بسم‌الله الرحمن الرحیم

امنیت سایبری در جهان – کشورهای آمریکایی و اروپایی

مقدمه و چکیده

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

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

آمریکا بدون تردید اولین کشور مورد بررسی در این گزارش است. با وجود اینکه آمریکا خالق اینترنت است و رویه‌ها و قوانین و مقررات و دکترین‌های حاکم بر این فضا را تدوین و اجرایی کرده است؛ اما در گذر زمان کشورهای دیگری چون روسیه و چین در عرصه سایبری قوت پیدا کرده و تلاش کرده‌اند تا دیدگاه های خود را در اداره این فضا اعمال نمایند. سه جنبه منحصر به فرد فرهنگ امنیت اطلاعات ایالات متحده عبارت است از: 1- واقع شدن شرکت‌های بزرگ در خاک این کشور؛ 2- سیاست خارجی انزواگرایانه ناشی از ترامپیسم 3- و تلاش برای تدوین رویه‌های عملیاتی تأمین امنیت در کنار تدوین اصول کلی این مسئله.

کانادا عضو دیگر قاره آمریکا است که مورد بررسی قرار گرفته است. در گزارش مربوط به این کشور، ابتدا با توصیف وضعیت بین‌المللی امینت سایبری، استدلال می‌کنیم که اجماع عمومی برای توقف حملایت سایبری ناممکن است. این موضوع اهمیت پرداختن به امنیت سایبری برای دولت‌ها را روشن می‌کند. همچنین توضیح داده می‌شود که بیشتر از هکرهای مستقل، تهدیدهای سایبری از سوی دولت‌های خارجی مطرح می‌شود. از همین رو، کانادا و مردم آن، احساس نگرانی زیادی نسبت به حملات سایبری دارند. اما نکته جالب اینکه کانادایی‌ها، ترجیح می‌دهند ناامنی سایبری از سوی بازیگران خارجی را تجربه کنند، اما دولت به داده‌های آنها، حتی با هدف ایجاد امنیت دسترسی نداشته باشد. از همین رو، اقدامات دولت کانادا برای افزایش امینت، بیشتر از جنس تبلیغی و آگاهی‌بخشی، مخصوصاً برای بخش خصوصی بوده است؛ چراکه مقبولیت کافی برای ورود به داده کاربران را ندارد؛ لذا امیدوار است بتواند با افزایش آگاهی مردم و بخش خصوصی، آنها را در برابر تهدیدات سایبری ایمن کند. همچنین، در کنار اقدامات داخلی، کانادا موفق شده با ورود به پیمان‌های بین‌المللی، در حفظ امنیت سایبری برای خود شرکایی به دست آورد.

اتحادیه اروپا، از این حیث که به صورت جداگانه اسناد مهمی را در این زمینه به تصویب رسانده، در عرض دیگر کشورها مورد بررسی قرار گرفته است. منافع و ظهور دیدگاه‌های مختلف بازیگران در اتحادیه، سبب بروز انتظارات متعدد در اتحادیه شده است. بدین سبب پیش از طراحی و اجرای خط‌مشی‌های مربوط به امنیت سایبری در اروپا، ضرورت ایجاد انسجام افقی و اتحاد میان دولت‌ها و تطبیق انتظارات، رویکردها و مسئولیت‌ها و با غایت کاهش تنش‌های سنتی میان دولت‌ها در اتحادیه، چالش نخست در حوزه امنیت سایبری اتحادیه اروپا شده است. چالش دوم اتحادیه ذیل تهدیدات امنیتی و نفوذ عنوان می‌گردد. ماهیت تهدیدات امنیت سایبری که اتحادیه با آن‌ها در سال‌های اخیر مواجه شده است، از سنخ تهدیدات اقتصادی است. ازاین‌رو هدف نهایی اتحادیه اروپا درزمینه امنیت سایبری، ایجاد یکپارچگی اصول اساسی مربوط به زیربنای پتانسیل اقتصادی است.

انگلیس و ایرلند شمالی (بریتانیا) یکی از اقتصادهای پیشرو در جهان است و توانسته منابع ملی قابل‌توجهی را برای رسیدگی به طیف وسیعی از مسائل امنیت سایبری به کار گیرد. برنامه علنی امنیت سایبری ملی انگلیس یک دهه قدمت دارد و رویکردی پیچیده به امنیت سایبری است که چندین بازیگر دولتی و خصوصی را شامل می‌شود. این بازیگران در چهارچوب یک برنامه‌ریزی قوی عمل می‌کنند که فضای سایبری را به‌عنوان یک حوزه استراتژیک و امنیت سایبری را وسیله‌ای برای پیگیری منافع ملی در داخل و خارج از کشور می‌داند. در این گزارش علاوه‌بر تشریح استراتژی امنیت سایبری انگلستان و شناخت نهادها و ذی‌نفعان اصلی آن، به برخی از پیامدهای اجتماعی امنیت سایبری انگلیس به‌طور خلاصه اشاره می‌شود. در پایان نتیجه گرفته می‌شود که با وجود برخی چالش‌های استراتژیک برای امنیت سایبری انگلستان در قالب برگزیت و براندازی روسیه ، انگلستان آمادگی نسبتاً خوبی برای مقابله با چشم‌انداز وسیع چالش‌های امنیت سایبری دارد.

نروژ با سرعت بسیار بالایی دیجیتالی شد. این موضوع باعث شده در معرض خطرات سایبری بیشتری قرار بگیرد. به‌طور کلی می‌توان دو استراتژی کلی را در رویکرد امنیت سایبری نروژ مشاهده کرد: یکی تلاش برای به خط کردن بخش خصوصی و متعهد کردن آنها نسبت به امنیت سایبری. اهمیت این مورد وقتی مشخص می‌شود که بدانیم مثل دیگر کشورهای توسعه یافته، بخش مهمی از زیرساخت‌های دیجیتالی نروژ در دست بخش خصوصی است. استراتژی دوم، نگاه به بیرون و تلاش برای حفظ نظم جهانی است. این بازتابی از رویکرد کلی نروژ به امنیت در حوزه دیجیتال به حساب می‌آید. ناتو که یک ستون استراتژیک امنیت نروژ است، در حوزه امنیت سایبری هم نقش کلیدی دارد. در مجموع می‌توان گفت نروژ سعی کرده بهترین شیوه‌ها از کشورهای مشابه را برای خودش بومی‌سازی کند.

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

آمریکا

مقدمه

در بررسی سیاست و موقعیت امنیت سایبری ایالات‌متحده، ضروری است که با شرایط منحصربه‌فرد ایجاد خود اینترنت شروع کنیم. با شروع دهه 1960، ایالات‌متحده اقداماتی را برای ایجاد آنچه که منجر به اینترنت امروزی شد، رهبری کرد. به این معنا که بخش عمده‌ای از تحقیقات و بودجه برای ایجاد اولیه اینترنت توسط دولت ایالات‌متحده تأمین شد؛ درحالی‌که بخش عمده‌ای از توسعه فناوری اولیه در دره سیلیکون کالیفرنیا انجام شد. درنتیجه، نمی‌توان گفت که خود اینترنت در ایالات‌متحده متولد شده است. تلاش‌های دولت ایالات‌متحده برای ایجاد یک سیستم به‌هم‌پیوسته برای انتقال داده‌ها در سال 1966 با تخصیص منابع برای این پروژه از برنامه موشک‌های بالستیک وزارت دفاع ایالات‌متحده آغاز شد. آرپانت[1] اصلی که در سال 1969 آغاز شد، چهار مرکز تحقیقاتی را در ایالات‌متحده به هم متصل کرد. گره‌های جدید غیرنظامی، نظامی و دانشگاهی در دهه‌های 1970 و 1980 اضافه شدند و این فناوری به‌تدریج گسترش یافت و آدرس‌های خارج از کشور را نیز در برگرفت. در سال 1990، ارتش ایالات‌متحده از موقعیت کنترلی خود در اینترنت خارج شد، اگرچه دولت ایالات‌متحده به ارائه حمایت مالی از گروه‌های بین‌المللی مانند کمیسیون بین‌المللی برای تعیین نام‌های شبکه[2] و جامعه اینترنت با بودجه تحت مدیریت بنیاد ملی علوم ایالات‌متحده[3] ادامه داد. ساخت سخت‌افزار فیزیکی (ستون فقرات اینترنت[4]) برای انتقال داده‌ها در داخل ایالات‌متحده و درنهایت به مکان‌های خارج از کشور نیز توسط بنیاد ملی علوم مدیریت و توسط شرکت‌های بین‌المللی مستقر در آمریکا از جمله IBM و MCI ساخته شد (Tyson, n.d.).

نقش پیشرو تاریخی آمریکا در توسعه امنیت سایبری

با توجه به این واقعیت که اینترنت در آمریکا متولدشده است، ایالات‌متحده از لحاظ تاریخی، مزایای داخلی خاصی را در زمینه توسعه وضعیت امنیت سایبری خود دارا است. برنامه‌ریزان و توسعه‌دهندگان فناوری ایالات‌متحده تصمیماتی گرفته‌اند که رویه‌ها و قوانینی را برای چگونگی ساختار اینترنت و نحوه رفتار آن تعیین کرده است. چنین اقداماتی شامل سرمایه‌گذاری در ایجاد و قرار دادن سخت‌افزارهای حیاتی از جمله کابل‌های داده برای ایجاد سابقه در رابطه با مسائلی مانند ذخیره‌سازی داده و پروتکل‌های انتقال داده است. به‌عنوان اولین محرک در این محیط جدید، پروتکل‌ها و رویه‌های ایالات‌متحده اغلب خود را به عنوان نقشه‌ای که سایر کشورها هنگام حرکت در حوزه فناوری از آن پیروی می‌کنند، نشان داده‌اند. یعنی ایالات‌متحده در طول تاریخ به‌عنوان یک هنجار دهنده در ایجاد انتظارات رفتاری در محیط آنلاین عمل کرده است.

در مراحل اولیه توسعه، خود اینترنت ممکن است به داشتن یک صبغه آمریکایی منحصربه‌فرد توصیف‌شده باشد، زیرا بسیاری از طراحان نرم‌افزار و سخت‌افزار به اصول پیشرفته‌ای مانند مقررات حداقلی و عدم دخالت دولت (همسو با فلسفه سیاسی آزادی‌خواهی) اعتقاد داشتند (مانجیکیان، 2020). درعین‌حال، ابتکارات سیاست خارجی ایالات‌متحده با هدف گسترش دامنه اینترنت در سطح جهانی، اغلب با غرض‌هایی در سیاست خارجی مانند غلبه بر فقر جهانی از جمله فقر اطلاعاتی و پیشبرد آزادی اطلاعات و آزادی مطبوعات درهم‌تنیده بود (مانجیکیان، 2020).

ایالات‌متحده همچنین نقش کلیدی در تعیین شرایط و استانداردهای بحث در مورد بهترین نحوه دفاع از «فضای سایبری ملی» ایفا کرده است. ایالات‌متحده اولین کشوری بود که در سال 2003 یک استراتژی ملی برای تأمین امنیت فضای سایبری تهیه کرد. این سند که توسط وزارت امنیت داخلی جدید آن زمان آمریکا صادر شد، تهدیدات منعطف بر فضای سایبری آمریکا، از جمله احتمال استفاده تروریست‌ها از این فضا برای بسیج حمایت از پیام‌هایشان و جذب طرفدار را تشریح می‌کرد. ایالات‌متحده همچنین اولین کشوری بود که یک فرماندهی سایبری نظامی ملی[5] را در سال 2009 تأسیس کرد و در ترسیم دکترین‌های استراتژیک حاکم بر آنچه که قلمرو پنجم[6] نامیده می‌شود، رهبری اولیه را بر عهده گرفت (قلمروهای استراتژیک دیگر عبارت‌اند از زمین، دریا، هوا و فضا).

---

[1] ARPAnet
[2] International Commission for the Assignment of Network Names (ICANN)
[3] United States' National Science Foundation
[4] the internet's "backbone"
[5] national military Cyber Command
[6] Fifth Domain

درواقع، ردپای مفهوم استفاده از فناوری فضای سایبری برای اهداف تهاجمی (به‌عنوان WME یا سلاح دارای اثر انبوه) را می‌توان در مفهوم عملیات مشترک بازدارندگی استراتژیک ایالات‌متحده در سال 2004 پیگیری کرد.

علاوه بر این ایالات‌متحده به توسعه مشترک یکی از اولین سلاح‌های سایبری به همراه اسرائیل در سال 2005 اعتبار دارد. کرم استاکس نت که ایران را هدف قرار داده بود، آسیب قابل‌توجهی به برنامه هسته‌ای ایران وارد کرد. امروزه، برنامه‌ریزان آمریکایی، چارچوب‌دهنده‌های کلیدی دکترین‌های استراتژیک فضای سایبری در زمینه‌هایی مانند دفاع سایبری فعال و همچنین در استفاده روزافزون از هوش مصنوعی برای شناسایی و پاسخگویی به تهدیدات سایبری نوظهور هستند. ایالات‌متحده همچنین مدلی را برای به اشتراک‌گذاری اطلاعات تهدیدات سایبری و واکنش اضطراری سایبری بین بخش‌های تجاری و دولتی، از طریق ایجاد تیم‌های واکنش اضطراری سایبری[7] ارائه کرده است. درواقع، اولین تیم واکنش اضطراری سایبری در سال 1988 در دانشگاه کارنگی ملون توسعه یافت. این مدل بر اساس نمونه ایالات‌متحده به‌طور گسترده در سراسر جهان اقتباس شده است.

مقامات نظامی و غیرنظامی ایالات‌متحده نیز از جمله اولین تحلیل‌گرانی بودند که تهدیدات سایبری‌ای را شناسایی کردند که مستقل و تک‌بعدی نبودند، بلکه با تمام بخش‌های زیرساخت اقتصادی، سیاسی و اجتماعی یک کشور درهم‌تنیده بودند. در ابتدای سال 2005، وزارت امنیت داخلی ایالات‌متحده مفهوم زیرساخت‌های حیاتی را تعریف کرد و به شانزده بخش از زیرساخت‌های آمریکا (از تصفیه آب تا حمل‌ونقل) اشاره کرد که به‌طور منحصربه‌فردی در برابر حملات سایبری آسیب‌پذیر بودند و نیاز به اقدامات خاصی برای سخت‌تر کردن این حملات محتمل و اطمینان از انعطاف‌پذیری آن‌ها داشتند (براون و همکاران، 2006). در همان زمان، دولت ایالات‌متحده برای دفاع از دارایی‌های اقتصادی آمریکا در فضای سایبری تلاش می‌کرد. این تلاش از طرقی مثل لابی کردن برای گسترش حمایت از مالکیت معنوی به کارهایی که در فضای سایبری وجود داشت و ذخیره شده بود انجام می‌گرفت.

آگاهی اولیه از پتانسیل مرگبار درگیری‌های سایبری و احتمال اینکه درگیری‌هایی که در فضای سایبری آغاز شده می‌تواند فراتر از آن رفته و پیامدهایی جدی در دنیای واقعی داشته باشد، باعث شد که دولت ایالات متحده نقشی پیشرو در توسعه قوانین و رویه‌های مری منجیکیان[8] با هدف جلوگیری از درگیری سایبری در مقیاس جهانی ایفا نماید. به همین دلیل، ایالات متحده نقش اساسی در توسعه چارچوب‌های حقوقی بین المللی برای حاکمیت فضای مجازی داشته است.

فرماندهی سایبری ایالات متحده آمریکا نقشی کلیدی در ایجاد استراتژی‌های بازدارندگی سایبری و همچنین در زمینه ایجاد اقدامات اعتمادساز در فضای سایبری ایفا کرده است و به دنبال جلوگیری از تشدید درگیری‌ها بین دولت‌ها از طریق ایجاد مکانیسم‌های به اشتراک گذاری اطلاعات و اقدامات مشترک بوده است (منجیکیان، 1394). در عین حال، وزارت بازرگانی ایالات متحده تلاش‌هایی را نیز برای جلوگیری از صادرات سلاح‌های سایبری به دشمنان آمریکایی و جلوگیری از استقرار قوانین سایبری ناقض حقوق شهروندان در مورد حریم خصوصی و آزادی بیان، داشته است. از منظر آمریکا، چنین تحولاتی ممکن است تا حد زیادی مثبت به نظر برسد، و در واقع، سیاستمداران آمریکایی از لحاظ تاریخی معتقدند که ایالات متحده به عنوان بنیان‌گذار اینترنت، مسئولیت منحصر به فردی در پاسبانی از فضای نظام بین‌المللی به عنوان ضامن صلح و ثبات دارد.

آیا هژمونی ایالات متحده آمریکا در فضای مجازی در حال افول است؟

با این حال، ایالات متحده علیرغم موقعیت پیشروی خود به عنوان توسعه‌دهنده دکترین‌ها و قابلیت‌های فضای سایبری، مطمئناً از موضوع حملات سایبری مصون نمانده است. در واقع، استراتژی ملی سایبری 2018 ایالات متحده اشاره می‌کند که ایالات متحده در سال‌های اخیر هدف حملات سایبری ایران، کره شمالی و روسیه و همچنین هدف جاسوسی صنعتی بزرگ چین بوده است (دوور و لی، 2017). علاوه بر این، ایالات متحده در جریان انتخابات ریاست جمهوری آمریکا در سال 2016 مورد حملات قابل توجهی برای هک قرار گرفت. بنابراین، ممکن است بپرسیم که آیا این ناتوانی نمایان شده ایالات متحده در دفاع در برابر حملات روسیه به سیستم انتخاباتی خود که از سال 2016 آغاز شد، نشان می‌دهد که این کشور احتمالاً در تلاش برای دفاع از فضای سایبری و جمعیت خود ضعیف یا حتی ناکام است (دوال، 2019). حال سؤال این است که آیا عصر زوال موقعیت پیشرو ایالات متحده فرارسیده است؟

به اعتقاد برخی تحلیل‌گران در سال‌های اخیر ایالات متحده هر گونه مزیت منحصربه‌فردی که در فضای سایبری در نتیجه موقعیت پیشرو اولیه خود در این محیط از آن برخوردار بود، رو به زوال نهاده است و تعداد و قدرت رقبای جدید در فضای مجازی در حال افزایش است (گیلی و گیلی، 2019). استراتژی سایبری وزارت دفاع ایالات متحده در سال 2018 اشاره می‌کند که ایالات متحده درگیر "رقابت راهبردی طولانی مدت با چین و روسیه" است (وزارت دفاع

[7] Cyber Emergency Response Teams (CERT)
[8] Mary Manjikian

ایالات متحده، 2018). در همین راستا، تحلیل‌گران آمریکایی سه نوع مزیت را شناسایی کرده‌اند که ممکن است چین در مقایسه با ایالات متحده در افزایش موقعیت قدرت خود در فضای سایبری داشته باشد. اولاً، چین درگیر تلاش‌های بلندمدت و هماهنگ برای انجام جاسوسی سایبری، سرقت اسرار تجاری ایالات متحده و به کارگیری فناوری‌های حاصله برای مزیت تجاری بوده است. ثانیاً، چین در تلاشی بلندمدت و هماهنگ برای ایجاد نفوذ در منطقه آسیا از طریق سرمایه‌گذاری در پروژه‌های موسوم به کمربند جاده ابریشم دیجیتالی که در سراسر آسیای جنوب شرقی تا پاکستان امتداد خواهد داشت، درگیر شده است. در نهایت، چین احتمالاً به عنوان یک دولت استبدادی و تک حزبی از مزایایی برخوردار است، از جمله اینکه این کشور توانایی وادار کردن بازیگران دولتی و خصوصی را به انجام اقدامات دفاعی دارد درحالی‌که این اقدامات در یک رژیم دموکراتیک محل تردید است.

برخلاف ایالات‌متحده، دولت چین می‌تواند محتوای اینترنتی ورودی و خروجی از کشورش را فیلتر و کنترل کند و همچنین به دنبال لغو ماهیت گمنامی موجود در اینترنت و ایجاد محدودیت بیشتر و احراز هویت شهروندان خود است؛ طوری که هویت دیجیتالی و واقعی آن‌ها کاملاً مرتبط باشد (سگال، 2018). درواقع، در محیط امروزی، رژیم‌های استبدادی از جمله روسیه، ممکن است در دفاع از فضای سایبری خود مزیتی داشته باشند، زیرا آن‌ها در موقعیت بهتری برای وادار کردن ارائه‌دهندگان خدمات اینترنتی خصوصی به اجرای سیاست‌های خاص در زمینه‌های نظارت و امنیت سایبری قرار دارند. (کلیمبورگ، 2011). در سال‌های اخیر، کشورهایی مانند هند، روسیه و چین، و همچنین تعدادی از کشورهای آفریقایی، در استفاده از به‌اصطلاح «کلید خاموش کردن اینترنت[9]» برای خاموش کردن ارتباطات اینترنتی منطقه‌ای و ملی در طول دوره‌های اختلالات اقتصادی، سیاسی یا اجتماعی موفق بوده‌اند. در مقابل، زمانی که رئیس‌جمهور اوباما در دوران تصدی‌اش این موضوع را مطرح کرد، این تصور که ایالات‌متحده باید یک کلید خاموش کردن اینترنتی در دسترس رئیس‌جمهور داشته باشد، برای مثال، به‌منظور پاسخ به انتشار سریع یک ویروس اینترنتی، به‌طور گسترده با مخالفت شهروندان و مقامات دولتی مواجه شد (استودارت، 2016).

به این معنا که فرهنگ آمریکایی از لحاظ تاریخی آزادی خواهانه بوده و به راه‌حل‌های «دولت بزرگ» برای مشکلات اقتصادی، سیاسی و اجتماعی بی‌اعتماد بوده است. آمریکایی‌ها اغلب نسبت به آنچه که به‌عنوان تجاوز دولت به زندگی خصوصی خود می‌دانند ابراز بی‌اعتمادی می‌کنند. جای تعجب نیست که اکثریت آمریکایی‌ها (57 درصد) احساس می‌کنند که نظارت بر ارتباطات اینترنتی خصوصی آن‌ها یا مشاهده داده‌های خصوصی آن‌ها برای دولت غیرقابل‌قبول است – مگر اینکه شهروندی مشکوک به ارتکاب جرمی از جمله تروریسم باشد (گیه‌ر، 2018). بنابراین، در فضای جامعه آمریکا، نمایندگانی (مجلس) مانند الکساندرا اوکاسیو–کورتز، نماینده ایالت نیویورک، مخالفت خود را با اشکال جدید نظارت بیومتریک اعلام کرده‌اند و استدلال می‌کنند که اتخاذ چنین فناوری‌هایی در یک رژیم دموکراتیک نامناسب است (دارنل، 2019).

درعین‌حال، رویدادهای اخیر در ایالات‌متحده، مانند حمله گسترده روسیه به سیستم انتخاباتی آمریکا که از سال 2016 از طریق رسانه‌های اجتماعی انجام شد، نشان می‌دهد که برنامه‌یزان آمریکایی ممکن است آسیب‌پذیری آمریکا را در برابر موارد جدید اشکال جنگ اطلاعاتی و جنگ سایبری، دست‌کم گرفته باشند؛ از جمله آن‌هایی که با نقاط قوت قدیمی روسیه در زمینه عملیات روانی و اطلاعات نادرست مرتبط هستند. در اینجا این امکان وجود دارد که مزایای قابل توجهی که آمریکا برای مدتی طولانی به عنوان «خالق اینترنت» از آن برخوردار بود، تحلیل‌گران نظامی و اطلاعاتی آمریکا را از خود راضی کرده باشد. جامعه دفاعی آمریکا با اعتقاد به اینکه ایالات متحده از رهبری فرماندهی در هر دو قابلیت دفاعی و تهاجمی در فضای سایبری برخوردار است، این واقعیت را تشخیص نداد که رسانه‌های اجتماعی یک جناح بی‌دفاع را نشان می‌دهند که آماده حمله از سوی دشمنان آمریکا بود (ریوتا، 2019).

علاوه بر این، بسیاری از جنبه‌های خاص «آمریکایی» اینترنت – مانند ظرفیت ارتباطی گمنامی و عدم وجود فیلترینگ – در کشورهای دیگر مورد بازاندیشی قرار می‌گیرند، زیرا دولت‌ها می‌کوشند دیدگاه‌های خود را برای فضای مجازی «خود» بیان و اعمال نمایند. درحالی‌که قبلاً چنین ظرفیت‌هایی به‌عنوان جنبه‌های ذاتی خود اینترنت در نظر گرفته می‌شد، در واقع کشورهای جدید نسخه‌های خود را از اینترنت ایجاد می‌کنند که شامل چنین توانایی‌هایی نمی‌شود. در واقع، اکنون تحلیل‌گران پیشنهاد می‌کنند که اینترنت باز و آزاد ممکن است به‌طور منحصربه‌فردی به‌عنوان یک عامل تهدید باشد. به‌عنوان‌مثال، تهدید اختلال گسترده اجتماعی که از طریق اشکال جنگ روانی آنلاین و مهندسی رسانه‌های اجتماعی ایجاد می‌شود، در جامعه‌ای که ویژگی آن آزادی بیان و فاقد مکانیسم فیلتری مانند «دیوار آتش بزرگ» چین است، بسیار بیشتر است. در نتیجه، ویژگی‌های فنی و سیاسی اینترنت آمریکایی که قبلاً به‌عنوان نقاط قوت ظاهر می شد، اکنون به‌طور فزاینده‌ای به‌عنوان نقاط ضعف به نظر می‌رسد.

کاهش شکاف توانمندی بین ایالات متحده و رقبای آن

[9] internet kill switch

تحلیل‌گرانی مانند جوزف نای، کاملاً پیش‌بینی‌شده، هشدار داده‌اند که ایالات‌متحده نباید انتظار داشته باشد که موقعیت پیشرو مهم خود را به‌عنوان اولین کشور، در رتبه‌بندی بین‌المللی قدرت‌های امنیت سایبری حفظ نماید. در مقایسه با منابع موردنیاز (از جمله پول، آموزش و نیروی انسانی) برای دستیابی به موقعیت پیشرو در توسعه سلاح‌های متعارف یا هسته‌ای، یک کشور می‌تواند نسبتاً ارزان و سریع رتبه خود را در بین قدرت‌های سایبری افزایش دهد (نای، 2016). به همین دلیل، سلاح‌های سایبری به‌عنوان یک تهدید نامتقارن در نظر گرفته می‌شوند که می‌تواند به‌آسانی توسط یک کشور کوچک و یک کشور قدرتمند مورد استفاده قرار گیرد.

بنابراین رتبه‌بندی جهانی قابلیت‌های سایبری بسیار پویا است. امروزه، سانگر پیشنهاد می‌کند که در واقع هفت قدرت سایبری مهم (که او از آن‌ها به‌عنوان «هفت خواهر درگیری سایبری» یاد می‌کند) وجود دارد، یعنی ایالات‌متحده، روسیه، چین، بریتانیا، ایران، اسرائیل و کره شمالی. این‌ها کشورهایی با قابلیت‌های سایبری تثبیت‌شده هستند که رویدادهای مهمی را در عرصه سایبری انجام داده‌اند. بااین‌حال، او خاطرنشان می‌کند که کشورهای دیگری – از ویتنام گرفته تا مکزیک – وجود دارند که به‌عنوان بازیگر در این عرصه نزدیک می‌شوند (سنگر، 2018). در این میان چین به‌طور خاص تمایل خود را برای پیشی گرفتن از ایالات‌متحده در رتبه‌بندی قدرت سایبری و جهش میان قدرت‌های موجود برای به دست گرفتن رهبری بیان کرده است (برنر و لیندسی، 2015). همان‌طور که سایر کشورها در حال دستیابی به قابلیت‌های سایبری قابل‌توجهی هستند، ادعا می‌کنند که توانایی تدوین دکترین‌های سایبری را مطابق با هنجارهای ملی خود و تشکیل اتحادها و گروه‌های قدرت جدید دارند. در اینجا می‌توان به ایجاد بازیگران جدید در فضای مجازی مانند سازمان همکاری شانگهای[10] اشاره کرد که در سال 2001 تشکیل شد (ایندیا تودی، 2018).

درعین‌حال، تلاش‌های آمریکا برای اداره و هدایت توسعه اینترنت از نظر سیاسی، اقتصادی و فرهنگی، با سوءظن بسیاری از کشورها از جمله دشمنان تاریخی آمریکا مواجه شده است؛ خصوصاً با توجه به تحولاتی مانند افشاگری‌های ادوارد اسنودن در سال 2013 در مورد میزان نظارت اینترنتی توسط آژانس امنیت ملی ایالات‌متحده. امروزه، ایالات‌متحده از دیگر بازیگران – مانند اتحادیه اروپا – در تدوین دکترین‌های مربوط به اطلاعات و حریم خصوصی داده‌ها عقب است. اتحادیه اروپا نقش پیشرو را در تدوین هنجارها و خط‌مشی‌های مربوط به حفاظت از حریم خصوصی کاربران و مبارزه با جرائم سایبری برعهده‌گرفته است. همچنین، کشورهای دیگری مانند چین به دنبال تغییر هویت خود از موقعیت هنجار گیر[11] به هنجار گذار[12] در محیط بین‌المللی از طریق پیشبرد ابتکاراتی مانند جاده ابریشم دیجیتال چین بوده‌اند (زنگ، 2017).

امروز، این پرسش پیش می‌آید که آیا ایالات‌متحده همچنان به‌عنوان یک هژمون جهانی در اینترنت عمل می‌کند؟ یا اینکه آیا اینترنت جهانی در حال تقسیم شدن به بلوک‌های منطقه‌ای یا خطوط ملی در طول آن است؟ به‌ویژه در ده سال گذشته، می‌توانیم واکنش‌های ملی سایر کشورها را با هدف پیشبرد و دفاع از ادعاها برای مدیریت و هدایت توسعه فضای سایبری ملی خود شناسایی کنیم. کشورهایی مانند چین و روسیه به‌ویژه این تصور را که ایالات‌متحده باید نقش پیشرو در توسعه و مدیریت فضای سایبری بین‌المللی ایفا کند، زیر سؤال برده‌اند و علاوه بر این، سؤالاتی را در مورد اینکه آیا اینترنت امروز حتی به یک هژمون جهانی نیاز دارد یا خیر، مطرح کرده‌اند.

موانع توسعه خط مشی امنیت سایبری ایالات متحده

در سال‌های اخیر، متخصصان امنیت اطلاعات شروع به صحبت از «فرهنگ امنیت اطلاعات[13]» کرده‌اند که می‌تواند به‌عنوان بسته‌ای از نگرش‌ها و رویه‌هایی تعریف شود که اعضای یک سازمان با اشاره به حراست از امنیت اطلاعات یک شرکت، حفظ و دنبال می‌کنند. فرهنگ امنیت اطلاعات شامل عواملی مانند چگونگی درک کارکنان از نقش‌ها و مسئولیت‌های خود در حفظ امنیت اطلاعات، راه‌هایی که در آن نقض امنیت اطلاعات توسط رهبری شرکت مورد توجه قرار می‌گیرد و چگونگی ادراک مردم از خطرات مرتبط با نقض امنیت اطلاعات را شامل می‌شود (بیور، 2015). ممکن است استدلال شود که کشورها فرهنگ امنیت اطلاعات خود را دارند. اینکه شهروندان یک کشور چگونه حقوق و مسئولیت‌های خود را در محیط آنلاین می‌بینند، چگونه به نقش دولت در نظم‌دهی و ایجاد امنیت در محیط نگاه می‌کنند و اینکه چه مواردی را به‌عنوان استفاده‌های قابل‌قبول و غیرقابل‌قبول از محیط آنلاین می‌دانند، مواردی هستند که ممکن

[10] Shanghai Cooperation Organization (SCO)
[11] norm takers
[12] norm setters
[13] Information security culture

است شهروندان، نگرش‌های متفاوتی در مورد آن‌ها داشته باشند. کشورها همچنین ممکن است سیاست‌ها و رویه‌های متفاوتی برای رسیدگی به نقض امنیت اطلاعات داشته باشند؛ از جمله اینکه کدام بازیگران درگیر هستند و چگونه با دولت ملی تعامل دارند.

در اندیشیدن به چالش‌هایی که ایالات‌متحده به‌ویژه در توسعه سیاست‌های امنیت سایبری با آن مواجه شده است، می‌توان استدلال کرد که فرهنگ امنیت اطلاعات ایالات‌متحده از سه جنبه منحصربه‌فرد است:

اول، ایالات‌متحده از این نظر منحصربه‌فرد است که بسیاری از بازیگران اصلی غیردولتی چهره‌های کلیدی در شکل‌دهی و ایجاد محیط آنلاین (مانند توییتر، گوگل و مایکروسافت) در داخل ایالات‌متحده ایجاد و واقع شده‌اند. بنابراین، چنین شرکت‌هایی از نزدیک با دولت ایالات‌متحده همکاری می‌کنند. با این حال، این شرکت‌ها لزوماً موضع خود را در پایبندی به قوانین، رویه‌ها و هنجارهای آمریکایی به‌عنوان اصلی‌ترین هویت خود در نظر نمی‌گیرند. بنابراین، در سال‌های پس از ظهور این بازیگران، ایالات‌متحده برای مدیریت این بازیگران و بیان ماهیت دقیق رابطه خود با آن‌ها تلاش کرده است.

در اینجا، سگال پیشنهاد می‌کند که در سال‌های اخیر، نوعی جدایی بین دره سیلیکون و واشینگتن، دی.سی. اتفاق افتاده است. در بسیاری از جنبه‌ها، از طریق ایجاد مشارکت‌های دولتی–خصوصی، به‌ویژه در زمینه‌هایی مانند مبارزه با جرائم آنلاین، بازیگران خصوصی همچنان با بازیگران دولتی همکاری می‌کنند. امروزه، مشارکت‌های دولتی–خصوصی شامل اتحاد اعتماد آنلاین و گروه بات‌نت‌های صنعتی[۱۴] است. علاوه بر این، گروه‌هایی مانند اتحاد ملی سایبری قانونی و آموزش [15]با بیش از 80 کسب‌وکار، اطلاعات تهدیدات سایبری را در اختیار تیم‌های واکنش اضطراری سایبری ملی و بین‌المللی قرار می‌دهند (سنای ایالات‌متحده[۱۶]، 2014). مایکروسافت یک برنامه اطلاعاتی تهدید سایبری دارد که اطلاعات مربوط به بات‌نت‌ها را هم برای ارائه‌دهندگان خدمات اینترنتی و هم برای تیم‌های واکنش اضطراری سایبری [17]تحت حمایت دولت ایالات‌متحده در دسترس قرار می‌دهد. مایکروسافت همچنین در سطح بین‌المللی با دولت‌ها نیز کار می‌کند، برای نمونه می‌توان به امضای قرارداد با تیم واکنش اضطراری رایانه‌ای اسپانیا[۱۸]، اشاره کرد. مایکروسافت همچنین دارای یک واحد جرائم دیجیتال با بیش از 100 متخصص فنی و حقوقی است که برای مبارزه با جرائم سایبری و بهبود امنیت سایبری مشغول به فعالیت هستند.

بااین‌حال، شرکت‌های فناوری مستقر در آمریکا نیز در برخی موارد مواضع سیاستی متضاد با اهداف اعلام‌شده امنیت سایبری آمریکا در پیش‌گرفته‌اند. به‌عنوان‌مثال، پس از حمله تروریستی 2015 سن برناردینو، دفتر تحقیقات فدرال ایالات‌متحده از شرکت اپل به دلیل دسترسی به سوابق تلفن همراه متعلق به یکی از تروریست‌ها شکایت کرد. یک مناقشه حقوقی جاری حول محور این موضوع وجود داشت که آیا تولیدکنندگان تلفن همراه در ایالات‌متحده باید ملزم به ایجاد یک "در پشتی[۱۹]" در دستگاه‌های خود باشند که به مجریان قانون ایالات‌متحده اجازه می‌دهد به اطلاعات کاربران دسترسی داشته باشند یا نه. مسائل ثانویه، حول قلمروهای سرزمینی متمرکز هستند که درخواست‌های ایالات‌متحده ممکن است در آن‌ها غالب باشد (به‌عنوان‌مثال، اگر داده‌های تولیدشده توسط یک کاربر آمریکایی در خارج از ایالات‌متحده در یک مقرّ اپل در اروپا ذخیره می‌شد، آیا اپل همچنان ازنظر قانونی موظف است این اطلاعات را به مجریان قوانین ایالات‌متحده تحویل دهد؟) و در سال 2016، مارک زاکربرگ، بنیان‌گذار فیس بوک، در مقابل کنگره ایالات‌متحده شهادت داد که فیس بوک در ماه‌های منتهی به انتخابات ریاست جمهوری ایالات‌متحده، تبلیغاتی با ماهیت سیاسی در پلتفرم خود فروخته است. قانون‌گذاران ایالات‌متحده استدلال کردند که زاکربرگ و تیمش باید دقت لازم را در راستی‌آزمایی خریداران این آگهی‌ها به کار می‌گرفتند تا از مداخله خارجی ناروا در انتخابات آمریکا محافظت می‌شد. زاکربرگ پاسخ داد که فیس‌بوک صرفاً «پلتفرمی است که محتوا را میزبانی می‌کند» و مسئولیت اخلاقی و قانونی‌اش برای نظارت بر این محتوا محدود است (چاندر، 2012). علاوه بر این، به نظر می‌رسید که او به این مسئله اشاره می‌کند که فیس‌بوک در قبال دولت آمریکا مسئولیت بیشتری نسبت به سایر دولت‌ها ندارد.

بنابراین آمریکا در موقعیت منحصربه‌فردی قرار دارد. ایالات‌متحده به‌عنوان میزبان سرزمینی بسیاری از این شرکت‌های فناوری بین‌المللی، موظف است از نزدیک با آن‌ها همکاری کند، به‌ویژه در زمینه مبارزه با موضوعاتی مانند رشد نفرت پراکنی یا سازمان‌دهی تروریستی آنلاین.

---

[14] Online Trust Alliance (OTA) & the Industry Botnet Group (IBG)
[15] National Cyber-Forensics and Training Alliance (NCFTA)
[16] U.S. Senate
[17] internet service providers and US government sponsored Computer Emergency Response Teams (CERTs)
[18] INTECO
[19] back door

با این حال، با توجه به این واقعیت که این بازیگران شرکت‌های خصوصی هستند، مسئولیت نهایی تصمیم‌گیری، برای مثال، اینکه کدام بازیگران بسیار خطرناک‌تر از آن هستند که اجازه حضور در رسانه‌های اجتماعی را داشته باشند، درنهایت نه بر عهده دولت، بلکه برعهده شرکت‌ها خواهد بود (چاندر، 2012). درعین‌حال، نه قوانین نیرومندی وجود دارد که چنین شرکت‌هایی را ملزم به اولویت دادن به منافع امنیتی ایالات‌متحده بر دیگر سیاست‌ها و اولویت‌های شرکتی خود کند و نه هنجارهای شرکتی در مورد این موضوع وجود دارد (در مقابل، شرکت‌های خصوصی مستقر در چین و روسیه ممکن است با قوانین بسیار سخت‌گیرانه‌تری در رابطه با اولویت‌ها و مسئولیت‌های سیاسی‌شان مواجه شوند).

امروزه، قانون‌گذاران آمریکایی پیشنهاد کرده‌اند که شرکت‌های انحصاری مانند فیس‌بوک را از بین ببرند تا از قدرتی که امثال این بازیگران غیردولتی برای تصمیم‌گیری درباره چنین موضوعاتی در مقایسه با اختیارات محدود ایالت‌ها دارند، جلوگیری نمایند. طرح‌های دیگر بر ایجاد انواع جدیدی از مشارکت‌های دولتی–خصوصی متمرکز شده‌اند که در آن دولت‌ها و شرکت‌ها با یکدیگر برای مبارزه با چنین تهدیداتی همکاری خواهند کرد. همان‌طور که شرکت‌ها فناوری های جدیدی را در زمینه‌هایی مانند هوش مصنوعی و تجزیه‌وتحلیل داده‌ها ایجاد می‌کنند، نیاز به بیان واضح‌تر و تنظیم نحوه همکاری دولت‌ها با این بازیگران روشن می‌شود.

دومین جنبه منحصربه‌فرد فرهنگ امنیت سایبری آمریکا، این واقعیت است که سیاست خارجی آمریکا به سمت موضع انزواگرایی و دستور کار «اول آمریکا» گرایش داشته است. چنین رویکردی در دوران ترامپ جدی‌تر شد. این موضوع از سوی بسیاری به‌عنوان کنار گذاشتن آمریکا از نقش رهبری و پیشرو بودن در جهان، تلقی می‌شود. همان‌طور که ویکت، اسمیت و اسمارت (2017) خاطرنشان کردند:

دیدگاه ترامپ بیشتر ناسیونالیستی است تا انزواطلبانه. او به‌خودی‌خود خروج ایالات‌متحده از جهان را پیشنهاد نمی‌کند؛ اما او تفسیر محدودتری از منافع حیاتی آمریکا نسبت به پیشینیان خود دارد و احتمالاً تعاملات بین‌المللی را بیشتر در چارچوب اقتصادی و از جنس کسب‌وکار ارزیابی خواهد کرد. موضع مبارزات انتخاباتی «اول آمریکا» او حاکی از تشخیص محدود از خیر عمومی جهانی یا تمایل به مداخله برای حمایت از آن است.

تعهد ضعیف‌تر به «خیر عمومی جهانی» به‌راحتی می‌تواند به تعهد ضعیف‌تر ایالات‌متحده برای حمایت از پایداری و امنیت مداوم خود اینترنت به‌عنوان یک کالای عمومی جهانی تبدیل شود. به‌خصوص اگر رئیس‌جمهور ترامپ در انتخابات 2020 به دور دوم ریاست جمهوری دست یابد، ممکن است شاهد تعهد مالی و سازمانی ضعیف‌تر آمریکا برای حمایت از طرح‌هایی مانند به اشتراک‌گذاری اطلاعات تهدیدات سایبری و فرصت‌های آموزشی امنیت سایبری ایالات‌متحده با متحدانی چون کشورهای اتحادیه اروپا و ناتو باشیم. چنین نتیجه‌ای می‌تواند یک چشم‌انداز سایبری کاملاً متفاوت را نه‌تنها در ایالات‌متحده بلکه در سطح جهانی ایجاد کند. برای مثال در حال حاضر، نمی‌توان واکنش قابل‌توجهی از سوی آمریکا به ابتکار عمل جاده ابریشم دیجیتال چین شناسایی کرد، و علی‌رغم اعلام آمریکا مبنی بر برداشتن گام‌هایی در جهت توسعه فرماندهی فضایی برای تأمین امنیت ماهواره‌های دیجیتال و جریان‌های داده، گام‌های محدودی در جهت تأمین این هدف برداشته‌شده است.

علاوه‌بر این، ممکن است انتظار داشته باشیم که شرکت‌های خصوصی وارد خلأ ناشی از کاهش حضور ایالات‌متحده در سطح بین‌المللی، به‌ویژه در حوزه امنیت سایبری شوند. بنابراین، تعجب‌آور نیست که، برای مثال، شرکت‌های خصوصی برای صدور بیانیه بین‌المللی Asilomar در سال 2017 در مورد توسعه اخلاقی هوش مصنوعی، که اصولی برای توسعه اخلاقی هوش مصنوعی از منظر صنعتی ارائه می‌دهد، همکاری کرده‌اند. در اینجا، شرکت‌های خصوصی در تدوین اصول، ایجاد اجماع و صدور بیانیه‌ها سریع‌تر از هر نهاد رسمی مانند وزارت دفاع ایالات‌متحده بوده‌اند (الکساندر، 2017).

آخرین جنبه فرهنگ امنیت سایبری ایالات‌متحده که می‌توان آن را منحصربه‌فرد توصیف کرد، روشی است که در آن بازیگران امنیت سایبری آمریکا به دنبال ایجاد تعادل بین الزامات دوگانه تدوین (1) رویه‌های عمل‌گرایانه به‌منظور واکنش به رخنه‌های امنیتی به‌خصوصِ واقعی و پیشنهادی، (2) و تدوین مجموعه گسترده‌تری از اصول در سطح انتزاع بالاتری بوده‌اند. در دوره ریاست جمهوری اوباما، ایالات‌متحده در رابطه با بروز برخی حوادث به‌خصوص امنیتی و ارائه نکردن حتی یک نظریه جهانی در مورد اینکه چه نوع حملات سایبری به چه عواقب خاصی منجر می‌شود، مقصر بود. در همین راستا، اخیراً تحلیل‌گران در بحث در مورد یک رخنه امنیتی که دفتر مدیریت و بودجه ایالات‌متحده را هدف قرار داده بود، استدلال کرده‌اند که ایالات‌متحده احتمالاً در تدوین دکترین‌ها و طرح‌های استراتژیک در مقیاس بزرگ بهتر از اجرای شیوه‌های خاص تأمین امنیت عمل کرده است (Dourado & O'Sullivan, n.d). به‌عبارت‌دیگر، درحالی‌که فرماندهی سایبری ایالات‌متحده دکترین‌هایی کلیدی را در زمینه بازدارندگی سایبری، کنترل تسلیحات سایبری و دفاع فعال سایبری تدوین کرده است، اما هنوز مشخص نیست که در صورت انجام حملات به انتخابات بعدی، ایالات‌متحده چه خواهد کرد. (در اینجا، ممکن است یک سیاست منسجم محرمانه وجود داشته باشد؛ بااین‌حال، اگر چنین باشد، شاید تابه‌حال این سیاست مؤثر عمل‌نکرده است.)

بنابراین تجربه آمریکا منحصربه‌فرد است. درحالی‌که سایر کشورها ممکن است از یک موقعیت ضعیف شروع به ایجاد فرهنگ، قوانین و خط‌مشی‌های امنیت سایبری قوی کرده باشند، ایالات‌متحده اما در موقعیتی پیشرو قرار دارد که از مزایای آن بهره‌مند است. و درست همان‌طور که تحلیلگران اولیه اینترنت پیشنهاد کردند که فقط یک رویداد ویرانگر مانند "پرل هاربر[20] سایبری" لازم است تا سیاست‌گذاران و شهروندان از خطرات ناشی از یک خط‌مشی سایبری به‌اندازه ناکافی قوی، آگاه شوند. ممکن است دوباره بپرسیم که چه نوع رویدادهایی می‌توانند به‌طور بالقوه منجر به بازنگری در موقعیت‌های فعلی امنیت سایبری آمریکا در زمینه‌های همکاری عمومی و خصوصی و تعهد منابع استراتژیک می‌شود.

[20] پرل هاربر (Pearl Harbor) یک بندر در مجمع‌الجزایر هاوایی است. معروفیت این بندر به خاطر حمله ارتش ژاپن به پایگاه دریایی ایالات متحده آمریکا در ۷ دسامبر ۱۹۴۱ است. در پی این حمله، آمریکا وارد جنگ جهانی دوم شد. در حمله هوایی ژاپنی‌ها ناوگان اقیانوس آرام آمریکا از جمله هفت رزمناو نابود شدند (توضیح مترجم).

کانادا

مقدمه

امروزه چند رویداد بر چرخه اخبار، 24 ساعته غالب هستند. از جمله، هک و نفوذ ادعایی روسیه به کنوانسیون ملی دمکراتیک 2017[۲۱] و همچنین تلاش هکرهای روسی برای دسترسی به زیرساخت‌های بریتانیا و ایالات متحده. این فعالیت‌های سایبری شرورانه، به سادگی آسیب‌پذیری پلتفرم‌های فناوری اطلاعات (IT) ما را آشکار کرد. به‌طور کلی دو نوع حمله سایبری وجود دارد: یکی علیه دولت‌ها و دستگاه‌های آنها و دیگری علیه بخش‌های دولتی و خصوصی مانند مؤسسات مالی، خدماتی و خدمات اینترنتی. در واقع هدف بخش بزرگی از حمله‌های سابیری از دسته دوم هستند.

این فصل در دو بخش اصلی تنظیم شده است. بخش اول به امنیت سایبری جهانی و محیط تهدید سایبری می‌پردازد که در آن مفهوم حاکمیت در فضای سایبری از جمله وضعیت فعلی حاکمیت بین‌المللی نشان داده شده است. بخش دوم با بیانیه استراتژی امنیت سایبری کانادا از جمله زمینه کانادا در مورد امنیت سایبری آغاز می شود. در این بخش درک فرهنگی کانادا، نهادها، نقش قانون‌گذار و پیامدهای اجتماعی امنیت سایبری مورد بحث قرار می‌گیرد.

امنیت سایبری جهانی و محیط تهدید سایبری

به طور کلی، مهاجمان سایبری یا داده‌ها را مورد هدف قرار می‌دهند (شایع ترین شکلی که باعث اختلال در سرویس می شود) و یا به سیستم‌های کنترل حمله می‌کنند (شکل نادری که برای دست‌کاری زیرساخت‌های فیزیکی در نظر گرفته شده است).

با در نظر گرفتن این دو شکل از حمله، کارشناسان معتقدند که آسیب فیزیکی ناشی از تروریسم سایبری در گذشته در مقیاس وسیع رخ نداده است، اگرچه فناوری و انگیزه بازیگران متعددی با سرعت در حال رشد است. علی‌رغم این واقعیت که بازیگران غیردولتی، مثل تروریست‌ها و هکرها، به رقابت برای دستیابی به سهم خود از منابع به حمله ادامه می‌دهند، «جاسوسی و خرابکاری پیچیده در حوزه سایبری هنوز به قابلیت‌ها، عزم و اراده یک دولت–ملت نیاز دارد. هنوز خطرناک‌ترین بازیگران در حوزه سایبری دولت–ملت‌ها هستند.» (تیلر، 2015). علاوه‌بر این، یک آژانس مجری قانون آمریکایی به نوع جدیدی از «تهدید سایبری ترکیبی ... که در آن دولت–ملت‌ها با هکرهای جنایتکار برای انجام فعالیت‌های مخرب کار می کنند» اشاره کرد (وزارت دادگستری ایالات متحده، 2017).

مفهوم حاکمیت در فضای سایبری

مریام وبستر[۲۲] حاکمیت را به سه صورت تعریف می کند:

1) قدرت برتر به ویژه بر بدنه سیاسی

2) آزادی از کنترل یا استقلال خارجی

3) نفوذ کنترل (مریام وبستر، 2018)

بر اساس مفهوم «وستفالن» از یک دولت–ملت که در آن مرزهای مشخص یک دولت از دیگری مشخص می‌شود، دولت–ملت‌های مدرن نیز حقوق مسلم خود را بر فضای سایبری دنبال می‌کنند. اکنون مفهوم حاکمیت، فضای مجازی را نیز در بر می‌گیرد که در آن بازیگران غیردولتی نه تنها از بازیگران دولتی بیشتر هستند، بلکه آزاد هستند تا در طیف گسترده‌ای از اقدامات شرکت کنند. با این وجود، هیچ اصطلاح مورد توافقی مانند فضای سایبری روسی یا ژاپنی یا آمریکایی وجود ندارد؛ زیرا همه افراد حق حضور در فضای مجازی را دارند. در اینجا سه تناقض بین حاکمیت دولت و فضای سایبری قابل ذکر است:

1. تضاد بین حاکمیت سایبری و روح اینترنت. انحصار حاکمیت کلاسیک دولت، بر خلاف روح اینترنت است که بر مفهوم اتصال نامحدود بین‌المللی استوار است.

---

[21] 2017 Democratic National Convention (DNC)
[22] Merriam-Webster

2. تضاد بین حاکمیت سایبری و حقوق بشر.
3. تضاد بین حاکمیت سایبری و مداخله انواع ذی‌نفعان در حکومت.

به منظور تقویت امنیت سیستم‌های اطلاعاتی و مخابراتی جهانی، سازمان ملل متحد در سال 2004 «گروه کارشناسان دولتی[۲۳]» را تأسیس کرد. پس از مشاهده تلاش‌های بیهوده توسط این مجموعه برای تدوین یک هنجار استاندارد برای رسیدگی به مسائل مربوط به حاکمیت دولت، از سوی کارشناسان و همچنین سیاست‌گذاران در ایالات متحده، دو دسته از پیشنهادات مطرح شد. یکی پیشنهاد ایجاد هنجارها با دشمنان ایالات متحده است که به‌طور سنتی هژمونی ایالات‌متحده را در مسائل سایبری به چالش می کشند. پیشنهاد دیگر سعی دارد ائتلافی از پیروان هنجارها یا افراد خوب بسازند تا اقدامات دفاعی مشترک انجام شود.

استراتژی امنیت سایبری کانادا

کانادا فضای سایبری را چنین تعریف می کند: «... دنیای الکترونیکی که توسط شبکه‌های به هم پیوسته فناوری اطلاعات و داده‌های موجود در آن شبکه‌ها ایجاد شده است. این یک مشترک جهانی[۲۴] است که در آن بیش از 1.7 میلیارد نفر برای تبادل ایده‌ها، خدمات و دوستی با هم مرتبط هستند.» (امنیت عمومی کانادا، 2: 2010).

علاوه بر این، دیدگاه کانادا در مورد امنیت سایبری چنین توضیح داده شده است: «امنیت سایبری قوی یک عنصر اساسی از نوآوری و شکوفایی کانادا است.» همچنین ذکر شده است که دولت و شرکای آن به کار بر روی سه موضوع اصلی ادامه خواهند داد: امنیت و انعطاف‌پذیری، نوآوری سایبری، و رهبری و همکاری (دولت کانادا، b2018).

در اولین استراتژی امنیت سایبری کانادا[۲۵](CCSS)، مشارکت بین بخش‌های استانی، ملی و خصوصی به عنوان یک عنصر حیاتی ذکر شده است. این سند، همچنین بر ماهیت مکمل استراتژی‌های ایالات متحده، بریتانیا و استرالیا تأکید می‌کند تا همه این کشورها بتوانند اطلاعات مربوط به تهدیدات و منابع لازم برای جلوگیری از حملات سایبری با هم به اشتراک بگذارند.

علاوه‌براین، کانادا تنها کشور غیراروپایی امضا کننده کنوانسیون شورای اروپا در مورد جرایم سایبری[۲۶] می‌باشد.

طرح «فضای سایبری را امن بگیر[۲۷]» هم با هدف ارائه پیشنهادات مربوط به افزایش امنیت سایبری به بخش خصوصی و مردمی در سال 2018 راه‌اندازی شد.

بستر امنیت سایبری کانادا

بر اساس کتاب حقایق اینترنتی[۲۸]، 75 درصد کانادایی‌ها نسبت به تهدیدات سایبری ابراز نگرانی کرده‌اند. این رقم نسبت به سال قبل 13 درصد افزایش یافته است. با این حال، امنیت سایبری کانادا مانند اکثر کشورهای غربی با امنیت ملی آمیخته است. امنیت این کشور به شدت بر «عملکرد بدون وقفه زیرساخت‌های حیاتی خود متکی است که اختلالات آن می تواند تأثیر جدی بر زندگی، ایمنی جوامع و اقتصاد داشته باشد.» (امنیت عمومی کانادا، 2016b).

دولت همچنین مرکز واکنش به رویدادهای سایبری کانادا[۲۹] (CCIRC) را برای نظارت و ارائه مشاوره کاهش تهدیدات سایبری و هماهنگی واکنش ملی به هر حادثه سایبری ایجاد کرده است (ایمنی عمومی کانادا، a2016). نُه سازمان دولتی کانادا مسئول اجرای CCSS هستند. CCIRC در محل اتصال بخش خصوصی و عمومی در کانادا قرار دارد که در آن مشارکت با مالکان و اپراتورهای زیرساخت‌ها حیاتی از اهمیت ویژه‌ای برخوردار است.

---

[23] Group of Governmental Experts (GGE): 25 کشور در این گروه عضو هستند که 5 جلسه در موضوع حکمرانی جهانی برگزار کرده‌اند. این گروه اصول حکمرانی خود را در گزارش‌های مربوط به سال‌های 2013 و 2015 منتشر کرده است.

[24] Global commons: دارایی‌هایی که تمام جهان در مالکیت آن سهم یکسانی دارند مانند اتمسفر و سطح اقیانوس‌ها.

[25] Canada's first Cyber Security Strategy (CCSS)

[26] Europe's Convention on Cyber Crime

[27] Get syber safe

[28] Internet factbook

[29] Canadian Cyber Incident Response Centre

همچنین کانادا دستورالعملی[30] را به تأیید کشورهای G7 رسانده است. این دستورالعمل "هشت بلوک اساسی" را برای ایجاد استراتژی امنیت سایبری توصیف می‌کند: 1) استراتژی و چارچوب امنیت سایبری، 2) حکومت، 3) ارزیابی ریسک و کنترل، 4) نظارت، 5) پاسخ‌گویی، 6) بازیابی[31]، 7) به اشتراک گذاری اطلاعات و 8) یادگیری مستمر (فریدمن، 2017).

فهم فرهنگی کانادا، نقش بخش خصوصی و قانون‌گذار

نگاهی گذرا به انواع مختلف حملات سایبری، سرقت داده‌ها و وضعیت آمادگی حمله سایبری، الگوهای خاصی از سازمان‌ها و افراد در کانادا را نشان می‌دهد. در این زمینه، چندین درک فرهنگی مرتبط با امنیت سایبری مورد بحث قرار می‌گیرد.

1- *سطح سازمانی:* درک کلی از حمله سایبری و پیامدهای آن بین سازمان‌های دولتی و غیردولتی متفاوت است. به طور معمول، بیشتر سازمان‌های دولتی به غیر از سازمان‌هایی که با امنیت ملی سر و کار دارند، دستورالعمل‌هایی ناظر به ماهیت امنیت سایبری ارائه می‌کنند که شامل بررسی نقش کارکنان و توجه به اقدامات پیشگیرانه است. با وجود اینکه بخش فناوری اطلاعات هر سازمان، نقض داده‌ها را نظارت می کند اما شعبه‌های فردی در سطح بخش یا زیربخش فاقد منابعی برای آموزش کارکنان و اجرای قوانین هستند. اما در سوی دیگر، سازمان‌های غیردولتی، به‌ویژه سازمان‌های تجاری، سرمایه‌گذاری هنگفتی بر روی زیرساخت‌های دفاع سایبری می‌کنند. آنها کارکنان خود را به‌طور مؤثر برای نقض احتمالی داده‌ها رصد می‌کنند و اطلاعات را با دیگران به روشی مشترک به اشتراک می‌گذارند. همان‌طور که معلوم شد، این سازمان‌های غیردولتی چابک هستند و می‌توانند خود را با تغییرات تطبیق دهند. ضرورت تغییر ذهنیت سازمان‌های دولتی برای مقابله با تهدیدات سایبری در حال تحول، نیازمند زمان است. مهم‌تر از همه، تغییر طرز تفکر از پیشگیری از سرقت داده به پذیرش سرقت داده مهم است. صرف نظر از انواع قابلیت‌های دفاعی سایبری موجود، یک مهاجم سایبری ممکن است راهی در داخل یک سیستم پیدا کند، زیرا تهدید حمله از درون می‌آید.

2- *سطح فردی:* از نظر فرهنگی، امنیت سایبری اغلب بر حسب ترس ناشی از احتمال از دست رفتن داده‌های شخصی از طریق آژانس‌های امنیتی دولتی با استفاده از ابزارهای نظارت انبوه یا توسط هکرهای ناشناس و شرکت‌های تجاری درک می‌شود. با این وجود، طبق یک نظرسنجی جدید، «کانادایی‌ها عمیقاً برای حفظ حریم خصوصی ارزش قائل هستند، اما می‌ترسند کنترلی که بر اطلاعات شخصی خود دارند را از دست بدهند» (Office of Privacy Commissioner of Canada، 2018b). به همین دلیل است که در یک نظرسنجی دیگر، 78 درصد از کانادایی‌ها به طور گسترده از الزامات سازمان‌های دولتی برای حفاظت مناسب از اطلاعات شخصی و 71 درصد از نوسازی قانون حفظ حریم خصوصی به‌گونه‌ای که بتواند برای دفتر نخست‌وزیر دفاتر وزرای کابینه قابل اجرا باشد، حمایت کردند. (CISION، 2017).

3- *تاب‌آوری سازمانی:* افراد و همچنین سیستم‌ها باید برای دریافت حمله و بازگشت به عملکرد عادی آماده باشند. در اینجا مفهوم تاب‌آوری باید به عنوان فرایندی از پایین به بالا و از بالا به پایین در نظر گرفته شود. فرآیند پایین به بالا شامل قوانین سازمانی ناظر به آگاهی امنیتی است که کارکنان باید از آنها با جدیت پیروی کنند (سولومون، 2017). رویکرد بالا به پایین شامل قابلیت‌های سخت‌افزاری سازمان برای دفاع از خود، دفع حمله و بازگشت به عملیات عادی با حداقل ضرر (هم سخت‌افزار و هم زمان خرابی) است. در یک وضعیت ایده‌آل، هر دو این رویکردها باید همگرا شوند و یک سیستم تاب آوری ایجاد کنند.

4- *گزارش سرقت داده‌ها:* دولت کانادا گزارش کردن سرقت داده‌ها را اجباری کرد. این قانون از این نظر اهمیت دارد که اکثر سازمان‌ها به دلیل ترس از دست دادن شهرت سازمانی، تمایلی به گزارش دادن به سرقت رفتن داده‌های خود ندارند. چنین طرز فکری باید تغییر کند تا از داده‌های شخصی مشتریان برای کسب‌وکار و همچنین سازمان‌های دولتی محافظت شود.

5- *نقش بخش خصوصی:* این نقش به دو دلیل مهم است: بخش خصوصی دارای اطلاعات شخصی میلیون‌ها کانادایی است. علاوه‌بر این، بسیاری از آنها برای سازمان‌های دولتی کار می‌کنند و با داده‌های حساس سروکار دارند. در این راستا، بررسی وضعیت جهانی امنیت اطلاعات در سال 2018 چهار درس ارزشمند را برای بخش خصوصی در سراسر جهان ارائه کرد. یکی، رشد دستگاه‌های دیجیتال به مدیریت ریسک می‌انجامد (اشاره به انفجار دستگاه های تلفن همراه)؛ دوم، رهبران کسب‌وکارها خطرات جدیدی را در ارتباط با فناوری‌های نوظهور می‌بینند (به عنوان مثال، GPS و فناوری‌های نظارتی)؛ سوم، تهدیدات سایبری برای یکپارچگی داده‌ها (اشتراک‌گذاری داده در بسیاری از پلتفرم‌های دیجیتال و همچنین رمزگذاری داده‌ها) و چهار، کارکنان فعلی عامل اصلی حوادث امنیتی هستند (عدم کنترل بر کارمندان در محل کار). (PWC، 2018).

6- *قانون‌گذار:* از نظر قوانین، کانادا موارد زیر را وضع کرده است:

1) قانون ضد هرزنامه

---

[30] G7 Fundamental Elements of Cyber Security

[31] recovery

2) قانون حفظ حریم خصوصی دیجیتال[۳۲]

3) قانون حفاظت از اطلاعات شخصی و اسناد الکترونیکی[۳۳]

کمیسیون رادیو تلویزیون و مخابرات کانادا[۳۴] مسئولیت اصلی اجرای قانون ضد هرزنامه را بر عهده دارد. همچنین در 10 مارس 2015، قانون محافظت از کانادایی‌ها در برابر جرائم آنلاین به اجرا درآمد. این قانون به آژانس‌های مجری قانون، قدرت‌های تحقیقاتی جدید و تخصصی می‌دهد تا علیه بهره‌کشی جنسی از کودکان اینترنتی اقدام کنند و فعالیت‌های جرایم سازمان‌یافته آنلاین را مختل کنند (Global Affairs Canada، 2018).

موارد متمایز کننده کانادا و پیامدهای اجتماعی قانون سایبری

همکاری جهانی و تفاهم بین دولت و بخش خصوصیِ ارائه دهنده خدمات فناوری اطلاعات، در حفاظت از فضای سایبری بسیار مهم است. در راستای این مفهوم، گروه Eyes-5 به دنبال توافق بریتانیا و ایالات متحده در سال 1946 ایجاد شد (فارل، 2013). در درجه اول، در این توافق‌نامه، کشورهای عضو[۳۵] بر سر اشتراک‌گذاری داده‌ها برای محافظت از امنیت ملی خود توافق کردند. در بیانیه اخیر خود، خطر ناشی از «بردارهای جدید برای آسیب» برجسته شد و از شرکت‌های فناوری اطلاعات (یعنی مجمع جهانی اینترنت برای مقابله با تروریسم[۳۶]، جایی که گوگل، فیس بوک، مایکروسافت و توییتر عضو هستند) خواسته شد تا با جوامع اطلاعاتی خود در مقابله با تروریسم و بهره‌کشی از کودکان همکاری کنند (هریس، 2018). بنابراین، کانادا، به عنوان عضوی از این گروه، واقعاً از مزایای منحصر به فردی در زمینه به اشتراک گذاری داده در میان توسعه یافته‌ترین کشورهای روی زمین برخوردار است.

همچنین کانادا دارای یک مؤسسه منحصربه‌فرد به نام OPC است که اولاً توصیه‌ها و اطلاعاتی را در مورد حفاظت از اطلاعات شخصی ارائه داده و ثانیاً اجرای دو قانون فدرال در مورد حریم خصوصی را بر عهده دارد. این مؤسسه نهادهای دولتی فدرال را تنظیم کرده و کسب‌وکارهای خصوصی را در مدیریت اطلاعات شخصی راهنمایی می‌کند. علاوه بر این، OPC نقش مهمی در نظارت و مشاوره به سیاست‌گذاران در مورد حفظ تعادل بین حقوق فردی برای حفظ حریم خصوصی در مقابل امنیت ایفا می کند. در واقع، نیاز به حفاظت از امنیت کانادایی‌ها بدون شک بر دوش دولت است، اما این نباید به ضرر حریم خصوصی مردم باشد. OPC همچنین تحقیقاتی را در مورد مسائل مربوط به حفاظت از حریم خصوصی در فعالیت‌های امنیت سایبری انجام می‌دهد. نظرسنجی این سازمان در سال 2016 دو دیدگاه اصلی در این زمینه را به ما نشان می‌دهد.

اول، 74 درصد از کانادایی‌ها احساس کردند که نسبت به ده سال پیش از اطلاعات شخصی خود محافظت کمتری دارند. با این حال، آنها حریم خصوصی را بر سایر موارد ترجیح می‌دهند و شدیداً به عدم دخالت سازمان‌های دولتی در زندگی خصوصی خود اعتقاد دارند. روندهای آماری نشان می‌دهد که کانادایی‌ها به طور فزاینده‌ای از مخمصه مسائل مربوط به حریم خصوصی دیجیتال آگاه می‌شوند و یاد می‌گیرند که چگونه از داده‌های شخصی محافظت کنند. به همین دلیل است که آنها بیشتر از قوانین امنیت سایبری و پیامدهای آن آگاه هستند.

دوم، علی‌رغم زندگی در عصر افول حریم خصوصی، در این نظرسنجی از کانادایی‌های شرکت‌کننده پرسیده شد که در مورد «نظارت دولت بر فعالیت‌های شهروندان برای اهداف امنیت عمومی» چه احساسی دارند. در پاسخ، 26 درصد ابراز نگرانی کردند و 40 درصد اظهار داشتند که تا حدودی نگران هستند؛ یعنی 66 درصد از کانادایی‌ها به طور کلی نگران هستند. این یافته به ما می‌گوید که جاسوسی سازمان‌های دولتی از شهروندان آن بدون دلیل موجه پذیرفته نیست و از این واقعیت ناشی می‌شود که کانادایی‌ها حریم خصوصی را بر ایمنی ترجیح می‌دهند. در این نظر سنجی 50 درصد مردم گفته‌اند که سازمان‌های مجری قانون در حال حاضر صلاحیت یا قدرت قانونی کافی برای جمع‌آوری اطلاعات خصوصی شهروندان برای امنیت ملی یا امنیت عمومی ندارند. با این وجود 33 درصد موافق نیستند که این سازمان‌ها به قدرت بیشتری برای جمع آوری اطلاعات نیاز دارند. این داده‌ها نشان می‌دهد که در حالی که اکثر کانادایی‌ها نیاز به نظارت بر شهروندانی را که ممکن است تهدیدی برای امنیت ملی باشند، ارزش می‌گذارند؛ اما از تأیید کلی جمع‌آوری اطلاعات پشتیبانی نمی‌کنند.

نتیجه‌گیری

[32] the Digital Privacy Act

[33] personal information protection and eletronic dcuments (PIPEDA)

[34] Canadian Radio-television and Telecommunications Commission (CRTC)

[35] استرالیا، نیوزلند، کانادا، بریتانیا و ایالات متحده آمریکا

[36] Global Internet Forum to Counter Terrorism

هر چه زندگی خصوصی و عمومی ما بیشتر دیجیتالی می‌شود، بیشتر مستعد دخالت بازیگران دولتی یا غیردولتی هستیم. در این راستا، تنها راهی که می‌توانیم آسیب‌پذیری‌های خود را بهبود بخشیم، آگاهی از آسیب‌پذیری‌های خود در دنیای سایبری و شناخت ابزارهای مناسب برای مقابله با آنها است. به همین ترتیب، مانند سایر دولت‌ها، کانادا نیز قوانینی وضع و مؤسساتی را تأسیس کرده است؛ اما وظیفه دفاع از خود در برابر تهدیدات سایبری بر عهده خود مردم است.

در این فصل ابتدا امنیت سایبری جهانی و محیط‌های تهدید سایبری و سپس مفهوم حاکمیت در دنیای سایبری و حکمرانی بین‌المللی در حوزه سایبری مورد بحث قرار گرفت. یکی از عواملی که مانع تدوین یک قانون/هنجار بین‌المللی بر رفتارهای سایبری می‌شود، تمایل دولت‌ها به انعطاف‌پذیر ماندن برای حمله به دیگر کشورها است.

پس از آن، این فصل محیط امنیت سایبری کانادا را که شامل درک فرهنگی، نهادهای آن، نقش قانون‌گذار و پیامدهای اجتماعی است، مورد بررسی قرار داد. دو چیز به وضوح مشخص می شود: کانادایی‌ها از قوانین سایبری آگاهی بیشتری دارند و نمی‌خواهند به نام جمع‌آوری داده‌ها برای امنیت ملی در زندگی خصوصی شان دخالت شود. کانادا همچنین دارای ویژگی‌های منحصر به فردی مانند عضویت Eyes-5 و فعالیت سازمانی مانند OPC است که بر اجرای قوانین سایبری در این کشور نظارت دارد.

با توجه به تحلیل‌های انجام شده در درک فرهنگی از محیط امنیت سایبری کانادا در بالا، منطقی است که درک کنیم که آگاهی و همکاری ذی‌نفعان دو عنصر مهم برای دفاع سایبری کانادا در آینده است. با این حال، برای تقویت دفاع سایبری خود، بخش‌های تجاری خصوصی و سازمان‌های دولتی کانادا باید در ایجاد تغییراتی در فرهنگ حفاظت از داده‌ها و اشتراک‌گذاری داده‌ها و حفظ تعادل بین حریم خصوصی و امنیت ملی با یکدیگر همکاری کنند.

اتحادیه اروپا

مقدمه

امنیت سایبری یکی از مهم‌ترین حوزه‌های اولویت‌بندی خط‌مشی برای اتحادیه اروپا است. در این راستا، اظهارات مقامات اتحادیه اروپا و زبان (ماهیت) اسناد سیاست‌گذاری، بر میزبانی شبکه‌ها و زیرساخت‌های حیاتی فعال شبکه‌ای که پایه و اساس فرایندهای اقتصادی و سیاسی اتحادیه را تشکیل می‌دهند، تأکید کرده است.

امروزه اتحادیه اروپا شامل صد میلیون شهروند است که از میلیاردها دستگاه متصل به اینترنت برای شرکت در فعالیت‌های تجاری، مشارکت در سیاست و شاید مهم‌تر از همه، برای برقراری ارتباط در خطوط منطقه‌ای، ملی و زبانی استفاده می‌کنند.

تا حدود زیادی، قانون اساسی فراملی اتحادیه چالش‌های امنیت سایبری اتحادیه اروپا و رویکرد سیاستی را تعریف می‌کند. همان‌طور که در سایر زمینه‌ها اتفاق افتاده است، انسجام مقاصد و نتایج خط‌مشی در همه عناصر اتحادیه، دغدغه اصلی آن نهادها و افراد است که منجر به فرمول‌بندی‌های جدیدی با نام «سایبری» شده است. همان‌طور که Barrinha و Farrand-Carrapico (2018) اشاره می‌کنند، اهمیت انسجام (اتحاد) برای اتحادیه اروپا نه‌تنها نیاز سنتی برای تطبیق انتظارات و رویکردها در سطح طبیعی و وسیع بروکراسی قاره‌ای (ادغام افقی) و چشم‌انداز عضویت در اتحادیه است بلکه این نیاز با مسئولیت‌های اتحادیه در مقابل کشورهای عضو و هم مقابل صنعت خصوصی پیوند خورده است.

از منظر دیدگاه‌های مختلف، اثربخشی اتحادیه اروپا در پاسخ به الزامات سایبری به‌کندی تحقق پیداکرده است. از قضا، احتمالاً تا حد زیادی ناشی از تلاش‌های زیاد برای اطمینان از انسجام در رویکرد در مراحل اولیه فرآیند نهادسازی بوده است.

در اروپا، استراتژی اولیه به‌عنوان تلاش مشترک چندین آژانس اتحادیه اروپا ظاهر شد و به‌طور گسترده در تلاش برای رسیدگی به جرم، مسائل دفاعی و حفاظت از زیرساخت‌های حیاتی شکل گرفت. درنتیجه، این امر تنها ابزارهای صریحی را در اختیار اتحادیه اروپا قرارداد تا بتواند تنش‌های سنتی را که در تعیین مسئولیت برای مسائل مختلف سایبری – خود اتحادیه اروپا یا کشورهای عضو – دارد، برطرف کند.

ادامه این فصل وضعیت امور سایبری را در اتحادیه اروپا توصیف می‌کند و ماهیت چالش‌ها برای تضمین انسجام در رویکرد را توضیح می‌دهد که حتی با توجه به پیشرفت‌های اخیر که رویکردهای امنیت سایبری را ساده‌سازی و متمرکز می‌کند، به نظر می‌رسد در سال‌های آینده ادامه پیدا کند. پس از ارائه یک چشم انداز کوتاه در مورد تاریخچه تهدیدات سایبری برای امنیت فراملی، این فصل به جزئیات توسعه استراتژی، نهادها و ابتکارات اصلی امنیت سایبری در دهه گذشته می‌پردازد که در قانون امنیت سایبری اتحادیه اروپا در سال 2019 به اوج خود رسید. در آخر، این فصل تجلی چالش‌های پایدار را در تلاش برای حفظ انسجام رویکرد در میان شرایط متغیر تکنولوژیکی و سیاسی مورد بحث قرار می‌دهد.

تجارب اروپا در امنیت سایبری

درحالی‌که تعداد زیادی از کشورهای غربی می‌توانند به یک یا چند تجربه اولیه مشخص در مورد تهدیدات سایبری برای امنیت ملی به‌عنوان انگیزه‌ای برای توسعه نهادها و استراتژی‌ها در زمینه امنیت سایبری اشاره کنند، فشاری که اتحادیه اروپا برای اقدام در مورد مسائل سایبری احساس می‌کند، بیشتر با تهدیدات اقتصادی تا تهدیدات ژئوپلیتیکی مواجهه شده است. در اتحادیه، هدف نهایی در زمینه امنیت سایبری، رفاه و یکپارچگی آن اصول اساسی است که زیربنای پتانسیل اقتصادی است. این تمرکز از بسیاری جهات، اتحادیه اروپا را به‌عنوان بازیگر سایبری در امور بین‌الملل کاملاً منحصربه‌فرد می‌سازد.

به همین جهت حملات سایبری (حملات باج‌افزاری با قابلیت کرم) در سراسر بخش‌های جامعه اروپایی میلیاردها دلار خسارت وارد کرد و اتحادیه اروپا را در مجموعه‌ای از تلاش‌های اخیرش برای ساده‌سازی و ایجاد یک چشم‌انداز استراتژیک منسجم در حوزه امنیت آنلاین اروپا برانگیخت.

سیاست امنیت سایبری اتحادیه اروپا: تلاش‌های اولیه

در طول دو دهه گذشته، تلاش در داخل اتحادیه اروپا برای تعریف بهتر دامنه مسائل مربوط به امنیت سایبری مرتبط با این سازمان – و مسئولیت‌های ناشی از آن – منعکس‌کننده چالش‌های مختلف است. در این جهت رویکردهای دولت در قبال مسائل فناوری اطلاعات در دو دسته ارائه می‌گردد:

1. رویکرد نخست: فناوری اطلاعات برای رشد بازارهای اروپایی از اهمیت ویژه برخوردار است.
2. رویکرد دوم: فناوری اطلاعات در کمک به نتایج دموکراتیک و تضمین ثبات در تعامل سیاسی در سراسر اتحادیه اروپا نتایج مهمی را ارائه می‌دهد.

با وجود این، توجه به این نکته حائز اهمیت است که تمرکز اولیه اتحادیه اروپا بر انسجام اهداف و نتایج اقتصادی بیش از انگیزه‌های اجتماعی و سیاسی برجسته را منعکس می‌کند.

تا اواخر دهه 2000، چند رویداد مهم امنیت سایبری تأثیر عمده‌ای بر سیاست اتحادیه اروپا در قبال مسائل سایبری داشتند. با وجود این، اگرچه اسناد امنیتی مانند استراتژی امنیت اروپا در سال 2003 در مسائل مربوط به امنیت اطلاعات باقی ماندند، اما افزایش جرائم سایبری در طول دهه 1990 باعث انسجام مجموعه‌ای از تلاش‌ها برای تطبیق بهتر توسعه وب یا مسئولیت‌های حاکمیتی سازمان شد.

همان‌طور که نگرانی‌های مشابه منجر به قانون تقلب و سوءاستفاده یارانه‌ای و قوانین بعدی ایالات‌متحده اواسط دهه 1980 شد، در اتحادیه نیز نگرانی در مورد مطالب و فعالیت‌های مضر آنلاین موجی از ابتکارات را ایجاد کرد. باهدف گسترش آگاهی از تهدیدات سایبری بالقوه برای مصرف‌کنندگان در اواسط دهه 2000 این دوره ادامه داشت که تمرکز زیادی بر روی هماهنگی ابتکارات دانش برای جمعیت کشورهای عضو، ایجاد تعاریف مشترک از ظاهر جرائم رایانه‌ای و استانداردسازی زبان برای اجماع در مورد اینکه چه چیزی امن است، قرار گرفت.

تغییر بازی سیاست در زمینه خط‌مشی سایبری در اواسط 2000 محقق گردید. با شکل‌گیری شکل جدیدی از تعارض بین‌المللی مشخص‌شده با ظهور جنایات سازمان‌یافته که مهم‌ترین تهدید برای امنیت سایبری بودند، اعضای اتحادیه اروپا وادار شدند تا اعتبار رویکردهای سیاست‌گذاری سازمانی واگذار شده به حاکمیت که بر مدیریت متمرکز تأکید داشت را دوباره ارزیابی کنند.

در سال‌های 2003–2004، با توجه به این نگرانی‌ها و کاستی‌ها، راه‌حل‌های سطح اعضا به‌طور مستقیم به امنیت سیستم‌های اطلاعاتی و ارتباطات دیجیتال نیز اعمال می‌شد. به‌طور خاص، مقامات اتحادیه اروپا نسبت به تفاوت چشم‌گیر قوانین کشورهای مختلف در برخورد با جرائم سایبری و حمایت از کاربران نگران شدند.

دفاع سایبری و اتحادیه اروپا

از اواسط دهه 2000 تغییر تمرکز به سمت کاهش اتکا به راه‌حل‌های کشورهای عضو به نفع راه‌حل‌های منسجم سازمانی، سیاست سایبری تحت اتحادیه اروپا در ساحت تمرکز بر حفاظت از زیرساخت‌های حیاتی و کاهش تهدیدات مجرمانه سایبری به‌طور قابل‌توجهی انجام‌شده است (از جمله حفاظت از کاربران سیستم های دیجیتال).

اوایل دهه 2010 حجم قابل‌توجهی از فعالیت‌های مخرب مورد سرقت اطلاعات ارزشمند صنعتی و دولتی به ارزش ترابایت قرار گرفت، توسط مقامات اتحادیه اروپا به‌عنوان تهدیدی آشکار و فعلی برای انسجام اقتصادی این قاره تلقی شد. به همین ترتیب، استفاده روزافزون از کدهای مخرب برای دستیابی به نتایج مخرب بسیار واقعی، سهامداران اروپایی را با نوعی تهدید سایبری مواجه کرد که برای اولین بار ارتباط مستقیم تروریسم فراملی به نظر می‌رسید. در این راستا، امنیت سایبری یک موضوع فرا سطحی بود که به همان اندازه که نیازمند تلاش‌های گسترده برای ایمن‌سازی بهتر جامعه دیجیتال اروپا بود، به واکنش هماهنگ نیاز داشت.

اولین گام‌های مهم در دفاع سایبری در سال 2010 رخ داد، با اولین تمرکز بر روی قابلیت‌های سایبری به‌عنوان یک منطقه حیاتی توسعه امنیت ملی که در برنامه توسعه ظرفیت (توانمندسازی) آن سال ظاهر شد. اما در سال 2014، تمرکز سیاست اتحادیه اروپا بر دفاع سایبری عمدتاً محقق گردید که ناشی از تهدید حملات صنعتی باانگیزه سیاسی از سوی قدرت‌های خارجی متخاصم بود.

تمرکز اولیه بر دفاع سایبری بر دو حوزه اصلی فعالیت تأکید داشت:

1- مکانیسم‌های هماهنگی واکنش به بحران

2- پرورش ظرفیت‌های سایبری ملی

طی سه سال(2010 الی 2013)، سازمان‌های اتحادیه اروپا مانند آژانس دفاعی اروپا (EDA) و کمیسیون اروپا تلاش کردند تا مجموعه‌ای از برنامه‌های طراحی‌شده برای تقویت توانایی‌های اتحادیه اروپا برای هماهنگ کردن تلاش‌های دفاعی کشورهای عضو را اجرا کنند.

استراتژی امنیت سایبری اتحادیه اروپا (EUCSS) که در سال 2013 منتشر شد، رابطه بین این تلاش‌ها را با هدف تشویق کشورهای عضو به اتخاذ نقشه‌های راه جامع برای توسعه قابلیت‌های دفاعی، فیلتر کردن پاسخ سایبری در بخش زیرساخت‌های واکنش به بحران در کشورهای عضو تعریف کرد.زاز زمان انتشار استراتژی امنیت سایبری اتحادیه اروپا ، اتحادیه اروپا به‌طور فزاینده‌ای نیاز به توانایی‌های بهتر برای شناسایی و بازیابی تهدیدات دیجیتالی پیچیده را در کنار نیاز آشکار به پاسخگویی در طول بحران تشخیص داده است.

بین سال‌های 2016 تا 2018، این سازمان گام‌های مهمی در توسعه چنین ظرفیت‌ها(توانمندسازی‌ها) برداشت. به‌عنوان‌مثال، در سال 2016، اتحادیه اروپا و ناتو بیانیه مشترکی صادر کردند که در آن همکاری در مورد مسائل سایبری متعددی از جمله نیاز به مبارزه با تهدیدات ترکیبی برای حاکمیت اروپا و نیاز به تقویت بیشتر دفاع دیجیتال قاره‌ای را اعلام کرد. در سال 2017، چارچوب همکاری ساختار یافته دائمی (PESCO) توسط شرکت‌کنندگان داوطلب موردتوافق قرار گرفت که شامل 25 نفر از 28 نیروی مسلح ملی کشورهای عضو اتحادیه اروپا بود.

با وجود طیف وسیعی از پیشرفت‌های امیدوارکننده که بر دفاع سایبری متمرکزشده‌اند، واکنش اتحادیه اروپا به تهدیدات سایبری از منظر امنیت فراملی تا حدودی پراکنده است. همان‌طور که گریفیث اشاره می‌کند، توانایی‌های اتحادیه اروپا (از سال 2018) در سازمان‌ها و نهادهایی که مأموریت‌ها و مسئولیت‌های هماهنگی آن‌ها همیشه به‌وضوح در قانون و سیاست تعیین نشده‌اند، مورد غفلت واقع می‌شوند. ثانیاً، در مواردی که حملات سایبری شامل یک عامل تهدید قابل‌شناسایی نمی‌شود، مشخص نیست که مسئولیت کشورهای عضو در کجاست.

یکپارچگی، انسجام و شرایط روی زمین

فراتر از دامنه مسائل دفاع سایبری، اتحادیه اروپا ظرفیت نهادی را برای مقابله با امنیت سایبری به شکلی جامع از اواسط دهه 2000 توسعه داده است.

در طول دو دهه گذشته، اتحادیه اروپا یک اکوسیستم قوی و متنوع از آژانس‌ها را ایجاد کرده است که وظیفه آن‌ها عناصر مختلف مأموریت امنیت سایبری، از EDA و DG امور داخلی (با انواع مأموریت‌های جرائم سایبری) تا DG برای ارتباطات، محتوا و فناوری، آژانس امنیت شبکه و اطلاعات اروپا (ENISA) و طیف کاملی از گروه‌های واکنش اضطراری رایانه‌ای (CERT) است.

از سال 2004، زمانی که آژانس امنیت شبکه و اطلاعات اروپا به وجود آمد، تأکید بر انسجام رویکرد اتحادیه اروپا به‌عنوان مجموعه‌ای توافق شده از اهداف مأموریت و زیربنای نهادی به‌عنوان پیش‌نیاز ضروری برای حفاظت گسترده‌تر از جامعه دیجیتال اروپا شده است.

به گفته کاراپیکو و بارینا (2017)، پروژه ساخت انسجام حداقل در امتداد دو خط و با در نظر گرفتن ادغام افقی و عمودی تکامل‌یافته است.

1. اتحادیه اروپا (و به‌طور خاص شورا) تلاش کرده‌اند تا اکوسیستم نهادی لازم برای ایمن‌سازی جامعه اروپایی را در چارچوب خود کشورهای عضو (یعنی روابط افقی) به‌صورت آنلاین ایجاد کنند. این به معنای تلاش برای تطبیق ابزارهای سیاستی و قوانین ملی مربوط به جرائم سایبری، حقوق کاربران و موارد دیگر است، و همچنین حصول اطمینان از اینکه رویکردهای هماهنگی با بخش خصوصی توسط بخش خصوصی حمایت می‌شود. به‌طور خاص، این امر اتحادیه اروپا را به ایجاد آژانس‌های تخصصی متعدد، از آژانس امنیت شبکه و اطلاعات اروپا گرفته تا عناصر اینترپل که مسئول تحقیقات جنایی سایبری هستند، سوق داده است.
2. اتحادیه اروپا تلاش کرده است اطمینان حاصل شود که درک مشترکی از دامنه و اهداف مأموریت سایبری اروپا وجود دارد. به‌طور افقی، این منجر به بیش از یک دهه ابتکار باهدف تجمیع و ادغام درک تأثیر اینترنت بر جامعه اروپا شده است. به همین ترتیب، این به معنای سرمایه‌گذاری قابل‌توجه و مذاکره پیرامون مفاهیم است. درنهایت، نیاز به تولید و حفظ معنای مشترک در گفتمان حاکمیت سایبری به سازوکارهایی برای تطبیق و شکل دادن به بیان اولویت‌های سایبری در سطح ملی منجر شده است.

به‌طورکلی، شاید جای تعجب نباشد که این تمرکز بر انسجام پیش از اثربخشی، یک اکوسیستم سیاست سایبری در اتحادیه اروپا ایجاد کرده است که با تدریج گرایی مشخص می‌شود. بسیاری از عناصر رویکرد اتحادیه به مسائل سایبری توسط اصطکاک‌های بین‌المللی تعریف می‌شوند که موانعی را برای پیشرفت ایجاد می‌کنند که در دیگر سیاست‌های بزرگ در سراسر جهان یافت نمی‌شوند. به‌عنوان‌مثال آژانس‌های اتحادیه اروپا با مشکلات خاصی در توسعه خود مواجه شده‌اند.

اتحادیه اروپا تنها با مسائل سنتی عدم تطابق منافع عمومی و خصوصی مواجه است (به‌ویژه در مقابل چیزهایی مانند اشتراک‌گذاری داده‌ها) و مشارکت کم‌سابقه در بخش‌های زیرساختی که باهم پیوند ضعیفی دارند (مانند بخش فناوری‌های اینترنت). همچنین خود را مجبور به انجام یک بازی چند سطحی با دولت‌های ملی می‌بیند که اغلب، باوجود تمایل به پیشرفت در مسائل امنیت سایبری، ازنظر سیاسی از تنظیم صنعت خصوصی متنفر هستند.

دستورالعمل NIS، ENISA و قانون امنیت سایبری اتحادیه اروپا

تدریج‌گرایی اتحادیه اروپا در زمینه امنیت سایبری به‌عنوان یک مانع مهم برای اثربخشی در تعدادی از جبهه‌ها ظاهر می‌شود. ماهیت چندوجهی اکوسیستم سایبری اتحادیه اروپا، به‌ویژه، اغلب به معنای کمبود منابع (یا گاهی اوقات، عدم دسترسی به منابع مناسب) برای آژانس‌هایی مانند ENISA، اینترپل، و EDA بوده است. به همین ترتیب، به‌ندرت یک دیدگاه استراتژیک برای منافع اتحادیه اروپا و رویکردهای امنیت سایبری ارائه‌شده است. درحالی‌که استراتژی های مهم متعددی اعلام‌شده و بیانیه‌های چشم‌انداز منتشرشده است، فراتر از این واقعیت دشوار است که به‌ندرت مجموعه‌ای از روش‌های کارآمد برای واکنش سریع به بحران‌های سایبری در سطح سازمانی را شامل می‌شود. علاوه بر این، موانع همکاری – به‌طور خاص، موانع ارتباط و دگرگونی معنا– در بین سهامداران اتحادیه اروپا و همتایان در کشورهای عضو تا به امروز بالا باقی‌مانده است.

بااین‌حال، در سال‌های اخیر چندین گام مهم در جهت کاهش این چالش‌ها برداشته‌شده است. برای مثال، در ژوئیه 2016، دستورالعمل 1148/2016 (ازاین‌پس «دستورالعمل NIS») (2016) برای ساده‌سازی بیشتر فرآیندهای کاهش تهدیدات سایبری در میان کشورهای عضو منتشر شد. از بسیاری جهات، این قانون که به‌صورت افقی کشورهای عضو را هدف قرار داده بود، بی‌شباهت به چارچوب امنیت سایبری داوطلبانه مؤسسه ملی استانداردها و فناوری (NIST) در ایالات‌متحده نیست؛ زیرا برای اولین بار تعاریفی از دسته‌های اپراتورها ارائه می‌دهد، انواع ذی‌نفعان صنعت خصوصی و انواع اقداماتی که باید توسط مقررات دولتی موردتوجه قرار گیرد، سپس تصویب این چارچوب‌ها توسط مقامات ملی را که از طریق انتشار استراتژی‌های مربوطه، ایجاد آژانس‌های وضع قوانین و اجرا (جایی که قبلاً وجود نداشتند) و پیروی از استانداردهای خاصی از رویه ملی (در رابطه با مواردی مانند اطلاع‌رسانی نقض داده‌ها) را الزامی کرد.

دستورالعمل NIS، ENISA، آژانس امنیت سایبری اتحادیه اروپا، نقش بسیار متمرکزتر و مهم‌تری را در تضمین امنیت سایبری قاره‌ای نسبت به آنچه تاکنون وجود داشته است، می‌کند. بر اساس این دستورالعمل، ENISA به‌عنوان تنها مسئول ارائه پشتیبانی توسط اتحادیه اروپا به کشورهای عضو و برای اطمینان از انطباق کشورهای عضو با دستورالعمل نام‌گذاری شده است. ENISA باید تخصص مربوطه را به آژانس‌های کشورهای عضو ارائه دهد و باید به توسعه همه دستورالعمل‌ها برای همکاری عمومی–خصوصی برای استفاده توسط گروه همکاری (واحد زیرمجموعه اتحادیه اروپا که مأموریت پشتیبانی را بر عهده دارد) کمک کند. علاوه‌بر این، دستورالعمل ENISA را در یک نقش مشاوره اجباری قرار می‌دهد که در آن کمیسیون اتحادیه اروپا باید قبل از اقدام رسمی توسط آژانس مشاوره شود. این دستورات، در کنار نقش جدیدی که آژانس تحت این دستورالعمل برای کمک به انتصاب نمایندگان در سطوح مختلف هماهنگی داده‌شده است، ENISA را به‌عنوان هسته تمام تصمیمات در رابطه با توسعه نیروی کار هماهنگ‌کننده سایبری اتحادیه اروپا و توزیع نیروی موردنیاز قرار می دهد. به‌طور ضمنی، آن‌ها همچنین ENISA را در موقعیتی قرار می‌دهند که دیدگاه‌های استراتژیک منسجم‌تری را در آینده بیان کند. قانون امنیت سایبری اتحادیه اروپا (2019)، که در اواسط سال 2019 به تصویب رسید، این نیروی محرکه ENISA را به پیشروی اجرای سیاست سایبری اتحادیه اروپا افزایش می‌دهد و این آژانس را تنها و دائمی مرجع برای طیف وسیعی از ابتکارات در سطح عملیاتی برای تقویت بحران سایبری است. درنهایت، این دستورات همچنین پیامدهای فعالیت امنیت سایبری در اتحادیه اروپا را در چارچوب مقررات عمومی حفاظت از داده‌ها (GDPR) ساده می‌کند.

GDPR که در کنار دستورالعمل NIS به تصویب رسیده است، بخشی از مقررات گسترده است که باهدف بهبود امنیت داده‌ها برای شهروندان اروپایی انجام می‌شود. اگرچه در مواردی که هر دو قانون اعمال می‌شوند، نقاط بالقوه متعددی برای تضاد عملیاتی وجود دارد، مانند زمانی که داده‌های شخصی در هنگام پاسخ به بحران به نقض داده‌ها پیدا می‌شود، قرار گرفتن ENISA در قلب اکوسیستم اروپا برای سیاست‌گذاری و اجرای سایبری حداقل وعده می‌دهد که به نظم بخشیدن به‌جایی که قبلاً ممکن است سردرگمی وجود داشته، باشد کمک کند.

نتیجه‌گیری

معماری سیاست‌گذاری و اجرای امنیت سایبری اتحادیه اروپا، هم ازنظر مسائلی که باید با آن‌ها دست‌وپنجه نرم کرد و هم در امتداد محورهای سنتی افقی و عمودی که مشخصه یکپارچگی در این قاره برای چندین دهه است، پیچیده است. همچنان مجموعه گسترده‌ای از چالش‌ها پیش روی سازمان و بازار واحد

وجود دارد. مهم‌تر از آن، نیاز واقعی به انسجام بیشتر بینش و اقدامات بعدی از سوی آژانس‌های اتحادیه اروپا، به‌ویژه وقتی صحبت از دفاع سایبری می‌شود، وجود دارد.

تحولات اخیر قطعاً گام‌های مهمی در ساده‌سازی چشم‌انداز نهادی سیاست سایبری برای اتحادیه اروپا برداشته است. علاوه بر پیش راندن ENISA به پیشانی این اکوسیستم، اختیارات جدیدی که به شورای اروپا برای تحریم حملات سایبری و ارائه گواهینامه سراسری اتحادیه اروپا (از جمله پیشرفت‌های دیگر) اعطاشده است، قاره را انعطاف‌پذیرتر ازآنچه در طول تاریخ بوده است، می‌سازد. با این حال، همان‌طور که رئیس‌جمهور ژان کلود یونکر در سخنرانی خود در سال 2017 اعلام کرد، اروپا هنوز در مورد حملات سایبری به‌خوبی مجهز نیست. بااین‌وجود، این بازگویی مختصر از تجربیات اروپا در زمینه امنیت سایبری و سیاست‌گذاری سایبری در مورد چیزی جز یک نکته احتیاط آمیز پایان نمی‌یابد. مسائل سایبری ناهمگون و مستعد دگرگونی هستند به‌گونه‌ای که مسائل کمی هستند.

آنچه اتحادیه اروپا را به‌عنوان یک بازیگر جهانی سایبری در میان دیگر بازیگران منحصربه‌فرد می‌کند – که به‌طورکلی، کشورهای مستقلی هستند که حقوق خود را دارند – وضعیت آن به‌عنوان یک نهاد حاکمیتی مشورتی و تدریجی بودن ناشی از نیاز به تضمین انسجام است. درواقع، حتی اگر تدریجی گرایی در این زمینه به نفع اروپا باشد، زیرا احتیاط منجر به تحولات محتاطانه سیاست‌ها می‌شود، به نظر می‌رسد معقول است که پیشنهاد کنیم رویکرد اتحادیه اروپا در برابر عدم تحقق مناطق تهدید جدید در آینده آسیب‌پذیر باشند.

انگلستان

مقدمه

انگلستان و ایرلند شمالی (بریتانیا) یکی از اقتصادهای پیشرو در جهان است و توانسته منابع ملی قابل‌توجهی را برای رسیدگی به طیف وسیعی از مسائل امنیت سایبری به کار گیرد. برنامه علنی امنیت سایبری ملی انگلستان، یک دهه قدمت دارد. این برنامه، رویکردی پیچیده به امنیت سایبری است که چندین بازیگر دولتی و خصوصی را شامل می‌شود. این بازیگران در چارچوب یک برنامه‌ریزی قوی عمل می‌کنند که فضای سایبری را به‌عنوان یک حوزه استراتژیک و امنیت سایبری را وسیله‌ای برای پیگیری منافع ملی در داخل و خارج از کشور می‌داند. انگلستان اذعان دارد که رفاه و دیده شدن در عرصه بین‌الملل آن را به هدفی جذاب برای مجرمان سایبری و دشمنان استراتژیک تبدیل می‌کند و در حال توسعه راه‌هایی برای مقابله با این تهدیدات است. این گزارش به تشریح استراتژی امنیت سایبری انگلستان و مفروضات آن در برنامه‌ریزی می‌پردازد، نهادها و ذی‌نفعان اصلی را مشخص می‌کند، قوانین مربوط به انگلستان را شرح می‌دهد و جنبه‌های مرتبط سیاست خارجی انگلستان را مورد بحث قرار می‌دهد. همچنین به برخی از پیامدهای اجتماعی امنیت سایبری انگلستان به‌طور خلاصه اشاره کرده و نتیجه می‌گیرد: درحالی‌که برخی چالش‌های استراتژیک برای امنیت سایبری انگلستان در قالب برگزیت و براندازی روسیه وجود دارد، انگلستان آمادگی نسبتاً خوبی برای مقابله با چشم‌انداز وسیع چالش‌های امنیت سایبری دارد.

استراتژی ملی امنیت سایبری

اولین استراتژی ملی امنیت سایبری انگلستان (NCSS) در سال 2009 و نسخه‌های بعدی آن در سال‌های 2011 و 2016 منتشر شد (دفتر هیئت دولت، 2011، 2006a، 2009a). استراتژی ملی امنیت سایبری فعلی انگلستان که در نوامبر 2016 منتشر شده است، بیانیه کاملی از اهداف ملی امنیت سایبری همراه با یک برنامه بررسی بلندپروازانه برای اندازه‌گیری پیشرفت به سمت اهداف استراتژیک آن است. این برنامه به‌عنوان دومین برنامه امنیت سایبری ملی پنج‌ساله (2016–2021) پس از نسخه پیشین خود در سال 2011 تنظیم شده است، اما به فراتر از چارچوب زمانی 2021 معطوف است تا چالش‌های در حال تحول ناشی از فناوری‌های نوظهور و سازگاری در ابزارها و قابلیت‌های متخاصم را تشخیص دهد. استراتژی ملی امنیت سایبری انگلستان مشارکت بین دولت، صنعت و جامعه را برای ارائه امنیت سایبری ملی بهتر از طریق تغییرات رفتاری چندبخشی در اولویت قرار می‌دهد، اما با تغییری مهم در تفکر دولت هدایت می‌شود. دولت تشخیص داد که برای هدایت نوآوری امنیت سایبری ملی، اتکای پیشین به بازار، تغییر مورد نیاز برای جلوتر بودن از تهدیدات پرشتاب را با مقیاس و سرعتی ناکافی ایجاد کرده است. بر این اساس، دولت موضع مداخله‌جویانه‌تری برای هدایت رفتارهای سایبری ایمن در بخش‌های مختلف اتخاذ کرده است که با سرمایه‌گذاری مالی به مبلغ 1.9 میلیارد پوند طی پنج سال حمایت می‌شود تا امنیت سایبری انگلستان را به‌طور قابل‌توجهی تغییر دهد (دولت انگلستان، 10: 2016a).

استراتژی ملی امنیت سایبری حول سه موضوع متقابل، دفاع، بازداشتن و توسعه سازماندهی شده است که با تعهد مجدد به اقدام بین‌المللی برای ترویج ابتکارات سایبری دوجانبه و چندجانبه که منافع ملی انگلستان و امنیت جمعی را ارتقا می‌دهد، پی‌ریزی شده است. «دفاع»[37] با تهدیدات سایبری در حال تحول مقابله می‌کند و حفاظت و تاب‌آوری جامعه و دارایی‌های انگلستان را از جمله از طریق آموزش عمومی و تبادل دانش با صنعت، به‌ویژه شرکت‌های کوچک و متوسط (SMEs) ارتقا می‌دهد. دفاع شامل یک برنامه دفاع سایبری فعال (ACD) می‌شود که ادعا می‌کند «به‌طور عینی» از طریق ابزارهای خودکار میزان بروز و اثرات تهدیدات سایبری رایج در سراسر حوزه عمومی را کاهش داده است (استیونز[38] و همکاران، 2019). «بازداشتن[39]» اقدامات برای شناسایی و تعقیب عوامل متخاصم در فضای مجازی را در اولویت قرار می‌دهد و این حق را برای خود محفوظ می‌دارد که در صورت لزوم، حمله به آن‌ها را به‌صورت قانونی پیگیری کند. بازداشتن بر توسعه قابلیت‌های حاکم، از جمله رمزنگاری، برای کاهش خطرات ناشی از جرائم سایبری، تروریسم سایبری و بازیگران سایبری خارجی، اعم از دولتی و غیردولتی تأکید می‌کند. هسته اجزای این اقدامات، ایجاد یک برنامه سایبری تهاجمی ملی (NOCP) در سراسر وزارت دفاع و ستاد ارتباطات دولت[40] (آژانس اطلاعاتی سیگنال‌های انگلستان) است که استراتژی ملی امنیت سایبری کنونی را از نظر جهت‌گیری «تهاجمی‌تر» از متقدمان آن که دارای نگرش دفاعی هستند، نشان می‌دهد. (کریستو[41]، 2016: 62–86؛ لونزدیل[42]، 2016). محور «توسعه» تحصیل، تحقیق و آموزش امنیت سایبری را برای کاهش شکاف مهارت‌های امنیت سایبری و حمایت از نوآوری و رشد بخش خصوصی ترویج می‌کند. در کنار طیف وسیعی از برنامه‌های توسعه و مشارکت آموزشی،

---

[37] Defend
[38] Stevens
[39] Deter
[40] Government Communications Headquarters
[41] Christou
[42] Lonsdale

یکی از مؤلفه‌های بسیار قابل مشاهده «توسعه» افزایش شمار مراکز عالی معتبر علمی در تحقیقات امنیت سایبری (ACE-CSR) در دانشگاه‌های انگلستان به شمار 19 عدد بوده است.

هویت درک شده انگلستان از خود یک محرک مهم در چارچوب امنیت سایبری ملی و جاه‌طلبی‌های استراتژیک آن است. سهم تاریخی انگلستان در نوآوری دیجیتال وضعیت این کشور را به‌عنوان «یکی از کشورهای پیشرو در جهان به لحاظ دیجیتالی» نشان می‌دهد (دولت انگلستان، 6: 2016a). آن‌گونه که به ناپلئون نیز منتسب است، انگلستان «ملت مغازه‌داران» است که یعنی ثروت انگلستان به‌جای هرگونه مزیت مادی ذاتی، از تجارت ناشی می‌شود. در مورد فضای مجازی که به‌عنوان فرصتی برای تقویت و ارتقای بهره‌وری و شکوفایی اقتصاد ملی دیده می‌شود نیز همین‌طور است. درواقع، همان‌طور که استراتژی ملی امنیت سایبری انگلستان روشن می‌کند، «آینده امنیت و رفاه انگلستان بر پایه‌های دیجیتال استوار است» (دولت انگلستان، 9: 2016a). این یک نتیجه عادی برای کشوری است که بیش از 10 درصد از تولید ناخالص داخلی خود را از اقتصاد دیجیتال تولید می‌کند که بالاترین نسبت در G-20 است (گروه مشاوره بوستون، 2015). سیاست امنیت سایبری همیشه همراه با سیاست‌های اقتصادی در انگلستان بوده است. برای مثال، اولین استراتژی ملی امنیت سایبری، همراه با دستور کار دولت دیجیتال انگلستانی، «راهنمای چگونگی حفظ موقعیت انگلستان به‌عنوان یک اقتصاد و جامعه دیجیتال پیشرو» راه‌اندازی شد (دولت انگلستان، 8: 2009b). استراتژی‌های بعدی مفهوم انگلستان را به‌عنوان کشوری پویا و مرکز بازرگانی معطوف به خارج و ظرفیت صنعت امنیت سایبری برای تبدیل‌شدن به یک بخش اقتصادی پررونق تقویت کرده است. جاه‌طلبی‌های تکمیلی در قانون اقتصاد دیجیتال (2017) بیان شده است.

نهادها و ذی‌نفعان

در انگلستان هیچ اداره یا سازمان دولتی مسئولیت امنیت سایبری را به‌تنهایی بر عهده ندارد. دفتر هیئت دولت که در قلب حکومت و خدمات مدنی قرار دارد، به‌طور رسمی مسئول توسعه سیاست و اجرای برنامه ملی امنیت سایبری (NCSP) که در آن مشخص شده است را بر عهده دارد. بسیاری از وظایف توسط اداره امنیت سایبری و دولتی (CGSD) در دفتر هیئت دولت هماهنگ می‌شود که منشأ آن در دفتر امنیت سایبری (و بعداً تضمین اطلاعات[۴۳]) که در سال 2009 تأسیس شد است. اداره امنیت سایبری و دولتی با شرکای دولتی کار می‌کند که هرکدام مسئولیت اجزای مختلف معماری امنیت سایبری انگلستان را بر عهده دارند. وزارت دیجیتال، فرهنگ، رسانه و ورزش (DCMS) در اقتصاد دیجیتال پیشتاز است. وزارت کشور، سازمان مادر سرویس امنیت داخلی (MI5) و آژانس ملی جرم و جنایت است و عملیات جرائم سایبری و ضد تروریسم را هدایت می‌کند. وزارت بازرگانی، انرژی و راهبرد صنعتی (BEIS) بر جنبه‌های گسترش و تعامل امنیت سایبری صنعتی، از جمله مقررات خاص برای صنعت غیرنظامی هسته‌ای نظارت می‌کند. وزارت آموزش (DfE) برنامه گسترده‌ای را برای آموزش امنیت سایبری و ایمنی آنلاین در مدارس ارائه می‌دهد. خود دفتر هیئت دولت نیز از طریق دبیرخانه حوادث غیرمترقبه مدنی دستور کار تاب‌آوری را کنترل می‌کند.

اداره امور خارجه و مشترک‌المنافع (FCO)، مسئول سرویس اطلاعات مخفی (MI6)، ستاد ارتباطات دولت و همچنین مرکز ملی امنیت سایبری (NCSC) در لندن است. همچنین مسائل دیپلماتیک ناشی از اقدامات سایبری خارجی، مانند انتساب یک سری عملیات سایبری خصمانه به سازمان اطلاعات نظامی روسیه در سال 2018 (NCSC، 2018) را مدیریت می‌کند. وزارت دفاع (MoD) فعالیت‌های شاخه‌های خدماتی و سازمان‌های اجرایی خود را برای توسعه قابلیت‌های مستقل و ارائه مزیت‌های عملیاتی، از جمله، با مشارکت ستاد ارتباطات دولت، از طریق برنامه ملی تهاجمی سایبری (NOCP) هماهنگ می‌کند. انگلستان اولین کشور در جهان بود که به توسعه «طیف کامل قابلیت سایبری نظامی» (بلیتز[۴۴]، 2013) اعتراف کرد و واحدهای سایبری مشترک در چلتنهام و کورشهام به ترتیب قابلیت‌های تهاجمی و دفاعی را ارائه کردند. این واحدها و سایر واحدها، از جمله ذخیره مشترک سایبری، در گروه سایبری نیروهای مشترک (JFCyG) قرار دارند که در می 2013 به‌عنوان جانشین گروه عملیات سایبری دفاعی ایجاد شد.

تحقیقات قبلی در مورد امنیت سایبری انگلستان حاکی از توسعه تاریخی ظرفیت و مسئولیت نهادی به‌جای توسعه دفعی آن است (هاروی، 2013). این به‌طورکلی درست است (همچنین رجوع کنید به پپر[۴۵]، 2010)، اما معماری کنونی نشان‌دهنده تلاشی قوی از سال 2009 برای ایجاد همکاری‌های بین دولتی است که توسط یک نهاد هماهنگ‌کننده مرکزی که به نخست‌وزیر، هیئت دولت و دبیرخانه امنیت ملی گزارش می‌دهد تسهیل می‌شود. مسئولیت‌ها به بخش‌هایی با تخصص و توانایی‌های موجود اعطا می‌شود. در مواردی که این بخش‌ها نیاز به تقویت دارند در صورت امکان، بودجه اضافه‌ای از برنامه سرمایه‌گذاری 1.9 میلیارد پوندی اعلام‌شده در استراتژی ملی امنیت سایبری 2016 تخصیص داده شده است. امنیت سایبری یکی از معدود حوزه‌های سیاستی است که وقتی بودجه‌های دیگر از طریق بررسی هزینه‌ها و اقدامات ریاضتی مالی کاهش می‌یابد، بودجه بیشتری دریافت می‌کند. بخش اعظمی از این بودجه به آژانس‌های اطلاعاتی، یعنی ویژگی تاریخی همه سیاست‌های امنیت سایبری دولت انگلستان هدایت می‌شود (استودارت[۴۶]، 20166). این مسئله پرسش‌هایی

---

[43] اعمالی که با تضمین دسترس‌پذیری، جامعیت، احراز هویت، محرمانگی و عدم انکار، از اطلاعات و سیستم‌های اطلاعاتی محافظت و دفاع می‌کند. این اعمال فراهم کردن بازیابی سیستم‌های اطلاعاتی با استفاده از قابلیت‌های حفاظت، تشخیص و عکس‌العمل را شامل می‌شود

[44] Blitz

[45] Pepper

[46] Stoddart

را در مورد انحراف داخلی اولویت‌های اعلام‌شده و تصرفات بوروکراتیک ایجاد می‌کند اما دولت در قبال این پرسش‌ها بر این اساس دفاع خواهد کرد که ستاد ارتباطات دولت میراث فنی و منابع لازم را برای کمک مؤثر منحصربه‌فرد به امنیت سایبری ملی دارد.

همان‌طور که دولت به‌طور کامل اذعان می‌کند، توانایی‌ها و دانش ضروری در خارج از بخش دولتی نیز وجود دارد. استراتژی ملی امنیت سایبری بخش خصوصی را به‌عنوان یک شریک کلیدی در دستیابی به جاه‌طلبی‌های اعلام‌شده برنامه ملی امنیت سایبری، از جمله توسعه بازار صادراتی قدرتمند در حوزه امنیت سایبری (دپارتمان تجارت بین‌الملل، 2018) می‌داند. این نگرش خلاف نظر دولت مبنی بر این است که بازار به اندازه کافی مخاطره سایبری را در نظر نگرفته و تاکنون به‌اندازه کافی در امنیت سایبری سرمایه‌گذاری نکرده است (دولت انگلستان، 2016b). درواقع، با در نظر گرفتن مالکیت خصوصیِ تقریباً تمام زیرساخت‌های حیاتی ملی، دولت انگلستان باید به مشارکت عمومی و خصوصی به‌عنوان راه‌حلی برای طیف وسیعی از مشکلات امنیت سایبری نگاه کند. این مشارکت‌ها به‌خوبی در انگلستان برای اهداف به اشتراک‌گذاری اطلاعات تهدید، تبادل دانش، ظرفیت‌سازی، توسعه مهارت‌ها، مشارکت‌های نوآوری، برون‌سپاری تخصصی، عرضه کالاها و خدمات و... تثبیت شده‌اند. با توجه به انگیزه‌های متفاوت بخش عمومی و خصوصی، تنش‌های ذاتی در چنین روابطی را می‌توان با تعبیه همه بازیگران در مراحل اولیه برنامه‌ریزی سیاست بهبود بخشید (کار[۴۷]، 2016)؛ بنابراین، انگلستان بخش خصوصی را علاوه بر توصیه‌های سیاستی غیررسمی ارائه‌شده توسط گروه‌های ذی‌نفع تجاری مانند شورای مشورتی تضمین اطلاعات (IAAC)، سازمان هوافضا و صنایع دفاعی (ADS Group) و جامعه تأمین‌کنندگان صنعت امنیت و تاب‌آوری (RISC) در طیفی از فعالیت‌ها که به توسعه سیاست امنیت سایبری کمک می‌کند، درگیر می‌کند. نکته قابل‌توجه مشارکت بین وزارت دفاع و صنعت در حفاظت سایبری دفاعی است که برای محافظت از زنجیره تأمین دفاعی در برابر تهدیدات سایبری کار می‌کند. این ابتکارات تضمین می‌کند که دولت بر مهارت‌ها و دانش بخش خصوصی برای درک محیط تهدید و راه‌حل‌های امنیت سایبری موجود سرمایه‌گذاری می‌کند. همچنین تعهد خرید تجاری را در حالی به‌طور ضمنی فراهم می‌کند که خطرات دوگانه عقب‌نشینی بخش خصوصی به سیاست‌های دولت و هرگونه نیاز فوری به مقررات دولتی را از بین می‌برد.

مرکز ملی امنیت سایبری اکنون تسهیل‌کننده اصلی تعامل عمومی_خصوصی است، اگرچه به‌هیچ‌وجه تنها نیست. یکی از نقش‌های کلیدی آن مشاوره به ادارات و سازمان‌های دولتی در مورد سیاست‌های امنیت سایبری، از جمله در مورد چگونگی سیاست‌گذاری «آینده‌نگر» در یک محیط فنی پویا است. این امر به یک دستور کار افق‌یابی گسترده‌تر در سراسر دولت گره خورده است و به این معنی است که مرکز ملی امنیت سایبری باید به دنبال تخصص از خارج از دولت برای آگاهی بخشیدن به مشاوره خود در زمینه علم و فناوری امنیت سایبری باشد (دفتر هیئت دولت، 2017). نمایندگان صنعت از طریق طرح‌هایی مانند «Industry 100» که کارکنان شرکت‌ها را در مرکز ملی امنیت سایبری بکار میگیرد تا روی مسائل خاصی از امنیت سایبری فنی و رفتاری کار کنند، جزء جدایی‌ناپذیری در این فرآیند هستند. این برنامه به‌عنوان یک سازوکار تبادل دانش بین صنعت و دولت عمل می‌کند تا تغییرات داخلی و خارجی را هدایت کند، اما توصیه‌های تخصصی را که مرکز ملی امنیت سایبری به سایر شرکای دولتی ارسال می‌کند و اساس توسعه سیاست را تشکیل می‌دهد نیز تضمین می‌کند. شرکت‌های خصوصی شرکای ضروری در ایجاد مرکز ملی امنیت سایبری به‌عنوان «صدای معتبر برای علم و فناوری امنیت سایبری» هستند (دفتر کابینه، 2017: 17). شرکت‌های با دامنه ملی، مانند BT و Nominet UK (رجیستری رسمی برای نام‌های دامنه .uk) مستقیماً با بخش‌های مختلف دولت از جمله مرکز ملی امنیت سایبری ارتباط برقرار می‌کنند. شرکت Nominet به همراه وزارت دیجیتال، فرهنگ، رسانه و ورزش ، همچنین یکی از سهام‌داران کلیدی در انجمن حکمرانی اینترنت انگلستان هستند که دیدگاه‌های صنعت و بخش سوم را به ارگان‌های سیاست‌گذار دولت نشان می‌دهد. در مواقعی نیز از شرکت‌ها دعوت می‌شود تا در مورد مسائل مربوط به سیاست‌های خاص برای کمیته‌های منتخب دولت مرکزی یا پارلمانی ارائه‌ای داشته باشند و در طول تهیه پیش‌نویس قانون (مانند قانون اختیارات تحقیق) و سیاست (مانند وزارت دیجیتال، فرهنگ، رسانه و ورزش ، 2018) مشورت‌های گسترده‌ای با صنعت صورت گرفته است.

قانون‌گذاری

مجلس انگلستان دخالت مستقیم کمی در سیاست و استراتژی امنیت سایبری دارد و مسئولیت آن بر عهده دولت است نه مجالس قانون‌گذاری مرکزی یا واگذارشده. بااین‌حال، مجلس در شکل‌دهی محیط قانونی‌ای که امنیت سایبری در آن عمل می‌کند و در اعمال نظارت بر فعالیت‌های بازیگران عمومی و خصوصی امنیت سایبری نقش مهمی دارد. انگلستان یکی از اولین کشورهایی بود که ضرورت جرم انگاری برخی جرائم مرتبط با رایانه را به رسمیت شناخت که منجر به قانون سوءاستفاده از رایانه (1990) شد. این قانون در طی سال‌ها و اخیراً نیز توسط قانون جرائم شدید (2015) اصلاح شده است. قانون سوءاستفاده از رایانه طیف وسیعی از دسترسی غیرمجاز به داده‌ها و سیستم‌های رایانه‌ای را غیرقانونی می‌داند. اصلاحات اخیر تعرفه‌ها را برای برخی تخلفات افزایش داده است، درحالی‌که همچنین اقدامات مخرب سایبری توسط شهروندان انگلستانی در خارج از قلمرو انگلستان را جرم انگاری می‌کند.

تصویب بعضاً ناخوشایند قانون اختیارات تحقیق (2016) مجلس (IPA) توجه ویژه جامعه اطلاعاتی را جلب کرده است. قانون اختیارات تحقیق با نام مستعار «منشور اسنوپر» ازنظر منتقدان، قدرت‌های نظارت الکترونیکی آژانس‌های اطلاعاتی انگلستان را توصیف و گسترش می‌دهد، اما در پاسخ به تقاضاهای پس از

[47] Carr

اسنودن، این موارد را با شفافیت و تدابیر بیشتر در مورد استفاده از آن‌ها، از جمله بررسی قضایی ضمانت‌نامه ارائه می‌دهد. این قانون یک کمیسیون دادگاه اختیارات تحقیق را برای اعمال نظارت در کنار کمیته اطلاعات و امنیت موجود (ISC) مجلس ایجاد کرد. قانون اختیارات تحقیق از برخی جهات مورد تکریم بوده و ارتقایی نسبت به قوانین قبلی است. برای مثال، این قانون به‌طور مطلوبی با قوانین نظارتی ایالات‌متحده و رویه جامعه اطلاعاتی در تضاد است اما توسط مبارزان حریم خصوصی و گروه آزادی‌های مدنی با استقبال ضعیفی مواجه شده است. این بازیگران به پیگیری اقدامات قانونی علیه آنچه که به‌عنوان یک حرکت اقتدارگرایانه در دولت انگلستان می‌دانند، در حال ادامه دادن هستند.

یکی دیگر از حوزه‌های کلیدی فعالیت قانون‌گذاری، حفاظت از داده‌ها است. قوانین موجود شامل قانون حفاظت از داده‌ها (1998) و مقررات حریم خصوصی و ارتباطات الکترونیکی (2003) است که برای همه سازمان‌هایی که اطلاعات شخصی افراد زنده را مدیریت می‌کنند اعمال می‌شود و مسئولیت‌های آن‌ها و مجازات عدم رعایت این مسئولیت‌ها را مشخص می‌کند. برخی مقررات با الحاق مقررات عمومی حفاظت از داده‌های اتحادیه اروپا (GDPR) در می 2018 در قوانین انگلستان تقویت شده است. قانون جدید حفاظت از داده‌ها در سال 2018، مأمور اطلاعات را ملزم به مطلع شدن از تمام موارد نقض داده‌ها می‌کند. همچنین مجازات شدید (تا 4 درصد از گردش مالی سالانه) برای عدم گزارش‌دهی و اقدامات غیرمسئولانه حفاظت از داده‌ها تعیین و چارچوب حفاظت از داده‌ها را سخت‌تر می‌کند. این امر نگرانی‌هایی را از سوی صنعت، به‌ویژه از سوی شرکت‌های کوچک و متوسط و خیریه‌هایی که در تلاش برای درک مقررات جدید هستند، چه برسد به پیروی از این مقررات، برانگیخته است. مرکز ملی امنیت سایبری با طیف وسیعی از منابع در دسترس برای کمک به این سازمان‌ها در انجام این کار واکنش نشان داده است. دولت همچنین دستورالعمل 2016 اتحادیه اروپا در مورد امنیت شبکه و سیستم‌های اطلاعاتی (دستورالعمل NIS) را اجرا کرده است که اپراتورهای ضروری زیرساخت‌های اطلاعاتی انگلستان را شناسایی کرده و مشوق امنیت سایبریِ بهتر است.

سیاست خارجی

انگلستان بارها اعتقاد خود را مبنی بر اینکه قوانین بین‌الملل در مورد فضای سایبری مانند هر حوزه عملیاتی دیگری اعمال می‌شود، ابراز کرده است. اولین استراتژی ملی امنیت سایبری این موضوع را پوشش می‌دهد اما از زمان استراتژی دوم در سال 2011، سیاست ملی امنیت سایبری وجود «مجموعه‌ای از اصول، رفتار و قوانین بین‌المللی مورد توافق را بیان کرده است که در فضای سایبری اعمال می‌شود» (دفتر کابینه، 18: 2011) حتی اگر موضوع چگونگی اعمال این موارد و پیامدهای مرتبط را کنار گذاشته باشد. دولت انگلستان همچنین جامعه بین‌المللی را تشویق می‌کند که مطابق با قوانین بین‌المللی و سایر هنجارهای رفتار بین‌دولتی عمل کند (به‌عنوان‌مثال، رایت، 2018). در مواردی که انگلستان دریافته است سایر کشورها آن چارچوب‌ها را به چالش کشیده‌اند، مطابق با مواد استراتژی ملی امنیت سایبری (دولت انگلستان، 50: 2016) حوادث سایبری را به بازیگران دولتی خاص نسبت داده است. قابل‌توجه در این زمینه، انتساب عمومی باج افزار «WannaCry» به کره شمالی و طیف وسیعی از عملیات سایبری تهاجمی به فدراسیون روسیه است (دفتر خارجی و مشترک‌المنافع، 2017؛ مرکز ملی امنیت سایبری، 2018). مشروعیت سیاسی انگلستان در این فضا، از جمله در نتیجه دخالتش در اقدامات نظارتی فراملی، همان‌طور که توسط ادوارد اسنودن در سال 2013 افشا شد، به چالش کشیده شده است. بااین‌حال، انگلستان علناً متعهد به حاکمیت حقوق بین‌الملل است، هم برای محدود کردن اقدامات خود و هم اقدامات دیگران و هم برای تسهیل عملیات سایبری خود در چارچوب‌های حقوقی بین‌المللی موجود.

یک مثال خوب از این پویایی با مشارکت انگلستان در فرآیند دستورالعمل تالین مرکز عالی دفاع سایبری ناتو (CCD COE) در تالین استونی ارائه شده است. دو مجلد دستورالعمل تالین (اشمیت[48]، 2013، 2017) به ترتیب در مورد اکتشافات هیئت حقوقی متخصص ناتو در مورد کاربرد قوانین بشردوستانه بین‌المللی در عملیات سایبری نظامی و ارتباط رژیم‌های قانونی دیگر با عملیات سایبری در زمان صلح گزارش می‌دهند. جلد اول نشان داد که جنگ سایبری نظامی توسط همان چارچوب‌های حقوقی بین‌المللی تنظیم می‌شود که سایر کاربردهای نیروی نظامی را شکل داده و محدود می‌کند. با توجه به خصوصیات لیبرال–دمکراتیک کشورهای عضو ناتو، این مسئله شاید تعجب‌آور نباشد، اما ادغام سریع آن در سیاست دفاع ملی قابل‌توجه بوده است.

انگلستان به‌سرعت یافته‌های خود را در برنامه‌ریزی دفاعی گنجاند (وزارت دفاع، 2013) و به‌عنوان یک بازیگر اصلی در ناتو، همچنین به تعهدات سیاست ناتو در قبال اصول تالین احترام می‌گذارد (به‌عنوان‌مثال، ناتو، 2014، 2016). دکترین سایبری نظامی انگلستان، تا حدی از استراتژی امنیت سایبری ملی متمایز شده است (اورمرود و ترنبول[49]، 2016)، اما ارتش و دولت هر دو به قوانین بین‌المللی در تدارک و اجرای عملیات سایبری احترام می‌گذارند. در مورد ارتش، از آنجایی‌که توصیه‌های حقوقی مانند اصول تالین به دکترین تبدیل می‌شوند، این امر عملیات سایبری ارتش انگلستان را محدود می‌کند، اما همچنین به آن‌ها اجازه می‌دهد تا از محیط سایبری به‌طور کامل با «بازی کردن تا لبه» (هایدن[50]، 2016) چارچوب دکترین استفاده کنند. به‌طور طبیعی، پذیرش «بازدارندگی

[48] Schmitt
[49] Ormrod & Turnbull
[50] Hayden

مدرن» و پاسخ‌های میان‌دامنه‌ای به تحریکات سایبری توسط انگلستان و (به‌طور مشترک با متحدان ناتو) (دونالدسون[۵۱]، 2017؛ لیندزی و گارتزک[۵۲]، 2017) همچنین به این معنی است که باید کاربرد رژیم‌های قانونی دیگر را برای آن شیوه‌های واکنش در نظر بگیرد.

سیاست امنیت سایبری انگلستان بدون تردید بر مطلوبیت ترویج هنجارهای بین‌المللی برای رفتار مسئولانه دولت در داخل و از طریق فضای سایبری تأکید کرده است. این قوانین به‌عنوان «قوانین راه» بیان می‌شوند که باید با شرکای بین‌المللی برای «حفاظت از آینده بلندمدت یک فضای سایبری آزاد، باز، صلح‌آمیز و امن» تدوین شوند (دولت انگلستان، 63: 2016a). انگلستان به‌عنوان عضو دائمی شورای امنیت سازمان ملل متحد، از زمان آغاز به کار در سال 2004 با گروه کارشناسان دولتی سازمان ملل متحد در امنیت اطلاعات (GGE) درگیر بوده است. این گروه در شکل دادن به دستور کار جهانی امنیت سایبری و در ترویج هنجار کاربرد قوانین بین‌المللی در فضای سایبری تا حدی موفقیت داشته است. بااین‌حال، گروه کارشناسان دولتی سازمان ملل توسط شکاف «جنگ سرد» دو پاره شده است که مانع از گزارش آن در 2016–2017 شد. این مسئله به‌طور گسترده‌ای به‌عنوان یک شکست و یک مانع حل نشدنی برای توسعه بیشتر هنجارهای جهانی تلقی می‌شود. با وجود این، وزارت امور خارجه و مشترک‌المنافع انگلستان به روح گروه کارشناسان دولتی سازمان ملل متحد متعهد باقی می‌ماند، حتی اگر مشخص نباشد چه چیزی ممکن است جایگزین آن شود (بوکات[۵۳]، 2017). انگلستان همچنین به‌طور کامل با گروه کاری جدید چین و روسیه در زمینه مسائل سایبری که در مجمع عمومی سازمان ملل در سال 2019 کارش را آغاز کرد، درگیر است.

انگلستان خود را «قهرمان» رویکرد چند ذی‌نفعی به حاکمیت جهانی اینترنت می‌داند (دولت انگلستان، 63 .p ،2016a). این کشور به میراث خود به‌عنوان یک مبتکر دیجیتالی افتخار می‌کند که اغلب از افرادی مانند آلن تورینگ و تیم برنرز لی استفاده می‌کند و از زمان آغاز به کار عضو اکثر سازمان‌ها و مؤسساتی بوده است که در جنبه‌های فنی، نظارتی و سیاستی حاکمیت اینترنت فعالیت می‌کنند. درحالی‌که نفوذ انگلستان کمتر از نزدیک‌ترین متحدش ایالات‌متحده است، انگلستان بازیگر مهمی در حاکمیت جهانی اینترنت و مشارکت‌کننده اصلی در همکاری و مشارکت بین‌المللی است. در این زمینه، انگلستان دولت را بیشتر تسهیل‌کننده و ضامن حکمرانی چند ذی‌نفع می‌داند تا ابزاری برای کنترل اینترنت جهانی (وزارت دیجیتال، فرهنگ، رسانه و ورزش، 2013). این موضع انگلستان را از اتخاذ مواضع قوی در مورد مسائل حاکمیتی جهانی، از جمله امنیت سایبری منع نمی‌کند، اما مرزی مفهومی بین آن و دولت‌هایی که بازتاب‌های خودکامه‌تری دارند مشخص می‌کند.

درزمینه خاص حکمرانی امنیت منطقه‌ای، همان‌طور که قبلاً ذکر شد، انگلستان یکی از اعضای کلیدی ناتو و نهادها و سازمان‌های اروپایی است که نقش‌های حیاتی در امنیت سایبری منطقه‌ای دارند. انگلستان یکی از امضاکنندگان اصلی کنوانسیون شورای اروپا در مورد جرائم سایبری (2001) بود که به دنبال هماهنگ کردن قوانین و عملیات بین‌المللی مبارزه با جرائم سایبری است. اگرچه تا سال 2011 این کنوانسیون را تصویب نکرد، اما انگلستان عضو فعال سازمان‌های پلیسی به‌ویژه یوروپل، آژانس مجری قانون اتحادیه اروپا و مرکز جدید جرائم سایبری اروپا (EC3) است که از جاه‌طلبی‌های کنوانسیون حمایت می‌کنند. انگلستان همچنین از کار آژانس اتحادیه اروپا برای امنیت شبکه و اطلاعات (ENISA) و طیفی از ابتکارات منطقه‌ای و فرا منطقه‌ای دیگر درزمینه حفاظت از زیرساخت‌های حیاتی، امنیت سایبری، جرائم سایبری و مبارزه با تروریسم حمایت می‌کند. اگرچه مقامات دولتی ادعا کرده‌اند که برگزیت بر همکاری امنیت سایبری انگلستان و اتحادیه اروپا تأثیری نخواهد داشت (استیونز و اوبراین، 2019)، اثرات خروج انگلستان از اتحادیه اروپا در سال 2019 (برگزیت) به‌ویژه در رابطه با پلیس جرائم سایبری، به اشتراک‌گذاری اطلاعات تهدیدات و درگیری آن با آژانس امنیت سایبری اتحادیه اروپا[۵۴] نامشخص است. طرف‌های مذاکرات خروج متعهد به حفظ پیوندهای نزدیک و قوی درزمینه مسائل امنیتی و اطلاعاتی هستند، اما تعاملات انگلستان با ترتیبات امنیت سایبری منطقه‌ای مشمول بررسی داخلی و خارجی خواهد بود (به‌عنوان‌مثال، دولت انگلستان، 2017).

مانند بسیاری از قدرت‌های امپریالیستی سابق، انگلستان روابط نزدیکی را با مستعمرات سابق خود حفظ می‌کند. در این مورد این کار از طریق رهبری اتحادیه کشورهای مشترک‌المنافع صورت می‌گیرد. انگلستان به‌عنوان منبع مشاوره و کمک به 52 کشور دیگر در این سازمان بین دولتی و به‌تبع آن جمعیت 2.5 میلیارد نفری موجود در آن عمل می‌کند. این امر به انگلستان دسترسی منحصربه‌فردی به کشورهای هر قاره می‌دهد و به آن اجازه می‌دهد تا امنیت سایبری را به‌ویژه پس از خروج از اتحادیه اروپا برای پیشبرد منافع ملی خود شکل دهد. علاوه بر انبوهی از اقدامات دوجانبه ظرفیت‌سازی و مشاوره، سازمان ارتباطات مشترک‌المنافع (CTO) از سال 2010 مجامع سالانه‌ای را برای ارتقای همکاری بین‌المللی در مورد مسائل امنیت سایبری و توسعه استراتژی‌هایی برای توسعه و اجرا، از جمله مدل حاکمیت سایبری مشترک‌المنافع (CTO) سازمان‌دهی کرده است. نشست سران کشورهای مشترک‌المنافع در سال 2018 در لندن شاهد انتشار بیانیه سایبری مشترک‌المنافع توسط ترزا می، نخست‌وزیر سابق بود، بیانیه‌ای از اصول و جاه‌طلبی‌ها برای بهبود امنیت سایبری در سراسر جامعه، اگرچه عمدتاً بر جرائم سایبری متمرکز بود (متشرک المنافع، 2018).

نگاه به آینده

---

[51] Donaldson
[52] Lindsay & Gartzke.
[53] Bowcott
[54] ENISA

سند ارزیابی ریسک امنیت ملی (NSRA) در سال 2015، مانند پیشینیان فوری خود، تهدیدات سایبری را در کنار تروریسم، جنگ بین دولتی، بیماری همه‌گیر و فجایع طبیعی، خطر «سطح یک» (احتمال زیاد و تأثیر بالا) در یک دوره پنج‌ساله برای انگلستان ارزیابی کرد. (دولت انگلستان، 2015). این ارزیابی به‌صراحت به حملات سایبری توسط کشورهای متخاصم و جرائم سایبری سازمان‌یافته در مقیاس بزرگ اشاره دارد، اما همچنین سایر گروه‌های خطر را نیز در بر می‌گیرد (بلاگدن[55]، 2018). این ارزیابی از خط‌مشی و استراتژی امنیت سایبری دولت و نیاز به واکنش بین بخشی و ملی خبر می‌دهد که در بالا ذکر شد: از منظر دولت، امنیت سایبری کلید امنیت ملی و اقتصادی است که بدون آن منافع ملی در داخل و خارج به خطر خواهد افتاد. نتایج مثبت زیادی برای این طرز تفکر وجود دارد: آگاهی عمومی بیشتر از مسائل سایبری؛ بهبود امنیت سایبری کسب‌وکار؛ روش‌های پیچیده‌تر مدیریت ریسک سایبری؛ بهبود تاب‌آوری اجتماعی و غیره. بااین‌حال، ارزیابی‌های داخلی دولت تاکنون از پیشرفت کلی انتقاد کرده‌اند (به‌عنوان‌مثال، اداره حسابرسی ملی، 2019) و واضح است که برنامه‌ریزی برای استراتژی ملی امنیت سایبری بعدی – که موعد مقرر آن سال 2021 است – باید به مسائل مربوط به منابع، هماهنگی درون دولتی، امنیت سایبری زنجیره تأمین و حفاظت از زیرساخت‌های حیاتی رسیدگی کند.

یکی از عوامل کلیدی در بهبود مستمر امنیت سایبری ملی انگلستان، ظهور جامعه اطلاعاتی عمومی‌تر، عمدتاً از طریق مرکز ملی امنیت سایبری بوده است. ظهور این جامعه اطلاعاتی ادامه روند طولانی‌تری است که در آن آژانس‌های مخفی از دهه 1990 در معرض نظارت عمومی قرارگرفته‌اند. همان‌طور که مدیر اجرایی مرکز ملی امنیت سایبری بیان می‌دارد، این یک ضرورت در «کار تیمی» امنیت سایبری است (مارتین، 2016). همچنان نگرانی‌هایی وجود دارد که علی‌رغم این موضع بازتر، سازمان‌های اطلاعاتی در قلب امنیت سایبری انگلستان نسبت به مردم انگلستان پاسخگو نیستند. به‌عنوان‌مثال، تصور می‌شود که سازوکار نظارتی اولیه کمیته اطلاعات و امنیت مجلس کمتر مستقل باشد و بنابراین کمتر ازآنچه ممکن است مؤثر باشد (دفتی[56]، 2018). همراه با مخالفت ضعیف پارلمانی نسبت به سیاست امنیتی دولت و سابقه نه‌چندان باشکوه آن در نظارت، مشخص نیست که اگر رویکرد کل کشور انگلستان در مورد امنیت سایبری از برخی خطوط هنوز درک نشده فراتر رود، مقاومت معنی‌دار در کجا ظهور خواهد کرد. استراتژی ملی امنیت سایبری سال 2009 شامل بخش کوتاهی بود که در آن بیان می‌کرد که ابزارهای امنیت سایبری باید معیارهای ضرورت و تناسب را داشته باشند و «بنیاد اخلاقی واضح و تدابیر حفاظتی مناسب برای استفاده ضروری است تا اطمینان حاصل شود که از قدرت این ابزارها سوءاستفاده نمی‌شود» (دولت انگلستان، 2009a: 10). این آرزو هنوز در هیچ بیانیه رسمی امنیت سایبری ملی ظاهر نشده است.

نتیجه‌گیری

انگلستان می‌تواند به‌طور قابل قبولی ادعا کند که یکی از یکپارچه‌ترین رویکردها برای امنیت سایبری ملی را در جهان دارد. به اعتراف خود، این رویکرد دیگر نمی‌تواند کامل‌تر از هر شکل دیگری از امنیت باشد؛ بنابراین، هدف امنیت سایبری انگلستان که به‌عنوان تمرینی در مدیریت ریسک تلقی می‌شود، به حداقل رساندن اختلالات جدی و به حداکثر رساندن رونق اقتصادی است، درحالی‌که توانایی خود را برای ایجاد نفوذ در خارج از کشور و فعالیت در سطح جهانی در راستای منافع ملی حفظ می‌کند، می‌تواند از قابلیت‌های حاکمیتی موجود سرمایه‌گذاری کند و درعین‌حال برای کمک به پروژه امنیت سایبری ملی با شرکای خود در بخش‌های مختلف ارتباط برقرار کند. این کشور امنیت سایبری را فرصتی برای معرفی خود در جهان هم به‌عنوان یک الگو و هم به‌عنوان نشان دادن تعهد خود به اینترنت باز و ایمن جهانی می‌بیند؛ مانند بسیاری از کشورها، انگلستان نیز با چالش‌هایی از محیط تهدید پویا مواجه است. انگلستان کشور ثروتمندی است که هدف جذابی برای مجرمان سایبری است و قدرت جهانی بزرگی است که در صورت زوال باید با سایر کشورهای قدرتمندی که در فضای سایبری نیز به دنبال مزیت هستند، مبارزه کند. تجربیات اخیر این کشور از خرابکاری اطلاعاتی و سایبری روسیه حاکی از راهی دشوار در پیش است و این منظر که بازدارندگی آن‌طور که ممکن است به‌سادگی عمل نمی‌کند بسیار واقعی است. استراتژی ملی امنیت سایبری جدید که برای سال 2021 برنامه‌ریزی‌شده است، باید این را در نظر بگیرد. خروج این کشور از اتحادیه اروپا در سال 2019 نیز پیش‌بینی‌ها در مورد امنیت سایبری آینده را مخدوش می‌کند، اما انگلستان برای مقابله با مقیاس و دامنه مسائل امنیت سایبری که در معرض آن قرار دارد، شاید بهتر از بسیاری از کشورهای دیگر باشد.

---

[55] Blagden
[56] Defty

نروژ

مقدمه

اهمیت سیاست‌گذاری در حوزه امنیت سایبری در کشور کوچک و دیجیتالی نروژ رو به رشد است. با این حال، نروژ مانند کشورهای بسیار پیشرفته با وجود منافع تجاری خصوصی و انبوه بازیگران از نظر فناوری، در ایجاد امنیت سایبری ملی با مشکلاتی مواجه شده است. در سال‌های اخیر تلاش‌هایی با هدف متحد کردن مؤسسات و سازمان‌های متفاوت در چارچوبی منسجم شکل گرفته است. این فصل خلاصه‌ای از اهمیت نسبی امنیت سایبری برای نروژ را بیان کرده و سپس سطح دیجیتالی‌سازی نروژ را با دیگر کشورها مقایسه می‌کند. در ادامه، تاریخچه و اسناد اصلی این حوزه را در سطح ملی و بین‌المللی بررسی می‌کند و در نهایت، با نکاتی در مورد مسیر پیش رو و چالش‌هایی که نروژ در رابطه با موضوع امنیت سایبری با آن مواجه است، فصل به پایان می‌رسد.

پیش‌زمینه، دیجیتالی شدن و امنیت

در کنار سایر کشورهای شمال اروپا، نروژ یکی از دیجیتالی‌ترین کشورهای جهان است که در شاخص DESI در سال 2018 بالاتر از میانگین اتحادیه اروپا قراره گرفته است. نروژ سطح بالایی از دیجیتالی‌شدن را طی کرده است؛ به‌ویژه در ملاک‌هایی چون گستره خدمات اینترنتی و خدمات عمومی دیجیتال مانند بانکداری، اخبار و دولت الکترونیک (کمیسیون اروپا، 2018). در نتیجه، اقتصاد و جامعه نروژ به شدت به عملکرد صحیح خدمات دیجیتال وابسته است. این سطح بالای دیجیتالی شدن، امنیت سایبری را به یک نگرانی بزرگ تبدیل می‌کند؛ به‌طوری که این کشور در گزارش سالانه آژانس‌های امنیتی، مدام در صدر فهرست کشورهای در معرض خطر قرار می‌گیرد.

نروژ به عنوان یک کشور کوچک، به طور سنتی به متحدان خارجی متکی بوده و همچنین به هنجارها و قوانین بین‌المللی که رفتار دولت را تنظیم می‌کند، وابسته بوده است (Riste، 2005). این امر به پیروی از قوانین امور بین‌الملل و نهادهایی مانند سازمان ملل متحد و به حداقل رساندن استفاده از زور و خطر درگیری را نتیجه داده است (همان). در صورت بروز خصومت‌ها و بحران بین‌المللی، امنیت نروژ باید به عضویت خود در سازمان پیمان آتلانتیک شمالی (ناتو) تکیه کند.

اما اولویت‌ها و رویکرد نروژ به امنیت سایبری به دلایل مختلفی متفاوت است: اول، مالکیت خصوصی گسترده زیرساخت‌های دیجیتال مستلزم همکاری نزدیک‌تر بین بخش عمومی و بخش خصوصی در تأمین امنیت سایبری است (نگاه کنید به، هیلی، 2013). علاوه بر این، عمده (اگر نگوییم همه) حوادث امنیت سایبری از آستانه نیروی مسلح نیستند. این موضوع مکانیسم‌های مختلفی از همکاری بین‌المللی را فرا می‌خواند. حوادث سایبریِ با انگیزه سیاسی، اغلب در یک منطقه خاکستری بین فعالیت مجرمانه و استفاده آشکار از زور عمل می‌کنند (نگاه کنید به، کلو، 2017). این موضوع واکنش‌های سیاسی را پیچیده و نهادها و سازمان های درگیر را سردرگم می‌کند. تأمین امنیت سایبری یک چالش جدید و چند وجهی برای اکثر جوامع است که برای رویارویی با آن به بازیگران و شیوه‌های مختلف نیاز است (Collier، 2018). در نتیجه، تطبیق امنیت سایبری در چارچوب‌های امنیتی سنتی مانند ناتو دشوار است (Fitton، 2016).

مروری کوتاه بر تاریخ امنیت سایبری نروژ

رویارویی با این چالش یک رویه در حال تکامل بوده و شکل‌های مختلفی به خود گرفته است. نروژ به‌عنوان یکی از اولین پذیرنده‌های فناوری‌های اینترنتی، سابقه نسبتاً طولانی در تلاش برای تأمین امنیت شبکه‌های دیجیتال دارد. تلاش‌های اولیه، مانند کتاب سفید 2001 از استورتینگ (پارلمان نروژ) امنیت فاوا را در درجه اول بر بخش ارتباطات مؤثر می‌دید. مشخصه این دوره افزایش اهمیت زیرساخت‌های ICT است؛ با این حال همچنان امنیت فاوا را نیازمند به اقدام هماهنگ یا رویکرد ملی کل‌نگر نمی‌داند. همچنین در سال‌های اولیه شاهد ایجاد مکانیزمی برای نظارت بر جریان داده‌ها در بخش‌های خصوصی حیاتی بودیم (St. Meld. 17، 2001–2002)، اما تلاش‌های هماهنگ کمی برای رسیدگی به مسائل امنیت دیجیتال وجود داشت. همان‌طور که دیجیتالی شدن سرعت خود را افزایش داد و کارکردهای بیشتری را در بر گرفت، نگرانی در مورد استفاده نادرست از فناوری ICT و تأثیرات آن بر جوامع افزایش یافت. این دوره همچنین شاهد ایجاد مؤسساتی مانند National CERT در سال 2006 و همچنین گسترش زیرساخت های موجود مانند VDI و تمرینات سراسری مانند ICT 2008 بود (St. Meld.22، 2007–2008).

یک تغییر قابل توجه با برجستگی افزایش امنیت اجتماعی پس از حملات Utøya 2011 رخ داد. درک شکست مکانیسم‌های واکنش دولت، نقطه شروعی برای بررسی گسترده در مورد چگونگی افزایش امنیت اجتماعی شد (به St. Meld. 29، 2011–2012 مراجعه کنید). این تمرکز گسترده‌تر، به ویژه در سال 2015 با انتشار گزارش کمیته آسیب‌پذیری‌های دیجیتال در جامعه[۵۷]، به سرپرستی پروفسور اولاو لیسن (دولت نروژ، 2015) مصادف شد. این کمیته ارزیابی، گسترده‌ای از آسیب‌پذیری‌های دیجیتال در جامعه نروژ را شناسایی کرد تا به عنوان مبنایی برای کارهای امنیتی بعدی مورد استفاده قرار گیرد. این کمیته به فهرست بلندبالایی از پیشنهادات برای هدایت کار روی امنیت فناوری اطلاعات و ارتباطات اشاره کرد که تا حد زیادی به عنوان چارچوبی برای انتشارات و ابتکارات بعدی استفاده شده است. از آن زمان، کار بر روی تقویت امنیت سایبری نروژ به طور قابل توجهی رشد کرده است.

امنیت سایبری: رویکرد، اسناد اصلی و ساختار

رویکرد نروژی به امنیت سایبری کاملاً در دایره درک غرب از همکاری چندجانبه بین بازیگران دولتی و خصوصی قرار دارد. در این رویکردِ ناشی از درجه بالای مالکیت خصوصی بر زیرساخت‌های حیاتی، امنیت سایبری به عنوان گردآوری بازیگران مختلف مفهوم‌سازی می‌شود. این بازیگران با فراهم کردن امنیت اجتماعی همکاری و در عین حال رقابت می‌کنند. (Collier، 2018). در نظر گرفتن این همکاری خصوصی–عمومی به عنوان یک نقطه نظر، چارچوب غالب برای درک امنیت سایبری در نروژ است. این رویکرد، بازتاب تلاش‌های در کشورهای بزرگ‌تری مانند ایالات متحده و بریتانیا به عنوان مهم‌ترین متحدان نروژ در سیاست امنیتی است.

ترکیبی از اتخاذ «بهترین شیوه‌ها» از کشورهای مشابه، تطبیق آنها با شرایط نروژی، و همچنین برخی تلاش‌ها در زمینه نوآوری، اکثر ساختار و وضعیت امنیت سایبری نروژ را توضیح می‌دهد. معماری امنیت اجتماعی نروژ بر چهار اصل اساسی استوار است:

1. مسئولیت: بیانگر آن است که سازمانی که مسئولیت امور روزمره را بر عهده دارد در صورت بروز بحران نیز باید پاسخگو باشد.
2. شباهت: سازماندهی برای مدیریت بحران باید شبیه سازمان‌دهی عادی باشد.
3. نزدیکی: با هر بحرانی باید در پایین‌ترین سطح ممکن برخورد کرد.
4. همکاری: هر مقام و بازیگری که درگیر امنیت است، مسئولیت دارد تا بهترین همکاری ممکن را بین بازیگران تضمین کند (St. Meld.10، 2016–2017).

در عمل این امر مستلزم ساختاری است که در آن هر وزارتخانه مسئولیت تأمین امنیت حوزه خود را بر عهده دارد. *وزارت دادگستری و امنیت عمومی* صرفاً نقش هماهنگ کننده را دارد که برقراری امنیت در سطح کلان را بررسی می‌کند.

سند اصلی خط مشی نروژ، استراتژی سایبری 2012 برای نروژ[۵۸] است. این استراتژی، همچنان اصلی‌ترین سند تعیین کننده اولویت‌های کشور در حوزه دیجیتال است؛ هرچند این استراتژی در دست بازنگری است. در این سند، اولویت‌های اصلی برای اقدامات آتی در چهار هدف کلی تعیین شده است:

1) هماهنگی بهتر و ایجاد درک مشترک از موقعیت‌ها

2) زیرساخت ICT قوی و ایمن برای همه

3) توانایی بالای مدیریت رویدادهای نامطلوب

4) سطح بالای آگاهی امنیتی (وزارتخانه های نروژ، 2012).

رویکرد امنیت سایبری عمدتاً همان رویکرد کلی به امنیت اجتماعی را منعکس می‌کند؛ البته همراه با برخی مؤلفه‌های اضافی برای مقابله با ماهیت ملی و فرابخشی امنیت سایبری. یک بازیگر حیاتی، *سازمان امنیت ملی (NSM)*[۵۹] است که در مالکیت مشترک وزارت عدلیه و امنیت عمومی و وزارت دفاع است. مسئولیت اصلی هماهنگی و نظارت بر امنیت سیستم‌ها و عملکردهای حیاتی تحت پوشش قانون امنیت[۶۰]، بر عهده این نهاد است. (سازمان امنیت ملی،

[57] Committee of Digital Vulnerabilities in Society
[58] 2012 Cyber Strategy for Norway
[59] National Security Authority (NSM)
[60] Security Act

2018b). روی کاغذ، NSM فقط برای خدمت به زیرساخت‌های حیاتی و همچنین مشاوره به سازمان‌ها و مؤسسات مختلف دیگری که وظیفه اجرای امنیت سایبری روزمره را بر عهده دارند، در نظر گرفته شده است؛ اما مالکیت آن بر تیم پاسخ‌دهی ملی و مرکز امنیت سایبری تازه تأسیس، نشان می‌دهد که این نهاد دارای نقش بزرگتری در مدیریت حوادث است (سازمان امنیت ملی، 2018).

در عین حال، بازیگران مختلف دیگری نیز در حوزه دیجیتال مسئولیت دارند. *پلیس*، مسئولیت اصلی بررسی اقدامات مجرمانه و حفظ نظم و قانون آنلاین را بر عهده دارد، اما برای انجام این وظیفه دچار چالش شده است. در سال 2018، *مرکز ملی جرایم سایبری (NC3)* با هدف افزایش صلاحیت‌ها در تحقیق جرایم دیجیتال، توسط پلیس نروژ تأسیس شد. علاوه بر پلیس، نهادهای اطلاعاتی مختلف نیز در شناسایی و پاسخگویی به تهدیدات مسئولیت دارند. *مرکز هماهنگی سایبری*[۶۱] این آژانس‌های مختلف را هماهنگ می‌کند. دفاع سایبری نیروهای مسلح نروژ[۶۲] وظیفه حفاظت از سیستم‌های ارتباطی نیروهای مسلح را بر عهده دارد و فراتر از این مأموریت نقشی ایفا نمی‌کند (دولت نروژ، 2012).

مالکیت بخش بزرگی از خدمات و زیرساخت‌های حیاتی توسط شرکت‌های خصوصی، یک مشکل برجسته شده برای جوامع مدرن است؛ به‌ویژه هنگامی که صحبت از ایمن سازی آنها از تهدیدها و خطرات دیجیتالی می‌شود (دان، کاولتی و سوتر، 2009). نروژ از این نظر تفاوتی با بقیه کشورهای مدرن ندارد و کارهای امنیتی روزمره، بیشتر توسط بازیگران خصوصی انجام می شود. *Telenor*، ارائه دهنده اصلی خدمات مخابرات، مهم‌ترین این شرکت‌ها است. تأمین امنیت نیز توسط بازیگران خصوصی متخصص در امنیت دیجیتال انجام می‌شود. برای نروژ، همکاری بین این بازیگران خصوصی و دولت برای حفظ سطوح کافی از امنیت سایبری بسیار مهم است. این همکاری وجود دارد و در حال بهبود است، اما تفاوت‌هایی در سطوح پیچیدگی و رویکردهای مورد استفاده دو بخش وجود دارد. برای امنیت سایبری، موضوعی که بخش‌های مختلف را در بر می‌گیرد و تلاش‌های هماهنگ را می‌طلبد، نیاز به اقدامات در سطح ملی مشهود است. فقدان یک نهاد ملی که وظیفه تضمین امنیت سایبری سراسری را داشته باشد، قابل توجه است. در سال 2017، وزارت عدلیه و امنیت عمومی تصمیم گرفت تا کمیسیونی را با این هدف تعیین کند. این کمیسیون تا زمان نگارش این مقاله به نتیجه نرسیده است (دولت نروژ، 2017).

- **چشم‌انداز بین‌المللی**

رویکرد سنتی نروژ به مسائل امنیتی رو به بیرون بوده است؛ یعنی اغلب نهادهای بین‌المللی را درگیر و بر اهمیت هنجارهای تنظیم‌کننده رفتار دولت تأکید می کند. ناتو، همچنان ستون استراتژیک مسلط برای امنیت ملی نروژ است و تا حدی با مسائل امنیت سایبری نیز همپوشانی دارد. فراتر از این، نروژ همچنین با شرکا و متحدان مختلف منطقه‌ای، از طریق همکاری‌های شمال اروپا، درگیر است. ابتکارات اروپایی به‌طور گسترده از طریق توافقنامه منطقه اقتصادی اروپا (EEA) اجرا می‌شود.

در سند "استراتژی امنیت سایبری بین‌المللی[۶۳]" بر نیاز به همکاری بین کشورها به منظور ارتقای صلح و ثبات در حوزه دیجیتال، در راستای حمایت نروژ از حقوق بین‌الملل تأکید می‌کند. این سند به وضوح بیان می‌کند که حقوق بین‌الملل به شکل فعلی‌اش برای فضای سایبری نیز قابل اجرا است. نروژ یک کشور کوچک علاقه‌مند به تداوم نظم جهانی است و توسط قوانین بین‌المللی کنترل می‌شود؛ لذا درخواست او برای تنظیم‌گری عمیق‌تر فضای سایبری در سطح جهانی جای تعجب ندارد.

برای نروژ، نیاز به امنیت سایبری در سطح جهانی و از طریق نهادهای رسمی ضروری به نظر می‌رسد. بنابراین استراتژی بین‌المللی بر نیاز نروژ برای مشارکت و کمک به پیشبرد کار در نهادهای بین‌المللی مانند اتحادیه اروپا، سازمان ملل، ناتو، سازمان همکاری اقتصادی و توسعه (OECD) و سازمان امنیت و همکاری در اروپا تأکید می‌کند. (OSCE).

همچنین این استراتژی خواستار نوعی از فضای دیجیتالی است که نوآوری، تجارت و ثبات را ترویج کرده و به عنوان مروج حکومت دموکراتیک و حقوق بشر عمل می‌کند. به ویژه برجسته کردن پتانسیل فضای مجازی برای گسترش دموکراسی، موضع نروژ را در تضاد با مفهوم روسی–چینیِ «حاکمیت سایبری» و حکومت چندجانبه قرار می‌دهد و از رویکرد چندجانبه غربی حمایت می‌کند. به طور کلی، درک نروژی از کاربرد حقوق بین‌الملل در فضای سایبری با پایبندی زیاد به هنجارهای بین‌المللی و درک آن هنجارها در راستای تفسیر «غربی» از موضوع تعریف می‌شود.

---

[61] The Cyber Coordination Center
[62] The Norwegian Armed Forces Cyber Defense
[63] International Cyber Security Strategy

موضوع اتحادیه اروپا نیز به امنیت سایبری این کشور ارتباط دارد. موقعیت نروژ به عنوان یکی از اعضای EEA، اما نه عضو اتحادیه، در موضوع امنیت سایبری یک نقطه قوت است. از آنجایی که این موضوع هم موضوعات امنیتی و هم موضوعات اقتصادی را پوشش می‌دهد، ماهیت درونی و بیرونی رویکرد نروژ به چالش کشیده می‌شود. به‌طور کلی، رویکرد نروژی تلاش می‌کند خود را با مقررات اتحادیه اروپا هماهنگ کند، با این حال نروژ تأثیر بسیار محدودی بر نحوه ایجاد این مقررات دارد که در نتیجه نگرانی‌هایی در مورد «کسری دموکراتیک» ایجاد می‌کند (Aale، 2012). نروژ دو بار موضوع عضویت را به رأی عمومی گذاشته است و هر دو بار این عضویت توسط اکثریت رد شده است. تغییر زمینه‌های ژئوپلیتیکی و تهدیدات امنیتی جدید مانند حملات سایبری، موضوع جایگاه نروژ در اروپا را مهم‌تر می کند.

- **خلاصه و راه پیش رو**

با اینکه که نروژ یک کشور پیشرو در دیجیتالی‌سازی بود، بخش اصلی کار روی امنیت سایبری در سال‌های اخیر انجام شده است. عمده فعالیت نروژ، ایجاد نهادهای جدید و گسترش اختیارات نهادهای قدیمی‌تر بوده است. این امر افزایش سرمایه‌گذاری روی توانایی نهادهای سنتی مانند پلیس و سرویس‌های اطلاعاتی را نیز در پی داشته است. رویکرد نروژ عمدتاً تدافعی بوده است. در حالی که افزایش تمرکز و منابع امنیت سایبری نروژ را بهبود بخشیده است، مشکلات و چالش‌های ساختاری در سال‌های آینده همچنان وجود خواهد داشت.

یک چالش قابل توجه تغییر محیط بین‌المللی است که یک سری سؤالات دشوار را برای دولت نروژ ایجاد خواهد کرد. روسیه در ارتباط با ناامنی‌های ناشی از ریاست جمهوری ترامپ، تردیدهایی را در پایه‌های سیاست امنیتی نروژ ایجاد کرده است. آنچه به‌عنوان یک تهدید فزاینده از سوی روسیه تلقی می‌شود، توانایی دولت نروژ را برای واکنش به چالش می‌کشد. فقدان مقررات بین‌المللی در مورد عملیات سایبری به سخت‌تر شدن واکنش و بازدارندگی از حوادث می‌انجامد. با انتشار «استراتژی بین‌المللی سایبری برای نروژ»، می‌توان استدلال کرد که این نیاز به بُعد بین‌المللی مورد توجه واقع شده است، اما برای نتیجه‌گیری در مورد تأثیر آن خیلی زود است. در حالی که این استراتژی اصول گسترده‌ای را در مورد چگونگی دستیابی به امنیت سایبری بیان می‌کند، اما فاقد جزئیات است و جنبه‌های مهمی مانند حالت‌های بازدارندگی را حذف می‌کند.

فراتر از سیاست بین‌المللی امنیت سایبری، استفاده حداکثری از منابع محدود در سال‌های آینده بسیار مهم خواهد بود. نیاز به کارگران ماهر در زمینه امنیت سایبری مدتی است که به رسمیت شناخته شده است، با این حال به تلاش بیشتری برای از بین بردن این شکاف نیاز است. از آنجایی که مجموعه استعدادها محدود است، همکاری نزدیک بین بازیگران دولتی و خصوصی و همچنین کشورهای متحد برای استفاده حداکثری از ظرفیت‌های موجود لازم است. موضوعی که برای بهبود همکاری عمومی و خصوصی وجود دارد، ایجاد انگیزه‌های مناسب برای شرکت‌های خصوصی است تا برای تأمین امنیت ارزش قائل شوند. فراهم کردن بخش امنیت سایبری خصوصی پر جنب‌وجوش، و همچنین گنجاندن آن در چارچوب امنیت سایبری بزرگ‌تر، در استفاده حداکثری از منابع و ظرفیت‌های محدود بسیار مهم خواهد بود. توانایی نروژ برای دور نگه داشتن مسائل امنیت سایبری در سال‌های آینده احتمالاً به توانایی همکاری عمومی و خصوصی بستگی دارد.

یک چالش مرتبط، رفت و برگشت بین امنیت و حریم خصوصی است. سیستم موجود برای مقابله با حوادث در سال‌های آینده کافی نخواهد بود. راه حل پیشنهادی نظارت دیجیتالی در مرز، تحت محدودیت‌ها و نظارت‌های دقیق، منشأ بحث‌های شدید در مورد رفت و برگشت بین امنیت و حریم خصوصی بوده است. مخالفان سیستم پیشنهادی عمدتاً به سهولت دستکاری این سیستم‌ها برای نظارت بر همه شهروندان اشاره می‌کنند (Datilsynet، 2017). طرفداران استدلال می‌کنند که افزایش دیجیتالی شدن هیچ انتخابی برای دولت باقی نمی‌گذارد و هیچ جایگزین مناسبی وجود ندارد (Løkke، 2017).

نکته پایانی تأکید بر ضرورت کارساز بودن تمهیدات امنیتی موجود و همچنین پرکردن خلأهای موجود است. یک چالش همیشگی شکاف بین بخش‌ها و وزارتخانه‌های مختلف در حصول اطمینان از کافی بودن اقدامات امنیتی است. فقدان یک مرجع متمرکز منجر به شیوه‌های امنیتی متفاوتی شده است. در حالی که برخی در خط مقدم کارهای امنیتی هستند، برخی دیگر عقب مانده و با مشکل مواجه هستند. تا زمانی که رویکرد غیرمتمرکز به امنیت در شرایط جمعی باقی بماند، مقابله با خطرات فراملی مانند امنیت سایبری چالش برانگیز خواهد بود. ابتکارات جدیدی برای بهبود هماهنگی ملی با سازمان‌های مورد انتظار مانند مرکز ملی امنیت سایبری و NC3 انجام شده است. راه اندازی این مؤسسات جدید در چارچوب فعلی موضوع اصلی در سال های آینده خواهد بود.

برای مطالعه بیشتر

آمریکا

- CSIS. (2020). “Significant Cyber Incidents.” https://csis-prod.s3.amazonaws.com/s3fs-public/200306_Significant_Cyber_Events_List.pdf?qRZXF65CUUOKTOl9rLVBMJhXfXtmJZMj
- Taylor, R. W., Fritsch, E. J., Saylor, M. R. & Tafoya, W. L. (2018). Cyber Crime and Cyber Terrorism. London: Pearson.
- Valeriano, B. & Jensen, B. (2019, January 15). The Myth of the Cyber Offense: The Case for Restraint. Washington, DC: CATO Institute. cato.org/publications/policy-analysis/myth-cyber-offense-caserestraint
- Van Puyvelde, D. & Brantly, A. (2017). US National Cybersecurity: International Politics, Concepts and Organization. Abingdon, Routledge.
- The White House. (2018, September). “National Cyber Strategy of the United States of America.” www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

کانادا

- Fundamentals of Cyber Security for Canada’s Critical Infrastructure Community. Building a Safe and Resilient Canada. www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/2016-fndmntls-cybr-Scrty-cmmnty-en.pdf
- Public Safety Canada. “Cyber Incident Management Framework for Canada.” www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-ncdnt-frmwrk/index-en.aspx
- Public Safety Canada. “National Strategy for Critical Infrastructure.” www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx
- Public Safety Canada. “Canada’s Cyber Security Strategy: For a Stronger and More Prosperous Canada.”http://publications.gc.ca/collections/collection_2010/sp-ps/PS4-102-2010-eng.pdf
- Public Safety Canada. “Canadian Cyber Incident Response Centre (CCIRC).” www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-en.aspx

اتحادیه اروپا

- Calcara, A., Csernatoni, R. & Lavallée, C. (eds.). (2020). Emerging Security Technologies and EU Governance: Actors, Practices and Processes. Abingdon: Routledge.
- Choucri, N. & Clark, D. D. (2018). International Relations in the Cyber Age: The Co-Evolution Dilemma.Cambridge, MA: MIT Press
- Christou, G. (2016). Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy (New Security Challenges). Basingstoke: Palgrave Macmillan.
- Ilves, L. K., Evans, T. J., Cilluffo, F. J. & Nadeau, A. A. (2016). “European Union and NATO Global Cybersecurity Challenges: A Way Forward,” PRISM, 6(2): 126–141.
- Wessel, R. A. (2019). “Cybersecurity in the European Union: Resilience through Regulation?” in E. Conde, Z. Yaneva & M. Scopelliti (eds.), Routledge Handbook of EU Security Law and Policy (pp.283–300). Abingdon, Routledge.
- Westby, J. (2019, October 31). “Why the EU Is about to Seize the Global Lead on Cybersecurity,”Forbes, forbes.com/sites/jodywestby/2019/10/31/why-the-eu-is-about-to-seize-the-global-lead-oncybersecurity/#38ffb62c2938

انگلستان

- Harrop, W. & Matteson, A. (2015). “Cyber resilience: A review of critical national infrastructure and cyber-security protection measures applied in the UK and USA,” in F. Lemieux (ed.), Current and emerging trends in cyber operations (pp. 149–166). London: Palgrave Macmillan.
- HM Government. (2016). “National cyber security strategy, 2016–2021.” https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
- Steed, D. (2019). The politics and technology of cyberspace. London, Routledge.

نروژ

- Norwegian Ministries. (2012). “Cyber Security Strategy for Norway.” www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/cyber_security_strategy_norway.pdf
- Norwegian Ministry of Foreign Affairs. (2017). “International cyber strategy for Norway.” www.regjeringen.no/globalassets/departementene/ud/dokumenter/sikpol/cyberstrategy_2017.pdf
- Norwegian Ministry of Foreign Affairs. (2018). “Digital Strategi for utviklingspolitikken.” (Digital Strategy for Development). www.regjeringen.no/globalassets/departementene/ud/dokumenter/utvpolitikk/digital_strategi2018.pdf
- NOU. (2015). 13 “Digital sårbarhet – Sikkert samfunn: Beskytte enkeltmennesker og samfunn i en digitalisert verden” (Lysne 1). www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf
- St. Meld. 38. (2016–2017). “Cyber Security – A Joint Responsibility.” www.regjeringen.no/en/dokumenter/meld.-st.-38-20162017/id2555996/

منابع

آمریکا

- Alexander, S. (2017, February 6). “Notes from the Asilomar Conference on Beneficial AI.” https://slatestarcodex.com/2017/02/06/notes-from-the-asilomar-conference-on-beneficial-ai/
- Beaver, K. (2015, September 28). “The Importance of a Security Culture across the Organization,” Securityintelligence.com. https://securityintelligence.com/the-importance-of-a-security-culture-acrossthe-organization/
- Brenner, J. & Lindsay, J. R. (2015). “Correspondence: Debating the Chinese Cyber Threat,”International Security, 40(1): 191–195.
- Brown, G., Carlye, M., Salmeron, J. & Wood, K. (2006). “Defending Critical Infrastructure,” Interfaces, 36(6): 530–544.
- Chander, A. (2012). “Facebookistan,” North Carolina Law Review, 1807(90). https://scholarship.law.unc.edu/nclr/vol90/iss5/15Facebookistan
- Darnell, C. (2019, May 22). “Concern over Facial Recognition Technology Unites Progressive and Conservatives in Congress,” Yahoo News. https://news.yahoo.com/concern-over-facial-recognitiontechnology-unites-progressives-and-conservatives-in-congress-234327186.html
- Deval, D. (2019). “The U.S. Response to the 2016 Russian Election Meddling and the Evolving National Strategic Thought in Cyberspace: (Part 2),” Academic and Applied Research in Military and Public Management Science, 18(1): 59–77.
- DeVore, M. R. & Lee, S. (2017). “APT (Advanced Persistent Threat)s and Influence: Cyber Weapons and the Changing Calculus of Conflict,” The Journal of East Asian Affairs, 31(1): 39–64. Retrieved from www.jstor.org/stable/pdf/44321272.pdf

- Dourado, E. & O'Sullivan, A. (n.d.). "Poor Federal Cybersecurity Reveals Weakness of Technocratic Approach." www.mercatus.org/publications/technology-and-innovation/poor-federal-cybersecurityreveals- weakness-technocratic
- Geiger, A. W. (2018, June 4). "How Americans Have Viewed Government Surveillance and Privacy since the Snowden Leaks," Pew Research. www.pewresearch.org/fact-tank/2018/06/04/how-americanshave-viewed-government-surveillance-and-privacy-since-snowden-leaks/
- Gilli, A. & Gilli, M. (2019). "Why China Has Not Caught up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering and Cyber Espionage," International Security, 43(3): 141–189.
- IndiaToday.in. (2018, June 10). "What Is the Shanghai Cooperation Organization and Why Is Its Membership Crucial for India?" India Today. www.indiatoday.in/education-today/gk-currentaffairs/story/what-is-shanghai-cooperation-organisation-and-why-does-its-membership-matter-for-india-1256624-2018-06-10
- Klimburg, A. (2011). "The Whole of Nation in Cyber Power," Georgetown Journal of International Affairs: 171–179. www.jstor.org/stable/pdf/43133826.pdf?refreqid=excelsior%3A76a84e45ce1ae5ce3507a0eea771e4c6
- Manjikian, M. (2020). Cyber Politics and Policies. Washington, DC: CQ Press.
- Manjikian, M. (2015). "Confidence-building in Cyberspace: A Comparison of Territorial and Weapons-based Regimes," Strategic Studies Institute, US Army War College, Carlisle, United States.
- Nye, J. (2016). "Deterrence and Dissuasion in Cyberspace," International Security, 41(3): 44–71.
- Riotta, C. (2019, October 9). "Russia Used Social Media to Support Trump in 2016 at Direction at Kremlin, Senate Intelligence Report Says," Independent. www.independent.co.uk/news/world/americas/us-politics/trump-russia-2016-intelligence-report-read-kremlin-facebook-a9148036.html
- Sanger, D. E. (2018). The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age. New York: Crown.
- Segal, A. (2018). "When China Rules the Web: Technology in Service of the State," Foreign Affairs, 97
- (5): 10–18.
- Stoddart, K. (2016). "Live Free or Die Hard: US-UK Cyber Policies," Political Science Quarterly, 131(4): 803–842.
- Tyson, J. (n.d.). "How Internet Infrastructure Works." https://computer.howstuffworks.com/internet/basics/internet-infrastructure4.htm
- United States Department of Defense. (2018). "Summary: Department of Defense Cyber Strategy." https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF
- U.S. Senate, Committee on the Judiciary, Subcommittee on Crime and Terrorism. (2014, July 15). "Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks." www.judiciary.senate.gov/meetings/taking-down-botnets_public-and-private-effortsto-disrupt-and-dismantle-cybercriminal-networks
- Wickett, X., Smith, J., & Smart, C. "America's International Role under Donald Trump." Chatham House Reports. January 18, 2017. https://www.chathamhouse.org/publication/americas-internationalrole-under-donald-trump
- Zeng, J. (2017). "Does Europe Matter? the Role of Europe in Chinese Narratives of 'One Belt, One Road' and 'New Type of Great Power Relations,'" Journal of Common Market Studies, 55(5): 1162–1176.

کانادا

- Alexander, D. C. (2014a). Cyber threats against the North Atlantic Treaty Organization (NATO) and selected responses. İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi (Istanbul Gelisim University Social Sciences Journal), 1(2), 1–36
- Alexander, D. C. (2014b). "Kuzey Atlantik Antlaşması Örgütü'ne (NATO) Karşı Siber Tehditler VeSeçilmiş Yanıtlar," İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi, 1(2): 1–36.

- CCDCOE. (2017). “Back to Square One? the Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly Estonia: NATO Coopeative Cyber Defence Center of Excellence.”
- CGI. (2016). “Will Canada’s Cybersecurity Legislation Impact Your Business? Be Aware of Your Obligations.” www.cgi.com/sites/default/files/white-papers/canada-cybersecurity-legislation-whitepaper.pdf
- CIRA. (2018). “2018 CIRA Canadian Internet Security Survey.”
- CISION. (2017). “Majority of Canadians Support Privacy Act Reform, Greater Transparency by Government, Businesses: Poll.” www.newswire.ca/news-releases/majority-of-canadians-support-privacy-act-reform-greater-transparency-by-government-businesses-poll-611876805.html
- Communications Security Establishment. (2014). “Mission, Vision and Values.” www.cse-cst.gc.ca/en/about-apropos/vision-mission
- Coop, A. (2017). “Cyber Security a Growing Concern for Canadians.” www.itworldcanada.com/article/cyber-security-a-growing-concern-to-canadians/399641
- Farrell, P. (2013). “History of 5-Eyes – Explainer.” www.theguardian.com/world/2013/dec/02/historyof-5-eyes-explainer
- Freedman, B. J. (2017). “Cyber Risk Management – G7 Cybersecurity Guidelines For The FinancialSector.” http://blg.com/en/News-And-Publications/Publication_4694
- Gemalto. (2017). “Data Breach Database.” https://breachlevelindex.com/data-breach-database
- Global Affairs Canada. (2018). “Cybercrime.” www.international.gc.ca/crime/cyber_crime-criminalite.aspx?lang=eng&_ga=2.127330884.892494619.1525240450-492751339.1521087974
- Government of Canada. (2015). “Canada Completes Ratification of Convention on Cybercrime.” www.canada.ca/en/news/archive/2015/07/canada-completes-ratification-convention-cybercrime.html
- Government of Canada. (2017). “Breach of Security Safeguards Regulations.” www.gazette.gc.ca/rp-pr/p1/2017/2017-09-02/html/reg1-eng.html
- Government of Canada. (2018a). “Canada’s Anti-Spam Legislation.” www.fightspam.gc.ca/eic/site/030.nsf/eng/h_00241.html
- Government of Canada. (2018b). “Canada’s Cyber Security Strategy: For a Stronger and MoreProsperous Canada.” http://publications.gc.ca/site/eng/9.693830/publication.html
- Government of Canada. (2018c). “Getcybersafe.” www.getcybersafe.gc.ca/index-en.aspx
- Hanna, J. (2017). “What Is the Five Eyes Intelligence Pact?” www.cnn.com/2017/05/25/world/uk-usfive-eyes-intelligence-explainer/index.html
- Harris, K. (2018). “‘Five Eyes’ Allies Urge Digital Industry to Stop Child Pornographers, Terrorists.”www.cbc.ca/news/politics/digital-security-online-five-eyes-pornography-terrorism-1.4803122
- Innovation Science and Economic Development Canada. (2017). “Version 2.0 – Digital Canada 1502.0.” www.ic.gc.ca/eic/site/028.nsf/vwapj/DC150-2.0-EN.pdf/$FILE/DC150-2.0-EN.pdf
- KERA News. (2012). “A Rare Case: Canadian Navy Officer Pleads Guilty To Selling Secrets To Russians.” http://keranews.org/post/rare-case-canadian-navy-officer-pleads-guilty-selling-secretsrussians
- Merriam-Webster. (2018). “Sovereignty.” www.merriam-webster.com/dictionary/sovereigntyMueller, M. (2017). “Debates on Global Governance and Cybersecurity.” www.internetgovernance.org/2017/04/03/debates-on-global-governance-and-cybersecurity/
- Office of the Privacy Commissioner of Canada. (2016). “Public Opinion Survey.” www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/por_2016_12/#fig1
- Office of the Privacy Commissioner of Canada. (2018a). “Privacy and Cyber Security: EmphasizingprivacyProtection in Cyber Security Activities.” www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/cs_201412/
- Office of the Privacy Commissioner of Canada. (2018b). “Privacy Breaches.” www.priv.gc.ca/en/privacy-topics/privacy-breaches/
- Public Safety Canada. (2010). “Canada’s Cyber Security Strategy: For a Stronger and More Prosperous Canada.” http://publications.gc.ca/collections/collection_2010/sp-ps/PS4-102-2010-eng.pdf

- Public Safety Canada. (2016a). "Canadian Cyber Incident Response Centre (CCIRC)." www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-en.aspx
- Public Safety Canada. (2016b). "Fundamentals of Cyber Security for Canada's Critical Infrastructure Community," Building a Safe and Resilient Canada. www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/2016-fndmntls-cybr-Scrty-cmmnty-en.pdf
- Public Safety Canada. (2018a). "Cyber Incident Management Framework for Canada." www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-ncdnt-frmwrk/index-en.aspx
- Public Safety Canada. (2018b). "National Strategy for Critical Infrastructure." www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx
- PWC. (2018). "The Global State of Information Security® Survey 2018." www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html
- Reuters Staff. (2017). "China, Canada Vow Not to Conduct Cyber Attacks on Private Sector." www.reuters.com/article/us-canada-china-cyber/china-canada-vow-not-to-conduct-cyber-attacks-on-private-sector-idUSKBN19H06A
- RSA Conference. (2017). "Power of Opportunity." www.rsaconference.com/events/us17
- Segal, A. (2017). "The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What?" www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what
- Smith, B. (2017). "The Need for Digital Geneva Convention." https://blogs.microsoft.com/on-theissues/2017/02/14/need-digital-geneva-convention/
- Solomon, H. (2017). "Focus on Security Basics and Be Good at Them, Says Risk Consultant." www.itworldcanada.com/article/focus-on-security-basics-and-be-good-at-them-says-risk-consultant/398876
- The US Department of Justice. (2017). "Canadian Hacker Who Conspired with and Aided Russian FSB Officers Pleads Guilty." www.justice.gov/opa/pr/canadian-hacker-who-conspired-and-aided-russian-fsb-officers-pleads-guilty
- Theiler, O. (2015). "New Threats: The Cyber-dimension." www.nato.int/docu/review/2011/11-september/Cyber-Threads/EN/index.htm
- United Nations. (2015). "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security Seventieth Session, Developments in the Field of Information and Telecommunications in the Context of International Security." New York: UN General Assembly.
- Yeli, H. (2017). A Three-Perspective Theory of Cyber Sovereignty (Vol. 2). China: China International Institute for Strategic Society

اتحادیه اروپا

- Barrinha, A. & Farrand-Carrapico, H. (2018). "How Coherent Is EU Cybersecurity Policy?" LSE European Politics and Policy (EUROPP) Blog. https://blogs.lse.ac.uk/europpblog/2018/01/16/howcoherent-is-eu-cybersecurity-policy/
- Bangemann Group. (1994). "Report on Europe and the Global Information Society," Bulletin of the European Union, Supplement 2/94.
- Bigo, D. (2000). "When Two Become One," in M. Kelstrup & M. C. Williams (eds.), International Relation Theory and the politics of European Integration, Power, Security and Community (pp. 171–205).London: Routledge.
- Biscop, S. & Andersson, J. (2008). The EU and the European Security Strategy: Forging a Global Europe.Abingdon: Routledge.
- Carrapico, H. & Barrinha, A. (2017). "The EU as a Coherent (Cyber) Security Actor?" Journal of Common Market Studies, 55(6): 1254–1272.
- Cremona, M. (2008). "Coherence through Law: What Difference Will the Treaty of Lisbon Make?" Hamburg Review of Social Sciences, 3(1): 11–36.
- Directive 2016/1148 of the European Parliament and the Council Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union (the "NISDirective").

- European Commission. (1993, December 5). "Growth, Competitiveness, and Employment. The Challenges and Ways Forward into the 21st Century," COM (93) 700 final.
- European Commission. (2017a, September 19). "State of the Union 2017 – Cybersecurity: Commission Scales up EU's Response to Cyber-Attacks," Press Release. http://europa.eu/rapid/press-release_IP17-3193_en.htm
- European Commission. (2017b, September 13). "Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU," Joint Communication to the European Parliament and the Council. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:0450:FIN
- European Commission. (2019). "The EU Cybersecurity Act." https://eur-lex.europa.eu/eli/reg/2019/
- 881/oj
- European Parliament and Council of the European Union. (2016, September). "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union," Official Journal of the European Union, L 194/119.
- European Union. (2016, June). "Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union's Foreign and Security Policy." www.eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf
- Healey, J. (ed.). (2013). "A Fierce Domain: Conflict in Cyberspace, 1986 to 2012." Cyber Conflict Studies Association.
- Langner, R. (2011). "Stuxnet: Dissecting a Cyberwarfare Weapon," IEEE Security & Privacy, 9(3):49–51.
- Lindsay, J. R. (2013). "Stuxnet and the Limits of Cyber Warfare," Security Studies, 22(3): 365–404.Markopoulou, D., Papakonstantinou, V. & de Hert, P. (2019). "The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation,"Computer Law & Security Review, 35(6): 105336.
- Martin, B. (2005). "Information Society Revisited: From Vision to Reality," Journal of Information Science,31(1): 4–12.
- Nuttall, S. (2005) "Coherence and Consistency," in C. Hill & M. Smith (eds.), International Relations and the European Union (pp. 91–112). Oxford: Oxford University Press.
- "Permanent Structured Cooperation (PESCO) – Factsheet." https://eeas.europa.eu/headquarters/headquarters-Homepage/34226/permanent-structured-cooperation-pesco-factsheet_en
- Pomorska, K. & Vanhoonacker, S. (2016). "Europe as a Global Actor: Searching for a New Strategic Approach," Journal of Common Market Studies, 53(S1): 216–229.
- Pupillo, L., Griffith, M., Blockmans, S. & Renda, A. (2018). "Strengthening the EU's Cyber Defence Capabilities," CEPS Task Force Report.
- Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency (Text with EEA Relevance), as Amended by Regulation (EC) No. 1007/2008 and Amended by Regulation (EC) No. 580/2011.
- Tickner, A. (1995). "Re-Visioning Security," in K. Booth & S. Smith (eds.), International Relations Today (pp. 175–197). Cambridge: Polity Press.
- Toje, A. (2005). "The 2003 European Union Security Strategy: A Critical Appraisal," European Foreign Affairs Review, 10(1), 117–133.
- Trauner, F. & Carrapico, H. (2012). "The External Dimension of Justice and Home Affairs after the Lisbon Treaty: Analyzing the Dynamics of Expansion and Diversification," Foreign Affairs Review, 17:1–18.
- Van Vooren, B. (2012). EU External Relations Law and the European Neighbourhood Policy. A Paradigm for Coherence. London: Routledge.
- Walden, I. (2005). "Crime and Security in Cyberspace," Cambridge Review of International Affairs, 18(1):51–68.

انگلستان

- Blagden, D. (2018). "The flawed promise of National Security Risk Assessment: Nine lessons from the British approach," Intelligence & National Security, 33(5), 716–736.
- Blitz, J. (2013, September 29). "UK becomes first state to admit to offensive cyber attack capability,"Financial Times. www.ft.com
- Boston Consulting Group. (2015, May 1). "The internet now contributes 10 percent of GDP to the UK economy, surpassing the manufacturing and retail sectors." fromwww.bcg.com/d/press/1may2015-internet-contributes-10-percent-gdp-uk-economy-12111
- Bowcott, O. (2017, August 23). "Dispute along cold war lines led to collapse of UN cyberwarfare talks,"The Guardian. www.theguardian.com
- Cabinet Office. (2011). "The UK cyber security strategy: Protecting and promoting the UK in a digital world." www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cybersecurity-strategy-final.pdf
- Cabinet Office. (2017). "Interim cyber security science and technology strategy: Future-proofing cyber security." www.gov.uk/government/uploads/system/uploads/attachment_data/file/663181/Embargoed_National_Cyber_Science_and_Technology_Strategy_FINALpdf.pdf
- Carr, M. (2016). "Public-private partnerships in national cyber-security strategies," International Affairs,92(1): 43–62.
- Christou, G. (2016). Cybersecurity in the European Union: Resilience and adaptability in governance policy. Basingstoke: Palgrave Macmillan.
- Commonwealth Telecommunications Organisation. (2014, March 3-4). "Commonwealth cybergovernance model." www.cto.int/media/pr-re/Commonwealth per cent20Cybergovernance per cent20Model.pdf
- The Commonwealth. (2018, April 20). "Commonwealth cyber declaration." www.chogm2018.org.uk/sites/default/files/Commonwealth per cent20Cyber per cent20Declaration per cent20pdf.pdf
- Defty, A. (2018). "Coming in from the cold: Bringing the intelligence and security committee into parliament," Intelligence and National Security, 34(1): 22–37.
- Department for Digital, Culture, Media and Sport. (2013, October 28). "UK paper on the roles of governments in internet governance." www.gov.uk/government/uploads/system/uploads/attachment_data/file/330740/UK_PAPER_ON_THE_ROLES_OF_GOVERNMENTS_IN_INTERNET_GOVERNANCE.docx
- Department for Digital, Culture, Media and Sport. (2018). "Secure by design: Improving the cybersecurity of consumer internet of things." www.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf
- Department for International Trade. (2018). "Cyber security export strategy." www.gov.uk//government/publications/cyber-security-export-strategy
- Donaldson, K. (2017, December 18). "UK would respond to a Russian cyberattack with the weapon of its choice," Bloomberg. www.bloomberg.com/news/articles/2017-12-18/u-k-would-respond-to-russian-cyberattack-with-weapon-of-choice
- Foreign and Commonwealth Office. (2017, December 19). "Foreign Office Minister condemns NorthKorean actor for WannaCry attacks." www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks
- Harvey, S. (2013). "Unglamorous awakenings: How the UK developed its approach to cyber," in J. Healey (ed.), A fierce domain: Conflict in cyberspace, 1986-2012 (pp. 251–264). Arlington: Cyber Conflict Studies Association; Washington, DC: Atlantic Council.
- Hayden, M. V. (2016). Playing to the edge: American intelligence in the age of terror. New York: PenguinPress.

- HM Government. (2009a). "Cyber security strategy of the United Kingdom: Safety, security and resilience in cyber space." webarchive.nationalarchives.gov.uk/+/http:/www.cabinetoffice.gov.uk/media/216620/css0906.pdf
- HM Government. (2009b). "Digital Britain: Final report." www.gov.uk/government/uploads/system/uploads/attachment_data/file/228844/7650.pdf
- HM Government. (2015). "National security strategy and strategic defence and security review 2015:A secure and prosperous United Kingdom." www.gov.uk/government/uploads/system/uploads/attachment_data/file/478936/52309_Cm_9161_NSS_SD_Review_PRINT_only.pdf
- HM Government. (2016a). "National Cyber Security Strategy 2016-2021." www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
- HM Government. (2016b). "Cyber security regulation and incentives review." www.gov.uk/government/uploads/system/uploads/attachment_data/file/579442/Cyber_Security_Regulation_and_Incentives_Review.pdf
- HM Government. (2017). "Security, law enforcement and criminal justice: A future partnership paper."www.gov.uk/government/uploads/system/uploads/attachment_data/file/645416/Security__law_enforcement_and_criminal_justice_-_a_future_partnership_paper.PDF
- Lindsay, J. & Gartzke, E. (2017). "Cybersecurity and cross-domain deterrence: The consequences of complexity," in D. van Puyvelde & A. F. Brantly (eds.), US national cybersecurity: International politics, concepts and organization (pp. 11–27). London and New York: Routledge.
- Lonsdale, D. J. (2016). "Britain's emerging cyber-strategy," The RUSI Journal, 161(4): 52–62. Martin, C. (2016, September 13). "A new approach for cyber security in the UK. Speech given at the Billington Cyber Security Summit." www.ncsc.gov.uk/news/new-approach-cyber-security-uk
- Ministry of Defence. (2013). Cyber primer. Shrivenham: Development, Concepts and Doctrine Centre.
- National Audit Office. (2019). "Progress of the 2016–2021 National Cyber Security Programme." www.nao.org.uk/report/progress-of-the-2016-2021-national-cyber-security-programme/
- National Cyber Security Centre. (2018, October 3). "Reckless campaign of cyber attacks by Russian military intelligence service exposed." www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed
- NATO. (2014, September 5). "Wales summit declaration. www.nato.int/cps/en/natohq/of per centEF per centAC per cent81cial_texts_112964.htm
- NATO. (2016, July 8). "Cyber defence pledge." www.nato.int/cps/en/natohq/of per centEF per centAC per cent81cial_texts_133177.htm
- Ormrod, D. & Turnbull, B. (2016). "The cyber conceptual framework for developing military doctrine," Defence Studies, 16(3): 270–298.
- Pepper, D. (2010). "The business of SIGINT: The role of modern management in the transformation of GCHQ," Public Policy & Administration, 25(1): 85–97.
- Schmitt, M. N. (ed.). (2013). Tallinn manual on the international law applicable to cyber warfare. Cambridge: Cambridge University Press.
- Schmitt, M. N. (ed.). (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge: Cambridge University Press
- Stevens, T. & O'Brien, K. (2019). "Brexit and cyber security," The RUSI Journal, 164(3): 22–30.
- Stevens, T., O'Brien, K., Overill, R., Wilkinson, B., Pildegovičs, T. & Hill, S. (2019). "UK active cyberdefence: A public good for the private sector." www.kcl.ac.uk/policy-institute/research-analysis/active-cyber-defence
- Stoddart, K. (2016). "UK cyber security and critical national infrastructure protection. International Affairs," 92(5): 1079–1105.
- Wright, J. (2018, 23 May). "Cyber and international law in the 21st century." www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

- Aale, P. K. (2012, January 16). “Rapport: EØS-avtalen er en demokratisk fiasko for Norge.” Aftenposten. www.aftenposten.no/norge/politikk/i/8m8jQ/Rapport-EOS-avtalen-er-en-demokratisk-fiasko-forNorge
- Collier, J. (2018). “Cyber Security Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision,” Politics and Governance, 6(2): 13–21.
- Datatilsynet. (2017). “Klart nei til digitalt grenseforsvar.” www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/hoeringsuttalelser/20172/klart-nei-til-digitalt-grenseforsvar/
- “Digitalt Grenseforsvar (DGF).” (2016, August 26). www.regjeringen.no/contentassets/ca1f705dbebd48cb9a61889d4cfee6bf/digitalt-grenseforsvar-lysne-ii-utvalget.pdf
- Dunn Cavelty, M. & Suter, M. (2009). “Public–Private Partnerships are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection,” International Journal of Critical Infrastructure Protection, 4(2): 179–187.
- European Commission. (2018). “Digital Economy and Society Index (DESI) 2018.” www.regjeringen.no/contentassets/5d2caddad8424250846b8dc93e259997/desi-indeksen_2018_norge.pdf
- FIRST. (2018). “Nordic Financial CERT.” www.first.org/members/teams/nordic_financial_certFitton, O. (2016). “Cyber Operations and Gray Zones: Challenges for NATO,” Connections: The Quarterly Journal, 15(2): 109–119.
- Healey, J. (ed.). (2013). A Fierce Domain, Conflict in Cyberspace 1986 to 2012. Arlington, VA: Cyber Conflict Studies Association.
- Kello, L. (2017): The Virtual Weapon and International Order. New Haven: Yale University Press.
- Lovdata. (2018). “Lov om nasjonal sikkerhet (Sikkerhetsloven).” https://lovdata.no/dokument/NL/lov/2018-06-01-24
- Løkke, E. (2017). “Trenger Norge et digitalt grenseforsvar?” Minerva. www.minervanett.no/trengernorge-digitalt-grenseforsvar/
- Muller, L. P., Gjesvik, L. & Friis, L. (2018): “Cyber-Weapons in International Politics – Possible sabotage against the Norwegian petroleum sector.” NUPI report. www.nupi.no/en/Publications/CRIStin-Pub/Cyber-weapons-in-International-Politics-Possible-sabotage-against-the-Norwegianpetroleum-sector
- National Security Authority. (2017): “Mnemonic AS tilfredsstiller kravene til NSMs kvalitetsordning for hendelseshåndtering.” https://nsm.stat.no/aktuelt/nsm-mnemonic/
- National Security Authority. (2018a, August 13). “NSM etablerer Nasjonal cybersikkerhetssenter.” https://nsm.stat.no/aktuelt/nsm-etablerer-nasjonalt-cybersikkerhetssenter/
- National Security Authority. (2018b). “About NSM.” https://nsm.stat.no/english/
- Norwegian Government. (2012, September 18). “Cyberforsvaret offisielt etablert i dag.” www.regjeringen.no/no/aktuelt/cyber/id699271/
- Norwegian Government. (2015). 13 “Digital sårbarhet – Sikkert samfunn: Beskytte enkeltmennesker ogsamfunn i en digitalisert verden” (Lysne 1). www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf
- Norwegian Government. (2017). “IKT-sikkerhetsutvalget.” www.regjeringen.no/no/dep/jd/org/styrerad-og-utval/tidsbegrensede-styrer-rad-og-utvalg/IKT-sikkerhetsutvalget/id2570775/
- Norwegian Ministries. (2012). “Cyber Security Strategy for Norway.” www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/cyber_security_strategy_norway.pdf
- Norwegian Ministry of Defense. (2014). “Forsvarsdepartementets retningslinjer for informasjonssikkerhetog cyberoperasjoner i forsvarssektoren.” www.regjeringen.no/globalassets/upload/fd/dokumenter/fdsretningslinjercyberoperasjoner.pdf

- Norwegian Ministry of Foreign Affairs. (2017). "International Cyber Strategy for Norway." www.regjeringen.no/globalassets/departementene/ud/dokumenter/sikpol/cyberstrategy_2017.pdf
- Norwegian Ministry of Foreign Affairs. (2018). "Digital Strategi for utviklingspolitikken." www.regjeringen.no/globalassets/departementene/ud/dokumenter/utvpolitikk/digital_strategi2018.pdf
- NOU. (2015). 13 "Digital sårbarhet – Sikkert samfunn: Beskytte enkeltmennesker og samfunn i endigitalisert verden" (Lysne 1). www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf
- Næringslivets Sikkerhetsråd. (2018). "Mørketallsundersøkelsen 2018." www.nsr-org.no/getfile.php/1311303-1537281687/Bilder/M%C3%B8rketallsunders%C3%B8kelsen/M%C3%B8rketallsunders%C3%B8kelsen%202018%20low.pdf
- Republic of Estonia. (2017, January 11). "Meeting of Nordic and Baltic heads of government focused on challenges of the modern era." www.valitsus.ee/en/news/meeting-nordic-and-baltic-heads-government-focused-challenges-modern-era
- Rid, T. (2011). Cyber War Will Not Take Place. New York: Oxford University Press.
- Riste, O. (2005). Norway's Foreign Relations – A History. Oslo: Universitetsforlaget.
- Schia, N. N. & Gjesvik, L. (2016). "China's Cyber Sovereignty Concept." NUPI Policy Brief. https://brage.bibsys.no/xmlui/bitstream/handle/11250/2434904/NUPI_Policy_Brief_2_17_Schia_Gjesvik.pdf?sequence=4&isAllowed=y
- St. Meld. 10. (2016–2017). "Risiko i et trygt samfunn – Samfunnssikkerhet." www.regjeringen.no/contentassets/00765f92310a433b8a7fc0d49187476f/no/pdfs/stm201620170010000dddpdfs.pdf
- St. Meld. 17. (2001–2002). "Samfunnssikkerhet – Veien til et mindre sårbart samfunn." www.regjeringen.no/contentassets/ee63e1dd1a16409fa0bb737bfda9279a/no/pdfa/stm200120020017000dddpdfa.
- pdf
- St. Meld. 17. (2006–2007). "Et informasjonssamfunn for alle." www.regjeringen.no/no/dokumenter/stmeld-nr-17-2006-2007-/id441497/
- St. Meld. 22. (2007–2008). "Samfunnssikkerhet – Samvirke og samordning." www.regjeringen.no/no/dokumenter/stmeld-nr-22-2007-2008-/id510655/
- St. Meld. 29. (2011–2012). "Samfunnssikkerhet." www.regjeringen.no/contentassets/bc5cbb3720b14709a6bda1a175dc0f12/no/pdfs/stm201120120029000dddpdfs.pdf
- St. Meld. 37. (2014–15). "Globale sikkerhetsutfordringer i utenrikspolitikken." www.regjeringen.no/contentassets/bdf4bd40d57d4dc79409de87419a2217/no/pdfs/stm201420150037000dddpdfs.pdf Englishversion: www.regjeringen.no/en/dokumenter/meld.-st.-37-20142015/id2423339/
- St. Meld. 38. (2016–2017). "IKT-sikkerhet – Et felles ansvar." www.regjeringen.no/contentassets/39c6a2fe89974d0dae95cd5af0808052/no/pdfs/stm201620170038000dddpdfs.pdf
- St. Meld. 39. (2003–2004). "Samfunnssikkerhet og sivilt-militært samarbeid." www.regjeringen.no/no/dokumenter/stmeld-nr-39-2003-2004-/id198241/sec8?q=digital#match_0
- St. Meld. 47. (2000–2001). "Telesikkerhet og -beredskap i et telemarked med fri konkurranse." www.regjeringen.no/contentassets/c3b2c417894448b080313b190a540f28/no/pdfa/stm200020010047000dddpdfa.pdf
- Tamnes, R. & Eriksen, K. E. (1999). "Norge og NATO under den kalde krigen." www.atlanterhavskomiteen.no/files/atlanterhavskomiteen.no/Tema/50aar/1a.htm