ریاست جمهوری
مرکز همکاری‌های تحول و پیشرفت

ارزیابی کلی توانمندی‌های سایبری و قدرت ملی


بسم الله الرحمن الرحیم

پیشگفتار

در فوریه سال ۲۰۱۹، مؤسسه بین‌المللی مطالعات راهبردی (IISS)[1] در یکی از مقالات خود در مجله سروایوِل[2] از تهیه روشی برای ارزیابی توانمندی‌های سایبری کشورها و تاثیر این توانمندی‌ها بر قدرت ملی آن‌ها خبر داد[3]. گزارش حاضر نیز مبتنی بر این روش است که به ارزیابی ۱۴ کشور منتخب و رژیم صهیونیستی می‌پردازد و جمع‌بندی و استنباطی کلی از وضعیت توان سایبری آن‌ها ارائه می‌کند.

این گزارش با معرفی توانمندی‌های سایبری که بیشترین تاثیرگذاری را در قدرت ملی دارند، می‌تواند به تقویت تصمیم‌گیری ملی کمک کند. به‌عبارت دیگر، اطلاعات مندرج در این گزارش ابزاری مفید برای دولت‌ها و شرکت‌های بزرگ در محاسبه خطر راهبردی و تصمیم‌گیری درباره سرمایه‌گذاری راهبردی خواهد بود.

اگرچه سایر سازمان‌ها نیز در این حوزه از روش‌های شاخص‌محور[4] استفاده کرده‌اند که عمدتاً حول امنیت سایبری هستند، اما روش ابداعی این موسسه دامنه گسترده‌تری دارد. زیرا این روش در اصل کیفی است و زیست‌بوم سایبری وسیع‌تری را برای کشورهای موردمطالعه و رژیم صهیونیستی بررسی می‌کند که شامل برهم‌کنش زیست‌بوم سایبری با امنیت بین‌المللی، رقابت اقتصادی و امور نظامی می‌شود.

۱۵ مطالعه موردی این گزارش براساس تصویری کلی و البته مقطعی از توان سایبری کشورها و رژیم صهیونیستی انجام شده‌اند. چرا که بی‌تردید شرایط ملی هر کشوری

1. International Institute for Strategic Studies
2. Survival

۳. رجوع شود به:
Marcus Willett, 'Assessing Cyber Power', Survival: Global Politics and Strategy, vol. 61, no. 1, February -March 2019, pp. 85-90.

۴. به‌عنوان نمونه می‌توان به «شاخص جهانی امنیت سایبری» اتحادیه بین‌المللی مخابرات، «شاخص آمادگی سایبری ۲» موسسه پوتوماک و «شاخص قدرت سایبری ملی ۲۰۲۰» دانشکده هاروارد کندی اشاره کرد.

تغییر خواهد کرد و راهبردها و سرمایه‌گذاری‌های آن‌ها در زمینه سایبری تحت‌تاثیر چالش‌های بسیاری مانند همه‌گیری کوید-۱۹ قرار خواهند گرفت. با این وجود، بخش عمده‌ای از سیاست‌ها و الگوهای مربوط به توانمندی‌های سایبری در این کشورها به احتمال زیاد پایدار خواهد ماند.

در مطالعات مذکور تقابل‌های شدید بین‌المللی در فضای سایبری مدنظر بوده‌است. به‌عنوان نمونه، سال ۲۰۱۵ چین در راهبرد نظامی جدید خود این نکته را متذکر شد: «فضای ماورای جو و فضای سایبری به حوزه‌های راهبردی جدیدی برای رقابت بین دولت‌ها تبدیل شده‌اند»[۱]. سال ۲۰۱۶ نیز ایالات متحده دولت روسیه و شخص ولادیمیر پوتین رئیس‌جمهور روسیه را متهم به حمله‌های اطلاعاتی پی‌درپی به انتخابات ریاست‌جمهوری آمریکا کرد[۲]. در ماه مِی سال ۲۰۱۹ هم دونالد ترامپ رئیس‌جمهور وقت ایالات متحده اعلام کرد اگر چین به اقدامات مخرب خود در فضای سایبری ادامه دهد، ایالات متحده وارد جنگ فناوری با این کشور خواهد شد[۳]. در مارس سال ۲۰۲۰ نیز ترامپ وضعیت اضطراری ملی در فضای سایبری اعلام کرد[۴] و این در پنج سال گذشته

۱. رجوع شود به:
State Council Information Office of the People's Republic of China, 'China's Military Strategy', 27 May 2015, http://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm.

۲. رجوع شود به:
United States Office of the Director of National Intelligence, Assessing Russian Activities and Intentions in Recent US Elections, 6 January2017,
https://www.dni.gov/files/documents/ICA_2017_01.pdf.

۳. رجوع شود به:
White House, 'Executive Order on Securing the Information and Communications Technology and Services Supply Chain', 15 May 2019,
https://trumpwhitehouse.archives.gov/presidential-actions/executive -order-securing-information-communications-technology-services-supply-chain.

۴. رجوع شود به:
White House, 'Text of a Letter from the President to the Speaker of the House of Representatives and the President of the Senate', 30 March 2020,
https://trumpwhitehouse.archives.gov/briefings-statements/text-letter-president speaker-houserepresentatives-president-senate-67.

چهارمین مرتبه بود که یکی از رئیس‌جمهورهای ایالات متحده وضعیت اضطراری اعلام می‌کرد. در آوریل سال ۲۰۲۱ نیز چین ایالات متحده را «قهرمان» حملات سایبری نامید[۱]. یک ماه پس از آن، در نشست وزرای خارجه گروه هفت (G7)[۲] از روسیه و چین خواسته شد تا فعالیت‌های سایبری خود را با هنجارهای بین‌المللی تطبیق دهند[۳]. در گزارش حاضر تلاش شده‌است شواهد بیشتری از این دست ارائه شود که طبق آن‌ها در بسیاری از کشورها سیاست‌ها و توانمندی‌های سایبری جزء تفکیک‌ناپذیر امنیت بین‌المللی محسوب می‌شوند.

کشورهای منتخب در این گزارش عبارتند از: ایالات متحده آمریکا، بریتانیا، کانادا، استرالیا (چهار عضو از کشورهای «ائتلاف اطلاعاتی کشورهای پنج چشم»[۴])، فرانسه، ژاپن (یکی دیگر از متحدان ائتلاف پنج چشم که علی‌رغم قدرت اقتصادی چشمگیرش در جنبه‌های امنیت فضای سایبری توانایی کمتری دارد)، چین، روسیه، ایران، کره شمالی (کشورهایی که تهدید اصلی سایبری برای منافع غرب به‌شمار می‌روند)، هند، اندونزی، مالزی و ویتنام (چهار کشوری که در مراحل اولیه توسعه قدرت سایبری خود هستند) و رژیم صهیونیستی (قدرتمندترین متحدان سایبری کشورهای ائتلاف پنج چشم). ابتدای هر فصل حاوی چکیده‌ای از ارزیابی کشور موردنظر است. به‌طور کلی، در این گزارش توانمندی‌های سایبری هر کشور در هفت حوزه به شرح زیر ارزیابی شده‌اند:

---

۱. رجوع شود به:
Nick Wadhams, 'U.S.-China Talks in Alaska Quickly Descend Into Bickering', Bloomberg, 19 March 2021, https://www.bloomberg.com/news/articles/2021-03-18/u-s-china-meetingwill-underscore-biden-s-continuity-with-trump.

۲. گروه هفت شامل هفت کشور صنعتی ایالات متحده، کانادا، ژاپن، بریتانیا، فرانسه،آلمان و ایتالیاست که سال ۱۹۷۵ با اهداف سیاسی و اقتصادی تشکیل شد.

۳. رجوع شود به:
'G7 Foreign and Development Ministers' Meeting, May 2021: Communiqué', London, 5 May 2021, http://www.g7.utoronto.ca/foreign/210505-foreign-and-development-communique.html.

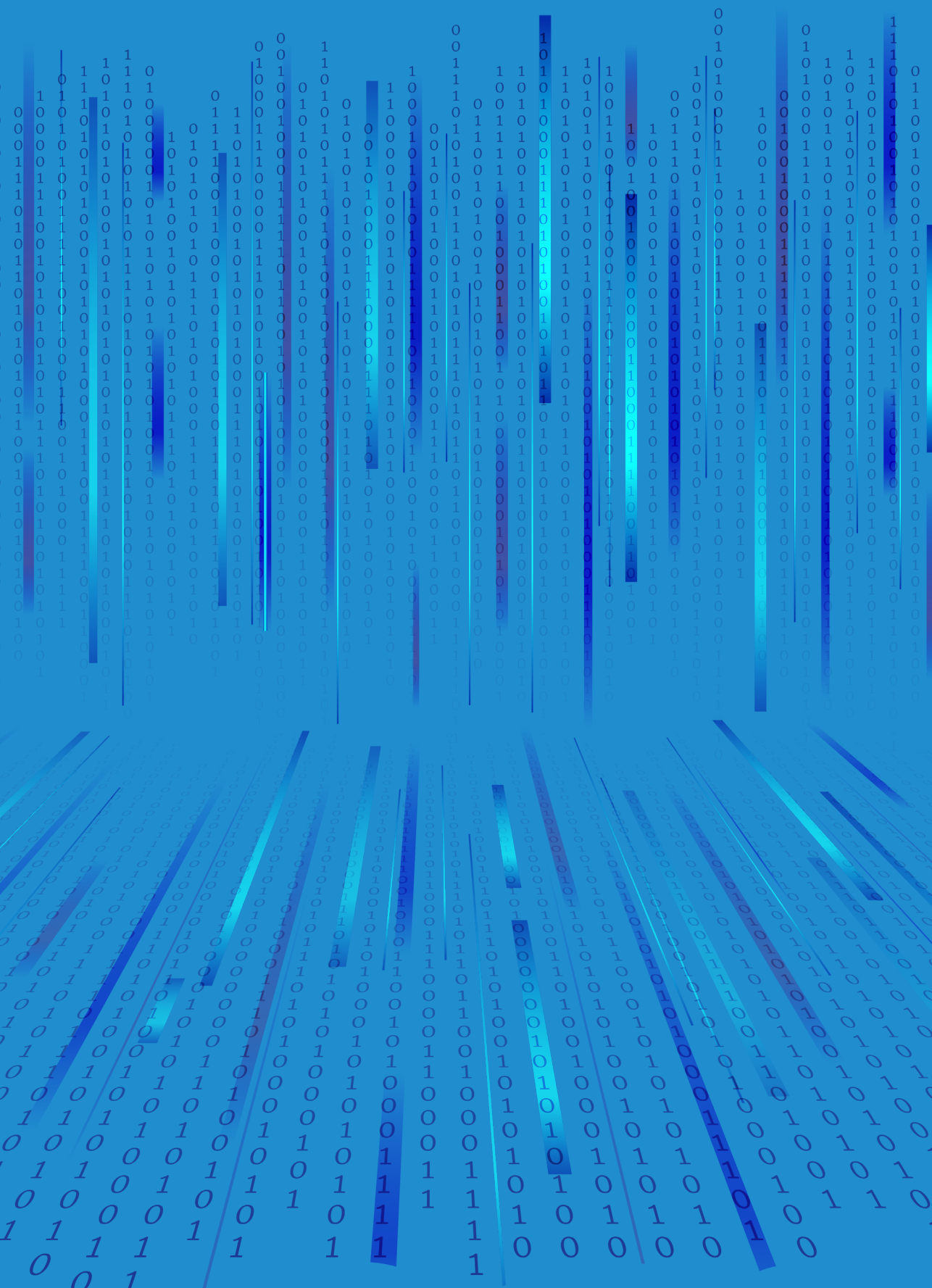
4. Five Eyes intelligence allies

- راهبرد و مبنای نظری (دکترین)
- حکمرانی، فرماندهی و نظارت
- توانمندی‌های محوری در زمینه اطلاعات سایبری
- توانمندی و وابستگی سایبری
- امنیت و تاب‌آوری سایبری
- رهبری جهانی در عرصه سایبری
- توانمندی‌های سایبری تهاجمی

مؤسسه بین‌المللی مطالعات راهبردی قصد دارد به تحقیقات خود در حوزه قدرت سایبری ادامه دهد و در مطالعات آتی تحلیل‌های عمیق‌تری از اقدامات کشورها در زمینه توانمندی‌های سایبری تهاجمی ارائه دهد. با کمک تیم‌های پژوهشی این موسسه در برلین، لندن، منامه، سنگاپور و واشنگتن، مطالعات کارشناسی گسترده‌تری در این زمینه انجام خواهد شد.

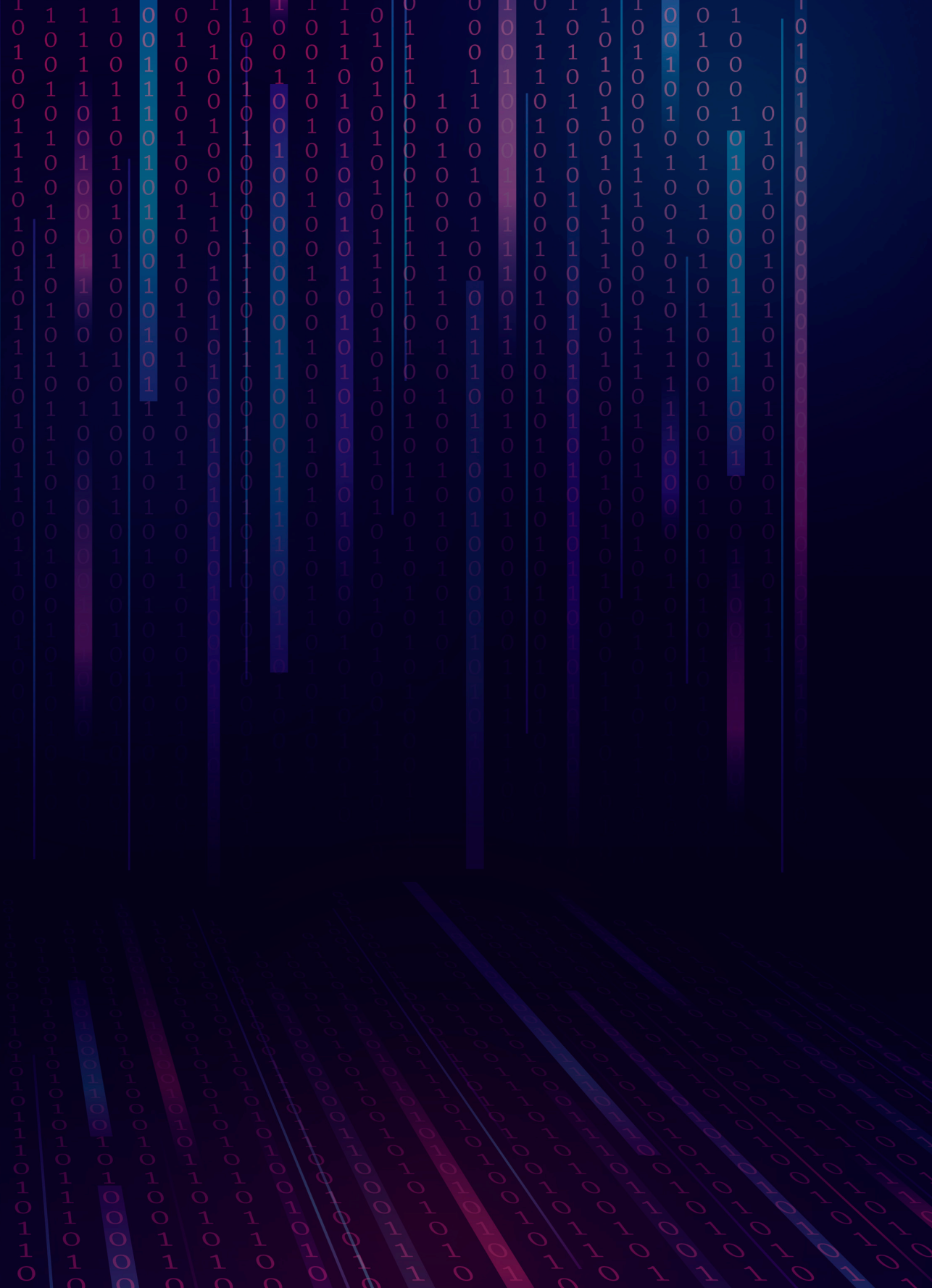
شایان ذکر است مولف این گزارش مؤسسه بین‌المللی مطالعات راهبردی است و مسئولیت کامل محتوای آن برعهده موسسه مذکور است، اما با توجه به اهمیت موضوع متن کامل گزارش مذکور توسط همکاران موسسه پویندگان توسعه فناوری و نوآوری ایرانیان به زبان فارسی ترجمه و تدوین گردید و در اختیار مخاطبان و دست‌اندرکاران محترم قرار می‌گیرد[1].

۱. لازم به ذکر است در ترجمه این اثر تلاش شده اصل امانتداری و انتقال بی‌کم‌وکاست محتوا تا حد امکان رعایت شود. به‌جز فصل ایران که به‌دلیل لحن نسبتا جانبدارانه مولف، موارد دارای بار معنایی منفی جهت حفظ شأن خواننده ایرانی تلطیف شده‌اند، در سایر فصل‌ها لحن و محتوای متن اصلی حتی‌المقدور حفظ شده‌است (متاسفانه مولف در فصل‌های مربوط به کشورهای ایران، روسیه، چین و کره شمالی از رویکرد علمی و غیرجانبدارانه تا حدی فاصله گرفته‌است).



ارزیابی کلی توانمندی‌های سایبری و قدرت ملی

فهرست



پروژه قدرت سایبری:
بافتار و روش‌شناسی

در دو دهـه اخیـر توانمندی‌های سـایبری به ابزاری با تاثیرگـذاری بالا برای اعمال قدرت ملـی کشـورها تبدیل شـده‌اند. این توانمندی‌ها عـلاوه براینکه همانند روش‌های سـنتی جاسوسـی برای دسـت‌یابی به اسرار دیگر کشورها استفاده می‌شوند، دولت‌ها آن‌ها را در امور بسـیار تهدیدآمیزتر نیز به‌کار می‌گیرند. ازجمله این موارد می‌توان به موارد زیر اشـاره کـرد: ایجـاد اختلال در موسسـات مالی، صنایع نفتی، نیروگاه‌های هسـته‌ای شـبکه برق و زیرسـاخت‌های مخابراتی کشـورهای دشـمن؛ مداخله در فرایندهای دموکراتیک؛ تخریب توانمندی‌هـای نظامـی یا ایجـاد اختلال در آن‌ها در زمان جنگ و در مواردی محدودسـازی امکان توسعه سلاح‌های هسته‌ای در دیگر کشورها.

برخـی از نمونه‌هـای عملیات‌هـای سـایبری دولت‌هـا علیـه دیگـر دولت‌هـا کـه در رسـانه‌ها افشـا شـده‌اند، عبارتند از: عملیات‌های سـایبری آمریکا و ایـران علیه یکدیگر؛ عملیات‌هـای سـایبری رژیـم صهیونیسـتی و ایـران علیه یکدیگـر؛ عملیات‌های سـایبری روسیه علیه استونی،گرجستان، اکراین؛ و اقدامات چین برای سرقت دستاوردهای علمی دارای مالکیـت فـکری (پتنت‌ها/اختراعات) دیگر کشورها. تاکـنون نمونه‌های بسیاری از عملیات‌های سـایبری دولت‌ها علیه دیگر کشورها افشـا شـده‌اند که در رسانه‌ها به‌طور گسـترده بازتـاب یافته‌انـد. عملیات‌هـای مداخله روسیـه در روندهای انتخاباتـی آمریکا و بریتانیا و متعاقب آن اقدام متقابل آمریکا علیه گروه روسی مستقر در سن‌پترزبورگ و یا عملیات‌های ایران علیه عربستان سعودی، کره شمالی علیه شرکت سونی و نظام بانکی جهانی ازجمله این موارد به شـمار می‌آیند.

بـا ایـن حـال، افشـاگری‌های رسـانه‌ای تنها بخـش کوچکی از ماجـرا را آشـکار کرده‌اند. درواقع، هر لحظه حجم زیادی از عملیات‌های سایبری دولتی در زمینه پایش و شناسایی

شبکه‌های مختلف انجام می‌شود که گاه شبکه‌ها به اشتباه این عملیات‌های نفوذ را حمله سایبری تصور می‌کنند و دست به اقدامات تلافی‌جویانه می‌زنند. در برخی از عملیات‌های پایشی نیز ممکن است کدهای درج‌شده در شبکه هدف موجب اختلال و بروز حادثه شوند. به‌بیان دیگر، افزایش حجم اشتباهات و حوادث ناشی از عملیات‌های پایش و نفوذ می‌تواند باعث درگیری‌های سایبری بین دولت‌ها شود و متاسفانه، همواره این خطر وجود دارد که درگیری‌ها از کنترل خارج شوند. علاوه بر این‌ها، خطر دستیابی تروریست‌ها و مجرمان به توانمندی‌های سایبری دولت‌ها نیز مطرح است و به‌دلیل وجود بازار باز، دولت‌ها نیز به‌راحتی می‌توانند به ابزارهای مخرب و به‌شدت کارآمد دسترسی داشته باشند.

بنابراین، امروزه فضای سایبری ضمن اینکه محیطی جدید و مخاطره‌آمیز برای دولت‌مردان محسوب می‌شود، به بستری مناسب برای جرائم سازمان‌یافته نیز تبدیل شده‌است. گفتنی آنکه هنوز برآورد دقیق هزینه‌های جرائم سایبری در سطح ملی به‌راحتی امکان‌پذیر نیست[۱]. البته مواردی مانند جرائم مربوط به کارت‌های اعتباری تا حدی قابل محاسبه هستند[۲]، ولی صدمه‌ای که به‌عنوان مثال به آبروی اشخاص یا اعتبار تجاری شرکت‌ها و ارزش سهام آن‌ها می‌رسد را نمی‌توان به سهولت کمّی‌سازی کرد. آمارها نشان می‌دهند از سال ۲۰۱۷ شمار حملات باج‌افزاری[۳] روند صعودی داشته و ده‌ها میلیارد دلار خسارت به بار آورده‌است. در کنار همه این خطرات باید توجه داشت که در عصر حاضر

۱. رجوع شود به
Eileen Decker, 'Full Count? Crime Rate Swings, Cybercrime Misses and Why We Don't Really Know the Score', Journal of National Security Law & Policy, vol. 10, no. 3, 13 February 2020, pp. 583-604, https://jnslp.com/wp-content/uploads/2020/05/Crime-Rate-Swings-Cybercrime-Misses.pdf.

۲. رجوع شود به
Ross Anderson et al., 'Measuring the changing cost of cybercrime' Boston, US, 3-4 June 2019, pp. 5-8, http://orca.cf.ac.uk/122684/1/Levi_Measuring%20the%20Changing%20Cost%20of%20Cybercrime.pdf.

۳. باج‌افزار یا ransomware نوعی بدافزار است که دسترسی به اطلاعات را منوط به پرداخت مبلغ باج می‌کند.

گروه‌های تروریستی در حال ارتقای مهارت‌ها و توانمندی‌های سایبری خود هستند و فعالان سیاسی-از هر طیفی-فضای سایبری را ابزاری بی‌نهایت ضروری در پیشبرد مقاصد خود می‌دانند. از این رو، خطرات ناشی از این فضا برای دولت‌ها و شهروندان بسیار زیاد و متنوع است و دولت‌ها جهت مقابله موثر با این خطرات و حفاظت از زیرساخت‌های ملی و شهروندان در برابر آن‌ها مجبور به سرمایه‌گذاری‌های هنگفتی برای تامین امنیت سایبری هستند. ورود دولت‌ها به این عرصه و درج موضوعات سایبری در برنامه‌ها و سیاست‌های ملی و تخصیص بودجه به این امر موجب رشد روزافزون صنعت سایبری و افزایش شتاب پیشرفت آن شده‌است.

افزون بر این، با افزایش وابستگی شهروندان به اینترنت و گسترش به‌کارگیری خدمات دیجیتال در امور شهری (شهرهای هوشمند)، دولت‌ها بیش از هر زمان دیگری به اهمیت مدیریت خطرات سایبری جهت حفاظت از اقتصاد و امنیت ملی پی برده‌اند و می‌کوشند تا در طراحی، ساخت و حکمرانی اینترنت در آینده سهیم باشند و حتی آن را تا حدودی در اختیار خود درآورند. در همین راستا، سالهاست که برخی از کشورها به رهبری روسیه و چین سعی می‌کنند به جای مدل کنونی به‌اصطلاح «اینترنت آزاد» که مروج حاکمیت مشارکتی بخش دولتی، بخش خصوصی و اشخاص و سایر ذینفعان به صورت متوازن است، مدلی از حاکمیت اینترنت را در سازمان ملل تصویب کنند که بیشتر مبتنی بر کنترل و نظارت دولتی باشد.

به‌دلیل اهمیتی که حاکمیت فضای سایبری در قرن بیست‌ویک پیدا کرده‌است، رقابت‌های بین کشورها نیز از این امر متاثر شده و دو کشور ایالات متحده و چین رقابت اقتصادی خود را در حوزه‌هایی مانند تولید ریزتراشه‌ها، مونتاژ رایانه، اینترنت

نسل پنجم (5G)، معماری‌های ابری و روترها و کابل‌ها متمرکز کرده‌اند و با ساخت برنامه‌های کاربردی داخلی و ممنوعیت برنامه‌های کاربردی یکدیگر حاکمیت خود را تقویت می‌کنند[1]. بنابراین، کشورها در حال حاضر با آگاهی از ضرورت پیشتاز بودن در فناوری‌های اطلاعات و ارتباطات در امنیت، اقتصاد و ژئوپلیتیک جهانی تنها راه تبدیل‌شدن به ابرقدرت را ابرقدرت بودن در عرصه دیجیتال می‌دانند.

افزایش یکباره و گسترده کاربران اینترنت در دوره همه‌گیری کوید-۱۹ مسائل امنیتی بسیاری را در فضای سایبری ایجاد کرد. درواقع، ممنوعیت‌های ارتباطات فیزیکی در این دوره موجب کاهش فرصت‌های ارتکاب جرائم فیزیکی و در مقابل، گسترش جرائم سایبری شد. اما تجربه کوید-۱۹ می‌تواند درس‌های خوبی برای دولت‌ها در زمینه مقابله با همه‌گیری ویروس‌های سایبری داشته باشد: همان‌طور که دولت‌ها به‌خوبی به تبادل اطلاعات و فناوری در زمینه پیشگیری و مقابله با ویروس کرونا پرداختند، می‌توانند در ارتقای امنیت فضای سایبری نیز با هم همکاری کنند و دی‌اِن‌اِی فنی و تجارب خود در زمینه مقابله با این ویروس دیجیتال را به‌اشتراک بگذارند و با ایجاد هنجارهای بین‌المللی در زمینه رفتار در فضای سایبری به افزایش امنیت آن کمک کنند.

با توجه به آنچه گفته شد، موسسه بین‌المللی مطالعات راهبردی با در نظرگرفتن وابستگی روزافزون اقتصاد و امنیت ملی کشورها به فضای سایبری و نیز اهتمام دولت‌ها به ارتقای قدرت سایبری تلاش کرده‌است روش‌شناسی جدیدی برای ارزیابی قدرت سایبری کشورها طراحی کند.

۱. رجوع شود به مباحث مربوط به برنامه شبکه پاک دولت ایالات متحده در وزارت کشور آمریکا:
'Announcing the Expansion of the Clean Network to Safeguard America's Assets', 5 August 2020, https://china.usembassy-china.org.cn/announcing-the-expansion-ofthe-clean-network-to-safeguard-americas-assets.

روش‌شناسی

بسیاری از روش‌های موجود برای ارزیابی قدرت سایبری شاخص‌محور و متمرکز بر امینت سایبری هستند. اما روش طراحی شده توسط این موسسه همه جنبه‌های قدرت سایبری را پوشش می‌دهد و رویکردی کیفی دارد. در این روش بازیگران غیردولتی تنها در صورتی که در ساخت و به‌کارگیری توانمندی‌های سایبری نقش داشته باشند، در ارزیابی مدنظر قرار می‌گیرند. به‌عنوان مثال، ارتش سایبری ایران یا سازمان تحقیقات اینترنتی روسیه (مستقر در سن‌پترزبورگ) که به‌ترتیب از ذینفعان دولتی ایران و روسیه هستند، در ارزیابی قدرت سایبری آن‌ها لحاظ شده‌اند. به‌طور کلی، ارزیابی کشورها در هفت حوزه انجام می‌شود:

- راهبرد و مبنای نظری (دکترین)
- حکمرانی، فرماندهی و نظارت
- توانمندی‌های محوری در زمینه اطلاعات سایبری
- توانمندی و وابستگی سایبری
- امنیت و تاب‌آوری سایبری
- رهبری جهانی در عرصه سایبری
- توانمندی‌های سایبری تهاجمی

در حوزه اول، همه اسناد مهم دولت‌ها صرف‌نظر از عنوان آن‌ها بررسی شده‌اند. این اسناد حاوی موضوعاتی ازقبیل اولویت‌ها و بودجه‌ها، تبیین سیاست مدیریت یا تشریح تغییرات سازمانی و یا نحوه ارتقای آگاهی عمومی نسبت به راهبردهای دولت می‌شوند. شایان ذکر است روش اخیر برخلاف مطالعات شاخص‌محور، به معرفی اسناد بسنده نمی‌کند و به تجزیه‌وتحلیل تحول و کیفیت آن‌ها نیز می‌پردازد.

در حوزه دوم به ساختارهای بالادستی دولتی و نظامی و نیز ساختارهای اجرایی از نظر روند تحول و میزان کارایی کنونی آن‌ها پرداخته می‌شود.

متاسفانه با وجود اهمیت محوری حوزه سوم یعنی توانمندی‌های سایبری دفاعی یا تهاجمی کشورها در شناسایی و شناخت تهدیدها و فرصت‌های فضای سایبری، به‌دلیل محرمانگی اطلاعات این بخش و عدم دسترسی عمومی، ارزیابی آن بسیار دشوار است.

حوزه چهارم پاسخ به این سوال را بررسی می‌کند: آیا دولت‌ها می‌توانند با کناره‌گیری از اینترنت جهانی حداکثر حفاظت در برابر دشمنان سایبری را برای کشور خود تضمین کنند؟ در پاسخ به این سوال، فرض می‌شود اگرچه هر گونه ارتباط اینترنتی مستلزم آسیب‌پذیری است، اما دسترسی به حجم عظیم داده و شبکه‌سازی جهانی می‌تواند موجب تقویت اقتصاد، حاکمیت و حتی توان نظامی ملت‌ها شود. بنابراین، در این گزارش هر دو جنبه مدنظر قرار می‌گیرد و برای ارزیابی میزان وابستگی کشورها، سطح چالاکی و گستره اقتصاد دیجیتال آن‌ها بررسی می‌شود. به این منظور، تعریف گروه ۲۰ از اقتصاد دیجیتال که کل اثرات اقتصادی فناوری‌های اطلاعات و ارتباطات در همه بخش‌ها و نه صرفا ارزش خروجی شرکت‌ها را لحاظ می‌کند، مبنای برآوردهای گزارش حاضر قرار گرفته است. افزون بر این، قدرت مطلق اقتصادی کشورها در عرصه سایبری نیز بررسی می‌شود و از آنجا که امکان ارزیابی کل بنیان علم و فناوری سایبری کشورها وجود ندارد، از میزان تحقیقات حوزه هوش مصنوعی به‌عنوان شاخص نیابتی[1] برای ارزیابی سطح توسعه سایبری کشورها استفاده می‌شود[2].

1. Proxy indicator

۲. زیرا تحقیقات حوزه هوش مصنوعی کاملا جهانی است و به‌راحتی نمی‌توان آن را به ملیت خاصی نسبت داد. درواقع، کشورها براساس اولویت‌های خود در رشته‌های مختلف مرتبط با هوش مصنوعی فعالیت می‌کنند و به‌همین‌ترتیب، به‌کارگیری هوش مصنوعی برای مسائل امنیت ملی یا نظامی بستگی به اولویت‌های دولت‌ها دارد. به‌عنوان نمونه، ایالات متحده در زمینه کارکردهای هوش مصنوعی در بخش سلامت پیشتاز است و چین در زمینه بهره‌وری انرژی. برای مباحث بیشتر رجوع شود به:
Artificial Intelligence in Society (Paris: OECD Publishing, 2019), https://doi.org/10.1787/eedfee77-en

حوزه پنجم شامل توانایی دولت‌ها در پاسخ‌دهی به رویدادها و فوریت‌های مهم سایبری و جبران خسارت‌ها (احیا) می‌شود. علاوه بر این، تدوین استانداردهای امنیتی، نوآوری فنی، مدیریت خطر در بخش‌های اقتصادی، کارآمدی صنعت امنیت سایبری بومی و سطح توسعه منابع انسانی دارای تخصص سایبری نیز در دامنه این حوزه قرار می‌گیرد. به‌منظور استفاده از معیاری استاندارد درباره وضعیت امنیت سایبری کشورها، رتبه آن‌ها در «شاخص جهانی امنیت سایبری»[1] در سال ۲۰۱۸ که توسط «اتحادیه بین‌المللی مخابرات» (ITU)[2] تهیه شده هم در بررسی اختصاصی هر یک از کشورها لحاظ شده‌است.

در حوزه ششم که به تعاملات بین‌المللی کشورها در عرصه سایبری می‌پردازد، میزان مشارکت و اثرگذاری آن‌ها حائزاهمیت است و درنتیجه، شامل مواردی از این قبیل می‌شود: بررسی دیپلماسی بین‌المللی، پیمان‌های رسمی، شرکت در هم‌اندیشی‌های بین‌المللی و مشارکت در همکاری‌های فنی و مناسبات بین‌المللی دوطرفه.

در حوزه آخر منظور از توانمندی‌های سایبری تهاجمی، عملیات‌هایی است که بیشتر به‌منظور اثرگذاری و نه صرفا گردآوری اطلاعات انجام می‌شوند و بنابراین، شامل همه عملیات‌هایی است که توسط عوامل نظامی یا شهروندان درجهت اثرگذاری شناختی یا تخریب فیزیکی (در زمان جنگ یا صلح) بر اهداف نظامی یا غیرنظامی انجام می‌شوند. لازم به ذکر است مفاهیمی مانند جاسوسی سایبری یا بهره‌برداری از شبکه رایانه‌ای که بیشتر مبتنی بر جمع‌آوری داده و اطلاعات هستند، در حوزه سوم بررسی می‌شوند. درمقابل، عوامل تاثیرگذار بر کشورها در استفاده از توانمندی‌های سایبری تهاجمی مانند اراده سیاسی، نظام‌های حقوقی و چارچوب‌های اخلاقی آن‌ها در گستره حوزه هفتم قرار دارند.

1. 2018 Global Cybersecurity Index
2. International Telecommunication Union

کشورهایی که در این گزارش بررسی می‌شوند، عبارتند از:

- چهار کشور از پنج کشور عضو ائتلاف اطلاعاتی پنج چشم شامل ایالات متحده، بریتانیا، کانادا و استرالیا؛
- سه متحد سایبری اصلی ائتلاف پنج چشم شامل فرانسه، رژیم صهیونیستی و ژاپن؛
- چهار کشور روسیه، چین، ایران و کره شمالی که تهدیدهای اصلی ائتلاف پنج چشم قلمداد می‌شوند؛ و
- چهار کشور سایبری در حال توسعه شامل هند، اندونزی، مالزی و ویتنام.

باید توجه داشت که در این مطالعه از بسیاری از کشورهای دارای قدرت سایبری قابل‌ملاحظه مانند آلمان و کشورهای اسکاندیناوی و یا کره جنوبی و نیز سایر کشورهای در حال توسعه صرف‌نظر شده‌است. زیرا مجریان این مطالعه در نظر داشتند در مرحله اول این روش‌شناسی را به گزیده‌ای ازکشورهای قدرتمند سایبری و کشورهای دارای توانمندی‌های سایبریِ درحال‌توسعه اعمال کنند و در مراحل بعد با توجه به نتایج این مطالعه اولیه، مطالعه جامع درباره همه کشورها انجام شود.

هر یک از بخش‌های این گزارش توسط کارشناسی خبره و با طرح و بررسی سوالاتی دقیق در رابطه با هفت حوزه موردنظر انجام شده‌است. نتیجه حاصله با توجه به شرایط، دیدگاه‌ها و منابع موجود کشورها برای هریک از آن‌ها متفاوت است، اما سعی شده‌است تا حد ممکن همه مطالعه‌ها مطابق با اهداف کلی پژوهش حاضر انجام شوند.

گردآوری داده‌ها ازطریق مطالعه متون موجود (ازجمله اسناد رسمی) و در برخی موارد ازطریق مصاحبه با کارشناسان انجام گرفته‌است. خوشبختانه حجم داده‌های دردسترس بیش از حد انتظار است و همین امر ارزیابی برخی از حوزه‌های ملموس مانند دامنه حفاظت و اجزای اقتصادی و صنعتی توانمندی‌های سایبری کشورها را تسهیل می‌کند.

حقایق کلیدی این گزارش از متن برنامه‌ها و راهبردهای منتشرشده کشورها، منابع انسانی مستقیم[1] و سرمایه‌گذاری‌های رسمی و بررسی فعالیت‌های آشکار آن‌ها استخراج شده‌اند. ارزیابی توانمندی‌های اطلاعاتی و سایبری تهاجمی کشورها سخت‌ترین بخش مطالعه است، چراکه به‌دلیل ماهیت محرمانه این توانمندی‌ها دسترسی به شواهدی مبنی بر وجود آن‌ها دشوار است.

تجزیه‌وتحلیل

در این بخش ۱۴ کشور منتخب به‌علاوه رژیم صهیونیستی با توجه به موضوعاتی کلیدی موردبررسی قرار می‌گیرند و جایگاه نسبی آن‌ها از نظر قدرت سایبری تبیین می‌شود.

چالش‌های ملی در مواجهه با فضای سایبری

همه کشورهای موردمطالعه درصدد تدوین چارچوب‌های سیاستی دائمی برای بهره‌برداری از فرصت‌های جدید یا مقابله با تهدیدهای جدید هستند. پویایی محیط سایبری از نظر فناوری، اقتصاد، سیاست و امنیت باعث شده‌است کشورهای پیشتاز به بازبینی و ارتقای مستمر اسناد راهبردی خود بپردازند. همزمان، ساختارهای سنتی دولت‌ها، مدیریت شرکت و نظام‌بخشی اجتماعی نیز همواره باید خود را با این محیط متغیر انطباق دهند.

نتایج مطالعه حاضر نشان می‌دهند که همه این کشورها هنوز شناخت جامعی نسبت به پیامدهای راهبردی فضای سایبری پیدا نکرده‌اند و درنتیجه، چشم‌اندازهای آرمانی و گاه تا حدی تخیلی از آینده ترسیم می‌کنند. برنامه‌ریزی برای اجرای پروژه‌هایی مانند ساخت شهرهای هوشمند و خودروهای بدون راننده، انجام جراحی از راه دور یا دستیابی به ربایتک نظامی در آینده نزدیک نشان از این دیدگاه غیرواقع‌بینانه دارند.

۱. منظور نیروهای انسانی است که به‌طور مشخص به فعالیت‌های مرتبط با فضای سایبری اشتغال دارند، درنتیجه افرادی که به‌صورت غیرمستقیم در این حوزه فعالیت دارند، در آمار محاسبه نمی‌شوند.

البته بیشتر این کشورها آمادگی کافی ندارند و به همین دلیل در هماهنگ‌سازی چنین چشم‌اندازهایی با روند سیاست‌گذاری ملی با چالش مواجه هستند. برخلاف بخش دولتی، سیاست مصرف‌کننده‌محور در بخش خصوصی کاملا بر سیاست‌های دولتی برتری دارد. درحقیقت، روند توسعه فضای سایبری در بخش خصوصی به‌حدی شتابناک است که در برخی از کشورها نگرانی‌هایی در مورد آینده بشر و نیز ماهیت رقابت‌های آتی به‌وجود آمده‌است و نوعی حس بحران و ناکارآمدی دولت‌ها در برابر توسعه بخش خصوصی بر بسیاری از محافل سیاسی آن‌ها سایه افکنده‌است. به بیان دیگر، نوعی رقابت نابرابر بین بخش خصوصی در توسعه فناوری‌ها و بخش دولتی در تهیه مقررات و استانداردها و اعمال نظارت شکل گرفته‌است. اگرچه این شرایط اثرات مثبت و منفی بسیاری بر تدوین راهبردهای ملی داشته‌اند، اما بیشتر دولت‌ها اعتقاد دارند راهبردهای کنونی آن‌ها نمی‌توانند اهداف موردنظر را محقق کنند. به‌طور کلی، کشورهای معدودی در تدوین و اجرای راهبردهایی موثر برای توسعه ملی موفق بوده‌اند، اما به نظر می‌رسد کشورهای کوچک‌تر مانند رژیم صهیونیستی عملکرد بهتری نسبت به کشورهای بزرگ داشته‌اند.

نقش سازمان‌های اطلاعاتی

مساله محرمانگی یکی از موانع اتخاذ رویکرد بین‌المللی مستند (مبتنی بر شواهد و اسناد رسمی) در مدیریت خطرات پیش‌روی عملیات‌های سایبری است. زیرا در کشورهای پیشتاز توانمندی‌های اطلاعاتی پیشرفته و سازمان‌های ذی‌ربط در به‌کارگیری آن‌ها عناصر کلیدی در عملیات‌های سایبری دفاعی و تهاجمی آن‌ها نیز محسوب می‌شوند. به‌عنوان مثال، توانمندی‌هایی که کشورهای عضو ائتلاف پنج چشم پس از یازده سپتامبر برای شناسایی اقدامات تروریستی طراحی کردند، کارکرد تهاجمی

نیـز دارنـد. به‌همیـن ترتیـب، روش‌های پیچیـده هک کـه دولت‌ها برای کسـب اطلاعات دربـاره رقبـای خود طراحـی کرده‌اند، در عملیات‌های سـایبری تهاجمی نیز بـه‌کار می‌روند. از همیـن روسـت کـه سـازمان‌هایی مانند سـازمان امنیت ملـی (NSA)[1] ایـالات متحده و سـتاد ارتباطـات دولـت (GCHQ)[2] در بریتانیا عامل اصلی شـکل‌گیری و اجرای رویکرد ملی این کشـورها در عرصه سـایبری هسـتند. این دو کشور در بین کشـورهایی قرار دارند که ضرورت افزایش شـفافیت در امنیت سـایبری را دریافته‌انـد و ابتکارهای متعددی مانند بهبود اشـتراک‌گذاری داده‌های مربوط به تهدیدها و آسـیب‌ها با صنعت و جامعه را برای افزایش شفافیت اجرا کرده‌اند.

رقابت صنعتی فناوری پیشرفته

در آینده تاب‌آوری سـایبری کشورها به زیرسـاخت‌های فیزیکی اینترنت جهانی و نحوه ساخت آن‌ها بستگی دارد. با توجه به نگرانی‌هایی که در سال ۲۰۲۰ در مورد شرکت هوآوی و خطرات بالقوه به‌کارگیری تجهیزات خارجی در زیرسـاخت‌های ملی حیاتی شـکل گرفت، بررسـی سـهم کشورهـا از دارایی‌هـایی جهانـی دیجیتـال می‌توانـد نـکات مفیـدی را درباره قدرت سایبری آن‌ها در اختیار ما بگذارد. با نگاهی به ملیت ۵۱ شرکت فناوری یا مخابراتی (تله‌کام)[3] که در زمره شرکت‌های برتر در فهرست رده‌بندی فورچون ۵۰۰[4] (۲۰۲۰) قرار دارند، درمی‌یابیـم کـه بیشـتر این شـرکت‌ها متعلق بـه ایالات متحـده و متحدانش و یا شـرکای نزدیـک آن‌هـا هسـتند. بـه بیـان دقیق‌تر، شـانزده شـرکت به آمریکا، ده شـرکت بـه ژاپن، شـش شـرکت به تایوان، دو شـرکت به کره جنوبی، هشـت شـرکت به اروپای غربی و یک

1. National Security Agency
2. Government Communications Headquarters
۳. جهت مشاهده فهرست شرکت‌های فناوری و مخابراتی به‌ترتیب به آدرس‌های زیر مراجعه شود:
https://fortune.com/global500/2020/search/?sector=Technology
https://fortune.com/global500/2020/search/?sector=Telecommunications
4. 2020 Fortune 'Global 500'

شـرکت به مکزیک تعلق داشته‌اسـت. هشت شـرکت باقیمانده متعلق به چین هستند که سهم بازار آن به سرعت در سراسر دنیا روبه‌گسترش است.

بـا ایـن حـال، در همه ایـن کشـورها به‌کارگیری فنـاوری دیجیتال مسـتلزم اسـتفاده از تجهیزات خارجی مختلفی است. به‌عنوان مثال، در کشور چین محصولات هشت شرکت آمریکایـی به‌وفـور در صنایـع آن اسـتفاده می‌شـود و بنابرایـن، آسـیب‌پذیری آن در برابـر رقیـب بالاسـت. چین این شـرکت‌ها که بخـش اعظم بـازار دیجیتـال آن را در اختیار دارند «هشت جنگجوی نگهبان»[1] می‌نامد[2]. دولت چین برای کاهش سطح خطر با شرکت‌های آمریکایـی در حکمرانـی امنیـت سـایبری ملی خـود ازجملـه در تدوین اسـتانداردهای فنی ملی مشـارکت کرده‌اسـت و به این ترتیب، امکان نظارت نسبی بر استفاده از فناوری‌های آمریکایی در شـبکه‌های داخلی را فراهم آورده‌اسـت. البته تحقـق این نوع نظارت به‌دلیل پیچیدگی ارتباطات نهادهای چینی و آمریکایی در فضای سـایبری چندان آسـان نیسـت. به‌عنوان مثال، در سپتامبر ۲۰۱۹ شرکت آی‌بی‌ام (یکی از هشت جنگجوی نگهبان) و بانک چیـن[3] اعـلام کردند همکاری‌های خود را به تولید نوآوری‌های دیجیتال جدید برای صنعت مالـی نیـز تعمیـم خواهند داد تا امـکان انجام ده‌هـا تریلیون دلار مبـادلات مالی جهانی در زیرسـاخت‌های مشـترک و با اسـتانداردهای یکسـان یا قابل‌تطبیـق را فراهم کننـد. البته وجود رقابت شـدید بین آمریکا و چین که از سـال ۲۰۲۰ نیز تشـدید شده‌است، موفقیت یا تداوم اینگونه همکاری‌ها را در هاله‌ای از ابهام فرو می‌برد.

رویکرد کل جامعه در امنیت سایبری

امروزه همـه کشورهـای بـرخوردار از توانمندی‌هـای سـایبری در پی اجـرای رویکرد کل جامعـه در اقدامـات حوزه امنیـت سـایبری هسـتند کـه به‌معنـی همـکاری نزدیـک بیـن

1. 8 guardian warriors

۲. شامل شرکت‌های Apple, Cisco, Google, and IBM, Intel, Microsoft, Oracle, Qualcomm

3. Bank of China

بخش‌های خصوصی، دولتی، دانشگاهیان، مشارکت‌های نظامی و غیرنظامی و البته افزایش آگاهی عمومی و راه‌اندازی پویش‌های همگانی جهت ارتقای سواد سایبری است. کشورهای مختلف روش‌های متفاوتی برای تحقق این امر اتخاذ کرده‌اند. در کشورهای اقتدارگرا مانند روسیه، چین و ایران اغلب از روش بالا به پایین استفاده می‌کنند تا راحت‌تر بر انتشار محتوا در فضای سایبری نظارت کنند و به‌همین دلیل، توجه کمتری به حفاظت از شبکه‌های حیاتی خود دارند. در این کشورها تلاش می‌شود نظارت دولتی مطلق بر اینترنت حاکم شود تا در صورت نیاز بتوانند از اینترنت جهانی که تحت‌نظارت ایالات متحده است مستقل شوند.

درمقابل، در کشورهای دارای نظام لیبرال‌تر بیشتر روی توسعه نوآوری ازطریق حمایت از بخش خصوصی و دانشگاه‌ها و نیز حمایت از حریم خصوصی و داده‌های افراد تمرکز می‌شود. این روش به ساخت صنعت امنیت سایبری پویای چندصد میلیاردی و سرمایه‌گذاری‌های کلان در امنیت سایبری توسط خود شرکت‌های ارائه‌کننده خدمات اینترنتی منتهی می‌شود. این دولت‌ها تلاش می‌کنند با ایجاد حاکمیتی متوازن با مشارکت دولت ملی، بخش خصوصی، سازمان‌های غیردولتی و دانشگاهیان به اینترنت جهانی چندذینفعی دست یابند.

شواهد نشان می‌دهند هر یک از این دو روش مزایا و معایب مختص به خود را دارند، ولی عملکرد کلی دموکراسی‌های لیبرال بهتر بوده و صنعت امنیت سایبری آن‌ها چابک‌تر است. این کشورها همچنین رتبه‌های بهتری در شاخص جهانی امنیت سایبری کسب‌کرده‌اند.

توانمندی‌های سایبری تهاجمی

قدرت‌های سایبری پیشگام از رویکردهای مختلفی در ساخت و به‌کارگیری توانمندی‌های سایبری تهاجمی استفاده می‌کنند. کشورهای دارای منابع انسانی و سرمایه

فراوان مانند ایالات متحده و چین به شدت سعی دارند مالکیت توانمندی‌های سایبری نظامی و غیرنظامی کاملا متمایز باشد، حال آنکه کشورهای دارای منابع محدودتر مانند بریتانیا، فرانسه و همچنین رژیم صهیونیستی از رویکردی ترکیبی از مالکیت نظامی و غیرنظامی بهره می‌برند که موجب پویایی عملیاتی بیشتر در دستاوردهای آن‌ها شده‌است.

علاوه بر این، بیشتر دولت‌ها ساخت و به‌کارگیری توانمندی‌های سایبری تهاجمی را تحت‌نظارت و کنترل شدید مقررات حقوقی قرار می‌دهند. اما برخی از کشورها مانند روسیه نسبت به هکرهای وطن‌پرست که فعالیت‌هایی همسو با منافع دولت دارند، اجازه اجرای عملیات از داخل خاک خود را می‌دهند و گاه حتی با آن‌ها هماهنگ نیز هستند.

دولت‌ها از منظر دیدگاه و مبنای نظری (دکترین) سایبری نیز با هم تفاوت‌هایی دارند. روسیه و چین آنچه را که دنیای غرب سایبر تهاجمی می‌خواند، صرفا جزئی فنی از توانمندی عملیاتی-اطلاعاتی بزرگ‌تر می‌دانند که به آن‌ها امکان کنترل فضای اطلاعاتی خود و تضعیف فضای اطلاعاتی کشورهای متخاصم را می‌دهد. به‌عبارت دیگر، سایبری تهاجمی یکی از بازوهای دستگاه تبلیغات این دولت‌ها و وسیله‌ای برای تولید/انتشار اخبار جعلی و روشی جهت نفوذ به زیرساخت‌های حیاتی کشورهای دشمن محسوب می‌شود. اگرچه کشورهایی مانند روسیه و چین با استفاده از این دیدگاه از مزایای به‌کارگیری منسجم همه منابع در برنامه‌های سایبری بهره‌مند می‌شوند، ولی این کشورها در مقایسه با ایالات متحده از ساخت و توسعه ابزارهای سایبری تهاجمی تخصصی و ویژه جهت هدف گرفتن دقیق شبکه‌های نظامی و غیرنظامی دشمن محروم می‌شوند. تکاپوی روسیه در سازمان ملل برای ممنوعیت این نوع ابزارهای تخصصی نظامی و ابزارهای نسبتا ناکارآمد روسیه مانند ناتپتیا[1] که در جنگ اکراین به کار گرفت، مصداق بارز این عدم‌توازن است.

1. NotPetya

علت اصلی تمایز قدرت سایبری آمریکا از سایر کشورها این است که آمریکا از توانمندی‌های تهاجمی دقیق و تخصصی در مقیاس کلان برخوردار است که حاصل پیشگامی آن-حتی پیش از چین-در سرمایه‌گذاری در این زمینه است. مزیت دیگر توانمندی‌های سایبری تهاجمی آمریکا شامل ائتلاف و همکاری آمریکا با سایر کشورهای قدرتمند این حوزه در ساخت و به‌کارگیری این توانمندی‌هاست. با این حال، تفاوت رویکرد نظری آمریکا و توجه بیشتر آن به محدودیت‌های حقوقی و اخلاقی موجب شده‌است تا بیش از کشورهایی که چنین محدودیت‌هایی برای خود قائل نیستند در معرض حملات سایبری قرار گیرد. درواقع، به نظر می‌رسد دستیابی به اهداف راهبردی در حملات سایبری چندان هم در گرو داشتن توانمندی‌های سایبری تخصصی و دقیق نیست. چنانچه ایران و کره شمالی با استفاده از توانمندی‌های سایبری توانسته‌اند نفوذ و قدرت خود را در کشورهای همسایه گسترش دهند و کشوری مانند روسیه حتی فراتر از منطقه و به سرزمین اصلی ایالات متحده نیز نفوذ کرده و توانسته‌است با موفقیت از ابزارهای غیرتخصصی برای تحقق اهداف موردنظر خود استفاده کند. شاید به همین دلیل ایالات متحده در سال ۲۰۱۸ «ابتکار بازدارندگی سایبری»[1] را جهت مقابله با حملات سایبری دشمنان و انتقال تمرکز از شبکه‌های داخلی به شبکه‌های کشورهای متخاصم تصویب نمود.

علی‌رغم حساسیت توانمندی‌های سایبری تهاجمی، هنوز مذاکرات و توافق‌های بین‌المللی قابل‌توجهی درباره استفاده از این توانمندی‌ها انجام نگرفته‌است. مهم‌ترین هنجارهای موجود که البته الزام‌آور نیز نیستند، از سوی سازمان ملل و جهت محدود

1. Cyber Deterrence Initiative

کـردن حملـه به برخی از زیرسـاخت‌های حیاتی ملی مطرح شـده‌اند[1]. علاوه بـر این، کمیته بین‌المللی سـازمان صلیـب سـرخ در سـال ۲۰۲۰ نسـبت به تعریف اسـتفاده مسـئولانه از توانمندی‌هـای سـایبری تهاجمـی اقـدام کـرد. بـه ایـن ترتیـب، بیـن اسـتفاده تخصصی و هدفمند به‌منظور به حداقل رساندن آسیب‌های جانبی (چنانچه در بدافزار استاکس‌نت[2] رخ داد) و اسـتفاده غیرتخصصی (کنترل‌نشـده) از آسیب‌پذیری‌های فناوری‌های اطلاعاتی جهانی که می‌تواند منجر به عوارض جانبی گسترده شود (مانند مورد ناتپتیا و واناکِرای[3])، تمایز ایجاد خواهد شـد. شـکی نیسـت رسـیدن به اجماع جهانی درباره خطرات انتشـار و توسـعه کنترل‌نشده این توانمندی‌ها مستلزم گفت‌وگوهای بین‌دولتی است تا کشورها بـه راه‌حل‌هایـی خلاقانـه جهـت حفاظـت از توانمندی‌هـای ملی حسـاس ضمـن افزایش شفافیت و قانونمندی در استفاده از این توانمندی‌ها دست یابند.

منابع

یکـی از ابعـاد انـدازه‌گیری قـدرت سـایبری شـامل ارزیـابی ورودی‌هـایی ماننـد سـرمایه انسانی، میزان سرمایه‌گذاری و کیفیت فناوری‌های مورداستفاده است. این در حالی است که شـمارش دقیق تعداد نیروی انسـانی که در حوزه سـایبری فعالیت دارند، به هیچ وجه سـاده نیسـت. زیرا ارقام انتشاریافته توسط کشورها صرفا مربوط به متخصصان و افرادی اسـت کـه بـه صورت مسـتقیم و در نهادهای دولتی در حوزه سـایبری فعالیـت می‌کنند و نیروی انسانی که در بخش خصوصی حضور دارند و یا به‌طور غیرمستقیم فعالیت می‌کنند

۱. در سـال ۲۰۱۵ گروه کارشناسـان دولتی کـه از سوی مجمع عمومی سـازمان ملـل انتخـاب شـده بودنـد، دربـاره دسـتیابی به «هنجارهای اختیاری» برای رفتار دولت‌ها در فضای سایبری به توافق رسیدند. جهت مشاهده سند توافق رجوع شـود بـه:
Secretary-General, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', A/70/174, 22 July 2015, https://undocs.org/A/70/174.

2. Stuxnet

3. WannaCry

را پوشش نمی‌دهند. این مساله در بخش نظامی دشوارتر می‌شود. به‌عنوان مثال، اگرچه ایالات متحده تعداد نیروهای سایبری تخصصی در واحدهای نظامی را اعلام کرده‌است (۶۰۰۰ نفر در ستاد فرماندهی سایبری)، اما این تعداد شامل افراد فعال در بخش‌های خدمات و پشتیبانی به‌ویژه قسمت گردآوری اطلاعات نمی‌شود. در مورد چین و روسیه نیز اگرچه تعداد نیروهای حوزه جنگ اطلاعاتی آن‌ها نسبتا روشن است، اما دقیقا مشخص نیست که چه تعداد به‌صورت تخصصی در حوزه سایبری فعالیت دارند (تعداد زیادی از کارکنان این بخش در حوزه‌های اطلاعاتی متعارف و مستقل از توانمندی‌های سایبری اشتغال دارند). البته باتوجه به اسناد رسمی برنامه‌ها و راهبردهای کشورهای ایالات متحده، چین و روسیه می‌توان حدس زد که این سه کشور دارای بیشترین تعداد نیروهای متخصص در زمینه توانمندی‌های سایبری تهاجمی هستند و آمریکا به‌واسطه مشارکت جدی بخش خصوصی آن از بقیه جلوتر است.

باآنکه در جنگ سایبری تعداد بالای نیروها بسیار موثر است، اما نباید فراموش کرد که یک نیروی زبده می‌تواند ارتش ده‌هزار نفری ناکارآمدی را از پا درآورد. بنابراین، کمبودهای مهارتی برای هر دو طیف دولت‌های اقتدارگرا و لیبرال-دموکراتیک خطری جدی محسوب می‌شود. با آنکه همه کشورها به ارتقای مهارت و تخصص نیروی کار سایبری خود اهتمام دارند، ولی مطالعات بریتانیا نشان می‌دهد که وضعیت آموزش و پژوهش در دولت‌های لیبرال-دموکراتیک بسیار بهتر است و کشورهایی مانند روسیه، چین، ایران و کره شمالی نظام آموزش سایبری توسعه‌یافته‌ای ندارند.

ارزیابی قدرت سایبری کشورها از نظر میزان سرمایه‌گذاری نیز به دلایل فوق‌الذکر دشوار است. شواهد موجود نشان می‌دهند کشورهای ایالات متحده، روسیه و چین بیشترین سرمایه‌گذاری در زمینه قدرت سایبری دارند. با توجه به رشد مستمر

بخش خصوصی و دانشگاهی کشوری مانند بریتانیا و همچنین رژیم صهیونیستی به نظر می‌رسد که سرمایه‌گذاری آن‌ها در زمینه توانمندی‌های سایبری نیز به همین نسبت چشمگیر باشد.

نیروی انسانی و حجم سرمایه‌گذاری بدون تردید از عناصر مهم در میزان قدرت سایبری کشورها هستند. با این حال، اراده سیاسی و کیفیت عملیات‌های سایبری- امکان تحقق اهداف سیاسی موردنظر- نیز در توانایی دولت‌ها در بهره‌برداری از قدرت سایبری نقش بسزایی دارندکه شوربختانه در اغلب موارد قابل ارزیابی و ردیابی نیستند.

ائتلاف‌های بین‌المللی

کشورها می‌توانند ضعف‌های خود در زمینه منابع و تخصص را ازطریق پیوستن به ائتلاف‌های بین‌المللی جبران کنند. یکی از قوی‌ترین ائتلاف‌ها در این حوزه شامل ائتلاف ۶۵ ساله مشارکت اطلاعاتی پنج چشم است که همه اعضای آن از توانمندی‌های سایبری بالایی برخوردارند. گفتنی است دو کشور ژاپن و فرانسه و همچنین رژیم صهیونیستی نیز با اعضای این ائتلاف پیوندهای دوجانبه قوی دارند. در این میان چین، روسیه، ایران و کره شمالی در هیچ ائتلاف بین‌المللی قابل‌ملاحظه‌ای حضور ندارند.

تحول نظامی

بسیاری از دولت‌ها به‌طور جدی به متحول‌سازی نظریه‌ها، راهبردها و ساختارهای نظامی خود در جهت شناخت فرصت‌ها و تهدیدهای فناوری‌های سایبری اهتمام دارند. البته عوامل متعددی بر روند تحول تاثیرگذار هستند که به‌عنوان نمونه می‌توان به سطح آسیب‌پذیری سایبری در سیستم‌های موجود، ظرفیت‌های ملی صنعتی-سایبری و مهارت‌ها، میزان وابستگی به توانمندی‌های اطلاعاتی غیرنظامی، تعهد مدیران و مقاومت

نظامیان سنت‌گرا در برابر تغییر و تحول اشاره کرد. تاکنون هیچ دولتی نتوانسته‌است نیروهای نظامی خود را به‌طور کامل به توانمندی‌های سایبری یکپارچه و پیشرفته تجهیز کند. البته ایالات متحده احتمالا به بیشترین پیشرفت در این زمینه نائل شده‌است.

شوک راهبردی

توسعه فزاینده و استفاده روزافزون از توانمندی‌های سایبری در کشورهای مختلف تا حد زیادی متاثر از شوک‌های راهبردی است. اولین شوک در سال ۱۹۹۱ در جنگ خلیج‌فارس رخ داد که برای اولین بار چین و روسیه شاهد استفاده آمریکا از سلاح‌های هوشمند و با هدایت دقیق بودند. عملیات‌های آمریکا در سال ۱۹۹۹ علیه دولت یوگسلاوی نیز همین تاثیر غافلگیرکننده را برای سایر قدرت‌ها داشت. در سال ۲۰۰۳ نیز استفاده ایالات متحده از ابزارهای سایبری علیه عراق واکنش‌های گسترده‌ای را در سطح جهان برانگیخت. این موارد و بسیاری از عملیات‌های دیگر موجب افزایش نگرانی روسیه و چین نسبت به آسیب‌پذیری آن‌ها در برابر حملات سایبری شده‌اند و به‌همین دلیل نیز این کشورها به لابی‌گری در سازمان ملل برای افزایش سطح نظارت دولتی بر فضای سایبری روی آورده‌اند.

بزرگ‌ترین شوک را افشاگری‌های ادوارد اسنودن[1] به بار آورد که در سال ۲۰۱۳ از میزان قدرت و دامنه عملیات‌های ایالات متحده و متحدانش پرده برداشت. تقریبا در همان دوره روسیه و چین نیز شوک‌هایی در فضای سایبری ایجاد کردند که معروف‌ترین آن‌ها سرقت پتنت‌های صنعتی توسط چین در سال ۲۰۱۱ و مداخلات روسیه در انتخابات آمریکا در سال ۲۰۱۴ و در سطح گسترده‌تر در سال ۲۰۱۶ بودند. اتفاقاتی از این دست ایالات متحده را به سوی سیاست مشارکت مستمر و دفاع روبه‌جلو سوق داد که این

1. Edward Snowden

امـر خـود به اجرای ابتـکار بازدارندگی سـایبری و تاسیس سـازمان تحقیقـات اینترنت در آمریکا منجر شد.

تجربـه ایـران نیز مشـابه سـایر کشورهاسـت. زیرا آگاهی نسـبت به نقـش اینترنت در شکل‌گیری حرکت‌های انقلابی کشورهای عربی موسوم به بهار عربی در دوره ۲۰۱۰ تا ۲۰۱۱ و نیز برخی اغتشاشـات در خود ایران باعث شـدند این کشـور انگیزه بیشتری برای توسعه توانمندی‌های سایبری خود پیدا کند.

رتبه‌بندی

۱۴ کشور موردمطالعه و نیز رژیم صهیونیسـتی از نظر قدرت سـایبری در سـه رده بزرگ دسـته‌بندی می‌شـوند: در رده اول کشورهای پیشتاز دنیا در همه حوزه‌های موردمطالعه قـرار دارنـد. رده دوم شـامل کشورهـای پیشـتاز دنیـا در برخـی از حوزه‌هـای موردمطالعـه می‌شـود. رده سـوم نیز کشورهایی هسـتند که در چند حوزه نسـبتا قدرتمند هستند، اما در بیشـتر حوزه‌هـا ضعف دارند. جالب توجـه این‌که در کشورهای رده دوم و حتی رده اول نیز ضعف‌هایی مشاهده می‌شود، اما در مقایسه با ضعف‌های بزرگ کشورهای رده سوم چندان قابل‌ملاحظه نیست.

ایـالات متحـده بزرگ‌ترین قدرت سـایبری دنیا اسـت که از اواسـط دهه نـود رهبران آن به‌طور جدی پیشـبرد قدرت سـایبری ملی را در دستورکار خود قرار داده‌اند و از آن زمان به بعد، آمریکا به توسـعه چشـمگیر توانمندی‌های سایبری نظامی و غیرنظامی خود اهتمام ویژه‌ای داشته‌اسـت و موفق به کسـب تجارب بسیاری در زمینه عملیات‌های سـایبری و سـاخت قوی‌تریـن بنیان صنعتـی دیجیتال دنیا شده‌اسـت. در عصر حاضر، شـرکت‌های برتر در حوزه تشـخیص و شناسـایی منبع حملات سـایبری و اجرای عملیات‌های تهاجمی سـایبری تخصصـی اعـم از نظامـی و غیرنظامی متعلـق به آمریـکا هسـتند. توانمندی‌های

اطلاعاتی درجه یک با دسترسی جهانی و تکنیک‌های پیشرفته رمزنگاری (و رمزخوانی) از دیگر ابعاد قدرت سایبری آمریکا است که ائتلاف‌های قوی آن با سایر کشورهای قدرتمند موجب تقویت روزافزون آن شده‌است. اما در مقایسه با کشورهایی مانند روسیه، چین و کره شمالی، این کشور در به‌کارگیری توانمندی‌های سایبری با محدودیت‌های سیاسی و حقوقی روبروست. آمریکا می‌کوشد در کنار استفاده مسئولانه از فضای سایبری، از میزان وابستگی خود به آن جهت تامین منافع ملی امنیتی، اقتصادی و سیاسی خود بکاهد. علاوه بر این مسائل، پیچیدگی ساختار حاکمیت و فرماندهی و نظارت فضای سایبری آمریکا به‌دلیل حضور نهادهای متعدد موجب تضعیف چابکی عملیاتی و کندی فرایندهای تصمیم‌گیری آمریکا شده‌است. درمقابل، رقبای آمریکا که با اینگونه مسائل روبرو نیستند بسیار راحت‌تر می‌توانند تکنیک‌های غیرپیشرفته خود را بدون دغدغه قوانین (داخلی یا بین‌المللی) برای اهداف تخریبی و تهاجمی مختلفی به‌کار گیرند. ایالات متحده برای جبران این نقص و از بین بردن عدم‌توازن موجود در عرصه بین‌المللی درصدد ایجاد اصلاحاتی در بافتار نظری خود برآمده‌است. اتخاذ اصول مشارکت مستمر و دفاع روبه‌جلو ازجمله این اقدامات اصلاحی به شمار می‌آید. با این حال، ایالات متحده همچنان در همه حوزه‌های موردمطالعه عملکرد عالی دارد و در رده اول بی‌همتاست.

پس از آمریکا، ۶ کشور استرالیا، کانادا، چین، فرانسه، روسیه و بریتانیا و همچنین رژیم صهیونیستی در رده دوم قرار دارند. هر یک از این کشورها در چند حوزه از توانمندی‌های سایبری پیشرو هستند.

رژیم صهیونیستی و بریتانیا در مقایسه با سایر کشورهای رده دوم قدرت بالاتری در حوزه امنیت سایبری، توانمندی‌های حوزه اطلاعات سایبری (ازجمله رمزنگاری) و ساخت و استفاده تخصصی از فناوری‌های سایبری تهاجمی دارند. هر دو مورد مذکور طبق

دستورکار سیاسی خود و با بهره‌گیری از رویکرد کل جامعه نسبت به امنیت سایبری توانسته‌اند به بنیان صنعتی قوی و روبه‌رشدی دست یابند. آنها با استفاده از رویکردهای نوآورانه به تقویت ظرفیت‌های نیروی کار ماهر خود می‌پردازند. علاوه بر این، هر دو مورد دارای زیست‌بوم شرکت‌های نوپا (استارتاپ) و نوآوری-فناوری پویایی هستند. قدرت اطلاعات سایبری رژیم صهیونیستی به‌شدت در منطقه متمرکز شده‌است و البته هیچ‌یک از کشورهای منطقه رقیب جدی برای آن محسوب نمی‌شوند. اما شواهد نشان می‌دهند که توانمندی‌های بریتانیا در زمینه اطلاعات سایبری گسترده‌تر است و دسترسی‌های جهانی دارد. دو شرکت فناوری یا تله‌کام در بین ۵۱ شرکت برتر در رده‌بندی فورچون۵۰۰ در سال ۲۰۲۰ متعلق به بریتانیا بود، در حالی که هیچ‌یک از شرکت‌های رژیم صهیونیستی در این فهرست قرار نگرفته‌اند. رژیم صهیونیستی و بریتانیا در زمینه توسعه زیرساخت‌های آینده اینترنت از کشورهای ایالات متحده، ژاپن و چین عقب افتاده‌اند. از این رو، هر دو مورد با ایالات متحده، یکدیگر و سایر کشورهای توانمند در حوزه سایبری به‌منظور جبران ضعف نسبی خود در این حوزه مشارکت و همکاری می‌کنند و تاکنون چندین عملیات سایبری تهاجمی با همکاری ایالات متحده اجرا کرده‌اند.

فرانسه به‌ویژه در حوزه امنیت سایبری از قدرت زیادی برخوردار است و دسترسی اطلاعاتی وسیعی دارد. اما احتمالا فرانسه از نظر توانمندی‌های سایبری تهاجمی به‌پای ایالات متحده و بریتانیا نمی‌رسد (شگفت‌زدگی فرانسه از افشاگری اسنودن درباره سطح توانمندی‌های گروه پنج چشم خود دلیلی بر این واقعیت است). تمایز سازمانی حوزه امنیت سایبری از حوزه‌های اطلاعات سایبری و سایبری تهاجمی در فرانسه یکی از دلایل این امر است. علاوه براین، تمایل فرانسوی‌ها به حفظ استقلال ملی در حوزه اطلاعات سایبری اگرچه تا حدی پیشرفت آن‌ها را در این زمینه کند کرده‌است (تنها یک شرکت

در میان ۵۱ شرکت برتر در رده‌بندی فورچون۵۰۰ در سال ۲۰۲۰ متعلق به فرانسه بود)، اما در مقایسه با کشورهایی که بیش از حد به ائتلاف‌های بین‌المللی وابسته هستند، این موضوع می‌تواند برای فرانسه امتیاز محسوب گردد.

کانادا و استرالیا به‌ویژه از اقتصاد دیجیتال قوی و زیست‌بومی چالاک در زمینه شرکت‌های نوپای فنی برخوردار است. این کشور یکی از پیشتازان عرصه امنیت سایبری است که حاصل همکاری نزدیک بین بخش‌های عمومی و خصوصی و نیز رویکرد نوآورانه آن در پرورش مهارت‌هاست. برای کانادا و همچنین استرالیا عضویت در ائتلاف پنج چشم به‌منزله جبران کمبودهای آن‌ها در توانمندی‌های بومی است. توسعه و به‌کارگیری توانمندی‌های سایبری تهاجمی در کانادا هنوز در مراحل اولیه است، حال آنکه استرالیا از توانمندی توسعه‌یافته‌ای برخوردار است که در عملیات‌های مشترک با آمریکا و بریتانیا از آن بهره‌برداری می‌کند. استرالیا می‌کوشد بخش‌های فناوری و امنیت سایبری خود را که در مقایسه با کانادا کوچک‌تر هستند، توسعه بخشد. هیچ‌یک از این دو کشور دارای نماینده‌ای در رده‌بندی فورچون۵۰۰ در سال ۲۰۲۰ نبودند.

چین و روسیه از نظر امنیت سایبری پس از کشورهای ائتلاف پنج چشم، فرانسه و رژیم صهیونیستی قرار دارند. گزارش‌های داخلی این کشورها، رتبه پایین آن‌ها در شاخص جهانی امنیت سایبری، فشار آن‌ها بر سازمان ملل از سال ۲۰۰۳ برای اعمال کنترل دولتی بیشتر بر فضای سایبری ملی و درنهایت تلاش‌های آن‌ها برای انزوای فنی از اینترنت جهانی (از این منظر چین از روسیه جلوتر است) همگی گواه بر این ادعا هستند. ازجمله عوامل موثر در این وضعیت توسعه‌نیافتگی صنعت امنیت سایبری و بنیان ضعیف مهارتی این کشورهاست. با این حال، پس از ماجرای اسنودن در سال ۲۰۱۳ احتمال دارد هر دو کشور به توسعه مخفیانه توانمندی‌های امنیت سایبری خود پرداخته باشند،

چنانچه برخی از گزارش‌های داخلی چین در مورد وضعیت امنیت سایبری این کشور در سال‌های ۲۰۱۷ و ۲۰۱۸ نیز مؤید این نکته هستند.

روسیه و چین در زمینه توسعه توانمندی‌های سایبری تهاجمی، میزان تجربه عملیاتی در سایبری تهاجمی، دامنه گسترش جاسوسی‌های سایبری و شفافیت جهت‌گیری سیاسی و مبنای نظری از همه قدرت‌های سایبری به‌جز ایالات متحده جلوتر هستند. به‌علاوه، گفته می‌شود توانمندی‌های این کشورها در زمینه به‌کارگیری فنون سایبری برای نفوذ و سرکوب گسترده اطلاعاتی به‌عنوان بخشی از پویش‌های اطلاعاتی ضد دشمنان بی‌رقیب است. البته میزان شناسایی و ردیابی عملیات‌های سایبری روسیه و چین توسط شرکت‌های تخصصی غربی در این موضوع تردید ایجاد می‌کند. این موضوع می‌تواند دلایل مختلفی داشته باشد. به‌طور کلی، فقدان تخصص و دانش کافی آن‌ها برای اجتناب از ردیابی عملیات‌ها یا توجه کمتر این کشورها در مقایسه با گروه پنج چشم به مساله نامرئی ماندن و یا پنهان کردن تخصص‌های بالای خود در پس دامنه وسیع عملیات‌ها را می‌توان ازجمله این دلایل برشمرد. هیچ شرکتی در فهرست ۵۱ شرکت برتر فورچون۵۰۰ در سال ۲۰۲۰ متعلق به روسیه نبود، حال آنکه هشت شرکت فناوری یا تله‌کام چین در این رده‌بندی قرار داشتند و حتی تعداد آن‌ها روبه‌افزایش هست. به‌عبارت دیگر، باآنکه قدرت چین در زمینه امنیت سایبری محل تردید است، ولی این کشور تنها کشوری از رده دوم است که احتمال پیوستن آن به آمریکا در رده اول وجود دارد. البته انتظار می‌رود روند پیشرفت چین به‌دلیل اقداماتی که آمریکا از سال ۲۰۱۹ برای بستن بازارهای خود و هم‌پیمانانش به روی شرکت‌های دیجیتال چین در پیش گرفته‌است، کند شود. بااین‌حال، چین دو امتیاز کلیدی دارد: یک میلیارد نفر از ۴/۵ میلیارد کاربر اینترنت (یعنی بیشتر از مجموع کاربران ایالات متحده و اتحادیه اروپا) در چین هستند و قیمت ارزان

فناوری‌های چینی باعث شده‌است که برای کشورهای درحال‌توسعه به‌ویژه دولت‌هایی که تمایل به کنترل و نظارت داخلی دارند، جذاب باشند. چین می‌کوشد از امتیاز دوم در برنامه راه ابریشم دیجیتال[1] (در قالب ابتکار یک کمربند یک راه) بهره‌برداری کند.

هفت کشور باقیمانده در رده سوم قرار دارند که هرکدام در یک یا چند حوزه از قدرت یا ظرفیت قدرت برخوردارند، ولی در بیشتر حوزه‌ها ضعف‌های اساسی دارند. با توجه به اینکه این کشورها هر کدام دارای توانمندی‌ها و نقطه‌ضعف‌های متفاوتی هستند، رتبه‌بندی آن‌ها چندان آسان نیست و از این‌رو، در این گزارش صرفا براساس ترتیب الفبایی (انگلیسی) قرار می‌گیرند.

هند با آنکه اقتصاد دیجیتال بزرگی دارد، اما بروکراسی پیچیده آن از شتاب توسعه امنیت سایبری این کشور کاسته‌است و درنتیجه، هند رتبه پایینی در شاخص جهانی امنیت سایبری دارد. این کشور از ظرفیت‌های نسبی در حوزه‌های اطلاعات سایبری و سایبر تهاجمی برخوردار است و اولویت آن بیشتر منطقه‌ای و به‌ویژه پاکستان است. در سال‌های اخیر هند به‌منظور جبران نقاط ضعف خود می‌کوشد ازطریق همکاری با کشورهای قدرتمندی مانند ایالات متحده، بریتانیا و فرانسه و نیز مشارکت در تدوین و ارتقای هنجارها و مقررات بین‌المللی جایگاه خود در عرصه سایبری را ارتقا بخشد.

اندونزی برنامه‌های بلندپروازانه‌ای برای توسعه اقتصاد دیجیتال در دست اجرا دارد (در حال حاضر، تنها ۷۳ درصد مردم اندونزی از اینترنت استفاده می‌کنند)، اما این کشور به نسبت سایر کشورها بسیار دیر دست به‌کار شده‌است و هم‌اکنون با تهدیدهای بزرگی در زمینه جرائم سایبری و تبلیغات سایبری تروریسم مواجه است. توانمندی اندونزی در زمینه اطلاعات سایبری از نظر نظارت داخلی نسبتا توسعه یافته‌است، ولی

1. Digital Silk Road

هنـوز دسترسـی جهانـی آن در سـطح ابتدایی اسـت. سـایبری تهاجمی هنـد نیز وضعیت مشابهی دارد.

ایران تاکنون از توانمندی‌های سایبری تهاجمی برای طیف متنوعی از اهداف استفاده کرده‌است. بـه نظـر می‌رسـد ایـران بـه سـطح بالایـی از بلـوغ عملیاتی دسـت یافته‌اسـت به‌طوری که می‌تواند به خارج از منطقه و بسـیار فراتر از دایره نفوذ خود دسترسـی داشـته باشـد. توانمندی‌هـای سـایبری ایران به‌مـدد ابزارهای داخلـی مانند ارتش سـایبری ایران تقویـت شده‌اسـت. ایـران دانـش و ابزارهـای سـایبری خـود را در اختیـار شـریک خارجـی خـود نیـز قـرار می‌دهد. با این حـال، تقریبا به‌طور قطعـی می‌توان گفت ایـران همچنان به ابزارهـا و فرآیندهـای پیچیـده سـایبری تهاجمی با دقت بالای جنگی دسـت نیافته‌اسـت. به‌عـلاوه، ایـران به‌دلیل داشـتن عدم دسترسـی به فناوری‌هـای نوظهـور تهاجمی امنیت سایبری جایگاه بالایی در شاخص جهانی امنیت سایبری ندارد. وابستگی جمعیت ایران بـه اینترنـت زیـاد اسـت و رونـدی روبه‌رشـد دارد. دولـت نیز مصمم اسـت حجـم خدمات دیجیتال خود را افزایش دهد. بااین‌حال، کشـور به‌دلیل ضعف‌های فناورانه، سـازمانی و اقتصـادی هنوز تـاب‌آوری دیجیتالی لازم و آمادگی کافی برای مقابلـه با حوادث/بحران‌های احتمالـی را نـدارد. ایـران سـرمایه‌گذاری‌های عظیمی در زمینه سـاخت بسـتر اینترنت ملی انجـام داده‌اسـت کـه براسـاس مسـتندات بین‌المللی به‌نظر نمی‌رسـد تحقـق این هدف در کوتاه‌مـدت امکان‌پذیـر باشـد. درمجموع می‌تـوان گفت ایران دارای اطلاعات سـایبری قدرتمندی در سطح منطقه است که تا حدی مرهون همکاری اطلاعاتی با روسیه است.

ژاپن صنعت فناوری پیشـرفته و دیجیتال بسـیار توانمندی دارد، به‌طوری‌که دارای ده نماینـده در رتبه‌بنـدی ۵۱ شـرکت فنـاوری یـا تله‌کام فورچون۵۰۰ در سـال ۲۰۲۰ بوده‌اسـت. از ایـن رو، ژاپـن بالاتـر از همـه کشـورهای اروپایـی و چیـن قـرار می‌گیـرد و تنهـا آمریـکا

جایگاه بهتری نسبت به آن دارد. اما از آنجایی که توانمندی‌های امنیت سایبری ژاپن قوی نیست، برای جبران این ضعف به همکاری با ایالات متحده و سایر کشورها روی آورده‌است. ژاپن به دلایل محدودیت‌های قانون اساسی خود تاکنون در زمینه توسعه توانمندی‌های سایبری تهاجمی فعالیتی نداشته‌است، ولی به نظر می‌رسد اخیرا تصمیم به بازبینی الزامات قانونی کشور گرفته‌است.

مالزی اولین عضو اتحادیه کشورهای آسیای جنوب شرقی (آسه‌آن)[1] است که به‌طور جدی سیاست امنیت سایبری خود را پیگیری می‌کند و بر توسعه بخش فناوری اطلاعات و ارتباطات متمرکز شده‌است. اگرچه مالزی از نظر سیاسی در عرصه توسعه فضای سایبری بسیار فعال است، اما نقش موثری در رشد بخش فناوری اطلاعات و ارتباطات جهانی ایفا نمی‌کند. به‌علاوه، شواهد چندانی نیز مبنی بر تمایل جدی رهبران مالزی برای توسعه توانمندی‌های سایبری تهاجمی و اطلاعات سایبری وجود ندارد.

شهرت **کره شمالی** در زمینه حمله‌های سایبری به سایر کشورها بر کسی پوشیده نیست. این کشور از روش‌های مجرمانه ابتدایی برای اجرای عملیات‌های باج‌گیری و کلاهبرداری سایبری در سطح وسیع و سرقت مالکیت فکری و مرعوب ساختن سایر کشورهای منطقه به‌ویژه کره جنوبی استفاده می‌کند. کره شمالی در مواردی نیز برای تخریب عمدی (مانند حمله به شرکت سونی در سال ۲۰۱۴) و یا تخریب غیرعمدی (مانند مورد واناکرای به‌دلیل از کنترل خارج‌شدن توانمندی‌های سایبری) در سال ۲۰۱۷ از این روش‌ها استفاده می‌کند. با این وجود، کره شمالی فاقد هرگونه توانمندی در زمینه اطلاعات سایبری یا توانمندی‌های سایبری تهاجمی پیشرفته و تخصصی است و در شاخص جهانی امنیت سایبری در بین ضعیف‌ترین کشورها قرار دارد. درواقع، بنیان

1. Association of Southeast Asian Nations (ASEAN)

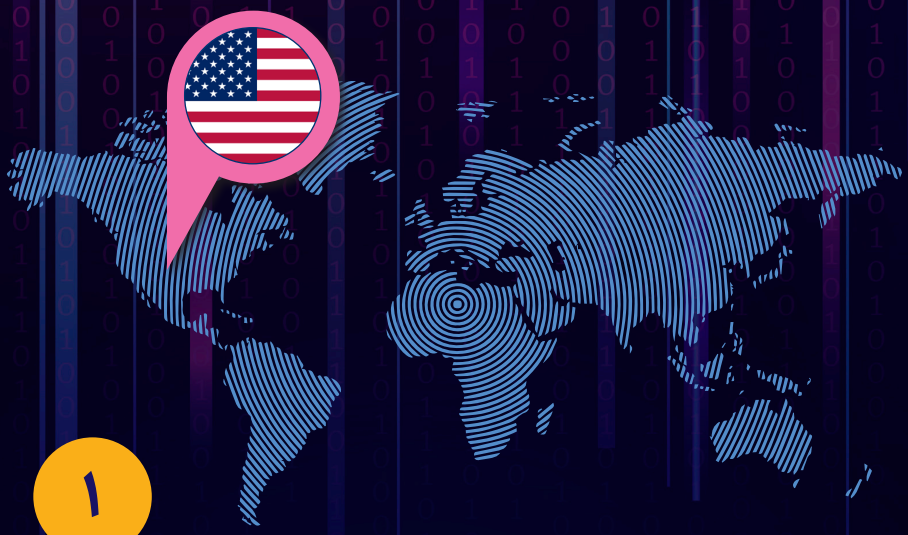
مهارتی این کشور به‌دلیل انزوای بین‌المللی ضعیف است. بااین‌حال، حداقل چهار میلیون وسیله متصل به شبکه‌های اینترنت همراه نسل سوم (3G) (برخلاف تصور عمومی) در کره شمالی وجود دارد و دولت از اینترنت برای ارائه خدمات استفاده می‌کند و برخی از زیرساخت‌های ملی آن نیز به اینترنت وابسته هستند. بااین‌حال، اتصال کشور به اینترنت جهانی محدود است و ازطریق شرکت‌های ارائه‌کننده خدمات چینی و روسیه انجام می‌شود که بسیار در معرض اختلال هستند. این بدان معناست که دولت مجبور است برای انجام هرگونه عملیات سایبری از خارج از کشور عمل کند.

ویتنام توسعه بخش فناوری اطلاعات و ارتباطات و ساخت بسترهای دولت الکترونیک را در اولویت قرار داده‌است. اگرچه در ویتنام سیاست‌های مربوط به امنیت سایبری منتشر شده و ساختارهای امنیت سایبری پایه ایجاد شده‌اند، اما عدم انتشار راهبرد جامع امنیت سایبری ملی باعث تضعیف مشارکت همگانی ذینفعان کلیدی و اطلاع‌رسانی عمومی شده‌است. به‌دلیل بودجه محدود و کمبود شدید استعدادهای سایبری در ویتنام، سازمان‌های دولتی هنوز با مشکلات زیادی در زمینه امنیت سایبری روبرو هستند. ترس حزب حاکم کمونیست از نیروهای برانداز داخلی موجب شده‌است دولت منابع را از آموزش مهارت‌های فنی سایبری به‌سمت کارهای ایدئولوژیکی و مدیریت افکار عمومی هدایت کند و درنتیجه، تمرکز خود بر توسعه توانمندی‌های سایبری اعم از دفاعی یا تهاجمی را کاهش دهد.

پیشرفت کشورها

از بین تمام عواملی که می‌توانند به ارتقای کشورها در رده‌بندی سه‌گانه کمک کنند، توانمندی در صنایع فناوری اطلاعات و ارتباطات بیشترین تاثیرگذاری را دارد و به همین دلیل، چین درصورت ادامه مسیر کنونی و مشروط بر اینکه نقاط ضعف خود در زمینه

امنیـت سـایبری را برطـرف کنـد، از بهترین موقعیت برای پیوسـتن به آمریـکا در رده اول برخـوردار اسـت. به‌همیـن ترتیب، ژاپـن نیز با وجود همـه نقاط ضعفی کـه دارد (که البته بایـد بـر آن‌ها فائق آید)، بهترین کشـور در رده سـوم اسـت که می‌تواند جایـگاه خود را به رده دوم ارتقا بخشد.



۱

ایالات متحده آمریکا

از اواسط دهه پایانی قرن بیستم تسلط در فضای سایبری از اهداف راهبردی ایالات متحده آمریکا به‌شمار می‌رود. گرچه امروز آمریکا خود را در معرض تهدید جدی روسیه و چین در فضای سایبری می‌داند، اما همچنان تنها کشوری است که بیشترین اثرگذاری جهانی را از نظر کاربردهای نظامی و غیرنظامی فضای سایبری دارد. آمریکا در پاسخ به شرایط موجود با جدیت در پی گسترش توانمندی‌های سایبری خود در زمینه امنیت سیستم‌های داخلی و پیشبرد مقاصد اقتصادی، سیاسی، دیپلماتیک و نظامی خود در خارج از مرزهاست. هم‌اکنون، ایالات متحده در زمینه توانمندی‌های حوزه فناوری اطلاعات و ارتباطات برتری کامل بر سایر کشورها دارد، اگرچه قدرت مطلق محسوب نمی‌شود. درواقع در شرایط کنونی، حداقل شش کشور اروپایی و آسیایی در چند حوزه از فناوری اطلاعات و ارتباطات پیشرو هستند که همگی به‌غیر از چین در شمار هم‌پیمان‌های نزدیک یا شرکای راهبردی ایالات متحده قرار دارند. آمریکا علاوه بر برخورداری از جایگاه برتر علمی و فناورانه، در مقایسه با سایر کشورها اقدامات موثرتری نیز برای حفاظت از زیرساخت‌های بنیادین ملی در فضای سایبری انجام داده‌است. این کشور درک خوبی از اهمیت اساسی این موضوع و ضعف‌های خود در فضای سایبری دارد و از همین رو، بیش از دو دهه است که برای بسیج جامعه جهانی جهت توسعه اصول امنیتی مشترک در فضای سایبری می‌کوشد. با توجه به شواهد موجود می‌توان گفت ایالات متحده در اجرای عملیات‌های سایبری تهاجمی احتمالا ظرفیت بسیار بیشتری در مقایسه با سایر کشورها دارد، اما ظرفیت واقعی آن هنوز به‌طور کامل بالفعل نشده‌است.

راهبرد و مبنای نظری (دکترین)

ایالات متحده طی سی سال اخیر توانسته‌است راهبردهای ملی استواری در زمینه دفاع و امنیت فضای سایبری تدوین کند که به‌طورکلی سه جهت‌گیری متفاوت دارند: دفاع داخلی، تعارض نسبی با رقبا و جنگ تمام‌عیار با دشمنان. بخش‌هایی از اسناد «راهبرد امنیت ملی ایالات متحده (۲۰۱۷)»[۱]، «راهبرد سایبری ایالات متحده (۲۰۱۸)»[۲] و «راهبرد سایبری وزارت دفاع (۲۰۱۸)»[۳] درباره این جهت‌گیری‌ها هستند که به‌وسیله هزاران صفحه بیانیه خط‌مشی و کتابچه‌های راهنمای نظری تبیین شده‌اند.

همزمان با پیشبرد راهبردهای امنیت ملی، ایالات متحده از همان اواسط دهه نود تحقق سیاست امنیت سایبری بخش غیرنظامی را نیز در دستورکار قرار داد که در آغاز بیشتر روی مقابله با جرائم سایبری و پیشگیری از خسارت به شرکت‌ها تمرکز داشت. به‌عنوان نمونه، راهبرد رسمی ایالات متحده در سال ۲۰۱۸ با انواع بیانیه‌های سیاسی، برنامه‌های عملیاتی و تصمیم‌ها و فرمان‌های حکومتی (حتی در روزهای پایانی ریاست‌جمهوری ترامپ) پشتیبانی و تبیین شده‌است[۴]. درواقع، آمریکا طی سه

۱. رجوع شود به:
White House, 'National Security Strategy of the United States of America', December 2017, https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

۲. رجوع شود به:
White House, 'National Cyber Strategy of the United States of America', September 2018, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

۳. رجوع شود:
US Department of Defense, 'Summary: Department of Defense Cyber Strategy 2018', https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

۴. رجوع شود:
White House, 'Executive Order on Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities', 19 January 2021, https://trumpwhitehouse.archives.gov/presidential-actions/executiveorder-takingadditional-steps-address-national-emergencyrespect-significant-malicious-cyber-enabled-activities

دهـه گذشـته توجـه شـدید و فزاینـده‌ای بـه حفاظـت از زیرسـاخت‌های حیاتـی اطلاعاتی خـود داشته‌اسـت (منظـور همان زیرسـاخت‌هایی اسـت کـه در دیگر کشـورها به‌عنوان «زیرسـاخت حیاتـی» و یـا ماننـد بریتانیـا به‌عنـوان «زیرسـاخت حیاتـی ملـی» شـناخته می‌شـوند)[1]. در همین راسـتا، آمریکا ذینفعان کلیدی (کسـب‌وکارها، دانشـگاه‌ها، دولت و بخـش خصوصـی و غیـره) را به‌طور موثری برای رویارویی ملی بـا چالش‌های حوزه منابع انسانی و فنی امنیت سایبری بسیج کرده‌است. آمریکا در این زمینه بر حذف شکاف‌های موجـود در حـوزه افشـای اسـرار دولتـی، سـرقت امـوال دارای مالکیت فکـری، مداخلات خارجـی در سیاسـت‌های کشـور و عملکـرد ضعیـف بسـیاری از بخش‌هـای اقتصـادی و اجتماعی از نظر امنیت سـایبری تمرکز داشته‌است.

هـدف ایـالات متحـده در عرصـه نظامـی به‌کارگیری حمله سـایبری در همه سـطح‌های عملیاتـی و فرماندهـی اسـت و در حـوزه دفاعی نیز این کشـور قصد دارد دفاعی گسـترده، اسـتوار و تاب‌آور داشـته باشـد[2]. با این‌که آمریکا در هر دو حوزه پیشتاز است، اما احتمال آسـیب‌پذیری آن در صـورت بـروز حمله سـایبری به‌دلیل وابسـتگی شـدید دیجیتالی این کشـور بالاسـت. بـه عبـارت دیگـر، تحقق دفـاع سـایبری جامع و مطلـق برای آمریـکا-و هر کشور دیگری-اگر غیرممکن نباشد، بسیار دشوار است[3].

۱. اصطلاح زیرساخت‌های اطلاعاتی حیاتی در مفهوم عام به همه سامانه‌های اطلاعاتی زیرساخت‌های حیاتی ملی گفته می‌شود.

۲. رجوع شود به:
United States Cyber Command, 'Beyond the Build: Delivering Outcomes through Cyberspace - The Commander's Vision and Guidance for US Cyber Command' 2015,
https://nsarchive2.gwu.edu/dc.html?doc=2692135-Document-27

۳. در اظهارات اعضای پنتاگون در سال ۲۰۱۵ به عوامل جدیدی اشاره شده‌است که در متن گزارش «ورای ساخت» نیـز موجـود اسـت؛ ازجملـه اینکـه «دفـاع سـایبری وزارت دفـاع در برابـر تهدیدهـای موجـود عملکـرد مناسـبی نـدارد» و اینکـه «واحدهـای نظامـی مجبورنـد بـا تجهیـزات قدیمـی و اطلاعـات موقعیتـی سـایبری ناکافـی (شـامل نظـارت و فرماندهـی، داده‌هـای هدف‌گیـری و اطلاعـات) کار کننـد».

راهبرد بین‌المللی ایالات متحده به نقل از گفته‌های رهبران سیاسی و نظامی[۱] آن دستیابی به برتری در عرصه سایبری و حفظ این برتری است[۲]. جزئیات این رویکرد را در راهبرد سایبری وزارت دفاع (۲۰۱۸) می‌توان یافت[۳] که مشتمل بر تعیین اهداف کوتاه‌مدت، شناسایی نقاط ضعف دفاعی و تهاجمی و تاکید بر ارتقای حداکثری مزیت‌های نظامی و اطلاعاتی کنونی می‌شود.

با توجه به اینکه اثر اصلی برنامه‌ریزی جامع و دقیق برای عملیات‌های سایبری در بسیج همه منابع بالقوه در سطح ملی و در شرایط عادی و فوریت‌ها تجلی می‌یابد، ایالات متحده در مقایسه با سایر کشورها بهترین وضعیت را از این نظر دارد. سیاست‌ها و برنامه‌های جامع آمریکا به‌خوبی تدوین و تبیین شده‌اند و با مشارکت بخش‌های وسیعی از نیروهای مسلح و دولت، کسب‌وکارها، اصحاب دانشگاه و جامعه مدنی تهیه و اجرا می‌شوند. راهبردهای سایبری آمریکا ضمن تایید روند پرشتاب تحول و تغییر فضای سایبری بر پیچیدگی استفاده از نقاط ضعف دشمنان نیز تاکید دارند.

یکی از بخش‌های کلیدی راهبرد سایبری وزارت دفاع (۲۰۱۸) شامل «ابتکار بازدارندگی سایبری» است که بر همکاری نزدیک آمریکا با متحدانش در واکنش به حمله‌های سایبری، شناسایی مبدا حمله‌ها، صدور بیانیه‌های عمومی در حمایت از اقدام‌های

۱. رجوع شود به:
United States Cyber Command, 'Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command',
https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010

۲. وزارت دفاع بایستی جهت حفظ برتری نظامی و منافع ایالات متحده روزانه در رقابت با رقبا به فعالیت‌های سایبری بپردازد. تمرکز ما روی دولت‌هایی است که تهدید راهبردی برای امنیت و رشد کشور محسوب می‌شوند به‌ویژه روسیه و چین. عملیات‌های سایبری به‌منظور گردآوری اطلاعات انجام می‌شوند و همزمان آمادگی توانمندی‌های سایبری برای انجام عملیات در صورت وقوع بحران یا منازعه حفظ می‌گردد. رجوع شود به:
US Department of Defense, 'Summary: Department of Defense Cyber Strategy 2018', p. 1:

۳. رجوع شود به:
White House, 'National Cyber Strategy of the United States of America', September 2018, p. 21.

انجام شده و اتخاذ رویکرد مشترک در پاسخ به عاملان حمله‌ها متمرکز است. باآنکه راهبرد ملی سایبری روش‌های غیرسایبری را نیز در مقابله‌به‌مثل با حمله‌های سایبری به‌رسمیت می‌شناسد، اما راهبرد سایبری وزارت دفاع (۲۰۱۸) تاکید جدی بر نقش عملیات‌های سایبری در دفاع از منافع کشور دارد که شامل رویکرد دفاع روبه‌جلو در شبکه‌های متخاصم جهت پیشگیری از حمله و رقابت مستمر با اپراتورهای این شبکه‌ها نیز می‌شود.

حکمرانی، فرماندهی و نظارت

ایالات متحده یکی از پیشگامان حکمرانی چندذینفعی امنیت در فضای سایبری محسوب می‌شود که برآیند نظام لیبرال آمریکا و اراده جدی بخش خصوصی آن در مخالفت با کنترل دولتی کسب‌وکارها است. حضور جدی بخش خصوصی آمریکا در امر حکمرانی، ارتقای امنیت زیرساخت‌های حیاتی کشور که اغلب در مالکیت خصوصی نیز هستند را در پی داشته‌است. علاوه براین، دولت فدرال به ۵۱ ایالت کشور مسئولیت‌های قابل‌ملاحظه‌ای در تامین امنیت سایبری ملی و مقابله با جرائم سایبری و ارائه خدمات آموزشی محول کرده‌است.

نهادهای متنوعی در اجرای سیاست‌های سایبری ایالات متحده دخیل هستند که همگی ذیل ریاست جمهوری فعالیت دارند. جامعه اطلاعاتی، نیروهای مسلح، وزارت‌های فدرال (امنیت داخلی، دفاع، دادگستری، بازرگانی، انرژی و حمل‌ونقل) و سایر نهادها مانند آزمایشگاه‌های ملی ازجمله این نهادها به شمار می‌آیند. شورای امنیت ملی (NSC)[1] به ریاست رئیس‌جمهور و کمیته رؤسا[2] به ریاست مشاور امنیت ملی وظیفه

1. National Security Council
2. Principals Committee

هماهنگ‌سازی فعالیت‌های همه این بازیگران را برعهده دارند[۱].

امور سیاست‌گذاری امنیت سایبری غیرنظامی آمریکا در دو مجرا انجام می‌گیرد: مجرای اول، در کاخ سفید این امر وظیفه مدیر سایبری ستاد شورای امنیت ملی است. رئیس‌جمهور نیز به‌طور مستقیم از مشاور امنیت داخلی (تحت‌نظارت مشاور امنیت ملی) و قائم‌مقام (دستیار) مشاور امنیت ملی در حوزه امنیت سایبری و فناوری‌های نوظهور مشورت می‌گیرد[۲]. مجرای دوم، وزیر امنیت داخلی ایالات متحده که از اعضای دائمی شورای امنیت ملی به شمار می‌رود، مسئولیت سیاست‌گذاری امنیت سایبری غیرنظامی در خارج از کاخ سفید را برعهده دارد. سازمان امنیت سایبری و امنیت زیرساخت‌ها (CISA)[۳] نیز در سال ۲۰۱۸ توسط وزارت امنیت داخلی جهت تقویت این حوزه راه‌اندازی شده‌است.

همه این نهادها در اجرای وظایف خود پیرو سیاست بسیج منابع بخش‌های خصوصی و دولتی و همکاری نزدیک این دو هستند. یکی از ابزارهایی که در این راستا به کار می‌رود شامل شورای مشورتی زیرساخت‌های ملی[۴] (زیرمجموعه ریاست‌جمهوری) است که

۱. کمیته رؤسا، اجلاس بین‌سازمانی بالادستی است که به مسائل خط‌مشی تاثیرگذار بر امنیت ملی رسیدگی می‌کند. اعضای آن اغلب شامل وزیر کشور، وزیر خزانه‌داری، وزیر دفاع، دادستان کل، وزیر انرژی، وزیر امنیت داخلی، رئیس سازمان برنامه و بودجه، نماینده آمریکا در سازمان ملل، مدیر سازمان توسعه بین‌المللی ایالات متحده و رئیس ستاد ریاست جمهوری می‌شود. مدیر اطلاعات ملی، رئیس ستاد مشترک و رئیس سازمان سیا در قالب مشاور در این کمیته می‌توانند حاضر شوند. علاوه بر این، کمیته می‌تواند معاون ارشد مشاور امنیت ملی، مشاور رئیس‌جمهور و مشاور امنیت ملی رئیس‌جمهور و مشاور حقوقی شورای امنیت ملی را به همه جلسات دعوت کند». رجوع شود به:
White House, 'Memorandum on Renewing the National Security Council System', 4 February 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/02/04/memorandumrenewing-the-national-security-council-system

۲. رجوع شود به:
Ibid. and Natasha Bertrand 'Biden taps intelligence veteran for new White House cybersecurity role', Politico, 6 January 2021, https://www.politico.com/news/2021/01/06/biden-white-house-cybersecurity-neuberger-455508.

3. Cybersecurity and Infrastructure Security Agency

4. National Infrastructure Advisory Council

مدیران اجرایی ارشد از بخش خصوصی، دولت فدرال و دولت‌های ایالتی را گرد هم می‌آورد تا برای کاهش خطرات سایبری و فیزیکی و بهبود امنیت و تاب‌آوری زیرساخت‌های حیاتی ملی هم‌اندیشی کنند[۱]. نهادهای ذی‌ربط امنیتی تاکنون ابتکارهای راهبردی متنوعی مطرح و اجرا کرده‌اند: مراکز اشتراک و تحلیل اطلاعات (ISACs)[۲] که اولین نمونه آن‌ها در سال ۲۰۰۹ در دولت بیل کلینتون بنیان‌گذاری شد، چارچوب بازبینی خطر و تاب‌آوری سایبری[۳] که توسط وزارت کشور و دانشگاه کارنگی ملون[۴] اجرا شد و ابتکار ملی آموزش امنیت سایبری[۵] که سازمانی زیرمجموعه موسسه ملی استاندارد و فناوری[۶] وزارت بازرگانی است.

ایالات متحده سرمایه‌گذاری‌های سنگینی برای توسعه فرماندهی و نظارت در عملیات‌های سایبری انجام داده‌است که بیشتر در دو حوزه متمرکز هستند: از میان برداشتن شکاف‌های سیاستی ازطریق ایجاد سازمان‌ها یا پست‌های جدید و تمرکززدایی تدریجی اختیارات در عملیات‌های دفاعی سایبری. تنها در سال ۲۰۲۱ دولت قریب به ۱۸/۷ میلیارد دلار برای ابتکارهای ویژه امنیتی از کنگره درخواست کرد[۷].

در اجرای سیاست‌های امنیت ملی سایبری آمریکا، نهادها و سازمان‌های مختلفی جهت تایید، فرماندهی و نظارت مشارکت دارند که به غیر از کاخ سفید و وزارت امنیت داخلی

---

۱. رجوع شود به:

CISA, 'National Infrastructure Advisory Council',
https://www.cisa.gov/niac

2. Information Sharing and Analysis Centers

برای اطلاعات بیشتر رجوع شود به وب‌سایت شورای ملی:

https://www.nationalisacs.org

3. Cyber Risk and Resilience Review
4. Carnegie Mellon University
5. National Initiative for Cybersecurity Education
6. National Institute of Standards and Technology

۷. رجوع شود به:

Office of Management and Budget, 'A Budget for America's Future: Analytical Perspectives', Washington DC, 2020, p. 265,
https://www.govinfo.g.ov/content/pkg/BUDGET-2021-PER/pdf/BUDGET-2021-PER.pdf.

مهم‌ترین آن‌ها عبارتند از: وزارت دفاع (شامل سازمان امنیت ملی (NSA) و ستاد فرماندهی سایبری)، اداره مدیریت اطلاعات ملی (ODNI)[1] که همه سازمان‌های اطلاعاتی کشور را هماهنگ می‌کند و سازمان مرکزی اطلاعات (سیا)[2] که به‌طور مستقیم به رئیس‌جمهور پاسخ‌گو است و به‌طور هماهنگ با اداره مدیریت اطلاعات ملی فعالیت می‌کند.

در حوزه فرماندهی و نظارت امنیت سایبری نظامی همه مناسبات مشابه سایر فعالیت‌های نظامی است، به‌طوری که رئیس‌جمهور فرمانده کل قواست و ستاد مشترک و نیروهای زمینی، هوایی، دریایی و زیردریایی همگی به‌طور مستقیم تحت‌نظارت او فعالیت دارند. البته وظایف فرماندهی کل قوا توسط وزارت دفاع و ازطریق نهادی به نام مرجع فرماندهی ملی[3] انجام می‌شوند.

در دوره باراک اوباما اجرای عملیات‌های سایبری تهاجمی مستلزم تایید مراجع مختلف و حکم ریاست‌جمهوری بود، اما در دوره ترامپ با افزایش حجم حمله‌های سایبری به آمریکا، او ابتکار بازدارندگی سایبری را مطرح کرد و طی حکمی محرمانه اختیار اجرای عملیات‌های سایبری تهاجمی را به نهادهای مختلف سایبری واگذار کرد.

در وزارت دفاع آمریکا سازمان‌های سایبری متعدد و با مسئولیت‌ها و وظایف مختلفی وجود دارد: ستادهای ویژه (تک‌ماموریتی) فرماندهی سایبری و افسر ارشد اطلاعات که مسئولیت تامین امنیت همه سیستم‌های رایانه‌ای (به استثنای پلتفرم‌های تسلیحاتی که توسط ستادهای ویژه فرماندهی یا فرماندهی جنگ مدیریت می‌شوند) را برعهده دارد.

به‌طور کلی، حکمرانی سیاست سایبری آمریکا از غنای بالایی از نظر تنوع ذینفعان و استعدادها برخوردار است و درنتیجه، در مقایسه با نظام‌های متمرکز در ایالات متحده

1. Office of the Director of National Intelligence
2. Central Intelligence Agency (CIA)
3. National Command Authority

تصمیم‌گیری درباره عملیات‌های سایبری مستلزم اتفاق آرای ذینفعان مختلف است. علاوه براین، در ایالات متحده قانون به‌شدت بر عرصه سایبری نظارت دارد و درنتیجه نظام سایبری آن بسیار قابل‌پیش‌بینی و البته محدودتر از نظام‌هایی است که قوانین محکمی در این رابطه ندارند. همچنین، امور فرماندهی و نظارت با جزئیات دقیق و با پشتیبانی اطلاعاتی قوی انجام می‌شوند.

توانمندی‌های محوری در زمینه اطلاعات سایبری

شواهد بسیار زیادی درباره تخصص پیشرو، دامنه و عمق بی‌نظیر توانمندی‌های محوری ایالات متحده در زمینه اطلاعات سایبری وجود دارد که بیشتر در ارتباط با توانمندی‌های سایبری با محوریت نظامی سازمان امنیت ملی، توانمندی‌های سایبری با محوریت غیرنظامی سازمان سیا (دامنه عمل آن خارج از مرزهاست) و توانمندی‌های اداره فدرال تجسس (سازمان اِف‌بی‌آی)[1] -مسئول امنیت داخلی- هستند.

ریاست سازمان امنیت ملی و ستاد فرماندهی سایبری ارتش ایالات متحده مشترک است و درنتیجه، این دو سازمان که کارکردهای سایبری تهاجمی، امنیت سایبری و اطلاعات سایبری دارند در نهایتِ هماهنگی و همکاری نزدیک با هم فعالیت می‌کنند. توانمندی‌های ایالات متحده با ائتلاف‌های بین‌المللی مانند ائتلاف پنج چشم که مهم‌ترین و قدرتمندترین ائتلاف سایبری دنیاست، بیش از پیش تقویت می‌شوند.

علاوه براین، سازمان‌های اطلاعاتی آمریکا همکاری‌های گسترده‌ای با شرکت‌های بخش خصوصی و دانشگاه‌ها در زمینه ساخت و توسعه فناوری‌های کلیدی

1. FBI Federal Bureau of Investigation

دارند[۱]. به‌منظور درک عمق و دامنه درهم‌تنیدگی فعالیت‌های نظامی-سایبری و خصوصی-دولتی آمریکا می‌توان به گزارش فرهنگستان‌های علوم، مهندسی و پزشکی این کشور (مارس ۲۰۱۹) رجوع کرد که درباره رویکردها و اقداماتی است که جامعه اطلاعاتی می‌تواند برای تطبیق با/یا بهره‌برداری از فناوری‌های به‌شدت متغیر اتخاذ کند[۲]. شواهد نشان می‌دهند یکپارچگی دولت، صنعت و دانشگاه در ساخت توانمندی‌های اطلاعاتی ایالات متحده از نظر عمق، دامنه و سرمایه‌گذاری با هیچ کشوری حتی چین قابل‌قیاس نیست.

بودجه درخواستی ۸۵ میلیارد دلاری برای سال ۲۰۲۱ و حضور چندین وزارت‌خانه علاوه بر سه سازمان اطلاعاتی اصلی در امور اطلاعات سایبری آمریکا دال بر این است که اندازه و پیچیدگی جامعه اطلاعات و امنیت آن بسیار گسترده است و لذا، هماهنگی امور سایبری آمریکا حتی پس از تشکیل اداره ملی مدیریت اطلاعات نیز دشوار است و یکی از چالش‌های جدی آن در عرصه سایبری محسوب می‌شود.

توانمندی و وابستگی سایبری

ایالات متحده از نظر ظرفیت فناوری اطلاعات و ارتباطات (اعم از اندازه و اقتصاد دیجیتال، نقش آن در نوآوری جهانی و مشارکت دولت و صنعت و دانشگاه) در دنیا بی‌نظیر است. تقاضای فزاینده جهانی برای مصرف محصولات/خدمات فناوری اطلاعات و

۱. رجوع شود به:
Director of National Intelligence, 'Industry Snapshot: Summary of Partner Responses to the FY 2015-2019 IC S&T Investment Landscape', 2015, p. 5,
http://www.dni.gov/files/documents/atf/In-STeP%20-%20Industry%20Snapshot.pdf

۲. رجوع شود به:
National Academies of Sciences, Engineering, and Medicine, 'A Decadal Survey of the Social and Behavioral Sciences: A Research Agenda for Advancing Intelligence Analysis', 2019,
https://www.nap.edu/catalog/25335/a-decadal-survey-of-thesocial-and-behavioral-sciences-a

ارتباطات ایالات متحده، موفقیت تجاری بی‌سابقه شرکت‌هایی مانند اپل، مایکروسافت و گوگل را در پی داشته‌است که آن‌ها نیز به‌نوبه خود با سرمایه‌گذاری‌های عظیم در تحقیق و توسعه پیشران شکل‌گیری آینده فضای سایبری هستند و امروزه شاهد وابستگی جهانی شدید به محصولات بازرگانی و مالکیت فکری آمریکا مانند فناوری‌های حوزه ریزتراشه‌های رایانه‌ای، کابل‌های مخابراتی زیردریایی، ماهواره‌های مخابراتی و رایانش ابری هستیم.

اما روی دیگر سکه، وابستگی زیاد زیرساخت‌های اقتصادی و مدنی ایالات متحده -در مقایسه با سایر کشورها- به فناوری‌های دیجیتال است که آسیب‌پذیری آن را در بسیاری ابعاد افزایش می‌دهد[1]. آمریکا بزرگ‌ترین اقتصاد دیجیتال دنیا را دارد و از منظر استفاده شخصی و تجاری از اینترنت یکی از کشورهای پیشرو است. سطح بالای تقاضا در این کشور محرک نوآوری بیشتری می‌شود که این امر نیز به‌نوبه خود موجب افزایش تقاضا می‌شود.

آمار ارائه شده توسط اداره تحلیل اقتصادی آمریکا[2] نشان می‌دهند اقتصاد دیجیتال ۹ درصد از تولید ناخالص داخلی این کشور را در سال ۲۰۱۸ تشکیل می‌داد. اما این آمار خروجی عظیم بخش‌هایی مانند خدمات مالی که با استفاده از محصولات و خدمات فناوری اطلاعات و ارتباطات ثروت هنگفتی تولید می‌کنند را شامل نمی‌شود. به‌عبارت

۱. به‌عنوان مثال طبق گزارش سازمان همکاری اقتصادی و توسعه، ایالات متحده در بین کشورهای این سازمان کمترین سهم (۱۲ درصد) ارزش افزوده خارجی از تقاضای داخلی را دارد. درواقع، ایالات متحده بزرگ‌ترین مصرف‌کننده ارزش افزوده خارجی صرفا براساس ارزش دلاری اقتصاد این کشور است: ۲/۲ تریلیون دلار که ۵۵ درصد این میزان مربوط به صنایع دیجیتال می‌شود. برای کسب اطلاعات بیشتر رجوع شود به:
OECD, 'Measuring the Digital Transformation', March 2019, p. 228,
https://www.oecdilibrary.org/sites/a87fd918en/index.html?itemId=/content/component/a87fd918-en#:~:text=However%2C%20while%20the%20United%20States,comes%20from%20more%20digital%2Dintensive

2. Bureau of Economic Analysis

دیگر، تنها با تکیه بر آمار متعارف خروجی‌های مستقیم فناوری اطلاعات و ارتباطات نمی‌توان حجم واقعی اقتصاد دیجیتال آمریکا را برآورد کرد[۱]. سایر بخش‌های اقتصاد مانند کشاورزی و سلامت از محصولات و خدمات فناوری اطلاعات و ارتباطات به نحوی برای تولید ثروت و نوآوری استفاده می‌کنند که قابل ردیابی در آمار ملی بخش فناوری اطلاعات و ارتباطات نیست[۲]. به‌عنوان مثال، یکی از محبوب‌ترین فناوری‌ها تجارت الگوریتمی سهام، ارز و اوراق بهادار است که اساسا بدون خدمات و محصولات فناوری اطلاعات و ارتباطات امکان‌پذیر نیست. این ثروت‌آفرینی پرسرعت و مبتنی بر فناوری‌های خودکار، آمریکا را به مرکز جهانی سرمایه‌داری دیجیتال تبدیل کرده است[۳]، به‌طوری که براساس تعریف گروه ۲۰[۴] درباره اقتصاد دیجیتال، سهم آمریکا از اقتصاد دیجیتال جهانی ۶۰ درصد است[۵].

۱. رجوع شود به:
Jessica R. Nielsen, 'New Digital Economy Estimates', Bureau of Economic Analysis, August 2020, https://www.bea.gov/system/files/2020-08/New-Digital-Economy-Estimates-August-2020.pdf

۲. رجوع شود به:
Erik Brynjolfsson and Avinash Collis, 'How Should We Measure the Digital Economy?', Harvard Business Review, November-December 2019, https://hbr.org/2019/11/how-should-we-measure-the-digital-economy.

۳. رجوع شود به:
US Federal Reserve, 'Fedwire Funds Service Monthly Statistics', https://www.frbservices.org/resources/financial-services/wires/volume-value-stats/monthly-stats.html

۴. رجوع شود به:
Dan Schiller, Digital Capitalism: Networking the Global Market System (Cambridge, MA: MIT Press, 2000)

۵. به عنوان نمونه رجوع شود به:
G20, 'G20 Digital Economy Development and Cooperation Initiative', 8 September 2016, http:// www.g20chn.org/English/Documents/Current/201609/P020160908736971932404.pdf.
طبق تعریف ارائه شده توسط گروه ۲۰ در سال ۲۰۱۶، اقتصاد دیجیتال عبارت است از طیف وسیعی از فعالیت‌های اقتصادی که مستلزم استفاده از دانش و اطلاعات دیجیتالی به‌عنوان عامل اصلی تولید و شبکه‌های اطلاعاتی جدید به‌عنوان فضای فعالیت است. سازمان همکاری اقتصادی و توسعه نیز در گزارش‌های متعددی به مساله ارزیابی و مقایسه اقتصاد دیجیتال کشورها پرداخته‌است که می‌توان به گزارش سال ۲۰۱۹ اشاره کرد:
Measuring the Digital Transformation: A Roadmap for the Future', 11 March 2019, https://www.oecd-ilibrary.org/docserver/9789264311992-en.pdf?expires=1595284992&id=id&accname=guest&checksum=DC8358091A60B496B5A6F525ECD799E6

بنابراین، برخی از کشورها ازجمله چین سودای رسیدن به این سطح از توانمندی و قدرت را دارند. طبق تحلیل‌های سازمان همکاری اقتصادی و توسعه بین سال‌های ۲۰۱۳ و ۲۰۱۶، چین و پنج کشور دیگر یعنی ایالات متحده، تایوان، ژاپن و کره جنوبی ۷۰ تا ۱۰۰ درصد کل پتنت‌های ۲۵ فناوری[۱] که به‌عنوان مرزهای فناوری دیجیتال شناخته می‌شوند را در اختیار داشته‌اند. البته سهم جهانی ایالات متحده در تولید همه این فناوری‌ها به استثنای دو مورد (وسیله‌های مبتنی بر مواد ارگانیک و تجهیزات کنترل) از چین بیشتر است[۲].

قدرت دیجیتال آمریکا درواقع ریشه در فرهنگ تخصص فنی و سرمایه‌گذاری نوآوری‌محور آن دارد. آمریکا میزبان ۵۹ دانشگاه از فهرست ۲۰۰ دانشگاه برتر رتبه‌بندی آموزش عالی تایمز[۳] است (جدول ۱) و محیط فناوری و کارآفرینی آن در دنیا نظیر ندارد. براساس یکی از مطالعات صنعتی، تعداد شرکت‌های نوپای ثبت‌شده در آمریکا در سال ۲۰۱۹ برابر با ۶۵,۳۲۱ شرکت بوده که ۹ برابر شرکت‌های نوپای هند یعنی دومین کشور این رده‌بندی است[۴].

---

۱. گزارش سازمان همکاری اقتصادی و توسعه با عنوان «ارزیابی تحول دیجیتال» نشان می‌دهد که این ۲۵ فناوری عبارتند از: تجهیزات کنترل، وسیله‌های مواد ارگانیک، انتقال داده دیجیتال، ذخیره دیجیتال متنوع، الگوریتم‌های مدل‌های زیستی، دسترسی کانال بی‌سیم، کنترل ترافیک در هواپیما، انتقال‌های چندگانه، تجهیزات سنکرون، کنترل ترافیک در خودروها، وسیله‌های فیلم، تلویزیون تعاملی، شبکه VOD و محدودیت‌های دسترسی، تحلیل صدا یا کلام، مدیریت ارتباط، سایر مدل‌های محاسباتی، به‌کارگیری اشیای سه‌بعدی، بازتاب امواج الکترومغناطیسی، خدمات ارتباطات بی‌سیم، تحلیل تصویر، الگوریتم‌های مدل‌های ریاضی، تجهیزات انتقال، سامانه‌های انتقال نزدیک به میدان، پروتکل‌های پرداخت و امنیت و تایید هویت.

۲. رجوع شود به:

Longmei Zhang and Sally Chen, 'China's Digital Economy: Opportunities and risks', International Monetary Fund Working Paper, no. WP/19/16, 17 January 2019, p. 4, https://www.imf.org/en/Publications/WP/Issues/2019/01/17/Chinas-Digital-Economy-Opportunities-and-Risks-46459

3. Times Higher Education

۴. برای اطلاعات بیشتر رجوع شود به:

Times Higher Education World University Rankings, 2021, https://www.timeshighereducation.com/worlduniversityrankings/2021/worldranking#!/page/0/length/25/sort_by/rank/sort_order/asc/cols/stats.

جدول ۱: ۲۰۰ دانشگاه برتر در فهرست آموزش عالی تایمز (۲۰۲۱)	
ایالات متحده	۵۹
بریتانیا	۲۹
چین (شامل هنگ‌کنگ)	۱۲
استرالیا	۱۲
کانادا	۸
فرانسه	۵
ژاپن	۲
رژیم صهیونیستی	۱

سرمایه‌گذاری خصوصی در بخش فناوری پیشرفته ایالات متحده که در دنیا همتا ندارد، عامل اصلی پیشتازی این کشور است. براساس آمار ارائه شده در سال ۲۰۱۹، سرمایه‌گذاری خطرپذیر در ایالات متحده بیش از سه برابر چین است (۱۳۵ میلیارد دلار در مقابل ۴۰ میلیارد دلار)[۱]. در گزارش رتبه‌بندی رقابت‌پذیری جهانی موسسه آی‌ام‌دی[۲] در سال ۲۰۲۲ که توانمندی کشورها در به‌کارگیری و توسعه فناوری‌های دیجیتال در سطح دولت، کسب‌وکارها و عموم جامعه موردارزیابی قرار می‌گیرد نیز ایالات متحده در جایگاه دهم و بسیار بالاتر از چین (رتبه هفدهم) قرار دارد[۳]. علاوه بر این، گزارش کنفرانس تجارت و توسعه سازمان ملل (آنکتاد)[۴] بیانگر این واقعیت است که ۶۸ درصد ارزش سرمایه بازارِ ۷۰ بستر دیجیتال بزرگ دنیا به ایالات متحده و تنها ۲۲ درصد به چین تعلق دارد. به‌طور کلی، هزینه‌کرد ایالات متحده در تحقیق و توسعه در دو دهه اخیر تقریبا همیشه

۱. اطلاعات مربوط به ایالات متحده از سازمان همکاری اقتصادی و توسعه و اطلاعات چین از منابع چینی اخذ شده‌است.

2. IMD (International Institute for Management Development) World Competitiveness Ranking
3. Institute for Management Development, 'World Competitiveness Ranking 2020', https://www.imd.org/news/updates/IMD-2020-World-Competitiveness-Ranking-revealed
4. United Nations Conference on Trade and Development (UNCTAD)

دوبرابر چین بوده و حاصل آن جایگاه کنونی آمریکا به‌عنوان پرچمدار عرصه فناوری‌های سایبری است. البته چین در سال‌های اخیر سعی می‌کند فاصله خود با ایالات متحده را کاهش دهد.

اتحادیه اروپا و آمریکا در سال ۲۰۱۶ بیشترین سهم (به‌ترتیب ۲۳ و ۱۵ درصد) را در انتشارات (با ارجاع بالا) حوزه هوش مصنوعی داشتند، ولی در سال ۲۰۱۸ با کاهش سهم این دو قدرت (به‌ترتیب ۱۷ و ۱۲ درصد)، چین توانست از آن‌ها پیشی بگیرد و سهم ۲۸ درصدی از انتشارات حوزه هوش مصنوعی را به خود اختصاص دهد (در همین سال هند نیز با پیشرفت سریع به سهم ۱۱ درصدی دست یافت). (لازم به ذکر است با توجه به منبع باز بودن این‌گونه مطالعات، دستاورد علمی یک کشور لزوما به‌معنی قدرت اقتصادی آن نیست. علاوه بر آن، اغلب این نوع انتشارات با همکاری کشورهای دیگر انجام می‌شوند و از این رو، نمی‌توان ارزش آن‌ها را صرفا متعلق به یک کشور دانست).

این نکته را نباید فراموش کرد که آمار نمی‌توانند به‌طور کامل گویای کیفیت و پویایی بخش هوش مصنوعی ایالات متحده باشند. به‌عنوان مثال، دانشگاه اِم‌آی‌تی[1] در سال ۲۰۱۸ دانشکده‌ای ویژه برای علوم کامپیوتر تاسیس کرد تا به صورت تخصصی به تحقیقات هوش مصنوعی در گروه‌های آموزشی غیر فناوری اطلاعات بپردازد[2].

در سال ۲۰۱۹ نیز دولت ترامپ ابتکاری ملی در حوزه هوش مصنوعی (دو سال پس از ابتکار چین) جهت حفظ پیشتازی کشور و هدایت روندهای هوش مصنوعی جهانی متناسب با ارزش‌ها، منافع و سیاست‌های ملی آمریکا اجرا کرد[3]. در سال ۲۰۲۰ هم دولت اعلام کرد میزان سرمایه‌گذاری خود در زمینه هوش مصنوعی غیردفاعی را تا سال ۲۰۲۲

1. MIT Massachusetts Institute of Technology
2. MIT News, 'MIT reshapes itself to shape the future', 15 October 2018, http://news.mit.edu/2018/mit-reshapes-itself-stephenschwarzman-college-of-computing-1015.
۳. رجوع شود به: کاخ سفید، هوش مصنوعی برای مردم آمریکا، https://trumpwhitehouse.archives.gov/ai

دوبرابر افزایش خواهد داد (ازجمله ازطریق تخصیص ۸۵۰ میلیون دلار به فعالیت‌های هوش مصنوعی در بنیاد ملی علوم)[1].

ایالات متحده ردپای بسیار عمیقی نیز در شرکت‌های بزرگ مخابراتی و فناوری پیشرفته به‌ویژه در زمینه مالکیت و تعمیر و نگهداری کابل‌های مخابراتی زیردریایی[2] دارد. به‌عنوان مثال، شرکت آمریکایی گوگل بزرگ‌ترین مالک کابل‌های زیردریایی است و شرکت‌های آمریکایی ۳۶ نماینده در بین ۱۶۹ عضو کمیته بین‌المللی حفاظت کابل[3] دارند (چین تنها یک نماینده دارد)[4]. علاوه بر این‌ها، ایالات متحده دارای زیرساخت‌های ملی مانند ایستگاه‌های کابل‌گذاری در سایر کشورها ازجمله در چین است. (اطلاعاتی درباره نحوه تعامل آمریکا با دولت‌های این کشورها و چگونگی واکنش آن در صورت مداخله آن‌ها در این زیرساخت‌ها در دست نیست[5]).

از نظر ارتباطات فضایی نیز تعداد ماهواره‌های عملیاتی آمریکا حداقل سه‌برابر بیشتر از چین است (جدول ۲). فعالیت‌های سایبری نظامی آمریکا وابستگی زیادی به

1. National Science Foundation

۲. رجوع شود به:

Doug Brake, 'Submarine Cables: Critical Infrastructure for Global Communications', Information Technology & Innovation Foundation, April 2019, http://www2.itif.org/2019-submarine-cables.pdf.

3. International Cable Protection Committee

۴. رجوع شود به:

International Cable Protection Committee, 'Member List', https://www.iscpc.org/about-the-icpc/member-list.

۵. طبق برنامه حفاظت از زیرساخت‌های ملی، فهرست جامع زیرساخت‌های حیاتی/منابع کلیدی (CI/KR) خارج از مرزهای کشور که فقدان آن‌ها می‌تواند بر سلامت عمومی، امنیت اقتصادی و امنیت ملی و داخلی اثر بگذارد، باید هر سال به‌روزرسانی شود. وزارت امنیت داخلی با همکاری دولت ابتکار «وابستگی‌های خارجی حیاتی» را ارائه نموده‌است تا این وابستگی‌های خارجی که ممکن است بر سیستم‌های داخلی به‌طور مستقیم یا غیرمستقیم تاثیر بگذارند، شناسایی شوند. برای اطلاعات بیشتر رجوع شود به:

Geoff Manaugh, 'Open Source Design 02: WikiLeaks Guide/Critical Infrastructure', Domus, 29 June 2011, http://www.domusweb.it/en/architecture/2011/06/20/open-source-design-02-wikileaksguide-critical-infrastructure.html

دارایی‌های فضایی آن دارد، چون اغلب این فعالیت‌ها مانند گردآوری اطلاعات، ارزیابی خسارت و هدف‌گیری ازطریق فضا انجام می‌شوند.

جدول ۲:	تعداد ماهواره‌ها (ژانویه ۲۰۲۱)
ایالات متحده	۱۸۹۷
چین	۴۱۰
روسیه	۱۷۶
بریتانیا	۱۶۷
ژاپن	۸۴
هند	۶۳
کانادا	۴۳
فرانسه	۲۲
رژیم صهیونیستی	۱۶
استرالیا	۱۳
اندونزی	۹
مالزی	۵
ویتنام	۴
ایران	۲

در حوزه تولید تراشه‌های رایانه‌ای نیز ایالات متحده بهترین موقعیت را دارد (جدول ۳). شرکت‌های آمریکایی علاوه بر داشتن بیشترین سهم از بازار جهانی، ۵۱ درصد فروش نیمه‌رساناها را نیز در اختیار دارند.

جدول ۳: سهم صنایع نیمه‌رسانای ملی از بازار جهانی در سال ۲۰۲۰ (درصد)

کشور	نوع نیمه‌رسانا			
	منطق	آنالوگ	حافظه	مجزا
ایالات متحده	۶۱	۶۳	۲۳	۲۳
کره جنوبی	۶		۶۵	۵
اتحادیه اروپا	۹	۲۲		۴۲
ژاپن	۶	۹	۹	۲۵
چین	۹			۵
تایوان	۹		۳	

نکته: توجه داشته باشید که سایر کشورهای فعال در این حوزه ذکر نشده‌اند و به همین دلیل مجموع ارقام در همه ستون‌ها به ۱۰۰ درصد نمی‌رسد.

با وجود همه توانمندی‌های ایالات متحده باید گفت اقتصاد دیجیتال این کشور به بازار و زنجیره جهانی وابسته است و شرکت‌های داخلی آن منتقد سیاست‌های کشور (در دوره ترامپ) درمورد تحریم شرکت‌های فناوری چینی هستند. زیرا بسیاری از شرکت‌های بزرگ حوزه فناوری اطلاعات و هوش مصنوعی مانند موتورولا و اینتل[1] مراکز تولید و ساخت خود را در دیگر کشورها ازجمله چین مستقر کرده‌اند.

امنیت و تاب‌آوری سایبری

از اواخر دهه نود، ایالات متحده مصمم‌تر از هر کشور دیگری دفاع از زیرساخت‌های اطلاعاتی حیاتی بخش سایبری خود را تقویت کرده‌است. در عین حال، ایالات متحده اذعان دارد که این امر بی‌نهایت دشوار بوده و کشور دارای نقطه ضعف‌های بسیاری

1. Motorola and Intel

است[1]. از سال ۲۰۱۱ سیاست‌های کشور آمریکا به‌طور فزاینده‌ای تحت‌تاثیر ضرورت تقویت دفاع سایبری داخلی به‌ویژه در زمینه مقابله با جاسوسی یا خرابکاری در زیرساخت‌ها یا فرایندهای سیاسی قرار گرفته‌است. دولت ترامپ در ایجاد و افزایش حس اضطرار برای آمادگی سایبری نقش بسیار پررنگی داشته و گزارش‌ها و طرح‌های متعددی درباره وضعیت امنیت سایبری داخلی ارائه کرده‌است. گزارش‌های ارائه شده در سال ۲۰۱۸ با عناوین «حمایت از زیرساخت‌های حیاتی در معرض بزرگ‌ترین تهدیدها»[2]، «حمایت از رشد و بقای نیروی کار حوزه امنیت سایبری ملی»[3]، «بیانیه امنیت ملی ریاست‌جمهوری[4] که حملات سایبری تلافی‌جویانه علیه کشورهایی که مرتکب حمله سایبری به ایالات متحده می‌شوند را مجاز می‌کند» و اذعان به اهمیت فرماندهی سایبری در دفاع داخلی به‌ویژه در مورد اقدامات تروریستی در خاک آمریکا[5] ازجمله این طرح‌ها به شمار می‌آیند.

جدیت اقدامات ایالات متحده را می‌توان به‌خوبی از محتوای حکم اجرایی دولت درباره اضطرار امنیت سایبری ملی در می ۲۰۱۹ دریافت[6]. در این حکم، قطع روابط تجاری و همکاری در انتقال فناوری بین آمریکا و چین در برخی حوزه‌های فناوری اطلاعات تحت شرایط خاص پیش‌بینی شده‌است. در همان روز انتشار حکم، وزارت بازرگانی اعلام کرد

۱. برای کسب اطلاعات بیشتر به خلاصه گزارش وزارت امنیت داخلی با عنوان «حمایت از زیرساخت‌های حیاتیِ در معرض بیشترین خطرها» ۸ می ۲۰۱۸ (بخش ۹ گزارش) مراجعه شود:
https://www.cisa.gov/publication/support-critical-infrastructure-greatest-risksection-9-report-summary

2. Support to Critical Infrastructure at Greatest Risk
3. Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce
4. National Security Presidential Memorandum
5. Cyber Command

۶. رجوع شود به:
White House, 'Executive Order on Securing the Information and Communications Technology and Services Supply Chain', 15 May 2019,
https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communicationstechnology-services-supply-chain.

شرکت هوآوی و ۶۸ شعبه غیرآمریکایی آن را به «فهرست نهادها»[1] می‌افزاید که به‌معنی ضرورت اخذ مجوز صادرات برای فروش یا انتقال فناوری به آن‌ها توسط اشخاص حقیقی و حقوقی آمریکایی بود[2].

در مارس ۲۰۲۰ نیز کمیسیون سولاریوم فضای سایبری[3] به درخواست کنگره گزارشی مشتمل بر «راهبرد بازدارندگی سایبری طبقاتی»[4] منتشر کرد که ضمن هشدار درباره حملات ویرانگر سایبری به ایالات متحده شامل توصیه‌های متعددی در چند سطح بود: ۱) شکل‌دهی رفتار (مشارکت با سایر بازیگران فضای سایبری و تاثیرگذاری بر آن‌ها)، ۲) انکار منافع (ساخت دفاع سایبری قوی‌تر) و ۳) تحمیل هزینه (تهدید به تلافی). برخی از توصیه‌های جالب این گزارش عبارتند از: احیای رای‌گیری کاغذی، مشارکت بخش خصوصی و بخش دولتی در مقابله با حملات سایبری و تاسیس اداره امنیت فضای سایبری و فناوری‌های نوظهور[5]. درنتیجه، در نوامبر ۲۰۲۰ رئیس سازمان امنیت سایبری و امنیت زیرساخت‌های آمریکا اعلام کرد که انتخابات گذشته یکی از ایمن‌ترین انتخابات تاریخ این کشور بوده‌است. (البته ترامپ او را به‌دلیل این اظهارات اخراج کرد، چراکه موجب افشای اقدامات مستمر دولت برای تحقق امنیت انتخابات شد).

به‌طور کلی، ایالات متحده ضمن آگاهی از وابستگی زیاد خود به فضای سایبری و تهدیدها و نقطه‌ضعف‌های موجود، اقدامات بسیار تخصصی و پیچیده‌ای برای تقویت

1. Entity List

۲. طبق قانون تایید صادرات ایالات متحده، فهرست نهادها شامل اسامی اشخاص خارجی خاص ازجمله کسب‌وکارها، موسسات پژوهشی، سازمان‌های دولتی و خصوصی، اشخاص و سایر افراد حقوقی می‌شود که مشمول الزامات ویژه‌ای برای صادرات، بازصادرات و/یا انتقال (داخل کشور) برخی اقلام مشخص هستند. برای اطلاعات بیشتر مراجعه شود به اداره صنعت و امنیت، فهرست نهادها:
https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list

3. Cyberspace Solarium Commission
4. strategy of layered cyber deterrence
5. Bureau of Cyberspace Security and Emerging Technologies

تـاب‌آوری و امنیت سـایبری ملـی انجام می‌دهد که تاثیر آن‌ها در عملکرد امنیت سـایبری آن طبق شاخص جهانی امنیت سایبری ۲۰۱۸ به‌روشنی مشهود است: کسب جایگاه دوم (پـس از بریتانیـا) در بیـن ۱۷۵ کشور[۱]. جالب این‌که حتی عملیات هکری که در پایان سـال ۲۰۲۰ توسـط روسیه علیه شـرکت آمریکایی سـولاروینـدز[۲] انجام شـد نیز نتوانست عملکرد مناسـب آمریـکا در حوزه امنیـت سـایبری را خدشـه‌دار کنـد. اگرچه این حملـه بسیاری از مشـتریان شـرکت ازجمله ۹ نهاد دولتی را تحت‌تاثیر قرار داد، اما به‌سـرعت توسط بخش خصوصی شناسایی و خنثی شد.

رهبری جهانی در عرصه سایبری

ایـالات متحـده از نقش‌آفرینـان اصلـی در بهبـود همکاری‌هـای بین‌المللـی در حوزه سـایبری قلمداد می‌شـود. این کشور در یکی از هدفمندترین اقدامات خود در سـال ۲۰۱۱ گروه ۸ را بـه پذیـرش اصولـی یازده‌گانـه بـرای حفاظـت از زیرسـاخت‌های اطلاعاتـی حیاتـی ترغیـب کـرد[۳]. براسـاس یکـی از ایـن اصول، کشورها به توسـعه و هماهنگی سـامانه‌های هشدار اضطراری، اشتراک‌گذاری و تجزیه‌وتحلیل اطلاعات مربوط به نقاط ضعف/تهدیدها/ اتفاقـات و هماهنگـی فعالیت‌های تحقیقاتی درباره حملات به زیرسـاخت‌ها طبق قوانین داخلـی متعهـد می‌شـوند (در آن زمان روسیه نیز عضـو گروه ۸ بود). علاوه بـر این، ایالات متحـده در سـال ۲۰۱۵ یکـی از عـاملان اصلـی ترغیـب «گروه کارشناسـان دولتـی» سـازمان

۱. رجوع شود به:
International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 62, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

2. SolarWinds

۳. رجوع شود به:
Group of Eight, 'G8 Principles for Protecting Critical Information Infrastructures', May 2003, http://www.cybersecuritycooperation.org/documents/G8_CIIP_Principles.pdf

ملـل به اتخاذ هنجارهای داوطلبانه برای حفاظت از زیرسـاخت‌ها در فضای سـایبری بود؛ فرایندی که بیش از ده سال طول کشید تا به سرانجام برسد[۱].

همزمان با کاهش اعتماد آمریکا به چین و روسـیه به‌عنوان شـرکای راهبردی به‌دلیل حملات سـایبری متعدد این کشـورها به ایالات متحده-و البته بسـیاری دلایل دیگر-این کشـور با کشـورهای دموکراتیک و همفکر رویکرد اینترنت باز و جهانی را در مقابل رویکرد کنتـرل مطلـق فضـای سـایبری که کشـورهای اقتدارگـرا حامی آن هسـتند، ترویـج می‌کند. ایـن پویـش در عرصه‌های مختلفـی فعالیت می‌کند، ولی تمرکز اصلـی آن روی جلوگیری از استفاده از فناوری‌های پیشرفته اطلاعات و ارتباطات برای سانسور یا نظارت داخلی بیش از حد اسـت. آمریکا به این نتیجه رسیده‌اسـت که دامنه حملات سـایبری روسـیه و چین به ایالات متحده چنان وسیع است که امکان هیچ‌گونه گفت‌وگوی مفیدی با آن‌ها وجود ندارد. درنتیجه، این کشـور نیز از سـال ۲۰۱۸ (با صدور بیانیه امنیت ملی ریاسـت‌جمهوری که در بخش قبل شـرح داده شـد) حق انجام اقدامات تلافی‌جویانه در عرصه دیپلماتیک و فضای سایبری را برای خود محفوظ می‌داند و در همین راستا، رهبری بیش از ۲۰ کشور را در ردیابی حملات سایبری برعهده دارد.

درواقع، آمریکا در بسیاری از حوزه‌های فضای سـایبری جایگاهی بالا دارد و دیپلماسـی سـایبری موفـق و پیشـگامی شـهروندانش در مجامـع جهانـی متعـدد ماننـد موسسـه

۱. از زمان صـدور قطعنامـه مجمع عمومی سـازمان ملـل در سـال ۲۰۰۴، یـک گـروه از کارشناسـان دولتـی بـرای دوره‌ای دوسـاله بـا هـدف بررسـی مسـائل امنیـت بین‌المللی فضـای سـایبری تشـکیل شده‌اسـت. تـا سـال ۲۰۱۸، ایـن گـروه موسـوم به گـروه کارشناسـان دولتی در حـوزه «پیشـرفت‌های فنـاوری اطلاعـات و ارتباطات از منظر امنیـت بین‌المللی» بـود و پـس از آن بـه گـروه کارشناسـان دولتـی در حـوزه «ارتقـای رفتـار مسـئولانه دولت‌هـا در فضـای سـایبری از منظر امنیـت بین‌المللـی» تغییـر نـام داد. در محافـل سیاسـی صرفـا ایـن گـروه بـا عنـوان گـروه کارشناسـان دولتـی (GGE) شـناخته می‌شـود. بـرای کسـب اطلاعـات بیشـتر مراجعـه شـود بـه:
UN Office for Disarmament Affairs, 'Developments in the field of information and telecommunications in the context of international security', undated, https://www.un.org/disarmament/ict-security.

مهندسان برق و الکترونیک (IEEE)[1] و آیساکا (انجمن حسابرسی و کنترل سامانه‌های اطلاعاتی)[2] و حضور در گروه‌های استانداردهای فنی در کنار هم‌پیمانانش موید این واقعیت هستند[3].

توانمندی‌های سایبری تهاجمی

ایالات متحده هر از گاهی پرده از برخی از توانمندی‌های سایبری دفاعی خود برمی‌دارد. معرفی تعداد محدودی از عملیات‌ها، اعلام رسمی ابتکار بازدارندگی سایبری و تعهد به اجرای اصول دفاع روبه‌جلو و مشارکت مستمر نمونه‌های بارز اقدامات ایالات متحده در این زمینه محسوب می‌شوند. با این وجود، بخش اصلی تجهیزات و توانمندی‌های سایبری و کاربردهای آن‌ها همچنان از اسرار مهم دولتی آمریکا قلمداد می‌شوند.

توانمندی‌های سایبری تهاجمی ایالات متحده از همه کشورها پیشرفته‌تر هستند و این کشور از تمام بنیان‌های اصلی در عرصه سایبری برخوردار است: توانمندی‌های سطح بالا در حوزه اطلاعات سایبری که مکمل آن گردآوری اطلاعات از منابع انسانی است، رهبری ائتلاف اطلاعاتی بسیار پیشرفته پنج چشم، بنیان دانشگاهی و صنعتی بسیار

1. Institute of Electrical and Electronics Engineers
2. Information Systems Audit and Control Association

۳. آیساکا دارای ۷۵ دفتر در ایالات متحده و تنها یک دفتر در چین (هنگ‌کنگ) است؛ تقریبا نیمی از ۴۱۹ هزار عضو موسسه مهندسان برق و الکترونیک نیز در سال ۲۰۲۰ در ایالات متحده مستقر بودند. موسسه مهندسان برق و الکترونیک بزرگ‌ترین سازمان صنفی جهان بوده و در سیاست‌های بین‌المللی فضای سایبری ذی‌نفوذ است. برای کسب اطلاعات بیشتر مراجعه شود به:
https://www.ieee.org/about/at-a-glance.html

داده‌های موجود درباره ریاست کمیته‌ها/دبیرخانه‌های استاندارد دال بر این است که شهروندان ایالات متحده پس از آلمان بیشترین پست‌ها را در این گروه‌ها در اختیار دارند: به‌عنوان نمونه آلمان در DIN ۱۳۲ پست ریاست، ایالات متحده در ANSI ۱۰۴ پست ریاست، بریتانیا در BSI ۷۷ پست ریاست، فرانسه در AFNOR ۷۷ پست ریاست و ژاپن در JISC ۷۴ پست ریاست دارند. برای کسب اطلاعات بیشتر مراجعه شود به:
Tim Nicholas Rühlig, 'Technical standardisation, China and the future international order: A European perspective', Heinrich Böll Foundation, Berlin, 2020, p. 22,
https://eu.boell.org/sites/default/files/2020-03/HBS-Techn%20Stand-A4%20web-030320.pdf

قدرتمند و چارچوب نظری و حقوقی کاملا بالغ به این کشور امکان استفاده مسئولانه از توانمندی‌های سایبری در نبرد و موقعیت‌های غیرجنگی (مسلحانه) را می‌دهد.

برآورد تعداد افراد شاغل در ستاد فرماندهی سایبری آمریکا (۶۰۰۰ نیروی نظامی و غیرنظامی) تا حدی می‌تواند بیانگر سطح توان سایبری آن باشد، هرچند به‌طور دقیق نمی‌توان تعداد افراد دارای تخصص ویژه در بخش سایبری تهاجمی را محاسبه کرد. البته حتی تعیین دقیق آمار نیروی کار ستاد فرماندهی آمریکا نیز ممکن است گمراه‌کننده باشد. زیرا افرادی که در سازمان‌هایی مانند سیا و سازمان امنیت ملی و بخش خصوصی به فعالیت‌های سایبری اشتغال دارند در این آمار لحاظ نمی‌شوند. علاوه بر آن، در عملیات‌های تخصصی و پیشرفته سایبری شاخص‌های کیفی بسیار بااهمیت‌تر از معیارهای کمّی هستند.

درمجموع، شواهد دال بر این هستند که ایالات متحده از قدرت بالایی در همه سطح‌ها و حوزه‌های توانمندی‌های سایبری تهاجمی برخوردار است. به‌عنوان مثال، این کشور در سال ۲۰۰۸ توانست عملیات بسیار پیچیده استاکس‌نت را علیه برنامه هسته‌ای ایران اجرا کند. استاکس‌نت ازطریق چندین بدافزار مجزا به شبکه ایران نفوذ پیدا کرد و با رصد طولانی‌مدت آن توانست درنهایت با حمله گسترده در حدود ۱۰۰۰ سانتریفیوژ را مختل کند. ایالات متحده استفاده از چنین توانمندی‌هایی را برای طیف گسترده‌ای از موقعیت‌ها (سناریوها) پیش‌بینی می‌کند: ازجمله اختلال در سامانه‌های راهبردی نظارتی و فرماندهی دشمن و سامانه‌های ناوبری موشک‌ها.

آنچه قطعی است ایالات متحده از توانمندی‌های سایبری در نبردهای متعارف کم‌شدت یا شدید علیه اهدافی مانند دارایی‌های ستاد فرماندهی و نظارت، دارایی‌های اطلاعاتی، بسترها و سامانه‌های تسلیحاتی و زیرساخت‌های ملی حیاتی مانند شبکه‌های

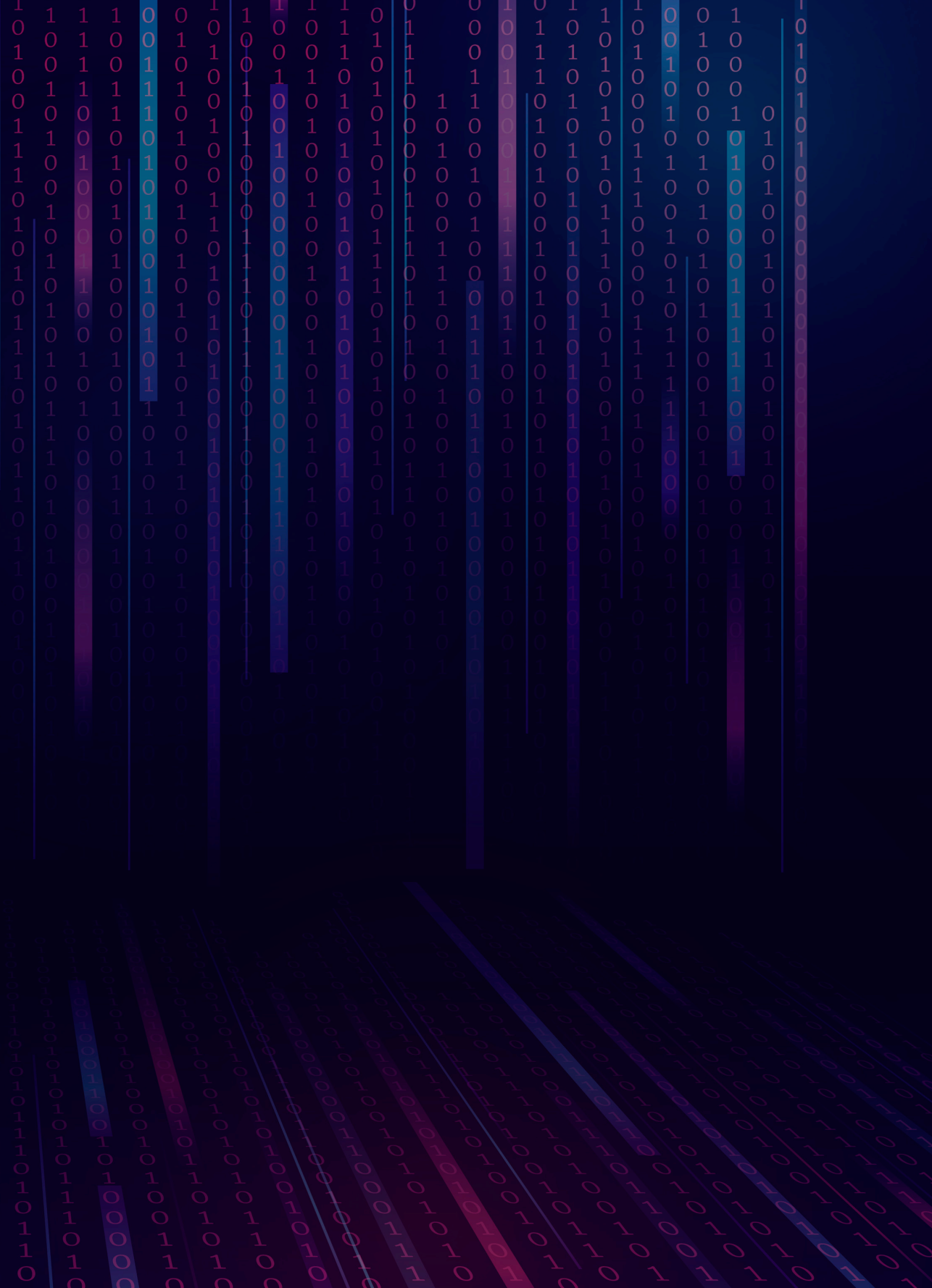
برق و سامانه‌های حمل‌ونقل استفاده می‌کند. با این حال، اظهارنظر درباره نحوه به‌کارگیری توانمندی‌های سایبری و توان واقعی آمریکا در عملیات‌های تهاجمی به‌ویژه از نوع نفوذ-اطلاعاتی و در سطحی پایین‌تر از جنگ (فیزیکی و تمام‌عیار) امری دشوار است. با توجه به اینکه توانمندی‌های ستاد فرماندهی سایبری آمریکا اساسا نظامی هستند، این توانمندی‌ها تحت‌نظارت شدید مقامات دولتی و براساس راهبرد دفاع روبه‌جلو و تلافی‌جویانه این کشور مورداستفاده قرار می‌گیرند. عملیات‌های سازمان سیا احتمالا گسترده‌تر است، ولی به‌دلیل پنهانی بودن نمی‌توان در مورد شدت و دامنه آن‌ها قضاوت کرد. به‌طور کلی، احتمال دارد تعداد عملیات‌های نفوذ-اطلاعاتی ایالات متحده نسبت به چین و روسیه -با توجه به تعداد بیشتر عملیات‌های افشاشده آن‌ها- کمتر باشد. البته این امر اصلا به معنی این نیست که توانمندی‌های آمریکا کمتر یا ضعیف‌تر است، بلکه دال بر استفاده مسئولانه‌تر آمریکا از توانمندی‌های سایبری خود است. اینکه روسیه و چین توانسته باشند به‌مدد عملیات‌های متعددی که در زمان صلح علیه کشورهای مختلف اجرا کرده‌اند، تجربه و مزیتی کسب کنند، محل تردید است. درهرحال، ایالات متحده با اجرای ابتکار بازدارندگی سایبری قصد دارد عرصه رقابت و منازعه را از فضای سایبری خود به قلمرو رقبا-دشمنانش منتقل کند.

در یک دهه گذشته، ایالات متحده بارها از توانمندی‌های سایبری خود جهت ایجاد اختلال در/یا تخریب سامانه‌های فناوری اطلاعات رقبا استفاده کرده‌است که برخی از آن‌ها مانند حمله به سازمان تحقیقات اینترنتی مستقر در روسیه به‌طور رسمی اعلام شدند و برخی دیگر (مانند حمله به ایران، کره شمالی و چین) ازطریق رسانه‌ها افشا شدند. یکی از جالب‌ترین مواردی که در رسانه‌ها افشا شد، حمله به سامانه‌های

موشک بالستیک کره شمالی قبل از پرتاب بود که در سال‌های ۲۰۱۴ و ۲۰۱۵ رخ داد[۱]. مورد دیگر که به‌طور رسمی توسط ترامپ در سال ۲۰۱۹ اعلام شد، اقدام تلافی‌جویانه علیه ایران به‌دلیل سرنگون‌سازی پهپاد آمریکایی بود[۲]. بدین‌ترتیب، ایالات متحده با اجرای چنین عملیات‌هایی سعی دارد بخشی از توان سایبری خود را که کاملا از نظر هماهنگی و اقتدار به بلوغ رسیده‌است به نمایش بگذارد، اما همه ظرفیت بالقوه آن هنوز پنهان و خارج از تیررس قضاوت قرار دارد.

۱. مراجعه شود به مقاله نیویورک‌تایمز در ۴ مارس ۲۰۱۷ با عنوان:
David E. Sanger and William J. Broad, 'Trump Inherits a Secret Cyberwar against North Korean Missiles', https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html ?action=click&module=RelatedCoverage&pgtype=Article&region=Footer.

۲. مراجعه شود به مقاله واشنگتن‌پست در ۲۳ ژوئن ۲۰۱۹ با عنوان:
Ellen Nakashima, 'Trump approved cyber-strikes against Iranian computer database used to plan attacks on oil tankers',
https://www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html.



۲

بریتانیا

بریتانیا توان سایبری بالایی دارد و در سطح سیاست‌گذاری کلان از نظارت راهبردی و شفاف برخوردار است. زیست‌بوم امنیت سایبری بریتانیا دارای ظرفیت‌های در کلاس جهانی است که شامل دو نهاد اصلی یعنی مرکز ملی امنیت سایبری (NCSC)[1] و ستاد ارتباطات دولت (GCHQ) (با توانمندی‌های بالا در زمینه اطلاعات سایبری) می‌شود. پیوند بین دولت بریتانیا و صنعت سایبری (بخش خصوصی) آن به‌تدریج روبه ارتقاست و دولت قصد دارد با رویکرد کل جامعه ظرفیت امنیت سایبری ملی را بیش از پیش توسعه دهد و با بهره‌برداری از نقاط قوت بخش خصوصی و دانشگاه‌ها سرمایه‌گذاری‌های کلانی در تحقیق و توسعه و نوآوری حوزه سایبری انجام دهد. طبق شواهد موجود، بریتانیا برای ارتقای غنای مهارت‌های سایبری خود به همکاری‌های نوآورانه و گسترده در همه بخش‌ها روی آورده‌است و درنتیجه، اقتصاد، جامعه و نیروهای مسلح آن هم‌اکنون نهایت استفاده را از مزیت‌های ارتباطات دیجیتال می‌برند که البته همین امر موجب افزایش سطح آسیب‌پذیری آن‌ها شده‌است. بریتانیا نیز همانند بسیاری از کشورها با مشکل کمبود نیروی کار ماهر در حوزه سایبری و عدم سرمایه‌گذاری‌های عظیم در مقایسه با ایالات متحده و چین مواجه است که البته به‌مدد ائتلاف‌های بین‌المللی کارآمد به ویژه با ایالات متحده می‌تواند این ضعف‌ها را تا حد زیادی جبران کند. نقطه‌ضعف احتمالی دیگر بریتانیا نداشتن بنیان صنعتی بومی برای ساخت و صادرات تجهیزاتی است که آینده فضای سایبری به آن‌ها بستگی دارد. بنابراین، بریتانیا می‌کوشد به کمک نفوذ بین‌المللی خود در ساخت آینده فضای سایبری نقش جدی داشته باشد. شواهد موجود نشان می‌دهند بریتانیا حداقل از اوایل قرن بیست‌ویکم به ساخت و به‌کارگیری توانمندی‌های سایبری تهاجمی

1. National Cyber Security Center

پرداخته‌است و سرمایه‌گذاری‌های بزرگی برای توسعه آن‌ها در دستورکار خود قرار داده‌است. بریتانیا همچنین یکی از طرفداران اصلی اعمال قوانین بین‌المللی به موارد استفاده از توانمندی‌های سایبری محسوب می‌شود.

راهبرد و مبنای نظری (دکترین)

دفاع سایبری از اواخر دهه نود همواره یکی از مساله‌های با اولویت بالا در امنیت ملی بریتانیا بوده و در اسناد راهبردی این کشور (ازجمله در اولین راهبرد امنیت ملی بریتانیا (NCSS)[1] در سال ۲۰۰۸) به‌وفور به آن اشاره شده‌است. البته اولین راهبرد ملی امنیت سایبری بریتانیا در سال ۲۰۰۹ تهیه شد و در سال‌های ۲۰۱۱ و ۲۰۱۶ به‌روزرسانی شد. با آنکه محور اصلی این راهبردها امنیت و دفاع سایبری است، ولی اشاره‌های ضمنی نیز به توسعه توانمندی‌های تهاجمی دارند. نسخه ۲۰۱۶ راهبرد ملی امنیت سایبری بر دفاع، بازدارندگی و توسعه متمرکز است و به توسعه توانمندی‌های صنعتی سایبری ملی، ظرفیت مهارتی و توانمندی‌های تحلیلی کشور نیز توجه ویژه دارد[2]. افزایش سرمایه‌گذاری دولت بریتانیا در بخش سایبری در دوره ریاضت مالی بیانگر اهمیت زیاد مسائل سایبری برای این کشور است. بودجه این بخش در برنامه ۲۰۱۶ الی ۲۰۲۱ با افزایش دوبرابری به مبلغ ۱/۹ میلیارد پوند (۲/۵ میلیارد دلار) رسید. توجیه دولت برای این افزایش بودجه این بود که بودجه‌های پیشین با دامنه و شتاب موردنیاز برای توسعه توانمندی‌های سایبری جهت مقابله با رشد سریع تهدیدها متناسب نبوده‌اند[3].

1. National Cyber Security Strategy

۲. رجوع شود به:

HM Government, 'National Cyber Security Strategy 2016-2021', 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

۳. همان، ص ۹.

راهبـرد ملـی امنیـت سـایبری بریتانیـا در قالب برنامـه امنیت سـایبری ملی (NCSP)[1] پیگیری و اجرا می‌شـود و نیروی سـایبری ملی (NCF)[2] مجری اصلی راهبرد توانمندی‌های سـایبری تهاجمـی اسـت. نیـروی سـایبری ملی در دسـامبر ۲۰۲۰ به‌طور رسـمی آغـاز به‌کار کرد و جایگزین برنامه ملی سـایبری تهاجمی (NOCP)[3] شـد که از سـال ۲۰۱۴ اجرا می‌شد. نیـروی سـایبری ملـی، راهبـرد ملـی سـایبری بریتانیـا را تحت‌نظـارت وزارت‌هـای دولت و کمیته‌هـای پارلمانی و در قالب برنامه امنیت سـایبری ملی اجرا می‌کند[4].

مرکز ملی امنیت سایبری که نهادی نوآورانه است بر اجرای برنامه ملی امنیت سایبری نظارت دارد و عملکرد آن توسط اداره ملی بازرسی (NAO)[5] سنجیده شده و نتایج به‌صورت عمومی منتشر می‌شود.

برنامـه ملی سـایبری تهاجمـی که در حال حاضر مجری آن نیروی سـایبری ملی اسـت، توانمندی‌های تخصصی در فضای سایبری با ظرفیت تهاجمی مطلوب را پوشش می‌دهد کـه در زمان و مکان مناسـب و برای بازدارندگی و اهـداف عملیاتی مطابق قوانین داخلی و بین‌المللی اسـتفاده می‌شـوند[6]. بریتانیا اولین بار در سال ۲۰۱۵ به توانمندی‌های سایبری تهاجمی خود اذعان داشـت و به‌طور رسـمی اعلام کرد در صورت نیاز برای پیشـگیری و یا مقابله با تهدیدها و نیز در زمان جنگ از آن‌ها استفاده خواهد کرد.

رئیس ستاد دفاع بریتانیا در سخنرانی رسمی در سال ۲۰۱۹ اعلام کرد هرروز رقابت بین کشـورها در عرصه سـایبری شدت بیشتری می‌گیرد و در نبرد «ایده‌ها» بازیگران غیردولتی

1. National Cyber Security Program
2. National Cyber Force
3. National Offensive Cyber Program
۴. دبیرخانه امنیت ملی از زیرمجموعه‌های اداره کابینه مسئولیت مدیریت این برنامه را از جانب مشاور امنیت ملی برعهده دارد. رجوع شود به:
National Audit Office, 'Progress of the 2016-2021 National Cyber Security Programme', 15 March 2019, p. 20, https://www.nao.org.uk/wp-content/uploads/2019/03/Progress-of-the-2016-2021-National-CyberSecurity-Programme.pdf.
5. National Audit Office
6. HM Government, 'National Cyber Security Strategy 2016-2021', p. 51

نیـز وارد شـده‌اند به‌طوری‌کـه جنـگ امـروزی به‌هیچ‌وجـه شـباهتی به جنگ‌هـای متعارف گذشته ندارد[۱]. نیروهای مسلح بریتانیا با هدایت وزیر دفاع و رئیس ستاد دفاع و براساس بودجـه دریافتـی و راهبردهای ملی، اهـداف راهبردی و عملیاتی خـود را تعیین می‌کنند. در اسـناد حـاوی مبنـای نظری (دکترین) نظامـی بریتانیا (به‌عنوان مثال، در سـندی که وزارت دفاع بریتانیا منتشـر کرده‌اسـت[۲] و جزء اسناد محرمانه طبقه‌بندی شده‌است) به روشنی بر به‌کارگیری توانمندی‌های سـایبری تاکید می‌شـود. در اسـنادی که در دسـترس عمومی قـرار دارند، نظریه رسـمی دولـت بریتانیا بر ضـرورت رویکرد نظامی در عرصـه عملیات‌های سـایبری، اطلاعاتـی و الکترومغناطیسـی تاکیـد دارد[۳]. اگرچـه در این اسـناد همانند متون ایالات متحده آشکارا کسب تسلط اطلاعاتی در عرصه سایبری موردنظر نیست، اما اجرای عملیات‌های سایبری نظامی کاملا مورد تاکید و تایید آن‌هاست.

حکمرانی، فرماندهی و نظارت

در بریتانیـا نخسـت‌وزیر و سـایر اعضـای اصلـی کابینـه خط‌مشـی راهبـردی در حـوزه سـایبری را تعییـن می‌کننـد و اداره کابینـه[۴] به آن‌ها در این زمینه مشـاوره می‌دهد. راهبرد ملی امنیت سایبری تجلی این خط‌مشی است و توسط مرکز ملی امنیت سایبری و نیروی

۱. رجوع شود به مقاله زیر از مجله تلگراف:
Dominic Nicholls, 'Britain is "at war every day" due to constant cyber attacks, Chief of the Defense Staff says', Telegraph, 29 September 2019,
https://www.telegraph.co.uk/news/2019/09/29/britain-war-every-day-due-constant-cyberattacks-chief-defense

۲. سـند وزارت دفاع تحت‌عنوان «یادداشـت مشـترک نظریه؛ ۱/۱۸ فعالیت‌هـای سـایبری و الکترومغناطیسـی» مورخ ۲۱ فوریه ۲۰۱۸ یکی از منابع عمومی تبیین‌کننده دیدگاه بریتانیاست:
https://www.gov.uk/government/publications/cyber-and-electromagnetic-activities-jdn-118.

۳. رجوع شود به:
UK Ministry of Defense, 'Joint Concept Note 2/17, Future of Command and Control', September 2017,
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643245/concepts_uk_future_c2_jcn_2_17.pdf.

4. Cabinet Office

سـایبری ملـی اجرا می‌شـود. علاوه برایـن، وزارت‌های ذی‌ربط شـامل وزارت کشـور، وزارت دفـاع، وزارت امـور خارجـه و وزارت دیجیتـال، فرهنـگ، رسـانه و ورزش (DCMS)[1] نیز دارای وظایف کاملا تعریف‌شده‌ای در این حوزه هستند.

برخلاف ایالات متحده و برخی کشورهای دیگر، بریتانیا ستاد فرماندهی سایبری نظامی مشـخصی بـرای هماهنگـی عملیات‌هـا و مدیریت دارایی‌های سـایبری دفاعـی و تهاجمی خـود نـدارد. با این حال، ارتـش بریتانیا آمادگی کافـی برای دفاع از شـبکه‌های خود را دارد. فرماندهی و نظارت سـایبری در حیطه اختیارات سـتاد فرماندهی راهبردی[2] بریتانیا اسـت کـه توسـط گـروه سـایبری نیروهـای مشـترک (JFCyG)[3] انجام می‌شـود. این گروه در سـال ۲۰۱۳ تشـکیل شده‌اسـت و امور فرماندهی و کنترل مرکز امنیت سـایبری نظامی بریتانیا[4]، واحدهـای سـایبری مختلـف در نیروهـای مشـترک ارتـش، واحدهـای تضمیـن اطلاعـات خدمات سـه‌گانه[5] و بخش ذخیره سـایبری را با استفاده از تجهیزات ارتش بریتانیا، نیروی هوایی سلطنتی و نیروی دریایی سلطنتی انجام می‌دهد.

نیروی سایبری ملی بریتانیا راه‌حلی بی‌همتا در فرماندهی امور سایبری تهاجمی است که عناصر سـایبری ذی‌ربط در سـتاد اطلاعات دولت (GCHQ)-سـازمان امنیت و اطلاعات سـایبری بریتانیـا-را بـا عناصـر سـایبری ذی‌ربـط در وزارت دفـاع، سـازمان اطلاعـات مخفی (SIS)[6] و آزمایشـگاه علـوم و فناوری دفاعی[7] در سـازمانی با فرماندهـی واحد ادغام می‌کند. ایـن سـازمان تمامی اولویت‌هـای امنیت ملی بریتانیا از مقابله با جرائم جدی تا تروریسـم بین‌المللـی، فعالیت‌هـای خصمانـه دولت‌هـا و آمادگـی بـرای جنـگ را پوشـش می‌دهـد.

1. Digital, Culture, Media, and Sport
2. Strategic Command
3. Joint Forces Cyber Group
4. MoD Corsham
5. Tri-Service Information Assurance Units
6. Secret Intelligence Service
7. Defense Science and Technology Laboratory

نیروی سایبری ملی سازمانی منحصربه‌فرد است و به‌عبارت دیگر می‌توان گفت تمامی توانمندی‌های سایبری تهاجمی ستاد فرماندهی سایبری، سازمان امنیت ملی، سازمان مرکزی اطلاعات و اداره فدرال تجسس ایالات متحده آمریکا در این سازمان تجمیع شده‌است. فرمانده نیروی سایبری ملی به رئیس ستاد ارتباطات دولت و فرمانده ستاد فرماندهی راهبردی گزارش می‌دهد و برحسب ماهیت عملیات‌ها، وزارت امور خارجه یا وزارت دفاع تاییدیه عملیات‌ها را صادر می‌کنند. اگرچه بخش اصلی فعالیت‌های نیروی سایبری ملی مشتمل بر اهداف غیرنظامی است، اما آماده‌سازی بریتانیا برای به‌کارگیری توانمندی‌های نظامی سایبری در جنگ‌های مسلحانه نیز از وظایف آن محسوب می‌شود.

در کنار بهره‌وری بیشتر، کاهش تعداد کارکنان و هزینه نسبت به ایالات متحده و چین از دیگر دلایل ایجاد نیروی سایبری ملی بریتانیا است که ضمن ارتقای چابکی عملیاتی، همه الزامات و مقتضیات ملی را اولویت‌بندی می‌کند و توانمندی‌های مهارتی و فنی را متناسب با نیاز به‌صورت متمرکز به‌کار می‌گیرد.

توانمندی‌های محوری در زمینه اطلاعات سایبری

ستاد ارتباطات دولت طی سی سال گذشته توانسته‌است توانمندی‌های شنود سیگنال و امنیت اطلاعات بریتانیا که از تاریخچه‌ای یکصدساله برخوردار است را متناسب با نیازهای فضای سایبری کنونی به‌خوبی ارتقا بخشد. شاهد این مدعا سابقه درخشان بریتانیا در شناسایی، ردیابی و اختلال در فعالیت‌های سایبری خطرناک؛ اختلال مبتنی بر توانمندی‌های سایبری در فعالیت‌های تروریستی؛ اقدامات صورت گرفته علیه جرائم اینترنتی و البته افشاگری‌های ادوارد اسنودن درباره دامنه و سطح بالای توانمندی‌های سایبری بریتانیا (به‌ویژه در زمینه رمزنگاری و علوم ریاضی) است. افزون

بر این، توانمندی‌های ستاد ارتباطات دولت به‌واسطه همکاری نزدیک و طولانی با ایالات متحده و عضویت در ائتلاف اطلاعاتی پنج چشم همواره در حال گسترش است. بریتانیا نیز همانند دیگر کشورهای عضو ائتلاف پنج چشم همه توانمندی‌های امنیت سایبری و اطلاعات سایبری خود را در سازمانی واحد یعنی ستاد ارتباطات دولت گرد آورده‌است که مرکز امنیت سایبری ملی از ارکان اصلی آن به‌شمار می‌رود.

شواهد نشان می‌دهند که نظام ارزیابی، اشتراک‌گذاری و استفاده از اطلاعات سایبری در بریتانیا کاملا بالغ است و توانایی ادغام با دیگر منابع اطلاعاتی را دارد. این امر مرهون سابقه طولانی کمیته اطلاعات مشترک[1] و بلوغ کلی نظام اطلاعاتی بریتانیاست. گزارش‌های پارلمان بریتانیا حاکی از آن است که همکاری نزدیکی بین ستاد ارتباطات دولت و دو نهاد اصلی اطلاعاتی دیگر یعنی سازمان اطلاعات مخفی (ویژه جمع‌آوری اطلاعات انسانی در خارج از کشور و عملیات‌های پنهانی) و سازمان اِم‌آی‌فایو[2] (ویژه تامین امنیت داخلی بریتانیا) وجود دارد. در امور تخصصی اطلاعات سایبری نیز مرکز امنیت سایبری ملی به‌عنوان قطب ادغام اطلاعات جاسوسی سطح بالا و اطلاعات اکتسابی بخش خصوصی عمل می‌کند.

نیروهای مسلح بریتانیا علاوه بر استفاده مستقیم از توانمندی‌های فوق، خود نیز دارای توانمندی‌های کارآمدی در زمینه اطلاعات سایبری هستند که آگاهی موقعیتی بریتانیا را بیش از پیش ارتقا می‌بخشند. برخی از این توانمندی‌ها شامل شنود میدانی اطلاعات توسط نیروهای مسلح و نیروهای ویژه، ارزیابی اطلاعات توسط سازمان اطلاعات وزارت دفاع و توانایی ادغام اطلاعات سایبری با اطلاعات (جاسوسی) سایر دارایی‌های نظامی می‌شود.

1. Joint Intelligence Committee
2. MI5 (Military Intelligence, Section 5)

توانمندی و وابستگی سایبری

بریتانیا به‌عنوان یکی از پیشروترین کشورهای اروپایی در زمینه ارتباطات دیجیتال دارای نرخ نفوذ اینترنت بالای ۹۰ درصد است. مطابق معیارهای گروه ۲۰، اقتصاد دیجیتال بریتانیا در سال ۲۰۱۸ از نظر سهم تولید ناخالص داخلی (بیش از ۵۵ درصد) در جایگاه دوم و پس از ایالات متحده (۵۹ درصد) قرار داشت. این سطح از به‌کارگیری فناوری دیجیتال ضمن این‌که همراه با منافع بسیار برای اقتصاد و جامعه بریتانیاست، افزایش آسیب‌پذیری را نیز به‌دنبال دارد. از همین روی، دولت بریتانیا جهت کاهش سطح خطر با بخش خصوصی در زمینه ارزیابی دقیق‌تر سطح تاب‌آوری شبکه‌های کشور ازجمله از نظر میزان وابستگی اقتصاد دیجیتال به شبکه‌های انرژی تجاری در زمان حاضر و آینده همکاری می‌کند. تنوع‌بخشی به منابع تامین‌کننده تجهیزات و خدمات فناوری اطلاعات و ارتباطات متناسب با نیازهای کشور یکی از اهداف دولت به‌ویژه پس از مطرح‌شدن مساله استفاده از تجهیزات شرکت چینی هوآوی است[۱].

فعالیت‌های نیروهای مسلح بریتانیا به‌شدت مبتنی بر توانمندی‌های شبکه‌ای پیشرفته‌ای است که امکان تبادل، انتقال و ادغام داده در سطح جهانی برای ماموریت‌هایی مانند هدف‌گیری، ناوبری، نظارت و فرماندهی و کنترل را برای آن‌ها میسر می‌سازد. بیشتر این توانمندی‌های نیروهای مسلح بریتانیا وابسته به فناوری‌های فضایی است[۲]. وزارت دفاع به‌منظور کاهش وابستگی خود به چند سامانه بزرگ فناوری اطلاعات که زمان

۱. رجوع شود به:
Longmei Zhang and Sally Chen, 'China's Digital Economy: Opportunities and risks', International Monetary Fund Working Paper, no. WP/19/16, 17 January 2019, p. 4,
https://www.imf.org/en/Publications/WP/Issues/2019/01/17/Chinas-Digital-Economy-Opportunities-and-Risks-46459

۲. ارتش بریتانیا علاوه بر دسترسی به سامانه‌های آمریکایی خود، مجموعه ماهواره‌های اسکای نت (Skynet) را نیز در اختیار دارد و وزارت دفاع قصد دارد دسترسی به خدمات اسکای‌نت پس از آگوست ۲۰۲۲ (پایان برنامه تامین مالی اسکای‌نت۵) را تمدید کند.

ساخت طولانی دارند، به قراردادهای کوچک با دوره زمانی کوتاه‌تر روی آورده‌است. به‌طور کلی، رویکرد بریتانیا در تحقیق و توسعه و نوآوری در زمینه توانمندی‌های سایبری و فناوری‌های ذی‌ربط مانند هوش مصنوعی از توزیع بالا در بین بخش‌های خصوصی و دولتی و دانشگاهی برخوردار است و کاملا با زیست‌بوم امنیت سایبری آن تناسب دارد. درواقع، شناسایی نقاط‌قوت صنعت در فعالیت‌های نوآورانه سریع و درنتیجه، تقویت مشارکت‌های بخش خصوصی و بخش دولتی در همه عرصه‌های ممکن هدف اصلی این رویکرد محسوب می‌شود. به لطف این رویکرد، بریتانیا زیست‌بومی شامل طیف متنوعی از مراکز رشد، شتاب‌دهنده‌ها، شرکت‌های نوپا، موسسه‌های پژوهشی و مراکز آموزش عالی تخصصی سایبری در اختیار دارد. برآورد میزان سرمایه‌گذاری در این نظام بسیار توزیع‌یافته دشوار است، اما بدون تردید شرکت‌های امنیت سایبری بریتانیایی صدها میلیون پوند ارزش دارند و به‌تبع آن، سرمایه‌گذاری‌های گسترده‌ای نیز در حوزه تحقیق و توسعه انجام می‌دهند. در کنار شرکت‌های داخلی، شرکت‌های بزرگی از بخش دفاعی ایالات متحده مانند لاک‌هید مارتین و نورث‌روپ گرومن[1] نیز نسبت به سرمایه‌گذاری‌های کلان در زمینه امنیت سایبری بریتانیا مبادرت می‌ورزند.

بخش هوش مصنوعی بریتانیا بسیار قدرتمند است و تا سال ۲۰۱۸ بالغ بر ۶۰۰۰ شرکت در این حوزه فعالیت داشتند که از آن میان ۲۸۰۰ شرکت به‌طور رسمی حوزه فعالیت خود را هوش مصنوعی معرفی کردند[2]. از این شرکت‌ها حدود ۴۰۰ مورد به‌صورت تخصصی در زمینه یادگیری عمیق (تحلیل داده خودکار) و ۳۰۰ مورد نیز در زمینه رباتیک، واقعیت

1. Lockheed Martin and Northrop Grumman

۲. رجوع شود به:
Organization for Economic Co-operation and Development, 'Measuring the Digital Transformation: A roadmap for the future', 11 March 2019, p. 34,
https://www.oecd.org/publications/measuring-the-digital-transformation-9789264 311992-en.htm

مجازی و اینترنت اشیا فعالیت داشتند. علاوه بر این، حدود ۲۵۰ شرکت در زمینه داده‌کاوی[1] و ۲۵۰ شرکت دیگر نیز در حوزه فناوری‌های تشخیصی فعالیت داشتند.

دانشگاه‌های بریتانیا در حوزه تحقیقات هوش مصنوعی در بالاترین رده‌های رتبه‌بندی‌های جهانی قرار دارند و از تاثیرگذارترین نهادهای این حوزه محسوب می‌شوند. به‌عنوان مثال، در یکی از فهرست‌های ۴۰ دانشگاه برتر از نظر تعداد انتشارات در دو کنفرانس برتر آکادمیک در سال ۲۰۲۰، دانشگاه‌های آکسفورد، کمبریج و دانشگاه کالج لندن[2] به‌ترتیب در جایگاه‌های هفتم، بیست‌ودوم و سی‌ام قرار داشتند[3]. دانشگاه چینهوا، دانشگاه پکینگ و دانشگاه جیائوتونگ شانگهای[4] از چین نیز به‌ترتیب رتبه‌های نهم، بیست‌وچهارم و چهل‌وسوم را در همین فهرست کسب کردند. همانطور که مشاهده می‌شود، بریتانیا و چین در این فهرست تقریبا در یک سطح قرار دارند، اما در رتبه‌بندی دیگری که براساس تعداد مقالات هوش مصنوعی بخش سلامت (صرفا براساس عنوان مقالات) در ۴۰ سال گذشته صورت گرفته‌است، بریتانیا در بین ۲۰ کشور برتر قرار ندارد[5]. به‌عبارت دیگر، با توجه به گستردگی و تنوع حوزه هوش مصنوعی ممکن است کشوری در یک رشته پیشرو و در رشته دیگر ضعیف باشد.

1. Data-mining
2. Oxford, Cambridge and University College London
۳. البته این رتبه‌بندی مانند اغلب نظام‌های رتبه‌بندی نقاط‌ضعف متعددی دارد. جهت مشاهده جزئیات رتبه‌بندی رجوع شود به:
Gleb Chuvpilo, 'AI Research Rankings 2020: Can the United States Stay Ahead of China?', 21 December 2020,
https://chuvpilo.medium.com/ai-research-rankings-2020-can-the-united-statesstay-ahead-of-china-61cf14b1216
4. Tsinghua University, Peking University, Shanghai Jiaotong University
۵. رجوع شود به:
Bach Xuan Tran et al., 'Global evolution of research in artificial intelligence in health and medicine: A bibliometric study', Journal of Clinical Medicine, vol. 8, no. 3, 14 March 2019, p. 9,
https://www.mdpi.com/2077-0383/8/3/360/pdf

برخلاف هدف راهبردی دولت بریتانیا (طبق اظهارات مقامات آن‌ها) مبنی بر تربیت متخصصان امنیت سایبری جهت پیشگامی در امنیت سایبری، گزارش‌های دولتی در سال ۲۰۲۰ نشان می‌دهند این کشور هنوز دچار کمبود نیروی کار متخصص در همه عرصه‌ها از مهارت‌های پایه گرفته تا تخصص‌های سطح بالاست[۱]. البته در پاسخ به این مشکل، اقدامات مختلفی برای توسعه مهارت‌های موردنیاز ازطریق بخش آموزش و نهادهای اجتماعی به‌ویژه توسط مرکز امنیت سایبری ملی و وزارت دیجیتال، فرهنگ، رسانه و ورزش انجام گرفته‌است. به‌عنوان مثال، ابتکار سایبرفرست (۲۰۱۶)[۲] تمدید و دامنه آن گسترده‌تر شده‌است و اکنون بخشی از یک برنامه ۸۴ میلیون پوندی (۱۱۴ میلیون دلار) آموزش سایبری است. این برنامه مشتمل بر دوره‌های آموزشی مختلف در زمینه امنیت سایبری و رشته‌های مرتبط در سطح مدارس، دانشکده‌ها (کالج‌ها) و دانشگاه‌ها می‌شود. این گونه ابتکارها تاکید ویژه‌ای بر ارتقای مهارت‌های دختران دارند و اگرچه هنوز نمی‌توان میزان موفقیت آن‌ها را ارزیابی کرد، اما با توجه به چارچوب کلی آن‌ها می‌توان گفت که نتیجه‌بخش خواهند بود.

در حوزه سایبری نیز نیروهای مسلح بریتانیا بسیار توانمند هستند. وزارت دفاع در زمینه تحقیق و توسعه سایبری با طیف متنوع و بزرگی از شرکت‌ها همکاری دارد که ازجمله آن‌ها می‌توان به لاک‌هید مارتین، نورث‌روپ گرومن، بی‌اِی‌ایی سیستمز، کی‌نِتیک، رِی‌تئون روک و ثِیلزیوکِی[۳] اشاره کرد. علاوه بر این‌که نیروی مسلح در هر یک از بخش‌های خود ابتکارهای متعددی برای جذب نیروهای سایبری اجرا می‌کند، برنامه‌ای

۱. رجوع شود به:
Department for Digital, Culture, Media and Sport, 'Initial National Cyber Security Skills Strategy: Increasing the UK's cyber security capability - a call for views', 3 May 2019, https://www.gov.uk/government/publications/cyber-securityskills-strategy/initial-national-cyber-security-skills-strategyincreasing-the-uks-cyber-security-capability-a-call-for-views

2. CyberFirst Initiative (2016)

3. BAE Systems QinetiQ, Raytheon, Roke and Thales UK

به نام نیروی ذخیره سایبری مشترک[1] نیز برای استخدام نیروهای کارآمد در دست اجرا دارد. با این حال، کارشناسان نظامی معتقدند بریتانیا در صورتی می‌تواند به سطح تخصص موردنیاز و هم‌ارز با ایالات متحده دست یابد که به تقویت مهارت‌های سایبری در همه سطوح نیروهای مسلح بپردازد.

اما شاید پیچیده‌ترین مساله در بریتانیا سطح کنترل و نظارت بر زیرساخت‌های مخابراتی ملی است. در حال حاضر، طراحی شبکه در اختیار شرکت بی‌تی[2] است که قبلا عرضه‌کننده انحصاری خدمات مخابراتی در بریتانیا بود. این شرکت با توجه به اندازه خود شبکه عمومی اصلی را در اختیار دارد. البته شرکت‌هایی مانند ویرجین‌مدیا[3] نیز از رقبای جدی آن هستند، به‌ویژه از زمانی که خدمات آی‌پی‌محور[4] نسل جدید در شبکه ارائه می‌شود. بی‌تی اپراتور اصلی حوزه مکالمات تلفنی کشور است که بیشتر زیرساخت‌های دسترسی شبکه به آن تعلق دارد. باآنکه همه شرکت‌های مخابراتی (تلـه‌کام) حاضر در بریتانیا ازجمله شرکت‌های خارجی دارای شبکه مخصوص به خود هستند، بریتانیا قصد دارد زیرساخت‌های بی‌تی را در اختیار سایر شرکت‌ها نیز قرار دهد. علت این امر آن است که رقبا نمی‌توانند زیرساخت‌ها و شبکه‌ای در اندازه بی‌تی داشته باشند و بنابراین، جهت جلوگیری از انحصار امکانات آن با سایر اپراتورها به‌اشتراک گذاشته می‌شود. به این ترتیب، سایر شرکت‌ها نیز می‌توانند به کمک زیرساخت‌های بی‌تی دامنه فعالیت‌ها و خدمات خود را توسعه بخشند.

درمجموع، رشد و توسعه شبکه‌های مخابراتی بریتانیا تحت‌تاثیر نیروهای بازار شکل می‌گیرد. شبکه‌های موبایل در بریتانیا مبتنی بر تجهیزات خارجی است که یا از شبکه‌های

1. Joint Cyber Reserve Force
2. BT
3. Virgin Media
4. IP-based Services

شرکت‌های با مالکیت خارجی و یا از شبکه شرکت بی‌تی استفاده می‌کنند. به‌عنوان مثال، شرکت هوآوی تجهیزات رادیویی برای شبکه‌های اینترنت همراه نسل چهارم (4G) فراهم می‌کند. مشارکت هوآوی در تامین تجهیزات بین ۵ تا ۳۰ درصد است که تحت‌نظارت شدید دولت بریتانیا (حتی در سطح رمزنگاری) انجام می‌شود. سایر شرکت‌های خارجی حاضر در این حوزه شامل سیسکو، اریکسون، فوجیتسو، نوکیا و سینا[1] می‌شوند که سطح نظارت بر آن‌ها به اندازه هوآوی نیست. واقعیت این است که بریتانیا طبق مدل غربی اینترنت آزاد و چندذینفعی رفتار می‌کند و به همین دلیل وابستگی چشمگیری به شرکت‌های تولیدکننده و اپراتورهای خارجی در زمینه مخابرات دارد.

انتقال داده در شبکه‌های بریتانیا از بهترین مسیر موجود براساس قیمت، زمان و پهنای باند انجام می‌شود. بیشتر رمزنگاری داده‌ها به برنامه‌های شناخته‌شده‌ای مانند فیس‌بوک، گوگل، مایکروسافت، تلگرام، واتساپ و سیگنال محول شده‌است و درنتیجه، ارائه‌کنندگان زیرساخت‌ها اعم از شرکت‌ها و دولت دسترسی مستقیم به محتوا ندارند. پیچیدگی شبکه‌های بریتانیا از این جهت برای آن مزیت محسوب می‌شود که سطح مشخصی از تاب‌آوری و افزونگی[2] (گزینه‌های جایگزین) را داراست. به‌عنوان مثال، نقاط (گره‌ها) دسترسی بریتانیا به اینترنت بسیار زیاد است و در جایگاه دوم پس از آلمان قرار دارد و ازاین‌رو، کارایی شبکه آن در صورتی متحمل آسیب جدی می‌شود که در گره‌های زیادی اختلال ایجاد شود. افزون بر آن، بریتانیا در قلمرو خود در ۸۸ نقطه دارای کابل زیردریایی است که در صورت خرابی چندین نقطه، همچنان سطح بالایی از افزونگی را خواهد داشت (البته بریتانیا به تامین امنیت و حفظ کارایی همه نقاط توجه زیادی دارد و هر گونه آسیب به حتی یکی از آن‌ها را رصد می‌کند).

1. Cisco, Ericsson, Fujitsu, Nokia and Siena
2. Redundancy

وابستگی بیشتر بریتانیا به زنجیره تامین خارجی در مقایسه با ایالات متحده و چین از نگرانی‌های عمده این کشور است، زیرا فضای سایبری آن را در معرض تهدیدهای بیشتری قرار می‌دهد. علاوه براین، جایگاه ضعیف‌تر بریتانیا در مقایسه با ایالات متحده یا چین از نظر سهم از بازار جهانی زیرساخت‌های شبکه موجب کم‌رنگ‌تر شدن نقش آن در شکل‌دهی به زیرساخت‌های فیزیکی فضای سایبری می‌شود[۱]. به نظر می‌رسد ابتکارهای جدید دولت در زمینه بهبود استانداردهای امنیتی تجهیزات و متنوع‌سازی شرکت‌های عرضه‌کننده خدمات/فناوری در راستای کاهش آسیب‌پذیری شبکه‌های ملی است.

ممنوعیت استفاده از تجهیزات هوآوی برای شبکه‌های نسل پنجم (5G) از سال ۲۰۲۱ همسو با این سیاست‌ها اعمال شده‌است که البته امتناع آمریکا از فروش فناوری ریزتراشه به شرکت هوآوی منجر به کاهش کیفیت محصولات این شرکت شد و عملا دسترسی بریتانیا به بسیاری از تجهیزات این شرکت (حتی برای استفاده در بخش‌های غیرحساس) را بسیار محدود کرد. به نظر می‌رسد مقابله آمریکا با چین بیش از آنکه در راستای تامین امنیت فضای سایبری باشد، در جهت جلوگیری از گسترش نفوذ فناوری‌های دیجیتال چین و به‌دلیل رقابت با بریتانیا است.

۱. با این حال، بریتانیا از صادرکنندگان فعال در حوزه تجهیزات مخابراتی است. به‌عنوان مثال، شرکت‌های BT و Vodafone به نصب و راه‌اندازی سیستم در دیگر کشورها اشتغال دارند. باید توجه داشت که ملیت طراحی یک محصول تمام‌شده معیار خوبی برای تشخیص محل ساخت اجزای آن نیست. چنانچه تحریم‌های آمریکا علیه هوآوی به تولیدکنندگان ریزتراشه‌ها در آمریکا نیز صدمه وارد می‌کند. لذا، خطرات زنجیره عرضه از پیامدهای اجتناب‌ناپذیر جهانی‌سازی توسعه و تولید فناوری است و رویکرد کنونی بریتانیا در این حوزه تا حدودی آینده‌نگرانه و پیشتازانه است. برای جزئیات بیشتر رجوع شود به:

UK Government, 'Huawei to be removed from UK 5G networks by 2027', 14 July 2020, https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5gnetworks-by-2027#:~:text=HUAWEI%20will%20be%20completely%20removed,sanctions%20against%20the%20telecommunications%20vendor.

امنیت و تاب‌آوری سایبری

ساخت زیست‌بوم امنیت سایبری ملی بریتانیا براساس رویکرد کل جامعه و در راستای تحقق همکاری نزدیک دولت، بخش خصوصی، دانشگاه و جامعه مدنی و به‌منظور ارتقای امنیت سایبری ملی است. رتبه اول بریتانیا در شاخص جهانی امنیت سایبری ۲۰۱۹ به‌خوبی سطح بالای کارآیی نظام سایبری آن را بیان می‌کند[۱]. مرکز امنیت سایبری ملی محور اصلی این زیست‌بوم است که از اکتبر ۲۰۱۶ و با هدف متمرکزسازی فعالیت‌های پراکنده حوزه سایبری و هماهنگ‌سازی وزارت‌خانه‌ها و بخش‌های خصوصی و دولتی ذی‌ربط در نهادی واحد راه‌اندازی شده‌است[۲]. گروه پاسخ فوری رایانه‌ای (CERT-UK)[۳] ملی بریتانیا نیز تحت مرکز امنیت سایبری ملی انجام وظیفه می‌کند.

دولت بریتانیا مقر مرکز امنیت سایبری ملی که زیرمجموعه ستاد ارتباطات دولت به‌شمار می‌رود را جدای از ستاد قرار داده‌است تا دسترسی بهتری به شرکت‌های خصوصی، جامعه و رسانه‌ها داشته باشد. علاوه براین، مرکز امنیت سایبری ملی ازطریق ارتباطات خود با واحد جرائم سایبری ملی[۴] -زیرمجموعه سازمان ملی جرائم[۵]-و واحدهای منطقه‌ای جرائم سازمان‌یافته[۶] به اجرای موثر قوانین سایبری کمک می‌کند و به‌واسطه اینکه زیرمجموعه ستاد ارتباطات دولت است با نیروی سایبری ملی نیز ارتباط نزدیکی دارد و با آن هماهنگ است.

---

۱. رجوع شود به:
International Telecommunication Union, 'Global Cybersecurity Index 2018', pp. 30, 62, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

۲. ازجمله تهیه گزارش‌های ارزیابی ملی، حفاظت از زیرساخت‌های ملی حیاتی، تضمین اطلاعات و گروه‌های پاسخ اضطراری ملی.

3. Computer Emergency Response Team
4. National Cyber Crime Unit
5. National Crime Agency
6. Regional Organized Crime Units

دولت و بخش خصوصی بریتانیا در تامین امنیت ملی این کشور همکاری فزاینده‌ای با یکدیگر دارند و مرکز ملی امنیت سایبری ازطریق مشارکت در اشتراک‌گذاری اطلاعات امنیت سایبری امکان تبادل اطلاعات بین دولت و صنعت در زمان واقعی را فراهم کرده‌است و از طریق مشارکت در رشد سایبری نیز ۱۰۰ شرکت را برای تامین امنیت سایبری دولت تایید کرده‌است. زیرساخت‌های ملی سایبری بریتانیا دارای ۱۳ بخش هستند[۱] که از سوی دولت موظف شده‌اند هر سال برنامه امنیت و تاب‌آوری بخشی خود را با تاکید بر مسائل امنیت سایبری تهیه کنند. به‌همین‌ترتیب، شرکت‌های بخش خصوصی نیز مسئولیت طراحی برنامه‌های تاب‌آوری و استمرار تجاری خود را برعهده دارند. در راستای تقویت هرچه بیشتر امنیت سایبری نیز دولت برنامه‌های متعددی برای افزایش آگاهی عمومی در زمینه‌های سواد سایبری، چالش امنیت سایبری، الزامات سایبری و ایمنی برخط (آنلاین)[۲] در سطح جامعه در دست اجرا دارد.

لازم به ذکر است راهبرد امنیت سایبری بریتانیا از سال ۲۰۱۶ دستخوش تحولات زیادی شده‌است. تا قبل از سال ۲۰۱۶، بریتانیا برای تامین امنیت فعالیت‌های شرکت‌ها به نیروهای بازار متکی بود و نمی‌توانست دامنه و سرعت عمل خود را متناسب با روند گسترش تهدیدها توسعه دهد. به همین دلیل، نقش مداخلات دولت در راهبرد امنیت سایبری از سال ۲۰۱۶ افزایش یافت تا بهتر به اهداف موردنظر خود دست یابد. در همین راستا، ابتکار دفاع سایبری فعال توسط مرکز ملی امنیت سایبری در سال ۲۰۱۶ اجرا شد. به‌موجب این ابتکار، دولت با شرکت‌های ارائه‌کننده خدمات اینترنت برای یافتن راهی

۱. این سیزده بخش از زیرساخت‌های حیاتی ملی بریتانیا عبارتند از: صنایع شیمیایی، هسته‌ای غیرنظامی، ارتباطات، دفاع، خدمات اضطراری، انرژی، تامین مالی، دولت، سلامت، فضا، حمل‌ونقل و آب. رجوع شود به:
Centre for the Protection of National Infrastructure, 'Critical National Infrastructure', https://www.cpni.gov.uk/critical-national-infrastructure-0

2. Cyber Aware, Cybersecurity Challenge, Cyber Essentials and Get Safe Online

جهت توقف و اختلال در فعالیت‌های مخرب در شبکه‌ها به‌منظور حمایت حداکثری از شهروندان بریتانیایی در برابر حملات با دامنه گسترده و پیچیدگی محدود همکاری می‌کند. اولین سطح از این فعالیت‌ها بر تعاملات شهروندان با دولت متمرکز بوده‌است که تاکنون تاثیر قابل‌توجهی بر کاهش حملات فیشینگ[1] داشته‌است (از ۵/۳ درصد به ۲/۲ درصد بین سال‌های ۲۰۱۶ تا ۲۰۱۸)[2]. در حال حاضر، دولت قصد دارد بخش‌های صنعتی را نیز به مشارکت در این رویکرد ترغیب کند.

با آنکه فرایندهای سازنده زیست‌بوم امنیت سایبری کاملا توسعه‌یافته هستند، اما شناسایی و تخمین اندازه نیروی انسانی و ظرفیت فنی این حوزه چندان آسان به نظر نمی‌رسد. تخصیص ۱/۹ میلیارد پوند (۲/۵ میلیارد دلار) در برنامه پنج‌ساله بریتانیا به بخش سایبری در مقایسه با سایر سرمایه‌گذاری‌های بریتانیا بسیار قابل‌توجه است (هرچند مشکلاتی جهت تامین این مبلغ توسط اداره ملی بازرسی عنوان شده‌است). وجود ۷۴۰ نفر نیروی متخصص در مرکز ملی امنیت سایبری نیز بیانگر سطح بالای تمرکز این نهاد در عرصه سایبری است، اگرچه تعداد واقعی کارکنان فعال در این عرصه در سطح دولتی و بخش خصوصی بسیار فراتر از این رقم است. حضور حدود ۱۰۰ شرکت دارای مجوز جهت فعالیت در زمینه تامین امنیت سایبری دولت نیز نشان از ظرفیت بالای بخش خصوصی بریتانیا دارد[3]. علاوه بر این، گزارش‌های ارائه شده در سال ۲۰۲۰

1. Fishing

۲. رجوع شود به:

National Cyber Security Programme', 2019, p. 11,
https://www.nao.org.uk/wp-content/uploads/2019/03/Progress-of-the-2016-2021-National-Cyber-Security-Programme.pdf

۳. طبق آمار دولتی حدود ۸۰۰ شرکت ارائه‌کننده خدمات امنیت سایبری در بریتانیا فعالیت دارند که تعداد آن‌ها بسیار بیشتر از ۱۰۰ شرکت موردتایید مرکز ملی امنیت سایبری است. این سطح از تنوع اگرچه از یک نظر موجب افزایش قدرت شرکت‌های بریتانیایی می‌شود، اما سهم آن‌ها از بازار را در مقایسه با شرکت‌های بزرگ خارجی مانند FireEye کاهش می‌دهد. صنعت امنیت سایبری بریتانیا شامل تعداد زیادی شرکت‌های کوچک و نوپا است که توسعه و رشد آن‌ها در گرو توجه به عوامل بازار است.

دال بر افزایش ۴۰ درصدی شرکت‌های حوزه امنیت سایبری و افزایش ۳۷ درصدی مشاغل حوزه سایبری بین سال‌های ۲۰۱۷ و ۲۰۱۹ هستند[۱]. با این همه، بریتانیا همچنان با چالش تامین نیروی کار تخصصی در عرصه سایبری مواجه است. در همین راستا، مرکز ملی امنیت سایبری ابتکارهای متعددی برای ارتقای مهارت و تخصص نیروی کار در دست اجرا دارد.

گزارش‌های ارائه شده درباره وضعیت کنونی امنیت سایبری بریتانیا در سال ۲۰۲۰ نشان می‌دهند میزان شناسایی حملات سایبری افزایش داشته‌است و تقریبا نیمی از کسب‌وکارها در تمام سال آماج حمله‌های سایبری بوده‌اند. با این حال، سطح تاب‌آوری کسب‌وکارها افزایش یافته و میزان خسارت‌های ناشی از حمله‌های سایبری به آن‌ها کاهش (۳۲۳۰ پوند یا کمتر از ۵ هزار دلار) داشته‌است. برخی تحقیقات کیفی در حوزه امنیت سایبری بریتانیا نیز بر این واقعیت دلالت دارند که بانک‌ها و شرکت‌های بیمه این کشور در زمینه تامین امنیت سایبری در بخش خصوصی پیشتاز هستند.

رهبری جهانی در عرصه سایبری

بریتانیا تمایل دارد با نقش‌آفرینی در عرصه‌های بین‌المللی در شکل‌گیری آینده فضای سایبری حضور موثری داشته باشد. در همین راستا، بریتانیا از اجرای قوانین بین‌المللی موجود و تدوین و اجرای هنجارهای بین‌المللی داوطلبانه درباره رفتار دولت‌ها

۱. رجوع شود به:
Sam Donaldson et al., 'UK Cyber Security Sectoral Analysis 2020', Department for Digital, Culture, Media and Sport, January 2020, pp. 2, 44, 63, 73,
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/861945/UK_Cyber_Sectoral_Analysis__2020__Report.pdf.

در فضای سایبری حمایت جدی می‌کند. بریتانیا از ابتکارهای امنیت سایبری سازمان ملل، اتحادیه اروپا و کشورهای عضو اتحادیه کشورهای مشترک‌المنافع در حوزه فضای سایبری حمایت می‌کند. از سال ۲۰۰۴ که گروه کارشناسان دولتی سازمان ملل تشکیل شد، بریتانیا نقش فعالی در آن داشته‌است[۱]. براساس طرح بریتانیا به‌عنوان مدل بلوغ ظرفیت امنیت سایبری ملت‌ها[۲] نیز این کشور برنامه‌های بین‌المللی متعددی جهت کمک به بهبود امنیت سایبری در بیش از ۸۰ کشور اجرا کرده‌است[۳]. در ماه می ۲۰۱۹ نیز بریتانیا همراه با هلند تصمیم گرفتند نظام تحریم‌های اتحادیه اروپا برای جریمه‌کردن مستقیم هکرهای رایانه‌ای را بپذیرند. البته خروج بریتانیا از اتحادیه اروپا می‌تواند اهرم‌های نفوذ و تاثیرگذاری آن در زمینه سیاست‌های امنیت سایبری و نظارت بر جرائم سایبری در سطح اروپا را تضعیف کند.

بریتانیا از پیشینه غنی در ائتلاف‌های بین‌المللی حوزه امنیت سایبری و اطلاعات سایبری برخوردار است. این کشور از شرکای مهم ائتلاف پنج چشم، ناتو و بسیاری از دولت‌های اروپایی است. علاوه براین‌ها، شواهدی مبنی بر گسترش همکاری‌های بریتانیا در زمینه امنیت سایبری با کشورهایی از خاورمیانه، آسیای جنوب شرقی-اقیانوسیه و آمریکای لاتین وجود دارد. همچنین، بریتانیا از سال ۲۰۱۶ طی توافقی همکاری نزدیکی در زمینه توسعه توانمندی‌های سایبری تهاجمی و دفاعی با ایالات

۱. رجوع شود به:
UN Office for Disarmament Affairs, 'Developments in the field of information and telecommunications in the context of international security',
https://www.un.org/disarmament/ict-security

2. Cybersecurity Capacity Maturity Model for Nations

۳. رجوع شود به:
Global Cyber Security Capacity Centre, 'Cybersecurity Capacity Maturity Model for Nations', Oxford University, 2017,
https://cybilportal.org/tools/cybersecurity-capacity-maturitymodel-for-nations-cmm-revised-edition

متحده دارد. این‌گونه مشارکت‌ها و ائتلاف‌های بین‌المللی امکان توسعه بیشتر توانمندی‌های سایبری بریتانیا که در سطح بالایی قرار دارند را برای این کشور فراهم می‌کنند.

توانمندی‌های سایبری تهاجمی

طبق اظهارات صریح وزرای دولت بریتانیا، این کشور از آمادگی لازم جهت استفاده از توانمندی‌های سایبری برای جلوگیری و مقابله با تهدیدها شامل تروریست‌ها و جنایتکاران سایبری و سایر بازیگران سایبری متخاصم برخوردار است. بریتانیا عملیات‌های سایبری تهاجمی را از اجزای جدایی‌ناپذیر جنگ‌های مدرن می‌داند و ارتش بریتانیا نیز بر استفاده از توانمندی‌های سایبری تهاجمی به‌عنوان ابزار نبرد تاکید دارد[۱]. درحقیقت، موضوع توانمندی‌های سایبری تهاجمی از منظر استفاده آزادانه از آن‌ها در فعالیت‌های نظامی برای اعمال قدرت، اثرگذاری نظامی مخرب و بازدارندگی به‌طور مفصل در اسناد رسمی تبیین‌کننده‌ی مبنای نظری نظامی بریتانیا موردبررسی قرار گرفته‌اند.

امور مربوط به توسعه توانمندی‌های سایبری تهاجمی در بریتانیا به‌طور مشترک توسط وزارت دفاع و ستاد ارتباطات دولت پیگیری می‌شود. از سال ۲۰۱۴ این حوزه تحت‌نظارت نیروی سایبری ملی بریتانیا قرار دارد که سرمایه‌گذاری‌های هنگفتی در زمینه توسعه منابع انسانی و مالی به‌منظور ارتقای توانمندی‌های سایبری انجام داده‌است و برنامه‌های متعددی در دست اجرا دارد. طبق اسناد کمیته‌های پارلمانی (۲۰۱۷-۲۰۱۶)، این نهاد در توسعه طیف گسترده‌ای از توانمندی‌های سایبری-از توانمندی‌های موردنیاز در

۱. جهت مشاهده مجموعه این اظهارات رجوع شود به:
'National Cyber Force transforms country's cyber capabilities to protect the UK', November 2020, https://www.gchq.gov.uk/news/national-cyber-force#:~:text=Defence%20Secretary%20Ben%20Wallace%20said,ability%20to%20conduct%20cyber%20operations.

زمان صلح برای عملیات‌های نفوذ/اطلاعات تا توانمندی‌های مورداستفاده در جنگ‌های تمام‌عیار-نقش بسزایی داشته‌است. این اسناد همچنین بر تلاش‌های گسترده ستاد ارتباطات دولت جهت بهره‌برداری از شبکه‌های رایانه‌ای (برای هک‌کردن) به‌عنوان ابزاری موثر و بخشی از عملیاتی‌سازی توانمندی‌های سایبری تهاجمی دلالت دارند.

اگرچه بریتانیا در سال ۲۰۱۸ به جمع سه کشوری (استرالیا و ایالات متحده) پیوست که به‌طور رسمی استفاده از توانمندی‌های سایبری تهاجمی را تایید می‌کنند، اما همان‌طور که انتظار می‌رود با توجه به اصل محرمانگی، شواهد زیادی درباره دامنه و سطح واقعی توانمندی‌های سایبری بریتانیا در دست نیست. با توجه به افشاگری‌های اسنودن، ستاد ارتباطات دولت بریتانیا از ابتدای قرن جدید در ساخت و به‌کارگیری فناوری‌های سایبری تهاجمی به‌ویژه در زمینه مقابله با تروریسم بین‌المللی پیشتاز بوده‌است[۱] و این کشور علاوه بر استفاده از توانمندی‌های سایبری خود در عرصه‌های سایبری، از توانمندهای سایبری در جنگ‌های واقعی ازجمله در جنگ افغانستان نیز بهره برده‌است[۲].

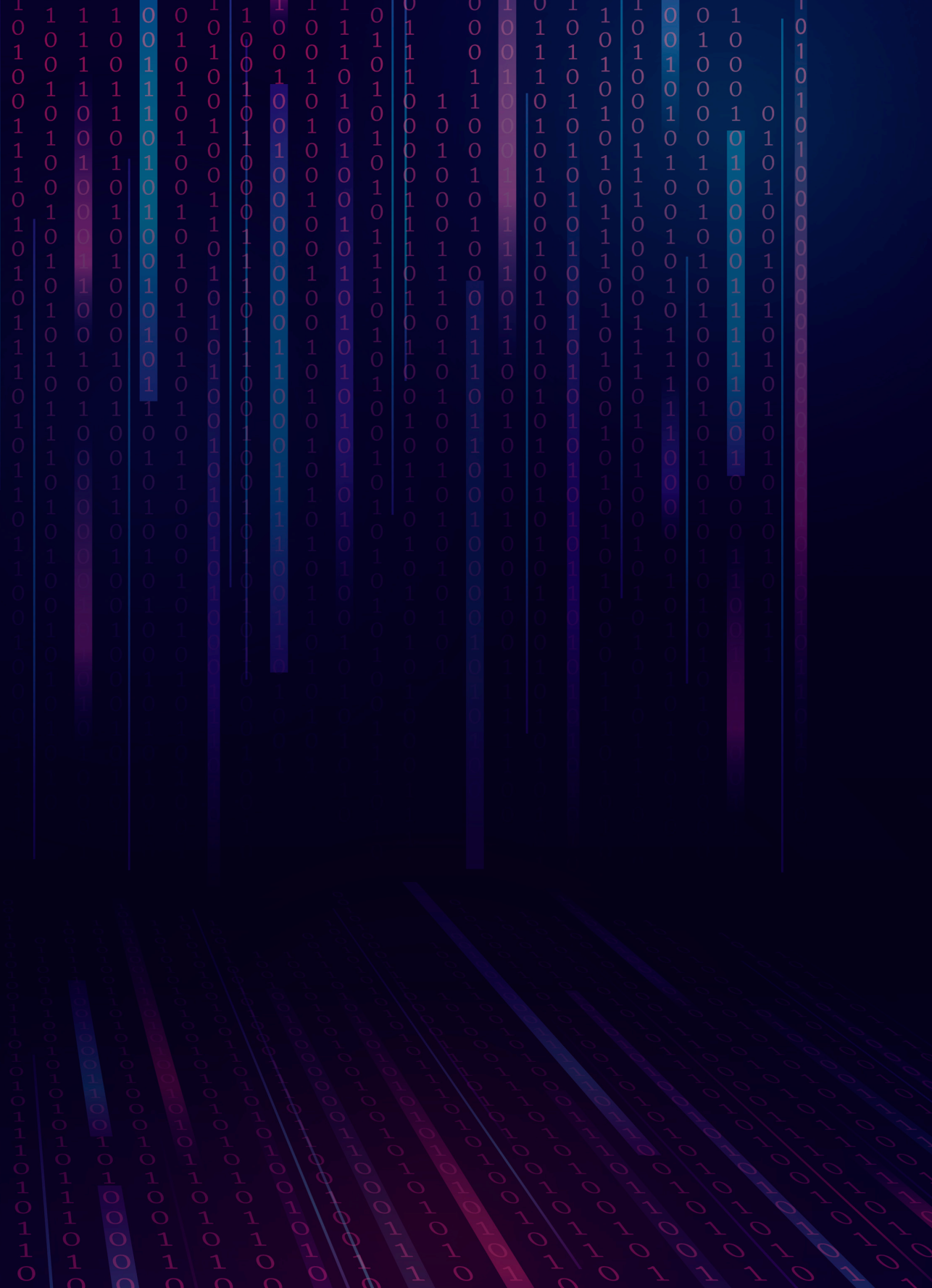
بریتانیا به‌طور رسمی اعلام کرده‌است از توانمندی‌های سایبری برای اهداف اطلاعاتی یا تهاجمی به‌طور کاملا مسئولانه و طبق قوانین داخلی و بین‌المللی استفاده خواهد کرد. درواقع، بریتانیا مطابق یکی از اصول قانون خود در به‌کارگیری توانمندی‌های سایبری ملزم است ضرورت و تناسب عملیات‌های سایبری را اثبات کند و درصورت اجرای این‌گونه عملیات‌ها برای اهداف نظامی ملزم است آن‌ها را تحت‌نظارت وزارت دفاع و طبق رویه‌های سازمانی و قانونی (ضمن توجه به اصول حقوق بشر و عدم‌تبعیض)

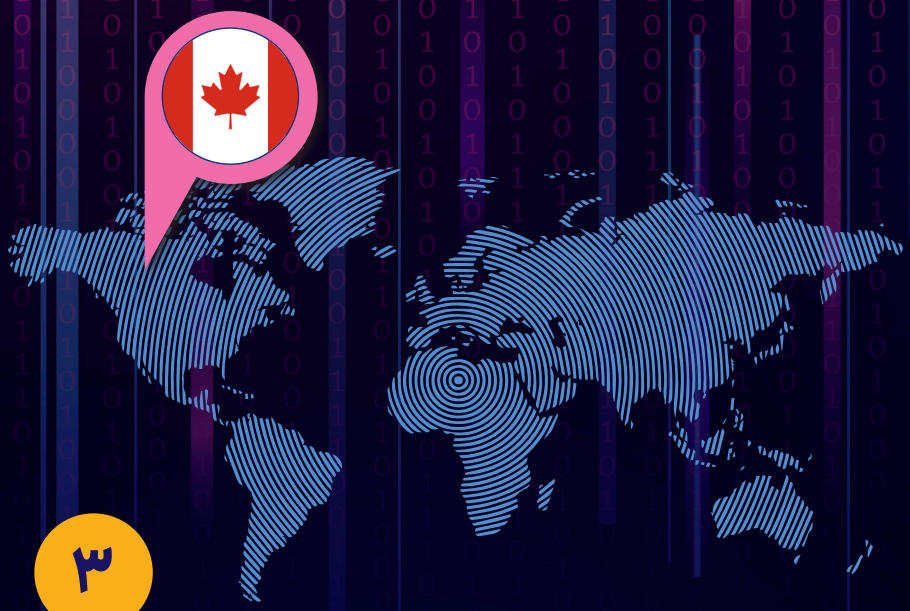
۱. دولت بریتانیا هنوز در تایید یا رد اطلاعات افشاشده توسط اسنودن اظهارنظر رسمی نداشته‌است.
۲. به‌استثنای مورد داعش، بریتانیا هیچ‌گاه به‌طور رسمی استفاده از عملیات‌های سایبری علیه دیگر کشورها را تایید نکرده‌است. برای جزئیات بیشتر رجوع شود به:
Gordon Corera, 'UK's National Cyber Force comes out of the shadows', BBC News, 20 November 2020, https://www.bbc.com/news/technology-55007946.

انجام دهد. به‌عبارت دیگر، در نظام سایبری بریتانیا توجه به عواقب ناخواسته و عوارض جانبی احتمالی عملیات‌های سایبری از اصول اساسی به شمار می‌رود. بریتانیا نیز همانند آمریکا ضمن محفوظ دانستن حق به‌کارگیری توانمندی‌های سایبری تهاجمی برای خود، استفاده از آن‌ها را منوط به زمان و شرایط خاص مانند اهداف عملیاتی ملی می‌داند[۱]. به‌علاوه، بریتانیا نیز مانند دیگر کشورهای متعهد به استفاده از توانمندی‌های سایبری در چارچوب مقررات حقوقی داخلی و بین‌المللی باید راهکارهایی جهت اقناع بهتر عموم جامعه درباره به‌کارگیری توانمندی‌های سایبری بیابد تا مشروعیت سیاسی لازم جهت اجرای عملیات‌های سایبری را کسب کند. به همین منظور، بریتانیا باید در مورد برنامه‌های ساخت، توسعه و به‌کارگیری توانمندی‌های سایبری با شفافیت بیشتری عمل کند.

احتمالا مهم‌ترین چالش بریتانیا در توسعه و استفاده از توانمندی‌های سایبری شامل سرمایه‌گذاری کلان مالی و توسعه منابع انسانی به‌ویژه جهت ارتقای مهارت‌های فنی محوری است که البته نیروی سایبری ملی با همین هدف شکل گرفته‌است. به‌طور کلی با توجه به شواهد موجود می‌توان دریافت که بریتانیا در کنار ایالات متحده یکی از پرچمداران اصلی توانمندی‌های سایبری تهاجمی در سرتاسر جهان است.

۱. رجوع شود به:
UK Parliament, 'Electronic Warfare: Question for Ministry of Defense', UIN 201591, tabled on 12 December 2018,
https://questions-statements.parliament.uk/written-questions/detail/2018-12-12/201591.





۳

کانادا

کانادا از کشورهای به‌شدت دیجیتالی با قدرت متوسط و اقتصاد پیشرفته است که رویکرد کل جامعه این کشور در امنیت سایبری کاملا با نظام دولت و سیاست خارجی آن هماهنگ است. همانند ایالات متحده و بریتانیا، سیاست‌های کانادا نیز بر اصل تنوع ذینفعان تاکید دارند و توانمندی‌های سایبری غیرنظامی آن نسبتا بالغ هستند که با مقررات و قوانین مناسبی حمایت می‌شوند و دولت با جدیت در جهت دیجیتال‌سازی کشور فعالیت می‌کند. اقتصاد قوی کانادا که در بسیاری از حوزه‌ها به فناوری‌های پیشرفته مجهز است، امتیازهای زیادی را برای این کشور در مقایسه با کشورهای با اقتصاد مشابه به ارمغان آورده‌است. با این حال، کانادا در تامین بسیاری از سخت‌افزارهای موردنیاز در سامانه‌های مدرن فناوری اطلاعات و ارتباطات به دیگر کشورها وابسته است. سیاست تاب‌آوری ملی کانادا اگرچه ساختار مناسبی دارد، اما در مرحله اجرا مطابق انتظارات عمل نمی‌کند. عناصر زیرساخت‌های حیاتی کانادا مانند شبکه‌های توزیع برق با ایالات متحده مشترک است. کانادا در زمینه سایبری در سطح بین‌المللی فعالیت دارد و در توسعه توانمندی‌های سایبری سایر کشورها نیز مشارکت می‌کند. حضور در ائتلاف‌های بین‌المللی باعث تقویت ظرفیت‌های سایبری کانادا ازجمله ارتقای دسترسی آن به دارایی‌های سایبری دیگر کشورها به‌خصوص در حوزه فضایی می‌شود. اگرچه توانمندی کانادا برای حضور در عملیات‌های سایبری جهانی در سطح بریتانیا و ایالات متحده نیست، ولی در زمینه توانمندی سایبری تهاجمی که از سال ۲۰۱۸ بستر حقوقی آن را فراهم کرده‌است از فرصت پیشرفت زیادی برخوردار است.

راهبرد و مبنای نظری (دکترین)

طبق اسناد عمومی کانادا، رویکرد کل جامعه در تامین امنیت سایبری از اولویت بالایی در این کشور برخوردار است. درنتیجه، توسعه توانمندی‌های سایبری تهاجمی و نظامی در کانادا در مقایسه با کشورهای سایبری قوی موردتوجه کمتری قرار دارد.

سیاست امنیت ملی کانادا (۲۰۰۴)[1] جامع‌ترین سند سیاست‌گذاری[2] و درواقع، راهنمای عمل سیاست‌گذاری این کشور محسوب می‌شود[3]. سایر اسناد بیشتر روی چالش‌های خاص امنیتی به‌ویژه تروریسم متمرکز هستند و توجه زیادی نیز به امنیت زیرساخت‌های حیاتی دارند. دو راهبرد امنیت سایبری کانادا (۲۰۱۰ و ۲۰۱۸) مهم‌ترین اسناد حوزه سیاست‌های سایبری این کشور محسوب می‌شوند. در راهبرد ۲۰۱۰ به صراحت بر تامین امنیت سیستم‌های دولتی تاکید شده که دستیابی به راه‌حل‌های فنی کارآمدی را در پی داشته‌است. این راهبرد بر تقویت مشارکت بین بخش‌های خصوصی و دولتی متمرکز است و ابتکارهای آن در زمینه تامین امنیت برخط شهروندان در زمان خود بسیار پیشرو بوده‌اند که بعدها توسط دیگر کشورها نیز به‌کار رفته و توسعه یافته‌اند. البته این راهبرد نسبتا کلی (بالادستی) است و جزئیات کمی درباره ابتکارها و منابع ارائه می‌کند.

راهبرد ۲۰۱۸ مشتمل بر طیف متنوعی از ابتکارهای فرادولتی است که از ایجاد مرکز امنیت سایبری کانادا[4] و واحد ملی هماهنگی جرائم سایبری[5] تا ابتکارهایی در زمینه نوآوری، رشد

1. National Security Policy (2004)

۲. رجوع شود به:
Canada Privy Council Office, 'Securing an Open Society: Canada's National Security Policy', 2004, http://publications.gc.ca/collections/Collection/CP22-77-2004E.pdf

۳. به عنوان نمونه رجوع شود به:
Public Safety Canada, 'Securing an Open Society: Canada's National Security Policy', 2015, https://www.publicsafety.gc.ca/cnt/ntnl-scrt/scrng-en.aspx

4. Canadian Center for Cyber Security
5. National Cyber Crime Coordination Unit

اقتصادی و توسعه استعدادهای سایبری را دربرمی‌گیرد. بودجه موردنظر برای این راهبرد ۵۰۰ میلیون دلار کانادا (حدود ۴۰۰ میلیون دلار آمریکا) است که به هشت وزارتخانه ذی‌ربط و طی پنج سال تخصیص می‌یابد. درواقع، راهبرد ۲۰۱۸ در نوع خود بسیار منحصربه‌فرد بوده و براساس رویکرد کل جامعه و با مشارکت و مشورت عمومی تدوین شده‌است.

این راهبرد با تاکید بر ایمنی عمومی کانادا و کاملا مطابق برنامه‌های موردانتظار اجرا شده‌است. در سال ۲۰۲۰ نیز ابتکارهای جدیدی با تمرکز جدی بر مبارزه با سوءاستفاده جنسی برخط از کودکان و بهبود تاب‌آوری زیرساخت‌های فیزیکی و دیجیتالی حیاتی ملی به این راهبرد اضافه شد. دولت کانادا گزارش عملکرد خود در اجرای این راهبرد را به‌طور بسیار شفافی به عموم جامعه ارائه کرده‌است.

اگرچه سیاست‌های کلان دولتی و وزارتی متعددی (حداقل ۱۲ سند سیاست) در حوزه امنیت سایبری و عملیات‌های سایبری دفاعی برای نیروهای مسلح کانادا (CAF)[1] و وزارت دفاع ملی (DND)[2] تدوین شده‌است، ولی به‌دلیل کمبود اسناد مرتبط با جزئیات اجرای این سیاست‌ها، ارزیابی آن‌ها چندان ساده نیست. در سال ۲۰۰۹، دیدگاه حاکم در کانادا فضای سایبری را عرصه نبرد می‌دانست و بر استفاده همزمان از توانمندی‌های سایبری و نظامی جهت ایجاد حداکثر کارایی تاکید داشت[3]. به‌بیان دیگر، حتی قبل از این سال نیز ملاحظات مربوط به جنبه‌های عملیاتی توانمندی‌های سایبری به‌طور کامل در کانادا شکل گرفته‌بود[4].

1. Canadian Armed Forces
2. Department of National Defense

۳. رجوع شود به:
Public Works and Government Services Canada, 'Defensive Cyber Operations', Letter of Interest, Solicitation No. W6369-17DE25/B, 2017, p. 1, https://buyandsell.gc.ca/cds/public/2017/12/18/637ad14072ef720ed0c51146992cca46/ABES.PROD.PW__QE.B049.E26594.EBSU000.PDF.

۴. رجوع شود:
Canadian Department of National Defense, 'Integrated Capstone Concept', 2009, pp. 28-30, http://publications.gc.ca/collections/collection_2012/dn-nd/D2-265-2010-eng.pdf.

در سال ۲۰۱۷ نیز مفهوم عملیات‌های سایبری نظامی در قالب یکی از سیاست‌های دفاعی کانادا به مباحث عمومی کشور راه یافت که درنتیجه آن وظیفه مهمی به ارتش در ارتباط با توانمندی‌های سایبری محول شد. درواقع، نیروهای مسلح کانادا موظف به حفظ اهداف امنیتی و دفاعی و تامین منافع راهبردی ازجمله منافع اقتصادی کانادا در برابر هرگونه تهدید فضایی و سایبری شدند[۱].

حکمرانی، فرماندهی و نظارت

باتوجه به این‌که کانادا کشوری با نظام دموکراسی پارلمانی به سبک بریتانیاست، نخست‌وزیر وظیفه فرماندهی و نظارت بر سازمان‌های سایبری را برعهده دارد و وزیر ایمنی عمومی و آمادگی بحران، وزیر دفاع ملی و سایر مقامات ذی‌ربط مانند مدیر سازمان امنیت ارتباطات (CSE)[۲]، مدیر سازمان اطلاعات امنیتی کانادا (CSIS)[۳] و فرمانده کل نیروهای مسلح کانادا در این رابطه به او گزارش می‌دهند. کانادا همانند هم‌پیمانان نزدیکش از رویکرد چندذینفعی در حکمرانی سیاست‌های امنیتی/سایبری و سیاست‌های صنعتی و آموزشی ذی‌ربط استفاده می‌کند. پلیس سوار سلطنتی کانادا، سازمان صنایع کانادا، هیئت خزانه‌داری و کمیساریای حفظ حریم خصوصی[۴] از دیگر نهادهای دولتی کانادا هستند که در این عرصه مشارکت جدی دارند. البته این رویکرد چندذینفعی به‌دلیل نداشتن مرجع عالی مشخص در کانادا موردانتقاد قرار دارد[۵].

۱. رجوع شود:
Canadian House of Commons, 'Standing Committee on National Defense, Evidence, Tuesday 30 January 2018', https://www.ourcommons.ca/DocumentViewer/en/42-1/NDDN/meeting-77/evidence

2. Communications Security Establishment
3. Canadian Security Intelligence Service
4. Royal Canadian Mounted Police, Industry Canada, Treasury Board Secretariat and Privacy Commissioner

۵. رجوع شود به:
Canadian Armed Forces, 'Strong, Secure, Engaged: Canada's Defense Policy', 2017, http://dgpaapp.forces.gc.ca/en/canadadefence-policy/docs/canada-defence-policy-report.pdf.

در حوزه امنیت سایبری غیرنظامی نیز سازمان ایمنی عمومی کانادا[1] مرجعیت دارد[2] و جنبه‌های عملیاتی امنیت سایبری توسط مرکز سایبری[3] وابسته به سازمان امنیت ارتباطات مدیریت می‌شود[4]. مرز مسئولیت‌ها و حوزه اختیارات نهادهای ذی‌ربط شامل سازمان امنیت ارتباطات، سازمان اطلاعات امنیت کانادا و نیروهای مسلح کانادا بسیار ظریف است و همگی تحت‌نظارت یا تحت‌مدیریت سطوح عالی دولتی و کابینه وزرا فعالیت می‌کنند. در سازمان ایمنی عمومی کانادا نهادی به نام ریاست کل امنیت سایبری ملی[5] وجود دارد که به معاون اول دولت (دومین مقام عالی غیرنظامی) گزارش می‌دهد[6].

از منظر تاریخی، توانمندی‌های سایبری نظامی کانادا ماهیت دفاعی دارند. البته سایر کاربردهای آن در اسناد سیاست‌های وزارت دفاع ملی و نیروهای مسلح هم پیش‌بینی شده‌است و در سال ۲۰۱۹ برای اولین بار در کانادا نیروی سایبری جهت داشتن آمادگی در نبردهای سایبری تهاجمی تشکیل شد. لازم به ذکر است که هرگونه موارد کاربرد توانمندی‌های سایبری تهاجمی در کانادا همانند سایر دارایی‌ها و عملیات‌های نظامی

1. Public Safety Canada

۲. رجوع شود به:

Public Safety Canada, 'Cyber Security in the Canadian Federal Government', 2018, https://www.publicsafety.gc.ca/cnt/ntnlscrt/cbr-scrt/fdrl-gvrnmnt-en.aspx

3. Cyber Center

۴. رجوع شود به:

Public Safety Canada, 'Speech on Canada's evolving national security architecture in a constantly changing and very difficult world', 15 January 2019, https://www.canada.ca/en/public-safety-canada/news/2019/01/speech-on-canadasevolving-national-security-architecture-in-a-constantlychanging-and-very-difficult-world.html

5. Director General for National Cyber Security

۶. رجوع شود به:

Public Safety Canada, 'Speech on Canada's evolving national security architecture in a constantly changing and very difficult world', 15 January 2019, https://www.canada.ca/en/public-safety-canada/news/2019/01/speech-on-canadasevolving-national-security-architecture-in-a-constantlychanging-and-very-difficult-world.html

تهاجمی باید به تایید دولت برسد و این توانمندی‌ها نیز تحت همان مقررات شدید نظامی هستند که در مورد سایر توانمندی‌ها و دارایی‌های نظامی اعمال می‌شود[۱]. به‌همین‌ترتیب، انجام عملیات‌های سایبری تهاجمی مستلزم کسب تایید وزیر دفاع ملی و وزیر امور خارجه است[۲].

ستاد مشترک فرماندهی نیروهای سایبری[۳] وظیفه نظارت و کنترل عملیات‌های سایبری کانادا را برعهده دارد. افسر ارشد اطلاعات دفاعی (DCIO)[۴] نیز وظیفه توسعه توانمندی‌ها و حفظ آمادگی سایبری را برعهده دارد و تحت امر رئیس ستاد دفاع و معاون دفاع (مقام ارشد وزارت دفاع ملی) انجام وظیفه می‌کند[۵]. وظیفه توسعه توانمندی‌های سایبری نظامی و فرماندهی و نظارت عملیاتی و راهبردی، ارتباطات، محاسبات و اطلاعات به افسری با درجه تک‌ستاره[۶] با عنوان رئیس کل سایبری[۷] تفویض شده‌است که تحت فرمان افسر ارشد اطلاعات دفاعی خدمت می‌کند[۸]. مرکز عملیات‌های شبکه‌ای نیروهای

---

۱. رجوع شود به:
Canadian Armed Forces, 'Strong, Secure, Engaged: Canada's Defense Policy', p. 72. For more information on the CAF's cyber planning,
https://www.canada.ca/en/department-nationaldefence/corporate/reports-publications/proactive-disclosure/cow-estimates-a-2019-20/joint-capabilities.html.

۲. رجوع شود به:
Numerous statements made during a Public Safety Committee meeting, 22 March 2018,
https://openparliament.ca/committees/public-safety/42-1/101/?singlepage=1

3. Joint Force Cyber Component Commander

4. Defense Chief Information Officer

۵. رجوع شود به:
Len Bastien (Defense Chief Information Officer and Assistant Deputy Minister, Information Management, Department of National Defense) statement at the National Defense Committee, 30 January 2018,
https://openparliament.ca/committees/national-defence/42-1/77/len-bastien-1/only

۶. One-star rank، همان

7. General Director Cyber

۸. رجوع شود به:
Commodore Richard Feltham (Director General, Cyberspace, Department of National Defense) statement at the National Defense Committee, 30 January 2018,
https://openparliament.ca/committees/national-defence/42-1/77/commodore-richard-feltham-1/only.

کانادا[1] نیز مسئولیت دفاع و رصد شبکه‌های وزارت دفاع ملی رابرعهده دارد[2] که البته حوزه فعالیت‌های آن به‌طور دقیق مشخص نیست. علت این امر آن است که نظارت بر شبکه‌های پشتیبان و داده‌های دولتی در محدوده وظایف سازمان امنیت ارتباطات و سازمان خدمات مشترک کانادا[3] نیز قرار دارد. آگاهی از موقعیت سایبری نیز ازجمله وظایف سازمان اطلاعات امنیت کانادا، سازمان امنیت ارتباطات، فرماندهی اطلاعات نیروهای کانادا[4] و واحدهای پشتیبانی سایبری «گروه عملیات‌های اطلاعات نیروهای مسلح»[5] محسوب می‌شود. دولت در سال ۲۰۱۹ تلاش‌های جدی برای ادغام این مراکز اطلاعاتی متنوع انجام داد[6].

توانمندی‌های محوری در زمینه اطلاعات سایبری

سازمان امنیت ارتباطات به‌عنوان نهاد متولی در زمینه توانمندی‌های محوری حوزه اطلاعات سایبری کانادا محسوب می‌شود و با ریاست غیرنظامی تحت‌نظارت وزارت دفاع ملی فعالیت می‌کند. این سازمان که تخصص فنی آن در سطح بین‌المللی شناخته‌شده است با عضویت کانادا در ائتلاف پنج چشم توانسته‌است توانمندی‌های خود را ارتقا بخشد. از آنجایی که سازمان امنیت ارتباطات همزمان مسئولیت امور مربوط به

1. Canadian Forces Network Operations Center

۲. رجوع شود به:
LCDR J.T.D.S. Turner, 'Royal Canadian Navy Cyber Incident Response Team', Canadian Forces College, 2016, p. 3,
https://www.cfc.forces.gc.ca/259/290/318/192/turner.pdf.

3. Shared Services Canada
4. Canadian Forces Intelligence Command
5. Armed Forces Information Operations Group

۶. رجوع شود به وب‌سایت رسمی دولت کانادا:
'Canadian Armed Forces Cyber Activities', 2019,
https://www.canada.ca/en/departmentnational-defence/corporate/reports-publications/proactive-disclosure/cow-estimates-a-2019-20/joint-capabilities.html.

اطلاعات سایبری و امنیت سایبری را نیز برعهده دارد، کیفیت هر دو حوزه به‌دلیل ادغام توانمندی‌ها بهبود یافته‌است.

سازمان امنیت ارتباطات کانادا در زیست‌بومی فعالیت می‌کند که در آن مسئولیت گردآوری اطلاعات انسانی خارجی و نیز تامین امنیت داخلی برعهده سازمان اطلاعات سری[1] کاناداست. همانند سایر شرکای ائتلاف پنج چشم، نهاد دفاعی کانادا نیز توانمندی‌های اطلاعاتی تخصصی دارد که تحت ستاد فرماندهی اطلاعات نیروهای کانادا[2] به کار گرفته می‌شوند. از نظر بودجه و دسترسی جغرافیایی، جامعه اطلاعاتی کانادا در سطح پایین‌تری نسبت به ایالات متحده و بریتانیا قرار دارد. البته به لطف هم‌پیمانان کانادا، این کشور از سطح دسترسی بالایی برخوردار است که از نقاط‌قوت مهم آن به‌شمار می‌رود.

توانمندی و وابستگی سایبری

توانمندی دیجیتال کانادا نسبتا بالاست، به‌طوری‌که نرخ نفوذ اینترنت در این کشور بالای ۹۰ درصد است[3]. میزان استفاده از تلفن همراه (۹۰ درصد خانوارها) در کانادا بسیار بیشتر از خط ثابت تلفن (۴۰ درصد) است و یک‌سوم خانوارها تنها از خدمات وایرلس (بی‌سیم) استفاده می‌کنند[4]. به‌طور کلی، بخش فناوری اطلاعات و ارتباطات کانادا از نرخ رشد بالایی برخوردار است[5].

1. Secret Intelligence Service
2. Canadian Forces Intelligence Command

۳. رجوع شود به:
International Telecommunication Union, 'Core Household Indicators', June 2019, https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2019/CoreHouseholdIndicators_Jun2019.xlsx.

۴. رجوع شود به:
Canadian Wireless and Telecommunications Association, 'Facts & Figures', 2019, https://www.cwta.ca/facts-figures.

۵. رجوع شود به:
International Trade Administration (United States), 'Canada: Country Commercial Guide', 3 August 2020, https://www.trade.gov/knowledge-product/canada-information-andcommunications-technology-ict#:~:text=The%20Canadian%20ICT%20sector%20is,with%20%249.3%20billion%20in%202019.

باآنکه سیاست‌های سختگیرانه کانادا فعالیت شرکت‌های آمریکایی مخابراتی و عرضه‌کننده اینترنت را در آن محدود می‌کند، اما دو کشور سطح بالایی از ادغام سایبری دارند که بیشتر مزایای آن (به‌ویژه از نظر جبران آسیب‌پذیری‌ها و مدیریت وابستگی‌هایش) به کانادا می‌رسد. ایالات متحده مقصد اصلی صادرات فناوری اطلاعات و ارتباطات کانادا محسوب می‌شود و در عین حال، دومین منبع واردات فناوری اطلاعات و ارتباطات آن نیز است[۱]. مشابه همکاری نزدیک دوکشور در عرصه دفاع هوایی، در حوزه حفاظت از زیرساخت‌های حیاتی نیز کانادا و آمریکا با هم مشارکت می‌کنند.

تجربه کانادا در تولید تلفن همراه برند بلک‌بری که زمانی از پیشتازان نوآوری و با محبوبیت جهانی بود[۲]، بازتاب ظرفیت دیجیتال و نیز چالش کانادا در حفظ مرز نوآوری بازار است. دولت کانادا از دیرباز در توسعه اقتصاد دیجیتال نقش فعالی داشته‌است. به‌عنوان مثال، کانادا در سال ۲۰۱۷ راهبرد ملی هوش مصنوعی را اجرا کرد[۳]. به‌علاوه، این کشور با اجرای طرحی ابتکاری در زمینه ترویج نوآوری در سال ۲۰۱۷ چند منطقه که دارای تعداد زیادی دانشگاه و شرکت‌های فناوری پیشرفته بودند را به‌عنوان خوشه‌های برتر[۴] در پنج حوزه پژوهشی مانند هوش مصنوعی و فناوری دیجیتال معرفی کرد[۵]. در این

۱. همان

۲. پس از مدتی شرکت آمریکایی اپل توانست جایگاه آن را با تلفن آیفون تصاحب کند.

۳. رجوع شود به:

OECD, Digital Economy Outlook 2020, Chapter 11, 'Artificial intelligence', https://www.oecd-ilibrary.org/sites/bb167041-en/1/3/11/index.html?itemId=/content/publication/bb167041-en&_csp_=509e10cb8ea8559b6f9cc53015e8814d&itemIGO=oecd&itemContentType=-book#section-213.

4. Superclusters

۵. این ابتکار با هدف تقویت سرمایه‌گذاری در حوزه‌های تعیین‌شده و با تخصیص گرنتی در حدود ۷۵۰ میلیون دلار آمریکا اجرا شد. برای دریافت جزئیات بیشتر به وب‌سایت رسمی دولت کانادا رجوع شود:

'About Canada's Supercluster Initiative program', 1 December 2020, https://www.ic.gc.ca/eic/site/093.nsf/eng/00016.html.

میان، تورنتو با داشتن ۲۶ درصد از خروجی بخش فناوری اطلاعات و ارتباطات کانادا قطب اصلی صنعت مخابرات این کشور است و سومین بخش فناوری و دومین مرکز مالی بزرگ در شمال آمریکا به‌شمار می‌رود[۱].

راهبرد ملی امنیت سایبری (۲۰۱۸) بر افزایش تعداد شرکت‌های سایبری و تقویت نوآوری متمرکز است[۲] و منشور دیجیتال کانادا (۲۰۱۹) نیز بر ضرورت افزایش همکاری دولت با بخش خصوصی و دانشگاه‌ها جهت گسترش تخصص‌های سایبری تاکید دارد[۳]. کانادا با داشتن ۴ خوشه نوآوری در میان فهرست ۱۰۰ خوشه برتر سازمان جهانی مالکیت فکری (وایپو)[۴] هم‌تراز بریتانیا (۴) و ژاپن (۵) محسوب می‌شود[۵].

کانادا در حوزه پژوهش و به‌کارگیری هوش مصنوعی نیز جایگاه مناسبی دارد. طبق رتبه‌بندی سازمان همکاری اقتصادی و توسعه از نظر تعداد مقالات هوش مصنوعی با بیشترین ارجاع، کانادا رتبه هشتم را دارد[۶]. با این حال به نقل از مهم‌ترین موسسه پژوهشی کانادا، اگرچه این کشور اولین کشوری است که در سال ۲۰۱۷ راهبرد ملی هوش

۱. رجوع شود به:
Toronto Global, 'Quick Facts',
https://torontoglobal.ca/Discover-Toronto-region/Toronto-region-quick-facts.

۲. رجوع شود به:
Innovation, Science and Economic Development Canada, 'Canada's Digital Charter in Action: A Plan by Canadians, for Canadians', 2019, https://www.ic.gc.ca/eic/site/062.nsf/vwapj/Digitalcharter_Report_EN.pdf/$file/Digitalcharter_Report_EN.pdf

۳. رجوع شود به:
Public Safety Canada, 'National Cyber Security Strategy -Canada's Vision for Security and Prosperity in the Digital Age', 2018,
https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf.

4. World Intellectual Property Organization

۵. رجوع شود به:
Cornell University, INSEAD and the World Intellectual Property Organization, 'Global Innovation Index 2020: Who Will Finance Innovation?', pp. 54-6,
https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2020.pdf

۶. رجوع شود به:
OECD, 'Measuring the Digital Transformation: A Roadmap for the Future', 2019, p. 37,
https://www.oecd.org/publications/measuring-the-digital-transformation-9789264311992-en.htm

مصنوعی خود را تدوین و اجرا کرده‌است، اما از آن پس از بیشتر کشورهایی که برنامه‌های مشابهی را اجرا کرده‌اند، عقب افتاده‌است[۱].

نیروهای مسلح کانادا وابستگی زیادی به سامانه‌های دیجیتال و ارتباطات مبتنی بر فناوری‌های فضایی دارند. اگرچه این نهاد خود دارای توانمندی‌های سایبری بالایی است، ولی با توجه به این‌که از سال ۱۹۵۷ بخشی از فرماندهی دفاع هوافضای شمال آمریکا (NORAD)[۲] ایالات متحده و کانادا محسوب می‌شود، از موقعیت منحصربه‌فردی در این حوزه برخوردار است. کانادا به‌دلیل مرزهای طولانی با ایالات متحده وابستگی زیادی به دارایی‌های مخابراتی زمینی آمریکا دارد. کانادا همچنین پس از چندین دهه همکاری فضایی با کشورهای ایالات متحده، بریتانیا، فرانسه و آلمان، فرماندهی ترکیبی نیروهای فضایی (CFSCC)[۳] را با همکاری آن‌ها در سال ۲۰۱۹ بنیان‌گذاری کرد[۴].

امنیت و تاب‌آوری سایبری

برنامه‌ها و سیاست‌های متعدد کانادا که اغلب در قالب سازمان‌های منطقه‌ای و استانی اجرا می‌شوند گواهی بر سطح بالای آمادگی آن برای واکنش به موقعیت‌های سایبری اضطراری است[۵]. به‌عنوان مثال، کانادا برنامه‌ای جامع به نام برنامه مدیریت

۱. رجوع شود به:
Canadian Institute for Advanced Research, 'Building an AI World: Report on National and Regional AI Strategies Second Edition', May 2020,
https://cifar.ca/wp-content/uploads/2020/10/building-an-ai-world-second-edition.pdf

2. North American Aerospace Defense Command

3. Combined Force Space Component Command

۴. رجوع شود به:
Cody Chiles, 'CFSCC establishment ceremony held at Vandenberg', Air Force Space Command, 2 October 2019,
https://www.afspc.af.mil/News/Article-Display/Article/1983986/cfscc-establishment-ceremony-held-at-vandenberg

۵. رجوع شود به وب‌سایت رسمی دولت کانادا:
'Emergency management organizations', Get Prepared website,
https://www.getprepared.gc.ca/cnt/rsrcs/mrgnc-mgmt-rgnztns-en.aspx

رویداد امنیت سایبری[1] تدوین کرده‌است که مشتمل بر فهرست همه ذینفعان و فعالیت‌ها و اقدامات لازم در زمان وقوع رویدادهای امنیت سایبری است[2]. نهادهای تنظیم‌گری صنعتی و بازیگران غیردولتی مکمل نیروهای دولتی در حوزه مقررات هستند. مرکز امنیت سایبری کانادا میزبان گروه ملی پاسخ اضطراری رایانه‌ای[3] است[4] و سامانه‌های نظامی نیز تحت‌نظارت نیروهای مسلح کانادا و وزارت ملی دفاع هستند که رویه‌های شفافی در گزارش‌دهی و ارجاع مسائل به مقامات ذی‌ربط دارند[5].

کانادا از بلوغ کافی در حفاظت از زیرساخت‌های حیاتی خود در برابر تهدیدهای سایبری برخوردار است[6]. دولت فهرستی از دارایی‌های زیرساختی حیاتی کشور در اختیار دارد که در صورت درخواست اپراتورهای آن‌ها، سازمان امنیت ارتباطات موظف به حمایت از آن‌هاست (این فهرست در دسترس عموم قرار ندارد).

مشارکت‌های بخش‌های خصوصی و دولتی از دیگر عناصر تاب‌آوری کانادا هستند که نهادهایی مانند اجلاس فرابخشی ملی[7] دولت‌های فدرال/استانی/ منطقه‌ای، زیرساخت‌های حیاتی و کارگروه زیرساخت‌های حیاتی فدرال/استانی/منطقه‌ای[8] را به

1. Cyber Security Event Management Plan

۲. رجوع شود به وب‌سایت رسمی دولت کانادا:
'Government of Canada Cyber Security Event Management Plan (GC CSEMP) 2019',
https://www.canada.ca/en/government/system/digital-government/onlinesecurity-privacy/security-identity-management/governmentcanada-cyber-security-event-management-plan.html.

3. National Computer Emergency Response Team

۴. رجوع شود به:
Canadian Centre for Cyber Security, 'About the Cyber Centre',
https://www.cyber.gc.ca/en/about-cyber-centre

۵. رجوع شود به:
Public Works and Government Services Canada, 'Defensive Cyber Operations', Letter of Interest, Solicitation No. W6369-17DE25/B, 2017, pp. B1-3.

۶. رجوع شود به:
'Government of Canada, Cyber Security Event Management Plan (GC CSEMP) 2019'

7. National Cross-Sector Forum

8. Federal-Provincial-Territorial Critical Infrastructure Working Group

هـم پیونـد می‌دهند. تقویت همکاری بیـن ذینفعان امنیت سـایبری در بخش خصوصی (ازجمله در بخش‌های مالی، انرژی و مخابرات) و دولت هدف اصلی شبکه تبادل اطلاعات امنیتی کانادا[1] محسوب می‌شود.

در همه حوزه‌های زیرساخت‌های حیاتی وابستگی قابل‌ملاحظه‌ای بین کانادا و ایالات متحـده وجـود دارد. به‌عنـوان مثـال، قطعی بـرق در هریـک از این کشـورها می‌تواند روی دیگری نیز تاثیر داشـته باشـد[2]. درواقع، عرصه سـایبری یکی از اجزای اصلی همکاری‌های جامـع دفاعـی کانـادا و ایـالات متحـده به‌شـمار مـی‌رود[3]. در سـال ۲۰۰۴، دوکشـور پیمانی بـرای تامیـن امنیـت سـایبری زیرسـاخت‌های حیاتی خـود امضا کردنـد[4]. ابتکار مشـترک سـازمان ایمنـی عمومی کانادا[5] و وزارت دفـاع داخلی ایالات متحده نیـز در جهت افزایش همکاری‌هـای دو کشـور در زمینه مدیریت رویدادهای سـایبری، اشـتراک‌گذاری اطلاعات مربوط به امنیت سـایبری با بخش خصوصی و همکاری مسـتمر برای اجرای پویش‌های آگاه‌سازی عمومی اجرا می‌شود[6].

کانادا همانند سـایر کشـورهای ائتلاف پنج چشم در معرض حملات سایبری متنوعی

1. Canadian Network for Security Information Exchange

۲. رجوع شود به:
For further information, see Public Safety Canada, ‘Critical Infrastructure’, updated 19 August 2020, https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx

۳. رجوع شود به:
National Defense and the Canadian Armed Forces, ‘The Canada-U.S. Defense Relationship’, Backgrounder, 4 December 2014, http://www.forces.gc.ca/en/news/article.page?doc=the-canada-u-s-defence-relationship/hob7hd8s.

۴. «توافـق بیـن دولـت کانـادا و دولـت ایـالات متحـده آمریـکا دربـاره همـکاری علـم و فنـاوری جهـت حفاظـت از زیرسـاخت‌های حیاتـی و امینـت مـرزی»، مـورخ ۱ ژوئـن ۲۰۰۴
https://www.treaty-accord.gc.ca/text-texte.aspx?id=105000.

5. Public Safety Canada

۶. رجوع شود به:
Public Safety Canada, ‘Cybersecurity Action Plan between Public Safety Canada and the Department of Homeland Security’, 2015, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cybrscrt-ctn-plan/index-en.aspx.

است: جرائم سایبری، زورگیری سایبری، تجاوز به حریم خصوصی، نفوذهای سایبری دولتی و استفاده از فضای سایبری برای اعمال نفوذ سیاسی[۱].

طبق پیمایشی که در سال ۲۰۲۰ با مشارکت فعالان صنعت، دولت و نهادهای غیرانتفاعی در کانادا انجام شد، بیشتر شرکت‌کنندگان در مطالعه به افزایش نگرانی از تهدیدهای سایبری اشاره کردند. البته تعداد سازمان‌هایی که قصد گسترش سرمایه‌گذاری در امنیت سایبری داشتند نیز کاهش یافته‌بود[۲].

با توجه به این‌که کانادا از سال ۲۰۱۰ امنیت سایبری را در شمار اولویت‌های اصلی خود قرار داده‌است، سرمایه‌گذاری بیشتری در زمینه امنیت سایبری پس از انتشار راهبرد امنیت سایبری ۲۰۱۸ انجام داده‌است، رویکرد آن نسبت به تاب‌آوری سایبری کاملا توسعه‌یافته است و به‌طور کلی، عملکرد آن در این محور تقویت شده‌است. رتبه نهم کانادا در شاخص جهانی امنیت سایبری ۲۰۱۸ به خوبی مؤید این حقیقت است[۳].

به‌نقل از سازمان ایمنی عمومی کانادا، همکاری در قالب ائتلاف اطلاعات پنج چشم در تامین تاب‌آوری امنیت سایبری کشورهای عضو نقش محوری دارد و این کشورها در زمینه توافقات راهبردی امنیت سایبری به‌ویژه از منظر اشتراک‌گذاری اطلاعات، پاسخ سایبری متوازن و هماهنگی سیاست‌های بین‌المللی به پیشرفت شایانی دست یافته‌اند[۴].

---

۱. مرکز امنیت سایبری کانادا،
'National Cyber Threat Assessment 2020', 20 November 2020, https://cyber.gc.ca/sites/default/files/publications/ncta-2020-e-web.pdf.

۲. مرکز ثبت اینترنت کانادا (CIRA)
'CIRA 2020 Cyber Security Report', https://www.cira.ca/cybersecurity-report-2020.

۳. اتحادیه بین‌المللی مخابرات،
'Global Cybersecurity Index 2018', p. 56, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

۴. رجوع شود به:
Amaliah Reiskind, 'Canada's Cyber Security: A Discussion with Public Safety Canada', NATO Association Canada, 22 August 2018, http://natoassociation.ca/canadas-cyber-security-a-discussion-with-public-safety-canada

رهبری جهانی در عرصه سایبری

کانادا در رویدادهای بین‌المللی حوزه فضای سایبری حضوری فعال دارد و سعی می‌کند در شکل‌دهی به گفتمان جهانی سایبری تاثیرگذار باشد. برنامه عمل امنیت سایبری ملی کانادا[1] در سال ۲۰۱۹ مشتمل بر راهبرد دیپلماتیک جامعی است که با هدف شکل‌دهی به محیط امنیت سایبری بین‌المللی در راستای منافع کانادا ازطریق ارتقای همکاری بین ذینفعان در حوزه‌های امنیت سایبری و جرائم سایبری و همچنین حمایت از اینترنت باز، آزاد و ایمن پیگیری می‌شود. طبق این رویکرد، کانادا در پی مشارکت در مذاکرات و گفت‌وگوهای بین‌المللی حوزه امنیت سایبری مانند گروه کارشناسان دولتی سازمان ملل است[2]. علاوه بر این، کانادا مجموعه‌ای از برنامه‌های ظرفیت‌سازی ضدتروریسم و ضدجنایت راه‌اندازی کرده‌است که ازطریق آن‌ها حدود ۱۵/۶ میلیون دلار کانادا (۱۲ میلیون دلار آمریکا) به ظرفیت‌سازی در آمریکای شمالی و جنوبی و جنوب شرق آسیا اختصاص داده‌است[3]. کانادا همچنین از امضاکنندگان فراخوان اعتماد و امنیت در فضای سایبری پاریس (۲۰۱۸)[4] است و کنوانسیون جرائم سایبری[5] را تصویب کرده‌است[6]. کانادا در کنار دیگر اعضای گروه ۷ در زمینه ایجاد سازوکار واکنش سریع[7] با هدف به‌اشتراک‌گذاری اطلاعات و تحلیل‌های تهدیدها جهت شناسایی فرصت‌های واکنش سریع و هماهنگ

1. National Cybersecurity Action Plan (2019-2024)

۲. رجوع شود به:
UN Office for Disarmament Affairs, 'Developments in the field of information and telecommunications in the context of international security', https://www.un.org/disarmament/ict-security.

۳. رجوع شود به:
Reiskind, 'Canada's Cyber Security: A Discussion with Public Safety Canada'.

4. Paris Call for Trust in Security in Cyberspace (2018)
5. Convention on Cyber Crime

۶. رجوع شود به:
Chart of signatures and ratifications of Treaty 185, Council of Europe, 2019, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=zrS8ISMY

7. Rapid Response Mechanism

به حمله‌های سایبری مشارکت داشته‌است[۱]. با اینکه کانادا در سال ۲۰۱۹ اعلام کرد قصد پیوستن به مرکز عالی دفاع سایبری مشترک ناتو[۲] را دارد، اما از مدت‌ها قبل از این تاریخ نیز در ائتلاف ناتو برای تقویت ظرفیت‌های سایبری حضور فعالی داشته‌است. به‌عنوان مثال، کانادا در سال ۲۰۱۳ در پروژه چندملیتی توسعه توانمندی‌های دفاع سایبری جهت بهبود توانمندی‌های رصد و دفاع ناتو شرکت کرد[۳]. کانادا در تیم رمزنگاری ناتو نیز به‌طور جدی فعالیت می‌کند و نماینده‌ای در حوزه سیاست‌گذاری سایبری در مقر ناتو دارد.

افزون بر این‌ها، کانادا در ابتکاری به رهبری ایالات متحده (در قالب ابتکار بازدارندگی سایبری) به اعلام برائت از بازیگران دولتی عرصه فعالیت‌های سایبری خصمانه می‌پردازد[۴]. از زمان آغاز این ابتکار در سال ۲۰۱۸، کانادا به‌طور هماهنگ (یا همزمان) با شرکایش به حدود ۲۲ کشور اتهام وارد کرده‌اند.

توانمندی‌های سایبری تهاجمی

کانادا با صراحت از توانایی و اراده خود در استفاده از توانمندی‌های سایبری تهاجمی ضمن الزام به قوانین بین‌المللی سخن می‌گوید. البته توانمندی‌های سایبری تهاجمی

۱. رجوع شود به:
Stephanie Carvin, 'Canada and Cyber Governance: Mitigating Threats and Building Trust', in Governing Cyberspace during a Crisis in Trust, Centre for International Governance Innovation, 2019, p. 93, https://www.cigionline.org/sites/default/files/documents/Cyber%20Series%20Web2.pdf
2. NATO Cooperative Cyber Defense Center of Excellence

۳. انجمن ناتو کانادا،
'In Pursuit of Total and Unbreachable Protection of Cyberspace, Part I: Canada, a Leader in Cyber Defense', 2018,
http://natoassociation.ca/in-pursuit-of-total-and-unbreachable-protection-ofcyberspace-part-i-canada-a-leader-in-cyber-defence

۴. رجوع شود به:
Communications Security Establishment, 'Canada and Allies Identify China as Responsible for Cyber-Compromise', 20 December 2018,
https://cse-cst.gc.ca/en/media/media-2018-12-20.

کانادا هنوز در مراحل ابتدایی هستند و اگرچه وزارت دفاع ملی و نیروهای مسلح کانادا تا حدی مجهز به توانمندی‌های سایبری هستند، اما در عملیات‌های سایبری به سازمان امنیت ارتباطات (تحت‌نظارت وزارت دفاع ملی) که سازمانی غیرنظامی است، وابستگی بسیار زیادی دارند. درنتیجه، در کانادا نیز همانند بریتانیا تمایز مشخصی بین توانمندی‌های سایبری تهاجمی نظامی و غیرنظامی وجود ندارد و این دو کشور تنها از نظر مرجع قانونی (قوانین داخلی و بین‌المللی) که مبنای صدور مجوز سیاسی جهت استفاده از آن‌ها هستند، با یکدیگر تفاوت دارند. به همین دلیل، سازمان امنیت ارتباطات و ارتش کانادا در حال بررسی تشکیل یک نیروی سایبری ملی متشکل از نیروهای نظامی و غیرنظامی همانند مدل بریتانیا است[۱]. این ایده به‌دنبال تصویب قانون سازمان امنیت ارتباطات[۲] مورخ سال ۲۰۱۹ مطرح شد که به سازمان امنیت ارتباطات امکان انجام عملیات‌های سایبری تهاجمی از جانب وزارت دفاع ملی و نیروهای مسلح کانادا را می‌دهد[۳]. به‌مدد این قانون، کانادا هم‌اکنون در موقعیت بهتری برای ارتقا و استفاده گسترده از توانمندی‌های سایبری تهاجمی قرار دارد و در این راستا می‌تواند از تجارب و دانش هم‌پیمانان خود مانند ایالات متحده، بریتانیا و استرالیا جهت استفاده از توانمندی‌های سایبری و ساخت و توسعه توانمندی‌های جدید بهره‌مند شود.

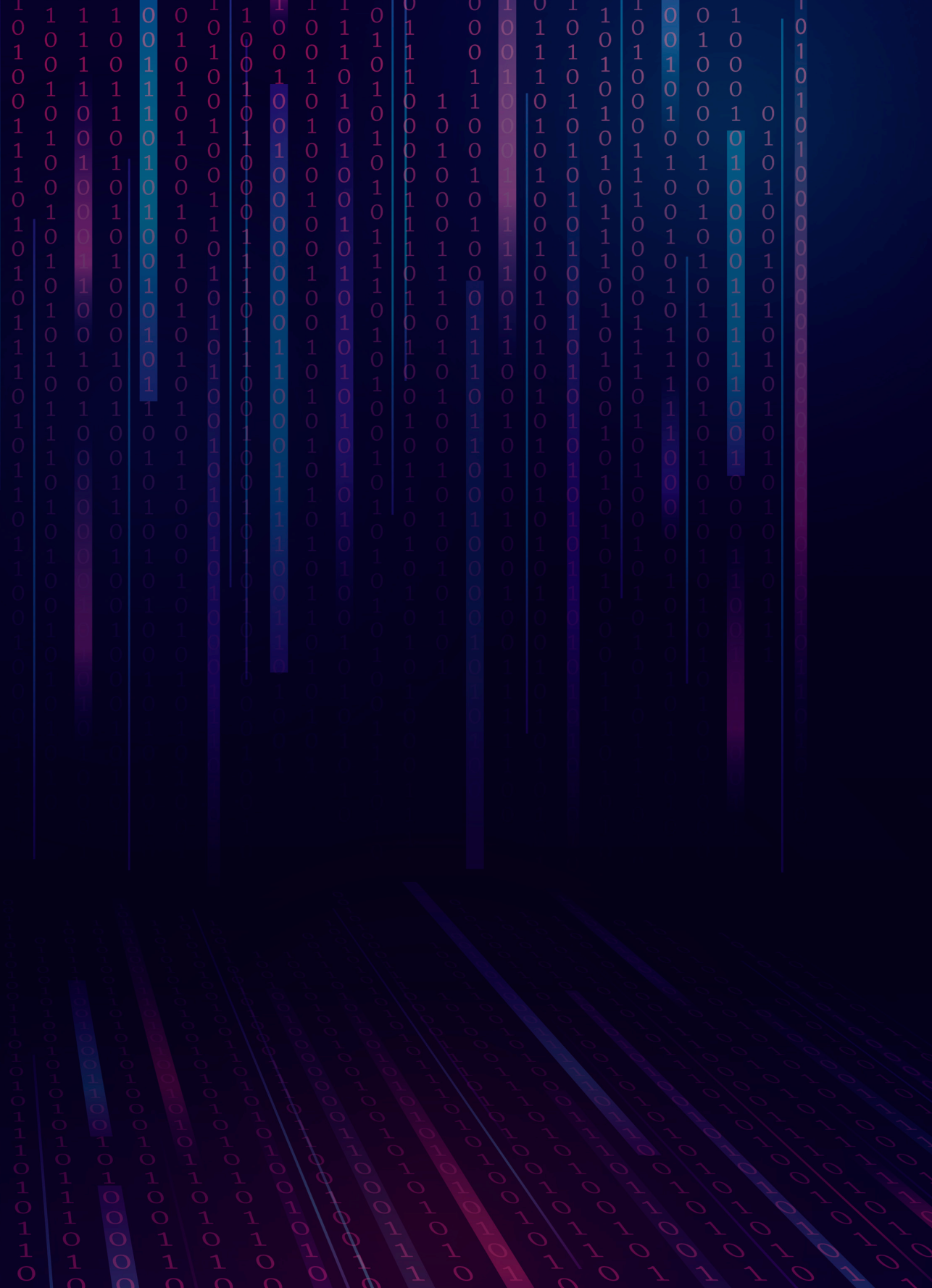
۱. رجوع شود به:

Government of Canada, 'Future Force Design', 17 April 2019, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/departmental-plans/departmentalplan-2019-20-index/planned-results/future-force-design.html.

2. CSE Act

۳. رجوع شود به:

Government of Canada, 'Order Fixing August 1, 2019 as the Day on which Part 3 of that Act Comes into Force: SI/2019-70', Canada Gazette, Part II, vol. 153, no. 15, http://www.gazette.gc.ca/rp-pr/p2/2019/2019-07-24/html/si-tr70-eng.html.



۴

استرالیا

راهبردهای امنیت سایبری استرالیا در راستای ارتقای امنیت ملی، امنیت سایبری تجاری و بنیان صنعتی برای دستیابی به اقتدار و خودکفایی و توسعه نیروی کار و شهروندی بین‌المللی مطلوب تدوین شده‌اند. اداره کل سیگنال‌های استرالیا (ASD)[1] نهاد اصلی در امور سایبری و بانفوذترین نهاد در سیاست‌گذاری سایبری استرالیا است. از سال ۲۰۱۷ همزمان با تاسیس لشگر جنگ اطلاعات (IWD)[2]، استرالیا همواره در زمینه تهیه و توسعه راهبردها و سیاست‌های سایبری نظامی خود فعالیت داشته‌است. استرالیا توانسته‌است به پیشرفت‌های قابل‌ملاحظه‌ای در زمینه تحقیقات و صنایع فناوری اطلاعات و ارتباطات دست یابد، هرچند هنوز بنیان‌های آن محدود است. با آنکه بودجه دفاعی و اطلاعاتی استرالیا چندان زیاد نیست، اما سطح توسعه‌یافتگی توانمندی‌های سایبری آن تا حد زیادی به‌واسطه عضویت ۷۰ ساله این کشور در ائتلاف پنج چشم قابل‌قبول است. استرالیا حضور پررنگی در عرصه دیپلماسی جهانی هنجارهای سایبری و ظرفیت‌سازی سایبری دارد. استرالیا در سال ۲۰۱۶ برای اولین بار به داشتن توانمندی‌های سایبری تهاجمی اذعان نمود. می‌توان گفت این کشور از طرفداران جدی ابتکار بازدارندگی سایبری ایالات متحده برای مقابله با فعالیت‌های سایبری سایر کشورهاست. درمجموع، استرالیا برای آنکه بتواند قدرت سایبری توانمندتری داشته باشد باید در زمینه آموزش عالی در این حوزه سرمایه‌گذاری کلانی انجام دهد و همزمان با آن، توانمندی‌های سایبری ملی خود را نیز توسعه بخشد.

1. Australian Signals Directorate
2. Information Warfare Division

راهبرد و مبنای نظری (دکترین)

اولین راهبرد امنیت سایبری استرالیا در سال ۲۰۰۹ پس از بازبینی راهبرد امنیت الکترونیک[1] (سال ۲۰۰۸) انتشار یافت[2]. این راهبرد مشتمل بر دو ابتکار اصلی بود: تشکیل تیم پاسخ فوری رایانه‌ای[3] به‌عنوان مکمل یا جایگزین تیمی که از سال ۱۹۹۴ فعالیت می‌کرد و در یکی از دانشگاه‌ها مستقر بود[4] و تاسیس مرکز عملیات‌های امنیت سایبری[5] ملی. البته باید خاطرنشان ساخت که این سند بیشتر شامل سیاست‌های لفاظانه بود تا عملی. درواقع، این سند حاوی اهداف بزرگی درباره موضوعاتی مانند حس مسئولیت‌پذیری مشترک بخش خصوصی و بخش دولتی، رویارویی با تهدیدهای فزاینده، حفاظت از ارزش‌های استرالیا، حفظ هویت، گسترش و ارتقای مهارت‌های نیروی انسانی و تقویت همکاری‌های بین‌المللی بود. در راهبرد مذکور متاسفانه بودجه جدیدی برای تحقق اهداف موردنظر به جز در حوزه امنیت ملی پیشنهاد نشده‌بود.

در آوریل ۲۰۱۶، دولت راهبرد امنیت سایبری جدیدی را به اجرا گذاشت[6]. دولت در راهبرد جدید که عنوان فرعی آن تحقق نوآوری، رشد و شکوفایی است، استفاده بهینه از فرصت‌های اقتصادی عصر اطلاعات و ارتقای امنیت را نیز مدنظر قرار داده است. مفاهیم

1. E-Security Strategy

۲. رجوع شود به:
Australian Government, Attorney-General's Department, 'Cyber Security Strategy', Canberra, November 2009.
https://www.enisa.europa.eu/topics/national-cyber-securitystrategies/ncss-map/AGCyberSecurity Strategyforwebsite.pdf

3. Computer Emergency Response Team

۴. رجوع شود به:
Gary Waters, 'National Cyber Emergency Policy for Australia: Critical Infrastructure', in Greg Austin (ed.), National Cyber Emergencies: The Return to Civil Defense (Abingdon: Routledge, 2020), pp. 93-105.

5. Cyber Security Operations Center

۶. رجوع شود به:
Australian Government, Department of the Prime Minister and Cabinet, 'Australia's Cyber Security Strategy: Enabling Innovation, Growth and Prosperity', Canberra, 2016.
https://www.homeaffairs.gov.au/cyber-security-subsite/files/PMCCyber-Strategy.pdf.

امنیتی موردتوجه در این سند همانند محتوای راهبردهای کشورهای دیگر ازجمله ایالات متحده، بریتانیا و فرانسه هستند: شناسایی، جلوگیری از/و پاسخ به تهدیدهای فضای سایبری ازطریق روش‌هایی مانند پیش‌بینی خطرات[1]. در مقایسه با راهبردهای پیشین، لحن اضطرار در این راهبرد قوی‌تر است و رویکردهای جدید بسیار زیادی نیز نسبت به مسائل امنیت سایبری مانند اشتراک‌گذاری اطلاعات بین دولت و بخش خصوصی دارد. همچنین، برای اولین بار در این سند استفاده دولت از توانمندی‌های سایبری تهاجمی برای جلوگیری از حمله‌های سایبری خصمانه یا پاسخ به آن‌ها جایز شمرده شده‌است.

گفتنی است همه فرایندهای برنامه‌ریزی برای تهیه راهبرد سایبری بخش غیرنظامی استرالیا به‌مدت ۱۸ ماه به‌طور موقت معلق شد. زیرا دولت در سال‌های ۲۰۱۵ و ۲۰۱۶ اصلاحات ساختاری گسترده‌ای را آغاز کرد که ازجمله می‌توان به تغییراتی در جایگاه اداره کل سیگنال‌های استرالیا، سازمان اطلاعات امنیتی استرالیا[2]، مرکز امنیت سایبری استرالیا[3] و اداره دادستان کل[4] اشاره کرد که همگی در جهت تاسیس وزارت کشور[5] جدید بودند (این وزارت سال ۲۰۱۷ به‌طور رسمی افتتاح شد).

استرالیا راهبرد امنیت سایبری جاه‌طلبانه‌تری در سال ۲۰۲۰ منتشر کرد که علاوه بر این‌که ردیف بودجه بسیار بیشتر از راهبردهای قبل را پیشنهاد داد، لحن آن نیز بیانگر عزمی راسخ‌تر برای توسعه امنیت سایبری بود[6]. در این سند از زبانی تندتر نسبت به

---

۱. همان، ص ۶.

2. Australian Security Intelligence Organization
3. Australian Cyber Security Center
4. Attorney General's Department
5. Department of Home Affairs

۶. رجوع شود به:
Australian Government, Department of Home Affairs, 'Australia's Cyber Security Strategy', Canberra, August 2020.
https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.

تهدیدهای کشورهای دیگر استفاده شده‌است (اگرچه دولت از سال ۲۰۱۲ بر ممنوعیت به‌کارگیری فناوری‌های هوآوی در سیستم‌های دولتی تاکید داشته‌است، اما در این سند نامی از کشور خاصی برده نشده‌است) و بر خطرهای ناشی از فناوری‌های همواره در حال تغییر و افزایش سطح ارتباط اینترنتی تاکید ویژه‌ای شده‌است. این سند نشان می‌دهد مساله امنیت سایبری به عمق تفکرات و مبنای نظری دولت استرالیا درباره امنیت ملی راه پیدا کرده‌است.

تغییرات راهبردهای سایبری استرالیا بین سال‌های ۲۰۱۶ و ۲۰۲۰ در سیاست دفاعی آن نیز منعکس شده‌است. به‌عنوان مثال، گزارش سیاست دفاعی وزارت دفاع (۲۰۱۶) حاوی اقدامات گسترده‌ای برای توسعه توانمندی‌های اطلاعاتی و سایبری به‌عنوان بخشی از سوگیری جدید کشور نسبت به جنگ در فضای اطلاعاتی است[۱]. در گزارش مذکور تهدیدهای سایبری یکی از شش محرک اصلی راهبرد نظامی استرالیا عنوان شده‌است[۲]. این سند بازتاب یکی از محورهای بنیادین سیاست امنیتی استرالیا و به‌عبارت دیگر تعمیق همکاری با آمریکا به‌ویژه ازطریق ادغام نیروهای نظامی در بالاترین سطح ممکن، تعامل‌پذیری و اشتراک‌گذاری اطلاعات (ازجمله اطلاعات مربوط به سیاست‌ها و عملیات‌های سایبری) [۳] است. طبق ارزیابی‌های دولت استرالیا، ایالات متحده حداقل به‌دلیل توانمندی‌های علمی و صنعتی آن تا دو دهه آینده همچنان قدرت اول سایبری جهان خواهد بود.

استرالیا همزمان با سازماندهی مجدد بخش غیرنظامی، اصلاحات ساختاری نیز در بخش نظامی در رابطه با فضای سایبری انجام داد. نیروی دفاعی استرالیا (ارتش)

۱. رجوع شود به:
Australian Government, Department of Defense, '2016 Defense White Paper', Canberra, 2016. https://www.defence.gov.au/WhitePaper/Docs/2016-Defence-White-Paper.pdf.

۲. همان، ص. ۴۱

۳. همان، ص. ۳۵

(ADF)[1] در ۳۰ ژوئن ۲۰۱۷ لشگر جنگ اطلاعات (IWD) جدیدی تشکیل داد که بایستی تحت‌فرماندهی گروه توانمندی‌های مشترک[2] (که رده نظامی آن معادل فرمانده هریک از نیروهای زمینی/هوایی/دریایی است) فعالیت می‌کرد.

یکی از اثرات اجتناب‌ناپذیر این اصلاحات تغییرات قابل‌توجه در مفاهیم عملیاتی و مبانی نظری حتی در بخش غیرنظامی بود. در سال ۲۰۱۸ دولت به این نتیجه رسید که راهبرد امنیت سایبری ۲۰۱۶ دیگر متناسب با اهداف کشور نیست و به همین دلیل نیز آن را به‌روزرسانی نکرد. درواقع، در آن زمان به‌دلیل افزایش تهدیدهای سایبری مانند استفاده فزاینده چین و روسیه از فضای سایبری برای مداخلات سیاسی، محیط سیاسی کشور متحمل تغییر زیادی شده‌بود.

در جولای ۲۰۲۰ استرالیا سند[3] به‌روزرسانی راهبرد دفاعی[4] و برنامه ساختار نیروها[5] را منتشر کرد[6] و به دنبال آن در آگوست همان سال راهبرد امنیت سایبری[7] جدید کشور را ارائه کرد. هر سه سند بیانگر افزایش نگرانی‌ها نسبت به تهدیدهای فضای سایبری، تعهد به تداوم اصلاحات و افزایش شتاب اصلاحات در برخی از حوزه‌ها و افزایش سرمایه‌گذاری هستند (به‌اعتقاد نخست‌وزیر استرالیا اسکات موریسون[8]، توانمندی‌های سایبری تهاجمی جدید بخش مهمی از قدرت بازدارندگی کشور به شمار

1. Australian Defense Force
2. Joint Capabilities Group

۳. رجوع شود به:
Australian Government, Department of Defense, '2020 Defense Strategic Update', Canberra, July 2020. https://www.defence.gov.au/StrategicUpdate-2020/docs/2020_Defence_Strategic_Update.pdf

4. Defense Strategic Update
5. Force Structure Plan

۶. رجوع شود به:
Australian Government, Department of Defense, '2020 Force Structure Plan', Canberra, July 2020. https://www.defence.gov.au/StrategicUpdate-2020/docs/2020_Force_Structure_Plan.pdf.

7. Cyber Security Strategy
8. Scott Morrison

می‌روند[۱].) در این اسناد برای اولین بار در تاریخ اسناد سیاست دفاعی استرالیا، تقویت توانمندی‌های سایبری و اطلاعاتی بیش از توانمندی‌های زمینی، هوایی و دریایی موردتاکید قرار داشتند. این سندها نشان می‌دهند دیدگاه دفاعی دولت به‌سمت مفهوم «اطلاعات به‌عنوان بخش تفکیک‌ناپذیر همه عملیات‌های نظامی» سوق پیدا کرده‌است[۲]. البته دولت و ارتش استرالیا (ADF) مفهوم «برتری اطلاعاتی»[۳] -مفهوم مورداستفاده آمریکا- را در اظهارات خود به‌کار نمی‌برند. در سال ۲۰۲۰، مبنای نظری جدیدی برای عملیات‌های فضای سایبری ارتش استرالیا منتشر شد که جزء اسناد طبقه‌بندی شده‌است. گفته می‌شود این سند مشابه مبنای نظری آمریکاست و فقط برخی از اولویت‌های آن با توجه به شرایط متفاوت استرالیا تغییر کرده‌است.

حکمرانی، فرماندهی و نظارت

کمیته امنیت ملی کابینه[۴] با ریاست نخست‌وزیر استرالیا وظیفه اتخاذ تصمیم‌های اصلی در زمینه سیاست امنیت کشور را برعهده دارد. درواقع، نخست‌وزیر در همه امور دولت صاحب‌اختیار است و فرماندهی کل قوا را برعهده دارد. به موازات این ساختار، فرمانده نیروهای دفاعی[۵] (ارتش) نیز در مسائل نظامی دارای مسئولیت‌های وزارت‌خانه‌ای (شامل همه نهادهای اطلاعاتی) و قانونی است. کمیته امنیت ملی کابینه مسئولیت سیاست‌های کلان مانند تایید راهبردهای جدید و اولویت‌های نهادها را

۱. رجوع شود به:
Australian Government, Prime Minister of Australia, 'Address - Launch of the 2020 Defense Strategic Update', Canberra, 1 July 2020.
https://www.pm.gov.au/media/address-launch-2020-defence-strategic-update.

۲. همان، ص. ۳۶

3. Information Dominance
4. National Security Committee of Cabinet
5. Chief of Defense Force

برعهـده دارد. کمیتـه بررسـی هزینه‌هـای کابینـه[1] نیز برنامه‌هـای بودجه را تاییـد می‌کند و البتـه به‌دلیـل اینکـه برخـی از اعضای آن در سـایر کمیته‌ها نیز عضو هسـتند، در مواردی صرفا به تصویب برنامه‌های موردتایید سـایر کمیته‌ها اکتفا می‌کند.

نهـاد اصلی اسـترالیا در حوزه اطلاعات سـایبری یعنی اداره کل سـیگنال‌های اسـترالیا به‌طور مستقیم به وزیر دفاع گزارش می‌دهد که وظیفه تایید عملیات‌ها و استانداردهای حفاظـت از حریـم خصوصـی شـهروندان را برعهـده دارد[2]. بنابرایـن باآنکـه ایـن نهـاد تحت‌نظارت سیاسـت غیرنظامی قرار دارد، اما باتوجه به اینکه ریاسـت آن فرمانده ارتش اسـت، تعداد زیادی از کارکنان آن نظامی هسـتند. اطلاعاتی درباره تعداد و توانمندی‌های نیروهای شاغل در اداره کل سیگنال‌ها منتشر نشده‌است.

در اواسـط سـال ۲۰۱۷ کـه لشـگر جنـگ اطلاعـات در ارتـش اسـترالیا تشـکیل شـد، مهم‌تریـن بخـش آن واحد مشـترک سـایبری[3] بود که طبق برنامه بایسـتی ظرف ده سـال نیروی‌هـای خـود را بـه ۱۰۰۰ نفـر افزایـش مـی‌داد. در ژانویـه ۲۰۱۸ ارتـش اسـترالیا اعـلام کرد واحد مشـترک سـایبری و واحد تازه‌تاسیس اطلاعات سـیگنالی مشترک[4] در کنار تیم‌های غیرنظامـی ارتـش تحت واحد جدیدی در لشـگر جنگ اطلاعات به نام فرماندهی سـایبری و اطلاعات سـیگنالی دفاعی (DSCC)[5] و به ریاسـت افسـری تک‌سـتاره با سابقه فرماندهی در تیم‌هـای اداره کل سـیگنال‌ها[6] فعالیـت خواهد کرد. هدف از تشـکیل این واحد جدید

1. Expenditure Review Committee of Cabinet

۲. رجوع شود به:

Australian Government, Australian Signals Directorate, 'Accountability'.
https://www.asd.gov.au/accountability

3. Joint Cyber Unit
4. Joint SIGINT Unit
5. Defense Signals Intelligence and Cyber Command

۶. رجوع شود به:

Australian Government, Department of Defense, 'Defense Chief Announces New Command', Canberra, 30 January 2018.
https://news.defence.gov.au/media/media-releases/defence-chief-announces-new-command.

سامان دادن به همه واحدها و نیروهای سایبری فعال در اداره کل سیگنال‌ها در یک ساختار فرماندهی منظم و هماهنگ بود[۱].

فرماندهی سایبری و اطلاعات سیگنالی دفاعی امکان هماهنگی و تجمیع امور عملیات‌های سایبری تهاجمی اداره کل سیگنال‌های استرالیا و نیز نظارت فرماندهی ارتش بر این امور را فراهم کرده‌است. درواقع، امور عملیات‌های سایبری تهاجمی از اختیارات اداره کل سیگنال‌ها محسوب می‌شود و درنتیجه لشگر جنگ اطلاعات در این زمینه اختیاری ندارد. لشگر جنگ اطلاعات بیشتر مسئولیت ارتقا، آموزش و حفظ کارکردهای فرماندهان ارتش را برعهده دارد[۲].

اداره کل سیگنال‌های استرالیا نهاد اصلی در امور فضای سایبری غیرنظامی است و وظایف خود را ازطریق مرکز امنیت سایبری استرالیا (ACSC)[۳] انجام می‌دهد. اداره کل سیگنال‌ها در امور سایبری غیرنظامی به وزیر کشور پاسخگوست و در امور سایبری بیشتر به نخست‌وزیر و وزیر دفاع گزارش می‌دهد. این اداره با سازمان اطلاعات امنیتی استرالیا (ASIO)[۴] نیز در عملیات‌های سایبری مشترک داخلی همکاری نزدیکی دارد.

توانمندی‌های محوری در زمینه اطلاعات سایبری

بخش اعظم توانمندی‌های استرالیا در زمینه اطلاعات سایبری در اداره کل سیگنال‌ها تجمیع شده‌است که با کارکردهای جنگ سایبری و امنیت سایبری آن ادغام شده‌اند.

۱. همان.

۲. لشگر جنگ اطلاعات این موضوع را چنین توضیح می‌دهد: این لشگر موظف به توسعه توانمندی‌های جنگ اطلاعاتی برای استفاده ارتش در همه فعالیت‌ها (مانند حفاظت از شبکه‌ها و سامانه‌های عملیاتی، اجرای رزمایش‌ها و رویدادهای آموزشی و حمایت از جامعه و منطقه در مواجهه با بلایا) است. این لشگر توانمندی‌های جنگ اطلاعاتی را می‌سازد و ارتش آن‌ها را به‌کار می‌گیرد. فرمانده عملیات‌های مشترک مسئولیت تطبیق نحوه اجرای توانمندی‌ها با دستورات دولت را برعهده دارد.

3. Australian Cyber Security Center

4. Australian Security Intelligence Organization

استرالیا تخصص و دسترسی سایبری خوبی در منطقه جنوب‌شرق و شرق آسیا به‌ویژه در چین و اندونزی دارد. اما توانمندی‌های سایبری اداره کل سیگنال‌های استرالیا برای مسافت‌های دور چندان توسعه‌یافته نیست و درنتیجه، در این زمینه به کشورهای ائتلاف پنج چشم وابسته است.

اداره کل سیگنال‌های استرالیا بخشی از نظام بالغ اطلاعات ملی این کشور است و با سایر عناصر ذی‌ربط در امنیت یعنی سازمان اطلاعات امنیتی استرالیا و سازمان خدمات اطلاعات سری استرالیا[1] همکاری مستمر دارد. گفتنی آنکه سازمان اطلاعات امنیتی استرالیا مسئولیت امنیت داخلی را برعهده دارد و سازمان خدمات اطلاعات سری استرالیا در زمینه عملیات‌های مخفی و گردآوری اطلاعات اشخاص در خارج از مرزها فعالیت دارد. استرالیا اداره اطلاعات ملی[2] را در سال ۲۰۱۸ به پیروی از ایالات متحده بنیان گذاشت تا به این ترتیب، دولت یگانه نهاد ذی‌ربط جهت هماهنگی و نظارت بر نهادهای فعال در زمینه گردآوری و تحلیل اطلاعات و نیز اجرای عملیات‌های مخفی باشد.

توانمندی و وابستگی سایبری

استرالیا از نظر میانگین استفاده از اینترنت، سرانه اشتراک اینترنت پهن‌باند همراه و نسبت شرکت‌های حوزه تجارت الکترونیک در زمره کشورهای برتر دنیا قرار دارد[3]. با این

1. Australian Secret Intelligence Service
2. Director of National Intelligence

۳. رجوع شود به:
International Telecommunication Union, 'Statistics', https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx;
Organization for Economic Co-operation and Development (OECD), 'Measuring the Digital Transformation: A roadmap for the future', 11 March 2019, pp. 54, 101, 121, https://www.oecd.org/publications/measuring-the-digital-transformation-9789264311992-en.htm.

حال، استرالیا در شاخص‌های نوآوری، رقابت‌پذیری و امنیت سایبری در میان ده کشور اول جهان قرار ندارد.

استرالیا از آغاز قرن جدید اقتصاد دیجیتال نسبتا بدون رشد بوده‌است، به‌طوری‌که می‌توان گفت سهم صنایع اطلاعات آن از ارزش افزوده جهانی بین سال‌های ۲۰۰۶ و ۲۰۱۶ به زحمت افزایش یافته‌است. استرالیا در ورودی نوآوری (دانش، پژوهش و سرمایه‌گذاری) رتبه سیزدهم دنیا را در سال ۲۰۲۰ کسب کرد[۱] و در خروجی نوآوری در همین سال رتبه سی‌ویک را از آنِ خود کرد که البته در حوزه‌ای مانند خروجی دانش رتبه آن حتی پایین‌تر یعنی چهلم بود[۲]. درنتیجه می‌توان گفت بین ورودی نوآوری و خروجی نوآوری در استرالیا تناسبی وجود ندارد. اگرچه استرالیا از نظر تخصص موسسات و دانشمندان و نیز دسترسی به سرمایه خطرپذیر در بین ده کشور اول دنیاست، اما در مرحله تجاری‌سازی نتایج علمی عملکرد ضعیفی دارد.

این عدم توازن در رویکرد استرالیا نسبت به هوش مصنوعی نیز دیده می‌شود. به‌عنوان مثال، استرالیا از نظر تولید مقالات هوش مصنوعی دارای بیشترین ارجاع موفق به رتبه دهم در سال ۲۰۲۰ شده‌است[۳]، اما فاقد ظرفیت صنعتی لازم جهت استفاده از این دانش برای کسب منافع اقتصادی است.

---

۱. رجوع شود به:
OECD, 'Measuring the Digital Transformation: A roadmap for the future', p. 71.

۲. رجوع شود به:
SC Johnson College of Business Cornell University, INSEAD and the World Intellectual Property Organization, Global Innovation Index 2020: Who Will Finance Innovation?, 2020, pp. xxxiv, xxxvi, 15. https://www.globalinnovationindex.org/Home.

۳. رجوع شود به:
Gleb Chuvpilo, 'AI Research Rankings 2020: Can the United States Stay Ahead of China?', 21 December 2020.
https://chuvpilo.medium.com/ai-research-rankings-2020-can-theunited-states-stay-ahead-of-china-61cf14b1216.

طبق نتایج مطالعه‌ای که در سال ۲۰۱۹ به خواست دولت انجام شد، استرالیا باید تا سال ۲۰۳۰ حداقل ۳۲ هزار و حتی احتمالا ۱۶۱هزار نیروی کار مجرب در زمینه هوش مصنوعی پرورش دهد تا بتواند ظرفیت‌های اقتصادی دانش علمی خود را بالفعل نماید[۱]. در همین راستا، دولت اقداماتی را آغاز کرده‌است و در سال ۲۰۱۹ نیز نهاد اصلی دولت در حوزه تحقیقات علمی ضمن انتشار نقشه‌راه هوش مصنوعی، فراخوان عمومی برای تدوین سیاست هوش مصنوعی داد. البته بدون تردید چنین ابتکارهایی سال‌ها طول می‌کشد تا به نتیجه عملی برسند[۲].

استرالیا در بخش فناوری اطلاعات و ارتباطات به‌ویژه در زمینه محاسبات کوآنتوم دستاوردهای خوبی داشته‌است، هرچند بیشتر تحقیقات این حوزه با سرمایه‌گذاری نهادهای دولتی یا سرمایه خطرپذیر آمریکا انجام می‌شوند[۳]. از همین روی، وزارت دفاع اهتمام ویژه‌ای به گروه علم و فناوری دفاعی[۴] خود دارد که برنامه تحقیق و توسعه فعالی در زمینه فناوری‌های سایبری در دست اجرا دارد[۵].

---

۱. رجوع شود به:
Australian Government, 'Artificial Intelligence: Solving problems, growing the economy and improving our quality of life', 2019, p. iv.
https://data61.csiro.au/~/media/D61/AI-Roadmap-assets/19-00346_DATA61_REPORT_AI-Roadmap_WEB_191111.pdf?la=en&hash=58386288921D9C 21EC8C4861CDFD863F1FBCD457

۲. برای کسب جزئیات بیشتر درباره سیاست هوش مصنوعی استرالیا رجوع شود به:
OECD AI Observatory, https://oecd.ai/dashboards/countries/Australia.

۳. به‌عنوان مثال رجوع شود به مورد محاسبات کوآنتومی در دانشگاه سیدنی:
'Global VC Bets on Australian Quantum Computing Start-Up Q-Ctrl in Us$15m Series A', Quantaneo, 10 September 2019. https://www. quantaneo.com/Global-VC-bets-on-Australian-quantumcomputing-start-up-Q-CTRL-in-US15m-Series-A_a205. html;
IARPA, 'US investing in quantum tech at Sydney University', Technology Decisions, 9 May 2016.
https://www.technologydecisions.com.au/content/it-management/article/us-investing-in-quantum-tech-at-sydney-uni-672014055.

4. Defense Science and Technology Group

۵. رجوع شود به:
Australian Government, Department of Defense, 'Defense Science and Technology Group'.
https://www.dst.defence.gov. au/division/cyber-and-electronic-warfare-division

دولت در سال ۲۰۱۸ سازمان ملی فضایی[1] را به‌منظور کاهش وابستگی تقریبا مطلق کشور به ماهواره‌های خارجی تاسیس کرد. این سازمان در سال ۲۰۱۹ الی ۲۰۲۰ بودجه محدودی معادل ۹/۸ میلیون دلار استرالیا (برابر با ۶/۸ میلیون دلار آمریکا) در اختیار داشت و دارای تنها ۱۳ ماهواره بود[2]. استرالیا همچنین در سال ۲۰۱۹ نیروی فضایی کوچکی همراه با فرانسه، آلمان، بریتانیا، کانادا و آمریکا تشکیل داد.

به‌طورکلی، استرالیا ظرفیت چندانی برای ارزیابی جنبه‌های امنیتی فناوری‌های وارداتی ندارد و همه توانمندی‌های آن نیز در نهادهای دولتی و برخی شرکت‌های بزرگ خصوصی متمرکز شده‌است. با این حال، استرالیا در بخش‌های پژوهش‌های علمی منبع‌باز و تجاری همکاری‌های بین‌المللی خوبی دارد و در اجرای عملیات‌های مخفی دارای مشارکت‌های قوی با هم‌پیمانان اطلاعاتی و نظامی خود است.

امنیت و تاب‌آوری سایبری

دولت‌های مختلف در استرالیا تاکنون اقدامات موثری در راستای ارتقای امنیت سایبری ملی و تاب‌آوری زیرساخت‌های حیاتی انجام داده‌اند. براساس فهرست راهبردهای مقابله با خطر اداره کل سیگنال‌های استرالیا، در سال ۲۰۱۱ پویشی آموزشی درباره چهار تهدید اصلی امنیت سایبری راه‌اندازی شد[3] که در سال ۲۰۱۷ این چهار تهدید اصلی به هشت تهدید اصلی افزایش یافتند و فهرست ۳۵ راهبردی اداره کل سیگنال‌ها نیز به فهرستی متشکل از ۳۸ راهبرد ارتقا یافت. دولت استرالیا

1. National Space Agency

۲. رجوع شود به:
Union of Concerned Scientists, 'UCS Satellite Database', updated 1 January 2021. https://www.ucsusa.org/resources/ satellite-database.

۳. رجوع شود به:
Waters, 'National Cyber Emergency Policy for Australia: Critical Infrastructure'

همچنین موفق به تهیه راهنمای امنیت سایبری همه بخش‌ها تا سال ۲۰۲۰ شد[۱]. موفقیت استرالیا در این امر موجب الگوبرداری کشورهای بریتانیا و کانادا از رویکرد آن شده‌است.

وضعیت امنیت سایبری ملی استرالیا ازجمله ضعف‌های خود دولت را می‌توان از محتوای بسیاری از اظهارات رسمی مقامات دولتی دریافت. گزارش‌های اداره ملی بازرسی استرالیا[۲] حاکی از این واقعیت هستند که نهادهای دولتی این کشور از ارتقای امنیت سایبری خود امتناع می‌کنند. به‌عنوان مثال، گزارش اداره ملی بازرسی استرالیا درباره سه نهاد دولتی در سال ۲۰۱۸ نشان می‌دهد تنها یکی از آن‌ها با چهار معیار اصلی اداره کل سیگنال‌های استرالیا-که البته استانداردهای چندان سطح بالایی هم نیستند[۳]- تطبیق داشته‌است[۴]. در سال ۲۰۱۹ نیز اداره ملی بازرسی استرالیا گزارش داد که اداره پست نتوانسته‌است خطرات امنیت سایبری را به‌طور موثر مدیریت کند[۵]. در سال ۲۰۲۰

---

۱. رجوع شود به:
Stilgherrian, 'Australia's cyber defense "pretty ordinary" before ASD's Top Four', ZDNet, 2 June 2015. https://www.zdnet.com/article/australias-cyber-defencepretty-ordinary-before-asds-top-four.

2. Australian National Audit Office

۳. به‌عنوان نمونه رجوع شود به راهنمای امنیت اطلاعات دولت استرالیا که در آن درباره حفاظت از اطلاعات ذخیره شده یا مبادله شده سازمان‌ها آموزش داده می‌شود.
Australian Government, Australian Signals Directorate, 'Australian Government Information Security Manual', September 2019. https://www.cyber.gov.au/ ism;
Australian Government, Australian Signals Directorate, 'Strategies to Mitigate Cyber Security Incidents' (which complements the advice in the ISM), February 2017.
https:// www.cyber.gov.au/publications/strategies-to-mitigate-cybersecurity-incidents;
Australian Government, Australian Signals Directorate, 'The Essential Eight Maturity Model', 26 June 2020.
https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model
4. Australian National Audit Office, 'Cyber Resilience', Auditor General Report, no. 53 of 2017-18, 28 June 2018. https://www.anao.gov.au/work/performance-audit/cyber-resilience-2017-18.

۵. رجوع شود به:
Australian National Audit Office, 'Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities', Auditor General Report, no. 1 of 2019-20, 4 July 2019.
https://www.anao.gov.au/work/performance-audit/cyber-resilience-government-businessenterprises-and-corporate-commonwealth-entities.

هـم یکـی ازکمیته‌هـای پارلمـان اسـترالیا با تاکید بـر عدم‌تطبیـق اغلب نهادهـای دولتی با اسـتانداردهای موردنظر خواسـتار بازرسـی‌های بیشـتری از وضعیت امنیت سـایبری این نهادها شـد[۱]. با این همه، اسـترالیا در شـاخص جهانی امنیت سـایبری در سـال ۲۰۱۸ رتبه دهم را در بین ۱۷۵ کشور کسب کرده‌است[۲].

در سـال ۲۰۱۶ دولـت به‌منظـور بهبـود عملکـرد ملـی و کاهش وابسـتگی بـه تجهیزات وارداتـی فنـاوری اطلاعـات و ارتباطات و نیروی کار خارجی یک مرکز رشـد[۳] امنیت سـایبری ایجـاد کـرد[۴]. ایـن مرکـز رشـد کـه اکنـون آست‌سـایبر[۵] نامیـده می‌شـود، گـزارش وضعیت رقابت‌پذیـری جهانی اسـترالیا از نظر امنیت سـایبری را به‌روزرسـانی می‌کنـد[۶]. گزارش ارائه شـده توسـط این مرکز رشد در سال ۲۰۱۹ نشان می‌دهد قسمت اعظم اشتغال و تقاضای امنیت سـایبری استرالیا به‌صورت برون‌سپاری تامین می‌شود، به‌طوری‌که سه‌چهارم این بازار در اختیار شـرکت‌های خارجی قرار دارد. البته بیشـتر این شرکت‌های خارجی در داخل اسـترالیا مسـتقر هسـتند و از نیروی کار استرالیایی اسـتفاده می‌کنند[۷]. این مساله خیلی

---

۱. رجوع شود به:
Joint Committee on Public Audit and Accounts, 'Report 485 Cyber Resilience', December 2020. https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Public_Accounts_and_Audit/CyberResilience2019-20/Report.

۲. رجوع شود به:
International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 58. https://www.itu.int/dms_pub/itu-d/opb/str/ D-STR-GCI.01-2018-PDF-E.pdf.

3. growth center

۴. ازجمله اهداف ایجاد این مراکز رشد عبارتند از: افزایش همکاری و تجاری‌سازی، بهبود فرصت‌های بین‌المللی و دسترسی به بازار، ارتقای مدیریت و مهارت‌های نیروی کار و شناسایی فرصت‌های اصلاح مقررات. برای اطلاعات بیشتر رجوع شود به:
Australian Government, Department of Industry, Science, Energy and Resources, 'Industry Growth Centers', https://www.industry. gov.au/strategies-for-the-future/industry-growth-centers.

5. AustCyber

۶. رجوع شود به:
AustCyber, 'Australia's Cyber Security Sector Competitiveness Plan - 2019 Update', December 2019, https://www.austcyber.com/ resource/australias-cyber-security-sector-competitivenessplan-2019.

۷. همان، ص ۳۳.

هم تعجب‌برانگیز نیست، زیرا بسیاری از کشورهای گروه ۲۰ ازقبیل چین، ژاپن، فرانسه، آلمان، بریتانیا و روسیه به‌شدت به فناوری اطلاعات و ارتباطات ساخت خارج وابسته هستند. این گزارش حاکی از آن است که استرالیا با موانع متعددی برای بهره‌برداری از مزیت‌های خود و ساخت یک بخش امنیت سایبری بزرگ و در کلاس جهانی روبروست. در پایان گزارش نیز پیشنهادهای متعددی برای توسعه بخش امنیت سایبری استرالیا مطرح شده است: توجه جدی به کمبود مهارت در بخش امنیت سایبری، ارتقای تحقیق و توسعه، بهبود دسترسی به بازارهای جهانی و طراحی معیارهای مناسب برای ارزیابی توسعه بخش امنیت سایبری و تاثیر اقتصادی آن بر کل اقتصاد[۱]. این گزارش تحقق امور پیشنهادی را در گرو ذهنیت به‌روزتر و پویاتر نسبت به امنیت سایبری می‌داند. بسیاری از سیاست‌مداران استرالیا اعتقاد دارند اگر این تغییرات عملی شود، استرالیا نیز می‌تواند شاهد پیشرفت‌هایی مانند رژیم صهیونیستی باشد.

بودجه پیشنهادی در راهبرد امنیت سایبری (۲۰۱۶) برای رفع مشکلات موردنظر در این راهبرد به هیچ‌وجه کافی نیست. به‌عنوان مثال، سواد دیجیتال به‌خصوص در سطح دانشگاهی یکی از حوزه‌هایی است که باید موردتوجه بیشتری قرار گیرد و در این راهبرد تنها ۳/۵ میلیون دلار استرالیا (معادل ۲/۷ میلیون دلار آمریکا) بودجه در دوره‌ای چهارساله (برنامه توسعه مراکز آموزش عالی) برای این حوزه پیشنهاد شده‌است[۲]. آست‌سایبر در سال ۲۰۱۹ گزارش داد که کمبود مهارت بیش از حد تصور است[۳]. در سال ۲۰۲۰ نیز دولت به

۱. همان، ص ۱۰.

۲. رجوع شود به:
Australian Government, 'Portfolio budget statements 2016-17: Budget related paper no. 1.5: Education and Training Portfolio', pp. 14, 20,
https://www.dese.gov.au/download/3174/education-andtraining-portfolio-budget-statements-2016-17-full-version/18354/document/pdf.

۳. رجوع شود به:
AustCyber, 'Cyber Security Competitiveness Plan - 2019 Update', p. 11.

این نتیجه رسید که توسعه نیروی کار امنیت سایبری بدون نیروهای مهاجر امکان‌پذیر نخواهد بود و بدین‌منظور، برنامه‌های ویزای جدیدی را برای جذب نیروی کار مهاجر از کشورهای دیگر معرفی کرد[۱]. این در حالی است که دانشگاه‌های استرالیا امکان تامین همه تقاضاهای موردنظر دولت را ندارند، به‌خصوص که خود دولت نیز آمادگی تخصیص بودجه موردنیاز را ندارد. در راهبرد امنیت سایبری (۲۰۲۰) مبلغ سرمایه‌گذاری بسیار بیشتری جهت توسعه نیروی کار، آموزش و جامعه در نظر گرفته شده و تا ۵۰ میلیون دلار استرالیا (معادل ۳۵ میلیون دلار آمریکا) به این موضوع اختصاص داده شده‌است[۲]. با این حال، دولت بیشتر طرفدار راه‌حل‌های مبتنی بر مشارکت کسب‌وکارها و جوامع است و به نظر نمی‌رسد مشوق چندانی به دانشگاه‌ها تخصیص دهد.

با آنکه استرالیا اصلاحاتی در جهت بهبود هماهنگی سیاست‌ها و ساختار حقوقی امنیت سایبری انجام داده‌است، اما مادامی که دولت خود عملکردی هماهنگ و ابزارهایی استاندارد اتخاذ ننماید، این اصلاحات نمی‌توانند به اندازه کافی تاثیرگذار

۱. چندین سال طول کشید تا استرالیا بتواند سیاست‌های مهاجرتی خود را به‌نحوی تدوین کند که موجب جذب متخصصان حوزه امنیت سایبری به کشور شود. دولت برنامه‌های خود را در سال ۲۰۱۷ با اجرای برنامه استعدادهای جهانی با حمایت کارفرما (Global Talent Employer Sponsored (GTES)) آغاز کرد که هدف آن جذب استعدادهای برتر برای موقعیت‌های شغلی تخصصی و مستلزم مهارت‌های بسیار بالا بود (در این برنامه هیچ اشاره مستقیمی به امنیت سایبری نشده‌بود). موقعیت‌های شغلی موردنظر در این برنامه در سایر برنامه‌های ویزا مانند دوره‌های رزیدنسی کوتاه‌مدت یا میان‌مدت (آموزش مستلزم اقامت و کار) پوشش داده نمی‌شد و نیروی کار استرالیایی نیز برای این موقعیت‌ها وجود نداشت. به‌دنبال آن، دولت در سال ۲۰۱۸ طرحی برای هفت حوزه موردتاکید اجرا کرد که امنیت سایبری را نیز پوشش می‌داد و همچنان مستلزم حمایت کارفرما بود. هدف این طرح جذب ۵ هزار مهاجر در سال اول اجرا بود. در نوامبر ۲۰۱۹، دولت برنامه جدیدی برای جذب مهاجران ماهر اجرا کرد که علاوه بر کارفرمایان، افراد مستقل هم امکان تقاضا برای شرکت در آن را داشتند. برای جزئیات بیشتر رجوع شود به:

Greg Austin, 'Twelve Dilemmas of Reform in Cyber Security Education', in Greg Austin (ed.), Cyber Security Education: Principles and Policies (Abingdon: Routledge, 2020), pp. 208-21,

۲. رجوع شود به:

Australian Government, Department of Home Affairs, 'Australia's Cyber Security Strategy 2020', p. 42.

باشند. درحقیقت، دولت استرالیا هنوز سرمایه‌گذاری کافی برای مقابله با تهدیدهای اساسی انجام نداده‌است[1]. ظاهرا تامین‌کنندگان زیرساخت‌های ملی حیاتی استرالیا هنوز به درستی از اهمیت تهدیدها و اثر کمبود نیروی کار ماهر-ازجمله در سطح مدیریت- بر افزایش این تهدیدها مطلع نیستند[2]. لازم به ذکر است که چنین مسائلی مختص استرالیا نیست و در همه کشورهای موردمطالعه دیده می‌شود.

رهبری جهانی در عرصه سایبری

استرالیا در بسیاری از سازمان‌های بین‌المللی مانند اتحادیه بین‌المللی مخابرات، آسه‌آن و سازمان همکاری‌های اقتصادی آسیا اقیانوسیه (اَپک)[3] در مدیریت مسائل فضای سایبری نقش فعالی دارد. از نمونه‌های بارز فعالیت‌های بین‌المللی این کشور می‌توان به ریاست مشترک استرالیا در یکی از کارگروه‌های امنیت سایبری در برنامه آسه‌آن پلاس[4] اشاره کرد. درواقع، استرالیا به تبعیت از اصلی که در گزارش دفاعی دولت در سال ۲۰۱۶ مطرح شده‌است (علی‌رغم اینکه مشکل کمبود منابع وجود ندارد، اما تامین کامل امنیت ملی بدون همکاری با شرکا امکان‌پذیر نیست) همکاری نزدیکی با

۱. رجوع شود به:
'Australia Needs Civil Defense against the Cyber Storm: Policy Report', Research Group on Cyber War and Peace UNSW, University of New South Wales Canberra, 31 March 2019, p. 3, https://www.unsw.adfa.edu.au/unsw-canberra-cyber/sites/accs/files/uploads/Policy%20 Report%20Cyber%20Civil%20Defence%2031%20March%202019_1.pdf.

۲. رجوع شود به:
Rajiv Shah, 'Protecting critical national infrastructure in an era of IT and OT convergence', Australian Strategic Policy Institute, Policy Brief, no. 18/2019, 12 July 2019, https://www.aspi.org.au/report/protecting-critical-national-infrastructure-era-it-and-otconvergence.

3. Asia-Pacific Economic Cooperation (APEC)

4. ASEAN Plus framework

هم‌پیمانان خود دارد[۱].

استرالیا به پیروی از سایر کشورها مانند چین و ایالات متحده در سال ۲۰۱۷ راهبرد مشارکت سایبری بین‌المللی[۲] خود را منتشر کرد که شامل همه جنبه‌های دیپلماتیک مدیریت فضای سایبری مانند جرائم سایبری، تجارت سایبری، امنیت سایبری، حقوق بشر، حریم خصوصی و امنیت بین‌المللی می‌شد[۳]. در این راهبرد، استرالیا نیز همانند هم‌پیمانان نزدیکش به دفاع سایبری فعال شامل تعیین استانداردهای رفتار دولت‌ها، اقدامات عملی برای اعتمادسازی و پاسخ به رفتارهای غیرقابل‌قبول دولت‌ها متعهد شده‌است[۴].

استرالیا از سال ۲۰۱۳ تا ۲۰۱۵ ریاست گروه کارشناسان دولتی سازمان ملل را نیز برعهده داشته‌است[۵]. علاوه براین، استرالیا از سال ۲۰۱۶ برنامه‌های ظرفیت‌سازی محدودی در حوزه امنیت سایبری در جنوب شرق آسیا و جنوب اقیانوسیه اجرا می‌کند. اثرگذاری این

۱. «باآنکه استرالیا دوازدهمین اقتصاد بزرگ دنیاست و توانمندی‌های نظامی پیشرفته و روبه‌رشدی دارد، اما نمی‌تواند به‌تنهایی از منافع امنیت سایبری خود در سطح جهان حفاظت کند و آن‌ها را توسعه بخشد. درنتیجه، ما با شرکایمان ازقبیل ایالات متحده،کشورهای آسه‌آن، سازمان پیمان آتلانتیک شمالی (ناتو) و سازمان ملل در راستای تحقق اهداف جهانی و مشترک به‌منظور ترویج و گسترش نظم جهانی پایدار و مبتنی بر قانون همکاری خواهیم کرد». برای جزئیات بیشتر رجوع شود به:
Australian Government, Department of Defense, '2016 Defense White Paper', Canberra, 2016, p. 45, https://www. defence.gov.au/WhitePaper/Docs/2016-Defence-WhitePaper.pdf.
2. International Cyber Engagement Strategy

۳. رجوع شود به:
Australian Government, Department of Foreign Affairs and Trade, 'Australia's International Cyber Engagement Strategy', October 2017, https://www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/australias-international-cyber-engagement-strategy.

۴. همان، ص ۴۴.
رجوع شود به:
UN Office for Disarmament Affairs, 'Developments in the field of information and telecommunications in the context of international security', https://www.un.org/disarmament/ict-security.

۵. رجوع شود به:
UN Office for Disarmament Affairs, 'Developments in the field of information and telecommunications in the context of international security', https://www.un.org/disarmament/ict-security.

نوع برنامه‌ها در مواردی که با همکاری سایر کشورها انجام می‌شوند بیشتر از پروژه‌هایی است که استرالیا خود به‌تنهایی اجرا می‌کند. با این حال، اثرگذاری برخی از جنبه‌های این برنامه‌ها همچنان محل‌تردید است. به‌عنوان مثال، در کشورهایی که بخش فناوری اطلاعات و ارتباطات ضعیفی دارند، منابع آموزشی آن‌ها محدود است و تنها چند مقام مسئول در نقش‌های مرتبط با امنیت سایبری دارند، اجرای برنامه‌های ظرفیت‌سازی برای امنیت سایبری چندان منطقی به نظر نمی‌رسد. به‌عبارت دیگر، کشورهای فقیری مانند کامبوج یا لائوس یا کشورهای کوچک جنوب اقیانوسیه نمی‌توانند همانند اندونزی یا ویتنام از این‌گونه برنامه‌ها بهره‌برداری کنند.

استرالیا بیش از دیگر هم‌پیمانان ایالات متحده از تصمیم این کشور برای اخراج شرکت چینی هوآوی از شبکه‌های ملی نسل پنجم (5G) حمایت می‌کند و در صف اول لابی بین‌المللی برای تحقق آن قرار دارد[1]. استرالیا اولین عضو ائتلاف پنج چشم بود که در آگوست ۲۰۱۸ به اپراتورهای مخابراتی خود توصیه کرد از خریداری تجهیزات و خدمات نسل پنجم هوآوی اجتناب کنند. این موضوع باعث تیرگی روابط استرالیا با چین به‌مدت دو سال شد و در روابط آن با کانادا و بریتانیا نیز مشکلاتی ایجاد کرد. البته به‌طور دقیق نمی‌توان گفت پشت‌پرده این تصمیم استرالیا ملاحظات کلان ژئوپلیتیک بوده یا صرفا به‌دلیل برخی مسائل فنی بوده‌است.

استرالیا با مشکل افزایش روبه‌رشد سرمایه‌گذاری‌های چین در بخش فناوری اطلاعات و ارتباطات کشورهای منطقه مواجه است. این مساله در ماجرای سال ۲۰۱۸ به‌خوبی خود را نشان داد که استرالیا کشور جزایر سلیمان را متقاعد کرد تا قرارداد با شرکت هوآوی برای نصب

۱. رجوع شود به:
'Australia, Huawei and 5G', IISS Strategic Comments, vol. 25, no. 28, October 2019, https://www.iiss.org/publications/strategic-comments/2019/australia-huawei-and-5g.

کابل‌های زیردریایی جهت اتصال به استرالیا را با قراردادی بدون حضور شرکت‌های چینی جایگزین کند[۱]. البته در مورد کشوری مانند پاپوآگینه‌نو[۲] که باوجود وابستگی به کمک‌های استرالیا حاضر به نادیده‌گرفتن هوآوی نیست، سیاست فشار استرالیا موفق نبوده‌است[۳].

استرالیا گفت‌وگوهای دوجانبه و چندجانبه‌ای با کشورهای دیگر شامل کانادا، چین، هند، اندونزی، ژاپن، نیوزیلند، کره جنوبی، بریتانیا و ایالات متحده پیش می‌برد که در این میان گفت‌وگوهای سه‌جانبه ایالات متحده-ژاپن-استرالیا از اهمیت ویژه‌ای در تبیین موضع کانبرا نسبت به آزادی اینترنت و رفتارهای خصمانه برخی دولت‌ها در فضای سایبری برخوردار است.

توانمندی‌های سایبری تهاجمی

دولت استرالیا در سال ۲۰۱۶ به‌طور رسمی به توانمندی‌های سایبری تهاجمی خود و استفاده از آن علیه تروریسم اذعان کرد[۴]. در سال ۲۰۱۹ نیز رئیس اداره کل سیگنال‌های

۱. رجوع شود به:
Rosie Perper, 'Australia snubbed Huawei and completed its undersea cable project to bring high-speed internet to Pacific Islands', Business Insider, 28 August 2019, https://www.businessinsider.com.au/australia-snubs-huawei-finishesundersea-cables-for-pacific-islands-2019-8?r=US&IR=T.

Alan Burkitt-Gray, 'Australia slams Huawei for "security vulnerabilities" in PNG data center', Capacity Media, 12 August 2020, https://www.capacitymedia.com/articles/3826128/ australia-slams-huawei-for-security-vulnerabilities-in-pngdata-centre.

2. Papua New Guinea

۳. رجوع شود به:
Alan Burkitt-Gray, 'Australia slams Huawei for "security vulnerabilities" in PNG data center', Capacity Media, 12 August 2020, https://www.capacitymedia.com/articles/3826128/ australia-slams-huawei-for-security-vulnerabilities-in-pngdata-centre.

۴. پارلمان استرالیا، رجوع شود به:
'National Security Update on Counter Terrorism: Address to the House of Representatives, Parliament House, Canberra', 23 November 2016, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22media/pressrel/4951827%22.

استرالیا اعلام کرد آن عملیات‌ها با همکاری شرکای حاضر در ائتلاف انجام گرفته و فرماندهی عملیات‌های مشترک[1] ارتش استرالیا مسئول ایجاد اختلال در مکالمات جنگی داعش و انجام عملیات نفوذ برخط بوده‌است[2]. وی همچنین تاکید کرد استرالیا از این توانمندی‌ها در مقابله با جرائم سایبری سازمان‌یافته فراساحلی نیز استفاده می‌کند[3]. استرالیا در اجرای ابتکار بازدارندگی سایبری ایالات متحده برای شناسایی حمله‌های سایبری خارجی، افشای منبع آن‌ها و مقابله با آن‌ها نیز همکاری می‌کند. تمام عملیات‌های سایبری تهاجمی استرالیا مطابق (تفسیر دولت از) قوانین بین‌المللی و تحت‌نظارت گروهی از وکلای خبره دولتی انجام می‌شوند.

اداره کل سیگنال‌های استرالیا در برنامه پنج‌ساله خود که در سال ۲۰۱۹ منتشر شد، بار دیگر بر اجرای عملیات‌های سایبری تهاجمی به‌عنوان عنصر ضروری جهت تامین امنیت داخلی (مقابله با جرائم سایبری) و نیازهای جنگی کشور تاکید کرده‌است[4]. اگرچه هدف این برنامه ساخت توانمندی‌های سایبری تهاجمی در کلاس جهانی است[5]، اما بر استفاده از توان مشارکت‌های بین‌المللی برای تقویت قدرت عملیاتی اداره کل سیگنال‌های استرالیا نیز تاکید دارد[6].

---

1. Chief of Joint Operation

۲. اداره کل سیگنال‌های استرالیا، رجوع شود به:
'Director-General ASD speech to the Lowy Institute', 27 March 2019,
https://www.asd.gov.au/ publications/speech-lowy-institute-speech.

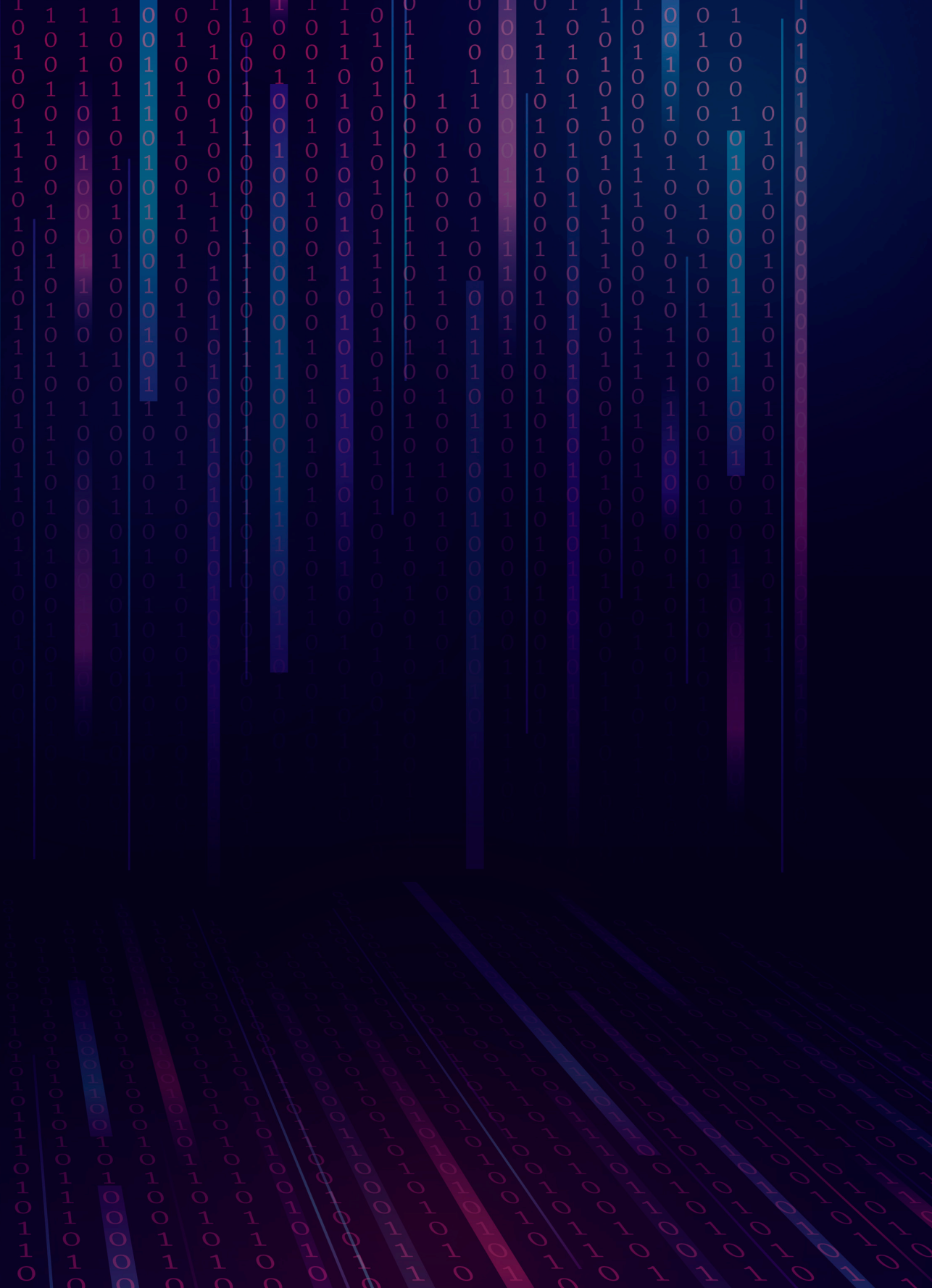
۳. همان.

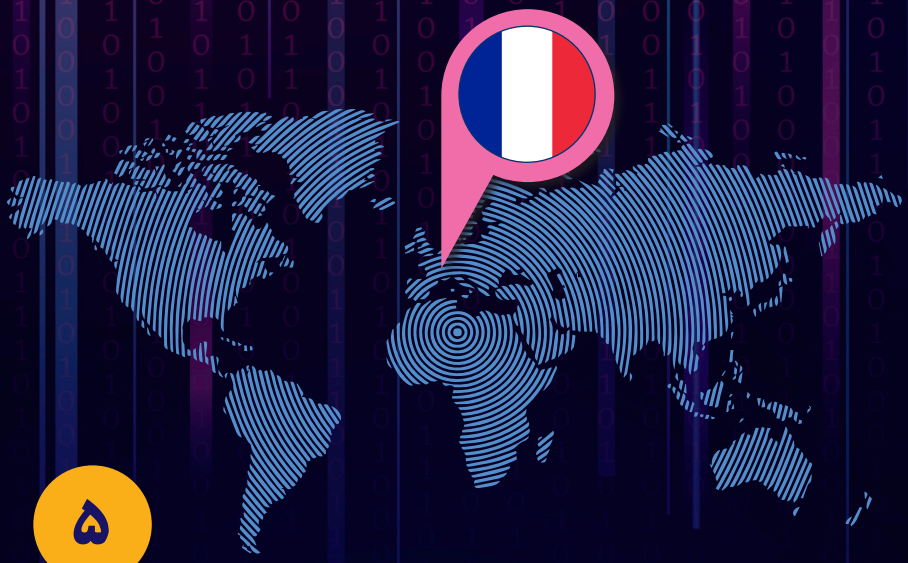
۴. در این برنامه چنین تصریح شده‌است: اداره کل سیگنال‌های استرالیا از عملیات‌های ارتش در سراسر جهان (ازجمله ازطریق ارائه توانمندی‌های سایبری تهاجمی و اطلاعاتی خود برای کمک به رزمندگان و پشتیبانی از کارکنان و دارایی‌های ارتش) حمایت می‌کند. برای جزئیات بیشتر رجوع شود به:
'ASD Corporate Plan 2019-20', Canberra, 2019, p. 7,
https://www. asd.gov.au/sites/default/files/2019-08/ASD_Corporate_Plan_ final_12.pdf.
(برخلاف عنوان برنامه، در اصل این برنامه برای دوره ۲۰۱۹ تا ۲۰۲۳ تدوین شده‌است).

۵. همان، ص ۸.

۶. همان، ص ۱۳.

درمجموع می‌توان گفت استرالیا توانمندی‌های سایبری تهاجمی موثری دارد. همکاری نزدیک و اجرای عملیات‌های مشترک با ایالات متحده و بریتانیا، استرالیا را در صف کشورهای پیشتاز توان سایبری تهاجمی قرار می‌دهد و عضویت آن در ائتلاف پنج چشم توانمندی‌های اطلاعاتی و آگاهی موقعیتی آن را برای اجرای عملیات‌های سطح بالا ارتقا می‌بخشد. بااین همه، استرالیا از نظر منابع و نیروی انسانی هنوز هم‌سطح شرکای تراز اول خود نیست. همانند بسیاری از کشورها، کمبود مهارت و ضعف نظام آموزشی مهم‌ترین محدودیت استرالیا در توانمندی‌های سایبری تهاجمی آن است. مقامات اداره کل سیگنال‌های استرالیا همواره در اظهارات رسمی خود به این مساله اشاره می‌کنند و خواستار توجه جدی برای رفع آن هستند.





۵

فرانسه

فرانسه دارای راهبردهای امنیت سایبری کاملا استواری است که از پشتوانه‌ی قوی نهادهای بالغ و بودجه کافی هم برخوردار هستند. علاوه براین، فرانسه دسترسی خوبی به اطلاعات سایبری دارد. در این کشور سازمان‌های ذی‌نفع در مسائل امنیت سایبری از نهادهای متولی بخش اطلاعات سایبری متمایز هستند. با آنکه فرانسه دارای نقاط‌قوت بسیاری در بخش فناوری اطلاعات و ارتباطات است، اما از نظر دیجیتال‌سازی اقتصاد و جامعه هنوز در شمار کشورهای پیشتاز قرار ندارد. با این حال، فرانسه در امنیت سایبری نسبتا توانمند و نوآور است و از رویکرد کل جامعه بهره می‌گیرد. این کشور ارتقای مقررات را از عناصر مهم در مقابله با تهدیدهای سایبری می‌داند و در همین راستا، قوانین جدیدی درباره اختلال در انتخابات و حفاظت از زیرساخت‌های حیاتی ملی تصویب کرده‌است. فرانسه در عرصه بین‌المللی نیز طرفدار رویکرد چندذینفعی در مواجهه با مسائل سایبری است. درمجموع، فرانسه علی‌رغم توانمندی‌های سایبری تهاجمی پیشرفته خود هنوز با ایالات متحده و بریتانیا فاصله قابل‌توجهی دارد. از یک سو، این کشور به‌دلیل تمایل خود به حفظ استقلال ملی در توانمندی‌های سایبری کلیدی هنوز نتوانسته‌است از منافع بالقوه ائتلاف با هم‌پیمانان اصلی خود بهره‌مند شود. از سوی دیگر، فرانسه در تامین امنیت سایبری وابستگی کمتری به کشورهای دیگر دارد.

راهبرد و مبنای نظری (دکترین)

تا سال ۲۰۱۱، رویکرد فرانسه در مسائل امنیت فضای سایبری براساس ترکیبی از نیازهای فنی امنیتی، چشم‌انداز تجاری و منافع نظامی بود. اما از آن پس، این کشور با اراده‌ای جدی‌تر به مدلی روی آورده‌است که داشتن دیدگاهی جامع نسبت به امنیت ملی در فضای سایبری را در اولویت می‌داند. در بین اسناد راهبرد سایبری فرانسه در قبل و پس از سال ۲۰۱۸ تناقض‌هایی از نظر بنیان فکری مشاهده می‌شود. به‌عنوان مثال، امنیت دیجیتال در یکی از گزارش‌های دفاعی فرانسه در سال ۲۰۰۸ از موضوعات اصلی به‌شمار می‌رود. در این گزارش چالش‌های انتشار پرشتاب اطلاعات و افکار ازطریق فناوری در محافل مختلف ازجمله فضای سیاسی موردبررسی قرار گرفته[۱] و برای اولین بار در تاریخ اسناد سیاست عمومی فرانسه به تهدیدهای جنگ اطلاعاتی و سایبری و ضرورت مقابله با آن‌ها اشاره شده‌است. تشکیل سازمان ملی امنیت سایبری (ANSSI)[۲] تحت‌نظارت اداره کل دفاع و امنیت سایبری (SGDSN)[۳] در سال ۲۰۰۹ بازتاب این اندیشه است. اولین راهبرد ملی امنیت سایبری این کشور در سال ۲۰۱۱ پس از حمله سایبری به برخی از وزارت‌خانه‌های فرانسه [۴] تدوین شد که به‌طور ضمنی بیانگر تمایل فرانسه برای تبدیل‌شدن به قدرتی سایبری-حداقل از منظر دفاعی-بود. در یکی از گزارش‌های دفاعی

۱. رجوع شود به:
Ministère des Armées, 'Livre blanc: Défense et sécurité nationale', 2008, http://archives.livreblancdefenseetsecurite.gouv.fr/2008/information/les_dossiers_actualites_19/livre_blanc_sur_defense_875/livre_blanc_1337/livre_blanc_1340/index.html.

2. National Cybersecurity Agency (Agence nationale de la sécurité des systèmes d'information)

3. Secretariat General of Defense and National Security (Secrétariat général de la défense et de la sécurité nationale)

۴. رجوع شود به:
Agence nationale de la sécurité des systèmes d'information, 'Défense et sécurité des systèmes d'information: Stratégie de la France', 2011, https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf.

در سال ۲۰۱۳ نیز بر لزوم داشتن مبنای نظری در زمینه پاسخ به تهدیدهای سایبری بزرگ در قالب اقدامات دفاعی هماهنگ و چندمرحله‌ای تاکید شده‌است[۱]. نکته قابل‌توجه در این گزارش این است که فرانسه دو سال پس از ایالات متحده و سه سال پیش از ناتو به‌طور رسمی از فضای سایبری به‌عنوان عرصه نبرد نظامی نام برده‌است.

در آن زمان فضای امنیتی فرانسه به‌دلیل مجموعه‌ای از وقایع در حال تغییر بود: افشاگرهای ادوارد اسنودن در سال ۲۰۱۳، ترورهای جهادی بین سال‌های ۲۰۱۲ و ۲۰۱۶، چندین رویداد بزرگ نشت داده مانند ماجرای ایمیل‌های ماکرون (نفوذ به ایمیل‌های اعضای ستاد انتخابات ریاست‌جمهوری امانوئل ماکرون[۲] در سال ۲۰۱۷ که منتسب به روسیه و به‌نفع نامزد حزب جبهه ملی مارین لوپن[۳] بود)[۴]. این وقایع فرانسه را به‌سمت اتخاذ رویکرد کل جامعه و بازنگری سیاست‌ها و راهبردهای سایبری کشور سوق دادند، به‌طوری‌که فرانسه در سیاست‌های امنیتی خود بیش از پیش به تهدیدهای مداخلات سیاسی، نشر اطلاعات غلط و تبلیغات افراط‌گرایانه (مبتنی بر روش‌های خشونت‌آمیز و تنفرپراکنی) توجه نشان داد.

از بارزترین نشانه‌های تغییر سیاست سایبری فرانسه، تشکیل ستاد فرماندهی سایبری تحت‌عنوان کام‌سایبر[۵] در ژانویه ۲۰۱۷ توسط وزارت نیروهای مسلح[۶] (MdA)

---

۱. رجوع شود به:
Ministère des Armées, 'Livre blanc: Défense et sécurité nationale', 2013, http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf.

2. Emanuel Macron
3. Marine Le Pen

۴. رجوع شود به:
Jean-Baptiste Jeangène Vilmer, 'The "#Macron Leaks" operation: A post-mortem', Atlantic Council, 20 June 2019, https://www.atlanticcouncil.org/in-depth-research-reports/report/the-macron-leaks-operation-a-post-mortem.

5. ComCyber
6. Ministry of Armed Forces (Ministère des Armées)

اسـت کـه جهت ارتقـای هماهنگی عملیات‌های سـایبری نظامـی راه‌اندازی شـد[۱] و درواقع سرآغاز شکل‌گیری مبنای نظری فرانسه در امور فضای سایبری نیز محسوب می‌شود[۲].

انتشـار گـزارش مطالعـه راهبردی دفاع سـایبری[۳] در فوریـه ۲۰۱۸ نقطه‌عطـف دیگری در سـیر تحول مبنای نظری فرانسـه اسـت که درواقع متضمن اصلاحات سـاختاری اساسـی متناسـب با بزرگی تهدیدهای موجود بود[۴]. این گزارش ضمن تشـریح نحوه سـازمان‌دهی و توزیـع اختیـارات مربـوط به عملیات‌هـای سـایبری در نهادهای دولتی ذی‌ربـط، چارچوب حقوقـی ملـی و بین‌المللـی مربـوط به اسـتفاده از آن‌ها را نیز مشـخص می‌سـازد[۵] و مبنای نظری امنیت سایبری در موقعیت‌های مختلف از زمان صلح تا شرایط جنگی را بر پایه روند دفـاع و پایـش در نیروی هوایی تبیین می‌کند[۶]. این گزارش با عبور از مدل دفاع منفعل در سـال ۲۰۰۸، مـدل دفـاع فعال را مطرح می‌سـازد که شـامل توسـعه توانمندی‌هـا، راهبرد و مبنای نظری سایبری تهاجمی با تمرکز بر سامانه‌های نظامی کشورهای رقیب می‌شود.

---

۱. رجوع شود به:
Ministère des Armées, 'Le commandement de la cyberdéfense (COMCYBER)', https://www.defense.gouv.fr/ema/organismesinterarmees/le-comcyber/le-comcyber/comcyber.

۲. طبق سند انتشاریافته در سال 2019، فرانسه از سال 2017 دارای مبنای نظری در حوزه توانمندی‌های سایبری تهاجمی بوده‌است. رجوع شود به:
Ministère des Armées, 'Éléments publics de doctrine militaire de lutte informatique offensive', 2019, p. 4, https://www.defense.gouv.fr/fre/content/download/551497/9393997/El%C3%A9ments%20publics%20de%20doctrine%20militaire%20de%20lutte%20informatique%20OFFENSIVE.pdf.

3. Strategic Review of Cyber Defense

۴. رجوع شود به:
Secrétariat Général de la Défense et de la Sécurité Nationale, 'Revue stratégique de cyberdéfense', 12 February 2018, http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revuecyber-public-v3.3-publication.pdf.

۵. رجوع شود به:
François Delerue and Aude Gery, 'France's Cyberdefense Strategic Review and International Law', Lawfare, 23 March 2018, https://www.lawfareblog.com/frances-cyberdefense-strategicreview-and-international-law

۶. رجوع شود به:
Arthur P. Laudrain, 'French Cyber Security and Defense: Strategy, Policy-Making and Coordination', SSRN Working Paper Series, v.2.3.3, 2019, p. 20, http://dx.doi.org/10.2139/ssrn.3432338.

نکته حائزاهمیت در گزارش ۲۰۱۸ اعتراف ضمنی فرانسه به نقطه‌ضعف خود از نظر دفاع سایبری در مقایسه با سایر اعضای شورای امنیت سازمان ملل است[۱]. در این گزارش توصیه می‌شود فرانسه تهدیدهای سایبری را با دقت و به‌طور کامل بررسی و تحلیل کند[۲] و برای ارتقای ثبات در فضای سایبری خود اهداف جدیدی ازقبیل مجازات عاملان حمله سایبری به فرانسه را در پیش گیرد. این گزارش براساس منشور سازمان ملل دسته‌بندی جدیدی نیز از حمله‌های سایبری ارائه می‌کند[۳] و سه فناوری را برای امنیت سایبری ملی حیاتی می‌داند: فناوری شناسایی حمله‌ها، فناوری رمزنگاری و فناوری شبکه رادیو و تلفن همراه جهت استفاده در شرایط اضطراری ملی[۴].

گزارش ۲۰۱۸ از نظر دامنه مطالعه و لحن اضطراری آن با اسناد مشابه کشورهای دیگر که تا آن زمان منتشر شده بود، تفاوت دارد. اگرچه در این سند همچنان موضع کلی فرانسه با موضع بریتانیا و ایالات متحده به‌ویژه از نظر تاکید بر رویکرد کل جامعه، توسعه مهارت‌ها و تحقق اهداف صنعتی ملی همسو است، اما در برخی از موضوعات دیگر دیدگاه‌های جدیدی را مطرح می‌کند.

وزارت نیروهای مسلح در سپتامبر ۲۰۱۸ سیاستی را برای نیروهای مسلح جهت مقابله با نشر اطلاعات غلط و مخرب اجرا کرد[۵] و به‌دنبال آن در سال ۲۰۱۹، دو سیاست

۱. رجوع شود به:
Secrétariat Général de la Défense et de la Sécurité Nationale, 'Révue stratégique de cyberdéfense', p. 7,
۲. همان، ص. 135.
۳. همان، ص. ۸۰.
۴. همان، ص. ۱۰۰-۹۶.
۵. رجوع شود به:
Florence Parly, 'Déclaration de Mme Florence Parly, minister des armées, sur la manipulation de l'information', Vie publique, 4 September 2018,
https://www.vie-publique.fr/discours/206652-declaration-de-mme-florence-parly-ministredes-armees-sur-la-manipulat.

دیگر یعنی سیاست وزارت‌خانه‌ای جنگ سایبری دفاعی[۱] و عناصر عمومی دیدگاه نظامی در جنگ سایبری تهاجمی[۲] را به اجرا گذاشت. طبق این سیاست‌ها، تحقق هدف راهبردی دستیابی به برتری در فضای سایبری مستلزم استخدام هزار نیروی سایبری جدید و تخصیص ۱/۵ میلیارد یورو (۱/۸ میلیارد دلار) تا سال ۲۰۲۵ است[۳].

افزایش بودجه‌های پیشنهادی دولت برای امنیت فضای سایبری در سال‌های ۲۰۲۰ و ۲۰۲۱ نشان‌دهنده نگرانی فزاینده فرانسه نسبت به تهدیدهای سایبری است. در سال ۲۰۲۰، بودجه محدودی معادل ۱۳۶ میلیون یورو (۱۶۱ میلیون دلار) برای حفاظت بهتر از سامانه‌های دولتی تخصیص یافت[۴]، اما در فوریه ۲۰۲۱ بودجه‌ای برابر با ۱ میلیارد یورو (۱/۲ میلیارد دلار) طی پنج سال اختصاص داده‌شد و متعاقب آن، راهبرد جدید امنیت سایبری نیز تصویب شد[۵]. با آنکه این راهبرد صرفا در قالب بیانیه مطبوعاتی ۳۳ صفحه‌ای منتشر شد، اما مشتمل بر اهداف نوآورانه‌ای است[۶] که به‌طور کلی مؤید محتوای گزارش مطالعه

1. Ministerial Policy for Defensive Cyber Warfare
Ministère des Armées, 'Politique ministérielle de lute informatique défensive', 2019.
2. Public Elements for the Military Doctrine for Offensive Cyber Warfare.
Ministère des Armées, 'Éléments publics de doctrine militaire de lutte informatique offensive', 2019.
۳. رجوع شود به:
Ministère des Armées, 'Communiqué: La France se dote d'une doctrine militaire offensive dans le cyberespace et renforce sa politique de lutte informatique défensive', 18 January 2018, https://www.defense.gouv.fr/fre/salle-de-presse/communiques/communique_la-france-se-dote-d-une-doctrine-militaireoffensive-dans-le-cyberespace-et-renforce-sa-politique-delutte-informatique-defensive
۴. رجوع شود به:
Agence nationale de la sécurité des systèmes d'information, 'Le Volet Cybersécurité de France Relance', September 2020, https://www.ssi.gouv.fr/agence/cybersecurite/le-volet-cybersecurite-defrance-relance.
۵. رجوع شود به:
'Un plan à 1 milliard d'euros pour renforcer la cybersécurité', Gouvernement.fr, 18 February 2021, https://www.gouvernement.fr/un-plan-a-1-milliard-d-euros-pour-renforcer-la-cybersecurite.
۶. رجوع شود به:
'Dossier de presse - Cybersécurité, faire face à la menace: la stratégie française', Gouvernement.fr, 18 February 2021, https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2021/02/210218_dp_cyber_vfinale.pdf.

راهبردی دفاع سایبری ۲۰۱۸ هستند و همزمان تاکید جدی‌تری روی حفظ اقتدار و استقلال و ارتقای رقابت‌پذیری کشور در بخش فناوری اطلاعات و ارتباطات دارند. به‌عنوان مثال، افزایش دوبرابری نیروی کار از ۳۷ هزار نفر به ۷۵ هزار نفر طی پنج سال یکی از اهداف موردتاکید در این راهبرد در حوزه امنیت سایبری است[۱].

فرانسه بین عملیات‌های سایبری تهاجمی و دفاعی تمایز مشخصی قائل است. به‌عبارت دیگر، نهاد اصلی امنیت سایبری فرانسه یعنی سازمان ملی امنیت سایبری فقط مسئول عملیات‌های دفاعی است و همانند سازمان امنیت ملی آمریکا و ستاد ارتباطات دولت بریتانیا بخشی از جامعه اطلاعات کشور به شمار نمی‌رود. این تمایز اختیارات ناشی از دیدگاه خاص سیاست‌مداران فرانسه مبنی بر این است که به‌دلیل اهداف و توانمندی‌های خاص نهادهای اطلاعاتی و نیز ماهیت پنهانی فعالیت‌های آن‌ها، عدم‌تمایز سازمانی می‌تواند در اهداف و فعالیت‌های بخش امنیت سایبری غیرنظامی که مستلزم شفافیت بیشتری هستند، اختلال ایجاد کند.

حکمرانی، فرماندهی و نظارت

در فرانسه رئیس‌جمهور به کمک دو نهادی که در سال ۲۰۱۸ بنیان‌گذاری شده‌اند، مسیر مسائل سایبری کشور را تعیین می‌کند. شورای دفاع و امنیت ملی (CDSN)[۲] مسئولیت تصمیمات مرتبط با سیاست‌های دفاع سایبری را برعهده دارد. ریاست اداره کل دفاع و امنیت ملی از جانب سازمان ملی امنیت سایبری و رئیس ستاد کل[۳] به نمایندگی از کام‌سایبر در این شورا حضور دارند. نهاد دیگر کمیته اجرایی

۱. همان، ص. ۶.

2. Defense and National Security Council (Conseil de defense et de sécurité nationale)

3. Chief of General Staff

دفاع سایبری[1] است که وظیفه اجرای تصمیمات بالادستی شورای دفاع و امنیت ملی را برعهده دارد و تحت‌نظارت رئیس‌جمهور انجام وظیفه می‌کند. کمیته راهبری دفاع سایبری[2] تحت اداره کل دفاع و امنیت ملی نیز موظف به تهیه گزارش سالانه درباره اجرای راهبرد ملی امنیت سایبری است[3]. البته فرایند تصمیم‌گیری درباره امنیت و دفاع سایبری در عمل از وزارتخانه‌ها شروع می‌شود و درنهایت به تایید نهاد نخست‌وزیری و ریاست‌جمهوری می‌رسد[4]. اداره کل دفاع و امنیت ملی نیز با تهیه دستورکار، نظارت و پیگیری اجرای برنامه‌ها تضمین‌کننده تحقق تصمیم‌های اتخاذشده محسوب می‌شود.

در ساختار حکمرانی سایبری فرانسه اختیارات ازطریق چهار مجرای اصلی تقسیم می‌شوند: در بخش غیرنظامی سازمان ملی امنیت سایبری تحت‌نظارت نخست‌وزیر صاحب اختیار است، در بخش نظامی کام‌سایبر با نظارت رئیس ستاد کل به امور رسیدگی می‌کند، در امور اطلاعات ریاست هر یک از سازمان‌های ذی‌ربط به وزارت‌خانه متبوع خود پاسخ‌گو است و در مسائل مربوط به جرائم سایبری نیروی پلیس با همکاری دادستانی و قضات اختیار امور را در دست دارد[5].

هر یک از نیروهای ارتش (زمینی/هوایی/دریایی) تحت‌ریاست کام‌سایبر دارای مرکز عملیات‌های امنیتی (SOC)[6] مختص به خود هستند که به امور عملیات‌های

1. Cyber Defense Executive Committee
2. Cyber Defense Steering Committee

۳. رجوع شود به:
Laudrain, 'French Cyber Security and Defense', p. 24

۴. همان.

۵. این موضوع در ص ۵۳ گزارش بررسی راهبردی دفاع سایبری (Revue stratégique de cyberdéfense') پیشنهاد شد و در سال ۲۰۱۹ اجرا شد. برای اطلاعات بیشتر رجوع شود به:
Institut des hautes études du ministère de l'Intérieur, 'Organisation de l'État français en gestion de crise cybernétique majeure', 2019,
https://inhesj.fr/articles/organisation-de-letat-francais-engestion-de-crise-cybernetique-majeure.

6. Security Operations Centre

سایبری دفاعی آن‌ها می‌پردازند[1]. مرکز تحلیل دفاع سایبری[2] به‌عنوان واحد عملیات‌های امنیتیِ وزارت نیروهای مسلح محسوب می‌شود که وظیفه بررسی و تحلیل خطرهای سایبری بین‌المللی را برعهده دارد و در کنار گزارش نتایج به کام‌سایبر، توصیه‌های لازم را نیز به سایر مراجع دولتی ارائه می‌کند. مرکز بررسی امنیت سامانه‌های اطلاعاتی[3] مسئولیت اجرای بازرسی‌های امنیتی و تست‌های نفوذ برای سامانه‌های نظامی را برعهده دارد. شرکت سیگنال‌های ۸۰۷[4] به‌عنوان شاخه عملیاتی کام‌سایبر در منطقه رنِه[5] مستقر است که تامین امنیت ارتباطات و سامانه‌های جنگی در عملیات‌ها وظیفه اصلی آن محسوب می‌شود. تعداد نیروهای کام‌سایبر در اواخر سال ۲۰۱۹ بالغ بر ۳۴۰۰ نفر بود که طبق شواهد قصد دارد تا سال ۲۰۲۵ آن‌ها را به ۴۵۰۰ نفر افزایش دهد[6].

همانند دیگر قدرت‌های سایبری بزرگ، کارایی نظام حکمرانی فضای سایبری فرانسه نیز به کمک سامانه‌های فنی با کیفیت بالا و در پرتو هماهنگی و تفاهم کافی بین نهادهای ذی‌ربط و رهبری سیاسی آگاه به ارزش توانمندی‌های سایبری در عملیات‌های مختلف ارتقا یافته‌است.

---

۱. رجوع شود به:

Laudrain, 'French Cyber Security and Defense', p. 19,

2. Centre for the Analysis of Cyber Defense (Centre d'analyse de lutte informatique defensive)
3. Center for the Review of Information Systems Security (Centre d'audit de la sécurité des systèmes d'information)
4. 807th Signals Company
5. Rennes

۶. رجوع شود به:

COMCYBER, 'GDA Tisseyre: "On est 3400 cybercombattants et on deviendra 4500 en 2025"', @ComcyberFR on Twitter, 12 September 2019,
https://twitter.com/ComcyberFR/status/117 2186486134968322.

توانمندی‌های محوری در زمینه اطلاعات سایبری

همانند کشورهای عضو ائتلاف پنج چشم، همه نهادهای اطلاعاتی فرانسه نیز از توانمندی‌های سایبری برخوردار هستند و مسئولیت‌های سایبری آن‌ها متناسب با این توانمندی‌ها تعیین می‌شود. برخی از نهادهای کلیدی در حلقه اول نظام سایبری فرانسه شامل اداره امنیت و اطلاعات دفاعی[1]، اداره اطلاعات نظامی[2] و اداره کل امنیت داخلی[3] هستند، اما اداره کل امنیت خارجی (DGSE)[4] محور تولید اطلاعات سایبری در فرانسه به شمار می‌آید.

برخلاف کشورهای ائتلاف پنج چشم، در فرانسه تمایز نهادی آشکاری بین توانمندی‌های دفاعی و تهاجمی سایبری و نیز بین امنیت سایبری و اطلاعات سایبری وجود دارد. کام‌سایبر که نهادی نظامی است در عملیات‌های سایبری تهاجمی نقش اصلی را بازی می‌کند. درحالی‌که تامین امنیت سایبری در حوزه اختیارات سازمان ملی امنیت سایبری قرار دارد. تفاوت دیگر فرانسه با کشورهای ائتلاف پنج چشم مربوط به دایره اختیارات اداره کل امنیت خارجی فرانسه است که همه امور حوزه گردآوری اطلاعات سیگنال‌ها و نیز اطلاعات انسان‌ها را برعهده دارد. به‌عبارت دیگر، توسعه توانمندی‌های اطلاعاتی-سایبری در فرانسه ازجمله صلاحیت‌های اداره کل امنیت خارجی است: برخلاف سازمان امنیت ملی در آمریکا و ستاد ارتباطات دولت در بریتانیا، در فرانسه هیچ نهاد تخصصی برای این حوزه وجود ندارد. این موضوع در کنار سایر تفاوت‌های نظام سایبری فرانسه مقایسه مستقیم آن را با دیگر قدرت‌های بزرگ سایبری دشوار می‌سازد. به‌عنوان مثال، طبق شواهد موجود سرمایه‌گذاری سالانه فرانسه در توانمندی‌های سایبری

1. Defense Intelligence and Security Directorate (Direction du Renseignement et de la Sécurité de la Défense)
2. Directorate of Military Intelligence (Direction du renseignement militaire)
3. General Directorate for Internal Security (Direction générale de la sécurité intérieure)
4. Direction générale de la sécurité extérieure

محوری در مقایسه با بریتانیا کمتر است. هنوز به‌طور دقیق نمی‌توان گفت تمایز نهادی بین اطلاعات سایبری و امنیت سایبری و نیز بین توانمندی‌های فنی و انسانی در فرانسه در مقایسه با دیگر مدل‌های موجود برای آن مزیت محسوب می‌شود یا خیر.

به‌طور کلی، توانمندی‌های اطلاعاتی-سایبری فرانسه به‌ویژه در برخی مناطق جغرافیایی مانند شمال آفریقا قوی است، اما دسترسی جهانی آن در سطح کشورهای عضو ائتلاف پنج چشم به‌خصوص آمریکا و بریتانیا نیست. درحقیقت، افشاگری‌های اسنودن درباره سطح تخصص و پیشرفت کشورهای پنج چشم نهادهای اطلاعاتی فرانسه را شگفت‌زده کرد. امروزه فرانسه به‌مدد برخی مشارکت‌های بین‌المللی ازجمله با بریتانیا و ایالات متحده و کشورهای مستعمره سابق خود توانسته‌است تا حد زیادی توانمندی‌های سایبری خود را ارتقا بخشد.

حمایت نهادهای اطلاعاتی از فعالیت‌های جاسوسی صنعتی کسب‌وکارها و صنایع کشور یکی دیگر از تفاوت‌های فرانسه با کشورهای عضو ائتلاف پنج چشم است. بنا به ادعای یکی از مدیران سابق اداره کل امنیت خارجی فرانسه، در زمان حضور او در این نهاد حدود یک‌چهارم منابع آن به چنین فعالیت‌هایی تخصیص می‌یافت[۱]. کسب‌وکارهای فرانسوی نیز انگیزه خوبی برای همکاری با نهادهای اطلاعاتی دولت دارند، زیرا در مقابل همکاری با دولت اطلاعات ارزشمندی دریافت می‌کنند. ظاهرا توانمندی‌های سایبری جزء تفکیک‌ناپذیر عملیات‌های جاسوسی صنعتی فرانسه هستند و هدف اغلب آن‌ها شرکت‌های چندملیتی اروپایی، سازمان‌های ایرانی و کشورهای آفریقایی فرانسوی‌زبان است[۲].

۱. رجوع شود به:
Isabelle Laumonier, 'Internet sous l'oeil des services de renseignement', Memoire Online, c. 2003, https://www.memoireonline.com/05/06/155/m_internet-sous-l-oeil-desservices-de-renseignement14.html.

۲. رجوع شود به:
'France and economic intelligence', Tarlogic, 6 November 2019, https://www.tarlogic.com/en/blog/france-and-economicintelligence.

توانمندی و وابستگی سایبری

فرانسه در میان کشورهای توسعه‌یافته در زمینه دیجیتال‌سازی جامعه و اقتصاد پیشتاز نیست. در سال ۲۰۲۰ در شاخص اقتصاد و جامعه دیجیتال[۱] اتحادیه اروپا، فرانسه رتبه پانزدهم را در بین ۲۸ کشور اروپایی (شامل بریتانیا) به خود اختصاص داد[۲]. طبق این شاخص، سهم بخش فناوری اطلاعات و ارتباطات از تولید ناخالص داخلی فرانسه ۴ درصد است[۳] که مشتمل بر ۱۱۰ هزار شرکت[۴] و بیش از ۷۰۰ هزار نفر نیروی کار می‌شود[۵]. البته در مفهومی وسیع‌تر از اقتصاد دیجیتال، بخش بانکداری فرانسه یکی از قوی‌ترین عملکردهای دیجیتال را دارد، به‌طوری‌که تنها صنعت فناوری مالی آن ۱۲۰ هزار شغل ایجاد کرده‌است[۶]. شرکت‌های فرانسوی در عرصه بین‌المللی بسیار فعال هستند: شرکت‌های وب به‌طور میانگین ۳۹ درصد گردش مالی خود را در بازارهای بین‌المللی

1. Digital Economy and Society Index

۲. رجوع شود به:
European Commission, 'EU Digital Economy and Society Index 2020', https://ec.europa.eu/digital-single-market/en/desi

۳. رجوع شود به:
Eurostat, 'Percentage of the ICT Sector on GDP', https://ec.europa. eu/eurostat/web/products-datasets/-/tin00074.

۴. رجوع شود به:
Ministry of the Economy and Finance, 'Numérique: Chiffres clés', 14 March 2019, https://www.entreprises.gouv.fr/ etudes-et-statistiques/numerique-chiffres-cles.

۵. رجوع شود به:
G. De Prato (ed.), The 2018 PREDICT Key Facts Report: An Analysis of ICT R&D in the EU and Beyond, European Commission, JRC Technical Report, 2018, https://publications.jrc.ec.europa.eu/ repository/bitstream/JRC112019/jrc112019_2018_predict_key_facts_report.pdf.

۶. رجوع شود به:
Ministry of the Economy and Finance, 'La Fintech, le numérique au service du secteur financier', 19 January 2018, https://www. economie.gouv.fr/entreprises/fintech-innovation-finance.

تولید می‌کنند[۱] و ۵۲ درصد از شرکت‌های نوپای حوزه فناوری مالی نیز در بیش از یک کشور فعالیت دارند[۲].

فرانسه از مصرف‌کنندگان بزرگ خدمات دیجیتال به‌شمار می‌رود: شرکت‌های فرانسوی بیش از همتایان خود در اروپا یا ایالات متحده در زمینه فناوری اطلاعات و امنیت سایبری سرمایه‌گذاری می‌کنند و درنتیجه، در حملات سایبری کم‌ترین هزینه را متحمل می‌شوند[۳]. محیط نوآوری و شرکت‌های نوپای فرانسه به یمن اصلاحات دولت ماکرون پویا و روبه‌رشد است. به‌عنوان نمونه، ایستگاه اِف[۴] در پاریس یکی از بزرگ‌ترین مراکز رشد اروپاست و با همکاری شرکت‌های مایکروسافت و تِیلز دیجیتال فَکتوری[۵] پروژه‌هایی در زمینه امنیت سایبری اجرا می‌کند. تخصص‌های اصلی شرکت‌های نوپای فرانسوی شامل هوش مصنوعی، بلاک‌چین، حریم خصوصی و ابزارهای مشارکتی ایمن[۶] می‌شود. تقریبا ۲۰ درصد از این شرکت‌ها دارای تاییدیه سازمان ملی امنیت سایبری فرانسه هستند[۷] و درنتیجه می‌توان گفت علاوه براین‌که کیفیت محصولات و خدمات آن‌ها موردتایید است، این شرکت‌ها می‌توانند با نهادهای دولتی نیز قرارداد منعقد کنند.

---

۱. رجوع شود به:

'La French Tech', Gouvernement.fr.
https://lafrenchtech.com/en.

۲. رجوع شود به:

'Baromètre EY - FD', France Digitale blog, accessed 8 July 2019,
http://www.francedigitale.org/barometre-ey-fd.

۳. رجوع شود به:

Hiscox, 'Hiscox Cyber Readiness Report 2019',
https://www.hiscox.co.uk/sites/uk/files/documents/2019-04/Hiscox_Cyber_Readiness_Report _2019.PDF.

4. Station F
5. Thales Digital Factory
6. Secure Collaborative Tools

۷. همان.

فرانسه در زمینه تحقیق و توسعه هوش مصنوعی از توان بالایی برخوردار است و در بین پنج کشور برتر اتحادیه اروپا قرار دارد[۱]. در سال ۲۰۲۰، فرانسه از نظر سهم مقالات در دو کنفرانس برتر هوش مصنوعی رتبه پنجم جهان را کسب کرد[۲]. در سال ۲۰۱۸، دولت راهبردی در زمینه هوش مصنوعی ارائه کرد که بر اهداف زیر متمرکز بود: ترویج اشتراک‌گذاری داده بین بخش‌های خصوصی و دولتی؛ احیای چهار بخش راهبردی سلامت، محیط‌زیست، حمل‌ونقل، دفاع و امنیت؛ ایجاد قطب‌های تحقیقات هوش مصنوعی بین‌رشته‌ای و دارای ارتباط با صنعت[۳]. دولت قصد داشت ۱/۵ میلیارد یورو (معادل ۱/۷۵ میلیارد دلار) طی دوره‌ای پنج ساله (تا پایان سال ۲۰۲۲) در این راهبرد سرمایه‌گذاری کند[۴].

تاب‌آوری زیرساخت اینترنت فرانسه به‌واسطه تنوع‌بخشی به نقاط دسترسی، افزایش ظرفیت ارتباط داخلی و تعداد بالای نقاط دسترسی بین‌المللی روبه‌رشد است. اینترنت فرانسه از نظر تعداد نقاط ارتباط داخلی رتبه پنجم را در اتحادیه اروپا دارد[۵]

---

۱. رجوع شود به:

European Commission, Joint Research Centre, 'AI Watch: TES Analysis of AI Worldwide Ecosystem in 2009-2018',
JRC Technical Reports, LU: European Commission, 2020, pp. 30-1, https://data.europa.eu/doi/10.2760/85212.

۲. رجوع شود به:

Gleb Chuvpilo, 'AI Research Rankings 2020: Can the United States Stay Ahead of China?', 21 December 2020, https://chuvpilo.medium.com/ai-research-rankings-2020-can-theunited-states-stay-ahead-of-china-61cf14b1216.

۳. رجوع شود به:

'AI for Humanity', AI for Humanity, 29 March 2018, https:// www.aiforhumanity.fr.

۴. همان.

۵. رجوع شود به:

Arcep, 'Baromètre de l'interconnexion de données en France', 27 June 2019, https://www.arcep.fr/cartes-et-donnees/nospublications-chiffrees/linterconnexion-de-donnees/barometrede-linterconnexion-de-donnees-en-france.html.

که معادل ۴ درصد کل دنیاست[۱]. شرکت اپراتور اُرَنج[۲] که دارای یک شبکه فیبر نوری (موسوم به WELDON) است، ۲۵ شهر بزرگ فرانسه را به دیگر کلان‌شهرهای اروپایی مانند بارسلون، فرانکفورت، لندن و مادرید متصل می‌کند[۳].

پس از بریتانیا، فرانسه دومین کشور اروپایی میزبان بیشترین کابل‌های فرا-آتلانتیک است و یکی از قطب‌های عبور کابل‌های آسیا از مسیر دریای سرخ محسوب می‌شود. البته از نظر اقتدار (استقلال) شبکه‌ای باید گفت که بیشتر شبکه‌های فرانسه به سرورهای ساخت ایالات متحده وابسته هستند[۴]. بااین‌حال، بنیان صنعتی فرانسه از نظر تنوع و توان فناورانه برای ملی‌سازی شبکه‌های اصلی-در صورت ضرورت-از آمادگی کافی برخوردار است: به‌عنوان مثال، شرکت‌های ثیلز، ارنج و اَتوس-بال[۵] همگی از نظر فناوری مخابرات ایمن یا انبوه در سطح اروپا یا جهان پیشتاز هستند. به‌موجب مقررات مصوب جولای ۲۰۱۹ در مجمع ملی[۶] فرانسه، شرکت‌های اپراتور اینترنت باید قبل از به‌کارگرفتن سخت‌افزارهای خارجی از دولت مجوز دریافت کنند[۷]. درنتیجه، بیشتر شرکت‌های فرانسوی به ناچار از شرکت چینی هوآوی چشم‌پوشی کرده‌اند.

---

۱. برای منبع محاسبات رجوع شود به:
Rowan Klöti et al., 'A Comparative Look into Public IXP Datasets', ACM SIGCOMM Computer Communication Review, vol. 46, no. 1, 11 January 2016, pp. 21-9, https://doi.org/10/f8bkst

2. Orange

۳. رجوع شود به:
Orange, 'Les Réseaux d'Orange: dossier de presse', February 2019, https://www.orange.com/sirius/edossiers/pdfs/reseauxorange-2017-fr/dp_reseaux_orange_fr_full.pdf.

۴. رجوع شود به:
France IX, 'France-IX's Infrastructure'. https://www.franceix.net/en/technical/infrastructure.

5. Atos-Bull

۶. National Assembly (مجلس عوام پارلمان فرانسه)

۷. رجوع شود به:
Wei Shi, 'French parliament passes "Huawei Law" to govern 5G security', telecoms, 26 July 2019, https://telecoms.com/498728/french-parliament-passes-huawei-law-togovern-5g-security.

سیاست فرانسه مبتنی بر حفظ اقتدار ملی در سخت‌افزارهای نظامی مهم مانند حسگرها، سامانه‌های فرماندهی و کنترل، شبکه‌های اصلی و فناوری رادارگریز است. شرکت ثیلز مسئولیت طراحی، تولید و راه‌اندازی شبکه‌های ایمن برای وزارت نیروهای مسلح و کل دولت را برعهده دارد[1]. اگرچه وابستگی نیروهای مسلح فرانسه به تجهیزات و برنامه‌های پیشرفته مبتنی بر فناوری‌های اطلاعات و ارتباطات به سرعت روبه‌افزایش است (ازجمله برای ناوهای جنگی نسل جدید و برنامه‌های رافائل اف فور و اِسکورپیون[2])، اما در عین حال دولت تلاش می‌کند این امر کارایی نیروها را در محیط‌های جنگ متعارف و با تجهیزات ارتباطی غیرمدرن کاهش ندهد.

فرانسه مجموعه بزرگی از انواع ماهواره‌های نظامی مختص ارتباطات ایمن، عملیات‌های تصویربرداری و اطلاعات سیگنالی نیز در اختیار دارد. فرانسه به مسائل امنیت در فضا بیش از پیش اهمیت می‌دهد، زیرا به‌خوبی دریافته است فضا صرفا محلی برای حمایت از زیرساخت‌های عملیات‌های زمینی نیست و خود می‌تواند عرصه نبرد نظامی باشد. بنابراین، این کشور برخورداری از آگاهی موقعیتی در فضا را اولین محور راهبردی در حفظ استقلال فضایی می‌داند. وزارت نیروهای مسلح مبلغ ۴/۳ میلیارد یورو (معادل ۵/۱ میلیارد دلار) به مدرن‌سازی ماهواره‌ها و رادارها و نیز حفاظت

1. ‘Thales Modernise Les Réseaux de Télécommunications Du Ministère de La Défense’, Thales Group, accessed 9 July 2019, https://www.thalesgroup.com/fr/monde/press-release/thalesmodernise-les-reseaux-de- telecommunications-du-ministere-dela-defense;

‘Thales Assure La Sécurité de l’accès à Internet Du Réseau Interministériel de l’État’, Thales Group, accessed 12 July 2019, https://www.thalesgroup.com/fr/worldwide/securite/press-release/thales-assure-la-securite-de-lacces-internet-du-reseau.

2. Rafale F4 and Scorpion

از دارایی‌های فضایی فرانسه اختصاص داده‌است[۱]. در فوریه ۲۰۲۱، دولت فرانسه از افتتاح مرکز عالی تحقیقات فضایی ناتو[۲] در منطقه تولوز[۳] خبر داد که بنا بر ادعای آن، بزرگ‌ترین زیست‌بوم فضایی اروپاست (که میزبان فرماندهی فضایی[۴] فرانسه، آکادمی فضا[۵]، شرکت‌های فضایی بین‌المللی و آزمایشگاه‌ها و مراکز تحقیقاتی متعددی است)[۶].

امنیت و تاب‌آوری سایبری

فرانسه در بسیاری از ابعاد برنامه‌ریزی تاب‌آوری و امنیت سایبری در رده کشورهای پیشتاز اتحادیه اروپا قرار دارد. به‌عنوان مثال، گزارشی دولتی در سال ۲۰۲۰ نشان می‌دهد شرکت‌های فرانسوی بیش از دیگر شرکت‌های اروپایی در زمینه مسائل امنیت سایبری سرمایه‌گذاری می‌کنند[۷]. مطالعه دیگری درباره امنیت سایبری در شرکت‌های فهرست‌شده در شش شاخص برتر بازار سرمایه[۸] حاکی از آن است که شرکت‌های فهرست شده در شاخص سی‌اِی‌سی۴۰[۹] پاریس دارای بالاترین سطح بلوغ

۱. رجوع شود به:
Arthur Laudrain, 'France's "Strategic Autonomy" Takes to Space', International Institute for Strategic Studies, Military Balance blog, 14 August 2019,
https://www.iiss.org/blogs/military-balance/2019/08/france-space-strategy.

2. NATO Center of Excellence
3. Toulouse
4. Space Command
5. Space Academy

۶. رجوع شود به:
Ministère de l'Europe et des Affaires Étrangères, 'Defense Establishment of the NATO space center of excellence in Toulouse - Communiqué issued by the Ministry for the Armed Forces', 5 February 2021,
https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-nonproliferation / news/article/defence-establishment-of-the-natospace-centre-of-excellence-in-toulouse.

۷. رجوع شود به:
European Union Agency for Cybersecurity, 'NIS Investments Report', December 2020, p. 7,
https://www.enisa.europa.eu/publications/nis-investments/at_download/fullReport

8. Six leading stock-market indexes
9. Paris's CAC 40

امنیت سایبری هستند[۱]. با این همه، دولت در سال ۲۰۲۱ از عملکرد بخش خصوصی و بخش دولتی در مقابله با تهدیدهای سایبری ناراضی بود و به همین دلیل، با انتصاب هماهنگ‌کننده ملی[۲] و اجرای برنامه شتاب‌بخشی[۳] سعی کرد مشکلات را برطرف کند. افزایش چهار برابری حمله‌های باج‌افزاری در سال ۲۰۲۰ یکی از جدی‌ترین تهدیدهای شناسایی‌شده در فرانسه بود که بیش از همه به نهادهای ارائه‌کننده خدمات دولتی آسیب رساند[۴].

مسئولیت هماهنگی امنیت زیرساخت‌های فرانسه برعهده اداره کل دفاع و امنیت سایبری است و اجرای سیاست‌های دولت در مورد زیرساخت‌های حیاتی ملی و انتخاب شرکت‌های موردنظر برای مدیریت و راه‌اندازی آن زیرساخت‌ها ازجمله وظایف آن محسوب می‌شود. طبق قانون برنامه‌ریزی دفاعی ۲۰۱۹-۲۰۱۴[۵]، وظایف این شرکت‌ها-اعم از دولتی یا خصوصی-شامل مواردی مانند تامین امنیت شبکه‌ها و سامانه‌های کنترل صنعتی، داشتن توانمندی‌های شناسایی تهدیدها و اجرای تست‌های نفوذ می‌شود. براساس قانون، نهادهای دولتی حق دارند توان دفاع سایبری شرکت‌ها را ارزیابی و تست کنند[۶] و عملیات‌های سایبری (هک معکوس) برای خنثی‌سازی منبع حمله‌ها اجرا

۱. رجوع شود به:
Wavestone, 'Top Companies Cybersecurity Index: 2020 Annual Reports'.
https://www.wavestone.com/app/uploads/2020/07/Wavestone-Cyberindex-top-companies -2020-EN.pdf.

2. National Coordinator

3. Acceleration

رجوع شود به:
'Dossier de presse - Cybersécurité, faire face à la menace: la stratégie française', Gouvernement.fr, p. 12.

۴. همان، ص. ۱۱-۷.

5. Defense Planning Law 2014-19

۶. رجوع شود به:
'Loi N° 2013-1168 Du 18 Décembre 2013 Relative à La Programmation Militaire Pour Les Années 2014 à 2019 et Portant Diverses Dispositions Concernant La Défense et La Sécurité Nationale - Article 22 | Legifrance', accessed 29 March 2019,
https://www.legifrance.gouv.fr/eli/loi/2013/12/18/2013-1168/jo/article_22.

کنند[۱]. در سال ۲۰۱۹، دولت قراردادهای سه‌ساله‌ای را با هشت شرکت تولیدی بزرگ برای ارتقای امنیت سایبری آن‌ها امضا کرد[۲] و مرجع بازارهای مالی[۳] فرانسه مقررات جدیدی تصویب کرد که شرکت‌های ارائه‌کننده محصولات/خدمات دیجیتال را ملزم به داشتن سامانه‌هایی با تاب‌آوری بالا می‌کرد[۴].

در راستای بهبود سطح همکاری بخش‌های خصوصی و دولتی در زمینه امنیت سایبری، دولت فرانسه قصد دارد پردیس ملی امنیت سایبری[۵] را با ماموریت‌های زیر تاسیس کند: ارتقای آگاهی عمومی و آموزش همگانی؛ تقویت به‌اشتراک‌گذاری مهارت، ابزار و داده در بین فعالان امنیت سایبری و افزایش ظرفیت داخلی در امنیت سایبری[۶]. هدایت این پروژه برعهده مدیر شرکت اُرنج است. سازمان ملی امنیت سایبری نیز در راستای افزایش همکاری‌های بخش خصوصی و بخش دولتی توانسته‌است قراردادهایی برای مشارکت با شرکت‌های مالی، راه‌آهن و هواپیمایی منعقد کند[۷].

توانمندی‌های دفاعی فرانسه از استانداردهای بالایی برخوردارند، به‌طوری‌که تیم فرانسوی در بین ۲۳ کشور شرکت‌کننده در مانور ۲۰۱۹ ناتو (Locked Shields) رتبه اول را

---

۱. رجوع شود به:
'Code de La Défense - Article L2321-2', L2321-2 Code de la défense § (2013).

۲. شرکت‌ها عبارتند از: Airbus, ArianeGroup, Dassault Aviation, MBDA, Naval Group, Nexter, Safran and Thales.
برای کسب جزئیات بیشتر رجوع شود به:
G20 Research Group, '2019 G20 Osaka Summit Interim Compliance Report', p. 223, http://www.g20.utoronto.ca/compliance/2019osaka-interim/08-2019-g20-complianceinterim -cyber-resilience.pdf.

3. Financial Markets Authority

۴. همان.

5. National Cyber Security Campus

۶. رجوع شود به:
'Un campus cybersécurite pour renforcer l'écosystème français', Gouvernement.fr, accessed 25 July 2019, https://www.gouvernement.fr/partage/11104-un-campus-cybersecuritepour-renforcer-l-ecosysteme-francais

۷. رجوع شود به:
Agence nationale de la sécurité des systèmes d'information, 'Rapports d'activités', https://www.ssi.gouv.fr/agence/missions/rapports-dactivites.

کسب کرد[۱] و در شاخص امنیت سایبری جهانی ۲۰۱۸ نیز فرانسه رتبه سوم را در بین ۱۷۵ کشور به‌دست آورد[۲].

نهاد تدارکات دفاعی فرانسه یعنی اداره کل تسلیحات[۳] (DGA) دارای یک بخش امنیت سایبری باسابقه تحت شعبه کنترل اطلاعات (Maîtrise de l'information) خود است که وظیفه آن حفاظت از سامانه‌های اطلاعاتی و جنگی نیروهای مسلح است و خدمات فنی و تخصصی در زمینه اطلاعات مربوط به تهدیدها، تحقیقات بالادستی و پشتیبانی بحران ارائه می‌کند[۴]. افزون بر آن، این بخش تحقیقاتی درباره سطح آسیب‌پذیری سامانه‌های نیروهای دفاعی انجام می‌دهد[۵] و از سال ۲۰۱۵ به تهیه و اجرای بازی‌های جنگ سایبری (نمونه‌هایی برای تمرین حمله سایبری در زمان واقعی) می‌پردازد[۶]. اولویت‌های تحقیق و توسعه اداره کل تسلیحات در زمینه دفاع سایبری شامل تولید سامانه‌های اطلاعاتی با تاب‌آوری بسیار بالا، یافتن راه‌حل‌هایی برای تضمین امنیت سامانه‌های جنگی و تعیین بهترین کاربردهای هوش مصنوعی در عملیات‌های سایبری

۱. رجوع شود به:
'France Wins Cyber Defense Exercise Locked Shields 2019', NATO CCDCOE, 12 April 2019, https://ccdcoe.org/news/2019/france-wins-cyber-defence-exercise-locked-shields-2019.

۲. رجوع شود به:
International Telecommunication Union, 'Global Cybersecurity Index 2018', pp. 30, 62, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

3. General Directorate of Armaments (Direction générale de l'armement)

۴. رجوع شود به:
Ministère des Armées, 'Livre blanc: Défense et sécurité nationale', 2013.

۵. رجوع شود به:
Assemblée nationale, 'Rapport d'information de Mme Alexandra Valetta Ardisson et M. Bastien Lachaud Déposé En Application de l'article 145 Du Règlement, Par La Commission de La Défense Nationale et Des Forces Armées, En Conclusion Des Travaux d'une Mission d'information Sur La Cyberdéfense', 4 July 2018, http://www2.assemblee-nationale. fr/documents/notice/15/rap-info/i1141/#P439_94811.

۶. رجوع شود به:
'La DGA Développe Les Jeux de Cyberguerre à Bruz', IntelligenceOnline, 11 March 2015, https://www.intelligenceonline.fr/renseignement-d-etat/2015/03/11/la-dgadeveloppe-les-jeux-de-cyberguerre-a-bruz,108065256-bre

(ازجمله عملیات‌های تهاجمی) می‌شود. صندوق سود سهام سرمایه‌گذاری‌های دفاعی به نام «دِف‌اینوِست» در سال ۲۰۱۷ با حمایت دولت و با بودجه اولیه ۵۰ میلیون یورو (معادل ۵۹ میلیون دلار) به‌منظور پشتیبانی از شرکت‌های کوچک و متوسط ایجاد شد[۱]. علاوه براین‌ها، دولت فرانسه در اداره کل دفاع و امنیت سایبری واحدی به نام کمیته مقابله با سوءاستفاده از اطلاعات[۲] تشکیل داده‌است تا به مسائل مربوط به نشر اطلاعات غلط سیاسی رسیدگی کند[۳].

تاکنون حداقل دو نمونه مداخله سایبری خارجی در فرانسه شناسایی شده‌است: هک شبکه تی‌وی‌فایوموند[۴] در سال ۲۰۱۶ و نفوذ به ایمیل‌های پویش انتخاباتی ماکرون در سال ۲۰۱۷. متخصصان این حمله‌ها را از جانب روسیه می‌دانستند. درنتیجه، در سال ۲۰۱۸ قانون جدیدی برای جلوگیری از نشر اطلاعات غلط در زمان انتخابات تصویب شد که میزان اثربخشی آن در آینده مشخص می‌شود. وزارت نیروهای مسلح در همکاری با شورای آتلانتیک[۵] تحقیقاتی تحلیلی درباره ماجرای نفوذ به ایمیل‌های انتخاباتی ماکرون انجام داده و تجربه خود را با هم‌پیمانانش به اشتراک گذاشته‌است[۶].

---

۱. رجوع شود به:
BPI France, 'Definvest: Fonds d'investissement dédié auxentreprises stratégiques de la Défense', accessed 8 July 2019,
https://www.bpifrance.fr/Toutes-nos-solutions/Participation-au-capital/Fonds-d-investissement-thematiques/Definvest.

2. Committee against Information Manipulation (Comité de lutte contre la manipulation de l'information (CLMI))

۳. رجوع شود به:
Sénat, 'Délégation Parlementaire au Renseignement: Rapport d)activité 2019-2020', 11 June 2020, http://www.senat.fr/rap/r19- 506/r19-50638.html.

4. TV5Monde
5. Atlantic Council

۶. رجوع شود به:
Jeangène Vilmer, 'The "#Macron Leaks" operation: A post-mortem'.

رهبری جهانی در عرصه سایبری

فرانسه مسئولیت بین‌المللی خود در زمینه امنیت سایبری را در قالب شورای امنیت سازمان ملل-به‌عنوان یکی از پنج عضو دائمی-اتحادیه اروپا و ناتو انجام می‌دهد و خواهان رویکردی چندذینفعی با مشارکت همه کشورها و حضور فعالان غیردولتی در مذاکرات و گفت‌وگوهای حول حکمرانی سایبری است. فرانسه در راهبرد بین‌المللی دیجیتال[۱] خود تاکید زیادی بر گسترش فضای سایبری باز، متنوع و قابل‌اعتماد دارد و اتحادیه اروپا را از بازیگران کلیدی این عرصه می‌داند[۲]. پاریس با ارتقای سازوکارهای نهادی موجود به‌ویژه با استفاده از ابتکار بین‌المللی «فراخوان پاریس برای اعتماد و امنیت در فضای سایبری»[۳] (نوامبر ۲۰۱۸) می‌کوشد از حجم حمله‌های هکری و فعالیت‌های برهم‌زننده ثبات در فضای سایبری بکاهد[۴]. فرانسه در شکل‌گیری گروه کارشناسان دولتی سازمان ملل[۵] و تدوین قانون امنیت سایبری[۶] اتحادیه اروپا نقش موثری داشته‌است. فرانسه در سال ۲۰۱۹ به نیوزیلند در فراخوان کرایست‌چرچ برای حذف محتواهای برخط تروریستی و

1. International Digital Strategy

۲. رجوع شود به:
Ministère de l'Europe et des Affaires Étrangères, 'Stratégie internationale de la France pour le numérique', Paris, 15 December 2017,
https://www.diplomatie.gouv.fr/fr/politique-etrangere-dela-france/diplomatie-numerique/la-strategie-internationale-de-lafrance-pour-le-numerique/#:~:text=Pr%C3%A9sent%C3%A9e%20 par%20le%20ministre%20de,diplomatique%20des%20ann%C3%A9es%20%C3%A0%20venir.&text=Elle%20 s'articule%20autour%20de,%3A%20gouvernance%2C%20 %C3%A9conomie%2C%20s%C3%A9curit%C3%A9.

3. Paris Call for Trust and Security in Cyberspace

۴. رجوع شود به:
Arthur Laudrain, 'Avoiding A World War Web: The Paris Call for Trust and Security in Cyberspace', Lawfare, 4 December 2018,
https://www.lawfareblog.com/avoiding-world-war-webparis-call-trust-and-security-cyberspace.

۵. رجوع شود به:
UN Office for Disarmament Affairs, 'Developments in the field of information and telecommunications in the context of international security'.
https://www.un.org/disarmament/ict-security.

6. Cybersecurity Act

افراط‌گرایانه خشونت‌آمیز[1] پیوست. البته پیش از آن نیز فرانسه خواستار تهیه چارچوب مقرراتی مناسبی در اتحادیه اروپا برای تضمین امنیت سایبری شده‌بود[2].

فرانسه دیپلماسی دوجانبه قوی با کشورهای تاثیرگذار سایبری دارد و ازطریق سازوکارهایی مانند گروه ۷ نیز دیپلماسی بین‌المللی خود را پیگیری می‌کند. به‌عنوان مثال، فرانسه و آلمان گزارش سومین ارزیابی سالانه امنیت فناوری اطلاعات و ارتباطات را در سال ۲۰۲۰ منتشر کردند[3]، سومین دور گفت‌وگوهای سایبری هند و فرانسه در سال ۲۰۱۹ برگزار شد[4] و در دوره ریاست فرانسه بر گروه ۷ نیز ابتکار به‌اشتراک‌گذاری بهترین تجارب و آموزه‌های حوزه اجرای داوطلبانه هنجارهای فضای سایبری آغاز شد[5]. فرانسه در سال ۲۰۱۸ همایش جهانی امنیت دیجیتال برای شکوفایی اقتصادی[6] را در سازمان همکاری اقتصادی و توسعه برگزار کرد. هدف اصلی فرانسه از برگزاری این همایش ارتقای موقعیت بخش خصوصی کشور به‌دلیل تاثیرگذاری بالای آن در امنیت و ثبات فضای سایبری بود.

1. Christchurch Call to Eliminate Terrorist and Violent Online Content

۲. رجوع شود به:
Ministère de l'Europe et des Affaires Étrangères, 'Guaranteeing Cybersecurity', undated, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-s-internationaldigital-strategy/article/guaranteeing-cybersecurity.

۳. رجوع شود به:
Federal Office for Information Security (Germany) and Agence Nationale de la Sécurité des Systèmes d'Information, 'Third edition of the Franco-German common situational picture', 2020, https://www.ssi.gouv.fr/uploads/2020/12/anssi-bsi-common_ situational_picture_2020.pdf

۴. رجوع شود به:
Ministère de l'Europe et des Affaires Étrangères, 'Indo-French Bilateral Cyber Dialogue', 20 June 2019, https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmamentand-non-proliferation/fight-against-organized-criminality/cyber-security/article/indo-french-bilateral-cyber-dialogue-20-06-19.

۵. رجوع شود به:
Ministère de l'Europe et des Affaires Étrangères, 'G7 French presidency - Cyber Norm Initiative: Synthesis of Lessons Learned and Best Practices', 26 November 2019, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digitaldiplomacy/news/article/g7-french-presidency-cyber-norminitiative-synthesis-of-lessons-learned-and.

6. Global Forum on Digital Security for Economic Prosperity

فرانسه در بسیج اتحادیه اروپا برای اعمال تحریم علیه عاملان حمله‌های سایبری به منافع ملی کشورها و اتحادیه اروپا نقش کلیدی داشته‌است. به‌عنوان مثال، فرانسه در سال ۲۰۲۰ به اولین دور تحریم‌های اتحادیه اروپا علیه چین و روسیه-به‌دلیل حمله‌های سایبری آن‌ها- ملحق شد[۱]. این تحریم‌ها شامل ممنوعیت سفر و توقیف اموال چهار عضو اداره اطلاعات نظامی روسیه (GRU) و دو تبعه چین می‌شد[۲].

در رابطه با انجام اقدامات تلافی‌جویانه در مقابل حمله سایبری پایین‌تر از آستانه حمله باید خاطرنشان ساخت که موضع فرانسه نسبت به هم‌پیمانان نزدیکش متفاوت است. زیرا باتوجه به تفسیر فرانسه از قوانین بین‌المللی، اگر چند حمله در مجموع از آستانه تهدید فراتر نروند ولی درمجموع برای کشور تهدیدکننده باشند، دولت فرانسه خود را مجاز به عملیات تلافی‌جویانه می‌داند[۳].

توانمندی‌های سایبری تهاجمی

کام‌سایبر فرانسه دارای نیروی عملیاتی متشکل از حدود ۳۴۰۰ نفر است که از آن میان، حدود ۶۰۰ نفر متخصص فناوری اطلاعات و ارتباطات هستند. کام‌سایبر قصد دارد

۱. رجوع شود به:
Ministère de l'Europe et des Affaires Étrangères, 'EU - Cyberattacks - Q&A from the press briefing', 30 July 2020,
https://www. diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/ france-and-cyber-security/article/eu-cyberattacks-q-a-from-thepress-briefing-30-jul-20.

۲. رجوع شود به:
Lorie Maglana and Sunny Man, 'Europe: EU imposes the first ever sanctions against cyber-attacks', Global Compliance News, 21 August 2020,
https://globalcompliancenews.com/eu-imposesthe-first-ever-sanctions-against-cyber-attacks-20200810.

۳. رجوع شود به:
Ministère des Armées, 'Droit International Appliqué Aux Opérations Dans Le Cyberespace', 9 September 2019,
https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqu%C3%A9+aux+op%C3%A9rations+Cyberespace.pdf.

تعداد نیروهای عملیاتی خود را تا سال ۲۰۲۵ به ۴۵۰۰ نفر افزایش دهد[۱]. بنا به اظهارات فرمانده کام‌سایبر، ۴۰ درصد نیروهای آن در زمینه عملیات‌های تهاجمی فعالیت دارند و انتظار می‌رود در سال‌های آتی سهم آن‌ها افزایش یابد[۲].

طبق اظهارات رسمی و غیررسمی و نیز افشای برخی گزارش‌های جرم‌شناسی فرانسه، دولت استفاده از فضای سایبری برای ایجاد اختلال[۳] و جاسوسی[۴] را تایید می‌کند. به گفته یکی از فرماندهان ارتش فرانسه، این کشور تاکنون چندین عملیات سایبری تهاجمی علیه گروه‌های تروریستی در منطقه ساحل (صحرا)[۵] و صحرای آفریقا اجرا کرده‌است[۶]. اگرچه شواهد چندانی از سایر عملیات‌های سایبری تهاجمی فرانسه در دست نیست،

۱. رجوع شود به:
Ministère des Armées, 'Le COMCYBER', 4 February 2021,
https://www.defense.gouv.fr/ema/organismes-interarmees/ le-comcyber/le-comcyber/comcyber.

۲. رجوع شود به:
Laurent Lagneau, 'Environ 40% des effectifs du Commandement de la cyberdéfense sont tournés vers les actions offensives', Zone Militaire, 9 May 2020,
http://www.opex360.com/2020/05/09/environ-40-des-effectifs-du-commandementde-la- cyberdefense-sont-tournes-vers-les-actions-offensives.

۳. رجوع شود به:
Nathalie Guibert, 'Général Lecointre: "L'indicateur de réussite n'est pas le nombre de djihadistes tués"', Le Monde, 13 July 2019,
https://www.lemonde.fr/international/article/2019/07/12/general-lecointre-l-indicateur-de- reussite-n-est-pas-le-nombrede-djihadistes-tues_5488379_3210.html.

۴. رجوع شود به:
Martin Untersinger and Jacques Follorou, 'La France suspectée de cyberespionnage', Le Monde, 21 March 2014,
https://www.lemonde.fr/international/article/2014/03/21/la-francesuspectee-de-cyberattaque_4387232_3210.html.

۵. ساحل در منطقه‌ای میان صحرای بزرگ آفریقا و ساوانای سودان واقع شده‌است که در شمال آفریقا از اقیانوس اطلس تا دریای سرخ امتداد یافته‌است و شامل شمال سنگال، جنوب موریتانی، مرکز مالی، جنوب الجزیره و نیجر، مرکز چاد، جنوب سودان، شمال سودان جنوبی و اریتره می‌شود.

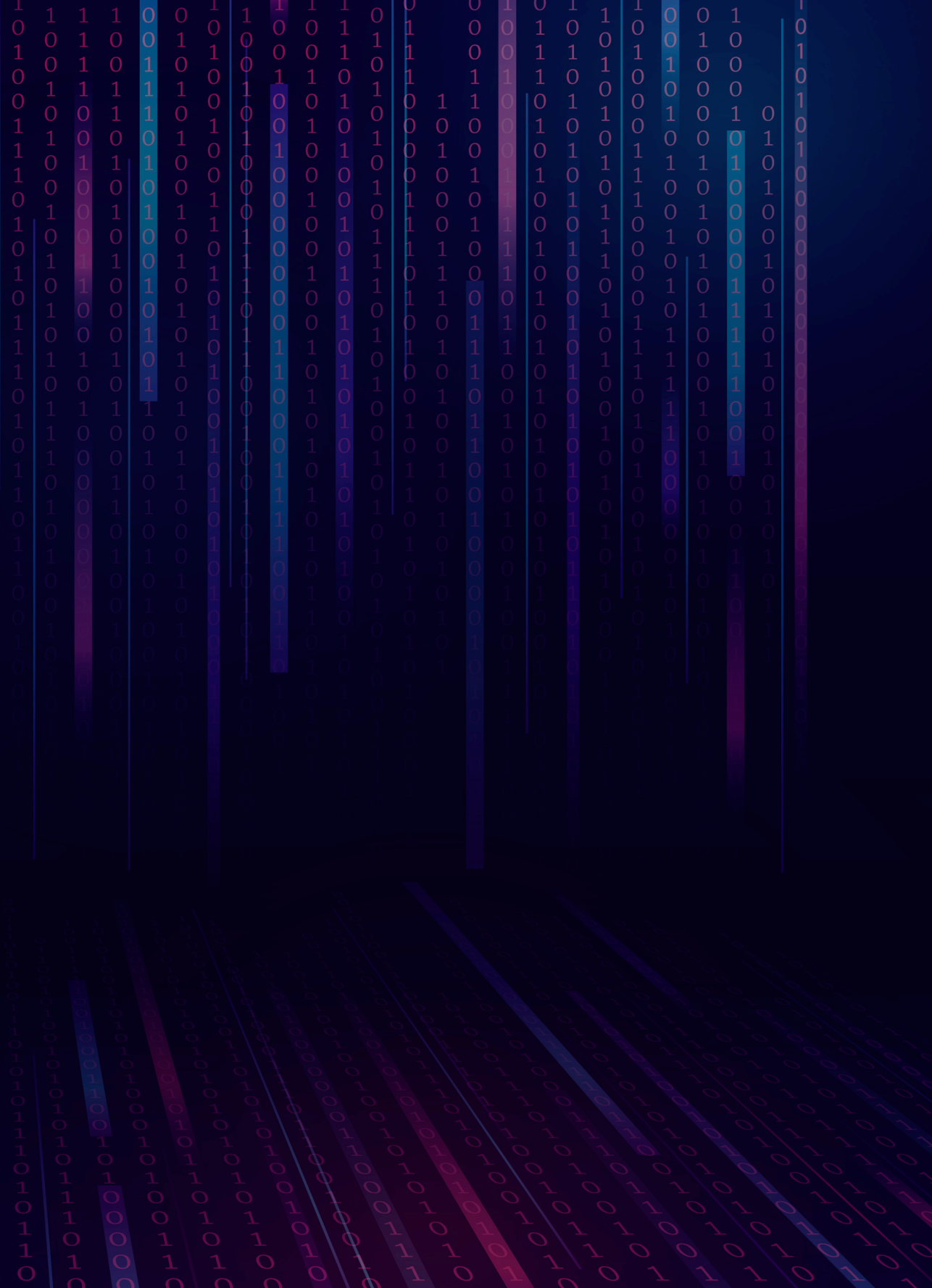
۶. رجوع شود به:
Simon Pascal, 'Cyberdéfense. "Nous allons accroître encore les capacités de la plaque rennaise"', Ouest-France.fr, 18 CYBER CAPABILITIES AND NATIONAL POWER: A Net Assessment 67 December 2020,
https://www.ouest-france.fr/politique/defense/ cyberdefense-nous-allons-accroitre-encore-les- capacites-de-laplaque-rennaise-7091506.

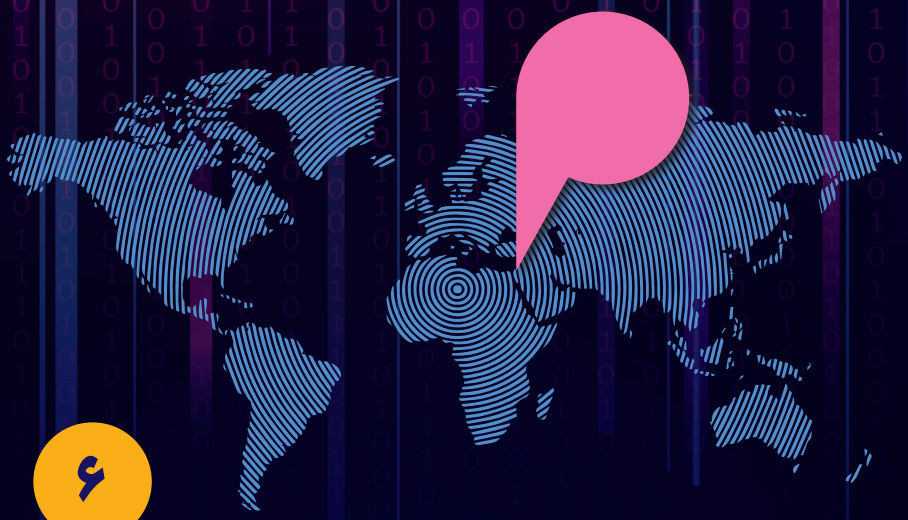
اما سوابق حمله‌های تلافی‌جویانه آن برای دفاع از منافع ملی بیانگر آمادگی بالای این کشور برای اجرای عملیات‌های سایبری تهاجمی در موقعیت‌های خاص است[۱]. سیاست رسمی فرانسه در مورد عملیات‌های سایبری تهاجمی علیه دیگر کشورها بر کاهش بار سیاسی، حقوقی و نظامی ناشی از خسارت‌های جانبی این حمله‌ها به زیرساخت‌های غیرنظامی کشورهای هدف تاکید دارد[۲]. بنابراین، به نظر نمی‌رسد فرانسه در عملیات‌های سایبری تهاجمی فراتر از مشاوره فنی به شرکت‌های خصوصی متکی باشد.

درمجموع و با توجه به شواهد موجود می‌توان گفت فرانسه توانمندی‌های سایبری تهاجمی قابل‌ملاحظه‌ای در اختیار دارد، اما همانند حوزه توانمندی‌های اطلاعاتی-سایبری، در این حوزه هم از بریتانیا و ایالات متحده ضعیف‌تر است.

۱. رجوع شود به:
Robert S. Dewar (ed.), 'National Cybersecurity and Cyberdefense Policy Snapshots: Collection 1', Center for Security Studies, 2018,
https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports_National_Cybersecurity_and_Cyberdefense_ Policy_Snapshots_Collection_1.pdf.

۲. رجوع شود به:
Laudrain, 'French Cyber Security and Defense', p. 9





۶

رژیم صهیونیستی

رژیم صهیونیستی از سال‌ها پیش (از ۲۰ سال قبل) فضای سایبری را تهدیدی بالقوه برای امنیت خود می‌داند. رژیم اشغالگر در ابتدا تهدید اصلی را حملات سایبری به زیرساخت‌های حیاتی می‌دانست، اما در ادامه احتمال هدف قرارگرفتن سایر دارایی‌های ارزشمند آن رژیم نیز مطرح شد. تحولات فناورانه و ژئوپلیتیک زمینه اصلاحات سازمانی زیادی را در نظام امنیت سایبری رژیم صهیونیستی ایجاد کرده‌است، به‌طوری‌که روش پاسخ‌دهی آن رژیم به تهدیدهای سایبری کاملا تغییر یافته‌است. تشکیل اداره ملی سایبری رژیم صهیونیستی (INCD)[1] در ستاد نخست‌وزیری در سال ۲۰۱۸ نقطه‌اوج اصلاحات ساختاری آن‌ها بود. علاوه بر این، رژیم اشغالگر پیش‌نویس راهبرد ملی سایبری خود مشتمل بر همکاری نزدیک بین دولت، بخش خصوصی و دانشگاه و با شرکای بین‌المللی را نیز تهیه کرده‌است. این نوع همکاری‌ها که به رهبری اداره ملی سایبری انجام می‌شوند، زیست‌بوم سایبری پویایی را برای رژیم صهیونیستی ایجاد کرده‌اند و سطح آمادگی و تاب‌آوری در بخش خصوصی آن را به‌میزان قابل‌توجهی افزایش داده‌اند. رژیم صهیونیستی اظهارات رسمی محدودی درباره توان و عملیات‌های سایبری تهاجمی خود مطرح می‌کند، اما تاکنون حملات مهمی به این کشور نسبت داده شده‌است که به‌عنوان نمونه می‌توان به حمله به تاسیسات ایران ازطریق بدافزار استاکس‌نت در فاصله سال‌های ۲۰۰۸ و ۲۰۱۰ و حمله به یکی از بندرهای ایران در سال ۲۰۲۰ اشاره کرد. باتوجه به چنین شواهدی به نظر می‌رسد که رژیم صهیونیستی از ظرفیت توسعه‌یافته‌ای در عملیات‌های سایبری تهاجمی برخوردار است و آمادگی استفاده از آن‌ها در طیف گسترده‌ای از موقعیت‌ها را دارد.

1. Israel National Cyber Directorate

راهبرد و مبنای نظری (دکترین)

رژیم صهیونیستی در سال ۲۰۰۰ به‌طور رسمی فضای سایبری را تهدیدی نوظهور برای امنیت ملی خود معرفی کرد و در سال ۲۰۰۲ نیز تصمیم گرفت نهادی تخصصی به‌منظور حفاظت از زیرساخت‌های اطلاعاتی رژیم تاسیس کند[۱]. از سال ۲۰۱۰ که بنیامین نتانیاهو دستور داد گروه ویژه‌ای برای تهیه راهبردی جهت قرارگرفتن رژیم صهیونیستی در میان پنج رتبه پیشتاز عرصه سایبری تشکیل شود، امنیت سایبری همواره یکی از اولویت‌های مهم امنیت این رژیم بوده‌است. سرپرستی این گروه ویژه که به آن ابتکار سایبری ملی[۲] اطلاق می‌شد، به پروفسور اسحاق بن اسرائیل[۳] رئیس شورای ملی تحقیق و توسعه[۴] محول شد و اعضای گروه نیز از میان کارکنان سازمان‌های کلیدی حوزه امنیت سایبری انتخاب شدند. مهم‌ترین توصیه عملی این گروه شامل ضرورت ایجاد سازمان دولتی جدید برای تامین امنیت سایبری به‌منظور ارتقای ظرفیت رژیم صهیونیستی در فضای سایبری و بهبود آمادگی آن برای مقابله با تهدیدهای سایبری بود[۵].

۱. کمیته امنیت ملی کابینه وزرا در سال ۲۰۰۲ مصوبه‌ای (Resolution B/84 on 'Responsibility for Protecting Computer Systems in Israel') صادر کرد که مبنای تشکیل «کمیته راهبری جهت شناسایی همه سیستم‌های کامپیوتری دولتی و خصوصی دارای اهمیت در امنیت» شد. برخی از این سیستم‌ها در اختیار ارتش رژیم صهیونیستی نیستند و متعلق به شرکت‌های دولتی یا خصوصی غیرنظامی هستند. مرجع امنیت اطلاعات نیز براساس همین مصوبه تشکیل شد تا به حفاظت از سیستم‌های کامپیوتری سازمان امنیت رژیم صهیونیستی (شین‌بت) بپردازد. به‌منظور کسب جزئیات بیشتر رجوع شود به:
Gil Baram, 'The Effect of Cyberwar Technologies on Force Buildup: The Israeli Case', Military and Strategic Affairs, vol. 5, no. 1, May 2013, p. 29,
https://www.inss.org.il/wp-content/uploads/systemfiles/MASA5-1Eng4_Baram.pdf.

2. National Cyber Initiative

3. Isaac Ben Israel

4. National Council for Research and Development

۵. در حال حاضر، فرایندی مشابه در رابطه با هوش مصنوعی نیز در جریان است که هدف آن قرارگرفتن رژیم صهیونیستی در بین پنج رتبه برتر است.
Éanna Kelly, 'Israel sets out to become the next major artificial intelligence player', Science Business, 2 July 2019, https://sciencebusiness.net/news/israel-sets-out-become-next-major-artificial-intelligenceplayer; and Lior Tabansky and Isaac Ben Israel, Cybersecurity in Israel (Cham: Springer International Publishing, 2015), pp. 47-50.

در اولین راهبرد امنیت سایبری[1] رژیم صهیونیستی (۲۰۱۷) مقرر شده‌است این رژیم به یکی از پیشگامان در به‌کارگیری فضای سایبری به‌عنوان موتور رشد اقتصادی، رفاه اجتماعی و امنیت تبدیل شود. این راهبرد بر مساله امنیت به‌ویژه ازمنظر حفظ ایمنی فضای سایبری و مقابله با تهدیدهای سایبری مختلف طبق منافع رژیم متمرکز است. علاوه بر این، رژیم صهیونیستی به‌موجب این راهبرد باید بکوشد تا به یکی از رتبه‌های پیشتاز در عرصه نوآوری فناورانه و شریکی فعال در فرایندهای جهانی شکل‌دهی به فضای سایبری تبدیل شود[2].

اگرچه رژیم صهیونیستی در مورد کاربردهای غیرنظامی فضای سایبری از شفافیت نسبی برخوردار است، اما درباره استفاده نظامی از فضای سایبری اطلاعات بسیار کمی منتشر می‌کند. درواقع، رژیم صهیونیستی هیچ‌گاه سندی تحت‌عنوان راهبرد سایبری نظامی منتشر نکرده‌است. با این حال، رویکرد رژیم صهیونیستی را می‌توان تا حدودی از اظهارات رسمی مقامات نظامی ارشد آن استنباط کرد. به‌عنوان مثال، یکی از مقام‌های رسمی رژیم صهیونیستی در اظهارات خود در سال ۲۰۰۹ فضای سایبری را سلاحی راهبردی و فضایی عملیاتی با کارکرد ویژه و متناسب با نیازهای دفاعی ناموزون رژیم قلمداد کرد[3] و یا ارتش رژیم صهیونیستی (نیروهای دفاعی رژیم صهیونیستی) در سال ۲۰۱۲ اعلام کرد «رژیم آمادگی استفاده از سلاح‌های سایبری را دارد»[4]. البته ماهیت این سلاح‌ها و شرایط به‌کارگیری آن‌ها همچنان نامعلوم است.

1. National Cyber Security Strategy

۲. خلاصه راهبرد امنیت سایبری رژیم صهیونیستی، سپتامبر ۲۰۱۷، ص. ۵،
https://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf.

۳. رجوع شود به:
Amir Oren, 'Zeyret helheymh hhedshh shel tesh"l nemtesat bershetvet mheshebyem', Haaretz, 1 January 2010, http://www.haaretz.co.il/misc/1.1182490

۴. رجوع شود به:
Gili Cohen and Oded Yaron, 'Barak Acknowledges Israel's Cyber Offensive for First Time', Haaretz, 6 June 2012, https://www.haaretz.com/barack-acknowledges-israel-s-cyberoffensive-for-first-time-1.5170714.

اولین سند حاوی مبنای نظری سایبری ارتش رژیم صهیونیستی که در سال ۲۰۱۵ در اختیار عموم قرار گرفت، حق پاسخ راهبردی و عملیاتی به تهدیدهای احتمالی ازجمله استفاده از ظرفیت‌های سایبری را برای رژیم صهیونیستی محفوظ می‌دارد[۱]. در این سند بر نقش مهم دفاع سایبری در حفظ کارکردهای نهادهای دولت و نیروهای نظامی تاکید می‌شود[۲]. علاوه بر این، در سند فوق توانمندی‌های سایبری نیروهای مسلح به‌عنوان ابزاری مناسب جهت ارتقای توان اطلاعاتی، اجرای عملیات‌های شبکه‌ای در ائتلاف‌های جهانی، تاثیرگذاری بر شناخت دشمن و اطلاعات آن و کسب مشروعیت تلقی می‌شوند[۳]. در این سند سلاح‌های سایبری عامل تقویت توان بازدارندگی تاکتیکی و راهبردی ارتش رژیم صهیونیستی محسوب می‌شوند[۴].

حکمرانی، فرماندهی و نظارت

در ساختار حاکمیت رژیم صهیونیستی، مهم‌ترین تصمیمات و سیاست‌های فضای سایبری توسط نخست‌وزیر، وزرا و مقامات ارشد کابینه اتخاذ می‌شود که همگی باید به تایید پارلمان برسند. نظام مشورتی چندذینفعی متشکل از کسب‌وکارها، دانشگاه‌ها و گروه‌های شهروندی مکمل این ساختار حاکمیتی است که درباره مسائلی مانند سیاست‌های مربوط به صنعت فناوری اطلاعات و ارتباطات، تحقیق و توسعه و حریم

۱. رجوع شود به:
Graham Allison, 'Deterring Terror: How Israel Confronts the Next Generation of Threats - English Translation of the Official Strategy of the Israel Defense Forces', Special Report, Belfer Center for Science and International Affairs, Harvard Kennedy School, August 2016, https://www.belfercenter.org/sites/default/files/legacy/files/IDF%20doctrine%20translation%20-%20web%20final2.pdf.

۲. همان، ص. ۲۲.
۳. همان، ص. ۳۸.
۴. همان، ص. ۴۸.

خصوصی اطلاعات شخصی در سیستم‌های فناوری اطلاعات و ارتباطات به کابینه مشاوره می‌دهند. به‌طور کلی، استفاده از تجهیزات فنی با کیفیت بالا، تعهد جدی سازمان‌های ذی‌ربط در به‌کارگیری عملیات‌های سایبری و آگاهی رهبری سیاسی از ارزش توانمندی‌های سایبری به‌عنوان نقاط‌قوت فرماندهی سایبری رژیم صهیونیستی در نظر گرفته می‌شوند.

در سال ۲۰۱۰ همزمان با افزایش آگاهی مقامات ارشد از اهمیت فضای سایبری، رژیم صهیونیستی به این نتیجه رسید که سازمان امنیت رژیم صهیونیستی (شین‌بت)[1] دیگر نمی‌تواند تنها مرجع حفاظت از سیستم‌های اطلاعاتی در بخش خصوصی رژیم باشد و باید راه‌حلی تخصصی‌تر برای هماهنگ‌سازی اقدامات حوزه امنیت سایبری بیابد[2].

در همین راستا، نتانیاهو در آگوست ۲۰۱۱ اداره ملی سایبری (NCB)[3] را تحت‌نظارت خود بنیان گذاشت که وظیفه آن حفاظت از زیرساخت‌های حیاتی در برابر تهدیدهای سایبری کشورهای دیگر یا گروه‌های تروریستی است[4]. ظرف چند سال بعد، کابینه با پی‌بردن به ضرورت ایجاد نهادی مستقل و تخصصی جهت تامین امنیت سایبری، مرجع ملی امنیت سایبری (NCSA)[5] را تاسیس کرد[6] که در سال‌های بعد با انسجام بیشتر حکمرانی سایبری، این دو نهاد با هم ادغام شد و در سال ۲۰۱۸ اداره سایبری رژیم صهیونیستی

1. Israeli Security Agency (Shin Bet)

۲. رجوع شود به:

Government of Israel, 'Mesper hhelth 3270', 17 December 2017, https://www.gov.il/he/Departments/policies/dec_3270_2017.

3. National Cyber Bureau

۴. رجوع شود به:

Baram, 'The Effect of Cyberwar Technologies on Force Buildup: The Israeli Case', pp. 29-32.

5. National Cyber Security Authority

۶. مصوبه زیر بیانگر راهبرد دفاع سایبری عملیاتی رژیم صهیونیستی برای بخش غیرنظامی است که هماهنگی همه نهادهای ذی‌ربط را می‌طلبد و زمینه تاسیس مرجع امنیت سایبری را فراهم کرد.

Government of Israel, 'Resolution no. 2444', 15 February 2015, https://www.ictrp.org/wp-content/uploads/2019/02/GovernmentResolution-No-2444-Advancing-the-National-Preparednessfor-Cyber-Security.pdf.

با هدف حفظ امنیت سایبری رژیم صهیونیستی و تقویت پیشتازی آن در عرصه جهانی فضای سایبری تشکیل شد[۱]. این اداره فقط مسئولیت امنیت سایبری را برعهده دارد و اجرای عملیات سایبری تهاجمی خارج از اختیارات آن است. درواقع، عملیات سایبری تهاجمی از مسئولیت‌های سازمان‌های اطلاعات سایبری و نیروهای نظامی رژیم صهیونیستی محسوب می‌شود.

اساس قانونی و مقرراتی وظایف اداره سایبری رژیم صهیونیستی لایحه‌ای است[۲] که نتانیاهو در سال ۲۰۱۸ به تصویب پارلمان رساند. این قانون با واکنش‌های گسترده در بین جامعه و نهادهای دفاعی مواجه شد. زیرا بسیاری معتقد بودند این قانون اختیارات مطلقی به نخست‌وزیر در زمینه اجرای عملیات‌های سایبری می‌دهد که می‌تواند علیه مخالفان سیاسی از آن‌ها استفاده کند. انتقاد دیگری که به این قانون وارد می‌شود این است که امکان گردآوری و انتشار بدون محدودیت اطلاعات توسط اداره سایبری رژیم صهیونیستی را فراهم می‌آورد[۳].

طی فرایندهای اصلاح نظام امنیت سایبری در سال ۲۰۰۲، مرجع ملی امنیت اطلاعات (NISA)[۴] در سازمان شین‌بت ایجاد شد که وظیفه مشاوره، آموزش و هماهنگی فعالیت‌های نهادهای ذی‌ربط و شرکت‌های خصوصی کلیدی در امنیت سایبری رژیم

۱. رجوع شود به:
Yigal Unna, 'National Cyber Security in Israel', Cyber, Intelligence, and Security, vol. 3, no. 1, May 2019, p. 170, https://www.inss.org.il/publication/national-cyber-security-in-israel.

۲. رجوع شود به:
Amir Cahane, 'The New Israeli Cyber Draft Bill - A Preliminary Overview', The Federmann Cyber Security Research Center -Cyber Law Program, undated, https://csrcl.huji.ac.il/news/new-israeli-cyber-law-draft-bill

۳. رجوع شود به:
Yaniv Kubovich, 'Cyber Bill Would Give Netanyahu Unsupervised Powers, Experts Warn', Haaretz, 19 March 2019, https://www.haaretz.com/israel-news/.premium-cyber-billwould-give-israeli-prime-minister- unsupervised-powersexperts-warn-1.7040402?v=A1C59A1E1CE4E3490E38639FFA872186.

4. National Information Security Authority
(در زبان عبری به آن رِئِم Re'em می‌گویند)

صهیونیستی را عهده‌دار شد. درحقیقت، این نهاد بر اجرای سیاست‌های مختلف در حوزه امنیت و حفاظت اطلاعات نظارت می‌کند[1].

طبق اطلاعات موجود می‌توان گفت دو نهاد در ارتش رژیم صهیونیستی مسئولیت امور سایبری را برعهده دارند:

- ارتش در سال ۲۰۰۹ امور توانمندی‌های سایبری تهاجمی را به واحد ۸۲۰۰[2]، بزرگ‌ترین واحد اداره کل اطلاعات نظامی، محول کرد[3] و در سال ۲۰۱۱، یک گروه سایبری ویژه جهت ساخت و به‌کارگیری سلاح‌های سایبری تهاجمی ایجاد کرد. در سال ۲۰۱۲ همزمان با افزایش بودجه و کارکنان برنامه‌های سایبری نظامی نیز اداره توانمندی‌ها و عملیات‌ها در واحد ۸۲۰۰ تشکیل شد[4].
- واحد C4I[5] و اداره کل دفاع سایبری[6] در ستاد کل ارتش[7] نیز مسئولیت پشتیبانی فنی و فناورانه از عملیات‌های زمینی، دریایی و هوایی ارتش ازجمله ماموریت‌های دفاع سایبری را برعهده دارند[8].

---

۱. رجوع شود به:
Lior Tabansky, 'Critical infrastructure protection against cyber threats', Military and Strategic Affairs, vol. 3, no. 2, November 2011, pp. 72-3,
https://www.inss.org.il/wp-content/uploads/sites/2/systemfiles/(FILE)1326273687.pdf.

2. Unit8200

۳. اداره کل اطلاعات نظامی (Military Intelligence Directorate)؛ رجوع شود به:
https://www.idf.il/en/minisites/military-intelligence-directorate.

۴. اداره توانمندی‌ها و عملیات‌ها (Office of Capabilities and Operations)؛ رجوع شود به:
Yaacov Katz, 'Security and Defense: Israel's Cyber Ambiguity', Jerusalem Post, 31 May 2012,
http://www.jpost.com/Features/Front-Lines/Security-and-Defense-IsraelsCyber-Ambiguity;

and Matthew S. Cohen, Charles D. Freilich and Gabi Siboni, 'Israel and cyber space: Unique threat and response', International Studies Perspectives, vol.17, no. 3, August 2016, p. 8,
https://www.researchgate.net/publication/288823312_Israel_and_Cyberspace_Unique_Threat_and_Response.

۵. C4I ('command, control, communications, computers, and intelligence') به فرماندهی، کنترل، ارتباطات، رایانه و اطلاعات اشاره دارد.

6. Cyber Defense Directorate
7. General Staff

۸. ارتش رژیم صهیونیستی؛
'C4I and Cyber Defense Directorate',
https://www.idf.il/en/minisites/c4i-and-cyber-defense-directorate.

توانمندی‌های محوری در زمینه اطلاعات سایبری

نهاد اطلاعات رژیم صهیونیستی از سه سازمان کلیدی تشکیل شده‌است: اداره کل اطلاعات نظامی[1] که اغلب با نام عبری آن یعنی اَمان[2] شناخته می‌شود و بزرگ‌ترین نهاد بوده و مسئولیت بیشتر جنبه‌های زمینی، هوایی و دریایی و اطلاعات سیگنال‌ها را برعهده دارد؛ سازمان اطلاعات مخفی (موساد)[3] که عهده‌دار امور اطلاعات خارجی است و سازمان امنیت رژیم صهیونیستی (شین‌بت) که عملیات‌های اطلاعاتی داخلی شامل فلسطین اشغالی را اداره می‌کند[4]. باتوجه به روابط غیردوستانه رژیم صهیونیستی با همسایگانش می‌توان دریافت که صرف هزینه (سرانه) این رژیم در بخش اطلاعات بسیار بیشتر از کشورهای توسعه‌یافته است[5].

در دوره نخست‌وزیری نتانیاهو (۲۰۰۹ تاکنون) توسعه توانمندی‌های حوزه اطلاعات سایبری از اولویت‌های اصلی رژیم صهیونیستی بوده[6] که بیشتر توسط واحد ۸۲۰۰ امان انجام شده است[7]. واحد ۸۲۰۰ که حدود ۸۰ درصد از کارکنان امان را در اختیار دارد هم‌تراز سازمان امنیت ملی ایالات متحده (NSA) و ستاد ارتباطات دولت بریتانیا است و حوزه اختیارات آن شامل توانمندی‌های سایبری دفاعی، سایبری تهاجمی و اطلاعات سیگنالی

1. Military Intelligence Directorate
2. Aman
3. Secret Intelligence Service (Mossad)

۴. رجوع شود به:
Antonella Colonna Vilasi, 'The Israeli Intelligence Community', Sociology Mind, vol. 8, March 2018, pp. 114-22, https://www.scirp.org/pdf/SM_2018032915444002.pdf.

۵. رجوع شود به:
Richard Silverstein, 'Israeli Intelligence Budget Nearly Doubles in Past Decade Under Netanyahu', Tikun Olam, 5 May 2017,
https://www.richardsilverstein.com/2017/05/05/israeliintelligence-budget-nearly-doubles-past -decade-netanyahu

۶. رجوع شود به:
Kacy Zurkus, 'Netanyahu Boasts of Israel's Cyber Intelligence', Info Security, 26 June 2019,
https://www.infosecurity-magazine.com/news/netanyahu-boasts-of-israels-cyber-1

۷. اداره اطلاعات نظامی ارتش رژیم صهیونیستی

می‌شود[۱]. این واحد ساخت و به‌کارگیری بدافزار استاکس‌نت علیه برنامه هسته‌ای ایران در بازه ۲۰۰۸ تا ۲۰۱۰ را در کارنامه خود دارد[۲].

فشارهای ناشی از بهار عربی و تحولات سریع فناورانه موجب سازماندهی مجدد امان در اوایل دهه ۲۰۱۰ شد که در محافل داخلی رژیم صهیونیستی از آن به تحول از اطلاعات مبتنی بر سیگنال‌های رادیویی و تلویزیونی به‌سمت اطلاعات اینترنت‌محور یاد می‌شود[۲]. موساد و شین‌بت به‌طور گسترده از توانمندی‌های خود در زمینه اطلاعات سایبری و نیز واحد ۸۲۰۰ بهره‌برداری می‌کنند. به‌عنوان مثال، یوسی کوهن[۳] رئیس موساد در سال ۲۰۱۹ توانمندی‌های سایبری را ابزار اصلی مبارزه خواند[۴] و رئیس شین‌بت ناداف آرگامان[۵] نیز در سال ۲۰۱۷ اعلام کرد توانمندی‌های سایبری مانع از ۲۰۰۰ حمله به رژیم صهیونیستی شده‌اند[۶].

---

۱. رجوع شود به:
Sean Cordey, 'The Israeli Unit 8200: An OSINT-based study', Center for Security Studies, Cyber Defense Project, December 2019, p. 8,
https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-12-Unit-8200.pdf

۲. رجوع شود به:
Amir Mizroch, 'Rise of Computer Vision Brings Obscure Israeli Intelligence Unit Into Spotlight', Forbes, 28 May 2018,
https://www.forbes.com/sites/startupnationcentral/2018/05/28/rise-ofcomputer-vision-brings -obscure-israeli-intelligence-unit-intospotlight/#91acc643c193.

۲. رجوع شود به:
Amir Rapaport, 'Revolution in the Intelligence Agencies', Israel Defense, 19 April 2014,
https://www.israeldefense.co.il/en/content/revolution-intelligence-agencies.

3. Yossi Cohen

۴. رجوع شود به مقاله روزنامه جروزلم‌پست در تاریخ ۲۶ ژوئن ۲۰۱۹:
Jonah Jeremy Bob, 'Mossad chief Yossi Cohen: Cyber intel is main tool against terrorism', Jerusalem Post, 26 June 2019,
https://www.jpost.com/israel-news/mossad-chief-yossi-cohencyber-intel-is-main-tool-against-terrorism-593617.

5. Nadav Argaman

۶. رجوع شود به مقاله روزنامه تایمز رژیم صهیونیستی در تاریخ ۲۷ ژوئن ۲۰۱۷:
'Shin Bet head says over 2,000 terror attacks thwarted with cybertech', Times of Israel, 27 June 2017,
https://www.timesofisrael.com/shin-bet-head-says-over-2000-attacksthwarted-with-cybertech

نهادهای اطلاعاتی رژیم صهیونیستی رابطه مستقیمی با رشد بخش فناوری دیجیتال این رژیم دارند و این نهادها در شرکت‌های نوپای نوآور جهت توسعه توانمندی‌های حوزه اطلاعات سایبری مرز دانش سرمایه‌گذاری می‌کنند و به‌تبع آن، شرکت‌های نوپای رژیم صهیونیستی از موقعیت بالایی در بازار جهانی توانمندی‌های حوزه اطلاعات سایبری برخوردار هستند.

نهادهای اطلاعاتی رژیم صهیونیستی از نظر عملیات‌های جسورانه و موفق و رفتارهای موردانتقاد شهرت زیادی دارند. با این همه و با وجود برتری منطقه‌ای رژیم صهیونیستی در توانمندی‌های سایبری، سطح دسترسی جهانی آن قابل‌مقایسه با کشورهای پیشتاز نیست. به‌منظور جبران این کمبود، رژیم صهیونیستی دارای ائتلاف‌های نزدیکی با نهادهای اطلاعاتی ایالات متحده و بریتانیا و نیز مشارکت‌هایی با برخی کشورهای دیگر مانند فرانسه، سنگاپور و امارات است.

توانمندی و وابستگی سایبری

رژیم صهیونیستی با تکیه بر این منطق که سرمایه‌گذاری در منابع انسانی و صنعت ضامن حفظ کیفیت بالا در دفاع سایبری و برتری سایبری در منطقه است، موفق به ساخت زیست‌بوم سایبری منحصربه‌فردی متشکل از دولت، دانشگاه و صنعت در دهه اخیر شده‌است. یکی از ابتکارهای پیشگام در این حوزه شامل ابتکار عرصه نوآوری سایبراسپارک[1] در شهر بئرشبع (بئرشبا)[2] در جنوب رژیم صهیونیستی است. این ابتکار در سال ۲۰۱۴ به‌صورت سرمایه‌گذاری خطرپذیر مشترک توسط اداره ملی سایبری رژیم صهیونیستی، شهرداری بئرشبع، دانشگاه بن گورین[3] و شرکای صنعتی مانند

1. CyberSpark Innovation Arena
2. Be'er Sheva
3. Ben Gurion University

شرکت‌های ایی‌اِم‌سی-آراِس‌اِی[1]، لاکهیدمارتین، آی‌بی‌اِم، دویچ‌تله‌کام[2]، جِی‌وی‌پی سایبر لَبز[3] و اِلبیت سیستمز[4] راه‌اندازی شد. ابتکار مذکور به ایجاد زیست‌بومی چندذینفعی برای دولت، دانشگاه، صنعت، دولت محلی و جامعه مدنی جهت ساخت و آزمودن مفاهیم و ایده‌های جدید در حوزه امنیت سایبری منجر شده‌است[5].

نتایج مطالعه پیمایشی سالانه مجله سایبرکرایم[6] درباره ۵۰۰ شرکت برتر امنیت سایبری مؤید رقابت‌پذیری جهانی صنعت سایبری رژیم صهیونیستی است[7]. ۴۲ شرکت رژیم صهیونیستی در سال ۲۰۱۸ در فهرست این مجله قرار داشتند و این کشور پس از ایالات متحده (با ۳۵۴ شرکت) رتبه دوم را از آنِ خود کرد. لازم به ذکر است که بریتانیا با برخورداری از تنها نصف تعداد شرکت‌های رژیم صهیونیستی در جایگاه سوم این فهرست قرار دارد و چین نیز فقط دارای شش نماینده در این فهرست است. به‌همین‌ترتیب، رژیم صهیونیستی در سال ۲۰۲۰ در جایگاه دوم در فهرست ۱۵۰ شرکت نوظهور امنیت سایبری این مجله قرار گرفت[8]. این رژیم همچنین در سال ۲۰۲۰

1. EMC-RSA
2. Deutsche Telekom
3. JVP Cyber Labs
4. Elbit systems

۵. رجوع شود به:
Deborah Housen-Couriel, 'National Cyber Security Organization: Israel', NATO Cooperative Cyber Defense Centre of Excellence, 2017, pp. 14-15,
https://ccdcoe.org/uploads/2018/10/IL_NCSO_final.pdf.

6. Cybercrime Magazine

۷. رجوع شود به:
Steve Morgan, 'Cybersecurity 500 by the Numbers: Breakdown by Region', Cybercrime Magazine, 21 May 2018,
https://cybersecurityventures.com/cybersecurity-500-by-the-numbersbreakdown-by-region.

۸. در سال ۲۰۲۰ ایالات متحده ۹۵ شرکت، رژیم صهیونیستی ۱۶ شرکت، بریتانیا ۸ شرکت و روسیه ۱ شرکت در فهرست ۱۵۰ شرکت برتر امنیت سایبری داشتند (چین هیچ شرکتی نداشت). رجوع شود به:
Steve Morgan, 'Hot 150 Cybersecurity Companies to Watch in 2021', Cybercrime Magazine, 5 January 2021,
https://cybersecurityventures.com/cybersecurity-companies-listhot-150.

توانست ۳۷ درصد سرمایه‌گذاری خطرپذیر جهانی در شرکت‌های امنیت سایبری را به خود جذب کند[۱].

یکی از ویژگی‌های بارز صنعت امنیت سایبری رژیم صهیونیستی، رابطه نزدیک آن با واحد ۸۲۰۰ ارتش است. در این واحد یک بخش فناوری به‌نام واحد ۸۱ وجود دارد که به‌طور اختصاصی به تحقیق و توسعه درون‌سازمانی در زمینه فناوری‌های مرز دانش می‌پردازد[۲]. بسیاری از افرادی که در شرکت‌های نوپای حوزه امنیت سایبری رژیم صهیونیستی فعالیت می‌کنند (به‌عنوان مثال، بنیان‌گذاران شبکه‌های پائولوآلتو، اِن‌اِس‌اُ و چِکرپوینت)[۳] از کارکنان سابق واحد ۸۲۰۰ هستند. همکاری نزدیک بین ارتش و بخش خصوصی رژیم صهیونیستی برای هر دو طرف مزیت محسوب می‌شود، زیرا فناوری‌های سایبری جدید در شرایط جنگی واقعی آزمایش می‌شوند و درنتیجه، کارایی و مقیاس‌پذیری آن‌ها قبل از عرضه به بازار جهانی به‌خوبی سنجیده می‌شود[۴].

طبق گزارش مرجع نوآوری رژیم صهیونیستی (۲۰۱۹)[۵]، بخش فناوری ۹/۲ درصد از بازار اشتغال این رژیم را دربرمی‌گیرد و میانگین حقوق در این بخش تقریبا دوبرابر میانگین ملی است. البته نتایج همین گزارش نشان می‌دهد که نرخ تاسیس مراکز تحقیق و

۱. اداره ملی سایبری رژیم صهیونیستی؛
'The Israeli cyber industry continues to grow: Record fundraising in 2020', 21 January 2021, https://www.gov.il/en/departments/news/2020ind

۲. رجوع شود به:
Sophie Shulman, 'Unit 81: The elite military unit that caused a big bang in the Israeli tech scene', CTech, 8 January 2021,
https://www.calcalistech.com/ctech/articles/0,7340,L-3886512,00.html
3. Palo Alto Networks, NSO and Checkpoint

۴. رجوع شود به:
Thomas McMullan, 'Israel's Silent Cyberpower Is Reshaping the Middle East', OneZero, 16 April 2019, https://onezero.medium.com/israels-silent-cyberpower-is-reshaping-themiddle-east-af1458d16a15
5. Israel Innovation Authority

توسعه توسط شرکت‌های چندملیتی در رژیم صهیونیستی روبه‌کاهش است[۱].

رژیم صهیونیستی از معدود مواردی است که امنیت سایبری را در سطح دبیرستان نیز آموزش می‌دهد[۲] و ارتش افسرانی را برای استخدام استعدادهای جدید به دبیرستان‌ها اعزام می‌کند[۳]. برنامه ماگشیمیم[۴] یکی از مهم‌ترین دوره‌های آموزشی در رژیم صهیونیستی است که برای جوانان مستعد در مناطق کمتربرخوردار پس از اتمام دبیرستان، دوره‌های آموزشی در حوزه رمزنگاری و هک برگزار می‌کند و اغلب فارغ‌التحصیلان این دوره‌ها را در واحدهای اطلاعات و سایبری ارتش به‌کار می‌گیرد[۵].

رژیم صهیونیستی از نظر تحقیقات هوش مصنوعی نیز در جایگاه خوبی قرار دارد. به‌عنوان مثال، این رژیم در سال ۲۰۲۰ جایگاه دهم را در بین ۵۰ رتبه برتر دارای بیشترین انتشارات در دو کنفرانس برتر هوش مصنوعی به خود اختصاص داد[۶]. ارتش رژیم

---

۱. اصل و خلاصه گزارش به‌ترتیب در منابع زیر یافت می‌شود:
High-Tech Human Capital Report 2019', Start-Up Nation Central, Israel Innovation Authority, February 2019, http://mlp.startupnationcentral.org/rs/663-SRH-472/images/Start-Up%20Nation%20Centrals%20High%20Tech%20Human%20Capital%20Report%202019.pdf.

Lilach Baumer, 'Israel's Tech Sector Grows, but Demand Still Outstrips Supply, Says Report', Calcalist, 26 February 2019,
https://www.calcalistech.com/ctech/articles/0,7340,L-3796731,00.html.

۲. رجوع شود به:
Gil Press, '6 Reasons Israel Became A Cybersecurity Powerhouse Leading the $82 Billion Industry', Forbes, 18 July 2017,
https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israelbecame-a-cybersecurity-powerhouse-leading-the-82-billionindustry/#29c1c94b420a

۳. رجوع شود به:
Cordey, 'The Israeli Unit 8200: An OSINT-based study', pp. 3, 12.

4. Magshimim

۵. رجوع شود به:
Daniel Estrin, 'In Israel, teaching kids cyber skills is a national mission', Times of Israel, 4 February 2017, https://www.timesofisrael.com/in-israel-teaching-kids-cyber-skills-is-anational-mission.

۶. رجوع شود به:
Gleb Chuvpilo, 'AI Research Rankings 2020: Can the United States Stay Ahead of China?', 21 December 2020, https://chuvpilo.medium.com/ai-research-rankings-2020-can-the-united-statesstay-ahead-of-china-61cf14b1216

صهیونیستی به‌طور گسترده از سلاح‌های خودکار مانند هارپی[1] (نوعی سلاح با قابلیت حرکت) و خودروهای نظامی کاملا خودکار (بدون سرنشین و ناوبر) استفاده می‌کند. در این کشور محیط کسب‌وکار شرکت‌های نوپای فعال در زمینه هوش مصنوعی بسیار شکوفاست و در آوریل ۲۰۲۰ بالغ بر ۱۱۵۰ شرکت نوپای فعال در این حوزه گزارش شده‌است[2]. شرکت‌های رژیم صهیونیستی از مزیت رقابتی بالایی در خدمات هوش مصنوعی حوزه رباتیک و خودکارسازی برخوردار هستند[3]. مرجع نوآوری رژیم صهیونیستی در پایان سال ۲۰۲۰ برنامه پنج‌ساله هوش مصنوعی با بودجه‌ای معادل ۵ میلیارد شِکل جدید[4] (برابر با ۱/۵۵ میلیارد دلار آمریکا) را معرفی کرد[5]. با آنکه بودجه این برنامه به دلایل سیاسی و مالی احتمالا کاهش می‌یابد[6]، اما پروژه‌های آغازین آن در حوزه‌های کلیدی و با اولویت بالا مانند ساخت یک ابرکامپیوتر، تقویت تحقیق و توسعه به‌ویژه در حوزه برنامه‌نویسی عصبی زبانی[7]، توسعه منابع انسانی و تامین تجهیزات پیشرفته برای دانشگاه‌های رژیم صهیونیستی متمرکز هستند که می‌تواند موجب تحول جدی در بخش هوش مصنوعی این کشور شود.

1. Harpy

۲. رجوع شود به:
Kyle Wiggers, 'Israel Risks Falling Behind in AI Despite Growth', VentureBeat, 17 February 2020, https://venturebeat.com/2020/02/17/israel-risks-falling-behind-in-ai-despite-growth

۳. مرکز تحقیقات مشترک کمیسیون اروپا؛
'AI Watch: TES Analysis of AI Worldwide Ecosystem in 2009-2018', JRC Technical Reports, 2020, p. 29, https://data.europa.eu/doi/10.2760/85212.

4. New Shekel

۵. رجوع شود به:
Israel Launches National AI Plan at Cost of 1.63 Bln USD', Xinhuanet, 23 December 2020, http://www.xinhuanet.com/english/2020-12/23/c_139613874.htm.

۶. رجوع شود به:
Meir Orbach, 'Israel Launches National AI Program, but Lack of Budget Threatens Its Implementation', CTECH,22 December 2020, https://www.calcalistech.com/ctech/articles/0,7340,L-3883355,00.html.

7. Neuro linguistic programming

امنیت و تاب‌آوری سایبری

رژیم صهیونیستی در ژانویه ۲۰۲۰ اعلام کرد در ۱۲ ماه گذشته هیچ حمله سایبری موفقی به زیرساخت‌های حیاتی آن انجام نشده‌است[۱]، اما نرخ اقدامات ایران برای حمله سایبری به این رژیم افزایش داشته‌است. به‌عنوان مثال، در آوریل ۲۰۲۰ حمله سایبری ناموفقی از سوی ایران به تاسیسات تصفیه آب رژیم صهیونیستی گزارش شد که حمله تلافی‌جویانه رژیم صهیونیستی به تاسیسات زیرساختی یکی از بندرهای ایران را در پی داشت[۲]. به‌دنبال اقدامات ایران، رئیس اداره سایبری رژیم صهیونیستی درباره احتمال فرارسیدن «زمستان سایبری»-کنایه از افزایش حملات به رژیم و بدترشدن تهدیدها- هشدار داد[۳]. انجمن تولیدکنندگان رژیم صهیونیستی[۴] نیز در سال ۲۰۲۱ اعلام کرد شناخت و مقابله با حمله‌های سایبری مستلزم اقدامات گسترده‌ای است و از این رو قصد دارد یک ستاد امنیت سایبری[۵] مشابه مرکز ملی امنیت سایبری بریتانیا تاسیس کند تا امکان پشتیبانی متقابل را برای اعضای انجمن فراهم کند[۶].

۱. اداره سایبری رژیم صهیونیستی؛
'Zero Successful Cyber Attacks on Critical National Infrastructures', 29 January 2020, https://www.gov.il/en/departments/news/cybertech2020.

۲. اداره سایبری رژیم صهیونیستی؛
'The Israel National Cyber Directorate: Iran is a main cyber threat on [sic] the Middle East', 29 June 2019, https://www.gov.il/en/departments/news/unna_cyber_week_2019

۳. رجوع شود به مقاله روزنامه تایمز رژیم صهیونیستی در تاریخ 28 می 2020:
"Cyber winter is coming," warns Israel cyber chief after attack on water systems', Times of Israel, 28 May 2020,
https://www.timesofisrael.com/israeli-cyber-chief-attack-on-water-systems-achanging-point-in-cyber-warfare.

4. Manufactures Association of Israel

5. Cyber Security Headquarters

۶. رجوع شود به:
Naveen Goud, 'Israel to Build a Cybersecurity Headquarters Serving Manufacturers', Cybersecurity Insiders, 7 January 2021,
https://www.cybersecurity-insiders.com/israel-to-build-acybersecurity-headquarters-serving -manufacturers/.

رژیم صهیونیستی به دلایل متعدد (ازجمله موقعیت ژئوپلیتیک، دلایل ایدئولوژیک، برخورداری از محیط تحقیق و توسعه غنی در زمینه فناوری اطلاعات و ارتباطات و ایفای نقش کلیدی در صادرات تسلیحات نظامی) همواره هدف حملات سایبری دیگر کشورها قرار می‌گیرد. با این حال، این کشور با برخورداری از بخش‌های داخلی پویا و چابک از وضعیت مناسبی در امنیت سایبری برخوردار است، هرچند در کمال شگفتی در شاخص جهانی امنیت سایبری (۲۰۱۸) در جایگاه سی‌ونهم از بین ۱۷۵ کشور قرار گرفت[۱].

وظایف اداره سایبری رژیم صهیونیستی همه جنبه‌های دفاع سایبری در حوزه غیرنظامی از تدوین سیاست‌ها و ساخت قدرت فناورانه تا دفاع عملیاتی در فضای سایبری را پوشش می‌دهد. اداره سایبری رژیم صهیونیستی با ارائه خدمات مشاوره و مدیریت حوادث به شرکت‌های غیرنظامی به‌ویژه شرکت‌های حوزه زیرساخت‌های ملی تلاش می‌کند تاب‌آوری فضای سایبری غیرنظامی را ارتقا بخشد[۲]. اداره مذکور به شرکت‌های خصوصی و مدیران زیرساخت‌های حیاتی در زمینه به‌کارگیری و راه‌اندازی بسترهای فناورانه جدید مشاوره می‌دهد و به آن‌ها در کسب دانش موردنیاز برای حفاظت از سیستم‌ها در برابر حمله‌های سایبری کمک می‌کند. سیستمی به نام شوکیس[۳] که در سال ۲۰۱۹ راه‌اندازی شده‌است، ارتباط شرکت‌های بخش خصوصی را با اداره سایبری برقرار می‌کند تا تصویری واقعی و جامع از سطح خطرات سایبری که با آن مواجه هستند را در اختیار داشته

۱. رجوع شود به:
International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 64, https://www.itu.int/dms_pub/itu-d/opb/str/DSTR-GCI.01-2018-PDF-E.pdf

۲. اداره ملی سایبری رژیم صهیونیستی؛
http://www.gov.il/en/departments/israel_national_cyber_directorate

3. Showcase

باشند. بدین‌ترتیب، اداره سایبری رژیم صهیونیستی می‌تواند با ادغام توانمندی‌ها و دانش نهادهای دولتی و بخش خصوصی معیارهای مناسبی برای طبقه‌بندی/درجه‌بندی خطرهای سایبری تهیه کند[۱].

علاوه براین، اداره سایبری به‌طور مرتب توصیه‌های لازم برای ایمن‌سازی اطلاعات و کاهش خطرات سایبری را در اختیار شرکت‌های خصوصی و شهروندان قرار می‌دهد. به‌عنوان مثال، اداره سایبری سه ابتکار در نوامبر ۲۰۱۸ راه‌اندازی کرد: اولین برنامه ملی پاسخ سایبری[۲]، راهنمای کسب‌وکارها در تشکیل گروه‌های پاسخ به بحران جهت آمادگی در برابر حوادث سایبری[۳] و یک مانور سایبری به نام دایره جادویی ۲ [۴] جهت آزمودن میزان کارایی همکاری این نهاد با بخش خصوصی. اداره سایبری در سال ۲۰۲۰ نیز دو راهنما درباره «کاهش خطرات سایبری برای سیستم‌های کنترل صنعتی»[۵] و «توصیه‌های مربوط به استفاده ایمن از زوم»[۶] را منتشر کرد.

---

۱. رجوع شود به:
Uri Berkowitz, 'Hesvet hemdeynh: hekyerv at hem'erekt shetkeyn at hhebrh shelkem lemteqpet Bhesyeyber hebah', Globes, 5 May 2019,
http://www.globes.co.il/news/article.aspx?did=1001284397

۲. اداره سایبری رژیم صهیونیستی؛
'National Cyber Concept for Crisis Preparedness and Management', 6 November 2018,
https://www.gov.il/BlobFolder/news/cybercrisispreparedness/en/Management%20of%20crisis%20situations%20english%20final.pdf.

۳. رجوع شود به:
Israel National Cyber Directorate, 'Organizational Preparedness for a Cyber Crisis: Characterization & Requirements from Crisis Management Team and IR Team', 8 November 2019,
https://www.gov.il/BlobFolder/news/cybercrisisforir/en/Cyber%20crisis_575941_eng%20final%2028.11.pdf

4. Magic Circle 2

5. Reducing Cyber Risks for Industrial Control Systems (Israel National Cyber Directorate, 'Guidelines on Protecting Industrial Control Systems', 13 May 2020,
https://www.gov.il/en/departments/general/icssolutions)

6. Recommendations on Using Zoom Safely ('Recommendations on Using Zoom Safely', 5 May 2020, https://www.gov.il/en/departments/general/zoom)

گروه پاسخ سایبری فوری[1] از دیگر عناصر مهم عملیات‌های دفاع سایبری رژیم صهیونیستی است که مسئولیت برقراری نظام گزارش‌دهی بیست‌وچهارساعته در سراسر کشور بین شرکت‌ها (خصوصی یا دولتی) و اداره سایبری را برعهده دارد[2] و اعضای آن از کارکنان سابق واحدهای سایبری ارتش رژیم صهیونیستی هستند.

رهبری جهانی در عرصه سایبری

رژیم صهیونیستی برای آنکه بتواند به حلقه کشورهای قدرتمند سایبری بپیوندد، در حال افزایش دامنه و عمق همکاری خود با شماری از کشورهاست. در همین راستا، رژیم صهیونیستی به رایزنی با کشورهای هم‌پیمان جهت انعقاد قراردادهای دوطرفه و چندطرفه، برقراری روابط نزدیک‌تر با سازمان‌های بین‌المللی و حفظ ارتباط خود با شرکت‌های چندملیتی روی آورده‌است. مشارکت رژیم صهیونیستی در تهیه هنجارهای داوطلبانه فضای سایبری توسط گروه کارشناسان دولتی سازمان ملل[3] بهترین نمونه از فعالیت‌های قدرتمند آن در عرصه همکاری‌های بین‌المللی است که به‌طور مرتب در اجلاس‌های بین‌المللی مربوط به آن شرکت می‌کند[4]. به‌علاوه، رژیم صهیونیستی تاکنون توانسته‌است چندین توافق دوجانبه در زمینه همکاری سایبری منعقد کند

1. Cyber Emergency Response Team

‘Cyber Emergency Response Team’,
https://www.gov.il/en/departments/news/119en

۲. اداره ملی سایبری رژیم صهیونیستی؛

۳. رجوع شود به:
UN Office for Disarmament Affairs, ‘Developments in the field of information and telecommunications in the context of international security’,
https://www.un.org/disarmament/ict-security.

۴. به‌عنوان نمونه به متن سخنرانی دادستان کل رُی شوندورف مراجعه شود:
General Roy Schöndorf, ‘Israel’s perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations’, 8 December 2020,
https://www.ejiltalk.org/israelsperspective-on-key-legal-and-practical-issues-concerning-theapplication-of-international-law-to-cyber-operations/.

که به‌عنوان نمونه می‌توان به قرارداد با هند و ژاپن در سال ۲۰۱۸[۱]؛ با کرواسی و رومانی و استرالیا در سال ۲۰۱۹[۲] و با یونان[۳] و مجددا با هند در سال ۲۰۲۰[۴] اشاره کرد.

همکاری با سازمان‌های خصوصی در زمینه اشتراک‌گذاری دانش یکی دیگر از جنبه‌های مهم همکاری‌های بین‌المللی رژیم صهیونیستی در حوزه سایبری است. به‌عنوان مثال، اداره سایبری رژیم صهیونیستی به‌همراه وزارت اقتصاد و صنعت[۵]، دانشگاه عبری اورشلیم[۶] و بانک توسعه داخلی آمریکا[۷] در سال ۲۰۱۸ کارگاه آموزشی دوهفته‌ای برای متخصصان سایبری و نمایندگانی از ۲۲ کشور آمریکای لاتین برگزار

---

۱. رجوع شود به:
Israel National Cyber Directorate, 'Lerashevnh, heskem shet'p lheylevpey meyd' vesheytevpey mev'p bethevm hesyeyber beyn yesheral veypen', 28 November 2018, http://www.gov.il/he/departments/news/cooperationjapan;

Israel National Cyber Directorate, 'Rash memshelt yesheral, benyemyen netneyhev verash memshelt hevdev nernedrh mevdey, nepgeshev heyvem bem'even hayervh hershemy shel memshelt hevdev, vhetmev 'el shevret heskemyem beyn hemdeynevt', 15 January 2018, www.gov.il/he/departments/news/india.

۲. رجوع شود به:
Israel National Cyber Directorate, 'Heskem hebnevt lesheytevp p'evelh bethevm hegnet hesyeyber beyn yesheral leqrevateyh', 12 September 2019, www.gov.il/he/departments/news/cybercroatia;

Israel National Cyber Directorate, 'Heskem hebnevt lesheytevp p'evelh bethevm hegnet hesyeyber beyn yesheral lervemneyh', 6 June 2019, www.gov.il/he/departments/news/israel_rumania;

Israel National Cyber Directorate, 'Australian-Israeli cooperation in the field of cyber', 29 January 2019, http://www.gov.il/he/departments/news/agree_australia.

۳. اداره ملی سایبری رژیم صهیونیستی؛
'Joint statement on cybersecurity signed between Greece and Israel', 16 June 2020, https://www.gov.il/en/departments/news/greece

۴. این توافق جدید با هند مشتمل بر گسترش حوزه‌های همکاری مورد تاکید در توافق ۲۰۱۸ است. رجوع شود به:
'India and Israel Sign Agreement to Expand Cooperation in Cyber Security', RepublicWorld.com, 16 July 2020, https://www.republicworld.com/india-news/general-news/india-and-israelsign-agreement-to-expand-cooperation-in-cyber-security.html.

5. Ministry of Economy and Industry
6. Hebrew University of Jerusalem
7. Inter-American Development Bank

کردند[۱]. اداره سایبری رژیم صهیونیستی به‌همراه وزارت اقتصاد و صنعت و موسسه صادرات[۲] در نوامبر همین سال نیز سمینار لبه سایبری ۲[۳] را برای مسئولان ارشد امنیت اطلاعات شرکت‌های بزرگ از ۱۴ کشور مختلف برگزار کردند[۴]. رویداد بین‌المللی سایبرتک[۵] (شبیه نمایشگاه) برای بخش خصوصی در سال ۲۰۲۰ نیز توانست ۱۸ هزار شرکت‌کننده ازجمله نمایندگانی از ۲۰۰ شرکت را به خود جلب کند[۶].

علاوه بر اداره سایبری، نهادهای دیگر رژیم صهیونیستی مانند واحد C4I و اداره کل دفاع سایبری ارتش نیز در همکاری‌های سایبری بین‌المللی مشارکت فعال دارند. به‌عنوان مثال، ارتش رژیم صهیونیستی با همکاری ستاد فرماندهی سایبری ایالات متحده در نوامبر ۲۰۱۹ چهارمین رزمایش گنبد سایبری[۷] خود را برگزار کرد. این رزمایش تنها بخش کوچکی از همکاری‌های سایبری دو کشور به‌شمار می‌رود. گروه رژیم صهیونیستی حاضر در این رزمایش تحت امر فرمانده تیپ دفاع سایبری[۸] بود و نمایندگانی از امان، نیروی هوایی، نیروی دریایی و نیروی زمینی رژیم صهیونیستی را شامل می‌شد[۹].

---

۱. اداره ملی سایبری رژیم صهیونیستی؛
'Shet'p bethevm hegnet hesyeyber beyn yesheral lemdeynevt ameryeqh helteyneyt vheqareybeyyem', 28 March 2018,
http://www.gov.il/he/departments/news/iadb
2. Export Institute
3. Cyber Edge 2.0

۴. اداره ملی سایبری رژیم صهیونیستی؛
Semyenr beynelavemy pevrets derk lentesyegy hebrevt vemmeshelvet memdeynevt yedyedvetyevt', 18 November 2018,
http://www.gov.il/he/departments/news/cyberedge.
5. Cyber Tech

۶. رجوع شود به:
Jean-Christophe Noël, 'Israeli Cyberpower: The Unfinished Development of the Start-up Nation', French Institute of International Relations, November 2020, p. 21, https://www.ifri.org/sites/default/files/atoms/files/noel_israeli_cyberpower_2020.pdf.
7. Cyber Dome
8. Cyber Defense Brigade

۹. رجوع شود به:
'Israel, US Conclude Joint Cyber Defense Exercise', Israel Defense, 10 November 2019, http://www.israeldefense.co.il/en/node/40871.

موارد فوق بیانگر این هستند که رژیم صهیونیستی در همکاری‌های بین‌المللی خود بر پیشرفت و توسعه در زمینه موضوعات کلیدی سایبری برای دو طرف تاکید زیادی دارد تا بدین‌ترتیب بتواند هدف مبنی بر تبدیل کشور به قدرت سایبری جهانی را تحقق بخشد.

توانمندی‌های سایبری تهاجمی

همانطور که رژیم صهیونیستی تاکنون به‌طور رسمی اطلاعاتی درباره توانمندی‌های خود در زمینه اطلاعات سایبری منتشر نکرده‌است، هیچ‌گونه جزئیاتی نیز درباره ساخت یا به‌کارگیری توانمندی‌های سایبری تهاجمی در دسترس عموم قرار نداده‌است. با این حال، از برخی اظهارات مقامات رژیم صهیونیستی می‌توان به توانمندی‌های سایبری و رویکرد این رژیم در به‌کارگیری آن‌ها پی برد. به‌عنوان مثال، وزیر دفاع سابق رژیم صهیونیستی ایهود باراک[1] در ژوئن ۲۰۱۲ برای اولین بار در اظهاراتی رسمی بر توانایی این رژیم برای انجام حمله سایبری صحه گذاشت و اگرچه او سرمایه‌گذاری در توانمندی‌های دفاعی را مهم‌تر از توانمندی‌های تهاجمی برشمرد، اما اذعان داشت که رژیم صهیونیستی در هر دو حوزه فعالیت دارد[2].

توانمندی‌های سایبری تهاجمی رژیم صهیونیستی از سال ۲۰۱۰ با افشای به‌کارگیری بدافزار استاکس‌نت تا حدی در معرض دید قرار گرفت. گزارش‌های موجود نشان می‌دهند استاکس‌نت با همکاری ایالات متحده (سازمان امنیت ملی) و رژیم

1. Ehud Barak

۲. رجوع شود به:
Gili Cohen and Oded Yaron, 'Sher hebyethevn hevdh lerashevnh bep'eyelvet seyyebr hetqepyet shel yesheral', Haaretz, 6 June 2012,
http://www.haaretz.co.il/news/politics/1.1725069.

صهیونیستی (واحد ۸۲۰۰) برای هدف گرفتن سامانه‌های نظارت، کنترل و جمع‌آوری داده (اسکادا)[1] سانتریفیوژهای غنی‌سازی اورانیوم ایران طراحی شده‌بود[2]. از آن پس، واحد ۸۲۰۰ بارها اقدام به ساخت و به‌کارگیری توانمندی‌های سایبری تهاجمی جهت تخریب زیرساخت‌های حیاتی ملی دشمنان بالقوه به‌ویژه ایران کرده‌است[3]. به‌عنوان مثال، شواهد موجود نشان می‌دهند بدافزار فلِیم[4] که در سال ۲۰۱۲ علیه ایران به‌کار رفت حاصل همکاری واحد ۸۲۰۰ و ایالات متحده بوده‌است[5]. در سال ۲۰۲۰ نیز به‌نقل از منابع غیررسمی اعضای این واحد برای اجرای حمله به تاسیسات زیرساختی یکی از بندرهای ایران به تلافی اقدامات ایران به تاسیسات تصفیه آب رژیم صهیونیستی نشان افتخار دریافت کردند[6]. شایان ذکر است که طبق اظهارات یکی از مقامات رسمی رژیم صهیونیستی این حمله تنها یکی از چندین حمله سایبری رژیم صهیونیستی بوده‌است[7].

درمجموع، رژیم صهیونیستی ازطریق گسترش همکاری‌های بین‌المللی خود به‌ویژه با ایالات متحده توانسته‌است در حوزه توانمندی‌های سایبری تهاجمی نیز دستاوردهای چشمگیری هم‌تراز با پیشرفت‌های قابل‌توجه خود در زمینه توانمندی‌های اطلاعات سایبری کسب کند.

---

1. Supervisory Control and Data Acquisition Systems

۲. رجوع شود به:
David E. Sanger, The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age (New York: Broadway Books, 2018), p. 25.

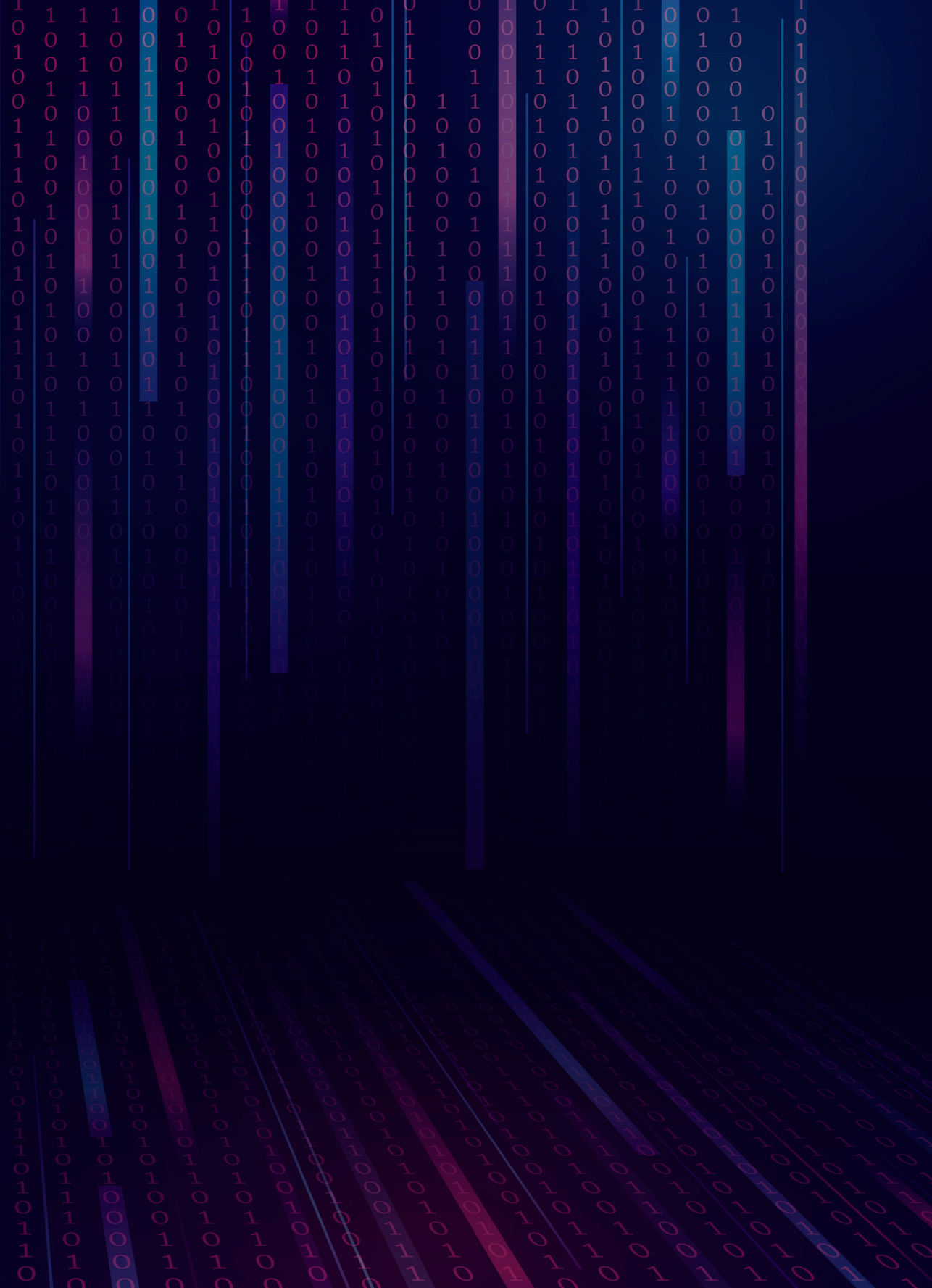
۳. رجوع شود به:
Cohen, Freilich and Siboni, 'Israel and cyber space: Unique threat and response', p. 8.

4. Flame

۵. رجوع شود به:
Tabansky and Israel, Cybersecurity in Israel, pp. 66-7.

۶. رجوع شود به مقاله روزنامه تایمز رژیم صهیونیستی در تاریخ ۲۵ ژوئن ۲۰۲۰:
'IDF's cyber warrior 8200 intelligence unit gets medal for "recent operations"', Times of Israel, 25 June 2020,
https://www.timesofisrael.com/idfs-cyber-warrior-8200-intelligence-unitgets-medal-for-recent-operations.

۷. همان



۷

ژاپن

با آنکه ژاپن از اوایل دهه هشتاد یکی از پیشگامان عرصه کاربردهای تجاری فناوری‌های اطلاعات و ارتباطات به‌شمار می‌رود، اما سابقه چندانی از نظر آمادگی برای تامین امنیت فضای سایبری ندارد. درواقع، اولین راهبرد امنیت سایبری نسبتا کامل ژاپن در سال ۲۰۱۳ براساس سیاست کلی امنیت کشور ارائه شد که بیشتر شامل اصول مفاهیم کلاسیک امنیت اطلاعات بود. امروزه رویکرد ژاپن نسبت به حکمرانی فضای سایبری به‌روزتر شده‌است، هرچند هنوز هم به سطح کشورهایی مانند ایالات متحده و بریتانیا به‌ویژه از منظر اشتراک‌گذاری اطلاعات با بخش خصوصی نرسیده‌است. با توجه به این‌که بسیاری از شرکت‌های ژاپنی تمایل چندانی به پرداخت هزینه‌های امنیت سایبری ندارند، راهکارهای دفاعی ژاپن از قدرت و کارایی بالایی برخوردار نیستند. می‌توان چنین گفت که ژاپن در دهه‌های گذشته برنامه‌ریزی‌های محدودی در زمینه تاب‌آوری داشته‌است، ولی در جریان بازی‌های المپیک و پارالمپیک ۲۰۲۰ تا حدی شتاب برنامه‌های تاب‌آوری آن بیشتر شد که با شیوع کوید-۱۹ بار دیگر این موضوع به حاشیه رفت. درنتیجه، این کشور هنوز هیچ راهبرد رسمی یا مبنای نظری رسمی در زمینه توانمندی‌های سایبری نظامی ندارد. البته ژاپن تغییرات سازمانی اندکی در نیروهای مسلح خود ایجاد کرده‌است که به‌عنوان نمونه می‌توان به تشکیل واحدهای تخصصی سایبری در نیروهای مسلح آن اشاره کرد. درحقیقت، محدودیت‌های قانونی و سیاسی ژاپن در زمینه استفاده از نیروهای نظامی مانع از توسعه توانمندی‌های سایبری تهاجمی آن شده‌اند. البته از سال ۲۰۲۰ همزمان با تشویق ایالات متحده و استرالیا و افزایش نگرانی‌های ژاپن نسبت به تهدیدهای چین و کره شمالی، این کشور با انگیزه بیشتری به تقویت توانمندی‌های سایبری خود می‌پردازد.

راهبرد و مبنای نظری (دکترین)

همان‌طور که از عنوان سند «اولین راهبرد ملی امنیت اطلاعات» ژاپن پیداست، این سند اولین راهبرد امنیت سایبری این کشور در نوع خود است[۱] که در سال ۲۰۰۶ منتشر شد (در آن زمان بیشتر کشورها اصطلاح امنیت اطلاعات را به امنیت سایبری ترجیح می‌دادند). البته این راهبرد صرفا روی جنبه‌های فنی امنیت سایبری که از اواسط دهه نود اهمیت پیدا کرده‌بود، تمرکز داشت و تغییر چندانی در سیاست‌های ژاپن ایجاد نکرد. به‌دنبال این راهبرد، سندهای سیاستی دیگری نیز در ژاپن تدوین شد. به‌عنوان مثال، راهبرد ۲۰۱۳ که برای اولین بار با نام «راهبرد امنیت سایبری» انتشار یافت، نقطه‌عطفی در تاریخ امنیت سایبری ژاپن محسوب می‌شود و حاصل اقداماتی است که سال قبل از انتشار آن انجام شده‌بود[۲]. در مقایسه با سندهای قبلی، این راهبرد تاکید جدی‌تری بر امنیت ملی و فضای سایبری به‌عنوان محیط عملیاتی برای سیاست، اقتصاد، دیپلماسی و تاثیرگذاری جهانی دارد و اولین سند دولت ژاپن محسوب می‌شود که وزارت دفاع را به مقابله با حمله‌های سایبری راهبردی دیگر دولت‌ها ملزم می‌کند. این سند فضای سایبری را صحنه جدید نبرد می‌داند و تشکیل اولین واحد دفاع سایبری در نیروهای دفاع از خود ژاپن (JSDF)[۳] (که از این پس ارتش نامیده می‌شود) و هماهنگی بیشتر بین نهادهای نظامی و غیرنظامی در دفاع سایبری را پیشنهاد می‌دهد. علاوه بر این، در این راهبرد بر اهمیت هنجارهای فضای سایبری و ضرورت داشتن رویکردی چندذینفعی در

۱. شورای امنیت اطلاعات، رجوع شود به:
The First National Strategy on Information Security: Toward the Realisation of a Trustworthy Society, 2 February 2006,
http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf

۲. شورای امنیت اطلاعات، رجوع شود به:
Cybersecurity Strategy: Towards a World-Leading, Resilient and Vigorous Cyberspace, 10 June 2013,
http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf

3. Japan Self-Defense Forces

حکمرانی اینترنت تاکید شده‌است. ژاپن راهبرد امنیت ملی جدیدی در سال ۲۰۱۳ منتشر کرد که اگرچه چندان به توانمندی‌های سایبری در آن توجه نشده‌است، اما به‌طور ویژه بر تدوین و تهیه هنجارهای رفتار در فضای سایبری و گسترش همکاری با کشورهای همسو در عرصه دفاع سایبری تاکید شده‌است[۱].

نسخه بازبینی‌شده راهبرد امنیت سایبری نیز در سال ۲۰۱۵ منتشر شد که بر لزوم ایجاد استانداردهای واحد برای امنیت سایبری در همه نهادهای دولتی و داشتن الزامات گزارش‌دهی و هماهنگی قوی‌تر در پاسخ به تهدیدهای سایبری تاکید می‌کرد[۲]. با توجه به امکان میزبانی ژاپن در بازی‌های المپیک و پارالمپیک (۲۰۲۰)، این سند بر ضرورت رویکرد جامع‌تر در امنیت سایبری نیز تاکید داشت. سند راهبرد امنیت سایبری ۲۰۱۵ اولین سند راهبردی ژاپن است که به موضوع مزایا و خطرات اینترنت اشیا پرداخته‌است (با توجه به اهمیت این موضوع، ژاپن در سال ۲۰۱۶ سندی اختصاصی برای آن تدوین کرد[۳]). در این سند به نقش فزاینده وزارت دفاع در واکنش به حمله‌های سایبری و اهمیت تقویت روابط با ارتش ایالات متحده در راستای «راهنمای همکاری دفاعی ایالات متحده و ژاپن»[۴] نیز تاکید شده‌است[۵]. سند راهبردی ۲۰۱۵ اولین سندی است که در سطح کابینه دولت

۱. وزارت امور خارجه ژاپن، رجوع شود به:
National Security Strategy, 17 December 2013,
http://japan.kantei.go.jp/96_abe/documents/2013/__icsFiles/afieldfile/2013/12/17/NSS.pdf

۲. دولت ژاپن، رجوع شود به:
Cybersecurity Strategy, 4 September 2015,
http://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf

۳. رجوع شود به:
National Center of Incident Readiness and Strategy for Cybersecurity, General Framework for Secure IoT Systems, 26 August 2016,
http://www.nisc.go.jp/eng/pdf/iot_framework2016_eng.pdf

4. Guidelines for US-Japan Defense Cooperation

۵. از سال ۱۹۷۹ تاکنون، محورهای همکاری دفاعی دو کشور براساس این راهنما تعیین می‌شود. رجوع شود به:
US Department of Defense, 'The Guidelines for U.S.-Japan Defense Cooperation', 27 April 2015,
https://archive.defense.gov/pubs/20150427_---_GUIDELINES_FOR_US-JAPAN_DEFENSE_COOPERATION.pdf.

ژاپن طرح شـد و بیانگر افزایش آگاهی رده‌های بالای دولت نسـبت به اهمیت امنیت در فضای سایبری است.

راهبرد امنیت سـایبری که در جولای ۲۰۱۸ (۲۰۲۰-۲۰۱۸) منتشـر شـد نیز تاکید ویژه‌ای بر بازی‌هـای المپیـک و پارالمپیـک دارد و نمـاد تحـول سیاسـت‌های ژاپن به‌شـمار می‌رود[۱]. در ایـن سـند بـه صراحت از تهدیدهای سـایبری کشـورهای متخاصم یاد شده‌اسـت و در همـان صفحـه اول دربـاره خطـر روزافـزون حمله‌هـای سـایبری سـازمان‌یافته، تخصصی و احتمـالا بـا حمایت دولت‌ها هشـدار داده می‌شـود. ادغام تدریجی فضـای واقعی و فضای سـایبری از دیگـر مسـائل موردتاکیـد در ایـن سـند اسـت کـه آن را حاصـل رشـد فزاینـده فناوری‌هـای سـایبری پیشـرفته‌ای مانند هوش مصنوعـی، اینترنت اشـیا، رباتیک و چاپ سـه‌بعدی می‌داند- همان عناصر محوری مفهوم جامعه اطلاعاتی یا به تعبیر دولت ژاپن جامعـه پنجـم[۲]. علاوه بر این‌ها، در این سـند بر لزوم ارتقـای آمادگی واکنش به حمله‌های سـایبری گسـترده، ابتکارعمل‌های جدید برای حفاظت از زیرساخت‌های حیاتی و افزایش همـکاری بیـن ذینفعـان تاکیـد شده‌اسـت. بهبـود امنیـت سـایبری در بخـش خصوصی براساس سیاست «دفاع سایبری فعال» ازجمله ازطریق اشتراک‌گذاری و بهره‌برداری بهتر از اطلاعـات مربوط به تهدیدها و آسـیب‌پذیری‌های سـامانه‌ها اولویت دیگر در این سـند به شمار می‌رود.

راهبـرد امنیت سـایبری ۲۰۱۸ از این نظر که بـرای اولین بار به توانمندی‌های بازدارندگی ژاپن در عرصه سـایبری اشـاره می‌کند، نقطه‌عطفی در سیاسـت‌های سـایبری این کشـور محسـوب می‌شـود. در این سـند وظیفـه هماهنگی توانمندی‌های سـایبری بـه دبیرخانه

۱. رجوع شود به:
National Center of Incident Readiness and Strategy for Cybersecurity, Cybersecurity Strategy, 27 July 2018, https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf
2. Society 5.0

امنیت ملی[1] محول شده‌است. دبیرخانه مذکور پشتیبان شورای امنیت ملی[2] است که به‌عنوان نهادی بین‌سازمانی مسئولیت هماهنگی سیاست‌های امنیت ملی را برعهده دارد. با این همه، ژاپن هنوز هیچ راهبرد سایبری نظامی رسمی یا مبنای نظری نظامی رسمی (مربوط به ارتش) درباره امنیت سایبری در فضای عمومی ندارد.

ژاپن از سال ۲۰۱۲ توسعه توانمندی‌های سایبری نظامی خود را با تشکیل واحد دفاع سایبری ۱۰۰[3] با قدرت آغاز کرد. (البته پیش از این نیز ارتش ژاپن فعالیت‌های مختلفی در زمینه سایبری داشته‌است[4]). راهنمای برنامه دفاع ملی ۲۰۱۹[5] بیش از هر سند دیگری بیانگر دیدگاه سایبری ژاپن است. در این سند بر لزوم پیوستگی و تعامل‌پذیری نیروهای ارتش به‌نحوی که به‌راحتی قابلیت ادغام با ساختارهای نیروهای دفاعی ایالات متحده در شرق آسیا را داشته باشند، تاکید می‌شود. جالب این‌که فضا، فضای سایبری و طیف‌های الکترومغناطیسی در این سند عرصه نبردهای جدید تلقی می‌شوند. این سند همچنین بر لزوم اجرای عملیات‌های نظامی دفاعی در فضای سایبری همسو با رویکرد کلی ارتش و دستیابی به برتری در عرصه سایبری و توانمندی‌های تهاجمی سایبری به‌عنوان بخشی از عملیات‌های دفاعی جهت مقابله با حمله‌های سایبری دشمنان متمرکز است[6]. به‌عبارت دیگر، کسب توانمندی‌های سایبری جهت پیشگیری از فعالیت‌های بازیگران متخاصم در عرصه سایبری از اولویت‌های امنیت سایبری در سند مذکور محسوب می‌شود[7].

1. National Security Secretariat
2. National Security Council
3. 100-Strong Cyber-Defense Unit
4. Richard J. Samuels, Special Duty: A History of the Japanese Intelligence Community (Ithaca, NY: Cornell University Press, 2019), pp. 228-9
5. 2019 National Defense Program Guidelines

۶. وزارت دفاع، رجوع شود به:
National Defense Program Guidelines for FY 2019 and beyond, 18 December 2018, https://www.mod.go.jp/j/approach/agenda/guideline/2019/pdf/20181218_e.pdf

7. National Center of Incident Readiness and Strategy for Cybersecurity, Cybersecurity Strategy, 27 July 2018.

در بیانیه دفاعی ۲۰۲۰[1] ژاپن بر این مساله تاکید شده‌است که فضای سایبری می‌تواند ماهیت نبردها را به‌طور جدی تغییر دهد و از این رو، باید توانمندی‌هایی جهت اجرای عملیات‌های فرادامنه‌ای در فضا، فضای سایبری و دامنه‌های الکترومغناطیسی طراحی و ساخته شود[2]. این سند ضمن پرداختن به ضرورت تقویت توانمندی‌های حوزه اطلاعات سایبری، بر اهمیت دستیابی به توانمندی‌های لازم جهت اختلال در نیروهای فرماندهی، کنترل، ارتباطات، کامپیوترها و اطلاعات دشمنان (C4I) نیز تاکید دارد[3].

برنامه دفاع میان‌مدت[4] سند دیگری است که به نقش ارتش ژاپن در فضای سایبری می‌پردازد. این برنامه اولویت‌های دفاعی کشور برای دوره ۲۰۱۹ تا ۲۰۲۳ را تبیین می‌کند[5]. در این سند بر ضرورت ایجاد واحدهای سایبری جدید در نیروهای زمینی تاکید ویژه‌ای می‌شود که خود می‌تواند بیانگر ضعف ارتش ژاپن در این حوزه باشد. علاوه بر این، ضرورت توسعه بیشتر توانمندی‌های فرماندهی، کنترل، ارتباطات، کامپیوترها و اطلاعات (C4I)، گسترش واحد دفاع سایبری موجود و مشارکت بیشتر در رزمایش‌های سایبری دوجانبه و چندجانبه نیز در این سند موردتوجه قرار گرفته‌اند.

حکمرانی، فرماندهی و نظارت

دولت ژاپن در سال ۲۰۱۴ نسبت به سازماندهی مجدد و ارتقای ساختار فرماندهی و نظارت خود اقدام کرد که منجر به ارتقای هماهنگی فعالیت‌های سایبری در سطح ملی شد.

1. 2020 Defense White Paper

Defense of Japan 2020, 2020, p. 41,
https://www.mod.go.jp/e/publ/w_paper/wp2020/DOJ2020_EN_Full.pdf.

۲. وزارت دفاع، رجوع شود به:

۳. همان، صص. ۲۶۷-۲۱۸

4. Mid Term Defense Program

۵. وزارت دفاع، رجوع شود به:

Medium Term Defense Program (FY 2019- FY 2023), 18 December 2018,
https://www.mod.go.jp/j/approach/agenda/guideline/2019/pdf/chuki_seibi31-35_e.pdf

اگرچه ساختار حکمرانی فضای سایبری ژاپن هم‌اکنون شبیه کشورهای هم‌پیمان آن مانند ایالات متحده و بریتانیاست، اما در بخش‌های خصوصی و دولتی نسبتا ضعیف است.

با تصویب قانون پایه امنیت سایبری[1] در سال ۲۰۱۴ زمینه ساختارهای کنونی امنیت سایبری ژاپن فراهم آمد (این قانون در سال‌های ۲۰۱۶ و ۲۰۱۸ اصلاح شد). به‌موجب این قانون که در ژانویه ۲۰۱۵ به اجرا درآمد، ستاد راهبردی امنیت سایبری (CSSH)[2] تشکیل شد و جایگزین شورای سیاست امنیت اطلاعات[3] شد که عملکرد سازمانی ضعیفی داشت. مرکز ملی آمادگی حادثه و راهبرد امنیت سایبری (NISC)[4] دیگر نهاد مهم در این حوزه است که بازوی اجرایی دبیرخانه کابینه محسوب می‌شود. این دو نهاد طبق قانون مسئولیت هماهنگی و اجرای راهبرد امنیت سایبری ژاپن را برعهده دارند. ستاد راهبردی امنیت سایبری نهاد رسمی جهت فرماندهی و نظارت امنیت سایبری ملی[5] در ژاپن است که ریاست آن را رئیس وزرای کابینه برعهده دارد. رئیس کمیسیون ملی ایمنی عمومی[6]، رئیس سازمان ملی پلیس[7]، چهار تن از وزرا (وزیر امور داخلی و ارتباطات، وزیر امور خارجه، وزیر اقتصاد، تجارت و صنعت و وزیر دفاع) و هشت متخصص سایبری که ریاست گروه‌های کارشناسی را برعهده دارند نیز از اعضای آن هستند.

ستاد راهبردی امنیت سایبری ژاپن با شورای امنیت ملی و ستاد راهبردی فناوری اطلاعات[8] از نظر سیاست‌ها هماهنگی کامل دارد. مرکز ملی آمادگی حادثه و راهبرد امنیت سایبری نیز اجرای سیاست‌های سایبری را با وزارت‌های ذی‌ربط هماهنگ می‌کند

1. Basic Act on Cyber Security
2. Cyber Security Strategic Headquarters
3. Information Security Policy Council
4. National Incident Readiness and Strategy for Cybersecurity

۵. دولت ژاپن، رجوع شود به:
Cybersecurity Strategy, 4 September 2015

6. National Public Safety Commission
7. National Police Agency
8. IT Strategic Headquarters

و از نظر قانونی همانند اپراتورهای زیرساخت‌های حیاتی ملی تحت‌نظارت ستاد راهبردی امنیت سایبری فعالیت دارد[۱]. به‌طور کلی، تهیه و ارتقای راهبرد امنیت سایبری کشور شامل تدوین استانداردهای مشترک، حفاظت از زیرساخت‌ها، توسعه منابع انسانی و اجرای راهبرد تحقیق و توسعه ازجمله وظایف ویژه مرکز ملی آمادگی حادثه و راهبرد امنیت سایبری به شمار می‌آیند[۲].

به‌منظور ارتقای همکاری و تبادل اطلاعات سایبری بین دولت، بخش خصوصی و دانشگاه‌ها و نیز درجهت تامین امنیت بازی‌های المپیک و پارالمپیک، متمم دوم قانون پایه امنیت سایبری در دسامبر ۲۰۱۸ تصویب شد که تشکیل شورای امنیت سایبری[۳] را در پی داشت. وظیفه این نهاد جدید شامل برقراری هماهنگی نزدیک بین مرکز ملی آمادگی حادثه و راهبرد امنیت سایبری، گروه ملی پاسخ فوری رایانه‌ای (JPCERT)[۴] و سایر نهادهای ذی‌ربط مانند موسسه ملی فناوری اطلاعات و ارتباطات[۵] و سازمان ارتقای فناوری اطلاعات[۶] است-این دو نهاد اخیر موظف به ارتقای همکاری اطلاعاتی بین دولت و بخش خصوصی هستند[۷].

۱. برخی از این هماهنگی‌ها عبارتند از: پایش مستمر فعالیت‌های تهاجمی علیه سامانه‌های اطلاعاتی نهادهای اداری، یافتن مستندات مربوط به علل حوادث و بازرسی نهادهای دولتی ذی‌ربط، گردآوری و تحلیل اطلاعات مربوط به امنیت سایبری داخلی و خارجی، ترویج همکاری‌های بین‌المللی و توسعه نیروی انسانی امنیت سایبری توسط نهادهای دولتی. برای جزئیات بیشتر رجوع شود به:
National Center of Incident Readiness and Strategy for Cybersecurity, Organizational Structure, http://www.nisc.go.jp/about/organize.html

۲. رجوع شود به:
National Center of Incident Readiness and Strategy for Cybersecurity, Cybersecurity Framework in the Government of Japan (handout), September 2019.

3. Cybersecurity Council
4. Computer Emergency Response Team
5. National Institute of Information and Communications Technology
6. Information-Technology Promotion Agency

۷. رجوع شود به:
Cyber Security Strategy in Japan: Present Situation and Challenges, presentation delivered by Tomoo Yamauchi, Deputy Director General, NISC, to the Foreign Press Center of Japan, 4 July 2019, https://fpcj.jp/wp/wp-content/uploads/2019/07/190704-Cybersecurity-StrategyForeign-Press-Center-1.pdf

در ژاپن فرماندهی و نظارت سایبری بخش نظامی در مقایسه با بخش غیرنظامی ضعیف‌تر است. در سال ۲۰۰۸، ستاد فرماندهی سیستم‌های C4[1] تحت فرماندهی مستقیم رئیس ستاد نیروهای مشترک[2] و با هدف نظارت بر شبکه‌های نظامی و پاسخ به حمله‌های سایبری توسط وزارت دفاع تاسیس شد. هریک از شاخه‌های ارتش ژاپن دارای واحد دفاع سایبری مجزایی است که مسئولیت تامین امنیت شبکه‌ها و سیستم‌های اطلاعاتی به‌ویژه در برابر حمله‌های سایبری داخلی را برعهده دارند[3]. در مارس ۲۰۱۹، ارتش ژاپن واحد دفاع سایبری منطقه‌ای را به‌عنوان بخشی از سپاه غربی نیروهای زمینی دفاع از خود ژاپن (JGSDF)[4] و با حدود ۶۰ نفر نیرو تشکیل داد. این واحد که اولین نهاد در نوع خود است، وظیفه دفاع و پشتیبانی از سیستم‌ها و شبکه‌های ارتش ژاپن را برعهده دارد[5].

در مارس ۲۰۱۴ نیز یک گروه دفاع سایبری با هدف هماهنگ‌سازی دفاع سایبری در کل ارتش و دفاع از زیرساخت‌های اطلاعاتی کشور تشکیل شد که طبق پیش‌بینی باید تعداد کارکنان آن تا سال ۲۰۲۱ از ۲۲۰ نفر به ۲۹۰ نفر افزایش یافته‌باشد[6]. منابع رسانه‌ای حاکی از آن هستند که کل نیروهای بخش دفاع سایبری ارتش ژاپن تا سال ۲۰۲۴ بالغ بر ۵۰۰ نفر خواهد بود[7].

1. C4 Systems Command
2. Joint Staff Office

۳. وزارت دفاع ژاپن، رجوع شود به:

'Regarding Response to Cyber Attack', undated, https://www.mod.go.jp/e/publ/answers/cyber/index.html

4. Western Army of the Japan Ground Self-Defense Force

۵. رجوع شود به:

Franz-Stefan Gady and Yuka Koshino, 'Japan and Cyber Capabilities: How Much Is Enough?', Military Balance blog, International Institute for Strategic Studies, 28 August 2020, https://www.iiss.org/blogs/military-balance/2020/08/japan-cyber-capabilities.

۶. رجوع شود به:

'Japan Embraces AI Tools to Fight Cyberattacks with US$237 Million Investment', CISO Magazine, 6 April 2020, https://cisomag.eccouncil.org/japan-embraces-ai-tools-to-fightcyberattacks-with-us237-mn-investment

۷. رجوع شود به:

Daishi Abe, 'Lagging China and the US, Japan to beef up cyberdefense', Nikkei Asia, 20 June 2020, https://asia.nikkei.com/Politics/Lagging-China-and-the-US-Japan-to-beef-up-cyberdefense.

توانمندی‌های محوری در زمینه اطلاعات سایبری

به دلایل سیاسی مختلف ازجمله مفاد قانون اساسی ژاپن که پس از جنگ جهانی دوم تغییر کرد، اندازه و بودجه سازمان‌های اطلاعاتی این کشور کمتر از دیگر کشورهای همتراز آن است. به‌عنوان مثال، میزان جمع‌آوری اطلاعات سیگنالی و درنتیجه اجرای عملیات‌های رصد و شناسایی برای دولت ژاپن به‌موجب ماده ۲۱ قانون اساسی این کشور به‌شدت محدود شده‌است. با این حال، ژاپن چندین سازمان فعال در این حوزه دارد که ستاد اطلاعات دفاعی (DIH)[۱] و بزرگ‌ترین سازمان زیرمجموعه آن یعنی اداره کل اطلاعات سیگنالی (DSI)[۲] بارزترین نمونه‌های آن هستند. علاوه براین، ژاپن سالهاست که میزبان تاسیسات اطلاعات سیگنالی ایالات متحده در چارچوب توافق‌نامه همکاری اطلاعاتی بین دو کشور است.

اداره کل اطلاعات سیگنالی ژاپن معادل سازمان امنیت ملی آمریکا و ستاد ارتباطات دولت بریتانیاست، هر چند که از نظر اندازه بسیار کوچک‌تر از آن دو است. تا قبل از سال ۲۰۱۲ این سازمان اطلاعات را با استفاده از ماهواره‌های مخابراتی گردآوری می‌کرد، اما پس از آن با کمک سازمان امنیت ملی آمریکا اطلاعات را کسب می‌کند (در آغاز این همکاری صرفا جنبه آزمایشی داشت[۳]). با آنکه این سازمان در سال ۲۰۲۰ از دولت تقاضای افزایش بودجه کرد[۴]، اما به‌دلیل فقدان منابع و نیز موانع قانونی (ماده ۲۱) هنوز این امر محقق نشده‌است.

۱. ستاد اطلاعات دفاعی (Defense Intelligence Headquarters) بزرگ‌ترین سازمان دفاعی ژاپن است که در سال ۲۰۲۰ بیش از ۲۰۰۰ نفر نیروی کار داشت.

2. Directorate for Signal Intelligence

۳. رجوع شود به:
Samuels, Special Duty: A History of the Japanese Intelligence Community, p. 232.

۴. وزارت دفاع ژاپن، رجوع شود به:
Defense Programs and Budget of Japan: Overview of FY2020 Budget Request, 2019, https://www.mod.go.jp/e/d_act/d_budget/pdf/200225a.pdf.

اداره اطلاعات و تحقیقات کابینه[1] که از بودجه نسبتا خوبی برخوردار است نیز نقش مهمی در عرصه سایبری ژاپن بازی می‌کند. این نهاد به‌طور مستقیم به نخست‌وزیر گزارش می‌دهد و مسئولیت هماهنگی و ارزیابی عملکرد جامعه اطلاعاتی کشور را برعهده دارد.

به‌طور کلی، توانمندی‌های بومی ژاپن در بخش اطلاعات سایبری نوپاست و این کشور در زمینه آگاهی موقعیتی و توسعه توانمندی‌های حوزه اطلاعات سایبری بیشتر وابسته به کشورهای هم‌پیمان خود به‌ویژه آمریکاست.

توانمندی و وابستگی سایبری

ژاپن یکی از پیشتازان عرصه فناوری‌های سایبری دنیاست. نتایج مطالعه صندوق بین‌المللی پول[2] (۲۰۱۹) نشان می‌دهند که اقتصاد دیجیتال ژاپن ۴۹ درصد از تولید ناخالص داخلی آن را تشکیل می‌دهد (در ایالات متحده این رقم ۶۰ درصد و در چین ۳۰ درصد است)[3]. در رتبه‌بندی جهانی فورچون ۵۰۰ در سال ۲۰۲۰، ژاپن با داشتن ۱۰ شرکت پس از ایالات متحده (با ۱۶ شرکت) در جایگاه دوم قرار گرفت (چین و مجموع کشورهای اتحادیه اروپا هر یک با ۸ شرکت در جایگاه سوم قرار داشتند)[4].

ژاپن بزرگ‌ترین تولیدکننده ربات‌های صنعتی و از پرچم‌داران توسعه زیرساخت‌های دیجیتال است. رشد فزاینده اقتصاد ژاپن به کمک فناوری‌های اطلاعات و ارتباطات

1. Cabinet Intelligence and Research Office
2. International Monetary Fund

۳. رجوع شود به:
Longmei Zhang and Sally Chen, 'China's Digital Economy: Opportunities and risks', International Monetary Fund Working Paper, no. WP/19/16, 17 January 2019, p. 4,
https://www.imf.org/en/Publications/WP/Issues/2019/01/17/Chinas-Digital-Economy-Opportunities-and-Risks-46459.

۴. برای کسب اطلاعات بیشتر درباره شرکت‌های فناوری رجوع شود به:
https://fortune.com/global500/2020/search/?sector=Technology.
برای کسب اطلاعات بیشتر درباره شرکت‌های مخابراتی رجوع شود به:
https://fortune.com/global500/2020/search/?sector=Telecommunications.

موجب وابستگی شدید آن به این فناوری‌ها نیز شده‌است. این کشور توانسته‌است به قدرتی مطلق در زمینه تولید ریزتراشه‌ها تبدیل شود، به‌طوری‌که شرکت‌های توکیو اوکا کُگیو (TOK)[۱]، جِی‌اِس‌آر کُرپوریشن[۲] و شین-اِتسو کِمیکال[۳] در تولید مقاومت‌های نوری ماوراء بنفش شدید (EUV)[۴] برای ساخت تراشه‌های هفت نانومتری پیشرو هستند[۵].

ژاپن چهارمین گروه بزرگ مخابراتی دنیا یعنی تلگراف و تلفن نیپون (NTT)[۶] را در اختیار دارد که متشکل از شعب متعددی مانند شرکت ارتباطات اِن‌تی‌تی[۷] (ارتباطات بین‌المللی)، شرکت اِن‌تی‌تی دوموکو[۸] (ارتباطات سیار) و شرکت مهندسی دریایی اِن‌تی‌تی[۹] (نصب و تعمیر/نگهداری کابل‌های زمینی) است[۱۰]. داده‌های ارائه شده توسط موسسه آی‌پی‌وی6[۱۱] در سال ۲۰۱۹ نشان می‌دهند که همه پنج اپراتور اصلی خدمات اینترنت در ژاپن (شامل بی‌بیکس، بیگ‌لوپ، جِی‌پی‌اِن‌ایی، اِم‌اِف نِیتیو6 و اُسی‌اِن) بومی هستند[۱۲]. ناوگان کوچک کشتی‌های کابل‌گذار شرکت مهندسی دریایی اِن‌تی‌تی

1. Tokyo Ohka Kogyo Co., Ltd.
2. JSR Corporation
3. Shin-Etsu Chemical
4. Extreme Ultra Violet

۵. رجوع شود به:
Hiroshi Fujiwara, 'Why Japan leads industrial robot production', International Federation of Robotics (IFR), 17 December 2018,
https://ifr.org/post/why-japan-leads-industrial-robot-production

6. Nippon Telegraph and Telephone
7. NTT Communications
8. NTT Domoco
9. NTT World Engineering Marine Corporation

۱۰. رجوع شود به:
Nippon Telegraph Telephone (NTT) Group,
https://www.ntt.co.jp/index_e.html

11. IPv6
12. Bbix, Biglobe, Jpne, Mf-native6 and Ocn

رجوع شود به:
Ipv6 Test, 'IPv6 in Japan', October 2019,
https://ipv6-test.com/stats/country/JP

نیـز ژاپـن را قـادر ساخته‌اسـت کـه زیرسـاخت اصلـی مخابراتـی خـود را بـه‌صورت بومی و مستقل توسعه دهد[۱].

البتـه ژاپـن از نظـر بهـره‌وری فناورانـه در مقایسـه بـا سـایر اعضـای سـازمان همـکاری اقتصادی و توسعه وضعیت مناسبی ندارد و برای جبران این شکاف نیازمند سرمایه‌گذاری بیشتر در توسعه منابع انسانی و ارتقای مهارت‌ها و تخصص‌های دیجیتال به‌ویژه در بین کارگران میانسـال و مسـن اسـت[۲]. درواقع، شکاف دیجیتال بین نسـل جوان و نسل پیر در ژاپن بسـیار زیاد اسـت و اعتراف وزیر امنیت سایبری ژاپن در سال ۲۰۱۸ به این‌که هرگز از رایانه استفاده نکرده‌است، نمادی از این واقعیت است[۳].

ژاپـن از نظـر توانمندی‌های هـوش مصنوعی از رقابت‌پذیری خوبی برخوردار اسـت. در رتبه‌بنـدی کشـورها از نظر تعداد مقالات در دو کنفرانـس تخصصی حوزه هوش مصنوعی در سال ۲۰۲۰، ژاپن جایگاه نهم را در بین ۵۰ کشور برتر به خود اختصاص داد[۴]. شرکت‌های ژاپنـی در تحقیقـات هـوش مصنوعـی بسـیار فعـال هسـتند و ۹ شـرکت ژاپنـی در بین ۱۰۰ شـرکت برتر دنیا قرار دارند که در مقایسـه با کره جنوبی با ۶ شـرکت و هند که اصلا شرکتی در این رده‌بندی ندارد، وضعیت ژاپن بسیار بهتر است. البته ژاپن از نظر میزان مشارکت بخش صنعت در تحقیقات هوش مصنوعی هنوز از کره جنوبی عقب‌تر است[۵].

---

۱. رجوع شود به:

NTT WE Marine, 'Cable-Laying Vessels', https://www.nttwem.co.jp/english/ship.

۲. سازمان همکاری اقتصادی و توسعه، رجوع شود به:

OECD Economic Surveys, April 2019, p. 44

۳. اخبار بی‌بی‌سی، رجوع شود به:

'Japan's cyber-security minister has "never used a computer"', 15 November 2018, https://www.bbc.co.uk/news/technology-46222026.

۴. رجوع شود به:

Gleb Chuvpilo, 'AI Research Rankings 2020: Can the United States Stay Ahead of China?', 21 December 2020, https://chuvpilo.medium.com/ai-research-rankings-2020-can-theunited-states-stay-ahead-of-china-61cf14b1216.

۵. همان

بخش‌های زیادی از فناوری‌های دیجیتال ژاپن به‌طور بالقوه ظرفیت ادغام در کارکردهای نظامی را دارند، اما دولت ژاپن در حال حاضر تمایل چندانی به این امر ندارد. در اسناد چشم‌انداز سالانه ژاپن نیز اشاراتی به رویکردهای جهانی نسبت به وابستگی دیجیتال در عملیات‌های نظامی و ضرورت ارتقای تاب‌آوری سامانه‌های فرماندهی و کنترل شده‌است[۱].

در راستای تقویت ظرفیت ماهواره‌های بومی، اداره کابینه در سال ۲۰۰۲ طرح‌هایی را برای به‌کارگیری و توسعه سامانه‌های ماهواره‌ای کوازی‌زنیث (QZSS/Michibiki)[۲] با رهبری سازمان اکتشاف هوافضا تصویب کرد[۳]. اولین ماهواره در سال ۲۰۱۰ پرتاب شد و به‌دنبال آن در سال‌های ۲۰۱۶ تا ۲۰۱۸ سه ماهواره دیگر در مدار قرار گرفت. ماهواره‌های کوازی‌زنیث که در اصل به‌منظور تقویت سامانه موقعیت‌یابی جهانی (GPS)[۴] ایالات متحده عملیاتی شدند، به ژاپن سطحی از خودمختاری اعطا می‌کنند و همزمان برای همه منطقه آسیا و اقیانوسیه نیز مفید هستند[۵]. در حال حاضر، این سامانه در سازمان بین‌المللی دریانوردی[۶] جهت ثبت در سامانه جهانی ناوبری رادیویی[۷] در دست بررسی است[۸].

---

۱. رجوع شود به:
Cabinet Office, 'Juntenchōeisei shisutemu ni tsuite', undated, https://www8.cao.go.jp/space/qzs/qzs.html

2. Quasi-Zenith Satellite System

3. Aerospace Exploration Agency

رجوع شود به:
Quasi-Zenith Satellite System (QZSS), 'Overview of the Quasi-Zenith Satellite System (QZSS)', https://qzss.go.jp/en/overview/services/sv01_what.html.

4. Global Positioning System

۵. رجوع شود به:
Quasi-Zenith Satellite System (QZSS), '[Report] Deliberations on QZSS at the 7th Session of the IMO's NCSR', 5 March 2020, https://qzss.go.jp/en/events/imo_200305.html.

6. International Maritime Organization

7. Worldwide Radio Navigation System

۸. وزارت دفاع، رجوع شود به:
Defense of Japan 2020, pp. 266-7.

ژاپن تمرکز زیادی بر جنبه امنیت ملی فضا دارد و توانمندی‌های موشکی کره شمالی و قدرت نظامی فزاینده چین موجب نگرانی این کشور شده‌اند. از این رو، ژاپن به‌طور جدی درصدد ارتقای توانمندی‌های فضایی خود برآمده‌است. در همین راستا، ژاپن در سال ۲۰۲۰ ستاد راهبردی سیاست فضایی ملی[1] را در اداره کابینه و با هدف برنامه‌ریزی عملیات‌های مشترک حوزه فضایی تشکیل داد. علاوه بر این، ژاپن در سال ۲۰۲۲ اسکادران عملیات فضایی[2] را جهت آماده‌شدن برای به‌کارگیری سامانه آگاهی موقعیتی فضایی[3] ایجاد کرد.

امنیت و تاب‌آوری سایبری

فناوری‌های دیجیتال و سایبری نقش محوری در اقتصاد و جامعه ژاپن بازی می‌کنند و با توجه به سطح بالای ارتباطات دیجیتال و نوپابودن کشور از نظر تاب‌آوری سایبری می‌توان دریافت که وقوع حمله‌های سایبری مستمر به زیرساخت‌های کشور منجر به آسیب‌های شدیدی خواهد شد[4].

برنامه‌ریزی‌ها و اقدامات ژاپن درجهت ارتقای تاب‌آوری سایبری بیشتر تحت‌تاثیر مسابقات المپیک و پارالمپیک ۲۰۲۰ توکیو آغاز شد. سیاست امنیت سایبری برای حفاظت از زیرساخت‌های حیاتی (۲۰۱۸)[5] به‌عنوان سند راهنمای عمل ژاپن در این حوزه محسوب می‌شود. این سند استفاده از مشارکت‌های بخش خصوصی و بخش دولتی جهت تقویت تاب‌آوری و احیای زیرساخت‌ها پس از حمله‌های سایبری را بسیار

1. Strategic Headquarters for National Space Policy
2. Space Operations Squadron
3. Space Situational Awareness System

۴. رجوع شود به:

National Center of Incident Readiness and Strategy for Cybersecurity, Cybersecurity Strategy, 27 July 2018.

5. Cybersecurity Policy for Critical Infrastructure Protection

حائزاهمیت می‌داند[۱]. با توجه به این‌که ۹۰ درصد دارایی‌های فناوری اطلاعات و ارتباطات ژاپن به بخش خصوصی آن تعلق دارد، این امر کاملا منطقی است[۲].

گروه پاسخ فوری رایانه‌ای ژاپن (JPCERT) با سازمان‌های هم‌تراز خود در دیگر کشورها و نیز گروه‌های تاکتیکی پاسخ فوری در بخش خصوصی و بخش دولتی ژاپن هماهنگ است. گروه پاسخ فوری رایانه‌ای دولتی یعنی مرکز ملی آمادگی حادثه و راهبرد امنیت سایبری (NISC) میزبان تیم هماهنگی عملیات امنیتی دولت[۳] نیز است که مسئولیت به اشتراک‌گذاری دقیق و بهنگام اطلاعات در ساختار گروه‌های پاسخ فوری رایانه‌ای را برعهده دارد[۴].

نبود اراده کافی برای به‌اشتراک‌گذاری داده‌های مربوط به حوادث سایبری به‌عنوان مانع اصلی در بهبود تاب‌آوری سایبری در بخش خصوصی برشمرده می‌شود. این امر ریشه در عوامل ساختاری و فرهنگی مختلفی دارد: ناآگاهی مدیران ارشد شرکت‌ها از اهمیت مسائل سایبری، وابستگی بیش از حد به نهادهای دولتی برای تامین امنیت سایبری و روش سنتی تجارت در ژاپن که مانع همکاری بین شرکت‌هاست[۵].

---

۱. رجوع شود به:
National Center of Incident Readiness and Strategy for Cybersecurity, 'Summary of Cybersecurity Policy for CIP (4th Edition)', 25 July 2018,
https://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4_summary.pdf.

۲. رجوع شود به:
Mihoko Matsubara, 'A Glimpse into Private Sector Security in Japan', Lawfare, 26 June 2018,
https://www.lawfareblog.com/glimpse-private-sector-cybersecurity-japan

3. Government Security Operation Coordination Team

۴. رجوع شود به:
National Center of Incident Readiness and Strategy for Cybersecurity, 'The Guidance on Operations of Information Security Measures of Government Agencies and Related Agencies', 31 August 2016, Revised 25 July 2018,
https://www.nisc.go.jp/eng/pdf/shishin30-en.pdf.

۵. سازمان ارتقای فناوری اطلاعات، رجوع شود به:
Information Technology Promotion Agency, 'Fact-finding survey on corporate CISOs and promotion of security measures', 25 March 2020,
https://www.ipa.go.jp/security/fy2019/reports/2019DL_index.html.

راهنمای مدیریت امنیت سایبری توسط وزارت اقتصاد، تجارت و صنعت[1] و یکی از زیرمجموعه‌های آن یعنی سازمان ارتقای فناوری اطلاعات[2] به‌منظور کمک به ارتقای اقدامات و استانداردهای امنیت سایبری در بخش خصوصی منتشر شده‌است[3]. این اصول براساس چارچوب امنیت سایبری موسسه ملی استاندارد و فناوری ایالات متحده[4] تهیه شده‌اند و درنتیجه، بیانگر تمایل ژاپن به استفاده از رویکرد آمریکا در عرصه امنیت سایبری و نیز فقدان نوآوری بومی در این زمینه است. علاوه براین، چارچوبی برای تهیه استانداردهای امنیت سایبری به‌نام استانداردهای مشترک اقدامات امنیت اطلاعات برای سازمان‌های دولتی و نهادهای مرتبط[5] از سال ۲۰۱۶ در دولت ژاپن شکل گرفته‌است. به‌طور کلی، ژاپن در برخی از عرصه‌های امنیت سایبری و بخش فناوری اطلاعات و ارتباطات توسعه‌یافته خود حضور نسبتا قوی دارد و در شاخص جهانی امنیت سایبری (۲۰۱۸) توانسته‌است رتبه ۱۴ را در بین ۱۷۴ کشور کسب کند[6].

دولت رزمایش‌های امنیت سایبری متعددی نیز برگزار می‌کند که یکی از بزرگ‌ترین آن‌ها در نوامبر ۲۰۱۹ با مشارکت بیش از ۵۰۰۰ نهاد خصوصی و دولتی برگزار شد. تشکیل شورای دفاع سایبری[7] در سال ۲۰۱۳ توسط وزارت دفاع با مشارکت حدود ده پیمانکار دفاعی نمونه دیگری از همکاری و مشارکت دولت با بخش خصوصی است. این شورا وظیفه هماهنگی

1. Ministry of Economy, Trade, and Industry
2. Information-Technology Promotion Agency

۳. وزارت اقتصاد، تجارت و صنعت، رجوع شود به:
'Cybersecurity Management Guidelines Revised', press release, 16 November 2017, https://www.meti.go.jp/english/press/2017/1116_001.html.

4. National Institute of Standards and Technology
5. Common Standards on Information Security Measures for Government Agencies and Related Agencies

۶. رجوع شود به:
International Telecommunication Union, 'Global CybersecurityIndex 2018', p. 62, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

7. Cyber Defense Council

تبـادل اطلاعـات بین دولـت و صنایع دفاع و برگـزاری رزمایش‌های سـایبری را برعهده دارد[۱].

رهبری جهانی در عرصه سایبری

پیشگامی در دیپلماسی سایبری از اهداف کلیدی ژاپن به شمار می‌آید. در این راستا، ژاپن می‌کوشد هنجارها و قوانین مربوط به رفتار دولت‌ها در فضای سایبری بین‌المللی را تثبیت کند و مدل چندذینفعی را در حکمرانی اینترنت ترویج دهد. ژاپن درصدد پیشـبرد دیپلماسـی بین‌المللـی جهـت ایجـاد فضـای سـایبری آزاد، ایمـن و عادلانـه و همچنیـن تقویت همکاری بین کشورها است[۲]. به‌طور کلی، این سیاست بر سه محور اصلی استوار اسـت: ترویج حاکمیت قانون در فضای سـایبری، گسترش اقدامات اعتمادافزا و افزایش همکاری بین‌المللی در زمینه ظرفیت‌سازی.

ژاپن تاکنون در پنج بخش از گروه کارشناسـان دولتی سـازمان ملل[۳] مشارکت داشته و همواره در راستای ترویج حاکمیت قانون و اعتمادسازی در فضای سایبری در چارچوب سازمان ملل تلاش کرده‌است[۴]. علاوه بر این، توکیو با گروه کارشناسی سایبری[۵] سازمان

۱. رجوع شود به:
'Jūyō infura 14 bun'ya ni yoru bun'ya ōdan-teki enshū o kaisai, yaku 5, 000-mei ga sanka (NISC)', ScanNetSecurity, 12 November 2019,
https://scan.netsecurity.ne.jp/article/2019/11/12/43217.html.

۲. رجوع شود به:
'Inauguration and Initiatives of the Cyber Defense Council', Japan Defense Focus, no. 44, September 2013, https://www.mod.go.jp/e/jdf/sp/no44/sp_activities.html#article03.

۳. سازمان ملل متحد، رجوع شود به:
UN Office for Disarmament Affairs, 'Developments in the field of information and telecommunications in the context of international security',
https://www.un.org/disarmament/ict-security

۴. سازمان ملل متحد، رجوع شود به:
Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 July 2015,
https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

5. Cyber Expert Group

جی۷ نیز همکاری دارد و با سازمان‌های منطقه‌ای ازجمله آسه‌آن همایش و گفت‌وگوهای متعددی در زمینه امنیت سایبری برگزار می‌کند[۱]. ژاپن عضو کنوانسیون جرائم سایبری نیز هست و با تبیین و ترویج این کنوانسیون در اجلاس‌های بین‌المللی سعی در تقویت قوانین بین‌المللی حوزه جرائم سایبری دارد[۲].

در سطح دیپلماسی منطقه‌ای نیز ژاپن با کشورهای عضو آسه‌آن در زمینه حفاظت از زیرساخت‌های حیاتی و پاسخ سریع به حوادث سایبری همکاری می‌کند[۳] و یکی از اعضای موثر در تشکیل تیم پاسخ فوری رایانه‌ای آسه‌آن به‌شمار می‌رود.

ژاپن به‌عنوان یکی از شرکای جهانی ناتو و عضو پیمان مشارکت صلح (PfP)[۴] در سال ۲۰۱۹ به مرکز عالی همکاری‌های دفاع سایبری (CCD COE)[۵] ناتو پیوست[۶] که از اهداف مهم آن ارتقای همکاری بین اعضای ناتو و شرکایش در اشتراک‌گذاری اطلاعات حوزه امنیت سایبری است. وزارت دفاع ژاپن هدف از پیوستن به این نهاد را توسعه دانش کشور در زمینه نحوه همکاری با ناتو در حوزه دفاع سایبری و بهبود مهارت‌های تاکتیکی وزارت دفاع و ارتش ژاپن اعلام کرده‌است[۷].

---

۱. وزارت دفاع ژاپن، ۲۰۱۹

۲. شورای اروپا، رجوع شود به:

'Japan joins Budapest Convention', press release, 3 July 2012, https://www.coe.int/en/web/cybercrime/news/-/asset_publisher/S73WWxscOuZ5/content/ japan-joins-budapest-convention?inheritRedirect=false

۳. رجوع شود به:

'Asean cybersecurity centre opens in Bangkok', Bangkok Post, 14 September 2018, https://www.bangkokpost.com/world/1540082/southeast-asian-cyber-security-centre-opens-in-thailand

4. Partnership for Peace

5. Cooperative Cyber Defense Center of Excellence

۶. رجوع شود به:

NATO Cooperative Cyber Defense Centre of Excellence, 'About Us', https://ccdcoe.org/about-us.

۷. وزارت دفاع، رجوع شود به:

'Participation in NATO Cyber Defense Exercise "Cyber Coordination 2019"', press release, 27 November 2019, https://www.mod.go.jp/j/press/news/2019/11/27a.html.

قدیمی‌ترین و قوی‌ترین ائتلاف سایبری ژاپن با ایالات متحده است. باتوجه به این‌که آمریکا ضامن نهایی امنیت ژاپن است، مناسبات کنونی بین ژاپن و ایالات متحده شامل گفت‌وگوی سایبری ایالات متحده-ژاپن[۱] و گفت‌وگوی همکاری سیاستی درباره اقتصاد اینترنت ایالات متحده-ژاپن[۲] از اهمیت ویژه‌ای برای دولت این کشور برخوردار هستند. گفتنی آنکه کارگروه سیاست دفاع سایبری[۳] توسط وزارت دفاع ژاپن و پنتاگون با اهداف زیر راه‌اندازی شده‌است: تعمیق به‌اشتراک‌گذاری اطلاعات، انجام رزمایش مشترک و گسترش گفت‌وگوهای سیاستی و افزایش همکاری در زمینه آموزش کارشناسان امنیت سایبری[۴].

ژاپن با سایر کشورهای آسیایی مانند هند و استرالیا نیز توافق همکاری در زمینه امنیت سایبری دارد و مقامات ژاپنی هر سال با همتایان خود از کره جنوبی و چین گفت‌وگوهایی را برگزار می‌کنند. علاوه بر این‌ها، ژاپن در پروژه TSUBAME-سامانه رصد ترافیک-با تیم پاسخ فوری رایانه‌ای آسیا اقیانوسیه (APCERT)[۵] در زمینه به‌اشتراک‌گذاری داده‌ها با تیم‌های پاسخ فوری رایانه‌ای ۲۳ کشور دیگر همکاری می‌کند[۶]. علی‌رغم همکاری نزدیک تیم‌های پاسخ فوری رایانه‌ای ژاپن با همتایان آمریکایی و آسیایی، این تیم‌ها همکاری چندانی با تیم‌های اروپایی ندارند.

ژاپن ۱۱ گفت‌وگوی دوجانبه با استرالیا، استونی، فرانسه، آلمان، هند، رژیم صهیونیستی، روسیه، کره جنوبی، اکراین، بریتانیا و ایالات متحده و نیز اتحادیه اروپا

1. Japan-US Cyber Dialogue
2. Japan-US Policy Cooperation Dialogue on the Internet Economy
3. Cyber Defense Policy Working Group

۴. وزارت دفاع ژاپن، ۲۰۱۹

5. Asia-Pacific Computer Emergency Response Team

۶. رجوع شود به:

Asia Pacific Computer Emergency Response Team, 'TSUBAME Working Group', https://www.apcert.org/about/structure/tsubame-wg/index.html

و ناتو در زمینه سایبری برگزار می‌کند و علاوه بر شرکت در اجلاس سیاست امنیت سایبری آسه‌آن-ژاپن[1] که در آن تمرکز بر ظرفیت‌سازی است، با چین و کره جنوبی نیز گفت‌وگوهای سه‌جانبه‌ای با نگاه ویژه به عملیات‌های کره شمالی برگزار می‌کند[2]. بریتانیا و اتحادیه اروپا جلسات متعددی در سطح وزرا و کارشناسان با ژاپن برگزار می‌کنند و در زمینه ظرفیت‌سازی مشترک و مشارکت فنی نیز با ژاپن همکاری دارند[3]. انتظار می‌رود پس از توافق ژاپن با کمیسیون اروپا در زمینه تبادل داده بدون نیاز به تایید مقامات ملی کشورها، همکاری ژاپن و اتحادیه اروپا در حوزه حفاظت از داده گسترش یابد که این امر نیز به‌نوبه خود به تسهیل مقررات حریم خصوصی داده بین آن‌ها منجر می‌شود[4].

توانمندی‌های سایبری تهاجمی

طبق قانون اساسی ژاپن پس از جنگ جهانی دوم، دولت این کشور حق ساخت و توسعه توانمندی‌های نظامی تهاجمی را ندارد. درواقع، ماده ۹ قانون اساسی ژاپن آن را از حق داشتن هر نوع نیروی نظامی محروم می‌کند. اگرچه این ماده از سال ۱۹۵۴ با تصویب قانون نیروی‌های نظامی دفاع از خود[5] نادیده گرفته شده‌است، اما هربار که دامنه فعالیت‌ها و توان نیروهای نظامی ژاپن افزایش می‌یابد، دولت‌ها مجبور می‌شوند

1. ASEAN-Japan Cybersecurity Policy Meeting

۲. آخرین دور این گفت‌وگوهای سه‌جانبه در دسامبر ۲۰۲۰ برگزار شد. برای کسب جزئیات بیشتر رجوع شود به:
Ministry of Foreign Affairs of Japan, 'The 5th Trilateral Cyber Policy Consultation', 10 December 2020, https://www.mofa.go.jp/press/release/press24e_000019.html

۳. رجوع شود به:
Wilhelm M. Vosse, 'Japan's Cyber Diplomacy', Research in Focus, EU Cyber Direct, October 2019, https://eucyberdirect.eu/wp-content/uploads/2019/10/vosse_rif_topublish.pdf.

۴. کمیسیون اروپا، رجوع شود به:
'European Commission adopts adequacy decision on Japan, creating the largest area of safe data flows', press release, 22 January 2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421.

5. Self Defense Force Act

با بحث‌های پیچیده حقوقی و سیاسی جامعه مدنی را اقناع کنند. از سال ۲۰۱۵ نیز ژاپن می‌کوشد با تفسیرهای جدید از قانون امکان کمک به هم‌پیمانان حتی درصورتی که خود تحت حمله نباشد را فراهم کند[۱]. این چرخش دیدگاه می‌تواند دفاع جمعی و دفاع در فضای سایبری را نیز توجیه کند[۲].

علاوه بر این، در اسناد رسمی این کشور نشانه‌هایی از تغییر ظریف سیاست‌ها از دفاع صِرف به‌سمت فعالیت‌های تهاجمی‌تر نیز مشاهده می‌شود. به‌عنوان نمونه، در سند سیاست‌های دفاعی ۲۰۲۰ بر حق نیروهای ارتش ژاپن برای اخلال در عملیات‌های سایبری دشمن در زمان حمله به این کشور تاکید شده‌است[۳]. برخی از سیاست‌گذاران ارشد ژاپن نیز معتقدند توانمندی‌های سایبری تهاجمی گزینه «مقابله بازدارنده» را در اختیار ژاپن قرار می‌دهند که می‌تواند بخشی از دفاع موشکی آن محسوب شود[۴]. البته تحقق این امر مستلزم تغییر قانون نیروی‌های نظامی دفاعی ژاپن است[۵].

---

۱. رجوع شود به:
Franz-Stefan Gady, 'Toothless tiger: Japan Self-Defense Forces', BBC News, 14 October 2015, https://www.bbc.com/news/world-asia-34485966

۲. رجوع شود به:
Daisuke Akimoto, 'Cybersecurity and Japan's Right to Self-Defense', Institute for Security and Development Policy, undated, https://isdp.eu/cybersecurity-japans-right-to-self-defense.

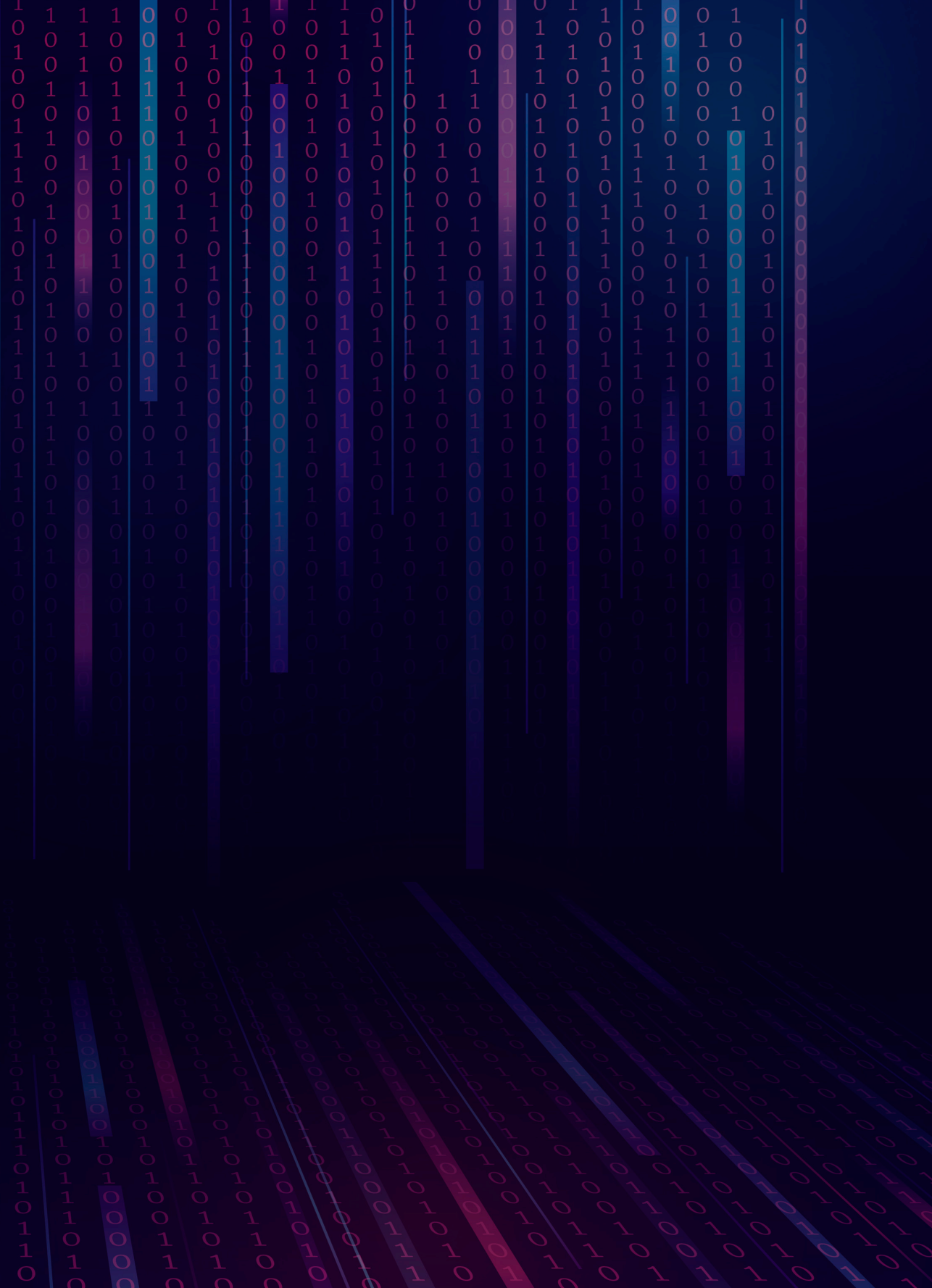
۳. به‌نقل از رسانه‌های خبری در سال ۲۰۱۹، وزارت دفاع ژاپن قراردادی با بخش خصوصی برای ساخت توانمندی‌های سایبری تهاجمی با هدف استفاده در عملیات‌های دفاعی منعقد کرده‌است. برای کسب جزئیات بیشتر رجوع شود به:
'Japan to develop 1st defense use computer virus against cyberattacks', Kyodo News, 30 April 2019, https://english.kyodonews.net/news/2019/04/e9e4df950d3d-japan-to-develop-1st-defenseuse-computer-virus-against-cyberattacks.html.

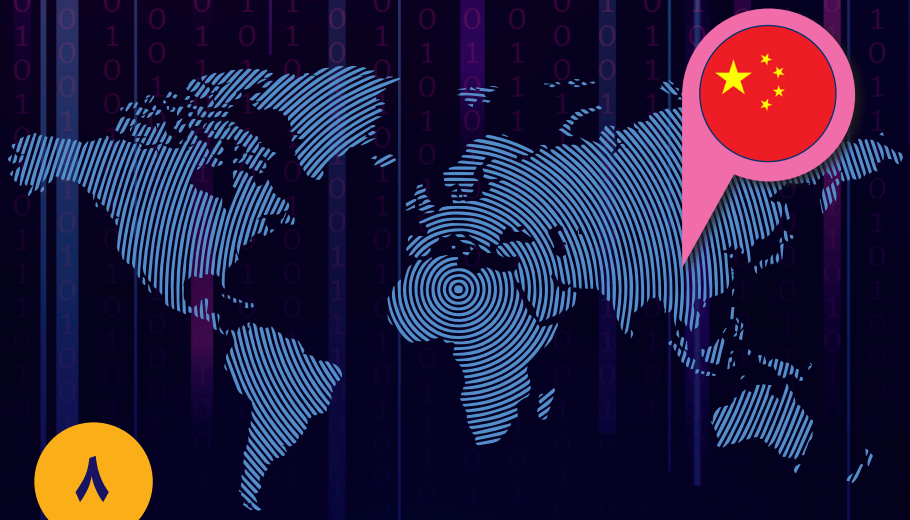
۴. وزارت دفاع ژاپن، رجوع شود:
Defense of Japan 2020, p. 218.

۵. رجوع شود به:
Franz-Stefan Gady and Yuka Koshino, 'Japan and Cyber Capabilities: How Much Is Enough?', Military Balance blog, International Institute for Strategic Studies, 28 August 2020, https://www.iiss.org/blogs/military-balance/2020/08/japancyber-capabilities.

درمجموع، شواهد کنونی نشان می‌دهند ژاپن در زمینه پاسخ تهاجمی به حملات سایبری هنوز به‌طور کامل به ائتلاف با آمریکا وابسته است. لازم به ذکر است که در راهنمای همکاری دفاعی آمریکا و ژاپن (۲۰۱۵) یک بخش کامل به فضای سایبری اختصاص یافته و در آن شرایط کمک آمریکا به ژاپن در دفاع سایبری تعیین شده‌است[۱]. در بدبینانه‌ترین تفسیر از این سند، کمک آمریکا به ژاپن به دفاع از زیرساخت‌های اطلاعاتی حیاتی آن که نیروهای نظامی آمریکا از آن‌ها استفاده می‌کنند، محدود می‌شود. اما در تفسیری دیگر، این سند حتی می‌تواند به‌معنی ماده پنج پیمان ناتو باشد و هرگونه حمله به ژاپن حمله به ناتو تلقی شود.

۱. رجوع شود به:
US Department of Defense, 'The Guidelines for U.S.-Japan Defense Cooperation'.





۸

چین

رهبران چین با جدیت به‌دنبال تحقق انقلاب اطلاعاتی هستند. در دهه نود که چین توسعه فناوری‌های اطلاعاتی را آغاز کرد، این کشور در مقایسه با کشورهای توسعه‌یافته در وضعیت مناسبی نبود، اما به کمک رشد اقتصادی سریع و انتقال فناوری از خارج توانست به‌سرعت پیشرفت کند، به‌طوری‌که اکنون یکی از گسترده‌ترین و قوی‌ترین نظام‌های پایش و سانسور سایبری با نظارت شدید دولتی را بنیان گذاشته‌است. تمایل چین برای تبدیل‌شدن به قدرت سایبری در راهبرد نظامی ۲۰۱۵ و راهبرد امنیت سایبری ۲۰۱۶ آن بازتاب یافته‌است. چین اهداف بلندپروازانه‌ای برای تولید بومی فناوری‌های محوری اینترنت به‌منظور قرارگرفتن در بین پیشگامان این عرصه تا سال ۲۰۳۰ دارد. با این حال، دفاع سایبری چین هنوز در مقایسه با ایالات متحده ضعیف است و سیاست‌های تاب‌آوری سایبری زیرساخت‌های حیاتی آن نیز به‌طور کامل توسعه نیافته‌اند. چین از اوایل دهه ۲۰۰۰ با ایالات متحده و هم‌پیمانانش در حوزه حاکمیت سایبری جهانی در رقابت مداوم است و اخیرا به‌دلیل افزایش رفتارهای خصمانه چین در فضای سایبری، آمریکا با جدیت و خشونت بیشتری به اعمال تحریم علیه شرکت‌های فناوری چینی می‌پردازد. چین سال‌هاست که با هدف کسب حقوق مالکیت فکری، افزایش نفوذ سیاسی، جاسوسی از دولت‌های دیگر و دست بالا داشتن در توانمندی‌های سایبری تهاجمی و مخرب در صورت بروز اختلاف با سایر کشورها، عملیات‌های سایبری گسترده‌ای در خارج از کشور انجام می‌دهد. با توجه به رشد فزاینده بنیان صنعتی چین در فناوری‌های دیجیتال می‌توان گفت این کشور که هم‌اکنون در رده دوم قدرت سایبری قرار دارد به احتمال زیاد در آینده نزدیک به ایالات متحده در رده اول خواهد پیوست.

راهبرد و مبنای نظری (دکترین)

رویکرد راهبردی چین نسبت به جنبه‌های امنیتی فضای سایبری بسیار متاثر از تهدیدهای ایدئولوژیکی، اقتصادی و نظامی از جانب ایالات متحده است و تثبیت زودهنگام مبنای نظری سایبری نظامی آمریکا در دهه نود، استفاده آمریکا از توان سایبری در جنگ کوزوو (۲۰۰۳) و جنگ عراق (۱۹۹۹) و حمایت آن از تحولات سیاسی مبتنی بر فضای اینترنت در کشورهای بلوک شرق اروپا و شمال آفریقا نمونه‌های بارز آن هستند.

از همان سال‌های اول تشکیل جمهوری خلق چین، بیشترین دغدغه راهبردی این کشور مربوط به مسائل داخلی فضای سایبری به‌ویژه جلوگیری از نفوذ افکار لیبرال غربی به کشور ازطریق فضای اینترنت بود. از سال ۲۰۰۳ تاکنون، چین همواره در سازمان ملل از اصل اقتدار سایبری حمایت می‌کند که دال بر داشتن کنترل بیشتر بر بخش ملی اینترنت است. در همین سال چین از پروژه سپر طلایی[1] نیز رونمایی کرد. این برنامه که به دیوار بزرگ آتشین[2] شهرت یافته‌است، همسو با تحقق سیاست کنترل مقتدرانه چین است و امکان نظارت و سانسور سراسری ازطریق فضای اینترنت را برای دولت فراهم می‌کند. در همین راستا، چین از سال ۲۰۰۹ در تلاش است برخی از اپلیکیشن‌های آمریکایی مانند فیس‌بوک، توییتر و یوتیوب را به‌دلیل مغایرت با قوانین سانسور خود محدود کند.

در سال ۲۰۱۳ یعنی ده سال پس از شروع تلاش‌های چین برای اصلاحات نسبی به‌منظور ارتقای توانمندی‌های سایبری کشور، افشاگری‌های ادوارد اسنودن موجب شگفت‌زدگی رهبران حزب کمونیست چین (CCP)[3] از میزان قدرت آمریکا و سطح آسیب‌پذیری چین در برابر آن شد. اطلاعات افشاشده حاکی از آن بود که توانمندی‌های

1. Golden Shield
2. Great Firewall
3. Chinese Communist Party

سـایبری چین از ایالات متحده به‌ویژه در حوزه دفاعی (از نظر دفاع از شـبکه‌ها و نه صرفا کنـترل و نظـارت) فاصلـه زیـادی داشـت. در سـال ۲۰۱۴، رئیس‌جمـهور شـی جین‌پینـگ مجموعـه‌ای از اصلاحـات سـازمانی و قوانیـن و مـقررات جدیـد را بـا هدف تبدیـل چین به قدرتی سایبری تصویب کرد. در همین راستا، سازوکار نهاد اصلی حزب کمونیست چین در حوزه سیاسـت‌های سـایبری[۱] اصلاح شد و نهاد دولتی جدیدی به نام اداره فضای سایبری چین (CAC)[۲] تاسیس شد. به‌دنبال آن، اقدامات و راهبردهای سایبری متعددی در حوزه غیرنظامی نیز اجرا شـد. اولین راهبرد ملی فضای سـایبری چین[۳] در سـال ۲۰۱۶ منتشر شد که با تصویب اولین قانون امنیت سـایبری چین در سـال ۲۰۱۷ تثبیت گردید[۴]. این راهبرد مشـتمل بـر ۹ ماموریت اصلـی بود و تاکید ویژه‌ای بر حفظ اقتـدار و ارتقای عناصر موثر در امنیت سایبری (صنعت و آموزش) داشت[۵].

اجـرای راهبـرد سـاخت چیـن ۲۰۲۵ را می‌تـوان مهم‌تریـن اقـدام چیـن در زمینـه ارتقـای صنعـت برشـمرد کـه در سـال ۲۰۱۵ ارائه شـد. بـا توجه به وابسـتگی زیـاد چین بـه واردات فناوری‌هـای اصلـی اینترنـت که بزرگ‌ترین نقطه‌ضعف آن محسـوب می‌شـود، این راهبرد جاه‌طلبانه قصد دارد تا ۷۰ درصد وابسـتگی واردات چین به فناوری‌های اینترنت را تا سـال

۱. ایـن نهـاد در سـال ۲۰۱۸ بـه یکـی از کمیسیون‌هـای حـزب کمونیسـت چیـن تبدیـل شـد و عنـوان کمیسـیون مـرکزی اطلاعات و امنیت سـایبری (Central Commission for Information and Cyber Security) را گرفت. در زبان انگلیسی از آن اغلـب بـا نـام کمیسـیون مـرکزی امور سـایبری یاد می‌شـود. نهـاد متناظر آن در دولـت اداره فضـای سـایبری چین اسـت کـه نقـش دبیرخانـه ایـن کمیسـیون را دارد.

2. Cyberspace Administration of China

۳. رجوع شود به: اداره فضای سایبری چین، راهبرد ملی امنیت فضای سایبری، ۲۰۱۶
https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy.

۴. رجوع شود به:
Rogier Creemers, Paul Triolo and Graham Webster, 'Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)', New America, 2018,
https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china.

۵. رجوع شود به:
Greg Austin, Cybersecurity in China: The Next Wave (New York: Springer, 2018), p. 8.

۲۰۲۵ کاهش دهد و این کشور را تا سال ۲۰۳۰ در زمره پیشتازان این عرصه قرار دهد. ابتکار یک کمربند یک راه مکمل راهبرد ساخت چین ۲۰۲۵ است که شامل طرحی به نام جاده ابریشم دیجیتال جهت گشودن بازارهای کشورهای درحال‌توسعه به روی فناوری‌های چینی می‌شود.

تمامی این اقدامات منجر به نتایج مثبت زیادی تا سال ۲۰۲۰ شدند که کاهش قابل‌توجه میزان جرائم سایبری داخلی[۱] نمونه بارز آن به شمار می‌آید. با این حال، مشکلات جدی بسیاری نیز مانند افزایش دوبرابری نفوذ به وب‌سایت‌های چینی به‌ویژه پورتال‌های دولتی همچنان وجود داشت[۲]. اجرای راهبرد سایبری چین با چالش‌ها و موانع داخلی متعددی مانند عدم‌توجه کافی به توسعه مهارت‌های امنیت سایبری در نظام آموزشی و موسسات آموزشی روبرو بود[۳]. مهم‌ترین مانع بیرونی نیز ائتلاف ایالات متحده و هم‌پیمانانش علیه چین برای محدودسازی توسعه صنعت سایبری این کشور است که ممنوعیت فروش فناوری ریزتراشه به شرکت هوآوی یکی از بارزترین نمودهای آن به‌شمار می‌رود. پیامدهای چنین اقداماتی هنوز به‌طور کامل مشخص نیست، ولی یکی از اثرات آن می‌تواند تلاش مضاعف چین برای پیشبرد راهبرد ساخت چین ۲۰۲۵ و استفاده از بازار بزرگ داخلی خود (حدود یک میلیارد نفر از چهار و نیم میلیارد کاربر جهانی اینترنت در این کشور هستند) و همچنین گسترش صادرات فناوری‌های چین به کشورهای درحال‌توسعه ازطریق ابتکار یک کمربند یک راه باشد.

---

۱. رجوع شود به: مرکز اطلاعات شبکه اینترنت چین، آمار توسعه اینترنت در چین، آگوست ۲۰۱۹، صص. ۳-۷۲ (گزارش شامل ۶ ماه اول ۲۰۱۹ می‌شود).
https://cnnic.com.cn/IDR/ReportDownloads/201911/P020191112539794960687.pdf.

۲. همان، ص ۷۴.

۳. رجوع شود به:
Greg Austin and Wenze Lu, 'Five Years of Cyber Security Education Reform in China', in Greg Austin (ed.), Cyber Security Education: Principles and Policies (Abingdon: Routledge, 2020).

یکی دیگر از جنبه‌های راهبرد سایبری چین پس از سال ۲۰۰۰، اجرای عملیات‌های سایبری در خارج از کشور به‌منظور اثربخشی راهبردی است. به‌عنوان مثال، این کشور تاکنون عملیات‌های جاسوسی صنعتی بسیاری برای کسب حقوق مالکیت فکری تجاری و دسترسی به اطلاعات شخصی افراد انجام داده‌است. البته چین عملیات‌های سایبری تهاجمی/تخریبی زیادی نیز انجام می‌دهد، اما همواره سعی می‌کند دامنه و شدت آن‌ها در حدی باشد که منجر به اقدامات تلافی‌جویانه شدید نگردد. تلاش برای مداخله در روند انتخابات تایوان از جمله این اقدامات است.

سابقه راهبرد و مبنای نظری چین در زمینه استفاده نظامی از توانمندی‌های سایبری به دهه ۲۰۰۰ برمی‌گردد که راهبرد ۲۰۰۴ مبنی بر «پیروزی در جنگ‌های محلی ازطریق توانمندی‌های اطلاعاتی» از اولین نمونه‌های آن محسوب می‌شود. در این راهبرد به‌کارگیری فناوری اطلاعات در همه ابعاد فعالیت‌های نظامی پیش‌بینی شده و حوزه اطلاعات بخش تفکیک‌ناپذیر همه حوزه‌های زمینی، دریایی و هوایی فعالیت‌های نظامی در نظر گرفته شده‌است. این اصل در سال ۲۰۰۵ مبنای نظری نظامی چین را تغییر داد، به‌طوری‌که از آن پس حفاظت از سامانه‌های اطلاعاتی یا تخریب آن‌ها می‌توانست از روش‌های جنگی ارتش آزادی‌بخش خلق (PLA)[1] باشد.

لازم به ذکر است در مبنای نظری نظامی چین فعالیت‌های مرتبط با شبکه (موضوعی که در دیگر کشورها عملیات‌های سایبری نامیده می‌شود)، از عناصر جنگ اطلاعاتی محسوب می‌شوند[2]. ارتش چین جنگ اطلاعاتی را نوعی نبرد علیه دشمنان

1. People's Liberation Army

به‌منظور کسب اطلاعات بیشتر درباره تغییرات ارتش رجوع شود به:
Greg Austin, 'China's Security in the Information Age', in Lowell Dittmer and Maochun Yu (eds), Routledge Handbook of Chinese Security (Abingdon: Routledge, 2015), pp. 355-70.

۲. رجوع شود به:
Yan Weifeng, Cong Meijun 'konghai yiti zhan' gouxiang kan zhanyi fazhan (Beijing: Haichao Press, 2016), p. 197.

برای کسب برتری در تولید و نشر اطلاعات به‌منظور تحقق اهداف راهبردی می‌داند و تحقق این امر یعنی خنثی‌سازی یا محدودسازی اقدامات دشمنان در این حوزه را «تسلط اطلاعاتی» می‌نامد[۱].

این مفهوم ارتباط نزدیکی با مفهوم چینی دیگری یعنی رویارویی سامانه‌ها دارد که نتیجه تلقی چین از عامل پیروزی ایالات متحده در جنگ اول خلیج‌فارس (۱۹۹۰-۱۹۹۱) ازطریق تخریب سامانه فرماندهی و کنترل عملیات عراق است[۲]. همان طور که در سند علم راهبرد نظامی چین مطرح شده‌است، پیش‌دستی یکی از اصول بنیادین تفکر نظامی این کشور به شمار می‌رود که در جنگ اطلاعاتی اهمیت آن دوچندان می‌شود: آسیب‌پذیری در برابر حمله گسترده به سامانه فرماندهی و کنترل، ضرورت سرعت عمل در فرود آوردن ضربه اول را افزایش می‌دهد[۳].

گستره این تفکر در دوره رئیس‌جمهور شی بیشتر شد. به‌عنوان مثال، در اولین راهبرد نظامی چین (سال ۲۰۱۵) که برای اولین بار فضای سایبری را به سیاست راهبردی و نظامی چین وارد کرد، بر این مساله تاکید شده‌است که اطلاعات صرفا ابزاری توانمندساز نیست

۱. از دیگر مفاهیم متناظر مورداستفاده در ارتش آزادی‌بخش خلق، فضای شبکه‌ای (wangluo kongjian) به‌جای فضای سایبری است. در فرهنگ لغت اصطلاحات نظامی ارتش آزادی‌بخش خلق، جنگ شبکه‌ای عبارت است از عملیات‌هایی که به قصد نابودی سامانه‌های شبکه‌ای و اطلاعات شبکه‌ای دشمن و اختلال در کارکرد آن‌ها ضمن حفاظت از سامانه‌های شبکه‌ای و اطلاعات شبکه‌ای داخلی کشور انجام می‌شوند. رجوع شود به:
Terminology Committee, Academy of Military Sciences, Military Terminology of the People's Liberation Army (Beijing: AMS Publishing, 2011), p. 286.

۲. رجوع شود به:
Dean Cheng, 'Winning Without Fighting: The Chinese Psychological Warfare Challenge', The Heritage Foundation, 12 July 2013, p. 2,
https://www.heritage.org/global-politics/report/winning-without-fighting-the-chinese -psychologicalwarfare-challenge/#_ftn1

۳. رجوع شود به:
Jeffrey Engstrom, 'Systems Confrontation and Systems Destruction Warfare: How the People's Liberation Army Seeks to Wage Modern Warfare', RAND Corporation, 2018, p.10,
https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1708/RAND_RR1708.pdf

و لازم است در تمام فعالیت‌های نظامی نقش محوری داشته باشد[۱]. تا سال ۲۰۱۹، بسیاری از منابع ارتش آزادی‌بخش خلق احتمال می‌دادند تسریع روند تغییرات ارتش و فرصت‌های فناورانه جدید می‌توانند به مسابقه تسلیحاتی برای هوشمندسازی یعنی استفاده از هوش مصنوعی در عملیات‌های نظامی، گردآوری اطلاعات و تصمیم‌گیری منجر شوند[۲].

البته وقوع چنین تغییراتی که در دیدگاه نظامی چین پیش‌بینی شده‌اند، مستلزم گذر زمان زیادی است. چین جدول زمانی ویژه‌ای برای تحقق آرمان‌های خود در زمینه ایجاد ارتشی در کلاس جهانی تا سال ۲۰۵۰ طراحی کرده‌است که طبق آن تا سال ۲۰۳۵ باید اصلاحات سازمانی مانند تغییر در ساختار نیروهای ارتش انجام شوند[۳]. چین نیز همانند ایالات متحده می‌کوشد راهبرد تسلط اطلاعاتی در فضای سایبری را محقق سازد. با این حال، چین به‌خوبی می‌داند که تحقق این هدف مستلزم دگرگونی ساختار نیروهای نظامی آن است.

حکمرانی، فرماندهی و نظارت

از سال ۲۰۱۴، رئیس‌جمهور شی در همه امور فضای سایبری اعم از نظامی و غیرنظامی اختیار تام دارد. تغییرات سازمانی که شی در سیاست سایبری بخش‌های نظامی و غیرنظامی اعمال کرده‌است، تمایل او برای سرعت بخشیدن به روند تغییرات و پیشرفت

۱. رجوع شود به:
China Aerospace Studies Institute, In Their Own Words: Foreign Military Thought - Science of Military Strategy 2013, 8 February 2021, pp. 58, 160-1, 221,
https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2021-02-08%20 Chinese%20Military%20Thoughts-%20In%20their%20own%20words%20Science%20of%20 Military%20Strategy%202013.pdf?ver=NxAWg4BPw_NylEjxaha8Aw%3d%3d

۲. رجوع شود به:
State Council Information Office of the People's Republic of China, 'China's Military Strategy', May 2015, http://eng.mod.gov.cn/Database/WhitePapers/2014.htm.

۳. به عنوان نمونه رجوع شود به:
'Réngōng zhìnéng jūnbèi jìngsài zhèngzài qiǎorán xīngqǐ', China Youth Daily, 17 October 2019, https://m.chinanews.com/wap/detail/zw/gn/2019/10-17/8981224.shtml.

در زمینه کاهش آسیب‌پذیری چین در برابر حملات و نفوذ به شبکه‌ها را نشان می‌دهد. در بخش غیرنظامی، اداره فضای سایبری چین مرجع اصلی در تمام سیاست‌های فضای سایبری کشور است. نهادهای قدرتمند مستقل دیگری نیز در این حوزه حضور دارند که وزارت امنیت عمومی (MPS)[1]، وزارت امنیت کشور (MSS)[2] و وزارت صنعت و فناوری اطلاعات[3] ازجمله این نهادها به شمار می‌آیند. اداره فضای سایبری چین دستورکار جدیدی در قالب مقررات ملی به اجرا گذاشته و دفترهای استانی مختلفی در ۳۱ استان کشور تاسیس کرده‌است.

رئیس‌جمهور شی در سال ۲۰۱۵ نیروی پشتیبانی راهبردی (SSF)[4] را برای رسیدگی به امور سایبری نظامی ایجاد کرد که هم‌اکنون مرکز بیشتر توانمندی‌های سایبری ارتش آزادی‌بخش خلق محسوب می‌شود. درواقع، نیروی پشتیبانی راهبردی واحد جدیدی نیست، بلکه حاصل سازمان‌دهی مجدد نیروهای ارتش آزادی‌بخش چین و ادغام و یکپارچه‌سازی برخی از نیروها در یک واحد فرماندهی مشترک است[5]. در حال حاضر، نیروی پشتیبانی راهبردی دارای دو عنصر اصلی است: واحد سامانه‌های فضایی که مسئولیت عملیات‌های فضایی را برعهده دارد و واحد سامانه‌های شبکه‌ای که مسئولیت عملیات‌های اطلاعاتی راهبردی را برعهده دارد. تشکیل نیروی پشتیبانی راهبردی از این جهت بسیار حائزاهمیت است که تحت عالی‌ترین نهاد تصمیم‌گیری نظامی یعنی کمیسیون مرکزی ارتش فعالیت می‌کند و توانسته‌است همه توانمندی‌های پراکنده در ساختار ارتش را یک‌جا گرد آورد.

1. Ministry of Public Security
2. Ministry of State Security
3. Ministry of Industry and Information Technology
4. Strategic Support Force

۵. رجوع شود به: مقاله مورخ ۲۶ اکتبر ۲۰۱۷ روزنامه شینهوا با عنوان «شی خواستار ساخت ارتش قوی است»، http://www.xinhuanet.com//english/2017-10/26/c_136708142.htm

یکپارچه‌سازی همه کارکردهای سایبری ارتش در نیروی پشتیبانی راهبردی به‌معنی تغییر نگرش و درک جدید ارتش آزادی‌بخش خلق از طیف مفاهیم/کارکردهای فضا، سایبر و الکترومغناطیسی به‌عنوان حوزه‌ای منحصربه‌فرد در عملیات‌های جنگی و نه صرفا ابزاری در خدمت دیگر حوزه‌های جنگی است[1]. کارکرد نیروی پشتیبانی راهبردی برای توانمندی‌های سایبری نظامی چین دو بعد دارد: این نیروی واحد قادر به اجرای عملیات‌های چندبعدی و پیچیده‌ای است که ارتش آزادی‌بخش چین برای نبردهای آینده برنامه‌ریزی می‌کند. به‌عبارت دیگر، تمام فعالیت‌های روانی، سایبری، الکترونیکی و فیزیکی می‌توانند در قالب یک راهبرد جنگی-اطلاعاتی واحد تجمیع شوند تا هریک برای هدفی خاص و در زمانی متفاوت در بحران یا جنگ استفاده شوند[2].

کارکرد دیگر به توان جنگی ارتباط دارد و می‌تواند آمادگی جنگی چین را بهبود بخشد و به تغییر راحت‌تر وضعیت ارتش از صلح به جنگ کمک کند. درواقع، ارتش آزادی‌بخش چین با ترکیب کارکردهای جاسوسی و حمله در واحدهای جنگ فضایی/سایبری و با تجمیع آن‌ها در یک فرماندهی واحد قصد دارد ضمن ارتقای نظارت و پایش میدان نبرد، امکان اجرای عملیات‌های نظامی ترکیبی و دست‌یابی به توانمندی‌های ویژه‌ای متناسب با شرایط/موقعیت‌های مستلزم تصمیم‌گیری و اقدام سریع را فراهم کند[3]. این امر می‌تواند شامل ساخت و توسعه بدافزارها و سایر سلاح‌های سایبری باشد که در عملیات‌های شناسایی/پایش و تهاجمی به‌کار گرفته می‌شوند.

۱. در علم راهبرد نظامی با عنوان قابلیت شناسایی، حمله و دفاع یکپارچه (zhen gongfang yitihua) شناخته می‌شود. رجوع شود به:
Costello and McReynolds, 'China's Strategic Support Force: A Force for a New Era', p. 12.

۲. همان ۴۰

۳. همان ۱-۴۰.

باآنکه واحدهای جنگی/اطلاعاتی راهبردی ارتش آزادی‌بخش چین در نیروی پشتیبانی راهبردی تجمیع شده‌اند، اما هنوز واحدهایی با وظایف و کارکردهای مرتبط با این حوزه وجود دارند که تحت فرماندهی‌های (تازه‌تاسیس) مشترک میدان نبرد[1] انجام وظیفه می‌کنند. البته اطلاعاتی درباره میزان کارایی این واحدها و همچنین میزان هماهنگی ماموریت‌ها و عملیات‌های آن‌ها با نیروی پشتیبانی راهبردی در دست نیست. مطابق یکی از گزارش‌های ارزیابی عملکرد نیروی پشتیبانی راهبردی که توسط ارتش آزادی‌بخش چین منتشر شده‌است، روند اصلاحات و سازماندهی واحدهای ادغام‌شده به‌خوبی در حال اجراست. البته محتوای این گزارش نشان می‌دهند که این تغییرات و اصلاحات هنوز در مراحل اولیه هستند و بنابراین نیروی پشتیبانی راهبردی احتمالا قادر به اجرای موثر عملیات‌های چندبعدی اطلاعاتی جنگی در کوتاه‌مدت یا میان‌مدت نخواهد بود.

توانمندی‌های محوری در زمینه اطلاعات سایبری

چین نهادهای اطلاعاتی خود را متناسب با نظام سیاسی منحصربه‌فرد و نیازهای راهبردی خود سازمان‌دهی کرده‌است. اولویت‌های نهادهای اطلاعاتی چین عبارتند از: حفظ حاکمیت حزب کمونیست چین، نظم عمومی، اطلاعات اقتصادی و سیاسی، اطلاعات فنی و علمی، اطلاعات نظامی و عملیات‌های پنهانی (شامل عملیات‌های نفوذ سیاسی). این اهداف اطلاعاتی توسط سازمان‌های مختلفی تحقق می‌یابند. برخی از این سازمان‌ها شامل نهادهای اطلاعاتی امنیتی تخصصی و مستقلی مانند وزارت امنیت کشور[2] و وزارت امنیت عمومی و نیروی پشتیبانی راهبردی در ارتش آزادی‌بخش خلق هستند. برخلاف نهادهای متناظر در کشورهای غربی، این نهادهای چینی همگی نقش

1. Joint-Theatre Commands

۲. وزارت امنیت کشور نهاد اصلی در حوزه جاسوسی و ضد جاسوسی غیرنظامی است.

عملیاتی قابل‌توجهی در تامین امنیت داخلی دارند و مکمل کار آن‌ها خدمات تحلیلی-اطلاعاتی است که توسط بخش‌های اصلی حزب کمونیست خلق (ازجمله اداره امور تایوان، واحد جبهه متحد، کمیسیون مرکزی امور فضای سایبری[1]، کمیسیون مرکزی سیاست و قانون و کمیسیون مرکزی نظامی[2]) ارائه می‌شوند.

ایجاد قدرتمندترین نظام نظارت/پایش داخلی در چین تاحدی حاصل واکنش آن به سیاست گشودن درهای کشور به روی دنیا ازطریق دسترسی به اینترنت و افزایش انواع مبادلات بین‌المللی است و تا حدی نیز به‌دلیل سیاست‌های خاص نظام حاکم در این کشور است. توانمندی‌های اطلاعاتی داخلی چین نتیجه کار شبکه پیچیده‌ای از سازوکارهای اجرایی و نهادهای امنیتی فوق‌الذکر است که به‌طور موازی با هم کار می‌کنند. کمیسیون مرکزی نظم و بازرسی[3] زیرمجموعه حزب کمونیست چین یکی از مهم‌ترین این سازوکارها است که به جمع‌آوری اطلاعات درباره اعضای حزب می‌پردازد. شبکه کمیته‌های حزب کمونیست چین یکی دیگر از این سازوکارهاست که در همه سطوح دولت، شرکت‌های تجاری بزرگ، بیمارستان‌ها، مدارس و دانشگاه‌ها حضور دارد. علاوه بر این‌ها، پروژه سپر طلایی با استفاده از فناوری اطلاعات و ارتباطات به ارتقای روش جمع‌آوری، تحلیل و انتقال اطلاعات در سازمان‌های امنیتی چین کمک می‌کند. چین ابتکارهای متعدد دیگری نیز برای ارتقای توانمندی‌های نظارتی خود اجرا کرده‌است. شبکه اسکای‌نت[4] که شامل حداقل ۲۰۰ میلیون دوربین در سراسر کشور

۱. رجوع شود به پانوشت ۳.

2. Office for Taiwan Affairs, United Front Department, Central Cyberspace Affairs Commission, Central Commission for Politics and Law and Central Military Commission

3. Central Discipline and Inspection Commission

4. Skynet

برای نظارت تصویری است[۱] و شارپ‌آیز[۲] که زیرمجموعه اسکای‌نت محسوب می‌شود و ویژه پایش مناطق روستایی است و با استفاده از کلان‌داده و هوش مصنوعی کنترل اجتماعی را تقویت می‌کند[۳]، ازجمله این ابتکارها به شمار می‌آیند.

علاوه بر آن‌ها، چین مجهز به سامانه سراسری است که با یکپارچه‌سازی داده‌های بسترهای نظارتی مختلف در خیابان‌ها، بخش‌های خصوصی و دولتی و گزارش‌های دیجیتالی دولت درباره همه شهروندان این فرصت را در اختیار مقامات کشور قرار می‌دهد تا افراد را در لحظه و در همه فضاهای مجازی و واقعی ردیابی کنند. متاسفانه براساس شواهد موجود نمی‌توان اطلاعات زیادی در مورد میزان کارایی یا جامعیت این سامانه کسب کرد.

در عین حال که چین دارای توانمندی بالایی در زمینه اطلاعات سایبری در سطح داخلی است، چین از این توانمندی‌ها برای جاسوسی گسترده در کشورهای خارجی نیز بهره‌برداری می‌کند. با آنکه اقدامات اطلاعاتی چین بیشتر از نظر حجم قابل‌توجه هستند تا سطح تخصص و پیچیدگی، اما گفته می‌شود چین ممکن است پس از افشاگری‌های اسنودن از توانمندی‌های اطلاعاتی کشورهای غربی اقتباس کرده باشد و فعلا از آن‌ها رونمایی نکرده باشد و یا این‌که در حجم سنگین سایر عملیات‌ها-غیرتخصصی-از دید پنهان مانده باشد[۴].

---

۱. رجوع شود به:
Brendon Hong, 'The American Money Behind Blacklisted Chinese AI Companies', Daily Beast, 2 January 2021, https://www.thedailybeast.com/the-american-money-behindblacklisted-chinese-artificial-intelligence-companies

2. Sharp Eyes

۳. رجوع شود به:
Josh Rudolph, 'Sharper Eyes: Surveilling the Surveillers (Part 1)', China Digital Times, 9 September 2019, https://chinadigitaltimes.net/2019/09/sharper-eyes-surveilling-the-surveillers-part-1.

۴. رجوع شود به:
Nicholas Eftimiades, Chinese Intelligence Operations (Abingdon: Routledge, 2017).

تحلیل و انتشار اطلاعات در چین به‌اندازه ایالات متحده و هم‌پیمانان اصلی آن پیشرفته نیست. برخی از مقامات امنیتی معتقدند با آنکه چین حجم عظیمی از داده درنتیجه‌ی نظارت‌های گسترده اطلاعاتی خود در اختیار دارد، اما امکان بهره‌برداری موثر از آن‌ها به‌دلیل محیط اطلاعاتی به‌شدت سیاست‌زده این کشور وجود ندارد. ماهیت زیست‌بوم اطلاعات چین از نظر نهادی و فرهنگ سازمانی بسته و سرکوب‌گر است و این ویژگی با پویش گسترده و خشن ضدفساد رئیس‌جمهور شی از سال ۲۰۱۲ شدیدتر نیز شده‌است. پاکسازی هزاران نفر از مقامات سازمان‌های امنیتی و اطلاعاتی چین حتی در سطوح بالا یکی از نتایج این پویش محسوب می‌شود. به‌طور کلی، نظام تحلیل اطلاعات در چین با کشورهای غربی بسیار تفاوت دارد و به‌دلیل ایدئولوژی‌محور بودن به‌شدت تحت‌تاثیر نفوذ سیاسی است.

توانمندی و وابستگی سایبری

مشارکت چین در صنعت جهانی فناوری اطلاعات و ارتباطات از سال ۱۹۸۴ آغاز شد و با کمک شرکت‌های مستقر در ایالات متحده (مانند موتورولا و مایکروسافت) به شکوفایی رسید. اقدامات رئیس‌جمهور سابق جیانگ زِمین[1] که بر تحول صنعتی ازطریق فناوری الکترونیک و فناوری اطلاعات تاکید داشت را می‌توان یکی از عوامل اصلی توسعه این بخش برشمرد. تلاش‌های جیانگ برای توسعه مبتنی بر فناوری اطلاعات موجب ترویج این تفکر در چین شد که جامعه اطلاعاتی پدیده‌ای همه‌شمول و ضامن امنیت و رونق کشور در آینده است[2]. در آن زمان (دهه نود تا ۲۰۰۰)، بخش خصوصی نوپای چین

1. Jiang Zemin

۲. رجوع شود به:

Greg Austin, Cyber Policy in China (Cambridge: Polity, 2014), p. 1.

نقش موثری در توسعه فناوری دیجیتال داشت. به‌عنوان مثال، شرکت علی‌بابا[1] در سال ۱۹۹۹ آغاز به کار کرد و لِنوو[2] در سال ۲۰۰۵ با خریداری یکی از شرکت‌های زیرمجموعه غول فناوری آی‌بی‌اِم به رشد چشمگیری دست یافت. به‌همین‌ترتیب، رهبران چین پس از جیانگ نیز راه او را ادامه دادند و در دوره شی دو پیشرفت مهم رخ داد: در سال ۲۰۱۴ دولت به‌طور رسمی هدف مبنی بر تبدیل شدن به قدرت سایبری را اعلام کرد و در سال ۲۰۱۵ نیز از راهبرد صنعتی ساخت چین ۲۰۲۵ رونمایی شد.

طبق اظهارات دولت چین در یکی از گزارش‌های رسمی در سال ۲۰۲۰، این کشور دوره توسعه سریع صنعت بومی فناوری اطلاعات و ارتباطات را پشت سر گذاشته و وارد مرحله دیجیتال‌سازی فراگیر جامعه و اقتصاد شده‌است[3]. علاوه بر این گزارش دولتی، صندوق بین‌المللی پول نیز در گزارش خود به جایگاه پیشتاز چین در تجارت الکترونیک و برخی از حوزه‌های فناوری مالی (فین‌تک) اشاره کرده و چین را دارای سریع‌ترین نرخ دیجیتال‌سازی معرفی کرده‌است[4]. ارزش افزوده اقتصاد دیجیتال چین در سال ۲۰۱۹ بالغ بر ۳۵/۸ تریلیون یوان (معادل ۵/۱۲ تریلیون دلار) بود که حدود ۳۶/۲ درصد از تولید ناخالص داخلی را دربرمی‌گرفت. اگرچه این رقم بیشتر از کشورهای برزیل، هند و آفریقای جنوبی بود، اما از ایالات متحده (۵۰ درصد) کمتر بود[5]. ارزش تخمینی بخش فناوری

1. Alibaba
2. Lenovo

۳. رجوع شود به:
China Academy of Information and Communications Technology, 'Zhōngguó shùzì jīngjì fāzhǎn báipíshū', May-July 2020, pp. 49-50, http://www.caict.ac.cn/kxyj/qwfb/bps/202007/P020200703318256637020.pdf.

۴. رجوع شود به:
Tahsin Saadi Sedik, 'Asia's Digital Revolution', Finance & Development, vol. 55, no. 3, September 2018, https://www.imf.org/external/pubs/ft/fandd/2018/09/asia-digital-revolution-sedik.htm.

۵. رجوع شود به:
China Academy of Information and Communications Technology, 'Zhōngguó shùzì jīngjì fāzhǎn báipíshū', p. 8.

اطلاعات و ارتباطات چین نیز در سال ۲۰۱۹ معادل ۷/۱ تریلیون یوان (یا ۱/۰۲ تریلیون دلار) بود که تنها ۷ درصد از تولید ناخالص داخلی آن را تشکیل می‌داد.

چین به‌دلیل توسعه‌یافتگی بسترهای برخط خود توانسته‌است در اقتصاد جهانی فناوری اطلاعات و ارتباطات نفوذ قابل‌توجهی داشته باشد. به‌نقل از آکادمی فناوری اطلاعات و ارتباطات چین، این کشور در بخش بسترهای برخط با سرگروهی شرکت‌های علی‌بابا و تنسنت[1] توانسته‌است از سطح تقلید به سطح پیشتازی در نوآوری جهانی ارتقا یابد[2]. به‌عنوان مثال، قبل از این‌که ایالات متحده در سال ۲۰۲۰ به مقابله با چین برخیزد، شرکت چینی تیک‌تاک[3] توانست در عرصه ویدئوهای کوتاه انقلابی جهانی برپا کند.

با وجود سیاست ساخت چین ۲۰۲۵ و تاکید همیشگی دولت از آغاز تشکیل جمهوری خلق چین بر توسعه علم و فناوری بومی، وابستگی روزافزون این کشور به فروشندگان خارجی برای تامین فناوری‌های اصلی اینترنت بزرگ‌ترین مانع رشد سایبری آن به‌شمار می‌آید. رسانه‌های چینی عبارت «هشت جنگجوی نگهبان» را برای شرکت‌های آمریکایی تامین‌کننده زیرساخت‌های مخابراتی چین ابداع کرده‌اند[4]: اپل، سیسکو، گوگل، آی‌بی‌ام، اینتل، مایکروسافت، اُراکل و کوالکوم[5]. این امر بر عمق وابستگی چین به این شرکت‌ها دلالت دارد.

درواقع، دولت چین می‌داند وابستگی آن به شرکت‌های فناوری خارجی بلندمدت خواهد بود و به همین علت از برخی از آن‌ها مانند مایکروسافت، اینتل و آی‌بی‌ام دعوت

1. Tencent

۲. همان ص ۲۷. در فهرست ۵۰۰ شرکت برتر جهانی فورچون (۲۰۲۰)، شرکت‌های علی‌بابا و تنسنت به‌ترتیب رتبه‌های ۱۳۲ و ۱۹۷ را به خود اختصاص داده‌اند.

3. TikTok

۴. رجوع شود به:
Shannon Tiezzi, 'New Report Highlights China's Cybersecurity Nightmare', Diplomat, 18 February 2015, https://thediplomat.com/2015/02/new-report-highlights-chinas-cybersecurity-nightmare

5. Apple, Cisco, Google, IBM, Intel, Microsoft, Oracle and Qualcomm

کرده‌است تا در زمینه تهیه استانداردهای ملی امنیت سایبری با مراجع چینی همکاری کنند. بدین‌ترتیب، چین خواهد توانست نظارت بهتری بر استفاده از فناوری‌های آمریکایی در شبکه‌های خود داشته باشد. علاوه بر این، چین علی‌رغم همه تلاش‌های خود برای مستقل شدن از سیستم عامل ویندوز (شرکت مایکروسافت)، هنوز تا ساخت سیستم عامل بومی که بتواند جایگزین اپل و مایکروسافت شود، راه طولانی در پیش دارد[۱].

هوش مصنوعی یکی از حوزه‌های اولویت‌دار در دولت شی است و در سال ۲۰۱۷ اولین راهبرد توسعه ویژه هوش مصنوعی را با هدف پیشگامی در این عرصه تا سال ۲۰۳۰ به اجرا گذاشت[۲]. در خلاصه چهاردهمین برنامه پنج‌ساله توسعه (۲۰۲۵-۲۰۲۰) چین نیز هوش مصنوعی در فهرست فناوری‌های راهبردی و آینده‌نگر مانند مخابرات کوانتوم و مهندسی زیستی قرار دارد که باید به‌طور ویژه توسعه یابند[۳]. با آنکه شرکت‌های چینی در برخی حوزه‌ها مانند تشخیص چهره پیشرو هستند، اما در اغلب حوزه‌های دیگر از شرکت‌هایی مانند گوگل و مایکروسافت فاصله بسیار دارند. آمریکا کماکان در توسعه بسترها و معماری پشتیبان هوش مصنوعی پیشتاز است و چین در بسیاری از این حوزه‌ها از آن عقب‌تر است. به‌عنوان مثال، چین دارای سهم ۱۳ درصدی از نرم‌افزارهای

۱. رجوع شود به:
Davey Winder, 'China Prepares to Drop Microsoft Windows, Blames US Hacking Threat', Forbes, 30 May 2019, https://www.forbes.com/sites/daveywinder/2019/05/30/chinaprepares-to-drop-microsoft- windows-blames-u-s-hackingthreat/?sh=d0a00282c50d

۲. رجوع شود به:
State Council of the People's Republic of China, 'Notice of the State Council Issuing the New Generation of Artificial Intelligence Development Plan', State Council Document no. 35, 8 July 2017, https://flia.org/wp-content/uploads/2017/07/A-NewGeneration-of-Artificial-Intelligence- Development-Plan-1.pdf.

۳. رجوع شود به:
Matt Ho, 'China's Hi-Tech Direction for the next Five Years', South China Morning Post, 11 November 2020, https://www.scmp.com/news/china/politics/article/3109316/chinas-hi-techdirection-next-five-years

منبع‌باز هوش مصنوعی است، حال آنکه این رقم برای ایالات متحده ۶۶ درصد است[۱]. همچنین، میزان سرمایه‌گذاری بخش خصوصی چین در هوش مصنوعی در مقایسه با آمریکا که دوسوم کل سرمایه‌گذاری جهان را در سال ۲۰۱۱ در اختیار داشت، بسیار اندک است[۲]. البته چین بعد از ایالات متحده رتبه دوم را در رتبه‌بندی ۲۰۲۰ از نظر مشارکت در دو کنفرانس معتبر هوش مصنوعی به خود اختصاص داده‌است[۳]. در حوزه محاسبات کوانتومی نیز چین وضعیت خوبی دارد: این کشور در سال ۲۰۱۷ موفق به ساخت رایانه‌ای ده کیوبیتی شد که رکورد رایانه نه کیوبیتی گوگل را شکست. البته گوگل و آی‌بی‌ام موفق به ساخت نمونه‌های ۵۴ کیوبیتی در سال ۲۰۱۹ شدند. با این حال، چین هنوز در عرصه تحقیق و توسعه مخابرات کوانتوم پیشتاز است و توانسته‌است بلندترین کابل مخابراتی کوانتومی (۲۰۰۰ کیلومتر) را بین پکن و شانگهای نصب کند و ارتباط ماهواره‌ای را در منطقه کوچک‌تری نیز برقرار کرده‌است[۴]. محققان چینی در سال ۲۰۲۱ اعلام کردند موفق به ساخت شبکه مخابراتی کوانتومی به طول ۴,۶۰۰ کیلومتر

۱. رجوع شود به:
Jeffrey Ding, 'China's Current Capabilities, Policies and Industrial Ecosystem in AI - Testimony before the U.S.-China Economic and Security Review Commission Hearing on Technology, Trade, and Military-Civil Fusion: China's Pursuit of Artificial Intelligence, New Materials, and New Energy', US-China Economic and Security Review Commission, 7 June 2019, p. 4,
https://www.uscc.gov/sites/default/files/June%207%20Hearing_Panel%201_Jeffrey%20Ding_China's%20Current%20Capabilities,%20Policies,%20and%20Industrial%20Ecosystem%20in%20AI.pdf.

۲. همان، ص ۴۰.

۳. رجوع شود به:
Gleb Chuvpilo, 'AI Research Rankings 2020: Can the United States Stay Ahead of China?', 21 December 2020, https://chuvpilo.medium.com/ai-research-rankings-2020-can-theunited-states-stay-ahead-of-china-61cf14b1216.

۴. رجوع شود به:
Priyankar Bhunia, 'World's longest unhackable communications link opened between Beijing and Shanghai', OpenGovAsia, 28 October 2017,
https://opengovasia.com/worlds-longest-unhackable-communications-link-openedbetween-beijing-and-shanghai

شـده‌اند که پس از دو سـال عملیات آزمایشی آماده استفاده خواهد بود[۱].

افزون بر این‌ها، سـطح توسـعه‌یافتگی توانمندی‌های سایبری مبتنی بر فضای چین مطلـوب اسـت. ایـن کشور ۴۱۰ ماهـواره در نـاوگان فضایی خـود دارد[۲] و به‌مـدد ناوگانی بـا ۱۳۲ ماهـواره تخصصـی نظامـی که دومیـن ناوگان بزرگ دنیـا بعد از آمریکاسـت، توان بـالایی در اجـرای عملیات‌هـای اطلاعاتـی، نظارتـی و شناسـایی (ISR) دارد[۳]. طبق گزارش سازمان اطلاعات دفاعی آمریکا در سال ۲۰۱۹، ماهواره‌های اطلاعاتی، نظارتی و شناسایی چیـن قابلیـت تصویربرداری الکتریکـی/نوری و رادار دهانه ترکیبی (سـار)[۴] و نیز گردآوری داده الکترونیـک و سیگنالـی را دارنـد[۵]. به‌عنوان نمونه می‌توان بـه ناوگان[۶] ماهواره‌های دوکاره یائوگان[۷] و ماهواره‌های اقیانوسی هایانگ[۸] اشاره کرد که برای شناسایی و ردیابی شـناورهای نظامی و غیرنظامی به کار می‌روند[۹].

---

۱. رجوع شود به:
Liu Zhen, 'China's experiment in quantum communicationbrings Beijing closer to creating a hack-proof network', South China Morning Post, 9 January 2021, https://www.scmp.com/news/china/science/article/3117005/chinas-experimentquantum-communication-brings-beijing-closer.

۲. رجوع شود به:
Union of Concerned Scientists, 'UCS Satellite Database', updated 1 January 2021, https://www.ucsusa.org/resources/satellite-database

۳. رجوع شود به:
IISS, The Military Balance 2021 (Abingdon: Routledge for the IISS, 2021), pp. 48, 191, 250.

4. Synthetic Aperture Radar (SAR)

۵. رجوع شود به:
Defense Intelligence Agency, 'Challenges to Security in Space', January 2019, https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf

۶. رجوع شود به:
Andrew Tate, 'China integrates long-range surveillance capabilities', Jane's Intelligence Review, vol. 29, no. 12, December 2017. See also Timothy Heath, 'China's Pursuit of Overseas Security', RAND Corporation, 2018, p. 30, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2271/RAND_RR2271.pdf.

7. Dual-use Yaogan satellite

8. Haiyang series

۹. رجوع شود به:
'Haiyang-2 (HY-2 or Ocean-2)', Globalsecurity.org, https://www.globalsecurity.org/space/world/china/hy-2.htm

چین با ساخت سامانه ناوبری ماهواره‌ای بیدو[1] توانسته‌است در زمینه هدایت موشک نیز به خودکفایی برسد و دیگر وابسته به فناوری آمریکایی جی‌پی‌اس نباشد. شبکه بیدو توانسته‌است در سال ۲۰۱۲ منطقه آسیا و اقیانوسیه و در اواسط سال ۲۰۲۰ همه دنیا را پوشش دهد. تحلیل‌گران نظامی چین اذعان دارند باتوجه به این‌که چین همانند ایالات متحده وابستگی زیادی به توانمندی‌های فضایی و سایبری دارد، نقاط ضعف مشابهی نیز در صورت بروز منازعه خواهد داشت[2].

درمجموع باید خاطرنشان ساخت که با آنکه چین به پیشرفت‌های زیادی در توانمندی‌های سایبری محوری دست یافته‌است، اما همان‌طور که جنگ تجاری چین و آمریکا در زمان ترامپ نشان داد، این کشور همچنان در بسیاری از فناوری‌های اصلی اینترنت به آمریکا وابسته است. چین دارای مزیت‌های متعددی ازجمله بازار داخلی بزرگ است که سود فراوانی در بازار دیجیتال نصیب آن می‌کند. اما طبق اعتراف شی در اظهارات خود در سال ۲۰۱۹، چین راهی طولانی در پیش دارد[3] و در مقابله با چالش‌های آمریکا باید زمان و انرژی زیادی صرف کند.

1. Beidou

۲. رجوع شود به:
Kevin L. Pollpeter, Michael S. Chase and Eric Heginbotham, 'The Creation of the PLA Strategic Support Force and its Implications for Chinese Military Space Operations', RAND Corporation, 2017, p. 7, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2058/RAND_ RR2058.pdf

3. Long March

رجوع شود به:
'China's Xi Jinping warns of new 'long march' as trade war with US intensifies', Straits Times, 22 May 2019,
https://www.straitstimes.com/asia/east-asia/chinese-president-xi-jinpingwarns-of-new-long-march-as-trade-war-intensifies

امنیت و تاب‌آوری سایبری

اگرچه امنیت اطلاعات از دهه نود تاکنون از اولویت‌های دولت چین بوده، اما تمرکز اصلی آن همواره بر امنیت محتوا و به‌عبارت دیگر، سانسور اطلاعات سیاسی در فضای سایبری بوده‌است. این رویکرد بازتاب سیاست‌های ایدئولوژی‌محور حزب حاکم است که همواره خود را در معرض تهدید می‌بیند[۱]. به نظر می‌رسد تمرکز بر امنیت محتوا و تحقق اهداف سانسور موجب دور افتادن چین از توسعه سایر توانمندی‌های امنیتی در حوزه شبکه شده‌است و این ضعف همچنان ادامه دارد.

رویکرد چین نسبت به امنیت شبکه تحت‌تاثیر زنجیره‌ای از اتفاقات در سال‌های اخیر تا حدی تغییر یافته‌است. پس از افشاگری اسنودن در سال ۲۰۱۳، چین باید با این واقعیت تحقیرآمیز روبرو می‌شد که واحد جاسوسی سایبری (واحد ۶۱۳۹۸) ارتش آزادی‌بخش چین توسط شرکت آمریکایی ماندیانت[۲] شناسایی شده‌بود. این رویداد شکاف عمیق امنیت سایبری در ارتش چین را آشکار ساخت. در همان زمان، برملا شدن ماجرای استراق سمع از رهبران ارشد چین به دستور یکی از افسران امنیت داخلی این کشور (سال ۲۰۱۲)، آسیب‌پذیری حاکمیت و خطر جاسوسی خارج از کنترل دولت مرکزی را گوشزد می‌کرد[۳].

تیم فنی ملی پاسخ فوری شبکه رایانه‌ای (CNCERT)[۴] نیز در گزارش خود در سال ۲۰۱۷، حمله از سوی کشورهای خارجی را بسیار متداول و حتی عادی توصیف می‌کرد و

---

۱. رجوع شود به:
Elliott Zaagman, 'Cyber Sovereignty and the PRC's Vision for Global Internet Governance', China Brief, vol. 18, no. 10, 5 June 2018, https://jamestown.org/program/cyber-sovereigntyand-the-prcs-vision-for-global-internet-governance.

2. Mandiant

۳. رجوع شود به:
Roger Faligot, Chinese Spies: From Chairman Mao to Xi Jinping (Melbourne: Scribe, 2019), p. 395.

4. National Computer Network Emergency Response Technical Team

آن را تهدیدی برای امنیت ملی می‌دانست. این گزارش با اشاره به صدمات جدید به داده‌ها و فراوانی جرائم، تعداد حملات به سامانه‌های کنترل صنعتی-که برخی از آن‌ها بسیار جدی و بااهمیت نیز بودند-را روبه‌رشد نشان می‌داد[۱]. اگرچه گزارش شش‌ماهه مرکز اطلاعات شبکه اینترنت چین در سال ۲۰۲۰ دال بر افزایش امنیت سایبری شخصی به‌ویژه در زمینه جرائم برخط بود، ولی طبق داده‌های آن وضعیت کلی امنیت سایبری کشور سیر نزولی داشت[۲]. براساس این گزارش، تعداد وب‌سایت‌های قربانی حمله‌های سایبری افزایش یافته‌بود و برخی از آن‌ها آلوده به بدافزارهایی از نوع درب پشتی (بک‌دور) شده‌بودند[۳]. علاوه بر این، میزان آسیب‌پذیری سیستم‌های در معرض خطر بالا نیز دوبرابر شده‌بود[۴].

تعداد زیاد سازمان‌ها، قوانین، مقررات و دستورات جدیدی که از سال ۲۰۱۴ عملیاتی شده‌اند بیانگر این است که چین هنوز در مراحل ابتدایی ساخت تاب‌آوری سایبری و ارتقای آمادگی سایبری قرار دارد. دولت، صنعت و دانشگاه‌های چین تعاملات نهادی خود را از سال ۲۰۱۶ با تشکیل انجمن امنیت سایبری افزایش داده‌اند و همین امر موجب ارتقای هماهنگی آن‌ها حول اهداف مشترک شده‌است[۵]. افزون بر این، پکن در سال ۲۰۱۶ اصلاحاتی را در ساختار کمیته فنی ملی استانداردسازی امنیت اطلاعات

۱. رجوع شود به:
China National Computer Network Emergency Response Team, '2016 Nián wǒguó hùliánwǎng wǎngluò ānquán tàishì zòngshù', National Computer Network Emergency Technology Processing Coordination Center, April 2017, pp. 14-20,
http://www.cac.gov.cn/wxb_pdf/CNCERT2017/2016situation.pdf

۲. همان، ص ۱۵.

۳. بک‌دور (Backdoor): نوعی بدافزار که با دور زدن سیستم امنیتی رایانه‌ها امکان دسترسی به اطلاعات یا نصب بدافزارها را به‌صورت پنهانی فراهم می‌کند. رجوع شود به:
China Internet Network Information Center, 'Statistical Report on Internet Development in China', September 2020, p. 69,
https://cnnic.com.cn/IDR/ReportDownloads/202012/P020201201530023411644.pdf.

۴. همان، صص ۲-۷۰.

۵. همان، ص ۷۳.

(NISSTC)[1] اعمال کرد که موجب مشارکت نمایندگانی از دولت، صدها شرکت چینی و تعدادی از شرکت‌های خارجی در آن شد. کمیته مذکور تا سال ۲۰۱۸ موفق شد ۳۰۰ استاندارد جدید امنیت سایبری را در زمینه حفاظت از زیرساخت‌های حیاتی اطلاعاتی، بررسی محصول و غیره منتشر کند[2]. در دسامبر ۲۰۱۹ نیز طرح حفاظت چندسطحی ۲ (MLPS ۲٫۰)[3] اجرا شد که ضمن افزودن دامنه مقررات اپراتورهای شبکه، الزامات تنظیم‌گری را هم افزایش داد[4]. چین به‌منظور تقویت امنیت زیرساخت‌های حیاتی اطلاعاتی خود سند اقدامات ارزیابی امنیت سایبری[5] را در سال ۲۰۲۰ منتشر کرد که مشتمل بر مجموعه‌ای از قوانین جهت مدیریت ارزیابی امنیت و قابلیت‌اطمینان زنجیره عرضه محصولات و خدمات مورداستفاده اپراتورهای زیرساخت‌ها بود[6]. دولت در جولای ۲۰۲۰ و اکتبر ۲۰۲۰ نیز به‌ترتیب پیش‌نویس قانون امنیت داده[7] و پیش‌نویس

1. National Information Security Standardization Technical Committee

۲. رجوع شود به:
Samm Sacks and Robert O'Brien, 'What to Make of the Newly Established Cybersecurity Association of China', Center for Strategic and International Studies, 25 May 2016,
https://www.csis.org/analysis/what-make-newly-establishedcybersecurity-association-china.

3. Multi-level Protection Scheme

۴. رجوع شود به:
Dora Wang, Charmian Aw and Cindy Shen, 'MLPS 2.0: China's Enhanced Data Security Multi-Level Protection Scheme and Related Enforcement Updates', ReedSmith, 9 October 2019,
https://www.reedsmith.com/en/perspectives/2019/10/mlps-20-chinas-enhanced-data-security-multi-level-protection.

5. Cybersecurity Review Measures

۶. رجوع شود به:
Lauren Dudley et al., 'China's Cybersecurity Reviews Eye "Supply Chain Security" in "Critical" Industries [Translation]', New America, 27 April 2020,
http://newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurityreviews-eye-supply-chain-security-critical-industries-translation;
Samm Sacks and Manyi Kathy Li, 'How Chinese Cybersecurity Standards Impact Doing Business in China', CSIS, 2 August 2018,
https://www.csis.org/analysis/how-chinesecybersecurity-standards-impact-doing-business-china.

۷. رجوع شود به:
Emma Rafaelof et al., 'Translation: China's Data Security Law (Draft)', New America, 2 July 2020,
http://newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-data-security-law-draft.

قانون حفاظت از اطلاعات شخصی را منتشر کرد که درواقع، اولین مقررات جامع چین در حوزه امنیت داده شخصی محسوب می‌شوند[۱].

صنعت امنیت سایبری چین بسیار کوچک‌تر از ایالات متحده است. طبق اطلاعات انجمن امنیت سایبری چین، کل درآمد این صنعت در سال ۲۰۱۹ بالغ بر ۵۲/۰۹ میلیارد یوان (۸/۰۹ میلیارد دلار)[۲] یعنی کمتر از ۷ درصد از صنعت جهانی امنیت سایبری بود[۳]. در مقایسه با آمریکا، شرکت‌های اصلی امنیت سایبری چین درآمد کمتری دارند و درنتیجه، حضور جهانی آن‌ها کمرنگ‌تر است. به‌عنوان نمونه، شرکت‌های سیسکو سیستمز، پالوآلتو نت‌ورکس و فورتینت[۴] در سه‌ماهه اول ۲۰۲۰ به‌ترتیب ۹/۱، ۷/۸ و ۵/۹ درصد از بازار جهانی را در اختیار داشتند[۵] و کل سهم آمریکا از بازار جهانی حدود ۴۰ درصد بود[۶].

---

۱. رجوع شود به:
Bryan Cave, 'China's Draft Personal Information Protection, Law: What Businesses Should Know', Lexology, 2 December 2020,
https://www.lexology.com/library/detail.aspx?g=f7f7b85c-545a-4fbe-a114-833044603750

۲. این رقم مربوط به درآمد شرکت‌هایی است که حداقل ۵۰ درصد کل درآمد آن‌ها از فروش محصولات و خدمات این بخش به‌دست می‌آید. با توجه به اینکه داده‌های این گزارش از حدود ۵۰۰ شرکت امنیت سایبری گردآوری شده‌است، محاسبات آن در مقایسه با سایر تخمین‌های موجود قابل‌اعتماد است. رجوع شود به:
Cybersecurity Association of China (CAICT), '2020 Nián zhōngguó wǎngluò ānquán chǎnyè tǒngjì bàogà', p.8,
https://www.cybersac.cn/News/getNewsDetail/id/1545

۳. رجوع شود به:
Gartner, 'Gartner Forecasts Worldwide Security and Risk Management Spending Growth to Slow but Remain Positive in 2020', 17 June 2020,
https://www.gartner.com/en/newsroom/press-releases/2020-06-17-gartner-forecasts-worldwidesecurity-and-risk-managem.

4. Cisco Systems, Palo Alto Networks and Fortinet

۵. رجوع شود به:
Statista, 'Leading cybersecurity vendors by market share worldwide from 2017 to 2020', 2 July 2020,
https://www.statista.com/statistics/991308/worldwide-cybersecurity-top-companies-bymarket-share

۶. همان.

چین در شاخص جهانی امنیت سایبری ۲۰۱۸ موفق به کسب رتبه ۲۷ در میان ۱۷۵ کشور جهان شد[۱]. با توجه به توسعه محدود مجموعه صنعت سایبری چین یعنی شرکت‌ها، محققان و سرمایه‌گذاران تاثیرگذار در طراحی و ساخت فناوری‌های امنیت سایبری می‌توان گفت این کشور ظرفیت زیادی برای بهبود امنیت سایبری در کوتاه‌مدت تا میان‌مدت ندارد. افزون بر آن، آموزش و پژوهش امنیت سایبری در چین هنوز در سطح ابتدایی است و رتبه‌بندی انجمن فارغ‌التحصیلان دانشگاهی چین[۲] در سال ۲۰۱۹ حاکی از آن است که هیچ‌یک از دانشگاه‌های این کشور در گروه دانشگاه‌های در کلاس جهانی قرار ندارند[۳].

رهبری جهانی در عرصه سایبری

از سال ۲۰۰۲ تاکنون، چین در سازمان‌های بین‌المللی مختلف مانند سازمان ملل و اتحادیه بین‌المللی مخابرات (ITU) در زمینه تهیه مقررات و هنجارهای جدید بین‌المللی در حوزه رفتار در فضای سایبری با هدف تشدید سانسور دولتی و افزایش اقتدار و استقلال در عرصه سایبری با کشورهای هم‌فکر (مانند روسیه و اعضای سازمان همکاری شانگهای) همکاری می‌کند[۴]. حداقل از سال ۲۰۱۰ که هیلاری کلینتون وزیر وقت امور

۱. رجوع شود به:
International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 63, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

2. Chinese University Alumni Association

۳. رجوع شود به:
Austin and Lu, 'Five Years of Cyber Security Education Reform in China'.

۴. اطلاعات بیشتر درباره میزان مشارکت چین در تعیین هنجارهای جهانی پایگاه‌های داده در منبع زیر یافت می‌شود:
Greg Austin, 'International legal norms in cyberspace: Evolution of China's national security motivations', in Anna Maria Osula and Henry Roigas (eds), International Cyber Norms: Legal, Policy & Industry Perspectives (Tallinn: NATO CCDCOE Publications, 2016), pp. 172-201.

خارجه ایالات متحده سخنرانی درباره آزادی اینترنت ایراد کرد، چین دریافت که شکاف ایدئولوژیکی عمیقی با کشورهای غربی از نظر حقوق بشر، جنبه‌های امنیتی و هنجارهای فضای سایبری دارد[۱].

چین در موارد معدودی با جامعه بین‌المللی توافق دارد. به‌عنوان مثال، نماینده چین در گروه کارشناسان دولتی سازمان ملل[۲] در سال ۲۰۱۳ از توافق جمعی درباره قانون بین‌المللی مرتبط با فضای سایبری حمایت کرد و یا در سال ۲۰۱۵ با نظر جمعی درباره تعیین هنجارهای داوطلبانه برای فضای سایبری موافقت کرد. اما باتوجه به این‌که چین می‌دانست روند کارگروه کارشناسان دولتی متناسب با اهداف آن نیست، به جمع کشورهایی پیوست که طرفدار ایجاد کارگروه پایان باز (OEWG)[۳] بودند. کارگروه پایان باز با هدف کاهش نفوذ کشورهای غربی و فراهم کردن فرصت حضور بی‌پروای همه کشورها در فرایندهای موردحمایت سازمان ملل در سال ۲۰۱۸ تشکیل شد[۴] و فعالیت خود را در سال ۲۰۱۹ به‌طور رسمی آغاز کرد.

اختلاف چین با اجماع عمومی در نشست‌های سازمان ملل درباره هنجارهای فضای سایبری، در فعالیت‌های دیپلماتیک آن درباره ترویج نوعی دستورکار جهانی برای

۱. رجوع شود به:
US Department of State, 'Remarks on Internet Freedom', Hillary Rodham Clinton, Secretary of State, Washington DC, 21 January 2010,
https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

۲. رجوع شود به:
UN Office for Disarmament Affairs, 'Developments in the field of information and telecommunications in the context of international security',
https://www.un.org/disarmament/ict-security.

3. Open-Ended Working Group

۴. قطعنامه مجمع عمومی سازمان ملل در ۵ دسامبر ۲۰۱۸: پیشرفت‌های حوزه اطلاعات و مخابرات از منظر امنیت بین‌المللی، قطعنامه ۷۳/۲۷، ۱۱ دسامبر ۲۰۱۸ https://undocs.org/en/A/RES/73/27. نام کامل این کارگروه عبارت است از: کارگروه پایان باز درباره پیشرفت‌های حوزه اطلاعات و مخابرات از منظر امنیت بین‌المللی. برای کسب جزئیات بیشتر رجوع شود به:
United Nations Office for Disarmament Affairs, 'Open-ended Working Group',
https://www.un.org/disarmament/open-ended-working-group.

حکمرانی اینترنت که با منافع این کشور سازگاری بیشتری دارد نیز نمود یافته‌است. چین اولین گام در این راستا را در سال ۲۰۱۴ برداشت یعنی زمانی که در پاسخ به مجموعه کنفرانس‌های حکمرانی اینترنت که در سال ۲۰۱۱ توسط بریتانیا و هم‌فکرانش در لندن بنیان‌گذاری شد، اجلاس اینترنت ووژن[1] را برگزار کرد.

وزارت امور خارجه و اداره اطلاعات اینترنتی دولتی چین نیز به‌طور مشترک چشم‌انداز راهبرد بین‌المللی همکاری در فضای سایبری[2] را در سال ۲۰۱۷ منتشر کردند که بیانگر آن بود که نظام کنونی حکمرانی جهانی منابع اساسی اینترنت، خواسته‌ها و منافع همه کشورها را در برنمی‌گیرد[3]. مساله اقتدار سایبری از مبانی مهم این سند است: اگرچه هنوز پکن مفهوم اقتدار سایبری را به درستی تبیین نکرده‌است، اما تا حدی بیانگر این موضوع است که دولت‌ها باید بر محتوا و شبکه‌های درون مرزهای خود مسلط باشند[4]. در همین راستا، چین در سپتامبر ۲۰۲۰ طی سمپوزیوم بین‌المللی پکن که در سطح مقام‌های عالی‌رتبه کشورها برگزار شد نیز ابتکار امنیت داده جهانی[5] را پیشنهاد داد که در تضاد کامل با برنامه ماه قبل ایالات متحده یعنی شبکه پاک بود[6]. ابتکار چین ضمن حمایت از رویکرد بی‌طرف و همه‌شمول در مسائل امنیت داده، بر احترام به حقوق مدیریت امنیت، اقتدار

1. Wuzhen Internet Forum
2. International Strategy of Cooperation in Cyberspace

۳. رجوع شود به:
Tai Ming Cheung, 'The rise of China as a cybersecurity industrial power: Balancing national security, geopolitical, and development priorities', Journal of Cyber Policy, vol. 3, no. 3, 2018, p. 313.

۴. رجوع شود به:
Zaagman, 'Cyber Sovereignty and the PRC's Vision for Global Internet Governance'.

5. Global Data Security Initiative

۶. رجوع شود به:
Chun Han Wong, 'China Launches Initiative to Set Global Data-Security Rules', Wall Street Journal, 8 September 2020,
https://www.wsj.com/articles/china-to-launch-initiative-to-setglobal-data-security-rules-11599502974.

و اختیار کشورها -یعنی همان مساله اقتدار سایبری موردنظر چین- تاکید می‌کند[۱].

پکن قوانینی مانند قانون امنیت کشور (۲۰۱۵) و قانون امنیت سایبری (۲۰۱۷) را در زمینه امنیت داده داخلی تصویب کرده‌است که به‌موجب آن‌ها شرکت‌های خارجی موظفند داده‌ها را در سرورهای داخلی ذخیره کنند و حقوق مالکیت فکری حساس، کدهای منبع تایید و ارزیابی را به مراجع چین تحویل دهند. قوانین دیگر ازقبیل قانون رمزنگاری ملی (۲۰۱۹) نیز حفظ منافع امنیت ملی از نظر کنترل فناوری‌های اطلاعاتی را تضمین می‌کنند[۲]. این‌گونه مقررات درواقع بیانگر نوع هنجارهایی هستند که چین قصد دارد در مجامع بین‌المللی به تصویب برساند و در عمل خطر سرقت حقوق مالکیت فکری افراد را افزایش می‌دهند. چین با اعمال اصلاحات متعدد در نهادهای بین‌المللی مانند مجمع حکمرانی اینترنت (IGF)[۳] سازمان ملل می‌کوشد تا ظرفیت تصمیم‌گیری خود را تقویت بخشد[۴]. درحقیقت، چین معتقد است ارتقای قانون‌گذاری سازمان ملل در عرصه سایبری در جهت ترویج رویکرد دولت‌محور در حکمرانی اینترنت است که با دیدگاه کشورهای غربی طرفدار جریان آزاد اطلاعات تناقض دارد[۵].

---

۱. رجوع شود به:
China Ministry of Foreign Affairs, 'Quánqiú shùjù ānquán chàngyì', 8 September 2020, https://www.fmprc.gov.cn/web/wjbzhd/t1812949.shtml.

۲. رجوع شود به:
National People's Congress of the People's Republic of China, 'Zhōnghuá rénmín gònghéguó mìmǎ fǎ (2019 nián 10 yuè 26 rì dì shísān jiè quánguó rénmín dàibiǎo dàhuì chángwù wěiyuánhuì dì shísì cì huìyì tōngguò'), 26 October 2019, http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74.shtml.

3. International Governance Forum

۴. این مجمع انجمنی چندذینفعی است که در چارچوب همایش جهانی جامعه اطلاعات سازمان ملل در سال ۲۰۰۶ بنیان‌گذاری شد. برای کسب اطلاعات بیشتر رجوع شود به:
'The Internet Governance Forum (IGF)', UN Internet Governance Forum, 24 June 2015, https://www.intgovforum.org/cms/2015/IGF.24.06.2015.pdf.

۵. رجوع شود به:
Adam Segal, 'When China Rules the Web: Technology in Service of the State', Foreign Affairs, vol. 7, no. 5, September-October102 The International Institute for Strategic Studies 2018, pp. 10-14, 16-18, https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web.

تاثیر مدل پیشنهادی چین برای حکمرانی اینترنت در دیگر کشورهای اقتدارگرا مانند روسیه و ویتنام کاملا مشهود است، چنانچه آن‌ها نیز قوانین مشابهی در زمینه تنظیم اینترنت تصویب کرده‌اند. چین اکنون در زمینه فناوری‌های نظارتی پیشتاز است و با صادرات این فناوری‌ها موجب تشدید اقدامات سرکوب‌گرانه در دیگر کشورها شده‌است. به‌عنوان مثال، شرکت هوآوی با نیروهای امنیتی زیمبابوه برای ساخت سامانه‌های تشخیص صدا و تصویر همکاری می‌کند و با صادرات گسترده فناوری‌های شهر هوشمند-ترکیبی از فناوری‌های کلان‌داده، هوش مصنوعی و ذخیره داده-به کشورهای دیگر سعی می‌کند ظرفیت نظارت و کنترل اجتماعی آن‌ها را افزایش دهد.

پکن تحقق منافع سایبری خود را ازطریق اجرای طرح راه ابریشم دیجیتال (از زیرمجموعه‌های ابتکار یک کمربند یک راه) دنبال می‌کند. این طرح به‌منزله ابتکاری جغرافیایی/اقتصادی است که با هدف تبدیل چین به قطب زنجیره عرضه دیجیتال جهانی با استفاده از خدمات و کالاهای دیجیتال چین و همچنین زیرساخت‌ها، استانداردها و قوانین ارائه شده توسط چین راه‌اندازی شده‌است. با آنکه این ابتکار هنوز در مراحل اولیه است، ولی شرکت‌های چینی توانسته‌اند کالاها و خدمات خود را در زیرساخت‌های حیاتی مخابراتی بسیاری از کشورها عرضه کنند.

شرکت‌های فناوری اطلاعات چینی از امتیازها و حمایت‌های دولتی زیادی ازجمله در قالب یارانه و ورودی‌های تحقیق و توسعه برخوردارند، به‌طوری‌که شرکت هوآوی به یکی از پرچمداران فناوری اینترنت نسل پنجم (5G) در دنیا تبدیل شده‌است. ظرفیت شرکت‌های چینی در تامین فناوری اینترنت نسل پنجم با واکنش شدید برخی از کشورهای غربی مواجه شده‌است. دراقع، این کشورها از ظرفیت جاسوسی،

نفـوذ و خطـرات امنیتـی کـه فناوری‌های چینی ممکن اسـت در برداشـته باشـند، نگران هسـتند[۱]. اگرچه پویش کشورهای غربی علیه هوآوی در اواسـط سـال ۲۰۲۰ خسـارت‌های زیادی به کسب‌وکار آن در این کشورها وارد کرد، اما نتوانست مانع درآمدزایی و توسعه فعالیت‌های آن در کشورهای دیگر شـود.

در حـال حاضـر، چیـن در تعییـن اسـتانداردهای جهانـی فناوری‌هـای نوپدیـد ماننـد اینترنـت اشیـا، نسـخه ۶ پروتـکل اینترنـت (IPv۶)[۲] و اینترنـت نسـل پنجـم نقـش قدرتمندی دارد. چین همچنین از جایگاه مهمی در سـازمان‌های بین‌المللی اسـتاندارد مانند سـازمان بین‌المللی استانداردسازی (ISO)[۳]، کمیسیون بین‌المللی الکتروتکنیک (IEC)[۴] و اتحادیـه بین‌المللـی مخابـرات برخوردار اسـت[۵]. با این همـه، کشورهای غربی و هم‌پیمانـان نزدیـک آن‌هـا با برخورداری از شـرکت‌های بزرگ در ایـن حوزه از نفوذ بالایی برخوردار هسـتند. در فهرسـت ۵۰۰ شـرکت برتـر جهانی فورچون (۲۰۲۰)، چیـن تنها دارای ۸ نماینـده اسـت، در حالـی کـه ۴۳ شـرکت در ایـن فهرسـت متعلـق به ایـالات متحده و متحدانش است[۶].

---

۱. رجوع شود به:
Nigel Inkster, China's Cyber Power, Adelphi 456 (Abingdon: Routledge for the IISS, 2015).

2. Internet Protocol Version 6

3. International Organization for Standardization

4. International Electrotechnical Commission

۵. رجوع شود به:
Kristin Shi-Kupfer and Mareike Ohlberg, 'China's Digital Rise: Challenges for Europe', MERICS Papers on China, no. 7, April 2019, p. 21, https://merics.org/sites/default/files/202006/MPOC_No.7_ChinasDigital-Rise_web_final_2.pdf

۶. برای کسب اطلاعات بیشتر درباره شرکت‌های فناوری رجوع شود به:
'Global 500', Fortune,
https://fortune.com/global500/2020/search/?sector=Technology.

برای مشاهده شرکت‌های مخابراتی این فهرست رجوع شود به:
'Global 500', Fortune,
https://fortune.com/global500/2020/search/?sector=Telecommunications

توانمندی‌های سایبری تهاجمی

چین نیز مانند روسیه در عملیات‌های اطلاعاتی/نفوذی زمان صلح به‌طور گسترده از توانمندی‌های سایبری سطح پایین استفاده می‌کند و درنتیجه، تجربه زیادی در روش‌ها و فنون این حوزه دارد. طبق دیدگاه‌های رسمی چین و شواهد موجود، احتمالا این کشور به ابزارهای سایبری تهاجمی موثری نیز برای استفاده در زمان جنگ دست یافته‌است. اگرچه چین هیچ‌گاه به‌طور رسمی اشاره‌ای به توانمندی‌های سایبری تهاجمی خود نکرده‌است، اما باتوجه به ادعاهای برخی مقامات ارتش آزادی‌بخش چین ظاهرا دارای توانمندی‌هایی در این حوزه می‌باشد[۱]. به‌عنوان مثال، در نسخه ۲۰۱۳ سند علم راهبرد نظامی بخش مجزایی به برخورد در فضای سایبری اختصاص داده شده و عملیات‌ها به چهار دسته شناسایی، حمله، دفاع و بازدارندگی تقسیم‌بندی شده‌اند که دو دسته اول ماهیت تهاجمی دارند[۲]. در عملیات‌های شناسایی با تعیین نقاط ضعف دشمن در زمان صلح زمینه برای عملیات‌های تهاجمی در زمان جنگ فراهم می‌شود. درواقع، در عملیات‌های شناسایی نفوذ موفق در سامانه‌های دشمن مستلزم اقداماتی مشابه حمله به شبکه است و از این رو، در زمان مناسب امکان تغییر عملیات شناسایی به عملیات تهاجمی وجود دارد[۳].

۱. رجوع شود به:
Kevin Pollpeter, 'Chinese Writings on Cyberwarfare and Coercion', in Jon R. Lindsay, Tai Ming Cheung and Derek S. Reveron (eds), China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain (New York: Oxford University Press, 2015).

۲. رجوع شود به:
Amy Chang, 'Warring State: China's Cybersecurity Strategy', Center for a New American Security, December 2014, p. 25,
https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS_WarringState_Chang_report_010615.pdf?mtime=20160906082142&focal=none.

۳. رجوع شود به:
Joe McReynolds, 'China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy', China Brief, vol. 15, no. 8, April 2015, p. 5,
https://jamestown.org/program/chinas-evolving-perspectives-on-network-warfarelessons-from-the-science-of-military-strategy.

دیدگاه سایبری چین این است که به‌محض بروز منازعه فیزیکی می‌توان از عملیات‌های تهاجمی به شبکه استفاده کرد و سامانه‌های دشمن را مختل کرد[۱]. در سند علم راهبرد نظامی نیز تصریح شده‌است که در زمان منازعه (جنگ) زیرساخت‌های غیرنظامی همانند زیرساخت‌های نظامی هدفی بالقوه هستند؛ به‌ویژه این‌که زیرساخت‌های نظامی به زیرساخت‌های غیرنظامی وابسته هستند و حمله به آن‌ها کمتر تشدید منازعه را در پی دارد و درنتیجه، هدف بهتری نسبت به زیرساخت‌های نظامی در حملات به شبکه محسوب می‌شوند[۲]. ارتش آزادی‌بخش چین نیز استفاده از توانمندی‌های پیشرفته مانند جنگ‌افزارهای الکترونیکی شبکه‌ای برای درج الگوریتم‌های مخرب در شبکه‌های دشمن حتی در صورت عدم وجود ارتباط کابلی را مد نظر دارد. به‌عنوان مثال، دای کینگ‌مین[۳] از رؤسای سابق ستاد کل ارتش چین در نوشته‌های خود در سال ۱۹۹۹ به ظرفیت استفاده از حمله سایبری وایرلس (مبتنی بر ارتباطات رادیویی) برای نفوذ به ارتباطات ماهواره‌ای یا سامانه‌های فرماندهی و کنترل ارتش دشمن اشاره کرده‌است[۴].

باتوجه به این‌که ادعاهای مقامات چینی درباره توانمندی‌های سایبری تهاجمی چین هیچ‌گاه در بوته آزمایش قرار نگرفته‌است، نمی‌توان به‌طور قطعی در مورد کارایی و نقش آن‌ها در زمان نبرد واقعی قضاوت کرد. البته ارتش آزادی‌بخش خلق و سازمان‌های جاسوسی چین تاکنون نفوذهای موفقی به شبکه‌های دولتی و تجاری ایالات متحده

۱. رجوع شود به:
Pollpeter, 'Chinese Writings on Cyberwarfare and Coercion', p. 7.

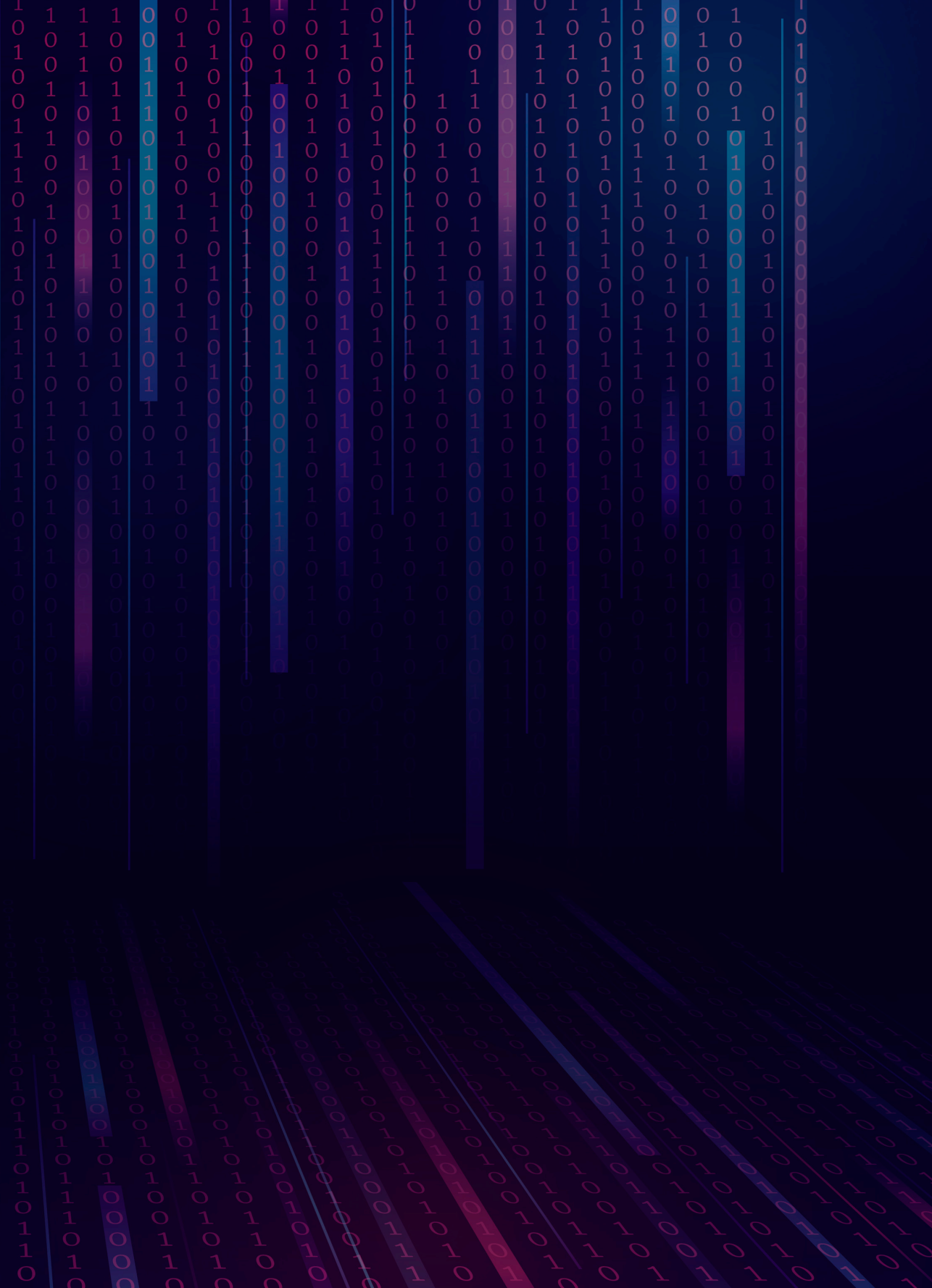
۲. رجوع شود به:
McReynolds, 'China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy', p. 5.

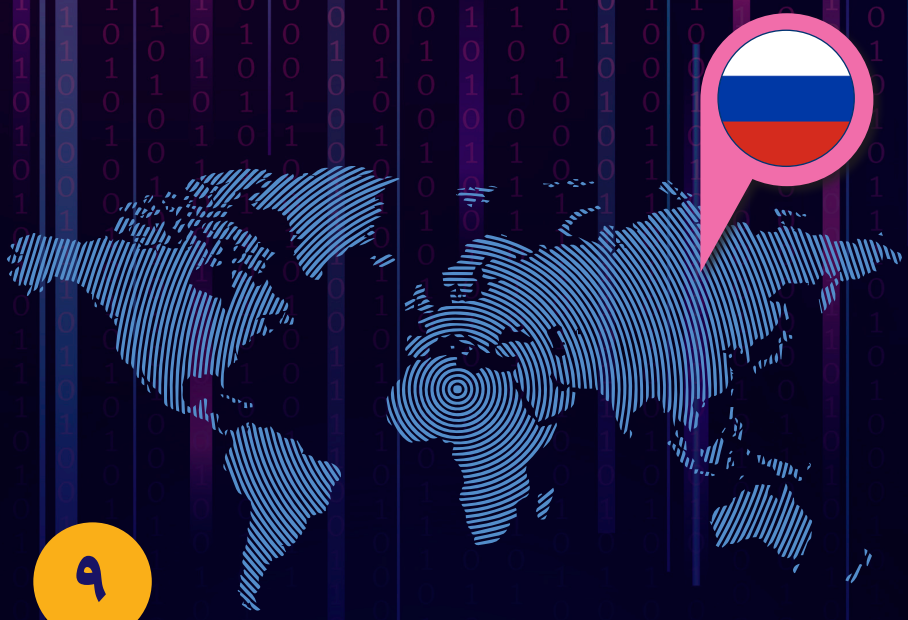
3. Dai Qingmin

۴. رجوع شود به:
Pollpeter, 'Chinese Writings on Cyberwarfare and Coercion', p. 8.

داشته‌اند و با به‌کارگیری بدافزارها اقدام به سرقت اطلاعات طبقه‌بندی‌شده یا حقوق مالکیت فکری این کشور کرده‌اند. این‌گونه عملیات‌های نفوذی می‌تواند برای اهداف نظامی نیز به‌کار رود و بی‌شک تجارب حاصله در این عملیات‌ها تا حدی نقاط ضعف ایالات متحده را برای چین آشکار کرده‌است[۱]. بدیهی است که ارتش آزادی‌بخش خلق چین از توانمندی و انگیزه کافی برای اجرای عملیات‌های مخرب و سرقت اطلاعات برخوردار است.

۱. همان صص. ۱۴-۱۳





۹

روسیه

راهبرد سایبری روسیه کاملا تحت‌تاثیر رقابت آن با غرب قرار دارد و از این رو، عملیات‌های سایبری را جزء تفکیک‌ناپذیر جنگ اطلاعاتی می‌داند. حکمرانی سایبری در روسیه متمرکز و سلسله‌مراتبی بوده و تحت‌نظارت مستقیم رئیس‌جمهور قرار دارد. این کشور به‌شدت وابسته به شرکت‌های فناوری اطلاعات و ارتباطات خارجی است و اقتصاد دیجیتال آن در مقایسه با کشورهایی مانند فرانسه و بریتانیا چندان توسعه‌یافته نیست. روسیه می‌کوشد ضعف‌های عمده خود در امنیت سایبری را ازطریق اعمال مقررات دولتی و ساخت اینترنت ملی و ترویج توسعه صنعت دیجیتال بومی برطرف کند. البته با توجه به وضعیت اقتصادی این کشور، چنین اهدافی غیرواقع‌بینانه به نظر می‌رسد. به‌مدت دو دهه روسیه در تلاش بوده‌است تا ازطریق اقدامات دیپلماتیک از تسلط غرب به‌ویژه آمریکا بر فضای سایبری بکاهد. روسیه دارای توانمندی‌های سایبری تهاجمی قابل‌توجهی است که از آن‌ها برای اخلال در سیاست‌ها و اقدامات کشورهای رقیب به‌خصوص آمریکا استفاده می‌کند. تاکنون این کشور عملیات‌های سایبری-اطلاعاتی گسترده‌ای انجام داده‌است که برخی از آن‌ها از سطح بالای تخصص و پیشرفت فناورانه برخوردار بوده‌اند. با این حال، به نظر می‌رسد ساخت توانمندی‌های سایبری دقیق و تخصصی سطح بالا که از الزامات جنگ‌های تمام‌عیار به‌شمار می‌روند، از اولویت‌های اصلی روسیه نیست. درمجموع، روسیه یکی از قدرت‌های سایبری رده دوم است و برای آنکه در رده اول در کنار آمریکا قرار گیرد باید ضمن ارتقای امنیت سایبری، سهم خود در بازار دیجیتال جهانی را افزایش دهد و تجهیزات نظامی سایبری تهاجمی تخصصی‌تر و دقیق‌تری بسازد.

راهبرد و مبنای نظری (دکترین)

در راهبرد و مبنای نظری سایبری روسیه توانمندی‌های سایبری از عناصر اصلی تقابل اطلاعاتی با غرب محسوب می‌شوند. در منابع روسی اغلب به‌جای عبارت فضای سایبری از «فضای اطلاعاتی» استفاده می‌شود و تضمین برتری اطلاعاتی روسیه هدف اصلی از اجرای عملیات‌های سایبری فنی در کنار به‌کارگیری سایر روش‌ها و ابزارها (به‌عنوان نمونه ازطریق نظارت و کنترل رسانه‌های اجتماعی) محسوب می‌شود. در ده سال گذشته روسیه از توانمندی‌های اطلاعاتی برای کسب قدرت راهبردی در برابر دولت‌های رقیب استفاده کرده‌است و این سیاست به قول والری گراسیموف[1] رئیس ستاد کل ارتش روسیه (CGS)[2] تا حدی با مفهوم «منطقه خاکستری» بین جنگ و صلح (۲۰۱۳) ارتباط دارد[3]. عملیات‌های اطلاعاتی روسیه علیه استونی (۲۰۰۷)، گرجستان (۲۰۰۸) و اکراین (۲۰۱۵-۲۰۱۴) نمونه‌هایی از این رویکرد روسیه هستند که ناظران غربی آن‌ها را نوعی جنگ سایبری می‌دانند. اما عملیات روسیه علیه کمیته ملی دموکرات ایالات متحده[4] در سال ۲۰۱۶ یکی از معروف‌ترین این عملیات‌های هک و سرقت اطلاعات بود.

در مبنای نظری امنیت اطلاعات روسیه (۲۰۱۶)[5] نیز مانند راهبرد امنیت ملی روسیه ۲۰۱۵[6] این تفکر لحاظ شده‌است که کشور همواره در معرض حمله‌های اطلاعاتی قرار

1. Valery Gerasimov
2. Chief of the General Staff

۳. رجوع شود به:

Valery Gerasimov, 'Tsennost' nauki v predvidenii', Voennopromyshlennyi kurier, 27 February 2013, https://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf. Translation available in Mark Galeotti; 'The "Gerasimov Doctrine" and Russian Non-Linear War', In Moscow's Shadows blog, 6 July 2014, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war

4. Democratic National Committee
5. Information Security Doctrine

رجوع شود به:

Presidential Administration, 'Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii', 6 December 2016, https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html.

6. 2015 National Security Strategy

دارد[1]. مبنای نظری روسیه ۲۰۱۶ از جنبه‌های زیادی شبیه مبنای نظری سایر کشورهای موردبررسی است و شامل بازدارندگی راهبردی، امنیت اطلاعاتی نهادهای دولتی و نظامی، زیرساخت‌های حیاتی ملی و شهروندان و مقابله با تهدیدهای دولت‌های متخاصم، جنایت‌کاران و تروریست‌ها می‌شود. تفاوت‌های اصلی آن نیز عبارتند از: عدم‌تمایز واقعی بین امنیت اطلاعات بخش نظامی و بخش غیرنظامی و تمرکز بر مقابله با اقدامات اطلاعاتی و روانی علیه ارزش‌های تاریخی، میهن‌پرستانه، اخلاقی و معنوی روسیه. به نظر می‌رسد روسیه در مسأله امنیت سایبری بر کنترل اطلاعات و محتوای موجود در شبکه‌ها تاکید دارد، چراکه مقامات روسی آن‌ها را منبع اصلی تهدید می‌دانند. درواقع، روسیه تهدیدهای سایبری را بخشی از پویش اطلاعاتی وسیعی می‌داند که دولت‌های رقیب برای تغییر ساختار اجتماعی آن به راه انداخته‌اند. به همین دلیل، در مبنای نظری ۲۰۱۶ بر افزایش نقش روسیه در مدیریت اینترنت کشور و رشد تولید فناوری‌های اطلاعاتی بومی تاکید زیادی شده‌است و براین اساس، روسیه به‌منظور مقابله با دشمنان خود را مجاز به راه‌اندازی پویش‌های اطلاعاتی علیه آن‌ها می‌داند. اسناد امنیت اطلاعاتی روسیه در سال‌های بعد نیز به مبانی سند ۲۰۱۶ ارجاعات بسیاری دارند.

مفاهیم نظامی حوزه فضای سایبری که در یکی از سندهای وزارت دفاع در سال ۲۰۱۱[2]

۱. رجوع شود به:
Katri Pynnöniemi and Martti J. Kari. 'Russia's New Information Security Doctrine: Guarding a besieged cyber fortress', Finnish Institute of International Affairs, Comment no. 26/2016, December 2016, https://www.fiia.fi/wp-content/uploads/2017/04/comment26_russia_s_new_information_security_doctrine.pdf

۲. وزارت دفاع، رجوع شود به:
'Kontseptual'nye vzgliady na deiatel'nost' Vooruzhionnykh Sil Rossiiskoi Federatsii v informatsionnom prostranstve', 22 December 2011, http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle.

و مبانی نظری نظامی روسیه ۲۰۱۴[۱] نیز ذکر شده‌اند، اساس مبنای نظری امنیت اطلاعاتی روسیه ۲۰۱۶ را تشکیل می‌دهند. اگرچه سند ۲۰۱۱ نقش نیروهای نظامی در فضای سایبری را تبیین می‌کند، اما مطالب آن کامل نیست و درواقع، صرفا به موضوعات مربوط به آگاهی از موقعیت، تهدیدها و حفاظت از نیروها می‌پردازد و هیچ اشاره‌ای به عملیات‌های اطلاعاتی یا سایبری تهاجمی نمی‌کند. مقدمه آن مشتمل بر بیانیه‌ای رسمی درباره تهدیدهایی است که از سوی سیاست‌های جنگ اطلاعاتی سایر کشورها متوجه روسیه می‌شود که خود شاهدی دیگر برای ذهنیت توطئه‌محور روسیه نسبت به فعالیت‌های برخط دیگر کشورها به‌ویژه کشورهای غربی است[۲].

نکته جالب‌توجه در مبنای نظامی ۲۰۱۴ اشاره به نوع جنگ‌های مدرن است که می‌تواند ترکیبی از نیروهای نظامی و ابزارهای سیاسی، اقتصادی، اطلاعاتی و سایر ابزارهای غیرنظامی باشد و همراه با استفاده گسترده از ظرفیت مخالفت مردمی و نیروهای عملیات‌های ویژه خواهد بود[۳]. در این سند خطرهای اطلاعاتی در رده دوازدهم تهدیدهای خارجی و جایگاه اول فهرست تهدیدهای داخلی قرار دارند. در این سند ده ویژگی اصلی جنگ‌های مدرن بیان شده‌است که سه مورد از آن‌ها به اطلاعات ارتباط دارد. این سند همچنین حاوی فهرست بلندبالایی از اقدامات بازدارنده و پیشگیرانه در برابر حمله نظامی به روسیه است که عملیات‌های اطلاعاتی در رده اول قرار دارند.

۱. رجوع شود به:
Katri Pynnöniemi and Martti J. Kari. 'Russia's New Information Security Doctrine: Guarding a besieged cyber fortress', Finnish Institute of International Affairs, Comment no. 26/2016, December 2016, https://www.fiia.fi/wp-content/uploads/2017/04/comment26_russia_s_new_information_security_doctrine.pdf.

۲. رجوع شود به:
Ministry of Defense, 'Kontseptual'nye vzgliady nadeiatel'nost' Vooruzhionnykh Sil Rossiiskoi Federatsiiv informatsionnom prostranstve', 22 December 2011, http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle.

۳. رجوع شود به:
Office of the President, 'The Military Doctrine of the Russian Federation', 25 December 2014, https://rusemb.org.uk/press/2029

در سال ۲۰۱۷، روسیه به‌دنبال سال‌ها تلاش برای توسعه نیروهای اطلاعاتی خود اعلام کرد «سپاه عملیات‌های اطلاعاتی» به نیروهای مسلح ملحق می‌شود[۱]. این سپاه قرار بود شکاف عملیاتی که در منازعه سال ۲۰۰۸ با گرجستان مشاهده شد را پر کند. با آنکه در رسانه‌های غربی واحدهای این سپاه به‌عنوان نیروهای سایبری معرفی می‌شوند، اما حوزه فعالیت آن‌ها بیشتر متناسب با تعریف روسیه از جنگ اطلاعاتی است. به‌عنوان مثال، در جنگ سوریه این واحدها از روش‌های روانی مانند توزیع هوایی اعلامیه‌های کاغذی یا پخش نوارهای صوتی به زبان‌های مختلف استفاده کردند[۲]. واحدهای سپاه عملیات‌های اطلاعاتی از قابلیت دسترسی به تلفن‌های همراه شهروندان ازجمله ارسال پیام به گوشی‌ها نیز برخوردارند و از این‌گونه روش‌های الکترونیک برای پروپاگاندا (جوسازی سیاسی)، نشر اطلاعات غلط و تضعیف روحیه سربازان حریف در جنگ سوریه و اکراین و علیه نیروهای ناتو استفاده کرده‌اند[۳].

1. Information-Operations Troops

رجوع شود به فصل:
'Russia under Threat' in Keir Giles, Moscow Rules: What Drives Russia to Confront the West (Washington DC: Brookings Institution Press, 2019), pp. 35-58.

۲. رجوع شود به:
Mikhail Klikushin, 'Putin's Army Demands "NATO Soldiers! Hands Up! Lay Down Your Weapons!"', Observer. com, 19 August 2016,
http://observer.com/2016/08/putins-armydemands-nato-soldiers-hands-up-lay-down-your-weapons.

۳. رجوع شود به:
Keir Giles, 'Assessing Russia's Reorganized and Rearmed Military', Carnegie Endowment for International Peace, May 2017,
https://carnegieendowment.org/2017/05/03/assessing-russias-reorganized-and-rearmed-military-pub-69853.

به عنوان مثال برای کسب جزئیات بیشتر درباره به‌کارگیری روش‌های مشابه رجوع شود به:
Dasha Zubkova, 'Defense Ministry: Russia Sending SMS Messages Asking Residents of Ukrainian Border Regions to Appear at Nearest Military Units', Ukrainian News, 27 November 2018,
https://ukranews.com/en/news/598565-defense-ministry-russia-sending-sms-messagesasking -residents-of-ukrainian-border-regions-to-appear.

روسیه در حال ارتقای سطح دیجیتال‌سازی ارتش در همه سطوح حتی بخش فرماندهی و نظارت است. زیرا این کشور به‌خوبی دریافته است برای آنکه بتواند به رقابت با ایالات متحده و کشورهای هم‌پیمانش بپردازد، نیازمند سازمان‌دهی مجدد و اصلاح ساختار رهبری و نیز همراهی کل جامعه است. اگرچه از سال ۲۰۱۷ تاکنون روسیه اسناد رسمی معدودی درمورد برنامه‌ریزی نظامی راهبردی منتشر کرده‌است، اما این موضوع از اهمیت زیادی برای این کشور برخوردار است. چنانچه گراسیموف رئیس ستاد کل در گزارش (بریف) به وابسته‌های نظامی در سال ۲۰۲۰ اظهار داشت مقابله راهبردی در فضای سایبری روزبه‌روز شدیدتر می‌شود و امکان دارد سامانه‌های هسته‌ای راهبردی در بخش فرماندهی و نظارت را هم تحت‌تاثیر قرار دهد[۱]. یکی دیگر از تحلیل‌گران نظامی روسیه نیز گفته است تسلط در فضای سایبری (در کنار قدرت نظامی) پیش‌شرط پیروزی در جنگ‌های مدرن است[۲]. به‌طورکلی، تحلیل‌گران نظامی روسیه بر جنبه‌های شناختی و روانی جنگ‌های سایبری بسیار تاکید دارند و توجه زیادی به جنگ اطلاعاتی چین نشان می‌دهند.

حکمرانی، فرماندهی و نظارت

رئیس‌جمهور روسیه از اختیار کامل در حاکمیت امنیت سایبری برخوردار است و ازطریق شورای امنیت[۳] وظایف حوزه فرماندهی و نظارت ملی را انجام می‌دهد. با آنکه اسناد سیاستی روسیه به رویکرد چندذینفعی در مدیریت امنیت سایبری ملی اشاره می‌کنند،

۱. رجوع شود به:
Ministry of Defense, ‘Nachal’nik General’nogo shtaba VS RF general armii Valeriy Gerasimov provel brifing dlya inostrannykh112 The International Institute for Strategic Studies attashe’, 24 December 2020, https://function.mil.ru/news_page/country/more.htm?id=12331668@egNews

۲. وزارت دفاع، رجوع شود به:
‘Prevoskhodstvo v kiberprostranstve stanovitsya odnim iz usloviy pobedy v voynakh’, 22 April 2019, https://function.mil.ru/news_page/country/more.htm?id=12227079@egNews.

3. Security Council

اما نظام سایبری این کشور دولتی و تحت‌ریاست رئیس‌جمهور است. طبق مبنای نظری امنیت اطلاعات ۲۰۱۶، دبیر شورای امنیت موظف است سالانه به رئیس‌جمهور درباره وضعیت امنیت سایبری کشور گزارش دهد. همه نهادهای امنیتی بالادستی روسیه دارای نماینده در شورای امنیت هستند و وزیر دفاع، رئیس سازمان امنیت فدرال (FSB)[1] و رئیس ستاد کل[2] اعضای دائمی آن را تشکیل می‌دهند.

ظاهرا از نظر رهبری و هماهنگی سیاست‌ها و عملیات‌های سایبری، رئیس‌جمهور پوتین وزارت دفاع را دراولویت قرار داده و درنتیجه، اداره اصلی ستاد کل[3] مسئولیت امور در عملیات‌های تهاجمی را برعهده دارد. خدمات رمزنگاری توسط اداره هشتم ستاد کل[4] انجام می‌شود که مسئولیت مدیریت اسرار نظامی مربوط به امور سایبری را نیز برعهده دارد. سازمان امنیت فدرال که اصلی‌ترین نهاد اطلاعاتی داخلی روسیه است نیز وظیفه دفاع در برابر حمله به سامانه‌های دولتی و زیرساخت‌های حیاتی ملی را برعهده دارد. به تعبیری می‌توان گفت این سازمان مجری همه مسئولیت‌ها و اختیارات نهادهای اطلاعات سیگنالی است که در سال‌های اولیه ریاست‌جمهوری پوتین منحل شدند. سازمان امنیت فدرال در سال ۲۰۱۸ مرکز ملی هماهنگی حوادث رایانه‌ای[5] را تاسیس کرد که فرمانده آن وظیفه مدیریت مرکز حفاظت داده و ارتباطات ویژه[6] را نیز برعهده دارد[7].

1. Federal Security Service

۲. رجوع شود به:
President of Russia, 'Security Council structure', http://en.kremlin.ru/structure/security-council/members.

3. Main Directorate of the General Staff
4. 8th Directorate of the General Staff
5. National Coordination Center for Computer Incidents
6. Center for Data Protection and Special Communication

۷. رجوع شود به:
Russian domestic security service launch new dedicated center to counter cyberattacks', Russia Today, 11 September 2018,
https://www.rt.com/russia/438142-russian-security-cyberattacks

سازمان فدرال کنترل فنی و صادرات (FSTEK)[1] از زیرمجموعه‌های وزارت دفاع وظایف متعددی ازجمله حفاظت از زیرساخت‌های اطلاعاتی حیاتی در سراسر کشور، دفاع در برابر عملیات‌های اطلاعاتی فناوری‌محور و با مبدا خارجی، دفاع فنی از اطلاعات و سیاست‌گذاری برای کنترل صادرات فناوری و عملیات‌های ضدجاسوسی داخل روسیه را عهده‌دار است[2]. علاوه براین، تنظیم مقررات استفاده از فناوری‌های اطلاعاتی خارجی نیز از وظایف این سازمان به شمار می‌رود.

پس از منازعه گرجستان و مباحثی که درباره تاسیس واحدهای تخصصی عملیات اطلاعات پیش آمد، سازمان امنیت فدرال ضمن رد کردن ادعای ایجاد توانمندی‌های اطلاعاتی نظامی در ارتش، این‌گونه توانمندی‌ها را در حوزه اختیارات خود دانست. با این حال، انحصار این سازمان مدت‌هاست که از بین رفته‌است و شاهد این مدعا نقش سایر نهادهای اطلاعات نظامی روسیه در فعالیت‌های جهانی جنگ اطلاعاتی آن و نیز واگذاری مسئولیت سیاست دفاع سایبری در سال ۲۰۱۷ به سازمان فدرال کنترل فنی و صادرات است که حوزه‌های اقتصاد و سیاست ملی را نیز شامل می‌شود.

مرکز ملی مدیریت دفاع[3] که در سال ۲۰۱۴ در مسکو بنیان‌گذاری شد، اولین قطب مشترک همه سازمان‌های دولت در حوزه اطلاعات و ارتباطات است که به‌طور شبانه‌روزی به اجرای عملیات‌های دفاعی می‌پردازد. مقر این مرکز در نزدیکی کاخ کرملین قرار دارد و وظایف آن به چهار دسته تقسیم می‌شود: فرماندهی، هماهنگی عملیات‌های نظامی، فرماندهی نیروهای هسته‌ای راهبردی و هماهنگی فعالیت‌های زمان صلح ازجمله

1. Federal Service for Technical and Export Control

۲. رجوع شود به:
Decree no. 569 of 25 November 2017, 'Ukaz Prezidenta RF ot 25 noiabria 2017 g. N 569 "O vnesenii izmenenii v Polozhenie o Federal'noi sluzhbe po tekhnicheskomu i eksportnomu kontroliu, utverzhdennoe Ukazom Prezidenta Rossiyskoi Federatsii ot 16 avgusta 2004 g. N 1085"',
http://ivo.garant.ru/#/document/71818302/paragraph/1:0

3. National Defense Management Centre

امنیت سایبری در نهادها و وزارت‌های ذی‌ربط در امنیت[۱]. این مرکز با ادغام ۴۹ نهاد نظامی، سیاست‌گذاری، اقتصادی و دیگر مراجع تحت ستاد کل توانسته‌است سرعت واکنش و تبادل اطلاعات دولت را به‌میزان زیادی بهبود بخشد[۲]. از سال ۲۰۲۰، هماهنگی امور رزمایش‌ها نیز به وظایف این مرکز افزوده شد که شامل هماهنگی نهادهای بسیار متنوع و زیادی می‌شود. به‌عنوان مثال، در رزمایش قفقاز ۲۰۲۰ که ۱۶۰ نهاد در آن شرکت داشتند، این مرکز ۳۸۰ فعالیت مشترک را هماهنگ کرد[۳].

توانمندی‌های محوری در زمینه اطلاعات سایبری

پس از فروپاشی اتحاد جماهیر شوروی در سال ۱۹۹۱، نهادهای اطلاعاتی آن با ساختار جدیدی سامان یافتند. در همین راستا، کمیسیون امنیت دولت[۴] معروف به کاگ‌ب (KGB)[۵] به دو سازمان مشتق شد: سازمان امنیت فدرال که وظایف کاگ‌ب در زمینه امنیت داخلی را برعهده گرفت[۶] و سازمان خدمات اطلاعات خارجی[۷] (SVR) که مسئولیت

۱. رجوع شود به:
Roger McDermott, 'Russia Activates New Defense Management Center', Eurasia Daily Monitor, vol. 11, no. 196, 2 November 2014,
https://jamestown.org/program/russia-activates-new-defense-management-center

۲. رجوع شود به:
Keir Giles, 'Russia's "New" Tools for Confronting the West -Continuity and Innovation in Moscow's Exercise of Power', Russia and Eurasia Programme, Chatham House, March 2016, p. 25,
https://www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf.

۳. رجوع شود به:
Ministry of Defense, 'Nachal'nik NTsUO general-polkovnik Mikhail Mizintsev vystupil s dokladom na konferentsii "Razvitiye sistemy mezhvedomstvennogo vzaimodeystviya v oblasti oborony v 2020 godu"', 20 November 2020,
https://function.mil.ru/news_page/country/more.htm?id=12325783@egNews

4. State Security Commission

5. Komitet gosudarstvennoi bezopasnosti

۶. رجوع شود به:
Russian Government, 'Federal Security Service', http://government.ru/en/department/113.

7. External Intelligence Service (Sluzhba vneshnei razvedki)

امنیت اطلاعات در خارج از کشور را عهده‌دار شد. با این حال، نقش اداره اصلی اطلاعات ارتش (GRU)[1] اندکی تغییر کرد و تنها عنوان آن در سال ۲۰۱۰ کوتاه‌تر شد و به اداره اصلی (GR)[2] تغییر یافت. نهادهای اطلاعاتی در روسیه از حمایت سیاسی بالایی برخوردارند و پوتین برای حفظ قدرت داخلی و بقای حکومت اقتدارگرایش بسیار به آن‌ها وابسته است. از نمودهای استفاده بی‌پروای دولت از قدرت اطلاعاتی می‌توان به ترور مخالفان داخلی و خارجی و نیز اخلال در روند انتخابات ایالات متحده در سال ۲۰۱۶ با مجوز پوتین اشاره کرد[3]. درواقع، ماهیت و حجم فزاینده فعالیت‌های اطلاعاتی روسیه در خارج از مرزها دال بر این است که نهادهای اطلاعاتی و امنیتی آن همچنان وارث نظام فلسفی کاگ‌ب هستند که فعالیت‌های اطلاعاتی را نوعی عمل سیاسی و نهادهای اطلاعاتی را در جنگ سیاسی مستمر با غرب می‌دانست-البته اکنون تاحدی با واقعیت‌های قرن بیست‌ویک تطبیق یافته‌اند[4].

در راستای تامین امنیت داخلی، روسیه فعالیت‌های برخط را ازطریق سامانه اقدامات تجسسی عملیاتی (SORM)[5] رصد می‌کند که مشتمل بر مقرراتی برای رصد و کنترل شرکت‌های ارائه‌کننده خدمات اینترنت روسی (ISPs)[6] می‌شود. این سامانه

1. Glavnoe razvedyvatel'noe upravlenie
2. Glavnoe upravlenie

۳. رجوع شود به:
United States Office of the Director of National Intelligence, 'Assessing Russian Activities and Intentions in Recent US Elections', 6 January 2017, p. ii,
https://www.dni.gov/files/documents/ICA_2017_01.pdf.

4. Mark Galeotti, 'Russian intelligence is at (political) war', NATO Review, May 2017,
https://www.nato.int/docu/review/2017/also-in-2017/russian-intelligence-political-war-security/en/index.htm

5. Sistema operativno-razysknykh meropriiatii
6. Internet Service Providers

رجوع شود به:
Keir Giles and Kim Hartmann, 'Socio-Political Effects of Active Cyber Defense Measures', in P. Brangetto, M. Maybaum and J. Stinissen (eds), 6th International Conference on Cyber Conflict, Proceedings (Tallinn: NATO CCDCOE Publications, 2014),
https://www.ccdcoe.org/uploads/2018/10/d0r0s0_giles.pdf

انـواع ابزارهـای نظـارت سـایبری را در اختیار نهادهای مجـری قانون قرار می‌دهـد[1] و امکان اخـذ فـراداده (متادیتـا) و محتوا از تلفن‌های همـراه و ثابـت (SORM-1) و ترافیک اینترنت (SORM-2) و سـایر رسـانه‌ها (SORM-3) را میسـر می‌سـازد. اگرچه در روسـیه اخذ چنین داده‌هایی مستلزم حکم دادگاه است، اما در عمل اغلب سازمان‌های امنیتی روسیه این موضوع را نادیده می‌گیرند.

همانند چین، در روسـیه نیز سوءاسـتفاده احتمالی از رسـانه‌های اجتماعی از مسائل مهـم امنیـت ملی شـمرده می‌شـود و درنتیجـه، اقداماتی بـرای جلوگیری از نشـر اطلاعات خطرناک (برای دولت) انجام می‌گیرد. قوانینی که در اصل برای حفاظت از داده و مقابله با تروریسـم تصویب شـده‌اند، قدرت نظارتی روسـیه را تقویت می‌کنند. درواقع، این قوانین امکان گردآوری و ذخیره داده‌های شخصی کاربران ازجمله همه ارتباطات نوشتاری/صوتی/تصویری، آدرس، اطلاعات پاسپورت، فهرست خویشان/دوستان و آشنایان، حساب‌های رسانه‌های اجتماعی، زبان‌هایی که مسلط هستند و سوابق همه پرداخت‌های الکترونیک را برای شرکت‌های ارائه‌کننده خدمات اینترنت فراهم می‌آورند.

باتوجـه بـه تعـداد روبه‌رشـد حمله‌هـای سـایبری بـه شـرکت‌ها و دولت‌هـای غربی که منتسب به اداره اصلی (GR) و سایر بازیگران روسی هستند و اینکه برخی از این حمله‌ها عملیات‌های پیچیده اطلاعاتی محسوب می‌شوند، می‌توان نتیجه‌گیری کرد که دسترسی منطقه‌ای و جهانی توانمندی‌های حوزه اطلاعات سایبری روسیه بسیار گسترده است.

همانند دیگر جنبه‌های عملیات‌های سایبری روسیه، سطح تخصص و پیچیدگی فنی عملیات‌های اطلاعاتی آن نیز در مقایسه با رقبا پایین‌تر است و البته در مواردی هم به نظر می‌رسـد که روسـیه صرفا نسـبت به رقبایش نگرانی کمتری برای برملا شدن فعالیت‌های

۱. همان.

جاسوسی خود دارد. این مسأله حتی در مورد عملیات‌های اطلاعات سایبری بسیار معروف روسیه که در پایان سال ۲۰۲۰ توسط آمریکا افشا شد نیز صدق می‌کند. چنانچه روسیه سامانه امنیتی بخش خصوصی آمریکا را با استفاده از روش‌هایی پیشرفته فریب داد و البته فقط به استفاده از برخی نقاط ضعف در فناوری اطلاعات اکتفا کرد (هک نرم‌افزاری که شرکت آمریکایی سولار ویندز[1] برای مشتریان زیادی در بخش دولتی و خصوصی ساخته‌بود)[2]. درمقابل، در عملیات سایبری ۲۰۰۸ که روسیه به شبکه‌های وزارت دفاع آمریکا نفوذ کرد، هدف‌گیری آن بسیار دقیق‌تر به نظر می‌رسید[3].

در مقایسه با ایالات متحده و چین، روسیه منابع مالی کمتری به سرمایه‌گذاری در توانمندی‌های اطلاعاتی تخصیص می‌دهد. یکی از روش‌هایی که روسیه برای جبران این ضعف به کار می‌گیرد، کم‌رنگ ساختن مرز بین بازیگران دولتی و غیردولتی عرصه توانمندی‌های سایبری است[4]. به‌عنوان مثال، استفاده روسیه از هکرهای به‌اصطلاح «وطن‌پرست» و تخصص‌های جرائم سایبری سازمان‌یافته کمک زیادی به تقویت توانمندی‌های سایبری آن کرده‌است[5]. از زمان حمله هکرهای روسی به استونی در سال

1. Solar Winds

۲. رجوع شود به:
David E. Sanger, Nicole Perlroth and Julian E. Barnes, 'As Understanding of Russian Hacking Grows, So Does Alarm', New York Times, 2 January 2021, https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html.

۳. رجوع شود به:
Ellen Nakashima, 'Cyber Intruder Sparks Response, Debate', Washington Post, 8 December 2011, https://www.washingtonpost.com/national/national-security/cyber-intrudersparks-responsedebate/2011/12/06/gIQAxLuFgO_story.html.

۴. رجوع شود به:
Andrew Foxall, 'Putin's Cyberwar: Russia's Statecraft in the Fifth Domain', Russia Studies Centre Policy Paper no. 9 (2016), The Henry Jackson Society, May 2016, https://www.stratcomcoe.org/afoxall-putins-cyberwar-russias-statecraftfifth-domain.

۵. رجوع شود به:
Cory Bennett, 'Kremlin's ties to Russian cyber gangs sow US concerns', Hill, 11 October 2015, http://thehill.com/policy/cybersecurity/256573-kremlins-ties-russian-cyber-gangs-sowus-concerns.

۲۰۰۷، کرملین از فناوری و حتی اطلاعات جاسوسی چنین گروه‌هایی در نزدیکی مرزهایش بهره‌برداری می‌کند. باآنکه اطلاعات دقیقی در مورد این‌که هکرهای وطن‌پرست و مجرمان سایبری به چه میزان از کرملین دستور می‌گیرند در دست نیست، ولی فعالیت‌های آن‌ها با اهداف و منابع دولت همسویی زیادی دارد.

توانمندی و وابستگی سایبری

روند توسعه اقتصاد دیجیتال در روسیه کند اما روبه‌رشد است و طبق آمار انجمن ارتباطات الکترونیک روسیه (RAEC)[1]، صنایع وابسته به اینترنت روسیه ۲۰ درصد از تولید ناخالص داخلی آن را تشکیل می‌دهند. محاسبات این انجمن حاکی از آن هستند که به‌دلیل الزامات سخت برخی از مقررات موجود یا در دست تصویب به‌ویژه قوانین مبارزه با تروریسم ۲۰۱۶ درباره ذخیره داده، ممکن است توسعه اقتصاد دیجیتال روسیه دچار رکود شود. در حال حاضر، رقابت‌پذیری دیجیتال روسیه در سطح متوسط است و در فهرست ۵۱ شرکت برتر فناوری یا مخابراتی فورچون ۵۰۰ در سال ۲۰۲۰ هیچ شرکتی متعلق به روسیه نبود، حال آنکه سهم ایالات متحده و چین از این شرکت‌ها به‌ترتیب ۱۶ و ۸ شرکت بود[2].

طبق فرمان پوتین در سال ۲۰۱۷، روسیه باید به جامعه‌ای اطلاعاتی تبدیل شود[3]. این

1. Russian Association for Electronic Communication

۲. برای کسب جزئیات بیشتر درباره شرکت‌های فناوری رجوع شود به:
'Global 500', Fortune,
https://fortune.com/global500/2020/CYBER CAPABILITIES AND NATIONALPOWER: A Net Assessment 113search/?sector=Technology. For the telecoms companies

برای کسب جزئیات بیشتر درباره شرکت‌های مخابراتی رجوع شود به:
'Global 500', Fortune,
https://fortune.com/global500/2020/search/?sector=Telecommunications

۳. رجوع شود به:
Office of the President, 'Ukaz Prezidenta Rossiiskoi Federatsii o Strategii po razvitii informatsionnogo obshchestva v Rossiiskoi Federatsii na 2017-2030 gody', 10 May 2017,
http://publication.pravo.gov.ru/Document/View/0001201705100002?index=0&rangeSize=1.

فرمان همسو با محتوای سند ۲۰۰۸ است که چالش‌های روسیه برای ساخت اقتصاد دیجیتال قوی‌تر را برمی‌شمرد. ازجمله اهداف سند اخیر عبارتند از: گسترش فناوری‌های رمزنگاری روسیه، جایگزینی فناوری‌های اطلاعات و ارتباطات خارجی با فناوری‌های ساخت داخل (به‌ویژه در زیرساخت‌های حیاتی ملی) و بهبود کارایی شبکه‌های ارتباطی داخلی برای پشتیبانی از سامانه متمرکز مدیریت و رصد شبکه الکترونیک روسیه[۱].

تعداد کاربران اینترنت در روسیه به آهستگی روبه‌رشد است. طبق مطالعه پیمایشی بنیاد افکار عمومی روسیه[۲] در سال ۲۰۲۰، ۶۹ درصد از پاسخ‌دهندگان در ۲۴ ساعت قبل از شرکت در این مطالعه پیمایشی برخط بودند[۳]. در روسیه برای دسترسی به اینترنت بیشتر از تلفن همراه استفاده می‌شود و در کلان‌شهرهای مسکو و سن‌پترزبورگ نرخ نفوذ اینترنت بالاتر از میانگین ملی است: حدود ۸۰ درصد در مقایسه با ۶۰ درصد در مناطق روستایی[۴]. در مقایسه با سایر کشورها، قیمت اینترنت در روسیه نسبتا ارزان است و این کشور توانسته‌است رتبه ۱۲ را از این نظر در رتبه‌بندی مجله اکونومیست به خود اختصاص دهد[۵]. با این حال، روسیه در رتبه‌بندی مجله اکونومیست از نظر آمادگی (ظرفیت جمعیت در زمینه مهارت، پذیرش فرهنگی و پشتیبانی سیاستی برای دسترسی به اینترنت) در جایگاه ۵۹ قرار دارد.

---

۱. رجوع شود به:
Sergey Sukhankin, 'Russia Adopts New Strategy for Development of Information Society', Eurasia Daily Monitor, vol. 14, no. 66, 16 May 2017,
https://jamestown.org/program/russia-adopts-new-strategy-development-informationsociety
2. Public Opinion Foundation

۳. رجوع شود به:
Fond obshchestvennoe mnenie, 'Internet i onlain servisy', 31 March 2020,
https://fom.ru/SMI-i-internet/14402.

۴. همان.

۵. رجوع شود به:
'The Inclusive Internet Index 2020', Economist Intelligence Unit, https://theinclusiveinternet.eiu.com/explore/countries/performance?category=affordability

روسیه با جدیت روی توانمندسازی و استقلال سایبری کشور درجهت ساخت اینترنت داخلی مجزا یا همان رونت ملی[1] متمرکز شده‌است. انتخاب مجدد پوتین در سال ۲۰۱۲ برای سومین دور ریاست‌جمهوری به‌معنی فشار جدی کرملین برای افزایش نظارت بر اینترنت داخلی بود. استفاده از رسانه‌های اجتماعی برای سازماندهی مخالفت عمومی در مسکو در سال ۲۰۱۱ و آگاهی از نقش این رسانه‌ها در شکل‌گیری بهار عربی، رئیس‌جمهور و طرفدارانش را بر آن داشت که هرچه سریع‌تر رونت را راه‌اندازی کنند. دو رویداد کرملین را در تصمیم خود مصمم‌تر کرد و باعث شد نظارت بر اینترنت را به‌عنوان مسأله امنیت ملی مطرح کند: افشاگری‌های ادوارد اسنودن در سال ۲۰۱۳ که حجم و ماهیت توانمندی‌های حوزه اطلاعات سایبری آمریکا را آشکار ساخت و اعتراضات میدان استقلال اکراین در سال ۲۰۱۴-۲۰۱۳ که در آن با حمایت اروپا و به کمک رسانه‌هایی مانند فیس‌بوک بر شمار معترضان چنان افزوده شد که درنهایت، توانستند دولت طرفدار مسکو ویکتور یانکوویچ[2] را ساقط کنند.

بیشتر مقررات مصوب در دوره سوم ریاست‌جمهوری پوتین (۲۰۱۲ الی ۲۰۱۸) در ارتباط با اقتدارگرایی اطلاعاتی هستند که یکی از مهم‌ترین اهداف آن‌ها جداسازی رونت از اینترنت جهانی است. وزارت ارتباطات در سال ۲۰۱۶ یکی از اهداف کلیدی خود را دست‌یابی به ۹۹ درصد ترافیک داخلی برای اینترنت رونت تا سال ۲۰۲۰ ذکر کرد[3] که البته ظرف یک سال این هدف به ۹۰ درصد کاهش یافت. لازم به ذکر است هدف روسیه صرفا این نیست که مانع خروج ترافیک اینترنت از سرورهای داخلی شود، بلکه این کشور قصد دارد در صورت بروز

1. Sovereign RuNet
2. Victor Yanukovych

۳. رجوع شود به:
'Russia's Communications Ministry plans to isolate the RuNet by 2020', Vedomosti, 13 May 2016, carried by meduza.io,
https://meduza.io/en/news/2016/05/13/communications-ministry-plansto-isolate-runet-by-2020

بحـران، ترافیـک اینترنـت کشور (ورودی یـا خروجی) را بـه‌طور کامل از ترافیـک بین‌المللی جـدا کنـد[۱]. با این‌حال، اگـر انزوای از اینترنت جهانی بیش از دوهفته طول بکشـد، روسیه نمی‌توانـد بـه هـدف خود برای تبدیل‌شـدن بـه اقتصاد دیجیتال دسـت یابـد. زیرا بخش اعظـم فعالیت‌های اقتصـادی و خدماتی روسیه ازقبیل مبادلات مالی بین‌المللی و تبادل اطلاعات بین‌المللی حوزه سلامت ازطریق اینترنت جهانی انجام می‌شود.

در دسـامبر ۲۰۱۹، دولـت روسیـه مدعـی شـد که موفـق شده‌اسـت رونت را بـه‌صورت آزمایشی از اینترنت جهانی جدا کند که شامل اجرای چندین سناریوی قطع ارتباط ازجمله شبیه‌سازی حمله سایبری از سوی دولتی متخاصم (فرضی) و پاسخ به حمله (حالت نبرد) می‌شـد. در ایـن آزمایش‌هـا نهادهـای دولتی و شـرکت‌های مخابراتی ازجمله شـرکت‌های ارائه‌کننده خدمات اینترنت حضور داشتند[۲].

روسیه قدرت فضایی مسـتقلی اسـت و دارای مجموعه‌های متعددی از ماهواره‌های مخابراتی و ناوبری است که برای اهداف نظامی و غیرنظامی به‌کار می‌روند و ماهواره‌هایی نیز برای طیف متنوعی از سایر کاربردها در اختیار دارد. سامانه ناوبری ماهواره‌ای روسیه گلونـاس (سـامانه نـاوبری ماهـواره‌ای جهانـی)[۳] هم‌تـراز سـامانه مکان‌یـابی جغرافیـایی آمریـکا (جـی‌پی‌اس) اسـت کـه ماهواره‌هـای آن بـه‌طور شـبانه‌روزی و با پوشـش جهانی انجام وظیفه می‌کنند. روسیه تا ژانویه ۲۰۲۰ دارای ۱۷۶ ماهواره عملیاتی بود که در مقایسه

۱. رجوع شود به:
Juha Kukkola, 'The Russian Segment of the Internet as a Resilient Battlefield', in Juha Kukkola, Mari Ristolainen and Juha-Pekka Nikkarila (eds), GAME PLAYER: Facing the structural transformation of cyberspace (Helsinki: Finnish Defense Research Agency, 2019), pp. 117-32, https://maanpuolustuskorkeakoulu.fi/documents/1948673/10330463/PVTUTKL+julkaisuja+11+Game+Player.pdf/9ff35e9b-3513-c490-c188-3e3f18e71bdd/PVTUTKL+julkaisuja+11+Game+Player.pdf.

۲. رجوع شود به:
Justin Sherman, 'Russia's Domestic Internet Is a Threat to the Global Internet', Slate, 24 October 2019, https://slate.com/technology/2019/10/russia-runet-disconnection-domesticinternet.html.

3. GLONASS (Global Navigation Satellite System)

با چین (۴۱۲ ماهواره تقریبا دوبرابر) و ایالات متحده (۱,۸۹۷ ماهواره حدود ده برابر) رقم بالایی به نظر نمی‌رسد[۱].

امنیت و تاب‌آوری سایبری

پوتین در طول دو دهه رهبری روسیه و از همان آغاز با انتشار اولین مبنای نظری امنیت اطلاعات در سال ۲۰۰۰، تاب‌آوری و امنیت سایبری ملی را به‌عنوان اولویت‌های اصلی دولت معرفی کرد. در همین راستا، دولت در سال ۲۰۱۶ به انتشار مجموعه‌ای از قوانین و اعمال اصلاحات در حوزه‌های فنی و اجتماعی امنیت اطلاعات پرداخت، ضمن اینکه نسخه جدید مبانی نظری امنیت اطلاعات را نیز تهیه کرد. راه‌اندازی رونت و سامانه اقدامات تجسسی عملیاتی (SORM) ازجمله عناصر کلیدی این سیاست‌های تاب‌آوری هستند.

عنصر دیگر شامل شبکه دولتی امن یعنی آرِاس‌نت[۲] است که به مقامات دولتی روسیه اختصاص دارد. در این شبکه همه کارمندان ایمیل شخصی و امن دارند و فقط ازطریق یک آدرس آی‌پی خاص (IP) و با استفاده از سیستم‌های مشخصی می‌توانند به آن دسترسی داشته باشند. با این حال، موارد متعددی از اختلال در این شبکه گزارش شده‌است.

دولت اقدامات تنظیم‌گری دیگری نیز انجام داده‌است که به‌عنوان نمونه می‌توان به تصویب قانونی در زمینه بومی‌سازی داده اشاره کرد. به‌موجب این قانون، همه شرکت‌ها ازجمله شرکت‌های ارائه‌کننده بسترهای اجتماعی ملزم هستند داده‌های کاربران را درون

۱. رجوع شود به:
Union of Concerned Scientists, 'UCS Satellite Database', 1 January 2021, https://www.ucsusa.org/resources/satellite-database.
2. RSNet

مرزهای کشور ذخیره کنند[۱]. به‌عنوان مثال، روسکومنادزور[۲] نهاد فدرال ناظر بر تطبیق و سانسور داده، اپل را مجبور به ذخیره‌سازی برخی داده‌های خاص داخل کشور کرده‌است. در سال ۲۰۱۶ نیز روسیه لینکدین را به‌دلیل عدم‌تطبیق با قانون بومی‌سازی داده مسدود کرد. در سال ۲۰۲۰ نیز طبق حکم دادگاهی در مسکو، توییتر و فیس‌بوک هریک مجبور به پرداخت ۶۳ هزار دلار جریمه بابت عدم‌تطبیق با مقررات روسیه شدند[۳].

ظاهرا در روسیه تعداد زیادی تیم پاسخ اضطراری رایانه‌ای (CERT)[۴] فعالیت دارند که شامل نهادهای دولتی و خصوصی می‌شوند. CERT.GOV.RU که مسئولیت شبکه‌های دولتی را برعهده دارد، FinCERT برای بانک روسیه[۵]، Kaspersky ICS CERT برای سامانه‌های کنترل صنعتی و CERT-GIB[۶] ازجمله آن‌ها به شمار می‌آیند. علاوه بر این، مجموعه‌ای از موسسات پژوهشی دولتی و شرکت‌های تجاری نیز در زمینه دفاع سایبری مشارکت دارند.

علاوه بر آن، دولت از سال ۲۰۱۳ از نوعی مناسبات بین بخش خصوصی و بخش دولتی برای اشتراک‌گذاری داده استفاده می‌کند که به‌عنوان نمونه می‌توان به GosSOPKA اشاره کرد که سامانه‌ای دولتی برای شناسایی، هشدار و رفع اثرات حمله‌های رایانه‌ای است. هدف این سامانه ایجاد حصاری ایمن برای همه منابع اطلاعات دولتی درون یک

۱. این قانون در سال ۲۰۱۵ تصویب شد و در سال ۲۰۱۹ مفاد سخت‌تری به آن افزوده شد. رجوع شود به:
Gorodissky and Partners, 'Russia Sets $280,000 Fine for Breaching Data Localization Law', 10 September 2019,
https://www.lexology.com/library/detail.aspx?g=5b43dda3-d68f-4f5b-8767-9846b649b5d9.

2. Roskomnadzor

۳. رجوع شود به:
'Russian court fines Twitter and Facebook 62,840 dollars each for refusing to localize user data', Meduza, 13 February 2020,
https://meduza.io/en/news/2020/02/13/russian-court-finestwitter-62-840-dollars-for-refusing-to-localize-user-data.

4. Computer Emergency Response Teams

5. Bank of Russia

۶. این شرکت در سال ۲۰۱۱ به‌عنوان ابتکاری در بخش خصوصی آغاز به کار کرد و در ادامه به یک کسب‌وکار بین‌المللی تبدیل شد. رجوع شود به:
Group-IB, https://www.group-ib.com

شبکه واحد است[۱]. انتظار می‌رود این حصار به تمام زیرساخت‌های حیاتی ملی تعمیم یابد، به‌طوری‌که همه اطلاعات مربوط به حمله‌های سایبری، هماهنگی و تحلیل در اختیار یک نهاد واحد قرار گیرد و سپس ماهیت حمله و توصیه‌های امنیتی لازم به اعضای درون این حصار اطلاع داده شود. مطابق ارزیابی تحلیل‌گران روسی در سال ۲۰۱۹، این سامانه هنوز در مراحل اولیه ساخت قرار دارد. گفتنی است جمهوری تیوا[۲] اولین منطقه روسیه بود که در سال ۲۰۱۹ به سامانه GosSOPKA پیوست[۳] و قوانینی برای اعطای یارانه جهت ساخت مراکز صنعتی GosSOPKA تصویب کرد.

در سال‌های ۲۰۱۹ و ۲۰۲۰ نیز روسیه اقداماتی جهت اجباری ساختن استفاده از نرم‌افزارهای نفوذ و شناسایی در سامانه‌های فناوری اطلاعات روسیه انجام داد که FSTEK نقشی کلیدی در آن ایفا کرد. طبق دستور سازمان امنیت فدرال، همه شرکت‌های ثبت‌شده با عنوان سازمان‌دهنده انتشار اطلاعات موظفند تجهیزاتی را نصب کنند که ماموران اطلاعاتی بتوانند به همه محتوای ارتباطات کاربران بدون نیاز به کسب مجوز و رمزگشایی دسترسی داشته باشند[۴]. در دسامبر ۲۰۱۹ نیز روسیه

۱. رجوع شود به:
'Ob utverzhdenii Pravil predostavleniia subsidiy iz federal'nogo byudzheta na sozdanie otraslevogo tsentra Gosudarstvennoi sistemy obnaruzheniia, preduprezhdeniia likvidatsii posledstvii komp'iuternykh atak (GosSOPKA) i vklyuchenie ego v sistemu avtomatizirovannogo obmena informatsiei ob aktual'nykh kiberugrozakh', Ofitsial'nyi internet-portal pravovoi informatsii, 9 October 2019,
http://publication.pravo.gov.ru/Document/View/0001201910090023.
2. Republic of Tyva

۳. رجوع شود به:
'2020: Zapusk Tsentra monitoringa i reagirovaniia s pravom ispolniat' funktsii tsentra GosSOPKA', TAdviser, 5 March 2020,
https://www.tadviser.ru/index.php/Продукт:Код_Безопасности:_Центр_мониторинга_и_реагирования.

۴. رجوع شود به:
Valeria Pozychanyuk and Petr Mironenko, 'FSB potrebovala ot internet-servisov onlain-dostup k dannym i perepiske pol'zovatelei', The Bell, 11 February 2020,
https://thebell.io/fsbpotrebovala-ot-internet-servisov-onlajn-dostup-k-dannym-iperepiske-polzovatelej.

قانون نصب نرم‌افزارهای پیش‌فرض را تصویب کرد که مطابق آن، برخی نرم‌افزارهای ساخت روسیه باید روی همه وسیله‌های دیجیتال وارداتی مانند تلویزیون، رایانه و تلفن هوشمند نصب شود. دولت همچنین فهرستی از نرم‌افزارهای موردتایید منتشر کرده‌است که مقرر شده‌است نصب آن‌ها از ۱ ژانویه ۲۰۲۱ آغاز شود (تاریخ قبلی شروع اجرای این قانون به‌دلیل شیوع کوید-۱۹ به این تاریخ تغییر یافت). اجرای این قانون به‌معنی این است که همه کاربران وسیله‌های دیجیتال به‌طور پیش‌فرض همه اپ‌ها و مجوزهای نظارت دولتی را روی وسیله‌های دیجیتال خود خواهند داشت[۱]. گفته می‌شود روسیه حتی اقداماتی برای بازرسی و تجسس عمیق در دست اجرا دارد. درواقع، نظام سایبری روسیه یکی از کنترل‌شده‌ترین نظام‌های دنیاست[۲]. روسیه هدف واضحی را دنبال می‌کند: داشتن نظام دفاع سایبری ملی انعطاف‌پذیر -و شاید پیچیده- که در تقابل‌های سایبری با سایر قدرت‌ها برای آن مزیت محسوب شود[۳]. با این حال، تاکنون شواهد چندانی درباره اثربخشی سیاست‌های روسیه برای تحقق این هدف به دست نیامده‌است.

با آنکه روسیه در شاخص جهانی امنیت سایبری ۲۰۱۸ توانست رتبه ۲۶ را از بین ۱۷۵ کشور کسب کند[۴] که رتبه نسبتا خوبی است، اما این کشور نیز همانند بسیاری

۱. رجوع شود به:
GMA Consult Group, 'Russia Authorizes 16 Preinstalled Applications for All Smartphones and Tablets', 20 December 2020, https://www.gma.trade/single-post/russia-authorizes-16-preinstalled-applications-for-all- smart-phones-and-tablets.

۲. رجوع شود به:
'Russia: Growing Internet Isolation, Control, Censorship', Human Rights Watch, 18 June 2020, https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship.

۳. رجوع شود به:
Kukkola, 'The Russian Segment of the Internet as a Resilient Battlefield', p. 117.

۴. رجوع شود به:
International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 62, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

از کشورها با افزایش سریع حمله‌های سایبری موفق روبرو است. به‌عنوان مثال، خرده‌فروشان برخط روسیه در سال ۲۰۲۰ شاهد افزایش دوبرابری حمله‌های سایبری بودند که سایت‌های آن‌ها را از دسترس خارج می‌کرد[۱]. به‌طور مشابه، تعداد رویدادهای نشت داده در بخش مالی روسیه نیز ۳۶/۵ درصد افزایش داشت[۲]. دولت روسیه در ژانویه ۲۰۲۱ درباره احتمال حمله‌های سایبری تلافی‌جویانه آمریکا هشدار داد[۳]. در فوریه ۲۰۲۱ نیز پوتین خطاب به هیئت‌مدیره سازمان خدمات امنیت فدرال اظهار داشت باید توجه بیشتری به امنیت سایبری شود، زیرا حتی اگر فقط حمله‌های بسیار خطرناک در نظر گرفته شود، تعداد حمله به وب‌سایت‌های روسی ازجمله وب‌سایت‌های دولتی تقریبا ۳۵۰ درصد در سال ۲۰۲۰ افزایش داشته‌است[۴]. در مارس ۲۰۲۰ نیز رئیس‌جمهور خطاب به اعضای کابینه اعلام کرد تعداد جرائم سایبری در شش سال گذشته ده برابر بیشتر شده‌است[۵]. گزارش روزنامه تجاری روسیه وِدوموستی[۶] نشان می‌دهد که بیش

---

۱. رجوع شود به:
'DDoS attacks on Russian online retailers double in 2020', TASS, 16 February 2021, https://tass.com/economy/1256821

۲. رجوع شود به:
'Data leaks from Banks of Russia', TAdviser, 29 January 2021, https://tadviser.com/index.php/Article:Date_leaks_from_Banks_of_Russia#.2A_The_number_of_leaks_from_the_financial_sector_in_Russia_grew_by_a_third

۳. رجوع شود به:
Lawrence Abrams, 'Russian government warns of US retaliatory cyberattacks', Bleeping Computer, 23 January 2021, https://www.bleepingcomputer.com/news/security/russian-government-warns-of-us-retaliatory-cyberattacks/.

۴. رجوع شود به:
Presidential Administration, 'Federal Security Service Board meeting', 24 February 2021, http://en.kremlin.ru/events/president/news/65068

۵. رجوع شود به:
Presidential Administration, 'Extended meeting of Russian Interior Ministry Board', 3 March 2021, http://en.kremlin.ru/events/president/news/65090

6. Vedomosti

از نیمی از حمله‌های سایبری شبیه‌سازی‌شده در سال ۲۰۱۹ با موفقیت به سامانه‌های دفاع سایبری کشور نفوذ پیدا کرده‌اند[۱].

رهبری جهانی در عرصه سایبری

روسیه از سال ۱۹۹۸ از قطعنامه مجمع عمومی سازمان ملل با عنوان «پیشرفت‌های حوزه اطلاعات و مخابرات از منظر امنیت بین‌المللی» حمایت می‌کند که ناظر بر فعالیت‌های خطرناک در فضای سایبری با احتمال تهدید صلح و امنیت بین‌المللی است. در آغاز سایر کشورها مخالفتی با این قطعنامه نداشتند، اما در اوایل ریاست‌جمهوری جورج دبلیو بوش، کاخ سفید به این نتیجه رسید که این قطعنامه می‌تواند ابزاری برای ترویج اقتدارگرایی از سوی روسیه، چین و همفکران آن‌ها و محدودسازی آزادی اینترنت باشد. درنهایت، این قطعنامه منجر به تشکیل گروه کارشناسان دولتی سازمان ملل برای رسیدگی به هنجارهای سایبری در سال ۲۰۰۲ شد[۲]. با آنکه تاکنون پیشرفت کمی در زمینه رفع اختلاف بین گروه‌های مخالف و موافق قطعنامه حاصل شده‌است، اما هر دو گزارش با توافق عمومی کشورهای عضو سازمان ملل درباره اعمال قوانین بین‌المللی به فضای سایبری به‌ترتیب در سال‌های ۲۰۱۳ و ۲۰۱۵ منتشر شده‌اند. این گزارش‌ها ضمن پذیرش اعمال قوانین بین‌المللی به

۱. رجوع شود به:
Angelina Krechetova and Ekaterina Kinyakina, 'Minkomsviazi povelo itogi pervykh uchenii po zakonu o "suverennom RuNete"', Vedomosti, 23 December 2019,
https://www.vedomosti.ru/technology/news/2019/12/23/819484-suverennomrunete

۲. رجوع شود به:
UN Office for Disarmament Affairs, 'Developments in the field of information and telecommunications in the context of international security',
https://www.un.org/disarmament/ict-security

فضـای سـایبری، توصیه‌هایـی در مـورد هنجارها، ظرفیت‌سـازی و اهمیت اعتمادسـازی ارائه می‌کنند[۱]. روسـیه به‌ویژه از سـال ۲۰۱۰ که پیش‌نویس کنوانسـیون امنیت اطلاعات بین‌المللـی را ارائـه کـرد، پویـش بین‌المللی دسـتیابی به توافـق یا پیمانی دربـاره امنیت بین‌المللـی اطلاعـات را نیـز رهبری می‌کند. در سـال ۲۰۲۰ هم روسـیه پیشـنهادی مبنی بر تعهـد کشـورها بـه عدم مداخلـه در فراینـد انتخابات سـایر کشـورها ازطریـق حمله‌های مبتنی بـر فناوری اطلاعات و ارتباطات را مطرح کرد[۲].

گفت‌وگوهـای روسـیه و دولت‌هـای غربـی دربـاره مسـائل فضـای سـایبری اغلـب بـا عدم‌تفاهـم و درک متقابـل همـراه هسـتند و هنجارهایـی کـه بـرای یـک طـرف امری بدیهـی محسـوب می‌شـوند، برای طـرف دیگـر تهدیدکننده بـه نظر می‌رسـند. علی‌رغم پیگیری‌هـای روسـیه بـرای تصویـب هنجارهـای پیشـنهادی خـود، اما واگرایـی موجود بیـن کشـورها باعـث تضعیـف اقداماتـی می‌شـود کـه کشـورهایی ماننـد روسـیه بـرای رسـیدن به توافق درباره اصول مشـترک یا قوانین بین‌المللی رفتار در فضای سـایبری انجام می‌دهند.

روسـیه با چین در دیپلماسی سایبری به‌ویژه ازطریق اجلاس‌های چندجانبه همکاری نزدیکـی دارد. نمود بارز این همکاری در رهبری مشـترک آن‌هـا در راه‌اندازی «کارگروه پایان باز» سـازمان ملل در سـال ۲۰۱۸ اسـت که با هدف مقابله با نفوذ کشـورهای غربی در گروه

۱. رجوع شود به:
Alex Grigsby, 'Unpacking the Competing Russian and U.S. Cyberspace Resolutions at the United Nations', Council on Foreign Relations, 29 October 2018,
https://www.cfr.org/blog/unpacking-competing-russian-and-us-cyberspace-resolutionsunited-nations

۲. رجوع شود به:
Anton Troianovski and David E. Sanger, 'Putin Wants a Truce in Cyberspace - While Denying Russian Interference', New York Times, 25 September 2020,
https://www.nytimes.com/2020/09/25/world/europe/russia-cyber-security-meddling.html

کارشناسان دولتی تشکیل شد[۱]. پیوستن به این کارگروه برای همه اعضای سازمان ملل آزاد است. با این حال، روسیه در همکاری عملیاتی با چین درباره جنبه‌های فنی سیاست سایبری محتاطانه عمل می‌کند.

توانمندی‌های سایبری تهاجمی

بیش از دو دهه است که روسیه مبانی نظری و توانمندی‌های سایبری خود را توسعه داده‌است و در تفکر راهبردی و اهداف و دستورالعمل‌های خود نیز به آن‌ها توجه دارد. ازجمله ویژگی‌های رویکرد روسیه در به‌کارگیری توانمندی‌های سایبری تهاجمی می‌توان به توان ثابت‌شده این کشور در ادغام این توانمندی‌ها در پویش‌های اطلاعاتی راهبردی و عملیات‌های نظامی وسیع (ولی با شدت کم) علیه کشورهای دیگر اشاره کرد. این ویژگی می‌تواند به‌منزله نقطه‌قوت رویکرد روسیه در امنیت سایبری در مقایسه با رویکرد کشورهای غرب باشد که صرفا روی پاسخ فنی به تهدیدهای فنی متمرکز هستند و از ورود به دامنه وسیع‌تر امکانات سایبری نسبتا غفلت کرده‌اند. درواقع، رویکرد روسیه امکان ادغام گزینه‌های مختلفی مانند انتشار اطلاعات غلط (دروغ‌پراکنی)[۲]، عملیات‌های تضعیف دولت‌ها و عملیات‌های جنگ الکترونیک و سایبری-فیزیکی را در اختیار آن قرار می‌دهد تا بدین‌ترتیب بتواند به اهداف جاه‌طلبانه‌ای مانند حتی سرنگونی و تغییر رژیم کشورها دست یابد.

۱. عنوان کامل این کارگروه عبارت است از: کارگروه پایان باز درباره پیشرفت‌های حوزه اطلاعات و مخابرات ازمنظر امنیت بین‌المللی (Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security)، برای کسب جزئیات بیشتر رجوع شود به:
https://www.un.org/disarmament/open-ended-working-group.

2. Disinformation

فهرست بلندبالایی از عملیات‌هایی از نوع حمله به زیرساخت‌های حیاتی ملی (مانند جلوگیری از دسترسی به رسانه‌های ارتباطی حیاتی) وجود دارد که به روسیه ارتباط داشته‌اند و یا به‌نحوی روسیه عامل آن‌ها بوده‌است. حمله به استونی (۲۰۰۷)، گرجستان (۲۰۰۸) و اکراین (۲۰۱۵) ازجمله نمونه‌های بارز عملیات‌های سایبری روسیه هستند. مداخله در انتخابات کشورهای غربی که معروف‌ترین آن انتخابات ۲۰۱۶ ایالات متحده بود، از دیگر نمونه‌های عملیات‌های سایبری تهاجمی روسیه است. علاوه بر این‌ها، روسیه از توانمندی‌های سایبری برای اخلال در روند تحقیقات بین‌المللی مانند آزمایش دوپینگ‌های ورزشی و تحقیقات مربوط به سرنگونی پرواز ام‌اچ۱۷ هواپیمایی مالزی[1] و یا استفاده از سلاح شیمیایی در بریتانیا نیز استفاده می‌کند. سازمان تحقیقات اینترنت که موسسه‌ای در ظاهر خصوصی و درواقع با ارتباطات نزدیک با دولت پوتین در سن‌پترزبورگ است و از سال ۲۰۱۳ فعالیت خود را آغاز کرده‌است نیز به نشر اطلاعات غلط می‌پردازد. به‌عنوان مثال، مراجع آمریکا از اقدامات این سازمان برای انتشار اطلاعات نادرست و انجام عملیات‌های رسانه‌ای علیه انتخابات ریاست‌جمهوری آمریکا در سال ۲۰۱۶ پرده برداشتند.

باآنکه روسیه از روش‌های بسیار متنوعی در این‌گونه عملیات‌های سایبری استفاده می‌کند، اما همه آن‌ها مبتنی بر همان روش قدیمی یعنی زنجیره شناسایی، نفوذ، گردآوری، تحلیل و اقدام هستند. این عملیات‌ها اغلب همراه با انتشار عمومی اطلاعات هک‌شده در بسترهای برخط و تبلیغ گسترده در رسانه‌های روسی هستند. ارائه اطلاعات هک‌شده از کمیته ملی دموکرات آمریکا به رسانه ویکی‌لیکس[2] در سال ۲۰۱۶ یکی از معروف‌ترین نمونه‌های این روش است. سایر روش‌های مورداستفاده روسیه

1. Malaysia Airlines flight MH17
2. WikiLeaks

عبارتند از: اعزام نیرو برای نفوذ مخفیانه به وسیله‌های الکترونیکی یا سیستم‌های رقبای سیاسی، اخلال در نشر اطلاعات/کنترل اطلاعات/تولید اطلاعات غیرواقعی در شبکه‌های اطلاعاتی و بهره‌گیری از مجرمان سایبری و هکرهای به‌اصطلاح وطن‌پرست. روسیه در به‌کارگیری ترول‌ها (پروفایل‌های برخط که به وسیله اشخاص مدیریت می‌شوند) و بات‌ها (پروفایل‌هایی که به صورت خودکار مدیریت می‌شوند) برای تولید، نشر و اعتباربخشی به اطلاعات نادرست ازطریق بهره‌برداری از روابط خاص بین رسانه‌های متعارف و بسترهای اجتماعی برخط نیز شهرت زیادی دارد. حتی گفته می‌شود روسیه در پی به‌کارگیری سایر تجهیزات (غیرسایبری) برای اثرگذاری سایبری بر دشمنانش در شرایط بحران است. به‌عنوان مثال، برخی گزارش‌ها نشان می‌دهند که روسیه درصدد استفاده از زیردریایی‌ها برای رصد یا حتی قطع ارتباطات اینترنتی بین ایالات متحده و اروپا[۱] و یا استفاده از تجهیزات فضایی خود برای اختلال در ارتباطات ماهواره‌ای غرب است.

این احتمال نیز وجود دارد که هر یک از سه نهاد اطلاعاتی اصلی روسیه (FSB, GU/GRU و SVR) دارای توانمندی‌های سایبری تهاجمی باشند. به‌عنوان مثال، سازمان امنیت فدرال ضمن برخورداری از توانمندی‌های سایبری مختص به خود، هکرهایی را برای مجازات یا ساکت کردن رقبای کرملین ازطریق حمله‌های سایبری استخدام می‌کند. اگرچه افشای عملیات‌های سایبری روسیه نمی‌تواند شواهد دقیقی از توانمندی‌های سایبری آن در اختیار ما قرار دهد، اما به نظر می‌رسد اداره اصلی (GR) عنصر کلیدی در عملیات‌های سایبری تهاجمی روسیه باشد. به‌بیان دقیق‌تر، اداره مذکور در سال ۲۰۱۵

۱. رجوع شود به:
Michael Birnbaum, 'Russian submarines are prowling around vital undersea cables. It's making NATO nervous', Washington Post, 22 December 2017, https://www.washingtonpost.com/world/europe/russian-submarines-are-prowling-aroundvital -undersea-cables-its-making-nato-nervous/2017/12/22/d4c1f3da-e5d0-11e7-927a-e72eac1e73b6_story.html.

ایستگاه تلویزیونی فرانسه را با پرچم دروغین خلیفه سایبری هک کرد[1]. اداره اصلی همچنین بازیگر اصلی در هک کمیته ملی دموکرات آمریکا در سال ۲۰۱۶ بود و در سال ۲۰۱۷ ویروس به‌شدت مخرب نات‌پتیا (NotPetya) را علیه اکراین به کار گرفت[2]. سازمان امنیت اکراین ۱۰۳ حمله سایبری روسیه علیه وب‌سایت‌های مراجع عمومی اکراین را در سال ۲۰۲۰ خنثی کرد: هدف این حمله‌ها نفوذ به سامانه‌های اطلاعاتی به‌منظور تغییر یا تخریب داده‌ها و یا تضعیف مشروعیت مقامات اکراینی ازطریق نشر اکاذیب بود[3]. شایان ذکر است هنوز معلوم نیست هدف عملیات‌های اطلاعات سایبری روسیه برای هک نرم‌افزار شرکت آمریکایی سولار ویندز تهاجمی بوده‌است یا خیر. (تحقیقات آمریکا در این زمینه ادامه دارد[4]).

درمجموع، روسیه امروزه به‌طور گسترده از توانمندی‌های سایبری با هدف رقابت با دشمنان بالقوه به‌ویژه آمریکا استفاده می‌کند. البته در مقایسه با روش‌ها و

1. Cyber Caliphate

رجوع شود به:

Andy Greenberg, 'A Brief History of Russian Hackers' Evolving False Flags', Wired, 21 October 2019, https://www.wired.com/

۲. رجوع شود به:

Anton Troianovski and Ellen Nakashima, 'How Russia's military intelligence agency became the covert muscle in Putin's duels with the West', Washington Post, 28 December 2018, https://www.washingtonpost.com/world/europe/howrussias-military-intelligence-agency-became-the-covertmusclein-putins-duels-with-the-west/2018/12/27/2736bbe2-fb2d-11e8-8c9a-860ce2a8148f_story.html.

۳. سازمان امنیت اکراین، رجوع شود به:

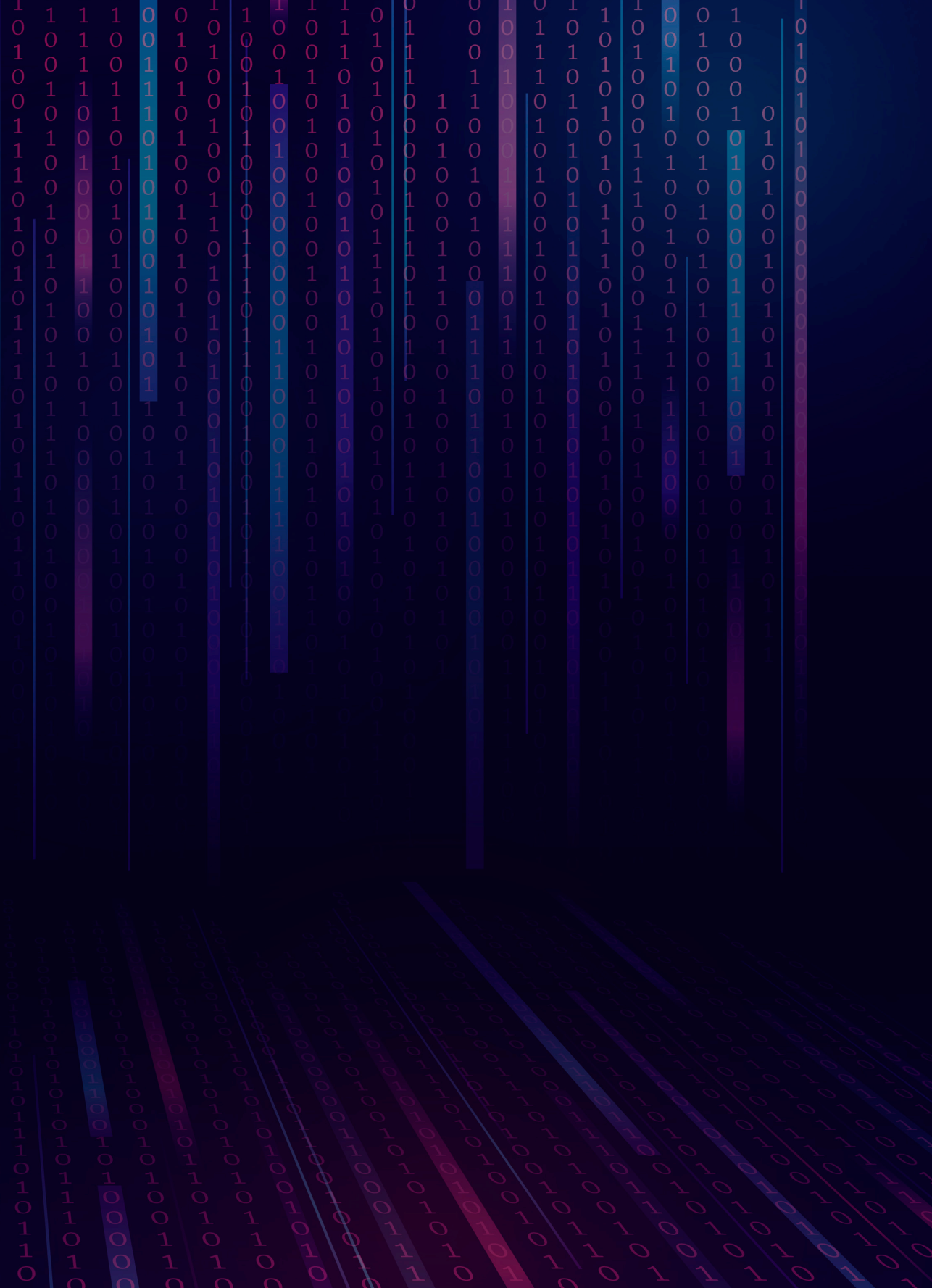
'SBU Blocks 103 Russian Cyber Attacks to Prevent Theft of State Bodies Data: Security Service of Ukraine', Security Service of Ukraine, 6 May 2020, https://www.sbu.gov.ua/en/news/1/category/1/view/7559#.SMNp6d9O.dpbs

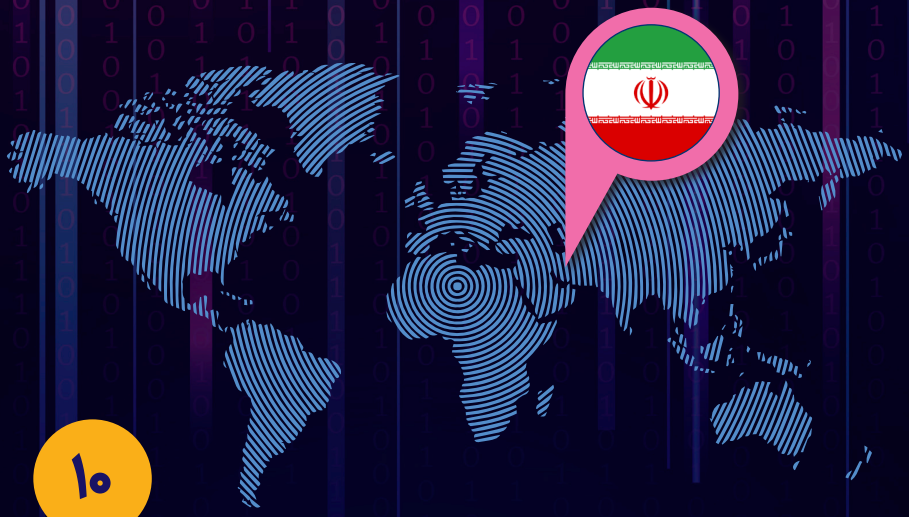
۴. کاخ سفید، رجوع شود به:

'Press Briefing by Press Secretary Jen Psaki and Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger, February 17, 2021', https://www.whitehouse.gov/briefing-room/press-briefings/2021/02/17/press-briefing-by-press-secretary-jen-psaki-and-deputy-nationalsecurity-advisor-for-cyber-and-emerging-technology-anneneuberger-february-17-2021.

فناوری‌های پیشرفته و دقیقی که آمریکا و متحدانش در عملیات‌های جنگی با شدت بالا استفاده می‌کنند، بسیاری از روش‌ها و ابزارهای مورداستفاده روسیه غیرتخصصی و با دقت پایین هستند. به‌عنوان نمونه، نمی‌توان ارزیابی دقیقی از تفاوت توانمندی روسیه در قیاس با توانمندی آمریکا و رژیم صهیونیستی در عملیات استاکس‌نت علیه ایران در بازه زمانی ۲۰۰۸ الی ۲۰۱۰ ارائه داد.

می‌توان گفت تلاش روسیه در عرصه‌های بین‌المللی برای غیرقانونی خواندن استفاده نظامی از ابزارهای سایبری تهاجمی بیانگر اعتراف ضمنی این کشور به ضعف خود در مقایسه با آمریکا و هم‌پیمانانش است.





۱۰

ج.ا.ایران

ایـران خـود را در معرض جنگ اطلاعاتی و سـایبری با دشـمنانش می‌داند. در سـال ۲۰۱۰ همزمان با افشـای حمله ایالات متحده و رژیم صهیونیسـتی با استفاده از ویروس اسـتاکس‌نت[1] بـه ایران، این کشور دسترسـی محدودی به تامین‌کننـدگان بین‌المللی تجهیـزات امنیت سـایبری داشـت و تعـداد محققان داخلـی فعال آن نیـز بسیار اندک بـود. بـا این حال، از آن زمان به بعد ایران به یکی از بازیگران سـایبری مصمم در مقابل دشـمنانش از جملـه ایـالات متحـده و رژیم صهیونیسـتی تبدیل شده‌اسـت. در عین حال، دولت ایران به افزایش نظارت سایبری برای مقابله با مخالفان داخلی و استفاده از توانمندی‌هـای سـایبری جهـت خنثی‌سـازی تهدیدهـای خارجـی نیـاز دارد، امـا رکـود اقتصادی، آشفتگی‌های سیاسی و کمبودهای داخلی بیانگر آن است که ایران نمی‌تواند به‌راحتـی یـا به‌سـرعت توانـایی دفـاع سـایبری بومـی خـود را ارتقـا بخشـد. درمجـموع، توانمندی‌هـای سـایبری ایـران بـا مقیـاس و پیچیدگـی برنامه موشـک‌های بالسـتیک یـا هسـته‌ای آن همخوانـی نـدارد. به‌عنـوان مثـال، اگرچـه ایـران بـه‌طور گسـترده‌ای از روش‌های سـایبری تهاجمی سطح پایین استفاده کرده و به موفقیت‌هایی هم در این زمینه دست یافته‌است، اما هنوز فاقد منابع، مهارت‌ها و زیرساخت‌های فنی موردنیاز برای توسعه و به‌کارگیری توانمندی‌های سایبری تهاجمی پیچیده است. درواقع، ایران قدرت سـایبری رده سـومی اسـت که از فناوری‌های سـایبری و توانمندی‌های عملیاتی نه‌چنـدان پیشـرفته‌ای بـرای پیشـبرد اهـداف راهبردی خـود ازجمله اسـتیلای قدرت و سیگنال‌دهی راهبردی استفاده می‌کند.

1. Stuxnet

راهبرد و مبنای نظری (دکترین)

رویکرد ایران نسبت به فضای سایبری اساساً ناشی از سیاست‌های اقتدارگرایانه داخلی و مواجهات بین‌المللی آن است. به‌بیان دیگر، با انتقال مالکیت شرکت مخابرات ایران[1] به سپاه پاسداران انقلاب اسلامی (IRGC)[2] در سال ۱۳۸۸ (۲۰۰۹ میلادی) پس از اعتراضات گسترده علیه دولت وقت که شبکه‌های اجتماعی یکی از محرکان اصلی آن بودند، سیاست سایبری کنونی ایران شکل گرفت[3]. البته ردپای توسعه سیاست سایبری بین‌المللی ایران را می‌توان در حملات استاکس‌نت جستجو کرد که در سال ۱۳۸۹ (۲۰۱۰ میلادی) افشا شد و ایران آن را به ایالات متحده و رژیم صهیونیستی نسبت داد.

در بسیاری از حوزه‌های مرتبط با امنیت سایبری، ایران هیچ‌گونه سند راهبردی و مبنای نظری رسمی منتشر نکرده‌است. ازاین‌رو، شاخص‌های اصلی توسعه امنیت سایبری آن را می‌توان اصلاحات سازمانی و تصویب قوانین مرتبط با این حوزه دانست. ارتش سایبری ایران[4] متشکل از گروهی از هکرهای حامی نظام، وفادار به حضرت آیت‌الله خامنه‌ای، رهبر معظم انقلاب اسلامی و احتمالا مرتبط با سپاه است که از سال ۱۳۸۸ و در پی نگرانی نیروهای محافظه‌کار از تبلیغات سیاسی ضدنظام و غرب‌گرایانه در فضای مجازی شروع به کار کرده‌اند. قرارگاه دفاع سایبری[5] در سال ۱۳۸۹ توسط نیروهای مسلح

1. Telecommunications Company
2. Islamic Revolutionary Guard Corps

۳. رجوع شود به:
Daniel Baldino and Jarrad Goold, 'Iran and the emergence of information and communications technology: The evolution of revolution?', Australian Journal of International Affairs, vol. 68, no. 1, 2014, pp. 17-35, p. 28.

4. Iranian Cyber Army
5. Cyber Defense Command

ایران ایجاد شد و نیروی پلیس سایبری (پلیس فضای تولید و تبادل اطلاعات یا فتا)[1] نیز در همین سال با هدف حفاظت از هویت ملی و مذهبی، ارزش‌های اجتماعی، آزادی قانونی و زیرساخت‌های ملی حیاتی در برابر حملات الکترونیکی تاسیس شد[2].

شورای عالی فضای مجازی[3] به دستور رهبر معظم ایران و در سال ۱۳۹۰ (۲۰۱۱ میلادی) با دو هدف اصلی تاسیس شد: بهره‌برداری کامل از پیامدهای مثبت فضای سایبری کشور و محافظت از کشور و مردم در برابر پیامدهای منفی فضای سایبری[4]. دو هدف فرعی مهم از تشکیل این شورا نیز شامل حمایت دولت از گروه‌های هکری حامی نظام و توسعه علوم، پژوهش، سیاست‌های فرهنگی و مطالعات راهبردی در حوزه فضای سایبری می‌شوند[5].

مجلس در سال ۱۳۹۱ (۲۰۱۲ میلادی) قانونی را برای ایجاد مرکز ملی فضای مجازی (NCC)[6] با اهداف گسترده سیاسی تصویب کرد. نحوه بیان جزئیات اهداف مرکز ملی فضای مجازی در این قانون مشابه اسناد راهبردی امنیت سایبری در برخی کشورهای دیگر است[7]. به‌عنوان مثال، در یکی از تبصره‌های این قانون به گسترش اقتدار کشور در حوزه توانمندی‌های فناوری اطلاعات و ارتباطات در برابر شرکت‌های قدرتمند جهانی تاکید می‌شود که مستلزم افزایش محتوای داخلی در شبکه جهانی

1. Cyber Police Force

۲. رجوع شود به:
United Nations Institute for Disarmament Research, UNIDIR Cyber Policy Portal, 'Iran (Islamic Republic of)', https://cyberpolicyportal.org/en/state-pdf-export/eyJjb3VudHJ5X2dyb3VwX2lkIjoiNjUifQ.

3. Supreme Council for Cyberspace

۴. رجوع شود به:
Small Media, 'Iranian Internet Infrastructure and Policy Report', February 2014, p. 3, https://smallmedia.org.uk/sites/default/files/u8/IIIP_Feb2014.pdf.

۵. همان، ص ۷.

6. National Cyberspace Center

۷. همان، ص ۴.

وب[1]، ترویج ایدئولوژی مذهبی و دولتی و آمادگی برای جنگ فرهنگی با دشمنان کشور است. این قانون انجام اقدامات دیپلماتیک در عرصه بین‌الملل با هدف کاهش نفوذ ابرقدرت‌ها در مدیریت اینترنت و محافظت از حقوق بین‌المللی کاربران ایرانی اینترنت را نیز ضروری می‌داند. به نظر می‌رسد مرکز ملی فضای مجازی به نمایندگی از شورای عالی فضای مجازی مسئولیت هماهنگی میان تمام سازمان‌های سایبری را برعهده دارد. شورای عالی فضای مجازی در برخی حوزه‌های سیاست‌گذاری به‌طور مستقیم با نهادهای پایین‌دستی مانند وزارت فناوری اطلاعات و ارتباطات[2] همکاری می‌کند.

بین ایران و ایالات متحده، رژیم صهیونیستی و برخی از کشورهای عربی حوزه خلیج‌فارس همچنان تنش‌های زیادی وجود دارد. می‌توان گفت پس از حملات سایبری موفق ایران به بانک‌های آمریکایی در سال ۱۳۹۱ که اقدامات تلافی‌جویانه جدی نیز در پی نداشت، ایران به این نتیجه رسید که سیاست امنیت سایبری کشور در مسیر درستی قرار دارد. یکی از سرداران سپاه در سال ۱۳۹۱ اعلام کرد که ایران چهارمین قدرت سایبری بزرگ در میان ارتش‌های سایبری جهان است[3] و طبق ادعای برخی گزارشات غیرمستند، دولت ایران ۱۲۰۰۰۰ نیروی شبه‌نظامی متخصص در عرصه سایبری دارد.

سرلشکر حسین سلامی، فرمانده کل سپاه پاسداران در سال ۱۳۹۸ (۲۰۱۹ میلادی) اعلام کرد که ایران در فضای جنگ اطلاعاتی تمام‌عیار با ایالات متحده و دیگر دشمنان انقلاب و نظام اسلامی قرار دارد و با ترکیبی از جنگ روانی و عملیات سایبری، تحریکات

1. World Wide Web
2. Ministry of Information and Communications Technology
۳. رجوع شود به:
'Iran Enjoys 4th Biggest Cyber Army in World', Ahlul Bayt News Agency, 2 February 2013, https://en.abna24. com/service/iran/archive/2013/02/02/387239/story.html.

نظامی، دیپلماسی عمومی و تاکتیک‌های ارعاب روبرو است[1]. ستاد کل نیروهای مسلح در تیرماه سال ۱۳۹۹ (جولای ۲۰۲۰) بیانیه‌ای مبنی بر دیدگاه ایران در مورد حق مقابله‌به‌مثل در برابر حملات سایبری صادر کرد که تقریبا می‌توان آن را سند رسمی راهبرد سایبری کشور تلقی کرد[2]. به‌طور کلی، تبیین مفاهیم، سیاست‌های کلان و چارچوب فعالیت‌های نیروهای مسلح به‌منظور مقابله با افزایش تعداد و تنوع تهدیدهای فضای سایبری هدف از صدور این بیانیه به شمار می‌آمد. در این بیانیه چنین آمده‌است که ایران «هرگونه استفاده عامدانه از نیروی سایبری با پیامدهای ملموس یا غیرملموس» در مرزهای کشور را نقض حاکمیت خود می‌داند و در صورتی که عملیات سایبری از آستانه‌ی «حمله مسلحانه متعارف» فراتر رود، حق قانونی مقابله‌به‌مثل را برای نیروی‌های نظامی خود محفوظ می‌داند.

درمجموع، دیدگاه راهبردی ایران تاثیر زیادی بر رویکرد آن در رابطه با تهدیدها و فرصت‌های فضای سایبری دارد. این مسأله به‌طور ویژه در مورد نظریه (دکترین) عمق راهبردی[3] ایران صدق می‌کند که هدف از آن اقدام علیه دشمنان دیرینه منطقه‌ای کشور (ازجمله رژیم صهیونیستی) است و استفاده از فرصت نفوذ به شبکه‌های ایالات متحده را ضروری می‌داند. به‌طور کلی، قابلیت‌های سایبری ایران بیشتر حاصل رقابت‌های درون‌سازمانی است و همانند راهبرد کلی آن، رویکرد مورداستفاده آن در فضای سایبری نیز از دوگانگی ذاتی رنج می‌برد.

---

۱. رجوع شود به:
Zak Doffman, 'Iran: "We Will Beat U.S. in Intelligence War" and "Punish Mistakes With Crushing Strikes"', Forbes, 19 May 2019,
https://www.forbes.com/sites/zakdoffman/2019/05/19/iranwe-will-beat-u-s-in-intelligence war-and-punish-mistakeswith-crushing-strikes/?sh=9a225d25e16d.

۲. رجوع شود به:
'General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat', Fars News Agency, 17 August 2020,
https://www.farsnews.ir/en/news/13990527000544/General-Safff-Iranian-Armed-Frces-Warns-f-Tgh-Reacin-Any-Cyber-Threa.

3. Doctrine of Strategic Depth

حکمرانی، فرماندهی و نظارت

شورای عالی فضای مجازی که رئیس‌جمهور ریاست آن را به‌عهده دارد، عالی‌ترین نهاد سیاست‌گذار ایران در زمینه فضای سایبری است. این شورا شامل ۲۷ عضو از بخش‌های مختلف دولت و جامعه ازجمله نیروهای مسلح، سپاه پاسداران انقلاب اسلامی، قوه قضائیه، مجلس شورای اسلامی، سازمان صدا و سیما، پلیس، وزارت ارتباطات و فناوری اطلاعات، وزارت اطلاعات، وزارت فرهنگ و ارشاد اسلامی و وزارت علوم، تحقیقات و فناوری می‌شود. شورای عالی فضای سایبری موظف به نظارت بر اعمال سیاست‌های سانسور در اینترنت، تنظیم نقاط تبادل اینترنت داخلی (IXP)[1]، جداسازی شبکه و فیلترکردن محتوا است[2]. مهم‌ترین سازمان‌های ذی‌ربط در حوزه سایبری ایران به شرح زیر هستند:

- مرکز ملی فضای مجازی؛
- سازمان ملی پدافند غیرعامل (NPDO)[3] که مسئولیت دفاع غیرنظامی سایبری و حفاظت از زیرساخت‌های حیاتی کشور را برعهده دارد؛
- پلیس سایبری؛
- سازمان اطلاعات سپاه (IRGC-IO)[4] که مسئولیت عملیات سایبری تهاجمی را برعهده دارد؛
- مرکز فرماندهی دفاع سایبری که بخشی از نیروهای مسلح است و در عملیات سایبری تهاجمی مشارکت می‌کند؛

1. Internet Exchange Points

۲. رجوع شود به:
Official Gazette of Iran, 'Mosavabbe shoraye aali fazaye majazi dar khosoos siyasat haye hakem bar rah andazi noghat tabadol terrafik dakheili (IXP) va ijad tamayoz beyne', 22 March 2013, http://www.rooznamehrasmi.ir/laws/ShowLaw.aspx?Code=1152.

3. National Passive Defense Organization
4. IRGC Intelligence Organization

- وزارت اطلاعات[1] که مسئولیت اطلاعات سیگنال‌ها را برعهده دارد؛ و
- سازمان‌های حفاظت اطلاعات[2] در نیروهای مسلح و دیگر نهادهای دولتی[3].

بنابراین، در ایران پنج مجرای اصلی برای فرماندهی این حوزه وجود دارد: مرکز ملی فضای مجازی، سپاه پاسداران انقلاب اسلامی، نیروهای مسلح، وزارت اطلاعات و بخش غیرنظامی (شامل سازمان پدافند غیرعامل و پلیس که اغلب برای کسب نفوذ بیشتر با یکدیگر رقابت می‌کنند). سپاه پاسداران ازطریق بسیج-نیروهای شبه‌نظامی زیرمجموعه سپاه-واحدهای سایبری و نیروهای نیابتی خود ازجمله سازمان جنگ الکترونیکی و دفاع سایبری سپاه پاسداران[4] و شورای سایبری بسیج[5] را فرماندهی می‌کند[6].

حکمرانی سیاست سایبری ایران تحت‌تاثیر مسائلی همچون تنش‌های سیاسی کشور در دو دهه اخیر، احساس قربانی بودن در تقابلات و تحریم‌های بین‌المللی و ضرورت شکست دادن دشمنان داخلی و خارجی کشور شکل گرفته‌است. ایران در جنگ‌های نیابتی در عراق، سوریه و یمن شرکت داشته‌است و همواره با نیروهای آمریکایی و رژیم صهیونیستی در منطقه تنش‌های نظامی دارد. شورای عالی فضای مجازی انجمنی چندذینفعی به‌شمار می‌رود که وظیفه تامین نیازهای غیرسیاسی و غیرنظامی شرکت‌های تجاری مانند امنیت سایبری را برعهده دارد. اگرچه این شورا

1. Ministry of Intelligence
2. Intelligence Protection Organizations
۳. سازمان‌های حفاظت اطلاعات ضمن اینکه سازمان‌های ضدجاسوسی محسوب می‌شوند، به‌عنوان پلیس سیاسی برای مقابله با مخالفان دولت نیز عمل می‌کنند.
4. Electronic Warfare and Cyber Defense Organization
5. Basij Cyber Council
۶. رجوع شود به:
Congressional Research Service, 'Iranian Offensive Cyber Attack Capabilities', 13 January 2020, https://fas.org/sgp/crs/mideast/IF11406.pdf.

واقعا نقش فوق را ایفا می‌کند، اما امنیت ملی همیشه در اولویت آن بوده و از سال ۱۳۹۹ با ترور سردار سرلشکر سپهبد شهید قاسم سلیمانی، فرمانده نیروی قدس سپاه پاسداران[1] و محسن فخری‌زاده که هدایت برنامه هسته‌ای ایران را بیش از دو دهه برعهده داشت نیز اهمیت آن تشدید شده‌است[2].

تیم ملی پاسخ فوری رایانه‌ای ایران زیرنظر وزارت ارتباطات و فناوری اطلاعات فعالیت دارد و با مراکز داخلی (مانند پلیس سایبری، سازمان پدافند غیرعامل، مراکز امنیت سایبری در دانشگاه‌های ایران و تیم‌های پاسخ فوری رایانه‌ای خارجی) در زمینه حفاظت از فضای سایبری کشور، بررسی یا کاهش حوادث و صدور هشدارها همکاری می‌کند[3].

توانمندی‌های محوری در زمینه اطلاعات سایبری

وزارت اطلاعات مرجع اصلی امور اطلاعاتی در ایران است. اگرچه این نهاد یکی از وزارتخانه‌های دولت به‌شمار می‌رود و وزیر آن نیز توسط رئیس‌جمهور (مشروط به تایید رهبر) تعیین می‌شود، اما بیشتر به‌صورت دستگاه اجرایی مستقلی عمل می‌کند. این سازمان موظف به رصد تهدیدهای سیاسی داخلی، جمع‌آوری اطلاعات

1. Quds Force in the IRGC

رجوع شود به:
'Qasem Soleimani: US strike on Iran general was unlawful, UN expert says', BBC News, 9 July 2020, https://www.bbc.com/news/world-middle-east-53345885

به گزارش بی‌بی‌سی، سردار سلیمانی یکی از قدرتمندترین مقامات اطلاعاتی ایران بود و وظایف متعددی ازجمله رهبری مأموریت‌های مخفی در کشورهای دیگر را برعهده داشت.

۲. رجوع شود به:
'Mohsen Fakhrizadeh: "Machine-gun with AI" used to kill Iran scientist', BBC News, 7 December 2020, https://www.bbc.com/news/world-middle-east-55214359.

۳. رجوع شود به:
'Markazeh modiriyat emdaad va hamahangie amaliyate rokhdad haye rayaneh ei', https://cert.ir/index.

خارجی و انجام عملیات ضدجاسوسی است[۱]. علاوه بر این‌ها، وزارت اطلاعات بر همه عملیات‌های پنهانی نظارت می‌کند و معمولا خود نیز مجری عملیات‌های داخلی است. وزارت اطلاعات ایران با سازمان‌های اطلاعاتی خارجی به‌ویژه سازمان اطلاعات خارجی روسیه[۲] نیز همکاری می‌کند. توانمندی‌های ایران در زمینه اطلاعات سایبری احتمالا تحت‌تاثیر موازی‌کاری و رقابت بین دو نهاد اطلاعاتی اصلی کشور یعنی سازمان اطلاعات سپاه و وزارت اطلاعات قرار دارد[۳]. به‌نظر می‌رسد سازمان اطلاعات سپاه قدرتمندترین نهاد امنیتی در ایران است و نقش اساسی را در عملیات‌های سایبری خارجی و داخلی و همچنین سیاست‌گذاری این حوزه ایفا می‌کند[۴].

رژیم صهیونیستی از نظر دسترسی به اطلاعات منطقه‌ای برتری قابل‌توجهی نسبت به ایران دارد و استاکس‌نت تنها نمونه کوچکی از قدرت آن است. اگرچه عملیات سایبری ایران در شبکه‌هایی در ایالات متحده، انگلستان و سایر کشورها شناسایی شده‌است، اما ماهیت تجربی و ساده این عملیات‌ها بیانگر آن است که ایران دسترسی چندانی به اطلاعات سایبری جهانی ندارد. البته باید دید که آیا ایران توانسته‌است در جنگ سوریه به‌واسطه همکاری نزدیکش با روسیه توانمندی‌های سایبری خود را ارتقا بخشد.

---

۱. رجوع شود به:
Carl Anthony Wege, 'Iran's Intelligence Establishment', Intelligencer, Summer 2015, pp. 64-5, https://www.afio.com/publications/WEGE%20Iranian%20Intel%20Services%202015%20Sep%2001%20FINAL.pdf.

2. Russia's External Intelligence Service

۳. رجوع شود به:
Eric Randolph, 'Iranian IRGC consolidates primacy in intelligence operations', Janes, 19 August 2020, https://www.janes.com/defence-news/news-detail/iranian-irgc-consolidates-primacy-in-intelligence-operations.

۴. رجوع شود به:
Insikt Group, 'Despite Infighting and Volatility, Iran Maintains Aggressive Cyber Operations Structure', Recorded Future, 2020, pp. 13-21, https://go.recordedfuture.com/hubfs/reports/cta-2020-0409.pdf.

اطلاعـات زیادی درباره تعداد نیروهای اطلاعات سـایبری ایـران و یا میزان مهارت آن‌ها در دسـت نیسـت. بودجه سـایبری (منتشر شـده) ایران در مقایسـه با کشورهایی مانند انگلسـتان بسیار اندک اسـت و این کشور با کمبود نیروهای ماهر و دارای تعهد سیاسـی لازم روبرو است. درست به همین دلیل است که ایران در اکثر عملیات‌های سایبری خود از فنون بسیار مقدماتی استفاده می‌کند و دولت بسیاری از این عملیات‌ها را به نهادهای دیگر-به‌ویژه به موسسات تحقیقاتی-برون‌سپاری می‌کند [۱].

توانمندی و وابستگی سایبری

علی‌رغـم اهـداف بلندپروازانـه زیـادی کـه دولـت ایـران در ارتباط بـا اقتصـاد دیجیتال تعییـن کرده‌اسـت، اقدامـات آن از عمـق زیـادی بـرخوردار نیسـت. دولت در سـال ۱۳۹۹ اعلام کـرد کـه بخـش دیجیتـال ۶/۵ درصد از تولیـد ناخالص داخلی این کشور را تشـکیل می‌دهـد کـه در مقایسـه بـا میانگیـن جهانـی ۱۵/۵ درصـد رقـم نـاچیزی اسـت[۲]. در اواخر سـال ۱۳۹۸ (ابتدای سـال ۲۰۲۰ میلادی)، شورای عالی فضای مجازی برنامه پنج سـاله‌ای[۳] را مـطرح کـرد که براسـاس آن مقرر شـد سـهم اقتصاد دیجیتـال تا پایان سـال ۱۴۰۳ (۲۰۲۵

۱. رجوع شود به:
Levi Gundert, Sanil Chohan and Greg Lesnewich, 'Iran's Hacker Hierarchy Exposed: How the Islamic Republic of Iran Uses Contractors and Universities to Conduct Cyber Operations', Future', 2018, https://go.recordedfuture.com/ hubfs/reports/cta-2018-0509.pdf.

۲. رجوع شود به:
'Iran Unveils Four Mega Projects to Boost Digital Economy', IFP News, 28 May 2020, https://ifpnews.com/iran-unveils-fourmega-projects-to-boost-digital-economy.

برای کسب اطلاعات مربوط به ارزیابی اقتصاددانان ایرانی رجوع شود به:
Amir Hossein Mozayani and Niloofar Moradhassel, 'How Much Has ICT Contributed to Iran Economic Growth', International Journal of Economics and Politics, vol. 1, no. 1, 2020, pp. 57-68, http://jep.sbu.ac.ir/article_87384.html.

۳. رجوع شود به:
'Iran Gov't Outlines Projects to Expand Digital Economy', Financial Tribune, 2 February 2020, https://financialtribune.com/articles/sci-tech/101979/iran-gov-t-outlines-projects-to-expanddigital-economy.

میلادی) به ۱۰ درصد از تولید ناخالص داخلی کشور افزایش یابد. اگرچه این نرخ رشد به‌نوبه خود چشمگیر است، اما در مقایسه با سهم بخش فناوری اطلاعات و ارتباطات در رقبای اصلی ایران یعنی ایالات متحده و رژیم صهیونیستی بسیار ناچیز است. ازجمله اهداف ایران در سال ۱۴۰۳ می‌توان به توسعه زیرساخت‌های اینترنت و تلفن همراه در ۸۰ درصد از مناطق روستایی با بیش از ۲۰ خانوار و همچنین فراهم‌کردن دسترسی به اینترنت پهن‌باند (با سرعت حداقل ۲۰ مگابیت بر ثانیه) برای ۸۰ درصد از خانوارهای ایرانی اشاره کرد[۱]. طبق یک مطالعه پیمایشی جهانی در مورد شمول دیجیتال در دوره ۲۰۲۰-۲۰۱۷، ایران در میان ده کشور برتر دارای بیشترین رشد قرار دارد. البته همان‌طور که پیش از این نیز اشاره شد، ایران در زمینه توسعه دیجیتال هنوز در مرحله ابتدایی قرار دارد و این کشور دارای رتبه جهانی ۳۷ در این زمینه است[۲].

وزارت ارتباطات و فناوری اطلاعات ایران در سال ۱۳۹۹ چندین پروژه زیرساختی را با هدف تقویت اقتصاد دیجیتال کشور آغاز کرد. ساخت مرکز داده در تهران، توسعه شبکه ملی اطلاعات[۳] (اینترنت داخلی با محوریت کنترل شدید دولت که از سال ۱۳۹۲ (۲۰۱۳ میلادی) در حال ساخت است) و برنامه حمایت از کسب‌وکارهای دیجیتالیِ متاثر از همه‌گیری کوید-۱۹ ازجمله این پروژه‌ها به شمار می‌آیند[۴]. مرکز داده تهران

۱. رجوع شود به:
Jamal Sophieh, 'An Overview of Digital Economy and Digital Transformation in Iran', Ministry of Information and Communications Technology, workshop presentation, July 2019, p. 22, https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2019/ jul-iran-dtx/Workshop-on-%E2%80%9CDigital Transformation-in-Digital-Economy%E2%80%9D/Session%2014%20-%20Iran.pdf.

۲. رجوع شود به:
'Qatar, UAE, Iran and Egypt Making Big Strides in Digital Inclusion', Consultancy-me.com, 3 March 2021, https://www.consultancy-me.com/news/3430/qatar-uae-iran-and-egyptmaking-big-strides-in-digital-inclusion.

3. National Information Network

۴. رجوع شود به:
'Iran Unveils Four Mega Projects to Boost Digital Economy', Iran Front Page, 28 May 2020, https://ifpnews.com/ iran-unveils-four-mega-projects-to-boost-digital-economy.

که با بودجه اولیه ۶۳ میلیون دلار تاسیس شده‌است، امکان افزایش ظرفیت کلی داده‌های کشور تا حدود ۲۵ درصد را فراهم آورده‌است. مرکز داده بزرگی نیز در تبریز ساخته شده‌است که به پایداری زیرساخت شبکه ایران و ارتقای ظرفیت آن در زمینه رایانش ابری کمک می‌کند[۱].

ایران در برخی از زمینه‌های تحقیقات علمی ازجمله حوزه‌های خاصی از هوش مصنوعی در بین ۲۰ کشور برتر جهان قرار دارد[۲]. تهران نیز از نظر تحقیقات مستعد دریافت پتنت در فهرست ۵۰ شهر برتر دارای خوشه‌های تحقیقاتی قرار گرفته است[۳]. با این حال، میزان سرمایه‌گذاری ایران در حوزه تحقیق و توسعه فناوری اطلاعات و ارتباطات در هر دو حوزه غیرنظامی و نظامی احتمالا کمتر از سایر کشورهایی است که اهداف بزرگی در این حوزه در سر دارند. زیرا ایران کمتر از ۱ درصد از تولید ناخالص داخلی خود را برای تحقیق و توسعه دولتی در تمام بخش‌ها صرف می‌کند که البته این رقم با روایت‌های دولت درباره اهداف بزرگ علمی آن مغایرت دارد[۴]. تحریم‌های بین‌المللی علیه ایران نیز محیط کسب‌وکار شرکت‌های نوپای فعال در حوزه فناوری را تضعیف کرده و درنتیجه،

۱. رجوع شود به:
'Iran to Open Second Largest Data Center over Weekend: Minister', Pars Today, 25 June 2020, https://parstoday.com/en/news/iran-i122999

۲. رجوع شود به:
S.F. Wamba et al., 'Are we preparing for a good AI society? A bibliometric review and research agenda', Technological Forecasting and Social Change, 2020, https://www.sciencedirect.com/science/article/abs/pii/S0040162520313081?dgcid=rss_sd_all;
Jiqiang Niu et al., 'Global research on artificial intelligence from 1990-2014: Spatially-explicit bibliometric analysis', ISPRS International Journal of Geo-Information, vol. 5,no. 66, pp. 7-9, https://www.mdpi.com/2220-9964/5/5/66/pdf.

۳. رجوع شود به:
Kyle Bergquist and Carsten Fink, 'The Top 100 Science and Technology Clusters', World Intellectual Property Organisation, 2020, p. 44, https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2020-chapter2.pdf.

۴. رجوع شود به:
Mehdi Garshasbi, 'R&D still unappreciated', Tehran Times, 2 January 2021, https://www.tehrantimes.com/ news/456487/R-D-still-unappreciated.

این شرکت‌ها شاهد رشد محدودی هستند. اگرچه شرکت‌های نوپای ایران در سال‌های ۱۳۹۲ تا ۱۳۹۵ (۲۰۱۳ تا ۲۰۱۶ میلادی) رشد سریعی را تجربه کردند، اما پس از آن، بسیاری از آن‌ها متمایل به انتقال کسب‌وکار خود به خارج از کشور شده‌اند[۱]. براساس برآوردهای غیررسمی، این شرکت‌ها در سال ۱۳۹۷ (۲۰۱۸ میلادی) کمتر از ۱ درصد از تولید ناخالص داخلی کشور را تشکیل می‌دادند[۲].

محیط سیاسی اقتدارگرا و پیامدهای رویارویی ژئوپلیتیک با کشورهای غربی به‌ویژه تحریم‌های مربوط به عدم‌شفافیت ایران در تعهدات هسته‌ای بین‌المللی، توسعه اقتصاد دیجیتال این کشور را مختل کرده‌است. سازمان ملل تحریم‌های متعددی علیه ایران در سال‌های ۱۳۸۵ الی ۱۳۹۴ (۲۰۰۶ تا ۲۰۱۵ میلادی) اعمال کرد و ایالات متحده نیز پس از خروج از برنامه جامع اقدام مشترک (برجام)[۳] در سال ۱۳۹۷ بار دیگر ایران را تحریم کرد. تولید ناخالص داخلی ایران در دو سال اول برجام (۱۳۹۵ و ۱۳۹۶) به‌ترتیب ۱۲/۵ و ۳/۷ درصد افزایش یافت، اما با بازگشت تحریم‌های ایالات متحده در سال ۱۳۹۷ به ۵/۴ درصد و در سال ۱۳۹۸ به ۶/۵ درصد کاهش یافت[۴]. حتی در صورت لغو کامل تحریم‌های هسته‌ای نیز مخالفت کشورهای غربی با سایر جنبه‌های سیاست ایران (مانند حمایت از حزب‌الله در لبنان و مقابله با رژیم صهیونیستی) باعث محدودیت تجارت این کشور

۱. رجوع شود به:
Mohsen Tavakol, 'Sanctions and Domestic Constraints Cripple Iran's Startups', Atlantic Council, 7 February 2020,
https://www.atlanticcouncil.org/blogs/iransource/sanctions-and-domesticconstraints-cripple-irans-startups/.

۲. رجوع شود به:
Najmeh Bozorgmehr, 'Start-up Republic: Can Iran's Booming Tech Sector Thrive?', Financial Times, 17 April 2018,
https://www.ft.com/content/ca7ab580-3d71-11e8-b9f9-de94fa33a81e.

3. Joint Comprehensive Plan of Action (JCPOA)

۴. رجوع شود به:
International Monetary Fund, 'Islamic Republic of Iran', October 2020,
https://www.imf.org/en/Countries/IRN.

در حوزه فناوری اطلاعات و ارتباطات با شرکت‌های اروپایی، آمریکای شمالی، ژاپنی و کره‌جنوبی خواهد شد.

در میان کشورهایی که تحقیقات هوش مصنوعی را با جدیت پیگیری کرده‌اند، ایران کمترین پیشرفت را داشته‌است. به‌عنوان مثال، ایران موفق به کسب رتبه ۳۳ در رتبه‌بندی مبتنی بر میزان مشارکت کشورها در دو کنفرانس معتبر هوش مصنوعی در سال ۲۰۲۰ شده‌است[۱]. با این حال، ایران در زمینه تحقیقات انجام‌شده در حوزه کاربرد فناوری هوش مصنوعی در بهداشت یا پزشکی رتبه بالاتری کسب کرده‌است. به‌عنوان مثال، ایران در فهرست کشورهای برتر از نظر تعداد مقالات منتشرشده رتبه دوازدهم و از نظر میزان ارجاع رتبه شانزدهم را به‌دست آورده‌است[۲]. ایران در پی آن است تا ظرفیت‌های تحقیقاتی خود در حوزه هوش مصنوعی را ازطریق همکاری با روسیه تقویت کند[۳]. ایران تاکنون چندین استفاده موفق از فناوری هوش مصنوعی در حوزه نظامی داشته‌است. به‌عنوان مثال، ایران در رزمایش‌های گسترده پهپادهای تهاجمی[۴] و همچنین هماهنگ‌کردن هرچه بیشتر تجهیزات نظامی در زمین، دریا و هوا از این فناوری استفاده کرده‌است[۵].

۱. رجوع شود به:
Gleb Chuvpilo, 'AI Research Rankings 2020: Can the United States Stay Ahead of China?', 21 December 2020, https://chuvpilo.medium.com/ai-research-rankings-2020-can-theunited-states-stay-ahead-of-china-61cf14b1216.

۲. رجوع شود به:
Bach Xuan Tran et al., 'Global evolution of research in artificial intelligence in health and medicine: A bibliometric study', Journal of Clinical Medicine, vol. 8, no. 3, 14 March 2019, p. 9, https://www.mdpi.com/2077-0383/8/3/360/pdf.

۳. رجوع شود به:
'Iran, Russia to Cooperate on Artificial Intelligence Research', Islamic Republic News Agency, 3 September 2020, https://en.irna.ir/news/84025992/Iran-Russia-to-cooperate-on-artificial-intelligenceresearch.

۴. رجوع شود به:
'Iran uses "artificial Intelligence" in drone drill', Mehr News Agency, 7 January 2021, https://en.mehrnews.com/news/168208/Iran-uses-artificial-intelligence-in-drone-drill.

۵. رجوع شود به:
Michael Rubin, 'Even Iran Wants an AI-Powered Military Drones', National Interest, 25 December 2020, https://nationalinterest.org/blog/reboot/even-iran-wants-ai-poweredmilitary-drones-175202.

برنامه فضایی ایران در طول دو دهه گذشته با مشارکت بخش علمی غیرنظامی و حضور جدی بخش نظامی (به‌ویژه برنامه موشک‌های بالستیک) به‌آرامی توسعه یافته‌است[۱]. ایران برنامه پرتاب ماهواره تحقیقاتی غیرنظامی را از سال ۱۳۸۸ آغاز کرده‌است. سپاه پاسداران پس از چندین پرتاب ناموفقِ ماهواره‌های غیرنظامی در سال‌های ۱۳۹۸-۱۳۹۹ (۲۰۱۹ الی ۲۰۲۰ میلادی)، بالاخره در فروردین ۱۳۹۹ توانست اولین ماهواره شناسایی نظامی خود به نام «نور» را با استفاده از پرتابگری ناشناخته با موفقیت در مدار قرار دهد[۲]. باآنکه ماهواره نور قرار است برای جمع‌آوری اطلاعات و تامین امنیت ارتباطات نظامی استفاده شود، اما پیشرفت ایران در پرتاب‌های ماهواره‌ای موجب نگرانی دیگر کشورها شده‌است. زیرا این کشورها احتمال می‌دهند که ایران این فناوری را در برنامه موشکی خود نیز به‌کارگیرد[۳]. ایران در بهمن ۱۳۹۹ (فوریه سال ۲۰۲۱) نیز با موفقیت موشک ماهواره‌بر جدیدی با قابلیت حمل ماهواره ۲۲۰ کیلوگرمی آزمایش کرد[۴].

امنیت و تاب‌آوری سایبری

ایران تاکنون راهبرد هدفمندی در حوزه سایبری منتشر نکرده‌است، البته این بدان معنا نیست که این کشور هیچ راهبرد منسجمی در این حوزه ندارد. شایان ذکر است

۱. رجوع شود به:
Andrew Hanna, 'Iran's Ambitious Space Program', The Iran Primer, United States Institute for Peace, updated 1February 2021,
https://iranprimer.usip.org/blog/2020/jun/23/iran%E2%80%99s-ambitious-space-program.

۲. رجوع شود به:
'Iran Launches Its First Military Satellite', Al-Jazeera, 22 April 2020,
https://www.aljazeera.com/news/2020/4/22/ iran-launches-its-first-military-satellite.

۳. رجوع شود به:
Michael Elleman and Mahsa Rouhi, 'The IRGC Gets into the Space-Launch Business', International Institute for Strategic Studies blog, 1 May 2020,
https://www.iiss.org/blogs/analysis/2020/05/iran-military-satellite-launch-irgc.

4. Hanna, 'Iran's Ambitious Space Program'.

کـه تهـران اقدامات مناسـبی در جهت تقویـت نظام رسیدگـی به موارد اضطراری سـایبری انجام داده‌اسـت. به‌عنوان مثال، سـازمان پدافنـد غیرعامل به‌عنوان نهادی شـبه‌نظامی متشکل از نیروهای سپاه و بسیج وظیفه حفاظت از زیرساخت‌های حیاتی ملی را برعهده دارد و نقـش و بودجـه ایـن سـازمان از زمـان شـکل‌گیری آن در سـال ۱۳۸۲ (۲۰۰۳ میلادی) همواره رو به افزایش بوده‌است[۱].

وزارت ارتباطات و فنـاوری اطلاعـات ایـران مسـئولیت توسـعه شـبکه ملـی اطلاعـات را برعهـده دارد کـه بـا هـدف تقویـت امنیـت مراکـز داده داخلـی و فراهم‌کـردن پهنـای باندِ لازم تشـکیل شده‌اسـت. مطابـق آیین‌نامـه تشـکیل شورای عالـی فضـای مجـازی، افزایـش آموزش‌هـای سـایبری در سـطح ملـی و همچنیـن تقویـت سیسـتم‌های شناسـایی، هشـدار و اشـتراک‌گذاری اطلاعـات در ایـران ضروری اسـت[۲]. سـازمان پدافنـد غیرعامـل از سـال ۱۳۸۹ رزمایش‌هـای محـدودی در زمینـه دفـاع سـایبری برگـزار می‌کنـد[۳] و سـایر سـازمان‌ها نیـز از آن پـس رزمایش‌هـای پراکنـده‌ای برگـزار کرده‌انـد. مرکـز ملـی

۱. رجوع شود به:
Farzin Nadimi, 'Iran's Passive Defense Organisation: Another Target for Sanctions', The Washington Institute, 16 August 2018,
https://www.washingtoninstitute.org/policy-analysis/view/irans-passive-defense-organization-another-target-for-sanctions.

۲. رجوع شود به:
Mehdi Safari, Hesam Seyedin and Katayoun Jahangiri,'Disaster risk governance in Iran: Document analysis', Journal of Education and Health Promotion, vol. 8, 2019, Table 5,
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6691616.

۳. رجوع شود به:
BBC Monitoring, 'Iranian Passive Defense Organization organizes "cyber exercises"', Islamic Republic News Agency, 21 August 2011.

سـردار سـرتیپ غلامرضـا جلالی رئیس سـازمان پدافنـد غیرعامـل در مهـر مـاه سـال ۱۳۹۸ از برگـزاری پنـج رزمایـش از ۱ فروردیـن ۱۳۹۷ (۲۱ مـارس ۲۰۱۸) تـا ۲۹ اسـفند ۱۳۹۸ (۲۰ مـارس ۲۰۱۹) بـا محوریـت «کارکـرد فضـای سـایبری و اینترنـت» خبـر داد. ازجملـه نتایـج بـه دسـت آمـده ایـن بـود کـه «۸۵ درصـد از زیرسـاخت‌های کشـور در صـورت قطـع اینترنـت می‌تواننـد بـه فعالیـت خـود ادامـه دهنـد». وی همچنیـن از برنامـه‌ریزی بـرای انجـام ۶۴ رزمایـش طـی دو مـاه آینـده خبـر داد.
رجوع شود به:
'Tehran: No Sign of US Cyber Attack after Drone Downing', Fars News Agency, 21 October 2019,
https://www.farsnews.ir/en/news/13980729000775/Tehran-N-Sign-f-US-Cyber-Aack-afer-Drne-Dwning.

فضای مجازی در سال ۱۳۹۷ کارگروه ویژه‌ای برای مقابله با عملیات سایبری ایالات متحده تشکیل داد و نیروهای مسلح نیز از ساخت سامانه ارتباطی جدید و ایمنی خبر داد که طراحی و ساخت آن در داخل کشور انجام شده‌بود[۱]. وزارت ارتباطات و فناوری اطلاعات نیز در سال ۱۳۹۸ (۲۰۱۹ میلادی) اعلام کرد که برنامه دفاع سایبری خود به نام «سپر دیجیتال» را اجرا کرده‌است[۲]. با این حال، توانایی‌های علمی ایران در زمینه دفاع سایبری پیشرفت زیادی نکرده‌است و باتوجه به ماهیت برنامه‌های دولت به نظر نمی‌رسد به‌زودی تغییر محسوسی در این روند رخ دهد[۳].

ایران در شاخص جهانی امنیت سایبری (۲۰۱۸) که از سوی اتحادیه بین‌المللی مخابرات (ITU) منتشر می‌شود، رتبه ۶۰ را در میان ۱۷۵ کشور جهان به خود اختصاص داد[۴]. پیش از این تاریخ نیز اتحادیه بین‌المللی مخابرات فقدان چارچوب‌های رسمی امنیت سایبری ملی در ایران ازجمله در زمینه اجرای استانداردهای معتبر و

---

۱. رجوع شود به:
'Defense Minister unveils Iran's new cyber achievements', Iran Press, 22 December 2018, https://iranpress.com/en/iran-i130976-defense_minister_unveils_iran's_new_cyber_achievements.

2. Digital Fortress

رجوع شود به:
Khosro Kalbasi, 'Iran Sets Up Digital Fortress to Forestall Rising Cyber Threats', Financial Tribune, 19 May 2019, https://financialtribune.com/articles/sci-tech/98058/iran-sets-up-digitalfortress-to-forestall -rising-cyber-threats

۳. رجوع شود به:
Y.M. Ramezan et al., 'The Role and Influence of the Digital Economy on the Strategic Model for Development of Cryptographic Science and Technology in the Islamic Republic of Iran', Journal of National Security, vol. 10, no. 35, Spring 2020, pp. 327-58, https://www.sid.ir/en/journal/ViewPaper.aspx?ID=749286.

مجله امنیت ملی توسط دانشگاه و پژوهشگاه عالی دفاع و تحقیقات راهبردی ایران منتشر می‌شود. نویسندگان مقاله در چکیده آن، مساله اصلی را فقدان مدلی با طراحی خوب و راهبردی برای توسعه علم و فناوری در حوزه رمزنگاری بیان می‌کنند.

۴. رجوع شود به:
International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 64, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

سازوکارهای صدور مجوز در بخش‌های دولتی و خصوصی را متذکر شده‌بود[۱]. علاوه بر این، ایران هنوز فاقد نظام دولتی برای ارزیابی ملی امنیت سایبری است و آیساکا (انجمن حسابرسی و کنترل سامانه‌های اطلاعاتی) که نهاد تخصصی جهانی ویژه متخصصان امنیت اطلاعات است و در ۱۸۸ کشور شعبه دارد هنوز در ایران نمایندگی رسمی ندارد[۲].

رهبری جهانی در عرصه فضای سایبری

سیاست خارجی ایران در حوزه سایبری تاکنون عمدتاً بر حملات آمریکا و رژیم صهیونیستی و به‌ویژه حمله استاکس‌نت متمرکز بوده‌است. ایران نیز همانند چین و روسیه خواهان تغییراتی در آینده فضای سایبری و همچنین به چالش کشیدن نفوذ غرب در این فضا است. با این حال، برخلاف چین (یا هند)، این کشور از منابع فنی کافی برای انجام این کار چه در سطح جهانی و چه در سطح منطقه‌ای برخوردار نیست. این کشور همچنین فاقد قدرت دیپلماتیک لازم برای تشکیل ائتلاف با سایر کشورهاست و بنابراین، نمی‌تواند تاثیر بسزایی بر سیاست سایبری بین‌المللی برجای گذارد.

با این وجود، ایران در چندین ابتکار سایبری بین‌المللی مشارکت دارد. وزارت ارتباطات و فناوری اطلاعات ایران رزمایش‌های سایبری غیرنظامی را با حضور چندین مرکز سایبری دانشگاهی کشور به‌صورت دوره‌ای و با همراهی متحدان روسی خود برگزار

۱. رجوع شود به:
International Telecommunication Union, 'Global Cybersecurity Index & Cyberwellness Profiles', 2015, p. 242, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf.

۲. آیساکا (ISACA) قبلاً با نام انجمن حسابرسی و کنترل سامانه‌های اطلاعاتی (Information Systems Audit and Control Association) شناخته شده بود، اما امروزه فقط با این نام اختصاری از آن یاد می‌شود. این نهاد مختص به تامین امنیت سیستمی است. رجوع شود به:
http://www.isaca.org

کرده‌است[1]. به‌علاوه، ایران عضو اصلی در سازمان همکاری شانگهای[2] است که همین امر یکی از مهم‌ترین ابزارهای روسیه و چین برای پیشبرد دستورکار خود در زمینه نفوذ بر اینترنت محسوب می‌شود چرا که تهران نیز رویکردی مشابه آن‌ها در این زمینه دارد. تیم ملی پاسخ فوری رایانه‌ای ایران بخشی از تیم پاسخ فوری رایانه‌ای سازمان همکاری اسلامی(OICCERT) و همچنین یکی از اعضای ائتلاف امنیت سایبری برای پیشرفت متقابل[3] به‌رهبری سازمان اینترنت و امنیت کره جنوبی[4] است. درمجموع می‌توان گفت ایران بیش از اینکه بخواهد نقش گسترده‌ای در مسائل فضای سایبری جهانی ایفا کند، اولویت اول خود را تامین امنیت سایبری کشور می‌داند.

توانمندی‌های سایبری تهاجمی

ایران برای اولین بار در سال ۱۳۸۹ یعنی زمانی که وب‌سایت یک گروه حقوق بشری داخلی را در واکنش به استفاده مخالفان از رسانه‌های اجتماعی در جریان ناآرامی‌های سال ۱۳۸۸ از دسترس خارج کرد، به استفاده از توانمندی‌های سایبری تهاجمی اذعان نمود. به احتمال زیاد از آن زمان به بعد مخالفان داخلی یکی از اهداف اصلی توانمندی‌های سایبری تهاجمی ایران هستند.

پس از افشای حمله استاکس‌نت به سانتریفیوژهای هسته‌ای ایران در سال ۱۳۸۹، ایران برای اولین بار از توانمندی‌های سایبری تهاجمی خود علیه اهداف خارجی

۱. برای کسب اطلاعات بیشتر درباره مراکزی که در این رزمایش‌ها همکاری کرده‌اند، رجوع شود به: https://cert.ir/partners.

2. Shanghai Cooperation Organization

3. Cybersecurity Alliance for Mutual Progress

در راستای دستیابی به پیشرفت متقابل، ائتلاف مذکور نهادهای دولتی، سازمان‌های عمومی و سازمان‌های غیرانتفاعی را از ۴۶ کشور (از سال ۲۰۲۰) گرد هم می‌آورد. لازم به ذکر است که اقتصاد اکثر این کشورها درحال‌توسعه است.

4. Internet and Security Agency

استفاده کرد. به‌عنوان مثال، ایران مجموعه‌ای از حملات ابتدایی از نوع منع سرویس (DoS)[1] علیه بانک‌های ایالات متحده در سال ۱۳۹۱ انجام داد[2]. در نیمه دوم سال ۱۳۹۱ (اواخر سال ۲۰۱۲ میلادی) نیز ایران به شرکت سعودی آرامکو[3] حمله کرد که عملیاتی جسورانه‌تر بود، زیرا در این حمله با استفاده از ویروس پاک‌کننده شامون (Shamoon) موفق به غیرفعال کردن ۳۰،۰۰۰ رایانه شد.

اگرچه در ایران از عملیات‌های سایبری مخل و مخرب به‌صورت محدود استفاده می‌شود، اما این عملیات‌ها یکی از اصلی‌ترین ارکان اعمال قدرت حاکمیت آن به‌شمار می‌روند[4]. اجرای عملیات اطلاعاتی در بسترهای رسانه‌های اجتماعی غربی روش جدیدی است که ایران تقریبا از سال ۱۳۹۷ به آن روی آورده‌است[5]. گفته می‌شود ایران در سال ۱۳۹۹ حمله سایبری ناموفقی به زیرساخت‌های مهم رژیم صهیونیستی (از قبیل آب و فاضلاب) کرده‌است[6]. علاوه بر این موارد، ایران حملات دیگری نیز علیه بیش از ۸۰ شرکت رژیم صهیونیستی انجام داده‌است که گمان می‌رود به‌منظور انتقام

1. Denial-of-service attacks

۲. شرح مختصری از این اقدام ایران در منبع زیر یافت می‌شود:
'U.S.-Iran Tensions: Implications for Homeland Security', Hearing before the Committee on Homeland Security, House of Representatives, 116th Congress, 2nd Session, 15 January 2020, https://www. govinfo.gov/content/pkg/CHRG-116hhrg41269/html/CHRG-116hhrg41269.htm.

3. Saudi Aramco

۴. فهرستی از حملات مشابه در سال های پس از سال ۱۳۹۱ (۲۰۱۲ میلادی) در منبع زیر یافت می‌شود:
Andrew Hanna, 'The Invisible U.S.-Iran Cyber War', The Iran Primer, United States Institute for Peace, updated 5 November 2020, https://iranprimer.usip.org/blog/2019/oct/25/invisible-us-irancyber-war.

۵. رجوع شود به:
Ed Parsons and George Michael, 'Understanding the Cyber Threat from Iran', F-Secure, undated, https://www.f-secure. com/en/consulting/our-thinking/understanding-thecyber-threat-from-iran.

۶. رجوع شود به:
Catalin Cimpanu, 'Two more cyber-attacks hit Israel's water system', ZDNet, 20 July 2020, https://www.zdnet.com/article/ two-more-cyber-attacks-hit-israels-water-system/.

ترور شـهید فخری‌زاده در آبان ۱۳۹۹ (نوامبر ۲۰۲۰) توسـط رژیم صهیونیسـتی بوده‌است[۱]. نفوذ به سیسـتم‌های بزرگ‌ترین پیمانکار دفاعی رژیم صهیونیسـتی و افشـای اطلاعات آن را می‌توان ازجمله اهداف ایران در این حملات برشـمرد[۲].

در حالـی کـه ایـران همچنان بـه عملیات سـایبری در کشورهـای دیگر ماننـد حمله به شـبکه‌های تجـاری ایـالات متحده ادامـه می‌دهد، بـه نظر می‌رسـد اکثر ایـن عملیات‌ها با هدف سـرقت داده انجام می‌شـوند. با این وجود، نقض شبکه یك سد کوچک در نزدیکی نیویورک در سـال ۲۰۱۳ یـک اسـتثنای جالـب در ایـن مورد بوده‌اسـت و از ایـن رو ممکـن اسـت تلاشـی بـرای پیش‌بینـی قابلیـت سـایبری در زیرسـاخت‌های مهـم ملـی در ایـالات متحده باشـد. اما از طرف دیگر، این موضوع نشـانگر محدودیت‌های دسترسی اطلاعات سـایبری ایران نیز اسـت، زیرا این سـد در مقایسـه با برخی از سـاختارهای عظیم برق آبی ایالات متحده بسیار کوچک است[۳].

در مجـموع، ایـران عملیات‌های سـایبری تهاجمـی خود را با انگیزه‌هـای مختلف انجام می‌دهد. تجربیات فزاینده این کشور در زمینه عملیات‌های سایبری تهاجمی نشان‌دهنده سطح بالایی از بلوغ عملیاتی آن و همچنین علاقه به استفاده از عملیات سایبری به‌عنوان

۱. رجوع شود به:
Jacob J, 'Iranian Hacker Group Pay2Key Attacks Top Israeli Defense Corporation, Leaks Data on Dark Web', International Business Times, 21 December 2020,
https://www.ibtimes.sg/iranian-hacker-group-pay2key-attackstop-israeli-defensecorporation-leaks-data-dark-web-54341.

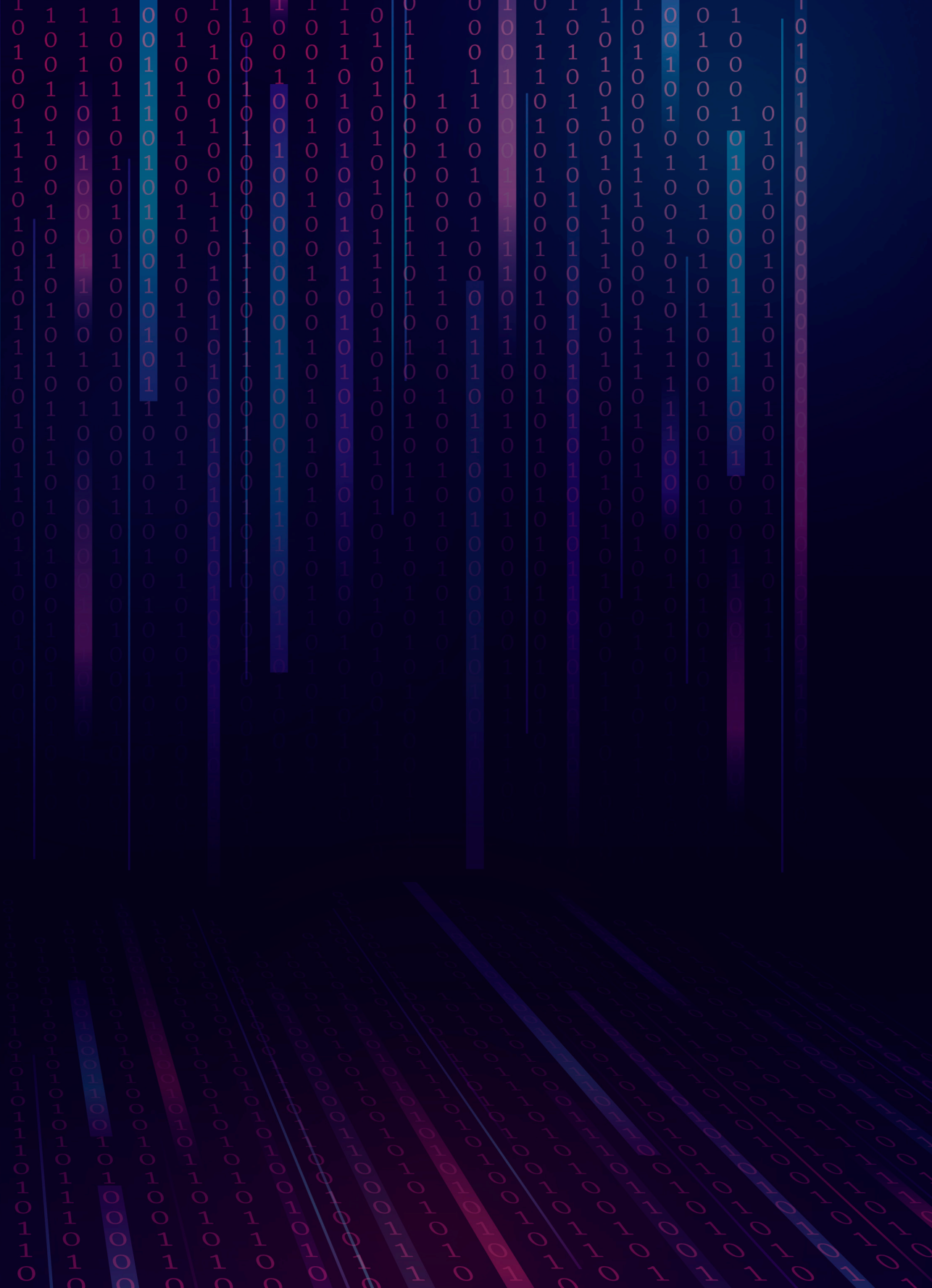
۲. رجوع شود به:
Omer Benjakob, 'Iranian Cyberattack Claims New Victim - and Israeli Hackers Vow Revenge', Haaretz, 4 January 2021,
https://www.haaretz.com/israel-news/tech-news/.premium.HIGHLIGHT-iranian-cyberattack-claims-new-victim-andisraeli-hackers-vow-revenge-1.9404606.

۳. رجوع شود به:
'Seven Iranian Hackers Indicted over Alleged Cyber Attacks Targeting US Banks and NY Dam', Trend Micro, 29 March 2016,
https://www.trendmicro.com/vinfo/de/security/news/cyber-attacks/seven-iranian-hackers-indicted-over-attacks-onbanks-ny-dam.

ابزاری مفید برای تحکیم اقتدار ملی است. جالب‌تر از همه این‌که، توانمندی‌های سایبری به ایران این امکان را داده‌اند که سطح دسترسی و نفوذ خود را در ایالات متحده افزایش دهد و این مزیتی است که با توانمندی‌های متعارف امکان‌پذیر نیست. با این حال، عملیات‌های سایبری ایران فاقد پیچیدگی‌های فنی لازم است و نشانه‌های کمی از روش‌ها یا اقدامات بومی نوآورانه در آن‌ها دیده می‌شود، به‌طوری‌که شرکت‌های غربی به‌راحتی قادر به شناسایی و ردیابی آن‌ها هستند. این امر تا حدی به‌دلیل این است که طراحی و اجرای بسیاری از این حملات به موسسات تحقیقاتی دانشگاه‌ها واگذار می‌شود. درمجموع، توانایی‌های سایبری ایران از نظر کیفیت و مقیاس بسیار کمتر از کشورهای غربی است. اگرچه تهران در حملات سایبری تهاجمی علیه عربستان سعودی[۱] و برخی از گروه‌های ضددولتی در سوریه موفق عمل کرده‌است[۲]، ولی به‌نظر می‌رسد که در سطح منطقه رژیم صهیونیستی دارای قابلیت‌های سایبری قوی‌تری است.

۱. رجوع شود به:
Seth G. Jones et al., 'Iran's Threat to Saudi Critical Infrastructure: The Implications of U.S.-Iranian Escalation', CSIS, August 2019,
https://csis-website-prod.s3.amazonaws.com/s3fspublic/publication/Jones_IransThreatSaudi _lay-out_UPDATE_09.17.pdf.

۲. رجوع شود به:
Insikt Group, 'Despite Infighting and Volatility, Iran Maintains Aggressive Cyber Operations Structure', Recorded Future, 2020, p. 16,
https://go.recordedfuture.com/hubfs/reports/cta-2020-0409.pdf.



۱۱

کره شمالی

کره شمالی به احتمال زیاد راهبرد سایبری سازمان‌یافته‌ای ندارد و عملیات‌های سایبری خود را صرفا براساس اصل فرصت‌طلبی انجام می‌دهد. اطلاعات چندانی درباره زیست‌بوم سیاست‌های سایبری این کشور در دست نیست، اما از سال ۲۰۱۵ با افشای بخش‌هایی از فعالیت‌های سایبری آن معلوم شد که بیشتر عملیات‌های کره شمالی از نوع جرائم سایبری و اخاذی سایبری جهت به‌دست‌آوردن ارزهای احتیاطی[1] است. علاوه براین، برخی از عملیات‌های سایبری این کشور از نوع عملیات‌های تلافی‌جویانه‌ای هستند که در پاسخ به توهین به رهبر حزب کارگران کره (KWP)[2] انجام می‌شوند. کنترل سیاست‌های سایبری این کشور کاملا در اختیار رهبری است و ازطریق سازوکارهای حزبی و نیروهای مسلح اعمال می‌شود. کره شمالی فاقد توانمندی در حوزه اطلاعات سایبری پیشرفته و تخصصی است. درواقع، زیست‌بوم دیجیتال این کشور بسیار ابتدایی است و تنها شامل سه تا پنج میلیون وسیله برخوردار از اینترنت -ازطریق اتصال به شبکه اینترنت داخلی (اینترنت دولتی)- می‌شود. دسترسی به اینترنت جهانی در این کشور بسیار محدود بوده و تحت‌کنترل شدید دولت قرار دارد. اتصال به اینترنت جهانی نیز صرفا ازطریق چند اپراتور محدود چینی و روسیه فراهم می‌شود و درنتیجه به علت نقاط ارتباط محدود و غیرمتنوع، اینترنت با قطعی و اختلال بسیار همراه است. درحقیقت، کره شمالی از نظر امنیت سایبری در شمار ضعیف‌ترین کشورها قرار دارد و روند توسعه بخش سایبری آن به‌دلیل انزوای خودخواسته، نبود مهارت‌های سایبری و ضعف نظام آموزشی و بخش فناوری اطلاعات و ارتباطات توسعه‌نیافته با آهنگی کند پیش می‌رود. علاوه براین،

۱. ارزهای احتیاطی (hard currency) به ارزهای با ارزش نسبتا ثابتی گفته می‌شود که به‌راحتی قابل تبدیل به ارزهای دیگر هستند. بسیاری از کشورها در مبادلات خود از این ارزها استفاده می‌کنند.

2. Korean Workers' Party

کره شمالی تاکنون تقریبا هیچ نقشی در دیپلماسی سایبری جهان نداشته‌است و روابط بین‌المللی محدودی برای حمایت از اهداف و منافع سایبری خود دارد. با وجود اشتیاق بسیار این کشور به انجام عملیات‌های سایبری تهاجمی، اما به‌دلیل ضعف مهارتی و نداشتن فنون و فناوری‌های پیشرفته و تخصصی از توانایی قابل‌ملاحظه‌ای در این حوزه برخوردار نیست. به‌عبارت دیگر، اگرچه کره شمالی در زمینه عملیات‌های سایبری تهاجمی در دنیا مشهور است، ولی از نظر قدرت سایبری در بین کشورهای رده سوم دسته‌بندی می‌شود.

راهبرد و مبنای نظری (دکترین)

درباره این‌که کره شمالی دارای راهبرد یا مبنای نظری رسمی در زمینه توانمندی‌های سایبری است، شواهد چندانی در دست نیست. اگرچه تا حدی می‌توان رویکرد کره شمالی را از اظهارات رهبر آن استنباط کرد، اما بررسی فعالیت‌های ملموس این کشور بهترین گزینه برای تخمین میزان قدرت سایبری آن است. اظهارات رسمی مقام‌های کره شمالی بیانگر نوعی نگاه لفاظانه و تفکر سنتی درباره استفاده از توانمندی‌های سایبری در نبردهای نظامی است، حال آنکه فعالیت‌های آن دال بر این هستند که اولویت‌های سایبری کره شمالی بیشتر بر نظارت و کنترل داخلی، تهدیدهای کره جنوبی، سرقت پول برای دستیابی به ارزهای احتیاطی (چون به‌دلیل تحریم‌های تجاری و مالی به آن‌ها دسترسی ندارد) و جاسوسی بیشتر برای کسب اطلاعات سامانه‌های جنگی راهبردی و در موارد معدودی نیز برای اجرای عملیات‌های تلافی‌جویانه علیه کشورهای دیگر تمرکز دارند.

به‌نقل از منابعی از کره جنوبی، رهبر کره شمالی کیم جونگ-اون[1] نقش قدرت سایبری را در رقابت‌های نظامی و سیاسی عصر جدید بسیار موثر می‌داند[2]. گزارش‌های موجود نشان می‌دهند که رهبر کره شمالی قبل از سال ۲۰۱۳ نیز جنگ سایبری را «شمشیری همه‌کاره» توصیف کرده‌بود که در کنار موشک‌ها و سلاح‌های هسته‌ای می‌تواند تضمین‌کننده برتری تمام‌عیار نیروهای مسلح کره شمالی باشد[3]. کیم جونگ-ایل[4] پدر رهبر کنونی کره شمالی نیز اظهارات مشابهی در این زمینه داشته‌است و به‌عنوان مثال در سال ۲۰۱۰ چنین گفته است: «اگر اکنون جنگ با گلوله و برای نفت است، در قرن بیست‌ویکم اطلاعات موضوع و ابزار جنگ خواهد بود. برنده جنگ کسی است که دسترسی بیشتری به اطلاعات نظامی و فنی رقیب داشته باشد، بهتر بتواند ساختار فرماندهی و کنترل اطلاعات دشمن را برهم زند و از اطلاعات خود موثرتر استفاده کند[5].»

سابقه حمله‌های سایبری کره شمالی تا حدودی بیانگر راهبرد و مبنای نظری آن هستند. برخی تحلیل‌گران چنین توصیف می‌کنند که عملیات‌های سایبری این کشور از انسجام نسبی برخوردار هستند. به‌عنوان مثال، وزارت دفاع ایالات متحده آمریکا معتقد است کره شمالی قادر است از توانمندی‌های نامتقارن سایبری به‌عنوان اهرم فشار در دیپلماسی بهره‌برداری کند[6].

1. Kim Jong-In

۲. رجوع شود به:
Ji Young Kong, Jong In Lim and Kyoung Gon Kim, 'The All-Purpose Sword: North Korea's Cyber Operations and Strategies', in T. Minárik et al. (eds), 11th International Conference on Cyber Conflict: Silent Battle (Tallinn: NATO CCDCOE Publications, 2019), pp. 1-20, https://ccdcoe.org/uploads/2019/06/Art_08_The-All-Purpose-Sword.pdf.

۳. همان، ص.۱

4. Kim Jong-Il

۵. همان، ص.۲

۶. وزارت دفاع آمریکا، رجوع شود به:
'Military and Security Developments Involving the Democratic People's Republic of Korea: Annual Report to Congress, Washington DC', 2012, https://archive.defense.gov/pubs/Report_to_Congress_on_Military_and_Security_Developments_Involving_the_DPRK.pdf.

با این حال، شدت بیشتر حمله‌های سایبری کره شمالی کمتر از آستانه تهدید جدی است[۱] و اغلب این حمله‌ها مانند اقدامات تلافی‌جویانه آن از نوع حمله‌های مجرمانه هستند و لذا، در سطحی نیستند که بتوانند اهرمی برای اعمال فشار سیاسی باشند. در این بین، تنها مورد استثنایی مهم که اتفاقا در رسانه‌ها نیز چندان بازتاب نیافته‌است را می‌توان حمله‌های سایبری مستمر کره شمالی به نهادها و زیرساخت‌های مدنی کره جنوبی (به‌عنوان مثال، تهدید علیه صنعت هسته‌ای غیرنظامی کره جنوبی در سال ۲۰۱۴)[۲] دانست. یکی از نمونه‌های معروف اقدامات تلافی‌جویانه کره شمالی علیه کره جنوبی، حمله سایبری به سرورهای شرکت سونی در سال ۲۰۱۴ است که قبل از انتشار رسمی فیلم کمدی «مصاحبه»[۳] درباره کیم جونگ-اون انجام شد. در این حمله ایمیل‌های داخلی و اطلاعات کارکنان شرکت به سرقت رفت و حافظه رایانه‌های آن پاک شد[۴].

پس از اعمال تحریم‌های اقتصادی سازمان ملل در سال ۲۰۱۳، کره شمالی سعی کرده‌است روش‌های تازه‌ای برای تامین هزینه فعالیت‌های سایبری خود بیابد و درنتیجه، از سال ۲۰۱۴ به بعد مجموعه‌ای از عملیات‌های پیچیده اخاذی و حمله به نهادهای مالی و معامله‌گران ارزهای دیجیتال با منبع کره شمالی شناسایی شده‌است. در یکی از گزارش‌های سازمان ملل در سال ۲۰۱۹، منافع حاصل از این حمله‌ها بالغ

۱. رجوع شود به:
Jenny Jun, 'Cyber Coercion: Insights from North Korea's Cyber Campaigns', unpublished paper, 2020, p. 1.

۲. همان، صص.۷-۶

3. The Interview

۴. رجوع شود به:
Edgar Alvarez, 'Sony Pictures Hack: The Whole Story', Engadget, 10 December 2014, https://www.engadget.com/2014/12/10/sony-pictures-hack-the-whole-story.

بـر ۲ میلیـارد دلار بـرآورد شده‌اسـت[۱]. یکـی از عملیات‌هـای کره شـمالی در سـال ۲۰۱۷ که از باج‌افـزار واناکـرای به‌صـورت غیرتخصصـی و کنترل‌نشـده اسـتفاده کرده‌بـود، منجر به خسـارت‌های گسـترده بیش از سـطح موردنظر کره شـمالی شـد، به‌طوری‌که بسـیاری از رایانه‌های نظام خدمات عمومی، شـرکت‌ها، سـازمان‌ها و اشـخاص در حدود ۱۵۰ کشـور را از کار انداخت[۲].

کره شـمالی عملیات‌های سـایبری با هدف جاسوسـی صنعتی نیز اجرا کرده‌اسـت که طی آن‌ها ارتش این کشور صنایع فضایی و بخش‌های فناوری پیشرفته و تولید را در کره جنوبی و دیگر کشـورهای آسـیایی هدف قرار داده‌اسـت. در سال ۲۰۲۰، کمیته تحریم‌های کره شـمالیِ شـورای امنیت سـازمان ملل گزارش مبسـوطی درباره فعالیت‌های مجرمانه ایـن کشـور در فضـای سـایبری منتشـر کـرد. طبـق ایـن گـزارش، کـره شـمالی حمله‌های متعـددی برای سـرقت پـول به‌منظور تامین هزینه‌هـای فعالیت‌های هسـته‌ای نظامی و برنامه‌های موشـکی تحت تحریم سازمان ملل اجرا کرده‌است[۳].

گفتـه می‌شـود ارتـش کـره شـمالی دارای توانمندی‌هـای سـایبری تهاجمـی اسـت کـه آن‌هـا را در راسـتای راهبـرد «جنگ سـریع، پیروزی سـریع» و در کنار تـوان نظامی خود به‌کار

۱. رجوع شود به:
United Nations Security Council, 'Report of the Panel of Experts established pursuant to resolution 1874 (2009), S/2019/691', 30 August 2019, pp. 2, 26, https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf.

۲. رجوع شود به:
United States US-CERT, 'North Korea Threat Advisory', jointly with the Department of State, the Department of Justice and the Federal Bureau of Investigation, 15 April 2020, p. 3, https://us-cert.cisa.gov/sites/default/files/2020-04/DPRK_Cyber_Threat_Advisory_04152020_S508C.pdf

۳. رجوع شود به:
UN Sanctions Committee, 'Report of the Panel of Experts established pursuant to resolution 1874 (2009), S/2020/151', United Nations Security Council, 2 March 2020, https://undocs.org/S/2020/151.

می‌گیرد[۱]. این راهبرد که به‌عنوان راهبرد کوتاه و قاطع نیز شناخته می‌شود، مستلزم حمله به‌اصطلاح رعدآسا و مشارکت همگانی نیروهای بومی است[۲]. در حال حاضر، اطلاعات زیادی درباره احتمال داشتن توانمندی‌های سایبری نظامی پیشرفته (فراتر از جنگ‌های الکترونیک متعارف) یا برنامه‌ریزی کره شمالی برای کسب این توانمندی‌ها در دست نیست. با این حال، کره شمالی در صورت بروز جنگ می‌تواند با استفاده از حمله سایبری -حتی با اجرای حمله‌های محدود- به زیرساخت‌های شهری کره جنوبی آسیب جدی وارد کند. احتمال دارد این کشور دارای برنامه‌هایی برای تحمیل خسارت به زیرساخت‌های نظارت و فرماندهی نظامی کره جنوبی باشد.

حکمرانی، فرماندهی و نظارت

عملیات‌های سایبری کره شمالی تحت‌نظارت مستقیم حزب کارگران کره و به‌وسیله ارتش و نهادهای اطلاعاتی آن انجام می‌شود. کیم جونگ‌اون، رهبر حزب کارگران و رئیس کمیسیون ملی دفاع[۳] کره شمالی، کنترل مستقیم این عملیات‌ها را در اختیار دارد. این اختیارات مستقیم رهبر تا حدی خطر تضعیف عملکرد کارکنان را افزایش می‌دهد.

---

۱. رجوع شود به:
Jenny Jun, Scott LaFoy and Ethan Sohn, North Korea's Cyber Operations (Washington DC: Center for Strategic and International Studies, 2016),
https://www.csis.org/analysis/north-korea%E2%80%99s-cyber-operations.

۲. حمله رعدآسا (Blitzkrieg-like) اصطلاحی با ریشه آلمانی به‌معنی حمله سریع، گسترده و با هدف کسب پیروزی زودهنگام است.

رجوع شود به:
In-bum Chun, 'North Korea's Military Strategy', Korea Economic Institute of America, Washington DC, 2018,
http://www.keia.org/publication/north-korea%E2%80%99s-military-strategy-2018.

3. National Defense Commission

اداره کل دیده‌وری (RGB)[1] یا واحد ۵۸۶ به‌عنوان سازمان اطلاعاتی اصلی کره شمالی محسوب می‌شود. این سازمان تحت‌نظارت ستاد کل ارتش در سال ۲۰۰۹ تاسیس شد، هرچند بیشتر منابع معتقدند درحال حاضر مستقل از ستاد کل و تحت امر رهبر فعالیت می‌کند. گزارش‌های ضدونقیضی درباره ساختار و کارکنان این واحد وجود دارد و ازاین‌رو، به‌طور دقیق نمی‌توان گفت چه بخش‌ها/کسانی در عملیات‌های سایبری کره شمالی دخیل هستند. به نظر می‌رسد واحد راهنمای جنگ سایبری که به آن واحد ۱۲۱ یا اداره ۱۲۱ نیز گفته می‌شود[2] عامل اصلی در عملیات‌های سایبری این کشور باشد. واحد مذکور در وهله اول وظیفه ارزیابی آسیب‌پذیری‌های سیستم‌های رایانه‌ای و شبکه‌های دشمن و متعاقب آن، بهره‌برداری از نقاط ضعف جهت ضربه‌زدن به دشمن و انجام جرائم مالی سایبری را برعهده دارد. این واحد زیرمجموعه اداره فنی[3] اداره کل دیده‌وری به شمار می‌رود که به‌نقل از حداقل یک منبع آگاه، در سال ۲۰۱۳ یا ۲۰۱۴ تاسیس شده و عامل حمله هکری به شرکت سونی در سال ۲۰۱۴ نیز بوده‌است[4].

در برخی گزارش‌ها به وجود واحدهای مهم دیگری ازجمله آزمایشگاه ۱۱۰ (که البته ممکن است زیرمجموعه واحد ۱۲۱ یا سازمان جدید همین واحد باشد) نیز اشاره شده‌است. واحدهای متعددی نیز به‌عنوان زیرمجموعه آزمایشگاه ۱۱۰ یا مرتبط با آن شناسایی شده‌اند. این واحدها عبارتند از:

1. Reconnaissance General Bureau
2. Cyber Warfare Guidance Unit

رجوع شود به:

Headquarters, Department of the Army, 'North Korean Tactics', 2020, p. E-1, https://fas.org/irp/doddir/army/atp7-100-2.pdf.'Unit' is one of the possible translations of the Korean word
gug; alternatives include 'bureau' and 'station'.

3. Technical Bureau

۴. رجوع شود به:

'North Korean Cyber Activity', Recorded Future, 2017, p. 6, https://go.recordedfuture.com/hubfs/reports/north-korea-activity.pdf.

- دفتر ۹۸ که به پایش پناهندگان کره شمالی (و شبکه پشتیبانی از آن‌ها) و اساتید دانشگاه در کره جنوبی و سایر کشورها می‌پردازد.
- دفتر ۴۱۴ که دارای تاسیساتی در چین و پیونگ‌یانگ است و بر دولت‌ها و شرکت‌های خارجی به‌منظور انجام عملیات‌های جاسوسی و خرابکاری متمرکز است.
- دفتر ۳۵ که به‌عنوان اداره‌ای فنی در زمینه ساخت بدافزارها و شناسایی نقاط ضعف رقبا فعالیت دارد[۱].

واحد ۹۱ احتمالا از نظر سازمانی هم‌تراز آزمایشگاه ۱۱۰ است و مسئولیت اجرای پروژه‌هایی با اولویت بالا مانند هدف گرفتن زیرساخت‌های غیرنظامی کره جنوبی و جاسوسی سایبری علیه هدف‌های خارجی دارای فناوری‌های هسته‌ای و نظامی را برعهده دارد[۲]. واحد ۱۸۰ نیز به فعالیت‌های سایبری مجرمانه در هدف‌های خارجی با هدف سرقت پول اشتغال دارد[۳].

شرکت‌های امنیت سایبری غربی معمولا اداره کل دیده‌وری و یک گروه خاص دیگر با وظایف مشابه را به‌ترتیب با نام‌های مستعار تهدید مستمر پیشرفته ۳۸ و ۳۷ (به اختصار اِی‌پی‌تی ۳۸ و ۳۷) معرفی می‌کنند[۴]. گفته می‌شود گروه ای‌پی‌تی ۳۷ به از بین

---

۱. رجوع شود به:
Kong, Lim and Kim, 'The All-Purpose Sword', p. 6, citing Moonbeom Park, 'Let's learn about enemy through various IoCs of real APT cases', In DragonCon 2018, 8 December 2018, Dragon Threat Labs.

۲. همان، ص.۶، رجوع شود به:
Mok Yongjae, '6 Cyber Units were built after Kim Jong-un regime', RFA, 22 November 2017.

۳. همان، ص.۶، رجوع شود به:
Matthew Ha and David Maxwell, 'Kim Jong Un's "All-Purpose Sword" - North Korean Cyber-Enabled Economic Warfare', Foundation for Defense of Democracies, October 2018, p. 13, https://www.fdd.org/wp-content/uploads/2018/09/REPORT_NorthKorea_CEEW.pdf.

4. Advanced Persistent Threat (APT37 and APT38)

رجوع شود به:

'APT 37 (Reaper): The Overlooked North Korean Actor', FireEye, 2018, https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf.

بردن ردپای خود ازطریق اقدامات شـدید تهاجمی شـهرت دارد[1]. دو گروه دیگر به نام‌های لازاروس و تی‌ایی‌اِم‌پی هرمیت[2] نیز شناسایی شده‌اند که با اداره کل دیده‌وری کره شمالی ارتبـاط دارنـد. اگرچه حمله‌های این گروه‌ها از الگوهای متفاوتـی پیروی می‌کند، ولی ظاهرا ابزارها و افراد مورداستفاده در آن‌ها مشترک است[3]. ماهیت ارتباط این گروه‌ها با اداره کل دیده‌وری و نحوه نظارت آن بر این گروه‌ها مشخص نیست.

براساس منابع موجود، ستاد کل ارتش کره شمالی دارای واحدهای سایبری دیگری به غیر از اداره کل دیده‌وری نیز می‌باشـد. بنا به ادعای شـرکت امنیت سایبری فایرآی[4] گفته می‌شود این واحدها بر ارعاب، جاسوسی صنعتی و کسب آمادگی برای نبردهای با شدت بالا شـامل تخریب سـامانه‌های فرماندهی و کنترل دشمن تمرکز دارند. شایان ذکر است هدف این واحدها صرفا محدود به نیروهای نظامی و صنایع کشـورهای دیگر نمی‌شـود و گروه‌های مختلفی از فعالان ضد نظام، پژوهشـگران و اصحاب رسـانه سـایر کشورها را نیز پوشش می‌دهند[5].

توانمندی‌های محوری در زمینه اطلاعات سایبری

شـواهد زیادی دربـاره توانمندی‌های اطلاعات سـایبری کره شـمالی موجود نیسـت، امـا می‌تـوان چنیـن تصور کرد که این کشـور دو اولویت اصلی یعنی حفظ نظام و هشـدار بهنـگام دربـاره احتمال حمله نظامی از جانب کره جنوبی یا پایگاه‌های آمریکایی مسـتقر

۱. رجوع شود به:

'APT 38: Un-usual suspects', FireEye, p. 22, https://content.fireeye.com/apt/rpt-apt38.

2. Lazarus and TEMP Hermit

۳. همان.

4. FireEye

۵. همان، صص.۸-۶.

در/نزدیکی شبه‌جزیره کره را مدنظر دارد. کره شمالی همچنین از عملیات‌های سایبری برای سرقت پول از نهادهای مالی بین‌المللی جهت کاهش اثرات تحریم‌های اقتصادی استفاده می‌کند.

به‌مدد محدودیت‌های گسترده در دسترسی به اینترنت داخلی، نظام کره شمالی از ظرفیت بالایی برای نظارت و کنترل کاربران اینترنت داخلی برخوردار است و این کشور قادر است بیشتر توان اطلاعات سایبری خود را روی کره جنوبی و نیروهای نظامی آمریکا متمرکز کند. به نظر می‌رسد دسترسی توانمندی‌های اطلاعات سایبری کره شمالی ورای شبه جزیره کره بسیار محدود بوده و در حد عملیات‌های مقطعی و در مقیاس کوچک است. عملیات‌هایی که تاکنون ردیابی شده‌اند بیانگر سطح پایینی از تخصص هستند، هرچند طبق ارزیابی‌های آمریکا سطح پیچیدگی آن‌ها روبه‌رشد است[۱].

طبق ادعای پناهندگانی از کره شمالی، کل نیروهای فعال در واحدهای سایبری این کشور در دوره کیم جونگ‌ایل حدود ۳۰۰۰ نفر بوده که در دوره کیم جونگ‌اون به ۶۰۰۰ نفر افزایش یافته‌است و بیشتر این رشد در واحد ۱۲۱ اداره کل دیده‌وری رخ داده‌است[۲]. طبق گزارشی در سال ۲۰۲۱، تعداد نیروهای سایبری کره شمالی به ۶۸۰۰ نفر رسیده‌است که تنها ۱۷۰۰ نفر از آن‌ها هکر هستند[۳]. باتوجه به ضعف نظام آموزشی،

۱. رجوع شود به:
US Department of State et al., ‘Guidance on the North Korean Cyber Threat’, 15 April 2020, p. 2, https://us-cert.cisa.gov/sites/default/files/2020-04/DPRK_Cyber_Threat_Advisory_04152020_S508C.pdf.

۲. رجوع شود به:
HP Security Research, ‘Profiling an enigma: The mystery of North Korea’s cyber threat landscape, 2014’, HP Security Briefing Episode 16, August 2014, https://time.com/wp-content/uploads/2014/12/hpsr_securitybriefing_episode16_northkorea.pdf; and Department of the Army, ‘North Korean Tactics’, p. E-1.

۳. رجوع شود به:
‘Bae saibeo jeonsa 6,800myeong … yeongjaehaggyoseo haekeo yugseong’, Yunhap News, 18 February 2021, https://www.yna.co.kr/view/MYH20210218017300038

تعداد محدود فارغ‌التحصیلان رشته‌های فناوری اطلاعات و دسترسی محدود به فناوری‌های اطلاعات و ارتباطات نمی‌توان انتظار داشت که نیروهای سایبری کره شمالی از مهارت بالایی برخوردار باشند و احتمالا بیشتر هکرهای آن به فعالیت‌های جاسوسی اشتغال دارند. درواقع، تخمین‌ها دال بر تعداد محدود شهروندانی است که امکان تحصیل در رشته‌های سایبری و استخدام در نیروهای سایبری را دارند، به‌طوری‌که سالانه تنها ۱۰۰ نفر در رشته‌های مرتبط با امنیت سایبری از دانشگاه نظامی کره شمالی فارغ‌التحصیل می‌شوند[۱].

توانمندی و وابستگی سایبری

کره شمالی به دنبال دستیابی به خودکفایی کامل ازجمله در فناوری‌های پیشرفته است، هرچند به نظر نمی‌رسد نظام آموزشی و اقتصاد این کشور ظرفیت لازم برای تحقق این هدف را داشته باشد[۲]. علت آن نیز این است که مردم و کسب‌وکارهای این کشور از دسترسی به دانش و فرصت‌های کسب درآمد ازطریق شبکه جهانی اینترنت محروم شده‌اند.

در سال ۲۰۰۸، شبکه اصلی تلفن همراه (3G) کره شمالی به نام کُریولینک[۳] با همکاری شرکت مصری اُراسکام تله‌کام هولدینگ[۴] و شرکت پست و مخابرات کره[۵] راه‌اندازی شد[۶].

۱. رجوع شود به:
Jason Bartlett, 'Why Is North Korea So Good at Cybercrime?', Diplomat, 13 November 2020, https://thediplomat.com/2020/11/why-is-north-korea-so-good-at-cybercrime

۲. رجوع شود به:
Pratik Jakhar, 'North Korea's high-tech pursuits: Propaganda or progress?', BBC News, 15 December 2018, https://www.bbc.com/news/world-asia-46563454

3. Koryolink

4. Orascom Telecom Holding

5. Korea Post and Telecommunication Corporations

۶. رجوع شود به:
'ICT in N. Korea 2', KBS World Radio, 31 January 2019, https://world.kbs.co.kr/service/contents_view.htm?lang=e&menu_cate=northkorea&id=&board_seq=356891&page=6&board_code=korea_closeup.

زیرساخت‌های این شبکه ازجمله خدمات نرم‌افزاری و ادغام در شبکه و نیز ساخت سیستم رمزنگاری محلی بیشتر به وسیله شرکت چینی هوآوی فراهم شده‌است[۱]. آمار ارائه شده در سال ۲۰۱۴ حاکی از آن بود که از جمعیت ۲۵ میلیون نفری کره شمالی حدود ۲/۸ میلیون نفر به شبکه کریولینک دسترسی داشتند[۲] و در سال ۲۰۱۹ تعداد کل کاربران تلفن همراه به حدود ۵ میلیون نفر می‌رسید[۳]. شبکه‌های همراه کره شمالی دسترسی مستقیم به اینترنت جهانی ندارند و ازطریق شبکه داخلی دولت به اینترنت متصل می‌شوند[۴]. تنها کاربران تلفن همراه که می‌توانند به اینترنت دسترسی داشته باشند، اعضای رده بالای حزب کارگران کره هستند که درمجموع تعداد آن‌ها کمتر از ۱۰،۰۰۰ نفر است.

در محدوده پسوند kp. (دامنه اینترنت کره شمالی) تنها ۹ دامنه (دامین) سطح بالا (مانند co.kp, gov.kp, edu.kp) و دامنه فرعی ثبت شده‌است[۵]. به غیر از آدرس‌های

۱. رجوع شود به:
Ellen Nakashima, Gerry Shih and John Hudson, 'Leaked documents reveal Huawei's secret operations to build North Korea's wireless network', Washington Post, 22 July 2019, https://www.washingtonpost.com/world/national-security/leaked-documents-reveal-huaweis-secret-operations-to-buildnorth-koreas-wireless-network/2019/07/22/583430fe-8d12-11e9-adf3-f70f78c156e8_story.html.

۲. رجوع شود به:
Williams, 'North Korea's Koryolink: Built for Surveillance and Control'.

۳. رجوع شود به:
Kim Ji-eun and Noh Ji-won, 'North Korea's Smartphone Industry Rapidly on the Rise', HanKyoreh, 17 March 2019, http://english.hani.co.kr/arti/english_edition/e_northkorea/886255.html.

۴. رجوع شود به:
Kim Ji-eun and Noh Ji-won, 'North Korea's Smartphone Industry Rapidly on the Rise', HanKyoreh, 17 March 2019, http://english.hani.co.kr/arti/english_edition/e_northkorea/886255.html

۵. رجوع شود به:
'How North Korea Revolutionized the Internet as a Tool for Rogue Regimes', Recorded Future, 9 February 2020, p. 5, https://go.recordedfuture.com/hubfs/reports/cta-2020-0209.pdf

آی‌پی که این دامنه‌ها در اختیار کاربران می‌گذارند، کاربرانی کره‌ای دارای مجوز می‌توانند ازطریق بستر چینی چاینا نت‌کام[1] و یک بستر روسی که ظاهرا در لبنان مستقر است نیز به اینترنت دسترسی داشته باشند[2]. به نظر می‌رسد مقامات رده‌بالای دولتی از مهارت‌های لازم برای به‌کارگیری اینترنت برخوردارند و به اهمیت امنیت سایبری واقف هستند[3]: نرخ استفاده این گروه از کاربران از اینترنت در سال‌های ۲۰۱۷ تا ۲۰۱۹ تا ۳۰۰ درصد افزایش یافته‌است که بیشتر به‌دلیل رشد عملیات‌های سایبری مجرمانه برای کاهش اثرات تحریم‌های سازمان ملل و ایالات متحده بوده‌است[4].

علاوه بر محدودیت در دسترسی به اینترنت، نظام کره شمالی محدودیت‌های دیگری نیز در سایر بخش‌های شبکه اعمال می‌کند. به‌عنوان مثال به‌منظور تسهیل نظارت دولتی، برخورداری از خدمات وای‌فای داخلی کره شمالی (موسوم به میرِی)[5] مستلزم داشتن سیم‌کارت است. علاوه براین، دولت سامانه عملیاتی به نام رِد اِستار[6] (نوعی سیستم لینوکس[7] تغییریافته) را برای ردیابی همه حرکات کاربران راه‌اندازی کرده‌است[8].

1. China Netcom

۲. همان.

۳. رجوع شود به:
Insikt Group, 'Shifting Patterns in Internet Use Reveal Adaptable and Innovative North Korean Ruling Elite',
Recorded Future, 25 October 2018,
https://go.recordedfuture.com/hubfs/reports/cta-2018-1025.pdf.

۴. رجوع شود به:
David E. Sanger, 'North Korea's Internet Use Surges, Thwarting Sanctions and Fueling Theft', New York Times, 11 June 2020,
https://www.nytimes.com/2020/02/09/us/politics/north-koreainternet-sanctions.html.

5. Mirae
6. Red Star
7. Linux

۸. رجوع شود به:
Joel Gunter, 'Analysis of North Korea's computer system reveals spy files', BBC News, 28 December 2015,
https://www.bbc.com/news/world-asia-35188570.

رد استار توسط موسسه پژوهش فناوری اطلاعات دولت به نام مرکز رایانه کره[۱] طراحی و ساخته شده‌است. این مرکز در سال ۲۰۱۵ به شرکتی تجاری تغییر یافت[۲]. در کره شمالی برای مالکیت رایانه به تاییدیه دولت نیاز است. بااین حال، بسیاری از کاربران می‌توانند از نرم‌افزارهای آمریکایی استفاده کنند[۳].

کره شمالی دارای ظرفیت بالایی در زمینه ساخت نرم‌افزار است[۴] و قصد دارد به قطب برون‌سپاری کشورهای همسایه (چین، ژاپن و کره جنوبی) تبدیل شود و حتی از هند نیز سبقت بگیرد[۵]. شرکت‌های فناوری کره شمالی اغلب به کمک شرکت‌های پوششی[۶] کار می‌کنند و خدمات بسیار متنوعی مانند طراحی اپ و وب‌سایت[۷]، نرم‌افزارهای مدیریت

1. Korean Computer Center

۲. رجوع شود به:
Mun Dong Hui, 'North Korean web developers still in business in China despite lower numbers', Daily NK, 19 April 2019,
https://www.dailynk.com/english/north-korean-webdevelopers-still-in-business-in-china-despite-lower-numbers.

۳. رجوع شود به:
Priscilla Moriuchi and Fred Wolens, 'North Korea Relies on American Technology for Internet Operations', Insikt Group, 2018,
https://go.recordedfuture.com/hubfs/reports/cta-2018- 0606.pdf.

۴. رجوع شود به:
Martyn Williams, 'Kim Chaek University ranks 8th in international programming contest', North Korea Tech, 4 May 2019,
https://www.northkoreatech.org/2019/05/04/kim-chaekuniversity-icpc-2019;

Kelly Kasulis, 'North Korean college coders beat Stanford University in a 2016 competition. Here's why that matters' Mic, 4 December 2017,
https://www.mic.com/articles/186412/north-korean-college-coders-beat-stanforduniversity-in-a-2016-competition-heres-why-that-matters.

۵. رجوع شود به:
Koichiro Komiyama, 'The Information Technology Industry in North Korea', KGRI Working Papers, no. 4, February 2019, p.5, Keio University Global Research Institute,
https://www.kgri.keio.ac.jp/docs/S180620190226.pdf.

۶. شرکت‌های پوششی (front/shell companies) به شرکت‌هایی گفته می‌شود که اغلب فقط روی کاغذ وجود دارند و دارای دفتر یا نیروی انسانی خاصی نیستند و نماینده یا پوشش شرکت دیگری برای فعالیت در بازار محسوب می‌شوند.

۷. رجوع شود به:
Hui, 'North Korean web developers still in business in China despite lower numbers'.

کسب‌وکار، برنامه‌های تشخیص هویت بیومتریک، شبکه‌های خصوصی مجازی و نرم‌افزارهای تشخیص چهره به مشتریان بین‌المللی خود ارائه می دهند[۱].

کره شمالی برنامه فضایی محدود اما فعالی دارد و پس از سه پرتاب ناموفق[۲] توانسته‌است دو ماهواره را با موفقیت در سال‌های ۲۰۱۲ و ۲۰۱۶[۳] در مدار قرار دهد. به نظر می‌رسد این ماهواره‌ها قابلیت انجام عملیات‌های شناسایی و هدف‌گیری دقیق برای برنامه‌های موشکی کره شمالی را دارند[۴] و تاکنون شواهدی دال بر تمایل کره شمالی به ساخت پایگاه صنعتی فضایی با اهداف غیرنظامی به دست نیامده‌است[۵].

نظام آموزش کره شمالی بر پرورش استعدادهای فناوری به‌ویژه در دانشگاه‌های برتر کشور مانند دانشگاه کیم ایل سونگ، دانشگاه فناوری کیم چائک و دانشگاه علم و فناوری پیونگ‌یانگ[۶] تمرکز دارد. در دانشگاه مورانبونگ[۷] نیز که اساتیدی گزینشی دارد،

---

۱. رجوع شود به:
Andrea Berger et al., 'The Shadow Sector: North Korea's Information Technology Networks', CNS Occasional Paper, no.36, May 2018,
https://www.nonproliferation.org/wp-content/uploads/2018/05/op36-the-shadow-sector.pdf.

۲. رجوع شود به:
'Space Threat 2018: North Korea Assessment', CSIS Aerospace, 12 April 2018,
https://aerospace.csis.org/ space-threat-2018-north-korea

۳. برای کسب جزئیات بیشتر درباره پرتاب موفق دو ماهواره Kwangmyongsong-3 و Kwangmyongsong-4 به‌ترتیب در سال‌های ۲۰۱۲ و ۲۰۱۶ رجوع شود به:
'KMS 3-2', NASA Space Science Data and Coordinated Archive, 14 May 2020,
https://nssdc.gsfc.nasa.gov/nmc/spacecraft/display.action?id=2012-072A;

'KMS4', NASA Space Science Data Coordinated Archive, 14 May 2020,
https://nssdc.gsfc.nasa.gov/nmc/spacecraft/display.action?id=2016-00A

۴. رجوع شود به:
Robert E. McCoy, 'What Are the Real Purposes of Pyongyang's New Satellites?', Asia Times, 19 December 2017,
https://asiatimes. com/2017/12/real-purposes-pyongyangs-new-satellites

۵. رجوع شود به:
Todd Harrison et al., 'Threat Assessment 2020', CSIS Aerospace, March 2020, p. 36,
https://aerospace.csis.org/wp-content/uploads/2020/03/Harrison_SpaceThreatAssessment20_WEB_FINAL-min.pdf#page=52.

6. Kim Il-sung University, Kim Chaek University of Technology and Pyongyang University of Science and Technology

7. Moranbong University

دوره‌های آموزشی در رشته‌های هک برگزار می‌شود[۱]. در سال ۲۰۲۰ نیز وجود دانشگاه دفاع ملی کیم جونگ-اون[۲] افشا شد که ظاهرا در حوزه علم و فناوری فعالیت می‌کند[۳]. به‌علاوه، دوره‌های آموزش رایانه به برنامه تحصیلی دانش‌آموزان از دوره راهنمایی به بعد افزوده می‌شود.

امنیت و تاب‌آوری سایبری

دفاع سایبری کره شمالی بسیار ضعیف است و از رتبه بسیار پایین آن در شاخص جهانی امنیت سایبری ۲۰۱۸ (رتبه ۱۷۱ در میان ۱۷۵ کشور جهان) کاملا مشهود است[۴]. این جایگاه نامناسب ریشه در مهارت‌های فنی متوسط و سیاست انزوای دولت از دنیای خارج ازجمله ایالات متحده دارد. با آنکه انزوای اینترنتی با هدف کمک به ارتقای امنیت سایبری ملی انجام می‌شود، اما کره شمالی هیچ برنامه سراسری مشخصی در زمینه دفاع سایبری ملی ندارد.

اگرچه کره شمالی به اندازه سایر کشورها به اینترنت وابسته نیست، ولی نمی‌تواند خود را نیز به‌طور کامل از دنیا جدا کند. این واقعیت که کره شمالی تنها از دو درگاه (نقطه اتصال) بین‌المللی اینترنت استفاده می‌کند، یکی از نقطه‌ضعف‌های اصلی آن

۱. رجوع شود به:
Bruce Harrison, 'How North Korea Recruits Its Army of Young Hackers', NBC News, 8 December 2017, https://www.nbcnews.com/news/north-korea/how-north-korea-recruits-trains-itsarmy-hackers-n825521.

2. Kim Jong-un University of National Defense

۳. رجوع شود به:
'NK establishes university named after leader Kim', Yonhap News Agency, 14 October 2020, https://en.yna.co.kr/view/ AEN20201014003000325.

۴. رجوع شود به:
International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 68, https://www.itu.int/dms_pub/itu-d/opb/str/ D-STR-GCI.01-2018-PDF-E.pdf

به‌شمار می‌رود و درنتیجه، تیم‌های هکری آن تنها در صورتی می‌توانند عملکرد مناسبی داشته باشند که خارج از کشور فعالیت کنند. تعداد حمله‌های سایبری با هدف اختلال در ارتباط اینترنتی کره شمالی بسیار زیاد است[۱]. به‌عنوان مثال، حمله‌ای که در مارس ۲۰۱۳ رخ داد و در اثر آن به ارتباط اینترنتی کره شمالی آسیب جدی وارد شد[۲]، ظاهرا از سوی ایالات متحده و کره جنوبی در انتقام از حمله کره شمالی به شبکه‌های بانکی و تلویزیونی کره جنوبی طراحی و اجرا شده‌بود. در سال ۲۰۱۴ نیز دو روز بعد از آنکه باراک اوباما اعلام کرد حمله به شرکت سونی پیکچرز[۳] بی‌پاسخ نمی‌ماند، به‌مدت دو روز اینترنت کره شمالی مسدود شد[۴]. در سال ۲۰۱۸، آمریکا سیاست مبنی بر دفاع روبه‌جلو در فضای سایبری را در پیش گرفت که هدف از آن محدودسازی رفتارهای خشونت‌آمیز کشورهایی مانند کره شمالی بود[۵]. در صورت بروز تقابل بین کره شمالی و سایر کشورها، قطع دسترسی این کشور به اینترنت به‌راحتی با مسدودسازی دو درگاه بین‌المللی آن امکان‌پذیر است.

---

۱. رجوع شود به:
Karen DeYoung, Ellen Nakashima and Emily Rauhala, 'Trump Signed Presidential Directive Ordering Actions to Pressure North Korea', Washington Post, 30 September 2017, https://www.washingtonpost.com/world/national-security/trump-signed-presidential-directive- ordering-actions-topressure-north-korea/2017/09/30/97c6722a-a620-11e7-b14ff41773cd5a14_ story.html.

۲. رجوع شود به:
'Significant Cyber Incidents Since 2006', Center for Strategic and International Studies, https://csis-website-prod.s3.amazonaws.com/s3fs-public/210129_Significant_Cyber_Events.pdf.

3. Sony Pictures

۴. رجوع شود به:
Yashwant Raj, 'North Korea suffers internet blackout after Sony hack', Hindustan Times, 24 December 2014, https://www.hindustantimes.com/world/north-korea-suffers-internet-blackoutafter-sony-hack/story-Iz7HFvyAPyWaYHd1Zqj52I.html.

۵. رجوع شود به:
US Department of Defense, 'Summary Department of Defense Cyber Strategy 2018', September 2018, pp. 1-2, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_ FINAL.PDF.

اگرچه بخش اعظم جمعیت کره شمالی بدون دسترسی به سامانه‌های دیجیتال زندگی می‌کنند، اما نیروگاه‌های برق و سایر تاسیسات زیرساختی آن مانند مخابرات به‌شدت به آن‌ها وابسته هستند. بیشتر نیروگاه‌های برق این کشور از تجهیزات قدیمی استفاده می‌کنند و بنابراین، امنیت چندانی ندارند. جدیدترین تاسیسات برق کره شمالی شامل چهار نیروگاه برق‌آبی است که با مشارکت چین راه‌اندازی شده‌اند و حتی این تاسیسات نیز در معرض حمله‌های سایبری قرار دارند. از آنجایی که بیشتر ساختمان‌های مسکونی کره شمالی به برق دسترسی ندارند، دولت‌های غربی در صورت حمله به تاسیسات شبکه برق تردید و نگرانی کمتری خواهند داشت.

رهبری جهانی در عرصه سایبری

کره شمالی به‌عنوان عضوی از سازمان ملل در سازمان‌هایی مانند اتحادیه بین‌المللی مخابرات و اجلاس جهانی سران درباره جامعه اطلاعات[1] دارای کرسی است، اما هیچ سابقه‌ای از فعالیت دیپلماتیک درباره هنجارها، استانداردهای فنی و سیاست‌های سایبری ندارد. در مجمع عمومی سازمان ملل معمولا کره شمالی همانند چین و روسیه به قطعنامه‌های مربوط به مسائل سایبری رای مثبت می‌دهد. به‌عنوان مثال، کره شمالی در سال ۲۰۱۸ در کنار ۱۱۸ کشور دیگر (در مقابل ۴۶ کشور اروپایی و هم‌پیمانان آن‌ها) به قطعنامه موردحمایت چین و روسیه درباره تشکیل کارگروه پایان باز سازمان ملل برای جنبه‌های امنیت بین‌المللی پیشرفت‌های حوزه فناوری اطلاعات و ارتباطات رای مثبت داد.

1. World Summit on the Information Society

توانمندی‌های سایبری تهاجمی

کره شمالی دست‌کم از سال ۲۰۰۹ به‌طور مکرر انواع عملیات‌های سایبری تهاجمی را علیه کره جنوبی اجرا می‌کند. اغلب این عملیات‌ها از نوع حمله‌های قطع دسترسی به خدمات پایه یا حمله‌های افشا و حذف داده از وب‌سایت‌های دولتی یا بخش خصوصی کشورهای مختلف هستند. از زمان اعمال تحریم‌های سخت‌تر از سوی سازمان ملل در سال ۲۰۱۳، کره شمالی از توانمندی‌های سایبری برای سرقت پول از سامانه‌های مالی جهانی استفاده می‌کند: سامانه بانکداری بین‌المللی سوئیفت[1] و بانک‌های بنگلادش، شیلی، کره جنوبی، تایوان و ویتنام ازجمله اهداف حمله کره شمالی هستند. هک و افشای داده شرکت سونی پیکچرز در سال ۲۰۱۴ و حمله غیرهدفمند با بدافزار واناکرای در سال ۲۰۱۷ از معروف‌ترین این حمله‌ها بوده‌اند. در گزارش سازمان امنیت سایبری و امنیت زیرساخت‌های ایالات متحده[2] در سال ۲۰۲۰، عملیات‌های سایبری مستمر کره شمالی تهدیدی برای ثبات بازارهای مالی بین‌المللی نامیده شده‌اند[3]. علاوه براین، شواهدی نیز موجود است که نشان می‌دهند کره شمالی از عملیات‌های سایبری برای شناسایی و پایش زیرساخت‌های حیاتی ملی کشورهای منطقه به‌ویژه کره جنوبی استفاده می‌کند.

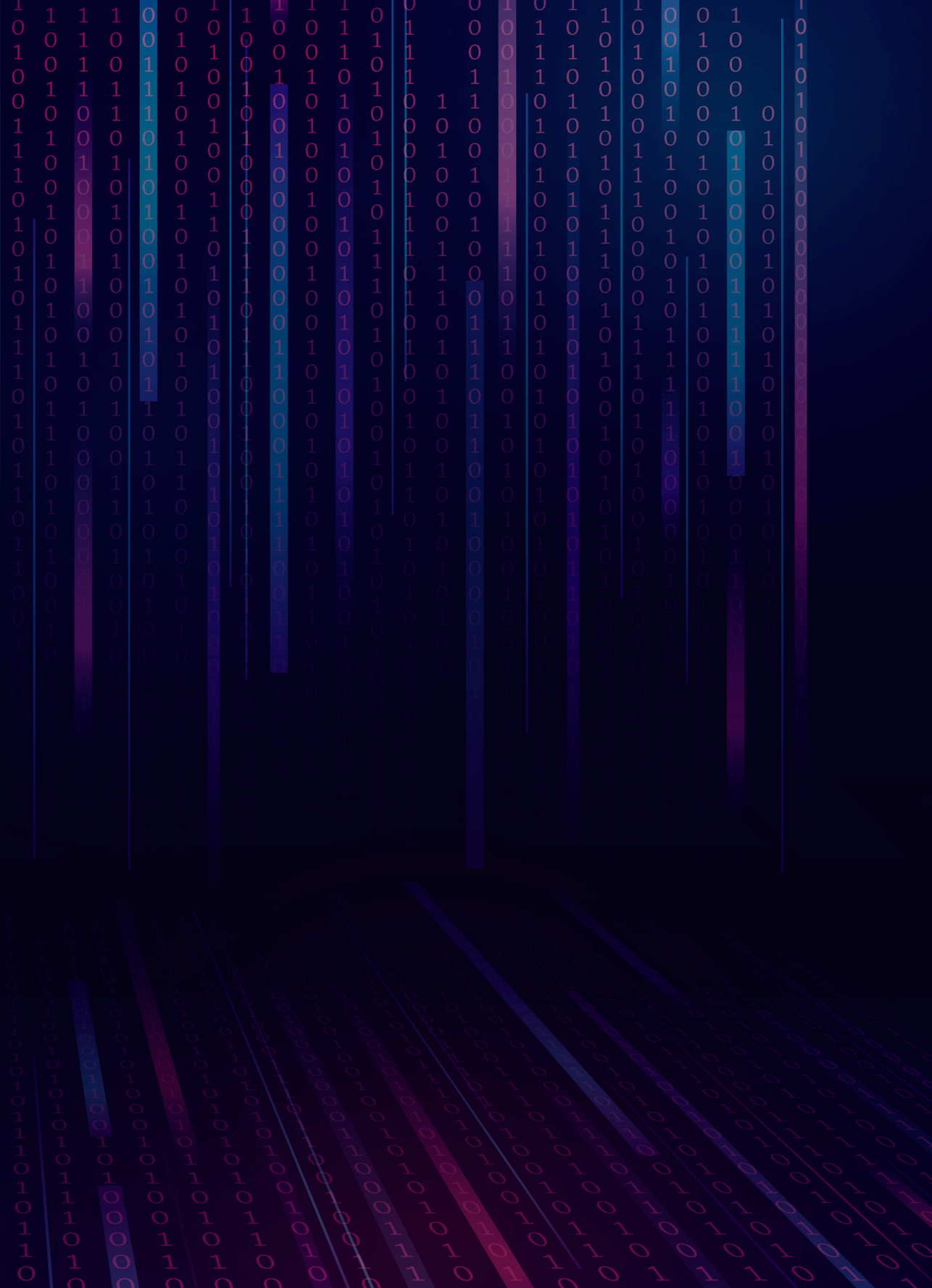
به‌طور کلی، روش‌های مورداستفاده کره شمالی در عملیات‌های سایبری و سطح تخصص آن‌ها تمایز زیادی با عملیات‌های سایبری مجرمانه ندارد. کره شمالی در این عملیات‌ها از توانمندی‌های دیگر کشورها نیز به روش‌های مختلف استفاده می‌کند. به‌عنوان مثال، کره شمالی در حمله به شرکت سونی نسخه ویرایش‌شده‌ای

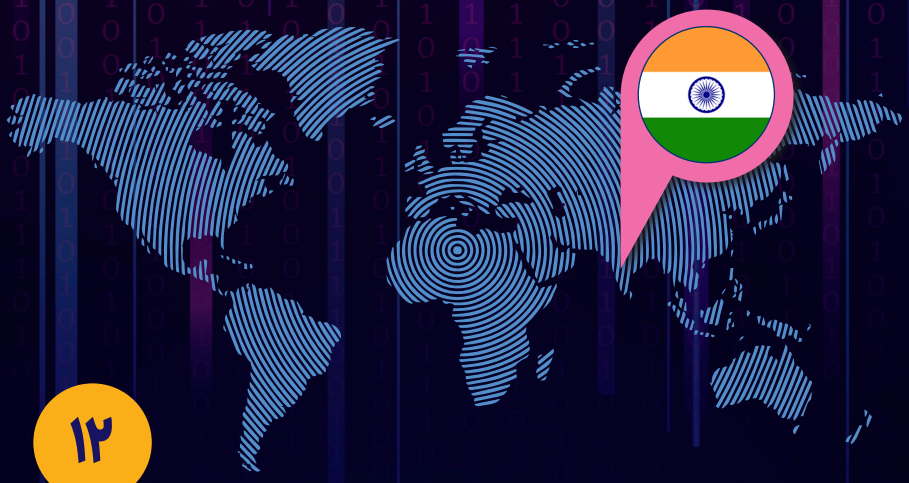
1. SWIFT
2. Cybersecurity and Infrastructure Security Agency

۳. رجوع شود به:
'Alert (AA20-106A): Guidance on the North Korean Cyber Threat', Cybersecurity and Infrastructure Security Agency, 15 April 2020 (revised 23 June 2020), https://us-cert.cisa.gov/ncas/ alerts/aa20-106a.

از بدافزار پاک‌کننده شامون از ایران را به کار گرفت. کره شمالی واناکرای را نیز براساس توانمندی‌هایی که از یکی از نهادهای اطلاعاتی آمریکا نشت کرده‌بود، ساخته‌است.

شرکت‌های امنیت سایبری غربی بسیاری از فعالیت‌های سایبری کره شمالی را شناسایی و ردیابی می‌کنند. بنابراین در صورت رخداد تقابل جدی، گزینه‌های سایبری کره شمالی زیاد نخواهد بود و مسلما سطح دسترسی سایبری-اطلاعاتی آن در حدی نیست که بتواند به شبکه‌های حفاظت‌شده نفوذ پیدا کند و یا در آن‌ها اخلال ایجاد کند. اما در صورت افزایش تنش در شبه‌جزیره کره همانند سال ۲۰۱۰، دامنه عملیات‌های سایبری کره شمالی افزایش خواهد یافت. احتمالا خطر اصلی این است که چنین عملیات‌هایی عامدانه و یا به‌دلیل اشتباهات محاسباتی از خسارت‌های مالی و مجازی فراتر روند و آسیب‌های جدی فیزیکی به بار آورند.





۱۲

هند

با آنکه هند در منطقه‌ای واقع شده‌است که درگیر بی‌ثباتی راهبردی است و دولت آن نیز به تهدیدهای امنیتی موجود آگاه است، اما تاکنون اقدامات چندانی برای تهیه و تثبیت مبانی نظری و تامین امنیت فضای سایبری خود انجام نداده‌است. روند اصلاحات نهادی در حاکمیت سایبری هند کند اما روبه‌افزایش است، به‌طوری‌که مراجع اصلی ذی‌ربط در هماهنگی امنیت سایبری نظامی و غیرنظامی اخیرا و به‌ترتیب در سال‌های ۲۰۱۸ و ۲۰۱۹ تاسیس شدند. این مراجع با سازمان اصلی اطلاعات سایبری هند یعنی سازمان ملی تحقیقات فنی[1] همکاری نزدیکی دارند. هند دسترسی خوبی به اطلاعات سایبری منطقه‌ای دارد و همزمان با شرکای خود ازجمله ایالات متحده به‌منظور توسعه سطح دسترسی خود همکاری دارد. برخورداری از فرهنگ استارتاپی پویا و فراوانی استعداد نقاط‌قوت اقتصاد دیجیتال هند محسوب می‌شوند. بخش خصوصی هند سریع‌تر از دولت برای ارتقای امنیت سایبری ملی وارد عمل شده‌است. هند در عرصه دیپلماسی سایبری نقش فعال و موثری دارد، اما در زمینه هنجارهای جهانی پیشتاز نیست و درمقابل، ترجیح می‌دهد با دولت‌های بزرگ این حوزه مناسبات نزدیکی برقرار کند. شواهد معدودی که در مورد توانمندی‌های سایبری تهاجمی هند موجود است نشان از تمرکز منطقه‌ای آن به‌ویژه روی پاکستان دارند. درمجموع، هند یکی از قدرت‌های سایبری رده سوم به شمار می‌رود و برای پیوستن به رده دوم باید از ظرفیت عظیم صنعتی-دیجیتال خود بهره‌برداری کند و رویکرد کل جامعه را برای ارتقای امنیت سایبری خود به‌کار گیرد.

1. National Technical Research Organization

راهبرد و مبنای نظری (دکترین)

به‌منظور تعیین خطوط اصلی رویکرد هند در امنیت سایبری باید سخنرانی‌های وزرا و مقررات و مصوبات دولتی آن را به جای جستجوی اسناد سیاستی آن بررسی کرد. زیرا هند در زمینه انتشار سیاست‌های جامع امنیت سایبری عملکرد چندان قوی نداشته‌است. وزارت فناوری اطلاعات و ارتباطات هند[1] در سال ۲۰۱۳ اولین سیاست امنیت سایبری ملی را منتشر ساخت[2] که سندی کوتاه مبنی بر ضرورت حفاظت از دولت، کسب‌وکارها و شهروندان در برابر حمله‌های سایبری بازیگران دولتی یا غیردولتی بود. این سند همچنین شامل توصیه‌های کلیدی برای سازمان‌های دولتی و شرکت‌های خصوصی ازجمله درباره تخصیص بودجه و نیروی انسانی موردنیاز برای تامین امنیت سایبری و تدوین سیاست‌های امنیت اطلاعات است. سند اخیر حاوی اهداف ملی در زمینه تامین امنیت سایبری است: آموزش ۵۰۰ هزار نیروی امنیت سایبری طی پنج سال، توسعه فناوری‌های بومی امنیت سایبری، ایجاد مشارکت‌های بخش خصوصی و بخش دولتی و ترویج فرهنگ امنیت سایبری و حریم خصوصی که می‌تواند کاربران را به رفتار مسئولانه در فضای سایبری ترغیب کند.

بخش خصوصی هند از همان آغاز مشارکت فعالی در زمینه تهیه سیاست‌های امنیت سایبری داشته‌است. دولت در سال ۲۰۲۰ قصد داشت راهبرد ملی جدیدی در زمینه امنیت سایبری تدوین کند که موضوعات اینترنت نسل پنجم (5G)، اینترنت اشیا و باج‌افزارها را شامل شود. با آنکه به نظر می‌رسد این برنامه متوقف شده‌باشد، اما روند

1. Ministry of Communications and Information Technology
2. National Cyber Security Policy

وزارت فناوری اطلاعات و ارتباطات، رجوع شود به:
'National Cyber Security Policy 2013', 2 July 2013, https://www.meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf.

اصلاح همه حوزه‌های سیاست امنیت سایبری مانند آموزش، مهارت‌ها، کنترل واردات و امنیت ملی همچنان ادامه دارد[۱]. تقابل نظامی با چین در مرز مورد اختلاف لاداخ[۲] در ژوئن ۲۰۲۰ و به‌دنبال آن افزایش سریع فعالیت‌های چین علیه شبکه‌های هند موجب افزایش نگرانی دولت نسبت به امنیت سایبری به‌ویژه در مورد سیستم‌های وارداتی از چین شد. نخست‌وزیر هند نارندرا مودی در ۲۰ آگوست ۲۰۲۰ در بخشی از سخنرانی خود در روز استقلال ضمن معرفی راهبرد جدید امنیت سایبری، وعده رونمایی از آن را در آینده نزدیک داد[۳]. در ژانویه ۲۰۲۱ نیز جلسه‌ای با حضور هیئت عالی‌رتبه‌ای از مقامات دولت برای بررسی راهبرد امنیت در بخش مخابرات تشکیل شد[۴]. احتمالا محورهای اصلی سیاست امنیت سایبری هند همسو با اولویت‌های بیان شده در طرح اولیه شورای امنیت داده هند (DSCI)[۵]- سازمان اصلی ذی‌ربط در امنیت سایبری بخش خصوصی- خواهد بود[۶]. این طرح پیشنهادی بیانگر ۲۱ حوزه اولویت‌دار در سیاست‌گذاری امنیت سایبری است و تهدیدهای فزاینده و اقدامات ناکافی دولت در زمینه مقابله با آن‌ها را متذکر می‌شود.

---

۱. رجوع شود به:
Aditi Agrawal, 'India's cybersecurity strategy policy in 2020, says National Cybersecurity Coordinator Rajesh Pant', Medianama, 22 June 2019,
https://www.medianama.com/2019/06/223-indias-cybersecurity-strategy-policy-in-2020-says -national-cybersecurity-coordinator-rajesh-pant

2. Ladakh

۳. رجوع شود به:
Elizabeth Roche, 'PM Modi says India to have new cyber security policy soon', Livemint, 15 August 2020, https://www.livemint.com/news/india/pm-modi-says-india-to-soon-havecyber-security-policy-11597461750194.html.

۴. رجوع شود به:
'Govt formulating new action plan, Chinese telecom giants could be out of game', Economic Times, 21 January 2021,
https://telecom.economictimes.indiatimes.com/news/govtformulating-new-action-plan-chinese-telecom-giants-couldbe-out-of-game/80391251.

5. Data Security Council of India

۶. رجوع شود به:
Data Security Council of India, 'National Cyber Security Strategy 2020: DSCI submission', 2020,
https://www.dsci.in/sites/default/files/documents/resource_centre/National%20Cyber%20Security%20Strategy%202020%20DSCI%20submission.pdf.

نیروهای مسلح هند در سال ۲۰۱۷ مبنای نظری مشترکی منتشر کردند که بیشتر محتوای آن حول مباحث جنگ اطلاعاتی بود و البته بر نقش مهم فضای سایبری نیز تاکید می‌کرد[۱]. این سند ادغام همه توانمندی‌های نیروهای مسلح را حیاتی برشمرده‌است و قدرت سایبری را نیز به‌اندازه قدرت زمینی، هوایی و فضایی ارتش و عملیات‌های نیروهای ویژه حائزاهمیت قلمداد می‌کند. سند مذکور قدرت سایبری را چنین تعریف می‌کند: توانایی استفاده آزاد و ایمن از فضای سایبری به‌منظور کسب مزیت نسبت به حریفان و جلوگیری از کسب چنین مزیتی توسط آن‌ها. بدین‌ترتیب، این سند (مبنای نظری) زمینه را برای ایجاد سازمان دفاع سایبری (DCA)[۲] هند فراهم کرد که درنهایت، در سال ۲۰۱۹ تاسیس شد. این سند اهمیت امنیت سایبری در اقتصاد و زیرساخت‌های ملی حیاتی را نیز یادآور می‌شود و دفاع از فضای سایبری کشور را هم‌سنگ دفاع از قلمرو، حریم هوایی و راه‌های تجاری می‌داند. علاوه بر این، مبنای نظری هند جنگ سایبری را بخشی از جنگ هیبریدی می‌داند که از عنصرهای کلیدی در جنگ نسل پنجم[۳] محسوب می‌شود (در این سند هیچ تعریف روشنی از جنگ هیبریدی یا جنگ نسل پنجم از منظر هند ارائه نشده‌است). سند جدید «مبانی نظری جنگ زمینی»[۴] ارتش هند که در سال ۲۰۱۸ منتشر شد نیز به توانمندی‌های سایبری می‌پردازد[۵]. این سند در لابه‌لای مباحث جنگ اطلاعاتی از فضای سایبری به‌عنوان بعد جدیدی از جنگ و از عوامل مهم در پیروزی نبردهای آینده یاد می‌کند.

۱. رجوع شود به:
Headquarters Integrated Defense Staff, Ministry of Defense, 'Joint Doctrine - Indian Armed Forces', 2017, https://bharatshakti.in/wp-content/uploads/2015/09/Joint_Doctrine_Indian_Armed_Forces.pdf.

2. Defense Cyber Agency
3. The 5th generation war
4. Land Warfare Doctrine

۵. رجوع شود به:
Indian Army, 'Land Warfare Doctrine 2018',
http://www.ssrij.com/MediaReport/DocumentIndianArmyLandWarfareDoctrine2018.pdf.

این سند پیش‌بینی می‌کند که توانمندی‌های سایبری در همه حوزه‌های نظامی ازجمله عملیات‌های پنهانی نفوذ خواهد کرد و از این رو، ارتش همزمان با توسعه و ارتقای توانمندی‌های سایبری دفاعی و بازدارنده خود به توسعه ظرفیت مقابله با تهدیدهای مستمر در فضای سایبری نیز خواهد پرداخت.

حکمرانی، فرماندهی و نظارت

اگرچه شکل‌گیری ساختار فرماندهی و نظارت سایبری هند از اوایل دهه ۲۰۰۰ آغاز شده‌است، اما همچنان غیرمتمرکز است. علت این امر آن است که اختیارات امنیت سایبری در چندین نهاد پراکنده است که خود منجر به هم‌پوشانی وظایف و روندهای زمان‌بر دیوان‌سالاری (بروکراتیک) شده‌است[1]. ساختار سیاسی فدرال هند نیز خود مزید بر علت شده و بر پیچیدگی این مسائل می‌افزاید. البته چندین نهاد کلیدی طی سال‌های ۲۰۰۴ و ۲۰۰۸ در وزارت‌های مختلف در این حوزه ایجاد شده‌است که همگی تحت لوای شورای امنیت ملی کابینه[2] انجام وظیفه می‌کنند. شورای امنیت ملی کابینه عالی‌ترین نهاد تصمیم‌گیری در زمینه سیاست‌های امنیت سایبری هند به‌شمار می‌رود. پس از آن، سازمان ملی تحقیقات فنی (NTRO)[3] که در سال ۲۰۰۴ و با الگوبرداری از سازمان امنیت ایالات متحده تاسیس شده‌است، سازمان سایبری اصلی هند محسوب می‌شود. این سازمان تحت‌نظارت مشاور امنیت ملی فعالیت می‌کند و موظف به جمع‌آوری اطلاعات

۱. رجوع شود به:
Tarun Krishnakumar, 'Cyber Insecurity: Regulating the Indian Financial Sector', Oxford University Faculty of Law, 21 August 2017,
https://www.law.ox.ac.uk/business-law-blog/blog/2017/08/cyber-insecurity-regulating-indian- financial-sector.

2. National Security Council of the Cabinet
3. National Technical Research Organization

فنی، شناسایی و دریافت سیگنال‌ها و انجام عملیات‌های نفوذ است[۱]. به‌همین‌ترتیب، تیم ملی پاسخ فوری رایانه‌ای (CERT-In)[۲] در سال ۲۰۰۳ تحت‌نظارت وزارت فناوری اطلاعات و الکترونیک[۳] تاسیس شد. در سال ۲۰۰۴ نیز هیئت ملی اطلاعات[۴] به‌عنوان کمیته‌ای مشورتی تشکیل شد تا ضمن تامین امنیت اطلاعات، سیاست ملی جنگ اطلاعاتی را هم تدوین کند[۵].

در سال ۲۰۰۸ با اصلاح قانون فناوری اطلاعات مصوب سال ۲۰۰۲، نهادهای دولتی از اختیارات گسترده‌ای برای صدور انواع حکم در زمینه شناسایی و دریافت سیگنال‌ها و پایش یا رمزگشایی انواع اطلاعات ازطریق هر منبع رایانه‌ای برخوردار شدند[۶]. علاوه بر این، قوانینی نیز برای حفاظت از شبکه‌های زیرساخت‌های حیاتی ملی تدوین شدند. در سال ۲۰۰۸، انجمن ملی شرکت‌های خدمات و فناوری اطلاعات[۷] که مهم‌ترین نهاد خصوصی در بخش فناوری اطلاعات و ارتباطات به شمار می‌رود، با راه‌اندازی شورای امنیت داده هند ابزاری موثر برای بسیج همه نیروها و اقدامات دولت در زمینه امنیت سایبری ایجاد کرد.

در گزارش وضعیت امنیت مورخ ۲۰۱۲-۲۰۱۱ که به دستور نخست‌وزیر هند تهیه شد، امنیت سایبری از حوزه‌های اصلی تاثیرگذار در توسعه کشور معرفی شد. این گزارش

---

۱. رجوع شود به:
B. Raman, 'Possible Misuse of New TECHINT Capabilities', Indian Defense Review, 5 December 2011, http://www.indiandefencereview.com/spotlights/possible-misuse-of-newtechint-capabilities.

2. Computer Emergency Response Team

3. Ministry of Electronics and Information Technology

4. National Information Board

۵. رجوع شود به:
Saikat Datta, 'Low on the IQ', Outlook, 4 July 2005, https://magazine.outlookindia.com/story/low-on-the-iq/227823.

۶. رجوع شود به:
'Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009', The Centre for Internet & Society, https://cis-india.org/internet-governance/resources/it-procedure-and-safeguards-forinterception-monitoring-and-decryption-of-information-rules-2009.

7. National Association of Software and Service Companies

همچنین حاوی توصیه‌هایی برای ایجاد نهاد فرماندهی سایبری متمرکز و نهادهای متناظر در بخش خصوصی با اختیار نظارت بر نهادهای دولتی بود[۱]. از سال ۲۰۱۳ و به‌دنبال کشف شواهدی مبنی بر جاسوسی سایبری کشورهای دیگر (مانند چین و ایالات متحده) علیه هند و نشت اطلاعات درباره توانمندی‌های سایبری تهاجمی این کشور، دولت به ضرورت توسعه سریع سیاست‌ها و اقدامات امنیتی سایبری پی برد. با این حال، روند توسعه نهادی امنیت سایبری در هند کند و پراکنده است.

مرکز ملی حفاظت از زیرساخت‌های اطلاعاتی حیاتی (NCIIPC)[۲] تحت‌نظارت سازمان ملی تحقیقات فنی در سال ۲۰۱۴ راه‌اندازی شد[۳] و مرکز ملی هماهنگی سایبری (NCCC)[۴] نیز در سال ۲۰۱۸ تحت تیم پاسخ فوری رایانه‌ای عملیات خود را آغاز کرد. وظیفه این مرکز به‌اشتراک‌گذاری اطلاعات بین نهادهای دولتی و هماهنگ‌سازی پاسخ‌های آن‌ها به حمله‌های سایبری است[۵]. سازمان دفاع سایبری نیز در سال ۲۰۱۹ تاسیس شد که نقش محوری در فرماندهی و نظارت فعالیت‌های سایبری نظامی هند ایفا می‌کند و ادغام و هماهنگی توانمندی‌های نیروهای ویژه، فضایی و سایبری همه نیروهای مسلح وظیفه اصلی آن محسوب می‌شود. این سازمان بخشی از ستاد دفاع یکپارچه[۶] و یا به‌عبارت

۱. رجوع شود به:
Vinod Anand, 'Defense Reforms and Naresh Chandra Task Force Review', Vivekananda International Foundation, 13 September 2012,
https://www.vifindia.org/article/2012/september/13/defence-reforms-and-naresh-chandra-task-force-review.

2. National Critical Information Infrastructure Protection Center

۳. سازمان ملی تحقیقات فنی، رجوع شود به:
https://ntro.gov.in/welcome.do.

4. National Cyber Coordination Center

۵. رجوع شود به:
'India now has a National Cyber Coordination Centre (NCCC) to monitor cyber threats', India Today, 11 August 2007,
https://www.indiatoday.in/education-today/gk-current-affairs/story/nccc-cyber-india-1029203-2017-08-11

6. Integrated Defense Staff

دیگر، ستاد مشترک نیروهای ارتش محسوب می‌شود که نمایندگانی غیرنظامی از وزارت امور خارجه[1] و سایر وزارت‌خانه‌ها در آن حضور دارند. سازمان دفاع سایبری دارای حدود ۱۰۰۰ نفر نیرو از همه واحدهای نیروهای مسلح است که در مرکز فرماندهی واقع در دهلی و سایر شعبه‌های آن در سراسر کشور مشغول به خدمت هستند[2]. این سازمان با عملیاتی‌سازی اصل ادغام همه توانمندی‌های نیروهای مسلح (از مبانی نظری امنیت سایبری در سال ۲۰۱۷)، نماد تحول نهادی و بلوغ رویکرد هند نسبت به کاربردهای نظامی فضای سایبری به شمار می‌آید.

توانمندی‌های محوری در اطلاعات سایبری

اولویت‌های اطلاعاتی هند به‌شدت تحت‌تاثیر تهدیدهای تروریستی داخلی و خارجی، خشونت سیاسی داخلی و اختلاف همیشگی آن با پاکستان درباره منطقه کشمیر است. اداره اطلاعات هند (IB)[3] بر امور داخلی متمرکز است و وظایف متعددی در زمینه فعالیت‌های ضدتروریستی و ضدجاسوسی با همکاری دولت‌های ایالتی و نیروهای شبه‌نظامی ملی برعهده دارد[4]. شاخه تحقیق و تحلیل (RAW)[5] نهاد ذی‌ربط در اطلاعات خارجی محسوب می‌شود. در حال حاضر، سازمان اطلاعات دفاعی وظیفه هماهنگی همه

1. Ministry of External Affairs

۲. رجوع شود به:
Rahul Bedi, ‘India setting up tri-service commands for special forces, cyber security, and space’, Jane’s Defense Weekly, 16 May 2019.

3. Intelligence Bureau

۴. رجوع شود به:
Mahendra Kumawat and Vinay Kaura, ‘Building the resilience of India’s internal security apparatus’, Observer
Research Foundation, Occasional Paper 176, November 2018,
https://www.orfonline.org/wp-content/uploads/2018/11/ORF_OccasionalPaper_176_Security_NEWFinalPDF.pdf.

5. Research and Analysis Wing

امور و نهادهای ذی‌ربط در اطلاعات و دفاع ازجمله اداره کل اطلاعات سیگنالی[1] را برعهده دارد. گردآوری اطلاعات توسط این سه نهاد به صورت دیجیتالی و آنی (به‌صورت زمان واقعی) ازطریق شبکه ملی اطلاعات (NATGRID)[2] انجام می‌شود. این شبکه همه منابع داده‌های شهروندان در سراسر پایگاه‌های داده دولتی و خصوصی را به هم پیوند می‌دهد و پایش اقدامات تروریسی تهدیدکننده شبکه‌های بانکی، مالی و حمل‌ونقل را تسهیل می‌کند. علاوه بر این، اداره اطلاعات و شاخه تحقیق و تحلیل به کمک سامانه‌ای که امکان دریافت اطلاعات ارتباطات اینترنتی ازجمله در رسانه‌های اجتماعی را فراهم می‌آورد، می‌توانند ترافیک اینترنت را پایش کنند[3]. این سه نهاد در عین حال که خود بخشی از توانمندی‌های اطلاعات سایبری هند محسوب می‌شوند، برای بسیاری از توانمندی‌های محوری اطلاعاتی به سازمان ملی تحقیقات فنی وابسته هستند. از دیگر نهادهای مهم حوزه اطلاعات سایبری هند می‌توان به بخش‌های زیرمجموعه وزارت کشور[4] ازجمله شاخه جرائم سایبری[5] و آزمایشگاه مرکزی علوم جرم‌شناسی[6] اشاره نمود.

به غیر از تهدیدهای داخلی، توانمندی‌های هند در زمینه اطلاعات سایبری بیشتر بر کشورهای نزدیک به‌ویژه پاکستان متمرکز هستند. به‌عنوان مثال، شواهدی درباره یک عملیات بزرگ جاسوسی و رصد سایبری موجود است که نشان می‌دهند هند از حدود سال ۲۰۱۰ چندین تیم سایبری را برای پایش آدرس‌های آی‌پی در پاکستان (و در

1. Signals Intelligence Directorate
2. National Intelligence Grid

۳. رجوع شود به:
Udbhav Tiwari, 'The Design & Technology Behind India's Surveillance Programmes', The Centre for Internet & Society, 20 January 2017,
https://cis-india.org/internet-governance/blog/the-design-technology-behind-india2019s- surveillanceprogrammes#_ftnref13.

4. Ministry of Internal Affairs
5. Cyber Crime Wing
6. Central Forensics Science Laboratory

سطح پایین‌تری در چین) و نیز جنبش‌های جدایی‌طلبانه در هند منصوب کرده‌است[۱]. دسترسی اطلاعات سایبری هند در مسافت‌های دورتر ضعیف است و از این رو، هند به‌منظور بهبود توانمندی‌های خود در زمینه آگاهی موقعیتی و افزایش دسترسی به‌ویژه برای عملیات‌های آتی از کشورهایی مانند ایالات متحده، بریتانیا و فرانسه کمک می‌گیرد.

هند با الگوبرداری از دولت بریتانیا کمیته مشترک اطلاعاتی را تشکیل داده‌است که مسئولیت گردآوری، ارزیابی و اولویت‌بندی همه اطلاعات و داده‌های دریافتی از نهادهای اطلاعاتی کشور را برعهده دارد[۲]. هند همچنین مرکز چندنهادی (MAC)[۳] را تحت اداره اطلاعات همراه با شعبه‌هایی در ایالت‌های مختلف تشکیل داده‌است که وظیفه ارتقای اشتراک‌گذاری اطلاعات بین واحدهای اطلاعاتی (ازجمله وزارت دارایی و وزارت دفاع) در سطح ایالتی و ملی را برعهده دارند.

توانمندی و وابستگی سایبری

هند با برخورداری از اقتصاد دیجیتالی به‌ارزش تقریبی ۱۹۰ میلیارد دلار یکی از قطب‌های فناوری اطلاعات و ارتباطات دنیا محسوب می‌شود[۴]. براساس برآوردها، بخش

۱. رجوع شود به:
Snorre Fagerland et al., 'Operation Hangover: Unveiling an Indian Cyber Attack Infrastructure', Norman Shark, May 2013,
http://docshare.tips/unveiling-an-indian-cyberattack-infrastructure_58a3ff6db6d87f499c8b462d.html.

2. Joint Intelligence Committee
رجوع شود به:
Musa Tuzuner (ed.), Intelligence Cooperation Practices in the 21st Century: Towards a Culture of Sharing (Amsterdam: IOS Press, 2010).

3. Multi-Agency Center

۴. این تخمین براساس برخی شاخص‌های محدود داخلی است. درواقع، مطابق رویکرد سازمان همکاری اقتصادی و توسعه (OECD) و سایر نهادهای مطالعاتی بین‌المللی باید گفت شاخص‌های بسیار بیشتری در ارزیابی اقتصاد دیجیتال دخیل هستند. براساس یکی از این تخمین‌ها، ارزش اقتصاد دیجیتال هند در سال ۲۰۱۹ معادل ۵۷۰ میلیارد دلار یعنی ۲۰ درصد از تولید ناخالص داخلی آن بوده‌است. برای کسب جزئیات بیشتر رجوع شود به:
'How the IT sector has emerged as a pillar of modern India', Hindu, 14 August 2020,
https://www.thehindubusinessline.com/news/national/how-the-it-sector-has-emerged-as-a-pillarof-modern-india/article32357389.ece.

بسیار بزرگ شرکت‌های نوپای فناورانه هند جایگاه سوم را در دنیا دارد[۱]. برخی گزارش‌ها نشان می‌دهند بخش‌های اصلی اقتصاد دیجیتال هند مانند خدمات مبتنی بر فناوری اطلاعات و ارتباطات و تولید الکترونیک ۱۰ درصد از تولید ناخالص داخلی آن را تا سال ۲۰۲۵ در اختیار خواهند داشت[۲]. البته هم‌اکنون تنها کمی بیش از نیمی از جمعیت ۱/۴ میلیارد نفری هند به اینترنت دسترسی دارند و مردان بسیار بیشتر از زنان از تلفن همراه و اینترنت استفاده می‌کنند[۳]. در هند دسترسی به اینترنت بیشتر ازطریق تلفن همراه است که سرعت دانلود آن کمتر از میانگین جهانی است. در بخش کشاورزی هند که هنوز هم معاش صدها میلیون نفر از مردم به آن وابسته است، در سال‌های اخیر به‌مدد مکانیزه‌سازی و دیجیتال‌سازی نسبی برخی ابزارها و فنون مبتنی بر ماشین‌آلات خودکار و مستقل به کار برده می‌شود. با این همه، بخش بزرگ‌تر جمعیت هند (حدود ۹۰ درصد) از مهارت‌های دیجیتالی پایه محروم هستند[۴]. ایجاد و افزایش دسترسی به انواع اپ‌ها و خدمات دیجیتال به زبان‌های محلی ازجمله اقدامات دولت هند برای رفع این چالش به شمار می‌آید.

---

۱. رجوع شود به:
Trisha Ray et al., The Digital Indo-Pacific: Regional Connectivity and Resilience, The Australian Government for the Quad Tech Network, February 2021, p. 8,
https://www.orfonline.org/wp-content/uploads/2021/02/thedigitalindopacific.pdf.

۲. رجوع شود به:
McKinsey Global Institute, 'Digital India: Technology to Transform a Connected Nation', March 2019,
https://www.mckinsey.com/ /media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20india%20technology%20to%20transform%20a%20connected%20 nation/digital-india-technology-to-transform-a-connected-nation-fullreport.ashx.

۳. رجوع شود به:
Romita Majundar, 'Gender gap in mobile and internet usage in India as per GSMA report', Business Standard, 9 March 2019,
https://www.business-standard.com/article/economy-policy/gender-gap-in-mobile-and-internet-usage-in-india-as-pergsma-report-119030900696_1.html.

۴. رجوع شود به:
Digital Empowerment Foundation, 'About', undated,
https://www.defindia.org/national-digital-literacy-mission

سرمایه‌گذاری خارجی نقش قابل‌توجهی در توسعه اقتصاد دیجیتال هند دارد، چنانچه هند اکنون قطب خدمات فناوری اطلاعات برون‌سپاری‌شده و محل تولید برندهای جهانی مانند دل[1] است. مجموع سرمایه‌گذاری ایالات متحده و ژاپن در فناوری اطلاعات و ارتباطات هند از سال ۲۰۱۴ تا سال ۲۰۲۰ به‌ترتیب بالغ بر ۳۰ و ۱۲ میلیارد دلار می‌شود[2]. چین نیز بیش از ۴ میلیارد دلار در فناوری اطلاعات و ارتباطات هند در همین بازه زمانی سرمایه‌گذاری کرده که سه‌چهارم آن متعلق به شرکت‌های علی‌بابا و تنسنت است[3].

زیرساخت‌های اصلی اقتصاد دیجیتال هند به تجهیزات وارداتی وابسته است. به‌عنوان مثال، چهار مورد از پنج وسیله همراه اصلی از نظر سهم بازار توسط شرکت‌های چینی ساخته شده‌اند[4] و تقریبا همه اپ‌های متداول در این کشور مانند پیام‌رسان فیس‌بوک، بَتل‌گِرَوند (PUBG)، آن‌نُون‌پلیر، شِیرایت، تیک‌تاک (حداقل تا قبل از ممنوعیت اپ‌های چینی در سال ۲۰۲۰)، تروکالر، یوسی بِروزِر و واتس‌اَپ[5] در خارج از کشور طراحی شده‌اند. در این میان، تنها مورد استثنایی شامل اپ دولتی آروگیا سِتو[6] است که برای ردیابی بیماران مبتلا به کوید-۱۹ ارائه شد و به‌سرعت فراگیر گشت. درنتیجه می‌توان گفت با وجود پیشرفت‌های قابل‌توجه شرکت‌های هندی در زمینه طراحی اپ و برنامه‌های دولت برای

1. Dell Computers

۲. رجوع شود به:
Ray et al., The Digital Indo-Pacific: Regional Connectivity and Resilience, p. 9.

۳. همان.

۴. رجوع شود به:
Sam Byford, 'Realme Takes Chunk of India Mobile Market as Samsung Slides', The Verge, 11 November 2019,
https://www.theverge.com/2019/11/11/20958932/india-mobile-marketshareq3-2019-idc-realme-samsung-xiaomi.

5. Facebook Messenger, PlayerUnknown's Battlegrounds, SHAREit, TikTok, Truecaller, UC Browser and WhatsApp

6. Aarogya Setu

توسعه سامانه‌های نسل پنجم (5G)، دولت هند همچنان نقش محدودی در نظارت بر وسیله‌ها و بسترهایی دارد که جریان داده را در کشور مدیریت می‌کنند.

هند در حوزه هوش مصنوعی وضعیت بسیار خوبی دارد و در دو مطالعه معتبر به جایگاه نهم[۱] و سیزدهم[۲] در سطح جهانی دست یافته‌است. قسمت اعظم فعالیت‌های تحقیق و توسعه هوش مصنوعی هند (۸۵ درصد) توسط دانشگاه‌ها انجام می‌شود[۳]. موسسه فناوری هند (IIT)[۴] در حیدرآباد با همکاری شرکت آمریکایی چندملیتی اِن‌ویدیا[۵] نسبت به ساخت اولین مرکز فناوری هوش مصنوعی هند با هدف شتاب بخشیدن به تحقیقات و تجاری‌سازی هوش مصنوعی اقدام کرده‌است[۶]. این مرکز قرار است به تحقیقات پیشرفته‌ای همسو با اولویت‌های راهبرد ملی هوش مصنوعی هند در حوزه‌های کشاورزی، شهرهای هوشمند و شناخت زبان بپردازد[۷]. جالب توجه است که

۱. رجوع شود به:
Jiqiang Niu et al., 'Global research on artificial intelligence from 1990-2014: Spatially-explicit bibliometric analysis', ISPRS International Journal of Geo-Information, vol. 5, no. 5, p. 8, https://www.mdpi.com/2220-9964/5/5/66/pdf

۲. رجوع شود به:
Gleb Chuvpilo, 'AI Research Rankings 2020: Can the United States Stay Ahead of China?', 21 December 2020, https://chuvpilo.medium.com/ai-research-rankings-2020-can-theunited-states-stay-ahead-of-china-61cf14b1216.

۳. رجوع شود به:
Richa Bhatia, 'Where Artificial Intelligence Research in India Is Heading', Analytics India Magazine blog, 27 March 2018, https://analyticsindiamag.com/where-artificial-intelligenceresearch-in-india-is-heading.

4. Indian Institute of Technology
5. Nvidia
6. AI Technology Center

رجوع شود به:
Anisha Kumari, 'IIT Hyderabad, NVIDIA Establish First AI Research Centre in India', NDTV, 9 July 2020, https://www.ndtv.com/education/iit-hyderabad-nvidia-establish-first-ai-researchcentre-in-india

۷. رجوع شود به:
Canadian Institute for Advanced Research, 'Building an AI World: Report on National and Regional AI Strategies Second Edition', May 2020, p. 22, https://cifar.ca/wp-content/uploads/2020/10/building-an-ai-world-second-edition.pdf.

مطالعه صورت گرفته توسط گروه مشاوره بوستون[۱] در سال ۲۰۱۸ نشان می‌دهد که هند بعد از ایالات متحده و چین رتبه سوم را از نظر به‌کارگیری هوش مصنوعی در فرایندهای صنعتی به خود اختصاص داده‌است[۲]. شرکت‌های نوپای هوش مصنوعی هند در سال ۲۰۱۹ با جذب ۷۶۲ میلیون دلار سرمایه شاهد افزایش ۴۴ درصدی سرمایه‌گذاری نسبت به سال ۲۰۱۸ بودند[۳].

صنعت فضایی هند تحت هدایت سازمان تحقیقات فضایی هند (ISRO)[۴] قرار دارد که یکی از شش سازمان فضایی بزرگ دنیا بوده و دارای یکی از بزرگ‌ترین ناوگان‌های ماهواره‌های مخابراتی و سنجش از راه دور با کاربردهای نظامی و غیرنظامی است[۵]. این سازمان ماهواره‌هایی با کاربری رصد و ناوبری نیز در اختیار دارد که ازجمله آن‌ها می‌توان به سامانه ماهواره‌ای ناوبری منطقه‌ای[۶] اشاره کرد که شامل سه مجموعه ماهواره می‌شود که قابلیت شناسایی سیگنال‌های الکترومغناطیسی کشورهای رقیب را دارند[۷]:

1. Boston Consulting Group

۲. رجوع شود به:
'India Ranked Third in Terms of Artificial Intelligence Implementation: Report - ET CIO', ETCIO, 26 April 2018, https://cio.economictimes.indiatimes.com/news/businessanalytics/india-ranked-third-in-terms-of- artificial-intelligenceimplementation-report/63922875.

۳. رجوع شود به:
AIMResearch, 'Report: Indian AI Startup Funding in 2019', 28 January 2020, p. 4, https://analyticsindiamag.com/report-indian-ai-startup-funding-in-2019.

4. Indian Space Research Organization

۵. رجوع شود به:
Indian Space Research Organization, 'About ISRO', https://www.isro.gov.in/about-isro.

۶. این سامانه دارای هفت ماهواره است که در اصل برای اهداف غیرنظامی به‌کار می‌روند، ولی داده‌های رمزگذاری‌شده‌ای نیز در اختیار نیروهای مسلح هند قرار می‌دهند. برای کسب جزئیات بیشتر رجوع شود به:
G.D. Sharma, Exploiting Indian Military Capacity in Outer Space (New Delhi: Centre for Joint Warfare Studies, 2016), https://cenjows.in/pdf/issue/Layout_Exploiting%20Indian%20Military.pdf.

۷. رجوع شود به:
Manu Pubby, 'Navy to Buy Rs 1,589 Crore Satellite From ISRO', Economic Times, 18 July 2019, https://economictimes.indiatimes.com/news/defence/navy-to-buy-rs-1589-crore-satellite-fromisro / articleshow/70283927.cms?from=mdr.

ماهواره‌های رصد دوکاره از سری‌های RISAT و Cartostat[1] و سری EMISAT که از سال ۲۰۱۹ در مدار قرار گرفته‌است. با توجه به محدودیت ظرفیتی نهادهای دولتی، دولت هند برای تامین تجهیزات فضایی مانند ماهواره و سامانه‌های احتراق به شرکت‌های بخش خصوصی روی آورده‌است. هند نیز همانند بسیاری از کشورها در تامین تجهیزات بخش فضایی به شرکت‌های خارجی وابسته‌است. به‌عنوان مثال، هند اجرای طرح سامانه پهن‌باند ماهواره‌ای برای شبکه ارتباطات دریایی[2] خود را به شرکت هیوز کامیونیکیشن ایندیا[3] سپرده‌است[4]. البته امروزه هند در تولید پرتابگرها[5] و برخی فناوری‌های ماهواره به خودکفایی رسیده‌است[6].

یکی از ویژگی‌های خاص اقتصاد سایبری هند، تعداد زیاد فارغ‌التحصیلان رشته‌های فناوری اطلاعات و ارتباطات است که هر ساله روانه بازار کار می‌شوند. شایان ذکر است تعداد فارغ‌التحصیلان رشته‌های فناوری اطلاعات و ارتباطات هند در سال ۲۰۱۹ معادل ۶۰۰ هزار نفر یعنی حدود ۵ برابر ایالات متحده بود[7].

---

۱. رجوع شود به:
Government of India, Department of Space, Indian Space Research Organization, 'List of Earth Observation Satellites',
https://www.isro.gov.in/spacecraft/list-of-earth-observation-satellites.

2. Naval Communication Network

3. Hughes Communication India

۴. رجوع شود به:
John Sheldon, 'Indian Military Space: Hughes India and Sterlite Tech Enable Satcom Connectivity for Indian Navy', Spacewatch, January 2019,
https://spacewatch.global/2019/01/indian-military-space-hughes-india-and-sterlite-tech-enablesatcom-connectivity-for-indian-navy.

5. Launch vehicle

6. Rajeswari Pillai Rajagopalan, Pulkit Mohan and Rahul Krishna, 'India in the Final Frontier: Strategy, Policy and Industry', ORF Special Report no. 100, Observer Research Foundation, 29 January 2020,
https://www.orfonline.org/research/india-in-the-final-frontier-strategy-policy-and-industry-60834.

۷. رجوع شود به:
Organization for Economic Co-operation and Development, Measuring the Digital Transformation: A Roadmap for the Future (Paris: OECD Publishing, 2019), p. 144,
https://www.oecd.org/publications/measuring-the-digital-transformation-9789264311992-en.htm.

امنیت و تاب‌آوری سایبری

هند دارای نهادهای دولتی متعددی در زمینه امنیت سایبری است که نیروی کار بسیار زیادی نیز در آن‌ها اشتغال دارند. هند همواره توجه زیادی به مساله جرائم سایبری داشته‌است، به‌طوری‌که اولین کشوری بود که در سال ۲۰۰۹ نسبت به راه‌اندازی پلیس سایبری و دادگاه‌های جرائم سایبری اقدام کرد. البته شاید مهم‌ترین ویژگی زیرساخت امنیت سایبری هند نقش بالای بخش خصوصی آن در این زمینه باشد که در تدوین سیاست‌ها و استانداردهای امنیت سایبری پیشتاز است. شتاب بالای ادغام اینترنت در اقتصاد و زندگی روزمره هند -البته در سطوح پایین- ضرورت توسعه توانمندی‌های امنیت سایبری در مقیاس و با شتابی بی‌همانند در کشورهای دیگر را برای آن دوچندان کرده است: در پنج سال گذشته صدها میلیون نفر هندی به تجارت الکترونیک روی آورده‌اند[1]. در نتیجه، این کشور با چالش‌های مهمی نظیر هماهنگی سیاست‌ها، برقراری ثبات (سیاستی و اقتصادی) در سراسر کشور و ارتقای مهارت‌های امنیت سایبری متناسب با اندازه جمعیت و نیازهای صنعت مواجه است.

در سال‌های اخیر، هند قربانی تعداد زیادی حمله‌های سایبری به‌ویژه به زیرساخت‌های حیاتی خود بوده‌است که اغلب آن‌ها را از جانب چین یا پاکستان می‌داند. به‌عنوان مثال، گزارش تیم پاسخ فوری رایانه‌ای هند حاکی از این واقعیت

۱. دولت مرجع یکتای تعیین هویت را در سال ۲۰۱۶ تاسیس کرد تا با ارائه روش‌های جدید تعیین هویت بتواند بانکداری و تجارت الکترونیک به‌ویژه در بستر تلفن همراه را ایمن‌تر سازد. روند کار این سازمان با شتاب زیاد روبه‌رشد است، به‌طوری‌که در حال حاضر ۱/۲۴ میلیارد نفر از جمعیت کشور در سامانه آن ثبت شده‌اند. برای کسب جزئیات بیشتر رجوع شود به:
Organization for Economic Co-operation and Development, Measuring the Digital Transformation: A Roadmap for the Future (Paris: OECD Publishing, 2019), p. 144, https://www.oecd.org/publications/measuring-the-digital-transformation-9789264311992-en.htm.

است که این کشور در سال ۲۰۱۹ شاهد بیش از ۳۹۴,۴۹۹ مورد حمله سایبری بوده‌است[۱]. تعداد حمله‌های منتسب به چین نیز در سال ۲۰۲۰ با رشد جهشی همراه بوده‌است[۲]. به‌علاوه، حمله‌های سایبری کره شمالی با استفاده از تجهیزات زیرساخت‌های دیجیتال چین یکی از دغدغه‌های دولت هند است. بیشتر حمله‌های سایبری که تیم پاسخ فوری رایانه‌ای هند تاکنون شناسایی کرده‌است، از نوع جاسوسی بوده‌اند[۳] که برخی از آن‌ها می‌توانسته‌اند منجر به خسارت‌های جدی به یکپارچگی شبکه‌ها و بسترهای هند شوند. این کشور در سال ۲۰۲۰ شاهد دومین تعداد بالای حمله‌های باج‌افزاری در دنیا بوده[۴] و به همین سبب نیز دولت ۱۱۷ برنامه کاربردی چینی را به دلایل امنیتی ممنوع اعلام کرده‌است[۵].

۱. رجوع شود به:
Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology, 'CERT-In Annual Report (2019)', p. 3,
https://www.cert-in.org.in/Downloader?pageid=22&type=2&fileName=ANUAL-2020-0001.pdf

۲. رجوع شود به:
Manu Kaushik, '200% rise in cyberattacks from China in a month; India tops hit list post Galwan face-off', Business Today, 24 June 2020,
https://www.businesstoday.in/technology/news/200-percent-rise-in-cyberattacks-from-china-in-a-month-india-topshit-list-post-galwan-face-off/story/407806.html.

۳. رجوع شود به:
Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology, 'CERT-In Annual Report (2019)', p. 3,
https://www.cert-in.org.in/Downloader?pageid=22&type=2&fileName=ANUAL-2020-0001.pdf

۴. رجوع شود به:
National Critical Information Infrastructure Protection Centre, 'NCIIPC Newsletter', January 2021, p. 2,
https://nciipc.gov.in/documents/NCIIPC_Newsletter_Jan21.pdf.

۵. رجوع شود به:
'India bans PUBG, 117 other Chinese apps for 'stealing, transmitting users' data' to servers outside India', First Post, 20 September 2020,
https://www.firstpost.com/india/india-banspubg-117-other-chinese-apps-for-stealing-transmitting-usersdata-to-servers-outside-india-8778561.

دهلی‌نو موسسات مالی خود را به‌شدت در معرض حمله‌های سایبری می‌بیند[۱]. در آگوست ۲۰۱۸ طی حمله‌های مستمر به بانک کازماس[۲] هند توسط گروهی از کره شمالی، ۱۳/۵ میلیون دلار از حساب‌های مشتریان آن اختلاس شد[۳]. گزارش گروه کارشناسی شورای امنیت سازمان ملل[۴] در جولای ۲۰۱۹ نشان می‌دهد که گروه‌هایی از کره شمالی طی دوره‌ای سه‌ساله از بانک‌های هندی حدود ۲۰۰ میلیون دلار سرقت کرده‌اند[۵]. از طرفی، بخش مالی این کشور به‌لطف دستورالعمل‌های سخت‌گیرانه بانک مرکزی هند (RBI)[۶] نسبت به سایر بخش‌های اقتصاد ایمن‌تر است. به‌عنوان مثال، فرآیند تایید هویت دوعاملی که بانک مرکزی هند با جدیت آن را اعمال می‌کند، اکنون در تمام مبادلات بانکداری اینترنتی و تجارت الکترونیک رعایت می‌شود[۷].

---

۱. رجوع شود به:
'Banks Most Vulnerable to Cyber Threats: National Cyber Security Coordinator', New Indian Express, 20 February 2019,
https://www.newindianexpress.com/business/2019/feb/20/banksmost-vulnerable-to-cyber-threats-national-cyber-securitycoordinator-1941363.html.

2. Cosmos Bank

۳. رجوع شود به:
Rashmi Rajput, 'UN Security Council Panel Finds Cosmos Bank Cyber Attack Motivated by N Korea', Economic Times, 27 March 2019,
https://economictimes.indiatimes.com/industry/banking/finance/banking/un-security-councilpanel-finds-cosmos-bank-cyber-attack-motivated-by-n-korea/articleshow/68589549.cms?from=mdr.

۴. گروه کارشناسی شورای امنیت سازمان ملل (A United Nations Security Council panel of experts) برای بررسی اقدامات کره شمالی جهت دور زدن تحریم‌های بین‌المللی منصوب شده‌است.

۵. رجوع شود به:
United Nations Security Council, 'Report of the Panel of Experts established pursuant to Resolution 1874 (2009)', 5 March 2019, S/2019/171,
https://www.ssecuritycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3CF6E4FF96FF9%7D/s_2019_171.pdf

6. Reserve Bank of India

۷. رجوع شود به:
Reserve Bank of India, 'Master Direction on Digital Payment Security Controls', 18 February 2021,
https://rbidocs.rbi.org.in/rdocs/notification/PDFs/MD7493544C24B5FC47D0AB12798C61CDB56F.PDF.

برخلاف دولت هند که در توسعه امنیت سایبری تا حدی کند عمل کرده‌است، بخش خصوصی آن اقداماتی بسیار بیشتر و موثرتر در این زمینه انجام داده‌است. علاوه بر ترویج استانداردها و الگوهای عالی امنیت سایبری و حریم خصوصی، شورای امنیت داده هند پروژه‌های ظرفیت‌سازی نیز در زمینه آموزش و صدور مجوز ازجمله برای نهادهای دولتی اجرا می‌کند. این شورا در سال ۲۰۲۰ مشارکت جدی دولت در زمینه ارتقای امنیت سایبری کشور را ضروری دانست و با توجه به توسعه اقتصاد دیجیتال پیشنهاد داد بودجه امنیت سایبری چهار برابر افزایش یابد. با این همه، هند در رتبه‌بندی اتحادیه بین‌المللی مخابرات (۲۰۱۸) با کسب رتبه ۴۷ در بین ۱۷۵ کشور در جایگاهی بسیار پایین‌تر از رقیب ژئوپلیتیک خود یعنی چین (با رتبه ۲۷) قرار داشت[۱].

هند برنامه‌های متعددی در زمینه سیاست‌های تاب‌آوری سایبری و آمادگی برای شرایط بحران در دست اجرا دارد. به‌عنوان مثال، مرکز ملی حفاظت از زیرساخت‌های اطلاعاتی حیاتی از زمان تاسیس خود در سال ۲۰۱۴ همواره به ترویج و ارتقای سیاست‌ها و رویه‌های امنیت سایبری در سراسر کشور پرداخته‌است. البته برنامه‌های ارتقای پاسخ فوری در سطح ایالت‌ها اغلب به کندی پیش می‌رود، چنانچه ایالت تامیل نادو[۲] به تازگی (در سال ۲۰۲۰) توانسته‌است راهبرد امنیت سایبری خود را ارائه نماید[۳].

---

۱. رجوع شود به:

International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 58, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

2. Tamil Nadu

۳. رجوع شود به:

Raja Simhan, 'TN govt working on giving the 'cyber resilience' edge to governance', The Hindu Business Line, 24 December 2020, https://www.thehindubusinessline.com/infotech/tn-govt-working-on-giving-the-cyber-resilience-edge-togovernance/article33409737.ece.

با این حال، شهر بمبئی به‌عنوان قطب مالی و تجاری منطقه مهاراشترا[1] دارای تیم امنیت سایبری کاملا سازمان‌یافته‌ای در نیروهای پلیس است و ایستگاه‌های پلیس سایبری در قسمت‌های مختلف این شهر وجود دارد.

مرکز ملی حفاظت از زیرساخت‌های اطلاعاتی حیاتی هند در مقایسه با نهادهای مشابه در کشورهای ثروتمندتر فاقد آمادگی لازم برای رویارویی با بحران‌های فوری سایبری و نیز توان برنامه‌ریزی برای ارتقای تاب‌آوری در سطح وسیع است، به‌طوری‌که در سال ۲۰۱۸ تنها در یک بخش (بخش برق قدرت) امکان سازمان‌دهی و هماهنگی ذینفعان حول اهداف موردنظر وجود داشت[2]. علاوه بر این، نشانه‌هایی نیز مبنی بر ناهماهنگی بین این نهاد با سایر نهادهای دولتی وجود دارد[3]. به‌عنوان مثال، پس از هک شدن پایگاه داده اطلاعات بیومتریک شهروندان (دومین پایگاه داده بزرگ دنیا) در مرجع یکتای تعیین هویت هند[4] در سال ۲۰۱۷، دقیقا مشخص نشده‌است که آیا اقدامی جهت بهبود دفاع سایبری آن انجام گرفته‌است یا خیر. به‌همین‌ترتیب، در مورد نیروگاه برق هسته‌ای کودان‌کولام[5] که در سال ۲۰۱۹ هدف حمله سایبری جدی قرار گرفت و در ابتدا انکار شد و درنهایت هم حجم حادثه ناچیز اعلام شد،

1. Maharashtra

۲. رجوع شود به:

Munish Sharma and Cherian Samuel, India's Strategic Options in a Changing Cyberspace (Delhi: Pentagon Press, 2018), p. 110, https://idsa.in/system/files/book/book_indias-strategic-options-incyberspace.pdf.

۳. رجوع شود به:

Saikat Datta, 'Defending India's Critical Information Infrastructure', Internet Democracy Project, 2016, https://internetdemocracy.in/wp-content/uploads/2016/03/Saikat-Datta-Internet-Democracy -Project-DefendingIndias-CII.pdf;

Shatabdi Mazumder, 'The Need for Re-conditioning of India's Cyber Security', Apeksha News Network, 28 September 2020, https://apekshanews.com/the-need-for-re-conditioning-of-indias-cyber-security.

4. Unique Identification Authority
5. Kudankulam Nuclear Power Plant

به‌طور قطع نمی‌توان گفت که آیا اقدامی درجهت ارتقای دفاع سایبری آن انجام گرفته‌است یا خیر[۱]. در منطقه مهاراشترا نیز وقتی صنعت برق از اوایل سال ۲۰۲۰ مورد حمله هکرهای چینی موسوم به گروه اِکوی قرمز[۲] قرار گرفت، ظاهرا تیم پاسخ فوری رایانه‌ای هند از نوامبر ۲۰۲۰ به پلیس ایالتی درباره این تهدید هشدار داده‌بود. این در حالی است که مرکز ملی حفاظت از زیرساخت‌های اطلاعاتی حیاتی هند در ۱۲ فوریه ۲۰۲۱ وزارت برق را از این موضوع مطلع کرد[۳].

با آنکه سازمان هماهنگ کننده امنیت سایبری ملی[۴] به‌طور دوره‌ای همه نهادهای دولتی ذی‌ربط را بازرسی می‌کند، اما دولت همچنان در هماهنگ ساختن نهادهای تازه‌تاسیس مانند مرکز ملی حفاظت از زیرساخت‌های اطلاعاتی حیاتی هند با نهادهای قدیمی‌تر که در مراحل مختلف از فرآیند دیجیتال‌سازی زیرساخت‌های خود هستند، با مشکلات بسیاری روبروست. مرکز ملی حفاظت از زیرساخت‌های اطلاعاتی حیاتی هند شرکت‌های بخش خصوصی مانند شرکت‌های نفتی و گازی را تحت پوشش خود درآورده‌است و می‌کوشد بخش خصوصی و بخش دولتی در کنار هم و با هماهنگی یکدیگر در زمینه تامین امنیت سایبری فعالیت کنند.

---

۱. رجوع شود به:
Sushovan Sircar and Vakasha Sachdev, 'Kudankulam Cyber Attack Did Happen, Says NPCIL a Day After Denial', The Quint, 1 November 2019,
https://www.thequint.com/news/india/kudankulam-nuclear-power-plant-malware-attackcorrect-confirms-npcil.

2. Red Echo

۳. رجوع شود به:
'Chinese cyber attack foiled: Power Ministry', Hindu, 1 March 2021,
https://www.thehindu.com/news/national/attacks-by-chinesegroups-thwarted-power-ministry/article33965683.ece.

4. National Cyber Security Coordinator

اولین رزمایش سایبری در نیروهای مسلح هند با نام سایبر اِکس[1] توسط دانشگاه دفاعی هند[2] در تاریخ ۲-۳۰ آوریل ۲۰۱۹ اجرا شد[3]. سازمان ملی تحقیقات فنی، هر سه شاخه نیروهای مسلح (زمینی/دریایی/هوایی)، دبیرخانه شورای امنیت ملی[4]، تیم پاسخ فوری رایانه‌ای هند، سازمان تحقیق و توسعه دفاعی[5]، مرکز ملی انفورماتیک[6] و فعالان بخش صنعت و دانشگاه در این رزمایش حضور داشتند.

رهبری جهانی در عرصه سایبری

هند به‌عنوان قدرتی هسته‌ای که یکی از بزرگ‌ترین نیروهای مسلح و اقتصاد دیجیتال روبه‌رشد را داراست، مصمم به افزایش نفوذ ژئوپلیتیک خود در منطقه و جهان است و به همین دلیل نیز هدف حمله‌های جاسوسی سایبری متعددی از سوی دولت‌های مختلف قرار می‌گیرد. دهلی‌نو از ضعف نسبی توانمندی‌های دفاعی خود آگاه است و می‌کوشد حکمرانی فضای سایبری را ازطریق دیپلماسی تحت نظم و مقررات بین‌المللی قرار دهد. همزمان، دهلی‌نو در تلاش است در تعامل با کشورهایی که به شبکه‌های آن حمله سایبری می‌کنند، رفتاری مبتنی بر رویکرد واقع‌بینانه داشته باشد.

براساس سیاست امنیت سایبری ملی هند (۲۰۱۳)، برقراری روابط دوجانبه و چندجانبه در زمینه امنیت سایبری و برقراری همکاری‌های جهانی با نهادهای ملی

1. CyberEx
2. Indian Defense University

۳. رجوع شود به:

Press Information Bureau, 'Cyber Exercise on Scenario Building & Response', 29 April 2019, http://pib.nic.in/newsite/PrintRelease.aspx?relid=189871.

4. National Security Council Secretariat
5. Defense Research and Development Organization,
6. National Informatics Center

فعال در زمینه اجرای قانون، خدمات امنیتی، نظام‌های قضایی و نیروهای مسلح سایر کشورها ازجمله اهداف دیپلماتیک این کشور در نظر گرفته شده‌اند.

از آنجا که هند با چالش‌های زیادی در دفاع از شبکه‌های باز و زیرساخت‌های عمدتا وارداتی خود مواجه است، جای تعجب ندارد که این کشور حامی هنجاری‌های بین‌المللی محدودسازی فضای سایبری است. به نظر می‌رسد هند دیگر چون گذشته با اصول حقوقی بین‌المللی نوپدید مانند هنجارهای داوطلبانه امنیت در فضای سایبری که گروه کارشناسان دولتی سازمان ملل مطرح کرده‌اند، مخالف نیست[1]. در سال ۲۰۱۷-۲۰۱۶، هند به‌عنوان عضوی از گروه کارشناسان دولتی از افزودن مبحث «حق دفاع از خود در فضای سایبری» در گزارش نهایی این گروه پشتیبانی کرد، هرچند این پیشنهاد نتوانست موافقت همه اعضا را کسب کند[2]. با این حال، هنوز نمی‌توان پیش‌بینی کرد که هند در آینده هم همچنان از حق دولت‌ها برای انجام اقدامات تلافی‌جویانه در برابر اعمالی که طبق قوانین بین‌المللی تهدید، استفاده از زور یا حمله مسلحانه تلقی می‌شوند، پشتیبانی می‌کند یا خیر.

مهم‌ترین مشارکت سایبری دوجانبه هند با ایالات متحده آمریکاست. هند و آمریکا از اوایل دهه ۲۰۰۰ به‌طور مداوم گفت‌وگوهای سایبری داشته‌اند و به‌ویژه از سال ۲۰۱۵ که دو کشور تصمیم گرفتند برنامه Track 1.5 را به‌منظور گردهم آوردن مقامات دولتی و رهبران کسب‌وکارها جهت همکاری در زمینه مسائل سایبری اجرا کنند، مشارکت بیشتری نیز داشته‌اند. درواقع، موضوع سایبری بخش اصلی بسیاری از توافق‌های

۱. رجوع شود به:
UN Office for Disarmament Affairs, 'Developments in the field of information and telecommunications in the context of international security',
https://www.un.org/disarmament/ict-security.

۲. مصاحبه با یکی از اعضای این گروه در آگوست ۲۰۱۷.

آمریکا و هند ازجمله توافق‌های مربوط به به‌اشتراک‌گذاری اطلاعات و همکاری حقوقی دوجانبه است[۱].

هند گفت‌وگوهای دوجانبه‌ای نیز با سایر شرکای خود مانند اتحادیه اروپا، روسیه و بریتانیا داشته و به‌ویژه با بریتانیا مشارکت سایبری خوبی شکل داده‌است و از سال ۲۰۱۲ گفت‌وگوهای مشترک سایبری آن‌ها همچنان تداوم داشته‌است. در آوریل ۲۰۱۸، هند و بریتانیا توافق‌نامه چارچوبی امضا کرده‌اند که مشتمل بر تعیین مجراهای همکاری دوجانبه در زمینه امنیت سایبری و ایجاد کارگروه‌های مرتبط با دیپلماسی سایبری، جرائم سایبری، پاسخ به حوادث و اقتصاد دیجیتال است[۲]. هر دو کشور درباره تاسیس یک مرکز عالی آموزش امنیت سایبری نیز به توافق اولیه‌ای دست یافته‌اند[۳].

توانمندی‌های سایبری تهاجمی

براساس اظهارات رسمی مقام‌های هندی و سایر منابع موجود می‌توان گفت هند توانمندی‌های سایبری تهاجمی نسبتا پیشرفته‌ای با تمرکز بر پاکستان در اختیار دارد و هم‌اکنون نیز در حال توسعه این توانمندی‌ها برای گسترش دامنه آن‌هاست.

---

۱. رجوع شود به:
Nayantara Ranganathan, ‘Cybersecurity and bilateral ties of India and the United States: A very brief history’, Internet Democracy Project, 30 September 2015, https://internetdemocracy.in/reports/cybersecurity-and-india-us-bilateral-ties-a-very-brief -history.

۲. رجوع شود به:
Rahul Roy-Chaudhury, ‘India-UK cybersecurity cooperation: The way forward’, International Institute for Strategic Studies blog, 22 November 2019, https://www.iiss.org/blogs/analysis/2019/11/sasia-india-uk-cyber-security-cooperation.

۳. رجوع شود به:
Rahul Roy-Chaudury, ‘India-UK cyber security cooperation: The way forward’, India Global Business, 15 November 2019, https://www.indiaglobalbusiness.com/igb-archive/india-ukcyber-security-cooperation-the-way-forward-india-globalbusiness.

شـواهد موجـود نشـان می‌دهند هنـد در نوامبر ۲۰۰۸ پـس از حمله‌های تروریسـتی در بمبئـی قصد داشته‌اسـت عملیات سـایبری به رهبری سـازمان ملی تحقیقـات فنی انجام دهـد[۱]. پـس از آن سـال نیـز یکی از مشـاوران سـابق امنیت ملـی هند تایید کرد کـه هند از ظرفیـت قابل‌ملاحظـه‌ای بـرای اجـرای عملیات‌هـای خرابـکاری سـایبری علیـه پاکسـتان برخوردار است[۲]. چنین به نظر می‌رسد که این ادعا صحت داشته باشد.

بـرآورد حجـم و جهـت‌گیری سـرمایه‌گذاری‌های هنـد در توانمندی‌هـای سـایبری تهاجمـی دشـوار اسـت، امـا نشـانه‌هایی مبنـی بر تغییـر نقطـه تمرکز آن به‌سـمت چین وجـود دارد کـه باتوجه به رشـد اقتصاد و قدرت منطقه‌ای چین منطقی به نظر می‌رسـد[۳]. شـواهدی نیز در دسـت اسـت که نخست‌وزیر مودی در سـال ۲۰۱۴ مایل به ایجاد نوعی نیروی مسـلح دیجیتال به‌عنوان بخشـی از پاسخ بازدارنده کشور بوده‌است[۴].

در گزارش انتشـاریافته توسـط یکی از اندیشـکده‌های معروف هند وابسـته به حزب حاکـم بهاراتیـا جاناتـا[۵] در سـال ۲۰۱۹ نیـز بـه دولـت توصیه شده‌اسـت تـا توانمندی‌های

۱. رجوع شود به:
Raj Chengappa and Sandeep Unnithan, 'How to PunishPakistan', India Today, 22 September 2016, https://www.indiatoday.in/magazine/cover-story/story/20161003-uriattack-narendra-modi-pakistan-terror-kashmir-nawaz-sharifindia-vajpayee-829603-2016-09-22.

۲. رجوع شود به:
M.K. Narayanan, 'The Best among Limited Options', Hindu, 1 November 2016, https://www.thehindu.com/opinion/lead/The-best-among-limited-options/article14990381.ece

۳. رجوع شود به:
Arditi Agrawal, 'India's Cybersecurity Strategy Policy in 2020, Says National Cybersecurity Coordinator Rajesh Pant', Medianama, 22 June 2019, https://www.medianama.com/2019/06/223-indias-cybersecurity-strategy-policy-in-2020-says -national-cybersecurity-coordinator-rajesh-pant.

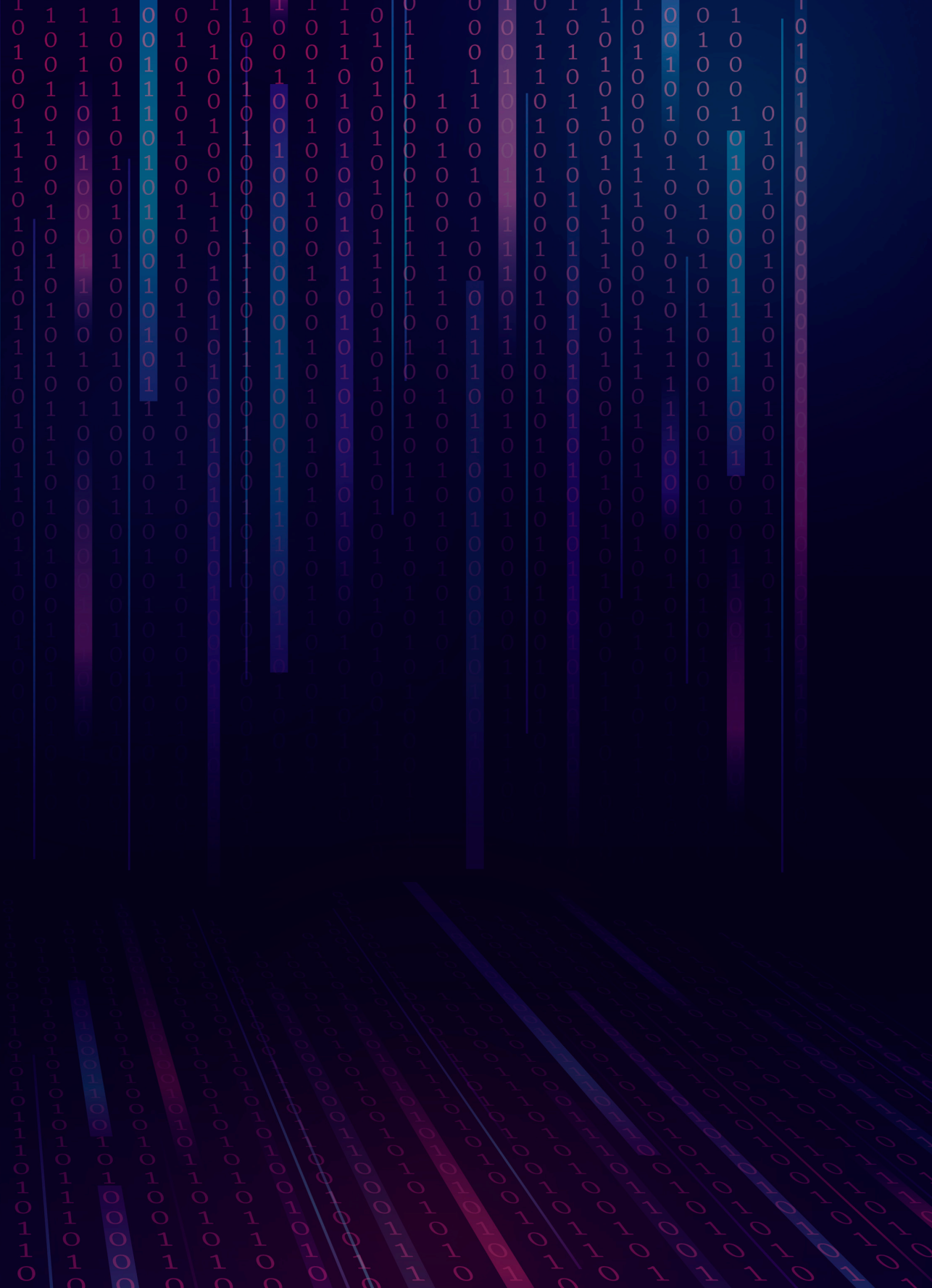
۴. رجوع شود به:
Narendra Modi, 'PM's Address at the Combined Commanders' Conference', 17 October 2014, https://www.narendramodi.in/amp/pms-address-at-the-combined-commanders-conference.

5. Bharatiya Janata Party

سـایبری تهاجمـی خـود را به‌سـرعت توسـعه دهـد، ولی تـا قبـل از عملیاتی‌شـدن درباره آن‌ها اطلاع‌رسانی عمومی نشود[۱].

درمجموع می‌توان گفت تمرکز همیشـگی هند روی پاکسـتان باعث شده‌اسـت این کشـور تجـارب و دانـش عملیاتـی خوبـی حداقـل در سـطح منطقـه‌ای در اختیـار داشـته باشـد. با این حال، هند با گسـترش دسترسی اطلاعات سـایبری خود باید بتواند امکان بهره‌بـرداری از توانمندی‌هـای سـایبری تهاجمی کشـور را در هدف‌های دورتـر نیز فراهم کنـد کـه البته با همکاری نزدیک با شـرکای بین‌المللی ازجمله ایالات متحده دسـت‌یابی به این هدف راحت‌تر خواهد شـد.

۱. رجوع شود به:
Vivekananda International Foundation, ‘Credible Cyber Deterrence in Armed Forces of India’, March 2019, https://www.vifindia.org/sites/default/files/Credible-Cyber-Deterrence-inArmed-Forces-of-India_0.pdf.



۱۳

اندونزی

اندونـزی اولیـن راهبرد رسـمی برای امنیت سـایبری در بخش غیرنظامی را در سـال ۲۰۱۸ یعنی یک سـال پس از تاسـیس سازمان سـایبری اصلی خود تدوین کرد، ولی آغاز تغییرات سـازمانی آن (مرتبط با مسـائل سـایبری) از حوالی سـال ۲۰۱۴ بود. با این‌حال، اندونـزی هنـوز هیچ‌گونه راهبرد یا مبنای نظری (دکترین) به‌طور رسـمی منتشـر نکرده اسـت. در اندونزی سیاسـت‌گذاری سـایبری در حوزه اختیارات رئیس‌جمهور قرار دارد. باآنکـه اندونـزی توانمندی‌های بسـیار محـدودی در زمینـه اطلاعات سـایبری دارد، اما سـرمایه‌گذاری‌های قابل‌توجهـی در پایـش سـایبری بـا هـدف تامیـن امنیـت سـایبری داخلـی خـود انجـام داده‌اسـت و فناوری‌های دیجیتال بیشـتری را در مقایسـه با سـایر کشـورهای درحال‌توسـعه بـه‌کار گرفته‌اسـت. در عرصـه سیاسـت‌های بین‌المللـی نیز اندونـزی به‌عنـوان عضـوی از گـروه ۲۰، سـازمان همـکاری اقتصـادی آسیا-اقیانوسـیه (اَپـک)، اتحادیـه کشـورهای جنوب شـرق آسـیا (آسـه‌آن) و سـازمان همکاری اسـلامی[1] حضوری فعال دارد. علی‌رغم اینکه اندونزی تا اندازه‌ای از توانمندی‌های حوزه اطلاعات سـایبری و جاسوسـی سایبری برخوردار است، ولی شـواهد چندانی مبنی براینکه قصد اسـتفاده از این توانمندی‌ها در عملیات‌های سـایبری تهاجمی داشـته باشد و یا اینکه قبلا عملیات تهاجمی انجام داده‌باشـد، در دست نیست. درمجموع، اندونزی کشوری رده سـوم در قـدرت سـایبری اسـت و باتوجـه بـه اینکـه انتظـار مـی‌رود تـا سـال ۲۰۳۰ به چهارمیـن اقتصـاد بـزرگ دنیا تبدیل شـود، در صورتی که دولت با درک ضرورت شـرایط راهبـردی فعلـی به سـرمایه‌گذاری‌های گسـترده در حوزه سـایبری روی آورد، این کشـور خواهد توانست به رده دوم صعود کند.

1. Organization of Islamic Cooperation

راهبرد و مبنای نظری (دکترین)

اندونزی تا سال ۲۰۱۷ تقریبا هیچ پیشرفتی در زمینه سیاست فضای سایبری نداشت. نهادها، بنیان حقوقی و مناسبات و هماهنگی‌های آن بسیار ضعیف بودند و هیچ راهبرد ملی نیز تدوین نکرده‌بود[۱]. تنها برخی زیرساخت‌های نهادی در این کشور بنیان‌گذاری شده‌بود: سازمان رمزنگاری ملی[۲] (تاسیس در سال ۱۹۴۶) تا حدودی متناسب با ضرورت‌های سایبری تقویت شده‌بود، یک تیم پاسخ فوری رایانه‌ای (CRET) نیز در سال ۱۹۹۷ به‌ابتکار بخش خصوصی تشکیل شد و یک تیم دولتی پاسخ رویداد-زیرساختی[۳] (که در عمل نوعی تیم پاسخ فوری رایانه‌ای است) نیز در سال ۲۰۰۷ ایجاد شد[۴]. البته بالغ بر ۱۶ تیم پاسخ فوری رایانه‌ای دیگر نیز تا سال ۲۰۱۶ ایجاد شد و تعدادی از قوانین و مقررات اصلاح شدند[۵].

تاسیس سازمان ملی رمزنگاری و سایبری (BSSN)[۶] با حکم ریاست‌جمهوری پیشرفت ویژه‌ای بود که در سال ۲۰۱۷ رخ داد که جایگزین سازمان ملی رمزنگاری شد[۷].

---

۱. رجوع شود به:
Yudhistira Nugraha, 'The future of cyber security capacity in Indonesia', Oxford Internet Institute, 2016, https://ora.ox.ac.uk/objects/uuid:70392ace-4bd6-4066-818e-a3adc1eeedf3.

2. National Crypto Agency

3. Government Infrastructure-Incident-Response Team

۴. نام کامل آن تیم پاسخ رویداد امنیت اندونزی در حوزه اینترنت و زیرساخت/مرکز هماهنگی یا (Indonesia Security Incident Response Team on Internet and Infrastructure/Coordination Center (ID-SIRTII/CC)) است. رجوع شود به:
'History Id-SIRTII/CC',
https://idsirtii.or.id/en/page/history-id-sirtii-cc.html.

۵. رجوع شود به:
Leonardus K. Nugraha and Dinita A. Putri, 'Mapping the Cyber Policy Landscape: Indonesia', Global Partners Digital, November 2016, pp. 14-15,
https://www.gp-digital.org/wp-content/uploads/2017/04/mappingcyberpolicy_landscape_indonesia.pdf.

6. National Cyber and Crypto Agency
رجوع شود به:
Badan Siber Dan Sandi Negara,
https://bssn.go.id/tentang.

۷. به‌عبارت دقیق‌تر، این سازمان مسئولیت‌های سازمان ملی رمزنگاری و تیم پاسخ رویداد امنیت اندونزی در حوزه اینترنت و زیرساخت و اداره کل امنیت اطلاعات وزارت فناوری اطلاعات و ارتباطات را برعهده گرفت.

علاوه براین، پلیس ملی در سال ۲۰۱۷ اعلام کرد تعداد نیروهای واحد جرائم سایبری را از ۴۰ نفر به ۱۰۰ نفر افزایش داده‌است[۱]. همزمان با آن، اندونزی دفاع سایبری را به‌عنوان بخشی از مفهوم کلی دفاع ملی در مقیاسی وسیعی توسعه داد[۲].

سازمان ملی رمزنگاری و سایبری در سال ۲۰۱۸ راهبرد ملی امنیت سایبری را منتشر کرد که مشتمل بر پنج هدف بود: تاب‌آوری سایبری، امنیت خدمات عمومی، اجرای قانون سایبری، فرهنگ امنیت سایبری و امنیت سایبری در اقتصاد دیجیتال[۳]. این راهبرد همسو با سیاست‌های ضدتروریسم اندونزی است و از دیگر اهداف موردتاکید آن می‌توان به ترویج مشارکت چندذینفعی و افزایش اعتماد جهانی به مدیریت اندونزی در فضای سایبری داخلی اشاره کرد. همانند بسیاری از کشورها انتشار راهبرد رسمی اندونزی زمینه را برای اقدامات وسیع‌تر دولت فراهم کرد. به‌عنوان مثال، پلیس ملی در همان سال ۲۰۱۸ اداره جرائم سایبری[۴] را برای مقابله با نشر اطلاعات غلط ازطریق رسانه‌های دیجیتال تاسیس کرد[۵].

---

۱. رجوع شود به:
Marguerite Afra Sapiie, 'Police Playing Tough in Combating Cybercrimes in Indonesia', Jakarta Post, 6 February 2017,
https://www.thejakartapost.com/news/2017/02/06/policeplaying-tough-in-combating-cybercrimes-in-indonesia-.html.

۲. رجوع شود به:
'Kemhan Dorong Pertahanan Nirmiliter Jadi Program Nasional', Antara, 8 May 2019,
https://www.antaranews.com/berita/860413/kemhan-dorong-pertahanan-nirmiliter-jadi-program-nasional.

۳. رجوع شود به:
Badan Siber Dan Sandi Negara, 'Indonesian Cyber Security Strategy',
https://bssn.go.id/strategi-keamanan-siber-nasional.

4. Cyber Crime Directorate

۵. رجوع شود به:
Cabinet Secretariat of the Republic of Indonesia, 'Cyber Crime Directorate Established to Combat Fake News', 4 October 2018,
https://setkab.go.id/en/cyber-crime-directorate-established-tocombat-fake-news.

سازمان ملی رمزنگاری و سایبری در دسامبر ۲۰۲۰ پیش‌نویس راهبرد ملی جدید امنیت سایبری را جهت استفاده از نظرات و پیشنهادهای عموم مردم منتشر ساخت[۱]. این راهبرد جدید ضمن توجه جدی‌تر به رخدادهای سایبری با اولویت ملی روی هفت حوزه خاص متمرکز شده‌است: مدیریت خطر در امنیت سایبری ملی، آمادگی و تاب‌آوری، زیرساخت‌های اطلاعاتی حیاتی، ظرفیت‌سازی، افزایش آگاهی، قانون‌گذاری و مقررات و همکاری‌های بین‌المللی. سایر اهداف آن عبارتند از: حفاظت از کشور در برابر هرگونه مداخله سایبری که می‌تواند به نظم عمومی آسیب برساند و ارتقای امنیت سایبری به‌منظور بهره‌برداری از ظرفیت‌های اقتصادی دیجیتال. به‌علاوه، پیش‌نویس راهبرد جدید براساس مقررات شماره ۷۱ مصوب سال ۲۰۱۹ درباره اجرای مبادلات و سیستم‌های الکترونیک[۲] تهیه شد که با قراردادن امنیت سایبری ذیل سیاست امنیت ملی اهمیت راهبرد امنیت سایبری را ارتقا بخشید.

باتوجه به روند کاهشی امنیت در اندونزی، یکی از اولویت‌های دولت همواره مقابله با تروریسم داخلی و افراط‌گرایی برخط و سرکوب مخالفت‌های سیاسی است. به‌عنوان مثال پس از اعتراضات گسترده در اکتبر ۲۰۲۰، پلیس با استناد به قوانین اطلاعات غلط توانست مجوز مقابله برخط با فعالان سیاسی[۳] و گروه‌های اسلامی مانند گروه هکری

۱. رجوع شود به:
Badan Siber Dan Sandi Negara, ‘Strategi Keamanan Siber Nasional’, 14 December 2020, https://cloud.bssn.go.id/s/qQZmyWaFf8ooc26/download.

۲. رجوع شود به:
Karis Kuniaran, ‘Ini Strategi BSSN Perkuat Keamanan Siber Nasional’, Merdeka, 14 December 2020, https://www.merdeka.com/ peristiwa/ini-strategi-bssn-perkuat-keamanan-siber-nasional.html.

۳. رجوع شود به:
Usman Hamid and Ary Hermawan, ‘Indonesia’s Shrinking Civic Space for Protests and Digital Activism’, Carnegie Endowment for International Peace, 17 November 2020, https://carnegieendowment.org/2020/11/17/indonesia-s-shrinkingcivic-space-for-protests-and -digital-activism-pub-83250.

«ارتش سایبری مسلمان»[1] -مروج عدم‌تحمل مذهبی در فضای سایبری- را دریافت کند[2]. در حال حاضر، در محافل سیاسی اندونزی مباحثی درباره میزان سانسور فضای سایبری توسط دولت مطرح است[3].

در مقایسه با بخش غیرنظامی می‌توان گفت سیاست‌های سایبری نظامی اندونزی از نظر موضوعات و تحلیل‌های مطرح‌شده شاهد پیشرفت‌های بیشتری بوده‌اند، البته در این بخش نیز هنوز نتایج ملموسی به‌دست نیامده‌است.

وزارت دفاع اندونزی (MoD)[4] در سال ۲۰۱۴ اصول راهنمای جامعی برای دفاع سایبری ملی تدوین کرد که نقطه تمرکز آن تامین امنیت دارایی‌های دفاعی در برابر حمله‌های سایبری بود[5] و توجه کمتری به تجهیزات جنگی مبتنی بر فناوری سایبری داشت. این اصول راهنما بر ضرورت توانمندی‌های ضدحمله جهت بازدارندگی تاکید داشتند، اما شامل مفهوم سایبری تهاجمی نمی‌شدند.

اندونزی در یکی از گزارش‌های دفاعی خود در سال ۲۰۱۵، دفاع سایبری را در کنار دفاع هوایی، حمله راهبردی و جنگ الکترونیک قرار داد و آن‌ها را چهار ستون دفاع ملی اندونزی نامید[6]. این سند امنیت سایبری را از اجزای تفکیک‌ناپذیر توانمندی‌های دفاع ملی توصیف

1. Muslim Cyber Army

۲. رجوع شود به:
Thomas Paterson, 'Indonesian cyberspace expansion: A double-edged sword', Journal of Cyber Policy, vol. 4, no. 2, 2019, pp. 216-34,
https://www.tandfonline.com/doi/pdf/10.1080/23738871.2019.1627476?needAccess=true.

۳. همان، ص. ۲۱۷.

4. Ministry of Defense

۵. رجوع شود به:
Peraturan Menteri Pertahanan Republik Indonesia, Nomor 82 tahun 2014 tentang, Pedoman Pertahanan Siber,
https://www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf.

۶. رجوع شود به:
Defense Ministry of the Republic of Indonesia, 'Defense White Paper 2015', November 2015, p. 109,
https://www.kemhan.go.id/wp-content/uploads/2016/05/2015-INDONESIADEFENCE-WHITE- PAPER-ENGLISH-VERSION.pdf.

می‌کند و بر اهمیت ادغام توانمندی‌های سایبری با سایر ابزارهای قدرت ملی تاکید دارد[۱] و خواستار تعهد دولت به مدرن‌سازی توانمندی‌های سایبری کشور است[۲].

وزارت دفاع در سال ۲۰۱۷ با همراهی سازمان ملی برنامه‌ریزی توسعه[۳] به ترویج مفهوم دفاع غیرنظامی پرداخت با این هدف که همه وزارت‌ها و نهادهای دولتی روش‌های دفاع غیرنظامی ازجمله در فضای سایبری را به‌کار گیرند[۴]. مقامات دفاعی اندونزی این ابتکار را همسو با مفهوم کلی دفاع کشور می‌دانستند که طبق آن، همه شهروندان مبارزانی بالقوه در همه عرصه‌های دفاعی ازجمله در فضای سایبری قلمداد می‌شوند.

افزون بر آن، نیروهای مسلح اندونزی در سال ۲۰۱۷ اولین اصلاحات نهادی را با راه‌اندازی واحدهای سایبری (مانند ساچوان سایبر یا سات‌سایبر[۵]) آغاز کردند که وظیفه تهیه مبنای نظری، سیاست‌ها، رویه‌ها و فنون مقابله با تهدیدهای سایبری را برعهده داشتند[۶]. ماموریت اصلی این واحدها تضمین امنیت سایبری زیرساخت‌های دفاعی حیاتی ملی است و همزمان برنامه بلندمدتی نیز برای توسعه توانمندی‌های سایبری در دست اجرا دارند[۷]. واحد سات‌سایبر علاوه بر وظایف فوق، مسئولیت پایش تحرکات نظامی خارجی (به‌ویژه واحدهای مجهز به موشک) در منطقه را نیز برعهده دارد. درمجموع،

۱. همان، ص. ۱۱۰.
۲. همان، ص. ۴۵.
3. National Development Planning Agency
۴. رجوع شود به:
'Kemhan Dorong Pertahanan Nirmiliter Jadi Program Nasional', Antara.
5. Satuan Siber or Satsiber
۶. رجوع شود به:
Satsiber, 'Sejarah',
https://satsiber-tni.mil.id/sejarah-20181230304.
۷. رجوع شود به:
Sri Hidayati and Rudi A.G. Gultom, 'Analisis Kebutuhan Senjata Siber Dalam Meningkatan Pertahanan Indonesia Di Era Peperangan Siber', Teknologi Persenjataan, vol. 1, no. 1, 2020, p. 90,
http://139.255.245.7/index.php/TPJ/article/viewFile/474/451.

تدوین راهبرد و مبنای نظری سایبری در اندونزی در مراحل آغازین است و هیچ مدرک مشخصی درباره این موضوع در اسناد غیردسته‌بندی‌شده کشور وجود ندارد.

حکمرانی، فرماندهی و نظارت

سازمان ملی رمزنگاری و سایبری نهاد اصلی امنیت سایبری اندونزی است و در چارچوب وزارت هماهنگی امور سیاسی، حقوقی و امنیتی[1] فعالیت می‌کند. این سازمان به‌طور مستقیم به رئیس‌جمهور پاسخگوست[2] و ریاست آن شامل چهار معاونت می‌شود که مسئولیت شناسایی و رهگیری تهدیدها، حفاظت، پاسخ و احیا و سیاست‌های فنی پایش و نظارت را برعهده دارند[3]. سازمان ملی رمزنگاری و سایبری اولین تیم پاسخ فوری رایانه‌ای دولت را در سال ۲۰۱۸ بر پایه تیم پاسخ فوری بخش خصوصی و تیم دولتی پاسخ رویداد-زیرساختی تشکیل داد[4].

از زمان تشکیل سات‌سایبر (۲۰۱۷) در نیروهای مسلح اندونزی (TNI)[5]، فرماندهی و نظارت سایبری از چارچوب سازمانی مشخصی در این کشور برخوردار شده‌است و مناسبات و اختیارات فرماندهی بین فرماندهی نیروهای مسلح اندونزی (برای

1. Coordinating Ministry for Political, Legal and Security Affairs

۲. رجوع شود به:

'Jokowi Strengthens Role of Cyber Agency', Tempo, 3 January 2018, https://en.tempo.co/read/914520/jokowi-strengthens-roleof-cyber-agency.

۳. رجوع شود به:

Badan Siber Dan Sandi Negara, 'Pimpinan Badan Siber Dan Sandi Negara', https://bssn.go.id/pejabat.

۴. رجوع شود به:

Mehda Basu and Yun Xuan Poon, 'Five steps in Indonesia's cyber battle plan: Interview with Lieutenant General (ret) Hinsa Siburian, Head of the National Cyber and Encryption Agency (BSSN), Indonesia', GovInsider, 17 September 2020, https://govinsider.asia/security/bssn-five-steps-in-indonesias-cyber-battle-plan.

5. Indonesian Army Forces (Tentara Nasional Indonesia)

عملیات‌های نظامی سات‌سایبر)[۱] و ریاست ستاد کل (برای مدیریت امور جاری) تقسیم شده‌است. سات‌سایبر در هر یک از سه نیروی ارتش دارای واحدهای سایبری است[۲]. مرکز دفاع سایبری[۳] مکمل کار سات‌سایبر[۴] است که تحت‌نظارت سازمان اطلاعات دفاعی[۵] وزارت دفاع قرار دارد[۶]. متاسفانه در بخش فرماندهی و نظارت سایبری اندونزی نیز از نظر تجهیزات عملیاتی ضعف‌هایی مشابه سامانه‌های مخابراتی نیروهای مسلح مشاهده می‌شود[۷].

وزارت امور خارجه اندونزی دارای مرکز فرماندهی دیجیتال[۸] مختص به خود است که وظیفه بهبود رویه‌های مدیریت بحران در فوریت‌های ملی سایبری و مدیریت دیپلماسی

۱. رجوع شود به منابع زیر:

TNI, 'Organizational Structure',
https://int.tni.mil.id/struktur.html.

Sekretariat Kabinet Republik Indonesia, 'Inilah Perpres No. 62 Tahun 2016 Tentang Susunan Organisasi Tentara Nasional Indonesia (1)', 19 January 2017,
https://setkab.go.id/inilah-perpres-no-62-tahun-2016-tentang-susunan-organisasitentara-nasional-indonesia-1.

۲. واحد سات‌سایبر در نیروی هوایی به‌طور رسمی در سپتامبر ۲۰۲۰ آغاز به کار کرد. رجوع شود به:
Achmad Nasrudin Yahya, 'Bentuk Peperangan Makin Tak Dapat Diprediksi, TNI AU Bentuk Satuan Siber', Kompas, 17 September 2020,
https://nasional.kompas.com/read/2020/09/17/07393261/bentukpeperangan-makin-tak-dapat-diprediksi-tni-au-bentuksatuan-siber.

3. Cyber Defense Center

۴. رجوع شود به:

Pushansiber. See Kementerian Pertahanan Republik Indonesia, 'Kapushansiber',
https://www.kemhan.go.id/bainstrahan/kapushansiber.

5. Defense Intelligence Agency

۶. رجوع شود به:

Kementerian Pertahanan Republik Indonesia, 'Badan Instalasi Strategis Pertahanan',
https://www.kemhan.go.id/bainstrahan.

۷. رجوع شود به:
Alex Firmansiyah Rahman, Syaiful Anwar and Arwin Datumaya Wahyudi Sumari, 'Analisis Minimum Essential Force (MEF) Dalam Rangka Pembangunan Cyber-Defense', Jurnal Pertahanan & Bela Negara, vol. 5, no. 3, 2018, pp. 63-85,
http://jurnal.idu.ac.id/index.php/JPBH/article/view/370.

8. Digital Command Center

بین‌المللی اندونزی در امور سایبری را برعهده دارد. ترکیب چنین کارکردهای متفاوتی در نهادی واحد امری غیرمعمول است، زیرا مدیریت بحران در رویدادهای سایبری مستلزم برخورداری از مهارت‌هایی بسیار متفاوت با مهارت‌های موردنیاز در دیپلماسی سایبری است و فعالیت‌های این دو حوزه هم‌پوشانی چندانی ندارند.

روی‌هم‌رفته، اندونزی نیازمند تغییر مبنای نظری و برنامه‌ریزی در زمینه نیروی کار و فناوری برای دستیابی به توانمندی‌های ابتدایی جنگ سایبری است و به‌دلیل وجود شکاف نظری بین سیاست‌گذاران و مجریان طرح‌های توسعه دفاع سایبری این کشور مسلما ایجاد همسویی و هماهنگی بین این ذینفعان برای توسعه همه‌جانبه بخش دفاع سایبری آن ضروری است.

توانمندی‌های محوری در زمینه اطلاعات سایبری

سازمان ملی رمزنگاری و سایبری به‌عنوان نهاد محوری هماهنگ‌کننده در زمینه توانمندی‌های سایبری بخش غیرنظامی ملی اندونزی نیز محسوب می‌شود[1]. به‌همین‌ترتیب، سازمان اطلاعات راهبردی (BAIS)[2] نهاد اصلی در حوزه اطلاعات نظامی و خارجی به‌شمار می‌رود که مکمل خوبی برای نیروهای پلیس نیز تلقی می‌شود. به‌عنوان مثال، سازمان اطلاعات راهبردی در انتخابات منطقه‌ای در سال ۲۰۱۸ در زمینه رصد سایبری تهدیدهای احتمالی کمک‌های شایانی به پلیس کرد.

در سال ۲۰۲۰ بودجه‌ای معادل ۲/۲ تریلیون روپیه اندونزی (۱۲۷ میلیون دلار) به سازمان ملی رمزنگاری و سایبری تعلق گرفت. البته طبق اظهارات ریاست آن، این سازمان برای

۱. رجوع شود به:
Margareth S. Aritonang, 'Police to Support National Cyber Agency', Jakarta Post, 4 January 2017, https://www.thejakartapost.com/news/2017/01/04/police-to-supportnational-cyber-agency.html.
2. Strategic Intelligence Agency (Badan Intelijen Strategis)

تحقق اهداف خود نیازمند بودجه‌ای برابر با ۳ تریلیون روپیه (۱۹۰ میلیون دلار) است[۱]. توسعه فناوری‌های بومی، تقویت مرکز ملی عملیات‌های امنیت سایبری[۲] (مسئول رصد شبکه‌های دیجیتال زیرساخت‌های ملی حیاتی اندونزی شامل انرژی، مخابرات و حمل‌ونقل) و استخدام فارغ‌التحصیلان واجدشرایط ازجمله اهداف موردنظر ریاست سازمان ملی رمزنگاری و سایبری به شمار می‌آیند[۳]. در اینجا ذکر این نکته ضروری است که توانمندی‌های اندونزی در زمینه اطلاعات سایبری توسعه‌یافته نیست و بنابراین افزایش دسترسی اطلاعاتی کشور فراتر از تروریسم داخلی نیازمند سرمایه‌گذاری بسیار بیشتری است.

توانمندی و وابستگی سایبری

اندونزی تا سال ۲۰۲۰ توانست خود را در زمره یکی از قدرت‌های دیجیتال نوظهور گروه ۲۰ قرار دهد. البته هنوز سطح این کشور از بسیاری از اعضا پایین‌تر است و تا رسیدن به اهداف موردنظر خود راهی طولانی پیش‌رو دارد[۴]. دولت برنامه‌های آموزشی گسترده‌ای را آغاز کرده‌است و قصد دارد ازطریق سیاست‌های مهاجرتی خود استعدادهای بین‌المللی را به کشور جذب کند و در پی ترویج فرهنگ راه‌اندازی شرکت‌های نوپا در کشور است[۵]. اقتصاد دیجیتال اندونزی طبق پیش‌بینی‌ها باید به رشد سالانه دو رقمی

۱. رجوع شود به:
'DPR "Ngotot" Perjuangkan Dana Rp20 Triliun Untuk BSSN', CNN Indonesia, 13 November 2019, https://www.cnnindonesia.com/teknologi/20191113191757-185-448102/dpr-ngotot-perjuangkan-dana-rp20-triliun-untuk-bssn
2. National Cyber Security Operations Center
۳. همان.
۴. رجوع شود به:
European Center for Digital Competitiveness, 'Digital Riser Report 2020', September 2020, https://digital-competitiveness.eu/wp-content/uploads/ESCP_Digital-Riser-Report_2020-1.pdf.
۵. همان، ص. ۷.

(۱۱ درصد) تا سال ۲۰۲۰ دست می‌یافت[۱]. به‌طور کلی، در آینده تجارت الکترونیک پیشران اصلی اقتصاد اندونزی خواهد بود. سه مورد از شرکت‌های نوپای اندونزی (گوجِک، توکوپدیا و تراوِلوکا)[۲] موفق به جذب سرمایه‌های هنگفتی شده‌اند (به‌ترتیب ۱۰/۵، ۷/۵ و ۲/۷۵ میلیارد دلار) که بیشتر ازطریق توسعه تجارت بین‌المللی حاصل شده‌است[۳]. دولت سودای تبدیل شدن به قطب تامین مالی اسلامی را نیز در سر دارد، هر چند هنوز در جایگاه چهارم این صنعت (پس از مالزی، عربستان سعودی و امارات متحده عربی) ایستاده‌است[۴] و تحقق این هدف مستلزم توسعه گسترده صنعت مالی و امنیت سایبری اندونزی است.

اگرچه نرخ کلی نفوذ اینترنت در اندونزی بالاست (۷۳ درصد جمعیت در نیمه سال ۲۰۲۰)[۵]، اما شکاف بزرگی بین منطقه جاوا[۶] و سایر جزایر کشور از نظر دسترسی به اینترنت

---

۱. رجوع شود به:
'e-Conomy SEA 2020 - At full velocity: Resilient and racing ahead', Google, Temasek, Bain & Company, November 2020, p. 32,
https://www.thinkwithgoogle.com/_qs/documents/10614/e-Conomy_SEA_2020_At_full_velocity__Resilient_and_racing_ahead_bMmKO5b.pdf.

2. Gojek, Tokopedia and Traveloka

۳. به‌منظور کسب اطلاعات بیشتر درباره ارزش شرکت‌های گوجک و توکوپدیا رجوع شود به:
'Indonesia's Gojek Mulls $18 Billion Merger With Tokopedia', PYMTS.com, 5 January 2021,
https://www.pymnts.com/news/partnershipsacquisitions/2021/indonesias-gojek-mulls-18-billion-mergerwith-tokopedia.
و به‌منظور کسب اطلاعات بیشتر درباره ارزش شرکت تراولوکا رجوع شود به:
Yoolim Lee, 'Traveloka Nears Fundraising at Lower Valuation', Bloomberg Quint, 10 July 2020,
https://www.bloombergquint.com/business/traveloka-is-said-near-fundraising-at-sharply-lowervaluation.

۴. رجوع شود به:
Fauziah Rizki Yuniarti, 'Indonesia could be Asia's next Islamic finance hub', Jakarta Post, 12 January 2021,
https://www.thejakartapost.com/academia/2021/01/12/indonesia-could-beasias-next-islamic-finance-hub.html.

۵. رجوع شود به:
Eisya A. Eloksari, 'Indonesian internet users hit 196 million, still concentrated in Java: APJII survey', Jakarta Post, 11 November 2020,
https://www.thejakartapost.com/news/2020/11/11/indonesian-internet-users-hit-196-million-still-concentratedin-java-apjii-survey.

6. Java

وجـود دارد[۱]. بـا این حال، نرخ نفوذ اینترنت در برخی از شـهرها مانند جاکارتا[۲] (۸۵ درصد)، سورابایـا[۳] (۸۳ درصـد) و باندونـگ[۴] (۸۲/۵ درصـد)[۵] نسـبتا بالاسـت. ۹۰ درصـد کاربـران در اندونزی ازطریق تلفن همراه به اینترنت دسترسی دارند.

رتبه اندونزی در شاخص جهانی نوآوری (۲۰۲۰) ۸۵ است که نشان از بنیان‌های ضعیف اقتصاد دیجیتال در این کشـور دارد[۶]. درواقع، اقتصاد دیجیتال در سـال ۲۰۲۰ تنها سـهمی ۱۲ درصدی از تولید ناخالص داخلی این کشور را دربرداشت[۷] که البته دولت امیدوار است تا سـال ۲۰۲۵ این رقم را به ۱۵ درصد افزایش دهد[۸]. متاسـفانه میانگین سطح مهارت‌های دیجیتـال جمعیت متناسـب با اهداف دولت اندونزی نیسـت[۹]. طبـق نتایج تحقیقاتی که

۱. همان.

2. Jakarta
3. Surabaya
4. Bandung

۵. رجوع شود به:
'Indonesian Internet Users Reach 200 Million Until 2Q of 2020', The Insider Stories, 10 November 2020, https:// theinsiderstories.com/indonesian-internet-users-reach-200- million-until-2q-of-2020.

۶. رجوع شود به:
'Global Innovation Index 2020: Who Will Finance Innovation?', SC Johnson College of Business - Cornell University, INSEAD and WIPO, September 2020, p. 17, https://www. globalinnovationindex.org/Home.

۷. رجوع شود به:
Vience Mutiara Rumata and Ashwin Sasongko Sastrosubroto, 'The Paradox of Indonesian Digital Economy Development', IntechOpen, 27 May 2020, https://www.intechopen.com/online-first/the-paradox-of-indonesiandigital-economy- development.

۸. رجوع شود به:
'Incar Jawara Dunia, Inilah Strategi RI Dalam Ekonomi Digital', Kementerian Komunikasi dan Informatika Republik Indonesia, November 2018, http:///content/detail/15306/incarjawara-dunia-inilah-strategi-ri-dalam-ekonomi-digital/0/sorotan_media.

۹. رجوع شود به:
Trisha Ray et al., 'The Digital Indo-Pacific: Regional Connectivity and Resilience', Quad Tech Network, ANU, CNAS, GRIPS, ORF, February 2021, p. 17, https://crawford.anu.edu.au/sites/default/files/publication/nsc_crawford_anu_edu_au/2021-02/thedigitalindopacific.pdf.

به سفارش شرکت خدمات وب آمازون[1] در شش کشور منطقه آسیا-اقیانوسیه انجام شده‌است، تنها ۱۹ درصد از پاسخ‌دهنده‌های اندونزیایی از مهارت‌های دیجیتال در شغل خود استفاده می‌کنند که دال بر فاصله زیاد اندونزی با کشورهایی مانند سنگاپور (۶۳ درصد) و استرالیا (۶۴ درصد) است[2]. این کمبود مهارت توسعه صنعت دیجیتال داخلی را با مشکلات جدی روبرو می‌کند. درحقیقت، اختلافات شرکت هوآوی و اندونزی در سال ۲۰۱۹ پرده از وابستگی زیاد آن به کشورهای خارجی در تامین زیرساخت‌های مخابراتی برداشت. یکی از مقامات ارشد وزارت هماهنگی امور سیاسی، حقوقی و امنیتی در این زمینه اظهار داشت برخورداری از سیستم مخابرات ایمن، قابل‌اعتماد، یکپارچه و اختصاصی در برابر تهدیدهای سایبری داخلی و خارجی ضروری است و باید این واقعیت را پذیرفت که سیستم کنونی قادر به پاسخ‌گویی به نیازهای امنیت اطلاعات ملی نیست[3].

اگرچه اندونزی در تحقیقات هوش مصنوعی روبه‌رشد است، ولی همچنان در این عرصه تازه‌وارد محسوب می‌شود. اندونزی اقداماتی درجهت افزایش همکاری بین دانشگاه و صنعت در زمینه تحقیقات هوش مصنوعی انجام داده‌است. به‌عنوان مثال، همکاری‌هایی بین دانشگاه اندونزی[4] و شرکت توکوپدیا[5] و موسسه فناوری باندونگ[6]

1. Amazon Web Services

۲. رجوع شود به:
Eileen Yu, 'Cloud, Data amongst APAC Digital Skills Most Needed', ZDNet, 25 February 2021, https://www.zdnet.com/ article/cloud-data-amongst-apac-digital-skills-most-needed/.

۳. رجوع شود به:
Coordinating Ministry for Political, Legal and Security Affairs, 'Tingkatkan Keamanan Informasi Nasional, Deputi VII Kominfotur Laksanakan FGD Merevival Kedaulatan Telekomunikasi', 27 June 2019, https://polkam.go.id/tingkatkan-keamanan-informasi-nasional-deputi-viikominfotur-laksanakan.

4. University of Indonesia

۵. رجوع شود به:
'UI Gandeng Tokopedia Bangun Pusat Penelitian Kecerdasan Buatan, Menristekdikti Harapkan Lulusan Indonesia Penuhi Kebutuhan SDM Perusahaan Startup', Ristek-Brin, 28 March 2019, https://www.ristekbrin.go.id/ui-gandeng-tokopedia-bangun-pusat-penelitian-kecerdasanbuatan-menristekdikti-harapkan-lulusan-indonesia-penuhikebutuhan-sdm-perusahaan-startup.

6. Bandung Institute of Technology

و شرکت بوکالاپاک[1] شکل گرفته‌است[2]. با این همه، میزان سرمایه‌گذاری شرکت‌های اندونزی در راه‌حل‌های هوش مصنوعی بسیار پایین‌تر (سرانه ۰/۲۰ دلار) از اقتصادهای توسعه‌یافته‌ای مانند سنگاپور (سرانه ۶۸ دلار) است[3]. گزارش‌های ارائه شده در سال ۲۰۲۰ نشان می‌دهند که ۷۴ شرکت نوپا در زمینه هوش مصنوعی در اندونزی فعالیت دارند[4] و در همین سال، دولت راهبرد ملی هوش مصنوعی[5] را با هدف توسعه گسترده هوش مصنوعی تا سال ۲۰۴۵ آغاز کرده‌است[6]. طبق پیش‌بینی‌ها، این راهبرد بر به‌کارگیری این فناوری در حوزه‌های خدمات اجتماعی، آموزش و پژوهش، سلامت، امنیت غذایی، جابه‌جایی، شهرهای هوشمند و اصلاحات بخش عمومی تمرکز خواهد داشت[7].

به‌نظر می‌رسد چین اشتیاق بسیاری برای مشارکت گسترده در توسعه اقتصاد دیجیتال اندونزی دارد. پس از آنکه هند در اوایل سال ۲۰۲۰ قوانین محدودکننده مالکیت چینی‌ها را اجرا کرد، شرکت‌های سرمایه‌گذاری خطرپذیر و سرمایه‌گذاران فناوری چین فعالیت‌های خود را به اندونزی منتقل کردند، به‌طوری‌که ۵۵ درصد از هجوم سرمایه به

1. Bukalapak

۲. رجوع شود به:
Arya Dipa, 'Bukalapak, ITB Launch AI, Cloud Computing Innovation Center', Jakarta Post, 2 February 2019, https://www.thejakartapost.com/news/2019/02/02/bukalapak-itb-launch-aicloud-computing- innovation-center.html.

۳. رجوع شود به:
Dylan Loh, 'ASEAN Faces Wide AI Gap as Vietnam and Philippines Lag Behind', Nikkei Asia, 9 October 2020, https://asia.nikkei.com/Business/Technology/ASEAN-faces-wide-AIgap-as-Vietnam-and-Philippines-lag-behind2.

۴. رجوع شود به:
Hugh Harsono, 'Why Indonesia Is Poised to Become the Next AI Start-up Hub', South China Morning Post, 25 August 2020,
https://www.scmp.com/tech/article/3098596/why-indonesia-poised-become-next-ai-start-hub.

5. National Strategy for Artificial Intelligence

۶. رجوع شود به:
Indonesia National Secretariat of Artificial Intelligence, 'Indonesia National Strategy for Artificial Intelligence', 10 August 2020,
https://ai-innovation.id/strategi.

۷. همان.

بخش فناوری این کشور را در نیمه اول سال ۲۰۲۰ به خود اختصاص دادند[۱]. شرکت هوآوی با بسیاری از نهادهای دولتی اندونزی ارتباطاتی برقرار کرده‌است تا به‌عنوان مثال ازطریق فراهم‌کردن زیرساخت‌های ابری برای ذخیره داده‌های دولتی بتواند روند دیجیتال‌سازی آن‌ها را شتاب بخشد[۲]. شرکت هوآوی علاوه بر تامین فناوری، متعهد به ارتقای استعدادهای دیجیتال و آموزش مهارت‌های امنیت سایبری اندونزی نیز شده‌است[۳]. چین و اندونزی در ژانویه سال ۲۰۲۱ تفاهم‌نامه‌ای درباره همکاری و سرمایه‌گذاری در بخش فناوری اطلاعات و ارتباطات امضا کردند که تمرکز اصلی آن موضوع امنیت بود[۴]. شرکت‌های چینی بخش بزرگی از بازار اندونزی را در اختیار دارند و در عین حال با رقابت شرکت‌های باسابقه آمریکایی، ژاپنی و اروپایی نیز مواجه هستند. به‌عنوان مثال، شرکت مایکروسافت در آغاز سال ۲۰۲۱ اعلام کرد به سه میلیون اندونزیایی آموزش مهارت‌های دیجیتال ارائه خواهد کرد. این ابتکار مایکروسافت در راستای تداوم اقدامات آن طی ۲۵ سال گذشته است و با همکاری وزارت فناوری اطلاعات و ارتباطات و چهار دانشگاه

۱. رجوع شود به:
Mercedes Ruehl, 'China's Tech Investors Turn from India to Indonesia', Financial Times, 29 November 2020,
https://www.ft.com/content/bcc935fd-ef40-4d6d-9939-ea18498e0283.

۲. رجوع شود به:
'Cybersecurity Becomes BSSN's Challenge in the Digitalization of Indonesia', Waktunya Merevolusi Pemberitaan, 28 August 2020,
https://voi.id/en/technology/12457/cybersecurity-becomesbssns-challenge-in-the-digitalization-of-indonesia.

۳. طبق منابع موجود، آکادمی هوآوی آسه‌آن (Huawei ASEAN Academy) متشکل از چندین دانشکده مهندسی‌فنی و کسب‌وکار است که با بیش از ۱۰۰ مربی، ۳۰۰۰ دوره آموزشی و بیش از ۱۰۰ محیط آینه‌ای (مشابه‌های برابر با اصل از شبکه‌ها) به فعالیت آموزشی می‌پردازد.

۴. رجوع شود به:
Chris Devonshire-Ellis, 'Investment Infrastructure Projects in Indonesia Contributing to Improved Manufacturing Capability', ASEAN Briefing, 4 February 2021,
https://www.aseanbriefing.com/news/investment-infrastructure-projects-in-indonesiacontributing-to-improved-manufacturing-capability

اندونـزی در راسـتای آمـوزش هـوش مصنوعـی، امنیـت سـایبری و علـوم داده ازطریـق برنامه‌های آموزشی سواد دیجیتال اجرا می‌شود[۱].

امنیت و تاب‌آوری سایبری

دیدگاه اندونزی نسبت به امنیت سایبری بسیار متاثر از افشاگری ادوارد اسنودن در سال ۲۰۱۳ است که درنتیجه آن توان سایبری استرالیا و نیز اقدامات جاسوسی آن علیه رهبران اندونزی افشا شد. باآنکه سازمان‌های امنیتی اندونزی پیش از این واقعه نیز تا حدی از فعالیت‌های جاسوسی استرالیا مطلع بودند، اما جامعه این کشور به‌شدت از اطلاعات افشاشده حیرت‌زده شد. دولت اندونزی در پاسخ به این رویداد در سال ۲۰۱۶ به دبیرکل شورای ملی تاب‌آوری[۲] ماموریت داد تا ضمن تهیه برنامه‌ای برای واکنش به پیشامدهای غیرمترقبه در حمله‌های سایبری[۳]، رزمایش‌های اضطراری همانند تمرینی که تیم ملی پاسخ فوری رایانه‌ای کشور پیش از برگزاری بازی‌های آسیایی ۲۰۱۸ جاکاراتا انجام داد را نیز اجرا کند[۴]. در حال حاضر، دارایی‌های دارای بیشترین اولویت که مستلزم بالاترین سطح حفاظت هستند به‌مدد متخصصان اندونزی شناسایی شده‌اند که از آن جمله می‌توان به شبکه‌های مخابراتی و بانکی، سامانه‌های پرداخت

۱. رجوع شود به:
'Microsoft to Establish First Datacenter Region in Indonesia as Part of Berdayakan Ekonomi Digital Indonesia Initiative', Microsoft Stories Asia, 25 February 2021, https://news.microsoft.com/apac/2021/02/25/microsoft-to-establish-firstdatacenter-region-in-indonesia-as-part-of-berdayakan-digitaleconomy-indonesia-initiative/

2. National Resilience Council

۳. رجوع شود به:
Arif Rahman and Oktarina Paramitha Sandy, 'Ini Urgensi UU Keamanan dan Ketahanan Siber' [interview with Colonel Arwin Datumaya Wahyudi Sumari], Cyberthreat.id, 26 April 2019, https://cyberthreat.id/read/305/Ini-Urgensi-UU-Keamanandan-Ketahanan-Siber.

۴. رجوع شود به:
Asia Pacific Computer Emergency Response Team, 'APCERT Annual Report 2018', p. 125, http://www.apcert.org/ documents/pdf/APCERT_Annual_Report_2018.pdf.

برخط، شبکه‌های بسته دولتی/نظامی و بخش خصوصی و مراکز داده اشاره کرد[1]. بااین حال، اندونزی هنوز از توانمندی‌های اولیه در دفاع سایبری و پاسخ به رویدادهای سایبری برخوردار نیست.

تعداد حمله‌های سایبری به اندونزی بین ژانویه و اکتبر سال ۲۰۲۰ تا شش برابر افزایش یافت که هدف بیشتر آن‌ها شرکت‌های تجارت الکترونیک بود. به‌عنوان مثال، اطلاعات ۹۱ میلیون نفر از کاربران شرکت توکوپدیا طی حمله به آن افشا گشت و طبق اعلام رسمی شرکت بینِکا[2] نیز داده‌های حدود ۱/۲ میلیون نفر از کاربران آن هک شد[3]. مطالعه پیماشی شرکت شبکه پالو آلتو حاکی از آن است که ۸۴ درصد از شرکت‌های اندونزیایی قصد دارند بودجه فناوری اطلاعات خود را افزایش دهند که از آن میان ۴۴ درصد شرکت‌ها قصد دارند نیمی از این بودجه را در زمینه امنیت سایبری سرمایه‌گذاری کنند[4].

دولت اندونزی علاوه بر این‌که پیش‌نویس راهبرد جدید امنیت سایبری را در سال ۲۰۲۰ به نظرسنجی عمومی گذاشت، مجموعه اصلاحات دیگری را نیز در دست اجرا دارد. سازمان ملی رمزنگاری و سایبری در فوریه ۲۰۲۱ تیم پاسخ رویداد امنیت سایبری ملی (CSIRT)[5] را تشکیل داد که مسئولیت امور دولتی و ملی را همزمان برعهده خواهد

۱. رجوع شود به:
Achmad Rouzni Noor, 'Strategi Indonesia Menjaga Kedaulatan Cyber', detikinet, 1 February 2016, https://inet.detik.com/cyberlife/d-3131768/strategi-indonesia-menjaga-kedaulatancyber.

2. Bihnneka

۳. رجوع شود به:
'Covid-19 and Cyberattacks: Which Emerging Markets and Sectors Are Most at Risk?', Oxford Business Group, 17 February 2021,
https://oxfordbusinessgroup.com/news/covid-19-and-cyberattacks-which-emerging-markets-and-sectors-aremost-risk.

۴. رجوع شود به:
Eisya A. Eloksari, 'Indonesian Businesses Ramp up Cybersecurity Budget amid Rampant Attacks', Jakarta Post, 23 July 2020,
https://www.thejakartapost.com/news/2020/07/22/indonesian-businesses-ramp-up-cybersecurity-budget-amidrampant-attacks.html.

5. Computer Security Incident Response Team

داشت[۱]. لازم به ذکر است پیش از این نیز در سال ۲۰۲۰[۲] دولت ۱۵ تیم در سطح پایین‌تری تشکیل داده‌بود[۳] که علاوه بر آن‌ها، دولت قصد دارد ۲۷ تیم دیگر هم در سطح وزارت‌ها و سایر نهادهای بخش دولتی راه‌اندازی کند[۴]. سازمان ملی رمزنگاری و سایبری در سال ۲۰۲۰ در چندین رزمایش سایبری حضور فعال داشت[۵] و در ابتدای سال ۲۰۲۱ نیز در رویداد آموزشی آزمایش امنیت سایبری اینترنت اشیا شرکت کرد که به‌طور مشترک به وسیله سفارت ایالات متحده و دانشگاه کارنگی ملون[۶] برگزار شد[۷]. سازمان ملی رمزنگاری و

۱. رجوع شود به:
'Kepala BSSN Resmikan Tim Tanggap Insiden Keamanan Siber (BSSN-CSIRT) Demi Tercipta Ruang Siber Yang Aman Dan Kondusif', Badan Siber Dan Sandi Negara, 25 February 2021,
https://bssn.go.id/kepala-bssn-resmikan-tim-tanggap-insidenkeamanan-siber-bssn-csirt-demi-tercipta-ruang-siber-yangaman-dan-kondusif/.

۲. سازمان ملی رمزنگاری و سایبری در فوریه سال ۲۰۲۰ تیم‌های دیگری نیز در سایر نهادها مانند وزارت تامین مالی و وزارت آموزش و فرهنگ و استان‌های جاوای مرکزی، جاوای شرقی، جاوای غربی، گورونتالو (Gorontalo)، جاکارتا، جزایر ریائو (Riau) و سوماترای (Sumatra) غربی تشکیل داد. برای دریافت اطلاعات بیشتر رجوع شود به:
'BSSN Gandeng Pemprov DKI Jakarta Bentuk Tim Tanggap Insiden Keamanan Siber', Badan Siber Dan Sandi Negara, 23 December 2020,
https://bssn.go.id/bssn-gandeng-pemprovdki-jakarta-bentuk-tim-tanggap-insiden-keamanan-siber;

'Resmikan Jogjaprov CSIRT, BSSN Harap Bisa Tekan Ancaman Siber di Yogyakarta', KOMPAS.com, 15 October 2020,
https://biz.kompas.com/read/2020/10/15/133036728/resmikan-jogjaprovcsirt-bssn-harap-bisa- te-kan-ancaman-siber-di-yogyakarta.

۳. رجوع شود به:
'Resmi Dibentuk, Kemenkeu-CSIRT Menutup Program Prioritas Strategis BSSN Di Tahun 2020', Badan Siber Dan Sandi Negara, 29 December 2020,
https://bssn.go.id/resmi-dibentukkemenkeu-csirt-menutup-program-prioritas-strategis-bssn-ditahun-2020.

۴. همان.

۵. این مانورها عبارتند از: مانور تمرین سایبری اتحادیه بین‌المللی مخابرات ۲۰۲۰، مانور رویداد پاسخ فوری رایانه‌ای آسه‌آن ۲۰۲۰، مانور رویداد پاسخ فوری رایانه‌ای سازمان همکاری اسلامی ۲۰۲۰، مانور سایبری آسه‌آن-ژاپن ۲۰۲۰ و مانور تیم پاسخ فوری رایانه‌ای آسیا-اقیانوسیه ۲۰۲۰. برای دریافت اطلاعات بیشتر رجوع شود به:
Id-SIRTII/CC, 'Activity'. 2020,
https://idsirtii.or.id/en/activity/year/2020.html.

6. Carnegie Mellon University

۷. رجوع شود به:
'APCERT Training: Implementing IoT Security Testing', ID-SIRTII/CC, 23 February 2021,
https://idsirtii.or.id/en/activity/detail_year/2021/92/apcert-training-implementingiot-security -testing.html;
'Carnegie Mellon University: Unhide Hidden Cobra', ID-SIRTII/CC, 15 February 2021,
https://idsirtii.or.id/en/activity/detail_year/2021/94/carnegiemellon-university-unhide-hidden-cobra.html.

سایبری با همراهی چندین نهاد دولتی در حال تهیه پیش‌نویس مقررات ریاست‌جمهوری درباره حفاظت از زیرساخت‌های اطلاعاتی حیاتی[1] است که مشتمل بر اقدامات و نهادهای ذی‌ربط در حفاظت از زیرساخت‌های اطلاعاتی حیاتی، افزایش آمادگی سایبری و شتاب‌بخشی به فرایند ترمیم و احیا پس از رویدادهای سایبری می‌شود[2]. سازمان ملی رمزنگاری و سایبری همه مالکان و ذینفعان را در این فرآیند مشارکت داده‌است تا در جریان سیاست‌ها و مقررات کشور در زمینه زیرساخت‌های اطلاعاتی حیاتی قرار گیرند[3].

علی‌رغم ادعاهای بلندپروازانه مقامات اندونزی، این کشور همچنان از کمبود مهارت سایبری رنج می‌برد. طبق مطالعه‌ای که دانشگاه آکسفورد در سال ۲۰۱۶ انجام داد، اندونزی فاقد حداقل برنامه‌های آموزشی در زمینه امنیت سایبری، نظام ارزیابی/تایید آموزش امنیت سایبری و نیز بودجه‌ای ملی برای حمایت از برنامه‌های ظرفیت‌سازی امنیت سایبری است. این مطالعه همچنین نشان می‌دهد که اندونزی تنها تعداد محدودی مربیان حرفه‌ای در حوزه امنیت سایبری در اختیار دارد و انتقال دانش از کارکنان آموزش‌دیده امنیت سایبری در بخش خصوصی صرفا به‌صورت مقطعی انجام می‌شود[4]. در سال ۲۰۲۰، رئیس سازمان ملی رمزنگاری و سایبری طی اظهاراتی درباره کمبود ملی مهارت اعلام کرد این سازمان اغلب برای یافتن شخص مناسب جهت یک جایگاه

1. Presidential Regulations on Vital Information Infrastructure Protection

۲. رجوع شود به:
'BSSN Beserta 13 Lembaga Pemerintah Formulasikan Rancangan Perpres Perlindungan Infrastruktur Informasi Vital', Badan Siber Dan Sandi Negara, 10 February 2021, https://bssn.go.id/bssn-beserta-13-lembaga-pemerintahformulasikan-rancangan-perpres-perlindunganinfrastrukturinformasi-vital

۳. رجوع شود به:
'BSSN Gelar Diseminasi Peraturan dan Kebijakan Sektor Infrastruktur Informasi Kritikal Nasional (IIKN)', Badan Siber Dan Sandi Negara, 10 February 2021, https://bssn.go.id/bssn-gelar-diseminasi-peraturan-dan-kebijakan-sektorinfrastruktur-informasi-kritikal-nasional-iikn

۴. رجوع شود به:
Nugraha, 'The future of cyber security capacity in Indonesia', pp. 12, 55.

شغلی در حوزه امنیت سایبری حدود شش ماه زمان صرف می‌کند[۱]. درواقع با توجه به حجم موقعیت‌های شغلی حساسی که نیازمند متخصصان سایبری هستند، دو دهه یا بیشتر طول خواهد کشید تا اندونزی بتواند به توانمندی‌های سایبری مستقل در زمینه دفاع سایبری نظامی دست یابد.

با توجه به ماهیت جزیره‌ای کشور اندونزی، امنیت سایبری دریایی برای این کشور اهمیت ویژه‌ای دارد و ازاین‌رو، سازمان ملی رمزنگاری و سایبری در حال توسعه ظرفیت‌های امنیت سایبری در مرکز اطلاعات دریایی[۲] است[۳]. نیروی دریایی اندونزی از سال ۲۰۱۶ آموزش دفاع سایبری را آغاز کرده‌است. در همین راستا، نیروی دریایی اندونزی در سال ۲۰۱۸ رزمایشی هشت‌روزه برگزار کرد[۴] که شامل بیش از ۵۰۰ نفر نیرو و سه سطح عملیاتی بود: حمله بندآوری خدمات[۵]، اقدامات ضدحمله و حمایت سایبری از عملیات‌ها[۶]. نیروی دریایی اندونزی در سال ۲۰۱۹ بخش سایبری را نیز به رزمایش بزرگ سالانه خود-آرمادا جایا[۷]-افزود.

---

۱. رجوع شود به متن مصاحبه زیر:
Basu and Yun, 'Five steps in Indonesia's cyber battle plan: Interview with Lieutenant General (ret) Hinsa Siburian, Head of the National Cyber and Encryption Agency (BSSN), Indonesia'.

2. Maritime Information Center

۳. رجوع شود به:
'BSSN Menerima Kunjungan Bakamla Dalam Rangka Kerjasama Keamanan Informasi', Badan Siber Dan Sandi Negara, 4 February 2021,
https://bssn.go.id/bssn-menerimakunjungan-bakamla-dalam-rangka-kerjasama-keamananinformasi

۴. رجوع شود به:
TNI, 'TNI AL Tingkatkan Kemampuan Pertahanan Siber', 6 November 2018,
https://tni.mil.id/view-140439-tni-altingkatkan-kemampuan-pertahanan-siber.html

۵. بندآوری (denial) نوعی حمله سایبری است که موجب کندی یا اخلال در روند ارائه خدمات توسط سامانه‌های برخط می‌شود.

۶. رجوع شود به:
Satsiber, 'Gubernor Aaal Hadiri Latihan Operasi Pertahanan Siber TNI AL 2018', 12 December 2018,
https://satsiber-tni.mil.id/gubernur-aal-hadiri-latihan-operasi-pertahanan-sibertni-al-2018-20181212674

7. Armada Jaya

اندونـزی در شـاخص جهانی امنیت سـایبری اتحادیه بین‌المللی مخابـرات (۲۰۱۸) رتبه چهل‌ویکم را در بین ۱۷۵ کشور کسب کرده‌است که در مقایسه با اندازه اقتصاد و اهداف آتی آن جایگاه چندان مناسبی به نظر نمی‌رسد[۱].

رهبری جهانی در عرصه سایبری

دولت اندونزی تقریبا از سال ۲۰۰۵ در قالب سازمان آسه‌آن، اجلاس منطقه‌ای آسه‌آن، اَپک، سازمان همکاری اسلامی و سازمان ملل در زمینه جنبه‌های مختلف مبارزه با جرائم سایبری به‌ویژه تروریسـم سـایبری و همچنین ایجاد چارچوب‌های حکمرانی بین‌المللی جهت ترویج ثبات راهبردی در فضای سایبری ازطریق بحث و بررسی هنجارهای سایبری فعالیت می‌کند.

کارشناسان اندونزیایی که اولین تیم پاسخ فوری رایانه‌ای این کشور را بنیان گذاشتند با همکاری همتایان ژاپنی و استرالیایی تیم پاسخ فوری رایانه‌ای آسیا-اقیانوسیه (APCERT)[۲] را در سال ۱۹۹۸ تشکیل دادند. علاوه بر این، اندونزی در تیم پاسخ فوری رایانه‌ای سازمان همکاری اسلامی نیز عضویت دارد و در سال ۲۰۱۸ معاونت آن را برعهده داشت[۳]. اندونزی همچنیـن در رزمایش‌هـای سـایبری بین‌المللی متعـددی ازقبیل همایش ظرفیت‌سـازی پاسـخ فوری امنیت شبکه چین-آسه‌آن (۲۰۱۸) مشـارکت داشته‌است[۴]. اندونزی در سال ۲۰۱۹ نیز به گروه کارشناسـان دولتی[۵] سـازمان ملل درباره هنجارهای سـایبری پیوسـت و

۱. رجوع شود به:
International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 58, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

2. Asia-Pacific Computer Emergency Response Team

۳. رجوع شود به:
Asia Pacific Computer Emergency Response Team, 'APCERT Annual Report 2018', p. 128.

۴. همان، ص ۸۸.

۵. رجوع شود به:
UN Office for Disarmament Affairs, 'Developments in the field of information and telecommunications in the context of international security', https://www.un.org/disarmament/ict-security.

از سال ۲۰۱۵ هر سال کنفرانس بین‌المللی سایبری تحت‌عنوان کُدبالی[1] را برگزار می‌کند[2]. اندونزی در سال ۲۰۲۰ در اجلاس وزرای اقتصاد دیجیتال[3] گروه ۲۰ شرکت کرد که در پایان آن دستورکار جامعی برای توسعه این بخش به‌ویژه از منظر امنیتی منتشر شد. اندونزی با چین نیز در زمینه مقابله با جرائم سایبری همکاری دارد که به‌عنوان نمونه می‌توان به استرداد شهروندان چینی اشاره کرد که متهم به انجام اقدامات سایبری علیه اهدافی در چین هستند.

توانمندی‌های سایبری تهاجمی

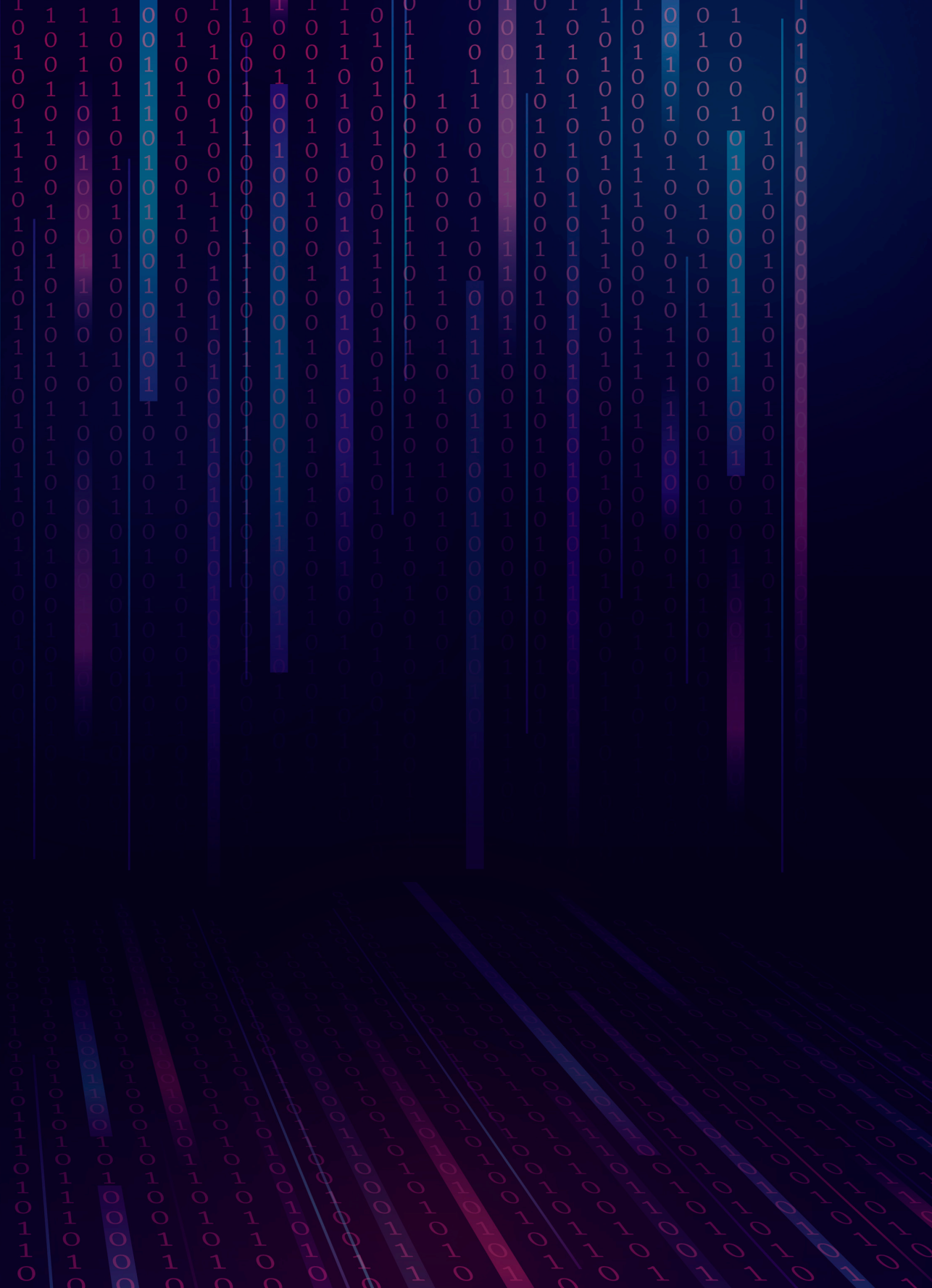
اندونزی از توانمندی‌های نسبتا توسعه‌یافته‌ای در حوزه پایش سایبری داخلی برخوردار است. به‌عنوان مثال، واحدی ویژه ضدتروریسم به نام دسته ۸۸ در نیروی پلیس این کشور تشکیل شده‌است که با حمایت شرکای بین‌المللی مانند استرالیا توانمندی‌های پایش سایبری خود را توسعه می‌بخشد[4]. بنا بر اطلاعات پراکنده‌ای که در مورد سایر توانمندی‌های سایبری تهاجمی اندونزی وجود دارد، توان سایبری این کشور جهت واکنش در زمان بروز بحران یا منازعه بسیار ضعیف است. از این رو، به نظر می‌رسد این کشور راه زیادی پیش‌رو دارد تا در این زمینه بتواند با کشورهای موردنظر خود یعنی استرالیا، چین، مالزی و ویتنام برابری کند.

1. CodeBali

۲. رجوع شود به وب‌سایت کنفرانس و نمایشگاه بین‌المللی امنیت سایبری کدبالی
'CodeBali International Cyber Security Conference and Exhibitions',
https://codebali.id.

3. Digital Economy Ministers Meeting

۴. رجوع شود به:
Muhammad Nadjib and Hafied Cangara, 'Cyber Terrorism Handling in Indonesia', Business and Management Review, vol. 9, no. 2, November 2017, pp. 278-9,
https://cberuk.com/cdn/conference_proceedings/conference_30092.pdf



۱۴

مالزی

مالـزی در زمینـه امنیت سـایبری از کشـورهای پیشـرو در منطقه به‌شـمار می‌رود و هماننـد سـایر کشـورهای هم‌تراز عملکرد خوبـی در این حوزه دارد. مالزی در سـال ۲۰۲۰ راهبردهـای جدیـدی در جهـت تامیـن امنیـت سـایبری برای بخـش غیرنظامـی و دفاع ملـی تهیـه کرد که این امر نشـان‌دهنده اهتمام آن به توسـعه امنیت سـایبری اسـت. بیانیه‌هـای رسـمی مالـزی در سـال ۲۰۲۰ بیشـتر بر سیاسـت‌های حـوزه دفـاع فعالانه در فضـای سـایبری تاکیـد داشـتند و در مـورد توانمندی‌هـای محـوری در زمینـه اطلاعـات سـایبری و نیز توسـعه توانمندی‌های سـایبری تهاجمی در این کشور اطلاعات چندانی وجـود نـدارد. در راسـتای پیشـبرد سیاسـت ارتقـای توسـعه اقتصـادی، ایـن کشـور در پـی ایجـاد و توسـعه بسـتر دیجیتالی-صنعتـی بومـی در کشـور اسـت و تـلاش می‌کند کاسـتی‌های خـود در زمینـه توانمندی‌هـای سـایبری را بـه کمـک متحدیـن بین‌المللی به‌ویژه ایالات متحده، بریتانیا، اسـترالیا و سـنگاپور جبران کند. به‌طور کلی، مالزی یک قدرت سـایبری رده سـوم اسـت، اما نقاط‌قوت آشکاری در سیاسـت امنیت سایبری و ظرفیت‌های دیجیتالی-اقتصادی این کشور وجود دارد که درصورت بهره‌برداری از آن‌ها می‌تواند به گروه قدرت‌های سایبری رده دوم صعود کند.

راهبرد و مبنای نظری (دکترین)

مالـزی در تدویـن سیاسـت‌ها، راهبـرد و مبنای نظری سـایبری خود بیش ازآنکـه متاثر از ملاحظات امنیت بین‌المللی باشـد، سیاسـت صنعتی‌سـازی و دسـتورکار توسـعه کشـور را مدنظـر داشته‌اسـت. به‌عبـارت دیگر، ضـرورت فراهم‌کـردن محیط دیجیتالـی آزاد و بـاز برای رشـد نوآوری و محیط داخلی باثبات برای حمایت از سـرمایه‌گذاری کاملاً با الزامات اقتصادی مالزی گره خورده‌است. علاوه براین، اولویت بالایی که دولت‌های متوالی مالزی برای مسائل امنیت داخلی قائل بوده‌اند نیز در شـکل‌گیری سیاست‌های سایبری آن تاثیر داشته‌است. توجـه مالـزی به فضای سـایبری بـه دهه نود برمی‌گردد، یعنـی زمانی که دولت بـرای اولین بار بـه قـدرت اینترنـت در تغییر روش ارائه خدمات عمومی و همچنین تسـریع توسـعه کشـور پـی بـرد. درسـت از همان زمان نیز مالزی سـاخت زیسـت‌بوم دیجیتال کشـور را آغـاز کرد و به‌منظور پیشـبرد این هدف مجموعه‌ای از سیاسـت‌های دولتی و مشوق‌های متعدد برای کسـب‌وکارها (ازجمله سـرمایه‌گذاری قابل‌توجه در جهت ایجاد زیرساخت‌های فنی) را به‌کار بست. هدف از این اقدامات سرعت بخشیدن به فرآیند گذار از اقتصاد مبتنی بر کشاورزی به اقتصادی مبتنی بر تولید و خدمات و درنهایت، دست‌یابی به اقتصادی کاملاً دانش‌بنیان بود.

دولت مالزی در سـال ۲۰۰۶ سیاسـت ملی امنیت سـایبری (NCSP)[1] را اعلام کرد که در آن ده محـور اصلـی از زیرسـاخت‌های اطلاعاتـی ملـی حیاتی[2] و وابسـتگی متقابل ایـن محورها مشـخص شده‌اند[3]. این سیاست مشـتمل بر رویکردی تدریجی برای ایجاد توانمندی‌های امنیت سایبری در سطح ملی بود.

1. National Cyber Security Policy
2. Critical National Information Infrastructure

۳. وزارت علـوم، فنـاوری و نـوآوری مالزی، «سیاسـت امنیـت سـایبری در سـطح ملـی: حرکتی رو به جلو»، زیرسـاخت‌های اطلاعاتی حیاتی در سـطح ملـی و فـدرال کـه در ایـن سیاسـت مشـخص شـده‌بودند شـامل بخش‌هایی اعـم از دفاع و امنیـت ملـی؛ بانکـداری و امور مالی؛ اطلاعـات و ارتباطات؛ انرژی؛ حمل‌ونقل؛ آب؛ خدمات بهداشـتی؛ دولت؛ خدمات ضروری و غـذا و کشـاورزی بودند.

دولت مالزی در سال ۲۰۱۶ چارچوب امنیت سایبری در بخش دولتی[1] را منتشر کرد که هدف آن ادغام و تجمیع تمامی دستورالعمل‌های مختلفی بود که از سال ۲۰۰۰ به‌منظور افزایش تاب‌آوری فضای سایبری در بخش دولتی ارائه شده‌بودند[2]. در سال ۲۰۱۷ نیز وزارت دفاع (MoD)[3] سیاستی در حوزه امنیت فناوری اطلاعات و ارتباطات تدوین کرد و پیرو این سیاست، کمیته‌ای ناظر بر فناوری اطلاعات و ارتباطات به ریاست دبیرکل وزارت دفاع یا معاونین وی تشکیل شد که مسئولیت ارزیابی و تایید نیازهای وزارت دفاع و نیروهای مسلح مالزی (MAF)[4] در زمینه فناوری اطلاعات و ارتباطات را عهده‌دار شد. علاوه بر کمیته مذکور، کمیته‌ای فنی نیز با هدف نظارت بر جنبه‌های فنی نیازهای وزارت دفاع و نیروهای مسلح در زمینه فناوری اطلاعات و ارتباطات تشکیل شد[5].

در سال ۲۰۲۰ راهبرد جدیدی در حوزه امنیت سایبری برای دوره ۲۰۲۰-۲۰۲۴ انتشار یافت[6]. از سال ۲۰۰۶ تاکنون این راهبرد اولین سند در نوع خود است که به پنج رکن سیاست شامل حاکمیت، چارچوب قانونی و اجرای آن، نوآوری در سطح جهانی، ظرفیت‌سازی و آموزش و همکاری جهانی می‌پردازد. راهبرد مذکور در بسیاری از ابعاد به‌ویژه در تاکید بر مبارزه با جرائم سایبری، حفاظت از زیرساخت‌های حیاتی ملی، نوآوری و آموزش افراد

1. Public Sector Cyber Security Framework

۲. رجوع شود به:
National Cyber Security Agency, 'RAKKSSA: Rangka Kerja Keselamatan Siber Sektor Awam', April 2016, https://www.nacsa.gov.my/doc/RAKKSSA-VERSI-1-APRIL-2016-BM.pdf.

3. Ministry of Defense

4. Malaysian Armed Forces

۵. رجوع شود به:
'Dasar Keselamatan Teknologi Maklumat Dan Komunikasi (DKICT)', January 2017, http://www.stride.gov.my/v2/images/contents/DKICT-MINDEF_VER-5_1-JAN-2017.pdf.

۶. رجوع شود به:
National Security Council, Prime Minister's Department, 'Malaysia Cyber Security Strategy 2020-2024', October 2020, https://asset.mkn.gov.my/web/wp-content/uploads/sites/3/2019/08/Malaysia CyberSecurityStrategy 2020-2024Compressed.pdf.

بیشتر برای رفع شکاف نیروی کار سایبری به راهبردهای سایر کشورها شباهت دارد. از دیگر اولویت‌های این راهبرد می‌توان به مبارزه با تروریسم و افراط‌گرایی خشونت‌آمیز به‌ویژه مقابله با تحریک و جذب نیرو ازطریق اینترنت اشاره کرد. طبق این راهبرد جدید، دولت مالزی موظف به دستیابی به سه اولویت راهبردی و فراگیر است که عبارتند از: زیست‌بوم حاکمیتی، بهبود امنیت بخش خصوصی (به‌ویژه برای اپراتورهای زیرساخت) و بهبود مدیریت حوادث امنیت سایبری. بنا بر اعلام دولت مالزی، اجرای این راهبرد مستلزم سرمایه‌گذاری ۴۳۴ میلیون دلاری در دوره چهارساله آن خواهد بود[۱].

گزارش سیاست دفاعی (۲۰۲۰) وزارت دفاع مالزی حاوی سیاست‌های بسیار قوی‌تری جهت داشتن دفاعی فعال در فضای سایبری تمامی بخش‌های نظامی و غیرنظامی است[۲]. در این گزارش ضمن تاکید بر ضرورت توسعه، برخی از توانمندی‌های سایبری تهاجمی-البته صرفا به‌منظور پاسخ به حمله سایبری به مالزی-و سه رکن دفاع ملی یعنی بازدارندگی متمرکز، دفاع همه‌جانبه و مشارکت‌های قابل‌اطمینان نیز معرفی شده‌اند. علاوه براین، گزارش مذکور بر تاب‌آوری سایبری به‌عنوان بخشی از رویکرد کل جامعه در دفاع تأکید می‌کند.

در این گزارش مفهوم «نیروی‌های آینده» معرفی می‌شود که لازمه اجرای بازدارندگی متمرکز است. یکی از ویژگی‌های اصلی نیروهای آینده شامل «قابلیت همکاری بین

۱. رجوع شود به:
Stuart Crowley, 'Malaysia to spend $434m on national cybersecurity strategy', W.media, 16 October 2020,
https://w.media/malaysia-to-spend-434m-on-national-cybersecuritystrategy/#:~:text=The%20first%20pillar%20will%20look,and%20formulating%20laws%20on%20cybersecurity.

۲. رجوع شود به:
Ministry of Defense, 'Defense White Paper: A Secure, Sovereign and Prosperous Malaysia', Kuala Lumpur, 2020,
http://www.mod.gov.my/images/mindef/article/kpp/DWP.pdf.

آن‌ها» است که یکی از وجوه‌اشتراک تمامی نیروهای مسلح مالزی از نظر مبانی نظری، روش‌ها و سیستم‌ها و تجهیزات به‌شمار می‌رود. لازم به ذکر است که نیروهای آینده مبتنی بر فناوری خواهند بود، به این معنی که از آخرین فناوری‌های دیجیتال مانند اینترنت اشیا و هوش مصنوعی بهره خواهند برد. این سیاست دفاعی نیروهای مسلح را موظف به بازنگری در مبانی نظری موجود کرده‌است تا بتوانند از فناوری‌های خودکار و بدون راهبر بیشتری در زمان نیاز به اصلاح ترکیب و آرایش کلی نیروهای مسلح استفاده کنند[1].

آرمان‌های موردنظر در گزارش سیاست دفاعی (۲۰۲۰) تا حدود زیادی به آرمان‌های نامبرده در سند قبلی یعنی سیاست دفاعی ملی (۲۰۱۰)[2] شباهت دارند. سیاست دفاعی ملی (۲۰۱۰) بر اهمیت چیرگی اطلاعاتی در سطوح عملیاتی، فنی و راهبردی به‌منظور حفاظت از اقتدار حاکمیت ملی تأکید داشت[3] و مطابق آن، توسعه توانمندی‌های جنگ سایبری به‌عنوان گامی مهم در جهت برهم‌زدن توازن قدرت در سایر کشورهای منطقه و دفاع از اهداف مهم ملی در برابر هر گونه تهدید قلمداد می‌شد.

حکمرانی، فرماندهی و نظارت

شورای امنیت ملی (NSC)[4] به ریاست نخست‌وزیر بالاترین مرجع تصمیم‌گیری در مورد مسائل امنیت سایبری مالزی است. این شورا دارای کمیته‌ای فرعی در زمینه امنیت سایبری به ریاست یکی از وزیران ارشد امنیتی است که در دسامبر ۲۰۲۰ برای اولین

۱. همان.

2. National Defense Policy of 2010

۳. رجوع شود به:
'Malaysia's National Defense Policy', 2010, pp. 12-13, https://web.archive.org/web/20181024164353/http://www.mod.gov.my/images/mindef/lain-lain/ndp.pdf.

4. National Security Council

بار تشکیل جلسه داد[۱]. سازمان ملی امنیت سایبری (NACSA)[۲] که در سال ۲۰۱۷ تشکیل شده‌است و مسئولیت اموری مانند تدوین، نظارت، سازماندهی و هماهنگی اجرای سیاست امنیت سایبری در بخش‌های دولتی و خصوصی را برعهده دارد نیز از این کمیته در سطح ملی پشتیبانی می‌کند. از دیگر مسئولیت‌های سازمان ملی امنیت سایبری می‌توان به اقداماتی درجهت قانون‌گذاری و اجرای قوانین در حوزه امنیت سایبری و همچنین همکاری‌های داخلی و خارجی در هر دو بخش دولتی و خصوصی اشاره کرد[۳]. سازمان ملی امنیت سایبری همچنین وظیفه هماهنگ‌سازی سایر سازمان‌های دولتی فعال در حوزه امنیت سایبری (ازجمله دفاتر دادستان کل[۴]، دفتر افسر ارشد امنیت دولتی[۵]، سازمان امنیت سایبری مالزی[۶]، وزارت ارتباطات و چندرسانه‌ای[۷] و وزارت تجارت داخلی و امور مصرف‌کنندگان[۸]) را برعهده دارد[۹].

وزارت دفاع و نیروهای مسلح مالزی در سال ۲۰۱۶ مرکز عملیاتی دفاع سایبری (CDOC)[۱۰] را با هدف محافظت از سیستم‌ها و شبکه‌های فناوری اطلاعات و ارتباطات

۱. رجوع شود به:
'National Security Council: Govt to set up special task force to identify cyber security issues', Malay Mail, 17 December 2020,
https://www.malaymail.com/news/malaysia/2020/12/17/nationalsecurity-council-govt-to-set-up-special-task-force-to-identifycyb/1932893.
2. National Cyber Security Agency

۳. رجوع شود به:
National Security Council, Prime Minister's Department, 'Frequently Asked Questions',
https://www.nacsa.gov.my/faq.php.
4. Attorney General's Chambers
5. Chief Government Security Officer
6. Cybersecurity Malaysia
7. Ministry of Communications and Multimedia
8. Ministry of Domestic Trade and Consumer Affairs

۹. رجوع شود به:
Cyber Security - Towards a Safe and Secure Cyber Environment (Kuala Lumpur: Academy of Sciences Malaysia, 2018), pp. 30-3,
https://issuu.com/asmpub/docs/cybersecurity
10. Cyber Defense Operations Centre

مشترک خود تاسیس کردند. مرکز عملیاتی دفاع سایبری از سال ۲۰۱۷ فعالانه به رصد تهدیدها و همچنین کاهش اثر حوادث امنیت سایبری اشتغال دارد[۱]. نیروهای مسلح مالزی در دسامبر سال ۲۰۲۰ و پس از یک سال برنامه‌ریزی از ایجاد بخشی تحت‌عنوان لشکر ارتباطات دفاعی و الکترونیکی[۲] خبر داد که وظیفه تقویت توانمندی‌های تهاجمی و دفاعی در عملیات‌های سایبری و همچنین اقدام به جنگ الکترونیکی را برعهده دارد[۳]. این بخش جایگزین لشکر ارتباطات و الکترونیک[۴] شده‌است که در سال ۱۹۹۳ تاسیس شده‌بود.

وزارت دفاع و نیروهای مسلح هر یک تیم‌های پاسخ فوری رایانه‌ای (CERT) مختص به خود را دارند. تیم وزارت دفاع موسوم به MinDefCERT حوادث رخ داده را به تیم پاسخ فوری رایانه‌ای دولت (GCERT MAMPU) گزارش می‌دهد و تیم نیروهای مسلح موسوم به MAFCERT مستقیماً به شورای امنیت ملی پاسخگوست. رهبری تیم پاسخ فوری رایانه‌ای نیروهای مسلح را رئیس مرکز عملیاتی دفاع سایبری برعهده دارد و این تیم دارای مدیران فناوری اطلاعات و ارتباطات در هر سه شاخه از نیروهای مسلح است[۵].

---

۱. رجوع شود به:
Muhammad Sabu, Hansard, Parliament of Malaysia, D.R.30.10.2018, 30 October 2018, p. 137.

2. Defense Communication and Electronic Division

۳. رجوع شود به:
'Launch Ceremony of Cyber and Electromagnetic Division Defense (BSEP)', Malaysia Military Times, 19 December 2020,
https://mymilitarytimes.com/index.php/2020/12/19/launch-ceremony-of-cyber-and-electromagnetic-division-defence-bsep.

لازم به ذکر است که ترجمه‌های انگلیسی مختلفی از نام این بخش وجود دارد، اما این بخش توسط نیروهای مسلح مالزی با عنوان لشکر ارتباطات دفاعی و الکترونیکی نامگذاری شده‌است.

4. Communications and Electronics Division

۵. رجوع شود به:
'Dasar Keselamatan Teknologi Maklumat Dan Komunikasi (DKICT)', pp. 23-5.

توانمندی‌های محوری در زمینه اطلاعات سایبری

جامعه اطلاعاتی مالزی توسط شورای امنیت ملی تحت‌نظارت نخست‌وزیر[1] این کشور اداره می‌شود[2]. به‌طور کلی، هماهنگی سیاست‌های امنیت ملی ازجمله در مواقع اضطراری وظیفه اصلی شورای امنیت ملی محسوب می‌شود[3]. کمیته ملی اطلاعات (NIC)[4] و بخش فرعی آن با نام واحد اطلاعات ملی[5] از زیرمجموعه‌های شورای امنیت ملی محسوب می‌شوند[6]. کمیته ملی اطلاعات وظیفه هماهنگی سایر نهادهای اطلاعاتی مانند شعبه ویژه[7] (زیر نظر پلیس سلطنتی مالزی[8])، سازمان اطلاعات خارجی مالزی[9] (زیر نظر نخست‌وزیر) و واحد اطلاعات ستاد دفاع[10] (تحت‌نظارت نیروهای مسلح) را برعهده دارد.

توانمندی اصلی اطلاعات سیگنالی به‌عنوان یکی از هزاران ماموریت و وظایف مالزی در زمینه امنیت ملی برعهده هنگ سلطنتی سیگنال‌ها (RSD)[11]، سپاه سلطنتی اطلاعات[12]

1. Prime Minister's Department

۲. رجوع شود به:
National Security Council, 'Directive No. 20, Policy and Mechanism of National Disaster Management and Relief',
https://www.adrc.asia/management/MYS/Directives_National_ Security_Council.html.

۳. رجوع شود به:
Majlis Keselamatan Negara, 'Sejarah', 20 January 2019,
https:// www.mkn.gov.my/web/ms/sejarah-mkn

4. National Intelligence Committee
5. National Intelligence Division

۶. رجوع شود به:
Philip H. J. Davis, 'All in Good Faith? Proximity, Politicization, and Malaysia's External Intelligence Organization', International Journal of Intelligence and Counterintelligence, vol. 32, no. 4, May 2019, pp. 691-716,
https://www.tandfonline.com/doi/abs/10.10 80/08850607.2019.1621105.

7. Special Branch
8. Royal Malaysia Police
9. Malaysian External Intelligence Organization
10. Defense Staff Intelligence Division
11. Royal Signals Regiment (Malay: Regimen Semboyan Diraja)
12. Royal Intelligence Corps

در ارتـش و بخش اطلاعات سـتاد دفاع (معادل سـازمان اطلاعات دفاعـی ایالات متحده[1]) اسـت. با سـازماندهی مجدد هنگ سـلطنتی سیگنال‌ها توسـط نیروهای مسلح در سال ۲۰۱۸، واحد سایبری تخصصی به نام RSD 99 تشکیل شد[2]. شعبه ویژه مسئولیت نظارت سـایبری بـر تهدیـدات داخلـی ناشـی از تروریسـم و اقدامـات خرابکارانـه را برعهـده دارد. سـازمان اطلاعـات خارجـی مـالزی که بـا عنوان رسـمی سـازمان تحقیقات نخسـت‌وزیری[3] شناخته می‌شود نیز احتمالا دارای واحد اطلاعات سایبری کوچکی است.

مالـزی بـرای گسـترش دامنـه اطلاعات سـایبری منطقـه‌ای و جهانی خود بـه همکاری بـا متحدان بین‌المللی به‌ویژه ایالات متحده، بریتانیا، اسـترالیا و سـنگاپور متکی اسـت. همـکاری امنیتـی بین کوالالامپور و این کشـورها بیشـتر در زمینه جمع‌آوری اطلاعات در دریای چین جنوبی و همچنین مبارزه با تروریسـم است.

توانمندی و وابستگی سایبری

اقتصاد دیجیتال مالزی حدود ۲۰ درصد از تولید ناخالص داخلی آن را تشکیل می‌دهد[4] و بنـا بـه پیش‌بینـی دولـت، ایـن بخـش می‌توانـد ازطریـق نوآوری‌هـای فناورانـه نقـش فزاینده‌ای در رشد اقتصادی کشور ایفا کند[5]. رهبری این اقدامات برعهده شرکت اقتصاد

1. US Defense Intelligence Agency

۲. رجوع شود به:
Marhalim Abas, 'Restructuring of the Signals Regiment', Malaysian Defense, 19 November 2019, https://www. malaysiandefence.com/restructuring-of-the-signals-regiment.

3. Research Department of the Prime Minister

۴. رجوع شود به:
'Malaysia's digital economy now contributes one fifth to GDP', Consultancy.asia, 7 July 2020, https://www.consultancy.asia/news/3370/malaysias-digital-economy-now-contributes-onefifth-to-gdp.

۵. رجوع شود به:
World Bank Group, 'Malaysia's Digital Economy: A New Driver of Development', September 2018, https:// openknowledge.worldbank.org/bitstream/handle/10986/303 83/129777.pdf.

دیجیتال مالزی[1] است و نظارت بر توسعه ابرکریدور چندرسانه‌ای[2] ازجمله وظایف آن به شمار می‌رود[3]. ابرکریدور چندرسانه‌ای مالزی طبق الگوی سیلیکون‌ولی[4] در کالیفرنیا ساخته شده و مشتمل بر حدود ۳۰۰۰ شرکت فناوری اطلاعات و ارتباطات است. دولت مالزی سیاست‌ها و طرح‌های کلان متعددی را در حوزه اقتصاد دیجیتال با مشارکت بخش خصوصی آغاز کرده‌است که از آن میان می‌توان به سیاست ملی انقلاب صنعتی چهارم (4 WRD Policy) با تاکید بر نسل چهارم صنعت؛ نقشه‌راه ملی تجارت الکترونیک[5] یا زیست‌بوم ملی تحلیل کلان‌داده[6]؛ منطقه آزاد تجارت دیجیتال[7] با هدف تبدیل مالزی به قطب تجارت الکترونیک و پردازش الکترونیکی سفارشات و طرح ملی اینترنت اشیا[8] اشاره کرد[9]. لازم به ذکر است که چارچوب ملی هوش مصنوعی[10] نیز در حال تدوین است.

طبق آمار ارائه شده در سال ۲۰۱۹، مالزی با ۳۲ میلیون نفر جمعیت دارای ۴۳/۳۸ میلیون اشتراک اینترنت پهن‌باند در وزارت ارتباطات و چندرسانه‌ای است[11]. با این حال،

1. Malaysia Digital Economy Corporation

رجوع شود به:

Malaysia Digital Economy Corporation, 'Who We Are', https:// mdec.my/about-mdec/who-we-are.

2. Multimedia Super Corridor

۳. رجوع شود به:

Malaysia Digital Economy Corporation, 'What We Offer', https://mdec.my/what-we-offer/msc-malaysia.

4. Silicon Valley
5. National eCommerce Roadmap
6. National Big Data Analytics Ecosystem
7. Digital Free Trade Zone
8. National IoT Framework

۹. رجوع شود به:

Malaysia Digital Economy Corporation, 'A Nation's Commitment to the Digital Economy', https://mdec.my/ about-malaysia/government-policies.

10. National AI Framework

۱۱. رجوع شود به:

'MCMC: 43.38 million Broadband Subscription in Malaysia, 82.2% 4G LTE Coverage', Malaysian Wireless, 18 May 2020, https://www.malaysianwireless.com/2020/05/mcmc-fixedbroadband-mobile-subscribers-malaysia

شـکاف دیجیتالی بین مناطق شـهری و روستایی مالزی به چشم می‌خورد و حداقل ۳/۵ میلیون مالزیایی سـاکن در مناطق روستایی یا نیمه‌شهری از اینترنت پرسرعت برخوردار نیسـتند[۱]. طـرح ملی فیبرسـازی و اتصال[۲] نمونـه‌ای از برنامه‌های توسـعه‌ای دولت مالزی اسـت که با هدف ایجاد یک شـبکه فیبر نوری برای خدمت‌رسانی به ۷۰ درصد از مدارس، بیمارستان‌ها، کتابخانه‌ها، ایستگاه‌های پلیس و دفاتر پست تا سال ۲۰۲۲ و ارائه اینترنت با سـرعت متوسـط ۳۰ مگابیت بر ثانیه در ۹۸ درصد از مناطق پرجمعیت کشـور تا سـال ۲۰۲۳ راه‌اندازی شده‌است[۳].

در مقایسـه با سـایر کشـورهای جنوب شـرق آسـیا، مالزی در زمینه تحقیقات هوش مصنوعـی پیشـرفت کمتـری داشته‌اسـت. به‌عنـوان مثـال، در رتبه‌بنـدی ۵۰ کشـور برتـر جهـان که براسـاس مشـارکت آن‌هـا در دو کنفرانس معتبر هوش مصنوعی در سـال ۲۰۲۰ انجام شده‌اسـت، مالزی در رتبه ۴۷ و در جایگاهی پایین‌تر از سـنگاپور (۱۲)، ویتنام (۲۷) و تایلنـد (۴۴) قـرار دارد. (از بیـن کشـورهای منطقه تنهـا اندونزی در جایـگاه پایین‌تری از مالزی است و نتوانسته در میان کشورهای این فهرست قرار گیرد[۴]). با این حال، بخش خصوصی مالزی سـرمایه‌گذاری‌های قابل‌توجهـی در زمینه فناوری هوش مصنوعی انجام داده‌اسـت. به‌عنـوان مثـال، شـرکت مالزیایـی G3 Global Bhd کـه شـرکتی تخصصـی در

۱. رجوع شود به:
B.K. Sidhu, 'Going beyond fibre for internet throughout Malaysia', Star, 28 January 2019, https://www.thestar.com. my/business/business-news/2019/01/28/going-beyondfibre.

2. National Ferberization and Connectivity Plan

۳. رجوع شود به:
Malaysian Communications and Multimedia Commission, 'National Ferberization and Connectivity Plan', https://www. nfcp.my/Nfcp/media/Docs/NFCP-FS002-v5c.pdf.

۴. رجوع شود به:
Gleb Chuvpilo, 'AI Research Rankings 2020: Can the United States Stay Ahead of China?', Medium.com, 20 December 2020,
https://chuvpilo.medium.com/ai-research-rankings-2020-canthe-united-states-stay-ahead-of-china-61cf14b1216

زمینه ارائه خدمات اینترنت اشیا و فناوری هوش مصنوعی است در سال ۲۰۲۰ قراردادی با دو شرکت فناوری چینی امضا کرد. به‌موجب این قرارداد، اولین پارک هوش مصنوعی مالزی در کوالالامپور تاسیس خواهد شد و ظاهراً تا سال ۲۰۲۵ بیش از ۱ میلیارد دلار سرمایه‌گذاری خواهد شد[۱]. با این وجود، نرخ به‌کارگیری فناوری هوش مصنوعی در مالزی (۸/۱ درصد) است که در مقایسه با کشورهایی مانند اندونزی (۲۴/۶ درصد) یا تایلند (۱۷/۱ درصد) رقم ناچیزی است[۲].

بیشتر کابل‌های فیبر نوری این کشور در اختیار دو شرکت تناگا ناسیونال[۳] و تله‌کام مالزی[۴] است که به‌طور مستقیم یا از ۱۵۰طریق سهام شرکت‌های کوچک‌تر اداره می‌شوند. شرکت تناگا ناسیونال بزرگ‌ترین شرکت برق مالزی[۵] و دارای ۱۲,۰۰۰ کیلومتر کابل فیبر نوری در سراسر کشور است که تنها بخش کوچکی از پهنای باند موجود را استفاده می‌کند[۶]. شرکت تله‌کام مالزی تنها شرکت ارائه‌دهنده اینترنت پهن‌باند پرسرعت در این کشور است که در قالب مشارکت دولت و بخش خصوصی به ۲/۵ میلیون خانوار در سراسر کشور خدمات ارائه می‌دهد. این شرکت دارای بیش از ۲۰ سیستم کابل زیردریایی به‌طول ۱۹۰,۰۰۰ کیلومتر و همچنین بیش

۱. رجوع شود به:
Royce Tan, 'AI Park Will Help Malaysia Take the Lead in Digital Future', Star, 17 October 2020, https://www.thestar. com.my/business/business-news/2020/10/17/ai-park-will-helpmalaysia-take-the-lead-in-digital-future.

۲. همان.

3. Tenaga Nasional Berhad
4. Telekom Malaysia Berhad

۵. رجوع شود به:
Tenaga Nasional, 'Corporate Profile', https://www.tnb.com. my/about-tnb/corporate-profile.

۶. رجوع شود به:
P. Prem Kumar, 'TNB expanding fixed broadband footprint in rural homes', The Malaysian Reserve, 26 November 2018, https://themalaysianreserve.com/2018/11/26/tnb-expanding-fixedbroadband-footprint-in-rural-homes.

از ۵۶۰,۰۰۰ کیلومتر کابل فیبر نوری است[۱]. تنها چهار مورد از این کابل‌های زیردریایی در خدمت خود مالزی هستند. شرکت‌های کوچک‌تر دیگری نیز کابل‌های فیبر نوری ارائه می‌دهند که به‌عنوان نمونه می‌توان به فایبرکام[۲] با ۱۱۰,۰۰۰ کیلومتر کابل در سراسر کشور[۳]؛ تایم دات‌کام[۴] با ۷۰۰۰ کیلومتر کابل در سراسر بزرگراه شمال-جنوب[۵] و فایبریل[۶] با ۴,۸۰۰ کیلومتر کابل در امتداد خطوط راه‌آهن اشاره کرد. شرکت‌های مخابرات سیار (تلفن همراه) مانند سل‌کام اَکسیاتا، دی‌جی و مَکسیس[۷] نیز دارای شبکه‌های فیبری مختص به خود هستند[۸]. ایالت پنانگ اولین ایالت مالزی است که از دسامبر ۲۰۲۰ به‌کارگیری کابل‌کشی فیبر نوری در ساخت‌وسازهای جدید را اجباری کرده‌است[۹].

شرکت مخابرات ماهواره‌ای MEASAT Global Berhad دارای ناوگان ماهواره‌ای متشکل از پنج ماهواره با پوشش آسیا، خاورمیانه و آفریقا است که ارتباطات ماهواره‌ای مالزی را تامین می‌کند. این شرکت مخابراتی سفارش ساخت ماهواره جدیدی به‌نام

---

۱. رجوع شود به:

Telekom Malaysia Berhad, 'Review of the Year & Key Achievements', 2020, https://www.tm.com.my/annualreport/#/ review-of-the-year-key-achievements.

2. Fibercomm

۳. رجوع شود به:

Fibrecomm Network, 'Company profile', https://www. fibrecomm.net.my/?page_id=10830.

4. TIME dotCom
5. North-South Expressway
6. Fiberail
7. Celcom Axiata, Digi and Maxis

۸. رجوع شود به:

Sidhu, 'Going beyond fibre for internet throughout Malaysia'.

۹. رجوع شود به:

Alexander Wong, 'Penang is the first state to make fibre optic infrastructure mandatory for new developments', SoyaCincau, 24 December 2020, https://www.soyacincau.com/2020/12/24/penang-fibre-optic-broadband-infrastructure-basic- utilityfirst-state-malaysia

MEASAT-3d به ایرباس داده که طبق انتظار باید در سال ۲۰۲۱ به فضا پرتاب می‌شد، اما با اندکی تاخیر در اوایل سال ۲۰۲۲ در مدار قرار گرفت[۱]. با قرارگرفتن این ماهواره در مدار ارائه اینترنت همراه نسل چهارم و پنجم تسهیل خواهد شد[۲].

امنیت و تاب‌آوری سایبری

مالزی در حوزه سیاست امنیت سایبری در منطقه خود پیشرو است. این کشور با تصویب قانون جرائم رایانه‌ای[۳] در سال ۱۹۹۷ یکی از اولین کشورهای آسیایی بود که قوانین مربوط به این نوع جرائم را تصویب کرد[۴]. در سال ۲۰۰۸ نیز کشور مالزی این افتخار را کسب کرد که به کانون برنامه جهانی امنیت سایبری (GCA)[۵] اتحادیه بین‌المللی مخابرات (ITU) تبدیل شود[۶]. مالزی از سال ۱۹۹۸ دارای مرجع نظارتی و

۱. به نقل از خبرگزاری مالای میل، این ماهواره در ۲۲ ژوئن سال ۲۰۲۲ در مدار قرار گرفته‌است (توضیح مترجم). برای دریافت اطلاعات بیشتر رجوع شود به:
https://www.malaymail.com/news/malaysia/2022/06/23/measat-3d-malaysias-latest- satellite-successfully-launched-into-orbit/13765

۲. رجوع شود به:
Caleb Henry, 'Measat buying single replacement for two satellites', SpaceNews, 6 May 2019, https://spacenews.com/ measat-buying-single-replacement-for-two-satellites.

3. Computer Crime Act

۴. رجوع شود به:
Computer Crimes Act 1997, Laws of Malaysia, Act 563, http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/ EN/Act%20563.pdf.

5. Global Cybersecurity Agenda

۶. رجوع شود به:
International Telecommunication Union, 'Global Cybersecurity Agenda', https://www.itu.int/en/action/ cybersecurity/Pages/gca.aspx.
اتحادیه بین‌المللی مخابرات برنامه جهانی امنیت سایبری را برنامه‌ای برای همکاری‌های بین‌المللی با هدف افزایش اعتماد و امنیت در جامعه اطلاعاتی می‌داند و همچنین تاکید می‌کند که این برنامه به‌منظور افزایش همکاری و کارایی، تشویق به همکاری با همه متحدان و همچنین ایجاد ابتکارات حاضر برای جلوگیری از اقدامات مکرر طراحی شده‌است.

قانون‌گـذاری تحت‌عنوان کمیسـیون ارتباطات و چند رسـانه‌ای اسـت[۱] و قانون حفاظت از اطلاعات شـخصی[۲] را نیز در سـال ۲۰۱۰ به تصویب رساند[۳].

مالزی در سال ۲۰۱۱ مرکز ملی هماهنگی و فرماندهی سایبری[۴] را برای مدیریت و نظارت بر حوادث سایبری و تعیین سطح و تأثیر احتمالی تهدیدات امنیت سایبری تاسیس کرد[۵] که هنگام وقوع بحران نقش مشـاور فنی را برای کمیته ملی مدیریت بحران سـایبری[۶] ایفا می‌کنـد[۷]. ایـن مرکـز اطلاعات موردنیاز خـود را از دو منبع دریافت می‌کند: سـازمان امنیت سایبری و کمیسیون ارتباطات و چندرسانه‌ای مالزی[۸].

مالزی توانسته‌اسـت پروژه‌ای آزمایشـی تحت‌عنوان پروژه هماهنگ نابودی بدافزارها و احیا[۹] را جهت تمرین مقابله با تهدید بدافزارها در سـطح ملی اجرا کند. شـاخص جهانی امنیت سـایبری که در سـال ۲۰۱۸ از سـوی اتحادیه بین‌المللی مخابرات منتشرشد[۱۰] نیز به چندین ابتکار بین‌سازمانی برای مبارزه با کلاهبرداری بانکی برخط، راه‌اندازی آزمایشگاه‌های

1. Communications and Multimedia Commission

رجوع شود به:
'Communications and Multimedia Act 1998', Commonwealth Legal Information Institute, http://www.commonlii.org/my/ legis/consol_act/cama1998289.

2. Personal Data Protection Act

۳. رجوع شود به:
Personal Data Protection Act 2010, Laws of Malaysia, Act 709, http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20709%2014%206 %20 2016.pdf.

4. National Cyber Coordination and Command Centre

۵. رجوع شود به:
National Cyber Coordination and Command Centre, 'About Us', http://www.nc4.gov.my/about_us.

6. National Cyber Crisis Management Committee

۷. رجوع شود به:
National Cyber Coordination and Command Centre, 'About Us'.

۸. رجوع شود به:
International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 38, https://www.itu.int/dms_pub/itu-d/opb/str/ D-STR-GCI.01-2018-PDF-E.pdf.

9. Coordinated Malware Eradication and Remediation Project

10. ITU's 2018 Global Cybersecurity Index

جرم‌شناسی دیجیتال و تبادل اطلاعات در حوزه‌های فنی امنیت سایبری اشاره می‌کند. علاوه بر این موارد، همکاری‌هایی بین دولت و صنعت به‌منظور تهیه راهنمای بهترین شیوه‌های حوزه امنیت ابری شکل گرفته‌است[۱].

شرکت‌های مالزیایی و چندملیتی که ازطریق همکاری با دولت به تقویت ظرفیت و توان داخلی کمک می‌کنند، نقش مهمی در افزایش تاب‌آوری کشور در برابر تهدیدهای سایبری دارند. به‌عنوان مثال، شرکت مالزیایی سایبر اینتلیجنس[۲] با همکاری سازمان امنیت سایبری مالزی و دانشگاه اسلامی بین‌المللی مالزی[۳] موفق به ایجاد محیط‌های مجازی (دامنه سایبری)[۴] برای شبیه‌سازی تهدیدهای سایبری شده‌است[۵].

مالزی اجرای رزمایش‌های ملی سایبری در زمینه زیرساخت‌های اطلاعاتی ملی حیاتی را با مشارکت بازیگران دولتی و خصوصی از سال ۲۰۰۸ آغاز کرده‌است. این رزمایش‌ها با نام رمز X-Maya به‌رهبری سازمان امنیت سایبری مالزی و شورای امنیت ملی اجرا می‌شوند. به‌طور کلی، آزمودن مهارت‌های فنی و جمعی کارکنان در همه ارکان زیرساخت‌های ملی حیاتی هدف اصلی این رزمایش‌ها در نظر گرفته می‌شوند[۶]. گزارش‌های دولتی نشان می‌دهند که جدیدترین دور از این رزمایش‌ها در سال ۲۰۱۷ انجام شده است. به نظر می‌رسد از آن زمان به بعد دولت سیاستی مبتنی بر رویکرد بخش‌محور را در پیش گرفته‌است. به‌عنوان مثال، دولت مؤسسات مالی را ملزم به تهیه طرح‌هایی برای

۱. رجوع شود به:
International Telecommunication Union, ‘Global Cybersecurity Index 2018’, p. 38.

2. Cyber Intelligence

3. International Islamic University Malaysia

4. Cyber range

۵. رجوع شود به:
Cyber Intelligence, ‘Cyber Intelligence (CI)’,
https://www. cybersecurityintelligence.com/cyber-intelligence-ci-4798.html.

۶. رجوع شود به:
CyberSecurity Malaysia, ‘Milestones’,
https://www.cybersecurity.my/en/about_us/milestones/main/detail/2325/ index.html.

واکنش به حوادث سایبری و برگزاری رزمایش‌های سالانه برای ارزیابی آن‌ها کرده‌است[۱]. دولت توسعه اقدامات مربوط به حفاظت از زیرساخت‌های مهم ملی را در راهبرد امنیت سایبری (۲۰۲۰)[۲] در اولویت قرار داده‌است و اپراتورهای زیرساخت‌ها را ملزم به تعهدات بسیار قوی‌تر جهت پیشگیری از حوادث سایبری و یا کاهش پیامدهای آن‌ها در صورت وقوع این حوادث می‌کند[۳].

با توجه به اینکه مالزی از زیرساخت‌های کلیدی امنیت سایبری به‌ویژه تعهد سیاسی دولت و آموزش باکیفیت برخوردار است، توان دستیابی به سطح پیشرفته‌ای از تاب‌آوری سایبری را دارد. طبق شاخص جهانی امنیت سایبری که توسط اتحادیه بین‌المللی مخابرات در سال ۲۰۱۸ منتشر شد، مالزی در میان ۱۷۵ کشور رتبه هشتم و در منطقه آسیا و اقیانوسیه پس از سنگاپور رتبه دوم را کسب کرده‌است[۴]. با این وجود، در ارتباط با توانمندی‌های مالزی در زمینه شناسایی و گزارش حملات سایبری و واکنش به این حوادث هنوز اطلاعات دقیقی وجود ندارد. به نظر می‌رسد که این کشور نیازمند ارتقای هماهنگی بین کارگزاران امنیت سایبری است، زیرا تحلیل منتشر شده در سال ۲۰۱۹ از فقدان هماهنگی در این کشور حکایت دارد[۵].

---

۱. رجوع شود به:
Chew Kherk Ying, 'Cyber Security 2020, Malaysia', Chambers and Partners, 16 March 2020, https:// practiceguides.chambers.com/practice-guides/ cybersecurity-2020/malaysia.
2. 2020 Cyber Security Strategy

۳. رجوع شود به:
National Security Council, Prime Minister's Department, 'Malaysia Cyber Security Strategy 2020-2024', pp. 30-9.

۴. رجوع شود به:
International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 58.

۵. رجوع شود به:
Azian Ibrahim et al., 'Cyber Warfare Impact to National Security - Malaysia Experiences', paper presented to FGIC 2nd Conference on Governance and Integrity 2019, Yayasan Pahang, Kuantan, Pahang, Malaysia, 19-20 August 2019, p. 222, https://knepublishing.com/index.php/KnE-Social/article/ download/5052/10067.

رهبری جهانی در عرصه سایبری

مالزی در مجامع منطقه‌ای و جهانی نقشی پیشرو در زمینه فنی ایفا می‌کند. سازمان امنیت سایبری مالزی به دبیرخانه دائمی تیم پاسخ فوری رایانه‌ای سازمان همکاری اسلامی (OIC-CERT)[۱] تبدیل شده‌است. لازم به ذکر است مالزی اولین برنامه ظرفیت‌سازی سایبری آسه‌آن را در سال ۲۰۱۵ اجرا کرد و این کشور دو بار در مقام نایب‌رئیس تیم پاسخ فوری رایانه‌ای آسیا-اقیانوسیه (APCERT)[۲] انجام وظیفه کرده‌است. آزمایشگاه جرم‌شناسی دیجیتال در سازمان امنیت سایبری مالزی که قادر به انجام تحقیقات جرم‌شناسی در زمینه جرائم رایانه‌ای، چندرسانه‌ای، موبایل، بیومتریک، رایانش ابری و دستگاه‌های جاسازی شده (سیستم‌های نهفته)[۳] است، اولین آزمایشگاه در آسیا و اقیانوسیه است که اینترپل آن را به‌رسمیت شناخته‌است[۴].

مالزی با بسترهای فنی و استاندارد دیگر ازجمله اجلاس تیم‌های امنیت و پاسخگویی به حوادث[۵]، موسسه اینترنتی برای اعداد و نام‌های اختصاص یافته (آیکان)[۶]، نشست وزیران مخابرات و فناوری اطلاعات آسه‌آن[۷] و انجمن مخابرات آسیا-اقیانوسیه (APT)[۸] نیز همکاری نزدیکی دارد[۹].

1. Organization of Islamic Cooperation's Computer Emergency Response Team
2. Asia-Pacific CERT
3. Embedded Systems

۴. رجوع شود به:
'Malaysia's cybersecurity, forensic labs among most advanced in the world', Sun Daily, 27 May 2019, https://www.thesundaily.my/local/malaysia-s-cybersecurity-forensic-labs-among-mostadvanced-in-the-world-KM916936.

5. Forum of Incident Response and Security Teams
6. Internet Corporation for Assigned Names and Numbers (ICANN)
7. ASEAN Telecommunications and Information Technology Ministers' Meeting
8. Asia-Pacific Telecommunity

۹. رجوع شود به:
Cyber Security - Towards a Safe and Secure Cyber Environment, p. 53.

چندین سال است که مالزی فعالانه مباحث مربوط به امنیت بین‌المللی را در مجمع منطقه‌ای آسه‌آن (ARF)[1] مدیریت می‌کند. این کشور به‌همراه ژاپن و سنگاپور ریاست نشست بین‌جلساتی مجمع منطقه‌ای آسه‌آن در زمینه امنیت و استفاده از فناوری اطلاعات و ارتباطات[2] را نیز برعهده دارد. اهداف این نشست عبارتند از: ارزیابی نیازهای منطقه‌ای برای ظرفیت‌سازی درحوزه امنیت فناوری اطلاعات و ارتباطات و کمک به توسعه محیطی صلح‌آمیز، امن، آزاد و مشارکتی برای گسترش امنیت فناوری اطلاعات و ارتباطات در میان دولت‌های عضو مجمع منطقه‌ای آسه‌آن[3]. مالزی در سال ۲۰۱۵-۲۰۱۴ در گروه کارشناسان دولتی سازمان ملل متحد (GGE)[4] عضویت داشت. این گروه به اتفاق‌آرا و علی‌رغم دیدگاه‌ها و منافع بسیار متفاوت اعضای خود، گزارشی در مورد هنجارهای اختیاری احتمالی ارائه کرد[5]. شایان ذکر است که مالزی در اقدامات ظرفیت‌سازی منطقه‌ای نیز مشارکت داشته‌است؛ این اقدامات در راستای ترویج، شفاف‌سازی و همچنین اجرای هنجارهای یازده‌گانه گروه کارشناسان دولتی در جنوب شرق آسیا اجرا شده‌اند[6].

1. ASEAN Regional Forum
2. ARF Inter-Sessional Meeting on the Security and Use of Information and Communications Technology

۳. رجوع شود به:
Association of Southeast Asian Nations, 'Co-Chairs' Summary Report - 1st ASEAN Regional Forum Inter-Sessional Meeting on Security of and in the Use of Information and Communication Technologies', Kuala Lumpur, 25-26 April 2018, p. 2,
http:// aseanregionalforum.asean.org/wp-content/uploads/2019/01/ ANNEX-12.pdf.

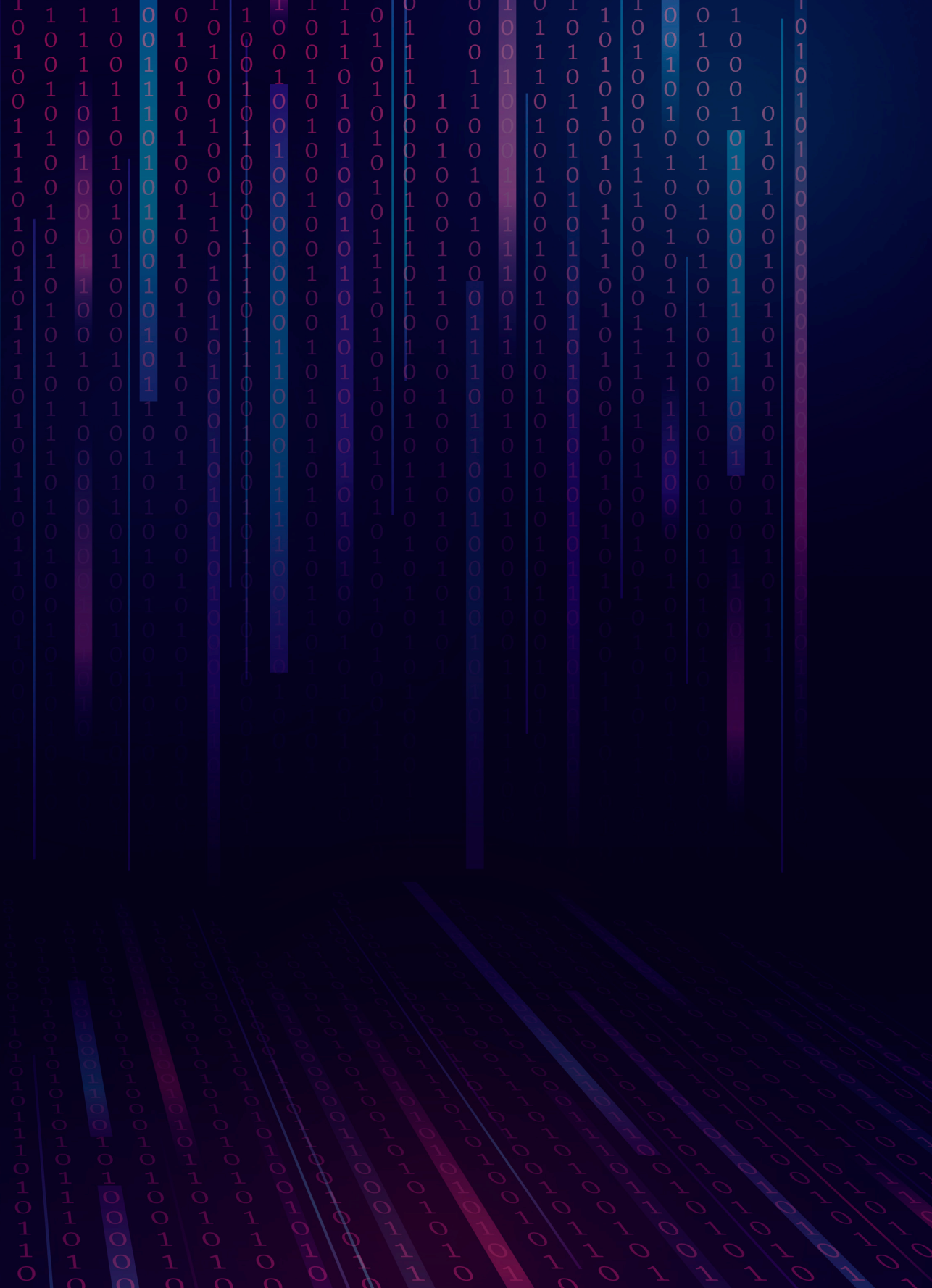
۴. رجوع شود به:
UN Office for Disarmament Affairs, 'Developments in the field of information and telecommunications in the context of international security',
https://www.un.org/disarmament/ict-security.

۵. رجوع شود به:
United Nations General Assembly, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', A/70/174, 22 July 2015, https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

۶. مقامات مالزی همراه با همتایان خود از سایر کشورهای عضو آسه‌آن در کارگاه‌های آموزشی مؤسسه سیاست راهبردی استرالیا (آوریل ۲۰۱۹) و دفتر امور خلع سلاح سازمان ملل متحد با همکاری سازمان امنیت سایبری سنگاپور (جولای ۲۰۱۹) شرکت کرده‌اند.

توانمندی‌های سایبری تهاجمی

به‌استثنای آرمان‌های بیان شده در سیاست دفاع ملی ۲۰۱۰ و سیاست دفاعی ۲۰۲۰، نشانه‌های کمی دال بر فعالیت مالزی در حوزه سایبری تهاجمی وجود دارد. مهم‌ترین رهنمودهای سیاسی این کشور حاکی از آن است که دولت مالزی استفاده از فضای سایبری برای پیشبرد برنامه توسعه اقتصادی را در دستورکار خود قرار داده‌است و انتظار می‌رود که این اولویت تغییر نکند. بنابراین، پیشرفت این کشور در جهت دستیابی به اهداف سایبری تهاجمی احتمالاً کند خواهد بود.



۱۵

ویتنام

ویتنام مجموعه‌ای از راهبردها در حیطه امنیت سایبری و به‌منظور تقویت قدرت ملی خود در فضای سایبری ازجمله در حوزه نظامی تدوین کرده‌است. در ویتنام ساختارهای حاکمیتی در حوزه سیاست سایبری تحت‌نظارت نظام سیاسی اقتدارگرای حزب کمونیست (CPV)[1] حاکم در این کشور قرار دارند. دولت این کشور تاکنون سیاست‌های متعددی اجرا کرده‌است که در رشد پایدار بخش فناوری اطلاعات و ارتباطات و همچنین پیشرفت چشمگیر در زمینه ساخت بسترهای دولت الکترونیک موثر بوده‌اند. با این حال، بسیاری از سازمان‌های دولتی به‌دلیل کمبود بودجه و همچنین کمبود شدید استعدادهای امنیت سایبری با مشکلات متعددی در تامین امنیت سایبری خود روبرو هستند. درواقع، به نظر می‌رسد نگرانی‌های حزب حاکم بابت تهدیدهای خرابکاری داخلی منجر به تغییراتی در تخصیص منابع مالی دولت می‌شود؛ به این معنی که احتمالاً دولت بخش محدودی از منابع مالی خود را صرف آموزش مهارت‌های سایبری فنی می‌کند و بیشتر آن را به امور تبلیغات ایدئولوژیکی و مدیریت افکار عمومی اختصاص می‌دهد که این مسأله خود موجب کاهش سرمایه‌گذاری در توانمندی‌های سایبری دفاعی و تهاجمی می‌شود. توانمندی‌های سایبری تهاجمی ویتنام نوظهور یا ضعیف هستند، اما گروهی مخفی و منتسب به دولت با نام مستعار تهدید مستمر پیشرفته ۳۲ یا به اختصار اِی‌پی‌تی ۳۲[2] در این کشور فعالیت دارد که قادر به اجرای حمله‌های سایبری نسبتاً پیشرفته‌ای است. درمجموع، ویتنام جزء قدرت‌های سایبری رده سوم است. البته این کشور دارای اهداف و ظرفیت‌های قابل‌توجهی در حوزه دیجیتال است که اگر بتواند توانایی‌های کلیدی خود در حیطه امنیت سایبری را تقویت کند، شرکت‌های فعال در زمینه فناوری اطلاعات و ارتباطات را تحت‌حمایت گیرد و سرمایه‌گذاری‌هایی در زمینه

1. Communist Party of Vietnam
2. Advanced Persistent Threat (APT32)

استفاده از فناوری‌های پیشرفته برای محافظت از زیرساخت‌های دیجیتال انجام دهد، خواهد توانست ظرفیت‌های خود را بالفعل سازد و به اهداف موردنظرش دست یابد.

راهبرد و مبنای نظری (دکترین)

ویتنام تا سال ۲۰۱۰ که اولین نقشه‌راه ملی خود تحت‌عنوان تصویب برنامه ملی توسعه امنیت اطلاعات دیجیتال[1] را منتشر کرد، قوانین و مقررات امنیت سایبری نسبتاً پراکنده‌ای داشت[2]. طرح مذکور جامع‌تر و بلندپروازانه‌تر از طرح‌هایی بود که اکثر کشورهای دیگر تا آن زمان تدوین کرده‌بودند. چهار هدف کلی این طرح جهت رفع ضعف‌های فنی و حقوقی کشور در حوزه امنیت اطلاعات عبارت بودند از: تامین امنیت زیرساخت‌های شبکه و اطلاعات؛ تضمین امنیت داده‌ها و برنامه‌ها؛ آموزش متخصصان امنیت سایبری و افزایش آگاهی عمومی در رابطه با امنیت اطلاعات؛ و تقویت چارچوب قانونی برای امنیت اطلاعات به‌ویژه در حوزه جرائم رایانه‌ای و رمزنگاری. در راستای پیشبرد این اهداف، دولت بودجه موردنیاز برای آموزش کارکنان سازمان‌های دولتی و تقویت امنیت اطلاعات در وزارت اطلاعات و ارتباطات (MIC)[3]، وزارت امنیت عمومی (MPS)[4]، کمیته رمزگذاری دولتی[5] و وزارت صنعت[6] را تامین کرد. ترویج تحقیق و توسعه نیز در این طرح موردتاکید زیادی قرار داشت.

1. Approving the National Planning on Development of Digital Information Security

۲. رجوع شود به:
Prime Minister's Decision No. 63/QD-TTg, 'Approving the National Planning on Development of Digital Information Security through 2020', 2010,
https://vanbanphapluat.co/decision-no-63-qd-ttg-approving-the-national planning-ondevelopment-of-digital-information-security-through-2020.

3. Ministry of Information and Communications
4. Ministry of Public Security
5. Government Cipher Committee
6. Ministry of Industry

در راستای تقویت نقشه‌راه ۲۰۱۰، دولت در سال ۲۰۱۶ اهداف جدیدی در قالب طرح امنیت اطلاعات شبکه[1] برای دوره ۲۰۲۰-۲۰۱۶ معرفی کرد[2]. این طرح بر ضرورت تحقیق و توسعه و همکاری دولت با شرکت‌های امنیت اطلاعات ویتنام ازطریق برون‌سپاری تاکید داشت و همزمان در پی برندسازی محصولات امنیت اطلاعات ساخت داخل نیز بود. انجمن‌های فناوری اطلاعات و ارتباطات ویتنام عاملان اصلی پیشبرد این ابتکار بودند[3]. این طرح همچنین توجه ویژه‌ای به ضرورت هماهنگی ملی در پاسخ به حوادث امنیتی داشت و در همین راستا، حداقل الزامات امنیتی در سامانه‌های ملی حائزاهمیت (زیرساخت‌های حیاتی و سامانه‌های ارتباطات دولتی حساس) را تعیین کرد. پیرو الزامات امنیتی مطرح شده در این طرح، شرکت‌های خصوصی موظف به رعایت مقررات جهت تامین امنیت شدند و عملکرد آن‌ها تحت‌نظارت/بازرسی مستمر قرار گرفت. شایان ذکر است که در این طرح اجرای رزمایش‌های امنیت سایبری توسط نهادهای دولتی و بخش خصوصی و نیز مشارکت آن‌ها در مجامع بین‌المللی نیز موردتاکید بود.

برای دولت ویتنام امنیت سایبری صرفا محدود به مسائل فنی حفاظت از شبکه‌ها نمی‌شود و نظارت بر محتوای سیاسی که این شبکه‌ها منتقل می‌کنند نیز در این مقوله قرار دارد. به‌عنوان مثال، قانون امنیت اطلاعات شبکه[4] که در نوامبر ۲۰۱۵ تصویب شد،

1. Network Information Security Plan

۲. رجوع شود به:
Prime Minister, 'Phê Duyệt Phương Hướng, Mục Tiêu, NhiệmVụ Bảo Dảm An Toàn Thông Tin Mạng Giai Doạn 2016-2020', 27 May 2016,
https://thuvienphapluat.vn/van-ban/Cong-nghe-thongtin/Quyet-dinh-898-QD-TTg phuong-huong-muc-tieu-nhiem-vubao-dam-an-toan-thong-tin-mang-2016-2020-313149.aspx.

۳. عاملان اصلی در ترویج ابتکار امنیت اطلاعات ویتنام عبارتند از: انجمن نرم‌افزار و خدمات فناوری اطلاعات ویتنام، انجمن پردازش اطلاعات ویتنام، انجمن اینترنت ویتنام، انجمن امنیت اطلاعات ویتنام و انجمن تجارت الکترونیک ویتنام.

4. Law on Network Information Security

ناظر بر این موضوع است[۱]. اگرچه تمرکز اصلی این قانون بر جنبه‌های فنی و مدیریتی جهت جلوگیری از دسترسی غیرمجاز به سامانه‌های فناوری اطلاعات و ارتباطات بود، اما محتوای آن به‌روشنی نشان می‌داد که سانسور و نظارت بر محتواهای سیاسی داخلی اولویت اصلی دولت است. این قانون کنترل مبادلات بین‌المللی در فضای سایبری را نیز ضروری می‌دانست و هرگونه فعالیت اطلاعاتی نهادهای ویتنامی و یا خارجی که از نظر دولت تهدیدی برای امنیت ملی محسوب شود را غیرقانونی می‌شمرد.

قانون امنیت سایبری[۲] که در ژوئن ۲۰۱۸ تصویب شد، بر حفاظت از امنیت ملی و تضمین نظم اجتماعی و ایمنی در فضای سایبری (ماده ۱)[۳] متمرکز بود و به‌وضوح از قانون ۲۰۱۵ سیاسی‌تر بود. این قانون برخلاف قانون ۲۰۱۵ شامل تعاریف گسترده‌ای در مورد محتواهای قابل‌قبول بود. به‌عنوان مثال، در ماده ۸ این قانون هرگونه تلاش برای «مخالفت با دولت» یا تحریف تاریخ ازطریق «انکار دستاوردهای انقلابی» اکیداً ممنوع اعلام شده‌بود. بومی‌سازی داده‌ها[۴] برای همه شرکت‌های داخلی و خارجی فعال در ویتنام یکی از بحث‌برانگیزترین مولفه‌های قانون ۲۰۱۸ بود که شرکت‌های خارجی آن را نقض محرمانگی تجاری و حقوق مالکیت معنوی خود تلقی می‌کردند[۵].

۱. رجوع شود به:
National Assembly, 'Luật an toàn thông tin mạng', 86/2015/QH13, 19 November 2015. For an official translation,
https://vanbanphapluat.co/law-no-86-2015-qh13-on-cyberinformationsecurity-2015.
2. Cyber Security Law
۳. رجوع شود به:
National Assembly, 'Luật An Ninh Mạng', 24/2018/QH14,12 June 2018,
https://luatvietnam.vn/an-ninh-quoc-gia/luat-an-ninh-mang-2018-164904-d1.html.
ترجمه انگلیسی- غیرسمی- را در لینک زیر می‌توانید مشاهده کنید.
https://data.allens.com.au/pubs/pdf/priv/cupriv22jun18.pdf.
۴. رجوع شود به:
Thomas J. Treutler and Giang Thi Huong Tran, 'Update on the Implementation of Vietnam's New Cybersecurity Law and Status of Implementing Decrees', Tilleke & Gibbins, 18 December 2019,
https://www.lexology.com/library/detail.aspx?g=8833627c-e189-4d60-a472-6ee742cc38fd.
۵. قانون بومی‌سازی داده‌ها در مورد آن دسته از شرکت‌های خارجی اعمال می‌شود که خدمات مخابراتی، ذخیره‌سازی و به‌اشتراک‌گذاری داده‌ها، تجارت الکترونیک، رسانه‌های اجتماعی و بازی‌های الکترونیکی برخط ارائه می‌دهند.

قانون دفاع ملی[1] که در سال ۲۰۱۸ ابلاغ شد، اولین سند دولتی رسمی است که دیدگاه ویتنام را در مورد به‌کارگیری توانمندی‌های سایبری در حوزه نظامی بیان می‌کند[2]. این قانون «جنگ اطلاعاتی» را به‌عنوان فعالیت‌ها و اقداماتی برای از کار انداختن سامانه‌های اطلاعاتی دشمن و حفاظت از سامانه‌های اطلاعاتی ویتنام تعریف کرده‌است و آن را ذیل مفهوم دفاع ملی همگانی[3] قرار داده‌است (ماده ۲) و به‌طور ویژه از جنگ سایبری و جنگ اطلاعاتی نام برده‌است. در همان سال، کمیته اجرایی حزب کمونیست (معروف به پولیتبورو)[4] قطعنامه‌ای مشتمل بر راهبردی جدید برای حفاظت از وطن در فضای سایبری[5] صادر کرد[6] که هدف آن پاسخ همگانی و با محوریت نیروهای مسلح به رویدادهای سایبری و ادغام دفاع سایبری با ضدحمله بود[7].

در یکی از گزارش‌های سیاست دفاعی در سال ۲۰۱۹ نیز فضای سایبری پنجمین حوزه عملیاتی -در کنار زمین، هوا، دریا و فضا- تعریف شده‌است که دفاع از حاکمیت ملی ویتنام در آن انجام می‌شود[8].

1. National Defense Law

۲. رجوع شود به:
National Assembly, 'Luật Quốc Phòng', 22/2018/QH14, 8 June 2018, https://thuvienphapluat.vn/van-ban/bo-may-hanhchinh/ Luat-quoc-phong-340395.aspx.

3. All-People National Defense
4. Politburo
5. Strategy for the Homeland Protection in Cyberspace

۶. رجوع شود به:
Politburo Resolution 29NQ/TW dated 25 July 2018. VuVan Hien, 'Enhancing the homeland protection under the Party's platform', National Defense Journal, 10 November 2020, http://tapchiqptd.vn/en/theory-and-practice/enhancingthe-homeland-protection-under-the-partys-platform/16265. html;

Ngo Xuan Lich, 'The whole military resolves to successfully fulfil the military-defense tasks in 2019', National Defense Journal, 4 January 2019, http://tapchiqptd.vn/en/theoryand-practice/the-whole-military-resolves-to-successfullyfulfil-the-militarydefence-tasks-in-2019/13088.html.

۷. رجوع شود به:
Ngoc Thuy Tran, 'Những Vấn Dề về Bảo vệ Tổ Quốc Trên Không Gian Mạng', Quan khu 7, 3 October 2019, https://baoquankhu7.vn/nhung-van-de-ve-bao-ve-to-quoc-trenkhong-gian-mang--1919396 49-0015044s34010gs.

۸. رجوع شود به:
Ministry of National Defense, '2019 Viet Nam National Defense', October 2019, p. 52, http://news.chinhphu.vn/Uploaded_VGP/phamvanthua/20191220/2019VietnamNationa lDefence.pdf.

حکمرانی، فرماندهی و نظارت

کمیته اجرایی حزب کمونیست ویتنام مسئولیت تنظیم سیاست‌های امنیتی این کشور ازجمله در حوزه فضای سایبری را برعهده دارد. در قیاس با اغلب کشورها، نیروهای مسلح ویتنام ازطریق ستاد فرماندهی سایبری خود نقش محوری‌تری در سانسور و نظارت سیاسی ایفا می‌کنند و بنابراین، کمیسیون نظامی مرکزی[1] حزب کمونیست عالی‌ترین نهاد تصمیم‌گیری ویتنام در حوزه امنیت ملی و احتمالاً مرجع اصلی فرماندهی و حاکمیت سیاست فضای سایبری این کشور قلمداد می‌شود. سایر نهادهای نزدیک به رهبری حزب مانند سازمان تبلیغات سیاسی[2] نیز در رسیدگی به مسائل امنیتی حساس نقش دارند.

سیاست‌های سایبری ابلاغ‌شده توسط رهبری حزب کمونیست عمدتاً به وسیله وزارت اطلاعات و ارتباطات، وزارت امنیت عمومی و وزارت دفاع ملی (MND)[3] اجرا می‌شوند. وزارت اطلاعات و ارتباطات مسئولیت هماهنگی جنبه‌های فنی امنیت سایبری و سیاست‌های گسترده برای مدیریت محتوا را نیز برعهده دارد.[4] تیم پاسخ فوری رایانه‌ای ویتنام (VNCERT)[5] در وزارت اطلاعات و ارتباطات نیز در زمینه هماهنگ‌سازی فعالیت‌های ملی پاسخ به حوادث[6] و همزمان جمع‌آوری و به‌اشتراک‌گذاری اطلاعات مربوط به حوادث و بدافزارها، هدایت عملیات‌های سایبری

1. Central Military Commission
2. Propaganda Department
3. Ministry of National Defense

۴. رجوع شود به:

National Assembly, 'Luật An Ninh Mạng', 24/2018/QH14.

5. Vietnam Computer Emergency Response Team .

۶. رجوع شود به:

'VNCTERT/CC Trung tâm Ứng cứu khẩn cấp không gianmạng Việt Nam', http://vncert.gov.vn.

و ارزیابی توانایی دفاع سایبری نهادهای دولتی و خصوصی فعالیت دارد[۱]. مرجع امنیت اطلاعات (AIS)[۲] نیز وظیفه تدوین قوانین و سیاست‌های مربوط به امنیت اطلاعات و انجام اقدامات فنی لازم برای حفاظت از زیرساخت‌های اطلاعاتی حیاتی را برعهده دارد[۳]. مرکز ملی احراز هویت الکترونیکی[۴] هم به ایمن‌سازی تراکنش‌های الکترونیکی ازطریق امضای دیجیتال و ارائه انواع خدمات احراز هویت ایمن می‌پردازد[۵].

وزارت امنیت عمومی دارای دو سازمان امنیت سایبری با عناوین سازمان امنیت سایبری و پیشگیری از جرائم مبتنی بر فناوری پیشرفته (A05)[۶] و سازمان امنیت اطلاعات و ارتباطات (A87)[۷] است. سازمان امنیت سایبری و پیشگیری از جرائم مبتنی بر فناوری پیشرفته وظیفه پیشگیری از جرائم سایبری مانند شرط‌بندی‌های برخط و انتشار اطلاعات نادرست را برعهده دارد و با سازمان‌های تحقیقاتی خارجی در زمینه پرونده‌های مربوط به مجرمان سایبری خارجی همکاری می‌کند. این سازمان در مورد قوانین و سیاست‌های امنیت سایبری نیز مشاوره می‌دهد و راه‌حل‌های مبتنی بر فناوری پیشرفته را با هدف افزایش ظرفیت دولت برای مقابله با جرائم سایبری ترویج

---

۱. رجوع شود به:
Ministry of Information and Communications, 'Cybersecurity Emergency Response Center established', 14 October 2019,
https://english.mic.gov.vn/Pages/TinTuc/139865/Cybersecurity-Emergency-Response-Center established.html.

2. Authority of Information Security

۳. رجوع شود به:
Ministry of Information and Communications, 'Authority of Information Security', 19 July 2020,
https://english.mic.gov.vn/pages/thongtin/114301/Authority-of-Information-Security.html.

4. National Electronic Authentication Centre

۵. رجوع شود به:
Ministry of Information and Communications, 'The National Electronic Authentication Centre', 19 July 2020,
https://english. mic.gov.vn/pages/thongtin/114304/NEAC.html.

6. Cyber Security and High-tech Crime Prevention

7. Information Security and Communications

می‌دهد[۱]. سازمان امنیت اطلاعات و ارتباطات نیز در مورد مسائل مربوط به سیاست، جنبه‌های حقوقی امنیت در زمینه‌های فرهنگ، اطلاعات و ارتباطات و همچنین مقابله با انتقاد از حزب کمونیست حاکم و افشای اسرار دولتی به نهادهای ذی‌ربط مشاوره ارائه می‌کند[۲].

در وزارت دفاع ملی نیز دو سازمان امنیت سایبری با عناوین سازمان فرماندهی سایبری[۳] و سازمان رمزنگاری دولتی[۴] وجود دارد. سازمان فرماندهی سایبری که در آگوست ۲۰۱۷ با هدف ارتقای سازمان سابق فناوری اطلاعات[۵] تأسیس شد، به رئیس ستاد کل[۶] گزارش می‌دهد که آن نیز تابع وزیر دفاع (یکی از اعضای کمیته اجرایی) است. این سازمان شامل ستاد فرماندهی، سه تیپ، مراکز سنجش و یک مرکز داده است و وظایف متعددی ازجمله انجام امور سیاسی، رسیدگی به مسائل فنی و لجستیک و اجرای عملیات‌های سایبری حرفه‌ای را برعهده دارد[۷]. سازمان رمزنگاری دولتی نیز مسئولیت حفاظت از شبکه‌های رمزگذاری شده کشور و همچنین تحقیق و توسعه در زمینه فناوری‌های مربوطه را برعهده دارد[۸].

---

۱. رجوع شود به:
'Chủ động, quyết liệt trong phòng, chống tội phạm trên không gian mạng', Thua Thien Hue Provincial Party Committee, 21 January 2020,
https://tinhuytthue.vn/tin-tuc-trong-nuoc/kh-cn/chu-dongquyet-liet-trong-ph-ograve ngchong-toi-pham-trecirc-n-kh-ocirc-ng-gian-mang.htm.

۲. رجوع شود به:
'Cục An ninh Văn hóa, thông tin, truyền thông báo công dâng Bác', Tiền Phong, 5 May 2018,
https://www.tienphong. vn/xa-hoi/cuc-an-ninh-van-hoa-thong-tin-truyen-thong-baocong-dang-bac-1269610.tpo.

3. Cyber Command
4. Government Cryptographic Agency
5. Information Technology Department
6. Chief of the General Staff

۷. رجوع شود به:
Ministry of National Defense, '2019 Viet Nam National Defense'.

۸. همان؛ ص ۷-۶۶.

ارتش خلق ویتنام (VPA)[1] دارای واحد سایبری ویژه‌ای به نام نیروی ۴۷ [2] است که وظیفه حفاظت از حزب حاکم در برابر «اخبار نادرست» و همچنین انتشار تبلیغات سیاسی دولت را برعهده دارد. ارتش خلق دارای کارگروه ویژه‌ای با بیش از ۱۰۰۰۰ نفر[3] عضو است که در زمینه انضباط ایدئولوژیک و جنگ اطلاعاتی آموزش دیده‌اند[4]. اعضای این کارگروه اغلب در رسانه‌های اجتماعی ازجمله فیس‌بوک و یوتیوب از انتشار اطلاعات خصمانه قبل از رویدادهای مهم سیاسی جلوگیری می‌کنند.

درمجموع باید گفت به‌غیر از مشاهداتی دال بر اطاعت بی‌چون‌وچرا از زنجیره فرماندهی، اطلاعات چندانی درباره ساختار حاکمیت سایبری ویتنام دردسترس عموم قرار ندارد تا بتوان برپایه آن‌ها ارزیابی معتبری از عملکرد حاکمیت و فرماندهی نیروهای سایبری آن داشت.

توانمندی‌های محوری در زمینه اطلاعات سایبری

توانمندی‌های حوزه اطلاعات سایبری ویتنام در وزارت امنیت عمومی، وزارت دفاع ملی و وزارت اطلاعات و ارتباطات آن تجمیع شده‌اند. اداره کل اطلاعات[5] و اداره کل امنیت

1. Vietnamese People's Army
2. Force 47

۳. رجوع شود به:
Hơn 10.000 người trong 'Lực lượng 47' dấu tranh trên mạng', Tuổi Trẻ, 25 December 2017, https://tuoitre.vn/hon-10-000-nguoi-trong-luc-luong-47-dau-tranh-trenmang-20171225150602912.htm.
در این منبع مشخص نشده‌است که آیا اعضای این گروه فقط به نظارت سیاسی می‌پردازند یا عملیات سایبری دیگری نیز انجام می‌دهند.

۴. رجوع شود به:
Maj. Gen., Associate Prof. Nguyen Hung Oanh, 'The Political Officer College grasps and executes the Politburo's Resolution 35', National Defense Journal, 16 October 2019, http://tapchiqptd.vn/en/research-and discussion/thepolitical-officer-college-grasps-and-executes-the-politburosresolution-35/14514.html.

5. General Department of Intelligence

(GDS)[1] در وزارت امنیت عمومی در زمینه جمع‌آوری اطلاعات داخلی و خارجی فعالیت دارند. واحد تخصصی A42 در اداره کل امنیت نیز وظیفه کنترل تماس‌های تلفنی، ایمیل‌ها و اینترنت ازطریق تجهیزات خریداری شده از فروشندگان خارجی فعالیت دارد[2]. علاوه بر این موارد، سازمان امنیت سایبری و پیشگیری از جرائم مبتنی بر فناوری پیشرفته زیرمجموعه وزارت امنیت عمومی (A05 - به بخش قبل رجوع شود) در زمینه تجهیزات فنی نوین سرمایه‌گذاری کرده‌است[3] و به برنامه امنیت دولتی[4] شرکت مایکروسافت پیوسته‌است تا بدین‌ترتیب بتواند آگاهی خود در زمینه تهدیدات سایبری را افزایش دهد[5].

به‌همین‌ترتیب، اداره کل اطلاعات نظامی[6] در وزارت دفاع ملی مسئولیت جمع‌آوری اطلاعات داخلی و خارجی را برعهده دارد. ستاد فرماندهی سایبری نیز اگرچه نهاد اطلاعاتی محسوب نمی‌شود، اما به احتمال زیاد دارای توانمندی‌های اطلاعاتی سایبری برپایه ظرفیت اطلاعات سیگنالی ارتش خلق است که کارایی آن در طول جنگ ویتنام به اثبات رسیده‌است. سازمان رمزنگاری دولتی که یکی دیگر از زیرمجموعه‌های وزارت دفاع ملی است، بخش بسیار مهمی از توانمندی‌های اطلاعات سایبری ویتنام به‌شمار می‌رود و مسئولیت تضمین امنیت سایبری رهبران نظامی و غیرنظامی این کشور را برعهده دارد.

1. General Department of Security

۲. رجوع شود به:
Carlyle A. Thayer, 'The Apparatus of Authoritarian Rule in Vietnam', Critical Studies of the Asia Pacific Series, vol. 31, no. 2, 2014, pp. 279-83, https://link.springer.com/chapter/10.1057/9781137347534_7#aboutcontent.

۳. رجوع شود به:
Hai Thanh Luong et al., 'Understanding Cybercrimes in Vietnam: From Leading-Point Provisions to Legislative System and Law Enforcement', International Journal of Cyber Criminology,vol. 13, no. 2, 2019, https://www.cybercrimejournal.com/LuongetalVol13Issue2IJCC2019.pdf.

4. Government Security Program

۵. رجوع شود به:
'VN to join Microsoft's network security protection programme', Viêt Nam News, 20 December 2019, https://vietnamnews.vn/society/570139/vn-to-join-microsofts-network-securityprotection-programme.html.

6. General Department of Military Intelligence

وزارت اطلاعات و ارتباطات علاوه‌بر ایفای نقش اصلی خود یعنی هماهنگی تمامی سازمان‌های دولتی فعال در حوزه امنیت سایبری، از توانمندی‌های اطلاعاتی سایبری نیز برخوردار است. به‌عنوان مثال، مرکز ملی نظارت بر امنیت سایبری (NCSC)[1] زیرمجموعه وزارت اطلاعات و ارتباطات با همکاری تیم پاسخ فوری رایانه‌ای ویتنام و مراکز کنترل امنیت سایبری استان‌ها[2] در زمینه مدیریت فضای سایبری کشور و تهدیدهای احتمالی در کمین آن فعالیت دارد.

گروهی که شرکت‌های امنیت سایبری آن را با نام اِی‌پی‌تی ۳۲ (APT32)[3] می‌شناسند، توانمندی‌های اطلاعات سایبری ویتنام را تا حدودی تقویت کرده‌است. این گروه در ظاهر نهادی غیردولتی است، اما شواهد حاکی از آن هستند که ارتباطات غیررسمی با دولت دارد. شرکت‌های امنیت سایبری ایالات متحده مدارک زیادی درباره بسیاری از عملیات‌های جاسوسی سایبری این گروه به‌دست آورده‌اند و به نظر می‌رسد این گروه کاملاً حرفه‌ای است، چراکه شرکت‌های خارجی، آسه‌آن و نهادهای دولتی چین (ازجمله نهادهایی که با همه‌گیری کوید-۱۹ مقابله می‌کردند) اهداف عملیات‌های آن بوده‌اند. درمجموع، با توجه به کمبود نیروی ماهر در حوزه فناوری اطلاعات و ارتباطات ویتنام می‌توان گفت توانمندی‌های این کشور در زمینه اطلاعات سایبری ضعیف هستند[4].

1. National Cyber Security Monitoring Centre
2. Cyber Security Control Centers

رجوع شود به:
Le Linh, 'Xây dựng trung tâm diều hành an ninh mạng dầu tiên cả nước', Diễn Dàn, 17 May 2019, https://enternews.vn/xay-dung-trung-tam-dieu-hanh-an-ninh-mang-dau-tien-canuoc-150441.html.

۳. رجوع شود به:
Nick Carr, 'Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations', FireEye, 14 May 2017, https://www.fireeye.com/blog/threatresearch/2017/05/cyber-espionage-apt32.html.

۴. رجوع شود به:
Tran Luu, 'Vietnam determines to develop digital economy', Saigon Online, 4 February 2020, https://sggpnews.org.vn/science_technology/vietnam-determines-to-develop-digitaleconomy-85491.html.

توانمندی و وابستگی سایبری

کمیته اجرایی حزب کمونیست ویتنام در سال ۲۰۱۹ اعلام کرد اقتصاد دیجیتال ویتنام در سال ۲۰۱۸ تنها ۱۵ درصد از تولید ناخالص داخلی آن را تشکیل داده‌است و بنابراین، سهم آن تا سال ۲۰۲۵ باید به ۲۰ درصد و تا سال ۲۰۳۰ به حداقل ۳۰ درصد[۱] افزایش یابد[۲]. شایان ذکر است که دستیابی به این اهداف صرفاً با اصلاح سیاست‌های اصلی کشور و سرمایه‌گذاری کلان می‌تواند میسر شود. در همین راستا، دولت ویتنام اجرای ابتکاراتی مانند برنامه ملی تحول دیجیتال که در سال ۲۰۲۰ آغاز شد[۳] و همچنین پروژه‌های دولت الکترونیک را در اولویت قرار داده‌است[۴] و ادعا می‌کند حوزه فناوری اطلاعات و ارتباطات این کشور چندین سال (دوره دقیق ذکر نشده‌است) شاهد نرخ رشد سالانه ۳۰ درصدی

۱. رجوع شود به:
Bui Thanh Truan, 'Difficulties and challenges in the development of digital economy in Vietnam', Political Theory, 25 August 2020,
http://lyluanchinhtri.vn/home/en/index.php/practice/item/723-difficulties-and-challenges-in-the-development-of-digitaleconomy-in-vietnam.html.

۲. رجوع شود به:
Chinese Academy of Information and Communications Technology, 'Quánqiú shùzì jīngjì xīn túj'ing (2019 nián)', October 2019, p. 12,
http://www.caict.ac.cn/kxyj/qwfb/bps/201910/P020191011314794846790.pdf.

3. National Digital Transformation Program

رجوع شود به:
Prime Minister, 'Introducing Program for National Digital Transformation by 2025 with Orientations Towards 2030', Decision 749/QD-TTg, 3 June 2020,
https://vanbanphapluat.co/decision-749-qd-ttg-2020-introducing program-for-nationaldigital-transformation.

در این برنامه دستیابی به اهداف زیر تا سال ۲۰۲۳ تصریح شده‌است: افزایش سهم اقتصاد دیجیتال از تولید ناخالص داخلی به ۳۰ درصد؛ تحول دیجیتال در بخش دولتی به‌طوری‌که ویتنام به یکی از چهار کشور برتر آسه‌آن در رتبه‌بندی دولت الکترونیک سازمان ملل تبدیل شود؛ پوشش سراسری شبکه تلفن همراه نسل پنجم و فراهم کردن دسترسی به اینترنت پهن‌باند برای کل جمعیت کشور.

۴. رجوع شود به:
Samaya Dharmaraj, 'Vietnam Committed to Supporting its Digital Economy with E-government', OpenGov Asia, 28 November 2019,
https://www.opengovasia.com/vietnamcommitted-to-supporting-its-digital-economy-with-e- government.

بوده‌است[۱]. با این حال، ویتنام تقریباً در تمام شاخص‌های آمادگی فناوری اطلاعات و ارتباطات پس از مالزی و بسیار عقب‌تر از سنگاپور قرار دارد و تنها اندکی جلوتر از اندونزی است[۲]. البته ضریب نفوذ اینترنت در این کشور در سال ۲۰۲۰ به ۷۰ درصد رسید[۳] و بازار تجارت الکترونیک آن پس از اندونزی و تایلند سومین بازار بزرگ در جنوب شرقی آسیا بود[۴]. اگرچه ویتنام به پیشرفت‌های قابل‌توجهی در زمینه دیجیتال‌سازی دست یافته‌است، اما هنوز راه زیادی تا تحول دیجیتال در پیش دارد. به‌عنوان مثال، تنها بخش کوچکی از کل پرداخت‌ها در این کشور بدون پول نقد انجام می‌شوند و حتی در معاملات تجارت الکترونیک نیز روش‌های پرداخت نقدی در زمان تحویل طرفدار بیشتری دارند[۵].

ویتنام در رتبه‌بندی ۵۰ کشور برتر جهان براساس مشارکت در دو کنفرانس معتبر هوش مصنوعی در سال ۲۰۲۰ عملکرد بسیار خوبی داشته‌است و در رده بیست‌وهفتم یعنی بالاتر از مالزی و تایلند-اما پس از سنگاپور-قرار گرفته‌است[۶]. به‌همین‌ترتیب، در

---

۱. رجوع شود به:
Ministry of Information and Communications, 'VN's IT industry maintains growth momentum', 25 December 2019,
https://english.mic.gov.vn/Pages/TinTuc/140438/VN-s-ITindustry-maintains-growth-momentum.html.

۲. رجوع شود به:
George Ingram, 'Development in Southeast Asia: Opportunities for donor collaboration', Brookings Center for Sustainable Development, December 2020, pp. 31-2,
https://www.brookings.edu/wpcontent/uploads/2020/12/Development-Southeast-Asia-Ch2-Digital.pdf.

۳. رجوع شود به:
Simon Kemp, 'Digital 2020: Vietnam', DataReportal, 18 February 2020,
https://datareportal.com/reports/digital-2020-vietnam.

۴. رجوع شود به:
'How can Vietnam's e-commerce players foster greater market growth?', Tech Wire Asia, 3 February 2020,
https://techwireasia.com/2020/02/how-can-vietnams-e-commerce-players-fostergreater-market-growth.

۵. رجوع شود به:
'Cashless payment remains low in Vietnam: CIEM', VietnamPlus, 24 June 2019,
https://en.vietnamplus.vn/cashlesspayment-remains-low-in-vietnam-ciem/154911.vnp.

۶. رجوع شود به:
Gleb Chuvpilo, 'AI Research Rankings 2020: Can the United States Stay Ahead of China?', 21 December 2020,
https://chuvpilo.medium.com/ai-research-rankings-2020-can-theunited-states-stay-ahead-of-china-61cf14b1216.

رتبه‌بندی ۱۰۰ شرکت برتر جهانی در زمینه تحقیقات هوش مصنوعی در سال ۲۰۲۰ نیز نشان داده شد که اگرچه شرکت‌های آمریکایی و چینی بخش اعظم این شرکت‌های برتر را تشکیل می‌دهند، اما یکی از شرکت‌های تحقیقاتی هوش مصنوعی ویتنام به نام VinAI نیز توانسته‌است در جایگاه سی‌ودوم قرار گیرد[۱]. این شرکت که بنیان‌گذار آن یکی از کارمندان سابق شرکت گوگل دیپ‌مایند[۲] است، خدمات کاربردی در زمینه هوش مصنوعی ارائه می‌دهد و اولین آزمایشگاه تحقیقاتی ویتنام محسوب می‌شود که در حوزه‌هایی مانند یادگیری ماشینی و یادگیری عمیق فعالیت می‌کند[۳]. ویتنام تاکنون فناوری هوش مصنوعی را در بخش‌هایی مانند مراقبت‌های بهداشتی، آموزش، حمل‌ونقل، کشاورزی و تجارت الکترونیک به‌کار گرفته است، اما درمجموع هنوز در مراحل اولیه رشد و توسعه است[۴]. دولت ویتنام در ژانویه سال ۲۰۲۱ راهبردی ده‌ساله را برای تحقیق و توسعه در زمینه هوش مصنوعی منتشر کرد که هدف از آن قرار گرفتن ویتنام در میان ۵۰ کشور برتر جهان تا سال ۲۰۳۰ بود[۵].

بخش قابل‌توجهی ازشبکه‌های مخابراتی ویتنام و به‌عبارت دیگر حدود ۷۵ درصد از تجهیزات موردنیاز مالکیت ملی دارند و دولت امیدوار است که تا سال ۲۰۲۲ کل

---

۱. همان.

2. Google DeepMind

۳. رجوع شود به:
'Who We Are - The First AI Research Lab in Vietnam with a Focus on Fundamental Research', VinAI Research, https://www.vinai.io/about-us.

۴. رجوع شود به:
'Vietnam Prioritises Artificial Intelligence Development', Star, 9 September 2019, https://www.thestar.com.my/business/smebiz/2019/09/09/vietnam-prioritises-artificialintelligence-development.

۵. رجوع شود به:
'Vietnam strives to enter world's Top 50 in terms of AI by 2030', VietnamPlus, 28 January 2021, https://en.vietnamplus.vn/vietnam-strives-to-enter-worlds-top-50-in-terms-ofai-by-2030/195485.vnp.

تجهیزات مخابراتی را ازطریق تولید داخلی تامین کند[۱]. شرکت مخابراتی ویتل[۲] متعلق به ارتش عضو کنسرسیومی است که کابل زیردریایی پرقدرتی با ظرفیت بیش از ۱۴۰ ترابایت بر ثانیه ترافیک را می‌سازد. این کابل به‌عنوان بخشی از پروژه کابل مستقیم آسیا[۳] توانسته‌است چین (هنگ‌کنگ و گوانگ‌دونگ[۴])، ژاپن، فیلیپین، سنگاپور، تایلند و ویتنام را به‌هم وصل کند و قرار است که تا پایان سال ۲۰۲۲ تکمیل شود[۵]. شرکت ویتل توانسته‌است فناوری نسل پنجم را نیز با موفقیت به‌کار گیرد[۶].

لازم به ذکر است که شرکت «گروه پست و مخابرات ویتنام» (VNPT)[۷] نیز محصولات فناورانه خود را به بیش از ۳۰ کشور صادر می‌کند[۸]. این شرکت دارای دو ماهواره ارتباطی با نام‌های VINSAT-1 و VINSAT-2 است[۹]. علاوه بر این موارد، ویتنام دارای دو ماهواره

---

۱. رجوع شود به:
'Việt Nam nhờ Mỹ kiểm định thiết bị 5G do Việt Nam sản xuấtdể có dủ khả năng vào thị trường Mỹ', ICT News, 21 January 2020,
https://ictnews.vietnamnet.vn/cuoc-song-so/viet-namnho-my-kiem-dinh-thiet-bi-5g-do-viet-nam-san-xuat-de-codu-kha-nang-vao-thi-truong-my-40145.html.

2. Viettel
3. Asia Direct Cable Project
4. Guangdong

۵. رجوع شود به:
Ministry of Information and Communications, 'Viettel among investors of new high-speed under-sea cable ADC', 22 June 2020,
https://english.mic.gov.vn/Pages/TinTuc/142715/Viettel-amonginvestors-of-new-high-speed- under-sea-cable-ADC.html.

۶. رجوع شود به:
Leo Kelion, 'Giới chuyên gia ngạc nhiên trước tuyên bố của Viettel về mạng 5G', BBC News Vietnamese, 21 January 2020,
https://www.bbc.com/vietnamese/vietnam-51190570.

7. Vietnam Posts and Telecommunications Group

۸. رجوع شود به:
'Vietnamese telecom giants on race of exporting telecom equipments', Xinhua, 24 February 2017,
http://www.xinhuanet.com//english/2017-02/24/c_136082932.htm.

۹. رجوع شود به:
Union of Concerned Scientists, 'UCS Satellite Database', updated 1 January 2021,
https://www.ucsusa.org/resources/satellite-database.

رصد زمین است که توسط مرکز ملی فضایی ویتنام (VNSC)[1] و موسسه فناوری فضایی[2] وابسته به آکادمی علم و فناوری ویتنام[3] مدیریت می‌شوند. با این حال، صنعت فضایی این کشور به‌شدت به مساعدت و سرمایه‌گذاری‌های خارجی متکی است. به‌عنوان مثال، کارشناسان ژاپنی در ساخت یکی از ماهواره‌های رصد زمین ویتنام به نام اژدهای کوچک (MicroDragon) مشارکت داشتند که در سال ۲۰۱۹ از ژاپن پرتاب شد[4]. هند نیز با سازمان ملی سنجش از دور ویتنام[5] در زمینه ساخت ایستگاه ردیابی و دورسنجی-دارای کاربردهای نظامی-همکاری کرده‌است[6].

امنیت و تاب‌آوری سایبری

بیش از یک دهه است که ویتنام در حال تهیه مجموعه‌ای دقیق از سازوکارها، سیاست‌ها و قوانین در حوزه امنیت سایبری ملی است. اگرچه تلاش‌های ویتنام تا حدودی موثر بوده‌است، اما هنوز راه زیادی پیش‌رو دارد. گزارش شرکت مایکروسافت در سال ۲۰۲۰ حاکی از آن است که این کشور در مقایسه با دیگر کشورهای آسیا و اقیانوسیه بالاترین میزان حملات باج‌افزار را تجربه کرده و یکی از سه کشور منطقه با بیشترین

1. Vietnam National Space Centre
2. Space Technology Institute
3. Vietnam Academy of Science and Technology

۴. رجوع شود به:
'Vietnam's MicroDragon Earth Observation Satellite Successfully Launched From Japan', SpaceWatch Asia Pacific, January 2019,
https://spacewatch.global/2019/01/vietnamsmicrodragon-earth-observation-satellite- successfully-launched-from-japan.

5. National Remote Sensing Department

۶. رجوع شود به:
Nandini Sarma, 'Southeast Asian Space Programs: Capabilities, challenges and collaborations', Observer Research Foundation, 7 March 2019,
https://www.orfonline.org/research/southeast-asian-space-programmes-capabilitieschallenges -collaborations-48799/#_ednref12.

حملات بدافزار بوده‌است[۱]. علاوه‌بر این، ویتنام در سال ۲۰۲۰ رتبه ششم جهان در زمینه دانلود ناخواسته کدهای مخرب داشته‌است[۲].

مرکز ملی نظارت بر امنیت سایبری (NCSC)[۳] که یکی از زیرمجموعه‌های مرجع امنیت اطلاعات ویتنام است، در سال ۲۰۱۸ در واکنش به تهدیدهای سایبری فزاینده تأسیس شد. این مرکز بر پشتیبانی و نظارت بر امنیت سایبری همه نهادهای دولتی و خصوصی، ارائه هشدارهای اولیه در برابر حملات سایبری و به‌اشتراک‌گذاری اطلاعات با سازمان‌های داخلی و بین‌المللی متمرکز است. این مرکز با مشارکت ائتلافی از شرکت‌های امنیت اطلاعات موفق به راه‌اندازی سیستم اشتراک‌گذاری اطلاعات و نظارت بر امنیت شده‌است که وزارتخانه‌های دولت مرکزی را به ادارات استانی متصل می‌کند[۴]. به‌عنوان مثال، این مرکز با همکاری وزارت اطلاعات و ارتباطات و وزارت امنیت عمومی در سال ۲۰۲۰ موفق به مهار نرم‌افزار جاسوسی VN84App شد که کاربران گوشی‌های هوشمند را هدف قرار می‌داد[۵].

۱. رجوع شود به:
M. Anh, 'Việt Nam là quốc gia có tỷ lệ nhiễm mã độc tốngtiền cao nhất khu vực', Doanh nhân, 24 June 2020, https://doanhnhansaigon.vn/it/viet-nam-la-quoc-gia-co-ty-le-nhiemma-doc-tong-tien-cao-nhat-khu-vuc-1099286.html.

۲. رجوع شود به:
Microsoft, 'Microsoft Security Endpoint Threat Summary 2019', June 2020, https://3er1viui9wo30pkxh1v2nh4wwpengine.netdna-ssl.com/wp-content/uploads/prod/sites/570/2020/02/Microsoft-Security-Endpoint-Threat-Summary-2019-Updated.pdf.

۳. رجوع شود به:
'Giới thiệu về NCSC', National Cyber Security Monitoring Centre, https://khonggianmang.vn/intro.

۴. رجوع شود به:
Phan Nghia, 'Vietnam introduces new information security system to facilitate e-governance', VnExpress, 29 November 2019, https://e.vnexpress.net/news/news/vietnam-introduces-new-informationsecurity-system-to-facilitate-e-governance-4019639.html.

۵. رجوع شود به:
Bao Lam and Chau An, 'Data stealing spyware rears head in Vietnam', VnExpress, 23 June 2020, https://e.vnexpress.net/news/news/data-stealing-spyware-rears-head-invietnam-4119828.html.

ابهامات زیادی درباره ساختار کلی تاب‌آوری ملی ویتنام وجود دارد. به نظر می‌رسد راهبرد حفاظت از وطن در فضای سایبری[۱] و طرح پیاده‌سازی آن به‌منزله سند اصلی سیاستی است که برنامه‌های پاسخ به حوادث جدی سایبری را تبیین می‌کند، هرچند مفاد آن در دسترس نیست. کمیته ملی راهبری پاسخ فوری ویتنام (NSCER)[۲] مسئول پاسخ‌گویی به چنین حوادثی است که وزارت اطلاعات و ارتباطات نیز با هدایت و هماهنگی اقدامات پاسخ فوری داخلی و یا بین‌المللی به آن کمک می‌کند[۳]. تیم پاسخ فوری رایانه‌ای ویتنام مسئولیت پاسخ به حوادث سایبری سطح پایین‌تر را برعهده دارد، اما در کنار سازمان‌های سایبری وزارت اطلاعات و ارتباطات، وزارت امنیت عمومی و وزارت دفاع ملی در کمیته ملی راهبری پاسخ فوری نیز مشارکت دارد. افزون بر آن، تیم پاسخ فوری رایانه‌ای ویتنام با سایر تیم‌های کوچک‌تر در سطح وزارتی، استانی و محلی و همچنین شرکت‌های فعال درحوزه‌های مخابراتی، خدمات اینترنتی، ذخیره‌سازی داده‌ها، بانکداری و حوزه مالی و نهادهای فعال در زمینه مدیریت زیرساخت‌های اطلاعاتی حیاتی یا سیستم‌های کنترل صنعتی نیز همکاری می‌کند[۴]. تیم پاسخ فوری رایانه‌ای ویتنام در سال ۲۰۱۹ یک رزمایش امنیت سایبری سراسری با تقریبا ۳۰۰ شرکت‌کننده برگزار کرد[۵].

۱. رجوع شود به:
Vu, 'Enhancing the homeland protection under the Party's platform'; Ngo, 'The whole military resolves to successfully fulfil the military-defense tasks in 2019'.

2. National Steering Committee for Emergency Response

رجوع شود به:
Prime Minister, 'Quyết Định: Ban Hành Quy Định Về Hệ Thống Phương Án Ứng Cứu Khẩn Cấp Bảo Dảm An Toàn Thông Tin Mạng Quốc Gia', 05/2017/QD-TTg, 16 March 2017, https://vanbanphapluat.co/quyet-dinh-05-2017-qd-ttg-hethong-phuong-an-ung-cuu-khan-cap-bao-dam-an-toan-thongtin-mang-quoc-gia.

۳. رجوع شود به:
'PM sets up national cybersecurity committee', Vietnam Law & Legal Forum, 2 April 2017, https://vietnamlawmagazine.vn/pm-sets-up-national-cybersecurity-committee-5785.html.

۴. رجوع شود به:
Prime Minister, 'Quyết Định: Ban Hành Quy Định Về Hệ Thống Phương Án Ứng Cứu Khẩn Cấp Bảo Dảm An Toàn Thông Tin Mạng Quốc Gia'.

۵. رجوع شود به:
Vietnam records more than 6,200 cyber attacks in seven months', AsiaOne, 1 August 2019, https://www.asiaone.com/digital/vietnam-records-more-6200-cyber-attacks-seven-months.

شایان ذکر است بخش خصوصی نقش فزاینده‌ای در تقویت امنیت اطلاعات ویتنام ایفا کرده و توانسته‌است صنعت امنیت سایبری این کشور را توسعه دهد. به‌عنوان مثال، شرکت ویتل شعبه‌ای راه‌اندازی کرده‌است که خدمات امنیت سایبری کنترل‌شده‌ای ارائه می‌دهد[۱]. شرکت گروه پست و مخابرات ویتنام هم در زمینه انجام تحقیقات امنیت سایبری فعالیت دارد و همزمان در شرکت‌های نوپای این حوزه سرمایه‌گذاری می‌کند. به‌علاوه، ۸ شرکت ویتنامی با همکاری یکدیگر باشگاه ارزیابی و نظارت بر امنیت سایبری ویتنام[۲] را با هدف بهبود ارزیابی و نظارت بر خدمات امنیت سایبری در سراسر کشور تشکیل داده‌اند.

با این وجود، ویتنام هنوز با چالش‌های قابل‌توجهی در زمینه امنیت سایبری خود مواجه است و حوادث آینده نشان خواهد داد که آیا کمیته ملی راهبری پاسخ فوری ویتنام قادر به برقراری هماهنگی مؤثر بین بخش‌های دولتی و خصوصی هست یا خیر. وزارت اطلاعات و ارتباطات اعلام کرده‌است که نیروی آموزش‌دیده کافی برای ایجاد تیم‌های پاسخ فوری رایانه‌ای موردنیاز در کشور وجود ندارد و شبکه تشکیل‌شده برای پاسخ فوری نیز نامنسجم و غیرحرفه‌ای است[۳]. به‌علاوه، سرمایه‌گذاری‌های حوزه تحقیقات و آموزش مصوب سال ۲۰۱۴ هنوز اجرا نشده‌اند[۴] و بررسی صورت گرفته در سال ۲۰۱۹ نشان می‌دهد که تقریباً نیمی از سازمان‌های دولتی فاقد بودجه لازم برای

۱. رجوع شود به:
'The first information security ecosystem built by Vietnamese', Acrofan, 20 February 2020, https://us.acrofan.com/detail.php?number=239640.

2. Vietnam Cyber Security Assessment and Audit Club

۳. رجوع شود به:
Samaya Dharmaraj, 'Vietnam strengthens human resources for information security tasks', OpenGov Asia, 9 July 2019, https://www.opengovasia.com/vietnam-strengthens-humanresources-for-information-security-tasks.

۴. همان.

تامین امنیت سایبری هستند[۱]. در سال ۲۰۲۰ نیز دولت طی گزارشی از اقدامات خود در زمینه تقویت امنیت سایبری خاطرنشان کرد که ۳۰ درصد از وزارتخانه‌ها هنوز به سطح موردنظر از امنیت سایبری نرسیده‌اند[۲]. در شاخص جهانی امنیت سایبری که در سال ۲۰۱۸ توسط اتحادیه بین‌المللی مخابرات منتشر شد، ویتنام در بین ۱۷۵ کشور رتبه ۵۰ را به خود اختصاص داده‌است[۳].

رهبری جهانی در عرصه سایبری

ویتنام سیاست سایبری خارجی خود را بر آسه‌آن متمرکز کرده‌است و مشتاقانه به تقویت همکاری در حوزه امنیت سایبری بین اعضای این اتحادیه و شرکای خارجی آن می‌پردازد. به‌عنوان مثال، ویتنام در دسامبر ۲۰۲۰ در چارچوب آسه‌آن به‌علاوه سه[۴] میزبان نشستی با چین، ژاپن و کره جنوبی در مورد همکاری‌های بین‌المللی در زمینه امنیت سایبری و مقابله با جرائم سایبری بود[۵]. ویتنام می‌کوشد اعضای آسه‌آن را به گسترش همکاری در زمینه هنجارهای سایبری[۶] و ایجاد سازوکارهای رسمی برای همکاری درحوزه

۱. رجوع شود به:
Chau An, ‘Vietnam carries potential to be a cybersecurity powerhouse: minister’, VnExpress, 17 April 2019, https://e.vnexpress.net/news/business/economy/vietnamcarries-potential-to-be-a-cybersecurity-powerhouseminister 3910754.html.

۲. رجوع شود به:
‘Cyber attacks targeting Vietnam’s information systems down 7.8 pct’, VietnamPlus, 4 November 2020, https://en.vietnamplus.vn/cyber-attacks-targeting-vietnams-information-systemsdown-78-pct/189811.vnp.

۳. رجوع شود به:
International Telecommunication Union, ‘Global Cybersecurity Index 2018’, p. 63, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

4. ASEAN Plus Three

۵. رجوع شود به:
Ministry of Public Security, ‘Asean +3 conference on cyber security opens in Hanoi’, 29 December 2020, http://en.bocongan.gov.vn/international-relations-cooperation/asean-3-conferenceon-cyber- security-opens-in-hanoi-t7615.html.

۶. رجوع شود به:
Li Ying Lee, ‘New ASEAN committee to implement norms for countries’ behaviour in cyberspace’, Channel News Asia, 2 October 2019, https://www.channelnewsasia.com/news/singapore/asean-cyberspace-working-level committeecybersecurity-11963602.

امنیت سایبری ترغیب کند[۱]. تیم پاسخ فوری رایانه‌ای ویتنام در ژوئن سال ۲۰۲۰ میزبان رزمایش سایبری آسه‌آن-ژاپن[۲] درباره روش‌های مقابله با وب‌سایت‌های جعلی بود[۳].

ویتنام به‌منظور گسترش توانمندی‌های خود در زمینه امنیت سایبری با دولت‌ها و شرکت‌های خارجی نیز همکاری می‌کند. به‌عنوان مثال، مرکز ملی نظارت بر امنیت سایبری ویتنام در سال ۲۰۱۹ قراردادی با شرکت کَسپرسکی[۴] (شرکت روسی فعال در زمینه امنیت سایبری) برای مقابله با چالش‌های امنیت اطلاعات امضا کرد[۵]. وزارت امنیت عمومی ویتنام نیز در سال ۲۰۲۰ با هند[۶]، برونئی[۷] و مالزی[۸] برای مقابله با جرائم سایبری وارد همکاری شد. ویتنام در انجمن جهانی تیم‌های امنیت و پاسخگویی به حوادث[۹] و تیم پاسخ فوری

---

۱. رجوع شود به:
'ASEAN Member States Agree to Move Forward on a Formal Cybersecurity Coordination Mechanism', CSA Singapore, 2 October 2019,
https://www.csa.gov.sg/news/press-releases/amcc-release-2019.

2. ASEAN-Japan Cyber Exercise

۳. رجوع شود به:
'Vietnamese tech experts join transnational cyber-attack exercise', Viêt Nam News, 26 June 2020, https://vietnamnews.vn/society/748743/vietnamese-tech-experts-join-transnationalcyber-attack-exercise.html.

4. Kaspersky

۵. رجوع شود به:
'National Cyber Security Center signs deal with Kaspersky for online security', VietNamNet, 24 January 2019, https://english.vietnamnet.vn/fms/science-it/216749/nationalcyber-security-center-signs-deal-with-kaspersky-for onlinesecurity.html.

۶. رجوع شود به:
'Vietnam-India strategic partnership in the fields of defense and security', National Defense Journal, 29 August 2017,
http://tapchiqptd.vn/en/events-and-comments/vietnamindia-strategic-partnership-in-the-fields-of-defense-andsecurity/10541.html.

۷. رجوع شود به:
'Việt Nam, Brunei, boost co-operation in combating crimes', Viêt Nam News, 14 February 2020,
https://vietnamnews.vn/politics-laws/592275/viet-nam-brunei-boost-co-operation-incombating-crimes.html.

۸. رجوع شود به:
Ministry of Public Security, 'Vietnam, Malaysia promote cooperation in security', 14 February 2020, http://en.bocongan.gov.vn/international-relations-cooperation/vietnam-malaysiapromote-cooperation-in-security-t6508.html.

9. Forum of Incident Response and Security Teams

رایانه‌ای آسیا و اقیانوسیه (APCERT) نیز عضویت دارد[۱]. اگرچه ویتنام به‌طور محرمانه علاقه خود را برای همکاری نزدیک با ایالات متحده و استرالیا در مسائل امنیت سایبری ابراز کرده‌است، اما به‌دلیل نگرانی‌های حقوق بشری در مورد قانون امنیت سایبری این کشور، هنوز موانع دیپلماتیک متعددی برای همکاری بین آن‌ها وجود دارد. با این وجود، ایالات متحده و استرالیا در زمینه‌های کمتر حساس سیاست فضای سایبری مانند آموزش حقوق بین‌المللی و توسعه شهرهای هوشمند با ویتنام همکاری دارند.

توانمندی‌های سایبری تهاجمی

با توجه به وظایف سیاسی گسترده مرکز فرماندهی سایبری ویتنام در داخل کشور و به گفته رئیس ستاد فرماندهی آن، با توجه به کمبود امکانات، تجهیزات و تسلیحات سایبری مناسب در این سازمان، بعید است که مرکز فرماندهی سایبری از موقعیت مناسبی برای انجام عملیات سایبری تهاجمی علیه دشمنان خارجی برخوردار باشد[۲]. نیروی ۴۷ نیز احتمالاً از توانایی‌های فنی لازم برای اجرای عملیات‌های مهم سایبری تهاجمی برخوردار نیست، چراکه هدف آن در درجه اول سیاسی و بیشتر شامل مدیریت افکار عمومی ازطریق مقابله با دیدگاه‌های خصمانه و انتشار تبلیغات سیاسی است[۳]. گروه اِی‌پی‌تی ۳۲

۱. رجوع شود به:
Adam Bannister, 'APCERT holds cyber drill to stress-test response capabilities of 32 CSIRTs', The Daily Swig, 6 April 2020,
https://portswigger.net/daily-swig/apcert-holds-cyberdrill-to-stress-test-response-capabilities-of-32-csirts.

۲. رجوع شود به:
'Xây dựng lực lượng Tác chiến không gian mạng, dáp ứng yêu cầu nhiệm vụ bảo vệ Tổ quốc', Tạp chí Quốc phòng, 17 October 2019,
http://tapchiqptd.vn/vi/bao-ve-to-quoc/xay-dung-lucluong-tac-chien-khong-gian-mang-dap-ung yeu-cau-nhiemvu-bao-ve-to-quoc/14505.html.

۳. رجوع شود به:
'Hơn 10.000 người trong 'Lực lượng 47' Dấu tranh trên mạng',Tuổi Trẻ.

هـم بیـش‌از آنکه بـه عملیات‌های سـایبری تهاجمی بپـردازد، در امور جاسوسـی صنعتی و ماننـد آن فعالیـت دارد. البته احتمالاً این گروه دارای برخی از توانمندی‌های قابل‌اسـتفاده در عملیات‌هـای سـایبری تهاجمـی اسـت. درمجمـوع براسـاس شـواهد موجـود بـه نظـر می‌رسـد حزب حاکم در ویتنام در حال حاضر توسـعه توانمندی‌های سـایبری تهاجمی را از اولویت‌های اصلی خود برنمی‌شمرد.

جمع‌بندی

به‌طور کلی، مطالعه‌های موردی در گزارش حاضر مشتمل بر نحوه واکنش دولت‌ها به فرصت‌ها و تهدیدهای مرتبط با توانمندی‌های سایبری می‌شوند. علاوه‌بر این، براساس این مطالعه‌های موردی می‌توان جایگاه نسبی هریک از کشورها در امنیت سایبری و تاثیر آن‌ها در توازن کلی قدرت جهانی را نیز تا حدی استنباط کرد.

بنیان‌های قدرت سایبری

موارد موردمطالعه از نظر راهبرد و مبانی نظری منتشر شده به‌ویژه با توجه به سطح تعادل بین سیاست‌های امنیت سایبری و سیاست‌های مرتبط با اطلاعات و کاربردهای سیاسی و نظامی دارایی‌های سایبری آن‌ها تفاوت‌های قابل‌ملاحظه‌ای با یکدیگر دارند. با وجود سطح بسیار بالای محرمانگی این امور، همه کشورها حداقل درباره یکی از ابعاد مختلف قدرت سایبری اسنادی در زمینه راهبرد، سیاست یا مبانی نظری خود منتشر کرده‌اند. ایالات متحده که از اوایل دهه نود به انتشار سیاست‌های سایبری خود پرداخته‌است، پرچم‌دار این عرصه محسوب می‌شود. البته در دهه نود کشورهای دیگری نیز بخش‌های پراکنده‌ای از تفکر سایبری نظری یا راهبردی خود را منتشر کرده‌اند، اما اولین موج انتشار سیاست‌های سایر کشورها-با دامنه و عمقی در سطح سیاست‌های انتشاریافته آمریکا-از دهه ۲۰۰۰ آغاز شد و سال ۲۰۱۵ شروع موج دوم این دست اقدامات بود.

هریک از مطالعه‌های موردی ترکیب منحصربه‌فردی از عناصر نظامی و غیرنظامی کشور موردمطالعه را نشان می‌دهند که بازتاب شرایط راهبردی خاص آن کشور و نیز ملاحظات سیاست‌گذاری آن هستند. با توجه به ماهیت به‌شدت متغیر تهدیدها و فرصت‌های سایبری، هیچ‌یک از موارد موردمطالعه از وضعیت توسعه راهبردهای خود رضایت ندارند.

کشورهـای موردمطالعـه و رژیـم صهیونیسـتی از نظر مناسـبات حکمرانـی، فرماندهی و نظـارت نیـز تفاوت‌هـایی بـا یکدیگـر دارنـد، به‌ویـژه فرهنـگ سیاسـی آن‌هـا از عوامـل اصلـی تاثیرگـذار در ایـن حوزه به‌شـمار می‌آید. نظام‌های دموکراسـی لیبـرال در کشورهای توسـعه‌یافته‌ای ماننـد فرانسـه، ژاپـن، بریتانیـا و ایالات متحده در مقایسـه بـا کشورهای درحال‌توسـعه ثروتمنـد ماننـد هنـد، انـدونزی و مـالزی در حکمرانـی سـایبری از سـازمان منسـجم‌تر و بالغ‌تری برخوردار هسـتند. در گروه اخیر، سـاختار حکمرانی کشورها همانند راهبردهـای امنیـت فضـای سـایبری آن‌هـا به‌کنـدی و ناهمسـان شـکل گرفته‌اسـت. در برخـی کشورهـا ماننـد چین، کره شـمالی، ایران و روسیه سـاختار حکمرانـی فضای مجازی شـفافیت کمتری دارد و تمرکز آن پایین اسـت. در بین این چهار کشور تنها در مورد چین می‌تـوان گفـت کـه دارای چارچـوب محکمـی مبتنـی بـر رویکـرد چندذینفعـی در حکمرانی فضای سـایبری اسـت، هرچند نظام سیاسـی چین نیز حزب کمونیسـت چین را به‌عنوان ذینفع اصلی به سایر ذینفعان ترجیح می‌دهد.

توانمندی‌های محوری در زمینه اطلاعات سایبری سنگ‌بنای قدرت سایبری محسوب می‌شـوند و تـوان کشورها در اجـرای عملیات‌های دفاعی یا تهاجمی در فضای سـایبری به شناخت آن‌ها از محیط سایبری یا همان «آگاهی موقعیتی سایبری» بستگی دارد. توسعه این توانمندی ازطریق تجمیع همه منابع اطلاعات از بخش‌های خصوصی و دولتی محقق می‌شـود. نهادهای اطلاعاتی نیز زمانی موثر هسـتند که قابلیت شناسـایی و ردیابی منبع حمله‌هـای سـایبری دولتی را داشـته باشـند و بتواننـد به‌نوبه خود عملیات‌های سـایبری سـطح بـالا و تخصصـی اجـرا کننـد. در عمـل، بسـیاری از کشورهـا توانمندی‌های سـایبری خود را روی امنیت داخلی متمرکز کرده‌اند و برخی نیز دارای دسترسـی منطقه‌ای هسـتند. درواقـع، تنهـا تعـداد کمـی از کشورهـا از شـناخت سـایبری بین‌المللـی کافـی بـرای اجـرای

عملیات‌های سطح بالای تخصصی برخوردار هستند. این کشورها عبارتند از: اعضای ائتلاف پنج چشم (استرالیا، کانادا، نیوزیلند، بریتانیا و ایالات متحده) که به‌صورت گروهی فعالیت می‌کنند، دو شریک بسیار توانمند این ائتلاف یعنی رژیم صهیونیستی و فرانسه که توانمندی‌های بومی خود را به‌وسیله توان ائتلاف تقویت می‌کنند و چین و روسیه. در کشورهای توانمند سایبری این نهادهای اطلاعاتی هستند که در تدوین سیاست و راهبرد ملی نقش اصلی بازی می‌کنند و نفوذ بسیار بالایی در رویکرد نیروهای مسلح در عملیات‌های سایبری تهاجمی دارند. درمجموع، همه موارد موردمطالعه به‌دلیل نقش محوری توانمندی‌های اطلاعاتی حساس در عملیات‌های سایبری از انتشار گسترده اطلاعات مربوط به سیاست‌های سایبری اجتناب می‌کنند.

اظهارنظر درباره اثربخشی راهبردهای سایبری دولت‌ها برای افزایش منابع-انسانی و مالی-امر ساده‌ای نیست، زیرا در بیشتر موارد امکان ارزیابی دقیق منابع مالی و انسانی کشورها وجود ندارد. با این حال، شواهد نشان می‌دهند سرمایه‌گذاری (انسانی و مالی) کشورهای ایالات متحده، چین و روسیه در مقایسه با سایر کشورهای توانمند سایبری بسیار بیشتر است. کشورهای دیگر این کمبود را با ائتلاف‌های قوی به‌ویژه با ایالات متحده جبران می‌کنند. ائتلاف پنج چشم کارآمدترین و بالغ‌ترین این ائتلاف‌ها است و کشورهای اقتدارگرا هنوز نتوانسته‌اند ائتلافی در این سطح تشکیل دهند.

طبق مطالعه‌های موردی کشورها، هیچ‌یک از آن‌ها آنقدر ارتش خود را توسعه نداده‌است که بتواند ادعا کند توانمندی‌های سایبری آن طیف کاملی از گزینه‌های دفاع و تهاجم را پوشش می‌دهند. در این بین، شواهد موجود بیانگر این هستند که ایالات متحده بیش از سایر کشورها در این زمینه پیشرفت داشته‌است و در حوزه‌های کلیدی مانند مبانی نظری، آموزش و اصلاح ساختار نیروهای انسانی بیشترین دستاورد را کسب

کرده‌است. هیچ مورد دیگری -احتمالا به‌جز رژیم صهیونیستی- نتوانسته‌است همانند آمریکا توانمندی‌های سایبری را در ابعاد مختلف نیروهای نظامی خود به‌کارگیرد. با آنکه به نظر می‌رسد ادغام توانمندی‌های سایبری نیروهای مسلح با نهادهای اطلاعاتی اصلی نقش اساسی در تحول نظامی (توسعه سایبری نیروهای مسلح) کشورها دارد، اما این امر می‌تواند موجب بروز مشکلاتی در حوزه فرماندهی و نظارت شود. اختلاف‌هایی که اکنون در محافل سیاسی ایالات متحده در مورد تداوم ریاست ستاد فرماندهی سایبری بر سازمان امنیت ملی مطرح است، بازتاب وجود چنین مسائلی هستند.

پس از ایالات متحده که در دهه نود به‌طور خودجوش اولین اقدامات مبنی بر توسعه و پذیرش نقش توانمندی‌های سایبری در قدرت ملی را شروع کرد، پیشرفت‌های سایر کشورها در این زمینه عمدتا از واکنش آن‌ها به بحران‌های راهبردی نشات گرفته‌است. با توجه به جدید بودن نوع حمله، واکنش ایران به افشای حمله استاکس‌نت آمریکا و رژیم صهیونیستی در سال ۲۰۱۰ با هدف جلوگیری از توسعه پروژه غنی‌سازی اورانیوم در ایران، بهت‌زدگی ایالات متحده و هم‌پیمانانش از افشای دامنه و میزان اثرات جاسوسی تجاری چین در سال ۲۰۱۱، اثر افشاگری‌های ادوارد اسنودن درباره توان ائتلاف پنج چشم روی روسیه و چین در سال ۲۰۱۳ و اقدام احتمالی روسیه برای اخلال در روند انتخابات ایالات متحده و برخی کشورهای اروپایی در سال ۲۰۱۶ نمونه‌هایی از این دست بحران‌ها هستند. به نظر می‌رسد در سال‌های اخیر زنجیره‌های افشاگری (بهت‌زدگی) و واکنش کشورها به آن‌ها ازجمله اعتراض‌های دیپلماتیک، عامل اصلی در شتاب بخشیدن به پیشرفت‌های اغلب کشورها در حوزه سیاست‌های امنیت سایبری بوده‌است. البته با توجه به این‌که تاکنون هیچ کشوری درنتیجه حمله‌های سایبری متحمل خسارت‌های مالی و جانی گسترده‌ای نشده‌است، نرخ متوسط اصلاح سیاست‌های سایبری از اصلاحات در سایر

بخش‌ها سریع‌تر نیست. درواقع، روند اصلاحات سیاست‌های سایبری حداقل یک دهه زمان می‌برد تا منجر به اثرگذاری قابل‌توجهی شود و به‌طور کلی، فرآیندی است که تقریبا هیچ‌وقت تکمیل و درنتیجه، متوقف نمی‌شود. یکی از موانع مهم پیش‌روی کشورها در اجرای اصلاحات، کمبود نیروی انسانی مجرب است. در بین موارد موردمطالعه، تنها رژیم صهیونیستی رویکردی قدرتمند در ارتقای مهارت شهروندان خود به‌کار گرفته که تا حد زیادی وابسته به ظرفیت خدمت وظیفه عمومی در ارتش آن است.

همه‌گیری کوید-۱۹ به کشورها یادآوری کرد که نباید منتظر شوند بحران آن‌ها را غافلگیر و وادار به واکنش کند و پیش از آن باید نرخ سرمایه‌گذاری خود در منابع انسانی سایبری را افزایش دهند.

جایگاه نسبی

با توجه به محرمانه‌بودن بسیاری از اطلاعات، رتبه‌بندی کشورها براساس شاخص‌های روش‌شناسی این مطالعه نمی‌تواند قطعی باشد. با این وجود، می‌توان سلسله‌مراتب کلی کشورها را تعیین کرد و آن‌ها را در یکی از سه رده مورداشاره در مقدمه این گزارش قرار داد: رده اول شامل کشورهای پیشتاز در همه شاخص‌ها، رده دوم شامل کشورهای پیشتاز در برخی از حوزه‌ها و رده سوم شامل کشورهایی که در برخی از حوزه‌ها دارای نقطه‌قوت نسبی هستند، ولی در بیشتر شاخص‌ها عملکرد ضعیفی دارند. نباید فراموش کرد که در کشورهای رده دوم و حتی رده اول نیز نقطه‌ضعف‌هایی دیده می‌شود، اما در مقایسه با ضعف‌های کشورهای رده سوم قابل‌چشم‌پوشی است.

ایالات متحده آمریکا تنها کشوری است که از قدرت کافی برای قرار گرفتن در رده اول برخوردار است. کشورهای استرالیا، کانادا، چین، فرانسه، روسیه، بریتانیا و همچنین رژیم صهیونیستی در رده دوم قرار دارند و با توجه به معیارهای ارزیابی این موسسه کشورهای

دیگر یعنی هند، اندونزی، ایران، ژاپن، مالزی، کره شمالی و تایوان در رده سوم هستند. با توجه به وزنی (ارزشی) که به هریک از شاخص‌ها داده می‌شود، امکان درجه‌بندی بهتری از کشورهای حاضر در رده‌های دوم و سوم وجود دارد. به‌عنوان مثال، اگر در رده دوم ترکیبی از امنیت سایبری در کلاس جهانی، اطلاعات سایبری در کلاس جهانی، توانمندی‌های سایبری تهاجمی پیشرفته و ائتلاف‌های سایبری قدرتمند ملاک باشد، رژیم صهیونیستی و بریتانیا در جایگاه بالا در این فهرست قرار می‌گیرند و درمقابل، در صورتی که حجم منابع -انسانی و مالی- تخصیص‌یافته به فضای سایبری، عملیات متهورانه نامحدود و انجام عملیات‌های روزانه اطلاعاتی مبتنی بر فناوری‌های سایبری به‌عنوان عوامل اصلی در نظر گرفته شوند، چین و روسیه کشورهای پیشتاز در رده دوم خواهند بود. درنهایت، در رده سوم درصورتی که برخورداری از ظرفیت بالا در امنیت سایبری معیار باشد، مالزی جایگاه اول را در این فهرست دارد و اگر تجربه عملیاتی معیار اصلی در نظر گرفته شود، ایران در جایگاه اول در این فهرست خواهد بود.

البته می‌توان گفت توانمندی در صنایع محوری که توسعه آینده فضای سایبری در گروی آن‌هاست و نقش تعیین‌کننده‌ای در تاب‌آوری سایبری کشورها دارد، معیار اصلی در رتبه‌بندی کشورها است. براین اساس، با توجه به وضعیت کنونی چین و در صورتی که ضعف‌های امنیت سایبری آن برطرف شود، این کشور بهترین گزینه برای قرارگرفتن در رده اول در کنار آمریکاست و ژاپن نیز در بلندمدت می‌تواند به جایگاه بالا در فهرست کشورهای رده دوم صعود کند.

اگرچه مطابق داده‌های این گزارش کشورهای ایالات متحده و چین در مقایسه با سایر کشورها از قدرت سایبری بسیار بالاتری برخوردار هستند، اما آمریکا همچنان قدرتمندتر از چین است. چین برای آنکه بتواند در آینده به آمریکا در رده اول ملحق

شـود بایـد حداقـل دو اقدام مهـم را انجام دهد: ۱) سـاخت مجموعه‌ای صنعتی-سـایبری در مقیـاس و بـا همان ویژگی‌هـای اصلی مجموعه ایالات متحده که مسـتلزم ایجاد ارتباط پویاتـر بیـن تحقیقـات دانشـگاه، صنعت و دولـت اسـت؛ و ۲) بهبود خروجی آموزشـی در رشـته‌های سـایبری ازجمله امنیت سـایبری پایه. پس از تحقق این پیش‌نیازهای داخلی، چین می‌تواند به چالش‌های دیپلماتیک پیش‌روی توسـعه قدرت سـایبری خود بپردازد. چیـن بـرای آنکه بتواند قدرت سـایبری خـود را درجهـت تاثیرگذاری جهانـی به‌کارگیرد باید ائتلاف‌های قدرتمندی نیز با سایر کشورهای توانمند در حوزه سایبری شکل دهد.

توازن ملاحظات قدرت

نخبـگان سیاسـی و دولت‌هـای مختلـف همگـی در مورد این مسـاله توافـق دارند که مزیت‌هـای قدرت سـایبری و به‌کارگیـری توانمندی‌هـای سـایبری در عملیات‌های منطقه خاکسـتری می‌تواند توازن قدرت بین ایالات متحده و هم‌پیمانانش از یک سـو و روسـیه و چیـن از سـوی دیگـر را برهم‌زنـد. اما فارغ از این اجمـاع کلی، جامعـه بین‌المللی هنوز در مـورد نحـوه ارزیابـی یا سـنجش رقابـت فناورانه کشـورها از نظر قدرت سـایبری بـه توافق نرسیده‌اسـت، به‌ویـژه این‌کـه پیچیدگـی ایـن وضعیت بـا پدیدآمـدن فناوری‌هـای جدید (مانند تراشـه‌های نانو، تراشـه‌های مبتنی بر کربن، معماری‌های ابـری، رایانش کوآنتومی، هوش مصنوعی، سلاح‌های خودکار و ربات‌های نظامی) نیز دوچندان می‌شود.

کشورهـای پیشـتاز عقیده دارنـد توانمندی‌های سـایبری باعث تقویت قـدرت نظامی شده و می‌توانند تاثیر قابل‌توجهی بر فرایندهای تصمیم‌گیری، کنترل سامانه‌های نظامی و شـکل‌دهی به نیروها داشـته باشند. طبق نتایج این گزارش، مفهوم سنتی توازن قدرت کـه براسـاس مناسـبات ژئوپلیتیـک تعریـف می‌شـود، بـا مفهـوم تـوازن قـدرت اطلاعاتی جایگزیـن خواهد شـد. ایـالات متحده و چیـن در پی تحقق مبنای نظری خود برای تسـلط

اطلاعاتی هستند که به‌معنای برتری جهانی آن‌ها در تولید فناوری‌های اطلاعاتی است. ایالات متحده همچنان خود را پیشتاز عرصه سایبری می‌داند و چین نیز به‌طور ضمنی به این حقیقت اذعان دارد. البته عوامل ژئوپلیتیک هنوز هم موثر هستند، به‌ویژه که ایالات متحده ائتلاف‌های بین‌المللی متعددی دارد (ناتو و ائتلاف با رژیم صهیونیستی و کشورهای عرب حاشیه خلیج‌فارس، ژاپن و کره جنوبی) که ضمن حفظ اهمیت ژئوپلیتیک خود به‌سمت مشارکت‌های سایبری نیز حرکت می‌کنند.

نویسندگان این گزارش معتقدند برتری صنعتی-دیجیتالی آمریکا با در نظر گرفتن ائتلاف‌های آن حداقل تا ده سال آینده باقی خواهد ماند. مبنای این استدلال دو دلیل زیر است: ۱) آمریکا همچنان از چین از نظر تولید فناوری‌های سایبری پیشرفته و به‌کارگیری آن‌ها جهت کسب قدرت اقتصادی و نظامی جلوتر است؛ و ۲) آمریکا و بسیاری از هم‌پیمانانش از سال ۲۰۱۸ تصمیم گرفته‌اند دسترسی چین به فناوری‌های غربی را محدود کنند. به این ترتیب، آن‌ها زمینه جدایی چین از غرب را فراهم می‌آورند که این امر نیز به‌نوبه خود چین را از توسعه فناوری‌های پیشرفته بومی بازمی‌دارد. این واقعیت که ایالات متحده تا چه حد این سیاست را با جدیت پیش خواهد برد و واکنش چین به آن چگونه خواهد بود، تعیین‌کننده سرنوشت توازن قدرت سایبری در آینده است.

ارزیابی کلی توانمندی‌های سایبری و قدرت ملی

گزارش حاضر حاوی روش‌شناسی جدیدی برای ارزیابی قدرت سایبری است و آن را درمورد ۱۴ کشور و رژیم صهیونیستی به‌کار بسته‌است:

- چهار عضو ائتلاف اطلاعاتی پنج چشم: ایالات متحده، بریتانیا، کانادا و استرالیا
- سه هم‌پیمان عضو ائتلاف پنج چشم که قدرت سایبری بالایی دارند: فرانسه، رژیم صهیونیستی و ژاپن
- چهار کشوری که از سوی اعضاء ائتلاف پنج چشم و هم‌پیمانان آن‌ها تهدید سایبری به‌شمار می‌روند: چین، روسیه، ایران و کره شمالی
- چهار کشوری که در مراحل ابتدایی توسعه قدرت سایبری هستند: هند، اندونزی، مالزی و ویتنام

این روش‌شناسی کیفی دارای دامنه گسترده‌ای است و هریک از کشورها را در هفت حوزه بررسی می‌کند. زیست‌بوم سایبری کشورها از نظر برهم‌کنش آن با امنیت بین‌المللی، رقابت اقتصادی و مسائل نظامی مورد تجزیه‌وتحلیل قرار می‌گیرد.

براساس نتیجه این تحلیل‌ها، موارد موردمطالعه به سه رده دسته‌بندی می‌شوند: رده اول شامل کشورهای پیشتاز در همه شاخص‌ها، رده دوم شامل کشورهای پیشتاز در برخی از حوزه‌ها و رده سوم شامل کشورهایی که در برخی از حوزه‌ها دارای نقطه‌قوت نسبی هستند، ولی در بیشتر شاخص‌ها عملکرد ضعیفی دارند.

درنهایت، یک کشور در رده اول، شش کشور به‌علاوه رژیم صهیونیستی در رده دوم و هفت کشور در رده سوم قرار می‌گیرند.

گزارش حاضر اولین اثر موسسه بین‌المللی مطالعات راهبردی در زمینه قدرت سایبری است و قدرت سایبری کشورهای دیگر در سال‌های آینده ارزیابی خواهد شد.

موسسه بین‌المللی مطالعات راهبردی (IISS)

این موسسـه که در سال ۱۹۵۸ بنیان‌گذاری شده‌است، به‌عنوان مرکزی مستقل در زمینه پژوهش، اطلاعات و مباحث مرتبط با منازعاتی که دارای جنبه نظامی هستند -صرف‌نظر از علت آن‌ها- عمل می‌کند.

The International Institute for Strategic Studies - UK

Arundel House | 6 Temple Place | London | wc2r 2pg | UK

t. +44 (0) 20 7379 7676 **f.** +44 (0) 20 7836 3108 **e.** iiss@iiss.org www.iiss.org

The International Institute for Strategic Studies - Americas

2121 K Street, NW | Suite 600 | Washington, DC 20037 | USA

t. +1 202 659 1490 **f.** +1 202 659 1499 **e.** iiss-americas@iiss.org

The International Institute for Strategic Studies - Asia

9 Raffles Place | #49-01 Republic Plaza | Singapore 048619

t. +65 6499 0055 **f.** +65 6499 0059 **e.** iiss-asia@iiss.org

The International Institute for Strategic Studies - Europe

Pariser Platz 6A | 10117 Berlin | Germany

t. +49 30 311 99 300 **e.** iiss-europe@iiss.org

The International Institute for Strategic Studies - Middle East

14th floor, GBCORP Tower | Bahrain Financial Harbour | Manama | Kingdom of Bahrain

t. +973 1718 1155 **f.** +973 1710 0155 **e.** iiss-middleeast@iiss.org

منبع

Cyber capabilities and national power: A Net Assessment, The International Institute For Strategic Studies,pdf.


مؤسسه پویندگان توسعه فناوری و نوآوری ایرانیان