بسم‌الله الرحمن الرحیم

امنیت سایبری در جهان – کشورهای آسیایی

مقدمه

رشد تمدنی انسان در دو دهه اخیر باعث شده دغدغه انسان‌ها از امنیت غذایی و جانی فراتر رفته و مفهوم امنیت سایبری شکل بگیرد. پیشتر خطرهایی که انسان‌ها تهدید می‌کردند، ناظر به نیازهای طبیعی او مانند غذا و پوشاک بود. امروزه، انسان‌ها در زندگی مجازی خود نیز، نیاز به امنیت دارند. همانند سایر شقوق امنیت، متولی اصلی حفظ امنیت سایبری مردم، حاکمیت‌ها هستند. به همین جهت معمولاً هرکشور سعی کرده متناسب با شرایط خارجی (مانند میزان تهدیدات) و داخلی (مانند فرهنگ جامعه) خود، به حفاظت از مرزهای سایبری‌اش بپردازد. معمولاً در این راستا، سندهای سیاستی مختلفی تصویب، شوراها و نهادهای متولی تأسیس و حتی پیمان‌نامه‌های خارجی و بین‌المللی تنظیم می‌شود.

در گزارش پیش‌رو، سیاست‌های امنیت سایبری چند نمونه از کشورهای آسیایی مورد بررسی قرار می‌گیرد. به‌طور خلاصه، آنچه در این گزارش بررسی می‌شود به شرح زیر است:

چین مهم‌ترین کشور بر هم زننده هژمونی آمریکا بر فضای سایبری است. به منظور ایجاد ثبات سیاسی و جلوگیری از تهدیدات نرم و سختِ داخلی و خارجی، جمهوری خلق چین در خط مشی امنیت سایبری خود دست به توسعه فناوری‌های پیشرفته و کنترل زیرساخت فضای سایبری و همچنین کنترل گردش اطلاعات و محتوا زده است. محصول این خط مشی‌ها، ایجاد دیوار آتش، نهادسازی و وضع قانون و مقررات بر تولید و انتشار محتوا و ذخیره‌سازی و انتقال داده، همگرا کردن بخش‌های سه‌گانه جامعه در راستای سیاست‌های ملی، ایجاد محدودیت در آزادی بیان و نظارت بر حریم خصوصی شده است. در جهت بین‌المللی نیز تلاش این کشور بر گفتمان سازی این مدل حاکمیت سایبری (cyber sovereignty) خود با شکل دادن به جاده ابریشم دیجتال و نفوذ در کشورهای آسیای جنوب شرقی و تقویت و استفاده از ظرفیت شرکت‌های بزرگ و فراملی چینی بوده است.

روسیه از کشورهای پیرو در بومی‌سازی سیاست امنیت سایبری دانسته می‌شود. رویکرد روسیه به امنیت سایبری و امنیت اطلاعات مبتنی بر تعهدی قوی به منافع ملی‌اش است. همان‌طور که طول زمان و تصمیمات سیاسی در صحنه عمل نشان می‌دهد، منافع دولتی به منافع فردی ارجح است. روسیه از دهه 1990 به‌طور فعال در مذاکرات بین‌المللی در مورد امنیت سایبری شرکت داشته است. برجسته‌ترین ابتکار ایجاد یک گروه دولتی ویژه از کارشناسان در زمینه استفاده و توسعه فناوری اطلاعات و ارتباطات تحت نظارت مجمع عمومی سازمان ملل بود. این گروه در دهه اخیر پیشرفت قابل‌توجهی در شرح و تفصیل درکی مشترک میان وضعیت نگرانی‌های امنیتی و قابل‌اجرا بودن قوانین بین‌المللی داشته است

کره‌جنوبی در سال‌های اخیر در حوزه فناوری دیجیتال پیشرفته، شبکه‌های کامپیوتری کارآمد و بالاترین نرخ نفوذ اینترنت پرسرعت عملکرد خوبی از خود به نمایش گذاشته است. با وجود توسعه و تحولات اخیر کره جنوبی در حوزه سایبری، این کشور مانند بسیاری از کشورها در زمینه امنیت سایبری آسیب‌پذیر بوده است. چالش‌های دولت کره در حوزه امنیت سایبری در دو محورِ تهدیدات و نفوذ خارجی و همچنین تهدیدات سایبری حاصل از تغییرات ژئوپلیتیکی شبه جزیزه خلاصه می‌گردد. مسائل اصلی چالش نخست در حوزه امنیت سایبری شامل هک، سرقت‌های بانک دیجیتالی و تضعیف زیرساخت‌های حیاتی از سوی دشمنان همسایه می‌شود. در محور دوم چالش‌ها مسئله اصلی کره جنوبی، تقویت زیرساخت‌های خود در مواجهه با تشدید رقابت تسلیحات سایبری در میان تبادل قدرت دو ابرقدرت ایالات متحده و چین است. از معایب حال حاضر در ساختار دولتی کره می‌توان به عدم وجود الزامات قانونی پایه جهت تداوم اجرای اصول طرح جامع امنیت سایبری در صورت تغییر و تحول دولت حاکم اشاره نمود.

باید توجه داشت که کشورها معمولاً در سیاست‌های مربوط به امنیت سایبری، ایده و شیوه حکمرانی سایبری خود را به نمایش می‌گذارند. بر این اساس، با مطالعه سیاست‌های امنیتی یک کشور در حوزه فضای مجازی، می‌توان به رویکرد حاکمیت آن در مواجه با فضای مجازی در دیگر حوزه‌ها هم پی برد. لذا این بررسی به ما کمک می‌کند تا ایده‌های موجود در حوزه حکمرانی فضای مجازی را شناخته و از تجربیات موفق و ناموفق دیگران برای طراحی الگوی مختار خود کمک بگیریم.

چین

مقدمه

از پایان جنگ سرد، ظهور چین جایگاهی را در مطالعه روابط بین‌الملل برای خود محفوظ داشته است. همان‌طور که قدرت فراگیر چین پس از یک دوره اصلاحات اقتصادی به‌طور پیوسته رشد کرد، نفوذ آن در جامعه بین‌المللی نیز به‌ویژه در زمینه سایبری و فناوری اطلاعات افزایش یافت. در حال حاضر، انقلاب در عرصه فناوری اطلاعات، از جمله اینترنت، شبکه‌های مخابراتی، سیستم‌های رایانه‌ای و فضاهای مجازی مرتبط، سبک زندگی انسان را تغییر داده و آثار عمیقی بر توسعه جامعه بشری بر جای گذاشته است (اداره فضای سایبری چین[1]، 2016). برای چین امروز، توسعه فناوری‌های پیشرفته[2] در قلب توسعه اقتصادی و امنیت ملی قرار دارد. ظهور شرکت‌های فناوری اطلاعات و ارتباطات (ICT) کلید رشد موازی میلیون‌ها شهروند و مصرف‌کننده چینی است که فعالانه در عصر اطلاعات شرکت می‌کنند. با وجود این، درحالی‌که جامعه در حال تغییر گسترده است، پکن دریافته است که پیشرفت‌های فناوری از پیشرفت‌ها در ظرفیت رسمی اداری برای مدیریت و کنترل فناوری‌های جدید پیشی گرفته است؛ بنابراین واکنش پکن ایجاد نهادها، قوانین و خط‌مشی‌های جدید برای مدیریت نرم‌افزار، سخت‌افزار و اطلاعات داخلی بوده است. این پیشرفت‌ها ویژگی‌های شرکت‌های ICT و کاربران اینترنت را در داخل و خارج از چین تغییر داده است (CSIS, n.d.). این نوشتار زمینه منجر به توسعه خط‌مشی امنیت سایبری چین و همچنین تأثیر و معنای خط‌مشی‌های دولتی، نهادها و هنجارهای قانونی این حوزه را موردبررسی قرار می‌دهد. علاوه‌بر این، این فصل پیامدهای خط‌مشی امنیت سایبری چین برای روابط بین‌الملل را مورد بحث قرار می‌دهد.

محیط داخلی و چالش امنیت سایبری

درحالی‌که اینترنت سهولت و کارایی بیشتری را در زندگی روزمره به ارمغان آورده است، این واقعیت که چین دارای بیشترین تعداد کاربران اینترنت در جهان و تعداد بالای حملات اینترنتی است، موضوع کم‌اهمیتی نیست.

توسعه اینترنت در چین

برای درک خط‌مشی امنیت سایبری چین، لازم است ابتدا تاریخچه استفاده از اینترنت در چین را بررسی کنیم. جالب اینجاست که هیچ توافقی در مورد اولین استفاده از اینترنت در چین وجود ندارد. درحالی‌که اسناد ثبت‌شده، نشان می‌دهد که مؤسسات دانشگاهی در دهه 1990 ایمیل‌هایی را به خارج از کشور ارسال می‌کردند، بحث در مورد زمانی که اولین ایمیل در سال 1986 یا 1987 تحویل داده شد، ادامه دارد.

به بیان وو ویمین[3]، از آکادمی علوم چین، یک ادعا این بود که اولین ایمیل برای دانشمند جک اشتاینبرگر[4] از سازمان اروپایی تحقیقات هسته‌ای (سرن)[5] در 25 اوت 1986، از یک ایستگاه کاری در مؤسسه فیزیک انرژی عظیم[6] ارسال شد. ادعای دیگر، به اولین ایمیلی اشاره می‌کند که توسط یک تیم تحقیقاتی مشترک چینی–آلمانی مستقر در مؤسسه چینی کاربردهای رایانه‌ای[7] به دانشگاه کارلسروهه در 20 سپتامبر 1987 تحت

---

[1] Cyberspace Administration of China
[2] cutting-edge technology
[3] Wu Weimin
[4] Jack Steinberger
[5] European Organization for Nuclear Research (CERN)
[6] Institute of High Energy Physics (IHEP)
[7] Chinese Institute of Computer Applications (ICA)

عنوان «در سراسر دیوار بزرگ، ما می‌توانیم به هر گوشه‌ای از دنیا دسترسی داشته باشیم» ارسال شد (گلدکورن[8]، 2012) که اولین گام چین به سوی عصر اینترنت را رقم زد.

درحالی‌که بحث‌ها در مورد مبدأ اولین ایمیل هنوز ادامه دارد، مناقشه‌ای در مورد پذیرش رسمی اینترنت توسط چین وجود ندارد. در 17 می 1994، اتصال TCP/IP میان مؤسسه فیزیک انرژی عظیم و مرکز شتاب‌دهنده خطی استنفورد[9] نشان‌دهنده ورود چین به فضای سایبری بود. یک هفته بعد، یک اتصال 64K بین مرکز ملی محاسبات و تسهیل شبکه‌سازی چین و Sprint در ایالات‌متحده برقرار شد و ارتباط چین با جهان را محقق کرد (PC World، 2004).

رشد اقتصادی مبتنی بر فناوری اطلاعات و ارتباطات

پکن توسعه اینترنت را به‌عنوان فرآیندی در تکامل از جامعه صنعتی به جامعه اطلاعاتی یا یک فرآیند اطلاعاتی‌سازی[10] می‌داند (PC World، 2004). در دو دهه گذشته، دولت چین به‌وضوح خط‌مشی‌های مدرن سازی را در عصر دیجیتال شناسایی کرده و فناوری‌های اطلاعاتی و ارتباطی جدید را در بخش‌های دولتی، صنعت، تجارت، آموزش و فرهنگ اتخاذ کرده است. اطلاعاتی‌سازی در حال حاضر هسته اصلی سیزدهمین برنامه پنج‌ساله چین (2016–2020) است که مستلزم کاربرد فناوری اطلاعات و ارتباطات پیشرفته در بخش‌های سیاسی، اقتصادی، نظامی، بهداشت، کشاورزی و محیط‌زیست است (آستین[11]، 2016).

هنگامی‌که اینترنت برای اولین بار در چین معرفی شد، سرعت پایین و زیرساخت‌های محدود کارایی آن را با مشکل مواجه کرده بود. از طریق اتصال خط زمینی، سرعت انتقال داده به تنها 64 کیلوبیت در ثانیه می‌رسید. از سوی دیگر، در سال 1996، چین تنها میزبان 2000 کامپیوتر بود که قابلیت اتصال به اینترنت را داشتند؛ اما پس‌ازآن و از زمان ظهور شرکت‌هایی مانند سینا، سوهو و نت ایز[12]، نسل اول کاربران اینترنت به‌سرعت در چین ظهور کردند. علیرغم اینکه اینترنت در حال حاضر مفهومی کلیشه‌ای است، اما در حال ایجاد تحول در زندگی و سبک زندگی میلیون‌ها انسان است. امروزه در چین، مردم از رایانه‌های شخصی، تبلت‌ها و تلفن‌های هوشمند برای بررسی ایمیل و ارتباط با دیگران از طریق برنامه‌های کاربردی رسانه‌های اجتماعی استفاده می‌کنند. به لطف توسعه نیرومند صنعت فناوری اطلاعات (IT)، میلیون‌ها نفر دست به تأسیس شرکت‌های خصوصی زده‌اند. برخی از شرکت‌های چینی از آن زمان به شرکت‌کنندگان اصلی صنعت فناوری اطلاعات جهانی تبدیل‌شده‌اند و امروزه جزو موفق‌ترین شرکت‌ها در چین هستند. تجارت الکترونیک بیش از 13 میلیون فرصت شغلی را در کشور کرده است. علی‌بابا، یکی از این شرکت‌های چینی، در حال حاضر پیشرو در تجارت آنلاین است و تعداد معاملات سالانه آن از مجموع eBay و آمازون بهتر است (فلورکروز و سو[13]، 2014).

در سال‌های اخیر، چین به پیشرفت‌های چشم‌نوازی در دنیای مجازی دست‌یافته است. مهم‌تر از همه، چین دارای بیشترین تعداد کاربران اینترنت است. درحالی‌که فناوری اینترنت به‌سرعت در حال رشد کردن بود تعداد کاربران چینی با سرعت انفجاری افزایش یافت. طبق گزارشی که مرکز اطلاعات شبکه اینترنت چین[14] در ژانویه 2018 ارائه کرد، چین میزبان 772 میلیون کاربر اینترنت است که 55.8 درصد از کل جمعیت این کشور را تشکیل می‌دهد (The Economic Times، 2018). چنین تعداد زیادی از کاربران اینترنت به یک نیروی محرکه برای رشد اقتصادی تبدیل‌شده است. بر اساس یک سند منتشرشده توسط آکادمی فناوری اطلاعات و ارتباطات که یکی از بخش‌های زیرمجموعه وزارت

---

[8] Goldkorn
[9] Stanford Linear Accelerator Center (SLAC)
[10] informatization
[11] Austin,
[12] Sina, Sohu, and NetEase
[13] FlorCruz & Sue
[14] China Internet Network Information Center (CNNIC)

صنعت و فناوری اطلاعات[۱۵] است، فعالیت‌های اقتصادی دیجیتال یا سایبری شامل تجارت الکترونیک، رایانش ابری و پرداخت آنلاین، در سال ۲۰۱۶ به ۳,۳۵ تریلیون دلار آمریکا رسید که نسبت به سال قبل از آن ۱۸,۹ درصد رشد داشته و ۳۰,۳ درصد از تولید ناخالص داخلی (GDP) چین را تشکیل می‌دهد(China Daily، 2017).

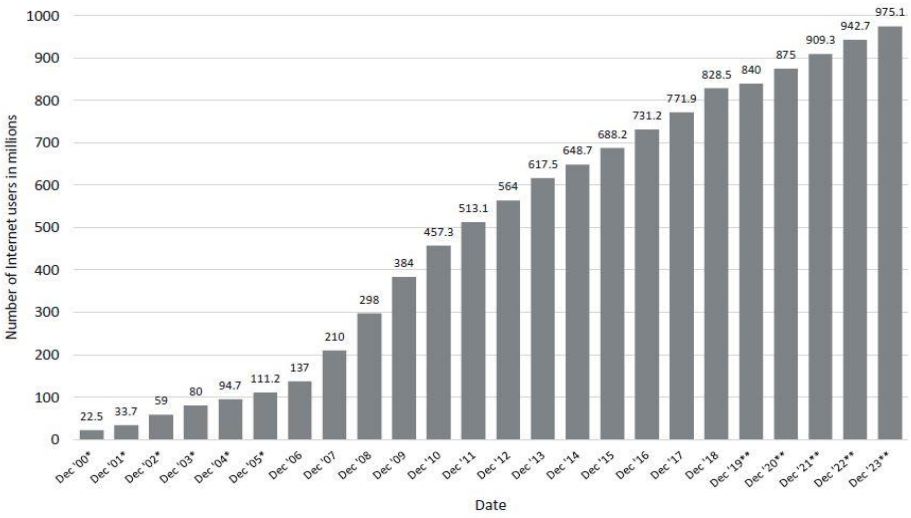
به‌طور خلاصه، کلید اطلاعاتی‌سازی، اینترنت است. در چین، زیرساخت اینترنت یا مستقیماً توسط دولت کنترل می‌شود یا متعلق به شرکت‌های خصوصی است که با دولت همکاری نزدیکی دارند. به این معنا، اینترنت بیشتر شبیه یک «اینترانت» در یک شرکت است و دولت ارائه‌دهنده خدماتی[۱۶] دفاع از اینترنت است. چنین ویژگی در تضاد با رویکرد ایالات‌متحده است (توماس[۱۷]، 2009: 455-456). از دید نخبگان سیاسی چین، اهمیت امنیت سایبری واضح است و توسعه فناوری اطلاعات و ارتباطات برای آینده امنیت و توسعه ملی حیاتی است. همان‌طور که رئیس‌جمهور چین، شی‌جین‌پینگ اشاره کرد، امنیت سایبری و اطلاعاتی‌سازی، هم ارتباط نزدیکی با یکدیگر دارند و هم ارتباط تنگاتنگی با توسعه ملی دارند، «امنیت ملی بدون امنیت سایبری ممکن نیست و هیچ مدرن سازی‌ای بدون اطلاعاتی سازی وجود ندارد»[۱۸] (اداره فضای سایبری چین، 2014).

چالش فزاینده امنیت سایبری

همان‌طور که جوزف نای اشاره می‌کند، امنیت سایبری عمدتاً با چهار نوع تهدید به چالش کشیده می‌شود: جاسوسی، جنایت و جرم، جنگ سایبری و تروریسم سایبری[۱۹]. تبیین‌های مرسوم برای این چالش‌ها عبارت‌اند از نقص در طراحی اینترنت، نقص در سخت‌افزار و نرم‌افزار و اتکای فزاینده به اینترنت به‌عنوان فضای ذخیره‌سازی برای سیستم‌های داده مهم (کلارک و نیک[۲۰]، 2010: 73؛ نای، 2010: 16). از سوی دیگر، گزارش‌های رسمی از ایالات‌متحده نیز حملات سایبری و جاسوسی سایبری را به‌عنوان چالش‌های اصلی امنیت سایبری معرفی می‌کنند. حملات سایبری به اقدامات تهاجمی بدون عاملِ قابل‌شناسایی اشاره دارد (کلپر[۲۱]، 2013: 1). هدف از چنین حملاتی ایجاد وحشت یا دستیابی به اهدافِ کنترل، خاتمه یا حذف داده‌ها است.

---

[15] Ministry of Industry and Information Technology (MIIT)
[16] service provider
[17] Thomas
[18] “there is no national security without cybersecurity, and no modernization without informatization”
[19] espionage, crime, cyber warfare, and cyber terrorism
[20] Clarke & Knake
[21] Clapper



نمودار 1- تعداد کاربران اینترنت در چین از دسامبر 2000 تا دسامبر 2023 (واحد: میلیون نفر)[۲۲]

درحالی‌که چین دارای بیشترین تعداد کاربران اینترنت در جهان است، با تعداد فزاینده‌ای از حملات سایبری نیز مواجه است. بر اساس گزارشی در سال 2016، زیان اقتصادی سالانه چین به دلیل حوادث امنیت سایبری بالغبر 915 میلیون یوان بوده است (People's Daily، 2016). اسب تروجان، بات نت، شبکه تلفن همراه، انکار سرویس توزیع‌شده، باگ‌های نرم‌افزاری و سخت‌افزاری و حفره‌های امنیتی[۲۳] در وب‌سایت‌ها به‌عنوان رایج‌ترین مسائل امنیتی شناسایی شده‌اند (مرکز اورژانس اینترنت ملی، 2017: 1). به همین ترتیب، در سال 2016، چین سند استراتژی ملی امنیت فضای سایبری را منتشر کرد که در آن چالش‌های داخلی و خارجی برای امنیت سایبری شناسایی شده بود. برای چین، چالش‌های خارجی به تعداد فزاینده خارجی‌هایی مربوط می‌شود که از اینترنت برای مداخله در سیاست داخلی چین سوءاستفاده می‌کنند. علاوه‌بر این، نظارت و جاسوسی وب در مقیاس بزرگ به‌شدت به امنیت ملی و حریم خصوصی کاربران تجاوز می‌کند و ممکن است به‌طور بالقوه به زیرساخت‌های اطلاعاتی مهم آسیب برساند یا منجر به درگیری‌های بین‌المللی شود. از سوی دیگر، چالش‌های داخلی، شامل شایعات آنلاین، فرهنگ افسرده‌آمیز و زننده، خشونت و اطلاعات خرافی است که ممکن است امنیت فرهنگی و سلامت جسمی جوانان را از بین ببرد. تروریسم اینترنتی و فعالیت‌های مجرمانه مستقیماً نظم و زندگی اجتماعی و دارایی شهروندان چینی را به چالش می‌کشد (اداره فضای سایبری چین[۲۴]، 2016).

در اصطلاح فنی، امنیت سایبری به محافظت از نرم‌افزار، سخت‌افزار و داده‌ها در برابر آسیب، دست‌کاری یا افشای اطلاعات به‌صورت تصادفی یا عامدانه اشاره دارد. درعین‌حال، سرویس اینترنت قطع نشده و در عملکرد عادی و متوالی باقی می‌ماند. از منظر نظم اجتماعی، درحالی‌که پکن مزایای اقتصادی عظیم فناوری اینترنت را به رسمیت می‌شناسد، گردش اطلاعات کنترل نشده تهدیدی جدی برای رژیم به شمار می‌رود، پدیده‌ای که بدون شک با حادثه میدان تیان‌آن‌مِن و انقلاب جاسمین[۲۵] بزرگ‌تر شده است؛ بنابراین، برای چین، ثبات سیاسی اولویت اصلی برای ایجاد سیاست‌ها و اقدامات مرتبط با امنیت سایبری است (چانگ، 2014: 32). با توجه به حادثه میدان تیان‌آن‌مِن در سال 1989، درک تأکید چین بر ثبات سیاسی دشوار نیست. ازآنجایی‌که نابسامانی‌های اجتماعی و تحولات پس‌ازاین حادثه، حزب کمونیست چین را به مرز فروپاشی رساند، پکن به‌شدت مراقب تمام جنبش‌های توده‌ای و اندیشه‌های سیاسی تائید نشده بود؛ بنابراین اتخاذ سرکوب سریع و مصمم، پاسخ موجهی به نظر می‌رسد

---

[22] Internet live States (2020) and Statista (2020)

[23] Trojan horse, botnet, mobile network, distributed denial of service (DDOS), software and hardware bugs, and security loopholes

[24] Cyberspace Administration of China

[25] the Tiananmen Square Incident and the Jasmine Revolution

(سوارتز[۲۶]، 2011: 1-5). از سوی دیگر، با توجه به اینکه چگونه انقلاب جاسمین جهان عرب را درنوردید و چگونه تظاهرات گسترده صلح را در منطقه برهم زد، برای پکن، ترس از روی آوردن مردم علیه رژیم کمونیست، نگرانی از چالش‌هایی مانند فساد، نابرابری ثروت، بیکاری و تورم را تحت‌الشعاع قرار می‌دهد (سوارتز، 2011: 4). در همین حال، چین همچنان مراقب رقابت شدید جهانی در توسعه فناوری اطلاعات و ارتباطات است. چین با توجه به پیشرفت‌های فناورانه سایر کشورها و به‌عنوان قربانی اصلی حملات سایبری و هک‌های اینترنتی، نیاز به توسعه قابلیت اینترنتی و توانایی خود برای مانور در دنیای مجازی را تشخیص می‌دهد. به‌طورکلی، چین امنیت سایبری را یک موضوع جهانی می‌داند که امنیت ملی، توسعه اقتصادی، سیاست داخلی و جامعه را به چالش می‌کشد و بر دفاع از حاکمیت، نظم سیاسی و ثبات اجتماعی تأکید می‌کند (راد[۲۷]، 2016: 6). ازنظر امنیت سایبری، برای چین، امنیت در دنیای واقعی بیشتر از امنیت در دنیای مجازی اهمیت دارد.

توسعه خط‌مشی‌های امنیت سایبری چین

طی سال‌ها، پکن دست به وضع قوانین و مقررات و تأسیس نهادهایی، باهدف افزایش توانایی دولت برای پایش و نظارت بر مطالب اینترنتی و جلوگیری از تهدیدات علیه حزب کمونیست زده است. به‌صورت هم‌زمان، نهادهایی برای اعمال حاکمیت قانونی تأسیس شدند و قوانین امنیت سایبری باهدف ایجاد موانع غیر تعرفه‌ای در برابر مخالفان تجاری، وضع گردیدند. در این بخش، توسعه خط‌مشی‌های امنیت سایبری چین، ازجمله مقررات، حکمرانی قانونی و قانون‌گذاری جدید سایبری را بررسی می‌کنیم.

وضع مقررات برای ایجاد نظم سایبری

نه‌تنها سال 1994 آغاز رسمی عصر اینترنت در چین است، بلکه نقطه شروعی برای حکمرانی سایبری در این کشور است. از سال 1994، پکن متعاقباً مجموعه‌ای از قوانین و مقررات مربوط به امنیت سایبری را وضع کرد؛ ازجمله تصمیم کمیته دائمی کنگره ملی خلق[۲۸] در مورد حفاظت از امنیت اینترنت، مقررات ارتباطات راه دور جمهوری خلق چین[۲۹]، مقررات مربوط به سرویس اطلاعات اینترنتی جمهوری خلق چین، فرمان حفاظت از امنیت سیستم اطلاعات رایانه‌ای جمهوری خلق چین، مقررات مربوط به اداره مخابرات سرمایه‌گذاری خارجی، رویکرد مدیریت امنیت شبکه اطلاعات رایانه‌ای بین‌المللی و تصمیم کمیته دائمی کنگره ملی خلق در مورد تقویت حفاظت از اطلاعات شبکه (یوشیائو و لو[30]، 2015: 232)

با توجه به سانسور و کنترل اینترنت، به‌سختی بتوان پروژه سپر طلایی[۳۱] را به سرپرستی آکادمیسین چینی فانگ بینکسینگ[۳۲] که به‌عنوان دیوار آتش بزرگ چین[۳۳] نیز شناخته می‌شود، نادیده گرفت. «دیوار آتش بزرگ» چین با مسدود کردن پروتکل اینترنت (IP) و فیلتر کردن سیستم‌های نام دامنه (DNS) و منبع یاب یکپارچه (URL) که به اصطلاحات یا عبارات یا اطلاعات حساسی مرتبط‌اند که دولت مرکزی تمایلی به انتشار آن‌ها ندارد، دست به سانسور می‌زند. برای مثال، اصطلاحاتی مانند حادثه میدان تیان‌آن‌من در 4 ژوئن، استقلال تایوان، استقلال تبت، استقلال سین‌کیانگ و فالون‌گونگ همگی به‌شدت توسط پکن تحت نظارت هستند و اغلب مسدود می‌شوند (اینکستر، 2016: 32). علاوه‌بر مسدود شدن اصطلاحات حساس سیاسی، گوگل، یوتیوب و سایر رابط‌های رسانه‌ای که منجر به افکار آزاد و جریان آزاد اطلاعات می‌شوند، همگی توسط پکن مسدود شده‌اند. رسانه‌های جریان اصلی غربی که علیه چین اتهامات جدی وارد می‌کنند مانند وال‌استریت ژورنال، بلومبرگ نیوز و واشنگتن‌پست و رسانه‌های اجتماعی مانند فیس‌بوک و توییتر، همگی توسط پکن بسته‌شده‌اند (لیندسی، 2015/2014: 18؛ یوشیائو و لو، 2015: 232).

---

[26] Swartz
[27] Raud
[28] National People's Congress Standing Committee
[29] People's Republic of China (PRC)
[30] Yuxiao & Lu
[31] Golden Shield project
[32] Fang Binxing
[33] Great Firewall of China

واضح است که دپارتمان‌های امنیت سایبری چین تلاش زیادی برای کنترل اطلاعات و فعالیت‌های اینترنتی انجام می‌دهند تا تمام تهدیدات احتمالی علیه دولت را محدود کنند.

حکمرانی قانونی/حکومت به‌وسیله قانون

در سال‌های اخیر، پکن فعالانه انواع مختلف سیاست‌های امنیت سایبری خود را به امید هم‌افزایی بین دولت حزبی و کسب‌وکارهای خصوصی و به‌منظور ایجاد پیشرفت‌های فناورانه و گسترش کاربست مدنی فناوری اطلاعات و ارتباطات، معرفی و ترویج کرده است؛ اما بااین‌حال به‌صورت هم‌زمان، پکن کنترل خود را بر استفاده از اینترنت تشدید کرده است که نشان‌دهنده پدیده نسبتاً جالبِ پیشبرد مشترک و متقابل بین توسعه و محدودیت است. به‌عنوان‌مثال، دفتر کمیسیون مرکزی امور فضای سایبری و اداره فضای سایبری چین[۳۴] که قبلاً به‌عنوان گروه مرکزی پیشرو برای امنیت سایبری و اطلاع‌رسانی شناخته می‌شد، مستقیماً به شی‌جین‌پینگ[۳۵] گزارش می‌دهند. این دفتر توسط شی‌جین‌پینگ در دسامبر 2013 تأسیس شد. لو وی[۳۶]، رئیس سابق دپارتمان تبلیغات پکن نیز به‌عنوان اولین رئیس این دفتر مشغول به فعالیت شد (پرلز و موزور[۳۷]، 2016). هدف دفتر مذکور، بازتعریف سیستم کنترل اطلاعات دیجیتال در چین و تائید بهبود کنترل دولت بر امنیت سایبری و خدمات اینترنتی است. از این‌رو، این دفتر از طریق سانسور و نظارت، کنترل خود را بر محتوای آنلاین تقویت می‌کند؛ همچنین به‌صورت هم‌زمان، از فناوری‌های جدید برای اجرای اشکال جدید تبلیغات و تثبیت نقش هژمونیک خود بر حاکمیت سایبری استفاده می‌کند (راد، 2016: 18–19) ازآنجایی‌که رئیس این دفتر از قدرت قابل توجهی برخوردار است، ناظران به آن عنوان «تزار اینترنتی[۳۸]» داده‌اند. در ژوئن 2016، لو وی پس از مجرم شناخته شدن به نقض نظم و انضباط دولتی استعفا داد.

در 27 فوریه 2014، «گروه مرکزی پیشرو برای امنیت سایبری و اطلاعاتی‌سازی[۳۹]» ایجاد شد. هدف این گروه به رهبری شخص شی‌جین‌پینگ، ساماندهی مجدد نهاد فوق، به‌منظور مدیریت سایبری و بهبود مسائلی مانند کارکردهای مشترک، مسئولیت‌پذیری و کارایی بود (اداره فضای سایبری چین[۴۰]، 2016؛ اینکستر[۴۱]، 2016: 40–41). علاوه‌بر افزایش کارایی مدیریت سایبری، این گروه پیشرو نیز به جنبش ضد فساد شی‌جین‌پینگ کمک کرد. هنگامی‌که رسانه‌ها و محافل آنلاین به‌طور گسترده در مورد رسوایی‌های دبیر سابق حزب چونگ کینگ بو شیلای و معاون شهردار چونگ کینگ وانگ لیجون در اواخر سال 2012 گزارش دادند، اقتدار پکن به‌شدت آسیب دید. اندکی بعد، پکن، نیویورک‌تایمز و سایر رسانه‌های غربی را که در این مسئله گزارشاتی ارائه کرده بودند، سانسور کرد و با عدم تمدید گذرنامه‌های خبرنگاران خارجی، مقابله سختی را با آنان انجام داد (America PEN، 2016: 31–32).

شی‌جین‌پینگ، در بیانیه‌ای صریح در سال 2013 بر تلاش حزب کمونیست چین در «تأسیس یک تیم قدرتمند برای به کنترل درآوردن زمینه‌های جدید در رسانه‌ها» تأکید کرد (پائولسون[۴۲]، 2015). از آن زمان، دولت چین تعداد زیادی پلیس سایبری را برای پایش و پیگیری موضوعات رایج و محبوب در محافل آنلاین به کار گرفته است. طبق گزارش‌ها، حدود دو میلیون پلیس یا به‌اصطلاح «تحلیل‌گر افکار عمومی» در دنیای مجازی گشت‌زنی می‌کنند (ژو و آلبرت[۴۳]، 2017). درحالی‌که مبارزه با فساد یکی از نیروهای محرک اصلی برای ایجاد نهادهای جدید بوده است، پکن به

---

[34] Office of the Central Cyberspace Affairs Commission and the Cyberspace Administration of China (CAC)
[35] Xi Jinping
[36] Lu Wei
[37] Perlez & Mozur
[38] "internet Czar"
[39] the Central Leading Group for Cybersecurity and Informatization was established
[40] Cyberspace Administration of China
[41] Inkster
[42] Paulson
[43] Xu & Albert

نفوذ عمومی رسانه‌های آنلاین پی برد و به نیاز به یک سیستم مؤثرتر برای کنترل اطلاعات اشاره کرد (لمپتون[۴۴]، 2014: 60-62). به‌عبارت دیگر، شاید بیش از حمایت از اقتدار دولت، آزادی مطبوعات و آزادی بیان[۴۵] ریشه سیاست‌های امنیت سایبری چین باشد.

علاوه‌بر نهادهای رسمی، تأسیس انجمن امنیت سایبری چین[۴۶] در سال 2016 نشان‌دهنده تلاش پکن برای تقویت امنیت سایبری است. این انجمن که تحت هدایت اداره فضای سایبری چین (CAC) تأسیس شده است، یک سازمان اجتماعی غیرانتفاعی است و توسط شورای دولتی تائید شده است تا امنیت سایبری چین را از طریق سازمان‌دهی و بسیج احزاب مختلف در جامعه تقویت نماید. درواقع این انجمن ابتکاری است برای همکاری بین دولت، کسب‌وکارها و دانشگاه‌ها، باهدف حکمرانی سایبری بهتر. علاوه‌بر این، این انجمن به‌طور فعال در بحث‌های سیاستی در مورد امنیت سایبری چین و مسائل مربوط به حکمرانی جهانی شرکت می‌کند (اوبرین[۴۷]، 2016؛ فیرست‌پست[۴۸]، 2016).

درنهایت، ذکر سهم‌یاری و نقش ارتش آزادی‌بخش خلق (PLA)[۴۹] در حکمرانی قانونی نیز حائز اهمیت است. در مطالعات استراتژیک (Zhanluexue) که توسط آکادمی علوم نظامی PLA در سال 2013 منتشر شد، وجود نیروهای سایبری در چین برای اولین بار برای جهان توصیف شد. مطالعات استراتژیک علاوه‌بر تأکید بر وظیفه نیروها برای حفاظت از امنیت سایبری، به اهمیت رقابت سایبری در زمان جنگ و صلح و وظایف مربوط به حمله و دفاع نیز اشاره می‌کند. در سال 2015، شورای دولتی چین، استراتژی نظامی چین را منتشر کرد و بر تهدید بالقوه نفوذ، براندازی و فساد فرهنگی تدریجی توسط کشورهای غربی از طریق بهره‌برداری از اینترنت تأکید کرد (کووالوسکی[۵۰]، 2017). با توجه به تأثیر شدیدی که چنین حملاتی ممکن است بر امنیت ملی داشته باشد، بخش سایبری PLA وظیفه نظارت بر شبکه‌های اطلاعات باز و جلوگیری از جاسوسی و حملات سایبری را بر عهده دارد (شورای دولتی جمهوری خلق چین[۵۱]، 2014). در دسامبر 2015، شی‌جین‌پینگ نیروی پشتیبانی استراتژیک[۵۲] را به‌عنوان بخشی از اصلاحات نظامی کلی خود تأسیس کرد. این نیرو، یک نیروی عملیاتی جدید است که پشتیبانی استراتژیک برای PLA در مورد مسائل مربوط به فضای بیرونی، فضای سایبری و الکترومغناطیسی فراهم می‌کند و نقش مهمی در تحقق نبرد مشترک یکپارچه با سایر نیروهای سنتی ایفا می‌کند (کاستلو[۵۳]، 2016).

به‌طورکلی، ایجاد خط‌مشی‌ها و نهادهای امنیت سایبری نه‌تنها نشان‌دهنده تمایل پکن برای تنظیم مجدد ساختار قدرت در سطح رهبری و اصلاح مشکل عدم پاسخگویی است، بلکه نشان‌دهنده اراده نخبگان سیاسی برای فشار به‌منظور ایجاد سیاست‌های سایبری مؤثرتر از طریق استفاده کارآمد از منابع دولتی است.

قانون‌گذاری جدید سایبری

به‌راحتی می‌توان از بحث قبلی نتیجه گرفت که اعمال سانسور چین در مورد آزادی بیان آنلاین مدتی است که شکل‌گرفته است. از زمان روی کار آمدن شی‌جین‌پینگ، علاوه‌بر موضوع آزادی بیان، می‌توان موضوع بازطراحی قدرت در نهادهای دولتی برای انجام بازبینی محتوا در دنیای سایبری را نیز مشاهده کرد. ازآنجایی‌که قوانین خاص همچنان نامشخص است، برخی از محتواها بر مهارت‌های ثبت اختراع و حقوق مالکیت معنوی تأثیر می‌گذارد و حقوق حریم خصوصی افراد را نقض می‌کند. باوجوداین، در 27 دسامبر 2016، پکن استراتژی امنیت سایبری خود را منتشر کرد که

---

[44] Lampton
[45] freedom of speech

[46] Cyber Security Association of China (CSAC)
[47] O' Brien

[48] First Post
[49] People's Liberation Army (PLA)
[50] Kowalewski
[51] The State Council of the People's Republic of China
[52] Strategic Support Force (SSF)
[53] Costello

به جزئیات عزم چین برای تحقق قوانین و هنجارهای مرتبط در مورد فضای سایبری و دستیابی به حکمرانی مؤثر می‌پردازد. در ادامه به برخی از تحولات اصلی در سال‌های اخیر پرداخته می‌شود.

در 1 ژوئیه 2015، کمیته دائمی دوازدهمین کنگره ملی خلق[۵۴]، قانون امنیت ملی را تصویب کرد که به‌نوبه خود توجه فراوانی را از سوی ناظران در مورد تعریف چینی امنیت سایبری به خود جلب کرد. بند 25 نیاز چین برای توسعه توانایی خود برای حفاظت از فضای سایبری و اطلاعات را پیشنهاد می‌کند و درعین‌حال بر اهمیت تحقیقات و کاربرد نوآورانه فاوا تأکید می‌کند. بند 59 همچنین پیشنهاد می‌کند که چین باید نهادها و مکانیسم‌های نظارتی برای امنیت ملی ایجاد کند و بررسی‌های امنیتی را برای سرمایه‌گذاری خارجی، منابع خاص، فناوری‌های کلیدی و محصولات ICT انجام دهد (کنگره ملی خلق، 2015). از طریق قانون امنیت ملی، برای اولین بار، چین به‌وضوح مفهوم «حاکمیت سایبری[۵۵]» یا گسترش حاکمیت دولت به اینترنت را معرفی کرد. بااین‌حال، این سؤال که دولت چگونه می‌تواند صلاحیت قضایی را در فضای سایبری اجرا کند، همچنان نامشخص است (بنت[۵۶]، 2015؛ پاندا[۵۷]، 2015).

در 27 دسامبر 2015، در هجدهمین نشست دوازدهمین کنگره ملی خلق، قانون مبارزه با تروریسم، برای اجرا در 1 ژانویه 2016 تصویب شد. این قانون انتشار جزئیات مربوط به تروریسم و تصاویر ظالمانه یا غیرانسانی را ممنوع می‌کند، همان‌طور که پکن فکر می‌کند چنین گزارشاتی ممکن است عامل تقویت تقلید را در مردم باشد. علاوه‌بر این، بدون تائید رسمی، افراد از انتشار اطلاعات قربانیان تروریست و اظهارات مربوط به فعالیت‌های دولتی در راستای مبارزه با تروریسم منع می‌شوند. درحالی‌که چین به‌طور گسترده به سانسور معروف است، قانون مبارزه با تروریسم چنین کنترلی را تقویت می‌کند (بی‌بی‌سی نیوز، 2015؛ شین هوا نت[۵۸]، 2016).

در 10 مارس 2016، اداره دولتی مطبوعات، انتشارات، رادیو، فیلم و تلویزیون و وزارت صنعت و فناوری اطلاعات به‌طور مشترک مقررات مربوط به خدمات انتشارات آنلاین را صادر کردند (وزارت صنعت و فناوری اطلاعات جمهوری خلق چین[۵۹]، 2016). برای اولین بار در تاریخ، این مقررات سرمایه‌گذاری خارجی و شرکت‌های سرمایه‌گذاری مشترک داخلی و خارجی را از ارائه خدمات انتشار آنلاین در چین منع می‌کند. علاوه‌بر این، همکاری بین ناشران آنلاین و سرمایه‌گذاری خارجی یا شرکت‌های سرمایه‌گذاری مشترک داخلی و خارجی، سازمان‌های خارجی یا پرسنل خارجی همگی قابل بررسی رسمی و اداری است. ناشران موظف‌اند قبل از اقدام، گواهی خدمات نشر آنلاین را دریافت کنند.

سرانجام، در 7 نوامبر 2016، چین قانون امنیت سایبری را تصویب کرد و در ژوئن 2017 به اجرا درآمد. این قانون تأکید پکن بر حاکمیت سایبری و کنترل اطلاعات را منعکس می‌کند. از نظر حاکمیت سایبری و در قیاس با مرزهای دنیای واقعی، چین تلاش می‌کند تا مرزهای را در فضای سایبری ترسیم کند. مفهوم حاکمیت سایبری را می‌توان در گزارش رسمی دولتی در سال 2010 در مورد اینترنت در چین دنبال کرد: اینترنت یک زیرساخت مهم دولتی که تابع حاکمیت چینی در داخل چین است. (چاینا دیلی[۶۰]، 2010). چین بین فضای داخلی و خارجی تمایز قائل می‌شود. درحالی‌که بخش تجاری و جامعه مدنی می‌توانند از طریق اینترنت توسعه یابند، دولت بیشترین میزان مسئولیت و اقتدار را برای حفظ صلح و ثبات در اختیار دارد. در مواجهه با امنیت سایبری، سود بازار کسب‌وکار در درجه دوم اهمیت قرار دارد. به‌عبارت‌دیگر، از نظر پکن، حتی اگر اینترنت جهانی باشد، وقتی صحبت از صلاحیت قضایی به میان می‌آید، دولت‌ها همچنان باید رهبری را بر عهده بگیرند (ژو[۶۱]، 2015: 4).

---

[54] Standing Committee of the Twelfth National People's Congress
[55] cyber sovereignty
[56] Bennett
[57] Panda
[58] Xinhua Net
[59] Ministry of Industry and Information Technology of the PRC
[60] China Daily
[61] Zhou

به‌طورکلی، می‌توان نتیجه گرفت که در رابطه با حکمرانی سایبری، چین با انجام اقدامات تنبیهی علیه حملات سایبری داخلی و خارجی، جاسوسی سایبری، توزیع اطلاعات غیرقانونی و مخرب و فعالیت‌های مجرمانه‌ای که ثبات اجتماعی و دولتی را مختل می‌کند، تلاش‌های خود را در جهت مدیریت این فضا افزایش می‌دهد. حفظ حاکمیت و امنیت سایبری و توسعه منافع اساسی همچنان اولویت چین است. در همین حال، قوانین و مقررات مربوط به اعمال سانسور علیه تجارت خارجی همچنان یکی از نگرانی‌های اصلی شرکت‌های خارجی در داخل و خارج از چین است.

دلالت‌های خط‌مشی امنیت سایبری چین برای روابط بین‌الملل

ازنظر جنبه بین‌المللی خط‌مشی امنیت سایبری چین، نویسندگان فکر می‌کنند که بحث‌ها بر مفهوم حاکمیت سایبری متمرکز است. با توجه به تفاوت‌های اساسی بین چین و دموکراسی‌های غربی، علی‌رغم ایجاد نهادها و هنجارهای قانونی، چین همچنان هدف حملات ناظرانی است که به تعدی مداوم چین به آزادی بیان و حریم خصوصی افراد با توجیه امنیت ملی، بدگمان هستند. از سوی دیگر، با توجه به نفوذ فزاینده چین در امور بین‌الملل، حاکمیت سایبری ممکن است به‌عنوان یک مفهوم جدید در نظر گرفته شود که می‌تواند برای تغییر شکل قوانین و اصول موجود حاکم بر فضای سایبری مورد استفاده قرار گیرد. درنهایت، مفهوم حاکمیت سایبری نیز ممکن است به‌عنوان یک راه مهم برای پکن برای دستیابی به فناوری‌های خارجی و محافظت از تجارت خود در برابر دیگران باشد.

اول، با بررسی دقیق قوانین و مقررات ذکرشده در بخش قبل، واضح است که حاکمیت سایبری در قلب قوانین قرار دارد که به‌نوبه خود بر آزادی بیان و حریم خصوصی افراد تأثیر می‌گذارد. به‌عنوان‌مثال، ازنظر قانون مبارزه با تروریسم تا حد زیادی رسانه‌ها از گزارش فعالیت‌های ضد تروریستی چین محدودشده‌اند. به همین ترتیب، بدبینان خاطرنشان می‌کنند که این قانون در خدمت اهداف سنتی پکن برای حفظ ثبات و اقتدار است و به دولت اجازه می‌دهد از راه‌های مختلف برای جلوگیری، سرکوب و مقابله با فعالیت‌های تروریستی استفاده کند. این قانون به پکن اجازه کنترل دقیق بر سازمان‌های خصوصی و دسترسی به اطلاعات خصوصی را می‌دهد که به‌نوبه خود آزادی بیان، تجمع مسالمت‌آمیز و مذهب را به چالش می‌کشد (سینگ[۶۲]، 2016).

ازنظر مقررات مربوط به خدمات انتشار آنلاین، دریافت مجوز و موافقت رسمی، محدود به «شهروندان چینی توانمندی است که به‌طور دائم در این کشور اقامت دارند» و «سرور و مرکز ذخیره‌سازی آن‌ها در چین واقع‌شده است». اگر ناشران آنلاین مطالبی را منتشر کنند که به امنیت ملی و ثبات اجتماعی مربوط می‌شود، طبق مقررات اداره دولتی مطبوعات، نشریات، رادیو، فیلم و تلویزیون، این مطالب باید در اختیار مقامات محلی قرار گیرد، یا در غیر این صورت از انتشار عمومی منع شود (چان، 2018: 8). از سوی دیگر، قانون امنیت سایبری از شرکت‌های خارجی می‌خواهد که تمام اطلاعات و داده‌های شخصی تولیدشده در چین را در داخل کشور ذخیره کنند و در مواقع تحقیق و بررسی، همکاری لازم را با دولت داشته و اطلاعات لازم را در اختیار دولت قرار دهند. بر این اساس، کاربران فردی باید هنگام استفاده از خدمات مخابراتی چین با هویت واقعی خود ثبت‌نام کنند (موزور[۶۳]، 2016). به‌طور خلاصه، از طریق کنترل در مقیاس بزرگ، قانون امنیت سایبری چین به‌طور مستقیم و منفعلانه به حق فردی برای آزادی بیان و حریم خصوصی لطمه می‌زند (کریمرز[۶۴]، 2017).

دوم، با توجه به ناسازگاری بین برداشت چینی از حاکمیت سایبری و مفاهیم موجود، در سال‌های اخیر، چین به‌طور فعال در حاکمیت جهانی اینترنت مشارکت داشته و تلاش زیادی برای ترویج مفهوم «حاکمیت سایبری» خود انجام می‌دهد که بر گسترش حاکمیت دولت به فضای‌مجازی و احترام متقابل بین کشورها در خصوص فضای مجازی مستقل و صلاحیت قضایی بر فعالیت‌های اینترنتی داخلی، تأکید می‌کند. دعوت چین به چنین گفتمانی از سوی روسیه، الجزایر، امارات متحده عربی و برخی از کشورهای آسیای مرکزی که طرفدار تشدید محدودیت‌ها در فعالیت‌های اینترنتی هستند، حمایت شد. کشورهای مذکور همگی با چین در ارائه پیشنهاده‌هایی در فرصت‌های مناسب و مهم ازجمله مجمع عمومی سازمان ملل

---

[62] Singh
[63] Mozur
[64] Creemers

متحد، به‌منظور ایجاد مفهوم حاکمیت سایبری در نهادهای بین‌المللی همکاری کرده‌اند. چنین اقداماتی، به‌وضوح با تأکید ایالات‌متحده بر آزادی اینترنت مغایرت دارد و به دنبال ایجاد مشروعیت خاصی در حقوق بین‌الملل است (نای[۶۵]، 2010: 18؛ گچلیک[۶۶]، 2017: 2-5).

علاوه‌بر این، مشاهده دقیق‌تر کنفرانس جهانی اینترنت[۶۷] جاه‌طلبی چین برای افزایش نفوذ جهانی خود را نشان می‌دهد. در نوامبر 2014، در اولین کنفرانس که در ووژن[۶۸] برگزار شد، شی‌جین‌پینگ مجدداً تأکید کرد که فضای اینترنت صلح‌آمیز تحت حکمرانی چندجانبه، می‌بایست تحت شرایط احترام و اعتماد متقابل تحقق یابد (The Economic Times، 2014). در دومین کنفرانس در سال بعد، شی، بیشتر از جامعه بین‌المللی دعوت کرد تا یک جامعه مجازی با سرنوشت مشترک بر اساس اصل حاکمیت سایبری ایجاد نماید (China Daily، 2015). چنین درخواست‌ها و دعوت‌هایی این واقعیت را آشکار می‌کند که چین از رژیم حاکمیت سایبری فعلی ناراضی است و به دنبال نقش رهبری قوی‌تر در فضای سایبری است. چین امیدوار است که توسعه آینده دنیای سایبری بتواند بیشتر با ایده‌ها و خواسته‌های این کشور هماهنگ باشد (روی[۶۹]، 2015).

قوانین داخلی ابزار مهمی است که پکن برای تقویت امنیت سایبری استفاده می‌کند. به‌ویژه از نظر قانون امنیت سایبری و قانون مبارزه با تروریسم، کنترل سخت‌تر چین بر ذخیره‌سازی داده‌ها، شرکت‌های خارجی را نگران این موضوع کرد که چین، اهدافی غیر از امنیت سایبری دارد. قانون امنیت سایبری تصریح می‌کند که شرکت‌های اینترنتی باید پشتیبانی فنی را ارائه دهند و بررسی‌هایی را توسط بخش‌های مرتبط با امنیت به دلیل رعایت امنیت ملی بپذیرند. علاوه‌بر این، شرکت‌ها باید از محدودیت در انتقال داده به خارج از کشور تبعیت نمایند، یا به‌عبارت‌دیگر، داده‌های چین باید در چین ذخیره شوند. چنین اقدامی نمونه‌ای از اعمال محدودیت‌های پکن بر محصولات شرکت‌های خارجی و درعین‌حال ترویج توسعه صنعت فاوای داخلی به نام امنیت ملی و سایبری است (اتاق بازرگانی ایالات‌متحده، 2016: 6-15). درحالی‌که قانون جدید امنیت سایبری چین بر مفهوم حاکمیت سایبری متمرکز است و به دولت صلاحیت رسیدگی به جرائم سایبری و حفاظت از امنیت سایبری را می‌دهد، در برخی جنبه‌ها، چین مشکوک به حمایت‌گرایی برای صنعت داخلی خود است (ژو[۷۰]، 2016).

درواقع، قانون مبارزه با تروریسم تصریح می‌کند که اپراتورهای مخابراتی و ارائه‌دهندگان خدمات باید نقاط اتصال فناورانه را در طراحی و استقرار محصول و خدمات خود ایجاد کرده و طرح رمزگذاری خود را برای بررسی توسط مقامات مربوطه ارسال کنند. بررسی درب پشتی (backdoor)[۷۱] و انطباق با مقررات برای رمزگشایی نیز در محدوده تقاضای دولت برای هوشیاری و مراقبت نسبت به فعالیت‌های تروریستی است (بلانچارد[۷۲]، 2015). در همین حال، شرکت‌های غربی فناوری اطلاعات و ارتباطات می‌ترسند که چین ممکن است از قانون مبارزه با تروریسم سوءاستفاده کند و موانع تجاری خود را بالا ببرد. در سال‌های اخیر، پکن ادعا کرده است که سیسکو و برخی نرم‌افزارها حاوی «درهای پشتی» هستند و از شرکت‌های نرم‌افزار خارجی که با بانک‌های چینی معامله می‌کنند، خواسته است که کد اصلی نرم‌افزار خود را برای بررسی دولتی ارائه کنند. نیازی به گفتن نیست که چنین خواسته‌هایی به هزینه توسعه شرکت‌ها می‌افزاید و ممکن است اقدامات تلافی‌جویانه را علیه شرکت‌های چینی در خارج از کشور ایجاد کند که به‌نوبه خود خطر جنگ تجاری را افزایش می‌دهد (لیوینگستون[۷۳]، 2015).

نتیجه‌گیری: آینده امنیت سایبری در چین

---

[65] Nye
[66] Gechlik
[67] World Internet Conference (WIC)
[68] Wuzhen
[69] Rui
[70] Zhu

[71] برنامه‌ای که با دور زدن روندهای عادی، امکان دستیابی به یک سامانه رایانه‌ای را فراهم می‌سازد.

[72] Blanchard
[73] Livingston

بر اساس مباحث مطرح‌شده در مورد خط‌مشی‌های امنیت سایبری چین در این فصل، نویسندگان این فصل را با سؤالاتی خاتمه می‌دهند که باید در آینده نزدیک بررسی شوند. اول، درحالی‌که دولت چین تلاش می‌کند تا کنترل خود را بر دنیای سایبری حفظ کند، همچنین به دنبال همگام شدن با رشد اقتصادی در دنیای واقعی است. گفته دنگ شیائوپینگ که «توسعه اصل مطلق است» تا به امروز بر تصمیمات سیاسی پکن تأثیرگذار بوده است. در واکنش به کاهش سرعت اقتصاد چین در سال‌های اخیر، شی‌جین‌پینگ، رئیس‌جمهور چین، طرح کمربند و جاده[۷۴] را پیشنهاد کرد؛ ابتکاری با هدف ادغام قاره اوراسیا و گسترش فرصت‌ها و خروجی‌ها برای تولید مازاد چین. فراتر از ژئوپلیتیک و اقتصاد، توسعه‌ای که کمتر موردبحث قرار گرفته، ساخت جاده ابریشم دیجیتال است؛ هرچند به همان اندازه مهم است. هدف جاده ابریشم دیجیتال بهبود زیرساخت اینترنت در آسیای جنوب شرقی، آسیای مرکزی، خاورمیانه و جنوب صحرای آفریقا و درعین‌حال ترویج همکاری در فناوری الکترونیک و ماهواره، تجارت الکترونیک و توسعه شهرهای هوشمند است. به این ترتیب، تعدادی از شرکت‌های فناوری پیشرفته، از جمله بایدو، علی‌بابا، تنسنت و جینگ دونگ، موقعیت دولت را در گسترش نفوذ چین از طریق ترویج فناوری مخابرات چین در سراسر جهان به اشتراک می‌گذارند.

چالش بالقوه صنعت فناوری چین در همگرایی با موضع دولت در مورد ابزار گسترش نفوذ چین، تأثیر چنین پدیده‌ای در سایر کشورها است. به‌عنوان‌مثال، در آسیای جنوب شرقی، جایی که بسیاری از شرکت‌های چینی با فناوری پیشرفته جایگاه دارند، بسیاری از دولت‌ها به سمت اتخاذ یا تقلید از خط‌مشی‌های امنیت سایبری چین حرکت کرده‌اند. در سال 2015، تایلند تمایل خود را برای ایجاد یک ابزار سانسور مشابه دیوار آتش بزرگ چین اعلام کرد، آرزویی که درنهایت به دلیل مخالفت شدید مردم ناکام ماند. در سال 2017، اندونزی قانونی را تصویب کرد که خواستار محلی‌سازی داده‌های جمع‌آوری‌شده توسط شرکت‌های خارجی شد. در سال 2019، ویتنام مجموعه‌ای از قوانین امنیت سایبری را وضع کرد که شباهت‌های زیادی با همتای چینی خود دارد. با توجه به تحولات، ایجاد ارتباط بین شرکت‌های چینی و دولت‌های آسیای جنوب شرقی در نحوه اثرگذاری چین بر این کشورها در سانسور و کنترل و حمایت از آن و فشار چین برای شکل‌گیری جاده ابریشم دشوار نیست.

روسیه

مقدمه

این فصل تحلیل پیچیده‌ای از دکترین‌های کلیدی روسیه ارائه می‌دهد که شکل‌دهنده امنیت اطلاعات در داخل بوده و خط‌مشی برای خارج از کشور را تعریف می‌کند. رویکرد روسیه به امنیت سایبری و امنیت اطلاعات مبتنی بر تعهد قوی به منافع ملی است. همان‌طور که گذر زمان و تصمیمات عملی سیاست نشان می‌دهد، منافع دولتی به منافع فردی ارجح است. هدف روسیه نه‌تنها حفاظت از فضای اطلاعات، بلکه کنترل آن به روشی پیشگیرانه است. همین ایده‌ها به جامعه بین‌المللی نیز سرایت می‌یابد. مفهوم روسیه از حاکمیت سایبری دقیقاً توجیه‌گر چنین اقداماتی است. در کنار آن، روسیه از دهه 1990 به‌طور فعال در مذاکرات بین‌المللی در مورد امنیت سایبری شرکت داشته است. برجسته‌ترین ابتکار ایجاد یک گروه دولتی ویژه از کارشناسان در زمینه استفاده و توسعه فناوری اطلاعات و ارتباطات تحت نظارت مجمع عمومی سازمان ملل بود. این گروه در دهه اخیر پیشرفت قابل‌توجهی در شرح و تفصیل درکی مشترک میان وضعیت نگرانی‌های امنیتی و قابل‌اجرا بودن قوانین بین‌المللی داشته است. بااین‌حال، آخرین گردهمایی این گروه به دلیل مناقشات سیاسی عمیق بین اعضای اصلی آن نتوانست بر پایه پیشرفت‌های قبلی بنا شود. علی‌رغم این مسئله، روسیه برای ادامه تلاش‌ها فشار آورد که منجر به دوگانه شدن مسیر در کارگروه آزاد سازمان ملل[۷۵] و گروه متخصصان دولتی[۷۶] شد. درحالی‌که کارگروه آزاد سازمان ملل عمدتاً توسط دولت‌هایی حمایت می‌شد که با ایده حاکمیت سایبری همراه بودند، گروه متخصصان دولتی قالب و ارزش‌های سنتی خود را حفظ کرد. باوجوداین، روسیه در هر دو طرح مشارکت دارد. جبهه دیگری برای ارتقای حاکمیت سایبری، کنوانسیون بین‌المللی جدید برای مبارزه با جرائم سایبری می‌باشد که توسط روسیه پیشنهاد شده است. درحالی‌که پیش‌نویس کنوانسیون در سازمان

[74] Belt and Road Initiative (BRI)
[75] UN – OEWG :Open-ended Working Group
[76] UN– GGE :Group of Governmental Experts

ملل با اشتیاق مواجه نشد، روسیه همچنان بر نیاز به یک معاهده جدید تأکید می‌کند که به حاکمیت دولت‌ها در طول تحقیقات فرامرزی جرائم سایبری احترام بگذارد.

بیانیه راهبرد ملی امنیت سایبری

ازآنجایی‌که امروزه امنیت سایبری برای بسیاری از سیاست‌گذاران یک کلمه رایج و لقلقه زبان است، در روسیه این اصطلاح در سطح رسمی مورد استفاده قرار نگرفته است. طیف گسترده‌ای از تعاریف مرتبط با به‌کارگیری فناوری اطلاعات و ارتباطات وجود دارد و روسیه ترجیح می‌دهد به‌جای مشتقات سایبری، در خصوص امنیت اطلاعات صحبت کند. دلیل این مسئله فقط ویژگی‌های زبانی نیست. این تفاوت از تفاوت‌های مفهومی در رویکردهای امنیتی دلالت دارد.

رایج‌ترین تعریف امنیت سایبری به سطح عملیاتی و زیرساختیِ به اشتراک‌گذاری اطلاعات و نه به محتوای آن فی‌نفسه اشاره دارد. سه‌گانه مشترک امنیت سایبری شامل اصول محرمانگی[۷۷]، صداقت و یکپارچگی[۷۸] و در دسترس بودن[۷۹] است. این سه اصل به‌ترتیب یعنی اطلاعات فقط برای حلقه موردنظر از کاربران در دسترس است، اطلاعات صحیح و کامل بدون هیچ‌گونه دسترسی غیر یا تغییر غیرمجاز است و هر زمان که لازم باشد می‌توان به آن اطلاعات دسترسی داشت. پارکر[۸۰] (2002) سه اصل دیگر را به این سه اصل اضافه کرد: تصاحب[۸۱] یا کنترل، اصالت[۸۲] و سودمندی[۸۳]. اصل اول لزوم حفظ کنترل بر اطلاعات را نشان می‌دهد زیرا از بین رفتن آن امنیت را با وجود حفظ محرمانگی و یکپارچگی آن تهدید می‌کند. اصل دوم در مورد اصالت نویسندگی اطلاعات است؛ و درنهایت، سودمندی به این معنی است که اطلاعات پس از همه این اقدامات احتیاطی همچنان قابل استفاده است.

می‌توان این اصول را در بسیاری از راهبردهای امنیت سایبری غربی مشاهده کرد. اکثر تهدیدات سایبری فهرست شده مربوط به زیرساخت‌های شبکه، موضوعات زیرساخت‌های حیاتی وابسته به کنترل‌های الکترونیکی، اهمیت جریان اطلاعات رایگان برای تجارت الکترونیک و مواردی از این دست است. رویکرد روسی بیشتر بر امنیت اطلاعات تمرکز دارد و سطح زیرساخت را به‌عنوان یک جزء پیش‌فرض می‌گذارد. تحلیل بیشتر دکترین‌های رسمی معنای امنیت اطلاعات (امنیت اطلاعاتی) را توصیف و به رهگیری تبلور این اصطلاح کمک می‌کند.

اولین دکترین در مورد امنیت اطلاعات در سال 2000 در روسیه ایجاد شد. این دکترین یک سند راهبردی است که مفهوم امنیت اطلاعات را از زاویه امنیت ملی که در آن منافع ملی نقش کلیدی دارد، صورت‌بندی می‌کند. وضعیت تحقق امنیت اطلاعات روسیه زمانی است که امنیت منافع ملی که با مجموع منافع فردی، اجتماعی و ملی (دولتی) تعریف می‌شود، در حوزه فناوری اطلاعات و ارتباطات محقق شده باشد. از آنجا می‌توانیم مبنای سه‌گانه‌ای را که برای امنیت اطلاعات مهم است (فرد، جامعه و دولت) استخراج کنیم. این سه‌گانه برای فهم ادراک روسیه از تهدیدات امنیت اطلاعات و همچنین سیاست روسیه برای تضمین امنیت اطلاعات مهم است.

دکترین سال 2000 چهار مؤلفه منافع ملی را در امنیت اطلاعات برجسته کرد: 1) احترام به آزادی و حق دسترسی و استفاده از اطلاعات؛ 2) حمایت اطلاعاتی (حساس سازی) از سیاست دولت روسیه در قبال شهروندان و جامعه بین‌المللی در مورد موضع رسمی این کشور در خصوص رویدادهای مهم و ارائه دسترسی به منابع اطلاعاتی باز دولتی؛ 3) توسعه فناوری‌های مدرن اطلاعات و ارتباطات و صنعت اطلاعات داخلی، اطمینان

---

[77] Confidentiality

[78] integrity : حفاظت داده در برابر حذف یا اصلاح و تغییر اطلاعات از سوی طرف های غیر مجاز. م.

[79] Availability
[80] Parker
[81] Possession
[82] authenticity
[83] utility

از نیازهای بازار داخلی برای محصولات خود و ورود این محصولات به بازار جهانی و 4) حفاظت از منابع اطلاعاتی در برابر دسترسی غیرمجاز، تضمین امنیت سیستم‌های اطلاعات و مخابراتی موجود یا در حال ساخت در روسیه (دکترین امنیت اطلاعات[۸۴]، 2000: قسمت اول، §1).

تهدیدها و چالش‌ها برای آن مؤلفه‌ها تعریف و به‌تفصیل شرح داده شده است. موضوعات اصلی در معرض تهدید در هر اولویت از منافع ملی، اقدامات برای تضمین امنیت و منابع کلیدی تهدیدها به دو دسته داخلی و خارجی تقسیم می‌شوند.

به‌طور قابل توجهی، همکاری بین‌المللی برای امنیت اطلاعات نیز مورد توجه قرار گرفت. حوزه اول به ممنوعیت توسعه، تکثیر و استفاده از «سلاح‌های اطلاعاتی» می‌پردازد («دکترین امنیت اطلاعات»، 2000: قسمت دوم، §7). سپس، اطمینان از امنیت تبادل بین‌المللی اطلاعات و ایمنی اطلاعات در حین انتقال آن از طریق کانال‌های مخابراتی ملی. نقطه مورد تمرکز دیگر، هماهنگی فعالیت‌های سازمان‌های مجری قانون در سراسر جهان برای پیشگیری از جرائم رایانه‌ای و همچنین جلوگیری از دسترسی غیرمجاز به اطلاعات سازمان‌های بین‌المللی مجری قانون مبارزه با جرائم سازمان‌یافته فراملی، تروریسم بین‌المللی، توزیع مواد مخدر و روان‌گردان و تجارت غیرقانونی سلاح‌ها و مواد شکافت‌پذیر هسته‌ای و همچنین قاچاق انسان بود. ایمنی شبکه‌های مخابراتی بین‌المللی بانکی نیز در اولویت همکاری‌های بین‌المللی قرار گرفت. برای تحقق این اهداف، روسیه با ایجاد همکاری نزدیک با کشورهای مشترک‌المنافع مستقل شروع کرد و سپس بر تضمین مشارکت فعال خود در همه سازمان‌های بین‌المللی فعال در زمینه امنیت اطلاعات، ازجمله استانداردسازی و صدور گواهینامه اقدامات امنیت اطلاعات تمرکز کرد.

بخش آخر این دکترین شامل توصیفی از نحوه اجرای سیاست‌های امنیت اطلاعات بود: قدرت، بین قوای مقننه، مجریه و قضایی در سطوح فدرال و سرزمینی تفاوت قائل می‌شود. بر این اساس، دولت سهام‌دار کلیدی در سیاست امنیت اطلاعات است که تحلیلی از تهدیدات امنیت اطلاعاتی علیه روسیه انجام می‌دهد، کار ادارات دولتی برای دفاع از کشور در برابر تهدیدات را سازمان‌دهی می‌کند، از فعالیت انجمن‌های عمومی برای محافظت از جامعه در برابر اطلاعات تحریف‌شده و نادرست حمایت می‌کند، توسعه، استفاده، صادرات و واردات ابزارهای امنیت اطلاعات را از طریق صدور گواهینامه و صدور مجوز کنترل می‌کند، از تولیدکنندگان داخلی ابزارهای امنیت اطلاعات حمایت می‌کند و همچنین اقداماتی را برای محافظت از بازار ملی در برابر نفوذ ابزارهای بی‌کیفیت خارجی انجام می‌دهد. همچنین دسترسی به منابع اطلاعاتی و ترویج شبکه‌های اطلاعاتی جهانی و تسهیل ورود روسیه به جامعه اطلاعاتی جهانی بر اساس مشارکت برابر نیز بر عهده دولت است. («دکترین امنیت اطلاعات»، 2000: قسمت سوم، §8).

با توسعه فناوری اطلاعات و ارتباطات و در دنیایی که به‌سرعت در حال تغییر است، راهبرد امنیت اطلاعات در سال 2000 اهمیت خود را از دست داده است. در این میان، قبل از انتشار نسخه به‌روز شده راهبرد در سال 2016، پیش‌نویس مفهوم راهبرد امنیت سایبری در روسیه در سال 2013 در حوزه عمومی ظاهر شد (Council.gov.ru، 2013). این پیش‌نویس تلاشی برای ادغام دو مفهوم: امنیت سایبری و امنیت اطلاعات و ترکیب آن‌ها در یک راهبرد مرتبط جدید برای روسیه بود. هدف، از بین بردن شکاف‌های موجود در مقررات امنیت سایبری در روسیه و ایجاد زمینه‌ای برای مشارکت جامعه مدنی و سازمان‌های تجاری در فرآیند تضمین امنیت سایبری، برخلاف آنچه در دکترین 2000 تثبیت شده بود بر مبنایی برابر با نهادهای دولتی بود.

بر اساس این مفهوم، فضای سایبر را باید به‌عنوان یک عنصر گرفته شده از فضای اطلاعاتی در نظر گرفت؛ بنابراین مفهومی محدودتر از آن است. بدین ترتیب:

فضای سایبر، حوزه‌ای از فعالیت در فضای اطلاعاتی است که توسط مجموعه‌ای از کانال‌های ارتباطی اینترنت و سایر شبکه‌های مخابراتی، زیرساخت‌های فناوری (که عملکرد آن‌ها را تضمین می‌کند) و هرگونه فعالیت انسانی که از طریق استفاده از آن‌ها انجام می‌شود (توسط افراد، سازمان‌ها و دولت) شکل گرفته است. (Council.gov.ru، 2013)

---

[84] Doctrine on Information Security

و امنیت سایبری «مجموعه‌ای از شرایطی است که تحت آن، همه اجزای فضای سایبر در برابر حداکثر تعداد ممکن تهدیدها و تأثیرات با پیامدهای نامطلوب محافظت می‌شوند». جالب اینجاست که این مفهوم ایده چندجانبه گرایی را برای اولین بار در چنین سطح سیاسی بالایی مطرح کرد.

اصول اساسی راهبرد امنیت سایبری آینده‌نگر شامل اصل «همکاری سازنده همه افراد جامعه اطلاعاتی – افراد، سازمان‌ها و دولت – در زمینه امنیت سایبری»، به معنای تقسیم مسئولیت‌ها بین ذی‌نفعان بود: دولت باید مقررات قانونی امنیت سایبری را اجرا و تلاش‌های ذی‌نفعان را هماهنگ کند، کسب‌وکارها باید امنیت سایبری زیرساخت‌های اطلاعاتی حیاتی تحت مالکیت خود را تضمین، استانداردهای امنیت سایبری را رعایت کنند و جامعه باید سطح سواد دیجیتال را افزایش دهد و بازخوردی را در مورد تلاش‌های دولت و کسب‌وکارها ارائه دهد.

علی‌رغم اینکه این مفهوم حاوی طیف وسیعی از ایده‌های مترقی برای توسعه امنیت سایبری است، از سوی صنعت به دلیل ابهام و عدم قطعیت مفاد آن و همچنین از سوی مقامات دولتی مورد انتقاد قرار گرفت، چراکه «در تضاد با سیاست دولت در این زمینه است.» (Коммерса́нть، 2013). پس از جلسات استماع پارلمانی درباره این مفهوم در پایان سال 2013، شورای امنیت باید آن را برای اجرای بیشتر بررسی می‌کرد. بااین‌حال، سرنوشت پروژه مشخص نیست و دلیلی وجود دارد که معتقدیم یا در مرحله تصویب، متوقف شده و یا رد شده است. در ششمین مجمع حاکمیت اینترنت روسیه در سال 2015، رهبر کارگروه مفهوم، گفت که او دیگر قصد ندارد این پروژه را پیش ببرد؛ زیرا هدف اصلی محقق و بحث عمومی و فعالیت قانون‌گذاری تشویق شده و ادامه دارد.

رئیس‌جمهور روسیه در پایان سال 2016، «دکترین جدید امنیت اطلاعات» را امضا کرد. در قسمت مقدماتی این دکترین یک بیانیه سلب مسئولیت وجود دارد که بر این اساس، دکترین، سند برنامه‌ریزی راهبردی در زمینه امنیت ملی در روسیه است که مفاد راهبرد امنیت ملی روسیه منتشرشده در سال 2015 را توسعه می‌دهد.

سه‌گانه – فرد، جامعه و دولت – در دکترین جدید باقی ماندند. امنیت اطلاعات روسیه یعنی:

موقعیت امنیت فرد، جامعه و دولت در برابر تهدیدات اطلاعاتی داخلی و خارجی که اجرای حقوق و آزادی‌های قانون اساسی یک فرد و شهروند، کیفیت مناسب زندگی برای شهروندان؛ حاکمیت، تمامیت ارضی و توسعه پایدار اجتماعی و اقتصادی فدراسیون روسیه؛ حفاظت و امنیت کشور در آن تأمین می‌شود (دکترین امنیت اطلاعات»، 2016: بخش اول).

منافع ملی روسیه در زمینه اطلاعات اکنون «نیازهای عینی مهم یک فرد، جامعه و دولت در تضمین امنیت و توسعه پایدار آن‌ها در حوزه اطلاعات است.»

به‌طور خاص، منافع ملی شامل شماری از مسئولیت‌های دولت و سایر بازیگران است که به پنج حوزه تقسیم شده و حول محور مصونیت محتوا، امنیت سایبری زیرساخت‌های اطلاعاتی، پیشرفت ظرفیت فناورانه و امنیت اطلاعات بین‌المللی بر اساس اصل حاکمیت ادغام شده است. («دکترین امنیت اطلاعات»، 2016: بخش دوم). این پنج حوزه به این شرح ذیل هستند:

اول، تضمین حقوق و آزادی‌های مردم طبق قانون اساسی برای دسترسی و استفاده از اطلاعات، صیانت از حریم خصوصی در استفاده از فناوری اطلاعات و ارتباطات؛ حمایت اطلاعاتی از نهادهای دموکراتیک همراه با سازوکارهای تعامل بین دولت و جامعه مدنی؛ و استفاده از فناوری اطلاعات و ارتباطات برای حفظ ارزش‌های فرهنگی، تاریخی و معنوی جمعیت چند قومی روسیه. دوم، تضمین عملکرد پایدار و تاب‌آور زیرساخت اطلاعاتی و در درجه اول زیرساخت حیاتی اطلاعاتی روسیه و شبکه مخابراتی یکپارچه آن در زمان صلح و زمان جنگ. سوم، توسعه صنعت فناوری اطلاعات و ارتباطات و الکترونیک روسیه و بهبود توسعه، تولید و بهره‌برداری از ابزارهای امنیت اطلاعات و نیز ارائه خدمات در زمینه امنیت اطلاعات. چهارم، ارائه اطلاعات موثق به افکار عمومی روسیه و جهان در مورد سیاست دولت و موضع رسمی آن در خصوص رویدادهای مهم اجتماعی در داخل کشور و در سراسر جهان. استفاده از فناوری اطلاعات و ارتباطات برای تأمین امنیت ملی در حوزه فرهنگ. پنجم، کمک به شکل‌گیری سیستم

امنیت اطلاعات بین‌المللی با هدف مقابله با تهدیدات استفاده از فناوری اطلاعات و ارتباطات به‌منظور نقض ثبات راهبردی و تقویت مشارکت راهبردی برابر در زمینه امنیت اطلاعات و همچنین حفاظت از حاکمیت روسیه در فضای اطلاعاتی.

بخش سوم دکترین نگرانی‌های اصلی دولت روسیه را در مورد امنیت اطلاعاتی تشریح و مجموعه‌ای از تهدیدها و چالش‌ها را متمایز می‌کند:

1. جریان اطلاعات فرامرزی در اهداف غیرقانونی ژئوپلیتیکی به بهای از دست رفتن ثبات راهبردی و همچنین در اهداف تروریستی و افراطی استفاده می‌شود.
2. افزایش ظرفیت کشورهای خارجی برای تأثیرگذاری بر زیرساخت‌های حیاتی اطلاعاتی و همچنین اطلاعات فنی آژانس‌های دولتی روسیه، سازمان‌های علمی و شرکت‌های نظامی–صنعتی به‌منظور اهداف نظامی.
3. سرویس‌های ویژه خارجی استفاده از ابزارهای اطلاعاتی نفوذ روانی را با هدف بی‌ثبات کردن سیستم‌های سیاسی و اجتماعی داخلی در مناطق مختلف جهان گسترش می‌دهند که منجر به تضعیف حاکمیت و تمامیت ارضی سایر دولت‌ها می‌شود.
4. افزایش حجم اطلاعات حاوی ارزیابی مغرضانه از سیاست دولت روسیه در رسانه‌های گروهی خارجی همراه با تبعیض آشکار نسبت به روزنامه‌نگاران روسی در خارج از کشور.
5. افزایش تعداد جرائم رایانه‌ای در بخش مالی و نقض حریم خصوصی در پردازش داده‌های شخصی.
6. کشورهای خاصی از فناوری اطلاعات و ارتباطات برای مقاصد نظامی استفاده می‌کنند که با قوانین بین‌المللی مغایرت دارد و هدف آن‌ها تضعیف حاکمیت، ثبات سیاسی و اجتماعی و تمامیت ارضی روسیه و متحدانش است که تهدیدی برای صلح بین‌المللی و امنیت جهانی و منطقه‌ای است.

این دکترین همچنین سطح بالای وابستگی به واردات سخت‌افزار و نرم‌افزار خارجی فناوری اطلاعات و ارتباطات را مشخص می‌کند که خطرات امنیتی را در استفاده از آن‌ها به همراه دارد، همچنین نرخ پایین برنامه‌های تحقیق و توسعه ملی در امنیت اطلاعات و اجرای آن‌ها را نشان می‌دهد. علاوه‌بر این، توزیع فعلی منابع موردنیاز برای عملکرد امن و پایدار اینترنت بین کشورها اجازه حاکمیت اینترنت برابر و مبتنی بر اعتماد را نمی‌دهد. درنهایت، فقدان هنجارهای حقوقی بین‌المللی که روابط بین‌الملل را در فضای اطلاعاتی تنظیم می‌کند و همچنین سازوکارها و رویه‌هایی برای کاربرد آن‌ها که ویژگی‌های فناوری اطلاعات و ارتباطات را در نظر می‌گیرد، شکل‌گیری یک سیستم بین‌المللی امنیت اطلاعات باهدف دستیابی به ثبات و مشارکت راهبردی برابر را دشوار می‌سازد. («دکترین امنیت اطلاعات»، 2016: بخش سوم).

گام‌های راهبردی برای جلوگیری از تهدیدات و مقابله با چالش‌های ذکرشده در بالا شامل مجموعه‌ای از اقدامات است. این اقدامات برای سیاست‌های نظامی، پیشگیری و مهار درگیری‌ها در فضای اطلاعاتی، ارتقای قابلیت‌های نیروهای مسلح برای انجام رویارویی اطلاعاتی و حفاظت از منافع متحدان روسیه در فضای اطلاعاتی است. در زمینه امنیت دولتی و عمومی، اقدامات شامل حفاظت از حاکمیت، ثبات سیاسی و اجتماعی و تمامیت ارضی، تأمین حقوق و آزادی‌های اساسی بشر و همچنین حفاظت از زیرساخت‌های اطلاعاتی حیاتی می‌شود. در زمینه اقتصاد، توسعه علم و فناوری همان افزایش سهم اقتصاد دیجیتال در نرخ تولید ناخالص داخلی ملی، جایگزینی واردات محصولات خارجی فناوری اطلاعات و ارتباطات، ایجاد نیروهای ذخیره‌ای از کارمندان در امنیت اطلاعات همراه با رواج فرهنگ امنیت اطلاعات شخصی است.

هدف اصلی همکاری بین‌المللی، شکل‌گیری یک سیستم پایدار از روابط بدون منازعه بین دولت‌ها در فضای اطلاعاتی است. برای تحقق این هدف، روسیه از حاکمیت خود در فضای اطلاعاتی از طریق اجرای یک سیاست مستقل با هدف تحقق منافع ملی محافظت خواهد کرد. اولاً، روسیه فعالانه در شکل‌گیری سیستم بین‌المللی امنیت اطلاعات شرکت خواهد کرد که مقابله مؤثری با استفاده از فناوری اطلاعات و ارتباطات به‌منظور مقاصد نظامی و سیاسی مغایر با قوانین بین‌المللی ارائه می‌کند. ثانیاً، روسیه به دنبال ایجاد سازوکارهای حقوقی بین‌المللی برای جلوگیری و حل‌وفصل درگیری‌های بین دولتی در فضای اطلاعاتی خواهد بود. ثالثاً، روسیه موقعیت خود را در سازمان‌های بین‌المللی کلیدی برای اطمینان از همکاری برابر و متقابلاً سودمند همه طرف‌های ذی‌نفع در زمینه اطلاعات ارتقاء خواهد داد.

شایان‌ذکر است، آخرین نکته در لیست گام‌های راهبردی که باید برداشته شود، توسعه سیستم حاکمیت ملی بخش روسی اینترنت است. این بند اشاره‌ای به ایده حاکمیت اطلاعاتی دارد و متضمن تغییرات جدی در سطح زیرساختی است که اکنون در قالب یک قانون جدید در حال انجام است. قانون عملکرد پایدار بخش روسی اینترنت در می 2019 امضا شد. هدف آن محافظت از رونت[۸۵] در برابر تهدیدات خارجی از طریق مسیریابی و کنترل متمرکز ترافیک اینترنت همراه با ایجاد سیستم نام دامنه ملی است (استادنیک[۸۶]، 2019).

این دکترین همچنین نقش کلیدی را برای سازمان‌های دولتی برای تأمین امنیت اطلاعات تعیین می‌کند. بااین‌حال، در میان «شرکت‌کنندگان» صاحبان زیرساخت‌های حیاتی اطلاعاتی و سازمان‌هایی که چنین اشیایی را اداره می‌کنند، رسانه‌ها و ارتباطات جمعی، بانکداری و سایر بخش‌های کارگزاران بازار مالی، کارگزاران سیستم‌های اطلاعاتی و ارائه‌دهندگان خدمات، سازمان‌های فعال در توسعه و بهره‌برداری از سیستم‌های اطلاعاتی و شبکه‌های ارتباطی، سازمان‌هایی که در این زمینه فعالیت آموزشی انجام می‌دهند، انجمن‌های عمومی، سایر سازمان‌ها و شهروندانی که در راهکار وظایف برای تضمین امنیت اطلاعات طبق قوانین فدراسیون روسیه مشارکت می‌کنند نیز هستند؛ بنابراین، دکترین اصل چند ذی‌نفعی را در برمی‌گیرد، اگرچه در حوزه وظایف و توانایی‌های هر یک از ذی‌نفعان در عمل خالی باقی می‌ماند. در این میان، دکترین اصولی را برای دولت تعیین می‌کند تا تعامل سازنده بین دستگاه‌های دولتی، سازمان‌ها و شهروندان را در حل مشکلات امنیت اطلاعات داشته باشد و تعادل بین نیازهای شهروندان در تبادل آزاد اطلاعات و محدودیت‌های مربوط به بیمه کردن امنیت ملی ازجمله حوزه اطلاعات را حفظ می‌کند.

برای جمع‌بندی بررسی دکترین‌ها باید گفت که علی‌رغم تشریح دقیق تهدیدات امنیت اطلاعات، هیچ‌کدام از آن‌ها به‌عنوان راهبردهای اصلی امنیت سایبری غرب نام برده نشده است، نه به نام کشورهای خارجی مخالف، نه به گروه تروریستی خاصی و نه به‌طور مستقیم به عدم تائید نقش آیکن در توزیع و مدیریت منابع اینترنتی اشاره نشده است.

حکمرانی بین‌المللی

روسیه از سال 1998 فعالانه درگیر سیاست‌های امنیت اطلاعات بین‌المللی بوده است. اولین ابتکار – نامه‌ای به دبیر کل سازمان ملل متحد در مورد مشکل در حال ظهور امنیت اطلاعات بین‌المللی بود؛ جایی که روسیه قطعنامه «تحولات در حوزه اطلاعات و مخابرات در زمینه امنیت بین‌المللی» را پیشنهاد کرد. این قطعنامه ضرورت جلوگیری از تبدیل‌شدن فضای اطلاعاتی به حوزه جدیدی برای رویارویی بین‌دولتی و درگیری‌های مسلحانه را صورت‌بندی کرد. علاوه‌بر این، پیشنهاد کرد که کشورهای عضو سازمان ملل متحد، دیدگاه‌های خود را در مورداستفاده از فناوری اطلاعات و ارتباطات برای مقاصد نظامی، تعریف «سلاح‌های اطلاعاتی» و «جنگ اطلاعاتی» و مصلحت دید خود را در خصوص ایجاد رژیم‌های حقوقی بین‌المللی برای منع توسعه انواع خطرناک سلاح‌های اطلاعاتی به‌طور سالانه به اطلاع دبیر کل برسانند. از زمان تصویب بدون رأی‌گیری قطعنامه، گزارش‌های سالانه دبیر کل به همراه دیدگاه کشورهای عضو سازمان ملل در مورد این موضوعات به مجمع عمومی ارائه شده است (مجمع عمومی سازمان ملل متحد[۸۷]، 1999).

بخش دوم ابتکار روسیه تأسیس گروه کارشناسان دولتی (گروه متخصصان دولتی سازمان ملل) بود. هدف آن بررسی تهدیدهای موجود و بالقوه ناشی از فضای اطلاعاتی و یافتن اقدامات مشارکتی ممکن برای مقابله با آن‌ها بود. این گروه در پنج نوبت در سال‌های 2004، 2010، 2013، 2015 و 2017 گردهمایی داشته است. برجسته‌ترین و پربارترین این گردهمایی‌ها گزارش‌های اجماعی سال‌های 2013 و 2015 بود. کشورهای شرکت‌کننده در مورد این موضوع کلیدی توافق کردند: حقوق بین‌الملل و همچنین مفهوم حاکمیت برای فضای سایبری/اطلاعاتی قابل اعمال است. آن‌ها همچنین هنجارها، قوانین و اصول رفتار مسئولانه دولت‌ها در حوزه فناوری اطلاعات و ارتباطات و همچنین اقدامات اعتمادساز، همکاری بین‌المللی و ظرفیت‌سازی را پیشنهاد کردند (مجمع عمومی سازمان ملل متحد ، 2015b). هیئت روسی علاقه‌مند به گزارش 2015

---

[85] RUnet
[86] Stadnik
[87] UNGA

بود؛ زیرا ترویج رفتار مسئولانه دولت عنصر کلیدی سیاست بین‌المللی امنیت اطلاعات است (Namib.online، 2013). روسیه اسنادی را برای بحث بین‌المللی در قالب‌های مختلف به سازمان ملل پیشنهاد کرد: مفهوم کنوانسیون امنیت اطلاعات بین‌المللی 2011 (Министерство иностранных дел Российской Федерации، 2011) و کد رفتار بین‌المللی برای امنیت اطلاعات با حمایت مشترک کشورهای عضو سازمان همکاری شانگهای در 2011 و 2015 (مجمع عمومی سازمان ملل متحد، 2015a). این اسناد مبتنی بر حاکمیت در محیط فناوری اطلاعات همراه با نقش کلیدی دولت‌ها در حاکمیت اینترنت و تأمین امنیت در فضای اطلاعاتی است.

اگرچه ویژگی کلیدی ابتکار سازمان همکاری شانگهای ماهیت صلح‌جویانه آن است – و برخلاف ابتکارات غربی برای تنظیم جنگ سایبری است – حتی پس‌ازاینکه آخرین نسخه شامل بخش حقوق بشر شد که رویکردی متوازن به این موضوع را ایجاد می‌کند و مجدداً تائید می‌کند که حقوقی که یک فرد در یک محیط آفلاین دارد، باید به‌صورت آنلاین نیز محافظت شود، حمایت کافی برای پذیرش دریافت نکرد؛ اما غیرقابل‌قبول‌ترین نکته بین‌المللی شدن حاکمیت اینترنت است که توسط روسیه در ارتباط با نگرش شکاکانه آن نسبت به آیکن حتی پس از انتقال آیانا ترویج شد. تنها هدف بین‌المللی کردن اینترنت جلوگیری از تصمیم سیاسی رهبری یک کشور از محدود کردن عملکرد اینترنت در کشور دیگر است. شاید لازم باشد سازمانی زیر نظر شورای امنیت سازمان ملل ایجاد شود که به‌جای یک سازمان خصوصی تحت صلاحیت یک کشور خاص، چنین تصمیماتی را بر اساس قوانین بین‌المللی اتخاذ کند.

با بازگشت به قوانین رفتار مسئولانه دولت، کار پنجمین گروه کارشناسان دولتی سازمان ملل در سال 2017 بدون گزارش اجماعی پایان یافت. علیرغم طعم تلخ عدم دستیابی به توافق و پیشنهادهای برخی از شرکت‌کنندگان گروه برای تکمیل این قالب (شورای اروپا در روابط خارجی[88]، 2017)، روسیه آمادگی خود را برای ادامه بحث درباره رفتار مسئولانه دولت‌ها در سازمان ملل اعلام کرد. به‌طورقطع، خط گسل اصلی بین دو اردوگاه، اختلاف‌نظر در مورد قابل‌اجرا بودن حقوق بین‌الملل بشردوستانه بود، زیرا «سناریوی جنگ و اقدامات نظامی را در چارچوب فناوری اطلاعات و ارتباطات مشروعیت می‌بخشد» (دفتر نمایندگی کوبا در خارج از کشور، 2017)، گزینه‌ای که کاملاً در تضاد با سیاست روسیه در امنیت اطلاعات بین‌المللی است. آقای کروتسکیخ، نماینده ویژه روسیه در همکاری‌های بین‌المللی در زمینه امنیت اطلاعات، قصد ارائه قطعنامه جدیدی را تائید کرد. وی خاطرنشان کرد که روسیه از میان فهرست گسترده اعضای سازمان همکاری شانگهای، شامل هند و پاکستان، کشورهای بریکس، آمریکای لاتین و خاورمیانه به دنبال حمایت از سند برای تبدیل‌شدن به حامیان مشترک است (Международная Жизнь، 2017).
در پایان سال 2018، پیش‌نویس قطعنامه‌ای دبیر کل را فرامی‌خواند تا یک گروه کاری جدید (کارگروه آزاد سازمان ملل) را به مجمع عمومی ارسال کند (مجمع عمومی سازمان ملل متحد، 2018a). تقریباً هم‌زمان، ایالات‌متحده سند مشابهی را باهدف ایجاد ششمین گروه متخصصان دولتی سازمان ملل در قالب سنتی ارائه کرد. درنهایت هر دو قطعنامه به تصویب رسید. وظیفه کارگروه آزاد سازمان ملل بحث در مورد اجرای هنجارهای سایبری توافق شده قبلی از گزارش‌های قبلی گروه متخصصان دولتی است، اما یک افزوده مهم به لیست وجود دارد (مجمع عمومی سازمان ملل متحد، 2018b). هنجار جدید اضافه‌شده می‌گوید که همه اتهامات علیه دولت‌ها در مورد سازمان‌دهی و/یا انجام فعالیت‌های غیرقانونی به‌وسیله فناوری اطلاعات و ارتباطات باید اثبات شود. این هنجار همچنین مختصراً به مشکل ارجاع دادن یک حادثه و نیاز به مطالعه تمام اطلاعات موجود و زمینه گسترده‌تر آن اشاره می‌کند. برخی از هنجارهای حذف‌شده از پیش‌نویس قطعنامه اصلی از نامه‌های سازمان همکاری شانگهای که در بالا ذکر شد وام گرفته‌شده‌اند. در عوض آن‌ها تا حدی در مقدمه قطعنامه گنجانده شدند: بندهای جدید نشان‌دهنده نگرانی فزاینده روسیه و سایر کشورها از موضوع «انتشار اخبار نادرست یا تحریف‌شده است که می‌تواند به‌مثابه دخالت در امور داخلی سایر کشورها تعبیر شود.» این مفاد دلیلی شد تا 46 دولت که عمدتاً از دموکراسی‌های غربی بودند، علیه این قطعنامه رأی دهند. کارگروه آزاد سازمان ملل گزارش اجماعی خود را تا سال 2020 ارائه خواهد کرد. وظیفه اضافی، بررسی امکان نهادینه کردن گفتگو در مورد اعمال قوانین بین‌المللی به‌طور منظم تحت نظارت سازمان ملل است. روسیه نیز مانند گذشته در ششمین گروه متخصصان دولتی سازمان ملل متحد شرکت خواهد کرد. نتیجه گزارشی در سال 2021 خواهد بود که نیازی به اجماع همه شرکت‌کنندگان ندارد، اما باید حاوی ضمیمه‌ای باشد که در آن 25 عضو گروه متخصصان دولتی

[88] ECFR

سازمان ملل مواضع ملی خود را در مورد کاربرد قوانین بین‌المللی در محیط فاوا درج کنند. هر دو گروه توافق کردند که کار خود را مکمل یکدیگر نگه دارند (نهاد پژوهش خلع سلاح سازمان ملل متحد[۸۹]، 2019).

در بهار سال 2017، به‌واسطه پیش‌نویس کنوانسیون سازمان ملل متحد در مورد همکاری در مبارزه با جرائم سایبری، نظرات روسیه بیشتر وارد سازمان ملل متحد شد. (مجمع عمومی سازمان ملل متحد، 2017). این سند حفاظت از حاکمیت دولت را در رأس قرار داده است: «این کنوانسیون به یک دولت عضو اجازه نمی‌دهد تا در قلمرو کشوری دیگر صلاحیت و وظایفی را که طبق قوانین داخلی آن منحصراً برای مقامات آن کشور دیگر محفوظ است، اعمال کند.» اساساً، کنوانسیون کشورهای عضو را ملزم خواهد کرد که اقدامات تقنینی و سایر اقدامات لازم را اتخاذ کنند تا اعمال پیش‌بینی‌شده در کنوانسیون را به‌عنوان یک جرم یا عمل غیرقانونی دیگر تحت قوانین داخلی خود تعیین و همچنین رویه‌های پیش‌بینی‌شده برای پیشگیری، سرکوب و بررسی جرائم و انجام اقدامات قضایی مرتبط با این جنایات را ایجاد کند. جالب‌توجه است، ماده 27 تصریح می‌کند که دولت‌ها باید جمع‌آوری بلادرنگ داده‌های ترافیکی را ایجاد کنند و از این طریق شهروندان خود را تحت نظارت قرار دهند. این سند مملو از مقررات دیگری است که برای کشورهای دموکراتیک غیرقابل‌قبول است. در آن تاریخ، این سند موردتوجه قرار نگرفت. بااین‌حال، روسیه این ایده را رها نکرد و قطعنامه جدیدی با عنوان «مقابله با استفاده از فناوری اطلاعات و ارتباطات برای مقاصد مجرمانه» به کمیته سوم ارائه کرد که در پایان سال 2018 نیز با رأی‌گیری به تصویب رسید. نکته مهم این است که این قطعنامه الزام می‌کند که در هفتاد و چهارمین نشست مجمع عمومی سازمان ملل متحد از سوی دبیر کل گزارشی به همراه دیدگاه‌های کشورهای عضو در مورد چالش‌های پیش روی این کشورها در مقابله با به‌کارگیری فناوری اطلاعات و ارتباطات به‌منظور مقاصد جنایی، ارائه شود. بدیهی است که هدف از این قطعنامه وادار کردن به معاهده جدیدی برای جایگزینی کنوانسیون بوداپست در مورد جرائم سایبری است. درحالی‌که خود متن حاوی ارجاعی به پیش‌نویس کنوانسیون طرح‌شده توسط روسیه در سال 2017 نیست، یک دستور کار تخصصی جدید برای نشست بعدی سازمان ملل ایجاد می‌کند. سرگئی لاوروف، وزیر امور خارجه روسیه، در افتتاحیه هفتاد و سومین نشست سازمان ملل متحد، مجدداً بر قصد آغاز روند مذاکره درباره کنوانسیون جدید جرائم سایبری (Министерство иностранных дел Российской Федерации، 2018a) تأکید کرد. انجمن‌های ارتباطات پیشرو از قطعنامه به دلیل اصطلاح مبهم «استفاده از فناوری اطلاعات و ارتباطات برای مقاصد مجرمانه» انتقاد کردند زیرا ممکن است به جرم انگاری فعالیت آنلاین اشاره کند:

به‌طور خاص، قوانین جرائم سایبری به شیوه‌هایی اعمال می‌شوند که مخالفان و انتقادات به دولت را سرکوب می‌کنند، اعتراضات مسالمت‌آمیز را غیرقانونی قلمداد می‌کنند، دسترسی بی‌رویه به داده‌های مردم را به دست می‌آورند و نسبت به ابزارهایی که امکان رمزگذاری و ناشناس ماندن را فراهم می‌کنند، سختگیری می‌کنند. (APC، 2018)

همین‌طور. قوانین ملی روسیه در مورد امنیت سایبری و اطلاعات در این راستا در حال توسعه است.

قوانین ملی در مورد امنیت سایبری

سیاست دولت در قبال اینترنت و فضای اطلاعاتی در ده سال گذشته در حال تحول بوده است. قبل از آن زمان، بخش روسی اینترنت همراه با خدمات دیجیتال را می‌توان با مجموعه‌ای از کلمات مشخص کرد: خودسازمان‌دهی، خودتنظیمی و عدم‌مداخله دولتی. پاسخ قطعی برای اینکه چه چیزی محرکی برای منافع دولتی دایر در تنظیم فضای اطلاعاتی شده است، وجود ندارد. خواه این محرک یک گرایش قابل توضیح برای مواجهه با ظرفیت و چالش دائماً در حال رشد دیجیتالی شدن باشد یا اینکه نخبگان حاکم متوجه نیروی فناوری اطلاعات و ارتباطات برای توانمندسازی شهروندان برای قیام علیه مقامات، همان‌طور که در بیداری اسلامی اتفاق افتاد، شده باشند. واقعیت این است که پارلمان مقررات انتشار اطلاعات در اینترنت را متعاقب اعتراضات پس از انتخابات روسیه در زمستان 2011، تصویب کرد. این کار با مسدود کردن صفحات وب و منابع اینترنتی

[89] UNIDIR

حاوی اطلاعات ممنوعه خارج از دادگاه و ایجاد «لیست سیاه» از منابع اینترنتی (همه خدمات اینترنتی که اجازه ارسال پیام را می‌دهند) آغاز شد[۹۰] (قانون فدرال[۹۱] FZ-97، 2014a) که این منابع را ملزم می‌کند اطلاعات مربوط به پذیرش، انتقال، تحویل و (یا) پردازش صدا، متن، تصویر یا سایر پیام‌های الکترونیکی کاربران اینترنت و اطلاعات مربوط به این کاربران را در داخل خاک روسیه نگه‌داشته و ظرف مدت شش ماه در اختیار دستگاه‌های دولتی مجاز انجام دهنده فعالیت عملیاتی و تحقیقاتی قرار دهد.

یکی دیگر از قوانین فدرال که برای شرکت‌های اینترنتی مشکل ایجاد کرد، حفاظت از داده‌های شخصی شهروندان روسیه و محلی‌سازی فیزیکی آن در داخل مرزهای روسیه بود (قانون فدرال FZ-242، 2014b). اگرچه همه غول‌های اینترنتی خارجی هنوز شرایط لازم را برای سازمان‌دهی ذخیره‌سازی و پردازش داده‌های شخصی در مراکز داده واقع در روسیه برآورده نکرده‌اند، شبکه حرفه‌ای لینکدین به دلیل عدم رعایت این قانون مسدود شد. در سال 2016 رئیس‌جمهور مجموعه‌ای از اصلاحات «ضد تروریستی» را در خصوص مقابله با تروریسم و قانون کیفری در قانون فدرال امضا کرد که «بسته یاروویا» نام گرفت (مدوزا،[۹۲] 2016). ناظر به امنیت اطلاعات، بسته یاروویا اپراتورها و ارائه‌دهندگان مخابراتی را ملزم به ذخیره هر نوع مکاتبات و داده‌های کاربر برای یک دوره زمانی خاص می‌کند.[۹۳] علاوه‌بر این، سازمان‌دهندگان انتشار اطلاعات در اینترنت را ملزم به رمزگشایی پیام‌های کاربران می‌کند. بنا به درخواست سرویس امنیت فدرال روسیه[۹۴]، شرکت‌ها ملزم به ارائه کلیدهای ترافیک رمزگذاری شده خواهند بود. پیام‌رسان تلگرام از ارائه کلیدهای رمزنگاری خودداری کرد و توضیح داد که چت‌های مخفی در تلگرام از رمزگذاری سرتاسری استفاده می‌کنند. به‌هرحال، این دلیلی برای تصمیم‌گیری برای مسدود کردن پیام‌رسان در خاک روسیه شد.

در رابطه با امنیت سایبری، پارلمان قانون FZ-187 را در سال 2017 در مورد امنیت زیرساخت اطلاعات حیاتی روسیه (CII) تصویب کرد (Consultant.ro، 2017). این قانون از اشیاء (یعنی اشیاء فیزیکی که زیرساخت‌های حیاتی را تشکیل می‌دهند) و افراد (یعنی صاحبان اشیاء) و مسئولیت‌های آن‌ها در رابطه با قانون تعریفی ارائه می‌دهد. اشیاء زیرساخت اطلاعات حیاتی شامل سیستم‌های اطلاعاتی، شبکه‌های اطلاعاتی و مخابراتی و سیستم‌های کنترل خودکارِ مالکان زیرساخت اطلاعاتِ حیاتی است. مالکان این زیرساخت می‌تواند شامل مؤسسات دولتی، اشخاص حقوقی روسی/ مؤسسان فردی شرکت‌ها باشند که با سیستم‌های فوق‌الذکر و شبکه‌ها در تمام بخش‌های اقتصاد، انرژی، تولید و دفاع در تعامل هستند. قانون افراد را مأمور به دسته‌بندی اشیاء زیرساخت اطلاعات حیاتی به‌منظور تعریف اهمیت آن‌ها و اولویت‌بندی امنیت آن‌ها، اطمینان از الحاق اشیاء زیرساخت اطلاعات حیاتی به سیستم ملی امنیت سایبری GosSOPKA[95] و درنهایت اقدامات سازمانی و فنی برای اطمینان از امنیت زیرساخت اطلاعات حیاتی می‌کند. علاوه‌بر این، این قانون شامل اصلاحاتی (منتشرشده در FZ-194 مجزا) به قانون جزایی است که مسئولیت کیفری را برای اعمال غیرقانونی / ناحق علیه اشیاء زیرساخت اطلاعات حیاتی تعیین می‌کند. بخشی از این قانون توسط مرکز ملی هماهنگی حوادث رایانه‌ای[۹۶] در جولای 2018 وضع شده بود. این مرکز مسئولیت تبادل اطلاعات در مورد حوادث رایانه‌ای بین اشیاء زیرساخت اطلاعات حیاتی را بر عهده دارد و همچنین به‌عنوان یک نقطه تماس برای تعامل با گروه‌های پاسخگویی حوادث رایانه‌ای[۹۷] خارجی عمل می‌کند.

---

[90] اطلاعات ممنوع طبق قانون فدرال FZ-139 شامل پورنوگرافی کودکان، تبلیغات مواد مخدر و خودکشی است. بعداً، قانون فدرال FZ-398 فراخوان برای شورش های دسته جمعی، فعالیت های افراطی، شرکت در رویدادهای جمعی (عمومی) که بر خلاف رویه تعیین شده انجام می شود را، به عنوان مبنایی برای ممانعت از تصمیم دادستانی عمومی اضافه کرد. در نهایت، FZ-187 که قانون ضد تکثیر غیر مجاز نامیده می شود، به درخواست صاحب حقوق اجازه می دهد تا سایت های حاوی محتوای بدون مجوز را مسدود کند.

[91] The Federal Law

[92] Meduaza

[93] این قانون در ژوئیه 2018 به اجرا درآمد. در آوریل 2018، دولت روسیه فرمانی را در مورد قوانین ذخیره سازی داده منتشر کرد: 30 روز برای ارائه دهندگان اینترنت و 6 ماه برای اپراتورهای مخابراتی. ابرداده در مورد حقایق ارتباطات باید به مدت 3 سال ذخیره شود. با این حال، به دلیل عدم وجود تجهیزات ذخیره‌سازی اطلاعات تایید شده با ظرفیت لازم، هیچ‌کس قانون را اجرا نمی‌کند.

[94] FSB

[95] سیستم دولتی برای تشخیص، پیشگیری و از بین بردن اثرات حملات رایانه ای

[96] NCCCI

[97] CERT(Computer emergency response team): گروه‌های تخصصی برای مدیریت رخدادهای امنیتی

(Официальный интернет-портал правовой информации، 2018b) تمام تعاملات بین‌المللی واکنش به حوادث باید فقط از طریق مرکز ملی هماهنگی حوادث رایانه‌ای انجام شود (به‌جز مواردی که توافقنامه‌های همکاری ویژه وجود دارد، اما حتی در آن زمان نیز مرکز ملی هماهنگی حوادث رایانه‌ای باید مطلع شود). اگر چنین اطلاعاتی امنیت ملی روسیه را تهدید کند، مرکز ملی هماهنگی حوادث رایانه‌ای می‌تواند از به اشتراک گذاشتن اطلاعات در مورد حوادث با همتایان خارجی خودداری کند. علاوه‌بر این، مرکز ملی هماهنگی حوادث رایانه‌ای در حال حاضر عملکردها و زیرساخت‌های تیم پاسخگویی حوادث رایانه‌ای دولتی[۹۸] را که در سال 2012 توسط سرویس امنیت فدرال روسیه برای پاسخ به حوادث در شبکه‌های دولتی روسیه تأسیس شد، به کار می‌گیرد.

درنهایت، برجسته‌ترین و راهگشاترین قانون که در بخش اول به آن اشاره شد، اخیراً – در ماه می 2019 – تصویب شده است. این اولین قانون در نوع خود است که هدف آن منحصراً تنظیم‌گری بخش ملی اینترنت است. مردم به دلیل ماهیت بسیار محدودکننده و چندپاره کننده‌اش آن را «قانون مقتدرانه رونت مقتدر» نامیدند (Официальный интернет-портал правовой информации، 2019). به‌طور خلاصه، قانون مسئولین اصلی عملکرد پایدار اینترنت در روسیه را تعریف می‌کند. آن‌ها اپراتورهای مخابراتی و مالکان و یا صاحب‌امتیازان موارد زیر هستند: (1) شبکه‌های ارتباطی فنی (مورداستفاده برای عملیات حمل‌ونقل/انرژی و سایر زیرساخت‌های غیر متصل به شبکه ارتباطی عمومی)؛ (2) نقاط تبادل ترافیک؛ (3) خطوط ارتباطی عبور از مرز دولتی؛ و (4) اعداد سیستم خودمختار (ASN). همه آزمودنی‌ها باید در تمرینات منظم برای بررسی پایداری عملکرد رونت شرکت کنند. روسکماندزور[۹۹]، یک نهاد ناظر فدرال روسیه در زمینه ارتباطات، فناوری اطلاعات و ارتباطات جمعی، مدیریت متمرکز شبکه‌های ارتباطی را در صورت تهدید برای ثبات و امنیت رونت با تعریف سیاست‌های مسیریابی برای اپراتورهای مخابراتی و سایر موارد و هماهنگ کردن اتصالات آن‌ها اجرا خواهد کرد. علاوه‌بر این، یک مرکز جدید برای نظارت و کنترل شبکه‌های ارتباطی عمومی تحت نظارت روسکماندزور پدید خواهد آمد. اپراتورهای مخابراتی موظف‌اند در شبکه‌های خود از نصب ابزارهای فنی تحت حمایت دولت برای مقابله با تهدیدات علیه ثبات، امنیت و یکپارچگی عملیات اینترنت در خاک روسیه اطمینان حاصل کنند. این ابزارهای فنی همچنین به‌منظور فیلتر کردن ترافیک و مسدود کردن دسترسی به منابع ممنوعه اینترنتی عمل خواهند کرد. این عمل قرار است جایگزین سیستم موجود «لیست سیاه» شود که در آن فیلترینگ و مسدودسازی توسط خود ارائه‌دهندگان انجام می‌شود. درنهایت، قانون ایجاد سیستم نام دامنه ملی را فراهم می‌کند که باید دسترسی به وب‌سایت‌های روسی را در مواقع اضطراری تضمین کند. اگرچه این قانون باید در نوامبر 2019 لازم‌الاجرا می‌شد، اما به دلیل عدم وجود دستورات و مصوبات مربوطه برای تنظیم ظرایف فنی هنوز آماده اجرا نیست.

برای نتیجه‌گیری از مقررات ملی، می‌بینیم که بیشترین توجه به امنیت اطلاعات شده است. هدف دولت کنترل جریان اطلاعات و فیلتر کردن محتوای نامطلوب به هر قیمتی است. ناظر به امنیت سایبری، تصویب اولین قانون زیرساخت‌های اطلاعاتی حیاتی چندین سال به طول انجامید و اکنون دولت در تلاش است تا کار روی قانونی را تکمیل کند که هدف آن کنترل زیرساخت رونت و مستقل ساختن آن از هرگونه خاموشی خارجی در مورد اضطراری است. این قانون اکنون برای دولت نه‌تنها برای اعلام حاکمیت خود در فضای سایبری، بلکه برای اطمینان از اجرای فنی آن و هم‌راستایی اینترنت با مرزهای ملی‌اش حیاتی است (مولر[۱۰۰]، 2017).

98 GOV-CERT
99 Roskomnadzor
100 Mueller

کره جنوبی

مقدمه

ازآنجایی‌که کره جنوبی دارای فناوری دیجیتال پیشرفته، شبکه‌های کامپیوتری کارآمد و بالاترین نرخ نفوذ اینترنت پرسرعت در جهان است، این کشور (ROK) به‌عنوان یک کشور دارنده «اینترنت قوی» شهرت پیدا کرده است. بااین‌وجود در پس این دستاوردها، ملت کره در برابر تهدیدات سایبری آسیب‌پذیر بوده است، به‌ویژه در برابر تهدیداتی که ادعا می‌شود کره شمالی با شروع حملات متعدد توزیع‌شده سرویس (DDoS) در جولای 2009، اغلب به وب‌سایت‌های دولتی، مالی و زیرساخت‌های حیاتی کره جنوبی نفوذ کرده و آن‌ها را فلج کرده است. این حملات سایبری کره شمالی، کره جنوبی را بر آن داشت تا حفاظت و امنیت فضای سایبری را به‌عنوان اولویتی برای امنیت ملی کره جنوبی قرار دهد. کره جنوبی برای تقویت قابلیت‌های سایبری خود، مجموعه‌ای از اقدامات ازجمله توسعه دیوارهای آتش، استخدام متخصصان سایبری، ایجاد فرماندهی جنگ سایبری، پیشرفت سازمان‌های آموزشی و پیشبرد چارچوب‌های قانونی حمایت از حفاظت سایبری را انجام داده است.

با در نظر گرفتن این حقایق، این فصل به سؤالات زیر می‌پردازد: کره جنوبی با چه چالش‌هایی در حوزه امنیت سایبری روبه‌رو بوده است؟ استراتژی امنیت سایبری کشور چقدر مؤثر بوده است؟ چه اقداماتی برای تقویت استراتژی امنیت سایبری آن لازم است؟

در پاسخ به این سؤالات، این فصل سه چالش اصلی امنیت سایبری را برجسته می‌کند که کره جنوبی با آن روبرو می‌شود.

1- ماهیت ذاتاً آسیب‌پذیر امنیت سایبری، تهدیدات سایبری کره شمالی، و مسابقه تسلیحاتی سایبری چین در ایالات‌متحده.

2- محتویات استراتژی امنیت سایبری کره جنوبی از طرح جامع امنیت سایبری ملی که در سال 2011 ساخته شد.

3- استراتژی امنیت سایبری ملی و برنامه اساسی تصویب‌شده در سال 2019.

این فصل بعد از این، استراتژی امنیت سایبری کره جنوبی را در منظر مقایسه‌ای ارزیابی می‌کند و بر حوزه‌هایی که نیاز به توسعه بیشتر در استراتژی امنیت سایبری این کشور دارند، تأکید می‌کند؛ مانند تقویت ساختار حاکمیت امنیت سایبری، ایجاد یک چارچوب قانونی جامع امنیت سایبری، پاسخ‌های مؤثرتر به حملات سایبری کره شمالی.

چالش‌های امنیت سایبری کره جنوبی

کره جنوبی در محیط امنیت سایبری خود با سه چالش اصلی روبرو بوده است. نخست، کره جنوبی مانند همه کشورها، از ماهیت ذاتاً آسیب‌پذیر امنیت سایبری مستثنی نیست. یعنی حفاظت کامل از فضای سایبری برای یک ملت تقریباً غیرممکن است، زیرا هکرهای تحت حمایت دولتی و/یا خصوصی می‌توانند با استفاده از فناوری سایبری به‌خوبی توسعه‌یافته به سیستم سایبری هر کشوری نفوذ کنند. مهارت‌های هک سایبری و جاسوسی به‌موازات پیشرفت بی‌پایان فناوری دیجیتال همچنان درحال‌توسعه هستند. درنتیجه، با توجه به هنری ناو (2019: 238)، «تخمین زده می‌شود که هرروز 55000 بدافزار جدید تولید می‌شود که حدود 200000 رایانه به «زامبی» تبدیل می‌شوند (رایانه‌هایی که توسط بازیگران خارجی کنترل می‌شوند) و میلیون‌ها رایانه در بسته‌بندی می‌شوند. نمونه‌های بسیار دیگری از این آسیب‌پذیری‌ها در سراسر جهان وجود داشته است، از جمله حملات سایبری کره شمالی به Sony Pictures Entertainment در سال 2014 و هک روسیه در شبکه کمیته ملی دموکرات ایالات‌متحده در سال 2015.

در این راستا، جامعه کره جنوبی که از طریق شبکه‌های رایانه‌ای کارآمد به هم متصل است، به‌شدت در برابر حملات سایبری خارجی و جاسوسی سایبری آسیب‌پذیر بوده است. به‌عنوان‌مثال، کره جنوبی در طول سه سال از 2015 تا 2017 بیش از 10000 حمله باج افزاری داشته است، بنابراین متحمل ضرر مالی حدود یک تریلیون وون کره شده است.

دوم، کره شمالی علاوه‌بر تهدیدات هسته‌ای و موشکی، یک تهدید جدی سایبری برای دولت و بخش خصوصی کره جنوبی نیز به شمار می‌رود. کره شمالی که تأکید بیشتری بر حاکمیت سایبری مانند چین و روسیه دارد تا آزادی در فضای سایبری که توسط کشورهای غربی حمایت می‌شود، توجه زیادی به تقویت امنیت رژیم خود از طریق کنترل اطلاعات در فضای محدود سایبری کشور داشته است. در مخالفت با افزایش تحریم‌های اعمال‌شده توسط شورای امنیت سازمان ملل متحد به دلیل تحریکات هسته‌ای/موشکی این کشور، کره شمالی برای توسعه سایبری خود تلاش کرده است؛ ازجمله ایجاد قابلیت‌هایی در تلاش برای انجام سرقت‌های بانک دیجیتال. با توجه به این حقایق، هکرهای کره شمالی اغلب به جنوب نفوذ کرده و وب‌سایت‌های دولت، امور مالی و زیرساخت‌های حیاتی کره را فلج کرده‌اند؛ اگرچه دولت کره شمالی به‌شدت هرگونه دخالت در آن را رد کرده است. حملات سایبری بسیار متفاوت از حملات متعارف هستند، به‌ویژه از دو جنبه:

1. اول، انتساب دقیق به بازیگران خاص در مورد حملات سایبری دشوار است.
2. دوم اینکه پاسخ دادن به حملات سایبری با پاسخ نظامی بسیار خطرناک است.

اولین بار حملات سایبری ثبت‌شده کره شمالی در ژوئیه 2009 روی داد. پیونگ‌یانگ چندین حمله DDoS را بر روی وب‌سایت‌های دفتر ریاست جمهوری کره، وزارت دفاع ملی و مجلس ملی انجام داد. درنتیجه، این وب‌سایت‌ها به دلیل درخواست‌های دسترسی ایجادشده توسط نرم‌افزارهای مخرب فلج شدند. در مارس 2011، هکرهای کره شمالی به بانک Nonghyup کره جنوبی حمله کردند و 273 سرور از 587 سرور این بانک را نابود کردند. این حملات در مورد 48000 کامپیوتر، و هفته‌ها طول کشید تا سیستم‌ها به‌طور کامل بازیابی شوند. به‌عنوان یکی از شدیدترین حملات سایبری که کره جنوبی متحمل شد، "حمله تاریک سئول" کره شمالی به انتشار بین‌المللی اصطلاحات – تهدید پایدار پیشرفته (APT) یا تروریسم سایبری کمک کرد.

توانایی کره شمالی برای فلج کردن زیرساخت‌های کره جنوبی، درنتیجه به انتشار روایت‌های "سایبری پرل هاربر" کمک می‌کند، که بر تأثیرات فیزیکی فاجعه‌بار تمرکز دارد. یک گروه هکر کره شمالی به نام Blunenoroff، متخصص در جرائم مالی که در سال 2016 شروع به کارکرد، گمان می‌رود که حملات مالی به مؤسسات مبادله ارزهای دیجیتال کره جنوبی انجام داده است. صرافی بیت کوین "یوبیت" دو بار در آوریل و دسامبر 2017 موردحمله قرار گرفت و پس از دست دادن حدود 20 میلیون دلار ورشکست شد. در ژوئن 2018، Conrail و Bithumb به ترتیب 37 میلیون دلار و 40 میلیون دلار درنتیجه چنین حملات سایبری کره شمالی از دست دادند. اگرچه به‌سختی می‌توان همه این حملات را به‌وضوح به کره شمالی نسبت داد، اما فرض کنید که کره شمالی بر اساس ترکیب کدهای مخرب استفاده شده در این حملات و نحوه عملکرد آن مسئول عملیات سایبری بوده است. این یک واقعیت شناخته‌شده است که بسیاری از گروه‌های هکر کره شمالی چنین اقدامی انجام می‌دهند.

چالش دیگر کره جنوبی این است که محیط امنیت سایبری این کشور شبیه تنظیمات ژئوپلیتیکی پیرامون شبه‌جزیره کره است. در محیط ژئوپلیتیکی، کره جنوبی بین دو ابرقدرت – ایالات‌متحده و چین – قرارگرفته است که رقابت استراتژیک و اقتصادی آن‌ها در اواخر دهه 2000 شروع شد. به دنبال موضع اعلام‌شده ایالات‌متحده، دولت کره جنوبی استدلال کرد که سیستم "تاد" عمدتاً برای محافظت از کره جنوبی در برابر موشک‌های کره شمالی است. بااین‌حال، چین با این ادعا که رادار باند X تاد می‌تواند تمام چین را پوشش داده و توان موشکی چین را کاهش دهد، واکنش نشان داد. دولت چین پس‌ازآن افراد مشهور کره جنوبی را از برگزاری نمایش در چین منع کرد و گردشگران چینی را از بازدید از کره جنوبی محدود کرد. بسیاری از کره جنوبی محصولات در بازارهای چین نیز تحریم شدند، به‌طوری‌که اقتصاد کره جنوبی که به‌شدت به چین وابسته است، آسیب جدی دید.

کره جنوبی متأثر از تشدید رقابت تسلیحاتی سایبری بین ایالات‌متحده و چین است. ایالات‌متحده برای پاسخ به حملات سایبری فزاینده چین، تمام تلاش خود را انجام داده است؛ از جمله تقویت قابلیت‌های سایبری خود با به‌روزرسانی استراتژی امنیت سایبری، بازسازی ساختار سایبری فرماندهی، پرورش بسیاری از جنگجویان سایبری، و ترویج همکاری امنیت سایبری با متحدان اطلاعاتی انگلیسی (مانند بریتانیا، کانادا، استرالیا و نیوزلند). پس از مشاهده فناوری پیشرفته آمریکا در جنگ‌های اول و دوم خلیج فارس، چین نیز منابع عظیمی را برای پیشبرد قابلیت‌های سایبری

خود و ایجاد ارتش قوی‌تر سرمایه‌گذاری کرده است. برای به حداکثر رساندن منافع استراتژیک و اقتصادی خود، کره جنوبی باید روابط متحدانه خود را با ایالات‌متحده حفظ کند و هم‌زمان با چین همکاری نزدیکی داشته باشد. بااین‌حال، تشدید رقابت قدرت سایبری آمریکا و چین، کره جنوبی را در موقعیتی دوسوگرا قرار می‌دهد. همان‌طور که در بالا ذکر شد، بسیاری از هکرهای کره شمالی برای انجام حملات سایبری در چین اقامت دارند. با توجه به این واقعیت، آمریکا دولت چین را برای حل این موضوع تحت فشار قرار داده است، اما چین موضوع تهدیدات سایبری کره شمالی را صرفاً بهانه‌ای برای محاصره چین از سوی آمریکا می‌داند.

استراتژی امنیت سایبری کره جنوبی

با توجه به این چالش‌ها، دولت کره جنوبی به دنبال محافظت از فضای سایبری ملی خود در برابر حملات سایبری بوده است. در آگوست 2011، این تلاش با ایجاد طرح جامع امنیت سایبری ملی، که "یک استراتژی پاسخ جامع در سطح ملی به‌منظور مقابله مؤثر با تهدیدات سایبری ملی که به‌طور فزاینده‌ای پیچیده و هوشمند می‌شوند" به اوج خود رسید.

طرح جامع امنیت سایبری ملی دارای پنج الزام اصلی بود:

- ایجاد یک سیستم تشخیص و پاسخ زودهنگام تهدیدات سایبری متشکل از بخش‌های خصوصی، عمومی و نظامی که باهم کار می‌کنند.
- تقویت امنیت زیرساخت‌های حیاتی و افزایش حفاظت از اطلاعات محرمانه.
- توسعه پلتفرم‌هایی برای ایجاد امنیت سایبری قوی‌تر، مانند تقویت چهارچوب‌های قانونی مقابله با تهدیدات سایبری؛
- ایجاد بازدارندگی در برابر تحریکات سایبری و تقویت همکاری‌های بین‌المللی.
- ارتقای مدیریت امنیتی اطلاعات و امکانات حیاتی، ازجمله برپایی روز حفاظت از اطلاعات در سطح ملی برای افزایش آگاهی عمومی.

ازنظر ساختار حاکمیت سایبری کشور، طرح جامع شامل ایجاد نقش‌های متفاوت اما مرتبط بین سازمان‌های مربوطه بود. به‌عنوان‌مثال، سرویس اطلاعات ملی (NIS) کنترل کلی امنیت سایبری در زمان صلح و بحران را در اختیار دارد، درحالی‌که کمیسیون ارتباطات کره (KCC) بر پخش و ارتباطات نظارت دارد.

وزارت اداره امور عمومی و امنیت (MOPAS) خدمات دولتی الکترونیکی را به مردم ارائه می‌دهد. آژانس ملی محاسبات و اطلاعات (NCIA) که تحت وزارت اداره امور عمومی و امنیت فعالیت می‌کند، از فعالیت‌های امنیت سایبری دولت‌های محلی پشتیبانی می‌کند. این طرح جامع پیشنهادهای مهمی برای امنیت سایبری ملی کره جنوبی ارائه کرد، اما فاقد جزئیات اجرایی بود. توسعه سریع فضای سایبری و افزایش تهدیدات برای امنیت سایبری توجه و اقدام پیشگیرانه‌تری را می‌طلبد.

برای تثبیت استراتژی امنیت سایبری خود، دفتر امنیت ملی دولت *مون‌جائه‌این*، اولین استراتژی ملی امنیت سایبری کشور را در آوریل 2019 معرفی کرد. دولت کره جنوبی تغییر سریع محیط سایبری و چالش‌های جدید، ازجمله آسیب‌پذیری تقویت‌شده در فضای سایبری و شدت فزاینده سایبری را تشخیص داد. تهدیدات، تشدید رقابت امنیت سایبری بین دولت‌ها و افزایش آسیب به مردم به دلیل جرائم سایبری استراتژی امنیت سایبری ملی چشم‌انداز و اهداف امنیت سایبری کره جنوبی و وظایف استراتژیک افراد، شرکت‌ها و دولت را مشخص می‌کند. چشم‌انداز این استراتژی ایجاد فضای سایبری آزاد و امن برای حمایت از امنیت ملی، ارتقای شکوفایی اقتصادی و کمک به صلح بین‌المللی بود، سه هدف ارائه کرد:

1. تقویت امنیت و انعطاف‌پذیری زیرساخت‌های اصلی کشور برای فعال کردن عملیات مستمر علی‌رغم هرگونه تهدید سایبری؛

2. برای افزایش قابلیت‌های امنیتی برای بازدارندگی، شناسایی و مسدود کردن سریع تهدیدات سایبری و پاسخگویی به هر حادثه به‌سرعت؛

3. برای پرورش یک اکوسیستم منصفانه و مستقل که در آن فناوری امنیت سایبری، منابع انسانی و صنایع در سطح بین‌المللی رقابتی هستند.

این استراتژی همچنین دارای سه اصل اساسی بود:

1. ایجاد تعادل بین حقوق فردی و امنیت سایبری؛

2. انجام فعالیت‌های امنیتی بر اساس حاکمیت قانون؛

3. ایجاد یک سیستم مشارکتی با افراد، مشاغل، دولت و سایر کشورها.

علاوه‌بر این، استراتژی ملی امنیت سایبری شش وظیفه راهبردی را ارائه کرد:

1. تقویت امنیت و انعطاف‌پذیری زیرساخت اصلی ملی در برابر حملات سایبری به‌منظور تضمین ارائه مستمر خدمات حیاتی.

2. گسترش ظرفیت برای جلوگیری مؤثر از حملات سایبری و واکنش سریع به حوادث امنیتی

3. اجرای یک چارچوب امنیت سایبری آینده محور بر اساس اعتماد متقابل و همکاری بین افراد، مشاغل و دولت.

4. ایجاد یک اکوسیستم نوآورانه برای صنعت امنیت سایبری که در آن رقابت فناوری، منابع انسانی و صنایعی که برای امنیت سایبری ملی حیاتی هستند، تضمین شود.

5. برای جلب توجه مردم به اهمیت به رسمیت شناختن امنیت سایبری و متقاعد کردن آن‌ها به اجرای قوانین اساسی امنیتی، درحالی‌که دولت هم‌زمان به حقوق اساسی شهروندان احترام می‌گذارد. اجرای سیاست‌ها و تسهیل مشارکت شهروندان؛

6. تبدیل‌شدن به یک کشور پیشرو در امنیت سایبری با تقویت مشارکت‌های بین‌المللی و هدایت تشکیل قوانین بین‌المللی

برای اجرای این استراتژی، در سپتامبر 2019، نه وزارتخانه دولتی کره جنوبی، ازجمله وزارت علوم و فناوری اطلاعات و ارتباطات، سرویس اطلاعات ملی، و وزارت دفاع ملی، طرح پایه امنیت سایبری ملی را با نظرات شرکت‌ها و کارشناسان خصوصی تدوین کردند. تا سال 2022، هر سازمان دولتی قرار است دستورالعمل‌های خود را برای اجرای استراتژی و برنامه اساسی ایجاد کند. همان‌طور که در جدول 1 نشان داده‌شده است، برنامه اساسی همان چشم‌انداز، اهداف و وظایف استراتژیک ارائه‌شده در استراتژی را دارد؛ اما برنامه 100 وظیفه تفصیلی را ارائه می‌کند. طرح اساسی به‌ویژه اهمیت مقابله بهتر با ظهور دنیای بیش‌ازحد متصل 5G را برجسته می‌کند.

ارزیابی مقایسه‌ای استراتژی امنیت سایبری کره جنوبی

استراتژی و طرح اساسی امنیت سایبری ملی کره جنوبی حدود ده سال پس از استراتژی مشابه آمریکایی و پنج سال دیرتر از نسخه ژاپن (سان[۱۰۱]، 2019) منتشر شد. باوجود تأخیر در انتشار، ایجاد استراتژی و برنامه اساسی بسیار مهم بود زیرا آن‌ها اولین استراتژی جامع امنیت سایبری در سطح ملی بودند که توسط رهبری عالی کشور تولید شد. خود استراتژی تا حدودی فاقد جزئیات در اجرا بود؛ اما برنامه اساسی که متعاقباً منتشر شد، اقدامات ملموس بسیاری را برای افزایش امنیت سایبری در کره جنوبی ارائه کرد.

[101] Sohn

جدول 1: طرح اساسی امنیت سایبری ملی کره جنوبی

Primary Tasks	Strategic Tasks
تقویت امنیت شبکه‌های ملی اطلاعات و ارتباطات	افزایش ایمنی زیرساخت‌های اصلی ملی
بهبود محیط امنیت سایبری برای زیرساخت‌های حیاتی	
توسعه زیرساخت‌های امنیت سایبری نسل بعدی	
اطمینان از بازدارندگی حملات سایبری	افزایش قابلیت‌های پاسخگویی به حملات سایبری
تقویت آمادگی در برابر حملات سایبری گسترده	
تدابیر جامع و فعال متقابل برای حملات سایبری	
افزایش قابلیت پاسخگویی به جرائم سایبری	ایجاد حکمرانی بر اساس اعتماد و همکاری
سهیل سیستم همکاری نظامی عمومی و خصوصی	
ایجاد و تسهیل یک سیستم اشتراک‌گذاری اطلاعات در سراسر کشور	
تقویت مبنای قانونی برای امنیت	
گسترش سرمایه‌گذاری در امنیت سایبری	ایجاد پایه‌هایی برای رشد صنعت امنیت سایبری
تقویت رقابت نیروی کار و فناوری امنیت سایبری	
ایجاد یک محیط رشد برای شرکت‌های امنیت سایبری	
ایجاد یک اصل رقابت منصفانه در بازار امنیت سایبری	
افزایش آگاهی در مورد امنیت سایبری و تقویت عملکرد امنیت سایبری	تقویت فرهنگ امنیت سایبری
تعادل بین حقوق اساسی و امنیت سایبری	
غنی‌سازی سیستم‌های همکاری دوجانبه و چندجانبه	رهبری همکاری‌های بین‌المللی در امنیت سایبری
رهبری ایمن(secure) در همکاری بین‌المللی	

باوجود این اهمیت، استراتژی و برنامه اساسی دارای نقاط ضعف زیر است:

1) این دو سند فاقد دستورالعمل‌های عملی و ملموس برای نحوه استفاده از دفتر امنیت ملی (دفتر ریاست جمهوری) به‌عنوان برج کنترل در موارد اضطراری امنیت سایبری هستند. دولت کره جنوبی با دسته‌بندی تهدیدات سایبری به‌عنوان خصوصی، عمومی و دفاعی به آن‌ها پاسخ می‌دهد. سرویس اطلاعات ملی به تهدیدات سایبری برای بخش‌های دولتی و عمومی رسیدگی می‌کند، درحالی‌که وزارت

علوم و فناوری اطلاعات و ارتباطات و وزارت دفاع ملی به ترتیب مسئولیت تهدیدات سایبری برای بخش‌های خصوصی و دفاعی را بر عهده‌دارند.

بااین‌حال، این سیستم فعلی نمی‌تواند مؤثر باشد، زیرا حملات سایبری که در یک بخش رخ می‌دهد می‌تواند به‌راحتی به بخش‌های دیگر منتقل شود. اداره امنیت ملی به‌عنوان یک برج کنترل در شرایط اضطراری سایبری، که کارکنان و بودجه بسیار محدودی دارد، در ایجاد و اجرای اقدامات سیاستی فراتر از هماهنگی سازمان‌های مختلف دولتی با مشکل مواجه خواهد شد. بر این اساس، لازم است دولت ROK یک سازمان جداگانه مانند مرکز ملی امنیت سایبری زیر نظر رئیس دفتر امنیت ملی ایجاد کند که دارای بودجه و کارکنان کافی باشد. ایجاد یک کمیته ملی امنیت سایبری، که در آن کارکنان خصوصی، دولتی و نظامی به‌طور مشترک تهدیدات سایبری را رصد کرده و به آن‌ها پاسخ می‌دهند، مزایای قابل‌توجهی نیز به همراه خواهد داشت.

2) دوم اینکه پایه قانونی کمی برای دولت کره جنوبی وجود دارد که به‌طور مداوم استراتژی و برنامه اساسی امنیت ملی جدید سایبری را بدون توجه به تغییرات یک دولت حاکم دنبال کند. ژاپن قانون اساسی امنیت سایبری را در نوامبر 2014 به تصویب رساند که اصول اساسی استراتژی امنیت سایبری و مسئولیت‌های دولت‌های مرکزی و محلی و سایر سازمان‌های عمومی را مشخص می‌کرد. بنابراین، این قانون نقش کلیدی در زمینه‌سازی استراتژی امنیت سایبری آن داشت. بخش اصلی این قانون، ایجاد مرکز ملی آمادگی و استراتژی در حوادث برای امنیت سایبری (NISC) بود که به‌عنوان یک برج کنترل امنیت سایبری کار می‌کند. در دسامبر 2015، ایالات‌متحده قانون امنیت سایبری را تصویب کرد که بخش‌های خصوصی را موظف می‌کرد تا در صورت نیاز برای امنیت سایبری، حجم عظیمی از اطلاعات شخصی خود را با آژانس‌های فدرال ایالات‌متحده به اشتراک بگذارند. این قانون نگرانی‌های مربوط به حقوق حریم خصوصی ناشی از اشتراک‌گذاری اطلاعات تهدیدات سایبری را برطرف کرد. بنابراین، تصویب یک قانون جامع امنیت سایبری برای اجرای موفقیت‌آمیز استراتژی ملی امنیت سایبری و برنامه اساسی برای کره جنوبی ضروری خواهد بود.

3) استراتژی و برنامه اساسی این واقعیت آشکار را نشان نمی‌دهد که کره شمالی تهدید اولیه سایبری برای جامعه کره جنوبی است. به نظر می‌رسد دولت فعلی *مون‌جائه‌این* محتاط است و نمی‌خواهد کره شمالی را بی‌دلیل با مسائل امنیت سایبری آزار دهد؛ زیرا دولت "مون" می‌خواهد چالش هسته‌ای/موشکی کره شمالی را به‌طور مسالمت‌آمیز حل کند و روابط بین کره‌ای را بهبود بخشد. با توجه به شرایط امنیتی پیچیده و ناپایدار در شبه‌جزیره کره، این رویکرد ممکن است منطقی باشد. بااین‌حال، چنین استراتژی منفعلانه‌ای می‌تواند به‌طور ناخواسته به کره شمالی این آزادی را بدهد که حملات سایبری خود را به جامعه کره جنوبی ادامه دهد برای به حداکثر رساندن قدرت بازدارندگی سایبری، لازم است دولت ROK در استراتژی رسمی امنیت سایبری خود، اسامی ایالت‌ها و گروه‌های هکری تحت حمایت دولت را که حملات سایبری مخربی علیه جامعه کره جنوبی انجام می دهند، به وضوح مشخص کند. خطرات خطوط قرمز یک واقعیت شناخته‌شده است: «بیش‌ازحد مشخص است، و حریف دقیقاً در مقابل خط فشار خواهد آورد. همان‌طور که فلورنو و سولمیر اشاره کردند، بسیار مبهم است، و حریف در مورد اینکه چه رفتاری منجر به پاسخ می‌شود، مطمئن نیست.» بااین‌وجود، مهم خواهد بود دولت کره جنوبی به کره شمالی هشدار واضحی در مورد هزینه‌های حملات سایبری بدهد.

اظهارات پایانی با پیامدهای سیاستی

کره جنوبی با چالش‌های مهمی در حوزه سایبری مواجه است، زیرا این کشور با پیچیدگی‌های ژئوپلیتیکی ناشی از تهدیدات هسته‌ای/موشکی کره شمالی و رقابت قدرت‌های بزرگ بین ایالات‌متحده و چین دست‌وپنجه نرم می‌کند. همان‌طور که قبلاً اشاره شد، به دلیل ماهیت ذاتاً آسیب‌پذیر امنیت سایبری کره جنوبی، کره شمالی یک تهدید سایبری جدی برای آن ایجاد کرده است.

علاوه‌بر این، کره جنوبی در بین رقابت تسلیحاتی سایبری آمریکا و چین قرارگرفته است. فضای مجازی به بخشی جدایی‌ناپذیر از زندگی مالی، اجتماعی، دولتی و سیاسی کره جنوبی تبدیل‌شده است. بنابراین، برای دولت کره جنوبی بسیار مهم است که قابلیت‌های امنیت سایبری خود را افزایش دهد، همان‌طور که قابلیت‌های ژئواستراتژیک و اقتصادی برای احساس تاریخی امنیت ملی آن ضروری است.

همان‌طور که در تحلیل بالا مشاهده می‌شود، کره جنوبی به‌جای تأکید بر حاکمیت سایبری، تأکید زیادی بر آزادی، باز بودن و امنیت در حوزه سایبری دارد، مشابه ایالات‌متحده، ژاپن و سایر کشورهای غربی. برای تقویت این ارزش‌ها در فضای سایبری و محافظت بهتر از بخش‌های دولتی و خصوصی در برابر حملات سایبری، کره جنوبی ابتدا باید یک آژانس ویژه ایجاد کند که بتواند به‌طور مؤثر به‌عنوان یک برج کنترل امنیت سایبری کار کند. همان‌طور که قبلاً ذکر شد، چنین مؤسسه‌ای باید دارای کارکنان کافی، بودجه متناسب و اختیارات قوی برای تدبیر استراتژی امنیت سایبری کشور باشد. همچنین باید نقش هماهنگی سایر سازمان‌های دولتی و خصوصی را نیز داشته باشد. همچنین برای دولت کره جنوبی ضروری است که یک چارچوب قانونی محکم برای حمایت از استراتژی امنیت سایبری ایجاد کند.

علاوه‌بر این، کره جنوبی باید تلاش کند تا قدرت بازدارندگی خود را در برابر تهدیدات سایبری کره شمالی با گنجاندن فعالیت‌های سایبری مخرب کره شمالی در استراتژی امنیت سایبری این کشور و ارسال سیگنال‌های هشداردهنده واضح درباره پیامدهای حملات سایبری بی‌امان به کره شمالی افزایش دهد. علاوه‌بر این اقدامات، ازآنجایی‌که ایجاد یک سپر امنیت سایبری مؤثر برای یک کشور غیرممکن است، دولت کره باید تمام تلاش خود را برای ارتقای همکاری بین‌المللی با سایر کشورهای هم‌فکر، مانند پنج چشم به‌علاوه سه (ایالات‌متحده آمریکا) به کار گیرد (کانادا، انگلستان، استرالیا و نیوزلند و همچنین ژاپن، آلمان و فرانسه).

برای مطالعه بیشتر

چین

- Austin, G. (2014). Cyber Policy in China (China Today). Cambridge: Polity Press.
- Austin, G. (2018). Cybersecurity in China. Cham: Springer. https://thediplomat.com/tag/chinacybersecurity/
- Wagner, D. (2019, May 13). “What China’s Cybersecurity Law Says about the Future,” International
- Policy Digest. https://intpolicydigest.org/2019/05/13/what-china-s-cybersecurity-law-says-aboutthe-
- future/
- Yang, Z. (2019, October 30). “China Cybersecurity,” The Diplomat. https://thediplomat.com/tag/china-cybersecurity/

روسیه

- Compendium of Regulatory Legal Acts of the Russian Federation and the Strategy Planning Documents in the Sphere of Information Security, The Russian Federation contributions to the UN and other international organizations, Bilateral Agreements and Joint Declarations at the Highest Level and at Governmental Level with the Participation of the Russian Federation.
- Demidov, O. (2012). “International regulation of information security and Russia’s national interests.« Security Index: A Russian Journal on International Security, 18(4). 10.1080/19934270.2012.714597
- Krutskikh, A. & Streltsov, A. (2014). “International law and the problem of international information security.« International Affairs 6, 64–76.
- National Association of International Information Security (НАМИБ). “International information security legal acts and fundamental documents for Russia translated into English.« http://namib. online/wp-content/uploads/2019/03/МИБ_английская-версия.pdf
- Stadnik, I. (2019). White paper Sovereign RUnet: What Does it Mean? Internet governance project, Georgia Institute of Technology. www.internetgovernance.org/research/sovereign-runet-whatdoes-it-mean/

کره‌جنوبی

- Butcher, L. (n.d.). “Defending Against Cyber Attacks in South Korea,” Korea Economic Institute, Seoul, South Korea. http://keia.org/defending-against-cyber-attacks-south-korea

- ENISA. (2013, December 30). “National Cyber Security Strategy of South Korea.” www.enisa.europa. eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactivemap/strategies/national-cyber-security-strategy-of-south-korea
- Ikeda, S. (2019, January 27). “Lessons for Organizations from the South Korea Defense Agency Cyber Attack,” CPO Magazine. www.cpomagazine.com/cyber-security/lessons-for-organizations-fromthe-south-korea-defense-agency-cyber-attack/
- Kang, T. J. (2019, March 8). “South Korea Cybersecurity,” The Diplomat. https://thediplomat.com/tag/ south-korea-cybersecurity/
- National Security Office. (n.d.). “National Cyber Security Strategy.” www.krcert.or.kr/filedownload. do?attach_file_seq=2162&attach_file_id=EpF2162.pdf

منابع

چین

- Austin, G. (2016, September 8). “Mapping and Evaluating China’s Cyber Power,” Lau China Institute, King’s College London. www.unsw.adfa.edu.au/australian-centre-for-cyber -security/sites/accs/files/uploads/Greg_Austin_Chinapercent27s_Cyber_Power_Policy_Papers-Issue-2.pdf
- BBC News. (2015, December 28). “China Passes Controversial New Anti-Terror Laws.” www.bbc.com/news/world-asia-china-35188137
- Bennett, C. (2015, May 8). “China Wants Cyber ‘Sovereignty’ in Latest National Security Law,” Thehill. http://thehill.com/policy/cybersecurity/241420-china-wants-cyber-sovereignty-in-latestnational-security-law
- Blanchard, B. (2015, December 28). “China Passes Controversial Counter-Terrorism Law,” Reuters.www.reuters.com/article/us-china-security/china-passes-controversial-counter-terrorism-lawidUSKBN0UA07220151228
- Chan, S. (2018, January 15). Cybersecurity Under Xi Jinping. Los Angeles, CA: Center for the Digitalfuture. www.digitalcenter.org/wp-content/uploads/2018/01/Cybersecurity-under-Xi-Jinping-analysis.pdf
- Chang, A. (2014). Warring State China’s Cybersecurity Strategy. Washington, DC: Center for a New American Security.
- China Daily. (2010, June 9). “The Internet in China White Paper.” www.chinadaily.com.cn/cndy/2010-06/09/content_9952206.htm
- China Daily. (2015, December 21). “Infographic: Achievements of the 2nd WIC.” www.chinadaily.com.cn/business/tech/2015-12/21/content_22761073.htm
- China Daily. (2017, July 20). “China’s Digital Economy Surges 18.9 per cent, Drives Growth.” www.chinadaily.com.cn/business/2017-07/20/content_30179729.htm

- Clapper, J. R. (2013, March 12). Statement for the Record Worldwide Threat Assessment of the US IntelligenceCommunity. Washington, DC: US Office of the Director of National Intelligence. www.dni.gov/files/documents/Intelligence per cent20Reports/2013 per cent20ATA per cent20SFR per cent20for per cent20SSCI per cent2012 per cent20Mar per cent202013.pdf
- Clarke, R. A. & Knake, R. K. (2010). Cyber War: The Next Threat to National Security and What to Do About It. New York: Harper Collins.
- Costello, J. (2016, February 8). "The Strategic Support Force: China's Information Warfare Service,"Jamestown Foundation. https://jamestown.org/program/the-strategic-support-force-chinas-information-warfare-service/
- Creemers, R. (2017, January 10). "Is China's Cybersecurity Law Visionary?" China-US Focus. http://cn.chinausfocus.com/peace-security/20170110/11856.html#eng
- CSIS. (n.d.). "China Cyber Outlook." www.csis.org/programs/technology-policy-program/technology-and-innovation/cybersecurity-and-governance/china
- Cyberspace Administration of China. (2014a, February 25). "Xi Jinping tan guanyu jiakuai wanshanhulianwang guanli lingdao tizhi" ("Xi Jinping discussed the hastening of the improvement of theinternet management and leadership system"). www.cac.gov.cn/2014-02/25/c_133142284.htm
- Cyberspace Administration of China. (2016, December 27). "Guojia wanglu kongjian anquan zhanlue"("National Cyberspace Security Strategy"). www.cac.gov.cn/2016-12/27/c_1120195926.htm
- First Post. (2016, March 18). "China Launches First Cybersecurity Organisation." www.firstpost.com/tech/news-analysis/china-launches-first-cybersecurity-organisation-3679171.html
- FlorCruz, J. A. & Sue, L. (2014, April 24). "From Snail Mail to 4G, China Celebrates 20 Years of Internet Connectivity," CNN. https://edition.cnn.com/2014/04/23/world/asia/china-internet-20th-anniversary/index.html
- Gechlik, M. (2017). Appropriate Norms of State Behavior in Cyberspace: Governance in China and Opportunities for US Businesses. Washington, DC: Hoover Institution.
- Goldkorn, J. (2012, August 2) "The Internet," The China Story. www.thechina story.org/keyword/theinternet/;https://www.firstpost.com/tech/news-analysis/china-launches-first-cybersecurity-organisation-3679171.html
- Inkster, N. (2016). China's Cyber Power. London: The International Institute for Strategic Studies.
- Internet Live States. (2020). "China Internet Users." www.internetlivestats.com/internet-users/china/
- Kowalewski, A. (2017, October 27). "China's Evolving Cybersecurity Strategy," Georgetown Security Studies Review. http://georgetownsecuritystudiesreview.org/2017/10/27/chinas-evolving-cybersecurity-strategy/
- Lampton, D. M. (2014). Following the Leader: Ruling China, from Deng Xiaoping to Xi Jinping. Berkeley,CA: University of California Press.

- Lindsay, J. R. (2014/2015). “The Impact of China on Cybersecurity,” International Security, 39(3): 7–40.
- Livingston, S. D. (2015, April 22). “Will China’s New Anti-Terrorism Law Mean the End of Privacy?”www.chinafile.com/reporting-opinion/viewpoint/will-chinas-new-anti-terrorism-law-mean-endprivacy
- Ministry of Industry and Information Technology of the PRC. (2016, February 14). “Provisions on the Administration of Online Publishing Services.” www.miit.gov.cn/n1146295/n1146557/n1146619/c4639081/content.html
- Mozur, P. (2016, November 8). “China’s Internet Controls Will Get Stricter, to Dismay of Foreign Business,” The New York Times. www.nytimes.com/2016/11/08/business/international/china -cyber-security-regulations.html
- National Internet Emergency Center. (2017). “2016 Nian Zhongguo Hulianwang Wanglu Anquan Taishi Zongshu.”
- National People’s Congress. (2015, July 7). “National Security Law of the People’s Republic of China.”www.npc.gov.cn/npc/xinwen/2015-07/07/content_1941161.htm
- Nye, J. (2010, May). “Cyber Power,” Harvard College. http://belfercenter.ksg. harvard.edu/files/cyberpower.pdf
- O’ Brien, R. (2016, May 25). What to Make of the Newly Established Cyber Security Association of China.Washington, DC: Center for Strategic and International Studies. www.csis.org/analysis/what-makenewly-established-cybersecurity-association-china
- Panda, A. (2015, July 1). “The Truth about China’s New National Security Law,” The Diplomat. https://thediplomat.com/2015/07/the-truth-about-chinas-new-national-security-law/
- Paulson, H. M. (2015). Dealing with China: An Insider Unmasks the New Economic Superpower. New York:Hachette Book Group.
- PC World. (2004, May 17). “China Celebrates 10 Years of Being Connected to the Internet.” www.pcworld.idg.com.au/article/128099/china_celebrates_10_years_being_connected_internet/
- PEN America. (2016), “Darkened Screen: Constraints on Foreign Journalists in China.” https://pen.org/sites/default/files/PEN_foreign_journalists_report_FINAL_online per cent5B1per cent5D.pdf
- People’s Daily. (2016, June 23). “Guoqu yinian woguo wangmin yin wanglu anquan shijian zaocheng jingji sunshi da 915 yi yuan” (“In the Past Year, Chinese Netizens Suffered an Economic Loss of 915 Million RMB Due to Cybersecurity Incidents”). http://sn.people.com.cn/n2/2016/0623/c190199-28556169.html
- Perlez, J. & Mozur, P. (2016, June 29). “Lu Wei, China’s Internet Czar, Will Step Down from Post, The New York Times. www.nytimes.com/2016/06/30/business/international/china-internet-lu-wei.html?_ga=2.36365474.346945526.1525389466-1633828418.1483632849
- Raud, M. (2016, August). China and Cyber: Attitudes, Strategies, Organisation. Tallinn, Estonia: NATO CCDCOE.

https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016_FINAL.pdf

- Rui, Z. (2015, December 17). “China Headlines: Xi Slams’ Double Standards, Advocates Shared Future in Cyberspace,” CCTV. http://english.cntv.cn/2015/12/17/ARTI1450334752126739.shtml
- Singh, A. P. (2016, March 29). China’s First Anti-Terrorism Law: An Analysis. New Delhi, India: Institute for Defense Studies and Analyses. www.idsa.in/idsacomments/china-first-anti-terrorism -law_apsingh_290316
- Statista. (2020). “Number of Internet Users in China from 2017 to 2023.” www.statista.com/statistics/278417/number-of-internet-users-in-china/
- Swartz, D. (2011, April 18). “Jasmine in the Middle Kingdom: Autopsy of China’s (Failed) Revolution,”China Digital Times. https://chinadigitaltimes.net/2011/04/jasmine-in-the-middle-kingdom-autopsy-of-chinas-failed-revolution/
- The Economic Times. (2014, November 19). “Chinese President Xi Jinping Calls for International Cooperation on Cyberspace Security.” http://economictimes.indiatimes.com/news/international/world-news/chinese-president-xi-jinping-calls-for-international-cooperation-on-cyberspace-security/articleshow/45205445.cms
- The Economic Times. (2018, January 31). “China’s Online Population Climbs to 772 Million.” https://economictimes.indiatimes.com/news/international/world-news/chinas-online-population-climbsto-772-million/articleshow/62726168.cms?from=mdr
- The State Council of the People’s Republic of China. (2014, August 25). “Ministry of Public Security.” english.www.gov.cn/state_council/2014/09/09/content_281474986284154.htm
- The US Chamber of Commerce. (2016, September 1). “Preventing Deglobalization: An Economic and Security Argument for Free Trade and Investment in ICT.” www.uschamber.com/sites/default/files/documents/files/preventing_deglobalization_1.pdf
- Thomas, T. L. (2009). “Nation-State Cyber Strategies: Examples from China and Russia,” in F. D. Kramer, S. H. Starr & L. K. Wentz (eds.), Cyberpower and National Security (pp. 465–466). Lincoln: University of Nebraska Press.
- Xinhua Net. (2016, August 6). “Xinjiang Issues China’s First Local Counterterrorism Law.” www.xinhuanet.com/english/2016-08/06/c_135567634.htm
- Xu, B. & Albert, E. (2017, February 17). Media Censorship in China. Washington, DC: Council on Foreign Relations. www.cfr.org/backgrounder/media-censorship-china
- Yuxiao, L. & Lu, X. (2015). “China’s Cybersecurity Situation and the Potential for International Cooperation,” in J. R. Lindsay, T. M. Chueng & D. S. Reveron (eds.), China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain (pp. 225–241). New York: Oxford University Press.
- Zhou, Z. (2015, December). “China’s Draft Cybersecurity Law,” China Brief, 15(24). https://jamestown.org/program/chinas-draft-cybersecurity-law/.

- Zhu, H. (2016, November 30). “China’s New ‘Cybersecurity’ Rules Look Like Cyberprotectionism Instead,” The Diplomat. http://thediplomat.com/2016/11/chinas-new-cybersecurity-rules-look-likecyberprotectionism-instead/296

روسیه

- APC. (2018). “UN General Assembly adopts record number of resolutions on internet governance and policy: Mixed outcomes for human rights online.« www.apc.org/en/news/un-general-assemblyadopts-record-number-resolutions-internet-governance-and-policy-mixed
- Consultant.ro. (2017, 26, July). “Federal law dated, 26. 07.2017No187-FZ.« www.consultant.ru/cons/cgi/ online.cgi?req=doc&base=LAW&n=220885&fld=134&dst=1000000001,0&rnd=0.2477406265980837#07294351284912781 [in Russian].
- Council.gov.ru. (2013). “Концепция стратегии кибербезопасности Российской Федерации” [“The Concept of the Russian Federation’s Cyber Secuity Strategy]. http://council.gov.ru/media/files/ 41d4b3dfbdb25cea8a73.pdf [In Russian].
- Cuba’s Representative Office Abroad. (2017). “71 UNGA: Cuba at the final session of Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security.« http://misiones.minrex.gob.cu/en/un/statements/71-unga-cubafinal-session-group-governmental-experts-developments-field-information
- “Doctrine on Information Security.« (2000). Part I, §1.
- “Doctrine on Information Security.« (2000). Part II, §7.
- “Doctrine on Information Security.« (2000). Part III, §8.
- “Doctrine on Information Security.« (2016). Part I.
- “Doctrine on Information Security.« (2016). Part II, §8.
- “Doctrine on Information Security.« (2016). Part III.
- ECFR. (2017). “The UN GGE is dead: Time to fall forward.« www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance
- GOSSOPKA – the State system of detection, prevention and elimination of consequences of computer attacks on information resources, operated by FSB.
- Коммерса́нтъ. (2013, November 29). “Koncepciya kiberbezopasnosti razoshlas’s gosudarstvennoi
- strategiei Predlozheniya senatorov nravyatsya poka tol’ko obshchestvennikam i biznesu [Концепция
- кибербезопасности разошлась с государственной стратегией. Предложения сенаторов нравятся
- пока только общественникам и бизнесу].« Kommersant. www.kommersant.ru/doc/2355154

- Международная Жизнь. (2017, December). “Cyber stability: Approaches, perspectives and challenges,”
- International conference, Moscow, December 2017.
- Meduza. (2016, June 22). “Irina Yarovaya’s ‘anti-terrorist’ war on civil rights.« https://meduza.io/en/feature/2016/06/22/irina-yarovaya-s-anti-terrorist-war-on-civil-rights
- Министерство иностранных дел Российской Федерации. (2011, September 22). “Convention on international information security.« www.mid.ru/en/web/guest/mezdunarodnaa-informacionnaabezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/191666
- Министерство иностранных дел Российской Федерации. (2018a, September 28). “Foreign Minister Sergey Lavrov’s remarks at the 73rd session of the UN General Assembly, New York, September 28, 2018.« www.mid.ru/en/press_service/minister_speeches/-/asset_publisher/7OvQR5KJWVmR/content/id/3359296
- Mueller, M. (2017). Will the Internet Fragment? Sovereignty, Globalization and Cyberspace. London: Polity.
- Namib. online. (2013, July 24). “Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года” [“Basic principles for State Policy of the Russian Federation in the field of International Information Security to 2020”]. Art. 11(б). http://namib.online/wp-content/uploads/2019/03/2013-07-24_Основы-гос политики-РФ-области-МИБ-на-период-до-2020-года.pdf [in Russian].
- Официальный интернет-портал правовой информации. (2018b, September 6). “Приказ Федеральной службы безопасности Россий ской Федерации от 06.09.2018 No. 52107” [“Order of the Federal Security Service dated 09.06.2018 No. 52107”] http://publication.pravo.gov.ru/Docu ment/View/0001201809100003?index=0 [in Russian].
- Официальный интернет-портал правовой информации. (2019, May 1). “The Federal Law dated 01.05.2019No. 90-FZ.« http://publication.pravo.gov.ru/Document/View/0001201905010025?fbclid=IwAR3POFABIeaD21PCGKdNDOMm-tDwZ-gU_uxyONSLw520E0cUT6x47m_sLjk [in Russian].
- Parker, D. B. (2002). “Toward a New Framework for Information Security,« In S. Bosworth, M. E. Kabay & E. Whyne (eds.), The Computer Security Handbook (4th ed.) (Chapter 3). New York: Wiley.
- Stadnik, I. (2019). “A closer look at the ‘Sovereign Runet’ law,« CircleID. www.circleid.com/posts/ 20190518_a_closer_look_at_the_sovereign_runet_law/
- The Federal Law 97-FZ. (2014a).
- The Federal Law 242-FZ. (2014b)
- UNGA. (1999, January 4). “Developments in the field of information and telecommunications in the context of international security.« UNGA A/RES/53/70 https://undocs.org/A/RES/53/70

- UNGA. (2015a, January 15). “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.« UNGA A/69/723. https://undocs.org/A/69/723
- UNGA. (2015b, July 22). “Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security.« UNGA A/70/174 https://undocs.org/A/70/174
- UNGA. (2017, October 16). “Letter dated 11 October 2017 from the permanent representative of the Russian federation to the United Nations addressed to the Secretary-General.« UNGA A/C.3/72/ 12. https://undocs.org/A/C.3/72/12
- UNGA. (2018a. October 29). “Developments in the field of information and telecommunications in the context of international security.« UNGA A/C.1/73/L.27/Rev.1 https://undocs.org/A/C.1/73/ L.27/Rev.1
- UNGA. (2018b). Developments in the field of information and telecommunications in the context of international security. UNGA A/RES/73/27. www.un.org/en/ga/search/view_doc.asp?symbol=A/ RES/73/27
- UNIDIR. (2019, June 6). “2019 cyber stability conference,« United Nations HQ, New York

کره‌جنوبی

- BBC News. (2017, December 19). “Bitcoin Exchange YouBit Shuts after Second Hack Attack.” www.bbc.com/news/technology-42409815
- BBC News. (2018, June 20). “Bithumb: Hackers Rob Crypto-exchange of $32m.” www.bbc.com/ news/technology-44547250
- BBC News. (2018, June 20). “Bithumb: Hackers Rob Crypto-exchange of $32m.” www.bbc.com/ news/technology-44547250
- Cha, J. (2019). “US-China Cyber Military Power Rivalry and the Rise of North Korean Threat: Implications for South Korean Cybersecurity,” in S. Kim (ed.), National Cybersecurity Strategy 2.0 (pp. 218–264). Seoul: Sahoepyungron Academy, Seoul. [in Korean].
- Chanlett-Avery, E., Rosen, L. W., Rollins, J. W. & Theohary, C. A. (2017, August 3). “North Korean Cyber Capabilities: In Brief,” Congressional Research Service, 7-5700. https://fas.org/sgp/crs/row/R44912.pdf
- Chivvis, C. S. & Dion-Schwarz, C. (2017, March 30). “Why It’s so Hard to Stop a Cyberattack—and Even Harder to Fight Back,” RAND Commentary. www.rand.org/blog/2017/03/why-its-so-hardto-stop-a-cyberattack-and-even-harder.html
- Electronic News. (2018, February 6). “Ransomware Attacks Exceeded 10,000 Cases over the Last Three Years.” http://m.etnews.com/20180206000358
- Flournoy, M. & Sulmeyer, M. (2018, September/October). “Battlefield Internet: A Plan for Securing Cyberspace,” Foreign Affairs. www.foreignaffairs.com/articles/world/2018-08-14/battlefield-internet

- Hong, S. (2019, September 9). “What Should Be the Control Tower of National Cybersecurity? National Security Office or National Intelligence Service,” Popcorn News. [in Korean] http://m.popcornnews.net/22550
- Hwang, J. (2017). “North Korea’s Cyber Security Strategy and the Korean Peninsula,” East West Studies, 29(1): 139–159. [in Korean].
- Kim, C. W. & Polito, C. (2019). “The Evolution of North Korean Cyber Threats,” Issue brief, The Asan Institute for Policy Studies, Seoul, South Korea.
- Kim, S. (2017). “Cybersecurity Strategies of Major Powers in World Politics: From the Comparative
- Perspective of National Strategies,” International and Regional Studies, 26(3): 67–108. [in Korean].
- Kong, J. Y., Lim, J. I. & Kim, K. G. (2019). “The All-Purpose Sword: North Korea’s Cyber Operations and Strategies,” 11th International Conference on Cyber Conflict: Silent Battle. https://ccdcoe.org/uploads/2019/06/Art_08_The-All-Purpose-Sword.pdf
- Ku, Y. (2019). “Privatized Foreign Policy? Explaining the Park Geun-hye Administration’s DecisionMaking Process,” Korea Journal, 59(1): 106–134.
- Lawson, S. & Middleton, M. K. (2019, March 4). “Cyber Pearl Harbor: Analogy, Fear, and the Framing of Cyber Security Threats in the United States, 1991–2016,” First Monday, 24(3). https://firstmonday.org/ojs/index.php/fm/article/view/9623/7736
- McCurry, J. (2014, December 23). “South Korean Nuclear Operator Hacked amid Cyber-attack Fears,” The Guardian. www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyberattack-hack
- Meyers, A. (2017, November 13). “North Korean Cyber Operations: Weapons of Mass Disruption,” 38North. www.38north.org/2017/11/ameyers111317/
- National Security Office. (2019, April). “National Cybersecurity Strategy,” https://www.itu.int/en/ITUD/Cybersecurity/Documents/National_Strategies_Repository/National%20Cybersecurity%20Strategy_South%20Korea.pdf
- Nau, H. (2019). Perspectives on International Relations: Power, Institutions, and Ideas. Washington, DC: CQ Press.
- Park, C. (2019, April 21). “Superficial National Cybersecurity Strategy,” Digital Times. [in Korean]www.dt.co.kr/contents.html?article_no=2019042202102369061001
- Potter, R. (2019, August 5). “Toward a Better Understanding of North Korea’s Cyber Operations,” 38North. www.38north.org/2019/08/rpotter080519/
- Reuters. (2017, May 20). “Exclusive: North Korea’s Unit 180, the Cyber Warfare Cell that Worries the West.” www.reuters.com/article/us-cyber-northkorea-exclusive/exclusive-north-koreas-unit-180-the-cyber-warfare-cell-that-worries-the-west-idUSKCN18H020
- Reuters. (2018, June 10). “Bitcoin Tumbles as Hackers Hit South Korean Exchange Conrail.” www.reuters.com/article/us-markets-bitcoin-korea/bitcoin-tumbles-as-hackers-hit-south-korean-exchangecoinrail-idUSKBN1J703I
- Sanger, D. E., Kirckpatrick, D. D. & Perlroth, N. (2017, October 15). “The World once Laughed at North Korean Cyberpower. No More,” The New York Times. www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html

- Sohn, Y. (2019, April 18). “The Blue House Security Office Published a Report 10 Years Later than the U.S. And 5 Years Later than Japan,” Joongang Ilbo. [in Korean] https://news.joins.com/article/23444687
- The National Cyber Security Council. (2011, August 2). “National Cyber Security Masterplan.” www.sicurezzacibernetica.it/db/%5BSouth%20Korea%5D%20National%20Cyber%20Security%20Strategy%20-%202011%20-%20EN.pdf
- The South Korean Government. (2019, September). “National Cybersecurity Basic Plan.” [in Korean]msit.go.kr/cms/www/m_con/news/report/__icsFiles/afieldfile/2019/09/03/(%EC%B0%B8%EA%B3%A0)%20%EA%B5%AD%EA%B0%80%20%EC%82%AC%EC%9D%B4%EB%B2%84%EC%95%88%EB%B3%B4%20%EA%B8%B0%EB%B3%B8%EA%B3%84%ED%9A%8D.pdf
- U.S. Department of the Treasury. (2019, September 13). “Treasury Sanctions North Korean StateSponsored Malicious Cyber Groups.” https://home.treasury.gov/index.php/news/press-releases/sm774
- The White House. (2018, September). “National Cyber Strategy of the United States of America.”www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
- Yonhap News. (2019, September 3). “Seoul to Implement Comprehensive Cyber Security Strategy by 2022.” https://en.yna.co.kr/view/AEN20190903002800320