان امنیت و همکاری اروپا و شورای دائمی سازمان امنیت و همکاری اروپا که در ماه جون ۲۰۱۰ برگزار شد، رویدادی مؤثر در زمینهٔ هموارسازی راه برای مذاکرات راهبردی امنیت سایبری بود. در این جلسه، ایالات متحده بحث و گفت‌وگو دربارهٔ هنجارهای مربوط به رفتار دولت را پیشنهاد داد. در نشستی مشابه در سال ۲۰۱۱، ایالات متحده پیشنهاد آغاز اقدامات اعتمادسازی دربارهٔ امنیت سایبری را مطرح کرد. روند موازی تکمیل گزارش گروه کارشناسان دولتی سازمان ملل در سال ۲۰۱۰ نیز حاکی از آن بود که اجماع کافی دربارهٔ

اقدامات اعتمادساز در عرصهٔ سایبری وجود دارد. در آپریل ۲۰۱۲، یک گروه غیررسمی سازمان امنیت و همکاری اروپا با ریاست ایالات متحده آمریکا و تحت نظارت کمیتهٔ امنیت ایجاد شد. روند کار در سازمان امنیت و همکاری اروپا همچنان ادامه دارد و توجه بسیاری از دولت‌های دیگر را در زمینهٔ پشتیبانی از رویکرد مبتنی بر هنجارها به خود جلب کرده است. سازمان امنیت و همکاری اروپا نخستین سازمانی است که هنجارهای سایبری را در یک چارچوب گسترده‌تر و چندجانبه به بحث و گفت‌وگو می‌گذارد. مرحلهٔ بعدی احتمالی رسیدگی به این موضوع در قالب اتحادیهٔ منطقه‌ای آسه‌آن است؛ جایی که چین نیز در آن کرسی دارد.

به موازات مباحثات سازمان امنیت و همکاری اروپا، روسیه و ایالات متحده به دنبال برگزاری برخی نشست‌های دوجانبه دربارهٔ نخستین مجموعهٔ اقدامات اعتمادساز سایبری، از جمله خطوط فوریتی و اقدامات دیگر، به توافق رسیده‌اند. کشورهای دیگر نیز ممکن است در حال بحث و گفت‌وگو دربارهٔ توافقات دوجانبهٔ مشابهی باشند.

تقریباً هم‌زمان با توسعهٔ سازمان امنیت و همکاری اروپا، مذاکرات سایبری بین‌المللی در سازمان ملل آغاز شد. در چارچوب سازمان ملل، مذاکرات بر سر امنیت سایبری در کمیتهٔ خلع سلاح صورت گرفته است. در سال ۲۰۰۹، قطعنامهٔ ۶۴/۳۸۶ سازمان ملل با عنوان تحولات حوزهٔ اطلاعات و ارتباطات در زمینهٔ امنیت بین‌المللی[1] به تصویب رسید.[2] این قطعنامه از کشورها خواسته است تا مذاکرات مربوط به امنیت سایبری را ادامه دهند و

1. ‘Developments in the Field of Information and Telecommunications in the Context of International Security’.

2. UNGA, Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/64/386, 2 July 2009.

یک گروه از متخصصان دولتی غیررسمی برای ارائهٔ توصیه‌های بیشتر تشکیل دهند. در سال ۲۰۱۰، گروه کارشناسان دولتی سازمان ملل متحد دربارهٔ تحولات حوزهٔ اطلاعات و ارتباطات در زمینهٔ امنیت بین‌المللی[1] گزارشی را تهیه کردند که طی آن از کشورها خواسته شده بود به منظور کاهش خطرات سایبری، همکاری‌های بین‌المللی را ارتقا بخشند و گفت‌وگو را بین کشورها تقویت کنند. در این گزارش اشاره شده است که دولت‌ها در حال فراهم آوردن ابزار جنگ سایبری هستند و افراد و سازمان‌های جنایتکار احتمالاً به عنوان نایب و نماینده، از این ابزارها استفاده می‌کنند. این گزارش خواستار کاهش خطرات جهانی، تداوم مذاکرات و همچنین حمایت از ظرفیت‌سازی در کشورهای کمترتوسعه‌یافته است. گزارش سال ۲۰۱۰ سازمان ملل متحد دربارهٔ امنیت سایبری حاکی از اجماع و توافقی عمومی است که حقوق بشردوستانهٔ بین‌المللی بر عرصهٔ سایبری اعمال می‌کند. به محض رسیدن حملات سایبری به آستانهٔ یک حملهٔ مسلحانه، کشورها باید طبق قوانین جنگی رفتار کنند. این امر اصول مختلفی نظیر تمایز بین اهداف نظامی و غیرنظامی، تناسب و ... را شامل می‌شود. تعیین زمان دقیق رسیدن حملهٔ سایبری به آستانهٔ یک حملهٔ مسلحانه بسیار دشوارتر است. گزارش سال ۲۰۱۰ تأیید کرد که مادهٔ ۵۱ منشور سازمان ملل متحد دربارهٔ دفاع از خود در صورتی اعمال می‌شود که حملات سایبری عواقبی مشابه با یک حملهٔ مسلحانه داشته باشد. دور بعدی مذاکرات گروه کارشناسان دولتی سازمان ملل متحد در آگوست ۲۰۱۲ برگزار شد. گزارش ارائه‌شدهٔ گروه کارشناسان دولتی سازمان ملل در سال ۲۰۱۳ همچنان بر لزوم همکاری و اعتمادسازی به منظور افزایش سطح اعتماد به عرصهٔ سایبری تأکید دارد؛ همچنین کاربرد

1. UNGA, Report of UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/65/94, 24 June 2010.

قوانین بین‌المللی، به ویژه منشور سازمان ملل، را تأیید می‌کند. این گزارش، با تصدیق فعالیت‌های ظرفیت‌سازی، دولت‌ها را موظف به مسئولیت‌پذیری در قبال اقدامات نادرست بین‌المللی انجام‌شده از قلمرو آن‌ها می‌داند. به طور کلی، گزارش گفته‌شده در زمینهٔ فرایند هنجارسازی در عرصهٔ سایبری است.

- **طرح‌های بین‌المللی در زمینهٔ مبارزه با جرایم سایبری**

با توجه به پیچیدگی حملات جنایتکارانهٔ سایبری و مداخلهٔ حوزه‌های قضایی متعدد در اکثر حوادث سایبری، مقابله با این تهدید جدید بدون همکاری گستردهٔ بین‌المللی برای نیروی انتظامی و سایر مقامات دولتی بسیار دشوار است. بررسی و پیگرد قانونی جرایم سایبری فراملّی دشوار است. بسیاری از کشورهای جهان قادر به رسیدگی به جرایم سایبری در قلمرو خود نیستند و می‌توانند به پناهگاه امنی برای مجرمان سایبری یا عوامل نیابتی سایبری تبدیل شوند.

در سال‌های اخیر، شبکه‌های جنایتکار سایبری توسعه‌یافته با گروه‌های جنایی سازمان‌یافته ادغام شده‌اند. شبکه‌های بین‌المللی جرایم سایبری سازمان‌یافته قدرتمندتر گشته و باعث افزایش آسیب‌پذیری اقتصادهای پیشرفتهٔ صنعتی و همچنین کشورهای نوظهور شده‌اند. کشورهای متخاصم یا گروه‌های تروریستی نیز ممکن است از شبکه‌های جرایم سایبری استفاده کنند. بنابراین، به منظور یاری‌رسانی به مقامات قانونی در مقابله با این تهدید روزافزون، مبارزه با جرایم سایبری باید در محوریت هر گونه فعالیت سیاست خارجی سایبری جای گیرد. تحقیقات موفقیت‌آمیز در زمینهٔ جرایم سایبری مستلزم همکاری گستردهٔ بین‌المللی قوهٔ قضاییه و نیروی انتظامی است. در برخی مناطق، ضعف نیروی انتظامی در برخورد با سازمان‌های جنایتکار سایبری سبب ایجاد یک چالش جهانی می‌شود. دستیابی به مناطق فاقد واحدهای جرایم فناورانهٔ پیشرفته و چارچوب‌های قانونی برای پیگرد جرایم سایبری دشوار است.

امروزه، چندین سازمان بین‌المللی و بخش خصوصی و دست‌اندرکاران نیروی انتظامی در زمینهٔ اقدامات نظام‌مند مقابله با جرایم سایبری در سطح جهان تلاش‌های چشمگیری انجام داده‌اند. شورای اروپا به دنبال ترویج کنوانسیون جرایم سایبری شورای اروپا، با ظرفیت‌سازی در عدالت کیفری و آموزش کارمندان قضایی و نیروی انتظامی، با حدود ۱۲۰ کشور ارتباط برقرار کرده است. بسیاری دیگر از سازمان‌های بین‌المللی و کشورهای صنعتی در آموزش نیروی انتظامی در کشورهای درحال‌توسعه مشارکت دارند.

به احتمال زیاد مؤثرترین ابزار بین‌المللی در امنیت سایبری، کنوانسیون جرایم سایبری گفته‌شده (کنوانسیون بوداپست) است که در سال ۲۰۰۱ در اختیار امضاکنندگان قرار گرفت. این کنوانسیون راهنمایی‌های سودمندی دربارهٔ حداقل چارچوب‌های قانونی ملی و الزامات اساسی همکاری بین‌المللی ارائه می‌دهد. در حال حاضر، ۵۱ کشور این کنوانسیون را امضا کرده‌اند که از این تعداد، ۴۰ کشور کنوانسیون را به تصویب نیز رسانده‌اند. بسیاری از کشورهای خارج از اروپا از دستورالعمل‌های این کنوانسیون پیروی کرده‌اند. اهمیت سیاسی کنوانسیون در این واقعیت نهفته است که این کنوانسیون تنها توافق‌نامهٔ بین‌المللی الزام‌آور در حوزهٔ مسائل سایبری است. کشورهایی که به کنوانسیون ملحق شده‌اند آمادگی هماهنگ‌سازی قوانین داخلی و مبارزهٔ جدی با جرایم سایبری را دارند. شورای اروپا به همراه بخش خصوصی و کشورهای عضو، در زمینهٔ تبلیغ کنوانسیون در سراسر جهان، یک پروژهٔ جهانی در زمینهٔ جرایم سایبری راه‌اندازی کرده‌اند.[1]

1. Council of Europe, Cybercrime Website: http://www.coe.int.

بسیاری از کشورهای خارج از اروپا، در آسیا و آمریکای لاتین، از این کنوانسیون الگوبرداری کرده و اصلاحات قانون‌گذاری را انجام داده‌اند. تعداد روزافزون کشورهایی که به این کنوانسیون می‌پیوندند، عامل بازدارندهٔ قابل توجهی برای گروه‌های جنایتکار است. علاوه بر ترویج کنوانسیون، شورای اروپا به آموزش مقامات نیروی انتظامی و قضایی پرداخته و دستورالعمل‌هایی برای امنیت سایبری ملی صادر کرده است. سالانه کنفرانس‌های اختاپوس[1] در زمینهٔ مبارزه با جرایم سایبری با شرکت تعداد زیادی از مقامات مهم بین‌المللی برگزار می‌شوند.

در این پروژهٔ جهانی، چندین برنامهٔ مفید منطقه‌ای و ملی تأمین مالی می‌شوند. پروژهٔ مشترک اتحادیهٔ اروپا و شورای اروپا در خصوص رسیدگی به جرایم سایبری در کشورها پیش از ورود به اتحادیهٔ اروپا، طی سال‌های ۲۰۱۰ ــ ۲۰۱۳ بر خط‌مشی‌ها و راهبردهای جرایم سایبری متمرکز شد. علاوه بر این، به هماهنگ‌سازی قانون‌گذاری و آموزش نیروی انتظامی و همکاری این نیرو با ارائه‌دهندگان خدمات اینترنتی نیز کمک کرده است. در آپریل ۲۰۱۱، پروژهٔ منطقه‌ای همکاری شرقی[2] اتحادیهٔ اروپا و شورای اروپا در زمینهٔ جرایم سایبری آغاز شد. این پروژه به ارائهٔ مشاوره در خصوص قانون‌گذاری جرایم سایبری، آموزش نیروی قضایی و انتظامی، تحقیقات مالی و همکاری‌های بین‌المللی پرداخت. یک پروژهٔ جدید اتحادیهٔ اروپا و شورای اروپا برای مقابله با جرایم سایبری با ابعاد جهانی در سال ۲۰۱۳ راه‌اندازی شد.

---

۱. Octopus Conferences، این کنفرانس، که شورای اروپا هر ۱۲ تا ۱۸ ماه برگزار می‌کند، یکی از بزرگ‌ترین سکوهای تبادل نظر در حوزهٔ جرایم سایبری است.

۲. Eastern Partnership، ابتکار عمل مشترک سرویس اقدام خارجی اتحادیهٔ اروپا به همراه اتحادیهٔ اروپا و کشورهای عضو آن و شش شریک اروپای شرقی.

در سال ۲۰۱۳، اتحادیهٔ اروپا دستورالعمل حمله به سیستم‌های اطلاعاتی[1] را به تصویب رساند. این بخشنامه به دنبال هماهنگی قوانین جزایی در سراسر اتحادیهٔ اروپاست. همچنین تلاش‌های مقامات انتظامی و قضایی در اتحادیه اقدام علیه این نوع جرم را تسهیل می‌کند. همچنین این پرونده به بررسی تناقضات موجود در قانون کیفری کشورهای عضو و لزوم همکاری مؤثر پلیس در اتحادیه می‌پردازد. علاوه بر قوانین بهبودیافتهٔ جرایم سایبری، اتحادیهٔ اروپا دارای شبکه‌ای کارآمد از واحدهای ملی جرایم سایبری است. رؤسای این واحدهای ملی به طور مرتب، تحت عنوان رسمی کارگروه واحدهای جرایم فناوری پیشرفته اتحادیهٔ اروپا[2] با یکدیگر ملاقات می‌کنند. این کارگروه با دایره‌های جرایم فناوری پیشرفتهٔ پلیس اروپا (یوروپل) و پلیس بین‌الملل (اینترپل) همکاری نزدیکی دارد و با ایالات متحده و سایر همتایان بین‌المللی خود ارتباط برقرار می‌کند. به منظور کمک به تحقیقات جرایم سایبری و تبادل اطلاعات بین کشورهای عضو، مرکز جرایم سایبری اتحادیهٔ اروپا[3] در سال ۲۰۱۳ در یوروپل تأسیس شد. هدف این مرکز کمک به تحقیقات مشترک، حمایت از ظرفیت‌سازی جهانی در آموزش اجرای قانون و گرد هم آوردن مقامات اجرای قانون برای سایر فعالیت‌هاست.

شبکهٔ جی-۸ (۲۴/۷)[4] برای جرایم سایبری فهرست کارآمدی را از نقاط تماس در اختیار مقامات اجرای قانون قرار می‌دهد. این امر همکاری عملیاتی در انجام تحقیقات و پی گرد قانونی جرایم فناوری پیشرفته را تسریع می‌کند.

---

1. Directive on Attacks on Information Systems
2. EU High Tech Crime Units Taskforce
3. EU Cybercrime Centre
4. G-8 24/7 Network

دفتر مقابله با مواد مخدر و جرم سازمان ملل متحد[1] نیز مدت زیادی است که به بررسی مسائل جرایم سایبری پرداخته است؛ خصوصاً از طریق نشست گروه متخصصان بین دولتی[2] که به انجام مطالعهٔ جامعی در حوزهٔ جرایم سایبری موظف بودند. در دفتر مقابله با مواد مخدر و جرم سازمان ملل متحد، برخی کشورها خواستار ابزار قانونی بین‌المللی جدیدی در خصوص جرایم سایبری شدند. با توجه به پیچیدگی‌های ورود به مباحث مربوط به یک ابزار جدید جهانی که مستلزم زمان و تلاش مضاعف خواهد بود، عاقلانه‌تر است که تأثیر کنوانسیون بوداپست را، که هم‌اکنون در دسترس است، در سطح جهانی گسترش دهیم.

- **ظرفیت‌سازی در امنیت سایبری و پرداختن به جرایم سایبری**

ظرفیت‌سازی در امنیت سایبری یکی از حوزه‌های سیاست‌گذاری است که به عنوان اولویتی برای دستیابی به فضای سایبری جهانی معتبرتر مطرح شده است. در کنفرانس سئول در حوزهٔ سایبری در سال ۲۰۱۳، یکی از مهم‌ترین مباحث و نتیجه‌گیری‌ها فراخوانی همهٔ کشورها برای مشارکت در ظرفیت‌سازی در امنیت سایبری بود. با آنکه به نظر می‌رسد این فراخوانی یکی از موضوعات سایبری جهانی مسلّم و بی‌چون‌وچراست، اما دستور کار بین‌المللی آن همواره در مرحلهٔ شکل‌گیری است. دو دوره از نشست‌ها پیش از کنفرانس سئول برگزار شد. کماکان هیچ گونه بررسی منسجمی دربارهٔ نتایج جلسات و جزئیات آن صورت نگرفته است. همچنین در مورد ظرفیت‌سازی سایبری شفاف‌سازی مفهومی انجام نشده است.

عدم برخورداری برخی کشورها از توانایی‌های فنی، آمادگی یا

1. The United Nations Office on Drugs and Crime (UNODC)
2. Intergovernmental Expert Group

چارچوب‌های قانونی برای مقابله با تهدیدات سایبری موضوع تازه‌ای نیست. امروزه بسیاری از سیاست‌گذاران به دنبال الگوهای ساختاردهی به فعالیت‌های ظرفیت‌سازی، روش‌های بکارگیری و چگونگی سنجش کارایی این قبیل فعالیت‌ها هستند.

چند مسئلهٔ مهم در رابطه با ظرفیت‌سازی وجود دارد که باید سیاست‌گذاران به آن توجه کنند: نخست، ظرفیت‌سازی در امنیت سایبری ملی باید با تلاش برای ایجاد ارتباطات و شبکه‌های ارتباطیِ جهانیِ امن‌تر و مطمئن‌تر همراه باشد. هدف اصلی آن است که ضمن گسترش شبکه‌های ارتباطی به بازارهای جدید، باید انتخاب معماری فناوری اطلاعات و توسعهٔ نرم‌افزاری نیز به عناصر امنیتی موجود افزوده شود. از آنجا که این هدف مستلزم توجه بیشتر عوامل اصلی بخش خصوصی به ویژگی‌های امنیتی است، همکاری مشترک بخش دولتی ـ خصوصی می‌تواند به ایجاد زیرساخت‌های سایبریِ جهانیِ مطمئن‌تر و ایمن‌تر کمک کند. بسیاری از کشورهای درحال‌توسعه ظرفیت بسیار محدودی برای نظارت و مدیریت حوادث عرصهٔ سایبری دارند. به منظور ایجاد این ظرفیت، آن‌ها باید با هدف مدیریت بهتر حوادث، اقدامات فنی و سازمانی جدیدی صورت دهند. حداقل الزاماتِ راه‌اندازی گروه‌های واکنش اضطراری رایانه‌ای ملی[1] عبارت‌اند از: آموزش تخصصی، دستیابی به تجهیزات و تبادل بهترین روش‌ها در شبکه‌های حرفه‌ای بین‌المللی گروه‌های واکنش اضطراری رایانه‌ای.

دومین عنصر مهم آن است که کشورها باید الگویی در زمینهٔ ارتباط سازمان‌های اجرای قانون با گروه‌های واکنش اضطراری رایانه‌ای، ارائه‌دهندگان خدمات اینترنتی و شبکه‌های مشارکت عمومی ـ خصوصی به

1. Computer Emergency Response Teams (CERTs)

منظور مدیریت حوادث توسعه دهند. مسئلهٔ اصلی، سرمایه‌گذاری در آموزش و پرورش است؛ از جمله مجموعهٔ گسترده‌ای از مهارت‌های الکترونیکی عمومی، دانش امنیت رایانه‌ای نیروی انتظامی، متخصصان فناوری اطلاعات، و سایر ذی‌نفعان ملی مرتبط.

عنصر سوم، که از اهمیت یکسانی برخوردار است، ایجاد یک چارچوب حقوقی مناسب برای تسهیل تحقیقات و پیگیری بموقع جرایم سایبری است. در وضعیت ایدئال، تلاش‌های صورت‌گرفته برای مبارزه با جرایم سایبری باید بخشی از یک راهبرد ملی گسترده‌تر در حوزهٔ امنیت سایبری تلقی شود که ذی‌نفعان مختلف را گرد هم می‌آورد و همکاری بین آژانس‌های مختلف ملی را تسهیل می‌کند. ملت‌ها به خط‌مشی‌ای برای مقابله با جرایم سایبری نیازمندند که یک رویکرد جامع ملی ایجاد کند و به مشارکت تصمیم‌گیرندگان مهم یاری رساند. این مهم شامل اقداماتی برای جرم‌انگاری تخلفات مربوط به جرایم رایانه‌ای و هماهنگ‌سازی حداقل مجازات با عملکرد عمومی بین‌المللی است. همچنین، تضمین وجود ابزار آیین دادرسی برای تحقیقات کارآمد حائز اهمیت خواهد بود. پیروی از الگوی کنوانسیون مبارزه با جرایم سایبری به منظور حصول اطمینان از وجود اقدامات امنیتی و شرایط لازم برای روند تحقیقات نیز توصیه می‌شود.

در سطح عملیاتی، بررسی کلی وضعیت با هدف شناخت تهدیدها و روندها و الگوهای جرایم سایبری بسیار حائز اهمیت است. ایجاد سازوکاری برای گزارش وقایع جرایم سایبری برای افراد و سازمان‌های دولتی و بخش خصوصی به همان اندازه مهم خواهد بود. علاوه بر این، نیروهای پلیس برای کمک به تحقیقات نیروی انتظامی نیازمندند که واحدهای جرایم سایبری ویژه یا جرایم فناوری پیشرفته‌ای را در اختیار

داشته باشند که کارشناسان متخصص جرایم رایانه‌ای در آن مشغول به کارند. پلیس باید در زمینهٔ نحوهٔ جمع‌آوری شواهد از دانش ویژه‌ای برخوردار باشد و کارشناسان جرم‌یابی رایانه‌ای نیز پشتیبانی شوند. واحدهای مشابه در مراجع قضایی باید واحدهای عملیاتی پلیس را برای پیگرد قانونی هر چه مؤثرتر پشتیبانی کنند. در نهایت، ظرفیت‌سازی امنیت سایبری مؤثر نیازمند یک گروه واکنش اضطراری رایانه‌ای کارآمد ملی است که در مرکزیت فعالیت‌های هماهنگ‌سازی یک کشور قرار گیرد و اطلاعات لازم را در اختیار نیروی انتظامی قرار دهد و به عنوان واسط بین سازمان‌های دولتی و بخش خصوصی عمل کند. گروه واکنش اضطراری رایانه‌ای و بخش خصوصی و شبکه‌های امنیت اطلاعات یک کشور باید برای ایجاد یک سیستم نظارت و واکنش به رخداد پایدار گرد هم جمع شوند.

فعالیت‌های امنیت سایبری باید ماهیت شبکه‌ای این دامنه را مدنظر قرار دهند و کلیهٔ ذی‌نفعان را در بر گیرند. شمار ذی‌نفعان امنیت سایبری زیاد است و رویکردهای ظرفیت‌سازی باید در امتداد مرزها و با گذشت زمان منسجم و یکپارچه شوند. کانون توجه باید به پیشگیری معطوف باشد و سرمایه‌گذاری در راهبردهای پیشگیرانهٔ فرامرزی بسیار حائز اهمیت است. ظرفیت‌سازی موفق موجب ایجاد رویکرد جامعه‌سازی و چارچوب‌های همکاری خواهد شد. در صورت وجود مشارکت دولتی ـ خصوصی، حداقل ظرفیت سازمانی و فناورانهٔ ملی در واکنش به رخدادها و چارچوب‌های نهادی مربوط، ظرفیت‌سازی پایدار خواهد بود. این رویکرد اساسی که از مشارکت و تخصص داخلی بهره می‌برد، مطلوب‌ترین رویکرد ظرفیت‌سازی بوده است، اما گاهی اوقات التزام آشکار دولت‌های ملی برای تضمین تعهد سیاسی سطح بالا ضرورت دارد.

تنها در صورت وجود تمام این عناصر ملی، همکاری‌های بین‌المللی و

منطقه‌ای موفق در هر زمینه‌ای از امنیت سایبری امکان‌پذیر خواهد بود: اجرای قانون، حفاظت از زیرساخت‌های مهم، شبکه‌های گروه‌های واکنش اضطراری رایانه‌ای و نهادهای مرتبط با امنیت ملی. امنیت سایبری مؤثر همواره نتیجهٔ هماهنگی و همکاری بین طیف گسترده‌ای از عوامل خواهد بود.

تنش‌های مربوط به آزادی اینترنت و آزادی بیان اینترنتی ممکن است گاهی با خواست واقعی دولت‌ها برای دستیابی به ظرفیت امنیت سایبری بیشتر در تضاد باشد. از ظرفیت‌سازی نباید برای کنترل دولتی و سانسور گستردهٔ ناعادلانه استفاده کرد. به احتمال زیاد اختلافات فعلی میان دولت‌ها بر سر آزادی بیان باقی خواهد ماند و مانع از توسعهٔ ظرفیت‌سازی خواهد شد. با این حال، همواره وجه مشترکی وجود دارد که مربوط به رژیم‌های مختلف سیاسی است: چگونگی تضمین یک محیط اینترنتی عاری از کلاهبرداری و جرم برای شهروندان.

در حال حاضر، فعالیت‌های بین‌المللی در زمینهٔ ظرفیت‌سازی برای امنیت سایبری، گسترده اما همچنان پراکنده‌اند. هدایت این تلاش‌ها در سطح جهانی مستلزم ارزیابی و بازنگری هر چه مؤثرتر است. همچنین تجزیه و تحلیل تمرکز منطقه‌ای و عملکردی برای ظرفیت‌سازی و وجود سازوکارهای هماهنگی بین‌المللی ضرورت دارد. برای داشتن یک الگوی ظرفیت‌سازی موفق، بهترین شیوه‌های همکاری اقتصادی برای توسعه[1] و امنیت سایبری باید با یکدیگر ادغام شوند. علاوه بر این، ایجاد سازوکار دسترسی اطلاعاتی[2] بین اهداکنندگان و گیرندگان نیز حائز اهمیت خواهد بود.

در آخر، شبکه‌های همکاری تاب‌آوری سایبری بین‌المللی غیررسمی موجود نیز برای ظرفیت‌سازی امنیت سایبری بسیار ارزشمند خواهند بود.

---

1. Development Cooperation
2. Clearinghouse Mechanism

چند انجمن بین‌المللی غیررسمی در حوزهٔ امنیت سایبری امکان توسعهٔ سیاست‌ها و تبادل تجربیات برتر[1] را فراهم می‌آورند. فرایند مِریدین[2] یک کتاب مرجع جهانی ارائه داده است که به طور مرتب به‌روزرسانی می‌شود و علاوه بر خط‌مشی‌های محافظت از زیرساخت‌های اطلاعاتی اساسی، حاوی نقاط تماس ضروری برای مقامات سایبری فنی در بیش از پنجاه کشور است. از آنجا که این مجمع تنها به نمایندگان دولت محدود می‌شود، سیاست‌گذاران امنیت سایبری و کارشناسان فنی ملی را به یکدیگر متصل می‌کند. مریدین شامل رویدادهای سالانه و منطقه‌ای است و به عنوان یک انجمن سایبری حرفه‌ای مطرح، به اعتمادسازی جهانی و تسهیل مشاوره بین سیاست‌گذاران می‌پردازد. شبکهٔ مریدین همچنین توصیه‌هایی ارائه می‌دهد، تجربیاتی برتر را به اشتراک می‌گذارد، و نیز دستورالعمل‌های امنیتی فناوری اطلاعات و کتابچهٔ راهنمای عملیاتی و سایر اطلاعات ضروری را در اختیار شرکت‌کنندگان خود قرار می‌دهد.

شبکهٔ انجمن گروه‌های امنیتی و پاسخگویی رویداد،[3] گروه‌های واکنش اضطراری رایانه‌ای را در سراسر جهان به یکدیگر متصل می‌کند و به عنوان انجمنی برای جامعهٔ فنی فعالیت دارد. در این شبکه، کارشناسان امنیت فناوری اطلاعات به تبادل اطلاعات و تجارب خود در خصوص روش‌های پاسخگویی رویداد با یکدیگر می‌پردازند. این انجمن تا حد زیادی بر پایهٔ شبکهٔ موثقی از اطلاعات تماس شخصی بنا شده و به عنوان بستر سودمندی برای واکنش در زمان بحران‌های سایبری عمل کرده است. در انجمن‌های تخصصی امنیت اطلاعاتِ زیادی با اهدافی مشابه وجود دارند که تا کنون مبنای سازوکارهای اصلی برای متخصصان بوده‌اند و مسئولیت تمامی آن‌ها

1. Exchange of Best Practice
2. Meridian Process
3. The Forum of Incident Response and Security Teams (FIRST)

تضمین ثبات در بخش جهانی فناوری اطلاعات و ارتباطات است. در غیاب سازوکارهای مدیریت بحران‌های نهادی، این شبکه‌های غیررسمی به دفعات اینترنت را نجات داده‌اند. این انجمن‌ها همچنین گروه‌های واکنش اضطراری رایانه‌ای سراسر جهان را به رسمیت می‌شناسند.

- **دفاع از حقوق بشر در عرصهٔ سایبری**

چشم‌اندازهای مختلف حکمرانی عرصهٔ سایبری در سیاست خارجیِ سنتی، به خصوص حوزهٔ حمایت از حقوق اساسی، نیز به کار گرفته شده است. ظهور اینترنت برقراری ارتباط بین گروه‌های مختلف اجتماعی و سیاسی در رژیم‌های غیردموکراتیک را تسهیل کرده است، حال آنکه این رژیم‌ها به سرعت نحوهٔ بهره‌برداری از فناوری اطلاعات و ارتباطات برای باقی ماندن در مقام قدرت را فراگرفته‌اند. در خصوص استفاده از فناوری اطلاعات و ارتباطات به منظور سانسور کردن، محدود کردن آزادی بیان اینترنتی، و استفاده از رسانه‌های اجتماعی برای خنثی کردن مخالفت سیاسی، نگرانی‌های فزاینده‌ای وجود دارد. مذاکرات حقوق بشر شامل دغدغه‌های روزافزونی دربارهٔ آزادی اینترنت، شکوفایی فناوری‌های نظارتی اینترنت و آزادی بیان در رسانه‌های الکترونیکی است. با توجه به تعدد کشورهایی که خواستار کنترل وبلاگ‌نویسی و رسانه‌های اجتماعی فعال از طریق فناوری‌های جدیدند، مذاکرات اینترنتی حقوق بشر نیز شامل موضوعاتی از قبیل مسئولیت اجتماعی شرکتی[1] محدودیت‌های تجاری و تحریم‌ها هستند.

دیپلمات‌هایی که مذاکرات امنیت سایبری را دنبال می‌کنند، باید از محدودیت‌های اساسی آزادی اینترنتی آگاه باشند. در بسیاری از موارد و به دلیل پیشینهٔ این موضوع فناوری‌محور، ممکن است روابط سایبری بین

1. Corporate Social Responsibility (CSR)

دولت‌ها را هنوز آژانس‌های فنی یا وزارتخانه‌های داخلی انجام دهند؛ جایی که آزادی اینترنت اغلب اوقات نگرانی اصلی نیست. به منظور گنجاندن روابط سایبری در تعامل سیاسی کلی با شرکای خارجی و اطمینان از تعادل جنبه‌های امنیتی و آزادی، وزارتخانه‌های امور خارجه باید نقش هماهنگ‌کننده‌ای در روابط سایبری خارجی ایفا کنند. در ۵ جولای ۲۰۱۲، شورای حقوق بشر سازمان ملل قطعنامه‌ای در خصوص «ترویج، حمایت و بهره‌مندی از حقوق بشر در اینترنت» به تصویب رساند. این قطعنامه بر اعلامیهٔ جهانی حقوق بشر، میثاق بین‌المللی حقوق مدنی و سیاسی، میثاق بین‌المللی حقوق اقتصادی، اجتماعی و فرهنگی و اهمیت اعمال حقوق بشر در توسعهٔ فوری فناوری تأکید بسیار دارد و تأیید می‌کند که تمامی افراد در صورت اتصال به اینترنت، از حقوق بشر و آزادی‌های اساسی اینترنتی برخوردارند و کلیهٔ دولت‌ها بدون در نظر گرفتن نوع رسانه باید از آن حقوق محافظت کنند. این قطعنامه حاوی متنی است که به دفعات نقل قول شده است: «[...] مردم باید کلیهٔ حقوقی را که در دنیای غیرمجازی (آفلاین) از آن برخوردارند در دنیای مجازی (آنلاین) نیز داشته باشند، به ویژه آزادی بیان [...]». بر آزادی بیان اینترنتی در چارچوب راهبردی اتحادیهٔ اروپا و برنامهٔ عملیاتی حقوق بشر و دموکراسی[1] نیز تأکید شده است و بند ۲۴ آن، یعنی «آزادی بیان مجازی و غیرمجازی»، خواستار اقدامات مختلفی دربارهٔ حمایت از حقوق اساسی اینترنتی است. همچنین یک اصل مشابه به «راهبرد امنیت سایبری اتحادیهٔ اروپا اضافه شده است: فضای سایبری آزاد، امن و ایمن» در بخش خط‌مشی بین‌المللی فضای سایبری اتحادیهٔ اروپا. گروه هشت (هفت) نیز حقوق بشر اینترنتی را از طریق اعلامیهٔ دوویل در مورد تعهدات جدید آزادی و دموکراسی[2] و اعلامیهٔ دوویل

1. Action Plan on Human Rights and Democracy
2. Deauville Declaration on Renewed Commitments for Freedom and Democracy

در بهار عربی[1] تأیید کرد. دستور کار حقوق بشر در فضای سایبری یک حوزهٔ جداگانه و ناشناخته در خارج از جامعهٔ حقوق بشر نیست. زیرا طیف گسترده‌ای از موضوعات و ابزارهای سیاست خارجی را در بر می‌گیرد. در جریان مذاکرات این قطعنامه، ایالات متحده با سوئد که حامی اصلی قطعنامه بود همکاری نزدیکی داشت و بیش از هشتاد کشور دیگر از جمله برزیل، ترکیه، نیجریه و تونس نیز مشترکاً از آن حمایت کردند.

پشتیبانی از مسئولیت‌پذیری اجتماعی سازمانی در بکارگیری فناوری‌هایی با استفادهٔ دوگانه[2] ابزاری تأثیرگذار است. اقدامات متعددی در سطح جهانی به این هدف یاری رسانده‌اند. شورای حقوق بشر سازمان ملل در سال ۲۰۱۱، مجموعه‌ای از اصول سازمان ملل را در خصوص تجارت و حقوق بشر تأیید کرد. همچنین این اصول با هدف حصول اطمینان از رعایت حقوق بشر در فعالیت‌ها و روابط تجاری شرکت‌ها، یک استاندارد جهانی برای نقش مشاغل و دولت‌ها تعیین ساخت. هدف کمیسیون اروپا[3] یعنی «راهبرد جدید اتحادیهٔ اروپا ۲۰۱۱ ـــ ۲۰۱۴ در خصوص مسئولیت اجتماعی شرکتی»، شناساندن خط‌مشی‌های مسئولیت اجتماعی شرکتی و انتشار تجارب برتر است. این راهبرد خواستار افزایش سطح اعتماد به بخش خصوصی اتحادیهٔ اروپا، بهبود فرایندهای خودتنظیمی[4] و تنظیم‌گری مشارکتی[5] و هماهنگی بهتر فعالیت‌های اتحادیهٔ اروپا با رویکرد جهانی مسئولیت اجتماعی شرکتی است. کمیسیون اروپا همچنین به منظور پیروی از اصول سازمان ملل رهنمون‌هایی دربارهٔ مسئولیت شرکتی در زمینهٔ احترام به حقوق بشر در بخش فناوری اطلاعات و ارتباطات ارائه داده است.

---

1. Deauville Declaration on the Arab Spring
2. Dual Use Technologies
3. The European Commission
4. Self-Regulation
5. Co-Regulation

دومین رویکـرد بـرای دیپلمـات‌هـا وضـع قـوانینی بـرای کنتـرل صـادرات، واسطه‌گری و حمل و نقلِ اقلامِ دارای استفادهٔ دوگانه است. هدف اصلی، محـدود کردن فروش گستردهٔ فناوری‌هایی است که امکان دارد به منظور نظارت بر اینترنت استفاده شوند. با وجود این خط‌مشی، ارزیابی دقیق خطـرات مربـوط بـه تحویـل فناوری‌های دوگانه به یک کشور معین بسیار دشوار است. برخی از این فناوری‌هـا در فعالیت‌های ضد تروریستی و حوزه‌های قانونی دیگر استفاده می‌شوند.

خط‌مشی سوم استفاده از تحریم‌ها علیه برخی کشورها با هدف ممانعت از بکارگیری فناوری‌های مخرب علیه مدافعان حقوق بشر است. اتحادیهٔ اروپا این تحریم‌ها را علیه سوریه و ایران در زمینهٔ تجهیزات یا نرم‌افزارهای رهگیری ارتباطات اعمال کرده است. اتحادیهٔ اروپا نخستین‌بار در سال ۲۰۱۲، این تحریم‌ها را علیه سوریه در زمینهٔ فروش، عرضه، انتقال یا صادرات تجهیزات یا نرم‌افزارهای کاربردی و سودمند برای نظارت یا رهگیری اعمال کرد. در آیین‌نامهٔ ۱۸ ژانویهٔ ۲۰۱۲، دامنهٔ این اقدامات بیشتر مشخص و توضیح داده شده است. این آیین‌نامه ممنوعیت صادرات برخی تجهیزات و فناوری‌ها یا نرم‌افزارها را دقیقاً مشخص می‌کند. همچنین ارائهٔ مساعدت فنی، خدمات کارگزاری، تأمین اعتبار یا کمک مالی یا ارائهٔ هر گونه خدمات ارتباطات از راه دور یا نظارت اینترنتی یا رهگیری را ممنوع می‌نماید.[1] آیین‌نامهٔ مشابهی در ۲۰۱۲، در خصوص ایران نیز منتشر شد.[2]

---

1. Council Decision 2012/36/CFSP of 23 January 2012 Amending Decision 2010/639/CFSP Concerning Restrictive Measures Against Belarus: http:// eur-lex.europa.eu.

2. Council of the European Union Decision 2012/168/CFSP Amending Decision 2011/235/CFSP Concerning Restrictive Measures Directed Against Certain Persons and Entities in View of the Situation in Iran', 23 March 2012: http://eurlex.europa.eu.

دفاع از حقوق بشر در عصر فناوری، یک چالش و مسئله‌ای اساسی به شمار می‌آید. بنابراین، دموکراسی‌های لیبرال باید از اصل حقوق اساسی در انتقال و صادرات فناوری محافظت کنند. این دولت‌های همفکر همچنین باید به تلاش خود برای حفظ اینترنت آزاد و عاری از هر گونه کنترل مستقیم دولت‌ها ادامه دهند.

- **حکمرانی اینترنت**

عوامل بخش خصوصی، اینترنت را همانند سایر فناوری‌های اطلاعات و ارتباطات توسعه داده و از آن محافظت کرده‌اند. لایهٔ حکومتیِ آن در قالب غیرانتفاعی و با هدایت شرکت اینترنتی برای نام‌گذاری و واگذاری شماره‌ها (آیکان)، به لایه‌های فنی اضافه شده است. این سازمان عملکردی هماهنگ‌کننده یا تنظیم‌کنندهٔ خط‌مشی‌های اینترنتی دارد. آیکان با سیستم‌های شناسه‌های منحصربه‌فرد اینترنت، دی‌ان‌اس و سایر خط‌مشی‌ها سروکار دارد. کشورها در کمیتهٔ مشورتی دولتی آیکان[1] که یکی از ارکان‌های اصلی است و به هیئت آیکان مشاوره می‌دهد، کرسی دارند. با این حال جوامع و مجموعه‌های فنی همواره حکمرانی اینترنت را بر عهده دارند، زیرا مسائل و تصمیمات روزمرهٔ آن نیاز به پیش‌زمینهٔ فناورانه دارند.

تصمیم ایجاد آیکان در دههٔ ۱۹۹۰ واکنشی بود به ادعای اتحادیهٔ بین‌المللی ارتباطات از راه دور[2] در خصوص اینکه اصلی‌ترین سازمان در عملکردهای اینترنتی است. از آن زمان به بعد، اتحادیهٔ بین‌المللی ارتباطات از راه دور به دنبال روش‌های جدیدی برای به دست گرفتن حکمرانی اینترنت بوده است. دموکراسی‌های لیبرال دربارهٔ اینکه الگوی بین دولتی

1. ICANN’s Government Advisory Committee (GAC)
2. International Telecommunication Union’s (ITU)

حکمرانی اینترنت به حکمرانی نامنسجم و کُند و غیرتعاملی منجر خواهد شد، ابراز نگرانی می‌کنند. نظارت ملی نیز سانسور اینترنتی را در کشورهای استبدادی تسهیل خواهد کرد.

در حال حاضر، مجمع حکمرانی اینترنت[1] و اجلاس جهانی سران دربارهٔ جامعهٔ اطلاعات[2] مهم‌ترین مجامع جهانی برای مذاکره دربارهٔ این موضوع هستند. مجمع حکمرانی اینترنت، که هرساله برگزار می‌شود، جامعهٔ ذی‌نفعان جهانی را گرد هم می‌آورد و در آن، دولت‌ها و بخش خصوصی و جامعهٔ مدنی دربارهٔ موضوعات مربوط به اینترنت به بحث و گفت‌وگو می‌پردازند. مذاکرات سازمان ملل دربارهٔ حکمرانی اینترنت سبب ایجاد دو گروه عمده شده است: نخست، گروه کشورهایی که از آیکان حمایت می‌کنند و حکمرانی چندذی‌نفعی مؤثرتری، همچون مداخلهٔ نزدیک‌تر دولت در تصمیم‌گیری آیکان، را پیشنهاد می‌دهند. دوم، گروه دیگری از کشورها که نسبتاً کمتر از آیکان حمایت می‌کنند و به دنبال یک ساختار جایگزین حکمرانی بین دولتی برای اینترنت هستند. این گروه از کشورها به دنبال زیر سؤال بردن الگوی فعلی حکمرانی اینترنت هستند و خواستار «همکاری پیشرفته»اند که به معنای کنترل بیشتر دولت‌ها در این زمینه است.

در کنفرانس جهانی ارتباطات بین‌المللی[3] سال ۲۰۱۲ در دبی، ۹۳ دولت از نقش بهبودیافتهٔ اتحادیهٔ بین‌المللی ارتباطاتِ راه دور در نظام‌مندسازی اینترنت حمایت کردند. در حالی که کشورهای عضو اتحادیهٔ اروپا، ایالات متحده و سایر کشورهای همسو پیمان جدید اتحادیهٔ بین‌المللی ارتباطات راه دور را در این کنفرانس امضا نکردند، رأی‌گیری دربارهٔ این موضوع

1. Internet Governance Forum (IGF)
2. World Summit of the Information Society (WSIS)
3. World Conference on International Telecommunications (WCIT)

نشان‌دهندهٔ گسترش اختلاف‌نظر جهانی بر سر حکمرانی اینترنت بود. ایالات متحده و اتحادیهٔ اروپا از الگوی فعلی نظارت نهادهای چندذی‌نفعی و غیردولتی بر اینترنت حمایت می‌کنند. بسیاری از کشورهای درحال‌توسعه و نوظهور، حمایت خود را از انتقال قدرت نظارتی اینترنت به اتحادیهٔ بین‌المللی ارتباطات راه دور اعلام می‌دارند.

برخی قدرت‌های نوظهور به طور منظم برای بحث دربارهٔ حکمرانی اینترنت، مدیریت محتوا و مسائل امنیت سایبری گرد هم جمع می‌شوند. آن‌ها نقش ویژهٔ خود را در ارتقای منافع کشورهای درحال‌توسعه می‌بینند و پیشنهاد می‌دهند که اینترنت باید با تمرکز ویژهٔ دولت‌ها بر تأثیر شبکه‌های اجتماعی بر جامعه اداره شود.

برخی کشورهای درحال‌توسعه که قادر به مقابله با تهدیدهای سایبری نیستند، صاحبان زیرساخت‌های اساسی اینترنت و ساختار مدیریتی تحت نظارت آیکان را برای نقایص امنیت اینترنت موجود مقصر می‌شمارند. برای بسیاری از کشورهایی که آزادی کمتری دارند، یک الگوی جدید تحت کنترل دولت دارای جذابیت بیشتری است، زیرا در این صورت روند سانسور اینترنت برای آن‌ها تسهیل خواهد شد. بنابراین، آن‌ها برای زیر سؤال بردن الگوی فعلی، به کشورهای نوظهور پیوسته‌اند. با این حال، آنچه به خوبی در سطح بین‌المللی توضیح داده نمی‌شود این است که یک الگوی حکمرانی اینترنت بین‌دولتی ممکن است به عدم حمایت از حقوق اساسی، چندپاره شدن اینترنت تعاملی و عواقب منفی اقتصادی منجر شود. برای حمایت از سلسله‌دلایل پذیرفتنی یک اینترنت آزاد، که نقش اصلی دیپلماسی سایبری خواهد بود، آگاهی بیشتری لازم است. همچنین کمک به توسعهٔ کشورهایی که قادر به مقابله با تهدیدات امنیت سایبری نیستند ضرورت خواهد داشت.

جامعهٔ بین‌المللی مطمئناً باید از تجربیات مشابه با کنفرانس جهانی ارتباطات بین‌المللی جلوگیری کند؛ جایی که قطبی شدن بر سر این موضوع صورت گرفت. اجلاس جهانی سران دربارهٔ جامعهٔ اطلاعاتی در سال ۲۰۱۵، با مشارکت جامعهٔ سیاست خارجی سایبری از آمادگی و هماهنگی بیشتری برخوردار بود. زمان آن فرارسیده است که روند حاکم را، که در آن حکمرانی اینترنت صرفاً به عنوان یک «موضوع تخصصی کامپیوتری» تلقی می‌شود، تغییر دهیم. در زمینهٔ حفظ الگوی چندذی‌نفعی، آیکان نیز باید به منافع مشروع سیاست عمومی، از قبیل دغدغه‌های نیروی انتظامی، مسئولانه‌تر پاسخ دهد.

برای دیپلمات‌ها، یادگیری جهت‌یابی در این زیرشاخهٔ دیپلماسی سایبری آسان نخواهد بود. بحث و گفت‌وگو دربارهٔ اینترنت همواره در مجامع مختلف، رویدادها، همایش‌ها، سمپوزیوم‌ها و نشست‌های ذی‌نفعان صورت می‌گیرد. با توجه به تعدد این جلسات، که برخی از آن‌ها کاملاً فنی هستند، حتی یک ناظر باتجربه در حوزهٔ فضای سایبری نیز دچار سردرگمی خواهد شد. در واقع، پیچیدگی این مسئله با تداخل جریان‌های کاری و بسیاری از جوامعی که با کلّیت حکمرانی اینترنت دست و پنجه نرم می‌کنند بیشتر می‌شود.

منابع

Communication from the Commission to the European Parliament, the Council ‘Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre’, COM (2012) 140 Final, Brussels, 28 March 2012.

Council Decision 2012/36/CFSP of 23 January 2012 Amending Decision 2010/639/CFSP Concerning Restrictive Measures Against Belarus: http://eur-lex.europa.eu.

Council of the European Union Decision 2012/168/CFSP Amending Decision 2011/235/CFSP Concerning Restrictive Measures Directed Against Certain Persons and Entities in View of the Situation in Iran’, 23 March 2012: http://eurlex.europa.eu.

Council of Europe, Cybercrime Website; http://www.coe.int/t/ DGHL/ cooperation/economiccrime/cybercrime/default_en.asp.

Directive 2013/40/EU on Attacks Against Information Systems and Replacing Council Framework Decision 2005/222/JHA, Official Journal of the European Union 14 August 2013,http: //eurlex. europa.eu.

Healey, J. (2013). A Fierce Domain: Conflict in Cyberspace, 1986-2012. (ED). Cyber Conflict Studies Association Publication in Partnership with the Atlantic Council.

Schmitt, M. (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press.

Tiirmaa-Klaar, H., Gassen, J., Gerhards-Padilla, E., & Martini, P. (2013). Botnets’ Springer Briefs in Cyber Security. Springer.

UNGA. (2009). Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/64/386.

UNGA. (2010. Report of UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/65/94, 24.

فصل دوم

مطالعهٔ جامع اقدامات و سازوکارهای جهانی دیپلماسی سایبری

درآمد

کمیسیون جهانی ثبات در فضای سایبری[1] در سال ۲۰۱۷، فهرستی از بیش از هشتاد اقدام و ابتکار منطقه‌ای و جهانی[2] در زمینهٔ دیپلماسی سایبری ارائه داد که به لحاظ ماهوی دو ویژگی مشخص دارد: ۱. عمدهٔ این اقدامات و ابتکارات در سال‌های اخیر (عمدتاً بعد از سال ۲۰۱۰) صورت گرفته‌اند که مقولهٔ سایبری و فضای سایبری به صدر توجهات حاکمیتی، به خصوص در عرصهٔ روابط بین‌الملل، تبدیل شده است؛ ۲. علاوه بر بازیگران رسمی (اعم از دولتی‌ها یا سازمان‌های منطقه‌ای و جهانی که معرف و نماینده حکومت‌ها هستند)، نقش بازیگران غیردولتی (اعم از بخش‌های خصوصی و صنعتی و کمپانی‌های آی‌تی) در آن بسیار برجسته است.

به لحاظ محتوایی، طیف وسیعی از موضوعات و محورهای مرتبط با اینترنت و فضای سایبری و حوزهٔ سایبری در این اقدامات و ابتکارات قابل شناسایی است که عمدهٔ آن‌ها و تعداد مواردی که این محورها در این اقدامات و ابتکارات بررسی شده‌اند، در جدول شمارهٔ ۱ قابل شناسایی است.

---

1. The Global Commission on the Stability of Cyberspace

۲. فهرست این اقدامات و ابتکارات در پایان همین کتاب ضمیمه است.

جدول شمارهٔ ۱. مهم‌ترین محورهای اقدامات و ابتکارات مرتبط با دیپلماسی سایبری

محورهای اصلی بحث‌شده	تعداد
اقدامات به‌اشتراک‌گذاری اطلاعات به صورت کلی[1](اطلاعات مربوط به راهبردها، خط‌مشی‌ها، قانون‌گذاری، الگوهای سرآمد، ظرفیت‌سازی)	۴۳
سازوکارهای همکاری بین‌المللی[2](همایش‌ها، کارگروه‌ها، دیپلماسی سایبری، تبادل آموخته‌ها)	۳۵
سازوکارهای همکاری دولت و بخش خصوصی	۳۱
سازوکارهای خاص برای همکاری فراملّی نیروی انتظامی و کمک‌های حقوقی متقابل برای جرایم سایبری	۳۰
ایجاد یک نقطهٔ تماس ملی یا سازمانی[3]برای تبادل اطلاعات (به ویژه دستور یا پیشنهاد گروه پاسخگویی به فوریت‌های رایانه‌ای)	۲۹
استانداردهای فنی توصیه‌شده یا مورد نیاز	۲۷
ایجاد فرهنگ امنیت سایبری یا امنیت اطلاعات[4]	۲۵
گفت‌وگوهای منظم[5]	۲۳
به‌اشتراک‌گذاری تهدیدات (به طور کلی)	۲۳
سازوکارهای همکاری دولت و بخش سوم (سازمان‌های غیردولتی، دانشگاهی، جامعهٔ مدنی، گروه‌های غیررسمی)	۲۲
ایجاد اصطلاحات رایج	۲۱
سازوکارهای محافظت از زیرساخت‌های بحرانی و خدمات اساسی	۱۹
تبادل بی‌وقفهٔ اطلاعات در ۲۴ ساعت شبانه‌روز در طول هفته[6]	۱۸

1. Information Sharing Measures in General
2. Mechanisms or International Cooperation
3. Establishment of Specific National or Organizational Point of Contact
4. Creating a Culture of Cyber Security or Information Security
5. Regular Dialogue
6. Real-Time, 24/7 Exchange

از بین بردن شکاف دیجیتالی[1](اشاره به فاصلهٔ بین مردمانی که به فناوری دیجیتال دسترسی مؤثری دارند با مردمانی که دسترسی بسیار محدودی به این فناوری‌ها داشته یا اصلاً دسترسی ندارند).	۱۵
برنامه‌های آموزش سایبری	۱۴
نظارت بر زنجیرهٔ تأمین[2]	۱۳
اجباری بودن اقدامات قانون‌گذاری عمومی در حوزهٔ امنیت سایبری	۱۲
توصیه به انتشار راهبرد امنیت سایبری و خط‌مشی و یا برنامهٔ پاسخگویی به حوادث	۱۱
مکانیسم‌های تحقیق و توسعهٔ اجباری	۱۱
تدوین سازوکارهای افشای آسیب‌پذیری	۱۰
ضرورت انتشار آمار و ارقام و شاخص‌ها	۱۰
سازوکارهای همکاری تجاری	۹
پیشرفت و آموزش و تأیید پرسنل امنیت سایبری	۹
برگزاری نشست‌ها و تمرینات شبیه‌سازی سایبری	۹
اصطلاحات مشترک زیرساخت‌های بحرانی	۸
توسعهٔ سازوکارهای ارزیابی ریسک به منظور افزایش امنیت سایبری، از جمله ارزیابی ریسک بیمه	۷
تضمین قابلیت همکاری فنی شبکه‌ها	۷
ضرورت تأیید متخصصان، محصولات یا خدمات	۷
تعیین مؤسسات دولتی یا نهادهای مسئول حکمرانی سایبری	۶
ضرورت ایجاد مراکز به اشتراک‌گذاری و تجزیه و تحلیل اطلاعات[3]	۶
توصیه به حفظ امنیت یا حریم خصوصی با طراحی محصولات و سامانه‌ها و خدمات	۶

1. Closing the Digital Divide
2. Supply Chain Supervision
3. Information Sharing and Analysis Centers (ISACs)

برنامه‌هایی برای آموزش قانون‌گذاران ملی و سایر پرسنل قانونی یا نظارتی در حوزهٔ امنیت سایبری	۶
تعریف جنسیت و سن و سایر تنوع‌های دست‌اندرکاران و نیروهای کار فضای سایبری	۵
تعاریف رایج جرایم سایبری	۵
ارتقای حکمرانی الکترونیکی	۳
تماس ویژهٔ سایبری برای مواردی که احتمال تشدید آن‌ها وجود دارد	۵
سازوکار انتساب اقدامات خصمانهٔ سایبری[1]	۲
توسعهٔ رهبری امنیت سایبری[2]	۲
استفاده از گواهی‌های هویت عمومی (گواهینامهٔ دیجیتال)[3] برای تأیید اعتبار کاربر	۲
ضرورت ایجاد انجمن پاسخگویی رویداد و گروه‌های امنیتی امری	۱

فراتر از محتوای برجسته‌شده در هر یک از اقدامات و ابتکارات صورت‌گرفته در ارتباط با حوزهٔ سایبری، مطالعهٔ جامع این اقدامات و ابتکارات حائز اهمیت است؛ زیرا از این طریق می‌توان به نقش بازیگران کلیدی، رویکردشان و بر این اساس، جهت‌گیری‌ها و مرزبندی‌های آنان و در بُعد عملیاتی، استراتژی‌های اتخاذشدهٔ این بازیگران با هدف پیشبرد دیپلماسی سایبری پی برد.

به این منظور آنچه در ادامه می‌آید نگاهی به مهم‌ترین بازیگران جهانی و منطقه‌ای عرصهٔ سایبری، تأملی در رویکردها و جهت‌گیری آن‌ها به مقولهٔ سایبری و نیز مهم‌ترین استراتژی‌های آنان در پیشبرد اهداف سایبری است که در چهار قسمت ارائه شده است: ۱. مهم‌ترین بازیگران جهانی (کشورها)،

1. Mechanism for Attribution of Hostile Cyber Activities
2. Developing Cyber Security Leadership
3. Utilize Generic Identity Certificates (Digital Certification)

۲. مهم‌ترین سازمان‌های جهانی (سازمان‌های بین‌المللی)، ۳. مهم‌ترین استراتژی‌های دوجانبه یا چندجانبه، ۴. ذی‌نفعان در بخش خصوصی. در پایان هر قسمت نیز تحلیل و جمع‌بندی‌ای از نقش و تأثیر هر یک از این بازیگران به صورت مقایسه‌ای ارائه شده است.

بازیگران جهانی (کشورها)

بر اساس سنت رایج در ادبیات سیاسی و روابط بین‌الملل، از کشورهای آمریکا، روسیه، انگلستان، چین و فرانسه به عنوان قدرت‌های برتر جهانی یاد می‌شود. با این حال، در عرصهٔ دیپلماسی سایبری این طبقه‌بندی کلاسیک لزوماً مصداق نمی‌یابد. علاوه بر این، آنچه در ذیل تحت عنوان مهم‌ترین بازیگران (کشورها) مطرح می‌شوند، کشورهایی هستند که در حوزهٔ سیاست‌گذاری سایبری و تدوین دیپلماسی سایبری در سطح بین‌الملل عمدتاً پیشگام‌اند.

- **روسیه**

روسیه در کنار آمریکا و چین، قدرت سایبری بزرگی محسوب می‌شود که این قدرت به سبب ساختار حکمرانی روسیه، این کشور را به لحاظ دفاعی در موقعیتی برتر قرار داده است. دغدغهٔ اصلی روسیه، اصل «حاکمیت ملی» این کشور است و اینکه تنها سازوکارهای اطمینان‌بخش «امنیت اطلاعات» می‌توانند آن را تضمین کنند. روسیه به طور کلی، چهار تهدید اصلی را در فضای سایبری شناسایی کرده است:

۱. استفاده از اطلاعات به عنوان سلاحی برای اهداف نظامی و سیاسی مغایر با قوانین بین‌المللی؛ به زعم روسیه، انتشار اسناد پاناما می‌تواند نمونهٔ بارز از یک حملهٔ اطلاعاتی علیه این کشور باشد؛

۲. استفاده از فناوری اطلاعات و ارتباطات برای اهداف تروریستی، مانند گروه‌های تروریستی که از اینترنت برای انتشار پیام خود و جذب طرفدار استفاده می‌کنند؛

۳. استفاده از فناوری اطلاعات و ارتباطات برای مداخله در امور داخلی دولت‌ها و نقض حاکمیت ملی این کشورها؛

۴. استفاده از ابزارهای رایانه‌ای برای مقاصد جنایی همچون ایجاد و انتشار بدافزارها.[1]

روسیه کلاً طرفدار یک «رژیم حقوقی بین‌المللی با هدف ایجاد شرایطی برای راه‌اندازی یک سامانهٔ امنیت اطلاعات بین‌المللی است». این رژیم حقوقی می‌تواند از طریق یک کنوانسیون پیشنهادی برای امنیت اطلاعات بین‌المللی، آیین‌نامهٔ رفتار سازمان ملل، و مشاوره‌های منظم دوجانبه و چندجانبه و همچنین ایجاد اتحادیهٔ بین‌المللی ارتباطات به عنوان نهاد حاکم بر اینترنت، و توسعهٔ اقدامات اعتمادساز در زمینهٔ کاهش خطر سوءبرداشت، پشتیبانی و تقویت شود. روسیه اذعان می‌دارد که قوانین و میثاق‌های بین‌الملل در فضای سایبری قابل اعمال است، اما همچنین استدلال می‌کند که با توجه به ویژگی‌های دائماً در حال تغییرِ حوزهٔ اطلاعات و فناوری‌های اطلاعات، وجود قانون و نهادهای جدید برای حفظ ثبات سایبری ضرورت دارند.[2]

رویکرد روسیه بر این فرض استوار است که محیطی تک‌قطبی در فضای سایبری به طور ذاتی مسبب ایجاد بی‌ثباتی و ناامنی می‌شود. از این رو، یک کشور یا یک قدرت نمی‌تواند و نباید بر فضای سایبری مسلط شود. علاوه بر این، اسناد راهبردی روسیه در حوزهٔ سایبری و امنیت ملی این کشور، به

1. NATO Cooperative Cyber Defense Centre of Excellence, 2017
2. Adam Taylor, 2017

دفعات بر ضرورت توازن فناورانه[1] و مشارکت استراتژیک عادلانهٔ[2] روسیه با سایر کشورها تأکید دارند. این رویکرد آشکارا در مقابل رویکرد آمریکاست که از طریق اشرافیت راهبردی خود در حوزهٔ فناوری اطلاعات به دنبال یک‌جانبه‌گرایی و تحمیل ارزش‌های خود به دیگران است.

- **ایالات متحده آمریکا**

ایالات متحده خواستار حفظ فضای سایبری «آزاد، تعاملی، ایمن و قابل اعتماد» است و استدلال می‌کند که تحقق آن در گروی این امور است: تدوین هنجارها، اقدامات اعتمادساز، ظرفیت‌سازی، همکاری در اجرای قانون و کلیهٔ مشاوره‌های دوجانبهٔ دولتی و مشارکت در اقدامات و ابتکارات منطقه‌ای و بین‌المللی.

آمریکا معتقد است که ملزم ساختن کشورها به پیروی از هنجارهای تدوین‌شده موجب می‌شود تا اقدامات آن‌ها قابل پیش‌بینی شود و سوءتفاهم‌هایی که به درگیری‌های احتمالی منجر می‌شوند کاهش یابند؛ ضمن آنکه به ثبات سیستم بین‌المللی نیز کمک خواهد کرد. برخلاف روسیه، ایالات متحده بر ضرورت وجود قانون جدید یا سازوکارهای مبتنی بر معاهده[3] برای ارتقای ثبات در فضای سایبری اعتقاد ندارد. در مقابل، واشینگتن بر این باور است که کشورها باید نحوهٔ اعمال قوانین بین‌المللی را، از جمله موارد حقوق بشر، آزادی بیان و ...، نیز در فضای سایبری به رسمیت بشناسند و تأیید کنند.

برخلاف چین و روسیه، ایالات متحده صریحاً اظهار داشته است که در صدد جلوگیری از فعالیت خصمانهٔ دولتی در فضای سایبری است. واشینگتن

---

1. Technological Parity
2. Equitable Strategic Partnership
3. Treaty-Based Mechanisms

همچنین به خاطر رویارویی با کرهٔ شمالی و چین رسماً اعلام کرده است که با استفاده از طیف کاملی از ابزارهای دیپلماتیک تحت اختیار خود، به اقدامات سایبری پاسخ خواهد داد و این پاسخ‌ها لزوماً حوزهٔ بخصوصی نخواهند داشت.

به لحاظ فناوری، به عنوان اصلی‌ترین محور رقابت در عرصهٔ سایبری، ایالات متحده آمریکا کشور چین را بزرگ‌ترین رقیب خود می‌داند و به همین دلیل نیز به طور روزافزون، استراتژی‌های تهاجمی‌تری برای مهار و کنترل چین در پیش می‌گیرد. در سال‌های اخیر جامعهٔ جهانی شاهد رقابت شدید فناوری شرکت‌های چینی با همتایان غربی خود در حوزهٔ فناوری نسل پنجم، هوش مصنوعی، اینترنت اشیا، اَپ‌ها و ... بوده است. همچنین رصد تحولات مربوط به اوج‌گیری منازعات سیاسی بین ایالات متحده آمریکا و چین در سه سال گذشته (۲۰۱۷ ـ ۲۰۲۰) نشان می‌دهد که عرصهٔ سایبری و فناوری مرتبط با آن، محور اصلی منازعهٔ دو کشور بوده تا حدی که وزیر امور خارجهٔ آمریکا در ژوئیهٔ ۲۰۲۰ با اشاره به تحولات صورت‌گرفته در روابط دو کشور رسماً از «شکست تعامل کورکورانهٔ» آمریکا با چین خبر داد.

- **بریتانیا**

بریتانیا همانند بسیاری از دموکراسی‌های غربی، موضع مشابهی با موضع ایالات متحده اتخاذ می‌کند و معتقد است سازوکار و نظم فعلی حاکم بر جهان، که فعالیت دولت‌ها در جهان فیزیکی را هدایت می‌نماید، باید بتواند به صورت برخط و اینترنتی نیز چنین کاری را انجام دهد. این کشور همچنین از هنجارها، درک مشترک دربارهٔ نحوهٔ اعمال قوانین بین‌المللی در فضای سایبری، اقدامات اعتمادسازی، ظرفیت‌سازی ــ از طریق مرکز جهانی ظرفیت امنیت سایبری در

دانشگاه آکسفورد[1] ــ و همکاری در زمینهٔ جرایم سایبری حمایت می‌کند.[2] انگلستان همچنین در دکترین امنیت سایبری ملی خود اذعان می‌دارد که در حال آماده‌سازی «برنامهٔ سایبری تهاجمی ملی» است و هنگامی که بحث «منافع ملی» به میان آید، از هیچ اقدامی برای مقابله با آن فروگذار نخواهد کرد.

بریتانیا در کنفرانس لندن در سال ۲۰۱۱، در خصوص فضای سایبری و کنفرانس‌های بعدی در مجارستان (۲۰۱۲)، سئول (۲۰۱۳)، هلند (۲۰۱۵) و هندوستان (۲۰۱۷) به دنبال شکل دادن به بحث بین‌المللی هنجارها بود.[3] هدف این کنفرانس‌ها ــ که تحت عنوان «کنفرانس لندن» شناخته می‌شوند ــ جا انداختن این ایده‌هاست: تدوین هنجارهای سایبری بر اساس قوانین بین‌المللی، اینترنت آزاد و باز که الگوی چندذی‌نفعی، با تأکید بر نقش آیکان، آن را اداره می‌کند، و لزوم ظرفیت‌سازی به منظور افزایش تعداد افرادی که به طور ایمن از فضای اینترنت بهره‌برداری می‌کنند.

با تأیید برگزیت و حتمی شدن جدایی این کشور از اتحادیهٔ اروپا، بریتانیا در حال بازطراحی سیاست‌های منطقه‌ای و بین‌المللی خود در آینده است؛ هرچند در کوتاه‌مدت به نظر می‌رسد که این کشور سیاست حفظ روابط استراتژیک با اتحادیهٔ اروپا و نیز نزدیکی بیشتر به آمریکا به خصوص در ارتباط با مسائل و چالش‌های فضای سایبری را به طور هم‌زمان دنبال می‌کند. در اوایل سال ۲۰۲۰ و تحت فشارهای آمریکا، بریتانیا همکاری خود با شرکت چینی هوآوی در زمینهٔ فناوری نسل پنجم (۵G) را لغو کرد.

---

1. Global Cyber Security Capacity Centre at the University of Oxford.

2. Global Cyber Security Centre, 2017

3. London Conference on Cyberspace: Chair's Statement, 2017; Budapest Conference on Cyber Security 2012; the Soul Conference on Cyberspace, 2017; Global Conference on Cyberspace 2015 & 2017.

- **چین**

چین در کنار روسیه و به عنوان یک قدرت سایبری نوظهور، رویکردی کاملاً مقابله‌جویانه با رویکرد آمریکا و دیگر دموکراسی‌های غربی را دنبال می‌کند. استدلال چین این است که کشورها برای هدایت رفتار خود در اینترنت به منظور بهبود ثبات سایبری باید چهار اصل را رعایت کنند: ۱. کشورها باید از طریق مخالفت با «اقدامات خصمانه و تجاوزگرانه» و «جلوگیری از نبردها و درگیری‌های تسلیحاتی»، فضای سایبری مسالمت‌آمیزی را توسعه دهند؛ ۲. کشورها برای شکل بخشیدن به فضای سایبری قلمرو خود ــ از جمله محافظت از زیرساخت‌های مهم در برابر بدافزارها به منظور قانونمندسازی اطلاعات سامانه‌های برخط (آنلاین) قابل‌دسترس در مرزهای آن کشور ــ از حق حاکمیت برخوردارند؛ ۳. دولت‌ها باید برای حکمرانی فضای سایبری رویکردی چندجانبه اتخاذ کنند و در این حین، سازمان ملل نقش اساسی در ایجاد اجماع بین‌المللی در خصوص قوانین فعالیت‌های برخط دارا باشد؛ ۴. کشورها باید تلاش کنند با پیاده‌سازی اهداف توسعهٔ پایدار[1] مزایای اتصال برخط را به اشتراک بگذارند.[2] چین به منظور اجرای این اصول موارد زیر را به کشورها توصیه می‌کند:

ــ تقویت صلح سایبری از طریق رویکردهای دوجانبه و منطقه‌ای یا چندجانبه با هدف گسترش ارتباطات، تقویت اعتماد متقابل و جلوگیری از درگیری در فضای سایبری.

ــ موافقت با یک آیین‌نامهٔ بین‌المللی رفتاری دولت‌ها برای امنیت اطلاعاتی، که در سال ۲۰۱۱ منتشر و در سال ۲۰۱۵ به‌روز شد.

---

1. Sustainable Development Knowledge Platform
2. Tian Sh., 2017

ـــ حمایت از طرح‌های ظرفیت‌سازی برای کاهش شکاف دیجیتال.

موضع کشور چین همسو با روسیه و برخلاف آمریکا این است که در حال حاضر هیچ گونه قوانین بین‌المللی عمومی برای کنترل رفتار دولت‌ها در فضای سایبری وجود ندارد و قوانین فعلی نیز، که دموکراسی‌های غربی مدعی ضرورت تسرّی آن به عرصهٔ سایبری هستند، از کفایت لازم برخوردار نیست. اگرچه پکن اسنادی را تأیید کرده است که به کاربرد قانون بین‌المللی اینترنت، از جمله اعلامیهٔ گروه جی ۲۰ آنتالیا یا گزارش گروه کارشناسان دولتی سازمان ملل متحد در سال ۲۰۱۳ اشاره دارد، اما چین مدعی است که چارچوب کلی قوانین موجود باید با وضع قوانین جدید و مختصِ فضای سایبری به‌روز شوند.[1]

چین در سال‌های اخیر از لاک دفاعی تاریخی در عرصهٔ سیاست خارجی خود خارج شده و به خصوص در عرصهٔ سایبری یک استراتژی سه‌وجهی شامل ۱. رویکرد تهاجمی با هدف تضعیف زیرساخت‌های اطلاعاتی و ارتباطی کشورهای رقیب، ۲. سرمایه‌گذاری تجاری ـ اقتصادی در زیرساخت‌های ارتباطی و اطلاعاتی کشورهای همسو و هدف، و ۳. مشارکت در استانداردسازی از طریق حضور فعال در نظام‌ها و استانداردسازی‌های فناوری در مجامع بین‌المللی را به طور هم‌زمان دنبال می‌کند. چین همچنین با هدف ترویج و تبلیغ دیدگاه‌های خود در عرصهٔ سایبری و همچنین تبلیغ شرکت‌های فناوری چینی از کنفرانس‌های سالانهٔ ووژن[2](موسوم به کنفرانس جهانی اینترنت) حمایت مالی عمده‌ای به عمل می‌آورد.[3]از نگاه بسیاری از تحلیلگران حوزهٔ سایبری، کنفرانس جهانی اینترنت که هر سال در ووژن برگزار می‌شود، نوعی ابتکار چین برای

1. G20 Leaders Communiqué, 2017
2. Wuzhen
3. World Internet Conference, 2017

ایجاد موازنه با کنفرانس لندن است که عمدتاً کشورهای غربی برگزار می‌کنند. چین از طریق ووژن بر اهمیت حکمرانی سایبری و ترویج رویکردهای چندجانبه در حل اختلافات بین کشورها تأکید می‌کند.

- **فرانسه**

فرانسه، مانند انگلستان و ایالات متحده، بر اعمال قوانین بین‌المللی در فضای سایبری و لزوم تسرّی و توسعهٔ هنجارهای فعلی تأکید دارد. فرانسه در راهبرد خود این گونه استدلال می‌کند که دستیابی به اجماع دربارهٔ هنجارها مستلزم گفت‌وگوهای بیشتری است. گفت‌وگوهای غیررسمی یا بحث در مجامع غیرسنتی می‌تواند به پیشرفت‌های غیرمنتظره‌ای منجر شود، و ظرفیت‌سازی برای کاهش تهدیدات سایبری مرتبط با زیرساخت‌های کلیدی ضروری است.

برخلاف ایالات متحده و انگلستان، ارزیابی‌های فرانسه نشان می‌دهد که وابستگی به برخی فناوری‌های انحصاری[1] می‌تواند تهدیدی برای آیندهٔ اقتصادی این کشور محسوب شود. در این خصوص اگرچه فرانسه با کشورهای روسیه و چین در این زمینه که معتقدند «تسلط» ایالات متحده در فضای سایبری تهدیدی ذاتی برای ثبات سایبری می‌باشد همسو است، اما این کشور هیچ راهبردی برای برون‌رفت از این وضعیت ارائه نمی‌دهد. فرانسه نیز یکی از معدود کشورهای غربی است که صریحاً با اشاره به تهدید عملیات اطلاعاتی خاطرنشان می‌کند که این نوع تهدیدات حتی اگر از لحاظ فنی پیچیده نباشند، اما سبب تضعیف اعتماد به زیرساخت‌های کلیدی شده است[2].

در سال‌های اخیر، فرانسه در ارتباط با حوزهٔ سایبری، توجه زیادی به موضوع کلان داده‌ها و نیز هوش مصنوعی به عنوان فاکتورهای مهم حکمرانی قرن ۲۱ از

---

1. On a Few Monopolies
2. Gordon C., 2016

خود نشان داده است. امانوئل مکرون، رئیس‌جمهوری این کشور، سال ۲۰۱۹ با اشاره به سیطرهٔ هوش مصنوعی بر زندگی سیاسی، اجتماعی و فرهنگی اروپا در عصر حاضر علناً هشدار داد که دولت‌ها و حتی ساختارها و نظام‌های قدرتمندی همچون ناتو تا آستانهٔ بحران و فروپاشی کامل پیش رفته‌اند.[۱]

- **هندوستان**

شعار «هند دیجیتال» که از سوی دولت فعلی هندوستان مطرح شده، از طریق دیپلماسی سایبری و به طور کامل بر بستر سایبری استوار است. دستیابی به هندِ دیجیتال که به پشتوانهٔ پتانسیل فناوری اطلاعات و ارتباطات (حدود ۲۰ درصد تولید ناخالص داخلی) و نیز زیرساخت‌های دیجیتال این کشور دنبال می‌شود، مستلزم ایفای نقش گسترده‌تر این کشور در سیاست‌گذاری‌ها و تصمیم‌سازی‌های مهم منطقه‌ای و بین‌المللی در زمینهٔ سایبری است. به طور مشخص تضمین امنیت دیجیتال این کشور در بُعد داخلی و اعتمادسازی، ظرفیت‌سازی و تقویت هنجارهای بین‌المللی برای مقابله با تهدیدات و حملات سایبری در بُعد خارجی، مهم‌ترین محور فعالیت‌های دیپلماتیک سایبری هندوستان را تشکیل می‌دهند.[۲]

هندوستان به عنوان کشور و قدرتی نوظهور، موضعی عمدتاً بینابین دو جبههٔ غربی (به رهبری آمریکا و انگلستان) و جبههٔ شرقی (به رهبری روسیه و چین) دارد. هندوستان بر این باور است که کشورها باید به دنبال توافق بر سر هنجارهای رفتاری مشترک باشند. دراین‌راستا، استراتژی هندوستان تعامل سازنده با هر دو جبههٔ غربی و شرقی است، به طوری که این کشور از یک سو میزبانیِ کنفرانس لندن[۳]را عهده‌دار شده، و از سوی دیگر با حضور در

---

۱. مصاحبهٔ امانوئل مکرون با هفته‌نامهٔ *اکونومیست*، ۷ نوامبر ۲۰۱۹.

2. Mukesh Dhirubhai Ambani, 2019

3. London Process

سازمان همکاری شانگهای در ژوئن ۲۰۱۷، در معاهدهٔ امنیت اطلاعات این سازمان مشارکت کرده است. نظر به اینکه اجماع دربارهٔ هنجارها ممکن است چالش‌برانگیز باشد، مواضع هندوستان در سال ۲۰۱۶ به دبیرکل سازمان ملل متحد دربارهٔ مسائل امنیتِ اطلاعات حاکی از آن است که کشورها باید اقدامات اعتمادسازی را به عنوان راهی برای دستیابی به توافق عمومی در خصوص هنجارها در اولویت قرار دهند.[1]

برخلاف ایالات متحده و دیگر کشورهای همسو، هندوستان به دنبال ایجاد گروه‌های کاری جدید در نهادهای چندجانبه است که یکی از مهم‌ترین آن‌ها کمیتهٔ استفادهٔ صلح‌آمیز از فضای ماورای جو[2] است که با میزبانی سازمان ملل به مباحثِ ثبات سایبری می‌پردازد. علاوه بر این، هند در چند سال گذشته گفت‌وگوهای دوجانبه با شرکای اصلی منطقه‌ای و بین‌المللی را دنبال کرده که مهم‌ترین آن‌ها عبارت بوده‌اند از: اولین دور گفت‌وگوهای سایبری با روسیه (۲۰۱۶)، سومین نشست گفت‌وگوهای سایبری با استرالیا (۲۰۱۹)، سومین دور گفت‌وگوهای سایبری با فرانسه (۲۰۱۹)، دومین دور گفت‌وگوهای سایبری با ژاپن (۲۰۱۸)، اولین دور گفت‌وگوهای سایبری با انگلستان (۲۰۱۸)، دومین دور گفت‌وگوهای سایبری با اتحادیهٔ اروپا (۲۰۱۸) و پنجمین دور گفت‌وگوهای سایبری با آمریکا (۲۰۱۸).

از دیگر ابتکارات هند در حوزهٔ دیپلماسی سایبری، ورود جدی این کشور به تعامل با پلتفرم‌های جهانی در زمینهٔ «حکمرانی داده»ها و واداشتن این پلتفرم‌ها به پذیرش مسئولیت ــ بند ۷۹ قانون فناوری اطلاعات هند[3] ــ در برابر محتواهایی است که از طریق آن‌ها جریان می‌یابند.

---

1. UN General Assembly, Resolution 70/237, 2017
2. Committee for the Peaceful Uses of Outer Space
3. Section 79 of the Indian Information Technology Act

جنبش ضد مهاجرت داده‌ها از این کشور، که در سال ۲۰۱۹ در این کشور مطرح شد، از دیگر تحولات مهم در هندوستان در ارتباط با دیپلماسی سایبری است که می‌توان به آن اشاره کرد. این موضوع که به ضرورت ذخیره‌سازی تمامی داده‌ها و اطلاعات مربوط به هندوستان در داخل این کشور اشاره دارد، اولین‌بار در کنفرانس گجرات (۲۰۱۹) از سوی یکی از تاجران و کارآفرینان بزرگ این کشور مطرح و مورد توجه خاص مقامات و مسئولان دولتی قرار گرفت.[1]

با توجه به اینکه هند بزرگ‌ترین بازار خارجی و نامحدود اَپ‌ها در جهان است، موضوع تعامل با پلتفرم‌ها و حکمرانی داده‌ها در این کشور دو محور مهم در تمامی سیاست‌ها، اقدامات و ابتکارات دولت هند در ارتباط با عرصهٔ سایبری را تشکیل می‌دهند.

- **ژاپن**

ژاپن به لحاظ استراتژیک، در جبههٔ دموکراسی‌های غربی جای می‌گیرد. با این حال در استراتژی‌های عملیاتی برای پیشبرد اهداف خود، اولویت را به کشورهای پیرامونی (آسیا و اقیانوسیه) داده است. در نگاه این کشور، فضای سایبری عامل گذار جوامع به جامعهٔ نوع ۵[2]خواهد بود که در آن ارزش‌ها و خدمات جدید به طور مداوم ایجاد می‌شود و رفاه بیشتری برای افراد جامعه به ارمغان خواهد آورد. بر اساس توازن استراتژیک ژاپن از فرصت‌ها و تهدیدهای حوزهٔ سایبری، این کشور دیپلماسی سایبری خود را بر پنج اصل استوار ساخته است: ۱. تضمین جریان آزاد اطلاعات، ۲. حاکمیت

---

1. Gujarat Conference, 2019

۲. Society 5.0 به توسعهٔ تاریخی جوامع بشری از جامعهٔ مبتنی بر شکار به جامعهٔ کشاورزی، صنعتی، اطلاعاتی و جامعهٔ عصر فضای سایبری، به عنوان آخرین مرحلهٔ آن، اشاره دارد.

قانون،۳. باز بودن، ۴. خودگردانی، و ۵. همکاری بین تمامی ذی‌نفعان.

همچنین در رویکرد ژاپن به مقولهٔ سایبری، هر گونه «حفرهٔ امنیتی» در سایر کشورها خطری بزرگ برای کل جهان، از جمله ژاپن، محسوب می‌شود. بر مبنای سه اصل ۱. ضرورت قانون‌گذاری و اطمینان از حاکمیت قانون، ۲. توسعهٔ اقدامات اطمینان‌بخش در زمینهٔ فضای سایبری، و ۳. همکاری در زمینهٔ بسترسازی و ظرفیت‌سازی در حوزهٔ فضای سایبری، ژاپن دو اولویت در زمینهٔ دیپلماسی سایبری خود مدنظر دارد:

اولویت نخست، اطمینان از همکاری سایبری در منطقه آسیا ـ اقیانوسیه، به عنوان حوزهٔ پیرامونی این کشور، و اولویت دوم، همکاری با جامعهٔ بین‌الملل (سازمان‌های جهانی) و نیز کشورهایی نظیر آمریکا و اروپاست که در زمینهٔ فضای سایبری، ارزش‌های مشترکی با کشور ژاپن دارند.

- **تحلیل و ارزیابی تطبیقی نقش بازیگران سایبری (کشورها)**

در یک برآیند کلی می‌توان گفت که موارد اختلافی بین رویکردهای مطرح‌شده در هر یک از بازیگران حوزهٔ سایبری به مراتب بیشتر و وسیع‌تر از موارد اشتراک و اتفاق نظر است. به لحاظ اصولی، از جمله معدود مواردی که این کشورها با یکدیگر توافق دارند، چهار معیار کلی و کلان برای ارتقای ثبات سایبری در عرصهٔ بین‌المللی است که شامل این موارد می‌شود: ۱. قوانین پایه (هنجارها یا پیمان‌های تعیین‌کننده)، ۲. تداوم گفت‌وگو (دوجانبه و چندجانبه)، ۳. اقدامات اعتمادسازی، و ۴. ظرفیت‌سازی و توسعه.

با این حال و به خصوص در عرصهٔ استراتژی‌های راهبردی و عملیاتی، با توجه به ایدئولوژی و منافع ملی هر یک از بازیگران، دیدگاه‌های بسیار متفاوت و گاه متضادی در ارتباط با هر یک از مقولات و مؤلفه‌های فضای سایبری نمایان می‌شود. روسیه و چین و فرانسه بر این باورند که تسلط یک

کشور بر فضای سایبری تعادل راهبردی حوزهٔ سایبری را تهدید می‌کند، در حالی که ایالات متحده، انگلستان، اتحادیهٔ اروپا و هندوستان اشاره‌ای به این امر ندارند. روسیه و چین و هندوستان معتقدند که سوءاستفاده از فناوری اطلاعات و ارتباطات و رسانه‌های اجتماعی ممکن است سبب تشدید تنش‌های اجتماعی گردد و باید نوعی تهدید محسوب شود. روسیه و چین به صراحت اظهار داشتند که دخالت در امور داخلی کشورها را از طریق حوزه‌های سایبری تهدیدی برای حاکمیت خود قلمداد می‌کنند.

همچنین تعاریف و اصطلاحات به‌کارگرفته‌شده در خصوص تهدید، در کشورهای مختلف با یکدیگر متفاوت است. ایالات متحده و اتحادیهٔ اروپا امنیت سایبری را محافظت از داده‌ها، نرم‌افزارها و سخت‌افزارها در برابر استفادهٔ غیرمجاز تعریف می‌کنند. روسیه، چین و برخی کشورهای سازمان همکاری شانگهای با بیان اینکه محتوای اطلاعات یا پیامی که به صورت اینترنتی منتقل می‌شود ممکن است با مداخله در امور داخلی کشورها ثبات بین‌المللی را تهدید کند، بکارگیری اصطلاح «امنیت اطلاعات و فضای اطلاعاتی» را ترجیح می‌دهند. ایالات متحده و اتحادیهٔ اروپا و دیگر کشورها تأکید کمتری بر محتوای ارتباطات اینترنتی دارند و معتقدند می‌توان از آن برای توجیه اعمال محدودیت در آزادی بیان، که تحت حمایت اعلامیهٔ جهانی حقوق بشر[1] و میثاق بین‌المللی حقوق مدنی و سیاسی[2] قرار دارد، سوءاستفاده کرد.

محل اختلاف اصلی بین رویکرد چین ـ روسیه[3] و رویکرد ایالات متحده و دیگر کشورهای همسو بر سر موضوع تدوین آیین‌نامه یا عهدنامهٔ رفتاری جدید در این زمینه است. دستهٔ دوم (محور ایالات متحده) دست‌کم به سه دلیل،

1. Universal Declaration of Human Rights
2. International Covenant on Civil and Political Rights (ICCPR)
3. Sino-Russian Approach

مخالف معاهده یا آیین‌نامهٔ رفتاری جدید هستند: ۱. دولت‌ها هنوز ارزیابی دقیقی در خصوص اعمال تمهیدات قوانین بین‌المللی موجود در فضای سایبری انجام ندادند. بدون انجام این کار، ایالات متحده و متحدانش معتقدند که امکان‌سنجی قانون جدید بدون شناسایی شکاف‌های مخصوص آن عجولانه و زودهنگام است. ۲. پیش از مذاکره دربارهٔ یک پیمان لازم است دولت‌ها به درک مشترکی از آن برسند. برای مثال، اختلاف‌نظر میان ایالات متحده و روسیه دربارهٔ امنیت اطلاعات ممکن است به درخواست‌هایی برای ممنوعیت «سلاح‌های اطلاعاتی» منجر شود که اسباب نگرانی ایالات متحده و اتحادیهٔ اروپا را در خصوص قانون‌گذاری در حوزهٔ آزادی بیان، که تحت نظارت قانون بین‌المللی حقوق بشر قرار دارد، فراهم می‌آورد. ۳. ماهیت ابزارهای سایبری، پیروی از پیمانی را که بکارگیری آن‌ها را محدود می‌کند، دشوار یا ناممکن می‌سازد. در واقع، بدافزارها و تکنیک‌های استفاده‌شده در انجام عملیات سایبری تهاجمی را نمی‌توان به مثابهٔ تانک‌ها یا موشک‌ها در عملیات جنگی نظامی در نظر گرفت و آن‌ها را محور اصلی برای توافق‌نامه‌های کنترل تسلیحات سایبری لحاظ کرد.

مهم‌ترین سازمان‌ها و نهادهای بزرگ جهانی

در بین سازمان‌های مهم جهانی، سازمان ملل متحد مهم‌ترین و اصلی‌ترین مرجع برای طرح دیدگاه‌ها و ابتکارات دربارهٔ دیپلماسی سایبری، هم از سوی بازیگران طرفدار رویکرد آمریکایی و هم از سوی طرفداران رویکرد چین ـ روسیه، بوده است. در واقع مصالحه‌ای که شکاف بین موضع روسیه ــ چین و موضع ایالات متحده ـ کشورهای غربی را از میان برمی‌دارد، در سازمان‌هایی با عضویت‌های گسترده‌تر همچون سازمان ملل متحد شکل می‌گیرد.

در کنار سازمان ملل، دیگر سازمان‌ها و نهادهای منطقه‌ای نیز از اهمیت بالایی برخوردار بوده‌اند. اگرچه در خصوص طرح‌های دیپلماتیکِ پیشنهادشده یا اقداماتِ صورت‌گرفته، هم در سازمان ملل و هم در سازمان‌ها و نهادهای منطقه‌ای، برآیند کلی این است که این اقدامات و ابتکارات عمدتاً بازتاب‌دهندهٔ منافع اعضای پیشنهاددهندهٔ آن است. با این حال، این گرایش جانبدارانه در ارتباط با سازمان‌ها و نهادهای منطقه‌ای که به خصوص گرایش‌های ایدئولوژیک و نظامی دارند پررنگ‌تر و آشکارتر است. برای مثال، طرح‌های مرتبط با ثبات سایبری در سازمان پیمان آتلانتیک شمالی (ناتو) یا گروه هفت (جی ۷)، نظریات ایالات متحده و انگلستان و فرانسه را بازتاب می‌دهد. به طور مشابه، طرح‌های سازمان همکاری شانگهای و بریکس[1] بازتابی از دیدگاه‌های روسیه و چین هستند.

آنچه در ادامه می‌آید، نگاهی به برخی از مهم‌ترین اقدامات و ابتکاراتی است که در حوزهٔ دیپلماسی سایبری در سطح سازمان‌های مهم بین‌المللی و منطقه‌ای صورت گرفته است:

- **سازمان ملل متحد**

در سازمان ملل، برای ارتقای ثبات و امنیت سایبری سه فعالیت عمده صورت گرفته است: نخست، تشکیل گروه کارشناسان دولتی سازمان ملل متحد در زمینهٔ تحولات حوزهٔ فناوری اطلاعات و ارتباطات در حوزهٔ امنیت بین‌المللی که مهم‌ترین طرح این سازمان است. از سال ۲۰۰۴، این گروه پنج نشست برگزار، و سه گزارش اجماع صادر کرده است. نخستین گزارش حاکی از آن است که کشورها به منظور «کاهش خطر سوءبرداشت» در فضای سایبری، هنجارها و

1. BRICS (Brazil, Russia, India, China and South Africa)

اقدامات اعتمادسازی و طرح‌های ظرفیت‌سازی را در نظر بگیرند.[1] گزارش اجماع دوم نخستین گزارشی بود که طی آن قدرت‌های بزرگ به صراحت تصدیق کردند که «حقوق بین‌الملل، به ویژه منشور سازمان ملل متحد برای حفظ صلح و ثبات و ترویج محیط فناوری اطلاعات و ارتباطاتِ آزاد، ایمن، صلح‌آمیز و قابل‌دسترس، مناسب و ضروری است».[2] این گزارش همچنین توسعهٔ اقدامات اعتمادسازی منطقه‌ای را تشویق می‌کند. سومین گزارش اجماع، کشورها را به پیروی از هنجارهای داوطلبانهٔ زمان صلح ترغیب می‌کند، از جمله:

ــ آگاهانه اجازه ندهند از قلمرو آن‌ها، به سبب بکارگیری فناوری اطلاعات و ارتباطات، در مسیر اقدامات غیرقانونی بین‌المللی استفاده شود.

ــ از روی عمد، با استفاده از فناوری اطلاعات و ارتباطات به زیرساخت‌های کلیدی کشوری دیگر آسیب نرسانند.

ــ به درخواست‌های کمک پاسخ دهند.[3]

البته گروه کارشناسان دولتی در نشست سال‌های ۲۰۱۶ ــ ۲۰۱۷ نتوانست به توافق عمومی دست یابد و بنا به استدلال ایالات متحده به دلیل عدم تمایل دولت‌ها به توضیح چگونگی اعمال قوانین، به خصوص حقوق بین‌الملل نظیر قانون درگیری مسلحانه[4] یا مسئولیت دولت، در فضای سایبری با شکست مواجه شد. کوبا با تکرار نظریات روسیه و چین اظهار داشت که تأیید قانون درگیری مسلحانه به فضای سایبری، به عنوان یک حوزهٔ درگیری نظامی، مشروعیت بخشیده و به عملیات سایبری تحت حمایت دولت، چراغ سبز نشان می‌دهد.

دوم، اعضای سازمان همکاری شانگهای پیش‌نویس آیین‌نامهٔ بین‌المللی

---

1. The UN General Assembly, A/65/201, 2017
2. The UN General Assembly, A/68/98, 2017
3. The UN General Assembly, A/70/174, 2017
4. Law of Armed Conflict (LOAC)

رفتار را به منظور امنیت اطلاعات، در مجمع عمومی سازمان ملل متحد منتشر کرده‌اند.[1] این آیین‌نامه پیشنهاد می‌کند کشورها داوطلبانه از «بکارگیری [فناوری اطلاعات و ارتباطات] ... برای انجام فعالیت‌هایی که خلاف حفظ صلح و امنیت بین‌المللی هستند خودداری کنند». برای مثال، این آیین‌نامه از کشورها درخواست می‌کند تا برای مبارزه با «فعالیت‌های جنایت‌کارانه و تروریستی» که با استفاده از فناوری اطلاعات و ارتباطات سبب تحریک «تروریسم، جدایی‌طلبی یا افراط‌گرایی» می‌شوند همکاری کنند، و دیگر آنکه کشورها از فناوری‌های اطلاعات و ارتباطات برای مداخله در امور داخلی دولت‌ها بهره‌برداری ننمایند. نسخه‌های مختلف این آیین‌نامه از سال ۲۰۱۱، در سازمان ملل متحد مطرح شده و به سبب ناسازگاری مفروض آن با قانون حقوق بشر انتقادهایی را به خود جلب کرده است.[2] همچنین با توجه به اینکه هنوز به عنوان یک قطعنامهٔ رسمی معرفی نشده است، بعید به نظر می‌رسد که از حمایت لازم برای تصویب در مجمع عمومی برخوردار شود.

سوم، مجمع عمومی سازمان ملل قطعنامه‌ای را در سال ۲۰۰۳ به تصویب رساند که طی آن از دولت‌ها می‌خواهد با فراخواندن ذی‌نفعان داخلی به کسب آگاهی در زمینهٔ خطراتِ امنیت سایبری و گام نهادن در مسیر کاهش آن‌ها، در حوزهٔ امنیت سایبری، فرهنگ‌سازی کنند.[3]

در مجموع دربارهٔ این فعالیت‌ها می‌توان گفت که سازمان ملل نیز همچون چند دههٔ گذشته، صحنهٔ رقابت قدرت‌ها (به خصوص جبههٔ غرب به رهبری آمریکا و جبههٔ شرق به رهبری چین و روسیه) برای تحمیل ایده‌های خود در حوزهٔ سایبری بوده است. هرچند با توجه به سابقهٔ طولانی

1. The UN General Assembly, A/69/723, 2017
2. The UN General Assembly, A/66/359, 2017
3. The UN General Assembly, A/RES/47/239, 2013

این رویارویی‌ها، جبههٔ غربی به رهبری آمریکا دست‌کم بـه صـورت ظـاهری موفقیت بیشتری در پیشبرد اهداف سایبری خود داشته است.

- **اتحادیهٔ اروپا**

رویکرد اتحادیهٔ اروپا بـه ثبـات سـایبری بـا ایـالات متحـده و انگلسـتان و بخش‌هایی از رویکرد فرانسه همسو است. این اتحادیه از تسـرّی و کـاربرد قوانین بین‌المللی در فضای سایبری و نیاز به هنجارهای سـایبری و اهمیـت اقدامات اعتمادسازی برای کاهش بی‌اعتمـادیِ راهبـردی حمایـت مـی‌کنـد.[1] اسناد استراتژی اتحادیهٔ اروپا تأکید بسزایی بر اهمیت محیط اینترنتـی آزاد و باز دارد؛ جایی که حقوق بشر به صورت برخط هم رعایت می‌شود.

شورای اتحادیهٔ اروپا، که نمایندهٔ رؤسای دولت یا کشور اعضای اتحادیهٔ اروپاست، اخیراً استفاده از بسته‌ابزارهای دیپلماتیک سایبری را تأیید کرده است. این بسته، نحوهٔ پاسخ‌دهی به عملیات سایبری، که از جمله شامل تحریم نیز می‌شود، را به سایر بازیگران ابلاغ می‌کند. با وجود آنکه بر اساس بسته‌ابزارهای دیپلماتیک سایبری، اعضای شورا تصدیق می‌کنند که تمامی کشورها از قدرت مستقل برای انتساب جرم و پاسخ دادن به یک حادثهٔ سایبری برخوردارند، اتحادیهٔ اروپا در صورت درخواست یکی از کشورهای عضو قربانی، آمادگی تحریم آن عامل را دارد.

دربارهٔ بسته‌ابزارهای دیپلماتیک سایبری اتحادیهٔ اروپا، در بـین تحلیلگـران هنوز دورنمای روشنی وجود ندارد؛ به خصوص اینکه در این بسته اگرچه بـا توجـه بـه ماهیـت، مقیـاس، پیچیـدگی، گسـتردگی و میـزان تـأثیر حمـلات صورت‌گرفته، برخی اقدامات محدودکننده پیش‌بینی‌شده، با این حـال ماهیـت اقدامات پیش‌بینی‌شده در عمل، تعیین و مشخص نشـده اسـت. بـا توجـه بـه

1. The UN General Assembly, A/RES/47/239, 2013

گذشت چند سال از تصویب بسته‌ابزارهای دیپلماتیک اتحادیهٔ اروپا، به ندرت کشورهای عضو این اتحادیه توانسته‌اند در خصوص اتخاذ یک راهبرد عملیاتی مشترک در ارتباط با کشورهای هدف به اتفاق نظر برسند. به خصوص اینکه برخی از اعضای این اتحادیه منافعی در همسویی با جبههٔ آمریکایی و برخی دیگر نیز منافعی در همسویی با جبههٔ روسیه ـ چین دارند. به طور کلی، این بسته بیشتر شبیه یک مانیفست است تا فراهم‌کنندهٔ برخی اقدامات عملی مشخص و روشن.

- **سازمان امنیت و همکاری اروپا**

کشورهای عضو سازمان امنیت و همکاری اروپا ــ که نهادی فراگیرتر از اتحادیهٔ اروپا محسوب می‌شود ــ برای ارتقا و ثبات سایبری با دو سِری از اقدامات اعتمادسازی داوطلبانه موافقت کرده‌اند. آن‌ها کشورهای عضو را به این مسائل تشویق می‌کنند:

ــ تبادل مقالات سفید،[1] اسناد راهبردی و دیدگاه‌های ملی در حوزهٔ موضوعات سایبری.

ــ برگزاری جلسات گفت‌وگوی مداوم برای کاهش خطرات سوءبرداشت که ممکن است ناشی از بهره‌برداری از فناوری اطلاعات و ارتباطات باشند.

ــ وضع قوانینی که امکان به‌اشتراک‌گذاری اطلاعاتِ «بهره‌برداری تروریستی یا جنایت‌کارانه از فناوری اطلاعات و ارتباطات» را فراهم می‌آورد.

ــ معرفی یک خط تماس ملی جهت تسهیل گفت‌وگو بین دولت‌ها دربارهٔ مسائل سایبری.

---

۱. مقالات سفید در سیاست عموماً به بیانیه یا گزارشی گفته می‌شود که از آن برای ارائهٔ ترجیحات یا اولویت‌های سیاسی دولت‌ها، پیش از معرفی این ترجیحات به عنوان قانون، استفاده می‌شد. انتشار یک مقالهٔ سفید دربارهٔ موضوعی خاص عموماً برای شناسایی افکار عمومی و سنجش انواع واکنش‌ها به آن اولویت‌ها و سیاست‌ها صورت می‌گیرد.

ــ شناسایی فرصت‌های همکاری به منظور بهبود امنیت سایبری زیرساخت‌های کلیدی.

ــ تشویق به افشای مسئولانهٔ آسیب‌پذیری‌های فناوری اطلاعات و ارتباطات.[1]

بر اساس اعلام دبیرخانهٔ سازمان امنیت و همکاری اروپا، تقریباً ۹۰ درصد کشورها خط تماس ملی را تعیین و معرفی کرده، و راهبردهای ملی سایبری و سازوکارهای سازمانی را دراین‌باره به اشتراک گذاشته‌اند که از طریق یک سکوی اشتراک‌گذاری اطلاعات به نام پی‌اُ اِل‌آی‌اس[2] در دسترس سایر اعضای سازمان امنیت و همکاری اروپا قرار گرفته است.[3]

همچنین سازمان امنیت و همکاری اروپا شبکهٔ ارتباطی ایمنی را راه‌اندازی کرده است که کشورها می‌توانند برای استعلام رسمی دربارهٔ اقدامات دولت دیگری، که یک تهدید یا خطر امنیتی برای آن‌ها به شمار می‌آید، از آن بهره‌برداری کنند. کشورهای عضو سازمان امنیت و همکاری اروپا استفاده از این شبکه را برای تحقیقات دربارهٔ فضای سایبری به تصویب رسانده، و مراحلی را که کشورها باید هنگام درخواست استعلام سایبری طی کنند طراحی کرده‌اند.

- **مجمع منطقه‌ای اتحادیهٔ آسه‌آن**[4]

تلاش‌ها برای بهبود پایداری و تاب‌آوری سایبری در حوزهٔ منطقهٔ جنوب شرق آسیا، موسوم به کشورهای عضو اتحادیهٔ آسه‌آن، دست‌کم از سال ۲۰۱۰ در جریان بوده است. در سال ۲۰۱۵، وزرای این اتحادیه با برنامه‌ای

---

1. Decision No. 1202 OSCE Confidence Building Measures, 2017
2. POLIS
3. OSCE Polis Home, 2017
4. Association for Southeast Asian Nations' Regional Forum (ASEAN RF)

برای ارتقای امنیتِ بکارگیری فناوری اطلاعات و ارتباطات موافقت کردند. همچنین در سال ۲۰۱۷ اعضای این اتحادیه توافق خود را دربارهٔ برگزاری یک نشست بین بخشی در حوزهٔ امنیت فناوری اطلاعات و ارتباطات اعلام کردند. مالزی و سنگاپور به عنوان اعضای اصلی آسه‌آن، و کشورهای چین، استرالیا، ایالات متحده، کرهٔ جنوبی به عنوان شرکای منطقه‌ای این اتحادیه، کارگاه‌ها و نشست‌های زیادی برای بالا بردن حساسیت اعضا به اهمیت هنجارها و اقدامات اعتمادسازی و ظرفیت‌سازی در راستای بهبود ثبات سایبری برگزار کرده‌اند.[1]

مجمع عمومی اتحادیهٔ آسه‌آن تلاش‌های خود را با هدف بهبود همکاری بین گروه‌های پاسخگویی فوریت‌های رایانه‌ای[2] بهبود توانایی گروه‌های پاسخگویی فوریت‌های رایانه‌ای ملی در پاسخ به حوادث از طریق تمرین و ایجاد یک شبکهٔ ارتباطی منطقه‌ای، به منظور تسهیل ارتباطات بحرانی، متمرکز ساخته است. با وجود این، ثابت‌قدم ماندن در این پروژه‌ها به دلیل عدم وجود دبیرخانهٔ ویژه در این اتحادیه یا منابع مالی پایدار دشوار بوده و مستلزم آن است که هر یک از کشورهای عضو با سازمان‌دهی طرح و تأمین سرمایه، آن را تقویت کند.

- **سازمان همکاری شانگهای**

سازمان همکاری شانگهای سازمانی منطقه‌ای است که به منظور همکاری‌های چندجانبهٔ امنیتی و اقتصادی و فرهنگی بین دول عضو تشکیل شده است. رهبران چین، روسیه، قزاقستان، قرقیزستان، تاجیکستان و ازبکستان در سال ۲۰۰۱ این سازمان را با هدف برقراری موازنه در برابر نفوذ آمریکا و ناتو در منطقه پایه‌گذاری کردند. این سازمان اخیراً به لحاظ

1. Chairman's Statement of the 24th ASEAN Regional Forum, 2017
2. CERT-to-CERT

تعداد عضو گسترش داشته و کوشیده است قدرت‌های منطقه‌ای بیشتری را، همچون هندوستان، ایران و ...، درگیر فعالیت‌های خود سازد.

سازمان همکاری شانگهای مهم‌ترین نهاد منطقه‌ای است که با هدایت دو کشور روسیه و چین رهبری می‌شود و هر دو کشور از آن به عنوان یکی از مهم‌ترین مکانیسم‌های بین‌المللی برای پیشبرد اهداف دیپلماتیک خود استفاده می‌کنند. اعضای سازمان همکاری شانگهای علاوه بر ترویج آیین‌نامهٔ رفتاری خود در سازمان ملل متحد، در سال ۲۰۰۹ توافق‌نامهٔ «همکاری در زمینهٔ امنیت اطلاعات» را امضا کردند. این توافق‌نامه آنچه را از دیدگاه اعضا، تهدیدِ عمدهٔ فضای اطلاعاتی محسوب می‌شود منعکس ساخته است (در واقع بازتابی تقریباً یکسان از تهدیدات مندرج در اسناد راهبردی روسیه و چین) و آنان را ملزم به همکاری می‌داند تا این تهدیدات کاهش یابد. این سند به منظور ارتقای امنیت و ثبات سایبری از اعضا می‌خواهد که از میان سایر اقدامات، موارد زیر را رعایت کنند:

ــ در فضای اطلاعاتی بین‌المللی به گونه‌ای عمل کنند که مطابق با «اصول و هنجارهای به رسمیت شناخته‌شدهٔ حقوق بین‌الملل» باشد.

ــ اقدامات جمعی در خصوص توسعهٔ هنجارهای حقوق بین‌الملل برای جلوگیری از گسترش و استفاده از سلاح‌های اطلاعاتی را به تفصیل شرح دهند.

ــ امنیت اطلاعات «ساختارهای کلیدی اعضا» را تضمین کنند.

ــ مقالات سفید را تبادل نمایند، تجربیات خود را به اشتراک بگذارند و به طور منظم به بحث و گفت‌وگو دربارهٔ مسائل امنیت اطلاعات بپردازند.

در سال ۲۰۱۵، چین به منظور به اشتراک گذاشتن بهترین روش‌های جلوگیری از بهره‌برداری از اینترنت برای مقاصد تروریستی، یک «رزمایش مشترک ضد تروریسم آنلاین» برگزار کرد.

با توجه به اطلاعات محدود قابل‌دسترس در حوزهٔ عمومی، مطالب گسترده‌ای در خصوص چگونگی اجرای برنامه‌های سازمان همکاری شانگهای وجود ندارد. با این حال، این امر می‌تواند یک موفقیت تلقی شود، زیرا مبنای توافقات دوجانبهٔ روسیه با چین و هندوستان با آفریقای جنوبی را تشکیل می‌دهد.[1]

- **گروه بریکس**

گروه بریکس، گروهی متشکل از قدرت‌های اقتصادی نوظهور است که شامل برزیل، روسیه، هندوستان، چین و آفریقای جنوبی می‌شود. در سال ۲۰۱۴، بریکس کارگروه کارشناسان سایبری را به رهبری مشاوران امنیت ملی اعضا، به منظور ایجاد مواضع مشترک در خصوص موضوعات سایبری و هماهنگی مواضع آن‌ها در ساختارهای چندجانبه، راه‌اندازی کرد. از سال ۲۰۱۴ رهبران بریکس:

ــ تأکید کرده‌اند «بهره‌برداری و توسعهٔ فناوری اطلاعات و ارتباطات از طریق همکاری بین‌المللی و بکارگیری هنجارها و اصول حقوق بین‌المللی پذیرفته‌شده برای تضمین یک فضای اینترنتی صلح‌آمیز و ایمن و آزاد» از اهمیت ویژه‌ای برخوردار است؛

ــ موافقت خود را با جلوگیری از بهره‌برداری از اینترنت «به عنوان یک سلاح» اعلام کرده‌اند؛

ــ اقدامات نظارتی گسترده و بهره‌برداری از فناوری اطلاعات و ارتباطات را «به منظور نقض حقوق بشر و آزادی‌های اساسی» محکوم شمرده‌اند؛

ــ خواستار ابزار الزام‌آور جهانی برای مقابله با جرایم سایبری شده‌اند؛

ــ بر اهمیت سازمان ملل به عنوان محلی برای ایجاد ثبات سایبری و مباحث حکمرانی اینترنت تأکید ورزیده‌اند؛

---

1. Shanghai Cooperation Organization, 2015

ــ یک شبکهٔ ارتباطی بین گروه‌های پاسخگویی به فوریت‌های رایانه‌ای در کشورهای عضو بریکس ایجاد کرده‌اند.[1]

با وجود اشارهٔ اطلاعیه‌های گروه بریکس به اهمیت رعایت «هنجارهای جهانی» و «اصول حقوق بین‌الملل» از سوی کشورها، در هیچ یک از این اطلاعیه‌ها از محتوای گزارش سال ۲۰۱۳ گروه کارشناسان دولتی سازمان ملل متحد مبنی بر آنکه «حقوق بین‌الملل، به ویژه منشور سازمان ملل متحد قابل اجرا بوده و برای حفظ صلح و ثبات ضروری است» استفاده نشده است. گزارش گروه کارشناسان دولتی در سال ۲۰۱۳، به صراحت تسرّی و قابلیت اجرایی قوانین بین‌المللی را در فضای سایبری تأیید می‌کند. هرچند بکارگیری اصطلاحاتی نظیر «هنجارهای جهانی» و «اصول قانون» از سوی بریکس را می‌توان به نوعی تصویب و تأیید خاموش قوانین موجود تلقی کرد. با توجه به مخالفت‌های روسیه و اینکه این کشور و چین خواستار معاهده‌ای جدید بوده و مسکو و پکن در حال ترویج آیین‌نامهٔ رفتاری سازمان همکاری شانگهای هستند، این نوع ابهام در اطلاعیه‌ها و بیانیه‌های گروه بریکس طبیعی به نظر می‌رسد.

- **سازمان ناتو**

سازمان ناتو مهم‌ترین سازوکار و ابزار بین‌المللی کشورهای غربی به رهبری آمریکا، به خصوص هنگام استفاده از اهرم نظامی برای پیشبرد اهداف دیپلماتیک، است. رویکرد ناتو به ثبات سایبری عمدتاً بازدارنده است. ناتو این کار را با اشارهٔ عمومی به قوانینی انجام می‌دهد که معتقد است قوانین جاری بین‌المللی در فضای سایبری نیز قابل تسرّی و اِعمال هستند (مانند حقوق بین‌الملل) و با این امید که مانع اقدام دشمنان احتمالی شود، به تفسیر فعالیت‌های سایبری تهاجمی علیه خود نیز می‌پردازد.

---

1. The 6th BRICS Summit, 2017

در سال ۲۰۱۴، رهبران ناتو با اِعمال قوانین بین‌المللی در فضای سایبری و اینکه دفاع سایبری وظیفهٔ اصلی اتحاد فراآتلانتیکی است موافقت کردند. همچنین اعضای ناتو توافق کردند که هر گونه عملیات سایبری تهاجمی ممکن است بر اساس مادهٔ ۵ معاهدهٔ آتلانتیک شمالی، به دفاع مشروع جمعی منجر شود، و اینکه چنین تصمیمی را تنها می‌توان در شورای آتلانتیک شمالی که در رأس ناتو قرار دارد اتخاذ کرد.[1]

تا کنون عمدهٔ اقدامات و فعالیت‌های بازدارندهٔ ناتو به تهدیدات حملات سایبری یا جاسوسی سایبری از سوی کشورهای قدرتمندی همچون روسیه و چین معطوف بوده است. هرچند این اتحادیه در قبال حملات سایبری کشورهایی همچون کرهٔ شمالی و ایران نیز هشدارهایی صادر کرده است. همچنین ناتو تا کنون در هیچ یک از موارد حملات و فعالیت‌های مخرب سایبری علیه اعضای این سازمان به حملهٔ نظامی، یا آنچه خود دفاع مشروع جمعی می‌نامد، اقدام نکرده است.

- **گروه ۲۰**

این گروه متشکل از بیست[2] کشور قدرتمند جهان در زمینهٔ اقتصادی است که در مجموع ۸۵ درصد کل اقتصاد جهانی و دوسوم جمعیت جهان را در بر دارند. اعلامیه‌های رهبران گروه ۲۰ در دو نوبت به اقداماتی در زمینهٔ ثبات و امنیت سایبری پرداخته است. نخستین‌بار و پربارترین آن‌ها اجلاس آنتالیا در سال ۲۰۱۵ بود.[3] در این اجلاس کشورهای عضو توافق کردند که

---

1. Wales Summit Declaration, 2016

۲. بیست عضو عبارت‌اند از: آرژانتین، استرالیا، برزیل، کانادا، چین، فرانسه، آلمان، هندوستان، اندونزی، ایتالیا، ژاپن، مکزیک، روسیه، عربستان، آفریقای جنوبی، کرهٔ جنوبی، ترکیه، انگلستان، ایالات متحده آمریکا و اتحادیهٔ اروپا.

3. G20 Leaders' Communiqué, Antalya Summit, 2017

مسئولیت ویژه‌ای برای ارتقای ثبات در فضای سایبری بر عهده دارند و همچنین تأیید کردند که «هیچ کشوری نباید سرقت مالکیت معنوی را به واسطهٔ استفاده از فناوری اطلاعات و ارتباطات، از جمله اسرار تجاری یا سایر اطلاعات محرمانهٔ کسب‌وکار، با هدف دستیابی به مزیت‌های رقابتی در شرکت‌ها یا بخش‌های تجاری انجام دهد». این توافق تقریباً با توافق ایالات متحده و چین در سال ۲۰۱۵ یکسان است و هنجارهایی علیه جاسوسی اقتصادی در زمینهٔ منافع تجاری وضع می‌کند. رهبران این گروه همچنین اعمال قوانین بین‌المللی در فضای سایبری را با استفاده از محتوای گزارش سال ۲۰۱۳ گروه کارشناسان دولتی سازمان ملل متحد تأیید کردند. مسئلهٔ ثبات سایبری برای دومین‌بار در سال ۲۰۱۷ نیز با تعهد رهبران به تضمین یک «محیط فناوری اطلاعات و ارتباطات ایمن» و تأکید بر «اهمیت رسیدگی جمعی به موضوعات امنیتی در رابطه با استفاده از فناوری اطلاعات و ارتباطات» مورد توجه قرار گرفت.

- **گروه ۸ (۷)**

این گروه از هشت کشور صنعتی جهان تشکیل شده است که حدود ۶۵ درصد اقتصاد جهان را در دست دارند. در ابتدا روسیه، فرانسه، آلمان، بریتانیا، ایتالیا، ژاپن، ایالات متحده آمریکا و کانادا اعضای گروه هشت را تشکیل می‌دادند. با این حال پس از بحران اوکراین در ۲۰۱۴، عضویت روسیه در این گروه به حالت تعلیق درآمد و از آن پس، این گروه به گروه ۷ مشهور شد. هرچند مجدداً از زمان روی کار آمدن دونالد ترامپ در سال ۲۰۱۶ در آمریکا، زمزمهٔ بازگشت روسیه به این گروه شنیده می‌شود.

گروه هفت تا کنون به دو طریق به ثبات سایبری و مسائل مرتبط با آن

کمک کرده است: نخست، از طریق زیرگروه رم ـ لیون[1] که در حوزهٔ جرایم فناورانهٔ پیشرفته به منظور تسهیل همکاری‌های بین‌المللی در زمینهٔ مبارزه با جرایم سایبری دارای یک شبکهٔ تماس ۲۴ساعتهٔ اجرای قانون است. از این شبکه در درجهٔ اول برای درخواست کمک از یک حوزهٔ قضایی برای دسترسی و حفظ اطلاعات قابل استناد بهره‌برداری می‌شود.[2]

دوم، رهبران یا وزرای خارجهٔ این گروه در اطلاعیه‌های سالیانهٔ خود با صحه گذاشتن بر برخی هنجارها و اقدامات اعتمادسازی و تلاش برای ظرفیت‌سازی، به پایداری و ضرورت ارتقای تاب‌آوری در عرصهٔ سایبری پرداخته‌اند. در سال ۲۰۱۱، رهبران این گروه در خصوص بهره‌برداری احتمالی از اینترنت برای «اهداف متناقض با صلح و امنیت بین‌المللی» ابراز نگرانی کردند.[3] در سال ۲۰۱۳، وزرای امور خارجهٔ این گروه تأیید کردند که قوانین بین‌المللی علاوه بر دنیای فیزیکی (آفلاین)، «متناسب» دنیای دیجیتال و برخط نیز هستند. استفاده از کلمهٔ متناسب برای حقوق بین‌الملل (به جای قابل اعمال)، در پی سازش و توافق بین روسیه و سایر اعضای گروه ۸ صورت گرفت و این بیانیه پیش از گزارش سال ۲۰۱۳ گروه کارشناسان دولتی منتشر شد.[4]

هنگامی که روسیه در سال ۲۰۱۴ از گروه ۸ اخراج شد، بیانیه‌های موضوعات سایبری این گروه بیشتر بازتاب‌دهندهٔ منافع کشورهای غربی به خصوص آمریکا بود. بیانیهٔ وزرای خارجهٔ این گروه در سال ۲۰۱۵، مفاد گزارش سال ۲۰۱۳ گروه کارشناسان دولتی سازمان ملل را در خصوص کاربردپذیری قانون و اهمیت

1. Roma-Lyon Sub Group
2. Thomas D., "G7 24/7 Cybercrime Network, 2017
3. Deauville G8 Declaration, 2011
4. G8 Foreign Ministers Meeting Chair's Statement, 2012

توانمندسازی شامل می‌شد و کنوانسیون بوداپست را نیز تأیید می‌کرد؛ اقدامی که تصویب آن با حضور روسیه در این گروه غیرممکن بود.[1]

در اطلاعیهٔ سال ۲۰۱۶ رهبران این گروه، مراحل ارتقای امنیت و ثبات سایبری نیز پیوست شده بود. این پیوست به صراحت بر این تفکر صحه گذاشت که فعالیت‌های سایبری ممکن است به «اعمال قدرت یا حملهٔ مسلحانه در چارچوب منشور سازمان ملل» منجر شود و دولت‌ها می‌توانند از «حق ذاتی دفاع مشروع از خود» در پاسخ به حملات مسلحانه از طریق فضای سایبری استفاده کنند.[2]

در سال ۲۰۱۷، وزرای خارجهٔ گروه ۷ بیانیه‌ای در خصوص رفتار مسئولانه در فضای سایبری صادر کردند. این بیانیه علاوه بر محتوای متن گروه ۷ در سال‌های ۲۰۱۵ و ۲۰۱۶، شامل هنجارها، اقدامات اعتمادسازی و توصیه‌های ظرفیت‌سازیِ برگرفته از گزارش‌های سال‌های ۲۰۱۳ و ۲۰۱۵ گروه کارشناسان دولتی سازمان ملل نیز بود. برخلاف اسناد قبلی، این نخستین بیانیه‌ای بود که اعمال قانون مسئولیت دولتی در فضای سایبری و استفاده از اقدامات متقابل را تأیید و تأکید می‌کند که یک کشور می‌تواند در چارچوب قوانین بین‌المللی «آزادانه در خصوص انتساب جرم تصمیم‌گیری کند».[3]

- **سازمان کشورهای آمریکایی**

سازمان کشورهای آمریکایی[4] سازمانی منطقه‌ای است که در سال ۱۹۴۸ پایه‌ریزی شد و ۳۵ عضو دارد و مقرّ آن ایالات متحده آمریکاست. هدف از

1. G7 Foreign Ministers' Meeting Communiqué, 2015
2. G7 Principals and Actions on Cyber, 2016
3. G7 Declaration on Responsible States Behavior in Cyberspace, 2017
4. Organization of American States (OAS)

تشکیل این گروه اساساً ایجاد چتر حمایتی و بسط نفوذ و تسلط آمریکا بر کشورهای آمریکای لاتین بوده است.

نقش اصلی سازمان کشورهای آمریکایی در ایجاد ثبات و امنیت سایبری، تلاش برای ظرفیت‌سازی در این حوزه بوده است. این سازمان از طریق کمیتهٔ آمریکایی مبارزه با تروریسم[1] آموزش‌ها و کمک‌های لازم را برای تدوین راهبردهای امنیت سایبری ملی و ایجاد قابلیت‌های واکنش سریع در برابر حوادث، به کشورهای آمریکای لاتین ارائه داده است.

در آپریل سال ۲۰۱۷، کمیتهٔ آمریکایی مبارزه با تروریسم قطعنامه‌ای را تصویب کرد که طی آن یک کارگروه برای انجام اقدامات اعتمادسازی در منطقه ایجاد شد. متن این قطعنامه به صراحت سه گزارش گروه کارشناسان دولتی سازمان ملل و تأیید اقدامات اعتمادساز آن‌ها را انگیزهٔ تشکیل این کارگروه قلمداد می‌کند.

- **تجزیه و تحلیل نقش سازمان‌های بین‌المللی در حوزهٔ سایبری**

سازمان‌های جهانی و منطقه‌ای بیش از آنکه مأمنی برای اشتراک نظر رویکردهای مختلف به حوزهٔ سایبری باشد، عملاً صحنهٔ رویارویی و تقابل دو جبههٔ اصلی غربی (آمریکا) و شرقی (روسیه و چین) بوده‌اند. در خصوص موارد اصلی اختلاف بین کشورها در ارتباط با فضای سایبری می‌توان به مسئلهٔ «هنجارها» یا «قوانین» مرتبط با فضای سایبری اشاره کرد. در واقع اینکه آیا قوانین و هنجارهای فعلی بین‌المللی قابلیت تسرّی و اعمال در فضای سایبری را دارند (دیدگاه کشورهای غربی) یا باید به فکر تدوین قوانین و هنجارهای جدید بر اساس یک عهدنامهٔ بین‌المللی به صورت مشارکتی بود (دیدگاه روسیه و چین)، وجه افتراق اصلی دو جبههٔ غربی و شرقی محسوب می‌شود.

---

1. Inter-American Committee Against Terrorism (CICTE)

در حال حاضر میان هنجارهای ترویج‌یافته در سازمان‌های تحت رهبری روسیه یا چین و هنجارهای سازمان‌هایی که ایالات متحده و هم‌پیمانانش وضع کردند، هم‌پوشانی بسیار کمی وجود دارد. تنها محلی که هر دو گروه را گرد هم جمع می‌آورد و تا حدودی توانسته مواضع آن‌ها را به هم نزدیک کند، گروه کارشناسان دولتی سازمان ملل متحد است و هنجارهای توافق‌شده در این گروه پذیرفته‌ترین هنجارها بوده و احتمال موفقیت آن‌ها نیز نسبتاً بالاست؛ هرچند این گروه نیز در یکی از آخرین نشست‌های خود (سال ۲۰۱۷) نتوانست به اجماع قابل قبولی که مورد تأیید هر دو طرف باشد، دست یابد. فقدان گزارش اجماع سال ۲۰۱۷ و عدم قطعیت دربارهٔ اینکه کدام بخش از سیستم سازمان ملل در صورت عدم وجود دستورالعمل جدید گروه کارشناسان دولتی به بحث و گفت‌وگو دربارهٔ هنجارهای سایبری خواهد پرداخت، پیش‌بینی تدوین هنجارهای جدید را در آیندهٔ نزدیک دشوار می‌سازد.

با توجه به اینکه گروه کارشناسان دولتی، سازمان امنیت و همکاری اروپا، مجمع منطقه‌ای اتحادیهٔ آسه‌آن، سازمان همکاری شانگهای و بریکس موارد زیر را برای ثبات سایبری حائز اهمیت خوانده‌اند، اقدامات اعتمادسازی امیدوارکننده‌ترین حوزهٔ سازش بین دو جبهه اصلی غربی ـ شرقی را ارائه می‌دهند:

ـــ تداوم مذاکرات دوجانبه یا منطقه‌ای؛
ـــ تبادل مقالات سفید، راهبردها و بهترین الگوها؛
ـــ شبکه‌های ارتباطی و خطوط تماس فوریتی؛
ـــ همکاری مجری قانون.

مهم‌ترین اقدامات و تعاملات دوجانبه و چندجانبه

فراتر از نهادها و سازمان‌های بین‌المللی، اهمیت حوزهٔ سایبری باعث شده که

کشورها و بازیگران مهم بین‌المللی به سوی مذاکرات دوجانبه یا چندجانبه با هدف اطمینان و نیز هم‌افزایی ظرفیت‌ها و توانمندی در حوزهٔ سایبری گام بردارند.

تعدادی از کشورها مسائل سایبری را در قالب یکی از موضوعات عدیده در مذاکرات امنیتی متداول یا به صورت مسئله‌ای مجزا و مستقل، در گفت‌وگوهای رسمی بین دولتی گنجانده‌اند. علاوه بر این، اندیشکده‌های زیادی را برای ترغیب گفت‌وگو بین رقبای احتمالی در خصوص مسائل سایبری، با استفاده از کانال‌های غیررسمی مسیر ۱/۵ مذاکرات یا مسیر ۲ مذاکرات،[1] راه‌اندازی کرده‌اند. این گفت‌وگوها شامل مسیر ۱/۵ بریتانیا ـ چین، مسیر ۲ ایالات متحده ـ چین، مسیر ۲ ایالات متحده ـ روسیه، مسیر ۱/۵ ایالات متحده ـ هندوستان، مسیر ۲ اتحادیهٔ اروپا ـ چین، و مجمع گارمیش[2] به رهبری روسیه است.[3]

اگرچه در حال حاضر فهرست بلندی از مذاکرات دوجانبه بین کشورها در ارتباط با دیپلماسی سایبری در جریان است، در ذیل فقط به آن دسته از مذاکرات پرداخته می‌شود که نتایج مشخصی به دنبال داشته‌اند و در نتیجهٔ آن‌ها، کشورها با انجام فعالیت‌های بخصوصی موافقت کرده‌اند؛ از جمله پیروی از یک هنجار یا انجام اقدامات اعتمادساز مشخص در حوزهٔ سایبری.

---

۱. مسیر مذاکرات ۱/۵ و ۲، نوعی دیپلماسی از کانال‌های فرعی تلقی می‌شوند. در مسیر مذاکرات ۱/۵ عمدتاً نمایندگان دولتی به صورت غیررسمی با نمایندگان و کارشناسان غیردولتی بر سر میز مذاکره می‌نشینند. در مسیر مذاکرات ۲، نمایندگان غیررسمی طرفین مذاکرات، بدون مشارکت نمایندگان دولتی مذاکره می‌کنند. هیچ یک از مذاکرات مسیر ۱/۵ و ۲ همانند دیپلماسی سنتی رسمیت ندارد، زیرا اساساً ماهیت این جلسات دولت با دولت نیست. این نوع مذاکرات عمدتاً با هدف جلب اعتماد افراد و تسهیل انجام گفت‌وگوهایی که گاهی مقامات رسمی نمی‌توانند یا نمی‌خواهند انجام دهند صورت می‌گیرد.

2. Garmisch Forum

3. Sino- U.K. Tact 1.5 Dialogue on Cyber Security, 2017

- **مذاکرهٔ ایالات متحده ـ روسیه**

در سال ۲۰۱۳، باراک اوباما و ولادیمیر پوتین، رؤسای جمهور دو کشور، با ایجاد یک کارگروه تحقیقاتی[1] در خصوص موضوعات سایبری و همچنین سه اقدام اعتمادساز موافقت کردند: ۱. به‌اشتراک‌گذاری اطلاعات فنی دربارهٔ بدافزار یا سایر شاخص‌های مخرب بین گروه‌های پاسخگویی به فوریت‌های رایانه‌ای؛ ۲. استفاده از مراکز کاهش خطر هسته‌ای[2] برای درخواست‌های رسمی در خصوص «فوریت‌های امنیت سایبری ملی»؛ ۳. استفاده از خط تماس فوریتی کاخ سفید ـ کرملین برای مدیریت بحران‌های سایبری احتمالی.[3]

فعالیت کارگروه کار تحقیقاتی در سال ۲۰۱۴ متوقف شد، اما روسیه و ایالات متحده خطوط ارتباطی را همواره باز نگاه داشته‌اند و برخی به دنبال از سرگیری مذاکرات سایبری رسمی بوده‌اند.[4] بهره‌برداری از سازوکار درخواست رسمی از طریق مراکز کاهش خطر هسته‌ای طی انتخابات سال ۲۰۱۶ ایالات متحده، با هشدار کاخ سفید به روسیه در خصوص امتناع از عملیات نفوذ اینترنتی گسترده‌تر، صورت گرفته است.[5]

همان طور که قبلاً نیز اشاره شد، مذاکرات روسیه و ایالات متحده آمریکا اگرچه همواره با فراز و نشیب‌های زیادی مواجه بوده، اما در سال‌های اخیر تنش‌های این دو کشور در حوزه‌های وسیعی، از مسئلهٔ اوکراین گرفته تا مداخله در انتخابات ریاست‌جمهوری آمریکا، مسائل موشکی، خروج احتمالی از پیمان کاهش سلاح‌های هسته‌ای و ...، گسترش یافته و آیندهٔ مذاکرات دوجانبه را در هاله‌ای از ابهام قرار داده است.

---

1. Standing Working Groups (SWG)
2. Nuclear Risk Reduction Centers (NRRC)
3. Fact Sheet: U.S.-Russian Cooperation on Information and Communications Technology Security, 2017
4. Evan P., 2016
5. David I., 2016

- **مذاکرهٔ ایالات متحده ـ چین**

در سال ۲۰۱۵، رئیس‌جمهور اوباما و رئیس‌جمهور شی جین‌پینگ[1] به توافق رسیدند که «هیچ کدام از کشورها سرقت مالکیت معنوی سایبری را، از جمله اسرار تجاری یا سایر اطلاعات محرمانهٔ کسب‌وکار، با هدف ارائهٔ مزیت‌های رقابتی به شرکت‌ها یا بخش‌های تجاری انجام ندهند یا به صورت آگاهانه از آن حمایت نکنند».[2] آن‌ها همچنین با برگزاری دو حوزه برای مذاکرات آتی موافقت کردند: ۱. گروهی متخصص برای بحث و بررسی در زمینهٔ هنجارهای سایبری، ۲. گروه دیگر هماهنگی وزرای مربوط است که به منظور «بررسی زمان‌بندی و کیفیت پاسخ به درخواست‌های اطلاعات یا امدادرسانی در خصوص فعالیت‌های مخرب سایبری» به صورت دوسالانه با یکدیگر دیدار می‌کنند. در بخشی از مذاکرهٔ گروه دوم، با برقراری یک خط فوریتی در صورت بالا رفتن میزان درخواست‌ها موافقت شد. این خط فوریتی در سال ۲۰۱۶ راه‌اندازی گردید.[3]

به دنبال این توافق، گزارش‌های شرکت‌های امنیت سایبریِ بخش خصوصی حاکی از آن هستند که سطح فعالیت سایبری چین در برابر اهداف بخش خصوصی ایالات متحده کاهش یافته است. تا به حال هیچ گونه اطلاعات عمومی در خصوص بهره‌برداری از این خط فوریتی در دسترس نیست.[4]

اگرچه تا چند سال پیش مذاکرات آمریکا ـ چین، در مقایسه با مذاکرات آمریکا ـ روسیه از تنش کمتری برخوردار بود، اما این تنش‌ها در یک سال

---

1. Xi Jinping
2. Fact Sheet: President Xi Jinping's State Visit to the United States, 2017
3. Third U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues, 2017
4. Adam S., 2016

اخیر به دلیل تشدید اختلافات دو کشور در زمینهٔ فعالیت‌های شرکت چینی هوآوی در حوزهٔ اینترنت نسل پنجم (5G)، فناوری هوش مصنوعی شرکت چینی زدتی‌ای و فعالیت شبکه‌های اجتماعی تیک‌تاک و وی‌چت به شدت افزایش یافته است. علاوه بر این، موضوع جاسوسی سایبری و سرقت اطلاعات و اسرار تجاری، که همواره آمریکا علیه چین مطرح می‌کند، بیش از گذشته دورنمای این مذاکرات را ابهام‌آلود ساخته است.

نکتهٔ حائز اهمیت دیگر در مذاکرات ایالات متحده ـ چین، وجود مسائل و چالش‌های فراملّی در روابط دو کشور است به طوری که آمریکا همواره چین را به تضعیف و تخریب زیرساخت‌های اطلاعاتی و ارتباطی کشورهای هم‌پیمان آمریکا و نیز تلاش برای وابسته ساختن کشورهای درحال‌توسعه از طریق سرمایه‌گذاری در حوزه‌های فناوری این کشورها متهم می‌کند.

- **مذاکرات روسیه با چین، هندوستان و آفریقای جنوبی**

روسیه به منظور تلطیف وجههٔ بین‌المللی‌اش و تثبیت خود به عنوان یک بازیگر مهم جهانی بسیار کوشیده تا با کشورهای آمریکا، انگلستان، فرانسه و کانادا مذاکره کند. با این حال، با وجود بن‌بست نسبی در مذاکرات روسیه ـ آمریکا، تقریباً هیچ یک از مذاکرات دوجانبهٔ این کشور با سایر کشورهای غربی موفقیت‌آمیز نبوده است. در عوض، تلاش‌های روسیه برای مذاکرات دوجانبه با کشورهای همسو یا مستقل در زمینهٔ مسائل حوزهٔ سایبری از موفقیت بیشتری برخوردار بوده است.

در سال ۲۰۱۵، روسیه و چین با الهام از کنوانسیون امنیت اطلاعات پیشنهادی روسیه و توافق‌نامهٔ امنیت اطلاعات سازمان همکاری شانگهای، توافق‌نامهٔ دوجانبه‌ای[1] امضا کردند. این توافق آن‌ها را به گفت‌وگوهای منظم دوجانبه، ایجاد

1. Agreement Between the Government of the Russian Federation and the Government of the People's Republic of China, 2017.

یک نقطهٔ تماس برای تسهیل روند تبادل اطلاعات و همچنین همکاری در ایجاد و انتشار هنجارهای سایبری ملزم می‌کند. بر اساس مادهٔ ۴ این توافق‌نامه، هیچ یک از دو کشور اجازه ندارد عملیات سایبری علیه یکدیگر انجام دهد، به طوری که برخی آن را به عنوان پیمان عدم تجاوز[1] نام‌گذاری می‌کنند[2].

به غیر از بیانیهٔ مشترکی که یک سال بعد صادر شد و در آن نقطهٔ تماس هر یک از طرفین را تعیین کرد و تلاش‌هایی برای همکاری در زمینهٔ فیلتر کردن اطلاعات به صورت آنلاین مطرح گردید، تا کنون اطلاعات محدودی در خصوص اجرای این توافق‌نامه در دسترس عموم قرار گرفته است.

علاوه بر چین، روسیه همچنین قرارداد مشابهی را با هندوستان در سال ۲۰۱۶ و با آفریقای جنوبی در سال ۲۰۱۷ امضا کرد. متن هیچ یک از این دو قرارداد علنی نشده است[3].

- **چارچوب همکاری‌های ایالات متحده آمریکا ـ هندوستان**

در سال ۲۰۱۶، ایالات متحده و هندوستان برای هدایت روابط دوجانبه‌شان بر سر یک چارچوب توافق کردند. بر اساس این چارچوب، هر دو کشور توافق کردند که در طیف وسیعی از اقدامات، از فعالیت‌های اجرای قانون علیه جرایم سایبری گرفته تا تبادل بهترین الگوهای امنیت فضای سایبری و همچنین ترویج هنجارهای سایبری توصیه‌شدهٔ گروه کارشناسان دولتی سازمان ملل متحد و گروه ۲۰، با یکدیگر همکاری نمایند. دهلی‌نو و واشینگتن نیز به صراحت توافق کرده‌اند که به «درک مشترکی از ثبات سایبری بین‌المللی و فعالیت‌های بی‌ثبات‌کننده» دست یابند. این چارچوب به مدت پنج سال اعتبار خواهد داشت.

ایالات متحده و هندوستان علاوه بر حفظ مذاکرات دوجانبهٔ فعلی خود

---

1. Non-Aggression Pact
2. Elaine K., 2016
3 Arun M. Sukumar, 2016

دربارهٔ همکاری در حوزه‌های فضای سایبری و فناوری اطلاعات و ارتباطات، توافق کردند در زمینهٔ تسهیل اجرای این امر، برای هر یک از حوزه‌های همکاریِ مشخص‌شده در چارچوب یک نقطهٔ تماس مشخص کنند.

- **مذاکرات دوجانبه و سه‌جانبهٔ ژاپن**

ژاپن به دلیل موقعیت ژئواستراتژیک خود و نیز وابستگی توسعهٔ اقتصادی و فناوری آن به ثبات بازارهای منطقه‌ای و بین‌المللی از جمله معدود کشورهایی است که در تدوین دیپلماسی سایبری خود هم با آمریکا (جبههٔ غرب) و هم با چین و روسیه (جبههٔ شرق) دغدغه‌های مشترک زیادی دارد. همین مسئله باعث شده تا ژاپن تعاملات دوجانبه و چندجانبه با طیف گسترده‌ای از کشورها در زمینهٔ اصول و مؤلفه‌های دیپلماسی سایبری خود همچون اصل اینترنت آزاد، امن و باز (با آمریکا و کشورهای غربی) و اطمینان از امنیت و حاکمیت ملی خود (با کشورهای روسیه و چین) داشته باشد.

با توجه به محورهای فوق‌الذکر، ژاپن در حال حاضر گفت‌وگوهای دوجانبه‌ای را در زمینهٔ فضای سایبری، با یازده کشور جهان، از جمله آمریکا، روسیه، فرانسه، آلمان، انگلستان، استرالیا، هندوستان، کرهٔ جنوبی، استونی، اوکراین و اسرائیل دنبال می‌کند. ضمن آنکه به طور هم‌زمان گفت‌وگوهایی با اتحادیهٔ اروپا و اتحادیهٔ آسه‌آن و نیز گفت‌وگوهایی سه‌جانبه با محوریت «ژاپن ـ چین و کرهٔ جنوبی» و نیز «ژاپن ـ آمریکا و کرهٔ جنوبی» در پیش گرفته است.

- **تجزیه و تحلیل مذاکرات دوجانبه در حوزهٔ سایبری**

مذاکرات دوجانبه و رسیدن به توافقات دوسویه در حوزهٔ سایبری در سال‌های اخیر به خصوص با هدف تقویت همکاری‌های دوجانبه، اعم از سیاسی و تجاری و اقتصادی، از یک سو و نیز یارگیری در منازعات سطح بالاتر به خصوص در

سطح سازمان ملل از سوی دیگر، با استقبال بیشتری روبه‌رو شده است.

با توجه به اینکه بسیاری از موضوعات فعال در روابط بین‌الملل و سیاست خارجی کشورها به عرصهٔ سایبری نیز کشیده شده است، پیش‌بینی می‌شود کشورهای بیشتری با هدف فائق آمدن بر چالش‌های پیش رو به برگزاری مذاکرات دوجانبه اقدام کنند و در این بین باید منتظر ظهور بازیگران جدیدی، همچون کرهٔ جنوبی، ژاپن، آفریقای جنوبی و ... نیز بود. اهمیت مسائل سایبری و تأثیر آن بر روابط بین کشورها به حدی است که حتی در حوزه‌های جغرافیایی همچون آفریقا و خاورمیانه و آسیای میانه نیز کشورها را به انجام اقدامات و تحرکات دیپلماتیک در این حوزه واداشته است.

فعالیت‌های بخش خصوصی: حکمرانی فراتر از دولت‌ها

در چشم‌انداز دنیای سایبری، آیندهٔ «سرزمین» به عنوان مهم‌ترین نماد حکومت‌ها در علم سیاست کلاسیک تیره و تار است. «سرحدّ» به مثابهٔ واحد تعیین سرزمین تماماً رنگ باخته و حیات دولت‌ها به آستانهٔ بحران به معنا و مفهوم یونانی[۱] آن رسیده است. در ادامهٔ نظرورزی‌های «بحران مشروعیت» هابرماس، «زوال هویت‌های سیاسی» کاستلز و «برخورد تمدن‌ها»ی ساموئل هانتینگتون، نوعی حس بی‌ثباتی به طور فراگیری تمامی واحدهای سرزمینی (کشورها) را فرا گرفته و الگوهای جدیدی از حکمرانی در حال جایگزین شدن هستند؛ هرچند چشم‌انداز آن همچنان مبهم است.

چندوجهی بودن، از جمله در زمینهٔ صاحبان منافع و ذی‌نفعان، یکی از ویژگی‌های منحصربه‌فرد حوزهٔ سایبری است که این امر به طور خاص بر تعدد

---

۱. Crisis در معنا و مفهوم یونانی به مرحله‌ای اشاره دارد که سوژه در آستانهٔ نابودی کامل است.

بازیگران این عرصه دلالت دارد. نخستین‌بار در تاریخ تمدن بشری است کـه در آن بازیگران غیردولتی حضوری گسترده، مستقل[1] و فعالی در عرصهٔ سیاست خـارجی و روابط بین‌الملل دارند و گاهی قدرت بـازیگری آن‌هـا از بسـیاری از کشـورها و حتی از مجموعِ بی‌شماری از کشورها نیز بیشتر و اثرگذارتر است. آنچه در ادبیـات دیپلماسی سایبری «حکمرانی فراتر از دولت‌ها» نامیده می‌شود، دقیقاً به نقـش‌هـایی اشـاره دارد کـه شـرکت‌هـا و کمپـانی‌هـای بخـش خصوصـی، بـه خصـوص امپراتوری‌های آی‌تی، در حکمرانی سایبری در عرصهٔ بین‌المللی ایفا می‌کنند.

بازیگران غیردولتی، از جمله سازمان‌های تحقیقـاتی، کمپـانی‌هـای آی‌تـی و شرکت‌های خصوصی نیز پابه‌پای بازیگران دولتی و بر اسـاس منـافع خـود بـه دنبال شکل‌گیری مباحثِ پایداری، تاب‌آوری، ثبات و امنیت در حـوزهٔ سـایبری بوده‌اند. پیشنهادهای آن‌ها شامل باز کردن فضا بـرای ایفـای نقـش گسـترده‌تـر، ترویج هنجارهای نوین برای رفتار دولت‌ها و ایجاد سـازمان‌هـای جدیـد بـرای کمک به چالش عمـومی در حـوزهٔ سـایبری اسـت. در ایـن بخـش، برخـی از مهم‌ترین این بازیگران و نیز پیشنهادهای آنان را مرور و بررسی می‌کنیم:

- **گوگل و شبکه‌های اجتماعی وابسته به آن**

در سال ۲۰۱۷، کشور دانمارک یکی از پرسابقه‌ترین دیپلمات‌های خـود بـه نام کاسپر کلینژ[2] را به عنوان سـفیر خـود در کمپـانی گوگـل منصـوب کـرد. انتصاب کاسپر کلینژ به عنوان اولین سفیر یک کشور در یک کمپـانی آی‌تـی

---

۱. به صورت تاریخی، کمپانی هند شرقی نقش مـؤثری در کنتـرل کشـورهای تحـت استعمار انگلیس داشته است. در دوران معاصر، کمپانی‌های بزرگ نفتـی نیـز بـه طـور مشابهی سیاست خارجی و بین‌المللی خاص خود را داشته‌اند. امـا در هـیچ برهـه‌ای از تاریخ، آن‌ها نقشی مستقل از دولت متبوع خود نداشته و همواره از سیاسـت دولـت‌هـا پیروی می‌کرده‌اند.

2. Casper Klynge

در درهٔ «سلیکون وَلی» در نوع خود بی‌سابقه بود و خبر از تحولی شگرف در ماهیت و آیندهٔ سیاست بین‌الملل می‌داد. به گفتهٔ مقامات دانمارک، این کشور فرایند انتصاب سفرای دیجیتال[1] در سایر غول‌های آی‌تی همچون اپل، آمازون و مایکروسافت را ادامه خواهد داد.

گوگل به عنوان بزرگ‌ترین پلتفرم[2] جهانی با شبکه‌هایی که بر بستر آن فعال است (شامل یوتیوب، فیس‌بوک، توییتر و ...) نقش زیادی در سیاست بین‌الملل ایفا می‌کند. علاوه بر این، شبکه‌های متعلق به آن از طریق ادغام عمودی، افقی و مُورب، انحصارطلبی منحصربه‌فردی در سه حوزهٔ اطلاع‌رسانی، خدمات و سرگرمی در پیش گرفته‌اند که دامنه و گسترهٔ اثرگذاری سیاسی، فرهنگی و اجتماعی جهانی آن‌ها را بیش از پیش افزایش می‌دهد.

مارک الیوت زاکربرگ،[3] مدیرعامل فیس‌بوک، از زمان انتخابات ۲۰۱۶ آمریکا تقریباً هر روز طرف مذاکرات سیاسی با مقامات عالی‌رتبهٔ دولت آمریکاست و همه‌روزه اخباری از نشست‌های علنی و محرمانهٔ وی در کمیته‌ها و کمیسیون‌های مختلف کنگرهٔ فدرال و پارلمان‌های ایالتی آمریکا به گوش می‌رسد. آخرین اقدام دسته‌جمعی این شبکه‌ها، یعنی استفاده از هوش مصنوعی برای تولید و نظارت بر محتوا در پلتفرم‌های مربوطه، نه‌تنها لرزه بر تن قانون اساسی ایالات متحده انداخته، بلکه به گفتهٔ رئیس‌جمهوری فرانسه، حاکمیت‌های ملی را نیز تا آستانه فروپاشی پیش برده است.[4]

---

1. Digital Ambassador

۲. گوگل، اپل، فیس‌بوک، آمازون و مایکروسافت پنج پلتفرم مشهور به گافام هستند که دامنهٔ اثرگذاری فعالیت‌های آن‌ها جهانی است. با توجه به اهمیت نقش آن‌ها در سیاست بین‌الملل، فصل نهم این کتاب به طور کامل به «گافام و دیپلماسی شرکتی» آن‌ها پرداخته است.

3. Mark Elliot Zuckerberg

۴. مصاحبهٔ مکرون با هفته‌نامهٔ *اکونومیست*، ۷ نوامبر ۲۰۱۹.

- **مایکروسافت و تلاش برای ایجاد یک سازمان انتساب**

بنا به استدلال برخی دانشگاهیان و شرکت مایکروسافت، یک سازمان انتساب مستقل می‌تواند با در اختیار داشتن گروهی متخصص از مناطق مختلف جغرافیایی برای بررسی شواهد، در دسترس قرار دادن شواهد به منظور بازنگری و بررسی دقیق و انتشار یافته‌های تحقیقاتی خود، به بهبود ثبات سایبری کمک کند.

شرکت مایکروسافت یکی از مطالعات اندیشکدهٔ رَند[1] را تحت حمایت مالی خود قرار داد تا به بررسی شرایط لازم یک سازمان انتساب برای تضمین انتساب‌های معتبر و مبتنی بر شواهد بپردازد. از دیدگاه این مطالعه، این سازمان باید:

ــ شامل ترکیبی از کارشناسان فنی و سیاست سایبری از نقاط مختلف جغرافیایی باشد؛ در مجموع بین بیست تا چهل نفر که از دانشگاه‌ها و شرکت‌های فناوری و سازمان‌های تحقیقاتی انتخاب شده‌اند؛

ــ نمایندگان دولتی را به کار نگیرد یا به اطلاعات ارائه‌شدهٔ دولت‌ها اعتماد نکند؛

ــ فعالیت‌های خود را با شفافیت انجام دهد و یافته‌های خود را منتشر سازد.[2]

این مطالعه تشکیل یک کنسرسیوم جهانی انتساب سایبری[3] بر اساس این ویژگی‌ها را پیشنهاد می‌کند. کشورها یا طرف‌های قربانی، که به دنبال تعیین تکلیف هستند، برای بهره‌جویی از تخصص لازم به این کنسرسیوم مراجعه می‌کنند. این کنسرسیوم شواهد را جمع‌آوری و آن‌ها را با توجه به چارچوب حوادث و روش‌های قابل‌دسترس برای عموم ارزیابی می‌کند و از طریق اکثریت آرا انتساب را انجام می‌دهد و این یافته‌ها را همراه مدارک و شواهد لازم به اطلاع مردم می‌رساند. پس از انتساب، این امر به عهدهٔ

---

1. RAND Corporation Study
2. John S. Davis II et al., 2017
3. Global Cyber Attribution Consortium

کشور یا طرف قربانی است که علت اقدامِ وی را بـرای پاسـخگویی کشـورِ خاطی تعیین کند. کنسرسیوم هیچ فشاری در این زمینه اعمال نخواهد کرد.

- **هنجارهای شرکت مایکروسافت و کنوانسیون دیجیتال ژنو**

مایکروسافت مسلّماً برجسته‌ترین شرکت فناوری اطلاعـات و ارتباطـات فعـال در بحث ثبات سایبری است که محصولاتش هم ابـزاری بـرای انجـام عملیـات سایبری تهاجمی تحت حمایـت دولـت اسـت و هـم هـدف ایـن تهاجمـات. هنجارهای پیشنهادی مایکروسافت به طور ضمنی به این مطلب اشـاره دارد کـه با توجه به تداوم انجام عملیات سایبری کشورها علیـه یکـدیگر، ایـن هنجارهـا برای محافظت از شرکت و مشتریان آن و صنعت فناوری اطلاعات و ارتباطـات در برابر گسترش ابزارهای تهاجمی ضرورت دارند. این شـرکت مجموعـه‌ای از هنجارها را به کشورهای مختلفی پیشنهاد کرده است که یـک هنجـار مـرتبط بـا صنعت جهانی فناوری اطلاعات و ارتباطات دارند. کشورها باید:

ــ شرکت‌های جهانی فنـاوری اطلاعـات و ارتباطـات را بـرای آسـیب رساندن به محصولاتشان هدف قرار ندهند (و شرکت‌های فناوری اطلاعات و ارتباطات نبایـد بـه کشـورها اجـازه دهنـد کـه تـأثیری منفـی بـر امنیـت محصولات مربوط بگذارند)؛

ــ خط‌مشی صریح و روشنی در زمینهٔ رسیدگی به آسـیب‌پـذیری‌هـایی داشته باشند که به جای ذخیره کردن یـا معاملـهٔ آن‌هـا، از افشـای مسـئولانه حمایت کند (و شرکت‌های فناوری اطلاعـات و ارتباطـات مـی‌بایـد بـرای کنترل آسیب‌پذیری‌ها از روش‌های افشای هماهنگ[1] استفاده کنند)؛

ــ در توسعهٔ سلاح‌های سایبری محدودیت اعمال کننـد و از محـدودیت و دقت و عدم قابلیت استفادهٔ مجدد هر کـدام اطمینـان حـاصل نماینـد (و

1. Coordinated Disclosure

شرکت‌های فناوری اطلاعات و ارتباطات باید با دفاع از خود در برابر چنین حملاتی، تأثیر آن‌ها را خنثی سازند)؛

ــ سلاح‌های سایبری را گسترش ندهند (و شرکت‌های فناوری اطلاعات و ارتباطات نباید برای اهداف تهاجمی دست به خریدوفروش آسیب‌های نرم‌افزاری بزنند)؛

ــ در شناسایی، مهار کردن، پاسخ دادن و رفع آثار ناشی از حوادث فضای سایبری به بخش خصوصی کمک کنند (و شرکت‌های فناوری اطلاعات و ارتباطات نیز باید دولت‌ها را در انجام چنین کاری یاری رسانند).[1]

از میان این هنجارها می‌توان گفت تنها یک مورد، یعنی پیشنهاد ارائهٔ خط‌مشی‌های روشن به کشورها به منظور افشای آسیب‌پذیری، به فرایندهای رسمی دیپلماتیک نفوذ کرده است و آن عبارت است از تشویق گروه کارشناسان دولتی سازمان ملل، سازمان امنیت و همکاری اروپا و گروه ۷ جهت انجام اقدامات اعتمادسازی برای تشویق افشای مسئولانهٔ آسیب‌پذیری‌های رایانه‌ای.

مایکروسافت در سال ۲۰۱۷، بحث کنوانسیون دیجیتال ژنو را برای مدون کردن هنجارهای پیشنهادی‌اش در قانون بین‌المللی مطرح کرد. برخلاف کنوانسیون‌های ژنو، که قوانینی را برای فعالیت کشورها طی درگیری‌های مسلحانه وضع می‌کنند، بنا به استدلال مایکروسافت، کنوانسیون دیجیتال ژنو فعالیت کشورها را در فضای سایبری و در طول زمان صلح، کنترل و قانون‌گذاری کرده و یک سازمان انتساب مستقل ایجاد خواهد نمود.[2]

---

1. From Articulation to Implementation: Enabling Progress on Cyber Security Norms, 2017

2. Brad S., 2017

- **راهنمای تالین**

راهنمای تالین[1] یک سند غیرالزام‌آور است که در سال ۲۰۱۲ گروهی متشکل از بیست متخصص مستقل حقوق بین‌الملل، به پیشنهاد مرکز عالی دفاع سایبری جمعی ناتو، به عنوان راهنمایی در زمینهٔ قوانین نافذ در جنگ سایبری تدوین کردند.

راهنمای تالین در واقع تلاشی برای تشریح نحوهٔ اعمال قوانین بین‌المللی موجود در فضای سایبری است. راهنماهای سال‌های ۲۰۱۳ و ۲۰۱۷ قوانین بخصوصی را مطرح می‌کنند که به عقیدهٔ مؤلفان آن، کشورها و بازیگران غیردولتی برای پیروی از قوانین بین‌المللی، موظف به رعایت آن‌ها در فضای سایبری هستند. مؤلفان این راهنما امیدوارند که تفسیر عمومی این قانون با شفاف‌سازی قوانین اساسی‌ای که دولت‌ها باید بر اساس آن‌ها به فعالیت بپردازند ثبات سایبری را بهبود بخشد.

روسیه و چین نگاه خوش‌بینانه‌ای به فرایند تالین ندارند. سفیر امور سایبری روسیه نخستین نسخه راهنمای تالین را به عنوان توجیهی برای «منافع خصمانهٔ غرب» مورد انتقاد قرار داد[2]. گزارش‌ها حاکی از آن هستند که این نگرانی‌ها به چین نیز منتقل شده است[3]. یک کارشناس چینی، که در تهیهٔ پیش‌نویس راهنمای سال ۲۰۱۷ مشارکت داشت، نیز آن را به همین دلایل و با بیان اینکه «مطابق با منافع و ارزش‌های غربی است» مورد انتقاد قرار داد[4]. فرایند تالین همچنین منافع چین و روسیه را نادیده می‌گیرد، به خصوص اینکه با ارائهٔ راهنمایی‌های دقیق دربارهٔ نحوهٔ تفسیر قوانین فعلی فضای سایبری از سوی کشورها، ضرورت وضع قانون جدید را تضعیف می‌کند.

---

1. Tallinn Manual
2. Tim S., 2017
3. Ashley D., 2015
4. Experts, Have You Heard of the Tallinn Manual?, 2017

- **موقوفهٔ کارنگی و هنجار پیشنهادی در برابر تضعیف سیستم مالی جهانی**

موقوفهٔ کارنگی برای صلح بین‌المللی[1] یک مؤسسهٔ غیرانتفاعی خصوصی امریکایی است که اندرو کارنگی، سرمایه‌دار آمریکایی، در سال ۱۹۱۰ برای «گسترش همکاری بین‌المللی» و با هدف نفوذ فعال امریکا در حوزه‌های مختلف بین‌المللی تأسیس کرد.

موقوفهٔ کارنگی برای صلح بین‌المللی در سال‌های اخیر مجموعهٔ هنجارهایی را علیه دست‌کاری در یکپارچگی داده‌های مالی پیشنهاد داده است. با این فرض که هیچ کشوری علاقه‌ای به تضعیف اعتماد به سیستم مالی جهانی ندارد، موقوفهٔ کارنگی برای صلح بین‌المللی معتقد است که کشورها نباید در هر گونه فعالیتی که عمداً در یکپارچگی داده‌ها یا الگوریتم‌های مؤسسات مالی، چه به صورت ذخیره‌شده و چه هنگام انتقال آن‌ها، دست ببرند یا آگاهانه از چنین فعالیتی پشتیبانی کنند».[2]

این هنجار که در ماه مارس سال ۲۰۱۷ مطرح شد، هنوز در اسناد نتیجهٔ مذاکرات گنجانده نشده یا مورد تأیید رسمی کشورها قرار نگرفته است.

جمع‌بندی و نتیجه‌گیری مباحث این فصل

بر اساس یک برآیند کلی، عمدهٔ تلاش‌های دیپلماتیک در زمینهٔ فضای سایبری را، که هم از سوی کشورهای قدرتمند، هم از سوی سازمان‌های بزرگ بین‌المللی و هم از سوی ذی‌نفعان و بازیگران بخش خصوصی دنبال شده، به طور کلی می‌توان در چهار دسته تقسیم کرد: ۱. تعیین هنجارها یا قوانین برای مدیریت فضای سایبری؛ ۲. اقدامات اعتمادساز در زمینهٔ

1. Carnegie Endowment for International Peace (CEIP)
2. Tim M., 2017

سایبری؛ ۳. ظرفیت‌سازی و توسعه در این حوزه و ۴. به رسمیت شناختن نقش بازیگران غیردولتی همچون کمپانی‌های بزرگ آی‌تی.

به رغم تلاش‌های چشمگیر در زمینهٔ موضوع قوانین و هنجارها برای مدیریت فضای سایبری، هنوز شکافی بزرگ بین ایالات متحده و متحدانش از یک سو، و روسیه و چین و متحدان آن‌ها از سوی دیگر به چشم می‌خورد. چشم‌انداز ایجاد روابط حسنه بین این دو جبهه به دو دلیل، مبهم به نظر می‌رسد: نخست، گروه کارشناسان دولتی محل اصلی بحث و بررسی هنجارها بوده‌اند که به دلیل عدم موفقیت آن در صدور گزارش اجماع سال ۲۰۱۷، وضعیت تمدید دستورالعمل آن مشخص نیست. دوم اینکه، همواره بین دیدگاه روسیه یا چین و ایالات متحده نسبت به تهدیدهای سایبری تفاوت‌های اساسی وجود دارد (برای نمونه، ابزار سایبری در مقابل سلاح‌های اطلاعاتی) که همین امر سبب دشوار شدن فرایند تدوین، وضع و اجرای هنجارهای مشترک در ارتباط با فضای سایبری می‌شود.

با این حال، اقدامات اعتمادسازی می‌تواند مسیر امیدوارکننده‌تری در رابطه با ایجاد ثبات سایبری پیش روی کشورها قرار دهد. در اقدامات اعتمادسازی موافقت کشورها با یک سِری اصول مشترک ضرورت ندارد، بلکه به رغم این اختلافات اصولی، به دلیل آنکه کشورها متوجه نفع مشترک خود در ارتقای ثبات خواهند شد، سبب تقویت همکاری نیز می‌شوند.

در زمینهٔ اقدامات اعتمادسازی، به ویژه در خصوص نقاط تماس و خطوط فوریتی، فعالیت‌های قابل توجهی به صورت دوجانبه و در مواردی در ساختارهای چندجانبه صورت گرفته است. با این حال و با وجود آنکه کشورها در برخی حوزه‌ها، خواه راهبردهای سایبری مشخص و خواه ساختارهای چندجانبه، به صراحت دربارهٔ برخی از خط‌مشی‌های سایبری

ابراز نگرانی کرده‌اند، اما دربارهٔ رسیدگی به آن مسئله هیچ گونـه فعـالیتی در ارتباط با پایدارسازی پیشنهاد نداده‌اند. در این زمینه، تلاش‌های گسترده‌تـری در حوزه‌های زیر می‌توان انجام داد:

ــ امنیت زنجیرهٔ تأمین: در گزارش‌های پی‌درپی گـروه کارشناسـان دولتـی، توافق‌نامهٔ امنیت اطلاعات سازمان همکاری شانگهای، آیین‌نامـهٔ رفتـار و قـوانین ملی در انگلستان، روسیه، چین و دیگر کشـورها بـه چـالش کـاهش تهدیـدات مربوط به زدوبندهای مخفیانهٔ سخت‌افزاری یا نرم‌افزاری اشاره شده اسـت. ایـن چالش یکی از نگرانی‌های اصلی بخش خصوصی است کـه محصـولات آن‌هـا غالباً هدف این گونه فعالیت‌ها قرار می‌گیرند. بـا ایـن حـال، هـیچ گونـه اقـدام اعتمادسازی بخصوصی برای رفع این نگرانی مشترک توسعه نیافته است.

ــ ترویج خط‌مشـی‌هـای افشـای آسـیب‌پـذیری: طبـق گـزارش گـروه کارشناسان دولتی در سال ۲۰۱۵، سازمان امنیت و همکاری اروپـا و بخـش خصوصی بر ایدهٔ توسعهٔ خـط‌مشـی‌هـای افشـای آسـیب‌پـذیری از سـوی کشورها مهر تأیید نهـاده‌انـد. آژانـس‌هـای امنیتـی دولتـی بـا افشـای نحـوهٔ شناسایی آسیب‌پذیری رایانه‌ای و اطـلاع‌رسـانی در زمینـه آن مـی‌تواننـد از طریـق آگـاه‌سـازی دیگـران نسـبت بـه نقـاط ضـعف رایانـه‌ای بـرای بهره‌برداری‌های آتی، ثبات فضای سایبری را بهبود بخشـند. ایـالات متحـده تنها کشوری است که تا کنون هیچ گونه اطلاعاتی راجع به فرایند زمینه‌های آسیب‌پذیری رایانه‌ای خود منتشر نکرده است.[1]

در آخر باید به نقش بازیگران غیردولتی در عرصهٔ فضای سایبری اشـاره کرد که زمینه‌های اثرگذاری آن‌ها به مدد فنـاوری‌هـای نـوین روزبـه‌روز در حال افزایش است. اگر تا چنـد سـال پـیش بخـش خصوصـی و ذی‌نفعـان

1. Alex G., 2014

غیردولتی خواستار به رسمیت شناخته شدن حداقل جایگاهی برای خود در عرصهٔ سایبری از سوی بازیگران دولتی و رسمی بودند، با ظهور کمپانی‌های بزرگ آی‌تی، پلتفرم‌های جهانی و ... چشم‌انداز مباحث سایبری بین‌المللی به سرعت دستخوش تغییرات آنی و غیرقابل پیش‌بینی شده است. امروزه هوش مصنوعی، اینترنت اشیا و بلاک‌چین به پلتفرم‌ها (به عنوان یکی از بازیگران غیردولتی) قدرت مضاعفی برای به چالش کشیدن بیشتر بازیگران دولتی و رسمی از مباحث و مسائل مربوط به فضای سایبری داده، تا حدی که دورنمای بیرون راندن آن‌ها از عرصهٔ «سیاست‌گذاری و مقررات‌گذاری» توسط این پلتفرم‌ها چندان دور از ذهن نیز نیست.

منابع

Agreement Between the Government of the Russian Federation and the Government of the People's Republic of China on Cooperation in the Field of International Information Security. (2017). The Ministry of Foreign Affairs of the Russian Federation, Accessed 8 November 2017; http://static.government.ru.

Agreement Between the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security. NATO Cooperative Cyber Defense Centre of Excellence.

Alex Grigsby, "Will China and Russia's Updated Code of Conduct Get More Traction in a Post-Snowden Era?" Net Politics (blog), the Council on Foreign Relations, January 28, 2015, https://www.cfr.org.

Andrei Soldatov and Irina Borogan, "Putin Brings China's Great Firewall to Russia in Cybersecurity Pact," the Guardian, November 29, 2016, https://www.theguardian.com.

Arun Mohan Sukumar. (2016). India and Russia Sign Cyber Agreement, Pushing the Frontier for Strategic Cooperation, Digital Frontiers (blog), Observer Research Foundation, 15 October 2016; http://www.orfonline.org.

ASEAN. (2017). Regional Forum Work Plan on Security and the Use of Information and Communication Technologies (ICTs)", ASEAN Regional Forum, Accessed 25 October 25 2017, http://www.asean2017.ph.

Basic Principles for State Policy of the Russian Federation in the Field of International Information Security to 2020 , NATO Cooperative Cyber Defense Centre of Excellence, Accessed 30 October 2017; https://ccdcoe.org.

Budapest Conference on Cybersecurity 2012," Budapest Conference on Cybersecurity, Accessed November 1, 2017; https://web.archive.org.

Coera, Gordon. How France's TV5 Was Almost Destroyed by 'Russian Hackers, BBC News, 10 October 2016; http:// www.bbc.com.

Cyber-Attacks: EU Ready to Respond with a Range of Measures, Including Sanctions", the Council of the European Union, Accessed 27 October 2017; http://www.consilium. europa.eu.

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, The European Commission, Accessed 20 October 2017; http://eeas.europa.eu.

Davis, John S., et al. Stateless Attribution: Towards International Accountability in Cyberspace", the RAND Cooperation, Accessed 1 November 2017; https: //www.rand.org.

Deauville G8 Declaration: Renewed Commitment for Freedom and Democracy, European Union Archives, 26 May 2011; http://ec.europa.eu.

Deeks, Ashley, Tallinn 2.0 and a Chinese View on the Tallinn

Process", Lawfare (blog), 31 May 2015; https://www. lawfareblog.com.

Decision No. 1202 OSCE Confidence Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies, Organization for Security and Co-operation in Europe, Accessed 25 October 2017; http://www.osce.org.

Dougherty, Thomas, "G7 24/7 Cybercrime Network", the Council of Europe, Accessed 31 October 2017; https://rm. coe.int.

Experts, Have you Heard of the Tallinn Manual (in Mandarin). Internet Dissemination Magazine, 22 February 2017; http:// china.huanqiu.com.

Fact Sheet: President Xi Jinping's State Visit to the United States", Statements and Releases, the White House of President Barack Obama, Accessed 1 November 2017; https:// obamawhitehouse.archives.gov.

Fact Sheet: U.S. Russian Cooperation on Information and Communications Technology Security", Statements and Releases, the White House of President Barrack Obama, Accessed 31 October 2017;https://obamawhitehouse.archives.gov.

First US-India Track 1.5 Cyber Dialogue Held in Washington DC, Observer Research Foundation, Last Modified June 8, 2016, https:// ssol.columbia.edu.

From Articulation to Implementation: Enabling Progress on

Cybersecurity Norms. Microsoft, Accessed 1 November 2017; https://mscorpmedia.azureedge.net.

5th Global Conference on Cyberspace, GCCS 2017, Accessed November 1, 2017; https://gccs2017.in.

Global Conference on Cyberspace 2015," GCCS 2015, Accessed November 1, 2017; https://www.gccs2015.com.

Global Cyber Security Centre", the University of Oxford, Accessed 1 November 2017; http://www.oxfordmartin.ox.ac.uk.

Grigsby, Alex, Disclosing Policies on Zero-Days as a Confidence-Building Measure", Net Politics (blog), the Council on Foreign Relations, 18 November 2014; https://www.cfr.org.

G7 Declaration on Responsible States Behavior in Cyberspace, G7 Information Centre, University of Toronto, 11 April 2017; http://www.g8.utoronto.ca.

G7 Foreign Ministers' Meeting Communiqué", G7 Information Centre, University of Toronto, 15 April 2015; http://www.g8. utoronto.ca/foreign/formin150415.html; "Convention on Cybercrime," Council of Europe, November 23, 2001, https://www.coe.int.

G7 Principals and Actions on Cyber," G7 Information Centre, University of Toronto, 27 May 2016; http://www.g8.utoronto.ca.

G8 Foreign Ministers Meeting Chair's Statement", G7 Information Centre, University of Toronto, 12 April 2012; http:// www.g8.utoronto.ca.

G20 Leaders' Communiqué, Antalya Summit", the G20, Accessed 31 October 2017; http://www.mofa.go.jp.

G20 Leaders Communiqué", Group of Twenty, Accessed 22 October 2017; http://www.mofa.go.jp.

Ignatius, David, In our New Cold War, Deterrence Should Come Before Détente", The Washington Post, 15 November 2016; https://www.washingtonpost.com.

Korzak, Elaine, The Next Level for Russia-China Cyberspace Cooperation?", Net Politics (blog), the Council on Foreign Relations, 20 August 2016; https://www.cfr.org.

London Conference on Cyberspace: Chair's Statement", Government of the United Kingdom, Accessed 1 November 2017; https://www.gov.uk.

Maurer, Tim, Ariel Levite, and George Perkovich. Towards a Global Norm Against Manipulating the Integrity of Financial Data", the Carnegie Endowment for International Peace, Accessed 1 November 2017; http://carnegieendowment.org.

Moscow in Talks with U.S. to Create Cyber Working Group: RIA Report, Reuters, July 20, 2017; https://www.reuters.com.

Mukesh Dhirubhai Ambani. (2019). Full Text of the Speech". Retrieved on 18 of February 2010; https://www. cnbctv18. Com.

Ninth International Forum State, Civil Society and Business Partnership on International Information Security," Information Security Institute, Last Accessed October 27, 2017; http://www. iisi.msu.ru.

OAS to Establish a Working Group on Cooperation and Confidence Building Neasures in Cyberspace", Organization of American States, 10 April 2017; http://us11.campaign-archive2.com.

OSCE Polis Home", OSCE Polis, Last Accessed 25 October 2017; https://polis.osce.org/home.

Perez, Evan, "First on CNN: U.S. and Russia Meet on Cybersecurity", CNN, 17 April 2016; http://www.cnn.com.

Press Release on Signing a Cooperation Agreement Between the Government of the Russian Federation and the Government of the Republic of South Africa on Maintaining International Information Security", the Ministry of Foreign Affairs of the Russian Federation, Accessed 1 November 2017; http:// www.mid.ru.

Putin, Vladimir, "Remarks at the Truth and Justice Regional and Local Media Forum", 7 April 2016; http://en.kremlin.ru.

Sarah McKune. An Analysis of the International Code for Conduct for Information Security," the Citizen Lab, September 28, 2015, https://citizenlab.ca.

SCO Hosts First Joint Online Counter-Terrorism Exercise in China", the Ministry of National Defense, the People's Republic of China, Accessed 30 October 2017;http://eng.mod.gov.cn.

Segal, Adam, "The U.S.-China Cyber Espionage Deal One Year Later," Net Politics (blog), the Council on Foreign Relations; https: //www.cfr.org.

Seoul Framework for and Commitment to Open and Secure Cyberspace," the Soul Conference on Cyberspace, Accessed November 1, 2017; http://www.mofat.go.kr.

Shaohui, Tian, International Strategy of Cooperation on Cyberspace," Xinhaunet, 3 Janruary 2017; http://news. xinhuanet.com.

Sino-European Cyber Dialogue, the Hague Center for Strategic Studies, Last Modified December 8, 2016; https://hcss.nl.

Sino- U.K. Tact 1.5 Dialogue on Cyber Security", Press Releases, Institute for Strategic Studies, Last Accessed 31 October 2017; https://www.iiss.org.

Smith, Brad, "The Need for a Digital Geneva Convention", Microsoft on the Issues (Blog), 14 February 2017; https:// blogs.microsoft.com.

Stevens, Tim, "Cyberweapons: an Emerging Global Governance Architecture", Palgrave Communications 3, 10 January 2017; https://www.nature.com.

Sustainable Development Knowledge Platform", the United Nations, Last Accessed 22 October 2017; https:// sustainable development .un.org/sdgs.

Taylor, Adam, Putin Saw the Panama Papers as a Personal Attack and May Have Wanted Revenge, Russian Authors Say", Washington Post, 28 August 2017; https://www. washingtonpost.com.

The UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/65/201 (July 30, 2010), Accessed 30 October 2017;http:// www.unidir.org.

The UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98 (June 24, 2013, Accessed 30 October 2017); http://www.un.org.

The UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174 (July 22, 2015), Accessed 27 October 2017; http:// www.un.org.

The UN General Assembly, 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, (A/69/723) 13 January 2015; Accessed 30 October 2017; https://ccdcoe.org.

The UN General Assembly, 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, A/66/359 (September 14, 2011), Accessed 30 October 2017; http://www.un.org.

The UN General Assembly, Resolution 57/239, Creation of a Global Culture of Cybersecurity, A/RES/47/239 (January 31, 2013), Accessed 22 October 2017, https://www.oecd.org.

The 6th BRICS Summit: Fortaleza Declaration," BRICS Information Centre, the University of Toronto, Accessed 31 October 2017; http://www.brics.utoronto.ca.

Third U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues", The United States Department of Justice, Accessed 1 November 2017, https://www.justice.gov.

Track 1.5 U.S.- China Cyber Security Dialogue," Center for Strategic and International Studies, Accessed October 27, 2017; https:// www.csis.org.

Twenty Sentences to Understand Sino-Russian Joint Declaration—the Past and Future of Sino-Russian Relations are All Here" (in Mandarin), Xinhuanet, June 27, 2017, http:// news. xinhuanet.com.

UN General Assembly, Resolution 70/237, Developments in the Field of Information and Telecommunications in the Context of International Security, S/RES/70, Accessed 24 October 2017, https://unoda-web.s3-accelerate.amazonaws.com.

UN General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/69/68 (June 24, 2013), Accessed October 30; https:// ccdcoe.org.

Wales Summit Declaration, Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales", the North Atlantic Treaty Organization, Accessed 26 October 2016; https://www.nato.int.

World Internet Conference", Wuzhen Summit, Accessed 28 October 2017, http://www.wuzhenwic.org.

فصل سوم

گذار ژاپن به دیپلماسی سایبری

درآمد

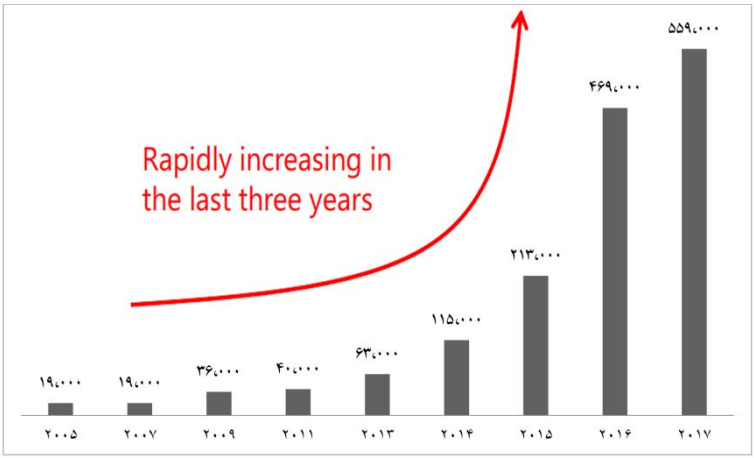
بر اساس آمار مؤسسهٔ ملی فناوری اطلاعات و ارتباطات ژاپن، این کشور، به خصوص از اوایل ۲۰۱۱، با حملات سایبری متعددی (نه‌تنها در نهادها و سازمان‌های دولتی، بلکه حتی در مؤسسات خصوصی آن) روبه‌رو بوده که در سه سال اخیر (۲۰۱۷ ــ ۲۰۱۹) به طور شگفت‌انگیزی اوج گرفته است. بر اساس آمار این مرکز ملی، میزان حملات سایبری در ژاپن از ۱۹ هزار حمله در سال ۲۰۰۵ آغاز شده و به ۵۵۹ هزار حملهٔ سایبری در سال ۲۰۱۷ رسیده است. طبق این گزارش، تنها در یک حملهٔ سایبری به مرکز خدمات مالی کوین‌چک[۱] در توکیو در سال ۲۰۱۸، این مرکز ۵۸ میلیارد ین[۲] از دست داد که در تاریخ کشور ژاپن بی‌سابقه بوده است.[۳]

---

۱. Coincheck، یکی از معروف‌ترین و بزرگ‌ترین شرکت‌های ژاپنی فعال در زمینهٔ خرید و فروش ارز دیجیتال.

۲. JPY، واحد پول ژاپن

3. Cyber Security Annual Report, 2018



نمودار شمارهٔ ۱. میزان حملات سایبری ژاپن در سال‌های اخیر. به نقل از مؤسسهٔ ملی فناوری اطلاعات و ارتباطات ژاپن

با توجه به پیش‌زمینهٔ گفته‌شده، بدیهی است که رویکرد ژاپن به فضای سایبری، همانند عمدهٔ کشورهای جهان، در ابتدا رویکردی دفاعی با هدف مقابله با تهدیدات فضای سایبری، به ویژه در ارتباط با حملات سایبری و جرایم سایبری و نیز جاسوسی سایبری بوده است. در مراحل بعدی، دولت ژاپن با توجه به درهم‌تنیدگی اقتصاد ژاپن با بازارهای جهانی از یک سو، و نیز پیشرفت و توسعهٔ فناوری ژاپنی در توسعهٔ فضای سایبری و مؤلفه‌های مرتبط با آن در سه حوزهٔ شبکه و نرم‌افزار و سخت‌افزار از سوی دیگر، رویکردهای فعالانه‌تری در ارتباط با فضای سایبری اتخاذ کرد. این نوشته با هدف آشنایی با رویکرد دولت ژاپن به مقولهٔ فضای سایبری در دو بخش تنظیم شده است: ۱. چارچوب امنیت سایبری دولت ژاپن با تأکید بر

رویکرد دفاعی که عمدتاً معطوف به سند امنیت سایبری این کشور (منتشرشده در سال ۲۰۱۵) است؛ ۲. گذار به دیپلماسی سایبری با تأکید بر ایفاگری نقش منطقه‌ای و بین‌المللی در حوزهٔ فضای سایبری که معطوف به بازنگری اساسی دولت ژاپن در سند امنیت سایبری (منتشرشده در سال ۲۰۱۸) است.

چارچوب امنیت سایبری دولت ژاپن

دیپلماسی سایبری ژاپن به طور اساسی ریشه در استراتژی امنیت سایبری آن دارد که برای نخستین‌بار در قالب سند امنیت سایبری ژاپن در سال ۲۰۱۴ مطرح شد و در سال ۲۰۱۵ به تصویب دولت این کشور رسید. دولت ژاپن در این سند، تحت تأثیر فرصت‌ها و تهدیدهای ناشی از ظهور عصر سایبری، قوانین پایهٔ امنیت سایبری را تدوین کرد و در آن علاوه بر تعریف نقش دولت و دولت‌های محلی و دیگر ذی‌نفعان در امنیت سایبری، مجموعهٔ قدرتمندی با عنوان مراکز استراتژیک امنیت سایبری[1] با هدف کنترل امنیت سایبری ملی طراحی کرد که می‌تواند با قدرت و اختیارات زیاد، دستورالعمل‌ها و توصیه‌ها و راهکارهایی برای نهادها و سازمان‌های ملی این کشور ارائه دهد.

در ادبیات سیاسی دولت ژاپن، فضای سایبری فضایی است که در آن مالکیت فکری، همچون ابداع فناوری و الگوهای جدید کسب‌وکار، به طور پیوسته ایجاد می‌شود و به عنوان یک پلتفرم مدرن همچنان به نقش فزایندهٔ خود در توسعهٔ پایدار اقتصاد جامعه ادامه خواهد داد. در این نگاه، چند مفهوم کلیدی وجود دارد که شناسایی آن به فهم سازوکار سند امنیت سایبری کشور ژاپن کمک زیادی می‌کند:

---

1. Cyber Security Strategic Headquarters

۱. فضای سایبری همچنان به گسترش لیبرالیسم و دموکراسی و توسعهٔ فرهنگی ادامه می‌دهد و تا آیندهٔ دور، بستری برای توسعهٔ فعالیت‌های مرتبط با نوآوری و فناوری در فعالیت‌های مردم جامعه می‌شود. به عبارت دیگر، فضای سایبری بستری برای تولید ارزش نامحدود[1] خواهد شد.

۲. فراتر از آن، در نگاه دولت ژاپن فضای سایبری عامل گذار جوامع به جامعهٔ نوع ۵ خواهد بود که در آن ارزش‌های نوین و خدمات جدید به طور مداوم ایجاد می‌شود و رفاه بیشتری برای افراد جامعه به ارمغان خواهد آورد.

۳. دنیای واقعی[2] و فضای سایبری به عنوان یک موجودیت مستقل[3] از یکدیگر وجود خارجی ندارند. به عبارت دیگر، ما با دو دنیای متفاوت روبه‌رو نیستیم، بلکه با یک دنیای یکپارچه[4] و به‌هم‌پیوسته مواجهیم که تفکیک آن‌ها از یکدیگر امکان‌پذیر نیست. بنابراین باید این دو را به عنوان یک وجود ارگانیک[5] در نظر گرفت که پیوسته در حال تغییر و تحول و تکامل است[6].

با این نگاه دولت ژاپن به مقوله فضای سایبری، جامعهٔ قرن ۲۱ با ترکیبی از فرصت‌ها و تهدیدهای ناشی از ظهور عصر سایبری مواجه است که شناخت و تمایز آن‌ها در هر گونه سیاست‌گذاری و برنامه‌ریزی استراتژیک برای حکمرانی در عصر فضای سایبری حائز اهمیت است. به عبارت دیگر، در هر گونه سیاست‌گذاری و برنامه‌ریزی در ارتباط با فضای سایبری باید توازن بین فرصت‌ها و تهدیدهای آن را لحاظ کرد (جدول شمارهٔ ۱).

---

1. Frontier for Generating Infinite Value
2. Real Space
3. Independent Entity
4. Integrated
5. Organic Entity
6. Cyber Security Strategy, 2018

جدول شمارهٔ ۱. تهدیدها و فرصت‌های برجسته‌شده در سند امنیت سایبری ژاپن (۲۰۱۸)

ردیف	فرصت‌ها یا مزایای فضای سایبری	تهدیدهای فضای سایبری
۱	پیشرفت در خدمات قابل ارائه در فضای سایبری و پذیرش وسیع آن از سوی مردم	تأثیرات عمیق بر جامعه به دلیل رکود کسب‌وکار، کاهش مشاغل و خدمات ارائه‌شده
۲	انقلاب بنیادین در هوش مصنوعی	کاهش رقابت‌پذیری به دلیل از دست دادن یا افشای اطلاعات
۳	توسعهٔ اینترنت اشیا	افزایش خسارت‌های ناشی از سرقت یا کلاهبرداری

اصول پنج‌گانهٔ امنیت سایبری ژاپن

دولت ژاپن در مسیر تدوین و اتخاذ سیاست امنیت سایبری خود، پنج اصل مهم و کلیدی را مبنا قرار داده که عمدتاً برگرفته از نظریات سرمایه‌داری و لیبرالیسم غربی است که دولت این کشور خود را موظف به اطمینان از رعایت آن‌ها می‌داند:

۱. تضمین جریان آزاد اطلاعات:[1] پیشرفت فضای سایبری به عنوان قطب و مرکز نوآوری‌های جدید منوط به تضمین جریان آزاد اطلاعات در آن است. ژاپن معتقد است که ایجاد یک محیط سایبری، که در آن انتقال اطلاعات نه سانسور خواهد شد و نه بدون هیچ دلیلی تغییر خواهد یافت، بلکه به صورت کامل به مخاطبان هدف ارسال خواهد شد، ضروری و

1. Assurance of the Free Flow of Information

الزامی است. لذا در هر گونه مقررات‌گذاری مرتبط با فضای سایبری، جریان آزاد اطلاعات باید محترم شمرده شود و به موضوع حریم خصوصی افراد نیز توجهی جدی معطوف گردد. در این خصوص، باید به ایجاد توازن بین مقررات‌گذاری لازم و دفاع از حریم خصوصی توجه مضاعفی صورت گیرد. به عنوان شرط اساسی برای جریان آزاد اطلاعات، اخلاقیات و عقل سلیم حکم می‌کند که به حقوق و منافع دیگران تجاوز نشود.

۲. حاکمیت قانون: در جامعهٔ به‌هم‌پیوسته و ادغام‌شدهٔ اطلاعاتی، قانون باید به همان نحوی که در دنیای واقعی اعمال می‌شود، در فضای سایبری نیز اعمال گردد. حاکمیت قانون تضمینی است برای فضای سایبری که بتواند به عنوان یک بستر امن و پایدار، همراه با قابلیت دسترسی یکسان برای همگان توسعه یابد.

در کشور ژاپن، فضای سایبری مشمول قانون و نیز دیگر اصول و ارزش‌ها می‌شود. همچنین از نظر کشور ژاپن، قوانین بین‌الملل و نیز دیگر قواعد و ارزش‌ها و دستورالعمل‌های بین‌المللی قابلیت تسرّی به فضای سایبری را دارند. لذا در عرصهٔ بین‌المللی نیز فضای سایبری باید از طریق حاکمیت قانون مدیریت شود. از سوی دیگر، بازیگران متنوعی با استفاده از فضای سایبری در اقصی نقاط جهان به گسترهٔ آن یاری رسانده‌اند. همچنین ضروری است دستورالعمل‌ها و قوانین بین‌المللی جدیدی مطابق با ارزش‌های جهانی، همچون آزادی و دموکراسی، برای توسعهٔ صلح و ثبات جامعهٔ بین‌الملل تدوین شوند. در این خصوص، ژاپن فعالانه برای تدوین و اجرای چنین قوانینی تلاش می‌کند و برای معرفی این دستورالعمل‌ها و قواعد بین‌المللی به سایر کشورها بر اساس شرایط و موقعیت‌های داخلی آن‌ها می‌کوشد.

۳. باز بودن[1]: ژاپن به جد معتقد است که فضای سایبری نباید به انحصار هیچ گروهی از بازیگران آن درآید؛ در واقع باید برای تمامی افرادی که می‌خواهند از آن استفاده کنند باز باشد. این فضا تنها از طریق باز بودن، می‌تواند ایده‌ها و دانش‌ها و ارزش‌های نوین را به هم مرتبط و جهانی سازد. همچنین از نظر دولت ژاپن، دسترسی اکثریت مردم نباید به سبب منافع سیاسی یک گروه خاص و کوچک منع یا قطع و یا محدود شود.

۴. خودگردانی[2]: در یک دهۀ گذشته، بازیگران مختلف از طریق حکمرانی خودگردان موجب توسعۀ قدرتمند اینترنت شده‌اند. حتی اگر فضای سایبری به یک چالش ملی تبدیل شود، که تلاش همه‌جانبۀ کشور را بطلبد، اصلاً درست و عملیاتی نیست که دولت مسئولیت برقراری و حفظ نظم در فضای سایبری را خود به عهده بگیرد.

با هدف دستیابی به توازن بین نظم و خلاقیت در فضای سایبری، ژاپن به ظرفیت‌های خودگردانی که اینترنت توسعه داده است، احترام می‌گذارد. ژاپن همچنین با توجه به فعالیت‌های متکی‌به‌خود[3]، نقش‌آفرینی هر ذی‌نفع در مدیریت اینترنت را پایه و اساس حکمرانی اینترنت می‌داند. لذا به دنبال ترویج توسعه و اجرای یک سازوکار خودگردان است که بر اساس آن تمامی نظام‌های اجتماعی متصل به فضای سایبری بتوانند به اهداف و مأموریت‌های خود دست یابند و از سوی دیگر از فعالیت بدخواهان در فضای سایبری جلوگیری کنند.

۵. همکاری بین ذی‌نفعان[4]: فضای سایبری یک فضای چندلایه و چندبُعدی متشکل از فعالیت ذی‌نفعان گوناگون در سطوح مختلف است. از این منظر، ضروری است که دولت و تمامی ذی‌نفعان مربوط، از جمله

---

1. Openness
2. Autonomy
3. Self-Reliant
4. Collaboration Among Multi-Stakeholders

اپراتورهای زیرساخت‌های کلیدی[1] شرکت‌ها، کمپانی‌ها و افراد، هدف مشترکی را طراحی و دنبال کنند. آن‌ها همچنین باید مسئولیت‌ها و وظایف سازمانی و حتی تلاش‌های فردی خود را در مسیر این هدف مشترک قرار دهند. دراین‌باره، دولت وظیفهٔ مدیریت تنظیم و تقویت روابط بین ذی‌نفعان را بر عهده دارد. دولت ژاپن در مدیریت چنین روابطی، اقدامات پویایی از طریق معرفی نظام تبادل اطلاعات تعاملی در زمان واقعی و با تمامی ذی‌نفعان، در نظر گرفتن عوامل و فاکتورهای فعالی همچون حملات سایبری در حال رشد و در حال انجام و دیگر اقدامات مشابه، انجام داده است.[2]

ژاپن مطابق با پنج اصل گفته‌شده و در زمینهٔ دفاع از امنیت، سلامت، حقوق و منافع مردم، هر گونه اقدام مؤثر و بادوام، از جمله سیاسی، اقتصادی، فناوری، حقوقی، دیپلماتیک و ...، را با هدف صیانت از این اصول به عنوان یک گزینه برای خود محفوظ می‌داند؛ برای مثال، دولت ژاپن هیچ گونه فعالیت تروریستی یا اقداماتی مرتبط با آن را، که صلح و امنیت مردم این کشور را تهدید می‌کند، تحمل نخواهد کرد.

اصول و مبانی سیاست امنیت سایبری ژاپن به طور مؤثری عیناً در سطوح منطقه‌ای و بین‌المللی نیز مصداق می‌یابد. از نظر دولت ژاپن، ایجاد یک وضعیت جهانی در ارتباط با فضای سایبری که به وضوح از طریق حاکمیت قانون اداره شود، تنها مسیر برای تثبیت بازار جهانی و الهام بخشیدن به نوآوری است. لذا در حوزهٔ دیپلماسی سایبری، تلاش این کشور علاوه بر امنیت ملی و داخلی، پیگیری صلح و ثبات در مقیاس جهانی است. بنابراین، در این چشم‌انداز بازیگران بدخواه و بدکردار سایبری هیچ جایگاهی نخواهند داشت.

---

1. Critical Information Infrastructure (Cii) Operators
2. Cyber Security Strategy, 2015

رویکردهای استراتژیک دولت ژاپن در امنیت سایبری

دولت ژاپن در مسیر اجرای اصول امنیت سایبری، که در بخش قبلی به آن پرداخته شد، رویکردهای استراتژیکی اتخاذ کرده است. این رویکردهای استراتژیک مبتنی بر سه فرض اساسی است که عبارت‌اند از:

۱. فعال بودن[1](در مقابل منفعل بودن): بر اساس این فرض، دولت ژاپن منتظر نخواهد بود تا به آن حمله کنند و دچار آسیب شود، بلکه برعکس، از طریق تحلیل تغییرات اجتماعی و خطرات سیاسی و ...، اقدامات فعالانه‌ای برای مقابله با هر گونه حمله‌ای اتخاذ خواهد کرد.

۲. بازیگری فعال[2] و نه منفعل: بر اساس این فرض، دولت ژاپن اقداماتی اتخاذ خواهد کرد تا فعالیت و ابتکارات بازیگران و ذی‌نفعان فضای سایبری را تسریع بخشد. همچنین دولت ژاپن به عنوان یک عضو مسئول، نقش فعالی در جامعهٔ بین‌الملل به منظور تأمین صلح و ثبات در فضای سایبری بر عهده خواهد داشت.

۳. تلقی فضای سایبری و فیزیکی با هم[3]، نه فضای سایبری به تنهایی: تمامی اشیا و جهان فیزیکی از طریق آی‌سی‌تی در فضای سایبری به هم متصل‌اند و دنیای واقعی در دنیای سایبری به‌هم‌پیوسته (یکپارچه یا ترکیب) شده است. باید توجه داشت که هر رویدادی در فضای سایبری ممکن است کل جامعه و کشور را تحت تأثیر قرار دهد. دولت ژاپن با دقت این تأثیر و تأثر را رصد و متناسب با آن، اقداماتی اتخاذ می‌کند[4].

با مسلّم دانستن سه فرض گفته‌شده در نظام فکری و حکمرانی دولت

---

1. Being Proactive
2. Acting As a Catalyst
3. Envisaging Cyber-Physical Space
4. Cyber Security Strategy, 2015

ژاپن در ارتباط با فضای سایبری، رویکردهای استراتژیک دولت ژاپن[1] در امنیت سایبری به شرح ذیل است:[2]

- **بهبود نشاط اجتماعی ـ اقتصادی[3] و توسعهٔ پایدار**

توسعهٔ پایدار و ایجاد نشاط اجتماعی ـ اقتصادی رویکرد نخست دولت ژاپن به مقولهٔ امنیت سایبری است. برای دستیابی به این هدف باید اطمینان حاصل شود که شرکت‌های ژاپنی از فرصت‌های جدید تجاری و کسب‌وکارهای مدرن عقب نخواهند افتاد. برای اطمینان از این موضوع، اقدامات ذیل ضروری است:

ـــ ایجاد سیستم‌های امن اینترنت اشیا (۲۰۱۵ و ۲۰۱۸)[4]: ایجاد سیستم‌های امن اینترنت اشیا خود مستلزم چهار مقولهٔ به هم مرتبط است: ۱. ایجاد مشاغل جدید و فعال بر اساس اینترنت اشیای امن؛ ۲. بهبود یا ارتقای چارچوب‌های ساختاری برای اینترنت اشیای امن؛ ۳. در نظر گرفتن رویکردهایی برای ارتقای امنیت سیستم‌های اینترنت اشیا؛ و ۴. اعمال و بکارگیری فناوری‌های توسعهٔ مرتبط با اینترنت اشیا.

ـــ ترویج مدیریت شرکت‌ها با یک ذهنیت امنیتی (۲۰۱۵): ترویج مدیریت شرکت‌ها با یک ذهنیت امنیتی نیز خود مستلزم مقولات ذیل است: ۱. تغییر شیوهٔ تفکر مدیریت اجرایی ارشد؛ ۲. تقویت نیروی انسانی مربوط به امنیت سایبری برای مدیریت پیشرفتهٔ تجارت؛ و ۳. تقویت ظرفیت‌های سازمانی.

ـــ ارتقای امنیت سایبری محیط کسب‌وکار (۲۰۱۵): در مسیر ارتقای امنیت سایبری محیط کسب‌وکار، این اقدامات لازم است: ۱. ترویج کسب‌وکارهای

---

۱. با توجه به اینکه سند اولیهٔ امنیت سایبری ژاپن در سال ۲۰۱۵ تدوین و مجدداً در سال ۲۰۱۸ بازنگری شد، برخی از این استراتژی‌ها و سازوکارهای مرتبط با آن، مربوط به سند امنیت سایبری سال ۲۰۱۵ و برخی دیگر مربوط به سند امنیت سایبری سال ۲۰۱۸ است.

2. Cyber Security Strategy, 2015, 2018

3. Socio-Economic Vitality

4. Iot Systems

مرتبط با امنیت سایبری؛ ۲. توسعهٔ محیط کسب‌وکاری عادلانه؛ و ۳. بهبود فضا برای شرکت‌های ژاپنی که در سطح جهانی عمل می‌کنند.

ــ پیشرفت در حوزهٔ سایبری به عنوان عرصهٔ پیشران تولید ارزش (۲۰۱۸): با یکپارچگی بیشتر دنیای واقعی با فضای سایبری، شرکت‌ها و کسب‌وکارهای جدید با خطرات بیشتری مواجه خواهند شد که توانایی مقابله با آن‌ها مستلزم این امور است: ۱. افزایش آگاهی‌های اجرایی و مدیریتی؛ ۲. تداوم و افزایش سرمایه‌گذاری در حوزهٔ امنیت سایبری؛ و ۳. ارتقای امنیت سایبری با تقویت نوآوری و حمایت از استفاده از فناوری‌های نوین.

ــ دستیابی به یک زنجیرهٔ تأمین که از طریق پیشران‌های به‌هم‌پیوسته، ارزش‌های جدید ایجاد می‌کند (۲۰۱۸): با شتاب گرفتن وحدت و یکپارچگی بیشتر دنیای واقعی با فضای سایبری و نیز گذار جوامع به جوامع نوع ۵، تجارت بین صنایع و شرکت‌ها، از طریق شبکه‌های خودکار، در مقیاس جهانی صورت می‌گیرد که قبل از این امکان‌پذیر نبود. این شبکه‌های خودکار که عمدتاً در بستر اینترنت جهانی شکل گرفته‌اند، عموماً در معرض مخاطرات زیادی قرار دارند که برای کاهش ریسک مرتبط با آن، چنین اقداماتی ضروری است: ۱. تدوین چارچوب امنیت سایبری برای مخاطرات زنجیرهٔ تأمین ارزش‌های جدید؛ ۲. ایجاد سازوکاری برای تأیید امنیت سایبری زنجیرهٔ تأمین ارزش‌های جدید؛ و ۳. ارتقا و ترویج ابتکارات مربوط به امنیت سایبری در سطوح شرکت‌های متوسط و بزرگ.[1]

- **ایجاد یک جامعهٔ امن و سالم برای مردم**

در سال‌های اخیر، تعداد و میزان حوادث سایبری در جهان به شدت افزایش یافته است. با هدف پاسخ به تهدیدهای سایبری و متعاقباً ایجاد جامعه‌ای که مردم بتوانند

1. Cyber Security Strategy, 2015, 2018

در آن زندگی سالم و امنی داشته باشند، دولت اقدامات ذیل را انجام می‌دهد:

ــ اقداماتی برای دفاع و امنیت مردم و جامعه (۲۰۱۵): برای دفاع از امنیت مردم و جامعه، اطمینان از انجام این اقدامات ضروری است: ۱. ایجاد محیط سایبری امن و ایمن برای کاربران؛ ۲. ترویج انجام اقدامات امنیتی سایبری توسط کاربران؛ و ۳. ارتقا و بهبود اقدامات علیه جرایم سایبری.

ــ اقداماتی برای دفاع از زیرساخت‌های اطلاعاتی مهم (۲۰۱۵): زیرساخت‌های اطلاعاتی کلیدی همواره نقش مهمی در توسعهٔ کشورها داشته است. برای اطمینان از امنیت زیرساخت‌های اطلاعاتی کلیدی، دولت ژاپن متعهد به انجام اقدامات ذیل است: ۱. بررسی مداوم حوزه‌ها و شیوه‌های دفاع از زیرساخت‌های اطلاعاتی مهم؛ ۲. اطمینان از مبادلهٔ سریع و بموقع و مؤثر اطلاعات؛ و ۳. ارائهٔ حمایت‌ها و پشتیبانی مناسب از حوزهٔ زیرساخت‌های اطلاعاتی کلیدی.[1]

ــ اقداماتی برای دفاع از سازمان‌ها و نهادهای دولتی (۲۰۱۵): با توجه به اینکه دولت و سازمان‌های دولتی نیز به عنوان بالاترین مرجع هماهنگی بین ذی‌نفعان و بازیگران فضای سایبری، با تهدیدات و چالش‌هایی مواجه‌اند، دولت ژاپن برای مقابله با این تهدیدها و چالش‌ها اقدامات ذیل را اتخاذ خواهد کرد: ۱. تقویت توانایی‌های دفاعی سیستم‌های اطلاعاتی و ترویج اقدامات چندلایه در برابر حملات سایبری احتمالی که این امر خود شامل پیشگیری از رویدادهای سایبری، جلوگیری از خسارت و گسترش خسارت و تلاش برای کاهش خسارت در این حوزه‌ها می‌شود؛ ۲. دستیابی به توانایی‌ها و ظرفیت‌های «پاسخ سازمانیِ» مطمئن‌تر و بادوام‌تر؛ ۳. سازگاری با پیشرفت فناوری و تغییر در سبک‌های کارایی کسب‌وکار؛ و ۴. بهبود اقدامات به صورت جامع از طریق گسترش حوزه‌های تحت رصد و مانیتورینگ.

---

1. The Cyber Security Policy for Critical Infrastructure Protection, 2018

ــ اطمینان از ایجاد محیط آموزشی امن و ایمن در دانشگاه‌ها و مراکز تحقیقاتی (۲۰۱۸): با توجه به مجهز بودن دانشگاه‌ها و مراکز تحقیقاتی وابسته به دانش و مهارت‌های روز، لازم است دولت از این ظرفیت برای ایجاد بستر سایبری امن استفاده کند. دراین‌باره این امور ضروری است: ۱. اتخاذ اقدامات متناسب با تنوع دانشگاه‌ها و مراکز تحقیقاتی وابسته؛ ۲. ارتقای هماهنگی و همکاری بین دانشگاه‌ها و مراکز تحقیقاتی وابسته.

ــ ایجاد یک چارچوبِ به‌اشتراک‌گذاری اطلاعات یا همکاری که فراتر از چارچوب‌های سنتی است (۲۰۱۸): به طور خودکار هر سازمان یا نهاد باید بتواند از عهدهٔ دفاع از خود در برابر حملات سایبری برآید. با وجود این، تغییر ماهیت حملات سایبری محدودیت‌های زیادی برای سازمان‌ها ایجاد کرده است. از این رو برای غلبه بر این محدودیت‌ها باید: ۱. سازوکار همکاری و تبادل اطلاعات بین ذی‌نفعان را ارتقا داد؛ ۲. به سوی یک مرحلهٔ جدیدی از همکاری و تبادل اطلاعات پیش رفت.

ــ تقویت آمادگی در برابر حملات سایبری گسترده (۲۰۱۸): پیش‌بینی وقوع حملات سایبری گسترده با توجه به یکپارچگی دنیای واقعی و فضای سایبری و پیامدهای گستردهٔ آن برای کشور ژاپن چندان دور از انتظار نیست. برای ارتقای سطح آمادگی در برابر این گونه حملات، دولت ژاپن به طور مستمر در صدر برنامه‌های خود به این امور توجه بسیاری دارد: ۱. اقدامات نظارتی و مانیتورینگ اینترنت به منظور پیش‌بینی و پیشگیری از حملات سایبری، ۲. برقراری مانورهای آمادگی هم در فضای سایبری و هم در دنیای واقعی، ۳. آموزش مهارت‌های آمادگی برای مقابله با این گونه حملات.[1]

---

1. Cyber Security Strategy, 2015, 2018

اطمینان از امنیت ملی و نیز صلح و ثبات بین‌المللی

امنیت ملی و ثبات بین‌المللی دو مقولهٔ لازم و ملزوم در نظریهٔ امنیت سایبری ژاپن است. از دیدگاه دولت ژاپن، نظام‌های اجتماعی ــ هم در سطح داخلی و هم در سطح خارجی ــ به طور روزافزونی به فضای سایبری وابسته‌اند. از این رو، تهدیدات و چالش‌های مربوط به نظام‌های اجتماعی به طور یکسان ــ هم در سطح داخلی و هم در سطح بین‌المللی ــ در حال افزایش است. بنابراین، دولت ژاپن برای اطمینان از مواجههٔ مؤثر با این چالش‌ها، اقدامات استراتژیک ذیل را مدنظر قرار داده است:

ــ اطمینان از امنیت ملی (۲۰۱۵): ضرورت اطمینان از امنیت ملی برای توسعهٔ پایدار و ایجاد نشاط اجتماعی و اقتصادی در جامعه اولویت نخست این کشور است. این امر شامل چنین مواردی می‌شود: ۱. افزایش و بهبود توانایی‌های پاسخگویی در نهادهای مرتبط با دولت؛ ۲. استفاده و حمایت از فناوری پیشرفتهٔ ژاپنی؛ و ۳. دفاع و حمایت از نظام اجتماعی و نهادهای دولتی.

ــ ایجاد صلح و ثبات در جامعهٔ بین‌الملل (۲۰۱۵): به موازات امنیت داخلی، با توجه به وابستگی شدید اقتصاد ژاپن به بازارهای جهانی، اطمینان از صلح و ثبات در جامعهٔ بین‌الملل نیز از اهمیت بالایی برخوردار است. دولت ژاپن مهم‌ترین استراتژی خود را برای اطمینان از صلح و ثبات جهانی بر اساس اقدام ذیل بنا نهاده است: ۱. ایجاد حاکمیت بین‌المللی قانون در فضای سایبری که این امر خود شامل تلاش برای توسعهٔ قوانین و هنجارهای جهانی و تحقق قواعد و هنجارهای جهانی می‌شود؛ ۲. ایجاد اقدامات اعتمادساز بین‌المللی؛ ۳. مقابله با فعالیت‌های سازمان‌های تروریستی بین‌المللی که از فضای سایبری استفاده می‌کنند؛ ۴. همکاری برای ظرفیت‌سازی در حوزهٔ امنیت سایبری؛ و ۵. توسعهٔ منابع انسانی در مقیاس و طراز جهانی.

ـــ همکاری و هماهنگی با کشورهای مختلف جهان (۲۰۱۵): بسیاری از اهداف و ایدئال‌های مطلوب برای ایجاد صلح و ثبات منطقه‌ای و بین‌المللی تنها از طریق تشریک مساعی بین کشورهای مختلف جهان امکان‌پذیر است. بر این اساس، دولت ژاپن با تقسیم‌بندی کشورهای جهان به مناطق با اولویت‌های متفاوت، سازوکارهایی برای تعامل و همکاری بیشتر با آن‌ها اتخاذ کرده است. در این تقسیم‌بندی، مناطق آسیا ـ اقیانوسیه، آمریکای شمالی، اروپا، و آمریکای لاتین، خاورمیانه و آفریقا به ترتیب، در اولویت برای همکاری و هماهنگی قرار دارند.

ـــ تعهد به یک فضای سایبری آزاد و امن و عادلانه (۲۰۱۸): با هدف ترویج ارزش‌های «آزاد»، «امن» و «عادلانه» در فضای سایبری در مقیاس جهانی، دولت ژاپن نقش فعالی در نهادها و سازمان‌ها و انجمن‌های بین‌المللی به عهده خواهد گرفت و می‌کوشد از این طریق، به ترویج و گسترش ایده‌های آزاد و عادلانه و امن در فضای سایبری و همچنین ترویج و ارتقای حاکمیت قانون در فضای سایبری بپردازد.

ـــ تقویت توانایی‌های دفاعی، بازدارندگی و آگاهی‌های موقعیتی (۲۰۱۸): حملات سایبری تهدید جدی برای دموکراسی تلقی می‌شوند و همواره این ظن واقعی نیز وجود دارد که برخی از این حملات از طریق برخی دُول حمایت می‌گردند. با هدف اطمینان از امنیت ملی و منافع ملی ژاپن باید اقداماتی در هر سه سطح دفاعی و بازدارندگی و آگاهی از هر موقعیتی، که به لحاظ سایبری در آن قرار دارد، بدین شرح صورت پذیرد:
۱. تاب‌آوری ملی (تقویت توانایی‌های دفاعی)، شامل اطمینان از ایفای مأموریت اصلی تمامی نهادها و سازمان‌ها، حمایت از فناوری پیشرفتهٔ ژاپنی و اتخاذ اقداماتی علیه استفادهٔ مخرب از فضای سایبری از سوی سازمان‌های

تروریستی؛ ۲. ارتقای ظرفیت‌ها و توانمندی‌های پیشگیری، شامل اقداماتی برای بازدارندگی مؤثر و نیز اقدامات اطمینان‌ساز؛ و ۳. تقویت آگاهی‌های موقعیتی، شامل تقویت توانمندی‌های سازمان‌های دولتی مرتبط، به اشتراک گذاشتن اطلاعات مربوط به تهدیدات سایبری و ...[1].

- **رویکردهای برش متقاطع (میان‌بُر) در امنیت سایبری**

برای تحقق سه هدف استراتژیکِ توسعهٔ پایدار و ایجاد نشاط اجتماعی و اقتصادی، ایجاد جامعهٔ امن و ایمن، و اطمینان از امنیت ملی و صلح و ثبات بین‌المللی ضروری است که دولت ژاپن با تلاش‌هایی خستگی‌ناپذیر به مجموعه اقداماتی دست بزند. دولت ژاپن برای تحقق این اهداف استراتژیک، گام‌هایی در میان‌مدت و بلندمدت، با همکاری و مشارکت بخش خصوصی و عمومی بر خواهد داشت که مهم‌ترین آن‌ها به شرح ذیل است:

ــ گسترش تحقیق و توسعه (۲۰۱۵): با توجه به انقلاب صورت‌گرفته در عرصهٔ فناوری و تحولات روزافزون آن، هر سه مقولهٔ شبکه و نرم‌افزار و سخت‌افزار نیازمند «تحقیق و توسعه» با همکاری تمامی ذی‌نفعان در این عرصه است. دراین‌باره تلاش عمدهٔ دولت در زمینهٔ تحقیق و توسعه با تمرکز بر موارد ذیل است: ۱. بهبود قابلیت‌های شناسایی و دفاع در برابر حملات سایبری؛ ۲. ترویج و تشویق تحقیقات بین‌رشته‌ای در زمینهٔ امنیت سایبری؛ ۳. اطمینان از امنیت فناوری‌های مهم و کلیدی؛ ۴. بهبود و ارتقای تحقیق و توسعه از طریق همکاری‌های بین‌المللی؛ و ۵. شراکت با نهادها و سازمان‌های مربوط.

ــ توسعه و اطمینان از نیروی ماهر برای امنیت سایبری (۲۰۱۵): دولت برای تضمین تأمین نیروی انسانی ماهر در زمینهٔ امنیت سایبری، دستورالعمل‌ها

1. Cyber Security Strategy, 2015, 2018

و راهنمایی‌های جامعی تدوین می‌کند. به خصوص اینکه نیروی کار ماهر برای فعالیت در بخش امنیت سایبری علاوه بر ظرفیت‌ها و توانمندی‌های فناوری باید به استانداردهای اخلاقی والا نیز مجهز باشد. این امر از طریق اقدامات ذیل تأمین می‌شود: ۱. توسعهٔ منابع انسانی متناسب با نیازهای اجتماعی در بخش‌های آموزش عالی و حرفه‌ای؛ ۲. توسعهٔ آموزش ابتدایی و متوسطه برای امنیت سایبری؛ ۳. کشف و پرورش و به دست آوردن بهترین استعدادها و مغزها که بتوانند در مقیاس جهانی عمل کنند؛ ۴. اشتغال‌زایی بلندمدت برای کارشناسان و متخصصان امنیت سایبری؛ و ۵. توسعهٔ منابع انسانی برای پیشرفت و توسعهٔ ظرفیت‌های سازمانی به صورت استراتژیک.

ـــ همکاری با هر کسی که بازیگر مهم در امنیت سایبری به حساب می‌آید (۲۰۱۸): با گسترش آی‌سی‌تی و استفادهٔ گسترده از فناوری‌های اینترنت پایه، به خصوص اینترنت اشیا، تقریباً هر کسی به یک عامل فعال در فضای سایبری تبدیل شده است. در چنین شرایطی لازم است هر عامل فعال یا بازیگر مهم در فضای سایبری، نقش و مسئولیت خود را در ایجاد امنیت سایبری از طریق فهم مسائل و موضوعات مرتبط با آن و نیز افزایش آگاهی‌های مرتبط با تحولات مربوط به این عرصه ایفا کند.

در حال حاضر، دبیرخانهٔ مراکز استراتژیک امنیت سایبری موسوم به ان‌آی‌اس‌سی[1] به طور مؤثری مسئولیت هدایت استراتژی‌های امنیت سایبری کشور ژاپن را بر عهده دارد. همچنین در یک همکاری و هماهنگی نزدیک با این دبیرخانه، هر یک از نهادها و سازمان‌های دولتی موظف‌اند تمامی اقدامات و ابتکارات لازم برای اطمینان از امنیت سایبری را اتخاذ کنند و به سرانجام برسانند.[2]

---

1. NISC (National Center of Incident Readiness and Strategy for Cyber Security): https://www.nisc.go.jp/eng/>.

2. Cyber Security Strategy, 2015, 2018

گذار به دیپلماسی سایبری در ژاپن

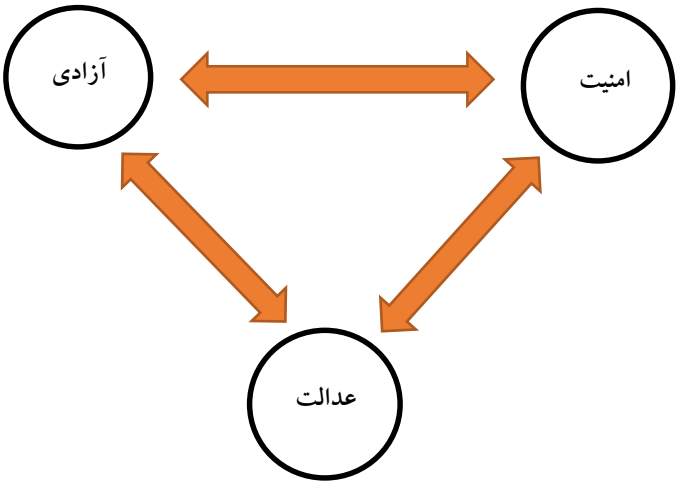
برای ژاپن به عنوان یک کشور توسعه‌یافته که از هر لحاظ، به ویژه اقتصادی و امنیتی و نظامی، به شدت به شرایط جهانی و سیاست بین‌الملل وابسته است، رویکرد صرف دفاعی در ارتباط با فضای سایبری، آن طور که در سند استراتژی سایبری سال ۲۰۱۵ تدوین شده بود، نمی‌توانست تأمین‌کنندهٔ منافع ملی و منطقه‌ای و بین‌المللی این کشور باشد. از این رو ژاپن به عنوان یک بازیگر جهانی، رویکرد فعالانه‌تری در ارتباط با فضای سایبری و استفاده از ظرفیت‌ها و پتانسیل آن برای پیشبرد اهداف منطقه‌ای و بین‌المللی خود اتخاذ کرده که به طور عمده در بازنگری دولت این کشور در سند استراتژی سایبری سال ۲۰۱۸ انعکاس یافته است. توسعهٔ اقتصادی ژاپن و فناوری‌های پیشرفتهٔ این کشور در حوزهٔ فضای سایبری (شبکه و نرم‌افزار و سخت‌افزار) نیز محرکی نیرومند برای دولت این کشور به منظور اتخاذ رویکردهای فعالانه‌تری در ارتباط با دیپلماسی سایبری بوده است.

هدف غایی دیپلماسی سایبری ژاپن

همان طور که قبلاً گفته شد، در نگاه دولت ژاپن فضای سایبری بستر ایجاد ارزش‌ها و خدمات جدید و عامل گذار این کشور به جامعهٔ نوع ۵ محسوب می‌شود. برای موفقیت‌آمیز بودن این گذار، فضای سایبری باید از طریق مشارکت همهٔ بازیگران در تولید ارزش‌های جدید، توسعه و گسترش یابد و این امر زمانی اتفاق خواهد افتاد که هر بازیگر و ذی‌نفعی از نقش و اهمیت خود آگاه باشد.

در سطح کلان، هدف غایی دیپلماسی سایبری دولت ژاپن، اطمینان از تحقق فضای سایبری آزاد و عادلانه و ایمن (نمودار شمارهٔ ۲) است. در سطح خُردتر و داخلی، دولت این کشور به دنبال اطمینان از امنیت ملی و

تأمین منافع ملی این کشور است. این امر از طریق توسعهٔ پایدار موجب ایجاد نشاط اجتماعی ـ اقتصادی و نیز ایجاد جامعه‌ای می‌شود که در آن همهٔ مردم بتوانند امن و ایمن زندگی کنند. برای اطمینان از تحقق این امر، نهادها و سازمان‌های ژاپنی باید همواره: ۱. از پایداری ارائهٔ خدمات و فعالیت‌های خود اطمینان یابند؛ ۲. نهایت همکاری و هماهنگی را بین خود داشته باشند؛ و ۳. بر اساس اصول مدیریت ریسک (تعیین و تحلیل و ارزیابی خطرات)، همواره مخاطرات تهدیدکنندهٔ فعالیت‌های خود را به حداقل برسانند.



نمودار شمارهٔ ۲. چارچوب دیپلماسی سایبری ژاپن

در سطح بین‌المللی نیز دولت ژاپن به دنبال اطمینان از ایجاد صلح و ثبات بین‌المللی در اقصی نقاط جهان است. با توجه به اهمیت فضای سایبری و نقش بی‌بدیل آن در روابط بین‌الملل، وزارت خارجهٔ ژاپن موظف به مشارکت و هدایت مباحث جهانی در خصوص چگونگی تضمین سه مفهوم مرکزی

امنیت و آزادی و عدالت در فضای سایبری است. در این زمینه، وزارت امور خارجهٔ ژاپن موظف است از طریق همکاری با سایر وزارتخانه‌ها و نهادهای مربوط و نیز ذی‌نفعان بخش خصوصی، سیاست خارجی این کشور را دربارهٔ فضای سایبری بر مبنای سه پایهٔ اصلی ذیل به پیش برد:

۱. قانون‌گذاری و اطمینان از حاکمیت قانون در فضای سایبری: تشویق و ترویج اعمال قوانین بین‌المللی موجود در فضای سایبری و تلاش برای قانون‌گذاری جدید در زمان‌های صلح.

۲. توسعهٔ اقدامات اطمینان‌بخش در زمینهٔ فضای سایبری: این اقدامات اطمینان‌بخش به خصوص باید در زمان‌های صلح صورت گیرد تا از برخورد و تضاد سایبری جلوگیری و اجتناب به عمل آید. همچنین این اقدامات از طریق «ثبات» و «شفافیت» در حوزهٔ فضای سایبری نیز ممکن است تشدید گردد.

۳. همکاری در زمینهٔ بسترسازی و ظرفیت‌سازی در زمینهٔ فضای سایبری: بسترسازی و ظرفیت‌سازی در زمینهٔ فضای سایبری برای توسعهٔ منابع انسانی ضروری است. در این رویکرد همچنین هر گونه «حفرهٔ امنیتی» در سایر کشورها، یک ریسک بزرگ برای کل جهان، از جمله ژاپن، محسوب می‌شود. بر مبنای سه پایهٔ گفته‌شده، ژاپن دو اولویت را در زمینهٔ دیپلماسی سایبری مدنظر دارد: نخست، اطمینان از همکاری سایبری در منطقهٔ آسیا ـ اقیانوسیه، به عنوان حوزهٔ پیرامونی این کشور، به خصوص اینکه با هدف تداوم توسعه و تضمین ثبات در منطقه، اقدامات اطمینان‌بخش باید به صورت مداوم صورت پذیرد.[1] دوم، همکاری با جامعهٔ بین‌الملل (سازمان‌های جهانی) و نیز کشورهایی نظیر آمریکا و اروپا که در زمینهٔ فضای سایبری، ارزش‌های مشترکی با کشور ژاپن دارند. این همکاری قبل از هر چیز باید معطوف به

1. ASEAN-Japan Collaboration on Information Security, 2010

اطمینان از حاکمیت قوانین بین‌المللی فعلی در عرصهٔ فضای سایبری و نیز حرکت به سوی تدوین قوانین، مطابق با تغییر و تحولات روز باشد.

با توجه به دو اولویت گفته‌شده، ژاپن در حال حاضر گفت‌وگوهای دوجانبه‌ای را در زمینهٔ فضای سایبری، با یازده کشور جهان، از جمله آمریکا، روسیه، فرانسه، آلمان، انگلستان، استرالیا، هندوستان، کرهٔ جنوبی، استونی، اوکراین و اسرائیل، دنبال می‌کند. ضمن آنکه به طور هم‌زمان گفت‌وگوهایی با اتحادیهٔ اروپا و اتحادیهٔ آسه‌آن و نیز گفت‌وگوهایی سه‌جانبه با محوریت «ژاپن ـ چین و کرهٔ جنوبی» و نیز «ژاپن ـ آمریکا و کرهٔ جنوبی» در پیش گرفته است.

ژاپن در سطوح جهانی نیز در قالب نهادها و نشست‌های جهانی، همچون کارشناسان دولتی سازمان ملل که از سال ۲۰۰۴ آغاز به کار کرده‌اند، گروه جی ۷ که کارگروه سایبری آن از سال ۲۰۱۶ شروع به فعالیت کرده، گروه جی ۲۰ و کنفرانس جهانی در زمینهٔ فضای سایبری، نقش فعالی در حوزه فضای سایبری در مقیاس منطقه‌ای و جهانی ایفا می‌کند.[1]

جمع‌بندی و نتیجه‌گیری این فصل

وابستگی توسعهٔ اقتصادی ژاپن به نفوذ شرکت‌ها، کمپانی‌ها و فناوری این کشور باعث حضور در عرصهٔ سایبری در مقیاس منطقه‌ای و جهانی شده است. اگرچه ژاپن به صورت تاریخی و سیاسی در ائتلاف کشورهای غربی به رهبری آمریکا و اروپا قرار دارد، اما موقعیت جغرافیایی این کشور در شرق آسیا و در همسایگی کشورهایی همچون روسیه و چین باعث شده تا این کشور همواره در تدوین سیاست‌های خود به فکر ایجاد نوعی توازن استراتژیک بین دو جبههٔ غرب و شرق باشد.

---

1. Cyber Security Strategy, 2015, 2018

رویکرد ژاپن به مقولهٔ سایبری نیز از این امر مستثنا نیست. به این اعتبار، دیپلماسیِ سایبری ژاپن را در مقایسه با سایر کشورهای پیشرو باید رویکردی بینابینی دانست. به این معنا که اگرچه در عرصهٔ بین‌المللی، رویکرد ژاپن بیشتر همسو با کشورهای آمریکا و اروپای غربی است، اما این کشور همسو با چین و روسیه دغدغهٔ مشترکی نیز در ارتباط با امنیت ملی و حاکمیت ملی دارد. به عبارت دیگر، اگرچه ژاپن به دنبال تحقق فضای سایبری آزاد و عادلانه و ایمن است، اما به خاطر سابقهٔ تهدیدات و حملات سایبری در این کشور، همانند چین و روسیه دغدغه‌هایی نیز در ارتباط با امنیت اطلاعات بین‌الملل دارد.

ژاپن فضای سایبری را عامل و بستر گذار کشورها به جوامع نوع پنج می‌داند. به همین دلیل معتقد است که تنها یک رویکرد همگرا با مشارکت همهٔ بازیگران می‌تواند متضمن امنیت، صلح و ثبات لازم در عرصهٔ سایبری برای گذار کشورها به جوامع نوع پنج باشد. رویکرد همگرا با مشارکت همهٔ بازیگران نیز تنها زمانی اتفاق خواهد افتاد که هر بازیگر و ذی‌نفعی از نقش و اهمیت خود آگاه باشد. به همین دلیل، ژاپن با هدف دستیابی به این هدف، تعاملات دیپلماتیک گسترده‌ای، هم با کشورهای بلوک غرب و هم با کشورهای بلوک شرق در قالب استراتژی‌های دوجانبه، چندجانبه و نیز منطقه‌ای و بین‌المللی آغاز کرده و در برخی موارد نیز به نتایج مطلوبی دست یافته است.

منابع

ASEAN-Japan Collaboration on Information Security (2010), National Center of Incident Readiness and Strategy for Cyber Security (NISC) Government of Japan August 26, 2016, Retrieved from: https://www.nisc.go.jp/eng/ on 20 of March 2019.

Cyber Security Annual Report in 2013, National Center of Incident Readiness and Strategy for Cyber Security (NISC) Government of Japan, 2013, Retrieved from: https://www.nisc.go.jp/eng/ on 20 of April 2019.

Cyber Security Annual Report in 2018, National center of Incident readiness and Strategy for Cyber Security (NISC) Government of Japan, 2018, Retrieved from: https://www.nisc.go.jp/eng/ on 20 of April 2019.

Cyber Security Strategy (July 2018), National Center of Incident Readiness and Strategy for Cyber Security (NISC) Government of Japan, Retrieved from: https://www.nisc.go.jp/eng/ on 20 of November 2019.

Cyber Security Strategy (September 2015), National Center of Incident Readiness and Strategy for Cyber Security (NISC) Government of Japan, Retrieved from: https://www.nisc.go.jp/eng/ on 20 of November 2019.

General Framework for Secure IoT Systems, National Center of Incident Readiness and Strategy for Cyber Security (NISC) Government of Japan August 26, 2016, Retrieved from: https://www.nisc.go.jp/eng/ on 20 of March 2019.

Japanese Government's Efforts to Address Information Security Issues (November 2007), National Center of Incident Readiness and Strategy for Cyber Security (NISC) Government of Japan, Retrieved from: https://www.nisc. go.jp/eng/ on 20 of November 2019.

The Cyber Ssecurity Policy for Critical Infrastructure Protection (4th Edition) (2018), National Center of Incident Readiness and Strategy for Cyber Security (NISC) Government of Japan. Retrieved from: https://www.nisc. go.jp/eng/ on 20 of November 2019.

فصل چهارم

ظهور و افول دیپلماسی سایبری آمریکا: بازگشت به رویکرد امنیتی ـ تهاجمی

درآمد

آمریکا با توجه به اشرافیت راهبردی در حوزهٔ فناوری اطلاعات و ارتباطات، به خصوص از طریق سازوکارهای مالکیت و مدیریت اینترنت، میزبانی از بزرگ‌ترین پلتفرم‌ها و قرارگرفتن در مرکز مهم‌ترین تحولات فناورانهٔ سایبری، پیشتاز کشورهای جهان در حوزهٔ فعالیت‌های مرتبط با فضای سایبری (اعم از امنیت سایبری یا دیپلماسی سایبری ــ جدول شمارهٔ ۱) محسوب می‌شود.

جدول شمارهٔ ۱. برخی از مهم‌ترین اسناد و اقدامات مرتبط با فضای سایبری در آمریکا

ردیف	نوع فعالیت‌ها یا اقدامات مرتبط با فضای سایبری
۱	سند استراتژی بین‌المللی برای فضای سایبری،[1] ۲۰۱۱
۲	سند استراتژی سیاست فضای سایبری بین‌المللی،[2] ۲۰۱۶
۳	تشکیل کمیسیون ارتقای امنیت سایبری ملی آمریکا[3] در وزارت بازرگانی، ۲۰۱۶

1. International Strategy for Cyberspace
2. International Cyberspace Policy Strategy
3. Enhancing National Cybersecurity

۴	قانون دیپلماسی سایبری آمریکا[1] ۲۰۱۷
۵	فرمان اجرایی ۱۳۸۰۰ ریاست‌جمهوری آمریکا در ارتباط با تقویت سایبری شبکه‌های فدرال و زیرساخت‌های کلیدی[2] ۲۰۱۷
۶	بازخوانی دیپلماسی سایبری آمریکا در عصر افزایش تهدیدها، ۲۰۱۸
۷	استراتژی سایبری ملی ایالات متحده آمریکا[3]

آمریکا اولین کشوری بود که در سال ۲۰۱۱ نخستین سند «استراتژی بین‌المللی فضای سایبری» خود را منتشر و از موضوع «دیپلماسی سایبری» سخن به میان آورد. در این سند، در حالی که چند اولویت ملی شامل اقتصاد، حفاظت از شبکه، اعمال قانون، فعالیت‌های نظامی، حکمرانی اینترنت، توسعهٔ بین‌المللی و آزادی اینترنت مطرح شده است، بر ۱. دیپلماسی، ۲. دفاع و ۳. توسعه به عنوان سه ستون اصلی، به منظور دستیابی به این اولویت‌ها تأکید شده بود.[4]

سپس کنگرهٔ این کشور در سپتامبر ۲۰۱۷، قانون دیپلماسی سایبری را تصویب، و دولت این کشور در نوامبر همان سال، آن را رسماً ابلاغ کرد. همچنین کمیتهٔ روابط خارجی کنگرهٔ آمریکا در فوریهٔ ۲۰۱۸، نشستِ بازخوانی و ارزیابی دیپلماسی سایبری آمریکا را تحت عنوان «دیپلماسی سایبری آمریکا در عصر تهدیدهای روزافزون» برگزار کرد که حاوی دیدگاه‌ها، استراتژی‌ها و اهداف راهبردی این کشور در حوزهٔ سایبری در عرصهٔ ملی، منطقه‌ای و بین‌المللی است.

---

1. US Cyber Diplomacy Act
2. Presidential Executive Order 13800 on Strengthening the Cybersecurity of Federal Networks and Infrastructure
3. National Cyber Strategy of US
4. White House, 2011

آنچه در این بخش در ارتباط با دیپلماسی سایبری آمریکا مورد مطالعه قرار گرفته، به طور خاص الف: قانون دیپلماسی سایبری آمریکا (سپتامبر ۲۰۱۷)، ب: بازخوانی قانون دیپلماسی سایبری آمریکا با عنوان «دیپلماسی سایبری آمریکا در عصر تهدیدهای روزافزون» (فوریهٔ ۲۰۱۸) و ج: سند «استراتژی سایبری» ملی ایالات متحده (سپتامبر ۲۰۱۸) می‌باشد.[۱] با توجه به اهمیت کشور آمریکا در ارتباط با موضوع دیپلماسی سایبری، در پایان نیز تحلیلی بر فراز و نشیب‌های رویکردهای امنیتی ـ نظامی و دیپلماتیک ایالات متحده به مقولهٔ فضای سایبری صورت خواهد گرفت.

نگاهی به قانون دیپلماسی سایبری آمریکا (۲۰۱۷)

قانون دیپلماسی سایبری آمریکا که در سال ۲۰۱۷ در کنگرهٔ این کشور تصویب شد، یکی از معدود قوانین این کشور است که با حمایت قاطع هر دو حزب دموکرات و جمهوری‌خواه این کشور به تصویب رسید. این قانون اگرچه در زمان ریاست‌جمهوری دونالد ترامپ به تصویب رسید، اما آشکار است که محصول رویکرد عمدتاً دیپلماتیک و سیاسی دولت باراک اوباما به مقولهٔ فضای

---

۱. در این فصل تأکید بر دیپلماسی سایبری رسمی آمریکاست که از طریق دولت و نهادهای قانونی و دولتی این کشور دنبال می‌شود. در عین حال باید در نظر داشت که این کشور میزبان ده‌ها کمپانی و شرکت بزرگ و چندملیتی آی‌تی است که هر کدام به تنهایی بازیگرانی جهانی با دایرهٔ اثرگذاری فراملّی در حوزهٔ سایبری محسوب می‌شوند. با توجه به اهمیت نقش این کمپانی‌ها در روابط بین‌المللی، تعدادی از این شرکت‌ها در قالب گافام به صورت مستقل در فصل نهم مورد مطالعه قرار گرفته‌اند.

سایبری بوده است[1] و ریشه در دو سند «استراتژی بین‌المللی برای فضای سایبری، ۲۰۱۱» و «استراتژی سیاست فضای سایبری بین‌المللی، ۲۰۱۶» دارد.

مبنای قانون دیپلماسی سایبری آمریکا، که معطوف به تلاش‌های جهانی این کشور برای حفظ سلطه و اشرافیت راهبردی خود در حوزهٔ اینترنت و شبکه است، عبارت است از: تلاش برای حفظ و گسترش زیرساخت اطلاعاتی و ارتباطی باز، مطمئن، امن و تعاملی در زمینهٔ امنیت ملی و نیز علائق اقتصادی کشور آمریکا.

قانون دیپلماسی سایبری آمریکا چند بخش اصلی دارد: ۱. کشفیات (پیش‌فرض‌ها)، ۲. سیاست فضای سایبری بین‌المللی ایالات متحده آمریکا، ۳. وظایف وزارت امور خارجهٔ ایالات متحده آمریکا، ۴. هماهنگی‌های اجرایی و مدیریتی فضای سایبری بین‌المللی، ۵. استراتژی بین‌المللی برای فضای سایبری، و ۶. گزارش‌های سالیانه از کشورهای خارجی در زمینهٔ فعالیت‌های حقوق بشری.[2]

۱. کشفیات (پیش‌فرض‌ها): قانون دیپلماسی سایبری آمریکا بر اساس یازده پیش‌فرض اساسی تنظیم شده است که این پیش‌فرض‌ها عمدتاً مبانی و تا حد زیادی دلایل و ضرورت تدوین این قانون (قانون دیپلماسی سایبری آمریکا) را تبیین می‌کنند. این پیش‌فرض‌ها را به طور کلی به سه دسته می‌توان تقسیم کرد:

ـــ مبانی فکری و ارزشی ایالات متحده آمریکا در ارتباط با فضای سایبری: در این خصوص، مهم‌ترین نکته اصلِ «باز، تعاملی، امن و قابل اتکا بودن» اینترنت، به عنوان فضای سایبری، در راستای منافع ملی آمریکاست.

---

۱. در دولت دونالد ترامپ بسیاری از رویکردهای تبیین‌شده در این قانون کنار گذاشته شد و حتی مهم‌ترین خروجی عینی آن در ساختار وزارت امور خارجهٔ آمریکا، یعنی «ادارهٔ هماهنگ کننده امور سایبری»، حذف و به یک واحد بسیار کوچک‌تر تقلیل یافت.

2. US Cyber Diplomacy Act, 2017

این موضوع ریشه در سند استراتژی بین‌المللی برای فضای سایبری آمریکا دارد که در ۲۰۱۱ تدوین و اعلام شد. بر اساس این سند، ایالات متحده به همکاری بین‌المللی برای ترویج زیرساخت‌های اطلاعاتی و ارتباطی باز، تعاملی، امن و قابل اتکا، که حامیِ تجارت بین‌الملل و افزایندهٔ امنیت بین‌الملل و موجب تقویت آزادی بیان است، متعهد می‌شود؛ به نحوی که هنجارهای رفتار مسئولانه راهنمای اقدامات دولت‌ها، همکاری و مشارکت پایدار و حمایت از حاکمیت قانون در فضای سایبری گردد.

ـــ به رسمیت شناختن رویکردها و اقدامات همسو با مبانی فکری و ارزشی ایالات متحده: بر این اساس، قانون دیپلماسی آمریکا تمامی رویکردها و اقدامات بین‌المللی را، که همسویی کامل با مبانی فکری و ارزشی ایالات متحده دارد، به رسمیت می‌شناسد. از جمله مهم‌ترین این رویکردها، که ایالات متحده خود نقشی اساسی در آن داشته است، می‌توان به توصیه‌های گروه کارشناسان دولتی[1] اعلامیهٔ رهبران گروه ۲۰ در سال ۲۰۱۷ در زمینهٔ قابلیت تسرّی قوانین بین‌الملل به رفتارهای دولت‌ها و بیانیهٔ گروه ۷[2] در ارتباط با رفتار مسئولانهٔ دولت‌ها در فضای سایبری اشاره کرد.

ـــ رد تمامی رویکردها و اقدامات غیرهمسو با مبانی فکری و ارزشی ایالات متحده آمریکا: بر این اساس، قانون دیپلماسی سایبری آمریکا به طور مشخص به دو دسته از رویکردهای غیرهمسو با مبانی فکری و ارزش‌های ایالات متحده در ارتباط با فضای سایبری اشاره می‌کند که عبارت‌اند از: نخست، اقدامات سازمان همکاری شانگهای و به طور مشخص پیشنهاد نظام‌نامهٔ استاندارد بین‌المللی برای امنیت اطلاعات[3] که کشورهای چین،

1. The Group of Governmental Experts (GGE)
2. Group of 7 (G7) Declaration
3. International Code of Conduct for Information Security

روسیه، قزاقستان، قرقیزستان، ازبکستان و تاجیکستان آن را در سال ۲۰۱۵ ارائه کردند. طبق این پیشنهاد، در مواقعی که امنیت داخلی کشورها در معرض تهدید قرار می‌گیرد، حق «جلوگیری از انتشار اطلاعات» و همچنین «کنترل فناوری اطلاعات و ارتباطات» برای دولت‌ها به رسمیت شناخته شده است؛ دوم، تلقی شش بازیگر (از جمله چهار کشور) به عنوان بازیگران سایبریِ تهدیدکننده برای ایالات متحده، نظیر ۱. روسیه به سبب تلاش برای نفوذ و دخالت در انتخابات ۲۰۱۶ آمریکا؛ ۲. چین که فعالانه ایالات متحده آمریکا و متحدان آن و شرکت‌های آمریکایی را هدف جاسوسی سایبری قرار می‌دهد، ۳. ایران به سبب استفاده از فضای سایبری به منظور جاسوسی، پروپاگاندا و حمله در مسیر اولویت‌های امنیتی و نیز تلاش برای مدیریت رویدادها و وقایع، تحت تأثیر قرار دادن برداشت‌های خارجی و نیز مقابله با تهدیدات متعارف، ۴. کرهٔ شمالی به دلیل اینکه پیش‌تر به طور هدفمند به کمپانی‌های تجاری آمریکا حملات سایبری می‌کرد، ۵. تروریست‌ها که از اینترنت برای ترویج، گسترش، جذب نیرو و سرمایه، هدایت فعالیت‌های مخرب، جمع‌آوری اطلاعات و ... در مسیر فعالیت‌های تروریستی خود استفاده می‌کنند، و ۶. گروه‌های تبهکار که از ابزارهای سایبری برای رفتارهای مخربشان، از جمله سرقت، کلاهبرداری، فریب و اخاذی از قربانیان خود، بهره می‌جویند.[1]

۲. سیاست فضای سایبری بین‌المللی ایالات متحده آمریکا: این بخش دربردارندهٔ مبانی فکری و مهم‌ترین ارزش‌های آمریکایی است که دولت این کشور می‌کوشد آن‌ها را به عنوان معیارهای اساسی و بین‌المللی در ارتباط با فضای سایبری و به منظور منافع ملی و امنیتی خود اعمال کند.

---

1. US Cyber Diplomacy Act, 2017

بر اساس این بخش، سیاست کلی ایالات متحده در ارتباط فضای سایبری، همکاری بین‌المللی با کشورهای همسو و دیگر شرکای بین‌المللی برای ترویج «حکمرانی اینترنت به صورت باز، تعاملی[1] قابل اتکا، بدون محدودیت[2] و امن بر اساس مدل چندذی‌نفعی است که حقوق بشر و دموکراسی و حاکمیت قانون شامل حق آزادی بیان، نوآوری، ارتباطات و رونق اقتصادی را به رسمیت می‌شناسد و در عین رعایت حریم خصوصی افراد، از آن‌ها در برابر فریب، کلاهبرداری و سرقت حفاظت می‌کند».

بر اساس این سیاست کلی، رئیس‌جمهوری ایالات متحده باید با مشورت با بازیگران خارجی، از جمله شرکت‌های فناوری، سازمان‌های غیردولتی و کارشناسان امنیتی، همواره در روابط دوجانبه و چندجانبه به صورت صریح موارد ذیل را دنبال کند: ۱. اطمینان از قابلیت تسرّی و اجرای قوانین بین‌المللی در فضای سایبری از جمله قانون درگیری نظامی؛ ۲. اطمینان از اینکه کشورهای قربانیِ فعالیت‌های مخرب سایبری حق انجام اقدامات مقابله‌جویانه را، البته مادامی که ناقض حقوق بشر یا دیگر هنجارهای اساسی نباشد، دارند؛ ۳. اطمینان از کاهش و محدود کردن ریسک تشدید حملات مخرب در فضای سایبری، از جمله حمله به زیرساخت‌های کلیدی؛ ۴. همکاری با کشورهای همسو برای ترویج ارزش‌های مشترک با آمریکا، همچون حقوق بشر، آزادی، حاکمیت قانون و ...؛ و ۵. تضمین و اطمینان از رفتار مسئولانهٔ کشورها در فضای سایبری.

با توجه به اهمیت مقولهٔ رفتار مسئولانهٔ کشورها ــ بر اساس بند ۵ مذکور ــ که ایالات متحده موظف به واداشتن دولت‌ها به رعایت آن‌هاست، قانون

---

1. Interoperable
2. Unfettered

دیپلماسی سایبری آمریکا تقسیم‌بندی دقیقی از بایدها و نبایدها در قالب رفتارهای «ایجابی» و «سلبی» بر اساس مبانی فکری و ارزش‌های خود ارائه می‌دهد که برخی از مهم‌ترین آن‌ها به شرح ذیل است:

ــ حذر از رفتارها و فعالیت‌های ناقض مالکیت معنوی نظیر سرقت اطلاعات، جاسوسی اطلاعات تجاری، و ... ؛

ــ اجتناب از فعالیت‌های مخرب سایبری یا حمایت آگاهانه از آن علیه نظم و امنیت بین‌المللی؛

ــ اطمینان از عاری بودن حوزهٔ جغرافیایی تحت حاکمیتشان از هر گونه فعالیت ناقض تعهدات بین‌المللی آن‌ها؛

ــ اجتناب از فعالیت در حوزهٔ آی‌سی‌تی که در تضاد با قوانین بین‌المللی است یا حمایت آگاهانه از آن که ممکن است خساراتی به زیرساخت‌های کلیدی وارد سازد؛

ــ عدم محدودسازی جریان فرامرزی (بین‌المللی) اطلاعات یا تلاش برای ذخیره‌سازی یا پردازش داده‌ها به صورت محلی؛

ــ ارائهٔ پاسخ سریع و همکاری مناسب با کشورهایی که زیرساخت‌های کلیدی آن‌ها مورد حملات سایبری مخرب قرار گرفته است (به خصوص حملاتی که از آن کشور نشئت گرفته باشد)؛

ــ تعیین پیشران‌ها و مشوق‌های اقتصادی برای ترویج محصولات آی‌سی‌تی امن و مطمئن و نیز توسعهٔ چارچوب حقوقی و سیاسی برای ترویج اینترنت امن؛

ــ اطمینان از اعمال و رعایت حقوق بشر و آزادی‌های اساسی در اینترنت و پایبندی به این اصل که انسان‌ها از همان حقوقی که به صورت طبیعی از آن برخوردارند، در فضای سایبری نیز بهره‌مند شوند؛

ــ همکاری در توسعه و اجـرای اقـداماتی بـه منظـور افـزایش ثبـات و امنیتِ استفاده از آی‌سی‌تی و جلوگیری از فعالیت‌های آی‌سی‌تی که ممکـن است برای صلح و امنیت بین‌المللی مضر باشد.

۳. وظایف وزارت امور خارجهٔ ایالات متحده آمریکا: بر اساس این بخش، وزارت امور خارجهٔ آمریکا باید با ایجاد تغییراتی در ساختار خود، به راه‌اندازی ادارهٔ امور سایبری[1] اقدام کند. رئیس ادارهٔ امور سایبری هم‌سطح و هم‌رتبهٔ سفیر است و مستقیماً از سوی رئیس‌جمهوری انتخاب خواهد شد.

بر اساس قـانون دیپلماسـی سـایبری آمریکـا، رئـیس ادارهٔ امـور سـایبری وزارت امور خارجه به عنوان بـالاترین مقـام سـایبری ایـن کشـور مسـئولیت اصلی توسعه و پیگیری دیپلماسی سایبری ایالات متحده را در جهان بر عهـده دارد و همچنین مسئول هماهنگی بین تمامی وزارتخانـه‌هـا، از جملـه وزارت بازرگانی، وزارت دفاع، وزارت خزانه‌داری، وزارت دادگسـتری، وزارت امـور داخلی و امنیت ملی، وزارت انرژی و نیز شورای امنیت ملی آمریکـا در امـور مربوط به فضای سایبری، هم در داخل و هم در خارج از این کشور، است.

همچنین علاوه بر رئیس ادارهٔ امور سایبری وزارت امور خارجه، قـانون دیپلماسی سایبری آمریکا نمایندهٔ دائم این کشور را در سازمان ملل موظـف می‌کند تا از حق وتو و قدرت و نفوذ ایالات متحده بـرای مخالفـت بـا هـر اقدامی، که خلاف سیاست سایبری بین‌الملـل (اصـول دیپلماسـی سـایبری) ایالات متحده است، استفاده کند.[2]

۴. هماهنگی‌های اجرایی دیپلماسی سایبری بین‌المللی: قانون دیپلماسـی سایبری آمریکا در این بخش از رئیس‌جمهوری ایالات متحده می‌خواهد که با هدف پیشبرد دیپلماسی سایبری این کشور، هماهنگی‌های اجرایـی را، بـه

1. Office of Cyber Issues
2. US Cyber Diplomacy Act, 2017

خصوص از طریق همکاری با کشورهایی همسو با ارزش‌های ایالات متحده، صورت دهد و به طور متناوب نتایج این هماهنگی‌ها را به اطلاع کنگره برساند. دراین‌باره، به طور مشخص به راهبرد گفت‌وگوهای دوجانبه با کشورهای ژاپن، انگلستان، چین، کرهٔ جنوبی، استرالیا، هندوستان، کنیا، اسرائیل و دیگر کشورهای همسو اشاره شده که گفت‌وگوهای دوجانبهٔ آمریکا با برخی از آن‌ها از سال ۲۰۱۴ آغاز گردیده و حتی به مرحلهٔ امضای قرارداد همکاری نیز رسیده است.[1]

۵. استراتژی بین‌المللی برای فضای سایبری: در این بخش، قانون دیپلماسی سایبری آمریکا از وزارت امور خارجهٔ این کشور می‌خواهد تا از طریق همکاری با سایر دپارتمان‌ها و آژانس‌های مرتبط در دولت فدرال، ظرف بازهٔ زمانی یک‌ساله از هنگام تصویب، یک استراتژی مدون در ارتباط با سیاست سایبری بین‌المللی (دیپلماسی سایبری) آمریکا تدوین کند. این استراتژی باید شامل تمامی موارد ذیل باشد:

۱. ارزیابیِ تمامی اقدامات انجام‌شده در زمینهٔ دیپلماسی سایبری آمریکا تا کنون؛ ۲. برنامهٔ اقدام برای فعالیت‌های آتی؛ ۳. ارزیابی ارزش‌ها و مفاهیم جایگزینِ ارائه‌شده از سوی سایر کشورها در ارتباط با فضای سایبری؛ ۴. توضیحات مفصّل همراه با جزئیاتِ تهدیدات جدید و در حال ظهور برای امنیت ملی آمریکا در فضای سایبری از سوی کشورهای خارجی، بازیگران مورد حمایت دولت‌ها و بازیگران خصوصی (این تهدیدات می‌تواند شامل تهدیدات زیرساخت‌های فدرال یا بخش خصوصی، مالکیت فکری، و حتی حریم خصوصی شهروندان آمریکا باشد)؛ ۵. ارزیابی ابزارهای سیاسیِ در اختیار رئیس‌جمهور به منظور مهار یا از بین بردن تنش‌ها با کشورهای

1. Ibid

خارجی و بازیگران مورد حمایت دولت‌ها و بازیگران بخش خصوصی در حوزهٔ فضای سایبری. این ارزیابی همچنین باید شامل اینکه به چه میزان از این ابزارها استفاده شده و اینکه آیا مؤثر بوده‌اند یا خیر، نیز باشد؛ ۶. ارزیابی منابع مورد نیاز برای انجام این اقدامات به منظور نهادینه‌سازی ارزش‌ها و هنجارهای مسئولانه از رفتار سایبری بین‌المللی؛ ۷. شفاف‌سازی این مسئله که قوانین و هنجارهای بین‌المللی، از جمله قانون مداخلهٔ نظامی، قابلیت اجرا در فضای سایبری و فعالیت‌های آی‌سی‌تی مرتبط با آن را دارد؛ و ۸ . شفاف‌سازی این مسئله که بر اساس قوانین بین‌الملل، کشورهای قربانیِ حملات مخرب سایبری حق انجام اقدامات متقابل متناسب را دارند.[1]

۶. گزارش‌های سالیانه از کشورهای خارجی در زمینهٔ فعالیت‌های حقوق بشر: این بخش به خصوص با توجه به قانون کمک‌های خارجی ایالات متحده آمریکا (۱۸۶۱) در نظر گرفته شده است و ضمن ایجاد اصلاحاتی در این قانون، از دولت آمریکا می‌خواهد تا دربارهٔ گزارش سالیانهٔ حقوق بشر از سایر کشورها، علاوه بر موارد پیشین، به طور دقیق اطلاعاتی از فعالیت‌های آن‌ها در زمینهٔ آزادی بیان با توجه به فضای سایبری تهیه کند که شامل این موارد باشد: ۱. میزان دسترسی مردم به اینترنت در سایر کشورها؛ ۲. میزان فیلتر، سانسور یا حذف دیدگاه‌های سیاسی و مذهبی (غیرخشونت‌آمیز) در اینترنت و فضای سایبری از سوی دولت؛ ۳. میزان اذیت و آزار، تعقیب قانونی یا مجازات افراد و گروه‌های دارای افکار یا عقاید سیاسی و مذهبی غیرخشونت‌آمیز در اینترنت یا فضای سایبری؛ ۴. میزان تلاش دولت‌ها برای کسب، جمع‌آوری و افشای اطلاعات شخصیِ افراد دارای افکار، عقاید، ایدئولوژی یا ارتباطات

1. US Cyber Diplomacy Act, 2017

غیرخشونت‌آمیز که میثاق بین‌المللی حقوق مدنی و سیاسی از آنان حمایت کرده است؛ ۵. میزان تلاش دولت‌ها برای رصد و مانیتور ارتباطات الکترونیکی افراد بدون توجه به حریم خصوصی و آزادی و حقوق بشر.[1]

برای تهیهٔ گزارش‌های سالیانهٔ حقوق بشری از سایر کشورها، قانون دیپلماسی سایبری آمریکا، وزارت امور خارجه و دیپلمات‌های این کشور را به همکاری نزدیک با سازمان‌های حقوق بشری، شرکت‌های فناوری و اینترنت و نیز دیگر سازمان‌های غیردولتی ترغیب می‌کند.

دیپلماسی سایبری آمریکا در عصر تهدیدهای روزافزون

همان طور که قبلاً گفته شد، نشست بازخوانی قانون دیپلماسی سایبری آمریکا با عنوان دیپلماسی سایبری آمریکا در عصر تهدیدهای روزافزون در فوریهٔ ۲۰۱۸ برگزار شد. این نشست اگرچه یک سند قانونی یا مانیفست رسمی نیست، اما به دو دلیل اهمیت فراوانی دارد: ۱. این نشست در کمیتهٔ روابط خارجی کنگره و با حضور سه تن از مقامات ارشد سابق این کشور در حوزهٔ سایبری، یعنی کریستوفر پینتر نخستین سفیر ایالات متحده در حوزهٔ دیپلماسی سایبری، جان میلر[2] معاون شورای «صنعت فناوری اطلاعات» در امور سیاست جهانی و امنیت سایبری، و مایکل سولمیر رئیس پروژهٔ امنیت سایبری مرکز بلفر وابسته به مدرسهٔ دولتی جان اف کندی در دانشگاه هاروارد و رئیس سابق برنامه‌ریزی و اجرای سیاست سایبری وزارت دفاع آمریکا، برگزار شد؛ ۲. در مباحث صورت‌گرفته بین کمیتهٔ روابط خارجی و نیز سه تن از کارشناسان برجستهٔ این حوزه، به طور مفصّل و دقیق به احصا و صورت‌بندی این امور پرداخته شد: مهم‌ترین گرایش‌های بین‌المللی در

1. Ibid
2. John Miller

حوزهٔ دیپلماسی سایبری، مهم‌ترین چالش‌های حوزهٔ آسی‌تیِ پیش روی ایالات متحده، و مهم‌ترین مسائل دفاعی آمریکا در حوزهٔ سایبری.

آنچه در ادامهٔ این بخش ارزیابی و بررسی می‌شود، رئوس مباحث و دیدگاه‌های هر یک از این سه کارشناس ارشد حوزهٔ سایبری آمریکاست.

- **کریستوفر پینتر: چالش‌های دیپلماسی سایبری آمریکا از منظر سیاست خارجی**

کریستوفر پینتر نخستین دیپلمات و سفیر ایالات متحده در حوزهٔ دیپلماسی سایبری است که از زمان راه‌اندازی ادارهٔ امور سایبری در وزارت امور خارجهٔ آمریکا، مسئولیت هدایت و رهبری و ادارهٔ آن را بر عهده داشته است.

مهم‌ترین چالش‌های حوزهٔ سایبری: کریستوفر پینتر علاوه بر طبقه‌بندی شش بازیگر حوزهٔ سایبری (شامل روسیه، چین، ایران، کرهٔ شمالی، تروریست‌ها و گروه‌های تبهکار) به عنوان مهم‌ترین عوامل تهدیدکنندهٔ ایالات متحده، از چند چالش جدید برای اشرافیت راهبردی ایالات متحده در این حوزه نام می‌برد: ۱. ظهور و توسعهٔ اینترنت اشیا و اینکه امنیت این اشیا دیگر در کنترل یک واحد مشخص قرار ندارد؛ ۲. ظهور گرایش جدید در بین برخی دولت‌ها برای تغییر الگوی حکمرانی اینترنت از مدل چندذی‌نفعی به الگوی حکمرانی کنترلی بین دولتی[1] که به نوعی ناقض جریان آزاد اطلاعات اینترنت و حقوق بشر است؛ ۳. تلاش برخی دولت‌ها برای کنترل و محدود کردن اینترنت که آشکارا برخلاف اصل «باز بودن» اینترنت است.

راهکارهای مقابله با چالش‌های جدید: کریستوفر پینتر دیپلماسی را مهم‌ترین اهرم برای مقابله با چالش‌های گفته‌شده از سوی ایالات متحده می‌داند. راهبردهایی که به نظر وی، آمریکا می‌تواند از طریق آن به مواجهه با این تهدیدها بپردازد عبارت‌اند از:

ـــ ایجاد هم‌پیمانی‌های استراتژیک و برقراری تعاملات چندجانبه: در

1. Intergovernmental Control

حالی که ایالات متحده با ده‌ها کشور (نظیر ژاپن، آلمان، انگلستان، فرانسه، مکزیک، کرهٔ جنوبی، آفریقای جنوبی، نیوزلند، استرالیا، کانادا، برزیل، آرژانتین و ...) در این حوزه وارد گفت‌وگوهای دوجانبه و چندجانبه شده است، باید از ظرفیت مختلف چندجانبه، از جمله کشورهای ناتو، گروه ۷، گروه ۲۰ و ...، نیز برای توسعهٔ دیپلماسی سایبری خود استفاده کند. همچنین لازم است تا علاوه بر کشورها، با بخش خصوصی و کمپانی‌های بزرگ حوزهٔ آی‌تی و سازمان‌های غیردولتی نیز وارد گفت‌وگو و مذاکره شود.

ــ ظرفیت‌سازی، تقویت همکاری و انجام اقدام جمعی: در حالی که ابزارهای دیپلماتیک همواره مؤثرند، بکارگیری آن‌ها به صورت جمعی و از طریق همکاری با شرکا و هم‌پیمانان استراتژیک اهمیت بسیار زیادی در مواجهه با تهدیدها دارد. علاوه بر این باید به کشورهای همسو در زمینهٔ ایجاد ظرفیت‌های سایبری، از جمله مهارت‌های مقابله با جرایم سایبری، ظرفیت مواجهه با حملات تروریستی و همچنین تدوین استراتژی ملی سایبری کمک کرد.

ــ پیشبرد سیاست استراتژیک و ایجاد اجماع برای ثبات سایبری جهانی: هدف استراتژیک آمریکا ترویج ارزش‌های اساسی، همچون اطمینان از اینترنت باز، جریان آزاد اطلاعات و مدل چندذی‌نفعی حکمرانی اینترنت، است که در سال‌های اخیر به شدت به چالش کشیده شده است. برای مواجهه با این چالش‌ها، ایالات متحده باید با ابتکارات دیپلماتیک، به ایجاد اجماع جهانی (هم در سطوح دولتی و هم در بخش خصوصی و جامعهٔ مدنی) در زمینهٔ ارزش‌های گفته‌شده اقدام کند و آگاهی و هشیاری لازم در مقیاس جهانی را در این زمینه ایجاد سازد. تشکیل ائتلاف آزادی آنلاین[1] با مشارکت برخی کشورها یکی از این ابتکارات مهم است. آمریکا همچنین

1. The Freedom Online Coalition

باید از کانال‌های مختلف دیپلماتیک، نظام‌های طرفدار «محلی‌سازی داده‌ها و پردازش داده‌ها به صورت محلی» را به چالش بکشد. دراین‌باره، ایالات متحده همچنین باید رهبری این مباحث را به عهده بگیرد: قابلیت تسرّی و اجرای قوانین بین‌المللی در حوزهٔ سایبری، توسعهٔ ارزش‌ها و هنجارهای رفتاری در فضای سایبری برای دولت‌ها به خصوص در زمان صلح، اقدامات اعتمادسازی عملی برای کاهش خطر تنش و درگیری در عرصهٔ سایبری.

ـــ بازدارندگی:[1] هر چقدر آمریکا برای ایجاد اجماع جهانی در زمینهٔ ارزش‌های پایه‌ای ایالات متحده تلاش کند، با این حال برخی بازیگران همواره برای نقض این ارزش‌ها در تلاش خواهند بود. ایالات متحده آشکارا اقدامات مناسبی تا کنون در زمینهٔ «بازدارندگی»، به خصوص در مقابل بازیگران دولتی، انجام نداده است. در قلب سیاست بازدارندگی باید پاسخ سریع و معتبر و بموقع به بازیگر خطاکار وجود داشته باشد. عدم چنین پاسخی به ایجاد یک رفتار هنجاری اشتباه برای بازیگر خطاکار مبنی بر «عدم واکنش» منجر می‌شود و اینکه می‌تواند مجدداً تهدید را تکرار کند یا گمان کند که تهدید او بدون هزینه بوده است.

ایالات متحده در سیاست بازدارندگی باید به طیف وسیعی از انواع پاسخ، از اِعمال قانون گرفته تا تحریم اقتصادی و حمله سایبری و ...، توجه نشان دهد. این وظیفهٔ دیپلمات‌هاست تا از کانال‌های مختلف و ابزارهای دیپلماتیک سازوکارهای بازدارندگی و نوع پاسخ این کشور به بازیگران خطاکار اطلاع‌رسانی کنند. همچنین اگرچه ایالات متحده همواره حق پاسخگویی را برای خود به تنهایی محفوظ می‌داند، اما مشروعیت این پاسخ‌ها هنگامی که به صورت جمعی و با همکاری چندین کشور مشترکاً صورت پذیرد، به طور قابل توجهی افزایش می‌یابد. لذا دیپلمات‌ها باید تلاش‌های مضاعفی برای

1. Deterrence

ایجاد چنین ائتلاف‌هایی برای پاسخ به بازیگران سایبری خطاکار انجام دهند.

ــ درج و لحاظ کردن دغدغه‌های سیاست خارجی در سیاست‌گذاری‌های کلان و تصمیم‌گیری‌های اجرایی و عملیاتی: ملاحظات سیاست خارجی نقش مهمی در اقدامات حساس، مداخلات نظامی، اعمال قانون و دیگر تصمیم‌گیری‌ها و سیاست‌گذاری‌های مرتبط با حوزهٔ سایبری دارد. بسیار ضروری و لازم است که وزارت امور خارجه همواره در مرکز ثقل این گونه تصمیم‌گیری‌ها و سیاست‌گذاری‌ها باشد. زیرا بدین صورت از قابل اتکا بودن سیاست‌ها و اقدامات ایالات متحده در حوزهٔ سیاست خارجی اطمینان می‌یابد و آمریکا نیز می‌تواند همواره مؤثرترین اقدامات را صورت دهد.

نگاهی به سوابق کریستوفر پینتر، نخستین و بالاترین دیپلمات سایبری آمریکا

کریستوفر پینتر فارغ‌التحصیل دانشکدهٔ حقوق استنفورد و نیز دانشگاه کُرنل است و چهره‌ای شناخته‌شده در سطح جهان در زمینهٔ امنیت سایبری و دیپلماسی سایبری و مبارزه با جرایم سایبری دارد. وی بیش از ۲۵ سال در پیگیری مسائل سایبری ایالات متحده و بین‌المللی درگیر بوده است؛ ابتدا به عنوان دادستان برخی از مشهورترین پرونده‌های جرایم سایبری در آمریکا، سپس به عنوان یک مقام ارشد در وزارت دادگستری، اف‌بی‌ای، شورای امنیت ملی و سرانجام وزارت امور خارجه. وی بیش از یک دهه سیاست‌های سایبری ایالات متحده را پیش می‌برد؛ مبدع و مبتکر سیاست‌ها و برنامه‌های سایبری این کشور بوده و همواره ایده‌ها، رویکردها و ابداعات جدیدی را برای مقابله با تهدیدات سایبری به سازمان‌ها، نهادها و دولت آمریکا پیشنهاد داده است.

کریستوفر پینتر در آخرین نقش خود، به عنوان بالاترین مقام سایبری دیپلماتیک ایالات متحده، هماهنگی و رهبری تلاش‌های دیپلماتیک این کشور را برای پیشبرد زیرساخت اینترنت و همچنین اطلاعاتی باز، تعاملی، ایمن و مطمئن بر عهده داشته و در این زمینه مشاوره‌های زیادی به دولت، به ویژه وزارت امور خارجهٔ آمریکا، داده است. مسئولیت اداره‌ای که کریستوفر پینتر بر عهده داشت

ــ ادارهٔ هماهنگ‌کنندهٔ امور سایبری ــ نخستین اداره و عالی‌ترین مقام در این کشور بود که به طور خاص به ابعاد دیپلماتیک موضوعات سایبری اختصاص یافته و موضوعات مهمی را اعم از امنیت ملی شامل ترویج هنجارهای رفتاری مسئولانه، ثبات سایبری، جلوگیری از جنگ سایبری، تقویت بازدارندگی سایبری، ارتقای امنیت سایبری، مبارزه با جرایم سایبری، ارتقای حکمرانی اینترنتی چندذی‌نفعی، پیشبرد آزادی اینترنت و حتی مسائل مربوط به حقوق بشر در فضای سایبری بر عهده داشت.

از جمله فعالیت‌های دیگر کریستوفر پینتر می‌توان به نقش وی در مذاکره دربارهٔ توافق حقوق مالکیت معنوی با کشور چین، مذاکره در زمینهٔ یک توافق جامع همکاری سایبری با کشور هندوستان و نیز دیگر تلاش‌های سیاسی وی برای استفاده از ابزارهای دیپلماتیک برای مقابله با حملات سایبری اشاره کرد. وی همچنین نقش سازنده‌ای در آغاز گفت‌وگوهای سایبری دولت آمریکا با ده‌ها کشور در اروپا، آسیا، آمریکا، خاورمیانه و حتی آفریقا داشته است. او و گروهش با پیشنهادِ چارچوبی بین‌المللی در زمینهٔ ثبات سایبری، در تدوین آن پیشگام بودند که این مهم به دنبال ایجاد یک اجماع جهانی دربارهٔ استانداردهای رفتاری قابل قبول و نیز توافق در زمینهٔ شفافیت و اعتمادسازی به منظور کاهش ریسک در محاسبه است که خود می‌تواند ناخواسته به درگیری در فضای سایبری منجر شوند.

پیش از پیوستن به وزارت امور خارجه، کریستوفر پینتر در کاخ سفید به عنوان مدیر ارشد «سیاست سایبری»، نقش هماهنگ‌کنندهٔ سایبری در شورای امنیت ملی را ایفا می‌کرده است. وی همچنین عضو ارشد گروهی بود که در ۲۰۰۹، در زمینهٔ مطالعه و تدوین سیاست فضای سایبری به رئیس‌جمهور کمک کرد که متعاقباً به ایجاد یک ادارهٔ جدید در شورای امنیت ملی این کشور، که منحصراً به مسائل سایبری می‌پرداخت، منجر شد.[1]

ــ ایجاد یک ساختار خلاقانه برای پیشبرد دیپلماسی سایبری: با توجه به اهمیت دیپلماسی و اینکه حوزهٔ سایبری یک حوزهٔ جدید، پردغدغه،

1. Christopher Pinter, 2019

مخاطره‌آمیز و نیازمند به رهبری و هـدایتِ بـین سـازمانی و فراسـازمانی در سطح ملی و جهانی است، ساختار بسیار چابک و خلاقانه‌ای بـرای پیشـبرد دیپلماسی سایبری ایالات متحده لازم اسـت. وزارت امـور خارجـهٔ ایـالات متحده در حال حاضر چنین ساختار خلاقانه‌ای ندارد، حتی به حـذف «ادارهٔ امور سایبری» اقدام کرده و جایگاه آن را تـا حـد بسـیار زیـادی تنـزل داده است و همچنین، در ساختار فعلی اهمیت بیشتری به مسـائل و موضـوعات اقتصادی نشان مـی‌دهـد. در سـاختار فعلـی وزارت امـور خارجـهٔ آمریکـا، مسئولِ امور سایبری با محدودیت‌های زیادی به لحاظ دسترسی به مقامـات بالاتر، دسترسی به منابع و بودجه، اسـتخدام نیروهـای حرفـه‌ای، ارتبـاط بـا سازمان‌های بیرونی و ... مواجه است. علاوه بر این، در حال حاضـر اگرچـه موضوعات اقتصادی بسیار مهم هستند، اما موضـوعات سـایبری، تهدیـدات ناشی از آن، و نیز ارزش‌های پایه‌ای ایالات متحده بـرای ایـن حـوزه نیـز از اهمیت بسیار بالایی، هم در سطح ملی و هم در سطح جهانی، برخوردارنـد. در این ساختار امکان رسیدگی و تمرکز به حد کافی بر موضوعاتی همچون بازدارندگی، هنجارهای رفتار مسئولانهٔ دولت‌ها، مقابله با تروریسم سـایبری، مقابله با جرایم سایبری، مقابله با محدود کردن اینترنت، گرایش‌های جدیـد ضد ارزش‌های پایه‌ای آمریکا و ... وجود ندارد.[1]

- **جان میلر: چالش‌های دیپلماسی سایبری آمریکا از منظر فناوری اطلاعات**

جان میلر معاون شورای صنعت فناوری اطلاعات[2] در امور سیاسـت جهـانی و امنیت سایبری است. شورای صنعت فنـاوری اطلاعـات نماینـدهٔ بـیش از شصت کمپانی بزرگ در حـوزهٔ فنـاوری اطلاعـات و ارتباطـات، از جملـه

1. U. S. Cyber Diplomacy in an Era of Growing Threats, 2018
2. "Information Technology Industry" Council

نـرم‌افـزار و سـخت‌افـزار، خـدمات دیجیتـال، شـبکه، امنیـت سـایبری، و کمپانی‌های اینترنت، است که عمدهٔ این کمپانی‌ها در مقیاس جهانی فعالیـت می‌کنند. این شورا از تمامی فعالیت‌ها و سیاست‌های عمـومی در ارتبـاط بـا نوآوری، دسترسی آزاد به بازارهای فعلی و در حال ظهـور، توسـعهٔ اقتصـاد دیجیتال، حق انتخاب مشتری و حریم خصوصی وی و ... حمایت می‌کند.

ـــ اهمیت جریان فرامرزی داده‌ها در صنعت فناوری اطلاعـات در فضـای سایبری: کلیدی‌ترین مفهوم بـرای صـنعت فنـاوری اطلاعـات، مفهـوم «داده» است و تمام تلاش این صنعت، نهادینه ساختن اهمیت جریـان فرامـرزی داده در اقتصاد جهانی در هر گونه سیاست‌گذاری و برنامه‌ریزی دولـت در حـوزهٔ اینترنـت و فضـای سـایبری اسـت. در واقـع داده، محـور و تقـاطعِ تمـامی فعالیت‌های نوآوری و فناوری است که موجب افزایش مزایا و فواید اینترنـت، از جمله پردازش ابری، اینترنت اشیا، داده‌های کـلان، هـوش مصـنوعی و ...، می‌شود. از این رو اصل «جریان بین‌المللی داده‌ها» به صـورت آزاد و سـریع و نامحدود برای این صـنعت و هـر کسـب‌وکـاری کـه در سـطوح منطقـه‌ای و بین‌المللی فعالیت می‌کند، امری ضروری است. لذا می‌توان اسـتدلال کـرد کـه تجارت بین‌الملل به طور وسیع به جریان فرامرزی داده‌ها وابسته است.

ـــ چالش‌های صنعت فناوری اطلاعات آمریکا در عرصهٔ فضای سایبری: در سال‌های اخیر و به عنوان گرایش‌های نوین در سیاست سایبری جهانی، دولت‌ها و کشورها اصل جریان فرامرزی داده‌ها را با چالش‌هایی اساسی مواجه ساخته‌اند و در بسیاری از موارد، با سیاست‌گذاری‌های سایبری اقدام به ایجاد دیوارهای مجازی[1] در مرزهای خود کرده‌اند که به طور کلی می‌توان آن‌ها را در مقولاتی همچون استانداردسازی، مقررات‌گذاری، قوانینِ حفاظت

1. Virtual Walls

از دیتاها و حریم خصوصی، آیین‌نامه‌های امنیت سایبری و ... تقسیم کرد که همگی چالش‌هایی اساسی در مسیر اصل جریان فرامرزی داده‌ها، در مقابل کمپانی‌های صنعت فناوری اطلاعات قرار داده‌اند. می‌توان این دیوارهای مجازی را، که عمدتاً موانع تجاری زیادی برای کمپانی‌های آمریکایی ایجاد کرده‌اند و اعتماد و همکاری ضروری برای اقتصاد دیجیتال جهانی را به چالش کشیده‌اند، به چهار دسته تقسیم کرد:

۱. محلی‌سازی اجباری: محلی‌سازی یا بومی‌سازی اجباری به صورت کلی به سیاست‌ها و الزاماتی اشاره دارد که کمپانی آی‌تی را وادار به انتقال همه یا بخشی از فعالیت‌های تجاری یا کسب‌وکار خود به داخل مرزهای کشور مقصد، به عنوان پیش‌شرط دسترسی به بازار آن کشور، می‌کند که از جمله شامل ذخیره یا پردازش داده‌ها در سرورها یا دیتاسنترهای داخل کشور می‌شود. سیاست محلی‌سازی اجباری، که در سال‌های اخیر بسیاری از کشورها آن را دنبال می‌کنند، خود شامل هفت الزام مرتبط با داده است که تماماً ناقض اصل جریان فرامرزی داده‌ها و نیز برخلاف منافع کمپانی‌های آمریکایی در عرصهٔ فناوری اطلاعات است. این الزامات هفت‌گانه عبارت‌اند از:

الف. الزامات محلی‌سازی داده‌ها: به این معنا که کمپانی‌ها باید الزاماً داده‌ها را در داخل یک کشور ذخیره و پردازش و اداره کنند؛ ب. الزامات محتوای محلی:[1] بدین معنا که میزان مشخصی از ارزش نهایی کالا یا خدمات الزاماً از منابع داخلی، چه از طریق خرید آن از منابع محلی یا تولید آن در داخل، به دست آمده باشد؛ ج. الزامات انتقال فناوری: الزام اینکه کمپانی‌ها مالکیت فکری فناوری را مستقیم یا از طریق آژانس‌های دولتی به داخل منتقل کنند؛ د. الزامات حضور به صورت محلی: به این معنا که کمپانی‌ها باید به تأسیس دفاتر محلی در آن کشور اقدام کنند یا از طریق تسهیلات و

1. Local Content Requirements

زیرساخت‌ها یا عوامل آن کشور، به تولید کالا و خدمات بپردازند؛ ه. الزامات تأییدیهٔ ارزیابی و استانداردها: به این معنا که کمپانی‌ها باید منطبق بر استاندارد منحصر به آن کشور، و نه استاندارد بین‌المللی، باشند یا از کانال ارزیابی‌های بیش از حد سخت و محدود آن‌ها بگذرند، نه از ارزیابی‌ها و استانداردهای بین‌المللی که موجب ایجاد این فناوری‌ها و نوآوری‌ها شده است؛ و. الزامات نوآوری بومی:[1] به این معنا که کمپانی‌ها باید از تکنولوژی بومی یا توسعه‌یافته در داخل آن کشور استفاده کنند؛ ۷. الزام استخدام داخلی: اینکه کمپانی‌ها الزاماً درصد خاصی از نیروی ماهر خود را از داخل آن کشور تأمین کنند.

۲. استانداردهای پنهان یا مقررات‌گذاری خاص کشورها: کشورهای مختلف به طور روزافزون با استدلال‌های دفاع از حریم خصوصی یا حفظ امنیت سایبری، مقرراتی وضع می‌کنند یا استانداردهایی دارند که برخلاف استانداردها و قوانین بین‌المللی است. این قوانین و مقررات عمدتاً چندلایه است که گاه همپوشانی‌های زیادی با یکدیگر دارند. مواجههٔ کمپانی‌های فناوری اطلاعات، که به صورت بین‌المللی فعالیت می‌کنند، علاوه بر محدودیت‌هایی که ایجاد می‌کنند، مستلزم اخذ تأییدیه‌های محلی و نیز عبور از کانال‌های ارزیابی محلی‌اند که با استانداردهای ارزیابی بین‌المللی سازگار نیستند. از جملهٔ این مقررات‌گذاری‌ها می‌توان به محدودیت‌های مربوط به انتقال داده‌های خصوصی اشاره کرد که خطرات بزرگی را متوجه جریان فرامرزی داده‌ها می‌کند.

۳. بازرسی‌ها و الزامات تست‌های امنیت سایبری برای کمپانی‌های خصوصی: در بسیاری از کشورها و حتی مناطق مهم، گرایش زیادی به ایجاد بازرسی‌های فنی بومی، تست‌های امنیت سایبری ملی و ... وجود دارد. الزام

1. Indigenous Innovation Requirements

کمپانی‌ها برای أخذ گواهینامهٔ انیسا[1] در اتحادیهٔ اروپا یا گواهینامهٔ «امنیت بومی» دپارتمان ارتباطات راه دور کشور هندوستان و ده‌ها مورد مشابه دیگر از جمله الزاماتی است که در مناطق مختلف جهان به کمپانی‌های صنعت فناوری اطلاعات ایالات متحده تحمیل می‌شود. در بسیاری از این بازرسی‌ها و گواهینامه‌ها و تأییدیه‌ها، عمدتاً به جای استانداردهای بین‌المللی، از قواعد و مقررات سخت و محدود بومی استفاده شده است. ضمن آنکه بر اساس تجارب اخیر، این استانداردها و گواهینامه‌ها در ارتباط با کمپانی‌های خصوصی بسیار سخت و تهاجمی عمل می‌کنند.

۴. اعمال حاکمیت قوانین بر فناوری و خدمات نوآوری: نگرانیِ در حال ظهور و جدی دیگر، اعمال قوانین قدیمی بر فناوری و نوآوری‌های جدید است. این مسئله به طور مشخص تأثیرات گسترده‌ای بر اقتصاد دیجیتال می‌گذارد و همین طور آثاری منفی و ناخواسته بر نوآوری و امنیت و دیگر ابعاد فضای سایبری خواهد داشت. دو نمونه از مصادیق اعمال قوانین قدیمی بر فناوری‌های نوین عبارت است از: توسعهٔ قوانین «کنترل صادرات» بر محصولات امنیت سایبری یا اعمال قوانین مبتنی بر بازار سنتی بر فروش محصولات و خدمات آنلاین.

ـــ راهبردهای مقابله با چالش‌های صنعت فناوری اطلاعات آمریکا: نکتهٔ بسیار حائز اهمیت این است که تهدیدات مربوط به صنعت فناوری اطلاعات آمریکا تنها مختص به معدودی از کشورها، مناطق یا اقتصادهای در حال ظهور نیست. این تهدیدها در همه جا وجود دارند: در روسیه،[2] چین،[3]

1. EU Agency for Network and Information Security (ENISA)
2. Package Laws (374-FZ and 375-FZ)
3. China's Cybersecurity Law (CSL)

اقتصادهای بزرگ و کلان همچون اتحادیهٔ اروپا[1] و ژاپن یا حتی اقتصادهای در حال ظهور همچون هندوستان[2] و برزیل. با توجه به اهمیت داده در صنعت فناوری اطلاعات، ایالات متحده باید از تمامی ابزارهای دیپلماتیک برای پیشبرد و نهادینه ساختن اصل جریان فرامرزیِ داده بهره جوید. اگرچه قانون دیپلماسی سایبری آمریکا (۲۰۱۷) بسیاری از مؤلفه‌های مربوط به صنعت فناوری اطلاعات، همچون ترویج جریان آزاد داده، نوآوری، شفافیت اقتصادی و ...، را پیش‌بینی می‌کند، اما ایالات متحده نیازمند به «نقشهٔ راه» برای عملیاتی کردن این اصول و مؤلفه‌هاست. بر این اساس، صنعت فناوری اطلاعات برای عملیاتی کردن آن‌ها، علاوه بر آنچه در دیپلماسی سایبری پیش‌بینی شده است، سه راهکار جدید ارائه می‌دهد:

۱. تلاش برای ارائه و نهادینه‌سازی «استاندارد بین‌المللی» از امنیت سایبری: برای مقابله با گرایش روزافزون کشورهای مختلف، که از استانداردهای امنیتی محلی، تدوین پروتکل‌های بومی، تأییدیه و گواهینامه‌های ملی در زمینهٔ امنیت سایبری حمایت می‌کنند، بدیهی است که ایالات متحده به یک استراتژی ملی قوی و خلاقانه و مبسوط نیاز دارد که هم صنعت و هم دولت از آنان حمایت کنند و هر دو در جهت توسعه و پیشرفت بین‌المللی آن همکاری داشته باشند.

۲. ابتکار یک چارچوب امنیت سایبری در سطح جهانی: استراتژی ملی که پیش‌تر به آن اشاره شد، می‌تواند به عنوان یک چارچوب امنیت سایبری در سطح جهانی دنبال شود. این چارچوب، که در مقابل هر گونه گرایش برای محدودسازی جریان فرامرزیِ داده قرار می‌گیرد، باید با مشارکت بخش خصوصی و دولت، گویای ارزش‌ها و هنجارهای نوین مرتبط با

---

1. ePrivacy Regulation (ePR), Data Protection Law, EU Cybersecurity Measures
2. India's Telegraph Rules

فناوری و نوآوری باشد و به دلیل انعطاف‌پذیری‌اش به رونق آن منجر شود. این چارچوب با پیگیری‌های ایالات متحده در سطح جهان، باید به عنوان استانداردی جهانی، به زبان مشترک رهبران و سیاست‌گذاران تبدیل گردد. تنها از این طریق است که ایالات متحده می‌تواند رهبری خود را در عرصهٔ سایبری و مؤلفه‌های مرتبط با آن حفظ کند.

۳. پیگیری توافقات چندجانبه در کنار رویکرد توافقات دوجانبه: برای پیگیری چارچوب امنیت سایبری در مقیاس جهانی، ایالات متحده علاوه بر رویکردها و گفت‌وگوهای دوجانبه با کشورهای همسو و شرکای استراتژیک، از بسترهای بین‌المللی زیادی، همچون گروه ۷، گروه ۲۰، سازمان همکاری اقتصادی آسیا ـ اقیانوسیه (اَپک) و ...، برخوردار است که باید با جدیت به آن توجه کرد.[1]

- **مایکل سولمیر: چالش‌های دیپلماسی سایبری آمریکا از منظر دفاعی**

مایکل سولمیر، رئیس پروژهٔ امنیت سایبری مرکز بلفر[2] وابسته به مدرسهٔ دولتی جان اف کندی در دانشگاه هاروارد و رئیس سابق برنامه‌ریزی و اجرای سیاست سایبری وزارت دفاع آمریکا است. وی به عنوان کارشناس در حوزهٔ دفاعی و امنیت سایبری، مهم‌ترین نیاز ایالات متحده را در حوزهٔ سایبری در سه دسته تقسیم‌بندی می‌کند:

۱. ارزیابی فضای بین‌الملل و تأکید بر ضرورت اتخاذ رویکرد دیپلماتیک: در ارتباط با فضای سایبری، ایالات متحده آمریکا در حال حاضر بیش از هر زمان دیگری نیازمند اتخاذ رویکردهای دیپلماتیک است. این ضرورت از آنجا ناشی می‌شود که کمپانی‌های آمریکایی در حوزه‌های مختلف در مقیاس جهانی

1. U. S. Cyber Diplomacy in an Era of Growing Threats, 2018
2. Belfer Center

عمل می‌کنند و به رغم سرمایه‌گذاری‌های کلانی که در زمینهٔ دفاع سایبری و افزایش ظرفیت‌های سایبری صورت گرفته است، هکرها و بزهکاران سایبری همچنان سیستم‌های ایالات متحده و شرکای آن را هک می‌کنند. از طرفی هنوز در مقیاس جهانی، ارزش‌ها و هنجارها و نُرم‌های استاندارد برای رفتار دولت‌ها وجود ندارد. در حالی که ایالات متحده از اینترنت باز، جریان آزاد اطلاعات و الگوی حکمرانی چندذی‌نفعی حمایت می‌کند، در بین کشورهای مختلف نظریات و دیدگاه‌های متفاوتی دربارهٔ نقش اینترنت در جامعه وجود دارد. از این رو نقش دیپلماسی بسیار حساس و کلیدی و الزامی است تا بتواند ارزش‌های آمریکایی را در این خصوص نهادینه و در عرصهٔ جهانی اعمال کند. در غیر این صورت الگوی جایگزین، مدل بسته حکمرانی دولت‌ها و نظارت و مانیتور محتواهایی است که از سوی شهروندان آن‌ها در بستر اینترنت جریان می‌یابد. این الگو به طور خاص مطلوبِ چین و روسیه است.

از این رو وزارت امور خارجه باید ادارهٔ مستقل در امور سایبری داشته باشد و به طور هدفمند دو هدف عمده را پیش ببرد: ۱. به طور مجزا تمام توجه و تلاش‌های خود را روی تمهیدات و توافقات دوجانبه متمرکز سازد؛ ۲. از منافع ایالات متحده در نهادها و سازمان‌های بین‌المللی حمایت کند.

۲. بازدارندگی و چالش‌های فَراروی آن: ایالات متحده، برای پیشبرد دیپلماسی سایبری، باید تا بیشترین حد ممکن دیپلمات‌های خود را به قدرت و نفوذ و سایر حمایت‌های فنی مجهز کند. یکی از راه‌های تجهیز دیپلمات‌ها افزایش بازدارندگی چندوجهی آمریکا در مقابل حملات هکرها و مجرمان سایبری دولتی و غیردولتی علیه زیرساخت‌های کلیدی است، زیرا آمریکا فقط با یک الگو یا یک شیوه از هک و ... مواجه نیست. مقابله با هکرها و مجرمان سایبری اگر بتواند به صورت جمعی و به اتفاق سایر شرکا دنبال شود، بسیار ایدئال خواهد بود.

البته نمی‌توان بر بازدارندگی در برابر تهدیدات سایبری شرط‌بندی کرد و در این زمینه آمریکا باید واقع‌بین باشد و انتظارات خود را در این زمینه مشخص کند. برای مثال، در برابر هزاران موشک هسته‌ای آمادهٔ پرتاب، بازدارندگی کمترین گزینه ممکن است. اما این دربارهٔ فضای سایبری صادق نیست؛ زیرا در این عرصه، علاوه بر بازدارندگی، گزینه‌های دیگری نیز وجود دارد که باید از آن‌ها استفاده کرد. بسیار مهم است که ایالات متحده از استراتژی جلوگیری و پیشگیری از حملات دشمنان نیز بهره جوید. در واقع نباید اجازه داد که دشمنان به مرحله‌ای برسند که بتوانند حملات سایبری به ایالات متحده داشته باشند. موفقیت در حوزهٔ امنیت سایبری باید در گذر زمان تقویت شود و بیش از پیش موجب تقویت و پشتوانهٔ تلاش‌های دیپلماتیک مضاعف قرار گیرد.

۳. امنیت سایبری، فعالیت‌های اطلاعاتی در چارچوب انتخابات آمریکا: این امر به خصوص با توجه به کمپین سایبری روسیه علیه انتخابات ریاست‌جمهوری ایالات متحده در سال ۲۰۱۶ حائز اهمیت است. در این خصوص، مسئلهٔ اول جلوگیری از تکرار آن نه‌تنها در آمریکا، بلکه در تمامی کشورهای دموکراسی‌خواه است که انتخابات آن‌ها بالقوه مستعد کمپین مشابه از سوی روسیه است. مسئلهٔ دوم، تحمیل هزینه به روسیه بابت این نوع رفتار سایبری است، نه به نحوی که برای دولتمردان آن‌ها قابل پیش‌بینی باشد، بلکه به صورتی که برایشان مهم و قابل توجه تلقی شود.

با این حال، همان طور که قبلاً گفته شد، آمریکا نمی‌تواند تنها به بازدارندگی اکتفا کند. در واقع باید به مرحله‌ای از اطمینان دست یافت که ایالات متحده ظرفیت‌ها و ابزارهای قابل توجهی روی میز داشته باشد تا از تکرار چنین رفتارهایی قبل از وقوع، پیشگیری و ممانعت کند. در نهایت نیز آمریکا باید سیستم‌ها و شبکه‌های خود را به لحاظ مقاومت و

پایداری در برابر حملات سایبری مشابه محکم‌تر و استوارتر سازد.[1]

سند استراتژی ملی سایبری آمریکا (۲۰۱۸)

سند استراتژی ملی سایبری آمریکا، که اواخر ۲۰۱۸ به فرمان ریاست‌جمهوری آمریکا ابلاغ شد، بر مبنای «راهبرد امنیت ملی آمریکا در ۲۰۱۷» استوار است و در آن ارکان اصلی، اهداف، راهبردها و اولویت‌های این کشور به منظور تأمین منافع و امنیت ملی آمریکا در حوزهٔ سایبری، به خصوص با تأکید و تمرکز بر کشورهای رقیب، تعیین شده است. سند استراتژی ملی سایبری آمریکا به لحاظ ماهوی از دو بُعد اهمیت دارد: ۱. در آن با اذعان به پایان اشرافیت راهبردی آمریکا در عرصهٔ سایبری، بر چالش‌های جدید این کشور در حوزهٔ قابلیت‌های زمینی، هوایی، دریایی و فضایی آمریکا از طریق اقدامات مخرب رقبا تأکید شده است؛ ۲. این سند به نوعی بازگشت ایالات متحده از رویکرد دیپلماتیک (مبتنی بر قانون دیپلماسی سایبری مصوب ۲۰۱۷) به رویکرد امنیتی ـ دفاعی ـ تهاجمی به عرصهٔ سایبری (در دورهٔ حاکمیت دولت دونالد ترامپ) محسوب می‌شود.

در ادبیات امنیت ملی آمریکا، موضوع امنیت سایبری به عنوان یک عنصر اساسی جایگاهی محوری دارد و دقیقاً بر اساس و منطبق با آن، چهار رکن اصلی برای آن تدوین شده که هر رکن نیز مبتنی بر چند راهبرد است:

رکن اول، حفاظت از مردم و سرزمین و سبک زندگی آمریکایی: بر اساس این رکن، تمامی مخاطرات امنیت سایبری این کشور باید از طریق حفاظت از شبکه‌ها و سیستم‌های اطلاعاتی و ارتباطی مدیریت شوند. این رکن خود سه راهبرد دارد: ۱. ایمن‌سازی شبکه‌ها و اطلاعات، ۲. ایمن‌سازی زیرساخت‌های

1. U. S. Cyber Diplomacy in an Era of Growing Threats, 2018

حیاتی، و ۳. مبارزه با جرایم سایبری و بهبود گزارش‌دهی رخدادها.

رکن دوم، ارتقای رونق آمریکایی‌ها: بر اساس این رکن، نفوذ و اشرافیت راهبردی آمریکا در اکوسیستم فناوری و نوآوری فضای سایبری باید حفظ شود و توسعه یابد و این امر از طریق تقویت اقتصاد دیجیتال ایمن و پویا و تحکیم نوآوری‌های قوی صورت خواهد پذیرفت. این رکن نیز خود بر دو راهبرد استوار است: ۱. تقویت یک اقتصاد دیجیتال پویا و مقاوم، ۲. تقویت و حفاظت از قوهٔ ابتکار و نبوغ ایالات متحده.

رکن سوم، حفظ صلح از طریق تقویت نقاط قوت: بر اساس این رکن، ایالات متحده باید به صورت پیشگیرانه به شناسایی و مقابله و تضعیف تمامی رفتارها و فعالیت‌های بی‌ثبات‌کنندهٔ مغایر با منافع ملی این کشور در فضای سایبری بپردازد تا اشرافیت راهبردی این کشور همواره حفظ شود. در این بخش، همچنین فضای سایبری در کنار نیروهای نظامی، دفاعی، فضایی، اتمی و اطلاعاتی، به عنوان یکی از قابلیت‌های مهم آمریکا برای حفظ صلح مطرح گردیده است که باید همواره تقویت شود. این رکن خود دارای دو راهبرد است: ۱. ارتقای ثبات سایبری از طریق هنجارهای ناظر بر رفتار مسئولانهٔ دولت‌ها،۲. انتساب و پیشگیری از رفتارهای غیرقابل‌پذیرش در فضای سایبری.

رکن چهارم، گسترش نفوذ آمریکایی: حفظ و گسترش نفوذ آمریکایی ناظر بر توسعهٔ ارزش‌های این کشور در ابعاد جهانی است. این ارزش‌ها عمدتاً ناظر بر دو اصل «باز بودن» اینترنت و «یکپارچگی و امنیت و قابل اتکا بودن» آن است. این رکن نیز خود دو راهبرد دارد: ۱. ترویج اینترنت باز، تعاملی، قابل اتکا و امن، ۲. ایجاد ظرفیت‌های بین‌المللی سایبری.[1]

1. National Cyber Strategy of United States of America, September 2018

جمع‌بندی و نتیجه‌گیری این فصل

برآیند کلی دیپلماسی سایبری آمریکا بر اساس تمامی اسناد راهبردی این کشور در ارتباط با فضای سایبری را می‌توان در قالب سه گزاره خلاصه کرد: ۱. تداوم رونق و شکوفایی نظام سیاسی، اقتصادی و اجتماعی آمریکا و نیز چشم‌انداز نفوذ آتی این کشور در عرصهٔ جهانی به طور اساسی به اینترنت جهانی امن و آزاد و پایدار وابسته است؛ ۲. اشرافیت راهبردی آمریکا در عرصهٔ فضای سایبری به طور وثیقی به جریان فرامرزی داده‌ها به صورت آزاد وابسته است، با این حال این موضوع هم از سوی هم‌پیمانان آمریکا، به عنوان مثال اتحادیهٔ اروپا، هند و ... در قالب جنبش «محلی‌سازی داده‌ها» و هم از سوی رقبای این کشور، به عنوان مثال چین و روسیه، به چالش کشیده شده است؛ ۳. قابلیت‌ها و توانمندی‌های بازدارندگی ایالات متحده، به خصوص در ارتباط با زیرساخت‌های کلیدی به شدت تضعیف شده و در معرض خطر حملات سایبری مخرب از جمله از سوی کشورهای رقیب، گروه‌های تروریستی و نیز گروه‌های تبهکار قرار گرفته است.

بر این اساس، استراتژی‌های پاسخ ایالات متحده آمریکا برای مواجهه با چالش‌های عرصهٔ سایبری فوق‌الذکر را می‌توان حول سه محور یا رکن اساسی توضیح داد: ۱. تلاش برای حفظ و گسترش ارزش‌ها و هنجارها و قوانین ملی این کشور در فضای سایبری در مقیاس جهانی؛ ۲. انجام اقدامات بازدارنده در برابر تهدیدات حملات سایبری از طریق تعمیم و تسرّی قوانین بین‌المللی فعلی به فضای سایبری؛ و ۳. در نهایت، پاسخ عملیاتی به حملات صورت‌گرفته به منافع این کشور در حوزهٔ سایبری. مهم‌ترین نکتهٔ برجسته و قابل توجه در رویکرد سایبری ایالات متحده، تعمیم قانون مقابلهٔ نظامی به عرصهٔ سایبری است، به نحوی که هر گونه حملهٔ سایبری به این کشور به خصوص اگر

معطوف به زیرساخت‌های کلیدی این کشور باشد، به عنوان «اعلان جنگ» تلقی می‌شود و می‌تواند با پاسخ نظامی از سوی این کشور مواجه شود.[1]

بر اساس سه رکن اساسی گفته‌شده، مسیر تحولات صورت‌گرفته را در ارتباط با دیپلماسی سایبری آمریکا می‌توان در دو بازهٔ زمانی تقسیم کرد:

۱. از سال ۲۰۱۱ تا ۲۰۱۷: این دوره عمدتاً تحت تأثیر دولت باراک اوباماست که مبتنی بر رویکرد دیپلماسی است و دولت ایالات متحده می‌کوشد از طریق سازوکارهای دیپلماتیک و در چارچوب تعاملات چندجانبهٔ منطقه‌ای و بین‌المللی، از جمله از طریق سازمان‌های بین‌المللی یا تعاملات دوجانبه، مسائل را پیش ببرد.

در این مقطع، با هدف پیگیری دیپلماسی سایبری در عرصهٔ منطقه‌ای و بین‌المللی، وزارت خارجهٔ ایالات متحده آمریکا نخستین کشوری بود که به صورت خاص، ادارهٔ هماهنگ‌کنندهٔ امور سایبری را ــ منحصراً به عنوان هماهنگ‌کنندهٔ امور سایبری ــ راه‌اندازی کرد. این وزارتخانه همچنین کریستوفر پینتر را به عنوان نخستین دیپلمات سایبری منصوب کرد که در واقع نخستین دیپلمات سایبری در جهان نیز محسوب می‌شد.

ادارهٔ هماهنگ‌کنندهٔ امور سایبری وزارت خارجهٔ آمریکا به طور مشخص دارای پنج کارکرد کلیدی بود: ۱. هماهنگی و مدیریت «تعاملات جهانی» وزارت امور خارجهٔ آمریکا در امور سایبری، ۲. خدمت به عنوان رابط وزارت امور خارجه با کاخ سفید و سایر ادارات و سازمان‌های فدرال در حوزهٔ سایبری، ۳. مشاوره دادن به وزیر و معاونان وزارت امور خارجه در زمینهٔ مسائل سایبری و تعاملات خارجی آمریکا در این زمینه، ۴. خدمت به عنوان رابط وزارت امور خارجه با بخش‌های خصوصی و

1. U. S. Cyber Diplomacy in an Era of Growing Threats, 2018

عمـومی در زمینـهٔ مسـائل سـایبری، و ۵. هماهنـگ‌کننـدهٔ امـور دفـاتر و نمایندگی‌های منطقه‌ای وزارتخانهٔ مرتبط به امور سایبری.[1]

۲. از سال ۲۰۱۷ تا زمان حاضر: این دوره عمدتاً تحت تأثیر روی کار آمدن دونالد ترامپ در این کشور است که مهم‌ترین ویژگی آن در پیش گرفتن رویکرد دفاعی ـ تهاجمی در زمینهٔ مسائل سایبری می‌باشد. مهم‌ترین نماد رویکرد جدید ایالات متحده، تقلیل ادارهٔ امـور سـایبری وزارت امـور خارجـهٔ ایـن کشـور از واحدی مستقل، که یک مقام عالی‌رتبه در سـطح سـفیر آن را اداره مـی‌کنـد، بـه واحدی زیرمجموعه است که وزیر امور خارجه مسئول آن را تعیین می‌سازد.

سویهٔ دیگر این تغییرِ رویکرد، اولویـت مسـائل تجـاری و اقتصـادی در سیاست خارجی ایالات متحده آمریکا در دوران دونالد ترامپ است کـه بـه تبع آن، دیپلماسی سایبری این کشور را نیز تحت تأثیر قـرار داده اسـت. بـر این اساس، هدف اصلی دولت جدید آمریکا کسب بیشترین منافع اقتصـادی و تجاری در تعاملات خارجی این کشور مـی‌باشـد تـا تـرویج ارزش‌هـای بنیادین آن، از جمله آزادی و باز بودن اینترنت و دیگر موارد مشابه. در ایـن خصوص، قابل ذکر است که دولت ترامپ در سیاست‌های مـدون خـود بـه نوعی آشکار ساخت که این کشور دیگـر دسـتور کـار «آزادی اینترنـت» را پیش نخواهد برد. برای مثال، پیش‌نویس اولیهٔ دسـتورالعمل اجرایـی امنیـت سایبری این کشور شامل بخشی با عنوان «آزادی و حاکمیت اینترنـت» بـود که وزارت خارجهٔ آمریکا را به تهیهٔ گزارشی دربارهٔ اقدامات حمایتی از ایـن فرایند چندذی‌نفعی در سایر کشورها برای رئیس‌جمهور ملزم می‌کرد. با این حال، این بخش در ویرایش نسخهٔ نهایی حذف شد.[2]

دربارهٔ دلایل بازگشت آمریکا به رویکرد دفاعی ـ تهاجمی علاوه بر

1. US State Department Website, 2017 2. Paul R., 2017

رویکرد شخصی رئیس‌جمهوری فعلی این کشور، می‌توان دلایل دیگری را نیز برشمرد:

۱. ایالات متحده آمریکا کشورهای چین و روسیه را به عنوان دو رقیب بسیار قدرتمند می‌بیند که از سه طریق تهدیدهایی بسیار جدی علیه آمریکا به شمار می‌آیند: قانون‌گذاری‌های به‌روز در ارتباط با مسائل سایبری با تأکید بر اصل حاکمیت مطلق[1] حکومت‌های ملی؛ دیپلماسی بین‌المللی و ائتلاف‌سازی با کشورهای درحال‌توسعه؛ و فعالیت‌های سرویس‌های اطلاعاتی با هدف سرقت اسرار تجاری، مداخله در روندها و فرایندها و اختلال در نظام سیاسی آمریکا. علاوه بر این، چالش جدی‌تر آمریکا در عرصهٔ دیپلماسی سایبری، چالش فناوری (از جمله فناوری نسل پنج و هوش مصنوعی شرکت‌های فنّاور و کمپانی‌های) چین است که علاوه بر تیره ساختن چشم‌انداز کسب تریلیون‌ها دلار از سوی شرکت‌های آمریکایی، به طور شگفت‌انگیزی اشرافیت راهبردی آمریکا در عرصهٔ سایبری، پیش‌افتادگی فناوری آمریکایی، امنیت زیرساخت‌های ارتباطی و اطلاعاتی آمریکا و نیز هم‌پیمانان و متحدان نزدیک این کشور را به چالش کشیده است.

۲. در کنار روسیه و چین، کشورهای ایران و کرهٔ شمالی نیز به عنوان قدرت‌های نوظهور در عرصهٔ سایبری محسوب می‌شوند که به زعم دولت آمریکا، تا کنون تهدیدات سایبری جدی علیه زیرساخت‌های کلیدی این کشور یا هم‌پیمانان آن عملیاتی کرده‌اند.

۳. ایالات متحده آمریکا تهدیدهای سایبری را فراتر از دولت‌ها می‌داند. در واقع در ارتباط با مسائل سایبری، بازیگران غیردولتی گاه قوی‌تر از بازیگران دولتی ظاهر می‌شوند و عمدتاً در نقش پراکسی (نیابتی) عمل می‌کنند. در واقع یکی از دلایل بازگشت آمریکا به رویکرد دفاعی ـ تهاجمی همین موضوع است.

---

1. Absolute Sovereignty

بر این اساس، در مجموع به نظر می‌رسد رویکرد دیپلماسی سایبری آمریکا در گذشته نتوانسته است پاسخگوی انتظارات ایالات متحده در خصوص تضمین نفوذ جهانی این کشور باشد. همچنین در مصون ماندن زیرساخت‌های کلیدی این کشور از روند روزافزون تهدیدات سایبری کشورها و حتی بازیگران غیردولتی موفق نبوده است. لذا به نظر می‌رسد رویکرد دیپلماتیک آمریکا تنها به ابزاری برای متحد کردن کشورهای هم‌پیمانش علیه بازیگران غیرمطلوب در ادبیات سیاسی این کشور تقلیل یابد و در عوض، ایالات متحده خود از طریق سازوکارهای تهاجمی، همچون اعمال تحریم یا حتی حملهٔ نظامی، به پیگیری و اعمال منافع ملی خود در حوزهٔ سایبری در مقیاس جهانی اقدام کند.

منابع

Cyber Diplomacy Act of 2017, House of Representative, United States of America.

National Cyber Strategy of United States of America, September 2018.

Office of the Coordinator for Cyber Issues, Christopher Painter www.cisac.fsi.stanford.edu.

US Cyber Diplomacy in the Era of Growing Threats (2018), Hearing before the Committee of Foreign Affairs, House of Representative, Available via the World Wide Web: http://www.foreignaffairs.house.gov/ or http://www. gpo. gov/fdsys/.

US State Department, Available via the World Wide Web: https://www.state.gov/.

US Presidential Executive Order 13800 on Strengthening the Cyber Security of Federal Networks and Infrastructure.

White House (2011), International Strategy for Cyberspace, Washington, DC.

White House (2015, September 25), FACT SHEET: President Xi Jinping's State Visit to the United States, Washington, DC.

White House (2016), International Cyberspace Policy Strategy, Washington, DC.

فصل پنجم

چین و گذار به دیپلماسی سایبری مدبرانه

درآمد

دیپلماسی سایبری چین از ابعاد و زوایای مختلف حائز اهمیت ویژه است. چین به عنوان یک قدرت سیاسی ـ اقتصادی نوظهور، رقیب نوپای نظام سرمایه‌داری به رهبری آمریکا محسوب می‌شود و چندین سال است که به پشتوانهٔ توسعهٔ اقتصادی و قدرت سرمایه‌گذاری‌های کلان خود در اقصی نقاط جهان، پابه‌پای روسیه قدرت‌های غربی و در رأس آن‌ها آمریکا را به چالش می‌کشد. این تقابل سیاسی، نظامی، تجاری و اقتصادی در حوزه‌های کلاسیک سیاست بین‌الملل امروزه بُعد جدیدی به خود گرفته و با قدرت گرفتن فناوری‌های اطلاعاتی و ارتباطی چینی، به عرصهٔ سایبری نیز کشیده شده است.

چین در دوران اخیر ـــ دوران حکومت شی جین‌پینگ ـ از لاک سیاست‌های دفاعی خود، که عمدتاً مبتنی بر امنیت داخلی و تضمین حاکمیت ملی بود، خارج شده و برنامه‌ها و سیاست نفوذ سایبری در عرصهٔ بین‌المللی و جهانی را به طور هم‌زمان از طریق یک استراتژی سه‌وجهی دنبال می‌کند: ۱. تهاجمی؛ از طریق نفوذ در زیرساخت‌های اطلاعاتی و ارتباطی کشورهای رقیب، به خصوص آمریکا و اروپا. این سیاست به طور خاص به

دنبال توسعهٔ توانمندی‌ها و ظرفیت‌های تهاجمی با هدف جاسوسی سایبری، خنثی‌سازی حملات سایبری و رسیدن به درجه‌ای از اقتدار سایبری است که بتواند سیستم‌های انفورماتیک و زیرساخت‌های ارتباطی و اطلاعاتی رقبای خود را در هر لحظه‌ای که اراده نماید، فلج کند. ۲. تجاری ـ اقتصادی؛ از طریق سرمایه‌گذاری گسترده در زیرساخت‌های کشورها و مناطق هدف به خصوص اروپا، آفریقا، خاورمیانه، آسیای میانه و آمریکای لاتین. این سیاست که به طور خاص از طریق برنامهٔ مشهور جادهٔ ابریشم جدید موسوم به «یک کمربند و یک جاده» دنبال می‌شود به دنبال ایجاد نوعی وابستگی سایبری کشورهای هدف به خود از طریق جایگزینی فناوری چینی با فناوری غربی (به خصوص آمریکایی) است. ۳. استانداردسازی؛ از طریق مشارکت جدی در تعریف استانداردها و پروتکل‌های جهانی فناوری (نرم‌افزار، سخت‌افزار و شبکه‌های مدرن). این سیاست به طور خاص از طریق حضور پُرتعداد و مؤثر تیم‌های سیاسی ـ فنی در نشست‌ها و همایش‌های فنی تعیین استانداردهای فناوری در سطوح جهانی دنبال می‌شود. از دیدگاه چین، کنترل یک استاندارد به معنای تصاحب سهم بزرگی از ارزش بازار فناوری مرتبط با آن است و به همین دلیل، رقابت سخت و حتی پیشی گرفتن چین در استاندارد فناوری نسل پنجم (5G)، فناوری هوش مصنوعی، اینترنت اشیا و ...، نگرانی‌های گسترده‌ای را در غرب ایجاد کرده است. در هر سه وجه استراتژی فوق شرکت‌های فناوری چینی از جمله هوآوی و زدتی‌ای[1] بازوان قدرتمند این کشور محسوب می‌شوند.

برای فهم بهتر ابعاد، محورها، استراتژی‌ها و رویکردهای عملیاتی دیپلماسی سایبری چین، این موضوع در ادامه در یک بستر تاریخی به

1. ZTE

خصوص در قالب سیر مواجههٔ این کشور با استراتژی‌های مقابله‌جویانهٔ آمریکا مورد ارزیابی قرار گرفته است.

تاریخچه و مبانی حکمرانی سایبری چین

ریشهٔ دغدغه‌های حکمرانی در فضای سایبری چین را باید هم‌زمان با ظهور اینترنت و اتصال این کشور به شبکهٔ جهانی وب دانست. از همان آغاز اتصال این کشور به اینترنت، سیاست‌گذاران و تحلیلگران چینی فضای سایبری را همچون شمشیری دولبه تصور کردند؛ به این معنا که در عین ضروری بودن برای رشد اقتصادی و حکمرانی مؤثر، تهدیدی برای ثبات داخلی و مشروعیت حکومت نیز محسوب می‌شد. از این رو به عنوان یک پدیده نوظهور، حکومت چین مبانی اصلی سیاست سایبری خود را، همانند سیاست کلاسیک این کشور در عرصهٔ بین‌الملل بر یک فرض مهم استوار ساخته است: تضمین حاکمیت ملی و عدم دخالت در امور داخلی کشورها. به این اعتبار، فضای سایبری نباید زمینه‌ای برای دخالت در امور داخلی کشورها، مبنایی برای به چالش کشیدن حاکمیت ملی کشورها یا دستاویزی برای گروه‌های برانداز (از جمله گروه‌های اپوزیسیون و نیز گروه‌های تبهکار یا گروه‌های تروریستی) باشد. در این چارچوب، رویکرد اساسی حکومت چین در عرصهٔ سایبری را، هم در بُعد داخلی و هم در بُعد خارجی و بین‌المللی، می‌توان بر اساس پنج اصل ذیل صورت‌بندی کرد:

۱. اصل حاکمیت ملی: بر اساس این اصل، عرصهٔ سایبری امتداد جهان واقعی است و کشورها حق اعمال حاکمیت ملی و نیز انتخاب الگوی ملی برای توسعهٔ این عرصه را دارند. شی جین‌پینگ، رئیس‌جمهوری چین، در کنفرانس جهانی اینترنت سال ۲۰۱۵ در ووژن در این زمینه اعلام کرد که

حاکمیت سایبری به معنای «احترام گذاشتن به حق هر کشور در انتخاب مسیر توسعهٔ اینترنتی، الگوی مدیریت اینترنتی، و خط‌مشی‌های عمومی خود در اینترنت است. لذا نخستین اصل در راهبرد سایبری ما احترام و محافظت از حاکمیت ملی در فضای سایبری است. وظیفهٔ راهبردی ما دفاع قاطعانه از حاکمیت ملی در فضای سایبری و مخالفت با تمام اقدامات صورت‌گرفته در زمینهٔ براندازی حکومت ملی یا تخریب حاکمیت ملی این کشور از طریق فضای سایبری است.[1]

۲. اصل امنیت اطلاعات ملی: در معنای وسیع، امنیت اطلاعات در برابر اصل امنیت سایبری قرار دارد که از سوی دموکراسی‌های غربی دنبال می‌شود. در حالی که دموکراسی‌های غربی همچون آمریکا و اروپا امنیت سایبری را به معنای ضرورت تحقق جریان آزاد اطلاعات در جهان تلقی می‌کنند؛ از دیدگاه چین، مسئلهٔ اصلی ضرورت «امنیت اطلاعات و ارتباطات» کشورهاست که باید به صورت ملی و محلی محافظت شود. در این چشم‌انداز، امنیت اطلاعات مقولهٔ بسیار گسترده‌تری است که کنترل جریان اطلاعات، سانسور محتوا و همچنین محافظت از شبکه‌ها و رایانه‌ها در مقابل سوءاستفاده‌های احتمالی را در بر می‌گیرد.

هر دو اصل فوق مربوط به ابعاد داخلی حکمرانی سایبری چین محسوب می‌شود و حاکمیت این کشور توانسته از طریق تدوین مکانیسم‌های دفاعی سایبری به خصوص فایروال بزرگ[2] که تماماً با استفاده از فناوری فیلترینگ و سانسور در این کشور اعمال می‌شود، دغدغه‌های مربوط به اصل حاکمیت ملی و ایجاد سَد در برابر نفوذ سایبری سایر کشورها را تا حدودی از بین ببرد.

---

1. “National Cyberspace Security Strategy”, December 27, 2016
2. Great Firewall

۳. اصل رویکرد جمعی بر مبنای مشارکت برابر همه کشورها: بر اساس این اصل، حکومت چین مخالف توزیع ناموزون منابع سایبری و کنترل آن از سوی کشورهای غربی به خصوص آمریکاست. به این اعتبار، چین به دنبال ایجاد نوعی توازن استراتژیک در حاکمیت بر عرصهٔ سایبری بین‌المللی از طریق مشارکت جمعی تمامی کشورها است. به طور مشخص، گزارش رسمی دولت چین در خصوص اینترنت در سال ۲۰۱۰[1] بر مبنای تفاوت‌های ملی تنظیم شده و بیان می‌دارد: «موقعیت‌های ملی و سنت‌های فرهنگی کشورهای مختلف متفاوت‌اند. بنابراین نگرانی دربارهٔ امنیت اینترنت نیز متفاوت است... ما باید به دنبال وجوه مشترک باشیم و تفاوت‌ها را حفظ، و آن را از طریق مبادلات توسعه دهیم و به طور مشترک از امنیت بین‌المللی اینترنت محافظت کنیم. [...] در داخل کشور چین اینترنت تحت صلاحیت حاکمیت چین است. حکمرانی اینترنت چین باید از سوی جامعهٔ جهانی مورد احترام و محافظت قرار گیرد».[2]

۴. قابلیت تسرّی و در عین حال نامکفی بودن قوانین بین‌المللی فعلی در عرصهٔ سایبری: از دیدگاه چین تمامی قوانین و حقوق بین‌المللی قابلیت تسرّی به عرصهٔ سایبری را دارد؛ با این حال، با توجه به ماهیت متفاوت عرصهٔ سایبری، قوانین و حقوق بین‌الملل فعلی پاسخگوی نیازها، مسائل و چالش‌ها و به خصوص تهدیدات ناشی از فضای سایبری نیست. از این رو باید از طریق مکانیسم‌های مختلف و بر اساس رویکرد جمعی و مشارکتی نسبت به هنجارمندی رفتارها در عرصهٔ سایبری اقدام نمود. این اصل به خصوص مخالف تلاش‌های آمریکا برای نظامی‌سازی فضای سایبری از

1. 2010 Internet White Paper
2. State Council Information Office, 2010

طریق تعمیم «قانون جنگ نظامی» به این عرصه، و استفاده از آن به عنوان تهدیدی برای حاکمیت ملی کشورها، تلاش برای براندازی دولت‌ها و اعمال فشار بر کشورهای مستقل می‌باشد.

۵. توسعه و ظرفیت‌سازی در عرصهٔ سایبری از طریق نهادهای جهانی: چین استفاده از پتانسیل و قابلیت‌های سایبری برای توسعه را بهترین زمینه برای اعتمادسازی بین کشورها و جامعهٔ جهانی می‌داند. از این رو همسو با دو اصل فوق، حکومت چین مکانیسم‌های مشروع جهانی همچون سازمان ملل متحد و دیگر نهادهای بین‌المللی وابسته به آن را مبنای اصلی مشارکت جمعی تمامی کشورها برای توسعهٔ ظرفیت‌های سایبری در خدمت جامعهٔ جهانی تلقی می‌کند.[1] این کشور به طور مشخص معتقد است که باید به نقش سازمان ملل در مدیریت بین‌المللی فضای سایبری توجه کافی معطوف شود.[2] فراتر از آن، چین با توجه به سلطهٔ ایدئولوژی‌های غربی بر مکانیسم‌های بین‌المللی رایج، تلاش‌هایی نیز از طریق تشریک مساعی با کشورهای همسو با خود از جمله سازمان همکاری شانگهای یا ابتکار راه‌اندازی کنفرانس جهانی اینترنت در راستای تقویت ظرفیت‌سازی سایبری داشته است.

گذار چین به دیپلماسی سایبری: اهداف، تهدیدها و راهبردها

همانند بسیاری از کشورها، رویکرد اولیهٔ چین به مقولهٔ سایبری رویکردی دفاعی ـ امنیتی همراه با اتخاذ سیاست‌های محافظه‌کارانه در واکنش به تهدیدات ناشی از ظهور این عرصه بوده است. بسیاری از سیاست‌های چین

1. Nigel I., 2016

2. The Internet in China, Information Office of the State Council of the People's Republic of China, 2010

برای مدیریت فضای سایبری در بُعد داخلی همچون راه‌اندازی فایروال بـزرگ سایبری، کنترل شدید جریان اطلاعات، فیلترینگ گسـتردهٔ اینترنـت و ... را در چارچوب همین رویکرد دفاعی ـ امنیتی می‌توان تحلیل کرد.

با این حال، در دوران ریاست‌جمهوری شی جـین‌پینـگ، و پـس از تثبیـت حاکمیت این کشور بر فضای سایبری داخلی، دولت چین دیپلماسی فعالانه‌تری را در حوزهٔ سایبری به خصوص در عرصهٔ منطقه‌ای و بـین‌المللـی اتخـاذ کـرده است. دیپلماسی سایبری چین به طور مشخص به دنبال دسـتیابی بـه دو هـدف کلی است: ۱. محدود ساختن تهدیـدهای احتمـالی ناشـی از فضـای سـایبری، ۲. شکل دادن به فضای سایبری در مسـیر گسـترش نفـوذ سیاسـی و نظـامی و اقتصادی چین در سطوح منطقه‌ای و جهانی. بر مبنـای دو هـدف فـوق کـه بـه صورت موازی از طریق مکانیسم‌های مختلف دنبال می‌شود، تهدیدات اصلی که از ناحیه فضای سایبری متوجه این کشـور اسـت، شناسـایی شـده و هـم‌زمـان راهبردهای عملیاتی برای مواجهه و پاسخ به این تهدیدات پیش‌بینی شده است.

الف: طبقه‌بندی تهدیدات سایبری

به اقتضای ماهیت فضای سایبری اگرچه تهدیدات ناشی از این عرصهٔ بسیار وسیع، گسترده و تا حد زیادی ابهام‌آلود است، اما بر مبنای یک تقسیم‌بندی راهبردی به خصوص با توجه به منشأ این تهدیدات، می‌توان سه نوع تهدید سایبری مرتبط با هم برای کشور چین از یکدیگر متمایز ساخت:

۱. تهدیدات سایبری ناشی از سیاست‌های ایالات متحده آمریکا: اصلی‌ترین و گسترده‌ترین تهدید چین در عرصهٔ سایبری از ناحیه سیاست‌های جهانی ایالات متحده آمریکاست. بخشی از این تهدیدات ناشی از تلاش آمریکا برای حفظ و تداوم سلطهٔ جهانی خود در عرصهٔ سایبری است و بخشی دیگر نیز ناظر بر سیاست‌های مقابله‌جویانهٔ آمریکا برای مهار و کنترل چین در این عرصه است.

نگرانی و دغدغهٔ اصلی چین در این زمینه، توزیع ناموزون منابع اینترنتی و اعمال نظر و کنترل آمریکا از طریق آیانا[1] و آیکان در اینترنت جهانی و در نتیجه فضای سایبری بین‌المللی است. به عنوان انعکاسی از این نگرانی و دغدغه، مطبوعات چینی همواره از اینکه ده سرور از سیزده سرور اصلی جهان در ایالات متحده مستقر شده‌اند و اینکه قرارداد فرایند آیانا بین آیکان و وزارت بازرگانی آمریکا بسته شده است شکایت دارند.[2] طبق گفتهٔ لو چوآنینگ،[3] محقق حوزهٔ سایبری، «ایالات متحده آمریکا عملاً کنترل و سلطه کاملی بر تدوین و مدیریت استانداردهای اینترنتی کلیهٔ سازمان‌های بین‌المللی و صنایع اصلی داشته و از بین‌المللی کردن عملیات و مدیریت‌های مربوطه یا واگذاری اختیارات به یک آژانس تخصصی سازمان ملل برای مدیریت امور امتناع ورزیده است».[4] برای به چالش کشیدن سلطهٔ جهانی آمریکا در عرصهٔ سایبری، چین در سال ۲۰۰۳ در نشستی مقدماتی برای نخستین اجلاس جهانی سران در خصوص جامعهٔ اطلاعاتی، خواستار جایگزینی الگوی حاکمیت چندذی‌نفعی با پیمان بین‌المللی اینترنت[5] و تشکیل سازمان اینترنتی بین دولتی[6] شد.[7] چین به طور مشخص معتقد است که باید به نقش سازمان ملل در مدیریت بین‌المللی اینترنت از طریق فراهم‌سازی زمینهٔ مشارکت بیشتر کشورها و دولت‌ها توجه بیشتری صورت گیرد.[8]

---

1. Internet Assigned Numbers Authority (IANA)
2. Chen Y., 2011; Yang Z., 2012
3. Lu Chuanying
4. Lu Chuanying, 2016
5. International Internet Treaty
6. Intergovernmental Internet Organization
7. Milton M., 2010
8. The Internet in China, Information Office of the State Council of the People's Republic of China, 2010

فراتر از سیاست‌های سلطه‌جویانهٔ جهانی آمریکا، چین به عنوان یک رقیب ایدئولوژیک نوظهور در مقیاس جهانی همواره مورد توجه خاص ایالات متحده بوده و دولت این کشور سیاست‌های مقابله‌جویانهٔ جدی‌ای برای مهار و کنترل چین دنبال می‌کند. به خصوص اینکه پیشرفت‌های فناورانهٔ چین و موفقیت نسبی این کشور در تدوین پروتکل‌ها و استانداردهای جهانی فناوری‌های نوین سایبری یا نفوذ کمپانی‌های آی‌تی چینی در زیرساخت‌های کلیدی کشورهای جهان چالش جدی برای سلطهٔ فناورانهٔ آمریکا ایجاد کرده است.

به صورت تاریخی، دستور کار مهار چین در عرصهٔ سایبری از سوی آمریکا سیاسی است و همواره در قالب محورهایی همچون «حمایت از اینترنت آزاد»، «حمایت از آزادی بیان»، «حمایت از حقوق بشر در عرصهٔ سایبری» و ... دنبال شده است. در واقع آنچه «دستور کار آزادی اینترنت» در تمامی اسناد راهبردی آمریکا در ارتباط با فضای سایبری مطرح بوده، تا حد بسیار زیادی معطوف به اقدامات مقابله‌جویانه با سیاست‌های داخلی چین و روسیه در ارتباط با اینترنت و جریان اطلاعات بوده است. بر مبنای راهبرد بین‌المللی آمریکا برای فضای سایبری، مقامات آمریکایی همواره مدعی بوده‌اند که از اصل «اینترنت آزاد» حمایت، و کشورهای ناقض این اصل را سرزنش کرده‌اند. به طور مثال، هیلاری کلینتون، وزیر خارجهٔ وقت آمریکا بین سال‌های ۲۰۱۰ و ۲۰۱۱ به طور مشخص طی سه سخنرانی در خصوص اینترنت آزاد، حمایت آمریکا را از آزادی بیان و عقیده در اینترنت و همچنین آزادی دسترسی به اینترنت و اتصال به وب‌سایت‌ها و افراد دیگر ابراز کرد. کلینتون در سخنرانی خود در ژانویهٔ سال ۲۰۱۰، از چین به سبب جبهه‌گیری در برابر «پیشرفت قرن آینده» انتقاد کرد و همچنین وعده داد که ایالات متحده برای کمک به مردم در

ممانعت از سانسور، فناوری‌های لازم را توسعه و توزیع خواهد کرد.[1]

در مقابل، چین و روسیه همواره سیاست‌های رسمی آمریکا در ارتباط با دستور کار اینترنت آزاد و جریان آزاد اطلاعات را سیاستی دوگانه و متناقض تلقی کرده‌اند که آمریکا از آن برای پوششی جهت توسعهٔ قابلیت‌های تهاجمی، نظامی‌سازی فضای سایبری و تسلط مداوم شرکت‌های فناوری آمریکایی دنبال می‌کند.

البته سیاست‌های مقابله‌جویانهٔ آمریکا برای مهار چین در پنج سال اخیر فراز و فرودهای زیادی داشته است. به خصوص پس از روی کار آمدن دونالد ترامپ در سال ۲۰۱۶ در آمریکا، دولت این کشور بر مبنای استراتژی ملی‌گرایی تبادلی[2] که در آن به دنبال کسب حداکثر سود در روابط تجاری با کشورها است، دستور کار اینترنت آزاد تا حدود زیادی کنار گذاشته شد. در سال‌های اولیه زمامداری ترامپ، در دستورالعمل اجرایی امنیت سایبری دولت آمده بود که سیاست آمریکا همچنان «ترویج اینترنت آزاد، تعاملی، قابل اعتماد و ایمن است»، اما کنار گذاشتن توافق‌نامه‌های تجارت آزاد و تضعیف روابط اتحادآمیز با چین به طور قابل توجهی توانایی واشینگتن را در دستیابی به اهداف خود در فضای سایبری تضعیف خواهد کرد.[3] بر این مبنا، دولت آمریکا اعتراض همیشگی به سیاست چین در کنترل اینترنت داخلی از طریق فایروال بزرگ، فیلترینگ اینترنت و کنترل جریان اطلاعات را کاهش و به یک موضوع ثانویه در روابط دو کشور تقلیل داد. حتی رکس تیلرسون،[4] وزیر خارجهٔ وقت آمریکا، در سفر خود به پکن در مارچ ۲۰۱۷، اگرچه مسئلهٔ

1. Hillary Clinton, 2010
2. Transactional Nationalism
3. Office of the Press Secretary, White House, 2017
4. Secretary Rex Tillerson

حقوق بشر و آزادی اینترنت را با مقامات چینی مطرح کرد، اما موضوع اصلی دیدار وی با شی جین‌پینگ، رئیس‌جمهوری چین تأکید بر توافق‌نامه تجارت بر مبنای احترام متقابل و همکاری بُرد ـ بُرد و پایان دادن به جنگ تجاری دو کشور بود، موضوعی که با استقبال چین نیز مواجه شد.[1]

نرم‌تر شدن موضع و رویکرد آمریکا در قبال چین در دوران ریاست‌جمهوری ترامپ البته دوام چندانی نیاورد. چشم‌انداز حصول توافق‌نامهٔ تجاری نهایی بین دو کشور خیلی سریع به دلیل اعمال تعرفه‌ها بر واردات کالا از سوی دو کشور از بین رفت. تداوم بروز اختلافات گسترده بین دو کشور که عمدهٔ آن‌ها ریشهٔ سایبری (از جمله سرقت اسرار علمی و نقض مالکیت معنوی از طریق جاسوسی سایبری، تضعیف زیرساخت‌های کلیدی از طریق حملات سایبری، نفوذ فناوری چینی در زیرساخت‌های اطلاعاتی و ارتباطی هم‌پیمانان آمریکا و ...) داشت، خیلی سریع مسائل و چالش‌های عرصهٔ سایبری را به دستور کار اصلی در روابط دو کشور بازگرداند.

این اختلافات در ماه‌های پایانی اولین دورهٔ ریاست‌جمهوری دونالد ترامپ تا جایی پیش رفت که مایک پومپئو، وزیر خارجهٔ ایالات متحده آمریکا، در ژوئیهٔ ۲۰۲۰ پس از بروز یک سری تنش‌های سخت مرتبط با مسائل سایبری همچون تحریم شرکت چینی هوآوی، بازداشت چندین دانشمند چینی به اتهام جاسوسی سایبری، بستن کنسولگری چین در هیوستون آمریکا، تحریم و ممنوع کردن فعالیت شبکه‌های اجتماعی تیک‌تاک و وی‌چت و ... رسماً اعلام کرد که استراتژی «تعامل کورکورانه» با چین شکست خورده است و این کشور دیگر نمی‌تواند اختلافات ایدئولوژیک خود با حکومت چین را نادیده بگیرد. از نگاه تحلیلگران

1. Hannah B., 2017

سیاسی، اعلان رسمی شکست استراتژی تعامل با دولت چین از سوی آمریکا به معنای بازگشت به دوران تاریک و پرتنش گذشته است[1] با این تفاوت که این بار، عمدهٔ چالش‌ها، چالش‌های سایبری است.

۲. چالش صلح سایبری و احتمال وقوع جنگ تمام‌عیار سایبری: با توجه به سیاست‌های تهاجمی دولت آمریکا، در چشم‌انداز سیاست سایبری چین احتمال وقوع جنگ تمام‌عیار سایبری بین کشورها دور از انتظار نیست. اگرچه چین چشم‌انداز وقوع چنین جنگی را بیش از هر چیزی در روابط آمریکا ـ روسیه می‌بیند، اما تبعات آن به طور خودکار دامن چین و سایر کشورها را نیز خواهد گرفت. از دیدگاه چین، آمریکا از طریق تسرّی قانون «جنگ نظامی» به فضای سایبری، دنبال نظامی‌سازی این عرصه است و این امر تهدید جدی برای امنیت جهانی است. کما اینکه چین تجربهٔ حملات سایبری به زیرساخت‌های هسته‌ای ایران و نیز سیر تقابل آمریکا ـ روسیه در جریان هک شدن سامانه‌های اینترنتی کمیتهٔ ملی حزب دموکرات آمریکا[2] و متعاقباً چالش‌های سایبری انتخابات ریاست‌جمهوری آمریکا را پیش چشم خود داشت. این مسئله باعث شد که در سال ۲۰۱۷ وزارت امور خارجهٔ چین و ادارهٔ فضای سایبری این کشور[3] به طور مشترک راهبرد بین‌المللی همکاری در فضای سایبری را صادر کردند.[4] نکتهٔ حائز اهمیت اینکه در این راهبرد بین‌المللی به اصل «صلح» پیش از حاکمیت ملی اشاره شده است و این بدین معناست که برای اولین‌بار در استراتژی سایبری چین، دیپلماسی خارجی بر مسائل سیاست داخلی اولویت یافته است.

---

1. BBC News, Retrived from https://www.bbc.com/ on 24/7/2020.
2. Democratic National Committee
3. Cyberspace Administration of China
4. State Council Information Office, 2017

۳. تهدیدات گروه‌های تروریستی: در ادبیات سایبری چین، تمامی فعالیت‌های شرارت‌انگیز از جمله فعالیت‌های گروه‌های نیابتی، گروه‌های تجزیه‌طلب، گروه‌های افراطی و ... در قالب فعالیت‌های تروریستی طبقه‌بندی می‌شوند. با توجه به اینکه چین از یک سو به دلیل سیاست‌های داخلی در ارتباط با فضای سایبری همچون سیاست فیلترینگ و کنترل اینترنت دارای مخالفان جدی و سرسختی است و هم به دلیل گرایش‌های تجزیه‌طلبانه در تبت، هنگ کنگ، تایوان و اخیراً ناحیهٔ مسلمان‌نشین اویغورها به شدت تحت فشار است، عرصهٔ سایبری فضا و زمینهٔ جدیدی برای به چالش کشیدن حاکمیت این کشور به وجود آورده است. از این رو، حکومت چین تمامی فعالیت‌های گروه‌های مخالف یا طرفداران گرایش‌های تجزیه‌طلبانه را تروریستی، نیابتی و هدایت‌شده از خارج از کشور می‌داند. از این رو، فعالیت گروه‌های تروریستی در عرصهٔ سایبری همچنان به عنوان یک تهدید اساسی برای این کشور باقی خواهد ماند.

ب: راهبردهای عملیاتی دیپلماسی سایبری چین

صورت‌بندی فوق از تهدیدات سایبری، حاکمیت چین را با هدف خنثی‌سازی این تهدیدات از یک سو و دستیابی به اهداف توسعه‌ای و نفوذ منطقه‌ای و بین‌المللی این کشور از سوی دیگر، به سمت ترکیب متنوعی از راهبردهای عملیاتی در دیپلماسی سایبری رهنمون ساخته است. برخی از این راهبردها معطوف به توجیه و تبیین سیاست‌های داخلی این کشور در ارتباط با کنترل جریان اطلاعات و فیلترینگ اینترنت و برخی دیگر نیز معطوف به پیشبرد نفوذ منطقه‌ای و بین‌المللی این کشور از طریق مکانیسم‌های مختلف بوده است. در ذیل به برخی از مهم‌ترین این راهبردها پرداخته شده است:

۱. نهادینه ساختن مقولهٔ «امنیت اطلاعات» در عرصهٔ بین‌المللی: امنیت اطلاعات مفهوم مرکزی و نقطهٔ ثقل دیپلماسی سایبری چین و نیز وجه تمایز

این کشور از دموکراسی‌های غربی است. از دیدگاه چین، امنیت اطلاعات مقولهٔ بسیار گسترده‌تری است که می‌تواند تمامی سیاست‌های داخلی چین در ارتباط با فضای سایبری را توجیه و تبیین کند. با توجه به اینکه مقولهٔ امنیت اطلاعات آشکار در برابر امنیت سایبری دموکراسی‌های غربی و طرفداران جریان آزاد اطلاعات قرار دارد و این کشور همواره از سوی دموکراسی‌های غربی به دلیل این سیاست‌ها سرزنش شده و در مظان اتهام بوده است، حکومت چین در سال‌های اخیر تلاش‌های زیادی در عرصه‌های بین‌المللی برای تبیین و نهادینه ساختن مفهوم امنیت اطلاعات به عنوان یک اصل حاکمیتی که حق همهٔ کشورهاست، مبذول داشته است. البته مسئلهٔ امنیت اطلاعات اولین‌بار توسط روسیه در سال ۲۰۰۴ در ارتباط با فضای سایبری به مجمع عمومی سازمان ملل پیشنهاد شد، با این حال چین نیز از همان ابتدا به این جریان پیوست و پابه‌پای روسیه در این زمینه فعالیت نمود.

سازمان ملل (و به خصوص گروه کارشناسان دولتی سازمان ملل[۱]) از سال ۲۰۰۴ که این مفهوم از سوی روسیه پیشنهاد شد، به مدت بیش از یک دهه صحنهٔ نزاع و تقابل بین طرفداران دو مفهوم امنیت اطلاعات (چین و روسیه و سازمان شانگهای) و امنیت سایبری (دموکراسی‌های غربی به رهبری آمریکا) بوده است. گروه کارشناسان سازمان ملل با هدف رسیدن با اجماع بین اعضای آن چندین نشست برگزار کرد تا اینکه توانست در نشست سال ۲۰۱۳ تا حدودی زمینهٔ مشترکی بین اعضا پیدا کند و بر سر آن به اجماع برسد. در واقع در ژوئن ۲۰۱۳، گروه کارشناسان سازمان ملل که اعضای آن متشکل از نمایندگان چین، روسیه، ایالات متحده و دوازده کشور دیگر بودند، بر سر

---

۱. UN Group of Government Experts، گروهی که تحت نظارت سازمان ملل در حوزهٔ امنیت اطلاعات فعالیت می‌کند.

«اعمال قوانین بین‌المللی و به ویژه منشور سازمان ملل متحد در فضای سایبری» به توافق رسیدند. بر اساس این توافق، اعضا تأیید کردند که «حاکمیت دولت و هنجارها و اصول بین‌المللی [...] در عرصهٔ سایبری می‌تواند اعمال می‌شود».[1]

گنجاندن دو مفهوم «حق حاکمیت دولت‌ها» و «هنجارها و اصول بین‌الملل» در عرصهٔ سایبری در این توافق یک‌جمله‌ای، اگرچه هم مطلوب چین و روسیه واقع شد و هم مطلوب دموکراسی‌های غربی، اما متعاقباً به دلیل برداشت متفاوت آن‌ها از این مفاهیم و عبارات، زمینه‌ساز اختلافات زیادی نیز بین آن‌ها شد. دمکراسی‌های غربی از این توافق به طور خاص به دنبال بهره‌برداری از تعمیم قوانین بین‌المللی فعلی، از جمله منشور سازمان ملل و کنوانسیون ژنو و ...، به عرصهٔ سایبری بودند تا به این بهانه سیاست‌های داخلی چین و روسیه و دیگر کشورهای همسو با آن‌ها را در محدودسازی فضای سایبری محکوم نمایند.

چین و روسیه در مقابل، به دنبال بهره‌برداری از اصل حاکمیت دولت‌ها در عرصهٔ سایبری برای اعمال سیاست‌ها و قوانین ملی خود در این عرصه بودند. به عبارت دیگر، مقامات چینی و روسی به جای پرداختن به پیامدهای اعمال قوانین بین‌المللی از جمله منشور سازمان ملل در فضای سایبری، بر پذیرش اقتدار دولتی این توافق تأکید می‌کنند. از دیدگاه چین، درست همان گونه که در قرن هفدهم شاهد گسترش حاکمیت ملی در قسمت‌هایی از دریا و در قرن بیستم در مرزهای هوایی بودیم، در حال حاضر نیز حاکمیت ملی باید به فضای سایبری توسعه یابد. در واقع بر اساس استدلال چین، خدمات اطلاعات و ارتباطات می‌تواند از مرزها فراتر برود، اما فضای سایبری نمی‌تواند بدون حاکمیت دولتی دوام بیاورد.[2]

---

1. United Nations General Assembly, 2013
2. Adam Segal, 2013

علاوه بر این، از دیدگاه چین کشورها در حوزهٔ زیرساخت‌ها و فعالیت‌های فناوری اطلاعات و ارتباطات قلمرو خود دارای صلاحیت قضایی نیز هستند. بنابراین می‌توانند خط‌مشی‌های عمومی اینترنت را بر اساس شرایط ملی خود تعیین کنند.

راهبرد امنیت اطلاعات چین در سطح داخلی، دلالت‌ها و پیامدهای اجرایی زیادی در حکمرانی سایبری ملی این کشور داشته که از جمله مهم‌ترین آن‌ها می‌توان به راه‌اندازی فایروال بزرگ سایبری برای کنترل جریان اطلاعات، سانسور و فیلترینگ اینترنت، واداشتن تمامی کمپانی‌های بزرگ آی‌تی به ارائهٔ نسخهٔ بومی از آخرین فناوری‌های خود به نحوی که تحت کنترل حاکمیت چین باشد، تدوین سیاست‌های سختگیرانه در محافظت از شبکه‌ها و رایانه‌های محلی این کشور و ... اشاره کرد. در سطح خارجی و بین‌المللی نیز چین از اعمال سیاست‌های مشابه در دیگر کشورهای همسو همچون روسیه، ایران، کشورهای عضو سازمان همکاری شانگهای و ... حمایت کرده و آن را حق حاکمیت ملی این کشورها دانسته است.

۲. هنجارمندسازی رفتار دولت‌ها در عرصهٔ سایبری: ایدهٔ امنیت اطلاعات در دیپلماسی سایبری چین دلالت‌های کاربردی دیگری نیز در عرصهٔ بین‌الملل داشته است. چین به همراه روسیه با تأکید بر اصل حاکمیت ملی، همچنین به دنبال تدوین استانداردهای رفتاری بین‌المللی به عنوان راهنمایی برای رفتار و عملکرد دولت‌ها ــ هنجارمندسازی رفتار دولت‌ها ــ در فضای سایبری بوده‌اند. در مرکز این راهبرد، ایدهٔ «عدم دخالت در امور داخلی کشورها» و نیز اصل برابری حاکمیت‌ها قرار دارد. چین و روسیه به طور مشخص به دنبال آن هستند که دولت‌ها نباید از اینترنت و فضای سایبری برای دخالت در امور داخلی دیگر کشورها استفاده کنند. علاوه بر این، کشورها باید با ایجاد یک نظام جهانی منصفانه و بی‌طرف برای مدیریت اینترنت بر اساس «اصول چندجانبه‌گرایی،

دموکراسی و شفافیت» در ادارهٔ فضای سایبری به صورت برابر مشارکت کنند.

تلاش‌های چین با همکاری روسیه برای هنجارمندسازی رفتار دولت‌ها در عرصهٔ سایبری به طور مشخص از طریق سازمان همکاری شانگهای[۱] و نیز گروه کارشناسان دولتی سازمان ملل دنبال شده است. در سپتامبر ۲۰۱۱، چین و روسیه با حمایتِ تاجیکستان و ازبکستان طی نامه‌ای، پیش‌نویس آیین‌نامهٔ بین‌المللی امنیت اطلاعات را به مجمع عمومی سازمان ملل ارائه دادند. این اقدام درست دو ماه پیش از کنفرانس لندن صورت گرفت که با ابتکار انگلستان برای شناسایی «هنجارهای رفتاری» در فضای سایبری برگزار شد و احتمالاً تلاشی برای خنثی کردن فعالیت‌های دیپلماتیک ایالات متحده و متحدان آن بوده است. این آیین‌نامه از ابتکار و تلاش سازمان ملل در تدوین هنجارها و قواعد مربوط به اطلاعات پشتیبانی می‌کند و دولت‌ها را به عدم بهره‌گیری از فناوری‌های اطلاعات و ارتباطات، از جمله شبکه‌ها، برای انجام اقدامات خصمانه یا تجاوزگرانه که تهدیدی برای صلح و امنیت بین‌المللی محسوب می‌شوند یا مسبب گسترش سلاح‌های اطلاعاتی یا فناوری‌های مربوط می‌گردند، فرامی‌خواند. این آیین‌نامه همچنین تأکید می‌کرد که مرجع سیاست‌گذاری برای موضوعات عمومی مرتبط با اینترنت حق حاکمیتی کشورهاست که دربارهٔ مسائل بین‌المللی خط‌مشی‌های عمومی مربوط به فضای سایبری ذی‌حق و مسئول‌اند.[۲]

در سال ۲۰۱۵، سازمان همکاری شانگهای مجدداً این آیین‌نامه را، با برخی

---

۱. سازمان منطقه‌ای اوراسیا که شامل چین، روسیه، قزاقستان، قرقیزستان، تاجیکستان و ازبکستان است. علاوه بر اعضای اصلی، مغولستان در سال ۲۰۰۴ و یک سال بعد ایران، پاکستان، هند و افغانستان نیز در سال ۲۰۰۵ و پس از آن بلاروس به عنوان عضو ناظر به سازمان ملحق شدند.

2. Draft International Code of Conduct for Information Security, 2011

اصلاحات جزئی، به سازمان ملل ارسال کردند. چین و روسیه به عنوان رهبران سازمان همکاری شانگهای امیدوار بودند با بهره‌گیری از پیامدهای سیاسی ناشی از افشای اطلاعات طبقه‌بندی‌شدهٔ ادوارد اسنودن[1] پیمانکار آژانس امنیت ملی آمریکا، با هدف جلب حمایت دیگر کشورهایی که در معرض تهدید نظارت و سلطهٔ ایالات متحده و اعضای گروه پنج چشم[2] قرار داشتند، از هنجارهای جدید امنیت اطلاعات بهره‌برداری کنند. نسخهٔ جدید آیین‌نامه (نسخهٔ ۲۰۱۵) موضوع حقوق بین‌الملل بشر را نیز تغییر داد. نسخهٔ ۲۰۱۱ این آیین‌نامه اعمال محدودیت‌های مبتنی بر «قوانین و مقررات ملی مربوط» را مجاز می‌شمرد. آیین‌نامهٔ جدید (نسخهٔ ۲۰۱۵) با استناد به محدودیت‌های مجاز تحت میثاق بین‌المللی حقوق مدنی و سیاسی، معیارهای ملی را جایگزین معیارهای بین‌المللی کرد. چنین تغییری ممکن است حتی در صورت مغایرت آن با کاربرد میثاق بین‌المللی حقوق مدنی و سیاسی، برای کشورهایی که به دنبال مطرح شدن در زمینهٔ حمایت از قوانین بین‌المللی بودند جذابیت داشته باشد.[3]

به موازات سازمان همکاری‌های شانگهای، گروه کارشناسان دولتی سازمان ملل نیز در نشست‌های خود صحنهٔ مقابله محور چین و روسیه در برابر دموکراسی‌های غربی در ارتباط با مقولهٔ «امنیت اطلاعات» و دلالت‌های کاربردی آن در عرصهٔ بین‌المللی، از جمله در زمینهٔ هنجارمندسازی رفتار دولت‌ها، بوده است. به طور مثال، در نشست‌های ۲۰۱۴ ــ ۲۰۱۵ گروه کارشناسان دولتی سازمان ملل، «هنجارها، قوانین یا اصول [رفتار] مسئولانهٔ دولت‌ها» و همچنین «چگونگی اعمال حقوق بین‌الملل در بکارگیری فناوری‌های اطلاعاتی و ارتباطی [ICT] از سوی

---

1. Edward Snowden

۲. Five Eyes، ایالات متحده آمریکا، کانادا، نیوزلند، انگلستان و استرالیا.

3. NATO Cooperative Cyber Defence Centre of Excellence, 2015.

کشورها» مورد بررسی قرار گرفتند. بـه خصـوص در سـال ۲۰۱۵، چـین و روسیه در زمینهٔ حمایت و توسعهٔ اصل هنجـاری « اعمـال حاکمیـت ملـی» تلاش‌های زیـادی انجـام دادنـد. در گـزارش پایـانی نشسـت سـال ۲۰۱۵، درست همانند گزارش سال ۲۰۱۳، آمده است: حاکمیت دولتی و هنجارهـا و اصول بین‌المللی برگرفته از حق حاکمیت، بـر رفتـار دولـت‌هـا در زمینـهٔ فعالیت‌های مربوط به فناوری اطلاعات و ارتباطات و همچنین بر صلاحیت قانونی آن‌ها در خصوص زیرسـاخت‌هـای فنـاوری اطلاعـات و ارتباطـات قلمروشان اعمـال مـی‌شـود. در ایـن گـزارش همچنـین بخشـی بـا عنـوان «چگونگی اعمـال قـوانین بـین‌المللـی در بکـارگیری فنـاوری اطلاعـات و ارتباطات» وجود دارد که به توسعهٔ بیشتر این ایده‌ها می‌پردازد و خاطرنشان می‌کند که کشورها باید از میان سـایر اصـول حقـوق بـین‌الملـل، حاکمیـت دولت، برابری حاکمیت، حل‌وفصل اختلافات به صـورت مسـالمت‌آمیـز، و عدم مداخله در امور داخلی سایر کشورها را رعایت کنند.[1]

۳. ابتکار کنفـرانس جهـانی اینترنـت و تقابـل آن بـا کنفـرانس لنـدن: سازمان ملل و دیگر نهادها و سازمان‌هـای وابسـته بـه آن از جملـه گـروه کارشناسان این سازمان و نیـز سلسـله‌نشسـت‌هـا و همـایش‌هـای مجمـع حکمرانی اینترنت[2] که همه‌ساله برگزار می‌شود، تنها بستر مواجههٔ چـین بـا سیاست‌های دموکراسی‌های غربی در ارتباط با اینترنت و فضـای سـایبری نبـوده اسـت. بـا توجـه بـه اینکـه بـه صـورت تـاریخی ایـدئولوژی دموکراسی‌های غربی گفتمان غالب در این نهادها و سازمان‌ها بوده، چـین از سـال ۲۰۱۲ بـه فکـر ایجـاد پلتفـرم جدیـدی در سـطح منطقـه‌ای و بین‌المللی برای تبیین سیاست‌های جهانی خود در زمینهٔ اینترنت و مسـائل

1. United Nations, 2015
2. Internet Governance Froum (IGF)

مرتبط با فضای سایبری بوده است؛ پلتفرمی که در نهایت در سال ۲۰۱۴ در قالب «کنفرانس جهانی اینترنت» شکل گرفت.

چین در نوامبر ۲۰۱۴ نخستین کنفرانس جهانی اینترنت را در ووژن، شهری تاریخی در نزدیکی هانگژو که دفتر مرکزی گروه علی‌بابا[1] در آنجا واقع شده است، برگزار کرد. این رویداد، که سازمان ملی فضای سایبری چین آن را برگزار کرد، در واقع محلی برای به نمایش گذاشتن اقتصاد اینترنتی چین و همچنین مجمعی برای ترویج دیدگاه‌های پکن در خصوص حاکمیت فضای سایبری بود. در بیانیهٔ ارائه‌شده در مراسم افتتاحیه این کنفرانس، شی جین‌پینگ خواستار سیستم مدیریتی چندجانبه، دموکراتیک و شفاف برای مدیریت اینترنت بین‌المللی شد.

اولین کنفرانس جهانی اینترنت با چالش‌های زیادی از سوی کشورهای غربی به خصوص رسانه‌ها و نمایندگان این کشورها که با اکراه در این اجلاس شرکت کرده بودند، مواجه شد. برخلاف چین که امیدوار بود این رویداد را به نمایشی برای شرکت‌های اینترنتی و فناوری آی‌تی چینی تبدیل کند، مطبوعات غربی روی سانسور و فیلترینگ فیس‌بوک، توییتر و سایر سایت‌های اینترنتی غربی در چین مانور تبلیغاتی زیادی انجام دادند. علاوه بر این، نمایندگان کشورهای غربی حاضر به امضای سند پایانی این همایش نشدند و کنفرانس مذکور بدون بیانیهٔ نهایی به پایان رسید. این سند که از قبل تدوین شده بود، شامل نُه محور اصلی از جمله تشویق به فعالیت‌های مشترک در زمینهٔ امنیت سایبری و مبارزه با تروریسم سایبری، توسعهٔ اقتصاد اینترنت و تقویت ارتباطات بود. این سند همچنین خواستار احترام به حق حاکمیت ملی کشورها بر اینترنت و فضای سایبری بود[2].

---

1. Alibaba Group
2. Josh Chin, 2015

به رغم چالش سیاسی و انعکاس تبلیغاتی منفی که کنفرانس جهانی اینترنت در سال اول با آن مواجه شد، اما چین در دومین کنفرانس جهانی اینترنت که سال بعد در ۲۰۱۵ برگزار شد، بر اهمیت سیاسی و دیپلماتیک این کنفرانس تأکید ورزید، به خصوص اینکه شخص رئیس‌جمهوری این کشور در سخنرانی افتتاحیهٔ آن حضور یافته و مواضع صریحی در ارتباط با فضای سایبری و چشم‌انداز مدیریت آن در آینده ابراز داشت. شی جین‌پینگ در سخنرانی خود اظهار داشت که احترام به حق تمامی کشورها برای انتخاب مستقلانهٔ مسیر توسعهٔ سایبری، الگوی مقررات سایبری و خط‌مشی‌های عمومی اینترنت خود و همچنین مشارکت در حکمرانی فضای سایبری بین‌المللی در شرایط کاملاً یکسان ضرورت دارد. او ادامه داد: هیچ کشوری نباید به دنبال هژمونی سایبری[1] باشد، در امور داخلی سایر کشورها مداخله کند، از فعالیت‌های سایبری تضعیف‌کنندهٔ امنیت ملی سایر کشورها چشم‌پوشی یا از آن‌ها حمایت نماید. شی جین‌پینگ همچنین از حکمرانی جهانی اینترنت انتقاد کرد که به گفتهٔ وی در منعکس کردن خواسته‌ها و منافع اکثر کشورها ناموفق بوده است. وی بدون اشاره به یک نهاد خاص تأکید کرد که حاکمیت سایبری باید دارای یک رویکرد چندجانبه با مشارکت تمامی کشورها باشد[2].

چین همچنین با راه‌اندازی یک کمیتهٔ عالی مشورتی با ریاست مشترک فادی چهاد[3]، رئیس سابق آیکان، و جک ما[4]، مدیرعامل علی‌بابا، سعی داشت بخشی از نیروی رویکرد چندذی‌نفعی برای حکمرانی اینترنت را به خدمت بگیرد. این کمیته به عنوان نخستین اقدام خود، طرح ووژن[5] را تصویب کرد که رویکردی چندذی‌نفعی به حکمرانی اینترنت را بر اساس

---

1. Cyber Hegemony
2. Kieren McCarthy, 2015
3. Fadi Chehade
4. Jack Ma
5. Wuzhen Initiative

اصل حاکمیت دولت در فضای سایبری ارائه کرده بود. این کمیته موظف به ترویج این پیام در عرصهٔ بین‌المللی و مشاوره دادن به سازمان فضای سایبری چین[1] در خصوص برنامه‌ریزی برای کنفرانس‌های آینده بود.[2]

البته از زمان راه‌اندازی این کمیته، جزئیات کمی دربارهٔ فعالیت‌های آتی آن ارائه شده است. به گزارش رسانه‌های دولتی چین، در جریان کنفرانس جهانی اینترنت در سال ۲۰۱۶،[3] این کمیتهٔ مشورتی نشستی به ریاست چهاد و جک ما برگزار کرد که ظاهراً دومین گردهمایی این گروه بوده است. نتیجهٔ این جلسه که گزارشی از وضعیت اینترنت بود، مجدداً تنها بر اصول طرح ووژن تأکید داشت و تحولات دیگری طی این گزارش مطرح نشد.

کنفرانس جهانی اینترنت به رغم آنکه بیش از شش سال از آغاز آن می‌گذرد، هنوز نتوانسته جایگاه بین‌المللی، حداقل در سطح مجمع جهانی حکمرانی اینترنت[4] یا کنفرانس لندن در زمینهٔ اینترنت، کسب کند. عمدهٔ کشورهای شرکت‌کننده در این کنفرانس از متحدان نزدیک چین یا اعضای سازمان همکاری شانگهای بوده‌اند. کشورهای غربی عمدتاً در سطح سفیر یا نمایندگان سفارتخانه در این کنفرانس شرکت می‌کنند و حتی از بخش خصوصی نیز نمایندگان یا مدیران میانی شرکت‌ها و کمپانی‌های بزرگ در آن حضور می‌یابند. با این حال، چین از این کنفرانس به عنوان ابتکاری برای به چالش کشیدن دستور کارهای دموکراسی‌های غربی در کنفرانس جهانی لندن استفاده می‌کند.

۴. مقابله با تروریسم سایبری: مقابله با تروریسم، یکی دیگر از راهبردهای اصلی در دیپلماسی سایبری چین است که به دلیل نزدیکی مواضع اعضا نسبت به مقولهٔ تروریسم، به خصوص از طریق سازمان

---

1. Cyber Administration of China
2. Kieren McCarthy, 2015
3. World Internet Conference (WIC)
4. IGF

همکاری شانگهای دنبال شده است. رویکردهای دیپلماتیک چین به تروریسم سایبری همچنین بخشی از تلاش‌های این کشور برای تدوین «استانداردها و هنجارهای رفتاری دولت‌ها در عرصهٔ سایبری» در سازمان همکاری شانگهای است. در حالی که این سازمان در ابتدا، غیرنظامی‌سازی مرزها و اعتمادسازی بین شرکا را مدنظر قرار داده بود، دستور کار آن به ابتکارات اقتصادی و تهدیدات امنیتی جدید گسترش یافت، به خصوص اینکه در زمینهٔ تهدیدات امنیتی، سازمان همکاری شانگهای روی «سه اقدام شرارت‌انگیز» متمرکز شده است: تروریسم و تجزیه‌طلبی و افراط‌گرایی.

در سال ۲۰۰۷، هنگامی که سازمان همکاری شانگهای فعالیت‌های خود در زمینهٔ کد امنیت اطلاعاتی را آغاز کرد، مقابله با تروریسم و استفاده از ظرفیت‌های اینترنت برای جمع‌آوری بودجه، تبلیغات، استخدام و سازمان‌دهی حملات تروریستی در رأس این همکاری‌ها قرار داشت. همسویی کشورهای سازمان همکاری شانگهای، هماهنگی و همکاری بین آژانس‌های سایبری ملی اعضا را بسیار تسهیل می‌ساخت و در نهایت یک بانک اطلاعاتی از سازمان‌ها و فعالیت‌های تروریستی مشکوک تشکیل شد که اطلاعات جمع‌آوری‌شده را در اختیار اعضا قرار می‌داد. در اکتبر ۲۰۱۵، چین و اعضای این سازمان نخستین رزمایش مشترک ضدتروریسمی اینترنتی را با عنوان ژیامن ۲۰۱۵[1] برگزار کردند. طی این رزمایش، اعضای این سازمان به‌اشتراک‌گذاری اطلاعات و هماهنگی برون‌مرزی به منظور واکنش سریع به بهره‌برداری یک گروه تروریستی شبیه‌سازی‌شده از رسانه‌های اجتماعی برای تحریک فعالیت‌های تروریستی را تمرین کردند[2].

سازمان ملل متحد یکی دیگر از بسترهای فعالیت‌های چین برای مقابله با

---

1. Xiamen, 2015
2. Peter W., 2015

تروریسم سایبری بوده است. در سپتامبر ۲۰۱۴ وانگ یی[1] وزیر امور خارجهٔ چین، در اجلاس شورای امنیت سازمان ملل متحد در خصوص تروریسم، خاطرنشان کرد: رسانه‌های اجتماعی به کارزاری برای تحریک ایدئولوژی گروه‌های تروریستی و افراطی، ابزاری برای برنامه‌ریزی حملات تروریستی و بستری برای جذب تروریست‌ها تبدیل شده‌اند. وانگ به‌اشتراک‌گذاری اطلاعاتی گسترده و همچنین اقدامات قاطعانه‌ای را برای متوقف ساختن بهره‌برداری از رسانه‌های اجتماعی به منظور گسترش ایده‌های افراطی پیشنهاد داد. وانگ یی به ویژه تأکید داشت که شرکت‌های اینترنتی می‌بایست سیاست‌های پیشگیرانه را اتخاذ کنند و همچنین به ضرورت فعالیت سازمان ملل در زمینهٔ تعریف کدهای رفتاری برای صنعت فناوری جهانی اشاره کرد[2].

دو ماه بعد، پکن میزبان سمپوزیوم مبارزه با تروریسم سایبری بود که مجمع جهانی مبارزه با تروریسم[3] آن را برگزار کرد و این سکوی غیررسمی مذاکره متشکل از بیست‌ونه کشور، اتحادیهٔ اروپا و آژانس‌های مختلف منطقه‌ای و سازمان ملل متحد برای حمایت از اجرای راهبرد جهانی ضد تروریسم سازمان ملل بود. در این سمپوزیوم ژانگ یسی[4]، معاون وزیر امور خارجهٔ چین، خاطرنشان کرد که چین نیز قربانی تروریسم سایبری شده است. زیرا اعضای نهضت اسلامی ترکستان شرقی[5] از رسانه‌های اجتماعی برای انجام فعالیت‌های تروریستی بهره‌برداری می‌کنند[6].

راهبرد سایبری ملی چین در سال ۲۰۱۶ حاکی از آن است که این کشور همچنان بر فعالیت‌های ضد تروریسم در سازمان ملل متمرکز خواهد بود. بر اساس این راهبرد، پکن از سازمان ملل متحد برای ایفای نقش پیشرو، پیشبرد

---

1. Wang Yi
2. Wang Yi, 2014
3. Global Counterterrorism Forum
4. Zhang Yesui
5. East Turkistan Islamic Movement
6. Adam S., 2017

تدوین هنجارهای به‌رسمیت‌شناخته‌شده در سطح جهانی برای فضای سایبری و همچنین پیمان بین‌المللی ضد تروریسم در فضای سایبری حمایت می‌کند.

۵. سرمایه‌گذاری تجاری ـ اقتصادی در حوزهٔ فناوری اطلاعات و ارتباطات: چین به عنوان دومین کشور قدرتمند در زمینهٔ فناوری سایبری، از تجارت و سرمایه‌گذاری در زیرساخت‌های اطلاعاتی و ارتباطاتی سایر کشورها به عنوان یک ابزار اقتصادی و به طور غیرمستقیم سیاسی به منظور توسعهٔ نفوذ منطقه‌ای و بین‌المللی خود استفاده می‌کند. این راهبرد به طور هم‌زمان از دو مسیر جداگانه دنبال می‌شود:

الف. نفوذ در زیرساخت‌های ارتباطی و اطلاعاتی کشورهای غربی و هم‌پیمان آمریکا از طریق سرمایه‌گذاری مستقیم در این زیرساخت‌ها، خرید سهام شرکت‌های آی‌تی و مشارکت در طرح‌های فناورانه. این سیاست به طور مشخص با این هدف دنبال می‌شود که چین به مرحله‌ای از اقتدار سایبری با هدف قابلیت نفوذ در زیرساخت‌های اطلاعاتی و ارتباطی، سامانه‌های نظامی و دیگر زیرساخت‌های کلیدی رقبای ایدئولوژیک دست یابد. این سیاست در سال‌های اخیر با واکنش تند ایالات متحده مواجه شده و این کشور از طریق اتخاذ سیاست‌های مقابله‌جویانه همچون برقراری رژیم‌های تحریمی علیه شرکت‌های چینی، فشار بر هم‌پیمانان غربی برای لغو همکاری با شرکت‌های چینی، بازداشت دانشمندان چینی و مسئولان و رؤسای شرکت‌های چینی و ... تلاش زیادی در راستای مهار چین و مسدودسازی راه‌های نفوذ چین داشته است.

ب. نفوذ در کشورهای درحال‌توسعه یا کمترتوسعه‌یافته از طریق سرمایه‌گذاری در زیرساخت‌های کلیدی این کشورها. این سیاست که به طور خاص در آفریقا، آسیای جنوب شرقی، آسیای میانه و آمریکای لاتین دنبال می‌شود، با هدف ایجاد نوعی وابستگی به فناوری چینی در این

کشورها و نیز در اختیار گرفتن بازار آن‌ها دنبال می‌شود. این سیاست نیز در سال‌های اخیر نگرانی‌های زیادی به خصوص در بین کشورهای غربی و در رأس آن‌ها آمریکا ایجاد کرده است. از دیدگاه محافل غربی، چین با فراهم آوردن منابع جایگزین بودجه‌ای می‌تواند فعالیت‌های ایالات متحده و اروپا را برای توسعهٔ هنجارهای غربی تضعیف کند. به خصوص اینکه در عمدهٔ موارد، کمک‌های چین بدون پیش‌شرط در قالب وام و کمک‌های توسعه‌ای در اختیار این کشورها قرار می‌گیرد.

اندیشکدهٔ دفاع و سیاست خارجی اتحادیهٔ اروپا در گزارشی دربارهٔ نفوذ چین در آفریقا و آسیا، بخش زیادی از ابعاد و جزئیات سرمایه‌گذاری‌های چین در کشورهای درحال‌توسعه را بیان می‌کند. در بخش‌هایی از این گزارش آمده است: در سال ۲۰۰۵، هواوی[1] چین یک مدرسهٔ آموزشی در ابوجا، پایتخت نیجریه، دایر کرد. پنج سال بعد، شرکت‌های مخابراتی چینی هواوی و زدتی‌ای[2] در پنجاه کشور آفریقا مشغول به فعالیت شدند و به بیش از سیصد میلیون کاربر آفریقایی خدمات ارتباطی ارائه می‌دادند. مراکز آموزشی این دو شرکت چینی در نُه کشور آفریقایی فعالیت دارند و برای بیش از بیست کشور شبکه‌های ارتباطی فیبر نوری و شبکه‌های دولت الکترونیکی ساخته‌اند.[3] چین با اعطای وام‌های ترجیحی و اعتبارات کافی به عنوان بخشی از سیاست برون‌مرزی[4]، در مسیر پیشبرد بین‌المللی‌سازی شرکت‌های چینی قدم نهاده است. در حال حاضر بخش عمده‌ای از سرمایه‌گذاری و تجارت خارجی چین به عنوان قسمتی از طرح یک کمربند و یک جاده (راه ابریشم جدید)[5] صورت می‌گیرد؛ یک راهبرد توسعه‌ای با محوریت اتصال و همکاری بین کشورهای چین و اوراسیا. این طرح دو مؤلفه

---

1. Huawei
2. ZTE
3. Andrea M., 2011
4. "Go Out" Policy
5. One Belt, One Road (OBOR)

دارد: ۱. کمربند اقتصادی جادهٔ ابریشم که چین را به خلیج فارس و سرزمین‌های مدیترانه و اقیانوس هند متصل می‌کند؛ ۲. جادهٔ ابریشم دریایی قرن بیست‌ویکم[1] که آبراه‌های منطقه‌ای را به یکدیگر پیوند می‌دهد. سرمایه‌گذاری چین ــ که به گفتهٔ رسانه‌های دولتی حدود ۵۱/۱ میلیارد دلار است ــ در شبکه‌ای از راه‌آهن‌ها، جاده‌ها، خطوط لوله، بندرها، معادن و شبکه‌های تأسیسات به کار گرفته شده است. بیشترین سرمایه‌گذاری‌ها در بخش‌های انرژی و معدن، زیرساخت‌ها و بخش‌های تولیدی صورت گرفته است.[2] اسناد رسمی چین همچنین بر لزوم ساختن جادهٔ ابریشم اطلاعاتی[3] از طریق کابل‌های نوری برون‌مرزی و سایر شبکه‌های خطوط اصلی[4] ارتباطی، پروژه‌های کابل نوری زیردریایی بین‌قاره‌ای و ارتباطات فضایی (ماهواره‌ای) تأکید کرده‌اند. در دسامبر ۲۰۱۶، وزارت صنعت و فناوری اطلاعات چین از یک برنامهٔ دوساله در زمینهٔ ساخت‌وساز و به‌روزرسانی شبکه‌های مخابراتی در آفریقا رونمایی کردند که سرمایهٔ مورد نیاز آن روی‌هم‌رفته معادل ۱۷۳/۷۳ میلیارد دلار تخمین زده شد.[5]

شرکت‌های چینی در نقاطی که در امتداد کمربند و جاده واقع شده‌اند سرمایه‌گذاری‌های کلانی کرده‌اند. شرکت‌های مخابراتی دولتی چین در حال برنامه‌ریزی عملیات جدید در آفریقا و آسیای جنوب شرقی هستند. شرکت چاینا کام‌سرویس[6]، یکی از شرکت‌های تابعهٔ چاینا تلکام[7]، ساخت مشترک ابربزرگراه اطلاعاتی آفریقا بین چین و آفریقا[8] را با سرمایه‌گذاری ۱۵ میلیارد دلاری و یک کابل نوری ۱۵۰هزار کیلومتری که ۴۸ کشور آفریقایی را تحت پوشش قرار

---

1. Twenty-First Century Maritime Silk Road
2. Yang Y., 2016
3. Information Silk Road
4. Trunk Line
5. Global Times, March 13, 2017
6. China Comservice
7. China Telecom
8. Africa’s Information Superhighway

می‌دهد، آغاز کرده است. چاینا یونیکام[1] در حال کابل‌کشی فیبر نوری بـرای اتصـال آسیای میانه، آسیای جنوب شرقی، آفریقا و آمریکای جنوبی است.[2] ایـن در حـالی است که شرکت‌های خصوصی نیز در این زمینه فعـال بـوده‌انـد. در سـال ۲۰۱۶، شرکت زدتی‌ای طی توافقی شرکت ترکیه‌ای نتاس[3] را با هدف توسـعهٔ نفـوذ خـود در منطقه خاورمیانه و آسیای میانه به مبلغ ۱۰۱/۲۸ میلیون دلار خریداری کرد.[4]

برخی از شرکت‌های بزرگ چینی[5] فعال در حوزهٔ فناوری اطلاعات و عرصهٔ سایبری	
شرکت تنسِنت[6]	تنسنت یکی از بزرگ‌ترین شرکت‌های آی‌تـی چـین اسـت کـه مالکیت شبکهٔ اجتماعی وی‌چت، بزرگ‌تـرین رسـانهٔ اجتمـاعی این کشور را نیز در اختیار دارد. وی‌چت رقیب شبکهٔ اجتمـاعی فیس‌بوک محسوب می‌شود.
هوآوی	هوآوی بزرگ‌ترین برند گوشی همـراه چـین اسـت کـه رقیـب شرکت آمریکایی اپل محسوب می‌شود. هوآوی پیشگام فناوری نسل پنجم در این کشور است.
بایدو[7]	بایدو بزرگ‌ترین موتور جسـت‌وجـوگر چـین محسـوب، و در دنیای اینترنت، رقیب گوگل محسوب می‌شود.
علی‌بابا	علی‌بابا بزرگ‌ترین فروشگاه آنلاین چین محسوب می‌شـود کـه رقیب آمازون می‌باشد.
زدتی‌ای	بزرگ‌ترین شرکت مخابراتی و تولیدکنندهٔ گوشـی‌هـای موبایـل در کشور چین است. زدتی‌ای به همراه هوآوی پیشگام فنـاوری نسل پنجم در این کشور است.

1. China Unicom
2. China Go Abroad, September 2016
3. Netas Telekomünikasyon
4. Bien P., 2016
۵. عمدهٔ این شرکت‌ها در شهر شنژن، مشـهور بـه درهٔ سـلیکون‌ولـی چـین، مسـتقر هستند.
6. Tencent
7. Baidu

شیائومی[1]	شرکت الکترونیکی که تولیدکنندهٔ گوشی‌های هوشمند تلفن همراه است.
کمپانی موبایل چین[2]	شرکت دولتی ارائه‌دهندهٔ خدمات موبایل در کشور چین است که با بیش از ۸۰۰ میلیون مشترک، بزرگ‌ترین کمپانی موبایل در جهان محسوب می‌شود.
تیک‌تاک[3]	شبکهٔ اجتماعی تیک‌تاک متعلق به شرکت چینی «بایت‌دنس» است. این شرکت سال گذشته (۲۰۱۹) شبکهٔ اجتماعی «موزیکال‌لی» آمریکایی را نیز خریداری کرد. این شبکه ویژهٔ به اشتراک گذاشتن ویدئوهای کوتاه است. این شبکه رقیبی برای شبکه‌های اجتماعی اینستاگرام، نت‌فلیکس، یوتیوب و اسنپ‌چت است.

۶. استانداردسازی در حوزهٔ فناوری‌های سایبری: به موازات تجارت و سرمایه‌گذاری در حوزه‌های مرتبط با فناوری اطلاعات و ارتباطات سایر کشورها، چین تلاش‌های گسترده‌ای نیز برای تأثیرگذاری بر نسل آتی استانداردهای فناوری این حوزه آغاز کرده است. چین پس از پیوستن به سازمان تجارت جهانی، تلاش وسیعی برای تعریف پروتکل و استانداردهای فناوری در نرم‌افزار، سخت‌افزار و فناوری‌های ارتباطی انجام داده است. به عقیدهٔ سیاست‌گذاران چینی کنترل یک استاندارد تصاحب سهم بزرگی از ارزش بازار فناوری را تضمین می‌کند. همچنین این نگرش در مطبوعات فناوری چین حاکم است که شرکت‌های درجه‌سه محصولات تولید می‌کنند، شرکت‌های درجه‌دو فناوری را توسعه می‌دهند و شرکت‌های درجه‌یک استانداردها را تعیین می‌کنند[4].

---

1. Xiaomi
2. China Mobile Ltd
3. TikTok
4. Adam S., 2011

چین در گذشته در زمینهٔ تعریف پروتکل‌ها و استانداردهای مربوط به تلفن‌های همراه نسل سوم و چهارم، وای فای (احراز هویت WAPI یا WLAN و زیرساخت‌های حریم خصوصی)، دی‌وی‌دی‌ها (AVS، استاندارد رمزگذاری صوتی ـ تصویری) و RFID (شناسایی از طریق فرکانس رادیویی)، فعالیت‌های چندانی نداشته و موفق نبوده است. اما در سال‌های اخیر مهارت‌ها و تجربیات خود را در سازمان‌های استاندارد جهانی ارتقا داده است.

پکن در سال‌های اخیر با اعزام هیئت‌های بزرگ به نشست‌های استانداردهای فنی و امنیتی، بر نسل آتی فناوری‌های اینترنت و ارتباطات (فناوری نسل پنجم– ۵G) متمرکز شده است. نیگل اینکستر[1] خاطرنشان می‌کند که چین بیش از چهل نماینده به نشست کارگروه مهندسی اینترنت سال ۲۰۱۵ اعزام کرده بود؛ سطحی از تعامل که نشانگر اهمیت بالای دستور کار حکمرانی جهانی برای این کشور است.[2] چین همچنین در گروهی فعال در زمینهٔ معماری اشیای دیجیتال در اتحادیهٔ بین‌المللی ارتباطات[3] که عبارت است از یک نظام مدیریت اطلاعات، که نقش مهمی در اینترنت اشیا دارد، فعالیت وسیعی دارد. طبق گفتهٔ وال استریت ژورنال، در زمینهٔ تعیین قابلیت‌ها و مشخصات تلفن همراه نسل پنجم[4] تعداد نمایندگان اعزام‌شدهٔ هوآوی به نشست سال ۲۰۱۶ وین دو برابر سایر شرکت‌های مخابراتی بود[5].

مجمع حکمرانی اینترنت[6] که از سوی سازمان ملل با هدف بررسی

---

1. Nigel Inkster
2. Inkster, “China’s Cyber Power.”
3. International Telecommunication Union (ITU)
4. 5G
5. Matthias V., 2017
6. IGF

مباحث سیاستی مرتبط با مدیریت اینترنت هرساله در یکی از کشورهای جهان برگزار می‌شود، محمل دیگری برای حضور بیشترین تعداد نمایندگان چینی از هر سه بخش دولتی، خصوصی و نهادهای مدنی است که با هدف تأثیرگذاری بر مدیریت اینترنت از سوی چین دنبال می‌شود.[1] بر اساس گزارش سالانهٔ آی‌جی‌اف، کارشناسان و هیئت نمایندگانی چینی، گردانندگان اصلی همایش مجمع حکمرانی اینترنت و نیز نشست‌های حاشیه‌ای این همایش در سال ۲۰۱۹ در کشور آلمان بوده‌اند.

در بین غول‌های فناوری، هوآوی بزرگ‌ترین کمپانی آی‌تی و تجهیزات مخابراتی چین است که به نمایندگی از این کشور در تنظیم پروتکل و استانداردهای فناوری نسل پنج پیشگام است. بر اساس برآوردهای جهانی از بین پنج شرکت بزرگ آی‌تی جهان، کمپانی هوآوی با اختلاف بسیار زیادی بیشترین تعداد استاندارد و پروتکل امنیتی مربوط به فناوری نسل پنج را توسعه داده است. پس از آن به ترتیب شرکت‌های اریکسون، نوکیا، کوالکام[2] و چاینا موبایل در رده‌های بعدی قرار دارند.[3]

پیشگامی چین در حوزهٔ فناوری نسل پنج نگرانی‌های زیادی در بین کشورهای غربی، به خصوص آمریکا ایجاد کرده است. با توجه به اینکه فناوری نسل پنج در واقع زیرساخت فناوری‌های دیجیتال نوین همچون اینترنت اشیا، هوش مصنوعی، و ... می‌باشد، پیشگامی چین در تدوین استانداردها و پروتکل‌های امنیتی این فناوری عملاً به معنای پایان حاکمیت و اشرافیت آمریکا در دنیای فناوری اطلاعات و ارتباطات است که قبلاً از طریق اینترنت جهانی تضمین شده بود. لذا اقدامات اخیر دولت آمریکا در ممنوعیت همکاری شرکت‌های آمریکایی با هوآوی، اعمال تحریم‌های

---

1. Juro O., 2016
2. Qualcomm
3. Guang Yang, 2020

وسیع علیه هوآوی، فشار به کشورهای اروپایی و هم‌پیمان غربی برای قطع همکاری با هوآوی، بازداشت برخی از مسئولان و مدیران هوآوی و ... نیز در چارچوب همین موضوع قابل ارزیابی و فهم است.

۷. ترویج صلح سایبری از طریق رویکردهای دوجانبه و چندجانبه: مسائل سایبری بخش بسیار مهمی از محورهای همکاری‌های دوجانبه و چندجانبهٔ چین را تشکیل می‌دهند. به خصوص با توجه به تفاوت‌های فاحشِ معیارهای الگوی حکمرانی سایبری ملی چین و نیز سوءظن‌های فراوانِ به سیاست‌های منطقه‌ای و بین‌المللی این کشور در ارتباط با مسائل سایبری، به ویژه در جهان غرب، دورنمای اینکه چین بتواند از طریق راهبردهای شش‌گانهٔ سایبری فوق اجماع جهانی ایجاد نماید، بسیار ضعیف است. با این حال از آنجایی که حوادث و مسائل سایبری نشان‌دهندهٔ نوعی دغدغه و نگرانی مشترک تمامی کشورهای عضو جامعهٔ جهانی است، چین با هدف ترویج صلح سایبری بخشی از تلاش‌ها و فعالیت‌های سیاسی و بین‌المللی خود را با هدف حل موضوعات و مسائل سایبری مختلف از طریق رویکردهای دوجانبه و چندجانبه با سایر کشورها، چه به صورت رسمی چه از طریق کانال‌های غیررسمی و ثانویه، دنبال می‌کند.[1]

در این میان سیاست چین در ارتباط با آمریکا در زمینهٔ مسائل سایبری پیچیده‌ترین و پرتنش‌ترین نوع روابط بوده و طیف وسیعی از موضوعات مختلف سایبری (از جاسوسی سایبری گرفته تا حملات سایبری و مالکیت معنوی و سرقت اسرار فناوری، نگرانی از نفوذ فناوری چینی در زیرساخت‌های اطلاعاتی و ارتباطی کشورهای غربی، و ...) را در بر می‌گیرد. هنگامی که ایالات متحده برای نخستین‌بار چین را به سرقت سایبری مالکیت

1. Adam S., 2017

معنوی متهم کرد، راهبرد اولیهٔ پکن انکار و گمراه‌سازی بود. متعاقب آن اعلامیه‌های متعددی از سوی این کشور در ارتباط با دست نداشتن هکرهای چینی در این حملات، اعتراضاتی مبنی بر غیرقانونی بودن عملیات هک در چین و اینکه چین بزرگ‌ترین قربانی فضای سایبری است، صادر می‌شد. با توجه به گزارش‌های سازمان‌های آمریکایی از دست داشتن ارتش خلق چین در حملات و تهدیدات سایبری، آمریکا بیشتر از چین خواستار گفت‌وگوهای دوجانبه دربارهٔ امنیت سایبری بوده و بیش از هرچیزی، بر حضور نمایندگان ارتش خلق چین در این مذاکرات تأکید می‌کند. با این حال، چین محور مذاکرات خود با آمریکا را عمدتاً به مذاکرهٔ راهبردی و اقتصادی محدود و صرفاً دیپلمات‌های وزارت خارجه را به این مذاکرات رهسپار می‌کند. حتی در موارد بسیار معدودی نیز، نمایندگان ارتش آزادی‌بخش خلق حاضر در این گفت‌وگوها به جای دایرهٔ عملیات سایبری، از وزارت امور خارجهٔ چین اعزام شده بودند. پنتاگون به نمایندگی از بخش‌های نظامی آمریکا بارها اصول این کشور در خصوص بهره‌برداری از عملیات سایبری تهاجمی را برای مقامات ارتش آزادی‌بخش خلق شرح دادند، اما ارتش آزادی‌بخش خلق چین پاسخی به آن‌ها نداده و یا به تکرار پاسخ‌های سیاسی وزارت امور خارجهٔ این کشور بسنده کرده است.[1]

تا پیش از آغاز اعمال فشار مستقیم واشینگتن در اواخر دورهٔ ریاست‌جمهوری باراک اوباما، پکن به پیروی از راهبرد انکار تمایل زیادی داشت. در مارچ ۲۰۱۳ تام دونیلون،[2] مشاور امنیت ملی آمریکا، دربارهٔ نگرانی‌های جدی دربارهٔ سرقت پیشرفته و هدفمند اطلاعات تجاری محرمانه و فناوری‌های اختصاصی از طریق نفوذ سایبری از جانب چین در مقیاسی بی‌سابقه سخنرانی

1. David E. Sanger, 2014
2. National Security Adviser Tom Donilon

کرد.[1] طبق گزارش‌ها، در ژوئن ۲۰۱۳ باراک اوباما، رئیس‌جمهور آمریکا، در دیدار از کالیفرنیا به شی جین‌پینگ، رئیس‌جمهور چین، هشدار داد که جاسوسی سایبری صدمات جبران‌ناپذیری به روابط دوجانبه خواهد زد. با این حال، بلافاصله پس از پایان اجلاس، اسنودن[2] در هنگ‌کنگ حضور یافت. افشاگری در خصوص عملیات گستردهٔ آژانس امنیت ملی، به پکن این اجازه را داد تا ایالات متحده را از موضوع منحرف و نقد کند. متعاقب آن، تلاش‌های ایالات متحده در زمینهٔ جاسوسی اقتصادی سایبری متوقف شد.

در می ۲۰۱۴، چین پس از متهم شدن پنج هکر ارتش آزادی‌بخش خلق خود به جاسوسی سایبری، تمام مذاکرات دوجانبه با آمریکا را به حالت تعلیق درآورد. پکن برای به‌روزرسانی سالیانهٔ وضعیت امنیت سایبری، از گفت‌وگوهای مسیر ۲ میان مرکز مطالعات راهبردی و بین‌المللی[3] و مؤسسهٔ روابط بین‌المللی معاصر چین[4] بهره‌برداری کرد، اما اظهار داشت که گفت‌وگوی رسمی فقط پس از حذف اتهامات از سر گرفته خواهد شد. البته این مذاکرات غیررسمی نیز سرانجامی نیافت زیرا تنها چند هفته قبل از ورود شی جین‌پینگ به کاخ سفید برای نخستین دیدار رسمی در سپتامبر ۲۰۱۵، واشینگتن چین را به اعمال تحریم‌های گسترده از جانب خود تهدید کرد.

در پی دیدار رئیس‌جمهوری چین از آمریکا در سال ۲۰۱۵، توافق‌نامه‌ای در زمینهٔ همکاری‌های سایبری بین دو کشور به امضا رسید.[5] این توافق‌نامه متعاقباً به عنوان الگویی برای مدیریت روابط سایبری با انگلستان و آلمان و

---

1. Liz Flora, 2013

۲. Snowden: کارپرداز پیشین سازمان جاسوسی آمریکا و کسی که اسناد زیادی را از فعالیت‌های جاسوسی این کشور افشا کرد.

3. Center for Strategic and International Studies

4. China Institute of Contemporary International Relations

5. U.S.-China Cyber Agreement, 2015

سایر کشورهای غربی نیز مورد استفاده قرار گرفت. در این توافق‌نامه هم برای جلوگیری از تحریم‌ها، و هم به دلیل برخی ملاحظات داخلی، پکن و واشینگتن توافق کردند که با هدف ارائهٔ مزایای رقابتی به شرکت‌ها یا بخش‌های تجاری، هیچ‌گونه سرقت سایبری مالکیت معنوی را، از جمله اسرار تجاری یا سایر اطلاعات محرمانهٔ تجاری، انجام ندهند یا آگاهانه از آن حمایت نکنند.[1] هر دو طرف همچنین به توافق رسیدند که هنجارهای رفتاری فضای سایبری را شناسایی و تأیید کنند و علاوه بر آن نسبت به راه‌اندازی دو کارگروه مشترک (یکی در زمینهٔ امنیت سایبری و دیگری در حوزهٔ جرم سایبری) و نیز برقراری یک خط تماس فوری بحران اقدام نمایند.

البته کارگروه اختصاص‌یافته به مسائل امنیتی تنها یک مرتبه قبل از پایان دولت رئیس‌جمهور اوباما با یکدیگر ملاقات کردند، اما کارگروه جرایم سایبری پیشرفت اندکی را در این زمینه بعداً گزارش دادند. دو طرف همچنین یک خط تماس فوری تعیین کردند و یک آدرس ایمیل به این موضوع اختصاص دادند و همکاری نسبتاً موفقیت‌آمیزی در از بین بردن برخی بات‌نت‌ها[2] و وب‌سایت‌های جعلی با یکدیگر داشتند. پس از دیدار رئیس‌جمهور ترامپ با رئیس‌جمهور شی جین‌پینگ در فلوریدا در آپریل ۲۰۱۷، واشینگتن و پکن با گفت‌وگوی جامع ایالات متحده ـ چین[3] حول چهار محور اصلی از جمله اجرای قانون و امنیت سایبری توافق کردند، هرچند این توافق نیز متعاقباً به دلیل بروز اختلافات گسترده در حوزه‌های مختلف چندان پایدار نماند و می‌توان آن را به نوعی شکست‌خورده تلقی کرد.[4]

---

1. Office of the Press Secretary, White House, September 25, 2015.
2. Botnets
3. United States-China Comprehensive Dialogue
4. Hannah B., 2017

علاوه بر آمریکا، چین سالانه یک گفت‌وگوی امنیتی با انگلستان نیز برگزار می‌کند که در درجهٔ اول بر جرایم سایبری تمرکز دارد. برای مثال، پکن و لندن در ۲۰۱۶ توافق کردند به هر گونه درخواست اطلاعات یا کمک از طرف دیگری در رابطه با فعالیت‌های مخرب سایبری پاسخ فوری دهند. آن‌ها همچنین اظهار داشتند که برای جلوگیری از بهره‌برداری از اینترنت به منظور تحریک، استخدام، تأمین مالی و برنامه‌ریزی فعالیت‌های تروریستی همکاری مؤثرتری خواهند داشت.[1]

علاوه بر ایالات متحده و انگلیس، مهم‌ترین رابطهٔ دوجانبهٔ پکن در زمینه مسائل سایبری با روسیه است. با توجه به نزدیکی مواضع سایبری دو کشور در سطوح ملی و بین‌المللی، دو طرف در زمینهٔ امنیت اطلاعات بین‌المللی در ۲۰۱۵ توافق‌نامهٔ همکاری امضا کردند.[2] این توافق‌نامه، مانند آیین‌نامهٔ رفتاری سال‌های ۲۰۱۱ و ۲۰۱۵، امنیت اطلاعات را به صورت گسترده‌ای تعریف می‌کند به طوری که انتقال اطلاعات تهدیدآمیز برای نظام‌های سیاسی و اجتماعی را نیز در بر گیرد. بر اساس این توافق‌نامه، دو کشور همچنین از نظام مدیریتی چندجانبه و دموکراتیک و شفاف اینترنت که نقش کشورها را در فرایند حکمرانی پررنگ‌تر می‌شمارد استقبال می‌کنند. برخلاف تلاش‌های پیشین، این توافق‌نامه شامل فهرستی از اقدامات قاطعانه، از جمله ایجاد نقاط تماس و کانال‌های ارتباطی و پروژه‌های علمی مشترک، می‌باشد. این پروژه‌ها سالیانه از طریق دو جلسهٔ مشاوره هماهنگی و ارزیابی می‌شوند. علاوه بر این، هر دو کشور توافق کردند که در ایجاد و انتشار هنجارهای قانونی بین‌المللی در فضای سایبری و هماهنگ‌سازی مواضع خود در مجامع مختلف بین‌المللی، از جمله سازمان ملل متحد، همکاری کنند.[3]

---

1. China–UK High Level Security Dialogue: Communique
2. Andrew R., 2015
3. Elaine K., 2015

جنجالی‌ترین مادهٔ توافق‌نامهٔ چین و روسیه، تعهد «عدم تجاوز» بود که به موجب آن، دو کشور توافق کردند از حملهٔ رایانه‌ای علیه یکدیگر خودداری کنند. البته جمله‌بندی این ماده دارای ابهام بود و به نظر نمی‌رسید جاسوسی را نیز شامل شود یا دست‌کم از آن جلوگیری کند. برای مثال، در فوریهٔ ۲۰۱۷ شرکت نرم‌افزاری چیهو ۳۶۰[1] گزارش سالانهٔ خود را در خصوص تهدیدهای مداوم پیشرفتهٔ[2] فعال در چین منتشر کرد و از سی‌وشش گروه جاسوسی در چین از جمله ای‌پی‌تی۲۸[3] که با سازمان جاسوسی روسیه در ارتباط بوده است نام برد. فایرآی[4] خاطرنشان کرد که عوامل چینی می‌کوشند پیمانکاران دفاعی و شرکت‌های مهندسی روسی بخش انرژی را به مخاطره بیندازند[5].

یکی دیگر از مهم‌ترین بخش‌های این توافق‌نامه مربوط به همکاری در زمینهٔ توسعهٔ نسل بعدی فناوری‌های فیلترینگ اینترنت است. فنگ بینگشینگ[6]، ملقب به پدر فایروال بزرگ، و لو وی، رئیس ادارهٔ فضای سایبری چین، در آپریل ۲۰۱۶ به منظور تبلیغ نسخهٔ چینی کنترل اینترنت به مجمع توسعه و امنیت فناوری اطلاعات و ارتباطات روسیه ـ چین[7] در مسکو، به روسیه سفر کردند. همچنین در ماه جون همان سال ولادیمیر پوتین، رئیس‌جمهور روسیه، به پکن رفت و ابلاغیهٔ مشترکی در خصوص فضای سایبری امضا کرد.

چین همچنین متعهد شده تا برخی سخت‌افزارهای مورد نیاز را برای ذخیرهٔ داده‌ها در روسیه تحت قانون یاروویا[8] ارائه کند. این قانون

---

1. Qihoo 360
2. Advanced Persistent Threats (APTs)
3. APT28
۴. FireEye یک شرکت امنیت سایبری واقع در میلپیتاس، کالیفرنیا.
5. Adam Segal, 2017
6. Fang Bingxing
7. Russia-China ICT Development & Security Forum
8. Yarovoya's Law

ارائـه‌دهنـدگان خـدمات اینترنتـی، اپراتورهـای تلفـن همـراه و موتورهـای جست‌وجوگر و سایر خدمات شبکه‌ای را ملزم به ذخیرهٔ کل ترافیک روسیه از جمله تمامی اتاق‌های گفت‌وگوی اختصاصی و ایمیل‌هـا و پسـت‌هـای شبکه‌های اجتماعی به مدت شـش مـاه از تـاریخ اول جـولای ۲۰۱۸ و بـا هزینهٔ خود می‌سازد. قرار است ابَرداده‌ها به مدت سـه سـال ذخیـره شـوند. برخی تخمین زده‌اند که عملیات ذخیره‌سازی مطابق این قـانون ـــ بـیش از ۵۹ میلیون ترابایت داده ــ ممکـن اسـت حـدود ۲/۵ تریلیـون روبـل (۳۹ میلیارد دلار) هزینه در بر داشته باشد. طبق گزارش‌ها، شرکت هواوی بـرای تهیهٔ سخت‌افزار، مذاکراتی با بولات[1]تولیدکنندهٔ تجهیزات مخـابراتی روسـی، انجام داده است[2].

پکن همچنین برای تقویت موقعیت منطقه‌ای و نقـش رهبـری خـود در گروه‌بندی‌های منطقه‌ای و کشورهای درحال‌توسعه از موضـوعات سـایبری استفاده می‌کند. از سال ۲۰۱۲، کارگروه سایبری اتحادیهٔ اروپـا ـ چـین[3] در اجلاس سالانهٔ اتحادیهٔ اروپا و چین شروع به کار، و تا به حال پنج نشسـت برگزار کرده است. به نظر می‌رسد این کارگروه بـرای اتحادیـهٔ اروپـا بیشـتر مجمعی به منظور ابراز نگرانی دربارهٔ خط‌مشـی‌هـای داخلـی چـین دربـارهٔ امنیت سایبری و همچنین بحث و مذاکره در خصوص حاکمیت اینترنـت و نقش دولت در فضای سایبری باشد. با این حال، چین نیز ایـن کـارگروه را محملی برای تقویت همکاری‌ها با اتحادیهٔ اروپا و نیز اعتمادسازی بیشتر در زمینهٔ مسائل سایبری می‌داند.

علاوه بر اتحادیهٔ اروپا، مشـارکت چـین در نشسـت مشـورتی سیاسـت

---

1. Bulat
2. Mikhail K., 2016
3. EU-China Cyber Taskforce

سایبری چین ـ ژاپن ـ کره، مجمع منطقه‌ای آسه‌آن[1] و مجمع آسیایی بوآئو،[2] مجمع همکاری چین و آفریقا،[3] مجمع همکاری چین و کشورهای عربی،[4] انجمن چین و جامعهٔ کشورهای آمریکای لاتین و کارائیب[5] و سازمان مشاورهٔ حقوقی آسیا و آفریقا[6] نیز قابل توجه است.

لایه‌های ساماندهی و اجرایی دیپلماسی سایبری چین

با هدف پیشبرد راهبردهای سایبری فوق، ساماندهی و مدیریت اجرایی دیپلماسی سایبری چین متأثر از سیاست خارجی این کشور و با رویکردی منطقه‌ای و جهانی از سه سطح تشکیل شده است:

سطح اول، عملکرد مستقیم وزارت امور خارجه است که هستهٔ اصلی را تشکیل می‌دهد و خود شامل دو لایه می‌باشد: لایهٔ نخست، وب‌سایت‌های وزارت امور خارجه و سفارتخانه‌ها و کنسولگری‌های خارج از کشور است که این وب‌سایت‌ها اطلاعاتِ دست اول جامعی دربارهٔ چین در اختیار رسانه‌های سایبری مختلف جهان قرار می‌دهند. بر اساس آمار وزارت امور خارجه، تنها در سال ۲۰۱۲، وب‌سایت‌های تحت مدیریت این وزارتخانه بیش از ۱۹۰ هزار خبر منتشر کرده‌اند. مضامین این اخبار شامل فعالیت‌های سازمان‌دهی‌شدهٔ وزارتخانه، فعالیت‌های مقامات دولتی و از همه مهم‌تر، سوابق کنفرانس‌های مطبوعاتی این وزارتخانه است که نگرش دولت به وقایع

1. ASEAN Regional Forum (ARF)
2. Boao Forum for Asia
3. Forum on China-Africa Cooperation (FOCAC)
4. China-Arab States Cooperation Forum
5. Forum of China and the Community of Latin American and Caribbean States
6. Asian-African Legal Consultative Organization

جاری جهان را تشریح می‌کند. با توجه به کمیت و کیفیت اطلاعات، وب‌سایت‌های اصلی وزارت امور خارجه در سال ۲۰۱۳ بیش از ۳۱ میلیارد بازدیدکننده داشته‌اند. لایهٔ دوم، استفاده از رسانه‌های اجتماعی است که امکان برقراری ارتباط مستقیم را برای دیپلماسی سایبری چین فراهم می‌آورد. در سینا ویبو[1] حساب کاربری رسمی دفتر دیپلماسی عمومی، «外交小灵通» (پیام‌رسان کوچک دیپلماسی)، بیش از ۶/۶ میلیون کاربر دارد. این سایت بیش از ۱۱/۵ هزار میکروبلاگ منتشر کرده است.

دفتر دیپلماسی عمومی در فیس‌بوک نیز صفحات دیپلماسی سایبری دولت را مدیریت می‌کند. علاوه بر این، بسیاری از ادارات وزارت امور خارجه نیز به منظور مشارکت در دیپلماسی سایبری چین حساب‌های رسمی خود را در شبکه‌های اجتماعی راه‌اندازی کرده‌اند. این وزارتخانه به عنوان هستهٔ اصلی سیستم نه‌تنها نقش‌آفرین بلکه صحنه‌گردان دیپلماسی سایبری چین نیز می‌باشد.

سطح دومِ دیپلماسی سایبری چین را عملیات سایر مؤسسات و نهادهای رسمی تشکیل می‌دهند. این سطح خود متشکل از دو لایهٔ اجرایی است که به رغم فعالیت‌هایی که به‌خودی‌خود معرف کشورند، از تصویر ملی چین به طور عملی پشتیبانی می‌کنند. لایهٔ اول فعالیت ادارات دولتی است. برای مثال، وزارت آموزش و پرورش و ادارهٔ ملی گردشگری چین از طریق حساب‌های کاربری رسمی خود با مردم در ارتباط‌اند. علاوه بر این، برخی سازمان‌های دولتی، مانند مؤسسهٔ امور خارجهٔ چینی‌ها[2] و کمیتهٔ مشورتی سیاست خارجی،[3] نیز با تبلیغ فعالیت‌های خود در وب‌سایت‌هایشان به پیشبرد دیپلماسی سایبری

1. Sina Weibo
2. Chinese People's Institute of Foreign Affairs
3. Foreign Policy Advisory Committee

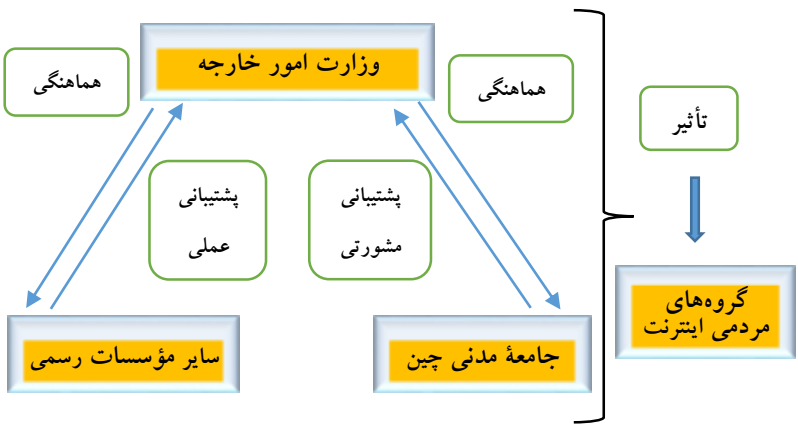
می‌پردازند. این سازمان‌ها پیش از انجام فعالیت‌های مهم باید با ارائهٔ دستور کار خود موافقت وزارت امور خارجه را کسب کنند.[1] لایهٔ دوم، که تأثیر بیشتری نیز دارد، فعالیت‌های رسانه‌های سایبری رسمی است که از این میان روزنامه‌های خلق[2]، چاینا دیلی[3]، سی‌سی‌تی‌وی و شینهوا فعال‌ترین آن‌ها هستند. برای مثال، روزنامه چاینادیلی، یکی از مجریان دیپلماسی عمومی چین، در حساب‌های رسمی توییتری خود مطالبی در حوزهٔ اخبار، فرهنگ و سیاست‌های خارجی چین در اختیار عموم جهان قرار می‌دهد. علاوه بر این، فعالیت‌های چاینا دیلی در دنیای واقعی ارتباطاتش را در فضای سایبری تقویت می‌کند. از جمله مهم‌ترین آن‌ها مجمع سالانهٔ پکن ـ توکیو است که چاینا دیلی و جنرونپو[4] به طور مشترک آن را راه‌اندازی کرده‌اند. از سال ۲۰۰۵، این مجمع با بررسی افکار عمومی چین و ژاپن و ترویج مذاکرات مؤثر میان نخبگان این دو کشور مهم‌ترین بستر برای دیپلماسی عمومی چین بوده است. دستاوردهای این مجمع به طور مرتب در وب‌سایت آن نمایش داده می‌شود. علاوه بر این، فعالیت‌های یک رسانهٔ سایبری رسمی از پشتیبانی و حمایت سایر رسانه‌های سایبری چین برخوردار است. به عنوان نمونه، مجمع پکن ـ توکیو از جانب رسانهٔ بانفوذی همچون تنسنت نیوز[5] پشتیبانی می‌شود. به همین ترتیب، سایر رسانه‌های سایبری چین نیز مطالب انتشاریافتهٔ شینهوا نت را منتشر می‌کنند. همکاری بین رسانه‌های مختلف سایبری چین به دلیل هماهنگی دولت بسیار گسترده و وسیع است.

لایهٔ سوم و نهایی، مشارکت جامعهٔ مدنی چین است که عمدتاً با ارائهٔ

---

1. Wang, J 2006
2. The People
3. ChinaDaily.com, CCTV, Xinhua News and People. cn.
۴. Genron NPO، سازمان غیردولتی ژاپنی.
5. Tencent New

مشاوره از دیپلماسی سایبری پشتیبانی به عمل می‌آورد. این مشارکت از دو بخش تشکیل شده است: اول، نظریات شهروندان چینی است که در آن دربارهٔ خط‌مشی‌های بین‌المللی در انجمن‌های اینترنتی چینی، مانند کلاب تیانیا[1] و گروه خلق[2]، بحث می‌شود[3]. در حقیقت، سیستم تابلوی اعلانات گروه خلق با محکوم شمردن بمباران سفارت چین در یوگسلاوی از سوی آمریکا در ۱۹۹۹ آغاز شد. در صورت درست عمل نکردن دولت چین در یک درگیری بین‌المللی، سیل انتقادات مردمی روانهٔ مجامع اینترنتی می‌شود. اظهارنظر در این انجمن‌ها می‌تواند عاملی اساسی برای روند تصمیم‌گیری و تغییر احتمالی دیپلماسی چین باشد. بنابراین، وزارت امور خارجه مقامات ویژه‌ای را برای انتقال افکار عمومی از تالارهای گفتمان اینترنتی استخدام کرده است. همچنین این وزارتخانه مستقیماً با مردم، اینترنتی مصاحبه می‌کند و نظریات آن‌ها را در دیپلماسی به کار می‌بندد.



نمودار شمارهٔ ۱. ساختار سه‌سطحی دیپلماسی سایبری چین

1. Tianya. Cn
2. People. cn
3. Wang, J 2006

مدیران بخش‌های مختلف وزارتخانه‌ها از طریق این مصاحبه‌ها، سؤالات کاربران چینی را می‌شنوند و به آن‌ها پاسخ می‌دهند. این فعالیت به طور هم‌زمان از چندین رسانهٔ سایبری چینی پخش می‌شود و کاربران چینی می‌توانند از طریق این رسانه‌ها در مصاحبه شرکت کنند. دولت با این روش ارتباط بین مقامات چینی و مردم را در فضای سایبری تسهیل می‌کند. بخش دوم گروه‌های نخبگان جامعهٔ مدنی چین هستند. اندیشکده‌های غیردولتی از لحاظ فکری به دیپلماسی سایبری کمک می‌کنند. برای مثال، مؤسسهٔ چارهار[1] که یک اندیشکدهٔ تخصصی در زمینهٔ مطالعات دیپلماتیک است، در حوزهٔ امور دیپلماتیک چین در اینترنت به بحث و گفت‌وگو می‌پردازد و از دیپلماسی سایبری چین پشتیبانی مشورتی به عمل می‌آورد. هان فانگمینگ[2]، بنیان‌گذار این اتاق فکر، به عنوان نمایندهٔ کمیتهٔ مشورت سیاسی خلق چین[3] و نایب‌رئیس شورای امور خارجه در این کمیته فعالیت می‌کند.

جمع‌بندی و نتیجه‌گیری این فصل

اگرچه چین در راستای برنامه‌ها و سیاست‌هایش برای گسترش نفوذ منطقه‌ای و بین‌المللی سایبری خود یک استراتژی سه‌وجهی مستقل و مدون دارد، اما فهم آن خارج از سیر مواجههٔ چین با سیاست‌های مقابله‌جویانهٔ دنیای غرب و در رأس آن‌ها آمریکا برای محدود ساختن قدرت و نفوذ این کشور امکان‌پذیر نیست.

برخی از ابعاد دیپلماسی سایبری چین با توجه به اهداف این کشور ــ از جمله اعمال حاکمیت ملی در عرصهٔ سایبری و در نتیجه خنثی‌سازی

---

1. Charhar Institute
2. Han Fangming
3. Chinese People's Political Consultative Committee (CPPCC)

تهدیدهای معطوف به امنیت داخلی این کشور از یک سو، و سرمایه‌گذاری‌های کلان تجاری و اقتصادی در حوزهٔ زیرساخت‌های ارتباطی سایر کشورها و در نتیجه گسترش نفوذ جهانی و بین‌المللی چین از سوی دیگر ــ دست‌کم تا کنون دارای موفقیت‌های نسبی بوده است. در واقع نهادینه ساختن این تفکر که فضای سایبری در امتداد فضای فیزیکی و جهان واقعی است و در نتیجه یک فضای حاکمیتی است، تا حد زیادی مرهون تلاش‌های چین و کشورهای همسو با آن همچون روسیه بوده است. به لحاظ گسترش نفوذ منطقه‌ای و بین‌المللی نیز باید گفت که بسیاری از برنامه‌ها و سیاست‌های چین از طریق سرمایه‌گذاری‌های کلان تجاری و اقتصادی در زیرساخت‌های ارتباطی و فناوری کشورهای هدف، به خصوص در کشورهای درحال‌توسعه در جنوب آسیا، آسیای میانه، آفریقا و ...، با استقبال گسترده مواجه شده است.

با این حال، بزرگ‌ترین مانع در پیشبرد اهداف دیپلماسی سایبری چین، همچنان وضعیت روابط این کشور با دنیای غرب و به ویژه سیاست‌های مقابله‌جویانه‌ای است که از سوی واشنگتن علیه پکن اتخاذ شده است. در این خصوص اگر از موضوعات ژئوپلیتیک تاریخی همچون اختلافات دو کشور در حوزهٔ دریای جنوبی چین، جنگ دو کره، مسئلهٔ تایوان، اختلافات مرزی با ژاپن، قضایای هنگ‌کنگ و ... صرف‌نظر کنیم، مهم‌ترین مسئلهٔ چین در عرصهٔ سایبری مسئلهٔ حاکمیت ملی این کشور است که آشکارا از سوی آمریکا و دیگر کشورهای غربی تهدید می‌شود. متقابلاً، مسئلهٔ جاسوسی سایبری، نفوذ چین در سامانه‌های انفورماتیک و زیرساخت‌های اطلاعاتی و ارتباطی کشورهای غربی از طریق فناوری 5G شرکت هوآوی، فناوری ارتباطی شرکت زدتی‌ای، چالش ظهور پلتفرم‌های چینی همچون علی‌بابا، وی‌چت، تیک‌تاک و ... از جمله موضوعات مهمی است که همواره

از سوی کشورهای غربی به عنوان تهدیدات اساسی ناشی از فعالیت‌های سایبری چین مطرح و برجسته می‌شود.

در سال‌های اخیر اختلافات جهان غرب با چین در زمینهٔ فعالیت‌های سایبری به قدری تشدید و گسترش یافته که حتی با وجود تقلیل موضوعاتی تاریخی و سنتی‌تر همچون «سانسور اینترنت»، «آزادی جریان اطلاعات»، و ... در ادبیات روابط آمریکا با چین به موضوعات ثانویه، هنوز چشم‌اندازی روشن از آیندهٔ این روابط وجود ندارد. در آخرین سال از دورهٔ اول ریاست‌جمهوری دونالد ترامپ در آمریکا، تنش‌های سخت مرتبط با عرصهٔ سایبری (از جمله تحریم شرکت‌های فناوری هوآوی و زدتی‌ای چین، لابی گستردهٔ واشنگتن با هم‌پیمانان خود برای لغو قرارداد همکاری با شرکت‌های فناوری چینی، بازداشت چندین دانشمند چینی به اتهام سرقت و جاسوسی سایبری، بستن کنسولگری چین در شهر هیوستون آمریکا) به اوج خود رسید؛ تا حدی که مایک پومپئو، وزیر خارجهٔ وقت آمریکا، در ژوئیهٔ ۲۰۲۰ رسماً از شکست استراتژی تعامل کورکورانهٔ این کشور با چین خبر داد.

در مجموع، باید گفت آن تقابل تاریخی را که زمانی در حوزهٔ فناوری نظامی و تسلیحات کشتارجمعی در دسته‌بندی‌های ایدئولوژیک ایام جنگ سرد بین دو جبههٔ شرق و غرب با محوریت آمریکا ـ شوروی در جریان بود، امروزه در عرصهٔ سایبری و در روابط بین چین و آمریکا (با همراهی کشورهایی همچون انگلستان، کانادا، استرالیا، اتحادیهٔ اروپا و ...) می‌توان ملاحظه نمود؛ تقابلی که محور اصلی آن را فناوری‌های ارتباطی و اطلاعاتی (فناوری 5G، هوش مصنوعی، اینترنت اشیا، شبکه‌های اجتماعی و ...) و نیز استانداردسازی‌های فنی و امنیتی مرتبط با آن‌ها تشکیل می‌دهند. با این تفاوت که این بار چشم‌انداز روشنی از پایان این تقابل فناورانه بین دو جبههٔ اصلی (آمریکا ـ چین) دست‌کم در کوتاه‌مدت وجود ندارد.

منابع

Baker, Peter, “For Trump, a Focus on U.S. Interests and a Disdain for Moralizing”, NewYork Times, April 4, 2017, https://www.nytimes.com.

Beech, Hannah, “Rex Tillerson’s Deferential Visit to China”, New Yorker, March 21, 2017, www.newyorker.com.

China –UK High Level Security Dialogue: Communique”, GOV. UK, June 13, 2016, https://www.gov.uk.

Chinese Firm Hopes to Wire Continent with Same Strategy that Boosted Internet Access Across China,” Global Times, March 13, 2017, www.globaltimes.cn.

Chuanying, Lu, “The International Cyberspace Rule-based System and the China-U.S. New Type of GreatPower Relations”, People’s Daily-Theory Channel, December 2, 2016, http://theory.people.com.cn.

Clinton, Hillary, “Remarks on Internet Freedom” (speech), The Newseum, Washington, DC, January 21, 2010; https://2009 2017.state.gov.

Flora, Liz, “Complete Transcript: Thomas Donilon at Asia Society New York”, Asia Society, March 11, 2013, http://asiasociety.org.

Guang Yang, “Who Are the Leading Players in 5G Standardization? An Assessment for 3GPP 5G Activities”, Startegy Analytics, March 16, 2020, https://www.strategy analytics. com.

Inkster, Nigel, “China’s Cyber Power”, Adelphi Series, no. 456, May 23, 2016.

Joe Uchill, “Obama Administration Confirms Drop in Chinese Cyber Attacks”, The Hill, June 28, 2016, http://thehill. com.

Jonathan Cheng and Josh Chin, “China Hacked South Korea Over Missile Defense, U.S. Firm Says”, Wall Street Journal, April 21, 2017, https://www.wsj.com.

Josh Chin , “I Don’t Declare: China’s Struggle to Sell Vision at Internet Summit”, Wall Street Journal, December 9, 2015, https://blogs.wsj.com.

Key Connectivity Improvements along the Belt and Road in Telecommunications & Aviation Sectors”, China Go Abroad, no. 4, EY, September 2016, https://www.ey.com.

Klementiev, Mikhail, “Russia in Talks with China’s Huawei on Data Storage Technologies’ Licensing”, Sputnik News, August 24, 2016, https:// sputniknews. com.

Korzak, Elaine, “The Next Level for Russia-China Cyberspace Cooperation?”, Net Politics (blog), August 20, 2015, https:// www.cfr.org.

Marks, Joseph, “U.N. body Agrees to U.S. Norms in Cyberspace”, Politico, July 9, 2015, https://www.politico.com.

Marshall, Andrea, “China’s Mighty Telecom Footprint in Africa”, New Security Learning, February, 14, 2011, www. newsecuritylearning.com.

McCarthy, Kieren, “The Firewall Awakens: ICANN’s Exiting

CEO Takes Internet Governance to the Dark Side", The Register, December 18, 2015, https://www.theregister.co.uk.

Mueller, Milton, Network and States: The Global Politics of Internet Governance (Cambridge, MA: MIT Press, 2010).

National Cyberspace Security Strategy", China Copyright and Media, December 27, 2016, https://chinacopyrightandmedia.wordpress.com.

NATO Cooperative Cyber Defence Centre of Excellence, "An Updated Draft of the Code of Conduct Distributed in the United Nations-What's New?", February 10, 2015, https://ccdcoe.org.

Office of the Press Secretary, White House, "Presidential Executive Order on Strengthening the Cyber Security of Federal Networks and Critical Infrastructure", May 11, 2017, https://www.whitehouse.gov.

Osawa, Juro, "Microsoft, Huawei Join in Cyber Security Message", Wall Street Journal, September 13, 2016, https://www.wsj.com.

Perez, Bien, "China's ZTE Takes Over Netas for $101m, Eyes Expansion in Turkey", South China Morning Post, December 6, 2016, https://www.scmp.com.

Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference", Office of the Press Secretary, White House, September 25, 2015, https://obamawhitehouse.archives.gov.

Report of the Group of Governmental Experts on Developments

in the Field of Information and Telecommunications in the Context of International Security", United Nations General Assembly, June 24, 2013; https://www.un.org.

Rosenzweig, Paul, "Revised Draft Trump EO on Cyber Security", Lawfare (blog), February 9, 2017, https://www.lawfareblog.com.

Roth, Andrew, "Russia and China Sign Cooperation Pacts", New York Times, May 8, 2015, https://www.nytimes.com.

Sanger, David E., "Chinese Curb Cyberattacks on U.S. Interests, Report Finds", NewYork Times, June 20, 2016, https://www.nytimes.com.

Sanger, David E., "U.S. Tries Candor to Assure China on Cyberattacks", NewYork Times, April 6, 2014, https://www.nytimes.com.

Scott Warren Harold, Martin C. Libicki, and Astrid Stuth Cevallos, "Getting to Yes with China in Cyberspace", Rand Corporation, 2016, https://www.rand.org.

State Council Information Office, "International Strategy of Cooperation on Cyberspace", March 2, 2017, http://www.scio.gov.cn.

State Council Information Office, People's Republic of China, "International Strategy of Cooperation on Cyberspace", March 2, 2017, http://www.scio.gov.cn.

State Council Information Office, People's Republic of China, "The Internet in China", Xinhua, June 8, 2010, https://www.sbs.ox.ac.uk.

Segal, Adam, Advantage: How American Innovation Can Overcome the Asian Challenge (New York: WW Norton, 2011).

Segal, Adam, "A Fancy Bear Finds Its Way into the Middle Kingdom", Net Politics, Council on Foreign Relations, February 15, 2017, https://www.cfr.org.

Segal, Adam, "Cyberspace Cannot Live without Sovereignty, Says Lu Wei", Asia Unbound (blog), Council on Foreign Relations, December 10, 2013, http://blogs.cfr.org.

Segal, Adam, "The Continued Importance of the U.S.-China Cyber Dialogue", Net Politics (blog), January 23, 2017, https://www.cfr.org.

The Internet in China, Information Office of the State Council of the People's Republic of China, 2010, http://www.china.org.cn.

United Nations, "Developments in the Field of Information and Telecommunications in the Context of International Security", July 22, 2015, https://undocs.org.

Verbergt, Matthias, "China's Huawei Battles to Own the Next Generation of Wireless Technology", Wall Street Journal, February 26, 2017, https://www.wsj.com.

Wang, J 2006, "Shi Xi Dang Dai Zhong Guo De Wang Luo Min Zu Zhu Yi" [Analysis on the Contemporary Online Nationalism in China], World Economics and Politics, v. 2, pp. 1-13.

Wang, Y 2009, "Factor Analysis in China's Diplomacy", World Economics and Politics, v. 9.

Woods, Andrew Keane, "The Tallinn Manual 2.0, Sovereignty 1.0", Lawfare (blog), February 8, 2017, https://www.lawfareblog.com.

Wood, Peter, "China Conducts Anti-Terror Cyber Operations with SCO Partners", China Brief 15, no. 20, Jamestown Foundation, October 19, 2015, https://jamestown.org.

Yiming, Chen, "US Covertly Building 'Shadow Internet' ", People's Daily, June 15, 2011; Yang Ziyan, "Cut Off the Internet' to Challenge Internet Control Power", People's Daily (overseas edition), August 9, 2012, Both Quoted in Michael Swaine, "Chinese Views on Cyber Security in Foreign Relations", China Leadership Monitor no. 42 (Fall 2013), http:// www.hoover.org.

Yuntao, Yang, "The First Authoritative Report on 'Belt and Road' Three-Year Progress Released", China Daily, September 26, 2016, www.chinadaily.com.cn.

فصل ششم

دیپلماسی سایبری روسیه: حاکمیت ملی و امنیت اطلاعات

درآمد

امروزه، عرصهٔ سایبری به کانون روابط بین‌المللی تبدیل شده است و در این میان، روسیه به عنوان یک قدرت سایبری با ویژگی‌های منحصربه‌فرد، بازیگری قهار و باسابقه در این عرصه محسوب می‌شود. روسیه نیز همانند اکثر قدرت‌های جهانی، مسائل سایبری را در مرکز ثقل سیاست خارجی خود قرار داده و بر مبنای ظرفیت‌های خود راهبردهای سایبری جدیدی اتخاذ کرده و دیپلمات‌هایی را برای پیگیری این اهداف استراتژیک برگزیده است.

دیپلماسی سایبری در قرن بیست‌ویکم عبارت است از مدیریت جهانی بدون مرز که در آن، روابط متقابل و درهم‌تنیدگی منافع و منابع نیازمند سازوکارهایی با کارایی بالاست. با توجه به وابستگی روابط پایدار و تجارت جهانی در دنیای جدید به حوزهٔ سایبری، و به دلیل سطح بالای تداخلات منافع ملی با ملاحظات منطقه‌ای و جهانی در دنیای سایبری، رویکردهای جدید این حوزه باید در ابعاد بین‌المللی در نظر گرفته شوند. از این رو روسیه نیز، همانند چین، به خوبی دریافته که به جای تمرکزِ صرف بر دفاع سایبری یا جنگ سایبری، توسعهٔ دیپلماسی سایبری نیز از اهمیت بالایی برخوردار است و باید بر آن نیز متمرکز شود.

تاریخچه و ملاحظات داخلی در ارتباط با حوزهٔ سایبری روسیه

در ادبیات مربوط به حوزهٔ سایبری، روسیه در کنار آمریکا، آلمان، انگلستان و چین یک قدرت سایبری بزرگ[1] محسوب می‌شود. این موضوع از این حیث حائز اهمیت است که بسیاری از تحلیلگران ارشد روسی بی‌توجهی نظام شوروی سابق را به ظرفیت‌های سایبری دلیل اصلی فروپاشی آن می‌دانند و معتقدند این تجربه هرگز نباید دوباره تکرار شود. بنابراین در دو دههٔ گذشته، روسیه تحت هدایت ولادیمیر پوتین و بر اساس تجربهٔ جنگ سرد، فضای سایبری و بستر اینترنت را زمینهٔ جدید جنگ با ایدئولوژی دنیای غرب می‌داند.

مهم‌ترین دغدغهٔ روسیه در دیپلماسی سایبری، اصل حاکمیت ملی کشور و اطمینان از عدم مداخلهٔ سایر کشورها، به خصوص از طریق حملات سایبری به بنیان‌ها و ساختارهای نظام سیاسی و اقتصادی و اجتماعی روسیه، است. در این خصوص، سیاستمداران روسیه همواره بر برخورداری از درجه‌ای از قدرت سایبری متقابل تأکید ورزیده‌اند که بر اساس آن بتوان «در تأسیسات و سیستم‌های مهم نظامی، صنعتی، ارتباطی و اداری دشمن اختلال ایجاد کرد، فشار اطلاعاتی ـ روانی زیادی با هدف اضمحلال رهبری نظامی ـ سیاسی دشمن وارد ساخت، و سربازان و جمعیت دشمن را هدف قرار داد» .

در نگاه رهبران روسیه، تضمین حاکمیت ملی این کشور نه از طریق آزادی اطلاعات، بلکه تنها از طریق امنیت اطلاعات در این کشور تضمین می‌شود. امنیت اطلاعات مفهومی است که در دیپلماسی سایبری کشور چین نیز مشهود است و این دو کشور در کنار موضوع حاکمیت ملی، همواره از این مقوله به عنوان یک راهبرد مهم در دکترین سیاسی و امنیتی خود در ارتباط با حوزهٔ سایبری استفاده کرده‌اند.

---

1. Cyber Heavyweight

به همین منظور و با هدف اطمینان از دو اصل تضمین حاکمیت ملی و نیز امنیت اطلاعات، روسیه از دو بازوی قدرتمند برخوردار است: ۱. سرویس اطلاعاتی این کشور[1]، ۲. لابراتوارهای کاسپراسکای.[2] در این خصوص، در حالی که لابراتوارهای کاسپراسکای برتری یا قدرت مقابلهٔ فناوری روسیه را با فناوری کشورهای غربی تضمین می‌کنند، سرویس اطلاعاتی روسیه یک بازوی تهاجمی محسوب می‌شود که تنها و مهم‌ترین هدف آن «مانیتور اینترنت» روسیه و نیز «افزایش ظرفیت تهاجمی» این کشور با هدف تضمین امنیت اطلاعاتی آن است. بر همین اساس، در دکترین امنیت اطلاعاتی روسیه آمده است که «امنیت ملی فدراسیون روسیه به طور وثیقی، وابسته به درجهٔ بالایی از امنیت اطلاعاتی روسیه است؛ وابستگی‌ای که چیرگی فناوری روسیه را می‌طلبد».[3]

مفهوم امنیت اطلاعاتی در دیپلماسی سایبری روسیه دو دلالت بسیار مهم دارد: نخست، به این کشور اجازهٔ مانیتور و سانسور و فیلترینگ جریان اطلاعات به هر میزان و درجهٔ لازم را می‌دهد. بر همین اساس، تمامی سرویس‌دهندگان اینترنتی[4] روسیه موظف به نصب نرم‌افزارهایی هستند که به سرویس اطلاعاتی این کشور اجازهٔ رصد جریان‌های اطلاعاتی را، از جمله ایمیل‌ها، می‌دهند. تمامی اطلاعات و داده‌های این کشور باید از کامپیوترهای سرویس اطلاعاتی این کشور عبور کنند و در آن ذخیره شوند. همچنین کمپانی‌های خارجی مقیم این کشور، از جمله مایکروسافت، موظف‌اند کدهای منابع و ذخایر داده‌های خود را در اختیار سرویس

1. The Federal Security Service (FSB)
2. Kaspersky Labs
3. Ryan C. Maness & Brandon Valeriano (2015)
4. Internet Service Providers (ISPs)

اطلاعاتی روسیه قرار دهند. دوم، این کشور را به لحاظ دفاعی، در مقایسه با کشورهای غربی، در یک موقعیت برتر قرار می‌دهد. در حالی که به دلیل مؤلفهٔ آزادی اطلاعات در دیپلماسی سایبری کشورهای غربی همچون آمریکا، جریان اطلاعات و منابع اطلاعاتی این کشورها همواره در درجه‌ای از ریسک و خطر دستبرد یا جاسوسی سایبری قرار دارند، روسیه توانسته است از طریق مکانیسم‌های امنیتی، لایه‌های دفاعی قدرتمندی در مقابله با هر گونه حملهٔ سایبری یا جاسوسی سایبری خارجی ایجاد کند که عمدهٔ آن از طریق شبکهٔ نرم‌افزاری قدرتمند کاسپراسکای تضمین می‌شود. این برتری دفاعی در عرصهٔ سایبری نوعی قدرت و جسارت و ظرفیت به این کشور می‌دهد تا با اطمینان بیشتری از قدرت سایبری به عنوان یک اهرم در پیشبرد سیاست خارجی خود استفاده کند و به همین دلیل، در ادبیات حوزهٔ سایبری، روسیه خطرناک‌ترین[1] و قَدَرترین[2] قدرت سایبری تلقی می‌شود.

بر این اساس و بر طبق برآوردهای محققان غربی، روسیه نه‌تنها هرگز ابایی از استفاده از قدرت سایبری‌اش برای پیشبرد سیاست خارجی خود ندارد (همانند تجربهٔ حملات سایبری به استونی ۲۰۰۷ و گرجستان ۲۰۰۸)، بلکه حتی توانایی و قدرت خنثی‌سازی و افشای بسیاری از حملات سایبری یا جاسوسی سایبری قدرت‌های غربی از این کشور و نیز کشورهای همسو با خود (همچون مورد جاسوسی استاکس‌نت از سایت‌های هسته‌ای ایران) را نیز دارد. با این حال، انزوای سیاسی پس از حملات سایبری به دو کشور استونی و گرجستان و محکومیتی که از سوی جامعهٔ بین‌المللی به دنبال داشت، روسیه را بیش از گذشته در ارتباط با

1. The Most Dangreous
2. The Most Cyber-Capable State

استفاده از قدرت سایبری به فکر واداشت و اینکه تنها باید در شرایط بسیار حساس از قدرت سایبری بهره جوید. کما اینکه سوابق حملات سایبری صورت‌گرفته در دو دهۀ اخیر نیز نشان می‌دهد که این کشور کمتر از این نوع حملات در خارجِ حوزۀ جغرافیایی شوروی سابق استفاده کرده است.

مبانی فکری دیپلماسی سایبری روسیه

با توجه به ملاحظات داخلی سیاسی و به خصوص اینکه روسیه از منظر ارتباطات بین‌الملل در موضع نسبتاً پایین‌تری در مقایسه با دموکراسی‌های غربی قرار دارد، این کشور از لحاظ نظری تمایل زیادی به رویکرد مشارکتی در ارتباط با دیپلماسی سایبری از خود نشان داده است. به عبارت دیگر، از نظر روسیه تنها تدابیر مشارکتی می‌تواند موجب افزایش ثبات و امنیت در حوزۀ امنیت فناوری سایبری، به خصوص در عرصۀ بین‌المللی، شود. بر این اساس، مبنای رویکرد مشارکتی روسیه بر چهار پایه استوار است که باید از سوی همۀ کشورها دنبال شود: ۱. تعیین هنجارها و قوانین و اصول رفتار مسئولانۀ دولت‌ها، ۲. تعیین اقدامات داوطلبانه (و نه اجباری) به منظور ارتقای شفافیت، ۳. اطمینان‌بخشی و اعتمادسازی بین کشورها، و ۴. ظرفیت‌سازی و توسعه در حوزۀ سایبری. با همین نگاه و بر اساس این مبانی فکری، تمایز آشکار رویکرد روسیه از رویکرد آمریکا به مقولۀ سایبری آشکار می‌شود. روسیه برخلاف آمریکا، که به دنبال تعمیم و تحمیل قوانین و ارزش‌های ملی خود در فضای سایبری در مقیاس جهانی است، بیشتر به دنبال تدوین استانداردها و کدهای رفتاری در فضای سایبری از طریق مشارکت بین‌المللی است.

در واقع از منظر دیپلماسی سایبری روسیه، تنها از طریق این تدابیر مشارکتی تمامی کشورهاست که می‌توان به فناوری اطلاعات و ارتباطاتِ

مسالمت‌آمیز و ایمن و باز امیدوار بود. همچنین به همین دلیل، روسیه در مقابل دیپلماسی سایبری کشورهای غربی که فقط به امنیت سایبری ـــ که به ضرورت محافظت از نرم‌افزار و سخت‌افزار و زیرساخت‌های کلیدی اطلاعاتی و همچنین اطلاعات کاربر در برابر خرابکاری اشاره دارد ـــ بر امنیت اطلاعات بین‌المللی تأکید دارد. این مفهوم هم امنیت سایبری را در بر می‌گیرد و هم بر جلوگیری از سوءاستفاده از فناوری‌های اطلاعات و ارتباطات در زمینهٔ اهداف سیاسی (همانند آنچه به انقلاب‌های رنگی در اقمار شوروی سابق یا بهار عربی منجر شد) تمرکز دارد.[1]

همچنین از منظر دیپلماسی سایبری روسیه، قوانین بین‌المللی و به ویژه منشور سازمان ملل متحد در فضای سایبری قابلیت تسرّی دارد و این مسئله دولت‌ها و حاکمیت‌ها را متعهد می‌سازد که ۱. از قلمرو آن‌ها نباید برای اقدامات سایبریِ غیرقانونی در سطح بین‌المللی استفاده شود؛ ۲. نباید فعالیت‌های حوزهٔ فناوری اطلاعات و ارتباطات را، که از روی عمد به زیرساخت‌های مهم آسیب می‌رسانند، آگاهانه پشتیبانی کنند؛ و ۳. به دنبال جلوگیری از گسترش فناوری‌های مخرب و اعمال خرابکارانهٔ پنهانی باشند.

اهداف اصلی دیپلماسی سایبری روسیه

به طور کلی هدف سیاست خارجی روسیه از یک سو، تثبیت و نمایش قدرت خود به عنوان یک بازیگر مهم جهانی است و از سوی دیگر، تلاش دارد تا ضمن تطهیر زوایای تاریک بازمانده از دورهٔ شوروی سابق، وجهه‌ای مدرن از روسیهٔ توسعه‌یافته به نمایش بگذارد. اهداف روسیه در دیپلماسی سایبری به عنوان یک عرصهٔ جدید نیز از این دو هدفِ مبنایی مستثنا نیست.

---

1. Nicu Popescu and Stanislav Secrieru, 2018

روسیه در این زمینه، به طور موازی اقداماتی به شرح ذیل دنبال می‌کند:

۱. پیگیری اصول و مبانی دیپلماسی سایبری خود در مجامع جهانی به خصوص با همکاری و حمایت کشورهای همسو. برای مثال، روسیه امیدوار است از طریق برگزاری نشست‌های گروه کارشناسان دولتی سازمان ملل، قطعنامه‌های مجمع عمومی سازمان ملل متحد را تقویت کند. در این رابطه، روسیه بر کشورهای عضو سازمان پیمان امنیت جمعی[1] سازمان همکاری شانگهای و بریکس تمرکز کرده است و آن‌ها نیز حمایت اولیهٔ خود را از موضع مسکو ابراز نموده‌اند. همکاری مداوم و تقویت‌شده در حوزهٔ مسائل سایبری با سازمان‌های منطقه‌ای همچنان از اهمیت بالایی در دستور کار دیپلماسی سایبری روسیه برخوردار است.

روسیه در این زمینه، فراز و نشیب‌های زیادی در مقایسه با مواضع سابق خود تجربه کرده، به طوری که از برخی مواضع قبلی خود عقب‌نشینی نموده و در برخی دیگر نیز دست به مقابله‌جویی‌هایی با ابتکارات دموکراسی‌های غربی زده است. برای مثال، روسیه حامی اصلی کنوانسیون جدید مقابله با جرایم سایبری است که حدود دو سال پیش به سازمان ملل ارائه شد. این ابتکار روسیه آشکارا در مقابل کنوانسیون بوداپست در حوزهٔ جرایم سایبری است که شورای اروپا آن را تصویب کرد. به طور مشخص، روسیه مخالف بند ۳۲ کنوانسیون بوداپست است که امکان دسترسی فرامرزی به اطلاعات رایانه‌ای ذخیره‌شده را بدون مجوز قبلی در طول تحقیقات جرایم سایبری فراهم می‌کند.[2] این در حالی است که روسیه خواستار تعدیل بند ۳۲ و تغییر آن به «همکاری اختیاری و نه اجباری» است.

---

1. Collective Security Treaty Organization (CSTO)
2. Convention on Cybercrime, 2001

۲. رسیدن به نوعی «توازن استراتژیک» با آمریکا در عرصهٔ سایبری که به خصوص از زمان به قدرت رسیدن دونالد ترامپ در آمریکا در ذهن دولتمردان روسی تقویت شده است. در این زمینه، یکی از اهداف اصلی روسیه عادی‌سازی روابط با ایالات متحده است. در سال ۲۰۱۷، مسکو به واشینگتن پیشنهاد داد که توافق‌نامهٔ دوجانبه‌ای دربارهٔ جلوگیری از فعالیت‌های نظامی خطرناک در فضای سایبری امضا کنند. پاسخ ایالات متحده آمریکا تا به حال واضح نبوده است. واشینگتن ابتدا با مذاکرات موافقت کرد، اما درست یک روز قبل از آغاز توافق‌نامه در پایان فوریهٔ ۲۰۱۸ در ژنو، آن را به تعویق انداخت. احتمال دارد یکی از دلایل این تردید تحقیقات ایالات متحده دربارهٔ مداخلهٔ احتمالی روسیه در انتخابات ریاست‌جمهوری سال ۲۰۱۶ باشد. دراین‌باره، قابل توجه است که در سال ۲۰۱۷ مسکو به واشینگتن پیشنهاد داد که توافق‌نامهٔ عدم مداخله در امور سیاسی یکدیگر را امضا کنند؛ موضوعی که دولت آمریکا باز هم از پیگیری آن خودداری کرد.[1] جان هانتسمن، سفیر آمریکا در مسکو، در مارس ۲۰۱۸ اعلام کرد که واشینگتن ممکن است دوباره به مذاکره دربارهٔ مسائل سایبری با مسکو تمایل داشته باشد مشروط بر اینکه هیچ گونه مداخله‌ای در انتخابات ماه نوامبر صورت نگیرد، اما مقامات روسی با قاطعیت، مداخلهٔ مسکو در سیاست داخلی آمریکا را انکار می‌کنند و تمایل ندارند حتی دربارهٔ پیشنهاد ضمانت یک‌طرفهٔ مبنی بر عدم مداخلات آتی وارد بحث شوند.

هرچند بدیهی است که با توجه به تنشی که روسیه در روابط با آمریکا و به تبع آن با دموکراسی‌های غربی مواجهه است، دیپلماسی سایبری این کشور با چالش‌ها و دست‌اندازی‌های اساسی روبه‌رو است، با این حال این مسئله

1. John H., 2017

مانع از آن نشده تا روسیه از پیگیری اصول و مؤلفه‌های اصلی دیپلماسی سایبری خود دست بردارد. در این خصوص روسیه همانند چین دو رویکرد عمده را در دیپلماسی سایبری خود به طور هم‌زمان پیش می‌برد:

۱. رویکرد جهانی بر مبنای سازمان ملل متحد: تاریخچهٔ تعاملات دیپلماتیک روسیه در زمینهٔ تأثیر فناوری اطلاعات و ارتباطات بر ثبات بین‌المللی حاکی از آن است که هدف برنامه‌های مسکو از همان ابتدا جلوگیری از درگیری‌ها و رقابت تسلیحاتی سایبری بین کشورها بوده است.[1] اوایل سال ۱۹۹۸، زمانی که مسکو نخستین قطعنامهٔ «تحولات حوزهٔ اطلاعات و ارتباطات از راه دور در زمینهٔ امنیت بین‌المللی» را در مجمع عمومی سازمان ملل متحد[2] اعلام کرد، روسیه با اشاره به چنین خطرهایی موضوع دخالت در امور داخلی کشورها را در دستور کار سیاست بین‌المللی قرار داد[3].

این سند، که بدون رأی‌گیری به تصویب رسیده بود، سبب ایجاد این نگرانی شد که از فناوری‌ها و ابزار نوین می‌توان به طور بالقوه در زمینهٔ مقاصدی مغایر با حفظ ثبات و امنیت بین‌المللی استفاده کرد و این مسئله ممکن است بر امنیت کشورها تأثیر منفی بگذارد. روسیه به منظور قابل قبول ساختن این قطعنامه برای اکثر کشورها، بر اهمیت نیاز به جلوگیری از سوءاستفاده از منابع اطلاعاتی و فناوری‌ها در زمینهٔ اهداف جنایت‌کارانه یا تروریستی تأکید ورزید. ایگور ایوانوف[4]، وزیر امور خارجهٔ وقت روسیه، در اظهارات خود فراتر رفت و خواستار رسیدگی به تهدید دیگری شد؛ تهدید نظامی‌سازی فضای سایبری با تأکید بر تأثیرات مخرب بالقوهٔ تسلیحات سایبری[5].

در سال ۱۹۹۹، روسیه با افزودن دو نکتهٔ حائز اهمیت برای مسکو

---

1. Elena Ch., 2013
2. UNGA
3. UN General Assembly, Resolution A/RES/53/70, 1999.
4. Igor Ivanov
5. Elena Ch., 2016

قطعنامهٔ دیگری ارائه داد: احتمال سوءاستفاده از فضای سایبری به منظور اهداف نظامی و لزوم ارائهٔ قوانین در زمینهٔ چگونگی کاهش این خطرات از سوی جامعهٔ جهانی. البته باید توجه داشت که در آن مقطع، سطح ارتباطات سایبری و آسیب‌پذیری کشورها در مقایسه با وضعیت فعلی امروزی بسیار کمتر بود. برای مثال، در دسامبر ۱۹۹۹ در سرتاسر جهان کلاً ۲۴۸ میلیون کاربر اینترنتی وجود داشت، و این تهدیدهای نوظهور در همهٔ کشورها مشهود نبودند یا دست‌کم به طور رسمی شناخته نشده بودند.[1] با این حال، هنگامی که در ۲۰۰۹ مجمع عمومی سازمان ملل متحد قطعنامهٔ مهم دیگری با عنوان «ایجاد فرهنگ جهانی امنیت سایبری و ارزیابی تلاش‌های ملی به منظور محافظت از زیرساخت‌های مهم اطلاعاتی» را به تصویب رساند، تلاش‌های دیپلماتیک روسیه به نتیجه رسید.[2]

از نظر مسکو، ابتکار سازمان ملل در سال ۲۰۰۴ در راه‌اندازی گروه کارشناسان دولتی تحولات حوزهٔ اطلاعات و ارتباطات از راه دور در زمینهٔ امنیت بین‌المللی[3] اقدام امیدوارکننده‌تری بود. روسیه، که به همراه ایالات متحده یکی از اصلی‌ترین اعضای این گروه بود، امید داشت که تلاش‌های این نهاد منتهی به تصویب نوعی قوانین اخلاقی برای کشورها در فضای سایبری شود. جلوگیری از نظامی‌سازی این عرصه دیگر یک هدف واقع‌بینانه نبود، زیرا تمام قدرت‌های بزرگ سایبری، از جمله خود روسیه، به طور فعال در حال توسعهٔ این نوع پتانسیل‌ها بودند. بنابراین، مسکو طبق این اصل وارد عمل شد: «چنانچه قادر نیستید مانع کاری شوید، سعی کنید آن را نظام‌مند سازید».

---

1. Internet Growth Statistics, (1995-2017)
2. Resolution Adopted by the General Assembly on 21 December 2009.
3. Group of Governmental Experts (UN GGE)

فعالیت‌های این گروه در ابتدا نتایج حائز اهمیتی به دنبال نداشت تا آنکه سرانجام در سال ۲۰۱۳، با هدف «ترویج بستر فناوری اطلاعات و ارتباطات مسالمت‌آمیز، ایمن، باز و مشارکتی»، پیش‌نویس یک گزارش اجماع را آماده کرد و اظهار داشت که «تدابیر مشارکتی‌ای که می‌تواند موجب افزایش ثبات و امنیت شود عبارت‌اند از: هنجارها، قوانین و اصول رفتار مسئولانهٔ دولت‌ها، اقدامات داوطلبانه به منظور ارتقای شفافیت، اطمینان و اعتماد بین کشورها و ظرفیت‌سازی». در این گزارش، برای نخستین‌بار تصریح شده است که «قوانین بین‌المللی و به ویژه منشور سازمان ملل متحد، در فضای سایبری قابل اجراست» و در عین حال اظهار داشت که «حاکمیت دولتی و هنجارها و اصول بین‌المللیِ برگرفته از حاکمیت دربارهٔ فعالیت‌های دولت در زمینهٔ فناوری اطلاعات و ارتباطات و صلاحیت آن‌ها با توجه به زیرساخت‌های فناوری اطلاعات و ارتباطات اعمال می‌شود». همچنین این گروه توصیه‌هایی در حوزهٔ اقدامات داوطلبانهٔ اعتمادسازی و ظرفیت‌سازی ارائه داد.

سال ۲۰۱۵ دستاوردی بزرگ برای دیپلماسی سایبری روسیه تلقی شد و آن زمانی بود که گزارش گروه کارشناسان دولتی سازمان ملل متحد پایه و اساس یک آیین‌نامهٔ اخلاقی سایبری دولتی[1] را در سطح بین‌المللی فراهم کرد. این متن شامل یازده هنجار بنیادین غیرسیاسی بود، از جمله اینکه دولت‌ها نباید آگاهانه اجازه دهند که از قلمرو آن‌ها برای اقدامات سایبری غیرقانونی در سطح بین‌المللی استفاده شود؛ نباید فعالیت‌های حوزهٔ فناوری اطلاعات و ارتباطات را، که از روی عمد به زیرساخت‌های مهم آسیب می‌رسانند، آگاهانه پشتیبانی نمایند؛ و در آخر، باید به دنبال جلوگیری از

---

۱. روسیه پیش‌تر در سال ۲۰۱۱، این آیین‌نامهٔ اخلاقی را از طریق سازمان همکاری شانگهای ارائه کرده بود که جزئیات آن در بخش بعدی آمده است.

گسترش فناوری‌های مخرب و اَعمال خرابکارانهٔ پنهانی باشند. تمامی این بندها، مبتنی بر اهداف و مبانی فکری دیپلماسی سایبری روسیه بود که به ابتکار این کشور و از طریق سازمان همکاری شانگهای مطرح شد.

۲. رویکردهای منطقه‌ای بر مبنای تعاملات دوجانبه و چندجانبه: روسیه هم‌زمان با رویکرد جهانی خود از طریق سازمان ملل، دیپلماسی سایبری خود را به صورت منطقه‌ای و با تلاش برای ترغیب و جلب همکاری سایر کشورها دنبال می‌کند. به عبارت دیگر، روسیه هم‌زمان با تلاش‌های جهانی، به دنبال شبکه‌ای از توافقات دوجانبه و چندجانبه با هدف اطمینان‌بخشی و تقویت اعتماد بین خود و سایر شرکای منطقه‌ای است و در این زمینه، به خصوص از کشورهای همسو با خود که بیشتر در صدد ارتقای حاکمیت دولتی و کنترل شدیدتر دولت بر اینترنت هستند، بهره‌مند بوده است. می‌توان رویکرد منطقه‌ای روسیه را در پیشبرد اهداف دیپلماسی سایبری به دو محور تقسیم کرد:

الف. از طریق تعامل بر مبنای سازمان‌های منطقه‌ای: در سپتامبر ۲۰۱۱ چهار کشور از سازمان همکاری شانگهای ــ روسیه، چین، تاجیکستان، و ازبکستان ــ یک آیین‌نامهٔ اخلاقی بین‌المللی برای امنیت اطلاعات ارائه نمودند.[1] چند روز بعد، روسیه نیز پیش‌نویس کنوانسیون بین‌المللی امنیت اطلاعات را به سازمان ملل تحویل داد. هر دو متن بازتاب‌دهندهٔ تحول تفکر سیاست خارجی روسیه در حوزهٔ سایبری هستند. در حالی که کشورهای غربی در آن زمان فقط از اصطلاح امنیت سایبری ــ که به ضرورتِ محافظت از نرم‌افزار و سخت‌افزار و همچنین اطلاعات کاربر در برابر افراد خرابکار اشاره دارد ــ استفاده می‌کردند، روسیه اصطلاح دیگری را اشاعه داد: «امنیت

1. UN Doc A/66/359

اطلاعات بین‌المللی». این مفهوم نه‌تنها امنیت سایبری را در بر می‌گیرد، بلکه بر جلوگیری از سوءاستفاده از فناوری‌های اطلاعات و ارتباطات در زمینهٔ اهداف سیاسی نیز تمرکز دارد. پیش‌نویس آیین‌نامهٔ اخلاقی و پیش‌نویس کنوانسیون ۲۰۱۱ ارائه‌شدهٔ روسیه بر اهمیت حاکمیت دولت در فضای سایبری تأکید دارند. علاوه بر این، پیش‌نویس کنوانسیون کشورها را به تأیید این امر ترغیب می‌کند که جنگ اطلاعاتی تهاجمی، «جنایتی علیه صلح و امنیت بین‌المللی» است و از آن‌ها می‌خواهد که از استفاده از فناوری‌های اطلاعاتی و ارتباطی به منظور مداخله در امور داخلی سایر کشورها خودداری کنند.[1] برخی تهدیدهای اصلی ذکرشده در این متن عبارت‌اند از: اقداماتی که با هدف تضعیف سیستم سیاسی و اقتصادی و اجتماعی یک دولت دیگر، و همچنین جنگ روانی که به منظور بی‌ثبات کردن جامعهٔ یک کشور صورت می‌گیرند. این پیش‌نویس همچنین به توضیح چگونگی جلوگیری از درگیری‌های نظامی و همچنین استفادهٔ شبکه‌های تروریستی از اینترنت و جرایم سایبری می‌پردازد. حال آنکه تأکید بر عدم دخالت در امور داخلی یک کشور به طور واضح یکی از دلایل اصلی روسیه برای تهیهٔ این پیش‌نویس بوده است.[2]

یکی از دلایل این نوع تفکرِ روسیه آن است که این کنوانسیون هم‌زمان با مسئلهٔ جهانی نقش فناوری‌های جدید ــ به ویژه رسانه‌های اجتماعی ــ در قیام‌های مردمی سال ۲۰۱۱ در کشورهای عربی، و همچنین در ایران و برخی کشورهای دیگر در فضای پساشوروی قبل از آن مطرح شد. تعداد قابل توجهی از افراد مؤثر بر تفکر مسکو در حوزهٔ دیجیتال متقاعد شده بودند که

---

1. Convention on International Information Security (Concept), September 22, 2011.

2. Russian Ministry of Foreign Affairs, 2011

«بهار عربی» و «انقلاب‌های رنگی» از بیرون کشور نشئت گرفته‌اند و مدیریت می‌شوند و از اینترنت به عنوان ابزاری برای ایجاد و برانگیختن احساسات ضد حکومتی بهره‌برداری شده است. بنابراین، محافظت از سیستم سیاسی روسیه در برابر نفوذ بیگانگان هدف اصلی بود. بدین منظور، حتی در داخل کشور نیز به مقررات ملی سخت‌گیرانه‌تری نیاز بود؛ البته این قوانین به اندازهٔ مقررات وضع‌شدهٔ چین مداخله‌گر نبود، اما از برخی جهات به قوانین آن کشور شباهت داشت. نمونهٔ آن، قانون فهرست سیاه اینترنت بود که در سال ۲۰۱۲ در روسیه به تصویب رسید و به مقامات این اجازه را می‌داد که برخی وب‌سایت‌ها را بدون محاکمه در فهرست سیاه قرار دهند و تعطیل کنند.[1]

البته باید دانست که تمام اعضای سازمان پیمان امنیت جمعی دغدغهٔ این تهدیدها را داشتند و مشتاقانه از برنامه‌های روسیه حمایت می‌کردند. نمایندگان این سازمان طی میزگردی در سال ۲۰۱۳، با ابراز نگرانی از شکست در جنگ اطلاعاتی در برابر «دشمنان غربی»، دربارهٔ لزوم «ابزار ضد تبلیغ» توافق کردند. تلاش‌های دیپلماتیک روسیه در گروه بریکس نیز کاملاً موفقیت‌آمیز بود. در سال ۲۰۱۵ به دنبال طرح مسکو، بریکس با ایجاد یک کارگروه در حوزهٔ فناوری اطلاعات و ارتباطات توافق کرد.

ب. از طریق تعامل بر مبنای مذاکرات دوجانبه: به موازات سازمان‌های منطقه‌ای، مسکو به طور هم‌زمان به دنبال شبکه‌ای از توافقات دوجانبه با هدف اعتمادسازی دوجانبه و نیز ایجاد اطمینان با شرکای اصلی خود بوده است. در این مسیر در سال ۲۰۱۳، روسیه نخستین توافق سایبری دوجانبه را با ایالات متحده امضا کرد. این توافق‌نامه تماماً بر جنبه‌های فنی همکاری متمرکز بود: به منظور تبادل اطلاعات بین تیم‌های ملی پاسخگویی به

1. Federal Law of Russian Federation NO. 139-FZ

فوریت‌های رایانه‌ای و ایجاد خطوط ارتباطی فوری مربوط به حوادث سایبری و کانال‌های تبادل اطلاعات حوادث بین مراکز کاهش خطر هسته‌ای. هرچند مسکو امیدوار بود که این اقدام گامی اولیه برای رسیدن به یک پیمان بسیار جامع با آمریکا باشد، اما درگیری‌های اوکراین در سال ۲۰۱۴ و سپس تنش سیاسی روسیه در روابط با آمریکا، به خصوص موضوع «مداخلهٔ روسیه در انتخابات سال ۲۰۱۶ آمریکا»، موجب نافرجام ماندن این برنامه‌ها شد.

علاوه بر ایالات متحده، بیشترین میزان همکاری دوجانبه روسیه در حوزهٔ سایبری با کشور چین بوده است که به طور سنتی مهم‌ترین متحد این کشور در عرصهٔ منازعات تاریخی با کشورهای غربی محسوب می‌شود. روسیه و چین به طور مشخص در سال ۲۰۱۵ یک توافق‌نامهٔ دوجانبه در حوزهٔ سایبری امضا کردند که محتوای آن چندین زمینه را برای همکاری متقابل مشخص می‌کرد. این زمینه‌ها شامل موارد ذیل می‌شدند: ۱. امنیت اطلاعات بین‌المللی، به طوری که دو کشور را به انتقال و تبادل اطلاعاتی که برای نظام‌های سیاسی و اجتماعی یکدیگر تهدیدآمیز تلقی می‌شد، متعهد می‌ساخت؛ ۲. حمایت از یک «نظام مدیریتی چندجانبه و دموکراتیک و شفاف» برای اینترنت که آشکارا نوعی مقابله جویی با حکمرانی آمریکا بر اینترنت از طریق آیکان محسوب می‌شد؛ ۳. ایجاد نقاط تماس و کانال‌های ارتباطی مشترک برای مواقع اضطراری؛ ۴. تعهد به عدم تجاوز که بر اساس آن روسیه و چین توافق کردند از حملهٔ رایانه‌ای علیه یکدیگر خودداری کنند؛ ۵. همکاری در زمینهٔ توسعهٔ نسل بعدی فناوری‌های فیلترینگ اینترنت؛[۱] ۶. تلاش برای ایجاد و ترویج هنجارهای قانونی بین‌المللی در زمینهٔ فضای سایبری و هماهنگ‌سازی مواضع خود در

---

۱. لازم به توضیح است که محور «تعهد به عدم تجاوز» این توافق‌نامه، بعداً و در پی وقوع برخی حملات سایبری مشکوک، موجب ایجاد ابهاماتی در روابط بین دو کشور شد.

مجامع مختلف بین‌المللی، از جمله در سازمان ملل متحد.[1]

به موازات کشورهای آمریکا و چین، روسیه برای همکاری سایبری با کشورهای آلمان، فرانسه، اسرائیل، کرهٔ جنوبی و ژاپن نیز تلاش‌های زیادی کرده است. برای روسیه کشورهایی مثل آلمان، فرانسه، اسرائیل و ژاپن از اهمیت بسیار بالایی برخوردارند و حتی اسامی این کشورها در اسناد داخلی شورای امنیت روسیه، در اولویت قرار گرفته‌اند[2]، اما تمامی این تلاش‌ها عمدتاً به دلیل تفاوت در رویکردهای آن‌ها به حوزهٔ سایبری، سوءظن کشورهای غربی به اهداف روسیه و نیز اتهامات واردشده به روسیه مبنی بر دخالت‌های سایبری این کشور در امور کشورهای غربی، ناکام مانده است. برای مثال، مذاکرات پیش‌بینی‌شدهٔ روسیه با آلمان، با این ادعا که دولت روسیه در پسِ گروه هکری «ماریا اسنیک» ــ که حملهٔ سایبری به وزارت امور خارجهٔ آلمان را ترتیب داده بود ــ قرار دارد، قبل از شروع با شکست مواجه شد.

با این حال، از سال ۲۰۱۵ این کشور توانست توافق‌نامه‌هایی دوجانبه در زمینهٔ اعتمادسازی و همکاری در فضای سایبری، هندوستان، آفریقای جنوبی، بلاروس و کوبا منعقد کند.

جمع‌بندی و نتیجه‌گیری این فصل

همان طور که گفته شد، روسیه در کنار آمریکا و چین یک قدرت سایبری بزرگ محسوب می‌شود. همچنین این کشور به دلیل ساختار حکمرانی آن، از موقعیت برتر دفاعی در برابر حملات سایبری در مقایسه با کشورهایی همچون آمریکا بهره‌مند است و در این زمینه از دو بازوی بزرگ کاسپراسکای و اف‌اس‌بی نیز برخوردار است.

---

1. Elaine K., 2015
2. Elena Ch., 2017

دیپلماسی سایبری روسیه به رغم فراز و فرودهایی که به لحاظ سیاسی و به ویژه در ارتباط با دموکراسی‌های غربی داشته، همواره از یک مزیت تاریخی برخوردار است و آن اینکه پیچیدگی‌های روزافزون و تهدیدات متعدد در حوزهٔ سایبری روزبه‌روز کشورهای بیشتری را ــ حتی در بین کشورهای غربی ــ با برداشت‌ها و رویکردهای سایبری این کشور همراه ساخته است.

برای مدت‌زمانی طولانی مرزبندی کشورهای مختلف در حوزهٔ سایبری کاملاً مشخص بود. روسیه و نزدیک‌ترین شرکای آن (چین و اعضای سازمان پیمان امنیت جمعی) با تأکید بر حق حاکمیت کشورها و عدم دخالت در امور داخلی دیگر کشورها، نیاز به قوانین رفتاری جهانی برای دولت‌ها را در فضای سایبری مطرح می‌کردند. در مقابل، ایالات متحده و متحدان آن به این افکار بدبین بودند و گمان می‌کردند که انگیزهٔ حقیقی این درخواست، قانونی کردن سانسور و توسعهٔ کنترل دولت است. با این وجود، افزایش تهدیدات فضای سایبری (جرایم سایبری، گسترش تبلیغات تروریستی و اقدامات خصمانه در سطح کشور) موجب نگرانی کشورهای غربی نیز شد. به نحوی که در حال حاضر این کشورها نیز به طور روزافزون، خواستار مقررات سخت‌گیرانه‌تر و اعطای حق بیشتر به دولت‌ها برای کنترل اطلاعات در قلمرو قدرتشان هستند. اخیراً حتی آنتونیو گوترش، دبیر کل سازمان ملل متحد، این ایده را برای نخستین‌بار علناً تأیید کرد و اظهار داشت که وجود مقررات جهانی به منظور کاهش تأثیر جنگ الکترونیکی بر غیرنظامیان ضرورت دارد. زیرا به عقیدهٔ او «جنگ بعدی با حملهٔ گستردهٔ سایبری برای تخریب ظرفیت نظامی ... و از کار انداختن زیرساخت‌های اساسی مانند شبکه‌های توزیع برق آغاز خواهد شد».[1] بر این اساس به نظر می‌رسد که در حوزهٔ دیپلماسی سایبری، دست‌کم

1. UN Chief Calls for Regulatory Scheme for Cyberwarfare, 2018

برداشت جهانی از مقولهٔ تهدیدات سایبری روزبه‌روز به برداشت روسیه نزدیک‌تر شود. روسیه به طور کلی چهار مؤلفه را در دیپلماسی سایبری خود تهدید اساسی تلقی می‌کند که به شرح ذیل هستند:[1]

۱. استفاده از اطلاعات به عنوان سلاحی برای اهداف نظامی و سیاسی مغایر با قوانین بین‌المللی؛ انتشار اسناد پاناما می‌تواند نمونهٔ بارز آن باشد که برخی تحلیلگران روسیه، آن را یک حملهٔ اطلاعاتی علیه این کشور تلقی می‌کنند؛[2]

۲. استفاده از فناوری اطلاعات و ارتباطات برای اهداف تروریستی، مانند گروه‌های تروریستی که از اینترنت برای انتشار پیام خود و جذب طرفدار استفاده می‌کنند؛

۳. استفاده از فناوری اطلاعات و ارتباطات برای مداخله در امور داخلی دولت‌ها؛

۴. استفاده از ابزارهای رایانه‌ای برای مقاصد جنایی، همچون ایجاد و انتشار بدافزارها.

بر مبنای این تهدیدات و در شرایط ایدئال، روسیه طرفدار یک «رژیم حقوقی بین‌المللی» است که در آن امنیت اطلاعات بین‌المللی تضمین شود. چنین رژیم قانونی‌ای می‌تواند با این امور تقویت و پشتیبانی شود: یک کنوانسیون پیشنهادی برای امنیت اطلاعات بین‌المللی، آیین‌نامهٔ رفتاری دولت‌ها مصوب سازمان ملل، مشاوره و همکاری‌های منظم دوجانبه و چندجانبه، ایجاد اتحادیهٔ بین‌المللی ارتباطات به عنوان نهاد حاکم بر اینترنت و نیز توسعهٔ اقدامات اعتمادساز به منظور کاهش خطر سوءبرداشت.

---

1. NATO Cooperative Cyber Defense Centre of Excellence, 2017
2. Adam Taylor, 2017; Vladimir Putin, 2016

روسیه اگرچه قوانین بین‌المللی مصوب جامعهٔ جهانی را قابل اعمال در فضای سایبری می‌داند، با این حال با حاکمیت یک‌جانبهٔ کشورها، از جمله آمریکا، بر این حوزه مخالف است. از این رو در اسناد راهبردی روسیه در ارتباط با حوزهٔ سایبری، به دفعات بر ضرورت ایجاد توازن استراتژیک از طریق برابری فناورانه و مشارکت راهبردی عادلانهٔ روسیه با سایر کشورها تأکید شده است و اینکه برخی کشورها (به طور مشخص آمریکا) نباید به دنبال بهره‌برداری از برتری فناورانهٔ خود به منظور تسلط بر فضای اطلاعاتی باشند.

روسیه با ائتلافی که توسط برخی کشورهای همسو از جمله چین و دیگر کشورهای عضو سازمان همکاری شانگهای تشکیل داده، توانسته تا حد زیادی جایگاه خود را به عنوان یک بازیگر اصلی در عرصهٔ سایبری تثبیت کند. شاید اوج موفقیت دیپلماسی سایبری روسیه را بتوان در برجسته ساختن اهمیت حملات و تهدیدات سایبری دانست که به طور یکسانی کلیت عرصهٔ سایبری را تهدید می‌کند. به این اعتبار، روسیه توانسته دکترین «ضرورت تضمین امنیت اطلاعات بین‌المللی» را در مجامع جهانی نهادینه سازد.

در حالی که از نظر سیاست‌ها و درک مشترک از تهدیدات سایبری، همپوشانی فزاینده‌ای بین روسیه و غرب ایجاد شده، اما پویایی منفی روابط ایالات متحده ـ روسیه و اتحادیهٔ اروپا ـ روسیه، دستیابی به هر گونه اجماع جهانی را بسیار دشوار می‌سازد. از منظر کشورهای غربی، روسیه از پتانسیل سایبری خود عمدتاً برای این امور بهره می‌جوید: ۱. جاسوسی (به عنوان رقیب)، ۲. جعل اطلاعات با هدف گمراهی افکار عمومی، و ۳. نفوذ به اهداف و زیرساخت‌های کلیدی رقیب و نگه داشتن آن‌ها در مرحلهٔ ریسک (مرحله‌ای از نفوذ که بتوان هر لحظه برای اهدافِ مقصود بحران ایجاد کرد).

این تقابل که البته ریشه در منازعهٔ تاریخی ایدئولوژیک کشورهای غربی با روسیه دارد، چشم‌انداز همکاری آتی دو جبهه را تیره و تار ساخته است. این در حالی است که بدون همکاریِ عوامل و قدرت‌های اصلی سایبری ــ از جمله روسیه و چین و کشورهای غربی ــ هیچ سیستم نظارتی بین‌المللی‌ای در حوزهٔ سایبری و فضای سایبری مؤثر واقع نخواهد شد.

منابع

Chernenko, Elena, “Cold War 2.0? Cyberspace as the New Arena for Confrontation”, Russia in Global Affairs, 1, April 15, 2013, http://eng.globalaffairs.ru.

Chernenko, Elena, «Политическая кибервойна началась» [“The Political Cyber War has Started”], Global Affairs Journal (9 October 2016), http://globalaffairs.ru.

Chernenko, Elena, “Russia Is Installing Anti-hacker Programmes”, Kommersant, November 30, 2017, https://www.kommersant.ru.

Council of Europe, Convention on Cybercrime, Budapest, November 23, 2001, see to: https://www.coe.int.

Creation of a Global Culture of Cyber Security and Taking Stock of National Efforts to Protect Critical Information Infrastructures”, Resolution Adopted by the General Assembly on 21 December 2009, http://www.un.org.

Federal Law of Russian Federation NO. 139-FZ, https://rg.ru.

Gady, Franz-Stefan & Greg Austin (2010), Russia, the United States, and Cyber Diplomacy Opening the Doors, the East West Institute.

Hudson, John, “How Secret Talks with Russia to Prevent Election Meddling Collapsed”, BuzzFeed, December 8, 2017, https://www.buzzfeednews.com.

Internet Growth Statistics, (1995-2017)”, Internet World Stats – Usage and Population Statistics, https://www.internetworldstats.com.

Krutskhikh, Andrey, Interview in Kommersant, April 23, 2018, https://www.kommersant.ru.

Korzak, Elaine, "The Next Level for Russia-China Cyberspace Cooperation?", Net Politics (Blog), August 20, 2015, https://www.cfr.org.

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, UN Doc A/66/359.

Maness, Ryan C. & Brandon Valeriano (2015), Russia's Coercive Diplomacy Energy, Cyber, and Maritime Policy as New Sources of Power, UK: Palgrave Macmillan.

Popescu, Nicu & Stanislav Secrieru (2018), Hacks, Leaks and Disruptions Russian Cyber Strategies, European Union, Institute for Security Studies, Paris.

Russian Ministry of Foreign Affairs, Convention on International Information Security (Concept), September 22, 2011, http://www.mid.ru.

UN Chief Calls for Regulatory Scheme for Cyberwarfare", Radio Free Europe/Radio Liberty, February 19, 2018, https://www.rferl.org.

UN General Assembly, Resolution A/RES/53/70, "Developments in the Field of Information and Telecommunications in the Context of International Security", January 4, 1999, http:// undocs.org.

فصل هفتم

دیپلماسی سایبری اتحادیهٔ اروپا: از تاب‌آوری سایبری تا بستهٔ دیپلماسی سایبری

درآمد

اتحادیهٔ اروپا بر اساس موازین سیاسی و تاریخی‌اش همواره می‌کوشد خط‌مشی صلح‌طلبی را ترویج داده و توسعه صلح و ثبات را از طریق گفت‌وگو و مذاکرات سیاسی، به عنوان دستور کار اصلی سیاسی خود حفظ کند. اگرچه سابقهٔ تلاش‌های دیپلماتیک اتحادیهٔ اروپا را در حوزهٔ فضای سایبری می‌توان به مشارکت این اتحادیه در تأسیس آیکان و نیز گفتمان حکمرانی اینترنت در دههٔ ۱۹۹۰ معطوف دانست، اما دورنمای دیپلماسی سایبری این اتحادیه ابتدا در سال ۲۰۱۳ با تدوین سند «استراتژی امنیت سایبری» و متعاقباً با تدوین «بستهٔ دیپلماسی سایبری» اتحادیهٔ اروپا در سال ۲۰۱۷ نمایان گشت که در آن چشم‌انداز فضای سایبری بین‌المللی منسجم از منظر این اتحادیه مشخص شد.

برآیند کلی از بستهٔ دیپلماسی سایبری اتحادیهٔ اروپا نشان می‌دهد که رویکردها، استراتژی‌ها و اهداف کلاسیک سیاست خارجی اتحادیهٔ اروپا عیناً به حوزهٔ سایبری نیز گسترش یافته است. هرچند در سال‌های اخیر، افزایش تهدیدات سایبری و حملات سایبری صورت‌گرفته به برخی از زیرساخت‌های

اطلاعاتی و ارتباطی کشورهایی همچون آلمان، انگلستان، فرانسه و ...، این اتحادیه را به لحاظ سیاسی در مواضع تهاجمی‌تری قرار داده است.

بستهٔ دیپلماسی سایبری اتحادیهٔ اروپا، به عنوان نماد استراتژی سایبری، مشتمل بر اصول و مبانی فکری این اتحادیه در حوزه مسائل سایبری و نیز چهار سازوکار عملیاتی آن شامل اقدامات پیشگیرانه، اقدامات مشارکتی، اقدامات تثبیت‌کننده و اقدامات محدودکننده، بر مبنای یک رویکرد جمعی توسعه یافته است.

به لحاظ اجرایی، علاوه بر مکانیسم‌های داخلی اتحادیهٔ اروپا برای تقویت مواضع و سیاست‌های یکسان در ارتباط با مسائل سایبری، این اتحادیه همچنین از طریق استراتژی‌های تعامل بین‌المللی در پلتفرم‌های جهانی همچون سازمان ملل؛ تعامل چندجانبه با سازمان‌های منطقه‌ای همچون سازمان همکاری‌های شانگهای، گروه بیست، گروه هفت، آسه‌آن و ...؛ و نیز تعامل دوجانبه با قدرت‌های سایبری همچون آمریکا، کانادا، استرالیا، کرهٔ جنوبی و ...؛ سیاست‌های سایبری خود را پیش می‌برد.

از آنجایی که دیپلماسی سایبری اتحادیهٔ اروپا در مقایسه با دیپلماسی سایبری ایالات متحده آمریکا، روسیه، ژاپن و چین، بر پایهٔ رویکرد و تصمیم جمعی قوام یافته و صلح‌طلبی و تعامل سیاسی را در اولویت قرار می‌دهد، از مزایای استراتژیکی برخوردار است. با این حال دقیقاً به همین دلیل متکی بودن به رویکرد جمعی، در عمل از کارایی کمتری برخوردار است.

تاریخچهٔ مباحث سایبری در اتحادیهٔ اروپا

اتحادیهٔ اروپا و کشورهای عضو آن به دنبال شناخت حملات و تهدیدات سایبری در طول سال‌های گذشته، به منظور تقویت امنیت سایبری در اروپا

و مقابله با حملات سایبری علیه زیرساخت‌ها، جاسوسی سایبری، سرقت مالکیت معنوی و تهدیدات ترکیبی با استفاده از ابزار سایبری تلاش‌های گسترده‌ای انجام داده‌اند. برخی از این تلاش‌ها معطوف به داخل اتحادیهٔ اروپا و برخی دیگر نیز معطوف به عرصهٔ بین‌المللی بوده است.

در سطح داخلی اتحادیهٔ اروپا، در درجهٔ اول ارتقای اقدامات پیشگیرانه، سازوکارهای هشدار زودهنگام، مقاومت و هماهنگی در اولویت قرار داشته‌اند. در این خصوص راهبرد امنیت سایبری اتحادیهٔ اروپا در سال ۲۰۱۳[1]، دستورالعمل امنیت شبکه و اطلاعات سال ۲۰۱۶[2] و چارچوب مشترک سال ۲۰۱۶[3] در خصوص مقابله با تهدیدات ترکیبی نقاط عطف مهمی در ارتباط با مسائل سایبری هستند. برای مثال، دستورالعمل امنیت شبکه و اطلاعات، کشورهای عضو را به ارتقای سطح امنیت سایبری در اتحادیهٔ اروپا به واسطهٔ تشکیل گروه‌های پاسخگویی به فوریت‌های امنیتی رایانه‌ای و یک مرجع ملی امنیت شبکه و اطلاعات ملزم کرده است. همچنین با هدف تسهیل همکاری‌های استراتژیک و تبادل اطلاعات، این اتحادیه گروه همکاری‌های امنیت شبکه و اطلاعات متشکل از نمایندگان کشورهای عضو، کمیسیون اروپا و آژانس اتحادیهٔ اروپا برای امنیت شبکه و اطلاعات (انیسا) و شبکهٔ تیم‌های پاسخگویی به فوریت‌های امنیتی رایانه‌ای را به منظور اشتراک‌گذاری اطلاعات مربوط به تهدیدات فعال و همکاری در زمینهٔ حوادث امنیت سایبری راه‌اندازی نمود[4].

---

1. 2013 EU Cybersecurity Strategy
2. 2016 Network and Information Security (NIS) Directive
3. 2016 Joint Framework
4. Ivan, 2019

نمایی از حملات سایبری در اتحادیهٔ اروپا

بیش از سه دهه است که برخی از کشورها از ابزارهای سایبری مخرب برای پیگیری اهداف و منافع خود در اقصی نقاط جهان استفاده می‌کنند. بر طبق گزارش مرکز مقابله با جرایم اینترنتی اف‌بی‌آی، در سال ۲۰۰۹ چیزی بیش از ۲۴۰ میلیون حمله مخرب سایبری شناسایی شده که خسارات ناشی از آن ۵۵۹,۷ میلیون دلار بوده است. هشت سال بعد استانیسالف کوزنتسوف، معاون اسبربانک روسیه، در مجمع اقتصاد جهانی در داووس بیان کرد که اگر شرایط فعلی در حوزه حملات سایبری بدون تغییر باقی بماند، خسارت ناشی از حملات سایبری به اقتصاد جهانی تا سال ۲۰۲۲ میلادی می‌تواند به ۱۰ تریلیون دلار برسد.[1]

حملات سایبری سال ۲۰۰۷ به استونی، در زمان اختلاف‌نظر مقامات تالین با روسیه در خصوص جابه‌جایی مجسمهٔ دوران اتحاد جماهیر شوروی، توجه ویژه‌ای را به این چالش امنیتی جلب کرد. در سال‌های بعد، اوکراین نیز چند بار مورد حملات سایبری قرار گرفت، از جمله حمله به شبکهٔ برق این کشور که به قطع موقت برق سراسری در سال‌های ۲۰۱۵ و ۲۰۱۶ منجر شد.[2]

در حالی که روزانه حوادث امنیت سایبری بسیاری اتفاق می‌افتد، دو حملهٔ سایبری وسیع که در سطح جهانی گسترش یافتند و چندین کشور عضو اتحادیهٔ اروپا را در سال ۲۰۱۷ تحت تأثیر قرار دادند، حاکی از گستردگی میزان خسارت‌های وارد شدهٔ ناشی از فعالیت‌های مخرب سایبری بودند. در ماه مه ۲۰۱۷، حملهٔ باج‌افزار واناکرای[3] به سرعت در

1. Yu, Wang, & Zhou, 2015.
2. Andy G., 2017
3. WannaCry ransomware attack

سراسر جهـان گسـترش یافـت و داده‌هـا را رمزگـذاری کـرد و خواسـتار پرداخت باج از طریق رمـزارز بیـت‌کـوین[۱] شـد. بـر اسـاس تخمـین‌هـای صورت‌گرفته، این حمله بیش از ۳۰۰ هزار رایانه را در ۱۵۰ کشور تحت تأثیر قرار داد و میزان خسارات ناشی از آن بین ۴ تا ۸ میلیـارد دلار بـود[۲]. در این میان، شرکت‌های خودروسازی رنو و نیسـان و هونـدا نیـز تحـت تأثیر این حمله قـرار گرفتنـد و ناچـار شـدند در تعـدادی از سـایت‌هـای فرانسه، انگلستان، رومانی، اسلوونی، ژاپن و هندوستان تولیـدات خـود را متوقف کنند یا کاهش دهند[۳]. این حمله همچنین سیستم خدمات درمـانی ملـی در انگلسـتان را تحـت تـأثیر قـرار داد و دسترسـی بیمارسـتان‌هـا و پزشکان به داده‌های بیماران را غیرممکن سـاخت کـه بـه لغـو عمـل‌هـای جراحی و معاینات پزشکی زیادی منجر شد[۴].

در ژوئن ۲۰۱۷، حملهٔ سایبری مهم نات‌پتیا[۵] از مبدأ خود در اوکراین به سایر نقاط جهان گسترش یافت و بر شرکت‌هـای اروپـایی بـی‌شـماری اثـر گذاشت. این حمله به یـک شـرکت دانمـارکی[۶]، کـه بـزرگ‌تـرین شـرکت حمل‌ونقل کانتینر در جهان است، آسیب شدیدی رساند و با آفلایـن کـردن بخـش بزرگـی از زیرسـاخت‌هـای فنـاوری اطلاعـات آن بـه خسـارت ۲۰۰ ــ ۳۰۰ میلیون دلاری این شرکت منجر شد. به دنبال این خسارت‌هـا، یکی از بزرگ‌ترین شرکت‌های داروسازی جهـان، مـارک انـد کـو[۷]، نیـز بـه ناچار تولید یکی از واکسن‌های کودکان خـود را متوقـف کـرد[۸]. بـر اسـاس

---

۱. Cryptocurrency Bitcoin
2. Andy G., 2017
3. The Independent, 13 May 2017; Rosemain, Mathieu, Le Guernigou, Yann and Davey, Mirror Online, 13 May 2017; Reuters, 21 June 2017.
4. BBC News, 15 May 2017
5. NotPetya
6. A.P. Møller-Mærsk
7. Merck & Co.
8. Paul R., 2017

ارزیابی کاخ سفید، کل خسارت‌های ناشی از حملهٔ سایبری نات‌پتیا بیش از ۱۰ میلیارد دلار محاسبه شده است.[1]

این حملات گسترده شدت تخریب احتمالی حملات سایبری مخرب را، که ممکن است عواقب جبران‌ناپذیری در زندگی مردم و زیرساخت‌ها به دنبال داشته باشد، به تصویر می‌کشند. این حملات همچنین نشان دادند که اقتصادهای پیشرفته و دیجیتالی در برابر این گونه حملات پیچیده که سرعت گسترش بالایی دارند آسیب‌پذیرترند. افزون بر آن، این حملات گسترده بحثِ نیازمندی کشورهای عضو اتحادیهٔ اروپا به همکاری با یکدیگر را برای پاسخگویی و جلوگیری از چنین حملاتی مطرح کرده و همچنین ضرورت اتخاذ مکانیسم‌های مشترک منطقه‌ای و بین‌المللی برای مدیریت عرصهٔ سایبری را یادآور می‌سازد.

در سطح بین‌المللی نیز اتحادیهٔ اروپا چه در سطح چندجانبه و چه از طریق روابط دوجانبه، مدت‌هاست که درگیر توسعهٔ یک چشم‌انداز و گفتمان روشن از آینده فضای سایبری در عرصهٔ بین‌المللی بوده است. از اوایل دههٔ ۱۹۹۰، اتحادیهٔ اروپا درگیر بحث‌های بین‌المللی در حوزهٔ حکمرانی اینترنت بود. استراتژی امنیت سایبری اتحادیهٔ اروپا در سال ۲۰۱۳، گامی اساسی در توسعهٔ دیپلماسی سایبری اتحادیهٔ اروپا بوده که ایجاد «سیاست منسجم بین‌المللی فضای سایبری برای اتحادیهٔ اروپا» را در بین پنج اولویت خود قرار داده است. اتحادیهٔ اروپا گفتمان‌های سایبری با کشورهای شریک را نیز توسعه داده است، مشارکت اتحادیهٔ اروپا و آمریکا (که تحت عنوان گفتمان سایبری اتحادیهٔ اروپا ـ آمریکا شناخته می‌شود) پیشرفته‌ترین نوع این گفت‌وگوهاست.

1. Andy G., 2017

در سال ۲۰۱۷، کمیسیون اروپا به منظور بهبود هر چه بیشتر انعطاف‌پـذیری سایبری و بازدارندگی و واکنش اتحادیهٔ اروپا، بستهٔ امنیت سایبری گسـترده‌ای را پیشنهاد داد. در دسامبر ۲۰۱۸، پارلمان و شورا و کمیسیون اروپایی در خصوص قانون امنیت سایبری، به توافقی سیاسی با هدف معرفی یک مجوز امنیت سایبری در سطح اتحادیهٔ اروپا و تحکیم انیسا دست یافتند.

افزایش تعداد و شدت حملات سایبری تحـت حمایـت دولـت‌هـا نیـز موجب توسعهٔ اهمیت سیاسی این چالش شد. در حـالی کـه اتحادیـهٔ اروپـا سال‌های متمادی با مسئلهٔ امنیت سایبری سروکار داشته، به اقدامات مربـوط به توسعهٔ واکنش مشترک دیپلماتیک اتحادیهٔ اروپـا علیـه عملیـات سـایبری مخرب تنها در چهار سال گذشته در سطح سیاسی توجه شده است.

در دوران ریاست کشور هلند در شورای اتحادیهٔ اروپا در سال ۲۰۱۶، این اتحادیه یک متن تفسیری غیررسمی با عنوان توسعهٔ پاسخ دیپلماتیک مشترک اتحادیهٔ اروپا علیه عملیات سایبری اجباری ارائه داد.[1] بنا به استدلال این سند، به منظور تأثیرگذاری بر رفتار متجاوزان بالقوه و در نتیجهٔ تقویت امنیت اتحادیهٔ اروپا، اخطار واضح و روشن به عواقب فعالیت‌های مخرب ضرورت دارد. این سند همچنین اصول اصلی بستهٔ دیپلماسی سایبری مورد نیاز را ارائه می‌دهد؛ از جمله اینکه پیشنهاد می‌کند پاسخ اتحادیهٔ اروپا باید متناسب با دامنه، مقیاس، مدت‌زمان، شدت، پیچیدگی، تبحر و تأثیر فعالیت سایبری باشد.[2]

تلاش‌ها در این زمینه ادامه یافت و در سال ۲۰۱۷، شورای امور خارجهٔ اتحادیهٔ اروپا اصول اصلی چارچوب پاسخ مشترک دیپلماتیک اتحادیهٔ اروپـا به فعالیت‌های سایبری مخرب را تأیید کرد که بستهٔ دیپلماسی سـایبری نـام

1. Council of The European Union, 2016
2. Council of the European Union, 2016

گرفت.[1] نتیجه‌گیری‌های شورای این اتحادیه به یک سری اقدامات احتمالی در چارچوب سیاست امنیتی و خارجی مشترک که مؤسسات اتحادیهٔ اروپا و کشورهای عضو قادر به انجام آن‌ها هستند، از جمله استفاده از قدرتمندترین ابزار ــ اقدامات محدودکننده (تحریم‌ها) ــ اشاره می‌کند. در اکتبر سال ۲۰۱۷، این چارچوب با تصویب سندی که حاوی دستورالعمل‌های اجرایی است با جزئیات بیشتری ارائه و تصویب شد.[2]

با توجه به این تاریخچه و نیز سوابق رویدادهای سایبری در کشورهای عضو اتحادیهٔ اروپا که در بالا به آن اشاره شد، سیر تحولات مربوط به تدوین سیاست‌های سایبری در اتحادیهٔ اروپا را در دو مقولهٔ به هم وابسته می‌توان صورت‌بندی کرد: الف. امنیت سایبری با تأکید بر مکانیسم‌های دفاعی ـ امنیتی؛ و ب. گذار به دیپلماسی سایبری با تأکید بر ایفای نقش نیروی صلح با آثار جهانی و بین‌المللی.

امنیت سایبری در اتحادیهٔ اروپا و سازوکارهای آن

امنیت سایبری نه‌تنها برای هر یک از کشورها به تنهایی بلکه برای اتحادیهٔ اروپا، به عنوان یک نهاد سیاسی بین‌المللی، نیز موضوع مهمی بوده است. این امر از تاب‌آوری شبکه‌ها، بازار واحد دیجیتال[3] یا پیگرد قانونی مجرمان سایبری فراتر رفته و شامل سیاست خارجی و امنیتی مشترک اتحادیهٔ اروپا[4] و سیاست مشترک امنیتی و دفاعی[5] نیز می‌باشد. در سطح

1. Council of the European Union, 2017
2. The 9 October 2017 Draft Version
3. Digital Single Market
4. EU’s Common Foreign and Security Policy (CFSP)
5. Com-mon Security and Defence Policy (CSDP)

اتحادیهٔ اروپا طیف وسیعی از نهادها و سازمان‌ها پاسخ یکپارچهٔ اروپایی به بحران‌های سیاسی ـ امنیتی مرتبط با فضای سایبری را دنبال می‌کنند که موارد زیر در رأس آن‌ها قرار دارند: آژانس امنیت شبکه و اطلاعات اتحادیهٔ اروپا (انیسا)؛ مرکز جرایم سایبری اروپا[1] در یوروپل؛ مرکز اطلاعات و موقعیت اتحادیهٔ اروپا؛[2] ریاست هیئت نظامی اتحادیهٔ اروپا[3] و اتاق وضعیت آن؛[4] مرکز اطلاعات و موقعیت اتحادیهٔ اروپا برای تحلیل و بررسی تهدیدات ترکیبی، معروف به سلول فیوژن ترکیبی؛[5] تیم پاسخ به فوریت‌های رایانه‌ای برای مؤسسات و آژانس‌های اتحادیهٔ اروپا؛[6] و مرکز هماهنگی واکنش اضطراری کمیسیون اروپا.[7] علاوه بر این‌ها، ساختارها و سازوکارهای جدیدی که بر اساس بخشنامهٔ امنیت شبکه و اطلاعات[8] ایجاد شده‌اند، مانند شبکهٔ تیم‌های پاسخگویی به فوریت‌های امنیتی رایانه‌ای[9] کشورهای عضو نیز باید در نظر گرفته شوند.[10]

علاوه بر این نهادها و سازمان‌ها، یک گروه کاری دیگر نیز با عنوان «کارگروه افقی مسائل سایبری»[11] در سال ۲۰۱۵ به منظور هماهنگ‌سازی

---

1. European Cybercrime Centre (EC3)
2. EU Intelligence and Situation Centre (INTCEN)
3. Intelligence Directorate of the EU Military Staff (EUMS INT)
4. SITROOM
5. Hybrid Fusion Cell
6. Computer Emergency Response Team for EU Institutions and Agencies (CERT-EU)
7. European Commission's Emergency Response Coordination Centre (ERCC)
8. Network and Information Security (NIS) Directive
9. CSIRTs
10. Christou, George, 2016
11. Horizontal Working Party on Cyber Issues

جنبه‌های سیاسی فضای سایبری در شورای این اتحادیه ایجاد شد. این کارگروه حق مشارکت در فعالیت‌های قانونی و غیرقانونی را داراست. این کارگروه در فوریهٔ ۲۰۱۵ تصمیم به تقویت دیپلماسی سایبری اتحادیهٔ اروپا در سرویس اقدامات خارجی اروپا[1] گرفت که در نتیجهٔ آن ارگانها، نهادها و سازمان‌های دیگری برای هماهنگی تجزیه و تحلیل استراتژیک سیاست خارجی و امنیتی مشترک اتحادیهٔ اروپا در ارتباط با مسائل و رویدادهای سایبری راه‌اندازی و تأسیس شدند. برخی از این نهادها و سازمان‌های جدید عبارت‌اند از: تیم دیپلماسی سایبری در اقدامات خارجی اتحادیهٔ اروپا و همچنین مرکز تجزیه و تحلیل اطلاعات اتحادیهٔ اروپا برای آگاهی موقعیتی غیرنظامی و ریاست هیئت نظامی اتحادیهٔ اروپا برای ارتش. در کنار این دو ارگان مهم، همچنین دانشمندان علوم کامپیوتری به منظور جلوگیری و بازسازی حملات سایبری و شناسایی مجرمان، به منابع متعددی در کشورها و شرکت‌های مختلف در تمامی سطوح سیاسی و امنیتی و نظامی دسترسی دارند و به آن‌ها استناد می‌کنند. اتحادیهٔ اروپا در مقام یک واحد کل و نیز هر یک از کشورهای عضو این اتحادیه برای هماهنگ‌سازی امور در این زمینه همچنین می‌توانند به همکاری تثبیت‌شدهٔ بین وزارتخانه‌ها و نیز آژانس‌های امنیتی یکدیگر تکیه کنند؛ به خصوص در زمینهٔ مبارزه با تروریسم که در این اتحادیه قوانین جدی و ویژه‌ای را در بر می‌گیرد.[2]

سیاست مشترک اتحادیهٔ اروپا در خصوص «تاب‌آوری، بازدارندگی و دفاع: برقراری امنیت سایبری مستحکم در اتحادیهٔ اروپا» در سپتامبر ۲۰۱۷، نقطهٔ آغازین همکاری را با هدف ایجاد اعتماد و امنیت بنا نهاد که بر چهار ستون امنیت سایبری اتحادیهٔ اروپا استوار است (جدول شمارهٔ ۱)[3].

---

1. European External Action Service (EEAS)
2. Christou, George, 2016
3. Bendiek, 2018

جدول شمارهٔ ۱. امنیت سایبری در اتحادیهٔ اروپا: حوزه‌های مسئولیت

سطح/مقوله	صلح، امنیت، عدالت	بازار واحد	سیاست مشترک امنیتی و دفاعی: دفاع سایبری	سیاست خارجی اتحادیهٔ اروپا: دیپلماسی سایبری
اتحادیهٔ اروپا	Europol (EC3) Eurojust EU-LISA	ENISA CSIRT CERT-EU	EDA GSA	EEAS SIAC (EU INTCEN, EUMS INT) EU SITROOM EU Hybrid Fusion Cell ERCC
ملی	مقامات اجرایی و حفاظت از داده‌ها	مقامات مسئول شبکهٔ پاسخگویی به حوادث رایانه‌ای ملی NIS	آژانس‌های دفاعی و نظامی و امنیتی	وزارت‌های امور خارجهٔ کشورهای عضو

CERT: تیم واکنش اضطراری رایانه‌ای
CSIRT: تیم پاسخگویی به فوریت‌های امنیتی رایانه‌ای
EC3: مرکز جرایم سایبری اروپا
EDA: آژانس دفاعی اروپا
EEAS: سرویس اقدامات خارجی اروپا
ENISA: آژانس امنیت شبکه و اطلاعات اتحادیهٔ اروپا (انیسا)
ERCC: مرکز هماهنگی پاسخگویی فوریتی
EU INTCEN: مرکز اطلاعات و موقعیت اتحادیهٔ اروپا
EU-LISA: آژانس اروپایی مدیریت عملیاتی سیستم‌های بزرگ فناوری اطلاعات در حوزهٔ آزادی و امنیت و عدالت

EU SITROOM: اتاق وضعیت اتحادیهٔ اروپا
EUMS INT: هیئت نظامی اتحادیهٔ اروپا، مأموریت هیئت‌مدیرهٔ اطلاعات
GSA: آژانس سیستم‌های ماهواره‌ای ناوبری جهانی اروپا
NIS: امنیت شبکه و اطلاعات
SIAC: ظرفیت تحلیل اطلاعات واحد

کارگروه افقی مسائل سایبری با ریاست چرخشی بین اعضا و کمیتهٔ سیاسی و امنیتی[1] مسئولیت اقدامات اجرایی مناسب در این خصوص را بر عهده دارد. کشورهایی که از عضویت قانونی برخوردارند می‌توانند طرح‌های خود را از طریق این مکانیسم به اجرا درآورند. بر این اساس، چهار ستون امنیت سایبری اتحادیهٔ اروپا شامل موارد ذیل می‌شود:

ستون اول: مفاد دستورالعمل حملات علیه سیستم‌های اطلاعاتی سال ۲۰۱۳، از جمله مجازات آن در خصوص عوامل خاطی و جنایتکار (مواردی که یک دولت حامی در پشت آن قرار ندارد)، قابل اجراست. برای مقابله با تهدید روزافزون جرایم سایبری برون‌مرزی، ابزارهای جدیدی برای مجازات هر چه مؤثرتر افراد خاطی برنامه‌ریزی شده است. دستورالعمل مدارک الکترونیکی[2] برای تسهیل دسترسی برون‌مرزی به شواهد الکترونیکی در حال بحث و بررسی است. بخشنامهٔ مبارزه با کلاهبرداری و جعل سند در کانال‌های پرداخت غیرنقدی همچون «بیت‌کوین» نیز در دست بررسی است. هدف اصلی آن نیز بهبود همکاری بین مقامات و مسئولان امور کیفری است.

ستون دوم: آژانس امنیت شبکه و اطلاعات اتحادیهٔ اروپا (انیسا) با

1. Political and Security Committee (PSC)
2. E-Evidence

افزایش تعداد کارکنان خود از حدود ۸۰ نفر به ۱۲۵ نفر و همچنین افزایش بودجهٔ سالانهٔ این آژانس از ۱۱ میلیون به ۲۳ میلیون یورو در حال ارتقاست. انتظار می‌رود این آژانس فعالیت‌های سالانهٔ امنیت سایبری پان ـ اروپایی[1] را سازماندهی و همکاری بین تیم‌های پاسخگویی به فوریت‌های رایانه‌ای کشورهای عضو را اداره کند. پیش از آن، این گونه فعالیت‌ها گاه‌به‌گاه به کشورهای متحد غیر عضو گسترش می‌یافت. هدف اصلی انیسا همکاری در تشکیل و اجرای چارچوب تأیید و تصدیق در سطح اتحادیهٔ اروپاست. در واقع هدف اصلی آن ایمن ساختن هر چه بیشتر محصولات و خدمات فناوری اطلاعات از طریق مشوق‌های بازار و فراهم آوردن امکان خرید آگاهانه برای کاربران است. بر اساس سازوکارهای انیسا، سیستم‌های تأیید انشعابی به منظور تقویت بازار واحد دیجیتال برای محصولات قابل اعتماد هماهنگ می‌شوند. این اقدامات بر اساس دستورالعمل امنیت شبکه و اطلاعات است که در می ۲۰۱۸ به اجرا درآمد و معیاری برای دستیابی به پیشرفت‌های مشابه در سازمان امنیت و همکاری اروپا نیز محسوب می‌شود.

ستون سوم: در دسامبر ۲۰۱۷، بیست‌وپنج وزیر دفاع کشورهای عضو اتحادیهٔ اروپا همکاری سازمان‌یافتهٔ دائمی[2] خود را آغاز کردند. دو مورد از هفده پروژهٔ آن‌ها صراحتاً به امنیت سایبری اروپا اختصاص یافت. بنا به گزارش‌ها، موارد دیگر به استانداردسازی سامانه‌های سرباز[3] پرداخته‌اند که عبارت‌اند از: تجهیزات الکترونیکی، ارتباطات زبانی و اطلاعاتی و نرم‌افزارها. در این میان، یونان قصد دارد تیم اضطراری فناوری اطلاعات اروپا را توسعه دهد و لیتوانی بر آن است تا

1. Pan-European
2. Permanent Structured Cooperation (Pesco)
3. Soldier Systems

مسئولیت برقراری دفاع سایبری اروپایی را بر عهده گیرد. برنامهٔ اصلی ایجاد حوزهٔ سایبری شنگن[1] برای مبارزه با جرم و جنایت‌های اینترنتی در سراسر مرزهای این اتحادیهٔ ملی است. تا اواخر سال ۲۰۲۰، بانک سرمایه‌گذاری اروپا[2] قصد دارد بیش از ۶ میلیارد یورو در توسعهٔ فناوری‌های به اصطلاح دومنظوره برای امنیت سایبری و امنیت غیرنظامی سرمایه‌گذاری کند.

ستون چهارم: اتحادیهٔ اروپا در توافق‌نامه‌های مشارکت استراتژیک خود با ایالات متحده، کانادا، چین، کرهٔ جنوبی و دیگر کشورها گفت‌وگوهای دوجانبه و چندجانبه‌ای در زمینهٔ مسائل سایبری انجام می‌دهد. اتحادیهٔ اروپا همچنین طراحی یک استراتژی در خصوص همکاری‌های بین‌المللی در فضای سایبری و همچنین پیشگیری از درگیری در زمینهٔ امنیت سایبری را در سپتامبر ۲۰۱۷ پیشنهاد کرده است، و دراین‌باره و به عنوان نخستین گام، ابزارهای سیاست خارجی و امنیتی مشترک و سیاست مشترک امنیتی و دفاعی و همچنین دستورالعمل‌ها و مکانیسم‌های خود در خصوص کنترل صادرات کالاهای دومنظوره را به‌روزرسانی کرده است[3].

گذار به دیپلماسی سایبری در اتحادیهٔ اروپا

از منظر اتحادیهٔ اروپا به رغم تمامی مکانیسم‌ها و برنامه‌های دفاعی ـ منیتی تدبیر شده، چالش‌ها و تهدیدهای سایبری از مرزهای ملی فراتر رفته و بر این اساس، امنیت سایبری به طور وثیقی با سیاست خارجی و روابط بین‌الملل گره خورده است. با توجه به تشدید حملات سایبری در سال‌های اخیر و نیز افزایش این تهدیدات، سطح اهمیت مقولات مرتبط با حوزهٔ

1. Cyber Schengen Area
2. European Investment Bank
3. Council of the European Union Conclusions, 2018

سایبری در سیاست خارجی این اتحادیه تا سطح مسائل و مباحث مهمی همچون خطرات تولید سلاح‌های هسته‌ای، تروریسم بین‌المللی و جرایم سازمان‌یافته بین‌المللی ارتقا یافته است.[1]

این تغییر ادراک از خطرات و تهدیدات سایبری در سطح اتحادیهٔ اروپا و ضرورت پرداختن به آن در سطوح فراملّی و بین‌المللی ناشی از دو واقعیت در سپهر سیاست بین‌الملل بوده است: الف) شکست یا ناکافی بودن تلاش‌ها و رویکردهای جمعی بین‌المللی برای مقابله با تهدیدات سایبری و ب) تصور اتحادیهٔ اروپا از نقش تاریخی خود به عنوان نیروی صلح و همسو با قوانین بین‌المللی. این دو واقعیت در حقیقت کشورهای عضو اتحادیهٔ اروپا را به این نتیجه رسانده که دیگر نمی‌توان صرفاً از طریق مکانیسم‌های دفاعی – امنیتی و یا مکانیسم‌های رایج بین‌المللی از خطرات بالقوه در این زمینه در امان بود و لذا باید به فکر تدوین سند دیپلماسی سایبری، به عنوان سند استراتژیک سایبری بین‌المللی، ویژهٔ این اتحادیه بود.

از این رو قبل از پرداختن به مبانی، اصول و راهبردهای عملیاتی دیپلماسی سایبری اتحادیهٔ اروپا، باید به مطالعه این دو واقعیت در سپهر سیاست بین‌الملل پرداخت:

الف) شکست یا ناکافی بودن تلاش‌ها و رویکردهای جمعی بین‌المللی برای مقابله با تهدیدات سایبری: با وجود آنکه عمدهٔ کشورهای جهان از لاک دفاعی ـ امنیتی در ارتباط با تهدیدات سایبری خارج و به سوی همکاری و تشریک مساعی در قالب سازمان‌های منطقه‌ای و جهانی روی آورده‌اند، اما از نظر اتحادیهٔ اروپا، عمدهٔ این تلاش‌های جمعی یا ناکارآمد و ناکافی بوده یا آشکارا از مبانی فکری، اصولی و ایدئال این اتحادیه فاصله داشته است. برخی از این رویکردهای جمعی و نیز دیدگاه

1. Tiirmaa-Klaar, Heli, 2013

اتحادیهٔ اروپا در ارتباط با آن‌ها به شرح ذیل بوده است:

۱. ناتو: ناتو حملات فضای سایبری را نوعی جنگ محسوب می‌کند که می‌توان به موجب مادهٔ ۵ معاهدهٔ آتلانتیک شمالی[1] شرط دفاع متقابل را فعال ساخت و لذا توجیهی برای اعلان جنگ باشد. در حال حاضر ناتو در حال بررسی این است که عملیات تهاجمی علیه شبکهٔ رایانه‌ای کشورهای عضو را بخشی از برنامهٔ عملیاتی خود در نظر گیرد یا خیر؟ به خصوص اینکه ناتو معتقد است روسیه به عنوان بزرگ‌ترین رقیب این ائتلاف، عمدهٔ برنامه‌ها و سناریوهای خود برای تضعیف دموکراسی‌های غربی را به فضای سایبری کشانده است[2].

به دنبال اجلاس سران ناتو در ورشو در سال ۲۰۱۶، همکاری‌های ناتو و اتحادیهٔ اروپا از طریق تبادل اطلاعات و اقدامات مشترک در زمینهٔ امنیت سایبری تقویت شده است. وزارت دفاع فدرال آلمان متعاقباً در همان سال و در مقالهٔ سفیدی راجع به سیاست امنیتی آلمان و آیندهٔ بوندس وهر[3]، از این پیشرفت استقبال و در زمینهٔ عملیاتی‌سازی آن، ششمین واحد سازمانی ــ واحد فضای سایبری و فضای اطلاعاتی ــ را برای ارتش خود ایجاد کرد که در حال حاضر حدود ۱۳۵۰۰ کارمند در آنجا مشغول به کارند.

در خصوص دفاع از خود یا دفاع متقابل در ناتو ممکن است از قابلیت‌های تدافعی و تهاجمی دفاع سایبری استفاده شود، اما «آیا این مسئله دربارهٔ قابلیت‌های تهاجمی در زمان صلح هم صادق است یا خیر؟»، همچنان در سطح اتحادیهٔ اروپا با عنوان یک «مسئله یا موضوع مهم» جای بحث دارد. منتقدان اتخاذ سیاست تهاجمی استدلال می‌کنند که اشاعهٔ

---

1. North Atlantic Treaty
2. Chertoff, 2018
۳. Bundeswehr، ارتش آلمان

بدافزارهای حملات سایبری مزایای کوتاه‌مدت پتانسیل بازدارندگی این قابلیت‌ها را توجیه نمی‌کند. آن‌ها تأکید می‌کنند که سازمان ملل متحد و سازمان امنیت و همکاری اروپا باید اقدامات اعتمادساز و امنیت‌ساز و همچنین کنترل تسلیحات را انجام دهند و هر گونه توسعهٔ قابلیت‌های دفاعی سایبری تهاجمی موجب بی‌اعتمادی و ناامنی متقابل و درگیری بیشتر می‌شود. آن‌ها معتقدند که تنها یک دیپلماسی سایبری طولانی‌مدتِ هماهنگ‌شده در سطح اروپا می‌تواند به برقراری امنیت در اروپا و جلوگیری از افزایش درگیری‌ها کمک کند. لذا همچنان یک نیرو و گرایش قوی در این اتحادیه وجود دارد که معتقد است نفع اتحادیهٔ اروپا در این است که خود را در موقعیت نیروی صلح در امنیت سایبری قرار دهد و بر سازش و برقراری ارتباط (در قالب گفت‌وگو) تأکید کند[1].

۲. سازمان ملل و گروه کارشناسان دولتی: در سطح یک رویکرد چندجانبه در سال ۲۰۱۵، گروهی متشکل از ۲۵ کارشناس دولتی بین‌المللی تحت نظر مجمع عمومی سازمان ملل متحد[2] به این اجماع رسیدند که قوانین بین‌المللی فعلی باید در فضای سایبری هم اعمال شود، از جمله برای دفاع مشروع[3]. با این حال، همین گروه در تابستان سال ۲۰۱۷، در خصوص تأسیس «شورای انتساب» و پیشنهاد شاخص‌هایی برای «انتساب حملات سایبری» به عاملان این حملات نتوانستند به

---

1. NATO Cooperative Cyber Defence Centre of Excellence, 2015.

۲. این گروه به گروه کارشناسان دولتی سازمان ملل متحد مشهور است که در سال ۲۰۰۴ در زمینهٔ تحولات حوزهٔ فناوری اطلاعات و ارتباطات در حوزهٔ امنیت بین‌المللی تشکیل شد.

3. United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015.

توافق برسند. به عنوان پیش‌شرط انتساب، یا همان شناسایی ابعاد فنی و حقوقی و سیاسیِ عامل حملهٔ سایبری، باید اطلاعات حساسی میان گروه‌های پاسخگویی به فوریت‌های رایانه‌ای و بین سرویس‌های مخفی و سازمان‌های امنیتی رد و بدل شود تا بتوان دربارهٔ شناسایی عامل یا عوامل حملهٔ سایبری اطمینان یافت.[1]

به دنبال شکست مذاکرات چندجانبه در سازمان ملل در سال ۲۰۱۷، کارشناسان امنیت سایبری اروپا خواستار شکل‌گیری ائتلاف‌های مشتاقان[2] در قالب کشورهای گروه ۲۰ یا گروه ۷ برای پیشبرد هنجارسازی بین‌المللی در حوزه‌های سایبری شدند. همچنین اتحادیهٔ اروپا خواستار مداخلهٔ بیشتر نهادهای غیردولتی در تدوین سیاست‌های منطقه‌ای و بین‌المللی مرتبط با فضای سایبری است. در این میان با توجه به چندوجهی بودن حوزهٔ سایبری، هر گونه برنامه‌ریزی، سیاست‌گذاری و تلاش برای هنجارسازی در این حوزه به طور مشخص مستلزم درگیر ساختن سایر ذی‌نفعان از جمله بخش خصوصی و جامعه مدنی نیز بود. در واقع به همین دلیل بخش خصوصی، به ویژه کمپانی‌های بزرگ آی‌تی، نیز دست به ابتکارات و اقداماتی در زمینهٔ صیانت از منافع خود زدند. برای مثال، در فوریهٔ ۲۰۱۷ شرکت مایکروسافت خواستار کنوانسیون دیجیتال ژنو[3] شد. منشور اعتماد[4] جدیدترین طرحی است که شرکت زیمنس در کنفرانس امنیتی مونیخ ارائه کرد و مشمول همین قاعده است. در نهایت، مجمع جهانی اقتصاد[5] نیز به دنبال ایجاد یک مرکز جهانی امنیت سایبری برای مقابله با جرایم سایبری و در نتیجه بهبود همکاری بین بخش خصوصی و بخش‌های دولتی یا به اصطلاح مشارکت‌های دولتی ـ خصوصی است.[6]

---

1. Bendiek, 2018.
2. Coalitions of the Willing
3. Digital Geneva Convention
4. Charter of Trust
5. World Economic Forum
6. Bendiek, 2018

۳. روی آوردن کشورها به مکانیسم‌های دوجانبه: با توجه به ناکارآمدی رویکردهای چندجانبه و ناتوانی در تشریک مساعی گسترده بین اعضای جامعهٔ جهانی، برخی کشورها ضمن ناامیدی از دستیابی به توافق همه‌جانبهٔ بین‌المللی در این خصوص، رویکردهایی دوجانبه یا منطقه‌ای را برای اقدام در این زمینه اتخاذ کرده‌اند. برای مثال، در سال ۲۰۱۶ شی جین‌پینگ و ولادیمیر پوتین، رؤسای جمهور روسیه و چین، توافق‌نامهٔ مشترک دوجانبه‌ای را در شانگهای امضا نمودند و مرحلهٔ جدیدی را در مشارکت استراتژیک جامع بین چین و روسیه اعلام کردند. همچنین پکن و مسکو نگرانی خود را مبنی بر احتمال سوءاستفاده از فناوری‌های اطلاعات و ارتباطات به منظور مداخله در امور داخلی دیگر کشورها اظهار داشتند. به اعتقاد رهبران چین و روسیه، جامعهٔ بین‌المللی باید بر اساس احترام متقابل و مصلحت و همچنین عدالت، همکاری کند و پاسخ‌های مشترکی در برابر تهدیدات مربوط به امنیت اطلاعات ارائه دهد.[1] قابل تأمل آنکه ایالات متحده نیز در سال‌های اخیر برای مقابله با جرایم سایبری، به توافقات دوجانبه و چندجانبه‌ای همچون توافق با چین، ژاپن، کرهٔ جنوبی، استرالیا، اسرائیل و ... روی آورده است.

با توجه به این رویکرد و گرایش جدید به الگوهای دوجانبه و چندجانبه از دیپلماسی سایبری و تلاش برای تحمیل آن در سطوح بین‌المللی، اتحادیهٔ اروپا نیز معتقد است که باید به عنوان یک بازیگر مهم جهانی در این زمینه به صورت مستقل از طریق تدوین یک استراتژی سایبری مشخص به ایفای نقش بپردازد. به خصوص از زمانی که ایالات متحده آمریکا نیز به استراتژی تعامل دوجانبه با ده‌ها کشور در زمینهٔ همکاری‌های سایبری روی آورده است، اتحادیهٔ اروپا تلاش‌های مضاعفی را برای ایفای نقش بیشتر در حوزهٔ مسائل سایبری آغاز کرده است.

---

1. Mikhail K., 2016

ب) تعهد اتحادیهٔ اروپا به «ارزیابی بایسته»[1] و تلاش برای باقی ماندن به عنوان نیروی صلح: مفهوم و بار حقوقی «ارزیابی بایسته» به این معناست که اتحادیهٔ اروپا باید اطمینان یابد که قلمرو کشورهای عضو این اتحادیه مبدأ هیچ گونه فعالیت تخریبی علیه سایر کشورها نخواهد بود. اتحادیهٔ اروپا با حمایت از «ارزیابی بایسته» در فضای سایبری، تضمین می‌کند که به اصول بین‌المللی پایبند بوده و بر آن است که دیپلماسی سایبری را در تعامل با طرف‌های ثالث در زمینهٔ مبارزه با حملات سایبری نیز تقویت کند. ارزیابی بایسته در واقع نوعی تعهد است مبنی بر اینکه تمامی کشورها باید تضمین کنند که از قلمرو حکومتی آن‌ها (از جمله از سیستم‌های رایانه‌ای و زیرساخت‌های واقع در کشورشان یا تحت کنترلشان) برای حمله به زیرساخت‌های کشورهای دیگر سوءاستفاده نخواهند کرد. در صورت نقض این تعهد، کشور هدف حق متوسل شدن به اقدام متقابل را دارد.

تمایل اتحادیهٔ اروپا به ایفای نقش نیروی صلح از تلاش کشورهای عضو برای تقویت اصل ارزیابی بایسته از طریق ابزارهای سیاسی سیاست خارجی و امنیتی مشترک آشکار است. ارزیابی بایسته به عنوان یکی از اصول مورد قبول در حقوق بین‌الملل، دلالت‌های کاربردی زیادی دارد. برای مثال، اتحادیهٔ اروپا نه‌تنها باید رعایت قوانین را در قلمرو خود تضمین کند، بلکه باید مسئولیت عواقب ناشی از اقدامات خود در فراسوی مرزهای این اتحادیه را نیز به عهده بگیرد. برای مثال از طریق سیاست صادراتی سخت‌گیرانه‌تر، آثار و پیامدهای تصمیمات اتحادیهٔ اروپا به مراتب از قلمرو این اتحادیه فراتر می‌رود. ایجاد انسجام در این زمینه و اطمینان از تعهد به ارزیابی بایسته تنها

---

1. Due Diligence

بر عهدهٔ اتحادیهٔ اروپاست. در مواردی که حمایت از فضای سایبری حائز اهمیت است، کشورهای عضو نباید از هیچ گونه مشارکتی با سایر کشورها در زمینهٔ ایجاد «فضای سایبری باز، جهانی، آزاد، صلح‌آمیز و امن» دریغ کنند.

مهم‌ترین و مؤثرترین ابزارهای اتحادیهٔ اروپا در این زمینه «پیشگیری» و «شناسایی» است. پیشگیری شامل اقدامات مندرج در بخشنامهٔ امنیت شبکه و اطلاعات، از جمله معرفی معیارهای کمیته و الزامات گزارش‌دهی برای اپراتورهای زیرساخت‌های کلیدی، است. ارائه‌دهندگان خدمات اینترنتی مجازند در صورت بروز اختلال، ترافیک داده را تجزیه و تحلیل کنند و در صورت لزوم، دسترسی مجرمان شناسایی‌شده را مسدود سازند.

شناسایی به معنای شفاف‌سازی و انتساب حملات است. در اینجا ارزیابی سیاسی تعیین‌کننده است. برای پیش‌بینی تهدیدات ترکیبی نظامی، باید تصویر کلی حوادث در فضای سایبری را در نظر گرفت. دربارهٔ حملات حرفه‌ای، به منظور به‌اشتراک‌گذاری تجزیه و تحلیل‌های مربوط به قطعات کد[1] و نحوهٔ شناسایی حمله از سوی آژانس‌های امنیتی بین کشورهای همسو، دیپلماسی سایبری مورد نیاز است. این گونه تحلیل‌ها اغلب امکان نتیجه‌گیری دربارهٔ گروه‌های هکری و منشأ آن‌ها را ممکن می‌سازد. هدف شبکهٔ پاسخگویی به فوریت‌های امنیتی رایانه‌ای فراهم آوردن امکان تبادل برای محافظت از زیرساخت‌های کلیدی است. دیپلماسی سایبری نیز برای تبادل اطلاعات به مقامات و مشاغل نیازمند است. گروه‌های عمومی و خصوصی واکنش اضطراری رایانه‌ای نیز برای جمع‌آوری دانش تخصصی در دیپلماسی سایبری ضرورت دارند.

از این منظر، دیپلماسی سایبری یکی از مؤلفه‌های مهم امنیت سایبری

---

1. Code Fragments

ملی به شمار می‌آید ضمن آنکه جنبهٔ اروپایی و حتی جهـانی را نیـز بـه آن می‌افزاید. تحقیقاتی که صرفاً بر اساس اطلاعات ملی، به خصوص بر مبنـای دفاعی ـ امنیتی، صورت می‌گیرند کافی نیستند. اتحادیهٔ اروپـا بـا چـارچوب پاسخگویی دیپلماتیک مشترک خود در سال ۲۰۱۷، سیاست امنیت سایبری غیرنظامی را در پیش گرفت. این امر مقاومت در برابر پاسخ‌دهی فـوری بـه تهدیدات فضای سایبری را تسهیل می‌کند. متعاقباً اتحادیـهٔ اروپـا اقـدامات سیاسی را به عنوان بخشی از سیاست امنیتی و خارجی مشترک بـرگزیـد تـا به عنوان نیروی صلح، تأثیرگـذار و متمـایز باشـد. ایـن رویکـرد بایـد یـک علامت سیاسی آشکار از سوی شرکا و رقبا در سراسر جهان به شمار آید.

با توجه به جمع‌بندی اتحادیهٔ اروپا از ایـن دو واقعیـت فـوق در سـپهر سیاست بین‌الملل مبنی بر ضرورت ایفای نقش در عرصهٔ سایبری به عنـوان یک بازیگر جهانی مستقل (در کنار سایر بازیگران) و بـاقی مانـدن در مـدار صلح‌طلبی به سبک و سیاق سنت کلاسیک، این اتحادیـه از مرحلـهٔ امنیـت سایبری گذار و در چارچوب آنچه «بستهٔ دیپلماسی سایبری» اتحادیـهٔ اروپـا نامیده می‌شود، تلاش‌هایی برای تبیین اصول، مبـانی و راهبردهـای سـایبری خود در عرصهٔ جهانی مبذول داشته است.

در بستهٔ دیپلماسی سایبری برخلاف استراتژی دفاعی ـ امنیتی سایبری ایـن اتحادیه بر ظرفیت‌سازی سـایبری بـه عنـوان پتانسـیلی بـرای تـنش‌زدایـی از درگیری‌ها و به تبع آن توسعهٔ نیروی صلح تأکید می‌شود. بـا توجـه بـه اینکـه محور بستهٔ دیپلماسی سایبری اعتمادسازی، هنجارسازی بین‌المللی، محافظـت از داده‌ها، آزادی بیان، حکمرانی اینترنت و ... می‌باشـد، برخـی از کشـورهای اروپایی به سـرعت خـود را بـا الزامـات محورهـای فـوق هماهنـگ کـرده و مکانیسم‌های سیاست‌گذاری، قانون‌گذاری و حتی تغییر سـاختار سیاسـی (بـه

خصوص در سیاست خارجی) خود را متناسب با نیازهای آن به‌روز کرده‌اند. هم‌اکنون تعدادی از کشورهای اروپایی (از جمله آلمان و فرانسه) سیاست‌هایی در این زمینه به تصویب رسانده‌اند و بیش از سی کشور این اتحادیه نیز دارای دیپلمات‌های سایبری در ساختار سیاست خارجی خود هستند و به عبارتی دارای دیپلمات متخصص در امور سایبری می‌باشند. دانمارک نیز نخستین کشوری است که یکی از دیپلمات‌های ارشد خود را به عنوان سفیر دیپلماسی سایبری منصوب کرده است.

اصول و مبانی بستهٔ دیپلماسی سایبری اتحادیهٔ اروپا

اتحادیهٔ اروپا نخستین‌بار در فوریهٔ ۲۰۱۵ به مسئلهٔ لزوم دیپلماسی سایبری مشترک در صورت مواجهه با تهدیدات و حملات سایبری پرداخت. متعاقباً در ماه جون ۲۰۱۷، توسعه و تدوین بستهٔ دیپلماسی سایبری را به منظور ارائهٔ پاسخ دیپلماتیک مشترک علیه فعالیت‌های مخرب سایبری پیشنهاد داد. بستهٔ دیپلماسی سایبری در نهایت در اکتبر ۲۰۱۷ تحت عنوان «پیش‌نویس» به تصویب رسید و در آن دستورالعمل‌های چارچوب «پاسخ دیپلماتیک مشترک اتحادیهٔ اروپا به فعالیت‌های سایبری مخرب» را اعلام نمود.

هدف اصلی این بسته تضمین پاسخگویی و کارایی سیاست خارجی و امنیتی اتحادیهٔ اروپا پیش از رسیدن به آستانهٔ درگیری‌های نظامی و مسلحانه است. این امر می‌تواند مکمل تلاش‌های اتحادیهٔ اروپا بر اساس دستورالعمل امنیت شبکه و اطلاعات به منظور پذیرفته شدن معیارهای کمیته و الزامات گزارش‌دهی و همچنین ایجاد سیستم‌های انعطاف‌پذیر فناوری اطلاعات و ارتباطات در بازار واحد دیجیتال باشد.

اتحادیهٔ اروپا در چارچوب دیپلماسی سایبری می‌کوشد به مهره‌ای کلیدی

در سیاست‌گذاری خارجی با نگاهی ویژه به امنیت سایبری در دنیا تبدیل شود. این مهم با مشخص کردن و بنا نهادن شش اصل کلیدی در اتحاد کشورها در مبحث دیپلماسی سایبری، که نشان‌دهندهٔ ارزش‌ها و منافع و اهداف اروپایی است، در حال پیگیری می‌باشد:

۱. عملیاتی بودن مُر قانون و قوانین حقوق بشر در فضای سایبری: دفاع از حقوق بشر و ترویج آن اصلی اساسی و عملیاتی در فضای سایبری تلقی می‌گردد. همچنین افزایش امنیت سایبری نباید موجب صدمه دیدن اصول ابتدایی حقوق بشر، مانند حقِ داشتن حریم خصوصی و حفاظت از اطلاعات شخصی و در نهایت آزادی بیان، شود.

۲. رفتار هنجارمند در فضای سایبری: قوانین فعلی اتحادیهٔ اروپا در رابطه با حملات سایبری بازتابی از قوانین وضع و ثبت‌شدهٔ موجود در گزارش سازمان ملل است که طی آن قوانین عمومی بین‌المللی را ملاک عملیات فرض می‌کند. به عبارت دیگر، از منظر اتحادیهٔ اروپا قوانین فعلی بین‌المللی معیار و ملاک رفتار هنجارمند در عرصهٔ سایبری نیز می‌باشد. با این حال، این اتحادیه بر به‌روزرسانی قوانین موجود حاکم یا قانون‌گذاری به‌روز به منظور مشخص کردن مباحث و ویژگی‌های خاص فضای سایبری تأکید دارد.

۳. ظرفیت‌سازی فضای سایبری: منظور از ظرفیت‌سازی در فضای سایبری به ویژه در ابعاد فناورانه و ساختاری با توجه خاص به تخصص منابع انسانی است. در سطح اتحادیهٔ اروپا سازمان‌ها و نهادهایی برای مدیریت حوادث با ساختاری متفاوت، مانند حوادث سایبری، تشکیل یافته‌اند؛ از جمله آژانس امنیت اطلاعات و شبکهٔ اروپایی که در سال ۲۰۰۴ رسماً آغاز به کار کرد. اتحادیهٔ اروپا با بکارگیری و تغییر چیدمان قوانین و نهادها و سازوکارهای موجود واکنشی متناسب با تهدیدهای سایبری ارائه

می‌دهد؛ برای مثال، ایجاد نهادی به نـام مرکـز جـرایم سـایبری اروپـا درون سازمان پلیس بین‌الملل اروپا یا ایجاد ستاد مشورتی بررسی مسائل سایبری.

۴. حکمرانی اینترنتی: اتحادیهٔ اروپا بهبود الگوی حکمرانـی چنـدوجهی را برای اینترنت دنبال می‌کند؛ الگویی کـه بـر اسـاس تعامـل و همـاهنگی میـان تمامی ذی‌نفعان بنا شده که متشکل اسـت از: دولـت‌هـای کشـورهای عضـو (نهادهای انتظامی و قضایی، نهادهای پاسخگوی حـوادث سـایبری، نهادهـای اطلاعاتی)، شرکت‌های خصوصی فعال در زمینهٔ فناوری و اطلاعات و صـنایع دفاعی، سازمان‌های بـین‌المللـی و میـان ـ دولتـی، سـازمان‌هـای مـردم‌نهـاد، اجتماعات مردمی، دانشگاه‌ها، متخصصان فنی و همچنین اتاق‌های فکر و ... .

۵. بهبود و ترویج جنبه‌های رقابتی اقتصاد و منافع اتحادیهٔ اروپا: این مهم با اتکا به اهمیت نقش فناوری و اطلاعات در بهبود و ایجاد بازار واحد اتحادیهٔ اروپا شکل می‌گیرد. با هدف کمک به دستیابی با بازار واحد اتحادیهٔ اروپایی، عرصهٔ سایبری نیز باید فضایی امن و سالم برای رقابت در حوزه‌های اقتصادی و تجاری و فارغ از مداخلات غیرضروری باشد.

۶. تعامل استراتژیک با شرکای کلیدی و سازمان‌های بین‌المللی: از منظر اتحادیهٔ اروپا، همکاری در زمینهٔ امنیت سایبری میان اتحادیهٔ اروپا یا با سازمان‌های ثالث بین‌المللی میان ـ دولتی برای دستیابی به آثار بین‌المللی اجتناب‌ناپذیر است. همچنین تعامل میان اعضای اتحادیه به منظور ایجاد ساختار کلی حقوقی و توافقات دوجانبه یا چندجانبه میان اعضا ضروری است.[1]

بر مبنای شش اصـل گفتـه‌شـده، اتحادیـهٔ اروپـا در اسـتراتژی دیپلماسـی سایبری خود، ده کشور را به عنوان شرکای اصلیِ تعامل و با هـدف دسـتیابی به توافقات دو یا چندجانبه در ارتباط با موضوعات سـایبری برگزیـده اسـت.

---

1. Council of the European Union, 2014

این ده کشور عبارت‌اند از: آمریکا، کانادا، مکزیک، برزیل، آفریقای جنوبی، چین، ژاپن، هندوستان، کرهٔ جنوبی و روسیه. مذاکرات اتحادیهٔ اروپا ـ آمریکا یکی از پیشرفته‌ترین تعاملات در زمینهٔ امنیت سایبری است که به ویژه در شکل کارگروه امنیت شبکه و جرایم سایبری در سال ۲۰۱۰ تأسیس شد.[1]

در بین ده کشور فوق، اتحادیهٔ اروپا اگرچه مذاکرات انتقادی و برخی همکاری‌ها با دو کشور روسیه و چین داشته است، اما این مذاکرات و همکاری‌ها هیچ وقت استراتژیک نبوده و به سطوح جدی برای همکاری نرسیده است؛ زیرا این اتحادیه اساساً روسیه و چین را در زمینهٔ امنیت سایبری به عنوان شریک به رسمیت نمی‌شناسد. متقابلاً از منظر اتحادیهٔ اروپا، هر دو کشور روسیه و چین به دلیل فعالیت‌های مخرب سایبری، از قبیل جاسوسی و سایر حملات برهم‌زنندهٔ امنیت با انگیزه‌های سیاسی، منابع اصلی ناامنی سایبری تلقی می‌گردند که حتی برخی از اقدامات غیرسازندهٔ آن‌ها متوجه اعضای اتحادیهٔ اروپا نیز بوده است؛ به خصوص روسیه که در پی حوادث مربوط به اوکراین و استونی، تعامل و همکاری اتحادیهٔ اروپا با این کشور بیش از پیش تیره‌تر شده است.[2]

ضمن آنکه دو کشور روسیه و چین نیز اساساً رویکرد متفاوتی را در مقایسه با اتحادیهٔ اروپا در قبال موضوعات مرتبط با امنیت سایبری از طریق سازوکار مجمع عمومی سازمان ملل و نیز بر اساس اصول «سازمان همکاری‌های شانگهای»، که در سال ۲۰۰۱ تأسیس گردید، دنبال می‌کنند. به عنوان مثال، در دههٔ ۹۰ میلادی و در چارچوب سازمان ملل، روسیه نخستین کشوری بود که قانون‌گذاری در رابطه با امور سایبری را ارائه کرد. در ۱۹۹۹، این تلاش‌ها به شکل‌گیری قطعنامهٔ مجمع عمومی سازمان ملل در زمینهٔ

---

1. Danca, 2015
2. Greenberg, 2017

توسعهٔ فناوری و ارتباطات در حوزهٔ تخصصی امنیت بین‌الملل منجر شد.[۱] در سال‌های اخیر نیز به ویژه روسیه و چین، از طریق سازوکار سازمان همکاری شانگهای تعاملات گسترده‌ای با سایر کشورهای جهان در زمینهٔ پیشبرد اصول و مبانی فکری خود در ارتباط با حوزهٔ سایبری برقرار ساخته‌اند. بسیاری از این اقدامات و تلاش‌هایی که دو کشور چین و روسیه در قالب سازمان ملل یا سازمان همکاری شانگهای انجام می‌دهند، اساساً مغایر با اصول و مبانی فکری سیاست خارجی اتحادیهٔ اروپا، از جمله در ارتباط با مسائل سایبری است.

راهبردهای عملیاتی بستهٔ دیپلماسی سایبری اتحادیهٔ اروپا

اصول و مبانی فکری بستهٔ دیپلماسی سایبری اتحادیهٔ اروپا از منظر تبیین سیاست‌ها و خط‌مشی این اتحادیه در ارتباط با فضای سایبری بین‌المللی، به خصوص با توجه به متفاوت بودن آن از مبانی دیپلماسی سایبری آمریکا و نیز مبانی دیپلماسی سایبری روسیه و چین دارای ارزش استراتژیک است. با این وجود، با توجه به رشد روزافزون حملات سایبری و نیز ضرورت مهار تهدیدات فوری سایبری، این بسته فاقد قدرت اثرگذاری بر محاسبات هزینه ـ فایده منابع این تهدیدات می‌باشد. به عبارت دیگر، اصول و مبانی فکری بستهٔ دیپلماسی سایبری اتحادیهٔ اروپا اگرچه در مقام نظر بسیار ارزشمند و به نوعی متفاوت است، اما در عمل قدرت بازدارندگی و اثرگذاری بر محاسبات عاملان تهدیدات و حملات سایبری را ندارد. از این رو، اتحادیهٔ اروپا در بستهٔ دیپلماسی سایبری طیفی از راهبردهای عملیاتی ایجابی (مشوق‌ها) و سلبی (تحریم‌ها) نیز ارائه می‌دهد که می‌تواند نقش مهمی در تسهیل همکاری در مهار تهدیدات سایبری و

---

۱. Gady &Austin, 2010

نیز تشویق به انجام رفتارهای هنجارمند در این عرصه داشته باشد.

تلاش اتحادیهٔ اروپا برای تعیین راهبردهای عملیاتی در بستهٔ دیپلماسی سایبری تا حدی تحت تأثیر راهبردهای عملیاتی **ایالات متحده آمریکا**، به خصوص دولت باراک اوباما، بوده است. در زمان ریاست‌جمهوری باراک اوباما برای نخستین‌بار در سال ۲۰۱۴، پس از آنکه یکی از شرکت‌های تابعهٔ آمریکایی شرکت سونی قربانی یک حملهٔ سایبری ویرانگر شد، تحریم‌های یک‌جانبه‌ای علیه عاملان آن حمله وضع کرد. دوسال بعد، به دنبال فاش شدن اطلاعات پرسنلی کارمندان دولت آمریکا طی یک حملهٔ سایبری گسترده‌تر، واشینگتن نیز همین واکنش را از خود نشان داد. فراتر از تحریم‌ها، همچنین گزارش‌های زیادی از حملات متقابل سایبری علیه زیرساخت‌های کلیدی برخی از کشورهای متخاصم از سوی دولت ایالات متحده گزارش شده که به عنوان مثال می‌توان به حمله به زیرساخت‌های هسته‌ای ایران با استفاده از ویروس «استاکس‌نت» اشاره کرد.

بر این اساس و با استفاده از تجربه **ایالات متحده آمریکا**، بستهٔ دیپلماسی سایبری اتحادیهٔ اروپا بیان می‌دارد که این اتحادیهٔ از تمامی واکنش‌های قانونی کشورهای عضو در برابر هرگونه حملهٔ سایبری یا مواجهه با رویدادهای سایبری حمایت می‌کند. اقدامات سیاسی این اتحادیه در شورای اتحادیهٔ اروپا با همکاری سرویس اقدامات خارجی اروپا هماهنگ می‌شود. در موارد حادتر و فراتر از سطح سیاسی، فعالیت‌های سایبری مخرب می‌تواند به اقدامات تنبیهی و اعمال زور یا حتی حملهٔ مسلحانهٔ متقابل مطابق با قوانین بین‌المللی و منشور سازمان ملل نیز منجر شود. در این حالت، کشورهای عضو اتحادیهٔ اروپا در زمینهٔ دفاع شخصی یا جمعی مطابق با مادهٔ ۵۱ منشور سازمان ملل متحد و قوانین بین‌المللی و بشردوستانه تصمیمی حاکمیتی به صورت مشترک

اتخاذ خواهند کرد. فراتر از این رویکرد کلی، برخی از مهم‌ترین راهبردهای عملیاتی در بستهٔ دیپلماسی سایبری اتحادیهٔ اروپا به شرح ذیل می‌باشد:

۱. اقدامات پیشگیرانه: این اقدامات شامل فعالیت‌هایی از قبیل اعتمادسازی، آگاهی‌افزایی و ظرفیت‌سازی در کشورهای ثالث می‌شود. در میان مذاکرات سیاسی اتحادیهٔ اروپا با کشورهای ثالث، این اتحادیه مذاکرات سایبری را با هدف تأثیرگذاری بر رفتار و نگرش طرفین مذاکره توسعه داده است. اتحادیهٔ اروپا همچنین از اقدامات اعتمادسازی، نظیر اقدامات توسعه‌یافتهٔ سازمان امنیت و همکاری اروپا، پشتیبانی می‌کند. گفت‌وگو با سازمان‌های منطقه‌ای، مانند اتحادیهٔ آفریقا یا اتحادیهٔ کشورهای جنوب شرق آسیا موسوم به آسه‌آن، از اهمیت ویژه‌ای برخوردار است. اتحادیهٔ اروپا و نهادهای منطقه‌ای مربوط می‌توانند چگونگی ایجاد ظرفیت‌های منطقه‌ای و بین‌المللی برای استفاده از فضای سایبری (ظرفیت‌سازی سایبری) را در توافق‌نامه‌های مشترک به صورت مشارکتی، همکاری یا حتی از طریق ابزار کمک به ثبات و صلح[1] تعیین کنند.

۲. اقدامات همکارانه: این اقدامات شامل فعالیت‌هایی از قبیل استفاده از گفتمان‌های سیاسی و موضوعی و یادداشت‌های دیپلماتیک می‌شود. برای تسهیل یک رویداد در حال رخداد، هیئت نمایندگی اتحادیهٔ اروپا در یک کشور میزبان می‌تواند یادداشتی دیپلماتیک[2] به دولت آن کشور ارسال کند. این امر نیازمند دستورالعمل نمایندهٔ عالی اتحادیهٔ اروپا در امور خارجه و سیاست‌های امنیتی[3] است. در شرایط درگیری، رئیس هیئت می‌تواند طرحی برای انجام مذاکرات جامع یا صرفاً ارسال پیام‌های کلیدی ارائه دهد. یادداشت‌های دیپلماتیک را می‌توان با همکاری کشورهای ثالث نیز تنظیم کرد و ارائه داد.

---

1. Instrument Contributing to Stability and Peace (ICSP)
2. Démarche
3. Union for Foreign Affairs and Security Policy

۳. اقدامات ثبات‌ساز: این اقدامات شامل فعالیت‌هایی از قبیل بیانیهٔ نمایندهٔ عالی اتحادیهٔ اروپا، یادداشت‌های دیپلماتیک، علامت‌دهی از طریق گفت‌وگوهای سیاسی و موضوعی به رهبری اتحادیهٔ اروپا می‌شود. این اقدامات به عنوان یک ارتباط استراتژیک اخطاردهنده عمل می‌کند مبنی بر آنکه متجاوز احتمالی می‌بایست از انجام فعالیت‌های مخرب سایبری اجتناب ورزد؛ در غیر این صورت و در صورتی که آن فعالیت مخرب به وقوع بپیوندد، شورای اروپا می‌تواند یکی از قوانین یا سیاست‌های این اتحادیه را، مشروط به تصویب آن به اتفاق آرا، علیه متجاوز احتمالی به اجرا درآورد. شورای اروپا همچنین می‌تواند قطعنامه‌ای برای اجرا و اعمال چنین قانونی یا مواضعی تصویب کند. در آن صورت، رأی‌گیری با اکثریت واجد شرایط، به استثنای اقدامات اجرایی مربوط به ارتش یا عملیات دفاعی[1] قابل انجام است. نمایندهٔ عالی اتحادیهٔ اروپا در امور خارجی و سیاست‌های امنیتی نیز می‌تواند بیانیه‌ای از جانب اتحادیهٔ اروپا صادر کند. البته این امر، باید پیشاپیش مورد توافق تمام کشورهای اتحادیهٔ اروپا قرار گیرد و معمولاً در مواردی به کار گرفته می‌شود که نیازی به پاسخ فوری نباشد. با این حال، نمایندهٔ عالی نیز می‌تواند در صورت نیاز به واکنش سریع، بیانیه‌ای با مسئولیت خود صادر کند، اما جلب توافق ۲۷ کشور عضو اتحادیهٔ اروپا در چنین شرایطی امکان‌پذیر نیست.

۴. اقدامات محدودکننده: این اقدامات شامل فعالیت‌هایی از قبیل تحریم‌ها[2] یا کنترل صادرات می‌شود. اتحادیهٔ اروپا به منظور دستیابی به اهداف سیاسی در پی حملات سایبری بزرگ، می‌تواند اقدامات محدودکننده‌ای را نیز اعمال کند. این اقدامات معمولاً مقامات دولتی کشورهای ثالث و همچنین شرکت‌های دولتی یا

1. Art 31 Para 2 TEU
2. Council of the European Union, 2014

اشخاص حقیقی و یا حقوقی دیگر را هدف قرار می‌دهد. شورا باید در خصوص تحریم‌ها به اتفاق آرا برسد؛ ضمن آنکه مطابقت آن‌ها با اهداف سیاست خارجی و امنیتی مشترک طبق مادهٔ ۲۴ معاهدهٔ اتحادیهٔ اروپا[1] نیز ضروری است.

تحریم‌ها را می‌توان به دو دستهٔ اصلی تقسیم کرد: مواردی که اتحادیهٔ اروپا مستقلاً دربارهٔ آن‌ها تصمیم‌گیری می‌کند و تحریم‌هایی که اتحادیهٔ اروپا به دنبال قطعنامهٔ شورای امنیت سازمان ملل موظف به تحمیل و اعمال آن‌هاست. طبق قانون اتحادیهٔ اروپا، تحریم‌ها باید هدفمند باشند، مثلاً ممکن است با رعایت معیارهای کمیتهٔ اصل حاکمیت قانون، اسامی افراد یا شرکت‌های بخصوصی به منظور مسدود کردن حساب‌های بانکی‌شان در فهرست تحریم‌ها قرار بگیرد. پیش‌شرط‌های مطابقت با قانون برای چنین مواردی در نظر گرفته شده‌اند، که به عنوان مثال صراحتاً بیان می‌کنند که افراد مورد نظر باید از دلایل قرار گرفتن اسامی خود در فهرست مربوط مطلع شوند و فرصت شکایت نیز در اختیار آن‌ها قرار گیرد.[2]

کنترل صادرات یکی دیگر از مکانیسم‌های اتحادیهٔ اروپا است که همسو با راهبرد تحریم‌ها مورد استفاده قرار می‌گیرد. اتحادیهٔ اروپا بر آن است با کنترل دقیق‌تر صادرات کالاهای دومنظوره، دیپلماسی سایبری را تقویت کند. بخشنامهٔ کالاهای دومنظورهٔ ماه مه ۲۰۰۹ الزامات و شرایط صدور مجوز مشترک را برای کشورهای عضو به منظور صادرات و تهیه و ترانزیت این کالاها تعیین می‌کند. در اواسط دسامبر ۲۰۱۷، کمیسیون اروپا نسخهٔ جدیدی از ضمیمه‌های[3] این بخشنامه را منتشر کرد. این به‌روزرسانی عمدتاً به قوانین جدیدی مربوط است که شامل برخی کالاها مانند سخت‌افزارهای فناوری

---

1. Art 24 TEU
2. Bendiek, 2018
3. Annexes I, Iia To Iig And IV

اطلاعات می‌باشد. دسته‌بندی کالاها بر اساس این موارد کنترل‌کننده صورت می‌گیرد: ۱. مقررات معاهدات و تعهدات بین‌المللی، به ویژه قطعنامهٔ ۱۵۴۰ شورای امنیت سازمان ملل، کنوانسیون سلاح‌های شیمیایی و کنوانسیون سلاح‌های بیولوژیکی، ۲. فهرست‌های کنترل رژیم‌های صادراتی چندجانبهٔ بین‌المللی، مهم‌تر از همه، گروه کنترل سلاح‌های نظامی موسوم به واسنار،[1] گروه تأمین‌کنندگان هسته‌ای[2]، گروه استرالیایی و رژیم کنترل فناوری موشکی[3]. این فهرست‌ها به طور ویژه‌ای دائماً اصلاح و به‌روزرسانی می‌شوند. صادرات کالاهای خاص به کشورهای تحت تحریم نه‌تنها در معرض کنترل شدیدتری قرار دارند، بلکه در بسیاری از موارد مجوز جداگانه‌ای نیز باید برای صادرات کالاهای دومنظوره دریافت شود. سرپیچی از این قوانین ممکن است به مجازات و جریمه‌های سنگینی منجر شود.

استفاده از مکانیسم «تحریم‌ها» و «کنترل صادرات» از سوی اتحادیهٔ اروپا علیه کشورهای مختلف در سال‌های اخیر رو افزایش بوده است. این اتحادیه نخستین‌بار در سال ۲۰۱۲، این تحریم‌ها را علیه سوریه در زمینهٔ فروش، عرضه، انتقال یا صادرات تجهیزات یا نرم‌افزارهای کاربردی برای نظارت یا رهگیری اعمال کرد[4]. متعاقب آن رژیم‌های تحریمی و نیز کنترل صادرات مشابهی از سوی این اتحادیه علیه کشورهایی همچون ایران، روسیه، ونزوئلا و ... صورت گرفت که براساس آن ارائهٔ هر گونه مساعدت فنی، خدمات کارگزاری، تأمین اعتبار یا کمک مالی یا ارائهٔ هر گونه

---

1. Wassenaar Arrangement
2. The Nuclear Suppliers Group
3. Missile Technology Control Regime (MTCR)
4. Council Decision 2012/36/CFSP of 23 January 2012 Amending Decision 2010/639/CFSP Concerning Restrictive Measures Against Belarus: http://eur-lex.europa.eu.

خدمات ارتباطات از راه دور یا نظارت اینترنتی یا رهگیری ممنوع شد[۱].

چالش‌های بستهٔ دیپلماسی سایبری اتحادیهٔ اروپا

از آنجایی که پیشبرد اهداف و راهبردهای عملیاتی بستهٔ دیپلماسی سایبری اتحادیهٔ اروپا مستلزم اتخاذ رویکرد جمعی واحد است، برخلاف سایر کشورها که از نظام‌های واحد تصمیم‌گیری و بدنهٔ اجرایی منسجمی برخوردار هستند، اتحادیهٔ اروپا در این زمینه با چالش‌های اساسی مواجه است. فراتر از آن، معیارهای فنی ـ حقوقی‌ای که در پس هر تصمیم‌گیری جمعی اتحادیهٔ اروپا قرار دارد، مزید بر علت شده تا دستیابی به اشتراک نظر بیش از پیش دشوار به نظر رسد. بر این اساس، در یک طبقه‌بندی وسیع، این چالش‌ها را می‌توان به سه دسته تقسیم کرد:

۱. چالش انتساب حملات سایبری: مهم‌ترین مسئله در ارتباط با چالش انتساب، فقدان شاخص‌ها و معیارهای معیّن برای منتسب کردن حملات سایبری به یک یا چند عامل است. در این خصوص، هر یک کشورهای اتحادیهٔ اروپا معیارهای مختلف و چندگانه‌ای را برای منتسب کردن حملات سایبری به عامل یا عاملان این حملات دنبال می‌کنند و در این زمینه نمی‌توانند به اشتراک نظر برسند. به طور مثال، در حالی که برخی کشورهای عضو اتحادیهٔ اروپا در سال‌های اخیر، انتساب حملات سایبری را به صورت علنی یا غیرعلنی به برخی عاملان دولتی (از جمله در ارتباط با روسیه) اعلام کرده‌اند،

---

۱ Council of the European Union Decision 2012/168/CFSP Amending Decision 2011/235/CFSP Concerning Restrictive Measures Directed Against Certain Persons and Entities in View of the Situation in Iran', 23 March 2012: http://eurlex.europa.eu.

برخی دیگر آشکارا خواستار امتناع از اعلام رسمی و علنی آن هستند. بنابراین، در سطح اتحادیهٔ اروپا، تا کنون نه‌تنها هیچ حمله سایبری رسماً به هیچ عاملی نسبت داده نشده، بلکه حتی هیچ گونه اقدام عملی نیز علیه عاملان دولتی یا غیردولتی شناسایی‌شدهٔ برخی از این حملات انجام نشده است.[1]

به طور مثال در سال ۲۰۱۸، بریتانیا و دانمارک به همراه ایالات متحده و استرالیا حملهٔ سایبری نات‌پتیا را به طور علنی به دولت روسیه منتسب کردند[2]در حالی که کانادا به طور مبهمی «بازیگران روسی» را مسئول این حمله می‌دانست.[3]حتی نیوزلند، نروژ، لیتوانی، استونی، لتونی، سوئد و فنلاند بیانیه‌های پشتیبانی خود را در این زمینه نیز صادر کردند. با وجود آنکه چندین کشور عضو اتحادیهٔ اروپا این حملهٔ مخرب را به روسیه منسوب کرده بودند و اتحادیهٔ اروپا پیشاپیش تصمیم خود در خصوص بستهٔ دیپلماسی سایبری و دستورالعمل‌های مربوط به اجرای آن را اتخاذ کرده بود، شورای اتحادیهٔ اروپا به طور کلی دربارهٔ انتساب این حملات به یک کشور خاص ــ در اینجا روسیه ــ به اجماع نرسید. نتایج شورای آپریل ۲۰۱۸ در خصوص فعالیت‌های مخرب سایبری بدون انتساب حملات، تنها «سوءاستفاده از فناوری‌های اطلاعات و ارتباطات، از جمله در واناکرای و نات‌پتیا [...]» را محکوم کرد. در حالی که کشورهای عضو اتحادیهٔ اروپا نتوانستند علیه بازیگران این حملات اقداماتی جمعی انجام دهند، خود این حملات، اتحادیهٔ اروپا را برای توسعهٔ یک بستهٔ دیپلماسی سایبری کارآمدتر تحت فشار قرار داد.

---

1. Council of the European Union Conclusions, 2018

2. Lord Ahmad of Wimbledon, 2018; Bussoletti, Francesco, Difesa & Sicurezza, 2018; Stilgherrian, 2018.

3. Communications Security Establishment, 2018

در پی حملهٔ سایبری خصمانه علیه سازمان منع سلاح‌های شیمیایی[1] که شورای اروپا آن را در اکتبر ۲۰۱۸ محکوم کرد، فوریت‌های جدیدی به وجود آمد. رهبران اتحادیهٔ اروپا نیز خواستار اقداماتی برای مبارزه با فعالیت‌های غیرقانونی و مخرب سایبری و ایجاد امنیت سایبری قدرتمند و همچنین تلاش به منظور ظرفیت‌سازی برای پاسخگویی و جلوگیری از حملات سایبری از طریق اقدامات محدودکنندهٔ اتحادیهٔ اروپا شدند. علاوه بر این، دونالد تاسک[2] رئیس وقت شورای اروپا، ژان ـ کلود یونکر[3] رئیس وقت کمیسیون اروپایی، و فدریکا موگرینی[4] نمایندهٔ عالی وقت، بیانیهٔ مشترکی در خصوص حملات سایبری روسیه صادر کردند و عملیات خصمانهٔ سایبری سرویس اطلاعات نظامی روسیه[5] را محکوم کردند. این وقایع و واکنش‌ها فشار بیشتری برای پیشبرد بهره‌برداری از این بستهٔ دیپلماسی سایبری بر نهادهای اروپایی وارد آورد.

کارگروه افقی شورای اتحادیهٔ اروپا در زمینهٔ مسائل سایبری، که نمایندگان کشورهای عضو اتحادیهٔ اروپا در آنجا با یکدیگر ملاقات می‌کنند، همچنان در حال بحث و بررسی رژیم تحریم‌های سایبری و انتساب و ارتباطات راهبردی به منظور بکارگیری در صورت بروز حوادث سایبری مخرب است. در این میان، به احتمال زیاد موضوع انتساب همچنان به عنوان دشوارترین آن‌ها باقی خواهد ماند.

مطابق دستورالعمل‌های اجرایی بستهٔ دیپلماسی سایبری، انتساب می‌تواند بر اساس تجزیه و تحلیل داده‌های فنی و اطلاعات جامع، از قبیل اطلاعات در خصوص منافع احتمالی متجاوز، صورت گیرد. با این حال واضح است

---

1. Organization for the Prohibition of Chemical Weapons (OPCW)
2. Donald Tusk
3. Jean-Claude Junker
4. Federica Mogherini
5. GRU

که مسئلهٔ انتساب بسیار پیچیده است که نه‌تنها تحت تـأثیر عوامـل فنـی قـرار می‌گیرد، بلکـه عوامـل (جغرافیـای) سیاسـی[1] و عوامـل اقتصـادی نیـز بـر آن تأثیرگذارند. همان طور که پیشاپیش در انتساب‌هـای متعـدد دیگـر نشـان داده شده، شناسایی منبع حمله با آنکه چالش‌های فنی بخصوصی را شامل می‌شود همواره امکان‌پذیر است. با این حال، اتخاذ تصمیم سیاسی برای انتسـاب یـک حمله به یک کشور یا شاخه‌ای از دولت و حتی فراتر از آن، توافق بر سر یک پاسخ دیپلماتیک مشترک، به احتمال زیاد همچنان برای هیئتـی متشـکل از ۲۷ یا ۲۸ کشور چالش‌برانگیز خواهد بود. برخی چالش‌هایی که موجب دشوارتر شدن هر چه بیشتر یک انتساب جمعـی از جانـب اتحادیـهٔ اروپـا مـی‌شـوند مختص به بخش امنیت سایبری هستند. حال آنکه موارد دیگـر، از قبیـل الـزام به اتفاق نظر، به طور کلی مربوط به سیاست خارجی اتحادیهٔ اروپاست.

علاوه بر این، با وجود اینکه برخی حملات سـایبری بسـیار گسـترده‌انـد، بسیاری از آن‌ها تنها افراد یا نهادهای محدودی را تحت تأثیر قـرار مـی‌دهنـد. شناسایی جزئیات این تأثیر همیشه آسان نیست. بخش خصوصـی بـه شـدت تحت تأثیر فعالیت‌های مخرب سایبری قرار گرفته است، اما به دلایـل تجـاری و اعتباری، شرکت‌ها غالباً مایل بـه اعـلام علنـی حمـلات سـایبری یـا ارائـهٔ گزارش (کامل) حوادث و خسارات نیستند که بدین معناسـت کـه شـواهد و اطلاعات ارزشمندی در خصوص تهدیدات و متخلفان وجود نـدارد. از آنجـا که حملات سایبری یک حوزهٔ بزرگ و قلمروهـای مختلفـی را تحـت تـأثیر قرار می‌دهد، دامنهٔ تأثیرات آن‌ها به طور کامل شناسایی نمی‌شـود و در نتیجـه آگاهی موقعیتی مشترک در خصوص امنیت سایبری وجود ندارد.

چـالش بـزرگ‌تـر در ارتبـاط بـا مسـئلهٔ انتسـاب مربـوط بـه امکانـات و

---

1. (Geo) Political

ظرفیت‌های فنی کشورهای عضو اتحادیهٔ اروپا است. واقعیت این است که تنها برخی از کشورهای عضو این اتحادیه از قابلیت سایبری و اطلاعاتی و فرایندهای سیاسی و اداری لازم برای انتساب صحیح حملات سایبری برخوردارند. در سطوح مختلف، این قابلیت‌ها به ویژه در کشورهای عضو بزرگ مانند انگلستان، فرانسه، آلمان، و همچنین در کشورهایی همچون هلند، سوئد، دانمارک، فنلاند و شماری از کشورهای اروپای مرکزی و شرقی به چشم می‌خورد. با این حال، کشورهای دیگری نیز وجود دارند که به تازگی به جمع کشورهای عضو این اتحادیه پیوسته‌اند و هنوز از قابلیت‌های لازم در سطح استانداردهای اروپایی برخوردار نیستند. از این رو، قابلیت‌های سایبری پیشرفته به خصوص در مواقع رویارویی با حریفان پیشرفته، مانند گروه‌های تهدید پیشرفته و مستمر[1] ضرورت بیشتری می‌یابد.

۲. چالش‌های اقدام جمعی در اتحادیهٔ اروپا: یکی از چالش‌های اصلی کشورهای اتحادیهٔ اروپا برای انجام اقدام جمعی، این واقعیت است که روند تصمیم‌گیری اتحادیه در خصوص مسائل سیاست خارجی بسیار دشوار و مستلزم تصمیم یکپارچهٔ تمامی دولت‌های اتحادیهٔ اروپاست. غالباً دستیابی به چنین هدفی آسان نیست، به ویژه دربارهٔ تصمیمات مربوط به کشورهای ثالثی که برخی کشورهای عضو پیوندهایی مستحکم یا منافعی مشترک با آن‌ها دارند؛ به طور خاص در اینجا می‌توان به کشور روسیه اشاره کرد که با برخی کشورهای عضو اتحادیهٔ اروپا (از جمله ایتالیا و اسپانیا) روابط پایدار و مستحکمی دارد.

برخورداری از توانایی فنی و نهادی برای انتساب حملات سایبری لزوماً به معنای ارادهٔ سیاسی برای درخواست حمایت از شرکای اتحادیهٔ اروپا و یک واکنش مشترک نیست. کشورهای عضو بزرگ با توانایی سایبری

1. Advanced Persistent Threat (APT) Groups

پیشرفته نیز دارای منافع بین‌المللی پیچیده‌ای هستند که ممکن است در رابطه با کشورهای ثالث نیاز به یک اقدام تعادل‌ساز ظریف داشته باشند. در برخی موارد، کشورهای عضو ممکن است مایل به مقابله با فعالیت‌های سایبری مخرب کشورهای ثالث از طریق چارچوب اتحادیهٔ اروپا نباشند و گاهی برای حل‌وفصل این مسئله یک‌جانبه عمل کنند.

مهم‌تر از آن، به دلایل مختلفی از جمله دغدغه‌های امنیت ملی و عدم اعتماد و تجربهٔ حرفه‌ای ناکافی، سازمان‌های اطلاعاتی کشورهای عضو نیز غالباً تمایلی به اشتراک‌گذاری اطلاعات طبقه‌بندی‌شده با همتایان اتحادیهٔ اروپا ندارند. از آنجا که انتساب حملهٔ سایبری به یک شخص یا کشور ثالث می‌تواند پیامدهای منفی سیاسی یا اقتصادی به همراه داشته باشد، بسیاری از کشورها تمایلی به موافقت با اقدامات مشترک خطیر تنها بر اساس اعتماد و اطلاعات ناقص دیگر اعضا ندارند. علاوه بر این، انجام یک انتساب نادرست به اعتبار آن‌ها لطمه می‌زند. در میان کشورهای عضو بزرگ، ایتالیا بیشتر از همه خواستار رعایت احتیاط در پرداختن به این مسائل، به ویژه در ارتباط با روسیه است.[1] در انتهای دیگر این طیف، دانمارک و بریتانیا به طور علنی به انتساب حملات سایبری پرداخته‌اند و شدیداً خواستار سیاست بلندپروازانه‌تری در اتحادیهٔ اروپا هستند.

۳. چالش اعمال تحریم‌های سایبری: علاوه بر چالش انتساب و نیز چالش اتخاذ رویکرد جمعی، مسئلهٔ استفاده از تحریم‌ها نیز چالش‌های عدیده‌ای را به میان می‌آورد. اتحادیهٔ اروپا قادر نیست بدون انتساب یک حملهٔ سایبری به خصوص به یک کشور، تحریم‌هایی را علیه عاملان آن حملهٔ سایبری اعمال کند. در عین حال، راه‌اندازی رژیم جدید تحریم و

1. Guarascio, Francesco 2018; Interviews With EU Member States Officials, October 2018-January 2019.

اعمال تحریم‌ها در حوزه‌ای که برخی تعاریف و قوانین بین‌المللی به خوبی در آن تثبیت نشده باشد، نیاز به بررسی دقیق‌تر دارند. مدارک و شواهد تأییدکننده و پشتیبان از فهرست تحریم‌ها باید به اندازهٔ کافی مستحکم و با استناد به اهداف واضح و روشن باشد تا بتوان بعداً در صورت مواجهه با شکایات رسمی، بر چالش‌های حقوقی در دادگاه فائق آمد.

بر اساس سند دستورالعمل‌های اجرایی در زمینهٔ اعمال تحریم‌ها، اتحادیهٔ اروپا می‌تواند از اقدامات محدودکننده‌ای علیه کشوری که فعالیت‌های سایبری مخرب انجام می‌دهد یا «مسئول اقدامات یک بازیگر غیردولتی است که تحت اختیار یا کنترل خود عمل می‌کند» بهره جوید. با این حال، انواع تحریم‌هایی که تا کنون در شورا بررسی شده‌اند، به جای کشورها، تنها اشخاص یا نهادها را مورد هدف قرار می‌دهند.

در اکتبر ۲۰۱۸ دانمارک، استونی، فنلاند، لیتوانی، لتونی، هلند، رومانی و انگلستان طی یک متن تفسیری در خصوص اقدامات محدودکنندهٔ سایبری، خواستار اجرای رژیم تحریم برای رسیدگی به فعالیت‌های مخرب سایبری با قید فوریت شدند. بر اساس این سند، رژیم تحریم‌های جدید برای تغییر رفتار و «تقویت اجماع دربارهٔ رفتار مسئولانهٔ دولت» با تحمیل پیامدهایی بر بازیگران جنایتکاری که در عمل از قانون فراتر می‌روند، ضرورت دارد.[1] با اخطار دادن در خصوص اینکه هر گونه فعالیت سایبری مخرب عواقبی را به دنبال خواهد داشت و با اعمال محدودیت بر تصمیم‌گیرندگانی که احتمال بهره‌برداری از ابزار مخرب سایبری از سوی آن‌ها وجود دارد (برای مثال با مسدود کردن دسترسی آن‌ها به منابع مالی) یا از طریق تهدید و اجبار به واسطهٔ تحمیل پیامدهای معنادار دیگر، تغییر در رفتار یا در محاسبات

1. Bujek, 2018

سود ـ زیان عاملان احتمالی تهدیدات سایبری محقق خواهد شد.

در مجموع، رژیم تحریم‌های سایبری مورد بحثِ اتحادیهٔ اروپا اگرچه از رژیم تحریم‌های اتحادیهٔ اروپا در خصوص استفاده و توسعهٔ سلاح‌های شیمیایی پیروی می‌کند، با این حال تحریم‌های سایبری با توجه به اینکه تعاریف و قوانین مربوط به رفتار قابل قبول و رفتار قابل تحریم به اندازهٔ قوانین استفاده از سلاح‌های شیمیایی در سطح جهانی به رسمیت شناخته نشده‌اند، با چالش پیچیده‌تری مواجه است.[1]

ضمانت‌های بستهٔ دیپلماسی سایبری اتحادیهٔ اروپا

اگرچه بر اساس استراتژی امنیتی اتحادیهٔ اروپا، امنیت سایبری یک حق قانونی ملی است و تأمین آن بر عهدهٔ اعضا قرار دارد،[2] اما با توجه به وابستگی متقابل عملکرد اعضا، امنیت سایبری هر یک از آن‌ها می‌تواند امنیت جمعی اتحادیهٔ اروپا را تقویت یا تضعیف کند. از این رو، این اتحادیه تلاش می‌کند تا از طریق هماهنگی، تدوین یا تکمیل اسناد حقوقی و سیاسی لازم، حداقلی از مبنا و بستر قانونی برای اقدام و عمل جمعی در برابر تهدیدات سایبری فراهم سازد. پیمان لیسبون[3] و به خصوص «بند همبستگی»[4] و کمک‌های متقابل آن، این بستر قانونی در شرایط حملات سایبری گسترده را فراهم کرده است. بند همبستگی تصریح می‌کند که کشورهای عضو اتحادیهٔ اروپا در صورتی که یک یا چند کشور از میان آن‌ها قربانی حملات تروریستی، بلایای طبیعی یا انسانی (از جمله حوادث سایبری جدی) شوند، حمایت متقابل خود را ارائه می‌دهند. روند اجرای آن بر اساس تصمیم

1. EU Council, 2018

2. European Commission, High Representative of the European Union for Foreign Affairs and Security Policy, 2013.

۳The Lisbon Treaty

4. Solidarity Clause

شورای اتحادیهٔ اروپا در جون ۲۰۱۴ تعریف شده است. بند کمکِ متقابل مندرج در مادهٔ ۴۲ پاراگراف هفت تی‌ای‌یو[1] تقریباً مطابق با مادهٔ ۵ پیمان ناتو است؛ هرچند در این ماده اولویت با اعضای ناتو است. با این حال کشور فرانسه برای نخستین‌بار در نوامبر ۲۰۱۵، در پی حملات تروریستی پاریس، به این بند استناد کرد و خواستار حمایت اتحادیهٔ اروپا شد. تحت چارچوب پاسخ دیپلماتیک مشترک اتحادیهٔ اروپا به فعالیت‌های سایبری مخرب در اکتبر ۲۰۱۷، در صورت تطابق پاسخ‌ها با قوانین بین‌المللی، حتی انتساب صریح حملات سایبری به منابع یا افراد خاطی بخصوص ضرورت ندارد و این امر حمایت سایر اعضا را تسهیل می‌کند.[2]

جمع‌بندی و نتیجه‌گیری این فصل

دورنمای اصلی دیپلماسی سایبری اتحادیهٔ اروپا با تدوین سند «استراتژی امنیت سایبری» در سال ۲۰۱۳ و سپس «بستهٔ دیپلماسی سایبری» این اتحادیه در سال ۲۰۱۷ نمایان شد که در آن چشم‌انداز سیاست سایبری بین‌المللی منسجمی با پنج اولویت مشخص شد: ۱. ترویج و دفاع از حقوق بشر در فضای سایبری، ۲. ارزش‌های رفتاری و اعمال قوانین امنیت بین‌المللی در حوزهٔ فضای سایبری، ۳. حکمرانی اینترنت، ۴. ارتقای رقابت و شکوفایی اقتصادی در فضای سایبری، و ۵. ظرفیت‌سازی و توسعه در حوزهٔ فضای سایبری[3].

بستهٔ دیپلماسی سایبری اتحادیهٔ اروپا همچنین تأکید می‌کند که این اتحادیه اولویت‌های فوق را با تأکید بر اصول مسلّم ۱. باز بودن اینترنت، ۲. آزاد بودن اینترنت، ۳. تلاش برای تدوین استانداردهای رفتاری، و ۴. قابلیت تسرّی حقوق و قوانین بین‌المللی فعلی در حوزهٔ فضای سایبری دنبال خواهد کرد[4].

---

1. TEU
2. Greenberg, 2017
3. Bendiek, 2018
4. Ivan

در ارتباط با اولویت‌های گفته‌شده و نیز اصول مسلّم اتحادیهٔ اروپا، موضوعی که مستقیماً به دورنمای عملیاتی دیپلماسی سایبری اتحادیهٔ اروپا اشاره دارد این است که از دیدگاه این اتحادیه، این اولویت‌ها به سبب ماهیت و حوزه و گسترهٔ متقاطع آن از طریق تعامل استراتژیک با سازمان‌های بین‌المللی(به خصوص سازمان ملل متحد، اتحادیهٔ اروپا، ناتو، اتحادیه آسه‌آن و ...) و همچنین شرکای اصلی (در قالب رویکردهای دوجانبه) دنبال و پیگیری خواهد شد.

در ارزیابی اتحادیهٔ اروپا، ایالات متحده آمریکا، کانادا، مکزیک، برزیل، کرهٔ جنوبی، آفریقای جنوبی و ژاپن به عنوان شرکای استراتژیک تلقی می‌شوند و گفت‌وگوهای دوجانبه‌ای با آن‌ها در ارتباط با فضای سایبری آغاز شده که پیشرفته‌ترین آن نیز مربوط به ایالات متحده بوده است. در کنار این کشورها، روسیه و چین نیز به عنوان دو بازیگر اصلی و جدی (عموماً به عنوان دو منبع اصلی تهدیدات سایبری) در نظر گرفته می‌شوند که تلاش‌هایی برای برگزاری گفت‌وگوهای انتقادی در حوزهٔ فضای سایبری و تعاملات بین‌المللی با آن‌ها صورت گرفته، اما تا کنون به نتیجهٔ ملموسی نرسیده است.[1]

در جمع‌بندی نهایی از دیپلماسی سایبری اتحادیهٔ اروپا، چند نکته را می‌توان برجسته ساخت:

۱. اگرچه سیاست‌گذاران امنیتی کشورهای اروپایی همواره بر توسعهٔ قابلیت‌های دفاع سایبری و تلافی سایبری[2] کشورهای عضو اتحادیهٔ اروپا تأکید داشته‌اند، با این حال اتحادیهٔ اروپا، به عنوان یک کل، همچنان به منظور حفظ موقعیت خود به عنوان نیروی صلح، استراتژی سایبری خود را (هم در بُعد امنیتی و هم در بستهٔ دیپلماسی سایبری)، بر مبنای انعطاف‌پذیری و تأکید بیشتر بر دیپلماسی بنا نهاده است. به همین دلیل، پاسخ مشترک دیپلماتیک اتحادیهٔ اروپا به

1. Danca, 2015
2. Cyber-Retaliation

فعالیت‌های مخرب سایبری،[1] در درجهٔ اول ابزارهای غیرنظامی‌ای را که می‌توانند به کاهش تهدیدات امنیت سایبری یا پیشگیری از درگیری و ثبات هر چه بیشتر در روابط بین‌الملل کمک کنند، در اولویت قرار داده است.[2] شاید همین در اولویت قراردادن دیپلماسی را بتوان وجه ممیزهٔ اصلی دیپلماسی سایبری اتحادیهٔ اروپا در مقایسه با آمریکا و نیز کشورهای چین و روسیه دانست.

۲. از نظر امنیت سایبری، به خصوص در بُعد عملیاتی و قابلیت اجرایی استراتژی‌های امنیتی پیشنهادی اتحادیهٔ اروپا، باید گفت که به رغم روشن بودن اصول و کلیات آن، هنوز برخی از مهم‌ترین ابعاد بین‌المللی آن و اینکه رویّهٔ این اتحادیه در مذاکره و تعامل استراتژیک با شرکای بین‌المللی چطور خواهد بود، چندان روشن نیست. به خصوص نوع و نحوهٔ واکنش یا برخورد این اتحادیه زمانی که به صورت کلی یا تنهایی هر یک از اعضای آن، در معرض حملهٔ مخرب سایبری قرار گیرند چطور خواهد بود، دارای ابهاماتی جدی است. به همین دلیل به رغم مواجه شدن اعضای اتحادیهٔ اروپا با حملات متعدد سایبری (به طور مثال استونی و اوکراین)، این اتحادیه کمتر توانسته نسبت به انجام عمل متقابل اقدام نماید و تنها به اعمال رژیم‌های تحریمی محدود بسنده کرده است.

۳. از بُعد دیپلماتیک، این اتحادیه در سال ۲۰۱۷ از بستهٔ دیپلماسی سایبری رونمایی کرد و در آن اصول و مبانی و نیز برخی راهبردهای عملیاتی به عنوان مبنایی برای واکنش منسجم و جمعی پیش‌بینی کرد. با این حال ماهیت این بسته به خصوص با توجه به چالش‌هایی که در این فصل به آن‌ها اشاره شد، در هاله‌ای از ابهام قرار دارد. به طور کلی، این بسته بیشتر شبیه یک مانیفست است تا فراهم‌کنندهٔ برخی اقدامات عملی مشخص و روشن. با این حال، از

---

1. Joint Eu Diplomatic Response to Malicious Cyber Activities
2. Bendiek, 2018

آنجایی که اصول و مبانی اصلی این بسته مورد تأیید کشورهای عضو این اتحادیهٔ است، شاید اتحادیهٔ اروپا باید به عنوان یک گام بلند و روبه‌جلو، چارچوب اجرایی این بستهٔ دیپلماسی سایبری را نهایی کند؛ چارچوبی که امکان انجام اقدامات جمعی عملی در چارچوب اقدامات پیشگیرانه، همکارانه، ثبات‌ساز و محدودکننده را در اختیار آن‌ها قرار دهد.

۴. هنوز برخی از کشورهای اروپایی (از جمله کشورهایی که سابقاً در بلوک شرق قرار داشتند) آگاهی و منابع انسانی، فنی و زیرساختی لازم را برای حفظ معیارهای اولیهٔ امنیت سایبری یا قابلیت تشخیص حملاتی که از طریق سرورها بر قلمرو آن‌ها تحمیل می‌شود را ندارند و به عبارتی، هنوز در فاز دفاعی ـ امنیتی سایبری هستند. به همین دلیل، این کشورها در مواجهه با ایدهٔ یک رویکرد جمعی برای امنیت سایبری، نسبت به اطمینان از حاکمیت ملی خود تردید دارند و آن را چشم‌اندازی غیرواقعی برای زمان حاضر می‌دانند. این امر تا حد زیادی دیپلماسی سایبری این اتحادیه به ویژه در ارتباط با ابعاد و مؤلفه‌های مهمی که پیش‌تر به آن‌ها اشاره شد (اعتمادسازی، هنجارسازی و محافظت از داده و ...)، با چالش مواجه می‌کند.

۵. کشورهای عضو اتحادیهٔ اروپا به منظور عملیاتی‌سازی بستهٔ دیپلماسی سایبری و بهبود امنیت سایبری خود باید دست به یک سری اقدامات دیگر نیز بزنند، از جمله تقویت قابلیت‌های سایبری، آگاهی‌افزایی در بین مردم و تصمیم‌گیرندگان و همچنین ایجاد و ارتقای فرایندهای دولتی داخلی در زمینهٔ اطلاع‌رسانی بهتر برای تصمیم‌گیری‌ها. به منظور اتخاذ تصمیمات مشترک، کشورهای عضو باید در زمینهٔ ارزیابی تهدیدات مشترک و فرهنگ مشترک انتساب تلاش کنند. بدین منظور، بهبود اشتراک‌گذاری اطلاعات امری ضروری است. همکاری با بخش خصوصی، نهادهای مدنی هم در سطح داخلی و هم در سطح بین‌المللی نیز هم‌زمان حائز اهمیت هستند.

منابع

Bendiek, Annegret, (2018). "The EU as a Force for Peace in International Cyber Diplomacy". German Institute for International & Security Affairs.

Bussoletti, Francesco, "All Five Eyes Countries Have Blamed Russia for the NotPetya Cyber Attack", Difesa&Sicurezza, 16 February 2018; Stilgherrian, "Blaming Russia for NotPetya was Coordinated Diplomatic Action", ZDNet, 22 April 2018.

Bujek, M. (2018) .Cybersecurity as the Basis for State and Society Security in the 21st Century. Safety&Defense. 13_8.

Chertoff, M. (2018).Cyber Operations Today: Preparing for 21st Century Challenges in an Information-Enabled Society. The Chertoff Group: Former Secretary of Homeland Security.

Christou, George, (2016). Cybersecurity in the European Union: Resillience and Adaptability in Governance Policy. UK, Palgrave Macmillan.

Council of the European Union. Outcome of Proceedings 6122/15. Council Conclusions on Cyber Diplomacy. Brussels, 11 February 2015.

Council of the European Union (2016), "Non-paper: Developing a Joint EU Diplomatic Response Against Coercive Cyber Operations", 5797/6/16, REV 6,۱۹ May 2016.

Council of the European Union (2017), "Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")", 10474/17, 19 June 2017.

Council of the European Union. An Outline for European Cyber Diplomacy Engagement. 9967/4/14, Brussels, 23.09.2014.

Council of the European Union conclusions (2018), "EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises", 10086/18, 26June 2018.

Cyber-Attack: Europol Says it Was Unprecedented in Scale", BBC News, 15 May 2017.

Cyber-Attack That Crippled NHS Systems Hits Nissan Car Factory in Sunderland and Renault in France", The Independent, 13 May 2017.

Dancă, Dana, (2015). "Cyber Diplomacy – A New Component of Foreign Policy". Journal of Law and Administrative Sciences.

Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities, The 9 October 2017 Draft Version is the Latest Version of the Document Available Online.

European Commission, High Representative of the European Union for Foreign Affairs and Security Policy. Joint Communication To The European Parliament, The Council, The European Economic And Social Committee And The Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. JOIN (2013) 1 Final, Brussels, 7.2.2013.

EU Council, Council Decision (CFSP) 2018/1544 of 15 October 2018concerning restrictive measures against the proliferation and use of chemical weapons.

Government of Canada, Communications Security Establishment, CSE Statement on the NotPetya Malware, 15 February 2018.

Gady, F.S, & Austin, G. (2010), Russia, the United States and Cyber Diplomacy: Opening the Doors. East West Institute. New York, p.10.

Greenberg, Andy, "How An Entire Nation Became Russia's Test Lab for Cyberwar", Wired, 20 June 2017.

Greenberg, Andy, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", Wired, 22 August 2017.

Guarascio, Francesco, "Italy Resisting EU Push to Impose Sanctions Overcyberattacks", Reuters, 12 October 2018 and Interviews with EU Member States Officials, October 2018-January 2019.

Ivan, Paul, (2019)."Responding to Cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox". European Policy Center.

Joint Statement by Presidents Tusk and Juncker and High Representative Mogherini on Russian Cyber Attacks, 4 October 2018.

Klementiev, Mikhail, "Russia in Talks with China's Huawei on Data Storage Technologies' Licensing", Sputnik News, August 24, 2016: https://sputniknews.com.

NATO Cooperative Cyber Defence Centre of Excellence, "An Updated Draft of the Code of Conduct Distributed in the United Nations-What's New?", February 10, 2015, https://ccdcoe.org.

Roberts, Paul, (2017). "NotPetya Infection Left Merck Short of Key HPV Vaccine", the Security Ledger.

Rosemain, Mathieu, Le Guernigou, Yann and Davey,

“Renault Stops Production at Several Plants After Ransomware Cyber Attack as Nissan also Hacked”, Mirror Online, 13 May 2017.

Reuters, 21 June 2017." Honda Halts Japan Car Plant After WannaCry Virus Hits Computer Network”.

Tiirmaa-Klaar, Heli (2013), “Cyber Diplomacy: Agenda, Challenges and Mission”, In Katharina Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn.

United Kingdom Foreign & Commonwealth Office, National Cyber Security Centre, and Lord Ahmad of Wimbledon, Foreign Office Minister Condemns Russia for NotPetya Attacks, 15 February 2018.

United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 22 July 2015.

Yu, S., Wang, G., & Zhou, W.(2015) Modeling Malicious Activities in Cyber Space. IEEE Network 87-83.

فصل هشتم

دیپلماسی سایبری مالزی

درآمد

هدف از تدوین این فصل، مطالعهٔ نحوهٔ مواجههٔ مالزی با فضای سایبری و نوع حکمرانی این کشور در این فضای جدید و نوظهور است. مطالعهٔ حکمرانی سایبری در مالزی و نوع مواجههٔ آن با فضای سایبری با هدف استفاده از تجربهٔ این کشور از این منظر حائز اهمیت است که مالزی به عنوان یک کشور درحال‌توسعه، توانسته است در حوزه‌های مختلف الگویی نسبتاً موفق از توسعهٔ بومی ارائه دهد که مورد توجه جامعهٔ جهانی نیز قرار گرفته است، به طوری که به عنوان یکی از مهم‌ترین دستاوردهای آن، بانک جهانی اخیراً اعلام کرد که مالزی با توجه به روند رشد خود، تا سال ۲۰۲۴ به جمع کشورهای پردرآمد خواهد پیوست. ضمن آنکه مالزی به عنوان یک کشور اسلامی، قرابت‌ها و مشترکات فرهنگی و دینی و تاریخی زیادی با ایران دارد و از این رو می‌توان در مقایسه با سایر کشورهای توسعه‌یافته و درحال‌توسعه، از الگوی آن برای هر گونه سیاست‌گذاری یا برنامه‌ریزی در این زمینه بهره برد.

مطالعهٔ نحوهٔ مواجههٔ مالزی با فضای سایبری و نوع حکمرانی این کشور در فضای سایبری به طور وثیقی با برنامه‌های توسعهٔ این کشور، به خصوص «چشم‌انداز ۲۰۲۰» مالزی و به تبع آن «زیرساخت اطلاعات ملی» این کشور عجین است. از این رو پیش از هر چیزی، مداقه در برنامهٔ چشم‌انداز ۲۰۲۰

مالزی، شناخت ابعاد مختلف آن و از همه مهم‌تر جایگاهی که بـرای فنـاوری ارتباطات و اطلاعات در این چشم‌انداز تصور شده ضروری است.

برنامهٔ چشم‌انداز ۲۰۲۰ مالزی: زمینه‌های ورود به سیاست‌گذاری فضای سایبری

آغاز برنامهٔ توسعهٔ مالزی موسوم به چشم‌انداز ۲۰۲۰ در سال ۱۹۹۱، که بـر اساس آن، این کشور باید از اقتصاد کشاورزی به اقتصاد «دانش‌بنیـان» گـذار کند، و هم‌زمانیِ آن با ساخت سوپر کریدور مـولتی‌مـدیاییِ ایـن کشـور بـه دست ماهاتیر محمد، نخست‌وزیر وقت، را می‌توان سرآغاز سیاست‌گـذاری و برنامه‌ریزی در ارتباط با فضای سایبری (با تأکید بر تهدیدها، فرصـت‌هـا، چالش‌ها و آسیب‌های مرتبط با آن) دانست.

اساس برنامهٔ چشم‌انداز ۲۰۲۰ مالزی بر استفادهٔ گسترده از ظرفیت‌های ارتباطاتی و اطلاعاتی به عنوان ابزاری برای توسـعه اسـتوار اسـت کـه بـه اسـتفادهٔ گسـترده از فناوری‌های نوین در بخـش صـنعت، بخـش خصوصـی، بخـش عمـومی و سـایر حوزه‌ها در سطح وسیع منجر می‌شود. بر اساس برنامهٔ چشم‌انداز ۲۰۲۰، دولـت بـه طور کلی ده حوزه را به عنوان حوزه‌های کلیدی در سطح ملی انتخاب کرده است که عمدهٔ تلاش‌ها، برنامه‌ریزی‌ها، سیاست‌گذاری‌ها و سـرمایه‌گـذاری‌هـا بـرای تحقـق اهداف چشم‌انداز ۲۰۲۰ در این ده حوزه متمرکز می‌شوند. این ده حوزه در واقـع ده حوزهٔ کلیدی‌اند که زیرساخت اطلاعاتی ملی[2] این کشور را تشکیل می‌دهند.

ده حوزهٔ کلیدی در زیرساخت اطلاعاتی ملی کشور مالزی

ده حوزهٔ کلیدی در زیرساخت اطلاعـاتی ملـی مـالزی، حـوزه‌هـا (فیزیکـی ـ سایبری)، سیستم‌ها و کارکردهایی هستند که برای توسعهٔ ملی مالزی حیاتی‌اند و

1. Multimedia Super Corridor
2. Critical National Information Infrastructure

هر گونه نقصان، اختلال یا تخریب آن تأثیر شگرفی در اقتصاد ملی، ایماژ ملی[1]، دفاع و امنیت ملی، ظرفیت‌های کارکردی دولت، سلامت و امنیت عمومی این کشور خواهد داشت. همچنین متناظر با این ده حوزه، نهادها و سازمان‌های مسئول که عمدتاً وزارتخانه‌های این کشورند نیز به عنوان نهادها و سازمان‌های مسئول و متولی این ده حوزه معرفی شده‌اند که باید بر اساس چشم‌انداز ۲۰۲۰ این کشور، برای دستیابی به اهداف ازپیش‌تعیین‌شده، سیاست‌گذاری و برنامه‌ریزی و اقدام کنند. این حوزه‌های کلیدی موسوم به «ده حوزهٔ زیرساخت اطلاعاتی ملی»، به همراه نهادها یا سازمان‌های متولی، هر کدام در جدول شمارهٔ ۱ نمایش داده شده‌اند که شامل موارد ذیل می‌شوند:

جدول شمارهٔ ۱. ده حوزهٔ کلیدی در زیرساخت اطلاعاتی مالزی به تفکیک نهادها یا سازمان‌های مذکور

ردیف	حوزهٔ زیرساخت	نهادهای مسئول
۱	دفاع و امنیت ملی	وزارت دفاع (نظامیان) و وزارت کشور (پلیس)
۲	بانکداری و فایننس	وزارت فایننس، بانک مرکزی و کمیسیون امنیت
۳	اطلاعات و ارتباطات	وزارت اطلاعات، ارتباطات و فرهنگ و کمیسیون مولتی‌مدیا
۴	انرژی	کمیسیون انرژی، شرکت ملی نفت و شرکت ملی برق
۵	حمل و نقل	وزارت حمل و نقل
۶	آب	کمیسیون ملی خدمات آب
۷	سلامت و بهداشت	وزارت بهداشت
۸	دولت	دپارتمان برنامه‌ریزی مدیریت، مدرن‌سازی و اجرایی (دفتر نخست‌وزیر)
۹	خدمات اضطراری	وزارت مسکن و شهرسازی
۱۰	غذا و کشاورزی	وزارت کشاورزی

1. National Image

با توجه به تمرکز بسیار زیاد چشم‌انداز ۲۰۲۰ مالزی بر استفاده از فناوری آی‌تی و حرکت بخش‌های صنعت، خصوصی، عمومی و دیگر حوزه‌ها به سوی سیستم اطلاعات دیجیتال[1] بدیهی است که دولت مالزی باید هم‌زمان با تغییر و تحولات فناوری‌های نوین، سیاست‌ها و استراتژی‌های نوینی برای صیانت و اطمینان از کارایی و عملکرد ده حوزهٔ کلیدی زیرساخت اطلاعات ملی این کشور اتخاذ کند.

تدوین سیاست امنیت سایبری ملی[2]: سناریویی برای حکمرانی فضای سایبری

تدوین سند سیاست امنیت سایبری ملی نخستین و مهم‌ترین نماد مواجههٔ دولت مالزی با فضای نسبتاً جدید سایبری بود که سابقهٔ آن به اوایل قرن ۲۱ برمی‌گردد. از ابتدا، برنامه‌ریزی برای تدوین سیاست امنیت سایبری ملی به وزارت علوم و فناوری و نوآوری[3] مالزی محول شده است. با توجه به این مسئولیت، این وزارتخانه در سال ۲۰۰۵ کار تحقیقاتی در این زمینه را آغاز و پس از یک سال مطالعه و تحقیق و بررسی، پیشنهادهای خود را در قالب سند سیاست امنیت سایبری ملی در ماه می ۲۰۰۶، به تأیید شورای ملی آی‌تی[4] مالزی رساند.

هدف راهبردی در سند سیاست امنیت سایبری ملی مالزی عبارت است از: «ده حوزهٔ کلیدی زیرساخت اطلاعاتی ملی این کشور باید امن و منعطف و خوداتکا باشد. این وضعیت با ترویج فرهنگ امنیت[5] در جامعه، به ثبات و توسعه و نیز ایجاد رفاه و ثروت در جامعه منجر خواهد شد».

---

1. Digital Information System
2. National Cyber Security Policy
3. Ministry of Science, Technology & Innovation (Mosti)
4. National It Council (Nitc)
5. Culture of Security

سیاست امنیت سایبری ملی مالزی بر اساس پنج محور اصلی تدوین شده که به شرح ذیل است:

۱. مقررات‌گذاری و قانون‌گذاری: در این کشور باید قوانین مکفی (اعم از اجرایی و نیز حقوقی و قضایی) برای رسیدگی به امور مربوط به فناوری‌های نوین اطلاعاتی و ارتباطی، از جمله در حوزهٔ سایبری، وجود داشته باشد.

۲. فناوری و نوآوری: این کشور باید به جدیدترین فناوری‌ها و نوآوری‌های ارتباطی دسترسی داشته باشد.

۳. همکاری بخش خصوصی ـ دولتی: برای تحقق اهداف توسعه‌ای، همکاری و همراهی بخش خصوصی با دولت ضروری است.

۴. سازمان‌دهی (ساختار یا سازمان‌دهی): حکمرانی در حوزهٔ فناوری و نوآوری به خصوص در حوزهٔ سایبری، نیازمند سازمان‌دهی بر اساس تفکیک وظایف و مسئولیت‌ها امری ضروری است.

۵. همکاری‌های بین‌المللی: یکی از اهداف مالزی در هر زمینه‌ای، تبدیل شدن به الگو و برند جهانی است. حوزهٔ سایبری نیز از این امر مستثنا نیست. مالزی با هدف تبدیل شدن به الگویی در مقیاس منطقه‌ای و بین‌المللی باید از طریق همکاری نزدیک با کشورهای جهان به خصوص در قالب سازمان‌های مهم بین‌المللی، همچون سازمان ملل و سازمان کنفرانس اسلامی، نقش مشارکت‌جویانه‌ای همراه با رهبری داشته باشد.[1]

در سیاست امنیت سایبری ملی مالزی، همچنین هشت حوزهٔ اصلی (پیشرو) تعریف و متناظر با هر حوزه، یکی از وزارتخانه‌ها، نهادها یا سازمان‌های این کشور به عنوان «پیشران»، مسئول آن حوزه تعیین شده است که باید نسبت به تأمین پنج محور گفته‌شده در حوزهٔ مسئولیتی خود اطمینان حاصل کند (جدول شمارهٔ ۲).

1. National Cyber Security Policy: The Way Forward, 2006.

جدول شمارهٔ ۲. هشت حوزهٔ اصلی سیاست امنیت سایبری ملی مالزی به تفکیک نهادهای متولی و وظایف

ردیف	حوزه[1]	پیشران‌ها	وظیفه
۱	حکمرانی مؤثر	وزارت علوم و فناوری و نوآوری	تأسیس مرکز ملی هماهنگی اطلاعاتی ـ امنیتی
۲	چارچوب حقوقی و قانونی	دادگاه عمومی (مدعی‌العموم)[2]	پیگرد قضایی و قانونی جرایم سایبری
۳	چارچوب فناوری امنیت سایبری	وزارت علوم و فناوری و نوآوری	صدور گواهی یا تأییدیه برای مدیریت امنیت ـ اطلاعات و تضمین آن
۴	فرهنگ امنیت و ظرفیت‌سازی	وزارت علوم و فناوری و نوآوری	کاهش تعداد حوادث امنیتی ـ اطلاعاتی از طریق افزایش آگاهی‌ها و مهارت‌ها
۵	تحقیق و توسعه به سوی خوداتکایی[3]	وزارت علوم و فناوری و نوآوری	پذیرش و استفاده از محصولات داخلی مربوط به حوزهٔ اطلاعاتی ـ امنیتی
۶	انطباق و اجرا[4]	وزارت اطلاعات و ارتباطات و فرهنگ	اطمینان از اجرا و انطباق قوانین مربوط در ده حوزهٔ کلیدی زیرساخت اطلاعاتی ملی
۷	آمادگی اضطراری[5] در حوزهٔ امنیت سایبری	شورای امنیت ملی	ایجاد انعطاف و آمادگی در ده حوزهٔ کلیدی زیرساخت اطلاعاتی ملی در مقابل جرایم سایبری، تروریسم، جنگ اطلاعاتی و ...

1. Thrust
2. Attorney General's Chambers
3. Self-Reliance
4. Compliance & Enforcement
5. Emergency Readiness

۸	همکاری‌های بین‌المللی	وزارت اطلاعات و ارتباطات و فرهنگ	برندسازی در سطح بین‌المللی از طریق اقدامات خلاقانه در حمایت و تقویت و امنیت ده حوزهٔ کلیدی زیرساخت اطلاعاتی ملی

بر این اساس، اگر دربارهٔ تأمین مؤثر شرایط هشت حوزهٔ گفته‌شده در هر یک از ده حوزهٔ کلیدی زیرساخت اطلاعاتی ملی این کشور اطمینان حاصل شود، مالزی به هدف راهبردی سایبری خود دست یافته است. در واقع وظیفه و مسئولیت هر یک از نهادهای ذکرشده در جدول شمارهٔ ۲ به عنوان پیشران، اطمینان از تحقق شرایط و وظایفی است که در سند سیاست امنیت سایبری ملی به آن اشاره شده است. تحقق این شرایط و وظایف، در واقع تضمین‌کنندهٔ تحقق اهداف مندرج در چشم‌انداز ۲۰۲۰ این کشور است.

- **هشت حوزهٔ پیشرو در سیاست امنیت سایبری ملی**

همان طور که قبلاً نیز گفته شد، سیاست امنیت سایبری ملی مالزی مبتنی بر هشت حوزه است که در هر حوزه، یکی از نهادها یا سازمان‌های مالزیایی به عنوان مسئول آن حوزه، اهداف و وظایفی را بر عهده دارند. این هشت حوزه عبارت‌اند از:

۱. حکمرانی مؤثر: این حوزه در واقع به معنای به رسمیت شناختن «وابستگی متقابل» هر ده حوزهٔ کلیدی زیرساخت اطلاعات ملی در کشور مالزی است. هدف از تعیین این حوزه عبارت است از: ۱. متمرکز ساختن هر گونه اقدام و فعالیت در ارتباط با امنیت سایبری ملی، ۲. تشویق و ترغیب همکاری مؤثر بین بخش‌های عمومی و دولتی و خصوصی، و ۳. ایجاد بستر تبادل اطلاعات در حوزه‌های مربوط.

۲. چارچوب حقوقی و قانونی: این حوزه بیشتر بـه موضـوعات حقـوقی و قضایی مربوط به فضای سایبری پرداخته و هدف از آن، تأمین یک «نظام قـانونی و حقوقی و قضایی» مکفی برای حوزهٔ سایبری است که همیشه در حال تغییر و تحول است. به این اعتبار، وجود قوانین و نیز مقررات‌گـذاری لازم بـرای ایجـاد اطمینان و اعتمادسازی در ده حوزهٔ کلیـدی زیرسـاخت اطلاعـات ملـی بسـیار ضروری است. اهداف جزئی‌تر این حوزه عبارت‌اند از: مطالعه و ارزیابی قـوانین سایبری مالزی، پیگیری و رصد طبیعت سیال و تغییر تهدیـدات امنیـت سـایبری مالزی، پایه‌گذاری برنامه‌های مدرن در زمینهٔ ظرفیت‌سازی در حوزهٔ سایبری برای مؤسسات و آژانس‌های ملی مجری قـانون، اطمینـان از همسـویی و همـاهنگی تمامی قوانین اجرایی داخلی با قوانین و معاهدات و کنوانسیون‌های بین‌المللی.

۳. چارچوب فناوری امنیت سایبری: به طور کلی، دستورالعمل‌ها و کتابچه‌های زیادی در بین مردم در ارتباط با امنیت سایبری وجود دارد. با این حال، بسـیاری از آن‌ها ناقص و دربردارندهٔ همهٔ دستورالعمل‌ها و راهنمایی‌های لازم نیستند. هدف از این حوزه که زیر نظر وزارت علوم، فناوری و نوآوری مالزی می‌باشـد، تـدوین و توسعه یک چارچوب فناوری امنیت سـایبری اسـت کـه نیازهـا و لـوازم «امنیـت اطلاعات» را مشخص می‌سازد، عناصر ده حوزهٔ کلیدی زیرساخت اطلاعاتی ملـی را کنترل و رصد می‌کند و سیستم‌ها و محصولات مربوط به «امنیـت اطلاعـات» را ارزیابی، تأیید و اجرایی می‌کند. زمانی که از امنیـت اطلاعـات صـحبت بـه میـان می‌آید، مسائل مهمی همچون مـدیریت اطلاعـات و کنتـرل فنـی و عملیـاتی و ... برجسته می‌شود که نقش مهمی در امنیت سایبری دارند.

۴. فرهنگ امنیت سایبری: این حوزه بـیش از هـر چیـز بـر ابعـاد انسـانی سیاست‌گذاری در حوزهٔ سـایبری متمرکـز اسـت. اهـداف دقیـق ایـن حـوزه عبـارت‌انـد از: الـف) توسـعه و تـرویج و حفـظ فرهنـگ ملـی امنیـت؛

ب) استانداردسازی و هماهنگی برنامه‌های آموزشی و آگاهی‌بخشی در زمینهٔ امنیت اطلاعات در هر ده حوزهٔ کلیدی زیرساخت اطلاعات ملی کشور؛ ج) پایه‌گذاری سازوکاری مؤثر در زمینهٔ توزیع و نشر سواد و دانش امنیت اطلاعات در سطح ملی؛ د) تعیین حداقل نیازمندی‌ها و کیفیت لازم برای کارشناسان و متخصصان امنیت اطلاعات. در این مورد باید تأکید کرد که توسعه و ترویج فرهنگ امنیت سایبری مستلزم رهبری و نیز مشارکت نهادها و سازمان‌های متعدد است. برای همین هدف، باید نقشه‌ای استراتژیک با مشارکت همهٔ وزارتخانه‌ها و نهادهای درگیر برنامه‌ریزی و مدیریت شود.

۵. «تحقیق و توسعه» به سوی خوداتکایی: برای دستیابی به خوداتکایی، در تمامی ده حوزهٔ کلیدی زیرساخت اطلاعات ملی باید یک چارچوب تحقیق و توسعهٔ یکپارچه تهیه و به اجرا گذاشته شود که مهم‌ترین هدف آن «به سوی خوداتکایی» باشد. اهداف دقیق این حوزه عبارت‌اند از: مدیریت و فرمول‌بندی و اولویت‌سنجی فعالیت‌های تحقیق و توسعه در زمینهٔ امنیت سایبری، تقویت و گسترش محققان حوزهٔ «امنیت اطلاعات»، ترویج توسعه و تجاری‌سازی مالکیت معنوی، فناوری و نوآوری از طریق تحقیق و توسعه، کمک در تقویت و توسعهٔ صنعت امنیت اطلاعات.

۶. انطباق و اجرا: با توجه به اینکه عمدهٔ رگولاتوری‌های ارتباطی و اطلاعاتی مالزی (شامل کمیسیون ارتباطات و مولتی‌مدیا، مخابرات مالزی، شبکه‌های تلفن همراه و ...) زیر نظر وزارت اطلاعات و ارتباطات و فرهنگ این کشور است، حوزهٔ انطباق و اجرا به این وزارتخانه واگذار شده است. اهداف دقیق این حوزه عبارت‌اند از: استانداردسازی برای سیستم‌های امنیت اطلاعات تمامی عناصر ده حوزهٔ کلیدی زیرساخت اطلاعات ملی، تقویت و نظارت و اطمینان از اعمال و اجرای این استانداردها، توسعه و تدوین یک چارچوب ارزیابی از ریسک و خطرات امنیت اطلاعات در این کشور.

برای دستیابی به این اهداف، وزارت اطلاعات و ارتباطات و فرهنگ مالزی مکانیسم‌های کنترلی مستقل و نیز حسابرسی‌ها و ممیزی‌های امنیتی متناوبی دارد که در ارتباط با دستگاه‌ها و نهادهای ده حوزهٔ کلیدی زیرساخت اطلاعات ملی این کشور اعمال می‌شود. این حسابرسی‌ها و ممیزی‌ها موجب شناسایی نقاط ضعف و حوزه‌هایی می‌شوند که به لحاظ امنیت سایبری نیاز به کمک دارند.

۷. آمادگی اضطراری در حوزهٔ امنیت سایبری: تیم واکنش اضطراری رایانه‌ای[1] ابزار مهمی برای کاهش تهدیدات سایبری در این کشور است. این گروه که در کمپانی امنیت سایبری مالزی مستقر است، به طور مداوم تهدیدات سایبری در این کشور را مانیتور و رصد می‌کند. اهداف دقیق‌تر این حوزه عبارت‌اند از: تقویت تیم واکنش اضطراری رایانه‌ای، توسعهٔ سازوکارِ شناسایی و گزارش‌دهی حوادث مربوط با امنیت اطلاعات، تشویق هر ده حوزهٔ کلیدی زیرساخت اطلاعات ملی این کشور به نظارت و رصد دائمی حوادث امنیت اطلاعات، انتشار بموقع توصیه‌ها و مشاوره‌ها در زمینهٔ تهدیدات سایبری، تشویق هر ده حوزهٔ کلیدی زیرساخت اطلاعات ملی این کشور به برگزاری برنامه‌های ارزیابی دوره‌ای در زمینهٔ امنیت اطلاعات.

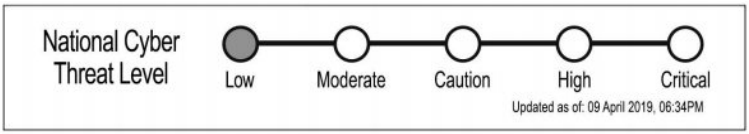
۸. همکاری‌های بین‌المللی: دامنهٔ فعالیت‌های سایبری محدود به مرزهای جغرافیایی کشورها نیست. از این رو موفقیت در زمینهٔ اقدامات و فعالیت‌های مرتبط با امنیت سایبری منوط به همکاری‌های منطقه‌ای و بین‌المللی است. اموری نظیر تبادل دانش و اطلاعات، بحث و ارزیابی چالش‌های پیش رو با سایر کشورها، فراگیری تجارب کشورهای دیگر و جلوگیری از تکرار اشتباهات دیگران، و از همه مهم‌تر، کمک و همفکری در جهت‌دهی به سیاست‌های منطقه‌ای و بین‌المللی در حوزهٔ سایبری، به

1. The Computer Emergency Response Teams (CERT)

مالزی کمک خواهد کرد تا بهتر بتواند هر ده حوزهٔ کلیدی زیرساخت اطلاعات ملی این کشور را مصون نگه دارد. اهداف دقیق‌تر این حوزه عبارت‌اند از: تشویق به مشارکت فعالانه در تمامی نهادها و سازمان‌های بین‌المللی مرتبط با امنیت اطلاعات، حضور در پانل‌ها و نیز آژانس‌های چندملیتی مربوطه، تشویق به مشارکت فعالانه در تمامی کنفرانس‌ها و فروم‌ها و رویدادهای علمی بین‌المللی مرتبط با امنیت اطلاعات، تقویت جایگاه استراتژیک مالزی در زمینهٔ امنیت اطلاعات از طریق میزبانی از کنفرانس‌ها و سمینارهای علمی بین‌المللی در زمینهٔ امنیت اطلاعات.[1]

ساختار سیاست‌گذاری و اجرایی حوزهٔ سایبری در کشور مالزی

پس از تدوین سند سیاست امنیت سایبری ملی، مدیریت اصلی حوزهٔ سایبری در کشور مالزی بر عهدهٔ وزارت علوم و فناوری و نوآوری این کشور گذاشته شده بود. با این حال، در بازنگری سال ۲۰۱۰ و با توجه به تغییر وظایف و مسئولیت‌های وزارتخانه‌ها، ساختار جدیدی ارائه شد.



شکل شمارهٔ ۱. ارزیابی دولت مالزی از وضعیت امنیت سایبری این کشور (آپریل ۲۰۱۹)

در ساختار جدید حکمرانی سایبری کشور مالزی و بر اساس حوزهٔ اول

1. Mohd Shamir b Hashim, 2011

(حکمرانی مؤثر)، که به وزارت علوم و فناوری و نوآوری واگذار گشته، راه‌اندازی «مرکز ملی هماهنگی اطلاعاتی ـ امنیتی» پیش‌بینی شده است. این مرکز بر اساس ساختاری که در نمودار شمارهٔ ۱ به نمایش درآمده، فعالیت‌های خود را انجام می‌دهد.[1]

- **شورای ملی آی‌تی مالزی**

این شورا در سال دو بار تشکیل جلسه می‌دهد. اعضای اصلی آن نخست‌وزیر (به عنوان رئیس)، معاون نخست‌وزیر، و وزیر علوم و فناوری و نوآوری (دبیر شورا) است. در این شورا همچنین نمایندگانی از بخش خصوصی و بخش دولتی و نهادهای مدنی حضور دارند.

در ذیل این شورا، سه کمیتهٔ دیگر شامل کمیتهٔ مشورتی امنیت سایبری ملی مالزی،[2] کمیتهٔ هماهنگی امنیت سایبری ملی مالزی،[3] کمیتهٔ ملی مدیریت بحران سایبری،[4] و همچنین کارگروه ملی مدیریت بحران سایبری[5] و کارگروه بحران سایبری[6] فعال‌اند که اعضای آن ترکیبی از نمایندگان هجده نهاد یا سازمان فعال در حوزهٔ سایبری در کشور مالزی هستند، از قبیل وزارت خارجه، وزارت کشور، وزارت دفاع، کمیسیون ارتباطات، شورای امنیت ملی، کمیسیون انرژی، کمیسیون ارتباطات و ... . نمودار شمارهٔ ۱ ساختار حکمرانی سایبری در کشور مالزی را همراه با جزئیات آن نشان می‌دهد.

---

1. National Cyber Security Policy: The Way Forward, 2006.
2. National Cyber Security Advisory Committee (NaCSAC)
3. National Cyber Security Coordination Committee (NC3)
4. National Cyber Crisis Management Committee (NCCMC)
5. National Cyber Crisis Management Working Group
6. Cyber Crisis Working Group

نمودار شمارهٔ ۱. ساختار حکمرانی سایبری در کشور مالزی

نهادها و سازمان‌های اجرایی ویژه در ارتباط با حوزهٔ سایبری در مالزی

برای رسیدگی به امور مربوط به حوزهٔ سایبری، اعم از آموزش و خدمات و تحقیقات مربوط به جرایم این حوزه، نهادها و سازمان‌هایی در کشور مالزی فعال‌اند که اهم آن‌ها به شرح ذیل است:

۱. کمپانی امنیت سایبری مالزی:[1] این کمپانی در دو سطح دولتی و خصوصی فعال است و فعالیت‌های آن زیر نظر وزارت علوم و فناوری و نوآوری است. وظیفهٔ این کمپانی دریافت گزارش‌ها در ارتباط با حوادث سایبری (Cyber 999) در این کشور است. برگزاری دوره‌های آموزشی در زمینهٔ فضای سایبری و ارائهٔ خدمات فنی مهندسی به شرکت‌ها و کمپانی‌های بخش‌های مختلف دولتی و خصوصی و صنعتی از دیگر وظایف این کمپانی است. این کمپانی دارای سه پلتفرم برای ارائهٔ خدمات است:

ـــ فضای سایبری مصون[2]: این دپارتمان نقش پیشگیرانه‌ای دارد و مسئول آموزش و افزایش آگاهی عموم مردم دربارهٔ مسائل فنی و موضوعات اجتماعی است که افراد در استفاده از اینترنت، به ویژه دربارهٔ خطرات و پیامدهای منفی آن، با آن‌ها روبه‌رو هستند.

ـــ کلینیک‌های سایبری[3]: این کلینیک‌ها مسئول ارائهٔ خدمات فوری و اضطراری به کاربران هنگام مواجهه با تهدیدات یا حملات سایبری است. بازیابی داده‌ها، پایش داده‌ها و ... از جمله مهم‌ترین خدمات مربوط به این کلینیک‌هاست.

ـــ توسعهٔ حرفه‌ای امنیت سایبری[4]: پلتفرمی جدید است که وظیفه‌اش تربیت کارشناسان امنیت اطلاعات، ترویج تبادل دانش و آخرین دستاوردها با پیشگامان بخش صنعت و دانشگاه‌ها و نیز تلاش برای توسعهٔ همکاری‌های ملی و منطقه‌ای و بین‌المللی در حوزهٔ فضای سایبری است.

---

1. Cybersecurity Malaysia
2. Cyber SAFE
3. CyberSecurity Clinics
4. Cyber Security Professional Development (Cyber Guru)

جدول شمارهٔ ۳. نهادها و اقدامات حاکمیتی فضای سایبری در مالزی

	نمونهٔ نهاد ملی	نمونهٔ شرکت‌های ملی
حاکمیت امنیتی	**کمپانی «امنیت سایبری مالزی»** **Malasiya Cyber Security**	این کمپانی در دو سطح دولتی و خصوصی فعال است و فعالیت‌های آن زیر نظر وزارت علوم، فناوری و نوآوری می‌باشد. این کمپانی سه پلتفرم برای ارائهٔ خدمات دارد: **الف) فضای سایبری مصون:** این دپارتمان نقش پیشگیرانه دارد و مسئول آموزش و افزایش آگاهی عموم مردم در مورد مسائل فنی و موضوعات اجتماعی است که افراد در استفاده از اینترنت، به ویژه در مورد خطرات و پیامدهای منفی آن، با آن‌ها روبه‌رو هستند. **ب) کلینیک‌های سایبری:** این کلینیک‌ها مسئول ارائهٔ خدمات فوری و اضطراری به کاربران به هنگام مواجهه با تهدیدات یا حملات سایبری هستند. بازیابی داده‌ها، پایش داده‌ها و... از جمله مهم‌ترین خدمات مربوط به این کلینیک‌ها است. **ج) توسعهٔ حرفه‌ای امنیت سایبری:** این یک پلتفرم جدید است که وظیفه‌اش تربیت کارشناسان «امنیت اطلاعات»، ترویج تبادل دانش و آخرین دستاوردها با پیشگامان بخش صنعت و دانشگاه‌ها و همچنین تلاش برای توسعهٔ همکاری‌های ملی، منطقه‌ای و بین‌المللی در حوزهٔ فضای سایبری است.
حاکمیت حقوقی و قضایی	**۱. شعبهٔ تحقیقات مولتی‌مدیا و جرایم سایبری** **۲. دادگاه ویژهٔ سایبری**	۱) این شعبه زیر نظر دپارتمان تحقیقات مربوط به جرایم تجاری پلیس فدرال (پادشاهی) مالزی است. تحقیقات اولیه در ارتباط با جرایم سایبری در این شعبه انجام می‌شود. این شعبه همچنین وظیفهٔ رصد تمامی فعالیت‌های جاری و ساری در فضای سایبری از جمله فعالیت‌های مرتبط با گروه‌های تروریستی، فعالیت‌های خلاف امنیت پادشاهی مالزی، فعالیت‌ها و تبلیغات خلاف دین اسلام و... را بر عهده دارد. ۲) این دادگاه جزئی از دادگاه فدرال مالزی است که در سال ۲۰۱۶ راه‌اندازی شد و ویژهٔ رسیدگی قضایی به جرایم مربوط به حوزهٔ سایبری از جمله حملهٔ هکری، قماربازی آنلاین، پورنوگرافی آنلاین، جاسوسی و... می‌باشد.
حاکمیت فنی	**تیم پاسخ اضطراری کامپیوتری**	فعالیت این تیم در سطح ملی است و همراه از طریق Cyber999 در دسترس می‌باشد. این تیم برای حوادث کامپیوتری، به خصوص آلوده شدن آن‌ها به ویروس، از کار افتادن شبکه‌های کامپیوتری و... در شرایط فوریت و اضطرار است.

۲. شعبهٔ تحقیقات مولتی‌مدیا و جرایم سایبری:[1] این شعبه زیر نظر دپارتمان تحقیقات مربوط به جرایم تجاری پلیس فدرال (پادشاهی) مالزی است و وظیفهٔ تحقیقات اولیه در ارتباط با جرایم سایبری را به عهده دارد. همچنین موظف به رصد تمامی فعالیت‌های جاری و ساری در فضای سایبری از جمله فعالیت‌های مرتبط با گروه‌های تروریستی، فعالیت‌های خلاف امنیت پادشاهی مالزی، فعالیت‌ها و تبلیغات خلاف دین اسلام و ... است.

۳. دادگاه ویژه سایبری:[2] این دادگاه جزئی از دادگاه فدرال مالزی است که در سال ۲۰۱۶ راه‌اندازی شد و ویژهٔ رسیدگی قضایی به جرایم مربوط به حوزهٔ سایبری، از جمله حملهٔ هکری، قماربازی آنلاین، پورنوگرافی آنلاین، جاسوسی و ... است.

۴. گروه پاسخ اضطراری کامپیوتری:[3] فعالیت این گروه در سطح ملی و همواره از طریق Cyber 999 در دسترس است. این گروه برای حوادث کامپیوتری به خصوص آلوده شدن آن‌ها به ویروس، از کار افتادن شبکه‌های کامپیوتری و ... در شرایط فوری و اضطراری است.[4]

قانون‌گذاری در ارتباط با فضای سایبری در مالزی

مقررات‌گذاری و قانون‌گذاری مقولهٔ مهمی در ایجاد امنیت و اطمینان و اعتماد در ارتباط با هر گونه سیاست‌گذاری و برنامه‌ریزی و اجرا در ارتباط با حوزهٔ سایبری است. هدف اصلی قانون‌گذاری در حوزهٔ سایبری در کشور

1. Cybercrime and Multimedia Investigation Branch
2. Special Cyber Court
3. Malaysia Computer Emergency Response Team (MyCERT)
4. Cyber Security Malaysia, 2019

مالزی حمایت و تقویت و امنیت هشت حوزهٔ کلیـدی مـرتبط بـا زیرسـاخت اطلاعات ملی این کشور است.

بر اساس شواهد موجود، کشور مالزی متناسب با تغییر و تحـولات سـریعی که در حوزهٔ آی‌تی و فضای سایبری روی می‌دهد، قانون‌گذاری مناسب و بدنـهٔ قانون‌گذاری کافی برای مواجهه با هر گونه تغییر یا تهدید از این ناحیـه را داشـته است. برخی از مهم‌ترین قوانینی که مسـتقیم یـا غیرمسـتقیم مربـوط بـه حـوزهٔ سایبری است به شرح ذیل است:

جدول شمارهٔ ۴. قوانین مرتبط با فضای سایبری در کشور مالزی

قوانینی که مستقیم مربوط به حوزهٔ سایبر است		قوانینی که غیرمستقیم مربوط به حوزهٔ سایبر است	
۱	Communication & Multimedia Act 1998	۱	Copyright Act 1987
۲	Optical Disk Act 2000	۲	Sedition Act 1948
۳	Computer Crime Act 1997	۳	Panel Cod2015
۴	Digital Signature Act 1997	۴	Defamation Act 1957
۵	Telemedicine act 1997	۵	Evidence Act 114A
۶	Electronic Commerce act 2006		
۷	Electronic Government Activities Act 2007		
۸	Personal Data Protection Act 2010		
۹	Anti-Fake News Act 2018		

نگاهی به تصویب و لغو قانون «ضد ـ اخبار جعلی» (۲۰۱۸) در مالزی

متأخرترین و یکی از جنجالی‌ترین قوانین مربوط به فضای سایبری در کشور مالزی، قانون ضد ـ اخبار جعلی بود که در اوایل ۲۰۱۸ و پس از مباحثه‌های فراوان در پارلمان این کشور به تصویب رسید. بر اساس این قانون، «هر گونه خبر، اطلاعات، داده‌ها و گزارش‌هایی که به صورت کلی یا جزئی خلاف واقع است، خواه به شکل سرمقاله، ضبط‌صوت یا تصویر یا به هر صورت دیگری که قابلیت القای کلمات یا افکار را داشته باشد، خبر جعلی محسوب می‌شد».

نکتهٔ جالب در ارتباط با این قانون، دامنهٔ شمول آن است که فراتر از مرزهای شهروندی و جغرافیایی این کشور را نیز در بر می‌گیرد. بر اساس این قانون، مادامی که خبر جعلی مربوط به کشور مالزی باشد، تمامی افراد اعم از شهروندان مالزیایی یا اتباع غیرمالزیایی از هر کشور و همچنین در هر مکانی (اعم از داخل یا خارج از این کشور) مشمول این قانون می‌شدند و در صورت ارتکاب جرم، دولت مالزی موظف به پیگیری و برخورد با آن‌هاست.

بر اساس این قانون، در ازای تولید و هم‌رسانی هر گونه خبر جعلی یا فیک نیوز، مجازات سنگینی برای متخلفان، از پرداخت جریمهٔ ۵۰۰ هزار رینگیت[۱] (معادل ۱۳۰ هزار دلار) یا مجازات حبس شش سال و یا هر دو، در نظر گرفته می‌شد. همچنین پس از محکومیت فرد خاطی و ناشر خبر جعلی، در صورت استمرار جرم، فرد متخلف روزانه به پرداخت ۳۰۰۰ رینگیت نیز جریمه می‌شد.[۲]

از همان ابتدا، هم از سوی مخالفان داخلی دولت و هم از سوی نهادها و سازمان‌های بین‌المللی طرح این قانون و تصویب آن با مخالفت‌هایی جدی

---

۱. واحد پول مالزی.

2. Anti-Fake News Act, 2018

مواجه شد. به خصوص هم‌زمان بودن طرح این قانون با چهاردهمین انتخابات سراسری در مالزی موجب گشت مخالفان دولت و نیز سازمان‌های حقوق بشری از آن به عنوان ابزاری برای سرکوبی آزادی بیان، تشویق روزنامه‌نگاران به خودسانسوری و در نهایت ایجاد فضای خفقان در کشور مالزی یاد کنند. این قانون اگرچه در نهایت تصویب و اجرایی شد، اما به دلیل برگزاری انتخابات و تغییر دولت دوام چندانی نیافت. در واقع چهاردهمین دورهٔ انتخابات پارلمانی در کشور مالزی مجالی برای تداوم این قانون جنجالی نداد. نتایج این انتخابات، که به حاکمیت شصت‌سالهٔ حزب حاکم این کشور پایان داد، به روی کار آمدن ائتلافی از احزاب اپوزیسیون منجر شد که از ابتدا و بر اساس معیارهای حقوق بشری مخالف طرح و تصویب این قانون در پارلمان قبلی بودند. لذا پس از آغاز به کار پارلمان چهاردهم و نیز روی کار آمدن دولت جدید به رهبری ماهاتیر محمد، یکی از نخستین اقدام‌های این پارلمان لغو قانون ضد اخبار جعلی بود که با استقبال افکار عمومی و نیز نهادها و سازمان جهانی مواجه شد. این قانون در نهایت در آگوست ۲۰۱۸، تنها در حدود کمتر از شش ماه از زمان تصویب آن لغو شد. هرچند اخیراً و به دنبال مواجههٔ جدید این کشور با سیل اخبار جعلی در فضای شبکه‌های اجتماعی، فراخوان‌های تازه‌ای مبنی بر تصویب مجدد قانون ضد اخبار جعلی همراه با جرح و تعدیل شنیده می‌شود.

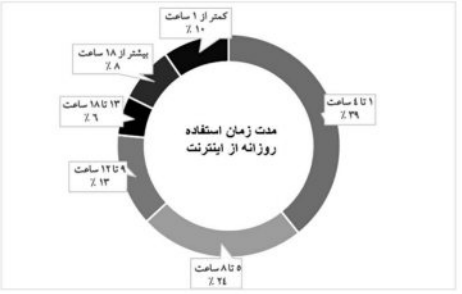
نظارت و فیلترینگ در فضای سایبری

مالزی یک کشور چندقومی و چندنژادی و چندمذهبی است. ضرورت ایجاد هارمونی و همزیستی مسالمت‌آمیز بین اقوام و نژادها و پیروان ادیان مختلف برای حفظ وجهه و پرستیژ این کشور به عنوان یک کشور اسلامیِ درحال‌توسعه و صلح‌طلب ایجاب می‌کند تا اینترنت و فضای سایبری نیز

همانند سایر فناوری‌های ارتباطی و اطلاعاتی از مکانیسم‌های خاص نظارتی و کنترل برخوردار باشند.

در حال حاضر، کمیسیون ارتباطات و مولتی‌مدیای مالزی[1] مسئول و متولی رصد و نظارت بر رسانه‌های این کشور، از جمله اینترنت و فضای سایبری، است و این کمیسیون از سازوکارهای قانونی و ابداعی مختلفی برای کنترل اینترنت و شبکه‌های اجتماعی استفاده می‌کند.

بر اساس گزارش کمیسیون ارتباطات و مولتی‌مدیای مالزی، ۸۷/۴ درصد مردم مالزی در سال ۲۰۱۸ به اینترنت و شبکه‌های اجتماعی دسترسی داشته‌اند که ۹۱ درصد آن از طریق تلفن همراه هوشمند بوده است.



سن	میانگین استفاده از اینترنت
زیر ۲۰ سال	۶.۷ ساعت
دههٔ ۲۰	۸.۰ ساعت
دههٔ ۳۰	۷.۳ ساعت
دههٔ ۴۰	۵.۹ ساعت
دههٔ ۵۰	۴.۵ ساعت
۶۰ سال و بالاتر	۳.۷ ساعت

نمودار شمارهٔ ۲. میزان ساعات استفاده از اینترنت به تفکیک گروه‌های سنی در مالزی

منبع: پیمایش ملی اینترنت در سال ۲۰۱۸

1. Malaysian Communications and Multimedia Commission

در کشور مالزی، فیس‌بوک و واتساپ محبوب‌ترین شبکه‌های اجتماعی در این کشور محسوب می‌شوند. ۹۶/۵ درصد کاربران اینترنت در مالزی صرفاً از شبکه‌های اجتماعی برای برقراری ارتباط با خانواده و دوستان و همکاران خود استفاده می‌کنند. ضمن آنکه محتوای آموزشی، محتوای سرگرم‌کننده و شایعات، اخبار، اطلاعات عمومی و اطلاعیه‌ها، تبلیغات تجاری و تخفیفات تجاری و موضوعات سیاسی به ترتیب بیشترین اطلاعاتی است که از طریق شبکه‌های اجتماعی در بین کاربران رد و بدل می‌شود.[1]

جدول شمارهٔ ۵. توزیع استفاده از شبکه‌های اجتماعی در مالزی

منبع: پیمایش ملی اینترنت در سال ۲۰۱۸

شبکه‌های اجتماعی	کاربران برنامه‌های ارتباطی: ۲۷.۸ میلیون
واتساپ	٪۹۸،۱
پیام‌رسان فیس‌بوک	٪۵۵،۶
ویچت	٪۳۶،۸
تلگرام	٪۲۵،۰
اسکایپ	٪۱۴،۲
لاین	٪۱۰،۲
کاکائو تاک (KakaoTalk)	٪۲،۱
سایر موارد	٪۱،۱

شبکه‌های اجتماعی	کاربران شبکه‌های اجتماعی: ۲۴.۶ میلیون
فیس‌بوک	٪۹۷،۳
اینستاگرام	٪۵۷،۰
یوتیوب	٪۴۸،۳
گوگل‌پلاس	٪۳۱،۳
توئیتر	٪۲۳،۸
لینکدین	٪۱۳،۳
سایر موارد	٪۰،۷

1. The Internet User, 2018

«فیلترینگ» و «حذف محتوا» دو مکانیسم اصلی کمیسیون ارتباطات و مولتی‌مدیای مالزی برای اطمینان از سلامت و صیانت از فضای سایبری در این کشور است. هرچند اعمال این دو مکانیسم بیشتر از طریق تعمیم قوانین فعلی و جاری مرتبط با رسانه‌ها (شامل قانون اسرار رسمی[1] قانون فتنه[2]، قانون مطبوعات چاپی و انتشار[3]، قانون پخش[4]، قانون امنیت ملی[5]، قانون سانسور فیلم[6]) به اینترنت و شبکه‌های اجتماعی در فضای سایبری صورت می‌گیرد.

فیلترینگ: بر اساس دستورالعمل کمیسیون ارتباطات و مولتی‌مدیای مالزی، سایت‌های اینترنتی غیراخلاقی، به خصوص سایت‌های پورنوگرافی، ممنوع و فیلتر هستند. با این وجود، قوانین گفته‌شده (به خصوص قانون فتنه، قانون اسرار رسمی، قانون امنیت ملی و ...) دستاویز خوبی در اختیار این کمیسیون قرار داد تا بر اساس آن، سایت‌های اینترنتی که این کمیسیون آن‌ها را نامناسب تشخیص دهد، نیز فیلتر شوند. این قوانین، همان طور که در ارتباط با سایر رسانه‌های چاپی و پخش مصداق می‌یابد، اجازه می‌دهد که افراد به عنوان مالکان شبکه‌های اجتماعی یا وب‌سایت‌ها و یا «عاملان پخش و انتشار» مطالبی که ناقض قوانین مذکورند، تحت تعقیب قانون قرار گیرند و مطابق جرایمشان و بر اساس مجازات تعیین‌شده محکوم شوند.

صعوداح وُک و شحفیذان محمد در ارزیابی خود از وضعیت اینترنت در این کشور خاطرنشان ساختند که این کمیسیون در سال ۲۰۱۴، بیش از شش‌هزار وب‌سایت را فیلتر کرده است، از جمله وب‌سایت‌های سیاسی، خبری، اجتماعی و فرهنگی. به اعتقاد این محققان، اعمال سخت‌گیرانهٔ

---

1. Official Secrets Act (OSA
2. Sedition Act
3. Printing Press Act (1984)
4. Broadcasting Act (1987)
5. Internal Security Act (ISA)
6. Film Censorship Act (2002)

قوانین فعلی و تعمیم بیش از حد آن به اینترنت و شبکه‌های اجتماعی بیش از هر چیزی موجب ایجاد خودسانسوری در مالزی شده است.[1]

حذف محتوا: دومین مکانیسم پرکاربرد در ارتباط با فضای سایبری و شبکه‌های اجتماعی صدور فرمان حذف محتوا از سوی کمیسیون ارتباطات و مولتی‌مدیاست. به طور خاص، بر اساس قانون اساسی مالزی، هر گونه انتشار مطالب یا اخبار علیه «دین اسلام» (اهل سنت و جماعت) و «نظام پادشاهی» کشور مالزی جرم محسوب می‌شود. از این رو مطالبی با مضمون ضدیت با دین اسلام یا ضد نظام حاکم بر این کشور، در صدر نظام مانیتورینگ کمیسیون ارتباطات و مولتی‌مدیا قرار داشته و در صورت مشاهدهٔ هر یک از آن‌ها، فرمان حذف محتوای مربوط صادر می‌شود. در سال‌های پس از ۲۰۱۳، که دولت این کشور تلاطمات سیاسی فراوانی را از سر می‌گذراند، بارها از این قوانین به صورت غیرشفاهی علیه مخالفان دولت استفاده شد. همچنین در سال‌های اخیر (به خصوص سال‌های ۲۰۱۵ و ۲۰۱۶)، موارد زیادی از درخواست این کمیسیون از فیس‌بوک، یوتیوب و حتی صاحبان وبلاگ‌های شخصی مبنی بر حذف برخی محتواها مشاهده شده است.[2]

همکاری بین‌المللی مالزی در حوزهٔ سایبری

مالزی به عنوان یک عضو فعال جامعهٔ بین‌الملل همواره می‌کوشد نقش مؤثری در زمینه‌های مختلف در عرصهٔ منطقه‌ای و بین‌المللی ایفا کند. اصولاً مالزی همواره در ارتباط با همکاری‌های منطقه‌ای و بین‌المللی رویکردی باز و ایجابی داشته است.

---

1. Saodah Wok and Shafizan Mohamed, 2017
2. Ahmad, 2009

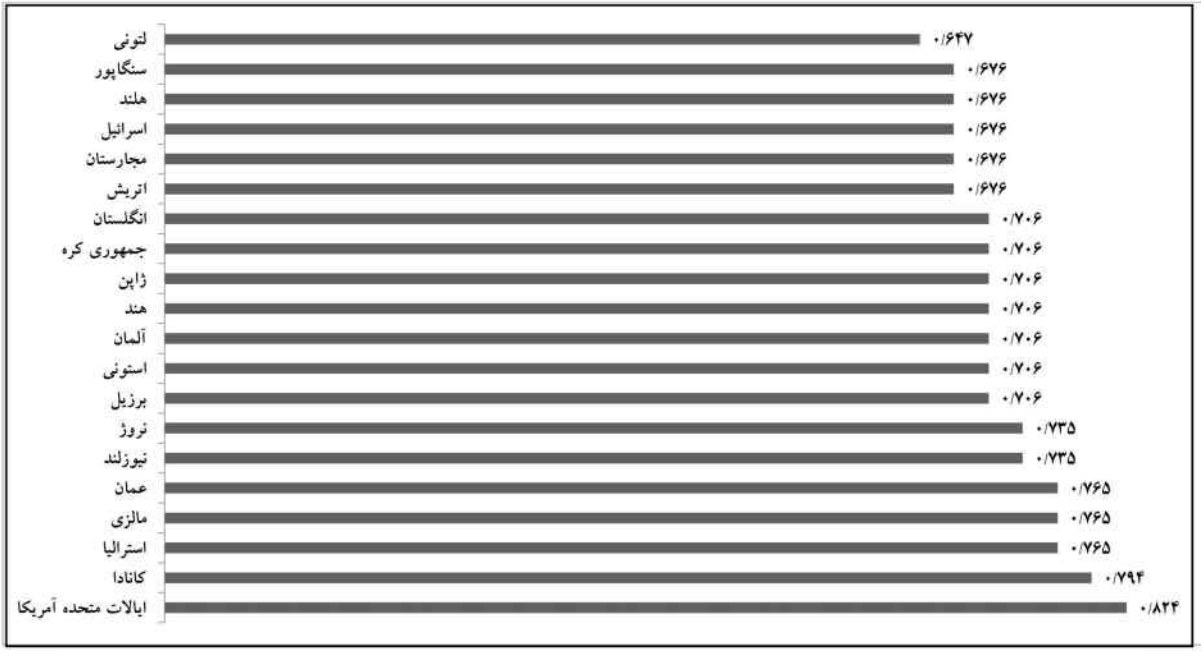
عرصهٔ سایبری نیز از این امر مستثنا نیست. از ابتدای ظهور شبکه‌های اجتماعی و شکل‌گیری فضای سایبری، دولت مالزی همواره مشارکتی جدی در زمینهٔ همکاری‌های بین‌المللی، به خصوص در چارچوب اتحادیهٔ منطقه‌ای کشورهای جنوب شرق آسیا (آسه‌آن)، کشورهای عضو سازمان کنفرانس اسلامی[1] و کشورهای مشترک‌المنافع[2] داشته است. همچنین در سال‌های اخیر، مالزی در ارتباط با فضای سایبری، رویکرد همکاری دوجانبه و سه‌جانبه و چندجانبه به خصوص با شرکای استراتژیک خود اتخاذ کرده است که از جمله می‌توان به همکاری دوجانبه با کرهٔ جنوبی[3]، همکاری سه‌جانبه با فیلیپین و اندونزی[4]، همکاری دوجانبه با استرالیا[5]، همکاری دوجانبه با هندوستان[6] و نیز همکاری با اتحادیهٔ اروپایی[7] اشاره کرد.

جایگاه جهانی مالزی به لحاظ حکمرانی سایبری

رویکرد باز و استقبال این کشور از همکاری‌های منطقه‌ای و بین‌المللی در حوزهٔ فناوری‌های نوین ارتباطات و اطلاعات موجب تثبیت موقعیت این کشور در عرصهٔ بین‌الملل در عمدهٔ حوزه‌ها، از جمله در زمینهٔ فضای سایبری، شده است. بر اساس ارزیابی‌های اتحادیهٔ بین‌المللی ارتباطات راه دور در زمینهٔ «آمادگی در حوزهٔ حملات سایبری»، مالزی در سال‌های اخیر همواره در بین بیست کشور اول جهان قرار داشته است.

---

1. Organization of Islamic Cooperation (OIC)
2. Commonwealth
3. Memorandum of Agreement, Malaysia-Republic of Korea
4. Trilateral Meeting on Security, Indonesia-Malaysia-Philippines
5. Memorandum of Understanding, Australia-Malaysia
6. Memorandum of Understanding, India-Malaysia
7. EU-Malaysia Partnership and Cooperation Agreement (PCA)



نمودار شمارهٔ ۳. مالزی در پنج سال گذشته همواره در بین بیست کشور اول جهان به لحاظ آمادگی در برابر حملات سایبری بوده است.
(ABI Research and ITU, Global Cyber Security Index)

جدول شمارهٔ ۶. رتبه‌بندی کشورها بر اساس شاخص امنیت سایبری

Global Cyber Security 2017- International Telecommunication Union (ITU)

کشورها	نمرهٔ GCI	مجاز	فنی	سازمانی	ظرفیت‌سازی	مشارکت
سنگاپور	۰,۹۲	۰,۹۵	۰,۹۶	۰,۸۸	۰,۹۷	۰,۸۷
ایالات متحده امریکا	۰,۹۱	۱	۰,۹۶	۰,۹۲	۱	۰,۷۳
مالزی	۰,۸۹	۰,۸۷	۰,۹۶	۰,۷۷	۱	۰,۸۷
عمان	۰,۸۷	۰,۹۸	۰,۸۲	۰,۸۵	۰,۹۵	۰,۷۵
استونی	۰,۸۴	۰,۹۹	۰,۸۲	۰,۸۵	۰,۹۴	۰,۶۴
موریس	۰,۸۲	۰,۸۵	۰,۹۶	۰,۷۴	۰,۹۱	۰,۷۰
استرالیا	۰,۸۲	۰,۹۴	۰,۹۶	۰,۸۶	۰,۹۴	۰,۴۴
گرجستان	۰,۸۱	۰,۹۱	۰,۷۷	۰,۸۲	۰,۹۰	۰,۷۰
فرانسه	۰,۸۱	۰,۹۴	۰,۹۶	۰,۶۰	۱	۰,۶۱
کانادا	۰,۸۱	۰,۹۴	۰,۹۳	۰,۷۱	۰,۸۲	۰,۷۰

همچنین در ارزیابی سال ۲۰۱۷ این سازمان جهانی از وضعیت کشورها بر اساس پنج شاخص قانونی، فنی، سازمانی، ظرفیت‌سازی و همکاری، مالزی با کسب نمرهٔ میانگین ۰/۸۹، رتبهٔ دوم در آسیا و رتبهٔ سوم جهانی را پس از سنگاپور و آمریکا داراست.[1]

جمع‌بندی و نتیجه‌گیری این فصل

با توجه به تأکید تمامی اسناد سایبری مالزی بر مفهوم «امنیت اطلاعات»، در ارزیابی نوع مواجههٔ این کشور با فضای سایبری می‌توان به وضوح، غلبهٔ رویکرد دفاعی و امنیتی را ملاحظه کرد. البته این لزوماً منفی نیست. این کشور به رغم رسیدن به آستانهٔ سال ۲۰۲۰، همچنان دوران گذار

1. Global Cyber Security Index (GCI), 2017

تکنولوژیک را تجربه می‌کند. وابستگی شدید حوزه‌های کلیدی زیرساخت اطلاعاتی ملی به فناوری‌های نوین اطلاعاتی و ارتباطی ایجاب می‌کند که رویکرد دفاعی و امنیتی با هدف اطمینان از کارایی و عملکرد این حوزه‌ها در مرکز ثقل هر گونه برنامه‌ریزی و سیاست‌گذاری قرار گیرد.

در عین حال وجه مثبت حکمرانی سایبری در مالزی رویکرد ایجابی این کشور به استفاده از ظرفیت‌ها و فرصت‌های آن برای توسعهٔ همه‌جانبه است. این کشور حاکمیت فناوری در عصر سایبری را به رسمیت می‌شناسد و به همین دلیل در عمدهٔ سیاست‌گذاری‌ها، بر دستیابی به آخرین فناوری‌ها و نیز استفادهٔ حداکثری از ظرفیت‌های فناوری و نوآوری تأکید کرده است. هرچند همین رویکرد ایجابی، آسیب‌ها و پیامدهایی جدی نیز برای این کشور داشته است، از جمله زیان ۱۲/۲ میلیارد دلاری اقتصادی ناشی از حملات سایبری به کشور مالزی.

البته نباید از نظر دور داشت که رویکرد بی‌طرفانه و موضع نسبتاً خنثای این کشور در موضوعات و مسائل مهم بین‌المللی نیز تا حد زیادی به در «حاشیهٔ امن» قرار گرفتن این کشور در چالش‌ها و تهدیدات جدی بین‌المللی، که جنگ سایبری و جاسوسی سایبری نیز از جملهٔ آن‌ها محسوب می‌شود، کمک کرده است.

شاید بتوان گفت مهم‌ترین نقطهٔ اتکای حکمرانی سایبری این کشور در عرصهٔ داخلی، رویکرد دفاعی ـ امنیتی و در عرصهٔ بین‌الملل نیز رویکرد همگرایانه با کشورهای خارجی، به خصوص کشورهای پیشرفته همچون اتحادیهٔ اروپا، آمریکا، استرالیا، کرهٔ جنوبی و ...، است. با این حال، مالزی به دلیل دشواری در برقراری توازن استراتژیک بین ملاحظات حکمرانی داخلی، به خصوص با توجه به تنوع قومی، مذهبی و نژادی این کشور و نیز الزامات همراهی با جریانات غالب حکمرانی بین‌المللی در عرصهٔ سایبری، هنوز فاصلهٔ زیادی تا مرحلهٔ دستیابی به اِشرافیت راهبردی در این حوزه برای پیشبرد اهداف توسعه‌ای خود دارد.

منابع

Ahmad JH., Perhubungan Awam Dan Teknologi Baru, Jurnal Pengajian Media Malaysia (Malaysian Journal of Media Studies), 2009, 11 (1): 9-20.

Anti-Fake News Act 2018, Laws of Malaysia.

Cyber Policy Portal, Retrieved July 2019, from: https:// cyberpolicyportal.org.

Cyber Security Malaysia Portal, Retrieved July 2019 from: https://www.cybersecurity.my/en/.

Global Cyber Security Index (GCI) (2017), International Telecommunication Union (ITU).

Internet Survey 2018, Malaysian Communications and Multimedia Commission.

ISACA and the IT Governance Institute, ISACA Overview, Retrieved July 12, 2019, From: http://www.isaca.org.

Ministry of Science, Technology and Innovation, "National R&D Roadmap for Self Reliance in Cyber Security Technologies", Unpublished.

Mohd Shamir b Hashim (2011), Malaysia's National Cyber Security Policy: The Country's Cyber Defense Initiatives, Ministry of Science, Technology and Innovation, Malaysia.

National Cyber Security Policy: The Way Forward", Ministry of Science, Technology and Innovation, Malaysia, Federal Government Administrative Centre, July 2006.

Wok. S, & Shafizan, Mohamed (2017), Internet and Social Media in Malaysia: Development, Challenges and Potentials, see to: http://dx.doi.org.

فصل نهم

گافام و دیپلماسی شرکتی

درآمد

گافام[1] در ادبیات سیاسی و روابط بین‌الملل، یک واحد سیاسی با مختصات حاکمیتی کلاسیک و قلمرو معیّن با مرزهای سرزمینی و جغرافیایی مشخص نیست، اما به دلیل بازیگری و نقش روزافزونی که در سطوح مختلف سیاسی، اقتصادی و اجتماعی جوامع ایفا می‌کنند، به نوعی «نظام‌های حکمرانی» نوظهور با قدرت بازیگری و تأثیر گسترده (اگر نگوییم نامحدود) تبدیل شده‌اند؛ این در حالی است که هیچ چشم‌انداز روشنی از آیندهٔ آن‌ها وجود ندارد و حدّ پایانی نیز برای ثروت و قدرت بلامنازع آن‌ها نیست.

گافام (گوگل، اپل، فیس‌بوک، آمازون و مایکروسافت) پنج پلتفرم بزرگ در مقیاس جهانی هستند که در سال‌های اخیر به پادشاهان آنلاین (سیاسی)، غول‌های آی‌تی (فناوری) یا امپراتوری‌های تجاری (اقتصادی)

---

1. GAFAM: Google, Apple, Facebook, Amazon, Microsoft.

مشهور شده‌اند.[۱] ترکیب سه مؤلفهٔ قدرت‌افزای سیاسی، فناوری و اقتصادی ظرفیت و پتانسیلی به این پلتفرم‌ها داده است که نمی‌توان نقش آن‌ها را در هیچ سپهر سیاسی و اقتصادی نظام‌های حکمرانی کشورها مورد توجه قرار نداد.[۲]

نکتهٔ حائز اهمیت در ارتباط با گافام این است که عمر عمدهٔ آن‌ها به کمتر از دو دهه می‌رسد. بر اساس تحقیق پیتر ایوانس و آنابل گاور، تا پایان سال ۲۰۱۶، در کل جهان حدود دویست پلتفرم قابل شناسایی بوده که ارزش بازار تخمینی آن‌ها به ۱.۳ تریلیون دلار می‌رسیده است. در رأس این پلتفرم‌ها، گافام قرار داشته که ارزش بازار تخمینی آن‌ها در همان زمان به بیش از ۲.۲ تریلیون دلار می‌رسیده است. حائز اهمیت آنکه ارزش بازار ده پلتفرم برتر (از جمله گافام) در سال ۲۰۰۶ تنها ۲۸۰ میلیارد دلار بوده است.[۳] فراتر از این، در عرصهٔ کسب‌وکار و فروش نیز این پلتفرم‌ها اصلی‌ترین «برندها» در بازار جهانی محسوب می‌شوند. بر اساس برآورد میلوارد براون، در بین صد برند مشهور جهانی نیز گافام با فاصله بسیار زیادی در بین ده برند برتر (گوگل رتبهٔ اول، اپل رتبهٔ دوم، مایکروسافت رتبهٔ سوم، فیس‌بوک رتبهٔ پنجم و آمازون رتبهٔ هفتم) قرار دارند.[۴]

---

۱. باید توجه داشت که در داخل آمریکا و در سایر کشورها، به ویژه چین، اتحادیهٔ اروپا و روسیه، پلتفرم‌های دیگری نیز وجود دارند که به سرعت در حال رشد هستند و دامنهٔ اثرگذاری فعالیت‌های آن‌ها نیز مدام در حال افزایش است.

2. Laure Claire Reillier & Benoit Reillier, 2017

3. Peter C. Evans and Annabelle Gawer, 2016

4. Millward Brown, 2016

جدول شمارهٔ ۱. مختصات و برخی مشخصات بزرگ‌ترین پلتفرم‌های موسوم به گافام

پلتفرم	کشور	ارزش (۲۰۲۰)	حوزه	شرکت‌های تابعه	منبع درآمد	امپراتوری
گوگل	امریکا: دومین برند جهان	۱۰۰۰ میلیارد دلار	موتور جست‌وجو، رایانش ابری و تبلیغات	آلفابت، یوتیوب، سیستم عامل اندروید، جی‌میل و شبکه‌های اجتماعی، گوگل، ویرایشگر تصاویر پیکاسا و پیام‌رسان فوری گوگل‌تاک، اورکات	۹۵ درصد درآمد از محل تبلیغات	سازمان‌دهی اطلاعات دنیا و دسترس‌پذیر کردن آنها برای عموم
اپل	امریکا: باارزش‌ترین برند جهان	۱۳۸۰ میلیارد دلار	لوازم الکترونیکی مصرفی، نرم‌افزار کامپیوتر و ارائه‌دهنده خدمات آنلاین	سخت‌افزار (آی پد، آی‌مک، مک‌بوک، آی‌پاد، آیفون، اپل‌واچ و اپل تی‌وی)، نرم‌افزار (آی‌تیونز، آی‌لایف، آی‌ورک، سیستم عامل موبایل آی‌اواس)	آیفون، آی‌پد و رایانه‌ای مک	فناوری
فیس‌بوک	امریکا: بزرگ‌ترین شبکهٔ اجتماعی	۶۳۲ میلیارد دلار	شبکهٔ اجتماعی	واتس‌آپ و اینستاگرام	تبلیغات	داده‌های شخصی
آمازون	امریکا	حدود ۱۰۰۰ میلیارد دلار	توزیع کالاها و محصولات	———	خرده‌فروشی کالا در اینترنت	خرید و فروش آنلاین
مایکروسافت	امریکا	۱۲۷۰ میلیارد دلار	چندرسانه‌ای، سیستم عامل مایکروسافت ویندوز، مایکروسافت آفیس، سیستم عامل داس	شبکهٔ تلویزیونی ام‌اس‌ان‌بی‌سی، سایت اینترنتی «ام‌اس‌ان»، خرید شرکت فنلاندی تولید تلفن همراه نوکیا	رایانه و سرویس ابری، انواع نرم‌افزار مانند مایکروسافت آفیس	فناوری

حکمرانی شبکه‌ای گافام

گافام در قالب حکمرانی شبکه‌ای در حوزه‌های مختلف، قلمروهایی با گسترهٔ جهانی همراه با اثرگذاری انحصاری برای خود ترسیم کرده است که دایرهٔ

بازیگری و نیز کرانه‌های آن نه‌تنها به مرزهای ملی و نیز سرزمین‌های جغرافیایی با مختصات سیاسی (ساختارهای حکمرانی فعلی) در ادبیات روابط بین‌الملل کلاسیک محصور نیست، بلکه اساساً در ذهنیت پلتفرمی آن‌ها نقش و جایگاهی برای دولت‌ها به مفهوم کلاسیک آن‌ها قابل تصور نیست. در واقع از منظر حکمرانی شبکه‌ای گافام، دولت‌ها اساساً در هر پنج حوزهٔ اساسی حکمرانی سیاسی، اقتصادی، اجتماعی، فناوری، زیست‌محیطی و حقوقی[1] مزاحم تلقی می‌شود.

جان پری بارلو در مقالهٔ معروفی که به «اعلامیهٔ استقلال فضای سایبری» شهرت یافت، اعلام داشت: «دولت‌های جهان صنعت! ای غول‌های فرسودهٔ گوشتالود و فولادین، من از فضای سایبری می‌آیم، خانهٔ جدید ذهن ... . ما، به نمایندگی از دنیای آینده، از شما استقبال نمی‌کنیم. شما در اینجا حاکمیتی ندارید».[2] بسیاری از اندیشمندان بیانیهٔ اعلان استقلال فضای سایبری بارلو را اعلان جنگ آشکار علیه دولت‌ها و ساختارهای حکمرانی کلاسیک دانسته که از بسیاری جهات چشم‌اندازی آشوبگرانه از آیندهٔ این نظام‌ها و ساختارهای رسمی ملی، منطقه‌ای و بین‌المللی و نیز تمامی اِلمان‌ها و مؤلفه‌های کلاسیک آن همچون قلمرو، سرزمین، مرز، اعمال حاکمیت، قوانین ملی و ... ارائه می‌دهد.

پیام اعلان جنگی که در اعلامیهٔ استقلال فضای سایبری علیه دولت‌ها[3] نهفته بود، با ظهور شرکت‌های بزرگ فناوری[4] موسوم به گافام (جدول شمارهٔ ۱) در یک دههٔ اخیر بیش از پیش از سوی دولت‌ها و مقام‌های رسمی

---

1. Political, Economy, Social, Technology, Environment & Legal
2. John Perry Barlow, 1996
3. States
4. Big Tech

دریافت شده است؛ جایی که آنگلا مرکل از آن به عنوان قلمرو نامکشوف[1] یاد می‌کند. امانوئل مکرون با اشاره به سیطرهٔ هوش مصنوعی بر زندگی سیاسی، اجتماعی و فرهنگی اروپا در قرن ۲۱ هشدار می‌دهد که دولت‌ها و حتی ساختارها و نظام‌های قدرتمندی همچون ناتو تا آستانهٔ بحران و فروپاشی کامل پیش رفته‌اند؛ یا دولت فعلی آمریکا را تا آستانهٔ بازنگری در قانون اساسی این کشور (بند ۲۳۰ «قانون رفتار سالم در ارتباطات» مصوب ۱۹۹۶ موسوم به سی‌دی‌ای[2]) پیش برده است.

دیپلماسی شرکتی گافام؛ گذار از دیپلماسی رسمی

اساساً اصول و قواعد بازیگری در پلتفرم‌ها نه بر اساس دیپلماسی رایج به معنای سنتی و رسمی آن، بلکه بر اساس آنچه عموماً دیپلماسی شرکتی[3] نامیده می‌شود، صورت می‌گیرد. البته منافع تجاری و اقتصادی گافام به شدت با منافع سیاسی دولت سرمایه‌داری مستقر در آمریکا در هم پیچیده است. به این اعتبار، هنوز نمی‌توان با اطمینان بالایی از گذار قطعی گافام از دیپلماسی رسمی دولت سرمایه‌داری به دیپلماسی شرکتی صحبت کرد. با این حال، تضاد روزافزون سیاست‌ها و برنامه‌های دولت سرمایه‌داری با سیاست‌ها و منافع گافام، اصطکاک روزافزون گافام با نهادهای رسمی و دولتی که به خصوص پس از انتخابات ۲۰۱۶ آمریکا به عرصهٔ عمومی نیز کشیده شده، شائبهٔ زیادی در زمینهٔ گذار گافام (به خصوص فیس‌بوک) از دیپلماسی رسمی دولت سرمایه‌داری و در پیش گرفتن دیپلماسی شرکتی از سوی این پلتفرم‌ها ایجاد شده است.

---

1. Neuland (Uncharted Territory)
2. Communications Decency Act
3. Corporate Diplomacy

مبنای دیپلماسی شرکتی، تلقی خاصی از نظام کاپیتالیستی است که ضمن حفظ مبانی ایدئولوژیکی ـ سیاسی آن، منافع اقتصادی‌ـتجاری این پلتفرم‌ها جایگزین منافع عمومی دولت سرمایه‌داری می‌شود. به طور مشخص برخلاف دیپلماسی دولت سرمایه‌داری که در آن بازار آزاد اصل اول و به طریق اولی، «رقابت» محور هر گونه فعالیت اقتصادی محسوب می‌شود، در دیپلماسی شرکتی «انحصار» جایگزین رقابت می‌گردد و اصولاً حق انتخاب مشتری در بازار آزاد به رسمیت شناخته نمی‌شود.[1] فراتر از نگرانی‌های مربوط به این نوع اولویت‌بندی و ارجحیت منافع پلتفرم‌ها، نفس اعمال حکمرانی شبکه‌ای است که نه از طریق فرایندهای شفاف و بی‌طرف، بلکه به صورت نامرئی، نامحسوس و بر اساس خودتنظیم‌گری[2] است که فقط یک غایت را دنبال می‌کند: حفظ منافع تجاری‌ـاقتصادی پلتفرم‌ها.

دیپلماسی شرکتی به طور مشخص از دو مسیر موازی اهداف و منافع تجاری و اقتصادی پلتفرم‌ها را پیش می‌برد: ۱. استفاده از ظرفیت شبکه‌های رسانه‌ای و اجتماعی برای جهت‌دهی، دست‌کاری و مدیریت افکار عمومی و ۲. استفاده از شبکه‌های اقتصادی ـ تجاری برای هدایت جریان سرمایه و نخبگانی جامعه را بر عهده می‌گیرند. غایت نهایی یا به عبارتی تقاطع هر دو مسیر حفظ و توسعهٔ منابع اقتصادی پلتفرم‌هاست که به طور ماهرانه‌ای از طریق ادغام‌های عمودی، افقی و مورب شرکت‌های مربوطه تأمین می‌شود.

دیپلماسی شرکتیِ پلتفرم‌ها که در قالب مکانیسم‌هایی همچون انحصارطلبی و انحصارگری ـ اعم از انحصارگری تک‌قطبی، دوقطبی و چندقطبی دنبال می‌شود ـــ تا حد بسیار زیادی ظرفیت حاکمیت‌های ملی در اعمال اقتدار سنتی

1. Denise Hearn & Jonathan Tepper, 2018
2. Self-Regulation

در حوزه‌های مختلف را تقلیل داده و این امر تا حدودی حتی شامل آمریکا به عنوان مهد نظام سرمایه‌داری و بستر اصلی ظهور این پلتفرم‌ها نیز می‌شود. به طور مشخص، رویارویی و خروش پلتفرم‌ها در واشنگتن‌دی‌سی طی دو دهۀ گذشته علیه ساختار سیاسی آمریکا (کنگره و دولت این کشور) و انتحار سیاسی که امروزه از سوی دولتمردان هر دو جناح جمهوری‌خواه و دموکرات این کشور علیه قدرت روزافزون این پلتفرم‌ها شاهد هستیم، مصداقی از تبلور و ظهور گستردۀ دیپلماسی شرکتی در سپهر سیاسی قرن بیست‌ویک است.

نمایی از تاریخچۀ تقابل دولت آمریکا با پلتفرم‌ها

سابقۀ تقابل و رویارویی دولت‌ها با شرکت‌های بزرگ در نظام سرمایه‌داری آمریکا به بیش از یکصد سال می‌رسد. برای مثال، در قالب آنچه مقابله با انحصارطلبی کارتل‌ها و تراست‌ها نامیده می‌شود، در سال ۱۹۱۱ دادگاه عالی آمریکا بر مبنای قانون ضد انحصار شرمن، شرکت استاندارد اویل را به چهار شرکت و شرکت امریکن توباکو را به ۳۳ شرکت تجزیه کرد.[1] با این حال و به دلایل مختلف، ازجمله رفتارها و عملکرد متناقض برخی از دولت‌های مستقر در آمریکا، این قوانین هیچ گاه نتوانسته آن طور که باید، مانع از شکل‌گیری شرکت‌ها و کمپانی‌های بزرگ شود.

در ارتباط با عرصۀ سایبری و به خصوص فعالیت پلتفرم‌ها، موضوع مقابلۀ دولت با آن‌ها به کلی متفاوت و متمایز از گذشته است. به خصوص از زمان انتخابات ریاست‌جمهوری سال ۲۰۱۶ و آشکار شدن موضوع «مداخلۀ احتمالی روسیه از طریق شبکه‌های اجتماعی به نفع دونالد ترامپ» و نیز «اتهام فیس‌بوک مبنی بر فروش اطلاعات رأی اولی‌ها به حزب جمهوری‌خواه»، برگ دیگری از تاریخ تقابل دولت سرمایه‌داری با شرکت‌های بزرگ (و در اینجا پلتفرم‌ها) رقم خورده است. در واقع، سیر مقابلۀ دولت آمریکا با پلتفرم‌ها که از سال ۲۰۱۶ آغاز و در حال حاضر با فرمان اجرایی دونالد ترامپ در ماه می ۲۰۲۰ در خصوص محدود کرد این پلتفرم‌ها به اوج خود

1. Denise Hearn and Jonathan Tepper, 2018

رسیده را می‌توان نقطه‌عطفی در این رویارویی تاریخی دانست.

فرمان اجرایی ترامپ[1] به طور مشخص خواستار تغییر/ اصلاح بند ۲۳۰ قانون «رفتار سالم در ارتباطات» مصوب سال ۱۹۹۶ است. بر اساس این بند، پلتفرم‌هایی همچون شبکه‌های اجتماعی عمدتاً «مسئول محتواهایی که کاربران پُست می‌کنند نیستند، اما می‌توانند با نیت خیر دست به انسداد برخی از پست‌ها بزنند؛ مثلاً صحنه‌های مستهجن، یا صفحات منعکس‌کنندهٔ آزار یا خشونت را حذف کنند». بر اساس ادعای فرمان اجرایی دونالد ترامپ، شبکه‌های اجتماعی به شدت از این بند برای سانسور آنلاین، محدودیت در آزادی بیان و جریان آزاد اطلاعات و ... سوءاستفاده می‌کنند و لذا کنگرهٔ آمریکا باید با تغییر/ اصلاح این بند، مانع محدود شدن دموکراسی در این کشور شود.

قبل‌تر از این فرمان اجرایی و از زمان انتخابات ۲۰۱۶ آمریکا، پلتفرم‌ها و به طور خاص گوگل، اپل، فیس‌بوک و آمازون با تحقیقات گستردهٔ دولت فدرال و دولت‌های ایالتی روبه‌رو بوده‌اند. به طور خاص فیس‌بوک هم اکنون از سوی ۴۵ دادستان و گوگل از سوی ۴۸ دادستان در آمریکا هدف تحقیقات گسترده قرار دارد. مدیران این پلتفرم‌ها بارها به جلسات استماع در کنگرهٔ این کشور فراخوانده شده تا به سؤالات و دغدغه‌ها و نگرانی‌های نمایندگان کنگره در ارتباط با عملکرد انحصارطلبانه خود پاسخ دهند. آخرین اقدام کنگرهٔ آمریکا علیه این پلتفرم‌ها، برگزاری جلسه استماع در کمیتهٔ ضدانحصار با حضور هم‌زمان مارک زاکربرگ مدیرعامل فیس‌بوک، جف بیزوس مدیرعامل آمازون، ساندار پیچای مدیرعامل گوگل، و تیم کوک مدیرعامل اپل در تاریخ ۲۹ ژوئیهٔ ۲۰۲۰ بود که رسانه‌های آمریکایی از آن به عنوان «به سیخ کشیدن کمپانی‌های بزرگ آی‌تی» یاد کردند. در این جلسه که به صورت آنلاین برگزار شده، نمایندگان کنگرهٔ آمریکا از هر دو حزب دموکرات و جمهوری‌خواه در مجموع بیش از دویست سؤال از رؤسای این پلتفرم‌ها در ارتباط با عملکرد این کمپانی‌ها از جمله در زمینهٔ استفاده از سیاست مشت آهنین برای ایجاد انحصار و حذف رقبا، سانسور محتوا، جانبداری سیاسی، شخصی‌سازی تبلیغات، استفاده از اطلاعات شخصی کاربران و .... پرسیدند[2].

---

1. Trump's Executive Order
2. Fortune, 2020

در حال حاضر، یک ائتلاف فراجناحی جدی متشکل از رهبران کنگره (هم در سنا و هم در مجلس نمایندگان) دنبال محدودسازی پلتفرم‌ها به هر نحو ممکن هستند. الیزابت وارن[1] (دموکرات)، امی کلوبشار[2] (دموکرات)، جاش هاولی[3] (جمهوری‌خواه)، لیندسی گراهام[4] (جمهوری‌خواه)، تد کروز[5] (جمهوری‌خواه)، ویلیام بار[6] (جمهوری‌خواه و دادستان سابق آمریکا)، مایکل هایدن[7] (رئیس سابق آژانس امنیت ملی و رئیس سازمان اطلاعات مرکزی آمریکا)، کریستوفر ری[8] (رئیس اف‌بی‌آی)، جو نگوس (دموکرات)، دیوید سیسی لاین (رئیس کمیته ضدانحصار کنگره) و ... از جمله مشهورترین رهبران کنگرهٔ آمریکا هستند که در قالب یک ائتلاف فراجناحی به دنبال محدودسازی قدرت و میزان اثرگذاری پلتفرم‌ها در جامعهٔ آمریکا می‌باشند.

مطالعهٔ دقیق کرونولوژیِ این رویارویی و به خصوص مجموعهٔ وقایعی که اخیراً به فرمان اجرایی ۲۸ ماه مه ۲۰۲۰ دونالد ترامپ در خصوص « محدود کردن حفاظت‌های وسیع حقوقی پلتفرم‌ها» منجر شد نشان می‌دهد که برخلاف رویهٔ تاریخی، دولت و کنگرهٔ این کشور در واقع در حال استفاده از آخرین اهرم‌ها و مکانیسم‌های ممکن برای کنترل و محدودسازی پلتفرم‌ها است و ای بسا که هم به دلایل فناورانه و هم به دلایل حقوقی و حتی دلایل سیاسی هیچ چشم‌انداز روشنی نیز برای آن وجود ندارد.

دستور اجرایی رئیس‌جمهوری آمریکا هم در شرایطی صادر شد که از ماه‌ها قبل از آن، پلتفرم‌ها در ائتلافی آشکار از آغاز گستردهٔ استفاده از هوش مصنوعی برای «فیلترینگ پیشگیرانه» با هدف مقابله با ترویج خشونت، مقابله با افکار حامی تروریسم، رواج اخبار جعلی و... خبر داده بودند. درست سه روز قبل از صدور این فرمان اجرایی، دونالد ترامپ خود هدف این سیاست جدید پلتفرمی قرار گرفت و توییتر بر یکی از پُست‌های رئیس‌جمهوری آمریکا برچسب «صحت‌سنجی» زد و حتی پس از صدور این فرمان، چندین بار پُست‌های دونالد ترامپ در توییتر را پنهان یا حذف کرد.

---

1. Elizabeth Warren
2. Amy Klobchar
3. Josh Hawley
4. Lindsey Graham
5. Ted Cruz
6. William Barr
7. Michael Hayden
8. Christopher Wray

فرمان اجرایی ترامپ برای محدود کردن قدرت پلتفرم‌ها، که در واقع اوج قدرت‌نمایی و استفاده از اختیارات یک رئیس‌جمهوری در آمریکا برای پیشبرد امورات مورد دلخواه تلقی می‌شود، تقریباً با هیچ استقبالی مواجه نشد. حقوق‌دانان آمریکایی شانس موفقیت این دستور اجرایی را بسیار ضعیف دانسته و منوط به ورود گستردهٔ کنگره و تغییر در قانون اساسی این کشور دانسته‌اند؛ امری که به ندرت صورت می‌گیرد. مدیران پلتفرم‌ها نیز به پشتوانهٔ قدرت عظیم فناورانهٔ خود آن را نوعی «واپسگرایی سیاسی» بی‌سابقه در تاریخ آمریکا دانستند که فناوری اجازهٔ اجرای آن را نخواهد داد.

صرف‌نظر از این فرمان اجرایی خاص رئیس‌جمهوری آمریکا در ارتباط با پلتفرم‌ها، برآیند مخالفت‌های حقوقی، سیاسی[1] و نیز موانع تکنولوژیکی که مانع از موفقیت این فرمان و دیگر اقدامات مشابه از سوی دولت سرمایه‌داری می‌شود نشان می‌دهد که توازن قدرت به نحو محسوسی به نفع پلتفرم‌ها در حال تغییر است و ای بسا که در آیندهٔ نزدیک جامعهٔ جهانی شاهد افول و زوال بیشتر مقتدرترین دولت سرمایه‌داری در برابر این پلتفرم‌ها نیز باشند[2].

مؤلفه‌های قدرت‌افزای گافام

مؤلفه‌ها و عناصر قدرت‌افزای گافام و دیگر پلتفرم‌های مشابه را می‌توان به صورت کلی به دو دسته تقسیم کرد: ۱. مؤلفه‌های سیاستی و ۲. مؤلفه‌های فناوری و نوآورانه.

---

۱. نکتهٔ حائز اهمیت این است که صرف‌نظر از مشکلات حقوقی فرمان اجرایی دونالد ترامپ و نیز موانع فناورانه‌ای که این فرمان با آن روبه‌رو است، به لحاظ سیاسی نیز شکستن یا محدود کردن قدرت این پلتفرم‌ها که عمدتاً آمریکایی هستند، با این استدلال که باعث برتری پلتفرم‌های چینی و غلبهٔ آن‌ها بر فناوری آمریکا خواهد شد، به شدت از سوی کارشناسان و تحلیلگران آمریکایی نهی شده است.

۲. لازم به یادآوری است که چالش‌های گافام برای سایر کشورها همچون کشورهای اروپایی، چین، روسیه و دیگر کشورهای نوظهور همچون ایران به مراتب بیشتر، پرتنش‌تر و تهدیدآمیزتر است زیرا این پلتفرم‌ها هیچ احساس مسئولیت یا پاسخگویی نسبت به مطالبات این کشورها ندارند.

۱. مؤلفه‌های سیاستی: این مؤلفه‌ها که در قالب دیپلماسی شرکتی از سوی پلتفرم‌ها دنبال می‌شوند، خود به دو صورت عمل می‌کنند:

ادغام: مهم‌ترین رویکرد پلتفرم‌ها و سایر شرکت‌های بزرگ که از سوی ناظران در سال‌های اخیر رصد شده، موضوع ادغام هر چه بیشتر آن‌ها در یکدیگر بوده است. برای مثال بر اساس گزارش دنیس هارن و جاناتان تپر، گافام در طول ده سال گذشته کنترل حدود پانصد شرکت بزرگ و کوچک دیگر را به دست گرفته و با خود ادغام کرده است.[1] ادغام خود در سه سطح صورت می‌گیرد. ادغام افقی[2] (مالکیت شرکت‌هایی با محصولات مشابه)، عمودی[3] (مالکیت مراحل مختلف تولید و توزیع محصول) و مورب[4] (مالکیت متقابل مشاغل مختلف).

انحصار: مهم‌ترین خروجی ادغام که در بالا به آن اشاره شد، ایجاد انحصار است که خود نیز به سه صورت ایجاد می‌شود: ۱. انحصار تک‌قطبی[5]: اینکه یکی از این پلتفرم‌ها به تنهایی انحصار همه‌جانبهٔ یک محصول/ خدمات را در اختیار داشته باشد؛ ۲. انحصار دوقطبی[6]: اینکه دو پلتفرم بتوانند انحصار یک محصول یا خدمات را با یکدیگر به دست آورند؛ ۳. انحصار چندقطبی[7]: اینکه بیش از دو پلتفرم بتوانند از طریق مکانیسم‌هایی، انحصار یک محصول یا خدمات را به دست آورند.

در سال‌های اخیر مؤلفه‌های ادغام و انحصار به صورت موازی از سوی این پلتفرم‌ها و شرکت‌ها دنبال شده‌اند. از نگاه این پلتفرم‌ها، «رقابت» مختص بازندگان است و تنها حوزه‌هایی ارزش سرمایه‌گذاری دارند که دارای نوعی انحصار هستند. لذا «ادغام»های صورت‌گرفته نیز حول محور «انحصار»ها متمرکز می‌باشد.

---

1. Denise Hearn & Jonathan Tepper, 2018
2. Horizontal Integration
3. Vertical Integration
4. Diagonal Integration
5. Monopoly
6. Duopoly
7. Oligopolies

البته باید در نظر داشت که منتقدان دیپلماسی شرکتی دو فرایند «ادغام» و «انحصارگری و انحصارطلبی» پلتفرم‌ها را عامل مرگ رقابت به عنوان مهم‌ترین وجه ممیزه و ویژگی ذاتی نظام‌های سرمایه‌داری می‌دانند.[1]

۲. مؤلفه‌های فناوری و نوآوری: این مؤلفه‌ها عمدتاً ناشی از پیشرفت فناوری هستند که بیشتر در داخل هسته‌های علمی و فنی خود پلتفرم‌ها شکل می‌گیرند. چهار صورت این فناوری‌ها که در حال حاضر موجب افزایش قدرت گافام شده‌اند عبارت‌اند از:

اینترنت اشیا: یک اکوسیستم اینترنت اشیا شامل تعداد زیادی فناوری متصل به شبکه است که قادر به تولید، جمع‌آوری، تحلیل یا پردازش اطلاعات جمع‌آوری شده بوده و به شبکه‌ای از ذی‌نفعان آن حوزه متصل است. اینترنت اشیا همچنین داده‌ها و تحلیل‌ها را به سرورهای داخلی یا مخازن انبوه[2] منتقل می‌کند. اینترنت اشیا در سال‌های اخیر به دلیل گردش بالای مالی آن‌ها به شدت مورد توجه پلتفرم‌ها بوده است. برای مثال، بر اساس برآورد فراست و سولیوان[3]، تنها در حوزهٔ سلامت میزان فروش اشیای پزشکی متصل به اینترنت در سال ۲۰۱۷، ۴۱ میلیارد دلار بوده و پیش‌بینی می‌شود با رشد ۲۶ درصدی به ۷۲,۲ میلیارد دلار در سال ۲۰۲۱ و ۱۵۸ میلیارد دلار در سال ۲۰۲۲ برسد (کل درآمد فناوری سلامت شامل هوش مصنوعی، واقعیت دیجیتال، و اینترنت اشیای پزشکی برای سال ۲۰۲۲، ۲۸۰ میلیارد دلار پیش‌بینی شده است[4]).

بر اساس برآوردهای صورت‌گرفته، پیش‌بینی می‌شود تا سال ۲۰۲۵، بیش از پنجاه میلیارد دستگاه از طریق شبکه (اینترنت اشیا) در بستر اینترنت

---

1. Denise Hearn and Jonathan Tepper, 2018
2. Cloud Repository
3. Frost & Sullivan
4. https://www. marketsandmarkets. com

متصل باشند و این حوزه بتواند تا سقف بیش از یازده تریلیون دلار درآمد برای صاحبان آن کسب نمایند.

داده‌های کلان[1]: داده‌های کلان، فناوری متشکل از ذخیره‌سازی و آنالیز پیچیده‌ای از انبوه اطلاعات دیجیتال است که به صورت مداوم تولید و در بستر شبکه توزیع می‌شود. برای فهم ارزش داده‌های کلان، همین بس که از آن به عنوان ذخایر جدید و منابع اصلی کشورها همچون منابع نفت و گاز یاد می‌شود. پلتفرم‌هایی همچون فیس‌بوک، گوگل و... که دارندهٔ حجم انبوهی از داده‌های کاربران هستند، در واقع صاحب غنی‌ترین منابع و ذخایر ثروت‌زا نیز می‌باشند و به همین دلیل به عنوان امپراتوری‌های «داده»ها شناخته می‌شوند. پیش‌بینی می‌شود میزان داده‌های ذخیره‌شده در بستر شبکهٔ اینترنت تا پایان سال ۲۰۲۵ به چهل زتا بایت[2] برسد[3].

رایانش ابری[4]: در راستای فناوری داده‌های کلان و نیز اینترنت اشیا، فناوری رایانش ابری مدلی برای ارتقای دسترسی بهینه به منابع شبکه برای افزایش سرعت و حجم ذخیرهٔ داده‌ها می‌باشد. پیش‌بینی می‌شود تا سال ۲۰۲۵، بیست زتا بایت از داده‌های موجود به صورت ابری مدیریت بشوند.

هوش مصنوعی: هوش مصنوعی در سال‌های اخیر برای اولین‌بار جایگزین تمامی فعالیت‌های انسانی در این پلتفرم‌ها شده است. به عبارت دیگر، به مدد هوش مصنوعی، انسان برای اولین‌بار در معرض محصول و دست‌ساختهٔ خود قرار می‌گیرد و قرار است از طریق آن محک شده و مورد قضاوت قرار گیرد. صرف‌نظر از ابعاد فنی هوش مصنوعی و کاربردهای متنوع آن در سایر

---

1. Big Data
2. Zettabyte
۳. هر زتابایت برابر با ۱۰۲۴ اگزابایت است؛ یعنی حدود دو میلیارد سال موسیقی.
4. Cloud Computing

حوزه‌ها، به خصوص عرصهٔ پزشکی، پلتفرم‌ها از هوش مصنوعی عمدتاً برای کنترل بیشتر و اعمال محدودیت بیشتر بر رفتار کاربران استفاده می‌کنند؛ به طور مثال آنچه فیلترینگ پیشگیرانه یا فیلترینگ حبابی نامیده شده است. اگرچه استفاده از هوش مصنوعی برای اعمال محدودیت‌هایی همچون نقض کپی‌رایت و... در نگاه اول ممکن است خوشایند به نظر برسد، اما سوءاستفاده از ظرفیت این فناوری در راستای منافع تجاری و اقتصادی پلتفرم‌ها از جمله در شخصی‌سازی تبلیغات، فروش داده‌ها و اطلاعات شخصی، و... بیشتر مشاهده و گزارش شده است. در واقع، روایت پلتفرم‌ها از اینکه «هوش مصنوعی چارهٔ همهٔ مشکلات است»،[1] روایتی فریب‌دهنده است که درست همانند الگوریتم‌ها، نقش عوامل انسانی و روابط اجتماعی ـ اقتصادی به عنوان زیربنای فعالیت‌های هوش مصنوعی را پنهان می‌سازد.

بلاک‌چین: بلاک‌چین را می‌توان به نوعی آخرین فناوری در عرصهٔ سایبری دانست که کاربرد گسترده‌ای، به خصوص در زمینهٔ رمزارزها، یافته است. امروزه از این فناوری برای ثبت، ضبط و حفظ داده‌ها به صورت رمزگذاری با استفاده از قابلیت هش‌شده[2] استفاده می‌کنند. نظام رمزگذاری در بلاک‌چین باعث مصون ماندن داده‌ها از هر گونه تلاش برای هک، سرقت یا دستبرد با هدف تغییر اطلاعات می‌شود. همچنین پلتفرم‌ها از این فناوری برای «تمرکززدایی» گسترده خدمات اپلیکیشن‌های خود استفاده می‌کنند و بدین ترتیب امکان نظارت و اعمال مقررات بر آن‌ها را بیش از پیش دشوار می‌سازند.

---

۱. این روایت به پاسخ مارک زاکربرگ، مدیرعامل فیس‌بوک، در جلسات استماع کنگرهٔ آمریکا اشاره دارد که در واکنش به ده‌ها اعتراض از سوی نمایندگان این کشور در ارتباط با «سوءاستفاده از داده‌ها»، «ترویج خشونت»، «عدم نظارت بر نفرت‌پراکنی»، «نقض حریم خصوصی» و... همواره از این عبارت استفاده می‌کرد.

2. Hash

پایه و اساس هر چهار فناوری فوق‌الذکر، الگوریتم‌ها هستند. در واقع در پس این فناوری‌ها، ایدئولوژی سرمایه‌داری نهفته است که از طریق الگوریتم‌ها بازتولید می‌شود و به همین جهت نیز عموماً از آن به عنوان «سرمایه‌داری الگوریتمی» یاد می‌شود. الگوریتم‌ها به صورت کلی مجموعه دستورالعمل‌هایی هستند که بر اساس فرمول‌های ریاضی و تحت عنوان آنچه «پروتکل‌های اینترنتی» نامیده شده، به صورت خودکار بر داده‌ها اعمال می‌شوند. مسئله اصلی در ارتباط با الگوریتم‌ها این است که این الگوریتم‌ها ساختهٔ دست انسان هستند و لذا شکی وجود ندارد که در تدوین آن‌ها منابع و منافع سازندگان آنها، به خصوص صاحبان گافام، در اولویت قرار می‌گیرد. به گفتهٔ میجر، «ایدئولوژی سرمایه‌داری شرکتی در موتورهای جست‌وجو نهادینه شده و از طریق منطق الگوریتمی و نظام‌های محاسباتی عمل می‌کند».[1] موضوعاتی همچون جهت‌دار بودن، گزینشی بودن، فقدان استاندارد واحد از جملهٔ مهم‌ترین ایرادات و انتقاداتی است که به نحوهٔ عملکرد الگوریتم‌ها وارد شده است.

ترکیب فناوری‌های پیچیده فوق و تبلور آن در انواع محصولات و خدمات گافام، منابع قدرت و ثروت آن‌ها را به میزان نامحدودی افزایش داده به نحوی که هیچ دولتی به تنهایی توانایی مقابله یا مهار آن‌ها را ندارد. در واقع بر اساس ذهنیت پلتفرمی گافام، این فناوری‌ها اساساً برای رهایی از دستورالعمل‌ها و مقررات‌گذاری نظام‌های سیاسی و نیز دور زدن دولت‌ها طراحی و توسعه یافته‌اند. لذا شکی وجود ندارد که چرخهٔ ایجاد و توسعهٔ فناوری‌های مرکزگریز مشابه آنچه در بالا به آن اشاره شد، همچنان ادامه خواهد داشت.

---

1. Mager, 2014, p. 32

چشم‌انداز توسعه گافام و چالش‌های آن برای حکمرانی

بر اساس موضوعات کلانی که در ارتباط با پلتفرم‌ها و عملکرد آن‌ها در بالا به آن‌ها اشاره شد، چشم‌انداز روشنی از آینده این پلتفرم‌ها، به خصوص با توجه به سرعت زیادی که آن‌ها به سوی ادغام و انحصار گام برمی‌دارند وجود ندارد. حتی از منظر حکمرانی، با مطالعه و در نظر گرفتن سابقهٔ بیش از دو دهه اصطکاک و تقابلی که بین آن‌ها و قدرتمندترین دولت سرمایه‌داری وجود داشته، احتمال به انقیاد درآمدن و واداشتن آن‌ها به رعایت ملاحظات سیاست‌های رسمی نظام‌های حکمرانی چندان امیدوارکننده نیست.

فراتر از آن، چالش‌های گافام و سایر پلتفرم‌ها برای نظام‌های سیاسی زمانی شدیدتر و پیچیده‌تر می‌شود که بحث نقش آن‌ها در ارتباط با منازعات مهم حاکمیتی (اعم از سیاسی، امنیتی، روابط خارجی و ...) کشورهای ثالث، کشوری غیر از آمریکا، در میان باشد. امروزه با توجه به کشیده شدن تمامی منازعات حاکمیتی کلاسیک به عرصهٔ سایبری، گافام و دیگر پلتفرم‌ها به یکی از طرف‌های اصلی منازعات هم در درون کشورها و هم در بین کشورها در عرصهٔ سایبری تبدیل شده‌اند. در واقع به دلیل قدرت بازیگری پلتفرم‌ها در عرصهٔ سایبری و قلمروهای انحصاری که آن‌ها در این عرصه برای خود در مقیاس جهانی و منطقه‌ای تعریف کرده‌اند، این پلتفرم‌ها به عنوان بازیگر مستقل در هر نوع منازعه‌ای حضور دارند و نقش مهمی در ایجاد توازن یا تغییر موازنه به نفع یا علیه کشورها در روابط بین‌الملل ایفا می‌کنند. به طور مثال در منازعه و درگیری مرزی بین چین و هند در ماه می ۲۰۲۰ که طی آن بیست سرباز هندی کشته شدند، هند دامنه‌های این منازعه را به عرصهٔ پلتفرم‌ها کشاند و از طریق حذف ۲۷۰ اَپ چینی از بازار دیجیتال این کشور، ضربه‌ای به مراتب سخت‌تر و کاری‌تر به چین وارد ساخت، موضوعی که در رسانه‌های جهان از آن به عنوان «نبرد در میدان پلتفرم‌ها» یاد شد.

از این رو، از منظر حاکمیت ملی کشورها دو موضوع مهم در ارتباط با نقش و جایگاه پلتفرم‌ها برجسته می‌شود: الف) با توجه به سرعت روبه‌رشد پلتفرم‌ها، تصور آینده‌ای که این پلتفرم‌ها تمامی تعاملات مرسوم در ساختارهای سیاسی کلاسیک، اعم از انتخابات، اقتصاد، فرهنگ و رسانه، کسب‌وکار، سلامت و پزشکی، و... را رقم بزنند یا دست‌کم تحت تأثیر قرار بدهند، دور از ذهن نیست. ب) حاکمیت‌گریزی پلتفرم‌ها، منافع تجاری و اقتصادی سرمایه‌های خصوصی آنها، محرمانه بودن ظاهری آنها، هوش مصنوعی، واقعیت دیجیتال و... اکوسیستم کاملاً به هم وابسته‌ای در ساختار اجتماعی جوامع قرن ۲۱ ایجاد می‌کند که دیگر با مکانیسم‌های سنتی و قدیمی قابل مدیریت نیست. در اثر ورود پلتفرم‌ها به ساختار نظام‌های اجتماعی جوامع، ساختار کلان سیاسی و تمامی ابعاد و مؤلفه‌های آن به یکی از متزلزل‌ترین بخش‌ها از لحاظ آمادگی کشورها (از جمله به لحاظ دفاع سایبری، رگیولاتوری، پاسخگویی سایبری و...) برای مواجهه با بحران‌های سایبری تبدیل شده‌اند.

بر این اساس، مهم‌ترین چالش‌های ناشی از گسترش روزافزون نفوذ گافام و دیگر پلتفرم‌ها در سپهر سیاسی، اجتماعی، اقتصادی و فرهنگی جوامع امروزی را به صورت ذیل می‌توان صورت‌بندی کرد:

۱. **حجم عظیم مبادلات مالی**: بر اساس آخرین برآوردی که در سال ۲۰۲۰ صورت گرفت، به لحاظ اقتصادی ارزش مجموع پنج پلتفرم گافام از ۵ هزار میلیارد دلار (۵ تریلیون دلار) فراتر رفت که می‌توان گفت از مجموع درآمد و تولید ناخالص ملی ده‌ها کشور بیشتر باشد. بر اساس برآوردی که در سال ۲۰۱۶ صورت گرفت، ۸۵ سنت از هر دلاری که به صورت آنلاین مبادله می‌شود، به جیب گوگل و فیس‌بوک می‌رفته است.[1] این حجم از درآمد و مبادلهٔ

1. Paul Dughi, 2016

مالی به پلتفرم‌ها برای اثرگذاری در ابعاد مختلف قدرت زیادی می‌دهد.

۲. امنیت اطلاعات و حریم خصوصی: مهم‌ترین دغدغهٔ عمومی و مشترک تمامی ذی‌نفعان مقابل پلتفرم‌ها (به ویژه دولت‌ها و کاربران)، مسئلهٔ حریم خصوص آن‌ها و نیز اطمینان از امنیت این داده‌ها در آینده است. برای مثال، امروزه از مارک زاکربرگ، مدیرعامل فیس‌بوک، به عنوان امپراتور «داده‌های شخصی» بیش از دو میلیارد کاربر یاد می‌شود که ارزش بالقوهٔ تجاری آن به مراتب بیشتر از منابع نفتی چندین کشور نفت‌خیز خاورمیانه است. اخبار و اطلاعاتی که روزانه از درز اطلاعات کاربران افشا می‌شود، و حتی این پلتفرم‌ها نیز ابایی از تأیید آن به دلایل مختلف ندارند، دلالت بر همین نگرانی‌های مربوط به حریم خصوصی دارد. دغدغه و نگرانی مهم‌تر اینکه برخی از تحلیلگران، مدعی وجود دست‌های پشت پرده با اهداف سیاسی یا اقتصادی در این گونه درزهای اطلاعاتی یا حتی فروش عامدانه و گستردهٔ اطلاعات فردی کاربران هستند که به عنوان مثال می‌توان به اتهام فروش اطلاعات رأی اولی‌ها در انتخابات ۲۰۱۶ آمریکا یا هک حساب‌های توییتری بیش از ۱۳۰ تن از رهبران سیاسی، اقتصادی و اجتماعی آمریکا در سال ۲۰۲۰ اشاره کرد.

۳. پیچیدگی مکانیسم عملکرد پلتفرم‌ها: در بسیاری از موارد نه فقط کاربران عادی، حتی حکومت‌ها و نظام‌های حکمرانی نیز در برابر فهم مکانیسم فعالیت پلتفرم‌ها به خصوص ابعاد فنی، حقوقی و ارتباطی آن‌ها همچون «آثار استرایسند»، «الگوریتم‌ها»، «واقعیت رمزگذاری پایان ــ به ــ پایان»، «فیلترینگ حبابی»، «حقوق دیجیتال»، «حق فراموش‌شدگی»، «آستروتورفینگ[1] و شهرت جعلی»، «فناوری نظیربه‌نظیر»، «دست‌کاری یا سرقت اطلاعات» و... آشکارا سردرگم یا با دشواری مواجه هستند یا اصلاً

---

۱. Astroturfing. ایجاد کمپین‌های جعلی برای جلب توجه.

از مکانیسم طراحی، شیوهٔ عمل و حتی نحوهٔ استفاده از آن‌ها آشنا نیستند، با این حال کاربران آن‌ها محسوب می‌شوند و روزبه‌روز بر دامنهٔ اثرگذاری این پلتفرم‌ها بر ساحت این جوامع افزوده می‌شود.

٤. محتوا در پلتفرم‌ها: در متون ارتباطی و رسانه‌ای، محتوا همواره پادشاه محسوب می‌شده و حتی در قانون اساسی آمریکا نیز اصل بر محتوا گذاشته شده و پلتفرم‌ها به عنوان مجاری و کانال‌های رسانه‌ای، صرفاً بستری برای انتقال محتواها محسوب می‌شوند. با این حال، در سال‌های اخیر و با ظهور پدیدهٔ ادغام‌های طولی، افقی و مورب شرکت‌های بزرگ، پلتفرم‌ها بر تخت پادشاهی آنلاین تکیه زده و این محتواست که نقش فرعی شاهزاده را به عهده گرفته است. فراتر آنکه صرف‌نظر از حجم انبوه محتواها که به صورت رایگان توسط کاربران تولید می‌شود، هوش مصنوعی به مدد الگوریتم‌های فنی آمده و بیش از ۴۳ درصد محتواهای آن‌ها را به صورت خودکار تولید می‌کنند.[1] لذا دیگر نمی‌توان نقش پلتفرم‌ها در تولید محتوا، جهت‌دهی به محتوا، گزینش محتوا، فریمینگ محتوا، ایجاد شبکه‌های معنایی از مفاهیم و مقولات و... که عموماً از طریق الگوریتم‌ها و به خصوص به مدد هوش مصنوعی صورت می‌گیرد را نادیده انگاشت و برای آن حاشیهٔ امن قائل شد.

۵. خودتنظیم‌گری و استقلال در مقررات‌گذاری: بر اساس بند ۲۳۰ «قانون رفتار سالم در ارتباطات» مصوب ۱۹۹۶ کنگرهٔ آمریکا، پلتفرم‌ها اساساً به عنوان بستری خنثی تلقی شده که صرفاً نقش مجرا (کانال) در انتقال محتوا را به عهده داشته و لذا مسئولیتی متوجه آن‌ها نیست. به استناد همین بند قانونی، پلتفرم‌ها همواره خود را در حاشیهٔ امن دانسته و از پاسخگویی به ساختارهای حکمرانی نظام‌های سیاسی طفره رفته‌اند. علاوه بر این، در موارد متعددی نیز

1. Paul Dughi, 2016

با توجیه پیچیدگی ابعاد فنی مسائل، جبر فناوری، هوش مصنوعی و... همواره بر اساس رویکرد خودتنظیم‌گری عمل کرده‌اند و از هر گونه پاسخگویی طفره رفته‌اند. این رویکرد امروزه با چالش اساسی مواجه شده و حتی در آمریکا نیز زمزمه‌هایی مبنی بر تغییر بند ۲۳۰ «قانون رفتار سالم در ارتباطات» در قانون آمریکا شکل گرفته است.

٦. خروج حجم زیادی از داده‌ها و اطلاعات از کشور: با توجه به اینکه عمدهٔ این پلتفرم‌ها و اپلیکیشن‌های آن‌ها خارجی هستند و مراکز ذخیرهٔ اطلاعات و داده‌های آن‌ها نیز در خارج از کشور می‌باشند، امکان استفاده از این داده‌ها در هر سمت و سویی، حتی جهت تضعیف روحی و روانی افکار عمومی، ایجاد بازارهای کاذب، ایجاد تقاضاهای کاذب، ایجاد شورش و اغتشاش‌های کاذب و...، توسط صاحبان آن امکان‌پذیر است. چالشی که امروزه تحت عنوان «حکمرانی داده» در کشورهای مختلف آغاز شده، دلالت بر همین موضوع دارد. موکش آمبانی[1] کارآفرین برجسته، در اجلاس گجرات ۲۰۱۹[2]، دغدغهٔ امروز هندوستان در ارتباط با خروج داده‌ها از این کشور را این گونه بیان کرد: «همان طور که گاندی جنبشی را علیه استعمار سیاسی هند به پیش برد، ما نیز باید دسته‌جمعی جنبشی علیه استعمار داده[3] راه**اندازی** کنیم. «داده» نفت جدید است، «داده» رفاه جدید است. مالکیت و کنترل داده‌های هند باید توسط مردم هند صورت گیرد نه توسط پلتفرم‌ها؛ به خصوص پلتفرم‌های جهانی. برای موفقیت در این تحول در جریان داده‌ها، ما باید سیر مهاجرت داده‌ها از هند را متوقف کنیم و مالکیت و کنترل آن را به هند برگردانیم. به عبارت دیگر، رفاه و امنیت هند را به هندی‌ها برگردانیم. آقای نخست‌وزیر!

---

1. Mukesh Dhirubhai Ambani
2. Gujarat Summit 2019
3. Data Colonisation

من مطمئن هستم که شما این را به عنوان یکی از سرفصل‌ها و اصول اساسی خود در مأموریت «هند دیجیتال» قرار خواهید داد».[1] مشابه همین دغدغه امروزه از سوی بسیاری از کشورها، حتی کشورهای اروپایی، نیز مطرح و برجسته شده است.

۷. انحصار سیستم‌های عامل در پلتفرم‌ها: اندروید، آی‌اواس[2] و ویندوز فون[3] سه سیستم عامل اصلی در دنیای کامپیوتر و موبایل‌ها هستند. اپلیکیشن‌ها، که امروزه به یک کسب‌وکار تمام‌عیار تبدیل شده‌اند، تماماً به سیستم عامل اندروید و آی‌اواس وابسته هستند که در انحصار گوگل و اپل، دو عضو اصلی گافام، قرار دارند. با وجود تلاش‌هایی که از سوی کشورهایی همچون چین، کره جنوبی و... برای رهایی از وابستگی به سیستم‌های عامل اندروید، آی‌اواس و ویندوز فون صورت گرفته، چشم‌انداز موفقیت آن‌ها در برابر سیستم‌های عامل گافام بسیار محدود و تا حدودی بسیار ناچیز است. لذا باید در نظر داشت که حیات تمامی اپلیکیشن‌ها و به نوعی کسب‌وکارهای آنلاین در اقصی نقاط جهان در دستان این پلتفرم‌هاست و اینکه آن‌ها از قدرت و حق هر گونه کنترل یا دخل و تصرفی در آنها، از جمله حذف تمام‌عیارشان از دنیای سایبری و واقعی، برخوردارند. حذف برخی از اپلیکیشن‌های کسب‌وکار ایرانی از بستر سیستم‌های عامل که در سال‌های اخیر اتفاق افتاد و یا حتی حذف نقشهٔ فلسطین از روی نقشه‌های جغرافیایی تهدیداتی است که نمی‌توان و نباید به آسانی از کنار آن‌ها گذشت.

۸. هک/ جاسوسی/ حذف یا دست‌کاری اطلاعات: وابستگی تمام‌عیار تمامی سیستم‌های عامل، اپراتورهای فعال، اپلیکیشن‌های مختلف به سه سیستم عامل اندروید، آی‌اواس و ویندوز فون تا حدود زیادی دست آن‌ها را برای

---

1. Mukesh Dhirubhai Ambani, 2019
2. IOS
3. Windows Phone

هر گونه دست‌کاری، حذف، جاسوسی و... کاملاً باز گذاشته است. با توجه به درهم‌تنیدگی منافع تجاری و اقتصادی پلتفرم‌ها با قدرت‌های لابیگر و حتی برخی دولت‌ها و محافل سیاسی در کشورهای غربی، اهمیت این موضوعات و احتمال همکاری و همراهی این شرکت‌ها با فعالیت‌های مخرب سایبری که چه به صورت رسمی و چه به صورت نیابتی از طریق گروه‌های پراکسی علیه برخی از کشورهای هدف طراحی و اجرا می‌شود، چندان دور از ذهن نیست. تا کنون اطلاعات زیادی در زمینهٔ جاسوسی سایبری، هک سیستم‌های عامل، تخریب زیرساخت‌های اطلاعاتی و ارتباطی کلیدی و ... از اقصی نقاط جهان گزارش شده است که ازجمله آن‌ها می‌توان به حملات سایبری به زیرساخت‌های هسته‌ای کشور اشاره کرد.

جمع‌بندی و نتیجه‌گیری این فصل

حامیان اتوپیای فناوری سایبری همچون جان پری بارلو ممکن است استدلال کنند که فضای سایبری دنیایی کاملاً متفاوت از دنیای واقعی است و به نوعی خطوط قرمز برای نظام‌های سیاسی جهت اعمال حکمرانی ملی بر آن‌ها ترسیم نمایند؛ اما این موضوع اسطوره‌ای بیش نیست که صرفاً برساخت ذهنیت پلتفرمی و تضمین‌کنندهٔ منافع اقتصادی، تجاری و ایدئولوژیک صاحبان آنهاست.

دانیل لامباچ استدلال می‌کند که فضای سایبری یک مکان واحد همچون یک قاره یا یک جزیرهٔ منفک نیست که نتوان به آن ورود پیدا کرد، بلکه یک فضای مسطح الکترونیکی متشکل از مجموعه‌ای پیچیده و متداخل از قلمروهای سایبری است که هرکدام توسط ذی‌نفعان (به طور خاص دولت‌ها، شرکت‌های خصوصی و کاربران) مختلف اداره می‌شود. وی می‌نویسد: «دولت بخش‌های ملی فضای سایبری را برای مثال از طریق وضع قوانین

داخلی (همچون محلی‌سازی داده‌ها، پرداختن بـه زیرسـاخت‌هـای مـوازی و تدوین دکترین دفاعی سایبری) ایجاد می‌کنـد. شـرکت‌هـا و کسـب‌وکارهـای خصوصی اکوسیستم‌های مشخصی در آن ایجاد می‌کننـد کـه در آن محصـول خود را بفروشند. کاربران نیز از طریق اجتماعات آنلاین یا گـروه‌هـای چـت، قلمروهای کوچک و قابل انعطافی ایجاد می‌نمایند. این قلمروها یا با یکـدیگر همپوشانی و تـداخل دارنـد یـا مـدام در حـال تغییـر هسـتند. درگیـری‌هـا و تداخلات معمول در آن بسیار زیاد است. اما کلیت عرصهٔ سایبری برای اعمال حکمرانی نظام‌های سیاسی یک مقولهٔ دست‌نیافتنی نیست».[1]

با توجه به اهمیت فضای سایبری، چنـدین سـال اسـت کـه کشـورهای مختلف بازیگران مهم ایـن عرصـه از جملـه گافـام را بـه عنـوان بـازیگران قدرتمند عرصهٔ دیپلماسی سایبری بـه رسـمیت شـناخته و تعـاملاتی کـاملاً مستقل از سازوکارهای دیپلماسی سنتی در روابط بین‌الملـل بـا آن‌هـا آغـاز کرده‌اند. بر اساس مطالعه‌ای که در این زمینه انجام شـد، اولـین رویکـرد در زمینهٔ تعامل با گافام و سایر پلتفرم‌ها، رویکرد قانون‌گذاری بوده که بـه طـور مشخص در ارتباط بـا مباحـث مهمـی همچـون «حکمرانـی داده»، «هـوش مصنوعی»، «اخلاق سایبری» و... صورت گرفته است.

در این زمینه، مرکز مطالعات بین‌الملل و استراتژیک[2] مسـتقر در آمریکـا در سال ۲۰۱۹ اعلام داشت که در این سال در مجموع بیش از پانصـد قـانون در سراسر جهان تصویب شده است که همگی بر ضرورت اعمال حق حاکمیـت کشورها در تعامل با گافام و دیگر پلتفرم‌ها در عرصهٔ سایبری نـاظر بـوده‌انـد.[3] از جمله مهم‌ترین مصادیق این رویکرد، ساختار قانون‌گذاری اتحادیـهٔ اروپـا و

1. Daniel Lambach,2019
2. Center for Strategic and International Studies
3. Center for Strategic and International Studies, 2019

قانون‌گذاران اروپایی است که به سمت اعمال قوانین سخت‌گیرانه‌تری در جهت مسئولیت‌پذیری هر چه بیشتر پلتفرم‌ها در قبال محتوای آن‌ها حرکت نموده‌اند. در مسیر معرفی تقسیم وظایف عادلانه‌تر، مصونیت واسطه‌ای پلتفرم‌ها در این اتحادیه به طور فزاینده‌ای محدود گردیده است. بر اساس محدودیت‌های اعمال‌شده از سوی قانون‌گذاران اروپایی، پلتفرم‌ها به خاطر به اشتراک‌گذاری محتوای ناقض قانون کپی‌رایت و سایر موارد نقض قانون مسئول شناخته می‌شوند.

مصادیق دیگر این رویکرد، قانون‌گذاری در کشورهای آلمان، هندوستان، ترکیه و نیجریه است که در سطح ملی برای محدودسازی دامنهٔ فعالیت پلتفرم‌ها و نیز مسدودسازی راه‌های فرار آن‌ها از چنگال قانون صورت گرفته است. بنا بر قانون اجرای شبکهٔ آلمان (۲۰۱۷)، پلتفرم‌ها می‌بایست از وجود ساختار کارآمد جهت ثبت شکایات راجع به محتوای مجرمانه اطمینان حاصل نمایند. نیجریه از سال ۲۰۱۳ شرکت‌های خدمات اینترنتی را ملزم به ذخیره‌سازی داده‌ها در داخل این کشور کرده است. به طور مشابهی، در کشور هندوستان نیز اعمال محدودیت بر دامنهٔ فعالیت و مسئولیت‌پذیری پلتفرم‌ها به تصویب بند ۷۹ قانون فناوری اطلاعات[1] این کشور منجر شد که مصونیت مشروط[2] برای پلتفرم‌ها ارائه می‌دهد.[3] همچنین پارلمان ترکیه در ژوئیهٔ ۲۰۲۰ قانونی را به تصویب رساند که بر اساس آن شبکه‌های اجتماعی خارجی که بیش از یک میلیون کاربر در داخل ترکیه دارند، باید در این کشور دفتر و نمایندگی محلی داشته باشند و به درخواست‌های مربوط به حذف محتوا عمل کنند. شرکت‌ها در صورت سرپیچی از این قانون با جریمهٔ نقدی روبه‌رو

1. Section 79 of the Indian Information Technology Act
2. Qualified Immunity
3. Matthias C. Kettemann , Stephan Dreyer & Daniel Lambach, 2019

می‌شوند و ممکن است سرعت تبادل داده آن‌ها به شدت محدود شود.[1]

در کنار رویکرد قانون‌گذاری و مقررات‌گذاری، برخی دیگر از کشورها رویکرد دیپلماتیک محسوس و عینی‌تری در این زمینه در ساختار حکمرانی سایبری خود ایجاد کرده‌اند که از جمله می‌توان به راه‌اندازی ادارات و دفاتر دیپلماسی سایبری در ساختار وزارت امور خارجه (آمریکا، انگلستان، آلمان و...)، یا حتی انتصاب سفرا و مقامات عالی‌رتبهٔ سایبری در شورای امنیت ملی (آمریکا)، انتصاب سفیر مخصوص در گافام (به طور خاص کشور دانمارک) و... اشاره کرد.

ایران نیز از این قضیه نمی‌تواند مستثنا باشد. نظام حکمرانی سایبری هر چه زودتر باید اهداف، جهت و رویکرد تعامل خود با پلتفرم‌ها را روشن و از مسیرهای مختلف، همچون قانون‌گذاری و مقررات‌گذاری، تعیین سفرای سایبری، تغییر در ساختار سیاست خارجی و... منافع ملی کشور را از طریق پلتفرم‌ها در عرصهٔ سایبری دنبال کند.

فراتر از آن باید در نظر داشت که عمدهٔ تحولات فناورانه و اثرگذار که در عرصهٔ سایبری اتفاق می‌افتد، در چارچوب فعالیت‌های همین پلتفرم‌ها صورت می‌گیرد. از این رو، ایران نیز باید از طریق همین پلتفرم‌ها یا راه‌اندازی یک پلتفرم مؤثر جدید به صورت مشارکتی، بخشی از یک طرح فناورانه بین‌المللی باشد تا بتواند درجه‌ای از تأثیرگذاری در آیندهٔ تحولات عرصهٔ سایبری را برای خود تضمین کند. به عبارت دیگر، تنها از طریق عضویت و مشارکت ایران در طرح‌های فناورانهٔ بین‌المللی است که نظام حکمرانی سایبری کشور می‌تواند اثرگذاری سایبری خود در آینده را تضمین کند و به نوعی تحولات سایبری در عرصهٔ جهانی را به خود وابسته سازد.

---

1. BBC News, Accessed on July 31, 2020

منابع

BBC News, “Turkey Imposes New Social Media Restrictions”. Accessed on July 31, 2020 at: https:// www. bbc.co.uk

Daniel Lambach (2019). “Cyberspace is Totally Separate from “the Real World”. In Busted! The Truth About the 50 Most Common Internet Myths. Edited by Matthias C. Kettemann and Stephan Dreyer. Internet Governance Forum Berlin, 25–29 November 2019.

Denise Hearn and Jonathan Tepper. (2018). “The Myth of Capitalism: Monopolies and the Death of Competition”. Wiley; 1 Edition.

Fortune, “Facebook and Amazon Grilled Over History of Aggressive Competitive Practices at Antitrust Congressional Hearing”. Accesed July 31, 2020 at https://fortune.com.

John Perry Barlow, A Declaration of the Independence of Cyberspace (1996) , https://projects. eff. org; Daniel Lambach, The Territorialization of Cyberspace, International Studies Review (2019) , https://doi. org.

Laure Claire Reillier & Benoit Reillier. (2017). Platform Strategy: How to Unlock the Power of Communities and Networks to Grow Your Business. Taylor & Francis Groups. 2019 Global Health Care Outlook Shaping the Future, (2019). Deloitte Centre for Health Solution (Report).

Paul Dughi (2016). “The Battle for the Online Throne: Content vs Platform”. Retrieved on 20 of January 2020 from: https://medium. com.

Mukesh Dhirubhai Ambani (2019). “Full Text of the Speech”. Retrieved on 18 of February 2010 from: https://www. cnbctv18. com.

Matthias C. Kettemann, Stephan Dreyer & Daniel Lambach (2019). “Busted! The Truth About the 50 Most Common Internet Myths”. Internet Governance Forum Berlin.

Medtech and the Internet of Medical Things, (July 2018). Deloitte Centre for Health Solution (Report).

Millward Brown, (2016). “Launchworks Reports” Retrieved on 20 of January 2020 from: http://www. millwardbrown. com.

The Future Health Index 2019: Transforming Healthcare Experiences, (2019). Philips Company (Report).

فصل دهم

گذار به دیپلماسی سایبری، چارچوب مفهومی و پیشنهاد الگوی عملی دیپلماسی سایبری در ایران

درآمد

جهان در یک دهۀ اخیر شاهد تغییرات بنیادی از منظر تحول در مفهوم «قدرت» و تغییر در موازنۀ منابع آن از «منابع سخت» به «منابع نرم» بوده است. این تغییر موازنه تا حد زیادی مرهون فناوری نوین ارتباطی و اطلاعاتی است که توانسته موجب «انقلاب در رسانه‌ها»، «سرعت در جریان اطلاعات و ارتباطات»، «قدرت گرفتن بیش از پیش افکار عمومی»، «جهانی‌سازی فرهنگ» و در نهایت ایجاد بستر و محیطی شود که در آن جوامع بیش از پیش به یکدیگر وابسته باشند. به همین دلیل، روش‌ها و ابزارهای سنتی همچون «قدرت نظامی»، «قدرت صنعتی» و «قدرت اقتصادی» در ادبیات نوین روابط بین‌الملل جای خود را به ابزارهای جدید قدرت همچون فضای سایبری و مؤلفه‌های اقتدارساز و توانمندساز در این عرصه داده است.

اگر تا چند سال پیش فضای سایبری یک موضوع صرفاً فنی و سخت‌افزاری برای متخصصان حوزۀ فناوری اطلاعات و ارتباطات بود، آن دوره امروزه پایان‌یافته تلقی می‌شود. جاسوسی سایبری، هک سایبری، سرقت

سایبری، نفوذ سایبری، اختلال در شبکه‌ها و یا نفوذ در شبکه‌ها،[1] نبرد پلتفرم‌ها و ... که در مقیاس فرامرزی به وقوع می‌پیوندند، امروزه موضوعاتی هستند که در صدر توجهات نظام‌های حکمرانی قرار گرفته و فضای سایبری را که با منافع، ارزش‌ها و هنجارهای بسیار متنوعی به پیش رانده می‌شود، به بحث برانگیزترین موضوع سیاسی روز تبدیل کرده است. در بُعد ایجابی نیز استفاده از ظرفیت‌های فضای سایبری برای اعتمادسازی، توسعهٔ کسب‌وکارها، توسعه همکاری‌ها، گسترش نفوذ و ... از جمله محورهایی است که در صدر برنامه‌ریزی‌های نظام‌های سیاسی و حکمرانی قرار گرفته است. از این رو دیپلماسی و فعالان آن عرصه، یعنی «دیپلمات‌ها»، نیز در کنار سایر بازیگران و ذی‌نفعان این حوزه وارد بازی شده و در آن نقش ایفا می‌کنند.

نقش دیپلماسی در فضای سایبری و به عبارتی نقش دیپلمات‌ها در فضای سایبری موضوعی است که در مقایسه با سایر موضوعات مرتبط، از جمله رویدادهای سایبری همچون امنیت سایبری، دفاع سایبری، و متناظر با آن نقش ژنرال‌های فنی یا امنیتی سایبری، کمتر به آن توجه شده است. در واقع عمدهٔ مباحث و مسائل فضای سایبری که تا کنون در محافل علمی، دانشگاهی و حتی سیاسی مطرح بوده، بیشتر بُعد فنی ـ امنیتی داشته و در آن بر چگونگی «انطباق با فناوری» و نیز «دفاع» از خود در مواجهه با ظهور فناوری‌های نوین و آثار و پیامدهای غیرقابل‌کنترل آن تأکید می‌شده است.

به لحاظ تاریخی، انتشار سند «استراتژی بین‌المللی فضای سایبری» آمریکا در سال ۲۰۱۱، که در آن منحصراً بر ابعاد «بین‌المللی» فضای سایبری تأکید شده، مهم‌ترین رویداد در دیپلماسی سایبری محسوب می‌شود. در این سند، فضای سایبری به عنوان بستری برای توسعهٔ ارزش‌های آمریکایی و ابزاری

1. Network Infiltration

برای تأمین منافع ملی این کشور در سراسر جهان تلقی می‌شد.

در سال ۲۰۱۵، چهار عضو سازمان همکاری‌های شانگهای، از جمله روسیه و چین، که تحت تأثیر انقلاب‌های رنگی و نیز بهار عربی نگرانِ مداخلات خارجی در امور داخلی خود بودند، نسخهٔ پیشنهادی کدها یا استانداردهای رفتاری بین‌المللی[1] در ارتباط با حاکمیت سایبری را تحویل مجمع عمومی سازمان ملل داده و خواستار قانون‌گذاری و مقررات‌گذاری بین‌المللی در ارتباط با فضای سایبری شدند، هرچند این پیشنهاد با نگرانی و گاهی مخالفت برخی کشورهای غربی (به رهبری آمریکا) مواجه شد که نگران نقض اصول پایه‌ای دموکراسی‌های غربی از جمله آزادی بیان و حقوق بشر شد.

متعاقباً مناقشه بین آمریکا و چین در سال ۲۰۱۵ بر سر نفوذ در شبکه‌ها، که به موضوعی دامنه‌دار در روابط بین دو کشور تبدیل شد، بُعد جدیدی از ظرفیت‌های فضای سایبری در روابط بین‌الملل را آشکار و جهانی ساخت و آن بحث گسترش و توسعهٔ دامنهٔ قدرت کشورها در سایر مناطق جهان از طریق فضای سایبری است. دربارهٔ مناقشهٔ آمریکا و چین، هر یک دیگری را به نفوذ در شبکه‌ها و سرقت اطلاعات محرمانهٔ شرکت‌ها و نهادهای دولتی یکدیگر متهم می‌کردند. یک بُعد این اتهامات، بر سنگ‌اندازی در مسیر توسعهٔ دیگری و بُعد دیگر آن بر استفاده از این اطلاعات و اسرار با هدفِ توسعهٔ خود، دلالت دارد.

در انتخابات ریاست‌جمهوری آمریکا در سال ۲۰۱۶ و موضوع نفوذ روسیه در شبکه‌های اطلاعاتی ایالات متحده به نفع دونالد ترامپ بیش از پیش به موضوع دیپلماسی سایبری دامن زد. از آن تاریخ به بعد، به دیپلماسی سایبری نه به معنای مواجههٔ سلبی در برابر فضای سایبری در سطوح ملی،

1. International Code of Conduct

بلکه در نقش مواجههٔ ایجابی برای استفاده از ظرفیت‌ها و پتانسیل آن برای توسعهٔ منابع قدرت و نفوذ در سایر مناطق جهان توجه شد. به این اعتبار، دیپلماسی سایبری متأخرترین مفهومی است که در تحولات سریع و پیچیدهٔ فضای سایبری وارد ادبیات روابط بین‌المللی شده است.

هدف از این فصل، بحث و مطالعهٔ نقش و جایگاه دیپلماسی در مسائل و چالش‌های روزافزون مرتبط با فضای سایبری در روابط بین‌الملل است؛ آن هم در زمانی که در معنای کارکردی دیپلماسی، و حوزه و گسترهٔ آن، و بازیگرانش تحول اساسی ایجاد شده است. به عبارت دیگر، هدف اصلی در این مطالعه عبارت است از: مفهوم‌پردازی در زمینهٔ دیپلماسی سایبری با هدف تبیین و تمایز آن از سایر مفاهیم مرتبط، ترسیم چارچوبی مفهومی برای اندیشیدن در این حوزه و در نهایت ارائهٔ الگویی عملی، تا بتوان بر مبنای آن به سیاست‌گذاری و برنامه‌ریزی در زمینهٔ دیپلماسی سایبری با توجه به مسائل و دغدغه‌های ملی پرداخت.

برای دستیابی به هدف فوق، از طریق مطالعهٔ اسنادی و نیز مطالعهٔ موردی چند کشور پیشرو، از جمله آمریکا، اتحادیهٔ اروپا، ژاپن، روسیه و چین، ابتدا تعاریفی از دیپلماسی ارائه می‌شود؛ سپس ضروری است برای فهم بهتر موضوع دیپلماسی سایبری، تفکیک و تمایزی بین این مفهوم و سایر مفاهیم مشابه همچون «دیپلماسی الکترونیکی»، «دیپلماسی دیجیتال»، «دیپلماسی رسانه‌ای» و «دیپلماسی عمومی» صورت گیرد. در نهایت و بر مبنای مطالعات موردی، با مطالعهٔ مهم‌ترین ویژگی‌ها و ملاحظات فضای سایبری، یک چارچوب مفهومی سایبری حاوی مقولات و مؤلفه‌ها و اصولی، که در تدوین دیپلماسی سایبری حائز اهمیت است، در قالب الگویی عملی ـ پیشنهادی ارائه خواهد شد.

نویسندگان کتاب بر آن هستند که نظام حکمرانی کشور در خصوص هر یک از مقولات این چارچوب پیشنهادی سایبری باید به یک جمع‌بندی و سیاست واحد (از جمله دارای ایده و گفتمان جدی از موضع مدعی) برسد تا بتواند به صورت منسجم و در قالب الگویی یکپارچه وارد تعامل استراتژیک با طرف‌های خارجی در عرصهٔ منطقه‌ای و بین‌المللی بشود.

تعریف دیپلماسی و انواع آن

دیپلماسی به معنای وسیع آن، هر گونه تلاش برای مدیریت و تطبیق اختلافات از طریق مذاکره و همکاری تعریف شده است.[1] هرولد نیکلسون، در تعریفی کلاسیک، دیپلماسی را برای صورت‌بندی پدیده‌های مختلفی همچون سیاست خارجی، تعامل، ابزارهایی برای ترغیب در مذاکره، یک هنر در مذاکره و نیز بخشی از سرویس خدمات خارجی مورد استفاده قرار داده است[2].

در ادبیات روابط بین‌الملل امروزی، دیپلماسی هستهٔ مرکزی سیاست بین‌الملل و اصلی‌ترین نهاد در تعریف و حفظ «جامعهٔ بین‌الملل» است[3]. از دیدگاه بول، دیپلماسی در واقع نگهبان جامعهٔ بین‌الملل و ضامن حفظ و تقویت آن محسوب می‌شود. از دیدگاه وی، دیپلماسی به طور کلی دارای پنج کارکرد است: ۱. تسهیل ارتباطات در سیاست‌های جهانی، ۲. تسهیل مذاکره دربارهٔ توافق‌ها، ۳. جمع‌آوری اطلاعات (شامل اطلاعات محرمانه و ...) از دیگر کشورها، ۴. اجتناب از اختلافات و برخوردها در روابط بین‌الملل و یا حداقل کاهش آن‌ها، ۵. نماپردازی[4] یک جامعهٔ دُول[5] (نماد جامعهٔ دولت‌ها)[6].

---

1. Wight 1979, p. 89
2. Harold G. Nicolson, 1963
3. Hall, 2006; Neumann, 2002, 2003
4. Symbolize
5. Society of States
6. Bull, 2002

یکی از مهم‌ترین مفروضات تعاریف مختلف از دیپلماسی ـــ حتی در عصر فضای سایبری ـــ این است که کارکردهای فوق تقریباً دست‌نخورده باقی‌مانده‌اند، اما متن[1] سوژه‌ها (بازیگران) و ابژه‌های (موضوعات کاری) آن تغییر پیدا کرده‌اند. بر این اساس، در حوزهٔ فضای سایبری هرچند این کارکردها همچنان پابرجاست، اما دیپلماسی صرفاً به فعالیت گروهی منتخب از مقامات برجستهٔ دولتی، که مهم‌ترین مسائل بین‌المللی را در موقعیت‌های اکازیون (مثلاً به صورت محرمانه، پشت درهای بسته و از مسیرهای مختلف)به مذاکره گذاشته و در مورد آن بحث می‌کنند، اشاره ندارد. دیپلماسی همچنین دیگر صرفاً به روابط بین دولت‌ها و کشورها نمی‌پردازد. در معنای وسیع و جدید آن، باید روابط گسترده‌تر و دیالوگ وسیع‌تری را مدنظر داشت که در آن علاوه بر دولت‌ها، به هویت‌های جدید، نظیر سازمان‌های منطقه‌ای و بین‌المللی (اعم از دولتی و غیردولتی)، شرکت‌های بین‌المللی، بازیگران خُرد و کلان ملی، سازمان‌های حمایتگر، صاحب‌نظران بانفوذ، مالکان شرکت‌های فناوری (از جمله گوگل، فیس‌بوک، توییتر) و ...، توجه می‌کند. دربارهٔ برخی از آن‌ها، از جمله مالکان شرکت‌های فناوری، دشواری کار؛ عدم انطباق «قدرت فزایندهٔ آن‌ها» با منافع ملی هیچ یک از کشورها و دولت‌هاست. به عبارت دیگر، این شرکت‌ها امپراتوری‌های جدیدی هستند که قدرت فزاینده‌شان با هیچ کشور یا دولت خاصی منطبق نیست. آنها، مستقل از نظام‌های سیاسی، بازیگران مستقلی هستند که عمدتاً به دنبال کسب بیشترین سود و حفظ منافع تجاری و اقتصادی خود هستند. همچنین به این موارد، باید ورود دیپلماسی به حوزه‌های سیاسی کم‌سابقه همچون تغییرات اقلیمی، محیط زیست، تروریسم جهانی، فضای سایبری و ... را نیز افزود.

---

1. Context

با توجه به موضوع این نوشتار، که در حوزهٔ دیپلماسی سایبری است، قبل از مفهوم‌پردازی در این زمینه و نیز مروری بر مطالعهٔ موردی سایر کشورها، ابتدا باید به تفاوت دیپلماسی سایبری با سایر مفاهیم و مقولات مشابه همچون دیپلماسی رسانه‌ای، دیپلماسی الکترونیکی، دیپلماسی دیجیتال، دیپلماسی عمومی و .... پرداخت؛ موضوعی که به دلیل امتناع از خلط معنایی آن، از اهمیت بالایی برخوردار است.

- **دیپلماسی رسانه‌ای**

با توسعهٔ رسانه‌ها در اواخر قرن گذشته، دیپلماسی حضور پررنگی در رسانه‌ها پیدا کرد. به عبارت دیگر، با ظهور رسانه‌های نوین، از جمله تلویزیون جهانی، دیگر قدرت به معنای سنتی آن، یا بالاترین مقام بودن به تنهایی، برای اعمال رهبری کفایت نمی‌کرد. در این مقطع، بخش زیادی از ارتباطات سیاسی جهان از طریق رسانه‌ها شکل می‌گرفت و حتی در برخی موارد رسانه‌هایی همچون سی‌ان‌ان نقش میانجیگری مهمی در برخی از مهم‌ترین رخدادهای جهانی ایفا کردند. برای مثال، تأثیر سی‌ان‌ان و نقش این تلویزیون در گفت‌وگوهای صلح خاورمیانه، انعکاس جهانی حوادث میدان «تیان آن من» چین و ... را می‌توان نام برد.

دیپلماسی رسانه‌ای از طریق فعالیت‌های متعدد رسانه‌ای عادی و ویژه توسط دولت‌ها نیز پیگیری می‌شود. استفاده از این کانال‌های رسانه‌ای، به ویژه در مواردی که بین دو طرف روابط رسمی وجود ندارد، همواره اهمیت خاصی دارد. در دیپلماسی رسانه‌ای، انتخاب رسانهٔ مؤثر و اثرگذار نقش بسزایی در موفقیت یا عدم موفقیت در تأمین اهداف دیپلماسی دارد. در بسیاری از کشورها و در مقاطع مختلف، برخی از رسانه‌ها از طریق دسترسی خاصی که به منابع قدرت و اطلاعاتی دارند، جزء کانال‌های ارتباطی و

دیپلماتیک ویژه محسوب می‌شوند. حتی برخی رسانه‌ها به دلایل تاریخی ممکن است از محبوبیت یا قدرت اثرگذاری خاصی در بین محافل قدرت برخوردار باشند که نمونه‌های آن در همهٔ کشورها به وفور یافت می‌شود.

- **دیپلماسی الکترونیکی یا دیپلماسی دیجیتال**

دیپلماسی الکترونیکی[1] که به دیپلماسی دیجیتال یا حتی دیپلماسی کامپیوتری نیز مشهور است، اشاره به استفادهٔ دیپلمات‌ها از ابزارهای دیجیتال (فناوری‌های نوین ارتباطی و شبکه‌های اجتماعی) در حوزهٔ سیاست و دیپلماسی، به خصوص در امور سفارت، دارد. به گفتهٔ تام فلچر[2] دیپلماسی دیجیتال نخستین‌بار در ۱۹۹۴، زمانی که نخست‌وزیر سوئد نخستین ایمیل دیپلماتیک را برای بیل کلینتون، رئیس‌جمهوری وقت آمریکا، ارسال کرد، زاده شد[3].

بسیاری از مباحث صورت‌گرفته در ارتباط با دیپلماسی دیجیتال، به طور فزاینده‌ای بر نقش روبه‌گسترش فناوری در انجام فعالیت‌های دیپلماتیک متمرکزند. در این خصوص، برخی از محققان بر ضرورت انطباق با فناوری‌های جدید به عنوان فاکتور کلیدی در تضمین حاکمیت «قدرت دولت» در یک جهان به شدت «شبکه‌ای‌شده» تأکید می‌کنند[4]. در دیپلماسی دیجیتال، مهم استفاده از فناوری‌های نوین در روابط دیپلماتیک بین کشورهاست و دراین‌باره، «ابزار» مهم‌تر از «هدف» تلقی می‌شود. به عبارت دیگر، صرف‌نظر از هدف و امکان یا امتناع تحقق آن، از ابزار دیجیتال برای برقراری ارتباط استفاده می‌گردد[5].

---

1. E – Diplomacy
2. Tom Fletcher
3. Fletcher, 2016
4. Melissen, 2015; Owen, 2015 and Hocking
5. Sandre, 2015

- **دیپلماسی عمومی**[1]

به موازات دیپلماسی دیجیتال، مفهوم دیگری که همسو و در پیِ آن اهمیت یافت، دیپلماسی عمومی بود. به دنبال جهانی‌سازی و ظهور جامعهٔ اطلاعاتی، قلمرو و مرزهای دیپلماسی و عرصهٔ فعالیت دیپلمات‌ها نیز دچار تحول شد. ضرورت پاسخگویی دیپلمات‌ها از عامه‌های خاص (در اینجا مقامات بالاتر) فراتر رفت و «انقلاب توقعات فزاینده» در افکار عمومی در جامعهٔ به شدت «اطلاعاتی‌شده»، نیز آن‌ها را ملزم به پاسخگویی به عموم مردم ساخت. بسیاری از محققان، توسعهٔ فناوری‌های ارتباطی نوین را به معنای انقلاب در دیپلماسی عمومی تلقی کرده‌اند.

دیپلماسی عمومی یا دیپلماسی مردمی، به هر گونه تلاشی گفته می‌شود که با هدف برقراری ارتباط مستقیم با عامه یا گروه‌های ذی‌نفع خاص در سطوح ملی و منطقه‌ای و بین‌المللی صورت می‌گیرد. در دیپلماسی عمومی، از فناوری‌های نوین ارتباطی برای تسهیل ارتباط با عامه استفاده می‌شود و به این اعتبار، به لحاظ معنایی و مفهومی به دیپلماسی دیجیتال نزدیک‌تر است. امروزه کاربرد و استفاده از فناوری‌های نوین ارتباطی، به خصوص شبکه‌های اجتماعی، برای ارتباط با عامه (اعم از خاص، عمومی، داخلی یا خارجی) به امری رایج تبدیل شده است[2].

استفاده از شبکه‌های اجتماعی در زمینهٔ دیپلماسی عمومی، به خصوص از سال ۲۰۰۶ با ظهور شبکهٔ توییتر، مرسوم و از سال ۲۰۰۹ در مقیاس جهانی اوج گرفت. آنچه امروزه دیپلماسی توییتری[3]، یا توئیپلماسی[4]، یا هشتگ دیپلماسی[5] خوانده می‌شود؛ در واقع به استفادهٔ مقامات و مسئولان سیاسی از شبکه‌های اجتماعی و وبسایت میکروبلاکینگ توییتر اشاره دارد

---

1. Public Diplomcay
2. Melissen, 2007
3. Twitter Diplomacy
4. Twiplomcy
5. Hashtag Diplomacy

که دیپلماسی عمومی را از این طریق توسعه می‌دهند. در این خصوص، شاید بتوان مایکل ا. مک‌فال، سفیر وقت آمریکا در روسیه، را یکی از پیشگامان دیپلماسی توییتری دانست که پس از شروع به کار در روسیه در سال ۲۰۱۱، کار خود را با توئیت به دو زبان انگلیسی و روسی آغاز کرد[1]. استفاده از توییتر در دیپلماسی عمومی در زمان مذاکرات هسته‌ای ایران با عنوان «#IranTalks» و «#IranDeal» به اوج خود رسید[2].

در حال حاضر نیز استفاده از شبکه‌های اجتماعی در زمینهٔ دیپلماسی عمومی بیش از گذشته در همهٔ کشورها رواج یافته است و مشهورترین آن‌ها در حال حاضر، استفادهٔ دونالد ترامپ، رئیس‌جمهوری آمریکا، از توییتر برای بیان افکار و عقاید خود به طور خاص و ارتباط با عموم مردم به طور کل است. در ایران نیز محمدجواد ظریف، وزیر امور خارجه، از این شبکهٔ اجتماعی برای بیان و نشر گستردهٔ پیام‌های دیپلماتیک تهران و ارتباط با افکار عمومی منطقه و بین‌الملل استفادهٔ وسیعی می‌کند.

به صورت تاریخی، رابطهٔ وثیقی بین دیپلماسی و رسانه وجود دارد و همان طور که اشاره شد، دیپلماسی در طول تاریخ همواره تحت تأثیر تحولات رسانه‌ها و فناوری‌های ارتباطی بوده است. آنچه در بالا، هم در دیپلماسی رسانه‌ای، هم در دیپلماسی دیجیتال و هم دیپلماسی عمومی به آن اشاره شد، عمدتاً ناظر بر ابعاد و مجاری دیپلماسی بوده که تحت تأثیر کانال‌های نوین رسانه‌ای قرار گرفته است.

با این حال، نباید از نظر دور داشت که تحولات رسانه‌ای و ظهور سریع فناوری‌های ارتباطی همچنین تأثیرات عمیقی بر کیفیت دیپلماسی، به خصوص از منظر زمان، سرعت و نوع واکنش نیز داشته است. آنچه امروزه تحت عنوان

---

1. Keleman, 2014
2. Landler, 2014

دیپلماسی در زمان واقعی[1] یا دیپلماسی فوری[2] نامیده می‌شود، در واقع ناظر بر انتقادات گسترده از تأخیر و فاصلهٔ زیاد واکنش‌های دیپلماتیک به تحولات سیاسی است که عمدتاً تحت تأثیر رسانه‌های نوین شکل می‌گیرند. برخی از پژوهشگران به خصوص از زمان وقوع بهار عربی و انقلاب‌های موسوم به شبکه‌های اجتماعی، نوعی «پس‌افتادگی» و «تأخیر در واکنش» برای دیپلماسی قائل شده‌اند و معتقدند دلیل این پس‌افتادگی ناشی از ۱. اعتماد بیش از حد به تحلیل‌های نهادهای اطلاعاتی سنتی و معیوب و ۲. ناتوانی در درک و فهم محیط‌های اطلاعاتی جدید بوده و در نتیجه سیاست‌گذاران و تصمیم‌سازان نتوانسته‌اند خود را با سرعت تحولات در متن جامعه همراه سازند[3].

- **امنیت سایبری[4] یا جنگ سایبری**

نخستین رویکرد به فضای سایبری، به خصوص پس از آغاز قرن بیستم، و با توجه به عدم آمادگی کشورها برای مقابله با چالش‌ها و آسیب‌های ظهور فضای سایبری، رویکرد امنیتی ـ دفاعی بوده است. این نوع رویکرد، دقیقاً همان رویکردی است که در ادبیات نظریِ فضای سایبری با مفاهیمی همچون دیپلماسی الکترونیکی یا دیجیتال خلط معنایی پیدا می‌کند.

در دههٔ اول قرن ۲۱ به طور مشخص سه رویداد سایبری موجب شکل‌گیری پارادایم امنیتی ـ دفاعی در ارتباط با فضای سایبری شد: ۱. حملهٔ سایبری به زیرساخت‌های اینترنتی دولت استونی در سال ۲۰۰۷ که بر اثر این حمله، تمامی زیرساخت‌های این کشور به خصوص زیرساخت‌های کلیدی که بر بستر اینترنت فعالیت می‌کردند از کار افتادند. در ارتباط با این حملهٔ سایبری، بیش از همه انگشت اتهام به سوی هکرهای روسی گرفته شد. ۲. در سال

---

1. Real Time Diplomcay
2. Instant Diplomcay
3. Philip Seib, 2012
4. Cyber Security

۲۰۰۸ و حملهٔ روسیه به گرجستان؛ در این زمان، حملات سایبری روسیه به زیرساخت‌های اینترنتی گرجستان پیش از حملهٔ نظامی بود و آثار مخرب‌تری نیز در این کشور بر جای گذاشت. حملهٔ سایبری روسیه به گرجستان در واقع نخستین حمله‌ای بود که در آن از فضای سایبری به عنوان یک نیروی ضربتی[1] علیه کشوری دیگر استفاده شد. ۳. حملهٔ ویروس استاکس‌نت به زیرساخت‌های سایت‌های غنی‌سازی در ایران در سال ۲۰۱۰؛ استفاده از ویروس استاکس‌نت در واقع نخستین تجربهٔ استفاده از سلاح سایبری[2] بود که به طور مستقیم برای تخریب زیرساخت اطلاعاتی سایت‌های غنی‌سازی نطنز در ایران استفاده شد. به دلیل پیچیدگی و حجم تخریب صورت‌گرفته، عمدهٔ کارشناسان اتفاق نظر داشتند که دست‌کم باید یک دولت در پشت طراحی این ویروس و نیز حملهٔ صورت‌گرفته قرار داشته باشد[3]. پس از وقوع این سه رویداد سایبری در دههٔ اول قرن ۲۱، دولت‌ها عمدتاً نقش فعال‌تری برای دفاع از منافع خود در زمینهٔ فضای سایبری در پیش گرفتند.

رویکرد امنیتی به فضای سایبری معلول توسعهٔ فناوری اطلاعات و ارتباطات و وابستگی بیش از پیش کشورها به ساختارهای شبکه‌ای برای ادامهٔ حیات است. در رویکرد امنیت سایبری که معطوف به تجربهٔ زیستهٔ اولیهٔ کشورها و دولت‌ها در مواجهه با فضای سایبری است، مقولات برجسته عبارت‌اند از: «جاسوسی سایبری»، «حملات سایبری»، «جنگ سایبری»، «هک سایبری» و «سانسور یا فیلترینگ». ویژگی دیگر این رویکرد، نگاه معطوف به مسائل و ابعاد داخلی حوزهٔ سایبری است که از جمله شامل اطمینان از حاکمیت ملی کشورها، افزایش ظرفیت‌های سایبری با هدف تسهیل در ارتباطات عمومی، ارتقای مدیریت دولتی در فضای سایبری و همکاری وسیع‌تر با بخش خصوصی، به خصوص در حوزهٔ کارآفرینی و کسب‌وکار، می‌شود.

---

1. Force Multiplier
2. Cyber Weapon
3. Renard, T. (2014)

به طور خاص، ایالات متحده آمریکا نخستین کشوری بود که در سال ۲۰۰۳ نخستین سند «استراتژی امنیت ملی سایبری» خود را تدوین و منتشر کرد. متعاقب آن و تنها در ظرف کمتر از یک دهه، ۳۵ کشور دیگر از جمله انگلستان، روسیه، چین، فرانسه و ... نیز اسناد مشابهی را تدوین و منتشر ساختند که به طور گسترده تحت تأثیر سند منتشرشدهٔ آمریکا قرار داشتند. در ارزیابی و مطالعهٔ لویجیف و هیلی (۲۰۱۲) از اسناد استراتژی امنیت ملی سایبری کشورها، پنج ویژگی شاخص قابل شناسایی است: ۱. فعالیت‌های سایبری نظامی، ۲. مقابله با جرایم سایبری، ۳. اطلاعات یا ضد اطلاعات، ۴. مدیریت بحران امنیت سایبری و حفاظت از زیرساخت‌های حیاتی، ۵. مدیریت اینترنت.[1] این ویژگی‌ها که در واقع وجه مشترک عمدهٔ اسناد استراتژی امنیت ملی سایبری مطالعهٔ آن‌هاست، نشان‌دهندهٔ نوع مواجههٔ اولیهٔ این کشورها با فضای سایبری بود.

ظهور دیپلماسی سایبری

دیپلماسی سایبری مفهومی جدید در ادبیات روابط بین‌الملل محسوب می‌شود که سابقهٔ آن تنها به اواخر دههٔ اول قرن ۲۱ بازمی‌گردد. اگرچه از این مفهوم در سال‌های اولیهٔ قرن ۲۱ نیز استفاده شد، اما در عمدهٔ آن‌ها نوعی خلط معنایی با سایر مفاهیم مشابه (که در بالا به آن‌ها اشاره شد) وجود داشت. برای مثال، در عمدهٔ آن‌ها بر تأثیر اینترنت و فناوری‌های نوین بر اهداف و ابزارها و ساختارهای دیپلماسی تأکید می‌شد[2]. یا در برخی متون دانشگاهی، دیپلماسی سایبری را در مفهوم و شرایط گذار دیجیتال[3] مطالعه می‌کردند و در امتداد دیپلماسی عمومی در عصر دیجیتال می‌دانستند[4]. حتی برخی از آن‌ها از

1. Luiijif and Healey, 2012
2. Potter, 2002
3. Digital Transformation
4. Kleiner, 2008; Weijin Wang, 2015

دیپلماسی سایبری با عنوان دیپلماسی عمومی۲[1] نام بـرده‌انـد کـه بـه اسـتفاده و پذیرش نوآوری‌های فناوری در زمینهٔ ارتباطات و اطلاعات در حوزهٔ دیپلماسـی اشاره دارد[2]. با وجود این، آنچه کمتر به آن توجه مـی‌شـود، فراینـد دیپلماسـی[3] لازم برای مواجهه با ابعاد بین‌المللی موضوعات سایبری است.

جدول شمارهٔ ۱. تفاوت دیپلماسی سایبری با سایر مفاهیم و مقولات مشابه

مفهوم	ابزار	نگاه به فناوری	ملاحظه	طراحان	هدف
دیپلماسی رسانه‌ای	رسانه‌ها	کانال اطلاعاتی یا مبانجی	—	رسانه‌ای‌ها و دیپلمات‌ها	کسب اطلاعات یا انتقال اطلاعات
دیپلماسی الکترونیکی (دیجیتال یا کامپیوتری)	فناوری	نگاه ابزاری مثبت	—	دیپلمات‌ها	تسهیل ارتباط با مخاطب
دیپلماسی عمومی یا مردمی	فناوری	نگاه ابزاری مثبت، برجسته‌سازی مسائل	—	دیپلمات‌ها	تسهیل و گسترش ارتباط با عامه
امنیت سایبری	فناوری و اندیشهٔ دفاعی	نگاه محتاطانه همراه با بدبینی	ملاحظات سیاست داخلی	استراتژیست‌های سایبری و ژنرال‌های سایبری	دفاع در برابر نفوذ فناوری سایبری خارجی
دیپلماسی سایبری	فناوری و اندیشهٔ تعاملی	نگاه ایجابی (مسائل، درک و فهم مسائل، حل مسائل)	ملاحظات سیاست داخلی و سیاست خارجی	استراتژیست‌های سایبری و ژنرال‌های سایبری و دیپلمات‌های سایبری	استفاده از ظرفیت فناوری سایبری برای تعامل استراتژیک دوجانبه، چند جانبه، بین‌المللی

1. Public Diplomacy 2.0
2. Tatar and Others, 2014
3. Diplomatic Process

مؤسسهٔ غرب ـ شرق[1] در نخستین تعریف در ارتباط با این موضوع بیان می‌دارد که «به دلیل سطوح بالای ارتباط بین‌المللی در دنیای سایبری، برای امنیت سایبری باید رویکرد جدیدی در ابعاد بین‌المللی در نظر گرفته شود. بنابراین در ارتباط با حوزهٔ سایبر، به جای تمرکز انحصاری بر دفاع سایبری یا جنگ سایبری، بسیار مهم است که دیپلماسی سایبری را توسعه دهیم»[2].

دیپلماسی سایبری به لحاظ نظری در مراحل اولیهٔ تکوین قرار داشته و هنوز یک تعریف جامعی از آن، که مورد اقبال عمومی باشد، ارائه نشده است. با این حال می‌توان آن را در دو سطح دنبال کرد: ۱. در معنای وسیع می‌تواند بر ادامهٔ دیپلماسی سنتی و کارکردهای مختلف آن با استفاده از سازوکارهای جدید در فضای سایبری دلالت داشته باشد. به این اعتبار تمامی فعالیت‌های جاری و ساری در دیپلماسی سنتی را می‌توان با اتخاذ مکانیسم‌های جدید در بستر فضای سایبری نیز دنبال کرد. ۲. دیپلماسی سایبری به معنای استفاده از منابع دیپلماتیک و انجام کارکردهای دیپلماسی برای حفظ و تأمین منافع ملی در ارتباط با فضای سایبری در بُعد منطقه‌ای و بین‌المللی آن است. در این سطح، با توجه به مرزبندی‌های جدید در منافع و منابع قدرت و ثروت، این امر مستلزم ورود سریع و بهنگام و قدرتمندانه به این حوزه است تا بتوان بر اساس منافع ملی، جایگاهی برای «ایفای نقش و بازیگری» ایجاد کرد.

---

1. East-West Institute
2. Gady and Austin, p. 1

برخی تعاریف موجود در زمینهٔ دیپلماسی سایبری
دیپلماسی سایبری عبارت است از: تحول دیپلماسی که تأثیر نوآوری‌های حوزهٔ فناوری اطلاعات و ارتباطات (ICT) را به سیاست خارجی و دیپلماسی پیوند می‌دهد.[1]
دیپلماسی سایبری در قرن بیست‌ویکم فقط به معنای مدیریت جهانی بدون مرز نیست، بلکه در صورت اتصال یکپارچه می‌تواند بهترین عملکرد را داشته باشد. این جهان ــ که کاملاً به معاملات مالی پایدار و تجارت جهانی وابسته است ــ در صورت مورد حمله قرار گرفتن از طریق فضای سایبری، کارایی مناسبی نخواهد داشت.[2]
دیپلماسی سایبری عبارت است از: استفاده از ابزارها و طرز تفکر دیپلماتیک برای حل چالش‌های فضای سایبری یا دست‌کم مدیریت آن‌ها. به عبارت دیگر، دیپلماسی سایبری به معنای اعمال دیپلماسی در فضای سایبری است.[3]
دیپلماسی سایبری از طریق مشارکت‌های راهبردی با سایر کشورهای سراسر جهان در زمینهٔ تقویت اقدامات جمعی و همکاری در برابر تهدیدهای مشترک، ایجاد ائتلافات همسو در مواجهه با موضوعات مهم سیاست‌گذاری، به اشتراک‌گذاری اطلاعات و طرح‌های ملی و مقابله با عوامل خرابکار عمل می‌کند.[4]
دیپلماسی سایبری را می‌توان تلاشی در زمینهٔ تسهیل ارتباطات، مذاکرات مربوط به توافق‌ها، و جمع‌آوری اطلاعات از سایر کشورها به منظور جلوگیری از ایجاد اصطکاک در فضای سایبری دانست. همچنین به عنوان اقداماتی برای استفاده از منابع و عملکردهای دیپلماتیک به منظور تأمین

1. Melissen, 2005
2. Gady and Austin, 2010
3. Riordan, 2019
4. Painter, 2018

منافع ملی در حوزهٔ فضای سایبری در نظر گرفته می‌شود. این اقدامات شامل امنیت سایبری، جرایم سایبری، اعتمادسازی، آزادی بین‌المللی و حکمرانی اینترنت است.[1]
دیپلماسی سایبری عبارت است از: بکارگیری ابزارها و تفکر دیپلماتیک برای حل چالش‌های فضای سایبری. استفاده از ابزارهای دیجیتالی برای ارتقای برنامه‌های دیپلماتیک گسترده‌تر و بهره‌برداری از فنون و طرز تفکر دیپلماتیک به منظور تجزیه و تحلیل و مدیریت چالش‌های فضای سایبری، فعالیت‌هایی جداگانه اما مرتبط‌اند.[2]

به اعتبار این دو سطح، فضای سایبری «بستری» محسوب می‌شود که باید در آن و برای تأمین منافع ملی خود دنبال تعریف و تعیین مکانیسم‌ها و سازوکارهای جدید هم در سطح ملی و هم در سطح منطقه‌ای و جهانی بود. تعریف این مکانیسم‌ها و سازوکارها مستلزم فهم چند مؤلفه به شرح ذیل است:

نخستین نکتهٔ حائز اهمیت در ارتباط با دیپلماسی سایبری «هدف» است که مهم‌تر از «ابزار» آن تلقی می‌شود. در واقع دیپلماسی سایبری عبارت است از: استفاده از «ابزارهای دیجیتال» به اضافهٔ «تفکر و اندیشهٔ دیپلماتیک» برای حل موضوعات و مسائلی که در ارتباط با فضای سایبری و در روابط بین کشورها وجود دارد (تأکید بر هدف). در این فرایند ابزارهای دیجیتال یاری می‌رسانند تا موضوعات دیپلماتیک بیشتر و بهتر برجسته شوند، ضمن آنکه تفکر دیپلماتیک نیز کمک می‌کند تا مسائل و موضوعات فضای سایبری بهتر تحلیل و مدیریت شوند.

---

1. Retrived from https://medium.com/ on 21 of January 2020.
2. Retrived from http://www.themarketforideas.com/ on 21 of January 2020.

دومین نکتهٔ حائز اهمیت در دیپلماسی سایبری بحث «انعطاف‌پذیری» است که در مقایسه با دیپلماسی سنتی بیشتر نمایان می‌شود. دیپلماسی سایبری علاوه بر ابعاد و ملاحظات داخلی، باید معطوف به ابعاد و ملاحظات خارجی نیز باشد، زیرا عرصهٔ آن فرامرزی است. برخلاف رویکردهای اولیه که عمدتاً حالت درون‌مرزی و تدافعی (دفاع در برابر نفوذ فناوری خارجی) داشت، رویکرد جدید به دنبال تعامل استراتژیک با طرف‌های خارجی است تا علاوه بر دفاع از خود، بتوان در عرصهٔ منطقه‌ای و بین‌المللی نیز نفوذ کرد. برای دستیابی به این هدف نمی‌توان با همان پیش‌فرض‌ها و ملاحظات سیاست داخلی، به مواجهه و پیگیری مسائل و موضوعات در عرصهٔ منطقه‌ای و بین‌المللی پرداخت. اساساً در عرصهٔ سیاست بین‌الملل (منطقه‌ای و بین‌المللی)، قدرت و ارزش منابع قدرت و ثروت و نفوذ کشورها به طور قابل‌توجهی کاهش یافته و به دلیل مواجهه با سایر قدرت‌ها و بازیگران بین‌المللی تقلیل می‌یابد. به عبارت دیگر، برخلاف عرصهٔ داخلی، در عرصه‌های خارجی یک دولت یا حاکمیت تنها بازیگر تلقی نمی‌شود، بلکه سایر بازیگران (اعم از دولت‌های خارجی یا ذی‌نفعان دیگر) نیز حضور دارند که ممکن است از قدرتِ تأثیرگذاریِ بیشتری نیز برخوردار باشند. لذا لازمهٔ آن، قابلیت «انعطاف‌پذیری» در مبانی دیپلماسی سایبری است.

سومین نکتهٔ حائز اهمیت، تعدد بازیگران و ذی‌نفعان در عرصهٔ دیپلماسی سایبری است. اگرچه در معنای کلاسیکِ مفهوم دیپلماسی، دولت‌ها عمدتاً به دنبال چارچوبی رسمی‌اَند که در آن فقط دولت‌ها و یا سازمان‌های رسمیِ بین‌المللی (همچون سازمان ملل) طرف ارتباط و تعامل دربارهٔ موضوعات مختلف به حساب می‌آیند، اما در مقولهٔ دیپلماسی سایبری این امر نه‌تنها امکان‌پذیر نیست، بلکه حتی ممکن است نقش سایر

بازیگران از دولت‌ها بیشتر و فراگیرتر باشد. برای مثال، در مقولهٔ «حکمرانی اینترنت»، انجمن معماری اینترنت[1] و کارگروه مهندسی اینترنت[2] نقش و قدرتشان به مراتب از بسیاری از دولت‌ها بیشتر است. یا در مقولهٔ «حقوق بشر» ممکن است قدرت یک نهاد یا انجمن بین‌المللی به مراتب بیشتر و بانفوذتر از رأی یک یا دو کشور در مجمع عمومی سازمان ملل و یا شورای حقوق بشر سازمان ملل باشد.

به اعتبار نکاتی که در بالا به آن اشاره شد، تمامی تلاش‌های بازیگران و ذی‌نفعان مختلف را، که به طور مستمر برای مدیریت تضادها و کشمکش‌های جاری و ساریِ فضای سایبری در سطح منطقه‌ای و بین‌المللی روی می‌دهد، می‌توان دیپلماسی سایبری نامید. اگر هدف اصلی از دیپلماسی ایجاد تفاهم و فهم مشترک از طریق گفت‌وگو یا مذاکره است، در نتیجه اولویت دیپلماسی سایبری نیز تلاش برای ایجاد فهم مشترک منطقه‌ای و بین‌المللی در زمینهٔ مهم‌ترین موضوعات فضای سایبری از طریق مذاکره یا گفت‌وگو بین تمامی بازیگران آن است.

- **تقاطع نهاد جامعهٔ بین‌الملل با جامعهٔ جهانی**

پیش‌تر گفته شد که دیپلماسی سایبری فراتر از مفهوم سنتی دیپلماسی تحت تأثیر پیشرفت خیره‌کنندهٔ فناوری به سطوح غیررسمی و غیردولتی نیز کشانده می‌شود. برای فهم بهتر این تحول، اینکه چگونه و چه موقع و کجا از این نوع دیپلماسی می‌توان در سطوح غیررسمی و غیردولتی استفاده کرد، باید بین دو مفهوم کلیدی جامعهٔ بین‌الملل[3] و جامعهٔ جهانی[4] تفاوت قائل شد.

---

1. Internet Architecture Board (IAB)
2. Internet Engineering Task Force (IETF)
3. International Society
4. World Society

به طور سنتی، دیپلماسی موضوع اساسی جامعهٔ بین‌الملل بوده است. با این حال، مفهوم جدیدی که متقارن با این مفهوم و به دنبال ظهور فضای سایبری شکل گرفته، مفهوم جامعهٔ جهانی است که به همان اندازه بااهمیت است. در حالی که اولی در مورد نهادینه ساختن هویت و علایق مشترک در بین دولت‌هاست، ایجاد و حفظ سازمان‌ها، قواعد و ارزش‌های مشترک را در مرکز «روابط بین‌الملل» قرار می‌دهد؛ اما دومی افراد و سازمان‌های غیردولتی و در نهایت، جمعیت جهانی را ــ به عنوان یک کل ــ نقطهٔ ثقل ترتیبات و هویت‌های اجتماعی جهانی می‌داند و توفّق بر سیستم دولت را در مرکز روابط بین‌الملل قرار می‌دهد. ایان کلارک برای فهم تمایز این دو بر آن است که جامعهٔ جهانی به جهان اجتماعی غیردولتی اشاره دارد که شکل فراملّیتی دارد و از «جامعهٔ دولت‌ها» (جامعهٔ بین‌الملل) قابل تفکیک است. هر دوی این‌ها، فضای عمومی بین‌الملل را شکل می‌دهند و شیفت دائمی بین آن‌ها، همراه با پیامدهای خاص خود در جریان است. به اعتقاد کلارک با توجه به تحلیل و تفکیک فوق و نیز تحولات سریعی که در حوزهٔ فناوری سایبری در حال وقوع است، می‌توان گفت که دیپلماسی سایبری در تقاطع جامعهٔ بین‌الملل و جامعهٔ جهانی سیال است با این تأکید که شیفت دائمی به نفع دومی در جریان است، به این معنا که روزبه‌روز بر نقش و بازیگری فعالان و ذی‌نفعان غیردولتی افزوده می‌شود.[1]

1. Clark, 2007

دیپلمات‌های رسمی کی و چگونه به دیپلماسی سایبری ورود پیدا می‌کنند

به رغم تعدد بازیگران عرصهٔ دیپلماسی سایبری، ورود دیپلمات‌ها به مقولات سایبری در عرصهٔ منطقه‌ای و بین‌المللی همچنان اجتناب‌ناپذیر می‌نماید. به لحاظ نظری سه نوع نقش و بازیگری برای دیپلمات‌های رسمی در عرصهٔ سایبری مفروض است:

۱. نقش همه‌جانبه و منحصربه‌فرد: دیپلماسی سایبری می‌تواند تمامی آن توسط دیپلمات‌ها در جلسات و نشست‌های کاری دوجانبه (روابط متقابل کشورها) یا حتی بین‌المللی و چندجانبه (نشست‌های بین‌المللی و منطقه‌ای همچون سازمان ملل و ...) دنبال شود. فراتر از مفهوم سنتی آن، این نوع دیپلماسی همچنین می‌تواند شامل تعامل و همکاری دیپلمات‌ها با بازیگران غیردولتی (برای مثال، رؤسا و مسئولان شرکت‌های بزرگ شبکه‌ها همچون فیس‌بوک، گوگل و ...)، شرکت‌های پیشروی فناوری (همچون اپل، سامسونگ و ...) و یا حتی سازمان‌های مدنی قدرتمند باشد. انتخاب نخستین سفیر در کمپانی گوگل از سوی کشور دانمارک مصداق بسیار روشن و آشکار این نوع تعامل به شمار می‌رود. این دیپلماسی همچنین می‌تواند در خدمت صداهای به اصطلاح «خفته» در دیگر کشورها از طریق فناوری نیز باشد؛ همانند نقشی که از طریق فناوری به معترضان ناراضی در کشور چین، روسیه و... داده می‌شود.[1] در سال‌های اخیر نیز ایالات متحده آمریکا به راه‌اندازی سفارتخانهٔ مجازی برای ارتباط با ایرانیان اقدام نموده و حتی یکی از دیپلمات‌های بلندپایهٔ خود را مسئول برقراری این ارتباط کرده که مصداق مورد اخیر نقش و کارکرد دیپلمات‌ها در دیپلماسی سایبری است.

۲. نقش ثانویه یا با تأخیر: دیپلمات‌ها حتی ممکن است تنها در بخشی از فرایند دیپلماسی سایبری ورود پیدا کنند و یا ورود متأخر داشته باشند. در این باره نکتهٔ حائز اهمیت در ارتباط با دیپلماسی سایبری می‌تواند تفکیک حوزه‌های صرفاً «فنی» در تعاملات خارجی و بین‌المللی کشورها از حوزه‌های «سیاسی» باشد که عموماً دیپلمات‌ها نقش کمتری در آن ایفا می‌کنند. به طور کلی، در روابط بین

1. Owen, 2015

کشورها همواره تعاملات فنی (به خصوص بین وزرای همتا در امور مخابرات، اقتصاد، حتی دادگستری) برقرار است که صرفاً به مسائل و مباحث فنی می‌پردازند تا مسائل سیاسی؛ در این حالت، دیپلمات‌ها عموماً نقش کمتری ایفا می‌کنند. عمدهٔ طرف‌های مذاکره و تعامل در این گونه موارد تکنسین‌های حرفه‌ای یا فن‌سالاران هستند. با این حال، در ارتباط با همین موضوعات و بحث‌های فنی نیز همواره برخی «حوزه‌های خاکستری» وجود دارد که موجب تنش در روابط بین کشورها شده و در نهایت به ورود دیپلمات ــ هرچند با تأخیر ــ به این مباحث برای حل‌وفصل نهایی آن‌ها منجر شده است.

۳. عدم ایفای نقش: در مواردی همچون تصمیمات کمپانی‌های بزرگ ممکن است نتوان هیچ نقشی برای دیپلمات‌های رسمی قائل شد؛ برای مثال، تصمیم شبکه‌های اجتماعی فیس‌بوک و توییتر برای محدودسازی فعالیت‌های سیاسی کاربران خود، از جمله مصادیق این حالت تلقی می‌شود. همه روزه در کمپانی‌های بزرگ آی‌تی، همچون اپل، سامسونگ، مایکروسافت و ...، و نیز پایگاه‌های اینترنتی، همچون گوگل، یاهو، اماس‌ان و ...، سیاست‌ها و تصمیماتی در قالب ادغام، انحصار، توسعه، نوآوری و ... صورت می‌گیرد که عمدتاً خارج از دایرهٔ اختیارات و تصمیمات دیپلماسی رسمی است و نمی‌توان در آنها نقشی برای دیپلمات‌های قائل شد. با این حال، آثار این تصمیمات نه فقط در سطوح ملی، بلکه در عرصهٔ منطقه‌ای و بین‌المللی نیز اجتناب‌ناپذیر است.

- **چالش‌های اساسی دیپلماسی سایبری، مسائل و ملاحظات**

فضای سایبری همسو و به موازات جهان واقعی در شکل‌گیری روابط بین‌الملل و نظام حاکم بر آن نقش ایفا کرده و به خوبی توانسته است خود را در ساختار روابط قدرت و منابع و منافع مرتبط با آن جای دهد. امروزه بسیاری از فعالیت‌های ضروری ملت‌ها و حکومت‌ها به خصوص در ابعاد تصمیم‌سازی و اجرا در فضای سایبری صورت می‌پذیرد. در مجموع، با توجه به «شیفت» امور و مسائل دنیای واقعی به دنیای سایبری از یک سو و

شکل‌گیری جامعهٔ جهانی جدید که در بالا به آن اشاره شد از سوی دیگر، طبیعی است که در تمام حوزه‌ها ــ از جمله در سیاست ــ نیز امور و مسائل مربوطه به فضای سایبری منتقل شود. این شیفت ماهوی در عمل به ایجاد دو چالش اساسی در حوزهٔ روابط بین‌الملل منجر شده که عبارت‌اند از: ۱. امکان تسرّی اصول، قوانین، معاهدات، توافقات و مؤلفه‌های دنیای واقعی به دنیای سایبری. به عبارت دیگر، یکی از مهم‌ترین چالش‌هایی که باید به آن پاسخ داد این است که «آیا نظم دنیای واقعی به فضای سایبری قابل تعمیم و تسرّی است؟». ۲. در صورت امکان، میزان پایداری این تسرّی ــ با توجه به سرعت تحولات تکنولوژیکی ــ به چه میزان خواهد بود؟

پاسخگویی به این دو چالش اساسی در فضای سایبری در زمینه‌های مختلف، از جمله «اعتمادسازی» بین بازیگران؛ «برقراری امنیت» برای همهٔ بازیگران، یا برخی از آنان، یا هیچ کس؛ امکان تسرّی و اِعمال قوانین بین‌المللی فعلی یا ضرورت تدوین قوانین بین‌المللی جدید؛ ناتوانی در شناسایی منشأ و مبدأ تهدیدات جدید؛ معضل انتساب حملات سایبری و ...، به دلیل پیچیدگی ماهیت این فضا و نوع روابط حاکم بر آن امکان‌پذیر نیست. پیچیدگی این فضا وقتی محسوس‌تر می‌شود که به نقش «امپراتوری‌های جدید» (همچون برندهای جهانی آی‌تی همانند مایکروسافت، گوگل، فیس‌بوک و ... که قدرتشان گاهی از مجموع بسیاری از کشورها بیشتر است) و تلاش آن‌ها در مدیریت این فضا نیز مورد لحاظ قرار گیرد.

هلی تییرما کلار در مقاله‌ای با عنوان «دیپلماسی سایبری: موضوعات، چالش‌ها و اهداف»، مهم‌ترین مسائلی که در دیپلماسی سایبری با آن مواجهیم را بدین گونه ذکر می‌کند: ۱. امنیت بین‌المللی و اعتمادسازی در فضای سایبری، ۲. ابتکارات بین‌الملل در مواجهه و مقابله با جرایم سایبری،

۳. ظرفیت‌سازی در حوزهٔ فضای سایبری، ۴. تعریف حقوق بشر در فضای سایبری، ۵. بحث بر سر مدیریت و حکمرانی اینترنت.[1]

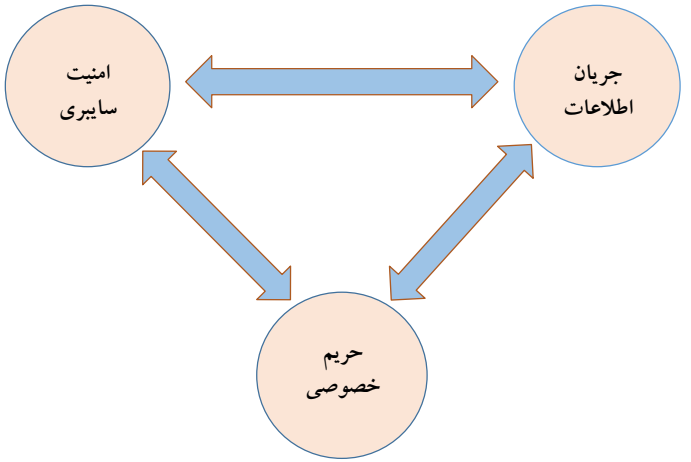
همان طور که ملاحظه می‌شود، در این تقسیم‌بندی امنیت سایبری بین‌المللی تنها یک مقوله تلقی می‌شود و تأکید بیشتر بر اعتمادسازی منطقه‌ای و بین‌المللی، ظرفیت‌سازی و توسعه، تعریف ارزش‌ها و هنجارهای بین‌المللی و نیز تعریف استانداردهای رفتاری در حوزهٔ مدیریت و حکمرانی اینترنتی است. این طبقه‌بندی اگرچه خروجی تفکر لیبرالیستی است، اما بدون شک بخش مهمی از مفهوم‌پردازی‌ها و نظرورزی‌ها در زمینهٔ دیپلماسی سایبری را شامل می‌شود. در مقابل، تقسیم‌بندی‌های مشابهی نیز از سوی تفکر غیرسرمایه‌داری (به خصوص کشورهای چین و روسیه) نمایندگی می‌شوند که علاوه بر اشتراک در برخی مقولات فوق، بر موضوع حاکمیت ملی در فرایندها و روندهای دیپلماسی سایبری در سطوح منطقه‌ای و بین‌المللی تأکید دارند. این دو نوع تفکر در عمل به ظهور دو نوع رویکرد غالب در دیپلماسی سایبری منجر شده که در ادامه به آن پرداخته می‌شود.

- **دو رویکرد عمده در دیپلماسی سایبری و مصداق‌های آن**

همان طور که در بالا به آن اشاره شد، موضوعات غالب در دیپلماسی سایبری، شامل امنیت سایبری، جرایم سایبری، اطمینان‌بخشی[2]، حریم خصوصی، آزادی جریان اطلاعات و حکمرانی یا مدیریت اینترنت است. این مفاهیم حوزه‌های متداخل فضای سایبری را در ارتباط با حاکمیت کشورها در عرصهٔ بین‌المللی تشکیل می‌دهند که به طور خلاصه می‌توان در قالب نمودار ذیل، به صورت تعامل سه‌گانهٔ امنیت سایبری، حریم خصوصی و جریان آزاد اطلاعات خلاصه کرد.

---

1. Tiirmaa-Klaar, 2013
2. Confidence-Building



شکل شمارهٔ ۱. رویکردهای جاری به دیپلماسی سایبری در کشورهای مختلف

با توجه به ویژگی‌ها و ملاحظات فضای سایبری و نیز اولویت‌های کشورهای مختلف از منظر حاکمیتی، می‌توان دو نوع رویکرد را از یکدیگر تفکیک کرد که وجه ممیزهٔ آن‌ها نوع برخوردشان با ۱. نحوهٔ جریان اطلاعات (آزاد یا محدود) و ۲. امکان تسرّی قوانین بین‌المللی به فضای سایبری است.

رویکرد نخست: این رویکرد بیشتر مربوط به کشورهای لیبرال غربی به رهبری آمریکاست. در این رویکرد دو محور قابل توجه است: اولویت دادن به جریان آزاد اطلاعات و اتخاذ رویکرد چندذی‌نفعی (دولت‌ها، کسب‌وکارها، جامعهٔ مدنی و ...)؛ تأیید قوانین بین‌المللی فعلی که قابلیت تسرّی و حاکمیت بر فضای سایبری را دارد.

رویکرد دوم: این رویکرد بیشتر متعلق به کشورهای حوزهٔ شرق به رهبری کشورهای روسیه و چین است. در این رویکرد نیز، دو محور قابل‌توجه است: ۱. اولویت به کنترل داخلی (ملی) بر اساس اصل حاکمیت (تقویت قانون‌گذاری، درخواست منابع بر اساس قوانین ملی)؛ ۲. حساسیت به اعمال قوانین بین‌المللی فعلی در فضای سایبری و تأکید بر ضرورت مقررات‌گذاری جدید.

در چارچوب دو رویکرد فوق، کشورهای زیادی تلاش کرده‌اند تا اسنادی با عنوان دیپلماسی سایبری تدوین کنند. با این حال، تعداد بسیار معدودی از آن‌ها همانند ایالات متحده آمریکا، دارای استراتژی مدون مجزایی در ارتباط با روابط بین‌الملل دارند. ایالات متحده خود به رغم اینکه نخستین سند سایبری را در سال ۲۰۰۳ تدوین و اعلان کرده بود، نخستین‌بار در ۲۰۱۱ و سپس در ۲۰۱۷، سند استراتژی بین‌المللی فضای سایبری[1] خود را منتشر کرد و در آن بر ابعاد بین‌المللی فضای سایبری متمرکز شد. پس از آمریکا، اتحادیهٔ اروپا (۲۰۱۳، ۲۰۱۵)،[2] روسیه، ژاپن (۲۰۱۳)،[3] چین، استرالیا (۲۰۱۶)[4] و ... نیز تلاش‌هایی برای تدوین دیپلماسی سایبری داشته‌اند. با توجه به اهمیت تجارب سایر کشورها در حوزهٔ دیپلماسی سایبری، در ادامه

1. US International Strategy for Cyberspace
2. Council Conclusions on Cyber Diplomacy
3. Japan's International Strategy on Cyber Security Cooperation
4. Cyber Security Strategy Committed to Establish an International Engagement Strategy

به صورت خلاصه، مقولهٔ دیپلماسی سایبری در کشورهای آمریکا، اتحادیهٔ اروپا، ژاپن، روسیه و چین بررسی می‌شود.

نگاهی به دیپلماسی سایبری آمریکا

آمریکا با توجه به اشرافیت راهبردی در حوزهٔ فناوری اطلاعات و ارتباطات، به خصوص از طریق اینترنت، پیشتاز کشورهای جهان در حوزهٔ دیپلماسی سایبری محسوب می‌شود. در خصوص دیپلماسی سایبری، آمریکا نخستین‌بار در ۲۰۱۱ سند استراتژی بین‌المللی فضای سایبری را منتشر ساخت. در این سند در حالی که چند اولویت ملی نظیر اقتصاد، حفاظت از شبکه، اعمال قانون، فعالیت‌های نظامی، حکمرانی اینترنت، توسعهٔ بین‌المللی و آزادیِ اینترنت مطرح شده بود، بر دیپلماسی و دفاع و توسعه[1] به عنوان سه ستون اصلی برای دستیابی به این اولویت‌های تأکیدشده بود.[2]

سپس کنگرهٔ این کشور در سپتامبر ۲۰۱۷، قانون دیپلماسی سایبری را تصویب و دولت این کشور در نوامبر همان سال آن را رسماً ابلاغ کرد. همچنین دولت ایالات متحده آمریکا در فوریهٔ ۲۰۱۸ نیز سند سایبری خود تحت عنوان دیپلماسی سایبری آمریکا در عصر تهدیدهای روزافزون[3] را رسماً ابلاغ نمود که حاوی دیدگاه‌ها، استراتژی‌ها و اهداف راهبردی این کشور در حوزهٔ سایبری در عرصهٔ ملی و منطقه‌ای و بین‌المللی است. مبنای قانون دیپلماسی سایبری آمریکا، که به تلاش‌های جهانی این کشور برای حفظ سلطه و اشرافیت راهبردی‌اش در حوزهٔ اینترنت و شبکه توجه دارد،

1. Diplomacy, Defense & Development (3D)
2. White House, 2011
3. U.S. Cyber Diplomacy in an Era of Growing Threats

عبارت است از: تلاش برای حفظ و گسترش زیرساخت اطلاعاتی و ارتباطی باز، مطمئن، امن و تعاملی در راستای تأمین امنیت ملی و نیز علایق اقتصادی آمریکا.

قانون دیپلماسی سایبری آمریکا همچنین دربردارندهٔ استراتژی‌های عملیاتی دربارهٔ این امور است: ۱. حفظ و گسترش ارزش‌ها، هنجارها و قوانین این کشور در فضای سایبری در مقیاس جهانی، ۲. اقدامات بازدارنده در برابر تهدیدات حملات سایبری از طریق تسرّی قوانین بین‌المللی فعلی به فضای سایبری، ۳. پاسخ عملیاتی به حملات صورت‌گرفته به منافع این کشور در حوزهٔ سایبری.[1]

نکتهٔ حائز اهمیت در ارتباط با سند دیپلماسی سایبری آمریکا هدایت و رهبری این کشور در همکاری بین‌المللی جهانی با هدف نهادینه‌سازی و اعمال ارزش‌های جهانی (آمریکایی) در حوزهٔ سایبری است. دراین‌باره، همچنین دیپلماسی سایبری آمریکا قانون «جنگ نظامی» را به حوزهٔ سایبری، به خصوص حملات سایبری که زیرساخت‌های کلیدی این کشور را هدف می‌گیرد یا جاسوسی تجاری از آن را به دنبال دارد، قابل تعمیم می‌داند.

با هدف پیگیری دیپلماسی سایبری در عرصهٔ منطقه‌ای و بین‌المللی، وزارت خارجهٔ ایالات متحده آمریکا همچنین نخستین کشوری است که به صورت خاص ادارهٔ هماهنگ‌کنندهٔ امور سایبری[2]را ــ منحصراً به عنوان هماهنگ‌کنندهٔ امور سایبری ــ راه‌اندازی کرده است. این وزارتخانه همچنین کریستوفر پینتر[3]را به عنوان نخستین «دیپلمات سایبری» منصوب

1. U.S. Cyber Diplomacy in an Era of Growing Threats, 2018
2. Office of the Coordinator for Cyber Issues
3. Christopher Painter (www.cisac.fsi.stanford.edu)

کرد که در واقع نخستین دیپلمات سایبری در جهان نیز محسوب می‌شود.[۱]

ادارهٔ هماهنگ‌کنندهٔ امور سایبری وزارت خارجهٔ آمریکا به طور مشخص دارای پنج کارکرد کلیدی است: ۱. هماهنگی و مدیریت تعاملات جهانی وزارت امور خارجهٔ آمریکا در امور سایبری، ۲. خدمت به عنوان رابط وزارت امور خارجه با کاخ سفید و سایر ادارات و سازمان‌های فدرال در حوزهٔ سایبری، ۳. مشاوره دادن به وزیر و معاونان وزارت امور خارجه در زمینهٔ مسائل سایبری و تعاملات خارجی آمریکا در این زمینه، ۴. خدمت به عنوان رابط وزارت امور خارجه با بخش‌های خصوصی و عمومی در زمینهٔ مسائل سایبری، ۵. هماهنگ‌کنندهٔ امور دفاتر و نمایندگی‌های منطقه‌ای وزارتخانهٔ مرتبط با امور سایبری.[۲]

نگاهی به دیپلماسی سایبری اتحادیهٔ اروپا

اگرچه سابقهٔ تلاش‌های دیپلماتیک اتحادیهٔ اروپا در حوزهٔ فضای سایبری را می‌توان به تلاش‌های این اتحادیه در تأسیس آیکان[۳] و نیز گفتمان «حکمرانی اینترنت» در دههٔ ۱۹۹۰ معطوف دانست، اما دورنمای دیپلماسی سایبری این اتحادیه در ۲۰۱۳، با تدوین سند «استراتژی امنیت سایبری» اتحادیهٔ اروپا نمایان شد که در آن چشم‌انداز سیاست فضای سایبری بین‌المللی منسجم[۴] با

---

۱. لازم به توضیح است که پس از روی کار آمدن دونالد ترامپ در ایالات متحده آمریکا، هم نقش و وظایف «ادارهٔ هماهنگ‌کنندهٔ امور سایبری» این کشور تقلیل یافت و هم کریستوفر پینتر از مقام خود به عنوان نخستین دیپلمات ارشد آمریکا در حوزهٔ سایبری از کار بر کنار شد. جزئیات این تغییرات به تفصیل در فصل چهارم آمده است.

2. US State Department Website, 2017

3. Internet Corporation for Assigned Names and Numbers (ICANN)

4. Coherent International Cyber-Space Policy

پنج اولویت مشخص شد: ۱. ترویج و دفاع از حقوق بشر در فضای سایبری، ۲. ارزش‌های رفتاری و اعمال قوانین امنیت بین‌المللی در حوزهٔ فضای سایبری، ۳. حکمرانی اینترنت، ۴. ارتقای رقابت و شکوفایی در فضای سایبری[1] ۵. ظرفیت‌سازی و توسعه در حوزهٔ فضای سایبری.

این سند همچنین تأکید می‌کند که اتحادیهٔ اروپا اولویت‌های فوق را با تأکید بر اصول مسلّم باز بودن اینترنت، آزاد بودن اینترنت، تلاش برای تدوین استانداردهای رفتاری، قابلیت تسرّی حقوق و قوانین بین‌المللی فعلی در حوزهٔ فضای سایبری دنبال خواهد کرد.

در ارتباط با اولویت‌های فوق و نیز اصول مسلّم اتحادیهٔ اروپا ـــ موضوعی که مستقیماً به دورنمای دیپلماسی سایبری اتحادیهٔ اروپا اشاره دارد ـــ این است که از دیدگاه این اتحادیه، این اولویت‌ها به خاطر ماهیت، حوزه و گسترهٔ متقاطع آن از طریق تعامل استراتژیک با شرکای اصلی و سازمان‌های بین‌المللی (به خصوص سازمان ملل متحد، اتحادیهٔ اروپا، ناتو، و ....) دنبال و پیگیری خواهد شد.

در ارزیابی اتحادیهٔ اروپا، ایالات متحده آمریکا، کانادا، مکزیک، برزیل، کرهٔ جنوبی، آفریقای جنوبی و ژاپن به عنوان شرکای استراتژیک تلقی می‌شوند و گفت‌وگوهای دوجانبه‌ای با آن‌ها در ارتباط با فضای سایبری صورت گرفته و پیشرفته‌ترین آن نیز مربوط به ایالات متحده است. در کنار این کشورها، روسیه و چین نیز به عنوان دو بازیگر اصلی و جدی (عموماً به عنوان دو منبع اصلی تهدیدات سایبری) در نظر گرفته می‌شوند که برای گفت‌وگوی انتقادی با آن‌ها در حوزهٔ فضای سایبری و تعاملات بین‌المللی تلاش‌هایی نیز صورت گرفته است[2].

---

1. Enhancing Competiveness and Prosperity 2. Danca, 2015

در ارزیابی سند استراتژی امنیت سایبریِ اتحادیهٔ اروپا باید گفت که به رغم روشن بودن اصول و کلیات آن، هنوز هم برخی از مهم‌ترین ابعاد بین‌المللی آن و اینکه رویّهٔ این اتحادیه در مذاکره و تعامل استراتژیک با شرکای بین‌المللی چطور خواهد بود، چندان روشن نیست. به خصوص نوع و نحوهٔ واکنش این اتحادیه زمانی که به صورت کلی یا اینکه هر یک از اعضای آن در معرض حملهٔ سایبری قرار گیرد چطور خواهد بود، دارای ابهام‌هایی جدی است. این اتحادیه در ژوئن ۲۰۱۷، از بسته‌ابزار دیپلماسی سایبری[1] رونمایی کرد و کوشید تا در آن، نوعی واکنش منسجم و جمعیِ[2] اعضای اتحادیهٔ اروپا را در صورت مواجهه با حملات سایبری مخرب پیش‌بینی کند. در این بسته اگرچه با توجه به ماهیت، مقیاس، پیچیدگی، گستردگی و میزان تأثیر حملات صورت‌گرفته، برخی اقدامات بازدارنده یا محدودکننده پیش‌بینی شده، با این حال ماهیت اقدامات پیش‌بینی‌شده در عمل تعیین و مشخص نشده است. به طور کلی، این بسته بیشتر شبیه یک مانیفست است تا فراهم‌کنندهٔ برخی اقدامات عملی مشخص و روشن.

نگاهی به دیپلماسی سایبری در ژاپن

برای ژاپن به عنوان یک کشور توسعه‌یافته که از هر لحاظ، به ویژه اقتصادی و امنیتی و نظامی، به شدت به شرایط جهانی و سیاست بین‌الملل وابسته است، رویکرد صرف دفاعی در ارتباط با فضای سایبری نمی‌تواند تأمین‌کنندهٔ منافع ملی و منطقه‌ای و بین‌المللی این کشور باشد. از این رو، به عنوان یک بازیگر جهانی، ژاپن نیز رویکردی فعالانه‌تر در ارتباط با فضای

1. Cyber Diplomacy Toolbox
2. Collective Response of EU Member States

سایبری و استفاده از ظرفیت‌ها و پتانسیل آن برای پیشبرد اهداف منطقه‌ای و بین‌المللی خود اتخاذ کرده است.

با توجه به اهمیت فضای سایبری و نقش بی‌بدیل آن در روابط بین‌الملل، وزارت خارجهٔ ژاپن موظف به مشارکت و هدایت مباحث جهانی در خصوص چگونگی تضمین سه مفهوم مرکزی ایمن،[1] آزادی[2] و عدالت[3] در فضای سایبری است. در این زمینه، وزارت امور خارجهٔ ژاپن موظف است که از طریق همکاری با سایر وزارتخانه‌ها و نهادهای متعلق و نیز ذی‌نفعان بخش خصوصی سیاست خارجی این کشور در این زمینه، فضای سایبری را بر مبنای سه پایهٔ اصلی ذیل به پیش برد:

۱. قانون‌گذاری و اطمینان از حاکمیت قانون[4] در فضای سایبری: تشویق و ترویج اعمال قوانین بین‌المللی موجود در فضای سایبری و تلاش برای قانون‌گذاری جدید و لازم در زمان‌های صلح.

۲. توسعهٔ اقدامات اطمینان‌بخش[5] در زمینهٔ فضای سایبری: این اقدامات اطمینان‌بخش به خصوص باید در زمان‌های صلح صورت گیرد تا از برخورد و تضاد سایبری جلوگیری و اجتناب به عمل آید. این اقدامات اطمینان‌بخش همچنین از طریق ثبات و شفافیت در حوزهٔ فضای سایبری نیز می‌تواند تشدید شود.

۳. همکاری در زمینهٔ بسترسازی و ظرفیت‌سازی در زمینهٔ فضای سایبری: بسترسازی و ظرفیت‌سازی در زمینهٔ فضای سایبری برای توسعهٔ منابع انسانی ضروری است. در این رویکرد همچنین هر گونه «حفرهٔ امنیتی» در سایر کشورها، ریسکی بزرگ برای کل جهان از جمله ژاپن محسوب می‌شود. بر

---

1. Security
2. Freedom
3. Fair
4. Rule of Law
5. Confidence Building Measures (CBMs)

مبنای سه پایهٔ فوق، ژاپن دو اولویت در زمینهٔ دیپلماسی سایبری مدنظر دارد:

اولویت نخست، اطمینان از همکاری سایبری در منطقهٔ آسیا ـ اقیانوسیه، به عنوان حوزهٔ پیرامونی این کشور؛ به خصوص اینکه با هدف تداوم توسعه و تضمین ثبات در منطقه، اقدامات اطمینان‌بخش باید به صورت مداوم صورت پذیرد.

اولویت دوم، همکاری با جامعهٔ بین‌الملل (سازمان‌های جهانی) و نیز کشورهایی که در زمینهٔ فضای سایبری، ارزش‌های مشترکی با کشور ژاپن دارند. این همکاری قبل از هر چیز باید معطوف به اطمینان از حاکمیت قوانین بین‌المللی فعلی در عرصهٔ فضای سایبری و نیز حرکت به سوی تدوین قوانین مطابق با تغییر و تحولات روز باشد.[1]

با توجه به دو اولویت بالا، ژاپن در حال حاضر گفت‌وگوهای دوجانبه‌ای در زمینهٔ فضای سایبری با یازده کشور جهان، از جمله آمریکا، روسیه، فرانسه، آلمان، انگلستان، استرالیا، هندوستان، کرهٔ جنوبی، استونی، اوکراین و اسرائیل دنبال می‌کند. ضمن آنکه به طور هم‌زمان گفت‌وگوهایی با اتحادیهٔ اروپا و اتحادیهٔ آسه‌آن[2] و نیز گفت‌وگوهایی سه‌جانبه با محوریت «ژاپن ـ چین و کرهٔ جنوبی» و نیز «ژاپن ـ آمریکا و کرهٔ جنوبی» دنبال می‌کند.

در سطوح جهانی نیز ژاپن در قالب نهادها و نشست‌های جهانی، همچون کارشناسان دولتیِ سازمان ملل که از ۲۰۰۴ آغاز به کار کرده، جی ۷[3] که کارگروه سایبریِ آن از ۲۰۱۶ شروع به فعالیت کرده، جی ۲۰[4]، کنفرانس جهانی در زمینهٔ فضای سایبری[5] نقش فعالی در زمینهٔ فضای سایبری در مقیاس منطقه‌ای و جهانی ایفا می‌کند.

---

1. The Government of Japan, 2015
2. Association for Southeast Asian Nations (ASEAN)
3. Group of 7 (G7)
4. Group of 20 (G20)
5. Global Conference on Cyber Space

نگاهی به دیپلماسی سایبری روسیه

روسیه بر اساس تجربهٔ جنگ سرد، فضای سایبری و بستر اینترنت را زمینهٔ جدید جنگ با ایدئولوژی دنیای غرب می‌داند. با همین نگاه، برخلاف آمریکا که به دنبال تعمیم و تحمیل قوانین و ارزش‌های ملی خود در فضای سایبری در مقیاس جهانی است، بیشتر به دنبال تدوین استانداردها و کدهای رفتاری در فضای سایبری از طریق مشارکت بین‌المللی است.

مهم‌ترین دغدغهٔ روسیه در دیپلماسی سایبری، اصل حاکمیت ملی کشورها و اطمینان از عدم مداخلهٔ سایر کشورها، به خصوص از طریق حملات سایبری به بنیان‌ها و ساختارهای نظام سیاسی و اقتصادی و اجتماعی این کشور، است. از نظر این کشور تدابیر مشارکتی‌ای که موجب افزایش ثبات و امنیت در حوزهٔ امنیت فناوری سایبری می‌شوند عبارت‌اند از: ۱. هنجارها، قوانین و اصول رفتار مسئولانهٔ دولت‌ها، ۲. اقدامات داوطلبانه (نه اجباری) به منظور ارتقای شفافیت، ۳. اطمینان‌بخشی و اعتمادسازی بین کشورها، ۴. ظرفیت‌سازی و توسعه در این حوزه. در واقع از منظر دیپلماسی سایبری روسیه، تنها از طریق این تدابیر مشارکتیِ تمامیِ کشورهاست که می‌توان به فناوری اطلاعات و ارتباطات «مسالمت‌آمیز»، «ایمن»، «باز» و «مشارکتی» امیدوار بود. به همین دلیل، روسیه در مقابل دیپلماسی سایبری کشورهای غربی که فقط به امنیت سایبری، یعنی ضرورت محافظت از نرم‌افزار و سخت‌افزار و همچنین اطلاعات کاربر در برابر خرابکاری، اشاره دارد بر «امنیت اطلاعات بین‌المللی» تأکید دارد. این مفهوم نه‌تنها امنیت سایبری را در بر می‌گیرد، بلکه بر جلوگیری از سوءاستفاده از فناوری‌های اطلاعات و ارتباطات در زمینهٔ اهداف سیاسی (همانند آنچه به انقلاب‌های رنگی در

اقمار شوروی سابق یا بهار عربی منجر شد) نیز تمرکز دارد.[1]

همچنین از منظر دیپلماسی سایبری روسیه، قوانین بین‌المللی به ویژه منشور سازمان ملل متحد، در فضای سایبری قابلیت تسرّی دارد و این مسئله دولت‌ها و حاکمیت‌ها را متعهد می‌سازد که ۱. از قلمرو آن‌ها نباید برای اقدامات سایبری غیرقانونی در سطح بین‌المللی استفاده شود؛ ۲. نباید فعالیت‌های حوزهٔ فناوری اطلاعات و ارتباطات را که از روی عمد به زیرساخت‌های مهم آسیب می‌رسانند آگاهانه پشتیبانی کنند؛ ۳. به دنبال جلوگیری از گسترش فناوری‌های مخرب و اعمال خرابکارانهٔ پنهانی باشند.

با توجه به ملاحظات فوق، روسیه دو رویکردِ عمده را در دیپلماسی سایبری خود به طور هم‌زمان به پیش می‌برد:

۱. رویکرد چندجانبه: سازمان ملل متحد و سازمان همکاری شانگهای دو محور اصلی تلاش‌های بین‌المللی روسیه برای پیشبرد اهداف دیپلماسی سایبری این کشور محسوب می‌شوند. در سپتامبر ۲۰۱۱، چهار کشور از اعضای سازمان همکاری شانگهای ــ روسیه، چین، تاجیکستان و ازبکستان ــ یک آیین‌نامهٔ اخلاقی بین‌المللی برای امنیت اطلاعات ارائه دادند[2]. چند روز بعد، روسیه نیز پیش‌نویس «کنوانسیون بین‌المللی امنیت اطلاعات» را به سازمان ملل ارائه داد. هر دو متن بازتاب‌دهندهٔ تحول تفکر سیاست خارجی روسیه در حوزهٔ سایبری هستند. پیش‌نویس آیین‌نامهٔ اخلاقی و پیش‌نویس کنوانسیون ۲۰۱۱ ارائه‌شدهٔ روسیه بر اهمیت حاکمیت دولت در فضای سایبری تأکید دارند. علاوه بر این، پیش‌نویس کنوانسیونْ کشورها را ترغیب به تأیید این امر می‌کند که جنگ اطلاعاتی تهاجمی، جنایتی علیه صلح و امنیت بین‌المللی است، و از آن‌ها می‌خواهد که فناوری‌های اطلاعاتی و ارتباطی به منظور

1. Popescu and Secrieru, 2018

2. UN Doc A/66/359

مداخله در امور داخلی سایر کشورها را به کار نگیرند.[1] برخی تهدیدهای اصلی ذکرشده در این متن عبارت‌اند از: اقداماتی که با هدف تضعیف سیستم سیاسی، اقتصادی و اجتماعی دولتی دیگر صورت می‌گیرد، و نیز مبارزات روان‌شناختی‌ای که برای بی‌ثبات کردن جامعهٔ یک کشور به وجود می‌آید. این پیش‌نویس به توضیح چگونگی جلوگیری از درگیری‌های نظامی و همچنین استفادهٔ شبکه‌های تروریستی از اینترنت و جرایم سایبری می‌پردازد.

۲. رویکرد دوجانبه: به طور هم‌زمان، مسکو به دنبال شبکه‌ای از توافقات دوجانبه با هدف اطمینان‌بخشی و تقویت اعتماد بین خود با سایر شرکای منطقه‌ای و بین‌الملل است. در این مسیر در ۲۰۱۳، روسیه نخستین توافق‌نامهٔ سایبری دوجانبه را با **ایالات** متحده امضا کرد. این توافق‌نامه به منظور تبادل اطلاعات بین تیم‌های ملی پاسخگویی به فوریت‌های رایانه‌ای و ایجاد خطوط ارتباطی فوری مربوط به حوادث سایبری و کانال‌های تبادل اطلاعات حوادث بین مراکز کاهش خطر هسته‌ای، عمدتاً بر ابعاد و جنبه‌های فنی همکاری متمرکز بود. مسکو امیدوار بود که این اقدام گامی اولیه برای رسیدن به یک پیمان بسیار جامع با آمریکا باشد، اما درگیری‌های اوکراین در سال ۲۰۱۴، موجب نافرجام ماندن این برنامه‌ها شد. با این حال، روسیه همچنان به تلاش‌های خود برای عادی‌سازی روابط خود، به خصوص در حوزهٔ فضای سایبری، ادامه داده است. در ۲۰۱۷، مسکو به واشینگتن پیشنهاد داد تا توافق‌نامهٔ دوجانبه‌ای دربارهٔ جلوگیری از فعالیت‌های نظامی خطرناک در فضای سایبری امضا کند. پاسخ ایالات متحده آمریکا تا به حال واضح نبوده است؛ واشینگتن ابتدا با مذاکرات موافقت کرد، اما درست یک روز قبل از آغاز توافق‌نامه در پایان فوریهٔ ۲۰۱۸ در ژنو، آن را به تعویق انداخت. همچنین

1. Russian Ministry of Foreign Affairs, 2011

در ۲۰۱۷، مسکو به واشینگتن پیشنهاد داد که توافق‌نامهٔ عدم مداخله در امور سیاسی یکدیگر را امضا کند. با این حال دولت آمریکا از پیگیری این طرح نیز خودداری کرد. سفیر آمریکا در مسکو، جان هانتسمن[1] در مارس ۲۰۱۸ اعلام کرد که واشینگتن ممکن است مجدداً به مذاکره در مورد مسائل سایبری با مسکو تمایل داشته باشد، مشروط بر اینکه هیچ گونه مداخله‌ای در انتخابات نوامبر صورت نگیرد. اما مقامات روسی با قاطعیت مداخلهٔ مسکو در سیاست داخلی آمریکا را انکار می‌کنند و بنابراین تمایل ندارند حتی دربارهٔ پیشنهاد ضمانت یک‌طرفهٔ مبنی بر عدم مداخلات آتی وارد مذاکره شوند.

به موازات کشور آمریکا، روسیه نیز تلاش‌هایی برای همکاری سایبری با کشورهای آلمان، فرانسه، اسرائیل، کرهٔ جنوبی و ژاپن داشته است اما تمامی این تلاش‌ها عمدتاً، به دلیل سوءظن کشورهای غربی به اهداف روسیه و نیز اتهاماتی که مبنی بر دخالت‌های سایبری روسیه در امور کشورهای غربی می‌شود، ناکام بوده است. با این حال، از سال ۲۰۱۵ این کشور توانسته توافق‌نامه‌های دوجانبه‌ای را در زمینهٔ اعتمادسازی و همکاری در فضای سایبری با چین، هندوستان، آفریقای جنوبی، بلاروس و کوبا منعقد کند.

نگاهی به دیپلماسی سایبری چین

چین نیز همانند روسیه در سال‌های اخیر از موضع دفاعی و واکنشی در ارتباط با فضای سایبری گذار و به خصوص در دورهٔ ریاست‌جمهوری شی جین‌پینگ، سیاست فعالانه‌تری در زمینهٔ فضای سایبری اتخاذ کرده است.

چین با توجه به رشد اقتصادی اخیر و افزایش چشمگیر سرمایه‌گذاری در زیرساخت‌های کشورهای مختلف در اقصی نقاط جهان، رویکرد تهاجمی‌تری

1. Jon Huntsman

را هم برای توسعهٔ نفوذ بین‌المللی خود و هم برای خنثی‌سازی سیاست‌های مقابله‌جویانهٔ رقبای ایدئولوژیک اتخاذ کرده است. این رویکرد را می‌توان در یک استراتژی سه‌وجهی به شرح ذیل صورت‌بندی کرد: ۱. تهاجمی؛ از طریق نفوذ در زیرساخت‌های اطلاعاتی و ارتباطی کشورهای رقیب، به خصوص آمریکا و اروپا. این سیاست به طور خاص به دنبال توسعهٔ توانمندی‌ها و ظرفیت‌های تهاجمی با هدف جاسوسی سایبری، خنثی‌سازی حملات سایبری و رسیدن به درجه‌ای از اقتدار سایبری است که بتواند سیستم‌های انفورماتیک و زیرساخت‌های ارتباطی و اطلاعاتی رقبای خود را در هر لحظه‌ای که اراده نماید فلج کند. ۲. تجاری ـ اقتصادی؛ از طریق سرمایه‌گذاری گسترده در زیرساخت‌های کشورها و مناطق هدف به خصوص اروپا، آفریقا، خاورمیانه، آسیای میانه و آمریکای لاتین. این سیاست که به طور خاص از طریق برنامهٔ مشهور جادهٔ ابریشم جدید موسوم به «یک کمربند و یک جاده» دنبال می‌شود به دنبال ایجاد نوعی وابستگی سایبری کشورهای هدف به خود از طریق جایگزینی فناوری چینی با فناوری غربی (به خصوص آمریکایی) است. ۳. استانداردسازی؛ از طریق مشارکت جدی در تعریف استانداردهای فناوری در نرم‌افزار، سخت‌افزار و شبکه‌های مدرن. این سیاست به طور خاص از طریق حضور پُرتعداد و مؤثر تیم‌های سیاسی ـ فنی در نشست‌ها و همایش‌های فنی تعیین استانداردهای فناوری (به خصوص در زمینهٔ فناوری نسل پنجم و نیز هوش مصنوعی) در سطوح منطقه‌ای و جهانی دنبال می‌شود.[1]

مهم‌ترین دغدغهٔ چین در دیپلماسی سایبری، به ویژه از منظر حکمرانی داخلی، به رسمیت شناختن اصل حق «حاکمیت سایبری» است. حاکمیت سایبری از نظر نظام حکمرانی چین به معنای احترام گذاشتن به حق هر

1. Segal, 2018

کشور برای انتخاب مسیر توسعهٔ اینترنت، انتخاب سبک و الگوی مدیریت اینترنت و انتخاب سیاست‌های عمومی در ارتباط با اینترنت در داخل کشور است. سویهٔ دیگر این اصل، مخالفت چین با هر گونه اقدامی است که حاکمیت ملی این کشور را از طریق شبکه (اینترنت یا فضای سایبری) به چالش بکشد.[1] بر مبنای این دغدغه، چین دسته‌بندی جامعی از انواع تهدیدات و چالش‌های سایبری ارائه می‌دهد که در رأس آنها، الف: چالش‌های ناشی از سیاست‌های مقابله‌جویانه آمریکا، ب: تهدید صلح سایبری و احتمال وقوع جنگ تمام‌عیار سایبری در جهان و ج: تهدید ناشی از گروه‌های شرور شامل تروریسم[2]، جدایی‌طلبی[3] و افراط‌گرایی[4] قرار دارند.

چین در چارچوب دیپلماسی سایبری و با هدف دستیابی به اهداف سه‌گانهٔ فوق و نیز پاسخگویی به تهدیدات فوق‌الذکر، هفت راهبرد عملیاتی را به طور هم‌زمان در عرصهٔ منطقه‌ای و بین‌المللی پیش می‌برد که شامل موارد ذیل می‌شوند: ۱. نهادینه ساختن مقولهٔ «امنیت اطلاعات» در عرصهٔ بین‌المللی، ۲. هنجارمندی‌سازی رفتار دولت‌ها در عرصهٔ سایبری، ۳. ابتکار کنفرانس جهانی اینترنت و تقابل آن با کنفرانس لندن، ۴. مقابله با تروریسم سایبری، ۵. سرمایه‌گذاری تجاری ـ اقتصادی در حوزهٔ فناوری اطلاعات و ارتباطات در اقصی‌نقاط جهان، ۶. مشارکت گسترده در استانداردسازی در حوزهٔ فناوری‌های سایبری و ۷. ترویج صلح سایبری از طریق رویکردهای دوجانبه و چندجانبه.

به لحاظ عملیاتی، چین دیپلماسی سایبری خود را از طریق مشارکت فعال در گفت‌وگوهای بین‌المللی، به خصوص از طریق مشارکت در گروه

---

1. Woods, 2017
2. Terrorism
3. Separatism
4. Extemism

کارشناسان دولتی سازمان ملل[1] و نیز سازمان همکاری شانگهای،[2] به پیش می‌برد. به موازات آن، چین گفت‌وگوهای دوجانبه‌ای نیز با کشورهای پیشرو در عرصهٔ سایبری، همچون ایالات متحده آمریکا، انگلستان، اتحادیهٔ اروپا و نیز روسیه، داشته است که موفق‌ترین آن‌ها، امضای توافق‌نامهٔ سایبری با کشور روسیه بوده است.

همچنین وزارت امور خارجهٔ چین از سال ۲۰۱۳، مقولهٔ دیپلماسی سایبری را به عنوان یک دستورالعمل جدید کاری برای دولت این کشور، به رسمیت شناخت و بر اساس همین دستورالعمل، دفتر دیپلماسی عمومی[3] این وزارتخانه به ادارهٔ دیپلماسی عمومی،[4] برای پیشبرد اهداف دیپلماسی سایبری این کشور در سه سطحِ وزارت امور خارجه، سایر ادارات و سازمان‌های دولتی و جامعهٔ مدنی چین، ارتقا یافت.[5]

چارچوب مفهومی دیپلماسی سایبری: پیشنهاد الگوی عملی دیپلماسی سایبری در ایران

بوک فضای سایبری را یک «عرصهٔ عمومی» می‌داند که دارای منافع مشترک جهانی است و تمامی دولت‌ها یا ملت‌ها به آن دسترسی قانونی و حقوقی دارند. از این منظر، فضای سایبری یک عرصهٔ عمومی جهانی شبیه دریاهای آزاد، آسمان و فضای بیرون از زمین ـ جو است. از این رو، نیازمند و مستلزم حداقل قانون و قانون‌گذاری (توافق یا اجماع جهانی) به منظور استفاده یا

1. UN's Group of Government Experts (GGE)
2. Shanghai Cooperation Organization (SCO)
3. Division of Public Diplomacy
4. Office of Public Diplomacy
5. Zhao, 2013

بهره‌برداری از آن و نیز اجتناب از برخورد یا تضاد دربارهٔ آن است.[1] هنری کیسینجر (۲۰۱۴) فقدان دیپلماسی را برای فضای سایبری مضر می‌داند، اما فراتر از آن، هشدار می‌دهد که این فقدان، نظم جهانی را بر هم خواهد زد[2]. به این اعتبار، فضای سایبری ترکیب پیچیده‌ای از موضوعات و مسائل و چالش‌هاست که ابعاد و زوایای داخلی و خارجی بسیاری دارد. در واقع همین ابعاد و زوایای خارجی است که هم موضوعات و مقولات مربوط را پیچیده می‌سازد و هم چگونگی ورود و تعامل دستگاه دیپلماسی به آن و بازیگری در کنار سایر بازیگران و ذی‌نفعان را تعیین می‌کند. به طور مشخص، فضای سایبری حوزه‌ای جهانی است که اتباع و شهروندان جهانی را به انحای مختلف به یکدیگر وصل و نوعی تعامل (اشتراک) و اصطکاک (تضاد) بین آن‌ها ایجاد می‌کند.

اگرچه ممکن است مسیر دیپلماسی در زمینهٔ فضای سایبری طولانی و پرفرازونشیب باشد، اما اجماعی جهانی وجود دارد که تنها راه دستیابی به توافق و نیز اجتناب از برخورد، دیپلماسی و تعامل دیپلماتیک است. با مفروض گرفتن این اصل، مسئلهٔ اصلی این است که دیپلماسی بر مبنای چه چیزی؟ مهم‌ترین شاخص‌ها و مؤلفه‌ها و اصول این دیپلماسی که قرار است مبنای تعامل دیپلماتیک قرار گیرد، کدام‌ها هستند؟ برای تدوین این دیپلماسی، چه مفاهیم و مؤلفه‌هایی باید در نظر گرفته شود؟

یک چالش اساسی و عمدهٔ دیگری نیز دراین‌باره وجود دارد که عبارت است از موازنه‌بخشی بین چالش‌های ملاحظات سیاست داخلی و چالش‌های ملاحظات سیاست خارجی. در حوزهٔ مسائل و چالش‌های داخلی، مسئلهٔ اصلی حاکمیت ملی است. صرف‌نظر از اینکه فضای سایبری امتداد دنیای واقعی یا دنیایی کاملاً متفاوت از آن است، موضوع حاکمیت ملی و

1. Buck, 2012
2. Kissinger, 2014

چالش‌هایی که در سطوح داخلی برای آن ایجاد می‌شود قابل انکار نیست. در حوزهٔ مسائل و ملاحظات خارجی، موضوعات اصلی منافع قدرت‌های جهانی، تضاد ارزش‌ها و استانداردهای جهانی و ظهور بازیگران جدید با منافع و منابع متضاد است که در بسیاری از موارد امکان دارد در تضاد کامل با حاکمیت ملی کشورها از منظر بیرونی (دوگانه یا تضاد جهانی ـ ملی) باشد.

به رغم همهٔ این ملاحظات، با توجه به اهمیت جهانی فضای سایبری به عنوان یک عرصهٔ مشترک و تأثیر آن بر روابط بین‌الملل، تمامی کشورها ناگزیر از تدوین چارچوبی از مقولات و مؤلفه‌های حوزهٔ سایبری (در نظر و عمل) هستند تا بر اساس آن بتوانند در عرصهٔ جهانی نقش ایفا کنند. در واقع بدون داشتن یک چارچوب مفهومی از مقولات حوزهٔ سایبری، که در آن به خوبی نظرورزی صورت گرفته و صورت‌بندی عملیاتی از تعاریف و اصول و منافع حاصل شده باشد، نمی‌توان در این حوزه وارد تعاملات منطقه‌ای و بین‌المللی شد.

با مطالعهٔ اسناد و منابع علمی منتشرشده در ارتباط با فضای سایبری و نیز ارزیابی رویکردهای ممکن به فضای سایبری (دو رویکرد کلان و تجربهٔ سایر کشورها که در بالا به آن پرداخته شد) می‌توان چارچوب (جدول مقولات حوزهٔ سایبری) زیر را مبنای رویکرد کشورها به فضای سایبری، هم در بُعد داخلی و هم در بعد بین‌المللی، دانست. این چارچوب قطعاً کامل نیست، اما فهرستی از مهم‌ترین مفاهیم، اصول و مقولات برای اندیشیدن به دست می‌دهد. در واقع، نوع مواجههٔ کشورها به هر یک از عناصر و مفاهیم این چارچوب، تعریفی که از آن ارائه می‌دهند، مواضعی که در قبال هر یک اتخاذ می‌کنند، موقعیت و مواضع کشورها را در دیپلماسی سایبری از یکدیگر متمایز می‌کند.

جدول شمارهٔ ۲. مقولات و مؤلفه‌های مهم در دیپلماسی سایبری[۱]

جرایم سایبری/ دادگاه سایبری	اساساً تعریف نظام حکمرانی سایبری کشور از جرم سایبری چیست؟ وضعیت جرایم سایبری در کشور از جمله آسیب‌ها، بزه‌ها، ناهنجاری‌ها و ... به چه میزان است؟ چه مکانیسم‌هایی برای رصد و مقابله با آن‌ها وجود دارد؟ در ارتباط با جرایم سایبری بین‌المللی چطور؟ فراتر از آن، در نظام حکمرانی سایبری کشور باید مرز قضایی[۲] تعیین نمود تا بر اساس آن حدّ و حدود ورود دستگاه قضایی به حوزهٔ سایبری، اعم از داخل و خارج از کشور، مشخص گردد.
دسترسی سایبری	این مقوله ناظر بر حق مصرف‌کننده در دسترسی یا دستیابی به سطح اطلاعات، خدمات و شبکه‌هاست. اینکه نظام حکمرانی سایبری به چه میزان حق مصرف‌کننده برای دسترسی به اطلاعات، خدمات و شبکه‌ها (اعم از داخلی و خارجی) را به رسمیت می‌شناسد.
داده‌ها و درجهٔ وابستگی سخت‌افزار/ نرم‌افزاری سایبری	اصولاً نگاه نظام حکمرانی سایبری به مقولهٔ «داده»ها در فضای سایبری چیست؟ این مقوله از منظر امنیت داده‌ها (اینکه داده‌ها و اطلاعات باید کجا ذخیره شوند ـــ حکمرانی داده)، موضوع سخت‌افزار (امکان استقلال یا وابستگی سخت‌افزاری در حوزهٔ سایبری تا چه میزان و در کجا مجاز است؟)، نرم‌افزار (امکان استقلال یا وابستگی نرم‌افزاری در حوزهٔ سایبری تا چه میزان و در کجا مجاز است؟) و کاربران (موضع نسبت به کاربران داخلی و خارجی) بسیار حائز اهمیت است.

۱. در تدوین مقولات این جدول، علاوه بر تحقیق در ادبیات نظری و مطالعات موردی که در فصل‌های این کتاب به آن‌ها اشاره شد، از تکنیک هم‌افزایی فکری در جلسات بحث متمرکز (Brain Storming) استفاده شده است.

2. Jurisdiction Border

جریان اطلاعات	این مقوله ناظر بر حق تولیدکنندهٔ محتواست. موضع نظام حکمرانی سایبری دربارهٔ این موضوع چیست؟ آیا آزادی مطلق را به رسمیت می‌شناسد یا معتقد به نوع مرزبندی و محدودیت در تولید و مصرف محتواست؟ تا چه حد سیاست‌ها در این زمینهٔ باز یا بسته یا محدود است؟
حکمرانی اینترنت	اساساً نظام حکمرانی سایبری موضعش در برابر حکمرانی اینترنت چیست؟ آیا به یک‌جانبه‌گرایی معتقد است یا چندجانبه‌گرایی؟ آیا معتقد به حاکمیت کشورها بر اینترنت است یا حاکمیت شرکت‌های بین‌المللی و یا حتی سازمان‌های جهانی را به رسمیت می‌شناسد؟ در خصوص مدیریت ترافیک داده‌ها چطور؟ آیا ارائه‌دهندگان خدمات اینترنتی در مورد کیفیت انتقال داده‌ها در بستر اینترنت بی‌طرف است؟
قابلیت تسرّی قوانین فعلی	از منظر نظام حکمرانی سایبری، آیا قوانین فعلی و جاری در عرصهٔ بین‌الملل قابلیت تسرّی به عرصهٔ سایبری را دارد؟ یا فضای سایبری را به عنوان یک مقولهٔ مستقل و جداگانه مستلزم قوانین بین‌المللی جدید می‌داند؟ آیا قوانین فعلی برای فضای سایبری مکفی است؟
حریم خصوصی	نظام حکمرانی سایبری به چه میزان حریم خصوصی کاربران (اعم از افراد) را در فضای سایبری به رسمیت می‌شناسد. فراتر از آن، چه مکانیسمی برای دفاع از حریم خصوصی افراد در برابر انواع سوءاستفاده‌های تجاری، سیاسی، اجتماعی و ... از حریم خصوصی کاربران و شهروندان خود دارد. آیا نظام حکمرانی مخالفتی با استفادهٔ گوگل از اطلاعات شخصی کاربران ایرانی اینترنت در تبلیغات تجاری دارد؟

اعتمادسازی/ عدم تخاصم (صلح سایبری)	مکانیسم نظام حکمرانی برای اعتمادسازی در حوزهٔ سایبری چگونه است؟ آیا الگویی برای پیمان عدم تخاصم سایبری به صورت دوجانبه، چندجانبه یا حتی با سازمان‌های غیررسمی و غیردولتی وجود دارد؟ اصول و مبانی آن‌ها چه هستند؟ نیز، شرکای اصلی برای اعتمادسازی یا عدم تخاصم چه کسانی هستند؟
بخش خصوصی	آیا نظام حکمرانی سایبری، بخش خصوصی داخلی یا خارجی را به عنوان یک بازیگر در فضای سایبری به رسمیت می‌شناسد یا صرفاً معتقد به حاکمیت دولتی در این فضاست؟ اگر بخش خصوصی رسمیت دارد، مکانیسم فعالیت آن چگونه است؟
ذی‌نفعان داخلی	آیا نظام حکمرانی سایبری، ذی‌نفعان داخلی از جمله سمن‌ها، نهادهای غیردولتی، گروه‌ها و اقلیت‌ها را در فضای سایبری به رسمیت می‌شناسد؟ اگر این بخش رسمیت دارد، مکانیسم فعالیت آن‌ها در این حوزه چگونه است؟
ذی‌نفعان خارجی	اساساً نظام حکمرانی سایبری به چه میزان نقش و بازیگری ذی‌نفعان و بازیگران خارجی در عرصهٔ فضای سایبری را به رسمیت می‌شناسد؟ (این بازیگران لزوماً طرف‌های رسمی و شناخته‌شدهٔ خارجی نیستند).
بازدارندگی و پاسخ به حملات سایبری	اصولاً نظام حکمرانی سایبری ما به چه میزان بازدارنده است؟ استراتژی نظام حکمرانی برای مواجهه با حملات سایبری چیست؟ آیا اساساً امکان حملات سایبری متقابل وجود دارد؟ در صورتی که حملات سایبری صورت گیرد، استراتژی پاسخ، نوع و درجهٔ آن چیست؟
زیرساخت‌های کلیدی	این مقوله بسیار مرتبط با امنیت سایبری است. آیا نظام حکمرانی سایبری دسته‌بندی مشخصی از زیرساخت‌های کلیدی اطلاعاتی و شبکه دارد؟ مثلاً، کدام‌یک از این زیرساخت‌های اطلاعاتی خط قرمز نظام حکمرانی سایبری محسوب می‌شوند و هر حملهٔ سایبری به آن تحمیل نمی‌شود؟

کسب‌وکار و راه‌اندازی مناطق آزاد سایبری	آیا نظام حکمرانی سایبری مؤلفه‌های جدید اقتصادی و کسب‌وکار در حوزهٔ فضای سایبری را به رسمیت می‌شناسد؟ آیا مکانیسمی برای تعامل دولت ـ کسب‌وکارهای جدید اندیشیده شده است؟ تعریف قلمرو فعالیت‌های اقتصادی در عرصهٔ سایبری، تعریف فعالیت‌های اقتصادی سایبری مجاز و غیرمجاز، موضوع مالکیت در ارتباط با فعالیت‌های اقتصادی سایبری، تعریف مناطق آزاد سایبری، و ... از جمله مهم‌ترین محورهای این حوزه است. برای مثال، موضوع رمز ارزها، دیتا ماینینگ، استارت‌آپ‌های سایبری و ... . این مقولات همچنین پیامدهایی دیگری نیز دارند که از جمله می‌توان به مقولهٔ بیمهٔ کسب‌وکارهای سایبری، حقوق بازنشستگی و ... آن‌ها اشاره کرد.
حقوق بشر	مفهوم مرکزی دیگر در دیپلماسی سایبری مفهوم حقوق بشر است که عمدتاً در زمینهٔ سیاست نظام حکمرانی سایبری در ارتباط با سایر مقولات نیز چالش‌برانگیز شده است. با توجه به ظرفیت‌های فضای سایبری، هم در تکثرگرایی و هم در مرکزگریز بودن، موضع نظام حکمرانی در این خصوص چیست؟ سؤال اساسی این است که موضع نظام حکمرانی در ارتباط با نقض یا محدودیت و یا آزاد گذاشتن هر یک از مقولات این چارچوب و ارتباط آن با مقولهٔ حقوق بشر چیست؟
شکاف آگاهی	مکانیسم نظام حکمرانی سایبری برای غلبه بر فاصلهٔ فقیر و غنی به لحاظ سواد سایبری، استفاده از ظرفیت‌های سایبری و ... چیست؟ با توجه به اینکه بخش زیادی از گردش اطلاعات و حتی آموزش در فضای سایبری صورت می‌پذیرد، چه مکانیسم‌هایی برای کمک به فقرای اطلاعاتی و جبران عدم دسترسی آن‌ها تدوین شده است؟

استانداردهای رفتاری/ امنیت بین‌الملل	آیا نظام حکمرانی سایبری کدهای رفتاری مشخصی برای اقدام و عمل در حوزهٔ سایبری دارد؟ آیا به دنبال تدوین نظام رفتاری منطقه‌ای و بین‌المللی در حوزهٔ فضای سایبری هست؟ معیارها و مبانی اصولی (مبانی دینی، ایدئولوژیک، ملی و ...) آن‌ها چیست؟ باید توجه داشت که این استانداردها متضمن امنیت بین‌الملل در سطح منطقه‌ای و جهانی هستند.
ظرفیت‌سازی و توسعه	آیا اساساً نظام حکمرانی فضای سایبری را به عنوان یک ظرفیت برای توسعه، به رسمیت می‌شناسد؟ آیا فضای سایبری در نظام برنامه‌ریزی و سیاست‌گذاری کشور جایگاهی سلبی دارد یا ایجابی؟
ژئوپلیتیک فضای سایبری (مرزها و قلمرو سایبری)	فضای سایبری چشم‌انداز «سرزمینی» واحدهای سیاسی(کشورها) را تیره‌وتار کرده است. مرزهای کلاسیک ملی معنا و مفهوم تاریخی خود را از دست داده است. «فروپاشی» امروزه دقیق‌ترین مفهومی است که برای تعبیر وضعیت حاکمیت‌های ملی، بدون هیچ استثنائی، مورد استفاده قرار می‌گیرد. در نظام حکمرانی سایبری کشور، سرحد یا مرزهای حاکمیتی ایران کجاست؟ برنامه کشور برای مقابله با اشغال قلمروهایی از فضای سایبری کشور چیست؟ چه برنامه‌ای برای اشغال قلمروهایی در فضای سایبری دشمنان وجود دارد؟
پلتفرم‌ها	پلتفرم‌ها (همچون گوگل، آمازون، اپل و ...) بر اثر انحصار و ادغام‌های افقی، عمودی و مُورب به بازیگران جدی فرامرزی تبدیل شده‌اند. نقش و بازیگری پلتفرم‌ها در قالب دیپلماسی شرکتی به خصوص از منظر «مقررات‌گذاری و خودتنظیم‌گری» حائز اهمیت است که عملاً بازیگران دولتی را از عرصه خارج کرده‌اند. بر این اساس، مبنای تعامل نظام حکمرانی سایبری کشور با این پلتفرم‌ها چیست؟ آیا هیچ برنامهٔ استراتژیک برای دیالوگ

	با این پلتفرم‌ها یا پلتفرم‌های جایگزین وجود دارد؟ اصولاً پلتفرم مطلوب نظام حکمرانی ایران کدام است؟
لایه‌های زیرساخت، خدمات و محتوا	به طور کلی، عرصهٔ سایبری متشکل از سه لایهٔ زیرساخت، خدمات و جریان محتوا در آن است. در صورت قطع دسترسی به اینترنت جهانی، نظام حکمرانی سایبری کشور چه برنامه‌ای برای پایداری زیرساخت شبکهٔ ملی، اطمینان از تداوم خدمات و جریان محتوا در آن دارد؟ در صورت قطع دسترسی به اینترنت جهانی، میزان تاب‌آوری تمامی امورات مبتنی بر شبکه، به خصوص کسب‌وکارها، به چه میزان است؟
جایگاه مردم	اصل اساسی در هر گونه نظام حکمرانی مردم است. در نظام حکمرانی سایبری کشور، چه جایگاهی برای مردم پیش‌بینی شده است؟ آیا مردم قطعاتی از پازل حکمرانی محسوب می‌شوند یا اینکه به کاربران/ مصرف‌کنندگانی خنثی تقلیل می‌یابند؟ استراتژی تعامل دولت ـ مردم، مردم ـ مردم، مردم ـ شرکت‌ها (پلتفرم‌ها و ...) در این نظام چطور طراحی شده است؟
تروریسم سایبری	از دیدگاه نظام حکمرانی سایبری، تعریف، معیار و شاخص تروریسم سایبری چیست؟ آیا نظام حکمرانی قادر به احصای لیست گروه‌های تروریستی سایبری هست؟ چطور می‌توان بین تروریسم سایبری و سایر انواع حملات سایبری تفکیک قائل شد؟
کنترل، نظارت و انحصار اطلاعات	نظام حکمرانی به چه میزان قائل به کنترل و نظارت بر اطلاعات جاری در بستر سایبری است؟ آیا مرزبندی مشخصی در این زمینه وجود دارد؟ آیا نظام حکمرانی تعریف مشخصی از اینکه چه نوع اطلاعاتی و به چه دلیل نباید در فضای سایبری جریان یابد، دارد؟ در ارتباط با انحصار اطلاعات چطور؟

بر این اساس، جدول مقولات و مفاهیم فوق چارچوبی برای تأمل و اندیشیدن در زمینهٔ فضای سایبری و اتخاذ هر گونه رویکردی در دیپلماسی سایبری است. این مقولات باید در نرم‌افزار معرفتی نظام حکمرانی سایبری کشور تبیین، و ابعاد و مؤلفه‌های آن به خوبی شکافته شود و در ارتباط با هر یک از آن‌ها به یک جمع‌بندی جامع و مانع برسد تا بتوان بر اساس آن به برآیند کلی یک سیاست واحد دست یافت. به عبارت دیگر، در ارتباط با هر یک از این مقولات باید به یک تعریف دست یافت و بر اساس آن تعریف، موضعی رسمی و شفاف اتخاذ نمود تا بتوان بر اساس آن وارد تعاملات دیپلماتیک در عرصهٔ منطقه‌ای و بین‌المللی شد.

این برآیند کلی که در اینجا دیپلماسی سایبری نامیده می‌شود با سیاست‌گذاری ملی در حوزهٔ فضای سایبری متفاوت است. در حالی که سیاست‌گذاری ملی صرفاً بُعد و مصرف داخلی دارد، دیپلماسی سایبری برای ایجاد و برقراری تعامل بین‌المللی است. در نهایت اینکه دیپلماسی سایبری سند استراتژیک حاوی اصول و مؤلفه‌هایی صریح و روشن است که در تعاملات منطقه‌ای و بین‌المللی به عنوان راهنما عمل می‌کند. این اصول و مؤلفه‌ها به صورت پایه‌ای باید دو ویژگی مهم داشته باشند: ۱. موقعیت کشور را در جایگاه مدعی و صاحب ایده و گفتمان قرار دهد؛ ۲. بسته به شرایط و موقعیت کشور از قابلیت انعطاف بالایی برخوردار باشد (قابل مذاکره باشد).

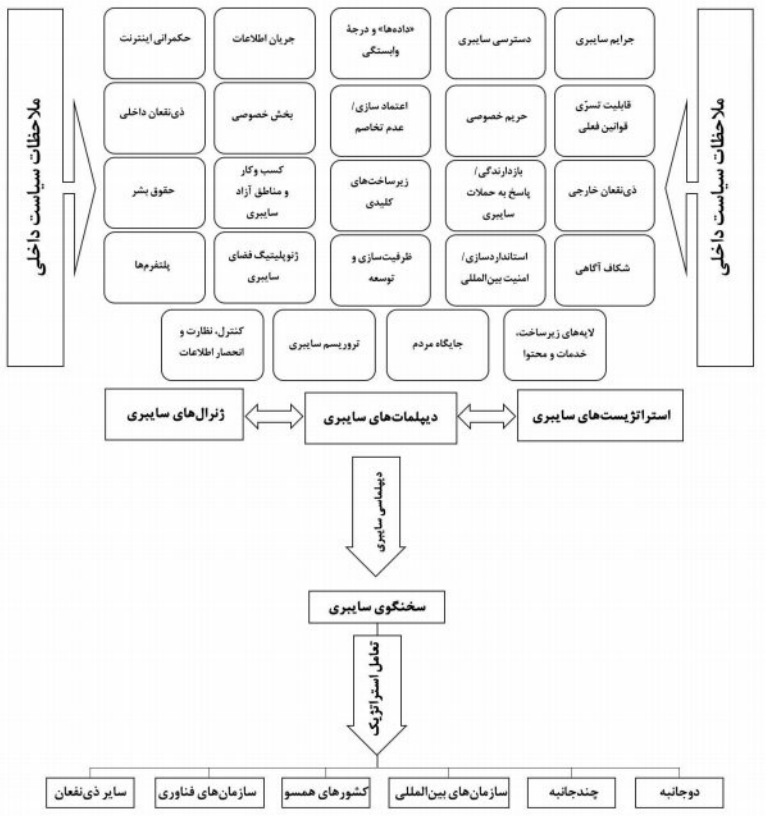
علاوه بر این چارچوب مفهومی، باید در نظر داشت که در دیپلماسی سایبری سه کانون قدرتمند نهادی وجود دارد که در تدوین آن، نقش اصلی را ایفا می‌کنند: ۱. ژنرال‌های سایبری (مسلط به ابعاد فنی ـ ایمنی حوزهٔ سایبری به خصوص در ارتباط با توانمندی‌ها و پتانسیل‌های فنی ـ مهندسی و آی‌تی داخلی)، ۲. استراتژیست‌های سایبری (مسلط به ملاحظات سیاست داخلی، اعم از سیاسی، اجتماعی، فرهنگی، ارتباطی و دینی، حقوقی، امنیتی و ....)،

۳. دیپلمات‌های سایبری (مسلط به ملاحظات سیاست خارجی و حقوق بین‌الملل که عمدتاً نمایندگان دستگاه سیاست خارجی هستند). فقدان هر یک از سه‌گانهٔ فوق، ضعف و خلأ جدی در مبانی، ماهیت و ابعاد سند دیپلماسی سایبری کشور ایجاد خواهد کرد.

دیپلماسی سایبری کشور در نهایت باید به عنوان یک سند مدون در مجامع جهانی (اجلاس‌ها و مجامع بین‌المللی، سازمان‌ها و نهادهای بین‌المللی و ...) با هدف تأثیرگذاری بر کنوانسیون‌ها و معاهدات بین‌المللی و نیز سایر اسناد منطقه‌ای و بین‌المللی مربوط به عرصهٔ سایبری ارائه شود. با توجه به سرعت تحولات در این حوزه، جهان همه‌روزه شاهد برگزاری نشست‌ها و اجلاسیه‌های بین‌المللی با هدف تدوین استانداردها، مقررات‌گذاری، تعیین کُدهای رفتاری، و .... در حوزه‌های مختلف سایبری است. حضور مؤثر (هم محتوایی و هم به لحاظ فنی) در این نشست‌ها و اجلاسیه‌ها می‌تواند در تعیین چشم‌انداز آتی این حوزه، به خصوص بر اساس منافع ملی کشورمان اثرگذار باشد.

البته باید اذعان داشت که در حال حاضر تنها معدودی از کشورها در ارتباط با چارچوب مفاهیم فوق دارای سند یا استراتژی مؤثر و منسجم و در عمل کاربردی هستند و دولتشان می‌تواند با قدرت دربارهٔ آن با زبان واحد سخن بگوید. در بسیاری از کشورها، سیاست خارجی به طور عام و دیپلمات‌ها به طور خاص از چالش‌های ساختاری داخلی رنج می‌برند؛ نظیر ضعف سیاست‌گذاری ملی، تعدد سازمان‌های تصمیم‌گیرنده، اختلافات سازمانی در زمینهٔ مرجعیت و مدیریت فضای سایبری، نهادها یا مراکز قدرتمند داخلی که استدلال‌ها و مبانی سیاست خارجی را زیر سؤال می‌برند، فقدان «ژنرال»های سایبری که بتوانند مختصات فنی فضای سایبری را به دیپلمات‌ها منتقل کنند و ... .

با این حال، با توجه به جدول مقولات حوزهٔ سایبری و نیـز ملاحظـاتی که پیش‌تر مطرح شد، می‌توان فراینـد تـدوین دیپلماسـی سـایبری را در دو سطح نظری و عملیاتی به شرح نمودار شمارهٔ ۱ متجسم ساخت.



نمودار شمارهٔ ۱. فرایند تدوین دیپلماسی سایبری (نظری و عملی)

بدیهی است در فقدان یک سند یا استراتژی جامع در ارتباط با چارچوب مفهومی فوق و از آن مهم‌تر، در صورت فقدان یک ساختار هماهنگ‌کننده یا تصمیم‌گیرندهٔ ملی در ارتباط با فضای سایبری، نمی‌توان انتظار داشت که نظام حکمرانی کشور بتواند در تعاملات بین‌المللی خود دربارهٔ نوع مواجهه با مسائل فضای سایبری، به صورت‌بندی دقیق و فرمول‌بندی مؤثر برای دفاع از منافع ملی کشور دست یابد. ضمن آنکه فقدان چنین استراتژی روشنی همواره کشور را در تعاملات منطقه‌ای و بین‌المللی نه در موضع صاحب ایده یا گفتمان که در موضع دفاعی یا ضعف (متهم) قرار می‌دهد که همواره باید در برابر الگوهای رایج (عمدتاً غربی) از خود دفاع کند.

دلالت‌ها و ضرورت‌های عملی دربارهٔ دیپلماسی سایبری ایران

مرحلهٔ دوم فرایند دیپلماسی سایبری، مرحلهٔ عملیاتی آن است که خود مستلزم دلالت‌ها و ضرورت‌های بسیاری برای نظام حکمرانی سایبری کشور، به خصوص دستگاه سیاست خارجی، است. در این خصوص، برخی صاحب‌نظران معاصر، همچون هلی تییرما کلار، با اشاره به ابعاد بین‌المللی فضای سایبری هشدار می‌دهند که درست همانند دوران پس از اختراع بمب اتم، فضای سایبری مستلزم تکاپوی جدی دیپلمات‌ها و در رأس آن، دستگاه‌های سیاست خارجی است تا بتوان از پیامدها و آسیب‌های جهانیِ به مراتب بیشتر و خطرناک‌تر آن (در مقایسه با بمب‌های هسته‌ای) اجتناب کرد.[1]

بر این اساس، و به عنوان یک اصل کلی، تأکید بر «تکاپو و پویایی جدی» دستگاه سیاست خارجی کشور در عرصهٔ بین‌المللی مهم‌ترین ضرورت عملی در ارتباط با دیپلماسی سایبری کشور است. در سطوح خُردتر، چند ضرورت

1. Tiirmaa-Klaar, 2013

عملیاتی دیگر نیز در سه سطح فردی (توانمندی دیپلمات‌ها)، سازمانی (تعیین سخنگوی سایبری و ایجاد ساختار مناسب) و ملی (تعیین شرکای استراتژیک) به شرح ذیل قابل ذکر است:

۱. سطح فردی یا توانمندی دیپلمات‌ها: دیپلماسی سایبری به لحاظ ظرفیت‌ها و توانمندی‌های فردی دیپلمات‌ها و افرادی که در این حوزه فعالیت می‌کنند نیز دلالت‌های زیادی دارد. واقعیت این است که فضای سایبری یک ظرفیت و مسیر کاری کاملاً جدید با ابزارها و مکانیسم‌های متفاوت در تنظیم روابط بین‌الملل ایجاد کرده است. این ظرفیت جدید، هم در عرصهٔ داخلی و هم در عرصهٔ خارجی فعالان، بازیگران و ذی‌نفعان متفاوتی دارد. رمز موفقیت در این عرصه و فضای جدید مستلزم آن است که متولیان دیپلماسی سایبری به طور صریح بتوانند به زبان سایبری صحبت کنند.

زبان سایبری به دانش، آگاهی و آشنایی کامل دیپلمات‌ها با مهم‌ترین مسائل و چالش‌های به سرعت روبه‌رشد در این عرصه اشاره دارد که شبکه‌های اینترنت، هوش مصنوعی، آخرین فناوری‌های ارتباطی و اطلاعاتی، مدیریت اینترنت، گفت‌وگوهای سایبری دوگانه و چندگانه، امنیت سایبری ملی و بین‌الملل، اطلاعات یا ضداطلاعات سایبری، کامپیوتر و امنیت شبکه و ... تنها بخش‌هایی از آن را تشکیل می‌دهد.

پیچیدگی فضای سایبری و سرعت تحولات فناورانه در آن از یک سو و تضاد یا ناپایداری منافع و منابع بازیگران در آن از سویی دیگر، بدون شک مستلزم ظهور نسل جدیدی از دیپلمات‌های آموزش‌دیده است که بتوانند با قدرت و آگاهانه موضوعات و چالش‌های آن را پیش ببرند. آن‌ها باید همپا و همانند دنیای واقعی، با موضوعات و چالش‌های موازی

و متداخل در فضای سایبری نیز آشنا باشند. آن‌ها باید بتوانند همانند و همپای دنیای واقعی، با در نظر داشتن تمامی ملاحظات سیاست خارجی، در حوزهٔ مسائل و چالش‌های فضای سایبری نیز آگاهانه تصمیم بگیرند و عمل کنند. برای مثال، دولت آمریکا کریستوفر پینتر را، که بیش از ۲۵ سال سابقهٔ فعالیت در حوزهٔ سایبری داشته، به عنوان دیپلمات ارشد سایبری این کشور منصوب کرده است.

۲. سطح سازمانی یا تعیین سخنگوی سایبری: اگرچه مسئولیت تدوین دیپلماسی سایبری یک مقولهٔ ملی است که در تدوین آن استراتژیست‌های سایبری، ژنرال‌های سایبری و دیپلمات‌های سایبری همگی با هم دست دارند، اما در نهایت پیاده‌سازی و پیشبرد اصول و مؤلفه‌های آن در عرصهٔ منطقه‌ای و بین‌المللی باید بر عهدهٔ یک نهاد یا سازمان، به عنوان سخنگوی سایبری، گذاشته شود.

در عمدهٔ کشورهای پیشرو در زمینهٔ مقولهٔ دیپلماسی سایبری، دستگاه‌های سیاست خارجی (وزارت امور خارجه) این مسئولیت را به عهده گرفته و متناسب با این مسئولیت، تغییراتی جدی در ساختار خود ایجاد کرده‌اند. این کشورها با ایجاد تغییرات ساختاری در چارت سازمان و نیز راه‌اندازی مکانیسم‌های ویژه، مسیرهای متفاوتی برای پیگیری و مواجهه و رصد تحولات فضای سایبری در پیش گرفته‌اند که از جمله شامل راه‌اندازی دپارتمان مستقل برای متمرکز کردن تمامی امور فضای سایبری (همانند انگلستان) یا راه‌اندازی ادارهٔ هماهنگ‌کنندهٔ امور سایبری (مانند ایالات متحده) و یا ترکیبی از این دو (مثل آلمان) می‌شود.

جدول شمارهٔ ۳. واحدهای اداری شکل‌گرفته در کشورهای متولی پیگیری امور دیپلماسی سایبری

نام کشور	نام واحد و محل استقرار آن
ایالات متحده	ادارهٔ هماهنگ‌کنندهٔ امور سایبری/ وزارت امور خارجه
انگلستان	واحد سیاست سایبری بین‌المللی[1]/ وزارت امور خارجه
آلمان	دوازده واحد که به طور هم‌زمان امور مختلف سایبری را رصد می‌کنند/ وزارت امور خارجه
چین	وزارت امور خارجه
ژاپن	وزارت امور خارجه

کشور ایران نیز با توجه به اینکه خود را صاحب گفتمان و ایدئولوژی جدید می‌داند، از این وضعیت مستثنا نیست. با توجه به اهمیت فضای سایبری و تغییرات شگرفی که در ماهیت این فضا صورت گرفته است، باید تغییر و تحولاتی در نظام حکمرانی سایبری در زمینهٔ نهادینه‌سازی و مأموریت‌گرا ساختن ظرفیت دیپلمات‌های سایبری در عرصهٔ منطقه‌ای و بین‌المللی صورت گیرد. در وهلهٔ اول، باید یکی از سازمان‌ها یا نهادهای کشور به عنوان سخنگوی سایبری کشور به رسمیت شناخته شود و سپس متناسب با آن تغییرات ساختاری به لحاظ سلسله‌مراتب اداری، کادر کارشناسی و تخصصی، وظایف، اختیارات و ... تعریف شود.

۳. **سطح ملی یا تعیین شرکای استراتژیک**: فراتر از سطح فردی و سازمانی

1. International Cyber Policy Unit

که عمدتاً مسائل داخلی تلقی می‌شوند، نظام حکمرانی سایبری کشور باید در عرصهٔ بین‌المللی نیز با هدف پیشبرد دیپلماسی سایبری خود به انتخاب شرکای استراتژیک دست **بزند**. در انتخاب شرکای استراتژیک لزوماً منظور دولت‌های خارجی یا سازمان‌های مهم بین‌المللی نیست. طیف متنوعی از بازیگران و ذی‌نفعان ممکن است در زمینهٔ اهداف کشور مفید و مناسب باشند. برای مثال، دانمارک نخستین کشوری بود که برای گفت‌وگو با غول آی‌تی (گوگل) دست به انتخاب سفیر ویژه در این کمپانی زد. ایالات متحده نیز در عمدهٔ کشورها، گروه‌ها، احزاب و سازمان‌های مخالف دولت حاکم را به عنوان شریک استراتژیک انتخاب می‌کند و از طریق فضای سایبری، اهداف و برنامه‌های خود را پیش می‌برد. حتی فراتر از آن ممکن است به دلیل منافع استراتژیک میان‌مدت و بلندمدت لازم باشد با کشورهای متخاصم نیز به نوعی دیالوگ بازدارنده اقدام نمود. برای مثال، اتحادیهٔ اروپا اگرچه در ادبیات سیاسی خود همواره روسیه و چین را منشأ تهدید سایبری و منبع جاسوسی سایبری می‌داند، اما همواره با این دو کشور در حوزهٔ مسائل و چالش‌های سایبری گفت‌وگوهای انتقادی (هرچند نه چندان موفقیت‌آمیز) داشته است.

کشور ایران نیز نمی‌تواند از این وضعیت مستثنا باشد. ایران با توجه به اهداف و اولویت‌های منافع ملی و سیاست خارجی، باید ابتدا شرکای اصلی خود در حوزهٔ سایبری را در سطوح مختلف، مثلاً دوجانبه، چندجانبه، در سطح سازمان‌ها و نهادهای بین‌المللی، شرکت‌ها و کمپانی‌های فناوری، گروه‌ها و نهادهای مردمی و ... برگزیند و سپس برای برقراری تعامل و آغاز گفت‌وگوهای استراتژیک اقدام کند. فراتر از آن حضور مؤثر و فعال و سازندهٔ کشور در ابتکارات منطقه‌ای و بین‌المللی در حوزهٔ دیپلماسی سایبری نیز بسیار ضروری است. همان طور که در فصل دوم به آن اشاره شد، در جهان بیش از هشتاد ابتکار منطقه‌ای و بین‌المللی

در زمینهٔ حوزهٔ سایبری شناسایی شده که به صورت سند یا استراتژی درآمده و به عنوان دستورالعملی برای راهنمایی فعالیت بازیگران متعدد در این حوزه عمل می‌کند. بسیاری از این اسناد و استراتژی‌ها حاصل ابتکارات کشورهای مختلف از طریق مذاکرات دوجانبه، چندجانبه، منطقه‌ای یا بین‌المللی و جهانی است. در حالی که متأسفانه کمتر اثری از کشور در عمدهٔ این ابتکارات و اسناد و استراتژی‌های سایبری دیده می‌شود. بنابراین، باید هر چه سریع‌تر مکانیسم‌های ورود به این تعاملات منطقه‌ای و بین‌المللی را با هدف اثرگذاری بموقع و مؤثر پیدا کرد.

جمع‌بندی و نتیجه‌گیری این فصل

دیپلماسی سایبری متأخرترین نوع دیپلماسی در سیاست خارجی و سپهر روابط بین‌الملل است. با وجود آنکه تنها کشورهای معدودی توانسته‌اند بر اساس منافع ملی و گفتمان حاکم خویش به ترسیم دیپلماسی سایبری خود اقدام کنند، برای کشورهایی همچون ایران که داعیهٔ استقلال و نیز گفتمان سیاسی جدیدی دارد این امر از اهمیتی دوچندان برخوردار است.

در این فصل از طریق مطالعات موردی سایر کشورها و نیز تکنیک هم‌افزایی فکری، بیست‌وچهار مفهوم و مقولهٔ اصلی در ارتباط با دیپلماسی سایبری احصا و مهم‌ترین موضوعات و سؤالات مرکزی هر یک از آن‌ها ارائه شد. همچنین با توجه به تجربیات سایر کشورها، الگویی عملیاتی برای تدوین دیپلماسی سایبری هم به صورت نظری و هم به صورت عملیاتی پیشنهاد شد که می‌تواند به عنوان اولین گام در تدوین دیپلماسی سایبری کشور مورد توجه نظام حکمرانی قرار گیرد.

با توجه به سرعت تحولات جهانی در عرصهٔ سایبری، تعدادی از

کشورهای پیشرفته با سرعت از طریق تعریف اصول و مبانی نظری دیپلماسی سایبری، تعیین دقیق راهبردهای عملیاتی و نیز تعریف مکانیسم‌های اجرایی مختلف، از جمله تعیین شرکای استراتژیک، اتخاذ رویکردهای دوجانبه و چندجانبه و ...، به صورت‌بندی و شکل‌گیری ائتلاف‌های جدید در عرصهٔ روابط بین‌الملل اقدام کرده‌اند. ایران نیز باید به طور مشابه با تدوین مبانی و اصول دیپلماسی سایبری، سیاست‌های راهبردی خود برای پیگیری منافع ملی و توسعهٔ نفوذ خود در عرصهٔ سایبری را تعیین کند. همچنین باید از طریق رویکردهای عملیاتی در قالب تعاملات دوجانبه، چندجانبه و ... وارد مکانیسم‌های سایبری منطقه‌ای و بین‌المللی شود و جایگاهی در شأن و صاحب گفتمان در این عرصه برای خود به دست آورد. در غیر این صورت، در ارتباط با هر یک از مقولات و مؤلفه‌های ذکرشده در چارچوب مسائل و مؤلفه‌های سایبری، در مواجهه با قدرت‌ها و کشورهای پیشرو در جایگاه متهم قرار خواهد داشت و همواره باید بر اساس چارچوب و گفتمان دیپلماسی سایبری آن‌ها پاسخگو باشد.

منابع

Barrinha, André and Thomas Renard (2017), Cyber-Diplomacy: The Making of an International Society in the Digital Age, European International Studies Association.

Buck, S. J. (1998), The Global Commons: An Introduction. Washington, DC: Island Press.

Bull, H. (1977/2002), The Anarchical Society: A Study of Order in World Politics (3rd ed.), Basingstoke: Palgrave.

Chernenko, Elena (2018), "Russia's Cyber Diplomacy", In Hacks, Leaks and Disruptions Russian Cyber Strategies, Ed. By Nicu Popescu and Stanislav Secrieru, Chaillot Papers, European Institute for Security Studies.

Clark, I. (2007), International Legitimacy and World Society, Oxford: OUP.

Danca, D. (2015), "Cyber Diplomacy – A New Component of Foreign Policy", Journal of Law and Administrative Sciences, No. 3.

Fletcher, T. (2016), Naked Diplomacy: Power and Statecraft in the Digital Age, London: William Collins.

Gady, F. S., and Austin, G. (2010), Russia, the United States and Cyber Diplomacy: Opening the Doors, New York, NY: East West Institute.

Hall, I. (2006), "Diplomacy, Anti-Diplomacy and International Society", In R. Little and J. Williams (Eds.), The Institutions of Anarchical Society (pp. 141–161), Basingstoke: Palgrave Macmillan.

Harold G. Nicolson, Harold G (1963), Diplomacy. London: Oxford University Press, 3rd Ed.

Hocking, B., and Melissen, J. (2015), Diplomacy in the Digital Age, The Hague: Clingendael Institute.

Hocking, B., and Melissen, J., Riordan, S., Sharp, P. (2012), Futures for Diplomacy: Integrative Diplomacy in the 21st Century, The Hague: Clingendael Institute.

Inkster, Nigel (2016), "China's Cyber Power", Adelphi Series, no. 456, May.

Japan and China Responses to the Global and Regional Challenges, eds. D. Mierzejewski, K. Żakowski, Łódź University Press, Łódź 2015, s. 143–159.: http://hdl.handle.net.

Keleman, Michele (2014), "Twitter Diplomacy: State Department 2.0", National Public Radio, Retrieved 28 April 2014.

Kissinger, H. (2014), World Order, New York, NY: Penguin Press.

Kleiner, J. (2008). The Inertia of Diplomacy. Diplomacy and Statecraft, 19 (2), 321–349.

Landler, Mark (2014), "In the Scripted World of Diplomacy, a Burst of Tweets", International New York Times, Retrieved 28 April 2014.

Maness, Ryan C. and Brandon Valeriano (2015), Russia's Coercive Diplomacy Energy, Cyber, and Maritime Policy as New Sources of Power, UK: Palgrave Macmillan.

Melissen, J. (2007), The New Public Diplomacy: Soft Power in

International Relations, New York, Palgrave Macmillan.

Neumann, I. (2002), The English School on Diplomacy (Clingendael Discussion Paper 79), The Hague: Clingendael Institute.

Owen, T. (2015), Disruptive Power: The Crisis of the State in the Digital Age, Oxford: OUP.

Painter, Ch. (2018), "The Rise of the Internet and Cyber Technologies Constitutes one of the Central Foreign Policy Issues of the 21st Century", The Foreign Service Journal, Retrieved from: https://www.afsa.org.

Popescu, Nicu and Stanislav Secrieru (2018), Hacks, Leaks and Disruptions Russian Cyber Strategies, European Union, Institute for Security Studies, Pari.

Potter, E. H. (2002), Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century, Montreal: McGill-Queen's University Press.

Renard, T. (2014), The Rise of Cyber-Diplomacy: the EU, its Strategic Partners and Cyber-Security.

Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General.

Riordan, Shaun (2019), Cyber Diplomacy: Managing Security and Governance Online, Polity Press, Cambridge, UK.

Russian Ministry of Foreign Affairs, Convention on International Information Security (Concept), September 22, 2011, http://www.mid.ru.

Sandre, A. (2015), Digital Diplomacy: Conversations on Innovation in Foreign Policy, Lanham, MD: Rowman and Littlefield.

Segal, A. (2016), The Hacked World Order: How Nations Fight, Trade, Maneuver and Manipulate in the Digital Age, Philadelphia, PA: Public Affairs.

Segal, A. (2018), Chinese Cyber Diplomacy in a New Era of Uncertainty, Hoover Institution, Stanford University.

Seib, Philip (2012) Real-Time Diplomacy: Politics and Power in the Social Media Era, New York, Palgrave Macmillan, 2012.

Tatar, Ünal and Orhan Çalık, Minhac Çelik, Bilge Karabacak (2014), "A Comparative Analysis of the National Cyber Security Strategies of Leading Nations", Proceedings of the 9th International Conference On Cyber Warfare and Security (Iccws-2014).

The European Strategic Partnership Observatory, Working Paper 7, June, p. 21.

The Government of Japan (2015), Cybersecurity Strategy, The Cabinet Decision.

Tiirmaa-Klaar, Heli (2013), "Cyber Diplomacy: Agenda, Challenges and Mission", In Katharina Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn.

UN Doc A/66/359 .Letter Dated 12 September 2011 from the Permanent.

Weijin Wang, Analysis on China's Cyber Diplomacy, On Their Own Paths.

Wight, M. (1979), Systems of States, Leicester: Leicester University Press.

White House (2011), International Strategy for Cyberspace, Washington, DC: The White House.

White House (2015, September 25), FACT SHEET: President Xi Jinping's State Visit to the United States, Washington, DC: The White House Office of the Press Secretary.

White House (2018), U.S. Cyber Diplomacy in an Era of Growing Threats, Washington, DC: The White House.

Woods, Andrew Keane (2017), "The Tallinn Manual 2.0, Sovereignty 1.0", Lawfare (blog), February 8, 2017, https://www.lawfareblog.com.

Zhao, K. (2013), "China's Diplomacy Has Stepped into the Age of Internet", People's Daily Online: www.news.xinhuanet. com.

سخن پایانی

واقعیت این است کـه بـیش از دو دهـه از ورود جهـان بـه عصـر حکمرانـی سایبری و گذار برخی کشورهای پیشرفته بـه جوامـع نـوع ۵[1] مـی‌گـذرد. بـر اساس رویهٔ تاریخی و به اقتضای رقابت و تضاد منافعی که به صورت دائمـی در تمامی عرصه‌ها وجود داشـته و دارد، در حـال حاضـر شـاهد شـدیدترین نزاع‌های سیاسی ـ ایدئولوژیک بین قدرت‌های بزرگ در عرصـهٔ سـایبری نیـز هستیم. اگرچه برخلاف مؤلفه‌ها و دستور کار دیپلماسی در عرصه‌های سـابق، محوریت و مرکز ثقل این نزاع‌ها فناوری است، اما آثار و تبعـات آن همچنـان اقتصادی، اجتماعی، فرهنگی و امنیتی نیز هست. برای مثال، بر کسـی پوشـیده نیست که ریشهٔ اصلی عمیق‌تر شدن نزاع فعلی آمریکا با چین نه بر سر دستور کارهای سنتی همچون جزایر دریای جنوبی یا مسئلهٔ کرهٔ شمالی یا تعرفه‌هـای واردات و صادرات است، بلکه در اصل بر سر فناوری نسل پنجم (۵G) است که به نظر می‌رسد چین در تعیـین ماهیـت ایـن فنـاوری و اسـتانداردهای آن دست‌کم پابه‌پای آمریکا در حال پیشرفت و از این طریـق توسـعهٔ نفـوذ خـود است. این فناوری به زبان ساده، چشم‌انداز کسب تریلیون‌هـا دلار را از چنـگ اقتصاد آمریکا خارج ساخته، زیرساخت‌هـای ارتبـاطی و اطلاعـاتی آمریکـا و تمامی کشورهای هم‌پیمان این کشور را به نفع چین تضـعیف یـا در دسـترس چین قرار داده و با توجه به فراهم ساختن بستر نفوذ گسـتردهٔ چـین از طریـق

---

1. Society 5.0

سرمایه‌گذاری‌های کلان اقتصادی در زیرساخت‌های ارتباطی بسیاری از کشورهای در حال توسعه و کمترتوسعه‌یافته، این کشور را در سپهر سیاست بین‌الملل قرن ۲۱ در جایگاهی برابر با آمریکا قرار داده است.

با توجه به مقدمهٔ فوق، باید دانست که از منظر حکمرانی، عرصهٔ سایبری نیز همانند چهار عرصهٔ سابق، دستور کار و گفتمان و چالش‌های زیادی دارد، با این تفاوت که هم ماهیت و جنس این دستور کار و گفتمان و چالش‌ها متفاوت است و هم سرعت تغییرات و تحولات در آن بسیار زیاد و غیرقابل‌پیش‌بینی است. در این میان، برخی از کشورها (همچون آمریکا، چین و تا حدودی روسیه و ژاپن) به اقتضای اشرافیت راهبردی در حوزهٔ فناوری و نیز قدرت بازیگری و نفوذی که در این عرصه کسب کرده‌اند، به سرعت در حال تعریف استانداردها، پروتکل‌ها، تعیین حوزه‌های نفوذ و قلمروهای سایبری، ایفای نقش در توسعهٔ فناوری و در نتیجه تصاحب سهمی از بازار و ارزش آن فناوری هستند. برخی دیگر از کشورها، از جمله کشورهای در حال توسعه، تلاش دارند از طریق مکانیسم‌های مختلف (از جمله حضور گسترده، مؤثر و پُرتعداد در نشست‌ها و جلسات بین‌المللی تصمیم‌ساز در زمینهٔ تدوین استانداردهای فنی مرتبط با عرصهٔ سایبری و فناوری‌های مرتبط با آن، مشارکت در طرح‌های فناورانه بین‌المللی مرتبط با عرصهٔ سایبری یا حتی مقررات‌گذاری در ارتباط با نحوهٔ تعامل با این عرصه در سطوح ملی) نقش و جایگاهی برای خود ایجاد نمایند. به طور مثال، کشورهای اروپایی (از جمله آلمان، فرانسه) از طریق برخوردهای سختگیرانه قضایی و سیاستی، هند، نیجریه و ترکیه از طریق تعامل حقوقی و قانونی با پلتفرم‌ها و عربستان از طریق مشارکت (خرید یا سرمایه‌گذاری) در طرح‌های فناورانه بین‌المللی به دنبال تثبیت جایگاه خود در آیندهٔ این عرصه هستند.

ایران نیز همانند تمامی کشورهای جهان از تبعات جریان‌های غالب در حکمرانی بین‌المللی عرصهٔ سایبری، آثار نزاع‌های سیاسی-ایدئولوژیک شکل‌گرفته در عرصهٔ سایبری، تأثیرات پلتفرم‌ها و فناوری‌های مرتبط با عرصهٔ سایبری در روابط بین‌الملل، صف‌بندی‌ها و مرزبندی‌های شکل‌گرفته در این عرصه و ... مستثنا نیست. با وجود ظرفیت‌ها و پتانسیل بالقوهٔ بالای کشور، نباید از این فرصت تاریخی برای گذار به عرصهٔ پنجم و اعمال حاکمیت و نیز ایفای نقش منطقه‌ای و بین‌المللی مؤثر در آن غفلت نماید. مسئلهٔ مهم و حائز اهمیت در ارتباط با حکمرانی در عرصهٔ سایبری این است که برخلاف برهه‌های تاریخی گذار در گذشته، گذار به این عرصه بیشتر جهشی است تا تدریجی و تکاملی. باید با نگاه و افق بلند، هر چه سریع‌تر به سوی تدوین دیپلماسی سایبری رفت و از این رهگذر، موضوعات، مسائل و چالش‌های سایبری منطقه‌ای و بین‌المللی را در دستور کار دیپلماسی دستگاه سیاست خارجی و نیز مکانیسم‌ها و سازوکارهای تنظیم قراردادها و همکاری‌ها و تعاملات منطقه‌ای و بین‌المللی قرار داد.

ورود به عرصهٔ حکمرانی سایبری در سطوح ملی و بین‌المللی از طریق تدوین دیپلماسی سایبری مستلزم فهم و درک برخی اصول و دلالت‌هایی است که در ذیل به آن پرداخته می‌شود:

- **اصول**

نقل است کلینتون برای وصف «عرصهٔ سایبری» از استعارهٔ «ژله» استفاده کرده است و اینکه نمی‌توان آن را به دیوار میخکوب کرد. اگرچه کنایهٔ «به دیوار میخکوب کردن ژله» کلینتون اشاره‌ای به عبث بودن تلاش‌های دولت چین و روسیه برای «کنترل» اینترنت داشت، اما این استعاره هم‌زمان به دو اصل مهم اشاره دارد:

۱. به همان اندازه که امکان کمی برای کنترل و محدودسازی عرصهٔ سایبری وجود دارد، به همان میزان هر چه بر پایه و اساس فضای سایبری سامان گیرد، نیز نمی‌تواند به طور اطمینان‌بخشی پایدار و استوار باشد. به این اعتبار می‌توان گفت که کلیت ساختار سایبری نظام بین‌الملل (به همراه تمامی نظام‌ها و زیرساخت‌های فنی، ارتباطی، اطلاعاتی، اقتصادی و ... که بر اساس آن هم در غرب و هم در شرق شکل گرفته) تقریباً به یک اندازه در معرض ریسک و خطر جدی قرار دارند.

۲. جنس، ماهیت و ساختار قدرت و اعمال حاکمیت در عرصهٔ سایبری متفاوت از چهار عرصهٔ حکمرانی سابق (زمین، دریا، هوا و فضا) است. برخلاف ماهیت سختِ قدرت در سایر عرصه‌ها، در عرصهٔ سایبری ماهیت قدرت نرم است. ساختار قدرت غیرمتمرکز، افقی و به صورت شبکه‌ای است. قدرت در عرصهٔ سایبری به شدت در نظام‌های پیچیده‌ای از شبکه‌های مختلف توزیع شده و ای بسا که در این ساختار شبکه‌ای، قدرت بازیگری نهادها و سازمان‌های غیردولتی یا حتی بازیگران بیرون از ساختار حاکمیت‌ها به مراتب بیشتر و گسترده‌تر از نهادها و سازمان‌های رسمی درون ساختار حاکمیتی باشد.

بر اساس اصول فوق، و نیز بر اساس فهم کلاسیک از سیاست بین‌الملل، تقریباً تمامی کشورهای جهان هم در غرب و هم شرق به دو جمع‌بندی شفاف در زمینهٔ عرصهٔ سایبری رسیده‌اند:

نخست: عرصهٔ سایبری امتداد دنیای فیزیکی و جهان واقعی است و لذا همچون زمین، دریا، هوا و فضا، به عنوان عرصهٔ پنجم، یک قلمرو حاکمیتی است که هم کشورها و نظام‌های سیاسی حق اعمال حاکمیت ملی بر آن را دارند و هم قوانین، ارزش‌ها، میثاق‌ها و عهدنامه‌ها و توافق‌نامه‌های مشترک بین‌المللی و جهانی قابلیت اجرا و تعمیم در این عرصه را دارند.

دوم: با توجه به ماهیت متفاوت عرصهٔ سایبری نسبت به عرصه‌های حاکمیتی سابق، نمی‌توان از طریق مکانیسم‌ها و سازوکارهای کلاسیک و سنتی به مدیریت این عرصه پرداخت. تجربهٔ تمامی کشورهایی که در این کتاب مورد مطالعه قرار گرفت، این است که حکمرانی در این عرصه مستلزم تغییرات پارادایمی در ذهنیت حکمرانان نسبت به مقولات مهمی همچون حکمرانی، قلمرو، اعمال حاکمیت، مرزها، امنیت، مشروعیت، ماهیت تهدیدها و حملات و ... به خصوص در مقایسه با سبک‌ها و شیوه‌های کلاسیک است.

- **دلالت‌ها**

اصول و جمع‌بندی‌ای که در بالا به آن‌ها اشاره شد، دارای معانی و دلالت‌های بسیاری در خصوص حکمرانی سایبری هم در بُعد داخلی و هم در بُعد بین‌المللی و جهانی است. صرف‌نظر از ابعاد داخلی حکمرانی سایبری که در این کتاب موضوعیت ندارد، در ارتباط با سیاست خارجی، مسئلهٔ بسیار واضح این است که نظام حکمرانی کشور برای توسعهٔ نفوذ و اقتدار سایبری خود در عرصهٔ منطقه‌ای و بین‌المللی باید به دنبال تدوین دیپلماسی سایبری مشخص با سازوکار اجرایی معین بر اساس مفاهیم و مقولاتی که در فصل دهم این کتاب به آن پرداخته شد، باشد. حرکت در مسیر تدوین دیپلماسی سایبری نیز مستلزم فهم الزامات دلالتی است که مهم‌ترین آن‌ها به شرح ذیل است:

۱. کلیت عرصهٔ سایبری به شیوه‌های سنتی و تنها بر اساس رویکردهای ملی قابل مدیریت نیست. لذا حتی در پیشرفته‌ترین کشورها نیز هیچ سازوکار ملی به تنهایی توانایی مدیریت و کنترل این عرصه، از حق اعمال حاکمیت گرفته تا مقابله با تهدیدات و حملات سایبری و ...، را نداشته و ندارد. مدیریت فضای سایبری تنها از طریق مکانیسم‌ها و رویکردهای جمعی مبتنی بر درک متقابل (ظرفیت‌سازی و اعتمادسازی) در سطوح منطقه‌ای و بین‌المللی

امکان‌پذیر است. رویکرد مشارکتی در حکمرانی در عرصهٔ سایبری تقریباً وجه مشترک رویکرد تمامی کشورها در تدوین دیپلماسی سایبری بوده است.

۲. تقریباً تمامی سیاست‌های پیشگیرانه و دفاعی سایبری کشورها یا با چالش اساسی مواجه شده و یا نشان داده‌اند که در برابر تهدیدات جدید سایبری به آسانی آسیب‌پذیرند. دنیا در حال گذار از مرحلهٔ «پیشگیری ـ دفاع» و تمرکز بر «قابلیت‌های شناسایی و ردیابی» فعالیت‌های سایبری است؛ امری که بازهم ضرورت همکاری و اتخاذ رویکردهای منطقه‌ای و بین‌المللی را دو چندان می‌کند. در فصل دوم به مهم‌ترین اقدامات و ابتکارات منطقه‌ای و بین‌المللی در عرصهٔ سایبری اشاره شد. ایران نیز باید مشارکت بیشتری در این اقدامات و ابتکارات منطقه‌ای و بین‌المللی با هدف گذار به اقتدار سایبری (در بُعد «شناسایی و ردیابی» حملات و تهدیدات سایبری) داشته باشد.

۳. در حال حاضر عمدهٔ طرح‌های فناورانه مهم از طریق مشارکت و سرمایه‌گذاری‌های مشترک منطقه‌ای و بین‌المللی دنبال می‌شود. با توجه به اینکه در عرصهٔ سایبری، فناوری و تحولات فنی ـ زیرساختی مرتبط با آن حرف اول و آخر را می‌زند، برای توسعهٔ اقتدار سایبری کشور در عرصهٔ جهانی، ایران باید بخشی از یک طرح «فناورانهٔ بین‌المللی» باشد تا بر اساس آن نوعی وابستگی متقابل به کشور ایجاد شود. به عبارت دیگر، مشارکت در یک طرح بین‌المللی فناورانه در حوزهٔ هوش مصنوعی، اینترنت اشیا، بلاک‌چین و ...، قدرت بازیگری کشور را در عرصهٔ سایبری بین‌المللی چندین برابر می‌کند. در عرصهٔ سایبری، انزوای فناورانه بزرگ‌ترین تهدیدی است که می‌تواند اساس حاکمیت یک کشور را به چالش بکشد.

۴. همان طور که در فصل نهم در ارتباط با گافام مطرح شد، پلتفرم‌ها بازیگران جدید عرصهٔ سیاست خارجی و روابط بین‌الملل هستند. تقریباً

شکی وجود ندارد که میدان نبرد و منازعات آتی کشورها در عرصهٔ سایبری و پلتفرم‌ها خواهد بود. منازعهٔ آمریکا با چین بر سر هوآوی، زد.تی.ای، تیک‌تاک، وی‌چت و ... مصداق روشنی از این ادعاست. علاوه بر این، عمده دارایی‌ها و دستاوردهای مهم فناوری در عرصهٔ سایبری در دست همین پلتفرم‌ها و کمپانی‌های بزرگ بین‌المللی است. تأثیرات فرامرزی فعالیت‌های این شرکت‌ها و کمپانی‌ها به لحاظ سیاسی، اقتصادی، فرهنگی و امنیتی بعضاً از کنشگری سیاسی و بین‌المللی مجموع دهها کشور نیز بیشتر است. در عرصهٔ سیاست بین‌الملل، این طیف از بازیگران نوین جهانی مستلزم تعاملات دیپلماتیک متفاوتی در مقایسه با سایر عرصه‌های کلاسیک است. در این بخش کشور نیاز به دیپلمات‌های مسلط به حوزهٔ فناوری دارد تا بتوانند به زبان سایبری صحبت کنند؛ موضوعی که از توان دیپلمات‌ها و سیاستمداران کلاسیک خارج است.

۵. پارامترهای قدرت در عرصهٔ سایبری نیز دیگر وابسته به بروکراسی سازمانی و قلمروهای فیزیکی وابسته به آن همچون مرز و حریم هوایی و دریایی و صادرات و واردات و نیز خط‌الرأس جغرافیایی و ... نیستند. پارامترهای قدرت در عرصهٔ سایبری بسته به تعریف و ایجاد «قلمروهای دقیق سایبری» در جهانی بدون مرز است که از طریق آن می‌توان برای ساختارهای حکمرانی کلاسیک قوام و تداوم ایجاد کرد. قلمروهای سایبری برخلاف گروه‌های نیابتی در عرصه‌های کلاسیک، فاقد مکانمندی و زمانمندی هستند و لذا محدودیت‌های آن‌ها را ندارند.

۶. کشور در حوزه‌های مختلف (نرم‌افزار، سخت‌افزار، شبکه و خدمات) نیاز به برندهای سایبری اقتدارساز در عرصهٔ منطقه‌ای و بین‌المللی دارد تا از طریق آن‌ها بتوان بیشتر در تدوین پروتکل‌ها و استانداردسازی‌ها در مجامع

و محافل فنی بین‌المللی مشارکت کرد. با توجه به اینکه هیچ دولتی به تنهایی توانایی تأمین بودجه و نیازهای مادی لازم برای برندسازی در عرصهٔ سایبری را ندارد، باید به فکر اقتصاد فناوری، اقتصاد شبکه‌ای، اقتصاد پلتفرمی و ... بود تا این عرصه از حکمرانی کشور نیز بتواند به صورت مستقل، خوداتکا و بدون نیاز به کمک‌های رسمی تداوم یابد. در واقع تنها از طریق به رسمیت شناختن و شکل‌گیری اقتصاد پلتفرمی با سازوکارهای مشخص سرمایه‌گذاری، توسعه و پیشرفت است که می‌توان نسبت به ظهور کمپانی‌ها و شرکت‌های بزرگ آی‌تی و فناوری ملی با زمینه و پتانسیل اثرگذاری فراملّی در سطح منطقه‌ای و بین‌المللی امیدوار بود. نمونه‌های چنین برندهای فناوری و سایبری را می‌توان به سهولت در هند، کره جنوبی، آفریقای جنوبی و دیگر کشورهای در حال توسعه نیز یافت.

۷. علی‌رغم ادعای استقلال عرصهٔ سایبری و خنثی بودن فناوری‌های مرتبط با آن، رقابت جریان‌های قالب حکمرانی بین‌المللی سایبری به همان سبک و سیاق گذشته به شدت ایدئولوژیک و سیاسی است، هرچند این رقابت‌ها عمدتاً در پوشش مسائل فنی، تجاری و اقتصادی روایت می‌شود. نزاعی که امروزه بر سر فعالیت‌های شرکت‌های هوآوی، زدتی‌ای، وی‌چت و تیک‌تاک بین آمریکا و چین درگرفته، فشاری که آمریکا برای قطع همکاری کشورهای اروپایی، کانادا و استرالیا با این شرکت‌های چینی راه‌اندازی کرده، شاهد روشنی بر این مدعاست. از این رو هر گونه برنامه‌ریزی، سیاست‌گذاری و تدوین استراتژی برای همراهی با این جریان‌ها یا بالعکس، هر گونه برنامه‌ریزی یا سیاست‌گذاری برای به چالش کشیدن این جریان‌ها در عرصهٔ منطقه‌ای و بین‌المللی نیز باید با توجه به ملاحظات سیاسی، ایدئولوژیک و البته در پوشش الزامات فنی و تجاری

باشد. به طور مثال با توجه به وابستگی تام و تمام حیات اقتصادی کمپانی‌های بزرگ آی‌تی آمریکا (از جمله گوگل، فیس‌بوک، اپل و ...) به «جریان آزاد و فرامرزی داده‌ها»، راه‌اندازی گفتمان‌ها و جریان‌هایی همچون اصل «محلی‌سازی داده‌ها»، «تدوین رژیم‌های بازرسی و الزامات تست‌های امنیت سایبری برای کمپانی‌های خصوصی»، «اعمال حاکمیت قوانین ملی بر فناوری و خدمات نوآوری» و ... از طریق کانال‌های دیپلماتیک و سیاسی کشور در سطح منطقه‌ای و بین‌المللی اثراتی به مراتب گسترده‌تر و وسیع‌تر از هر گونه اقدام سیاسی یا حتی نظامی دیگری می‌تواند در مواجهه و مقابله با سیاست‌های این کشور داشته باشد.

پیوست‌ها

فهرست مهم‌ترین اقدامات و ابتکارات صورت‌گرفته در ارتباط با دیپلماسی سایبری در سطح بین‌الملل

ردیف	پیمان‌های چندجانبه
۱	سازمان همکاری شانگهای، آیین‌نامهٔ بین‌المللی رفتار برای امنیت اطلاعات ۲۰۱۵. Shanghai Cooperation Organization, International Code of Conduct for Information Security.
۲	اتحادیهٔ بین‌المللی مخابرات، قانون اساسی، کنوانسیون و مقررات اداری (مقررات رادیویی و مقررات ارتباط از راه دور (ملبورن) (دبی)، ۲۰۱۴ و ۲۰۱۶. International Telecommunication Union, Constitution, Convention and Administrative Regulations (Radio Regulations and Telecom Regulations (Melbourne) (Dubai).
۳	شورای اروپا، پروتکل الحاقی کنوانسیون جرایم سایبری، در خصوص جرم‌انگاری انجام اعمال نژادپرستانه و بیگانه‌هراسی از طریق سیستم‌های رایانه‌ای، ۲۰۰۳. Council of Europe, Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems.
۴	شورای اروپا، کنوانسیون جرایم سایبری، ۲۰۰۱. Council of Europe, Convention on Cybercrime.

۵	سازمان تجارت جهانی، توافق‌نامهٔ کلی تجارت کالا و خدمات (الحاقیِ ارتباطات از راه دور)، ۱۹۹۷. WTO, General Agreement on Trade in Goods and Services (Annex on Telecommunications).
	پیمان‌های منطقه‌ای
۶	اتحادیهٔ آفریقا، دستورالعمل‌های امنیتی زیرساخت‌های اینترنتی آفریقا: طرح مشترک جامعهٔ اینترنت و کمیسیون اتحادیهٔ آفریقا (توصیه‌ها)، ۲۰۱۷. African Union, Internet Infrastructure Security Guidelines for Africa: A Joint Initiative of the Internet Society and the Commission of the African Union (Recommendations).
۷	اتحادیهٔ اروپا، طرح پیشنهادی مقررهٔ اتحادیهٔ اروپا دربارهٔ تقویت آژانس امنیت سایبری اتحادیهٔ اروپا (ENISA)، ۲۰۱۷. EU, Proposal for an EU Regulation on Strengthening ENISA.
۸	اتحادیهٔ اروپا، آیین‌نامهٔ رفتاری ارائه‌دهندگان خدمات ابری، نسخهٔ ۱/۷، ۲۰۱۷. EU, Code of Conduct for Cloud Services Providers, v. 1.7.
۹	اتحادیهٔ اروپا، ارتباطات مشترک، انعطاف‌پذیری، بازدارندگی و دفاع: تأمین امنیت سایبری اتحادیهٔ اروپا، ۲۰۱۷. EU, Joint Communication, Resilience, Deterrence and Defence: Building Strong Cyber Security for the EU.
۱۰	سازمان کشورهای آمریکایی (OAS)، کمیتهٔ ضد تروریسم بین آمریکایی، کارگروه همکاری و اقدامات اعتمادسازی در فضای سایبری، ۲۰۱۷. OAS, Inter-American Committee Against Terrorism, Working Group on Cooperation and Confidence-Building Measures in Cyberspace.
۱۱	آسه‌آن، بیانیهٔ ریاست (بندهای ۲۳ و ۳۲) و برنامهٔ ظرفیت سایبری آسه‌آن، ۲۰۱۷. ASEAN, Chairman’s Statement (para’s 23 and 32) and ASEAN Cyber Capacity Programme.

۱۲	دبیرخانهٔ عمومی ایبرو ـ آمریکا، ارتباطات ویژه در خصوص همکاری در زمینهٔ امنیت سایبری، ۲۰۱۶. Ibero-American General Secretariat, Special Communication on Cooperation on Cyber Security.
۱۳	اتحادیهٔ اروپا، دستورالعمل امنیت شبکه، ۲۰۱۶. EU, Network Security Directive.
۱۴	اتحادیهٔ اروپا، حفاظت عمومی از مقررهٔ اطلاعات، ۲۰۱۶. EU, General Protection of Data Regulation.
۱۵	شورای اروپا، حکمرانی اینترنت ــ راهبرد شورای اروپا ۲۰۱۶ ــ ۲۰۱۹، ۲۰۱۶. Council of Europe, Internet Governance – Council of Europe Strategy 2016-2019.
۱۶	ناتو، اعلامیهٔ اجلاس ورشو بند ۵ کاربست‌پذیری در فضای سایبری، ۲۰۱۶. NATO, Warsaw Summit Communique re Article 5 Applicability in Cyberspace.
۱۷	آسه‌آن، برنامهٔ کاری مجمع منطقه‌ای در خصوص امنیت و کاربرد فناوری اطلاعات و ارتباطات، ۲۰۱۵. ASEAN, Regional Forum Work Plan on Security of and in the Use of ICTs.
۱۸	سازمان همکاری اقتصادی آسیا ـ اقیانوسیه، برنامهٔ عملیاتی راهبردی کارگروه ارتباطات از راه دور و اطلاعات ۲۰۱۶ ــ ۲۰۲۰، ۲۰۱۵. APEC Telecommunications and Information Working Group Strategic Action Plan 2016-2020.
۱۹	سازمان همکاری اقتصادی آسیا ـ اقیانوسیه، سیستم قوانین حفظ حریم خصوصی فرامرزی و چارچوب حریم خصوصی، ۲۰۱۵. APEC Cross Border Privacy Rules (CBPR) System and Privacy Framework
۲۰	اتحادیهٔ اروپا/ آژانس امنیت سایبری اتحادیهٔ اروپا، راهنمای روش مناسب افشای آسیب‌پذیری، ۲۰۱۵. EU/ENISA, Good Practice Guide on Vulnerability Disclosure.

۲۱	اتحادیهٔ آفریقا، کنوانسیون امنیت سایبری و محافظت از داده‌های شخصی، ۲۰۱۴. African Union, Convention on Cyber Security and Personal Data Protection.
۲۲	اتحادیهٔ اروپا، راهبرد امنیت سایبری اتحادیهٔ اروپا: فضای سایبری آزاد، ایمن و مطمئن، ۲۰۱۳. EU, Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace.
۲۳	اتحادیهٔ کشورهای عربی/ شورای همکاری خلیج فارس، کنوانسیون عربی در زمینهٔ مبارزه با جرایم فناوری اطلاعات، ۲۰۱۳. League of Arab States/ Gulf Cooperation Council, Arab Convention on Combating Information Technology Offences.
۲۴	اتحادیهٔ اروپا، کمیسیون اقتصادی آفریقا، برنامهٔ عملیاتی منطقه‌ای آفریقا در خصوص اقتصاد دانش (ARAPKE)، ۲۰۰۵. UN Economic Commission for Africa , African Regional Action Plan on the Knowledge Economy (ARAPKE).
۲۵	سازمان کشورهای آمریکایی، اتخاذ یک راهبرد جامع بین آمریکایی برای مقابله با تهدیدات فضای سایبری: یک رویکرد چندبعدی و چندرشته‌ای به ایجاد فرهنگ امنیت سایبری، ۲۰۰۴. OAS, Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cyber Security: a Multidimensional and Multidisciplinary Approach to Creating a Culture of Cyber Security.
۲۶	اتحادیهٔ اروپا، کمیسیون اقتصادی آفریقا، طرح ابتکاری جامعهٔ اطلاعاتی آفریقا، ۱۹۹۶. UN Economic Commission for Africa, African Information Society Initiative.

پیمان‌های دوجانبه	
۲۷	آمریکا ـ هندوستان، ۲۰۱۷. US-India, 2017.
۲۸	چین ـ اتحادیهٔ اروپا، توافقات امنیت سایبری/ اجلاس مشترک، ۲۰۱۲. China-EU Cyber Security Agreements/ Joint Summit 2012.
۲۹	چین ـ روسیه، امنیت اطلاعات/ توافق، ۲۰۱۵. China-Russia Information Security Agreement.
۳۰	توافق چین ـ آمریکا، ۲۰۱۵. China-US Agreement.
۳۱	آمریکا ـ روسیه، ۲۰۱۵. US – Russia.
۳۲	چین ـ ژاپن ـ کره، تفاهم‌نامهٔ مشترک در مورد تیم پاسخگویی به رخدادهای امنیتی کامپیوتر با مسئولیت ملی، ۲۰۱۱. China-Japan-Korea Joint MOU on CSIRT with National Responsibility.
طرح ابتکاری یک‌جانبهٔ دولتی با هدف اعمال برنامه‌های بین‌المللی	
۳۳	چین، راهبرد بین‌المللی همکاری در فضای سایبری، ۲۰۱۷. China, International Strategy of Cooperation on Cyberspace.
۳۴	هلند، ساخت پل‌های دیجیتال ـ راهبرد سایبری بین‌المللی، ۲۰۱۷. Netherlands, Building Digital Bridges- International Cyber Strategy.
۳۵	استرالیا، راهبرد مشارکت سایبری بین‌المللی، ۲۰۱۷. Australia, International Cyber Engagement Strategy.
۳۶	آمریکا، راهبرد بین‌المللی مختص فضای سایبری، ۲۰۱۷. US, International Strategy for Cyberspace.

سازمان‌های بین‌المللی **شورای امنیت سازمان ملل متحد، مجمع عمومی و گروه کارشناسان دولتی (GGE)**	
۳۷	گروه متخصصان دولتی در حوزهٔ تحولات حوزهٔ اطلاعات و ارتباطات از راه دور در زمینهٔ امنیت سایبری، ۲۰۱۵. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE).
۳۸	قطعنامهٔ ۲۱۷۸ شورای امنیت، ۲۰۱۴. Security Council Resolution 2178.
۳۹	گروه متخصصان دولتی ۲۰۱۳. GGE 2013.
۴۰	گروه متخصصان دولتی ۲۰۱۰. GGE 2010.
۴۱	قطعنامهٔ ۵۷/۲۳۹ مجمع عمومی سازمان ملل: ایجاد فرهنگ جهانی امنیت سایبری، ۲۰۰۳. UNGA Resolution 57/239: Creation of a Global Culture of Cyber Security.
همایش‌های سازمان‌های تخصصی	
۴۲	اتحادیهٔ بین‌المللی مخابرات، کنفرانس جهانی توسعهٔ ارتباطات راه دور (دبی، ۲۰۱۴) قطعنامهٔ ۴۵ ـ سازوکارهای تقویت همکاری در حوزهٔ امنیت سایبری، از جمله مقابله و مبارزه با هرزنامه، ۲۰۱۴. ITU, World Telecommunication Development Conference (Dubai, 2014) Resolution 45 – Mechanisms for Enhancing Cooperation on Cyber Security, Including Countering and Combating Spam.
۴۳	اتحادیهٔ بین‌المللی مخابرات، دستور کار جهانی امنیت سایبری، ۲۰۰۷. ITU, Global Cyber Security Agenda.

۴۴	اتحادیهٔ بین‌المللی مخابرات، اجلاس جهانی جامعهٔ اطلاعات، تعهدات تونس، ۲۰۰۵. ITU, World Summit on the Information Society, Tunis Commitments.
	سازمان‌های استاندارد
۴۵	مؤسسهٔ ملی استاندارد و فناوری آمریکا، چارچوب بهبود زیرساخت بحرانی امنیت سایبری ۱/۱، ۲۰۱۷. US NIST, Framework for Improving Critical Infrastructure Cyber Security 1/1.
۴۶	مؤسسهٔ ملی استاندارد و فناوری آمریکا ـ طرح ملی آموزش امنیت سایبری، چارچوب نیروی ـ کار امنیت سایبری، ۲۰۱۷. US NIST-NICE Cyber Security Workforce Framework.
۴۷	مؤسسه ملی استاندارد و فناوری آمریکا، راهنمای به‌اشتراک‌گذاری اطلاعات تهدید سایبری، ۲۰۱۶. US NIST, Guide to Cyber Threat Information Sharing.
۴۸	ایزو ۲۷۰۰۱ ـ تکنیک‌های امنیتی فناوری اطلاعات ـ سیستم‌های مدیریت امنیت اطلاعات ـ الزامات، ۲۰۱۳. ISO 27001 -Information Technology Security Techniques Information Security Management Systems – Requirements.
۴۹	ایزو ۲۹۱۴۷ ـ افشای آسیب‌پذیری برای فروشندگان، ۲۰۱۴. ISO 29147, Vulnerability Disclosure to Vendors.
۵۰	ایزو ۲۷۰۳۲، دستورالعمل‌های امنیت سایبری، ۲۰۱۲. ISO 27032, Guidelines for Cyber Security.
۵۱	بخش استانداردسازی مخابرات، X. 1500، تبادل اطلاعات امنیت سایبری ـ بررسی اجمالی امنیت سایبری، ۲۰۱۱. ITU-T, X.1500 Cyber Security information exchange – Overview of Cyber Security.

۵۲	سازمان امنیت و همکاری اروپا، اعلامیهٔ مینسک، ۲۰۱۷. OSCE, Minsk Declaration.
۵۳	سازمان امنیت و همکاری اروپا، تصمیم شورای وزرا ۵/۱۶، فعالیت‌های مرتبط با کاهش خطرات درگیری‌های ناشی از بکارگیری فناوری اطلاعات و ارتباطات، ۲۰۱۶. OSCE, Ministerial Council Decision 5/16, Efforts Related to Reducing The Risks of Conflict Stemming from the Use of ICTs.
۵۴	سازمان امنیت و همکاری اروپا، تصمیم ش. ۱۲۰۲ در خصوص اقدامات اعتمادساز به منظور کاهش خطرات درگیری‌های ناشی از بکارگیری فناوری اطلاعات و ارتباطات، ۲۰۱۶. OSCE, Decision No. 1202 on Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of ICTs.
۵۵	سازمان امنیت و همکاری اروپا، تصمیم دائمی شورا ش. ۱۱۰۶، ۲۰۱۳. OSCE, Permanent Council Decision No. 1106.
	اظهارنامه‌های بین‌دولتی
۵۶	اعلامیهٔ شیامن رهبران گروه بریکس، ۲۰۱۷. BRICS, Leaders Xiamen Declaration.
۵۷	جی ۲۰، بیانیهٔ مبارزه با تروریسم، ۲۰۱۷. G20, Statement on Countering Terrorism.
۵۸	جی ۷، اعلامیهٔ مربوط به رفتار مسئولانهٔ کشورها در فضای سایبری، ۲۰۱۷. G7, Declaration on Responsible States Behavior in Cyberspace.
۵۹	جی ۷، اصول و اقدامات مربوط به فضای سایبری، ۲۰۱۶. G7, Principles and Actions on Cyber.
۶۰	بریکس، دستور کار و برنامهٔ عملیاتی توسعهٔ فناوری اطلاعات و ارتباطات، ۲۰۱۶. BRICS, ICT Development Agenda and Action Plan.
۶۱	جی ۲۰، اطلاعیهٔ رهبران اجلاس آنتالیا، ۲۰۱۵. G20, Antalya Summit Leaders Communique.
۶۲	جی ۷، اطلاعیهٔ نشست وزیران امور خارجه، ۲۰۱۵. G7, Foreign Ministers' Meeting Communiqué.

اقدامات غیردولتی‌ها	
موقوفهٔ کارنگی، به سوی یک هنجار جهانی در برابر دست‌کاری در داده‌های مالی، ۲۰۱۷. Carnegie Endowment, Toward A Global Norm Against Manipulating the Integrity of Financial Data.	۶۳
مرکز عالی همکاری‌های دفاع سایبری ناتو، راهنمای تالین ۲/۰، ۲۰۱۷. CCDCOE, Tallinn Manual 2.0.	۶۴
مرکز جهانی ظرفیت امنیت سایبری آکسفورد، الگوی بلوغ ظرفیت امنیت سایبری برای ملت‌ها، ۲۰۱۷. Oxford Global Cyber Security Capacity Centre, Cyber Security Capacity Maturity Model for Nations.	۶۵
موقوفهٔ کارنگی (اروپا)، حکمرانی فضای سایبری: نقشهٔ رهبری خط‌مشی سایبری در آن سوی اقیانوس اطلس (ص ۷۴ – ۷۵)، ۲۰۱۶. Carnegie Endowment (Europe), Governing Cyberspace: A Road Map for Transatlantic Cyberpolicy Leadership (pp. 74 - 75).	۶۶
ائتلاف آزادی اینترنتی، دستور کار تالین برای آزادی اینترنتی، ۲۰۱۴. Freedom Online Coalition, Tallinn Agenda for Freedom Online.	۶۷
نشست چندذی‌نفعی جهانی در مورد حکمرانی اینترنت، بیانیهٔ چندذی‌نفعی، ۲۰۱۴. Netmundial, Multistakeholder Statement.	۶۸
دانشگاه استنفورد، پیش‌نویس کنوانسیون بین‌المللی برای تقویت حفاظت در برابر جرایم سایبری و تروریسم، ۲۰۰۱. Stanford University, Draft International Convention to Enhance Protection from Cyber Crime and Terrorism.	۶۹

اقدامات بخش‌های صنعتی و آی‌تی بزرگ	
فیس‌بوک، ایجاد جامعهٔ جهانی، ۲۰۱۷. Facebook, Building Global Community.	۷۰
گوگل، امنیت دیجیتال و فرایند قانونی: نوسازی استانداردهای دسترسی برون‌مرزی دولت در عصر ذخیره‌سازی ابری، ۲۰۱۷. Google, Digital Security & Due Process: Modernizing Cross-Border Government Access Standards for the Cloud Era.	۷۱
انجمن اینترنتی جهانی برای مبارزه با تروریسم، ۲۰۱۷. Global Internet Forum to Counter Terrorism.	۷۲
مایکروسافت/ RAND، سازمان بین‌المللی انتساب حملهٔ سایبری، ۲۰۱۷. Microsoft/ RAND, International Cyberattack Attribution Organization.	۷۳
مایکروسافت، کنوانسیون دیجیتال ژنو، ۲۰۱۷. Microsoft, Digital Geneva Convention.	۷۴
آیکان یا شرکت اینترنتی نام‌ها و شماره‌های واگذارشده، پیش‌نویس چارچوب اپراتور رجیستری برای پاسخ به تهدیدات امنیتی، ۲۰۱۷. ICANN, Draft Framework for Registry Operator to Respond to Security Threats.	۷۵
مایکروسافت، از طرح ایده تا اجرا: امکان پیشرفت در هنجارهای امنیت سایبری، ۲۰۱۷. Microsoft, From Articulation to Implementation: Enabling Progress on Cyber Security Norms.	۷۶
هیئت سازمان بین‌المللی کمیسیون‌های اوراق بهادار، راهنمای تاب‌آوری سایبری زیرساخت‌های بازار مالی، ۲۰۱۶. Board of the International Organization of Securities Commissions, Guidance on Cyber Resilience for Financial Market Infrastructures.	۷۷
کمیسیون اوراق بهادار و بورس، راهنمای امنیت سایبری، ۲۰۱۶. Securities and Exchange Commission, Cyber Security Guidance.	۷۸

۷۹	آیکان، بیانیهٔ مونته‌ویدئو در خصوص آیندهٔ همکاری‌های اینترنتی، ۲۰۱۳. ICANN, Montevideo Statement on the Future of Internet Cooperation.
	سازمان‌های اجرای قانون
۸۰	اینترپل، راهبرد جهانی جرایم سایبری، ۲۰۱۷. Interpol, Global Cybercrime Strategy.
۸۱	یوروپل، مرکز جرایم سایبری یوروپل (EC3)، گروه ویژهٔ اقدام مشترک علیه جرایم سایبری، ۲۰۱۴. Europol, European Cybercrime Center (EC3), Joint Cybercrime Action Taskforce.
	سایر اقدامات و برنامه‌ها
۸۲	تمهیدات واسنار در خصوص کنترل صادرات سلاح‌های متعارف و کالاها و فناوری‌های دومنظوره، ۲۰۱۷. Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.
۸۳	فرایند نصف‌النهار برای حفاظت از زیرساخت‌های اطلاعات بحرانی، ۲۰۰۵. Meridian Process for Critical Information Infrastructure Protection.

نمایه

Governance in the Fifth Dom: Toward Cyber Diplomacy

Abbas Ghanbari Baghestan

&

Abdolhosein Kalantari

2021

زمین، دریا، هوا و فضا؛ و هم اکنون عرصه سایبری، به عنوان عرصهٔ پنجم حکمرانی، حوزه‌ای نسبتا جدید برای بسط قدرت و نفوذ در تعاملات منطقه‌ای و بین‌المللی کشورهاست. در مطالعه‌ای که در کتب، متون علمی و نیز اسناد رسمی سایبری کشورها صورت گرفت، در مجموع بیش از هشتاد سند یا اعلامیه تبیین کنندهٔ دیپلماسی‌سایبری کشورها، استراتژی‌های ملی، دوجانبه و چندجانبه منطقه‌ای و بین‌المللی در ارتباط با دیپلماسی‌سایبری و رویکردهای جهانی به این مقوله شناسایی شده که همگی نشان از درجه و اهمیت این موضوع در بازیگری منطقه‌ای و بین‌المللی در دیپلماسی نوین جهانی دارد.

این کتاب پس از مطالعه جامع اقدامات و سازوکارهای منطقه‌ای و بین‌المللی در ارتباط با دیپلماسی‌سایبری و نیز شناسایی مهمترین بازیگران این عرصه در سطوح ملی، بین‌المللی و بخش خصوصی، به ارزیابی و تحلیل دیپلماسی‌سایبری چند کشور از جمله آمریکا، روسیه، چین، ژاپن، اتحادیه اروپا و مالزی پرداخته است.

در یک فصل جداگانه، پلتفرم ها (به خصوص گافام) به عنوان بازیگران جدید در سپهر سیاست بین‌الملل، در چارچوب دیپلماسی شرکتی، عوامل قدرت‌افزای آنها در حکمرانی شبکه‌ای و نیز چالش‌هایی که از این ناحیه متوجه دیپلماسی به معنای کلاسیک آن شده، واکاوی شده است.

کتاب در نهایت با احصاء مبانی، اصول و مکانیسم های راهبردی و اجرایی دیپلماسی‌سایبری کشورهای مورد مطالعه، و نیز از طریق تکنیک هم‌افزایی فکری در جلسات بحث متمرکز با محققان و اندیشمندان عرصه سایبری، در مجموع ۲۴ مقوله به عنوان «جدول مقولات سایبری» برای تدوین الگوی عملی دیپلماسی سایبری کشور پیشنهاد داده است.

ژئوپلیتیک سایبری

بازدارندگی

تروریسم سایبری

حریم خصوصی

قلمروسایبری

استراتژیست سایبری

لایه های زیرساخت

بخش خصوصی

محتوا

عدم‌تخاصم

تسری

جرایم سایبری

مرزسایبری

کسب وکارسایبری

دسترسی

مردم

ذی‌نفعان

ISBN 978-622-97700-6-1

قیمت: ۶۵۰۰۰۰ ریال