مرکز ملی فضای مجازی
انتشارات پژوهشگاه فضای مجازی

امنیت سایبری در اتحادیه اروپا

تاب‌آوری و انطباق‌پذیری در سیاست حکمرانی

نویسنده: جورج کریستو

مترجمان: محمدرضا سعیدآبادی
محمود جوادی

امنیت سایبری در اتحادیه اروپا

تاب‌آوری و انطباق‌پذیری در سیاست حکمرانی

نویسنده

جورج کریستو

مترجمان

محمدرضا سعیدآبادی (عضو هیئت علمی دانشگاه تهران)

محمود جوادی

بهار ۱۴۰۰

سرشناسه	:	کریستو، جورج، ۱۹۷۳- م،
		-Christou, George, 1973
عنوان و نام پدیدآور	:	امنیت سایبری در اتحادیه اروپا: تاب‌آوری و انطباق‌پذیری در سیاست حکمرانی/ نویسنده: جورج کریستو؛ مترجمان: محمدرضا سعیدآبادی، محمود جوادی
مشخصات نشر	:	تهران : انتشارات پژوهشگاه فضای مجازی، ۱۴۰۰
مشخصات ظاهری	:	۳۲۲ صفحه
شابک	:	۹۷۸-۶۲۲-۹۷۷۰۰-۸-۵
وضعیت فهرست‌نویسی	:	فیپا
یاداشت	:	عنوان اصلی : Cyber security in the European Union : resilience and adaptability in governance policy , 3015
موضوع	:	جرایم کامپیوتری -- کشور های عضو اتحادیه اروپا -- پیشگیری
موضوع	:	Computer crimes -- European Union countries -- Prevention
موضوع	:	تروریسم رایانه ای -- کشورهای عضو اتحادیه اروپا -- پیشگیری
موضوع	:	Cyberterrorism -- European Union countries -- Prevention
موضوع	:	جنگ سایبری -- کشور های عضو اتحادیه اروپا
موضوع	:	Cyberspace operations (Military science) -- European Union countries
موضوع	:	فضای مجازی -- تدابیر ایمنی
موضوع	:	Cyberspace -- Security measures
موضوع	:	امنیت ملی -- کشورهای عضو اتحادیه اروپا
موضوع	:	Cyberspace -- Security measures
شناسه افزوده	:	سعیدآبادی، محمدرضا، ۱۳۴۵ - ، مترجم
شناسه افزوده	:	جوادی، محمود، ۱۳۶۸ -، مترجم
شناسه افزوده	:	javadi, mahmoud
شناسه افزوده	:	پژوهشگاه فضای مجازی
رده‌بندی کنگره	:	HV۶۷۷۳/۳
رده‌بندی دیویی	:	۳۶۴/۴
شماره کتابشناسی ملی	:	۷۶۶۷۶۹۶
اطلاعات رکورد کتابشناسی	:	فیپا

مشخصات :

عنوان: امنیت سایبری در اتحادیه اروپا: تاب‌آوری و انطباق‌پذیری در سیاست حکمرانی

نویسنده: جورج کریستو

مترجمان: محمدرضا سعیدآبادی، محمود جوادی

ناشر: انتشارات پژوهشگاه فضای مجازی

صفحه‌آرا و طراح جلد: میترا مرادیان

سال و نوبت چاپ: ۱۴۰۰- اول

شمارگان: ۱۰۰۰ نسخه

شابک: ۹۷۸-۶۲۲-۹۷۷۰۰-۸-۵

قیمت: ۱۲۰۰۰۰۰ ریال

فهرست مطالب

فصل ۶: امنیت شبکه و اطلاعات و دفاع سایبری در اتحادیه اروپا

فصل ۷: همکاری فراآتلانتیک در امنیت سایبری؛ همگرایی در امنیت تاب‌آور؟

فصل ۸: جمع‌بندی: به‌سوی امنیت تاب‌آور کارآمد در اتحادیه اروپا؟

مقدمه مترجمان

در سطح نظام جهانی، دورانی که هم‌اکنون در آن به سر می‌بریم، دوران انتقالی و گذار نام گرفته است و دولت-ملت‌های مختلف ازجمله قدرت‌های منطقه‌ای و جهانی در تلاش برای تبدیل اراده، خواست و نگرانی عامه خود به اراده، خواست و نگرانی‌های عامه در این دوران گذار هستند، چراکه تحقق این امر به معنای تعیین نظم آتی جهانی و تثبیت رهبری بر نظام جهانی پساگذار می‌باشد.

ازجمله مؤلفه‌های لازم برای رهبری بر نظم کنونی و آتی جهانی، سیطره و مدیریت بر «مشترکات جهانی» است. در طول سالیان پس از جنگ سرد و دوران نظام تک قدرت محور، «نظم قانون محور بین‌المللی» یا به تعبیر ساده‌تر، «نظم غرب محور»، نظم تثبیت‌شده نظام جهانی به شمار می‌آید، ولیکن آنچه این نظم غرب محور و حافظان این نظم را به چالش می‌کشاند، ناتوانی آن‌ها در تسلط کامل و بی‌قیدوشرط بر مشترکات جهانی است. به سخن دیگر، ماهیت مشترکات جهانی می‌تواند چالش بالقوه‌ای باشد که عدم تثبیت برتری غرب در آن به‌منزله تهدیدی برای منافع بلندمدت و نظم مطلوب آتی آن به‌حساب آید.

بر اساس تعاریف موجود بخصوص در ادبیات غربی، مفهوم «مشترکات جهانی» این‌گونه تعریف شده است که «حوزه‌ها و قلمروهایی که خارج از اختیارات دولت‌های ملی است، درعین‌حال تمامی دولت‌ها بر این حوزه‌ها و قلمروها متکی بوده و کل نظام بین‌الملل را در همه

عرصه‌های اقتصادی، .تجاری، نظامی و امثال آن به هم پیوند می‌زند.» بر این اساس، «دریا»، «هوا»، «فضا» و «سایبر»، چهار قلمرویی است که مفهوم مشترکات جهانی را شکل داده و حافظان نظم غربی نیازمند تثبیت برتری خود در این قلمروها هستند تا بتوانند کماکان رهبری بر نظم و نظام جهانی را در دست داشته باشند

توجه غرب به حوزه‌های دریا، هوا و فضا دارای سابقه طولانی است، به‌طوری‌که غرب و نظم غربی توانسته بر این سه حوزه مسلط شود، اما «فضای سایبر» تنها قلمرویی است که جهان غرب و نظم غربی در مدیریت و کنترل آن ناتوان بوده است. این ناتوانی و نقص ناشی از گستردگی عرصه فضای سایبر و بازیگران بهره‌مند از آن و نیز متعاقباً بی‌نظمی درونی فضای سایبر است.

قدرت‌های غربی و موافقان نظم غرب محور در اسناد کلان خود به این موضوع اشاره دارند که به دلیل در دسترس عام بودن و وابستگی شدید زیرساخت‌های خود به فضای سایبر، کنشگران دولتی و غیردولتی تهدیدات بالقوه‌ای نه‌تنها برای منافع راهبردی آن‌ها بلکه برای نظم کنونی غرب محور به شمار می‌آیند.

بر اساس چنین تهدیداتی است که حافظان نظم غرب محور ازجمله کشورهای اروپایی و اتحادیه اروپا هم به‌منظور حفاظت خود در برابر این تهدیدات و هم از منظری کلان‌تر، با هدف تسلط بر قلمرو سایبر به‌عنوان آخرین محور مشترکات جهانی، مبادرت به تدوین و اجرای راهبردها، سیاست‌ها، برنامه‌ها و راهکارهایی می‌ورزند.

علاوه بر آنچه اشاره شد، تردیدی نیست که گسترش فزاینده فناوری‌های ارتباطی و اطلاعاتی در سطح کشورهای اروپایی و همچنین پیگیری جدی اتحادیه اروپا در افزایش رشد و توسعه اقتصادی از بستر فضای دیجیتال و سایبر، امنیت اتحادیه را هم‌ردیف با امنیت سایبری آن کرده است؛ بدین معنی که هر عامل تهدیدزا برای امنیت سایبری اتحادیه اروپا و اعضای آن به‌مثابه تهدیدی برای امنیت سرزمینی و وجودی آن‌ها به شمار می‌آید. از همین روست که اتحادیه اروپا در دهه دوم سده جدید تلاش مضاعفی برای تدوین و اجرای سیاست‌ها و راهبردها در خصوص امنیت سایبری اتحادیه داشته است. به‌رغم اهمیت موضوع امنیت و بخصوص امنیت سایبری اتحادیه اروپا، این مقوله چندان از سوی جوامع علمی غربی و ایرانی موردتوجه قرار نگرفته است

که لذا تألیف و ترجمه این اثر با هدف تکمیل این خلأ در هر دو جامعه مذکور انجام گرفته است.

کتاب حاضر در هشت فصل، سه ستون اصلی راهبرد امنیت سایبری اتحادیه اروپا (۲۰۱۳)، یعنی جرائم سایبری، امنیت شبکه و اطلاعات و دفاع سایبری، را مورد واکاوی قرار می‌دهد. بااین‌حال، جورج کریستو، نویسنده کتاب در فصل ابتدایی به‌تفصیل، موضوع اکوسیستم امنیت سایبری جهانی را بررسی و چارچوب مفهوم جدیدی تحت عنوان «امنیت تاب آور» ارائه می‌کند که به‌نوعی، مفهومی در برابر رویکرد سنتی «امنیت کنترلی» است. بر اساس آنچه نویسنده کتاب اشاره داشته است، شش شرط ضروری برای تحقق امنیت تاب آور کارآمد در فضای سایبری وجود دارد:

۱) قابلیت انطباق در ساختار جدید و مفروضات عملیاتی

۲) پذیرش پیچیدگی منطق حکمرانی

۳) توسعه شراکت‌های مبتنی بر اعتماد در میان کنشگران اصلی فضای سایبری

۴) پذیرش جمعی ادراکات مشترک در خصوص مفاهیم کلیدی

۵) تصدیق فرهنگ امنیت سایبری در میان تمامی ذینفعان

۶) وجود انسجام و هماهنگی درونی در میان سطوح و کنشگران.

همان‌طور که اشاره شد، این کتاب ابتدا به سه محور جرائم سایبری، امنیت شبکه و اطلاعات و دفاع سایبری، مصرح در سند امنیت سایبری اتحادیه اروپا پرداخته و سپس، رویکرد امنیت سایبری بریتانیا به‌عنوان نمونه مطالعاتی و البته کشوری پیشرفته و مترقی در عرصه فضای سایبر مورد واکاوی قرار گرفته است. کریستو در فصل پایانی و پیش از جمع‌بندی مباحث به موضوع روابط فراآتلانتیکی در عرصه فضا و امنیت سایبری پرداخته و میزان پیشرفت‌ها و همچنین آسیب‌پذیری‌های این روابط ناشی از افشاگری‌های ادوارد اسنودن را تبیین کرده است.

یکی از محاسن و نقاط قوت این کتاب، توجه و تحلیل نویسنده به روندها و رویه‌ها بوده و کمتر اسیر ساختارها و بروکراسی‌ها شده است و به همین دلیل است که برای مثال، خروج یا عدم خروج بریتانیا از اتحادیه اروپا تأثیری بر تحلیل نویسنده در این کتاب نخواهد گذاشت. این بدین معنی است که جورج کریستو تلاش کرده تا از سطوح ابتدایی امنیت سایبری در اتحادیه

اروپا فراتر رفته و عمق و کُنه این موضوع را واکاوی نماید. ناگفته نماند مفهومی که نویسنده کتاب درصدد تبیین آن است (یعنی امنیت سایبری تاب‌آوری کارآمد)، الگویی بوده که ظرفیت بومی‌سازی آن در سطح نظام فناوری ارتباطات و اطلاعات جمهوری اسلامی ایران و همچنین توسعه آن در محیط پیرامونی ایران است. این الگو که بر اساس نوع سوم تاب‌آوری در عرصه امنیت سایبری تدوین و تحلیل شده است، مبتنی بر مؤلفه‌هایی نظیر انعطاف‌پذیری، انطباق‌پذیری و استانداردها، ارزش‌ها و هنجارهای مشترک است و همین مقوله عاملی در تائید این مدعا است که ایده اصلی کتاب که اگرچه نویسنده معتقد است به‌طور کامل در سطح اتحادیه اروپا اجرایی نشده است می‌تواند به‌مثابه عنصری کلیدی در راستای ایجاد و تقویت همگرایی منطقه‌ای در عرصه فضا و امنیت سایبری به شمار آید.

سخن پایانی و مرسوم آنکه، برگردان فصول این کتاب بسیار کاربردی مانند هر اثر پژوهشی کامل و عاری از نقص نیست و راهنمایی خوانندگان محترم در رفع نقایص و ایرادات موجب امتنان مترجمین می‌باشد. همچنین، از پژوهشگاه فضای مجازی وابسته به مرکز ملی فضای مجازی، به ویژه آقای دکتر عبدالحسین کلانتری، رئیس محترم پژوهشگاه، صمیمانه قدردانی می‌نماییم که با دقت و دلسوزی و در یک فضای حرفه‌ای این اثر را به بهترین شکل به زیور طبع آراسته و به محضر شما خواننده محترم تقدیم نموده است.

محمدرضا سعیدآبادی
محمود جوادی
اسفند ۱۳۹۹

دیباچه

امروز دنیای خصوصی و کسب‌وکار ناگزیر به فناوری‌های اطلاعاتی و ارتباطی نوین وابسته شده است. شبکه‌های اجتماعی، بازیابی اطلاعات، خرید، زنجیره‌های تأمین و درواقع، همه فعالیت‌ها در بستر اینترنت انجام می‌شود. فضای جهانی سایبر در حال تبدیل‌شدن به یک دهکده مجازی، کوچک و بدون مرز است. الگوهای جدید کسب‌وکار، علی‌رغم نقشی که در اشتغال‌زایی و رشد اقتصادی ایفا می‌کنند، اغلب مخاطرات جدیدی را نیز به همراه دارند. جرائم، جاسوسی، خرابکاری و جنگ سایبری ازجمله این مخاطرات است. همین مسئله پرداختن به تهدیدهای سایبری، آگاهی‌بخشی درباره امنیت فناوری های اطلاعاتی و ارتباطی و ارائه راهکارهای امنیتی را ضروری کرده است. علاوه بر این، امروز، نیازمند ساختار حکمرانی جدیدی در فضای سایبری هستیم. شرایط قومیتی و فرهنگی مختلف حاکم بر آمریکا، اروپا و آسیا دستیابی به مرام‌نامه‌ای مشترک برای فعالیت در جهان سایبریِ کاملاً جدید را دشوار کرده است.

اتحادیه اروپا که از ۲۸ کشور عضو تشکیل شده است، نمونه موفق دهه‌های اخیر در حوزه هماهنگ‌سازی بازار و رشد اقتصادی است. البته بحران مالی سال ۲۰۰۹ میلادی، بیکاری جوانان و سایر مسائل اجتماعی مشابه ازجمله چالش‌هایی هستند که همچنان پیش روی اروپا قرار دارد. در همین راستا، راهکار بازار واحد دیجیتال کمیسیون اروپا که سال ۲۰۱۶

منتشر شد، نشان‌دهنده تعهد جدی اروپا به تبدیل‌شدن به رهبری جهانی و رقابت‌پذیر بودن در حوزه فناوری‌های اطلاعاتی و ارتباطی است. امروز امنیت و در دسترس بودن فناوری‌های اطلاعاتی و ارتباطی اهمیتی فزاینده یافته و حریم خصوصی در حال تبدیل‌شدن به مسئله‌ای مهم در جهانی است که در آن فراموش کردن هر آنچه در اینترنت قرار بگیرد غیرممکن است. امروز شاهد رشد فزاینده موارد نفوذ امنیتی و داده‌ای هستیم و جرائم سایبری خود به «کسب‌وکاری» جدید تبدیل شده‌اند.

کمیسیون اروپا طرح‌های ابتکاری متعددی را برای بهبود شرایط اجرا کرده است. دستورکار امنیت شبکه و اطلاعات در سال ۲۰۰۱، نخستین امریه حریم خصوصی در اینترنت در سال ۲۰۰۲، تأسیس آژانس امنیت شبکه و اطلاعات اتحادیه اروپا در سال ۲۰۰۴، ابلاغیه زیرساخت‌های اطلاعاتی حیاتی در سال ۲۰۰۹، دستورکار دیجیتال اروپا در سال ۲۰۱۰ و راهبرد امنیت سایبری اتحادیه اروپا در سال ۲۰۱۳ ازجمله این طرح‌های ابتکاری هستند. اما این اقدامات چه تأثیری داشتند؟ امروز رهبران سیاسی، مدیران عامل بخش صنعت و تیم‌های واکنش اضطراری رایانه‌ای از آگاهی کافی در این زمینه برخوردار هستند. اکثر کشورهای عضو اتحادیه اروپا راهبردهایی ملی را در زمینه امنیت سایبری تدوین کرده‌اند. با وجود این، اتحادیه اروپا هنوز فاقد چارچوب حکمرانی کلی در زمینه امنیت شبکه و اطلاعات و سامانه کلی گزارش‌دهی حوادث (مانند آنچه در حوزه مخابرات شاهد آن هستیم) و اطلاع‌رسانی امن درباره تهدیدها و حملات است. امریه امنیت شبکه و اطلاعات که موضوع مذاکرات فعلی پارلمان اروپا و شورای اتحادیه اروپا است، درصدد رفع این مشکلات است. اما در این زمینه همچنان با مانعی اساسی روبرو هستیم. به‌عبارت‌دیگر، امنیت سایبری اغلب بخشی از امنیت ملی تلقی می‌شود و همین دیدگاه باعث شده است موضوع امنیت سایبری زیرمجموعه حاکمیت ملی قرار گیرد. بنابراین، هنوز تا دستیابی به فضای سایبری امن و آزاد در اروپا راهی طولانی در پیش داریم.

این کتاب با عنوان «امنیت سایبری در اتحادیه اروپا: تاب آوری و انطباق پذیری در سیاست حکمرانی» به قلم جرج کریستو کاملاً به‌موقع انتشار یافته است. در این کتاب، در همین راستا،

نویسنده با چالش توصیف و تحلیل وضعیت فعلی امنیت سایبری در اتحادیه اروپا روبرو شده است و ما را با درکی عمیق‌تر از نحوه دستیابی به تاب آوری کارآمد امنیتی آشنا می‌کند. کریستو به توصیف اکوسیستم اتحادیه اروپا در زمینه حکمرانی امنیت سایبری می‌پردازد و مشخص می‌کند که این سازمان تا چه اندازه در دستیابی به رویکرد جامع امنیت سایبری در اکوسیستم خود موفق بوده است. علاوه بر این، نویسنده فهرستی مختصر از شرایط لازم برای دستیابی به امنیت و تاب آوری کارآمد ارائه می‌دهد. کریستو ثابت می‌کند امنیت سایبری پایه و اساس مزایای اجتماعی و فرهنگی اروپا و رشد اقتصادی کشورهای این قاره است. او نشان می‌دهد که امنیت فناوری اطلاعاتی و ارتباطی نقشی حیاتی در دستیابی به این مزایا و رشد اقتصادی دارد.

امروز، اکثر سیاست‌مداران همچنان به‌صورت سیلویی فکر و عمل می‌کنند. به‌عبارت‌دیگر، ازنظر این سیاست‌مداران جنگ سایبری به حوزه دفاع، جرائم سایبری به حوزه اجرای قانون، حریم خصوصی به حوزه قضایی و ... اختصاص دارد. فناوری و مهاجمان هیچ تفاوتی بین این حوزه‌ها قائل نیستند. حمله استاکس‌نت در زمره جرائم سایبری قرار دارد، نوعی خراب‌کاری سایبری است و یا جنگ سایبری محسوب می‌شود؟ پاسخ این سؤالات، با توجه به تفاسیر سیاسی مختلف، متفاوت خواهد بود. فناوری استاکس‌نت که اکنون علنی شده است، می‌تواند بار دیگر برای حمله به کارخانه‌های خودروسازی، حمله منع سرویس به زیرساخت‌های حیاتی یا باج‌گیری سایبری مورد استفاده قرار گیرد. بنابراین، تمامی بازیگران و ذی‌نفعان باید با یکدیگر همکاری نمایند. در این میان، فرایندهایی مانند گزارش‌دهی حوادث و به اشتراک‌گذاری اطلاعات، کلید این همکاری به شمار می‌روند.

دستاورد کریستو ارائه تصویری از فضای سایبری جهان و تحلیل رابطه اتحادیه اروپا و ایالات‌متحده آمریکا و منافع ملی (ازجمله منافع ملی بریتانیا) است که هر دو حوزه جرائم سایبری و جنگ سایبری از سوی نویسنده مورد بررسی قرار گرفته است و وی بحث را با یک سؤال به پایان می‌رساند: آیا «امنیت تاب‌آور» راهکار نهایی است؟

پیام این کتاب که کاملاً با آن هم‌نظر هستم، از این قرار است: «اتحادیه اروپا چاره‌ای جز

تقویت اعتماد و امنیت در فضای سایبری ندارد. تقویت اعتماد و امنیت در فضای سایبری لازمه و پیش‌شرط تحقق آرمان‌ها، تقویت ارزش‌ها و بازتعریف هویت این سازمان در نظم پویای جهانی بوده که بطور فزاینده‌ای به کنش‌پذیری متقابل و ارتباطات دیجیتالی وابسته است.»

از خواندن این کتاب لذت ببرید!

پرفسور اودو هلمبرشت

رئیس آژانس امنیت شبکه و اطلاعات اتحادیه اروپا

مقدمه مؤلف

اهمیت فضای سایبری در زندگی روزمره دولت‌ها، کسب‌وکارها و شهروندان باعث شده است حفظ امنیت این فضا به یکی از ضروری‌ترین چالش‌های امنیتی قرن بیست‌ویک تبدیل شود. جهان سایبری و فناوری‌های مرتبط با آن، از یک‌سو، فرصت‌های اجتماعی، فرهنگی، اقتصادی و سیاسی مختلفی را برای همگان ایجاد کرده است و از سوی دیگر، به دلیل ماهیت بی‌مرز آنها، تهدیدهایی را با خود به همراه داشته‌اند که در قالب حملات سایبری و جرائم سایبری بروز یافته‌اند. اتحادیه اروپا نیز در مقابل این تهدیدها مصون نیست. حملات منع سرویس توزیع‌شده به شبکه‌ها و سامانه‌های دولتی و خصوصی استونی در سال ۲۰۰۷ میلادی و حملاتی که در سال ۲۰۱۱ میلادی نهادهای اتحادیه اروپا را هدف گرفته بودند ازجمله معروف‌ترین پرونده‌ها در این حوزه هستند. این حملات زنگ هشداری برای اتحادیه اروپا بود و باعث شد مسئله امنیت سایبری به‌سرعت وارد دستورکار سیاسی این سازمان شود. در ادامه، اتحادیه اروپا نخستین راهبرد امنیت سایبری خود را در سال ۲۰۱۳ تدوین کرد. هدف این راهبرد اولویت‌بندی و ادغام سیاست‌ها و اقدامات داخلی این نهاد در دو قلمروی داخلی و خارجی بود. این سازمان به‌خوبی دریافته بود ماهیت جهانی و آزاد اینترنت باعث شده دیگر نتواند به‌تنهایی از عهده مقابله با چالش‌های امنیت سایبری برآید.

کتاب پیش رو شرایط بین‌المللی، منطقه‌ای و ملی گسترده‌تر را نیز مدنظر قرار می‌دهد و بر

همین اساس، به بررسی چالش‌های پیش روی اتحادیه اروپا در حوزه امنیت سایبری در دو دوره قبل و بعد از انتشار راهبرد امنیت سایبری این اتحادیه می‌پردازد. این کتاب، با استفاده از مفاهیم تاب آوری و حکمرانی امنیتی و ادغام آن‌ها، چارچوبی جدید برای فهم و ارزیابی میزان پیشرفت اتحادیه اروپا در فراهم آوردن شرایط لازم برای ظهور اکوسیستم سایبری تاب آور و امن در اروپا و فراتر از آن ارائه می‌کند. بر اساس استدلال‌های مطرح‌شده، فراهم آوردن این شرایط دستیابی به تاب‌آوری، انطباق‌پذیری و هماهنگی را ممکن می‌کند که لازمه تقویت امنیت فضای سایبری و اطمینان و اعتماد به آن است. اتحادیه اروپا و شهروندان آن چاره‌ای جز این کار ندارند. درواقع تقویت اعتماد و امنیت در فضای سایبری لازمه و پیش‌شرط تحقق آرمان‌ها، تقویت ارزش‌ها و (باز)تعریف هویت اتحادیه در نظم پویای جهانی بوده که بطور فزاینده‌ای به کنش‌پذیری متقابل و ارتباطات دیجیتالی وابسته است.

قدردانی

از همکارانم در دپارتمان علوم سیاسی و مطالعات بین‌الملل دانشگاه واریک که طی فرایند تحقیق و نگارش این کتاب، همواره با انرژی مثبت خود مشوقم بودند، سپاسگزارم و به طور ویژه، از استوارت کرافت، کریس هیوز، مت واتسون، شاون برسلین، ریچارد آلدریخ، مایک اسمیت، نیک وان-ویلیامز، کریس موران، اوز حسن و کریس براونینگ، برای کمک‌هایشان و گفتگو درباره ایده‌های مطرح‌شده در این کتاب سپاسگزارم. همچنین، از همه اشخاص مذکور برای آنکه وقت خود و امکانات لازم را در اختیارم قرار دادند تشکر می‌کنم. در شرایطی که روند نگارش کتاب با سرعت کامل پیش نمی‌رفت، گفتگو با آن‌ها کمک شایانی به پیشبرد کارم داشت. از همکارانم در تیم سایبری مؤسسه دبلیو.ام.جی دانشگاه واریک و به‌صورت خاص، تیم واتسون و کارستن میپل، برای گفتگوهای بسیار مفیدی که در زمینه جوانب مختلف تحقیق داشتیم و هدایتم در جهت درست سپاسگزارم. راهنمایی‌های آن‌ها باعث شد با اشخاصی در دولت و صنعت آشنا شوم که کمکم کردند طی روند تکامل کتاب، شکاف‌های اطلاعاتی موجود را برطرف کنم. همچنین، از الینور دیوی کوریکان و هانا کاسپار، مشاوران و هماهنگ‌کنندگان سفارش‌های انتشارات پالگریو، برای راهنمایی‌ها، توصیه‌ها و مهم‌تر از همه، صبر و حوصله‌ای که برای تحویل نسخه نهایی کتاب داشتند، سپاسگزارم.

بخش بزرگی از تحقیقات انجام‌شده برای نگارش این کتاب بدون کمک‌های مالی پروژه بزرگ

چارچوب هفتم کمیسیون اروپا با عنوان «تغییر نظم جهانی: تکامل شبکه‌های اروپا» ممکن نمی‌شد. از این کمک‌ها بسیار ممنونم. از متخصصان و مقامات متعددی که طی فرایند نگارش کتاب، دعوتم برای گفتگو درباره تحقیقاتم را پذیرفتند قدردانی می‌کنم. این گفتگوها به من کمک کرد به درک روشن‌تری از ابعاد مختلف راهبرد، سیاست‌ها و شیوه‌های در حال تحول اتحادیه اروپا در حوزه امنیت سایبری دست پیدا کنم. از کیریاکوس رولاس، از بخش سرویس اقدام خارجی اتحادیه اروپا، برای حمایت‌های همیشگی وی طی روند نگارش این کتاب سپاسگزارم. از اودو هملبرشت و کارکنان تحت مدیریت وی در آژانس امنیت شبکه و اطلاعات اتحادیه اروپا و الساندرا فالچینلی از اداره کل شبکه‌های ارتباطات، محتوا و فناوری کمیسیون اروپا تشکر می‌کنم. از علاقه تمامی این افراد به تسهیل تحقیقاتم در برهه‌های زمانی حساس کمال تشکر را دارم. تعاملاتم با ذی‌نفعان و متخصصان دولتی و خصوصی، در مقام مشارکت‌کنندگان فعال در بستر امنیت شبکه و اطلاعات اتحادیه اروپا، کمک شایانی به تلاش‌هایم برای نگارش این کتاب کرد. این تعاملات نه‌تنها باعث تقویت درک و فهم من از موضوع شد بلکه در جریان تحقیقات به تأیید برخی از ادعاها و دقیق‌تر شدن برخی دیگر نیز کمک شایانی کرد.

همچنین، طی فرایند نگارش این کتاب، در کنفرانس‌های انجمن دانشگاهی مطالعات اروپای معاصر و انجمن مطالعات بین‌الملل، به ارائه سخنرانی‌هایی درباره عناصر مختلف تشکیل‌دهنده کتابم پرداختم و کارگاه‌های آموزشی متعددی را نیز در زمینه امنیت سایبری و مسائل مرتبط با آن در بریتانیا و بروکسل برگزار کردم. طی همه این فعالیت‌ها، بازخوردهای مثبتی دریافت کردم که واقعاً برایم مفید بودند. در پایان و مهم‌تر از همه، از خانواده‌ام برای حمایت همیشگی‌شان سپاسگزارم. از آلیسون، کنستانتینو و آندریاس برای عشقشان، درکشان و حمایت‌هایشان طی مراحل مختلف این پروژه به‌صورت ویژه تشکر می‌کنم.

فصل اول

مقدمه

وجه متمایز امنیت سایبری در اتحادیه اروپا

از دو دهه پیش، فناوری‌های اطلاعات و ارتباطات و به‌طور ویژه اینترنت به ابعاد بسیار مهم زندگی اجتماعی، سیاسی و اقتصادی جهان تبدیل شده است و امروزه ستون اصلی جامعه اطلاعات جهانی را تشکیل می‌دهد. تکامل و توسعه این فناوری‌ها فواید بسیاری را در کنار ازدیاد نهادهای خصوصی و دولتی و فعالان این عرصه برای افراد جامعه در بر داشته است؛ این فناوری‌ها شاهد تأثیرات مثبت شبکه‌های اجتماعی بر قیام بهار عربی در سال ۲۰۱۱ و یا استفاده فزاینده از تجارت الکترونیک از سوی کسب‌وکارها و افراد بوده است. بااین‌حال، فناوری‌های اطلاعات و ارتباطات تهدیدات جدی سایبری را به همراه داشته که در سال‌های اخیر از طریق جاسوسی سایبری و جرائم سایبری در اکوسیستم مجازی و شبکه‌ای که در آن زندگی می‌کنیم، نمود یافته است.

برای بیان تعداد اندکی از چنین حملات مهمی، بدون یادآوری حمله به تعدادی از نهادهای اتحادیه اروپا (کمیسیون اروپا و پارلمان اروپا) در سال ۲۰۱۱ می‌توان به تهاجم‌ها به نهادهای خصوصی و دولتی کشور استونی در سال ۲۰۰۷، حملات به سیستم‌های کشور گرجستان از خاک روسیه در سال ۲۰۰۸، حمله کرم استاکس‌نت به برنامه هسته‌ای ایران در سال ۲۰۰۹، تغییر مسیر ترافیک حساس رایانامه‌های دولت آمریکا توسط رساننده خدمات اینترنتی (آی‌اس‌پی[1])

1. Internet Server Provider (ISP)

چینی به سمت این کشور و اقدامات ویکی لیکس در سال ۲۰۱۰ اشاره داشت. جدای از وقوع چنین حملات مهمی، حمله به شرکت‌ها نیز در چند سال اخیر افزایش یافته است (Net Losses Report 2014). چنین رویدادها و حوادثی، آسیب‌پذیری فناوری‌های اطلاعات و ارتباطات را آشکار کرده و در کانون توجه موضوعات سیاستی قرار داده که دامنه نفوذ آن تا دستورکار امنیت اطلاعات نیز پیش رفته است. نظر به آنکه حکمرانی امنیتی طراحی شده به‌منظور مقابله با تهدیدات سایبری باید با بسیاری از سطوح، فعالان، نهادها و افراد درون اکوسیستم سایبری در تعامل باشد، این حملات سایبری، ماهیت جهانی و چندبعدی معضل تضمین اطلاعات را نیز دوچندان ساخته است.

در چنین بستری، اتحادیه اروپا طی ۱۰ سال اخیر اقدام به تدوین سیاست‌های خود در خصوص تهدیدات سایبری کرده است، اگرچه این تلاش‌ها غالباً منفک از یکدیگر بوده‌اند. در سال های اخیر راهبرد امنیت داخلی اتحادیه اروپا[1] (ISS, November 2010) و دستورکار دیجیتال اروپا[2] (۲۰۱۰) راهنمای جامعی برای فعالیت‌های اروپا در این حوزه فراهم کرده است. باوجوداین، اتحادیه اروپا پیشنهادهای دقیق تری در بستر راهبرد اروپایی امنیت اینترنت[3] (ESIS 2011) و راهبرد امنیت سایبری اتحادیه اروپا[4] (EUCSS 2013) ارائه کرده است.

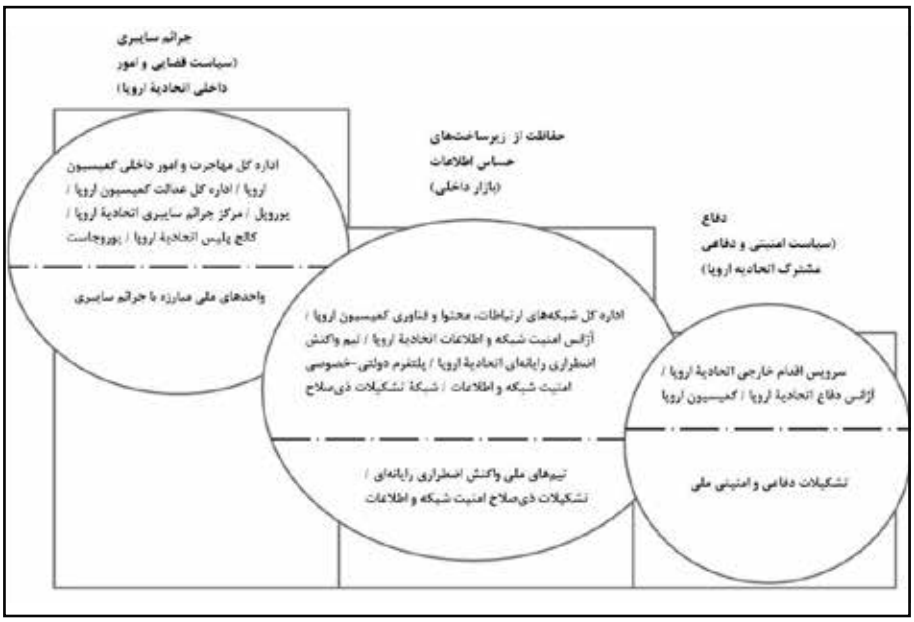
از دیدگاه نهادی، سرویس اقدام خارجی اتحادیه اروپا[5] نقش مرکزی حلقه هماهنگ‌کننده در ایجاد توافق و سیاستگذاری پیرامون امنیت سایبری اتحادیه اروپا را در حوزه خارجی بر عهده دارد و این درحالی است‌که تیم واکنش اضطراری رایانه‌ای اتحادیه اروپا[6] در عرصه داخلی توانسته است ابعاد فنی چنین نقشی را به اجرا درآورد. اداره کل شبکه‌های ارتباطات، محتوا و فناوری[7] و همچنین اداره کل مهاجرت و امور داخلی[8] کمیسیون اروپا به ترتیب پیشرو در طراحی سیاست گذاری ها در رابطه با امنیت شبکه و اطلاعات و جرائم سایبری هستند و دراین‌بین پارلمان اروپا نیز

1. EU's Internal Security Strategy (ISS)
2. Digital Agenda for Europe
3. European Strategy for Internet Security (ESIS)
4. Cybersecurity Strategy for the European Union (EUCSS)
5. European External Action Service (EEAS)
6. EU Computer Emergency Response Team (CERT)
7. Directorate General for Communications Networks, Content and Technology (DG Connect)
8. Directorate-General for Migration and Home Affairs (DG HOME)

با در نظر داشتن مقررات و امریه‌ها نقش کلیدی در فرآیند سیاست‌گذاری‌ها را بر عهده دارد. فراتر از این، آژانس‌های کلیدی اتحادیه اروپا از قبیل آژانس دفاع اتحادیه اروپا[1] بر توسعه دفاع سایبری اتحادیه اروپا تمرکز دارد و آژانس امنیت شبکه و اطلاعات اتحادیه اروپا[2] با ذی‌نفعان مربوطه جهت ایده پردازی برای پیشنهادها و توصیه‌ها در خصوص اجرای مناسب امنیت اطلاعات (ازجمله جرائم سایبری) و با کشورهای عضو اتحادیه اروپا در راستای اجرای مقررات اتحادیه اروپا در خصوص بهبود تاب‌آوری زیرساخت‌های حساس اطلاعات و شبکه‌ها همکاری می‌کند. درنهایت، آژانس همکاری‌های پلیسی اتحادیه اروپا (یوروپل) [3] و بالأخص مرکز مقابله با جرائم سایبری اتحادیه اروپا[4] است که حول ابعاد عملیاتی و راهبردی جرائم سایبری تمرکز دارند (ن.ک. شکل ۱-۱).

قطعاً امنیت سایبری یکی از عمده‌ترین مشکلات دستورکار سیاسی اتحادیه اروپا است که بعد از حملات سایبری به پارلمان اروپا، کمیسیون اروپا و طرح معاملات آلاینده‌های اتحادیه اروپا[5] در مارس ۲۰۱۱ که مورد اخیر حداکثر هزینه‌ای بالغبر ۳۰ میلیون یورو در اثر سرقت سهمیه آلایندگی تحمیل کرده است، این معضل جدی‌تر نیز شده است (Leyden 2011). هزینه جرائم سایبری تحمیل شده به اتحادیه اروپا سالانه در حدود ۸۵ میلیون یورو تخمین زده می‌شود (EU prepares to launch first cybercrime centre, 2012) و تحلیل‌های خاصی این‌گونه برآورد می‌کنند که در اروپا، افزون بر آسیب وارده به تجارت، رقابت، نوآوری و رشد اقتصادی، نزدیک به ۱۵۰ هزار شغل به دلیل جرائم سایبری در چند سال آینده از بین خواهد رفت (Net Losses Report 2014).

1. European Defence Agency (EDA)
2. European Network and Information Security (ENISA)
3. European Union Agency for Law Enforcement Cooperation (Europol)
4. European Cybercrime Center (EC3)
5. EU›s Emission Trading Scheme



شکل ۱-۱. ستون‌های مرکزی راهبرد امنیت سایبری اتحادیه اروپا
منبع: جمع آوری شده از داده‌ها در راهبرد امنیت سایبری اتحادیه اروپا (p. 17 ,2013)

چنین مشکلاتی به جهت پیچیدگی و اغلب ابهام‌آمیز بودن و ماهیت چندبعدی امور قضایی به‌سختی قابل حل‌وفصل هستند و اگرچه اتحادیه اروپا در این زمینه با رشد سیاست گذاری های خود روبه‌رو بوده است، اما تا تبدیل‌شدن به اکوسیستمی یکپارچه، کارآمد و تاب‌آور جهت تسلط بر تهدیدات سایبری راه طولانی پیش رو دارد. یقیناً به‌رغم آنکه رویکرد جامع اتحادیه اروپا در قبال امنیت سایبری به همراه تأکید بر تسریع این موضوع به اولویت سیاسی اتحادیه تبدیل شده است، اما هنوز مشخص نیست چگونه تهدیدات سایبری را می‌توان در مفاهیم حکمرانی به‌منظور برقراری بستر و نظامی پایدار و تاب‌آور تحت نظارت قرار داد و آن‌ها را جهت‌دهی کرد. به‌طور خلاصه، درحالی‌که قطعاً اتحادیه اروپا از ابزارها و سازوکارهای زیادی برای برخورد با امنیت سایبری بهره می‌گیرد، اینکه از آن‌ها چگونه استفاده می‌کند را باید توسعه بخشیده و سازگاری و انسجام در میان نهادها و بازیگران دخیل را در آن چیزی که می‌توان آن را در قالب اکوسیستم حکمرانی امنیتی در حال تکامل توصیف کرد، بهبود بخشد.

سؤالات و اهداف اصلی کتاب

بنابراین هدف این کتاب تشریح تکامل نظام حکمرانی اتحادیه اروپا در رابطه با امنیت سایبری و ارائه فهم عمیق‌تری از چگونگی توانایی اتحادیه اروپا در ساخت امنیت تاب‌آور کارآمد (ن.ک. فصل ۲) در خصوص موضوعات مرتبط با تهدیدات سایبری است و همچنین این کتاب زمینه پاسخگویی به سؤالات کانونی زیر را فراهم می‌آورد:

- چگونه می‌توانیم اکوسیستم حکمرانی امنیت سایبری در حال تکامل اتحادیه اروپا را توصیف و درک نماییم؟
- اتحادیه اروپا تا چه حد توانسته است رویکردی جامع در رابطه با امنیت سایبری در این اکوسیستم در حال تکامل ایجاد نماید و شرایط لازم را برای امنیت تاب‌آور کارآمد تثبیت نماید؟
- ماهیت اکوسیستم تاب‌آور در حال ظهور در اتحادیه اروپا چیست؟

مسئله موردنظر در فضای اتحادیه اروپا ۱۲۵ است. اگر اتحادیه اروپا قادر به تسهیل برقراری شرایط لازم برای امنیت تاب‌آور در فضای سایبری در کوتاه‌مدت و بلندمدت نباشد، بنابراین با خطر از بین رفتن اعتماد و اطمینان به اینترنت مواجه هستیم و اتحادیه اروپا نیز در برابر حملات سایبری آسیب‌پذیر باقی می‌ماند و از همه مهم تر به شیوه ای مؤثر قادر به واکنش و بهبود در این رابطه نخواهد بود. بهبود نحوه برقراری امنیت سایبری توسط اتحادیه اروپا برای پیوستگی منافع اجتماعی، اقتصادی، مالی و فرهنگی که شهروندان و کسب‌وکارها از اینترنت به دست می‌آورند و از همه مهم‌تر، رشد فناوری‌های اطلاعات و ارتباطات، ضروری است. به‌علاوه، این موضوع که آیا اتحادیه اروپا به اهدافی که در سند دستورکار دیجیتال اروپا (۲۰۱۰) برای خود تعیین کرده است، دست می‌یابد یا خیر، دارای اهمیت است و به همان اندازه، اینکه آیا به راهبرد اروپا ۲۰۲۰[1] به‌عنوان نیروی پیشران این سند خواهد رسید یا خیر مهم است. بنابراین ایجاد و تقویت اعتماد و امنیت در فضای سایبری گزینه پیش روی اتحادیه اروپا نیست؛ این

1. Europe 2020 Strategy

مسائل ملزومات و پیش‌نیازهای تحقق بلندپروازی، ارتقای ارزش‌ها و (باز)تعریف هویت و نظم پویای جهانی اتحادیه اروپا است که به شکل فزاینده‌ای به قابلیت همکاری درونی و ارتباطات دیجیتالی آن بستگی دارد.

ازلحاظ نظری و مفهومی، آثار کمی در خصوص تحلیل راهبرد امنیت سایبری اتحادیه اروپا و اکوسیستم در حال ظهور امنیت سایبری انتشار یافته است. تحقیقات گسترده‌تری از زوایای مختلف در خصوص امنیت سایبری به‌طور پیوسته با افزایش روبه‌رو بوده است (ن.ک. فصل ۱) و برخی از نویسندگان خاص دیدگاه‌های متعددی در خصوص راهبرد اتحادیه اروپا از طریق بکارگیری مفهوم قدرت سایبری (Klimburg and Tirmaa-Klaar 2011; Sliwinski 2014) و تاب‌آوری (Miriam Dunn Cavelty 2013) ارائه کرده‌اند. باوجوداین، چنین تلاش‌هایی در رابطه با پوشش و یا بازتاب مفهومی اکوسیستم نوخاسته منعطف در اتحادیه اروپا و همچنین قاره اروپا جامع نبوده است. بحث من این نیست که چنین رویکردهایی هیچ منفعتی در برنداشته است، درواقع حرف من کاملاً برعکس این قضیه است. اگر می‌خواهیم به درک عمیق‌تری از مقدار مسیر طی شده توسط اتحادیه اروپا برای دست‌یابی به امنیت تاب‌آور کارآمد در اکوسیستم در حال تکامل اتحادیه دست یابیم، چنین آثاری نیاز بیشتری به مصداق و توسعه دارند. بحث کتاب این‌گونه است که تاب‌آوری سازگار و منعطفی باید وجود داشته باشد که رویکرد اتحادیه اروپا را به سمت امنیت سایبری هدایت نماید یعنی اتحادیه اروپا باید از طریق حالت‌های حکمرانی و سازوکارهای مناسب بر توسعه شرایط امنیت سایبری تاب‌آور کارآمد تمرکز نماید تا بدین‌وسیله به بازیگر تأثیرگذار و رهبری در فضای سایبری تبدیل شود که فعالیت‌های مطلوبی در امنیت سایبری و ابعاد بسیار متعدد آن بر عهده گیرد (ن.ک. فصول ۲ و ۶).

با توجه به آنچه اشاره شد، اهداف کتاب از سه بخش تشکیل شده است:

- ارائه تحلیلی جامع و مفهوم محور از اکوسیستم در حال ظهور امنیت سایبری اتحادیه اروپا
- بکارگیری چارچوب مفهومی نوین در امنیت سایبری اتحادیه اروپا از طریق منابع تاب‌آور و حکمرانی امنیتی
- ایجاد درک عمیق‌تری از پیشرفت در طراحی رویکرد و راهبرد امنیت سایبری اتحادیه اروپا

و موارد استفاده‌ای که این رویکرد به‌منظور امنیت سایبری تاب‌آور کارآمد در اروپا و فراتر از آن در بر دارد.

بحث من این است که چنین عملی زمان‌بر و نیز ضروری است، بالأخص با توجه به شرایط حال حاضر مبنی بر نبود توجه به رویه‌های در حال تکامل اتحادیه اروپا در حوزه امنیت سایبری در عصر تغییر و تحول داخلی نهادی به پیروی از تصویب معاهده لیسبون[1] (۲۰۰۹) و افزایش چالش‌های امنیتی در فضای سایبری، عرصه‌ای که شهروندان، دولت‌ها، کسب‌وکارها و سایر فعالان به‌طور فزاینده‌ای ازلحاظ فرهنگی، مالی، اقتصادی، سیاسی و راهبردی تهدید می‌شوند (تصوری یا واقعی). مشخصاً درحالی‌که ایده‌های در حال تکامل بسیاری وجود دارد که از طریق مشورت و مباحثه حول موضوع امنیت سایبریِ کارآمد به بهترین نحو عمل می‌کند و کمیسیون اروپا و سایر آژانس‌ها از قبیل آژانس امنیت شبکه و اطلاعات اتحادیه اروپا فعالانه در طراحی تعاریف مشترک از مسئله (امنیت سایبری چیست) و راه‌حل‌های آن (منظور از تاب‌آوری، انواع مختلف شراکت عمومی–خصوصی در امنیت سایبری چیست) مشارکت دارند و هدف این کتاب نیز ارزیابی چگونگی کارکرد و مشارکت در ایجاد فهم و اجرای منعطف‌تر و شایع‌تر ستون‌های اصلی راهبرد امنیت سایبری اتحادیه اروپا جرائم سایبری، امنیت شبکه و اطلاعات (حفاظت از زیرساخت‌های حساس اطلاعات) و دفاع سایبری (ن.ک. فصول ۵ و ۶) است. به‌علاوه، این کتاب درصدد گنجاندن این مفهوم در بستر جهانی و گسترده‌تر (ن.ک. فصل ۲) و همکاری خاص‌تر حوزه فراآتلانتیکی (ن.ک. فصل ۷) است. علاوه بر این، کتاب به تاب‌آوری ملی از طریق ارائه تحلیل جامع از ملاحظات بریتانیا به‌عنوان عضو توسعه‌یافته اتحادیه اروپا در حوزه امنیت سایبری می‌پردازد (ن.ک. فصل ۴).

پیش از بیان ساختار کتاب باید طبقه‌بندی‌های خاصی اضافه و پارامترهایی روشن شوند. اولین مورد در این رابطه است که با این نظر که اتحادیه اروپا به بسیاری از مسائل حساس و امنیتی در سطح ملی می‌پردازد، واقعاً چه نقشی را می‌تواند در امنیت سایبری بر عهده گیرد.

1. Lisbon Treaty

راهبرد امنیت سایبری اتحادیه اروپا قبول دارد.

«عمدتاً وظیفه کشورهای عضو است تا به چالش‌های امنیتی در فضای سایبری بپردازند» (EUCSS 2013, p.4)، ولی اتحادیه اروپا نیز به‌خودی‌خود دارای نقش کلیدی در قالب یک بازیگر است. به همین دلیل، روشن است که اتحادیه اروپا می‌تواند تسهیل‌کننده باشد و بستری در حوزه های مختلف امنیت سایبری فراهم آورد که شرایط لازم را برای ظهور فرهنگ کارآمد امنیت سایبری در کشورهای عضو به وجود آورد و به شکل حساس با این کشورها چه ضعیف و چه قوی به‌منظور برقراری حداقل استانداردها و مهارت های حقوقی، فنی، سیاسی، اقتصادی، راهبردی و عملیاتی موردنیاز اتحادیه اروپا با هدف رشد در قالب عضو و اکوسیستمی تاب‌آور در رابطه با امنیت سایبری به همکاری بپردازد. نه‌تنها این مورد، بلکه اتحادیه اروپا می‌تواند به‌صورت حلقه منطقه‌ای مؤثر برای مبادله فعالیت های مناسب در کشورهای عضو و به‌صورت بین‌المللی از طریق تکامل، ارتقا و طرح اصول هنجارهای حکمرانی اینترنت، ازجمله مسائل حساس امنیت سایبری عمل نماید. یقیناً، با در نظر داشتن ماهیت بدون مرز و فراملی امنیت سایبری و دسترسی خارجی و تأثیر اتحادیه اروپا، این اتحادیه نه‌تنها در اروپا بلکه در چارچوب جهانی دارای نقشی حساس در ایجاد فرهنگ تاب‌آور و امنیت سایبری است .

دومین مسئله، مربوط به بحث های در حال اجرا در خصوص چگونگی تعریف امنیت سایبری و ابعاد مختلف آن امنیت سایبری، جرائم سایبری، جاسوسی سایبری، تروریسم سایبری، هکتیویسم سایبری و غیره است. درحالی‌که ماهیت و ذات این تعریف برای محققان به یک موضوع بدل شده است (برای مثال ن.ک. Di Camillo and Miranda 2011) و بسیاری از سازمان های منطقه ای و بین‌المللی و آژانس ها نیز به ارائه تعاریف مختلفی مبادرت ورزیده‌اند ولی قصد ندارم آشکار در این کتاب به این بحث‌ها وارد شوم. این مسئله به معنی کم‌اهمیت بودن این تعاریف نیست، بلکه هرکدام از چنین بحث‌هایی در تحلیل های مربوطه خود قرار گرفته و بحث‌ها در این خصوص در هر فصل بررسی خواهد شد. قطعاً یکی از بخش‌های مرکزی این تحلیل بر ظهور (یا عدم ظهور) تعاریف و درک های مشترک در بین ابعاد مختلف امنیت سایبری تمرکز دارد و نقطه آغازین آن یعنی تعریف پذیرفته‌شده توسط اتحادیه اروپا (ازجمله

آژانس های مربوطه آن) و کشورهای عضو است. در این مثال اتحادیه اروپا امنیت سایبری را در مفهومی گسترده تعریف می‌کند که بیشتر حول ماهیت آن تمرکز دارد (ن.ک. کادر ۱-۱). بااینکه کشورهای عضو اتحادیه اروپا در خصوص دفاع سایبری حساس هستند، اما در اسناد این اتحادیه تعریفی از این مسئله ارائه نشده است و عدم تمایل برخی از کشورها در این مسئله به جهت راهبردهای دفاع سایبری مخصوص به خود است (ن.ک. فصل ۶). این اتفاق دلیل این موضوع است که چرا دفاع سایبری برخلاف جرائم سایبری و امنیت شبکه و اطلاعات ذیل، سیاست بین دولتی امنیتی و دفاعی مشترک و نه در صلاحیت مشترک و جامع اتحادیه اروپا طبقه بندی می‌شود.

کادر ۱-۱. تعاریف اتحادیه اروپا از امنیت سایبری و جرائم سایبری

امنیت سایبری: «اقدامات و فعالیت‌هایی که برای حفاظت از حوزه سایبری، چه در عرصه نظامی و چه غیرنظامی، در برابر تهدیداتی بوده که ممکن است در ارتباط با، یا عامل ایجاد آسیب به شبکه‌ها و زیرساخت‌های وابسته به هم باشد. امنیت سایبری تلاش می کند از دسترسی و یکپارچگی شبکه‌ها» و زیرساخت‌ها و محرمانه بودن اطلاعات موجود در آن‌ها محافظت کند.
جرائم سایبری: «دامنه گسترده‌ای از فعالیت‌های مجرمانه که شامل سیستم‌های رایانه‌ای و اطلاعاتی چه به صورت ابزار اولیه و چه به صورت هدف اصلی است را شامل می‌شود. جرائم سایبری شامل جرائم سنتی (برای مثال، کلاه‌برداری، جعل اسناد و هویت)، جرائم محتوایی (برای مثال پخش آنلاین پورنوگرافی کودکان یا تحریک نفرت نژادی) و جرائم مخصوص سیستم‌های رایانه‌ای و اطلاعاتی (برای مثال، حمله به سیستم‌های اطلاعاتی»، خودداری از ارائه خدمات و بدافزارها) است.

EU Cybersecurity Strategy (2013, p.3)

سومین موضوع این است که، درحالی‌که نویسنده اعتراف و قبول می‌کند که تحلیل امنیت سایبری به‌منظور دست‌یابی به نتیجه‌ای جامع در هر حوزه‌ای باید ماهیت میان‌رشته‌ای داشته باشد –یعنی ارزش برابری را برای «لایه فیزیکی» (سخت‌افزار)، «لایه منطقی» (نرم‌افزار و پروتکل) و محتوا و یا «لایه اجتماعی» (فرهنگ، تعاملات بشر، ایده ها و سیاست گذاری ها) قائل گردید (Benkler 1998, 2007)– این کتاب مورد آخر را با تأکید حول شرایط اجتماعی و سیاست گذاری ها برای امنیت که باید در قالب فرهنگ تاب‌آوری ظهور یابد، در اولویت قرار می‌دهد. ازاین‌جهت، کتاب تحلیلی فرامتنی از تکامل منطق سیاست‌گذاری و امنیتی و همچنین

تحلیلی معاصر از رویه‌ها و کاربردهایی که این تحلیل برای تضمین امنیت کارآمد در قالب رویکردی تاب‌آور را داراست، ارائه می‌کند. بنابراین، آن افرادی که انتظار تحلیلی عمیق از راه حل های فنی و فناورانه موضوع امنیت سایبری دارند به‌احتمال‌زیاد ناامید شوند(!)؛ ولی امیدوارم این تحلیل حداقل گفتگوی بیشتری را در لایه های مختلف در خصوص روابط بین چالش‌های سیاست گذاری، فرهنگی و فنی برقراری اکوسیستم امنیت سایبری تاب‌آور در اروپا و فراتر از آن به وجود آورد. در کل راه حل های فنی تنها زمانی امکان پذیر هستند که محیط حقوقی و سیاست گذاری مناسبی وجود داشته باشد تا بتوان آن‌ها را به نحو مؤثری اجرا کرد.

چهارمین نکته این که، درحالی‌که کتاب پوشش جامعی از آنچه در قالب سه ستون اصلی راهبرد امنیت سایبری اتحادیه اروپا شناخته می‌شود را ارائه می‌دهد، همچنان ابعاد مهم بسیاری از امنیت سایبری اتحادیه اروپا و کشورهای اروپایی وجود دارد که مجالی برای پوشش آن‌ها نیست. ازاین‌جهت کتاب حاضر، به بررسی فرعیات سیاست گذاری اتحادیه اروپا و همکاری داخلی، رقابت و مناقشه بین اعضای اتحادیه اروپا و آژانس‌ها نمی‌پردازد. علاوه بر این، اولویت‌های ذکرشده در راهبرد امنیت سایبری اتحادیه اروپا (۲۰۱۳) از قبیل توسعه منابع صنعتی و فنی ملازم امنیت سایبری و تدوین سیاست‌های فضای سایبری منسجم و بین‌المللی برای اتحادیه اروپا به‌طور واضح در کتاب آورده نشده است، ولی تا حدی در مورد موضوع بُعد بین‌الملل، تحلیل عمیقی با در نظر گرفتن بستر بین‌المللی (فصل ۳) و مشارکت فراآتلانتیکی (فصل ۷) صورت گرفته است. به‌غیراز این، چندین مسئله همچون امنیت رایانش ابری، فناوری های هوشمند (شهرها، محیط‌ها، ابزارها و غیره) و سیستم‌های صنعتی کنترل‌شونده از طریق فناوری اطلاعات برای تضمین عنصر تمرکز و عمیق بودن عناصر اصلی در راهبرد امنیت سایبری اتحادیه اروپا که مورد تحلیل گرفتند در کتاب آورده نشده است. در آخر، تصمیم بر آن شد یک مطالعه موردی عمیق از یک کشور (بریتانیا، ن.ک. فصل ۴) را ارائه نماییم تا اینکه به‌جای آن مطالعات موردی متعدد ولی کمتر حقیقی کشورها را بکار گیریم، اگرچه پیشرفت‌ها در اتحادیه اروپا در این نوشتار اشاره به ستون‌های اصلی راهبرد امنیت سایبری اتحادیه اروپا دارد. این انتخاب‌ها آشکارا دامنه تحلیل را محدود می‌کنند، ولی با آگاهی از اینکه همه مسائل سایبری اروپا را تحت تأثیر قرار

نمی‌دهد، اتحادیه اروپا و کشورهای عضو را می‌توان در پژوهشی منفرد از این قبیل بررسی کرد.

درنهایت، با در نظر داشتن ماهیت پویای پیشرفت ها در فناوری های اطلاعات و ارتباطات و سیاست گذاری های امنیت سایبری و اجرای هر چه گسترد تر آن و ماهیت تکوینی بسیاری از اقدامات اتحادیه اروپا که نشئت‌گرفته از راهبرد امنیت سایبری (EUCSS 2013) است، یک نکته احتیاطی لازم به یادآوری است. خواننده باید آگاه باشد هرچه در این کتاب ارائه می‌شود، هرچند در بستر تاریخی، تصویری از پیشرفت ها، سیاست گذاری ها و اقدامات در دو سال پس از زمان انتشار راهبرد امنیت سایبری است. احتمال زیادی وجود دارد در زمان چاپ این کتاب بسیاری از ابعاد راهبرد امنیت سایبری اتحادیه اروپا و درنتیجه سیاست گذاری ها و اقدامات تکامل و تغییر کرده باشد. بااین حال بلندپروازی این کتاب است که تحلیل ارائه شده بستری را برای بازتاب تکامل آتی رویکرد اتحادیه اروپا و ماهیت و جهت گیری سیر آن در ارتباط با شرایط لازم به‌منظور ظهور یک اکوسیستم سایبری ایمن و تاب‌آور در اروپا فراهم نماید.

ساختار و سازماندهی کتاب

هدف کتاب ارائه دلیل جامع و مفهومیِ پیش برنده تکامل سیاست گذاری ها و راهبردهای اتحادیه اروپا است. به همین منظور، فصل دوم چارچوب و نشانگر مفهومی‌ای برای درک اکوسیستم در حال تکامل حکمرانی امنیت سایبری اتحادیه اروپا ارائه می‌کند. این فصل منابع نظری امنیت سایبری را در حالت کلی تر و در رابطه با اتحادیه اروپا مرور کرده و چارچوبی برای تحلیل از طریق مسئله‌مند کردن و آمیختن مفاهیم تاب‌آوری و حکمرانی امنیتی مطرح می‌کند. درواقع، این فصل بحث مفهومی در ارتباط با امنیت را در قالب رویکردی تاب‌آور و شرایط پایه ای که اجازه خواهند داد چنین رویکردی در اتحادیه اروپا و اروپا ظهور کند، مطرح می سازد.

فصل سوم، چارچوبی جهانی را معرفی می‌کند که در آن به عملکرد و تعامل اتحادیه اروپا در ارتباط با سیاست گذاری امنیت سایبری اشاره دارد. امنیت فناوری های اطلاعات و ارتباطات و اینترنت بر اساس فصل سوم، چارچوبی جهانی را معرفی می‌کند که در آن به عملکرد و تعامل

اتحادیه اروپا در ارتباط با سیاست‌گذاری امنیت سایبری اشاره دارد. امنیت فناوری‌های اطلاعات و ارتباطات و اینترنت بر اساس ماهیتِ هرکدام، بدون مرز هستند و به همین منظور بسیاری از چالش‌ها نه‌تنها نیازمند پاسخ‌های ویژه اتحادیه اروپا، بلکه نیازمند پاسخ‌های عمومی–خصوصی هماهنگ در سطح جهانی نیز هستند. فصل چهارم، ارزیابی مهمی در خصوص تکامل سیاست‌گذاری امنیت سایبری در سطح ملی ارائه می‌کند که کانون آن بر تکامل سیاست‌گذاری امنیت سایبری در بریتانیا به‌عنوان یک کشور پیشرفته است. درحالی‌که این فصل تنها یکی از کشورهای عضو اتحادیه اروپا را مورد تحلیل عمیق قرار می‌دهد، پیشرفت‌های صورت‌پذیرفته در جغرافیاهای دیگر و بازتاب اقدامات مناسب را که ظرفیت اشاعه در بستر اتحادیه اروپا دارد نیز برجسته می‌سازد.

فصول پنجم و ششم نیز تحلیل عمیقی از سیاست‌های اتحادیه اروپا در سه ستون اصلی امنیت ارائه می‌دهد: جرائم سایبری، امنیت شبکه و اطلاعات و دفاع سایبری. این دو فصل، چگونگی تکامل پیشنهادها، منطق‌ها و اقدامات تسهیل‌کننده برقراری شرایط لازم برای امنیت تاب‌آور نوظهور، ازجمله سازوکارهای حکمرانی مختلف در این سه ستون را بررسی می‌کنند. فصل هفتم نیز به واکاوی عمیق‌تری در خصوص رابطه اتحادیه اروپا با ایالات‌متحده آمریکا به‌عنوان یکی از مهم‌ترین روابط بین‌الملل اتحادیه در خصوص امنیت سایبری و جرائم سایبری پرداخته است. این فصل بر تحلیل رابطه میان اتحادیه اروپا و آمریکا و کاربردهای آن برای اتحادیه اروپا با هدف طراحی بُعد راهبرد امنیت سایبری و اکوسیستم فراآتلانتیکی تمرکز دارد. به‌طور جزئی‌تر، این فصل شباهت‌ها و تفاوت‌ها میان منطق امنیت اتحادیه و آمریکا در مسائل مختلف مرتبط با امنیت در فضای سایبری را تحلیل می‌کند تا بدین طریق به بررسی الف) محدوده‌ای که این شرکا آن را پوشش می‌دهند و یا در آن از هم فاصله می‌گیرند و ب) چگونه این مسئله به برقراری رویکرد امنیت تاب‌آور فراآتلانتیکی در خصوص امنیت سایبری تأثیر می‌گذارد، بپردازد.

فصل هشتم یافته‌ها و تأثیرات کلی این پژوهش در سطح اتحادیه اروپا را در بسترهای ملی و جهانی خلاصه می‌کند. این فصل در ابتدا، میزان مسیری که اتحادیه اروپا در گنجاندن شرایط لازم برای رویکرد امنیت تاب‌آور نوظهور طی نموده است را بررسی می‌کند؛ و دوم تأملاتی را

در خصوص رویکرد امنیت تاب‌آور و حالت‌های در حال ظهور حکمرانی برای دست‌یابی به این مهم در اتحادیه اروپا و مسیری برای تحقیق و تمرین امنیت تاب‌آور در تکامل اکوسیستم امنیت سایبری اتحادیه اروپا ارائه می‌کند.

فصل دوم

مفهوم‌سازی امنیت تاب آور در فضای سایبری

مقدمه

بسیاری از راهبردهای امنیت سایبری درون و ورای اروپا به ایجاد و توسعه تاب‌آوری کارآمد سایبری اشاره می‌کنند، اما این موضوع عمدتاً بدون تعریف و شالوده شکنی دقیق از مفهوم تاب‌آوری، مؤلفه‌های آن در سطوح مختلف و پیش‌شرط‌ها و اشکال حکمرانی موردنیاز برای دستیابی به آن صورت گرفته است. درنتیجه تاکنون ازلحاظ نظری و مفهومی، رویکردها به امنیت سایبری گزینشی بوده و از نظریه‌های انتقادی و سنتی حوزه روابط بین‌الملل و مفاهیمی چون قدرت سایبری بهره گرفته شده است. در راستای هدف اصلی کتاب، فصل حاضر به شکلی گسترده‌تر به نظریه‌پردازی‌های کنونی امنیت سایبری می‌پردازد و از طریق بررسی دقیق مفهوم تاب‌آوری و حکمرانی امنیت، به این نظریه‌پردازی‌ها خواهد افزود تا رویکردی کل‌نگر نسبت به ارزیابی تکامل اکوسیستم حکمرانی امنیت سایبری در اتحادیه اروپا به دست آید. علاوه بر این، فصل حاضر نه‌تنها به دنبال ایجاد یک چارچوب ارجاعی برای درک سیستم ارتباطات متقابل اینترنتی[1] (ENISA 2011c) است، بلکه به‌طور ویژه تر، شرایطی را که به شکل بالقوه می‌تواند به امنیت سایبری تاب‌آور در فضای اروپا منجر گردد، بررسی می‌نماید.

علاوه براین، در این فصل مفاهیم تاب آوری و حکمرانی امنیت بررسی و تعریف می شوند و نحوه عملیاتی شدن آن‌ها در تحلیل امنیت سایبری اتحادیه اروپا تشریح خواهد شد. هدف این

1. Internet Interconnection System

فصل، ترکیب ادبیات پژوهشی موجود در باب تاب آوری و حکمرانی امنیت، به منظور ساخت و تثبیت رویکردی است که امنیت را به مثابه پایداری تلقی می‌کند. این موضوع امکان مفهوم‌سازی حکمرانی نوظهور در راهبرد امنیت سایبری اتحادیه اروپا و مهم‌تر از آن، چگونگی ارتباط این موضوع با دستیابی به امنیت تاب‌آور کارآمد در اروپا را فراهم می‌سازد. بی تردید چنین چارچوبی وجوه مشترکی با آثار مفهومی موجود دارد، اما بر ادبیات موجود هم چیزی می افزاید، به ویژه با معرفی برداشتهای مختلف از مفهوم پایداری که از طریق آنها می شود حکمرانی امنیت سایبری را درک و ارزیابی کرد.

به‌اختصار، هدف فصل حاضر فراهم آوردن چارچوب و نشانه‌های مفهومی برای توضیح نحوه تکامل نظام حکمرانی اتحادیه اروپا در امنیت سایبری است تا درک عمیق‌تری بدست آید که چگونه اتحادیه اروپا می‌تواند یک اکوسیستم حکمرانی امنیت تاب‌آور با در نظر گرفتن مسائل حوزه تهدید سایبری ایجاد نماید. چنین چارچوبی می‌تواند ارائه پاسخ‌هایی به لحاظ مفهومی متقن را به سؤالات محوری مجلد حاضر تسهیل نماید: چگونه می‌توان اکوسیستم در حال تکامل حکمرانی امنیت سایبری اتحادیه اروپا را تبیین و درک نمود؟ اتحادیه اروپا تا چه میزان توانسته رویکردی جامع و تاب‌آور به امنیت سایبری درون اکوسیستم در حال تکامل خود ایجاد نماید؟ ماهیت اکوسیستم تاب‌آور نوظهور درون اتحادیه اروپا چیست؟ استدلال نهان مطرح شده در سرتاسر این فصل و کتاب حاضر این است که شکلی اجتماعی-اکولوژیکی تر، انطباق پذیرتر و انعطاف پذیرتر از تاب آوری باید پیشران رویکرد اتحادیه اروپا به امنیت سایبری باشد.چنین رویکردی اتحادیه اروپا را قادر خواهد ساخت که به بازیگری تأثیرگذار در فضای سایبر و رهبری با عملکرد مطلوب در حوزه امنیت سایبری و ابعاد مختلف آن تبدیل شود.

ساختار این فصل برای دستیابی به اهداف خود بدین شکل است. در بخش نخست، مرور و بررسی شیوه نظریه‌پردازی و مفهوم‌پردازی امنیت سایبری در ادبیات پژوهشی این حوزه و فراتر از آن صورت می‌پذیرد. بخش دوم به ادبیات پژوهشی خاصی می‌پردازد که برای شکل‌دهی به چارچوب این کتاب مورداستفاده قرار خواهد گرفت که برای مثال شامل تاب‌آوری و حکمرانی امنیت است؛ و شرایط و نشانه های مفهومی که می‌تواند در فهم اکوسیستم نوظهور امنیت

سایبری اتحادیه اروپا مورداستفاده قرار گیرند نیز ترسیم خواهد شد. در این فصل همچنین رابطه میان ابعاد گسترده تر ادبیات پژوهش و امنیت به‌عنوان چارچوب تاب‌آور در تحلیل اکوسیستم امنیت سایبری اتحادیه اروپا نیز تصریح می‌گردد. نهایتاً بخش پایانی نیز استدلال مطرح در فصل حاضر و دلالت‌های آن در تحلیل نوشتار حاضر را به شکل خلاصه بیان می‌کند.

رویکردها به تحلیل امنیت سایبری

آثار نظری متقن پیرامون امنیت سایبری هرچند به‌سرعت در حال تکمیل است اما به شکلی تعجب‌آور بسیار اندک هستند. آثار موجود بر ایالات‌متحده و سایر مناطق جغرافیایی تمرکز دارند (برای مثال: Kshetri 2013) و هیچ نوع تحلیل جامع و نظری در خصوص امنیت سایبری اتحادیه اروپا انجام نشده است. در ادبیات موجود از طیف متنوعی از رویکردها به‌منظور تحلیل موضوع استفاده شده که از رویکردهای سنتی راهبردی و مدیریتی ملی (Libicki 2007, 2009; Janczewski and Colarik 2007; Mehan 2008; Janczewski 2008; Clarke and Knake 2010) تا رویکردهای تاریخی (Carr 2009) و رویکردهای «تروریست» محور (Veron 2003; Colarik 2006; Wiemann 2006) را در برمی‌گیرد. این رویکردها کمتر به جنبه‌های نظری پرداخته و بیشتر بر خطر واقعی و حال حاضر تهدیدات سایبری و مدیریت بالقوه خطرات توأم با آن پرداخته‌اند؛ در دیگر آثار نیز به چگونگی مقابله با دشمنان سایبری و ایجاد صلح سایبری پرداخته شده است (Clarke and Knake 2010). آثار دارای جنبه‌های مفهومی، روش‌شناختی و نظری بیشتر، از رویکردهای حکمرانی (تنظیمی) (Brown and Marsden 2007; Mueller 2010)، رویکردهای عملگرایانه، همه‌جانبه و تطبیقی (Karatzogianni 2006, 2009; Eriksson and Giacomello 2010)، رویکردهای نوآورانه ترکیبی (Deibert et al. 2012)، رویکردهای قدرت سایبری; (Kramer et al. 2010; Nye, Jr 2010; Klimburg 2011a; Betz and Stevens 2011; Sliwinski 2014)[1] و رویکردهای انتقادی‌تر که درصدد یافتن پاسخ این سؤال بوده‌اند که سیاست‌های سایبری تا چه میزان امنیتی شده‌اند (Eriksson 2001; Bendrath et al. 2007; Dunn Cavelty 2007, 2008) نیز بهره برده‌اند. آثار اخیر که به آن‌ها اشاره

شد، از جنبه اهداف فرامتنی و این واقعیت که اغلب آثار پیرامون مفهوم حکمرانی ازلحاظ فکری مشابهت‌هایی با رویکرد فصل حاضر در نوع تحلیل اکوسیستم در حال تکامل حکمرانی اتحادیه اروپا دارند، دارای اهمیت است که در ادامه به این آثار خواهم پرداخت.

کاراتزوجیانی[1] (۲۰۰۹) به شکلی مفید بر چگونگی مفهوم‌سازی نقش رسانه‌های جدید در تنش‌های سایبری تمرکز می‌کند، اما در اثر وی هیچ نوع ارتباط نظری واقعی با سیاست‌های امنیت سایبری به شکل صرف و همچنین هیچ نوع تمرکز خاصی بر اتحادیه اروپا وجود ندارد. اریکسون[2] و جیاکوملو[3] (p.3-11,2010) نیز به‌رغم عدم تمرکز بر اتحادیه اروپا، به ادبیات موجود در رابطه با عصر و امنیت دیجیتال پرداخته و بیان می‌کنند که در ادبیات موجود به شکلی گسترده «امنیت» و یا «نظریه» مورد غفلت قرار گرفته است. برخی نویسندگان (Castells 1996, 1997, 1998; Mowlana 1997) ادبیات جامعه اطلاعاتی[4]را تحلیل و بیان می‌کنند که این ادبیات بر مقوله‌های دولت و امنیت اجتماعی تمرکز نکرده و در عوض به امنیت شرکت‌ها و بازار پرداخته است. درعین‌حال، موضوعی که آن‌ها امنیت عصر دیجیتال می‌نامند، سیاست‌محور بوده و درنتیجه نظریه‌پردازی حوزه امنیت سایبری را نادیده می‌گیرند. این نویسندگان درنهایت به این نتیجه می‌رسند که بیشتر آثار این حوزه در معرض خطر احساسی کردن تهدیدات سایبری (سناریوی پرل هاربر الکترونیکی)[5] بوده و درنتیجه در رابطه با ابزارهای موردنیاز برای پرداختن به مسائل مرتبط با پردازش روزانه تضمین اطلاعاتی بزرگ‌نمایی می‌کنند.

مقوله‌ای که آن‌ها اساساً استدلال می‌کنند این است که نوعی شکاف بین نظریات روابط بین‌الملل و امنیت در عصر دیجیتال وجود دارد و متعاقباً به سودمندی نظریات واقع‌گرایی، لیبرالیسم و سازه‌انگاری برای درک و توضیح امنیت در عصر دیجیتال اشاره می‌کنند؛ سپس نتیجه می‌گیرند که اتخاذ رویکردی «عملگرا» برای مفروضات گونه‌شناختی و نه جهانی، روشی را برای به‌کارگیری دیدگاه‌های ادبیات‌های مختلف فراهم می‌کند. نکته جالب این است که آن‌ها نشان می‌دهند نظریات لیبرالیسم و سازه‌انگاری مرتبط‌ترین چارچوب‌های نظری روابط

1. Karatzogianni
2. Eriksson
3. Giacomello
4. Information Soceity (IS)
5. Electronic Pearl Harbour

بین‌الملل هستند. لیبرالیسم بر بازیگران و جوامع شبکه‌ای غیردولتی فراملی، «وابستگی متقابل آسیب‌پذیر» و تأکید بر نفوذپذیری مرزها و از سوی دیگر، سازه‌انگاری بر تحلیل گفتمان، معناشناسی، نمادها و هویت در بحث امنیت عصر دیجیتال تأکید دارد.

چنین رویکرد عملگرایانه‌ای توسط نویسندگان مختلف و با هدف تحلیل جنبه‌های سیاسی تهدیدات و حفاظت در برابر آن‌ها استفاده شده و تحلیل‌هایی ژرف‌کاوانه در رابطه با امنیتی شدن فضای سایبری توسط ایالات‌متحده (Bendrath et al. 2010, p.57)، چالش‌های ناشی از پیچیدگی نظریه‌پردازی در مورد امنیت در عصر دیجیتال (Dunn Cavelty 2010, p.85)، رویکردهای نهادگرای لیبرال در مورد یک رژیم جهانی تضمین اطلاعات (Valeri 2010, p.132) و رویکردی کل‌نگر که از ادبیات موجود پیرامون همکاری‌های بین‌المللی، مقررات و توزیع سیاستی (Hosein and Eriksson 2010, p.158) مطرح می‌سازد. چنین آثاری بدون تردید مرتبط با هدف کتاب حاضر برای تبیین و درک اکوسیستم نوظهور امنیت سایبری اتحادیه اروپا است. ارتباط آن‌ها بی‌شک به‌واسطه یادآوری پیچیدگی‌های هر نوع تحلیل سیاست‌های فضای سایبری می‌باشد. علاوه بر این، تصریح نیاز به اتخاذ رویکردی که متن، تغییر و اقدام را از دو جنبه خصوصیت پردازی اکوسیستم نوظهور در اتحادیه اروپا و همچنین شناسایی الگوهای پیچیده تداوم و تغییر در ارتباط بااینکه چگونه یک نظام حکمرانی تاب‌آور امنیت سایبری برای اتحادیه اروپا توسط انبوه بازیگران در فضای این اتحادیه و فضای جهانی چارچوب‌بندی، ایجاد و اعمال می‌کند، از دیگر جنبه‌های اثر حاضر است.

دان کاولتری[1] (2007، 2008a) از چشم‌انداز «مطالعات امنیتی» به موضوع امنیت سایبری ورود کرده و مانند اریکسون و جیاکوملو (۲۰۱۰) به فقدان کاربرد نظریات روابط بین‌الملل در این حوزه اشاره می‌کند. دان کاولتری چشم‌اندازی که آن را دیدگاهی نیمه سازه‌انگارانه می‌نامد، از روش تمرکز مکتب کپنهاگ بر اعمال گفتاری استفاده کرده و کار خود را با چارچوب‌بندی و نظریه برجسته‌سازی[2] تکمیل می‌کند. رویکرد وی دارای چندین مزیت در بحث تحلیل امنیت سازه‌انگاری قرار می‌گیرد. بر اساس آن، ماهیت برساخته اجتماعی تهدیدات سایبری به رسمیت

1. Dunn Cavelty
2. Agenda-setting Theory

شناخته شده، اما درعین‌حال «مقاصد و اهداف به شکل تجسم‌یافته درون ساختاری‌های عینی و نهادینه‌شده فکری و عملی شناخته می‌شوند» (p.7 ,2008). لذا، تأکید کاولتری صرفاً بر سخن به‌عنوان عملی گفتمانی نبوده، بلکه بر این نکته است که چگونه برداشت‌های بازیگران می‌تواند بر اقدام و عمل تأثیرگذار باشد. رویکرد این نویسنده به یک دستورکار پژوهشی منتهی شد که بر چگونگی برساخته شدن موضوعات امنیت سایبری به‌عنوان تهدید و متعاقباً مرحله امنیتی شدن برحسب اقداماتی که برای مقابله با تهدیدات سایبری صورت می‌گیرند، تمرکز دارد. یافته‌های اصلی کاولتری جالب‌توجه است و دارای الزاماتی آشکار برای کنترل امنیت سایبری در اروپا می‌باشد، به‌خصوص با توجه به توجیه و حفظ انواع یا اشکال (استثنایی) از حکمرانی در نبود آنچه ممکن است خطراتی واقعی یا مشهود به شمار روند. بااین‌حال، به‌رغم آنکه چنین رویکردی از جنبه فکری برای مهیا نمودن متن با در نظر گرفتن چارچوب‌بندی و تغییرات تاریخی مناسب است، اما صریحاً برساخته شدن سیاست را به اشکال دولت ربط نمی‌دهد (ن.ک. Christou et al. 2010; Christou and Croft 2012). به‌طور خاص، این رویکرد از جزئیات ترتیبات حکمرانی در حال تکامل[۲] در بافت امنیت سایبری تاب‌آور در حال ظهور غافل می‌ماند. پس بااینکه در کتاب حاضر از بافت مرتبط با سیاست و رویه امنیت سایبری اتحادیه اروپا غفلت نمی‌شود، اما سؤال کلیدی نیز صرفاً بر چگونگی امنیتی شدن یا نشدن فضای سایبری تمرکز نخواهد داشت، بلکه بر چگونگی شکل‌گیری منطق و ماهیت تاب‌آوری درون اکوسیستم در حال تکامل حکمرانی امنیت سایبری توسط رویه‌ها متمرکز خواهد بود.

یکی دیگر از رویکردهای مفهومی به امنیت سایبری از چشم‌انداز قدرت سایبری بوده است. جوزف نای[1] (۲۰۱۰) در تلاش برای نشان دادن انواع رفتارها، ابزارها و منابعی که می‌توانند در جهان سایبر در مفهوم گسترده آن، مورداستفاده بازیگران دولتی و غیردولتی قرار گیرند، قدرت سایبری را به‌عنوان «توانایی استفاده از فضای سایبری به‌منظور ایجاد مزیت و نفوذ در سایر محیط‌های عملیاتی و هم‌راستا با ابزارهای قدرت» تعریف می‌کند (p.4 ,2010). وی در ادامه میان ابزارهای فیزیکی و اطلاعاتی و قدرت سخت و نرم در فضای سایبری تمایز قائل شده و.

1. Joseph Nye

مثال‌هایی از چگونگی استفاده از آن‌ها درون (قدرت سایبری درونی) و بیرون (قدرت سایبری بیرونی) نیز ارائه می‌دهد (Joseph Nye Jr 2010, p.5) .

ارتباط مفهوم قدرت سایبری، پیوند آن با اشکال مختلف حکمرانی در دسترس برای بازیگران در فضای سایبری و مهم‌تر از آن نوع تاب‌آوری و درنتیجه امنیت سایبری است که یک بازیگر یا دولت می‌تواند بدان دست یابد. بااینکه جوزف نای ارتباط میان قدرت نرم و سخت را با جنبه‌های سه‌گانه قدرت نشان می‌دهد (Ibid., p.7)، چنین قدرتی همچنین نشان‌دهنده این است که چگونه بازیگران و ازجمله اتحادیه اروپا می‌توانند امنیت اطلاعات و تهدیدهای صورت‌گرفته نسبت به زیرساخت‌های حیاتی اطلاعات را کنترل و مدیریت نمایند. از سوی دیگر این موضوع نشان‌دهنده منابع قدرت بازیگران دخیل در هر نوع اکوسیستم امنیت سایبری است و اینجا است که جوزف نای ادعا می‌کند به‌رغم تحدید شکاف میان بازیگران دولتی و غیردولتی از برخی ابعاد خاص، اما این موضوع به معنای برابر شدن آن‌ها نیست؛ به‌عبارت‌دیگر، هرچند که شبکه‌ها به‌عنوان یک ابزار حکمرانی از اهمیت بیشتری برخوردار شده‌اند، اما دولت‌ها هنوز هم ازلحاظ دسترسی به منابع، قدرتمندترین بازیگران به شمار می‌روند. درنتیجه وی بیان می‌کند که دولت‌ها اشکال مختلفی از راه‌حل‌های قدرت سایبری با ماهیت درون‌نگر و برون‌نگر در اختیار داشته که هردوی آن‌ها تحت تأثیر فضا و زمان قرار دارند. بااینکه وی ادعا می‌کند درون چنین چارچوبی است که راهبردهای مختلف تدافعی و تهاجمی بسته به میزان توانایی دولت‌ها برای آن‌ها فراهم می‌شود، اما همچنین به دشواری همکاری‌های بین‌المللی به‌منظور قاعده‌مندسازی «هنجارهای رفتاری» در حوزه‌هایی نظیر جرائم سایبری یا جاسوسی سایبری نیز اشاره می‌کند .(Ibid., p.18)

بتز[1] و استیونز[2] (۲۰۱۱) نیز همانند جوزف نای (۲۰۱۰) بر راهبرد دولتی و قدرت سایبری تمرکز می‌کنند، هرچند که آن‌ها به‌هیچ‌عنوان نقش بازیگران غیردولتی را در فضای سایبری مستثنا نمی‌سازند. بلکه، قدرت سایبری را به‌عنوان شکلی از قدرت در نظر می‌گیرند که در فضای سایبری گردش می‌کند و تجربیات افرادی را که درون و در راستای این فضا کنش انجام

1. Betz
2. Stevens

می‌دهند، شکل می‌دهد (Betz and Stevens 2011, p.44). از سوی دیگر، به این نکته اشاره می‌کنند که در یک جامعه شبکه‌ای دارای ساختارهای پیچیده اجتماعی که نیروی محرکه آن نوآوری‌های فناورانه است، قدرت بازیگران غیردولتی به شکلی قابل‌توجه افزایش می‌یابد؛ آن‌ها همچنین سیال بودن فضای سایبری را شناسایی می‌کنند که متشکل از بازیگران متعدد بوده و دائماً در نوسان و جریان است (Ibid., p.38). و نیز بیان می‌کنند که بخش اعظم ترس دولت‌ها ناشی از تعدد و اشاعه بازیگران فضای سایبری است که با هدف دستیابی به اهداف خود، در پی بهره‌برداری از فرصت‌های این محیط می‌باشند. به بیان آن دو، «این بازیگران از افراد حقیقی و شهروندان تا سازمان‌های مدنی و کمپانی‌های تجاری، از گروه‌های تروریستی و شورشی تا شاخه‌هایی از قدرت دولت، از نهادهای چندجانبه جهانی و غول‌های رسانه‌ای، از گروه‌های انفرادی تا تمامی یک شبکه و موجودات غیرانسانی به شکل نرم‌افزار و سخت‌افزار تشکیل می‌شوند...» (Ibid., p.38-39).

آن‌ها در موضوع شناسایی پیچیدگی قدرت در فضای سایبری به دنبال توسعه مفهوم قدرت سایبری هستند و در این راه چهار شکل متمایز از قدرت سایبری را شناسایی می‌کنند:

۱) اجباری/زوری که به معنای استفاده مستقیم یک بازیگر فضای سایبری از اجبار و زور برای تعدیل رفتار و شرایط زیست بازیگر دیگر است و می‌تواند توسط بازیگران دولتی یا غیردولتی انجام شود و همچنین در تعاملات میان بازیگران دولتی و غیردولتی و بین بازیگران غیردولتی دیده می‌شود؛ ۲) نهادی که شامل کنترل غیرمستقیم بازیگر فضای سایبری توسط یک بازیگر دیگر است که اصولاً به‌واسطه مداخلات نهادهای رسمی و غیررسمی صورت می‌گیرد و می‌تواند توسط بازیگران دولتی (ازجمله زیرمجموعه‌های دولت) و بازیگران غیردولتی نیز اعمال شود؛ ۳) ساختاری که با هدف حفظ ساختارهایی که تمامی بازیگران در آن واقع شده‌اند و کنش‌های آن‌ها را در قبال سایر بازیگرانی که با آن‌ها ارتباط مستقیم دارند کنترل و تعدیل می‌کند، بر چگونگی کارکرد قدرت تمرکز دارد؛ و ۴) مولد که به ساخت موضوعات اجتماعی از طریق گفتمان تعدیل‌شده و اجرایی‌شده در فضای سایبری می‌پردازد و حوزه‌های احتمال را که کنش را تسهیل و تحدید می‌نمایند، تعریف می‌کند (که شامل ساخت گفتمانی بازیگران تهدیدکننده

در فضای سایبری به‌منظور مشروعیت بخشی به اقدامات علیه آنان است) (Betz and Stevens 2011, p.45-53). آن‌ها در شناسایی این اشکال قدرت سایبری به این نکته نیز معترف‌اند که تمامی آن‌ها دارای وابستگی متقابل هستند. این بدان معناست که قدرت سایبری یک مفهوم یکپارچه نیست و درنتیجه در مفهوم‌سازی امنیت تاب‌آور در فضای سایبری باید رویکردی جامع اتخاذ شود که امکان حضور هر چهار نوع قدرت سایبری را در هر سناریویی فراهم سازد (Betz and Stevens 2011, p.52-53).

کلیمبرگ[1] (2011a) نیز به مفهوم قدرت سایبری می‌پردازد. ابعاد این نوع قدرت که ازنظر کلیمبرگ اهمیت دارند شامل این موارد هستند: هماهنگی جنبه‌های عملیاتی و سیاسی در ساختارهای دولتی؛ جامعیت سیاست‌ها از طریق ایجاد ائتلاف‌های بین‌المللی و چارچوب‌های حقوقی و همکاری بین بازیگران غیردولتی فضای سایبری. وی برخلاف جوزف نای ادعا می‌کند که از میان این ابعاد، مورد سوم با توجه به ماهیت اینترنت و فضای سایبری، مهم‌تر از سایر جنبه‌ها است. در این بخش قسمت اعظم کنترل در تسلط کسب‌وکارها و جامعه مدنی بوده و ظرفیت‌های دولتی صرفاً به نفوذ غیرمستقیم و نه مستقیم محدود است. کلیمبرگ در این رابطه بر مبنای الگوی توانمندی یکپارچه (ن.ک. Klimburg and Tiirmaa-Klar 2011, p.11)، به ضرورت اتخاذ رویکردی یکپارچه در قبال امنیت سایبری اشاره می‌کند و از دیدگاه وی بازیگران غیردولتی باید نسبت به همکاری با دولت‌ها ترغیب شوند. وی در ادامه ادعا می‌کند که «مهم‌ترین بُعد قدرت سایبری را درنتیجه می‌توان توانایی انگیزش و جذب شهروندان دانست که درواقع یک رویکرد درون‌نگر مبتنی بر قدرت نرم است که برای شکل‌دهی به کلیت مفهوم توانمندی سایبری در سطح ملی ضروری است» (2011, p.43). وی به طولانی شدن درک واقعیت اهمیت اتخاذ رویکرد جامع به قدرت سایبری توسط ایالات‌متحده اشاره می‌کند و مدعی است که روسیه و چین هر دو «دارای توانمندی‌های سایبری غیردولتی قدرتمند و آشکاری هستند که با دولت‌های خود تعامل می‌کنند» (ibid., p.43-44). وی آشکارا از یک الگوی مشارکت عمومی خصوصی‌ای حمایت می‌کند که توسط اهداف و خواسته‌های مشترک

1. Klimburg

به‌پیش برود. وی به‌رغم ارائه مثال‌هایی از مشارکت دوجانبه بازیگران دولتی و غیردولتی در چین، روسیه، ایالات‌متحده (و همچنین بریتانیا و اتحادیه اروپا)، به جزئیات ماهیت چنین مشارکتی فراتر از نیاز به ایجاد اعتماد متقابل و یا سازوکارهای احتمالی چنین مشارکتی برای امنیت سایبری در اتحادیه اروپا و فراتر از آن، کل اروپا نمی‌پردازد. البته باید به این نکته نیز توجه داشت که الگوهای همکاری و اجبار و شبکه‌های همکاری‌های جنایتکارانه چین و روسیه مثال‌های حکمرانی از مقوله‌ای که با هنجارها و ارزش‌های اتحادیه اروپا برای امنیت سایبری و حکمرانی اینترنت همخوانی داشته باشند، نیستند (EU Principles and Guidelines 2011)؛ هرچند که مفهوم هنجاری فراگیر مشارکت و رویکرد «همگرا» مطلوب است.

کلیمبرگ و تیرما کلار[1] (۲۰۱۱) مفهوم قدرت سایبری را مطابق نکته‌ای که در مورد ابعاد سه‌گانه آن گفته شد، در گزارشی برای پارلمان اروپا به‌کار بردند. مهم‌ترین نتایج گزارش یاد شده این بود که سیاست‌های امنیت سایبری اتحادیه اروپا در حوزه‌های جرائم سایبری و حفاظت از زیرساخت‌های حیاتی اطلاعات[2] در ایجاد تاب‌آوری کلی درون اتحادیه اروپا (تاب‌آوری در مفهومی که تاکنون تعریف نشده است) مؤثر بوده و توانمندی‌های جنگ سایبری آن هنوز در چارچوب سیاست امنیتی و دفاعی مشترک اتحادیه اروپا[3] به‌اندازه کافی توسعه پیدا نکرده است. به‌طور بنیادی‌تر و بر اساس ابعاد قدرت سایبری، نظام درونی نهادی اتحادیه اروپا در برابر حملات سایبری آسیب‌پذیر است. هرچند تأسیس تیم واکنش اضطراری رایانه‌ای اتحادیه اروپا تا حدودی به حل این مشکل کمک کرده، اما نبود اجرای کافی تمهیدات حفاظت اطلاعات سبب شده تا نهادهای اتحادیه در برابر حملات بی‌دفاع باشند و تبادل اطلاعات ضعیفی بین مقامات دخیل در سیاست امنیت سایبری وجود داشته باشد. افزون بر این، از حیث همکاری و طبعاً انسجام، هیچ نهادی به‌طور مشخص مسئول امنیت سایبری اتحادیه اروپا نبوده و حتی سیاست مشترکی نیز در این زمینه وجود ندارد (که با وجود یک سند راهبرد امنیت سایبری، هنوز یک مسئله اصلی است). در سطح بین‌المللی نیز ادعا می‌شود که اقدامات اتحادیه اروپا در موضوعاتی چون امنیت سایبری به‌خصوص در نهادهایی نظیر شرکت اینترنتی برای نام‌ها و شماره‌های واگذارشده

1. Tiirmaa-Klaar
2. Critical Information Structure Protection (CIIP)
3. EU's Common Security and Defence Policy (CSDP)

(آیکان)[1] می‌تواند به شکلی قابل‌توجه افزایش یابد (Ibid., p.36).

از جنبه درونی نیز، این‌گونه بحث می‌شود که در فضای پس از دوران انعقاد سیاست دفاعی و امنیتی مشترک ذیل پیمان لیسبون، اقدامات اندکی به‌منظور ایجاد یک سیاست یکپارچه امنیت سایبری در اتحادیه اروپا صورت گرفته است. به‌طور دقیق‌تر، هیچ مفهومی در رابطه با نمایش قدرت «سخت» و «نرم» از طریق یک رویکرد یکپارچه امنیت سایبری و درنتیجه کمک به تعریف امنیت بین‌المللی سایبری بر اساس ارزش‌های اتحادیه وجود ندارد (Ibid., p.37). در سمت مثبت موضوع، این‌طور ادعا می‌شود که کمک‌های اعطایی در قالب برنامه پژوهشی امنیت سایبری اتحادیه اروپا توانسته کمک شایان توجهی در حمایت از ایجاد تاب‌آوری داشته باشد و کمیسیون اروپا نقشی حیاتی در پیشبرد دستورکار توسعه افقی و عمودی سیاست‌های امنیت سایبری در کشورهای عضو (به‌خصوص اعضای ضعیف‌تر) داشته است.

فراتر از این، بر اساس یافته‌های این مطالعه که مبتنی بر شرایط بُعد سوم قدرت سایبری که توسط کلیمبرگ (۲۰۱۱a) به‌عنوان همکاری با بازیگران غیردولتی (جامعه مدنی و بخش خصوصی) بیان شد، میزان مشارکت و ورود اتحادیه اروپا به بحث امنیت سایبری از توسعه کافی برخوردار نیست. در این گزارش پیشنهاد شده که به‌منظور تکامل تاب‌آوری اتحادیه اروپا در برابر تهدیدات سایبری، این اتحادیه باید تلاش‌های خود را مبنی بر مشورت با جامعه مدنی (برای مثال بازیگران فنی که بر روی نرم‌افزارهای منبع باز کار می‌کنند) افزایش دهد که البته کمیسیون اروپا ازلحاظ تاریخی نسبت به این اقدام مشتاق بوده و باب آن را باز گذاشته است. هرچند که برای مثال ابتکارات و طرح‌هایی مانند مشارکت عمومی-خصوصی اتحادیه اروپا در تاب‌آوری[2] به‌منظور همکاری و به اشتراک‌گذاری اطلاعات وجود دارد، (البته این برنامه توسط برنامه دیگری با نام پلتفرم عمومی- خصوصی امنیت شبکه و اطلاعات[3] جایگزین شد؛ ن.ک. فصل ۶ همین کتاب). بااین‌حال گزارش مذکور بیان می‌کند که فاصله زیادی تا ایجاد یک رویکرد کاملاً اروپایی به مسئله اشتراک اطلاعات در موضوع حملات سایبری وجود دارد.

1. Internet Corporation for Assigned Names and Numbers (ICANN)
2. European Public Private Partnership for Resilience (EP3R)
3. Network and Information Security Public Private Platform

ادبیات امنیت سایبری یقیناً موضوعات جالبی پیرامون اکوسیستم نوظهور حکمرانی امنیت سایبری اتحادیه اروپا و رویکرد این اتحادیه به امنیت سایبری را برجسته می‌سازد. اتحادیه اروپا یک دولت سنتی به معنای صرف آن نیست، بلکه دارای ساختار نهادی خاص خود است و ترکیبی از تعهدات فراملی و بینادولتی در کنار منطق متغیر هرکدام از اعضا در موضوعات تهاجم و دفاع سایبری در بحث امنیت سایبری در آن دیده می‌شود. درنتیجه بااینکه استدلال می‌شود به یک رویکرد یکپارچه برای اینکه اتحادیه اروپا بتواند کماکان نسبت به ارزش‌ها و اصولی که برای اینترنت و امنیت پایدار، تطبیقی و تاب‌آور پایبند بماند، نیاز است، اما اتحادیه درعین‌حال باید به دنبال افزایش توانمندی‌های نرم خود از طریق تأثیرگذاری ساختاری و (بر)ساختن گونه نهادین و نه هر نوع از قدرت سخت الزام‌آور باشد.

قدرت سخت و توسعه توانمندی‌های تهاجمی به هر شکل با توجه به حساسیت کشورهای عضو دشوار، و اگر نگوییم غیرممکن، است اما با توجه به مطلوبیت این موضوع نیاز است به آن پرداخته شود، البته به صورتی که منطق امنیت ملی به شکلی باشد که حقوق افراد را خدشه‌دار نسازد، بازیگران ذی‌نفع را از معادله کنار نگذارد، اعتماد متقابل را دچار فرسایش نگرداند و آسیب‌پذیری‌های احتمالی بیشتری برای اکوسیستم امنیت سایبر اتحادیه ایجاد ننماید (Dunn Cavelty 2013, 2014; Christou 2014). عنصر ساختاری مسلماً به‌واسطه ارتباط با بافتی که اتحادیه اروپا راهبرد خود را درون آن شکل می‌دهد و در یک جهان شبکه‌ای چندقطبی بر دیگران تأثیر می‌گذارد و محدودیت‌ها و فرصت‌هایی که از منظر اجرای چنین راهبردی وجود دارند که به شکلی اجتناب‌ناپذیر بر بستر ایجاد توازن میان حقوق و امنیت قرار دارند، بسیار اهمیت دارد. جنبه نهادی نیز هم از جهت تعاملات آن نهادهای مرتبط جهانی و سازمان‌های خصوصی فعال در عرصه امنیت سایبری و هم از جهت نقش نهادها و به‌خصوص آژانس‌های آن نظیر آژانس امنیت شبکه و اطلاعات اتحادیه اروپا و مرکز مقابله با جرائم سایبری اتحادیه اروپا در ایجاد امنیت تاب‌آور در فضای سایبری آن دارای اهمیت قابل‌توجهی می‌باشد. سؤالی که رویکرد قدرت سایبری، آن را بدون جواب می‌گذارد و این اثر پژوهشی در پی واکاوی آن می باشد، این بوده که کدام نوع از رویکردهای حکمرانی و پلتفرم‌ها و ابزارهای وابسته به آن می‌توانند به

بهترین شکل شرایط موردنیاز برای اتخاذ یک رویکرد امنیتی کارآمد نوظهور در اروپا را تسهیل نمایند؟

در این رابطه، پژوهش مولر[1] (۲۰۱۰) به دلیل استفاده از حکمرانی به‌عنوان عنصر اصلی تحلیل سیاست‌های جهانی اینترنت، اهمیت قابل‌ملاحظه‌ای دارد؛ اما بااینکه مولر در حقیقت صرفاً بر روی موضوعات امنیت سایبری تمرکز نمی‌کند، سؤال مفهومی مطرح‌شده توسط وی سؤالی جالب‌توجه است: با توجه با واقعیت تولید همتا (حکمرانی غیر سلسله‌مراتبی) یا شبکه‌های فراملی و کنترل دولت یا کشور (حکمرانی سلسله‌مراتبی) در بحث حکمرانی اینترنت به‌طور عام، در کدام عرصه می‌توان حوزه‌های مسائل و سیاست‌های مرتبط با اینترنت را تعیین کرد؟ وی در این راستا تلاش می‌کند حکمرانی شبکه‌ای را نظریه‌پردازی کرده و ادعا می‌کند این موضوع تنها در صورتی می‌تواند در تحلیل حکمرانی اینترنت مؤثر باشد که به شکلی دقیق و به‌عنوان نظریه اشکال سازمانی استفاده شود؛ به صورتی که با استفاده از آن قادر باشیم میان «خوشه‌بندی بازیگران سیاسی در شبکه‌های آزاد نفوذ حول نهادهای حکمرانی و شبکه‌ها به‌عنوان نوعی برساخته غیرآزاد سازمانی» تمایز قائل شویم (p.51 ,2010). وی در ادامه چهار شیوه که روابط شبکه‌ای می‌توانند منجر به تغییرات نهادی شوند را معرفی می‌کند: از طریق رسمی کردن و نهادینه ساختن روابط شبکه‌ای؛ از طریق تلاش‌های دولت‌ها برای تحمیل قواعد سلسله‌مراتبی بر اشکال مختلف شبکه‌ها؛ به‌واسطه بهره‌برداری دولت‌ها از روابط شبکه‌ای و انطباق با آن‌ها و درنهایت به چالش کشیدن سیاست تنظیم مجدد و توسعه خوشه‌های مرتبط حول نهادهای حکمرانی.

وی در بررسی این مفروضات در ارتباط با امنیت سایبری و با استفاده از مواردی چون ارسال هرزه نگاره‌ها و فیشینگ، ادعا می‌کند به‌رغم قوانین متعددی که در حوزه امنیت سایبری در اروپا و ایالات‌متحده و همچنین حقوق بین‌الملل نظیر کنوانسیون جرائم سایبری شورای اروپا[2] تصویب شده‌اند، «چنین باقی‌مانده‌های سلسله‌مراتبی تماماً در حال وابسته شدن به روابط شبکه‌ای تولیدات همتا می‌باشند و تأثیر آن‌ها رو به کاهش است ... کارگزاران سلسله‌مراتب ... باید ضمن

1. Mueller
2. Council of Europe's 'Convention on Cybercrime'

مشارکت به بخشی از شبکه اپراتورهای متعلق به ذی‌نفعان متعدد و میان حوزه‌های قضائی مختلف تبدیل شوند» (Ibid., p. 173). وی این‌طور نتیجه می‌گیرد که برخلاف امنیتی شدن خاص فضای سایبری توسط دولت ایالات‌متحده[۳] و تقاضا برای انواع سخت‌تر «قدرت سایبری» به‌منظور مقابله با اشکال معلق تهدیدات سایبری برخاسته از فضای سایبری، چنین اشکالی از قدرت نمی‌توانند مستقل از اشکال نرم‌تر، کنونی و در حال ظهور تولیدشده و فراملی وجود داشته باشند. در حقیقت موضوعی که به شکلی گسترده‌تر در رابطه با این استدلال جالب‌توجه است و البته با استدلالی که پیش‌تر در رابطه با قدرت سخت مطرح شد نیز همخوانی دارد، این است که نیاز به حفظ آزادی و فضای باز به‌منظور حفظ امنیت در این رویکرد نهفته است (Ibid., p. 180). به‌عبارت‌دیگر، امنیتی شدن فضای سایبری، درحالی‌که نیازمند تخصیص منابع و ابزارهای دیگری برای برخورد با خطرات است، اما می‌تواند استفاده از چنین تاکتیک‌هایی را برای تروریست‌ها و مجرمان سایبری نیز مشروعیت بخشد. این موضوع می‌تواند به ناامنی بیشتر فضای سایبری و نه تأمین امنیت فزاینده آن منجر شود.

درنتیجه رویکرد مولر را می‌توان برای تحلیل رژیم امنیت سایبری اتحادیه اروپا مناسب دانست. اکوسیستم امنیت سایبری اتحادیه اروپا سازنده بوده و سؤالات جالبی از ماهیت تعاملات میان آژانس‌های اتحادیه اروپا و شبکه و بازیگران دخیل در تولید صرف امنیت سایبری جهانی و در اروپا برمی‌خیزد. علاوه بر این، با پیشبرد تحلیل مولر، سؤالات مهمی پیرامون ماهیت منطق در حال ظهور تاب‌آوری و همچنین همکاری، هماهنگی و اعتماد مطرح می‌شوند که درصورتی‌که اتحادیه اروپا قصد دارد در ایجاد یک رویکرد مشترک به مسائل امنیت سایبری موفق باشد و پیشرفت نماید، باید به‌خصوص با در نظر گرفتن مشارکت عمومی–خصوصی به آن‌ها پاسخ گوید. فراتر از این موضوع لازم است سؤالاتی نه‌تنها در رابطه با نهادها و شبکه‌های حکمرانی پرسیده شود، بلکه باید به این موضوع نیز پرداخته شود که کدام‌یک از انواع مختلف حکمرانی در مسائل امنیت سایبری رایج‌تر هستند و ذیل چه شرایط سیاسی، حقوقی و فناورانه، آن‌ها می‌توانند اکوسیستم تاب‌آوری قابل انطباقی را برگزینند.

فهم اتحادیه اروپا در حوزه امنیت سایبری

اکوسیستم‌ها و تاب‌آوری

بخش حاضر پس از بررسی ادبیات مسلط حوزه امنیت سایبری، در ادامه با استفاده از مسئله مند کردن حکمرانی تاب‌آور و امنیت به استدلال و چارچوب مفهومی اصلی خود می‌پردازد. برای تأکید مجدد، استدلال پژوهش حاضر این بوده که چنین ادبیاتی بسیار مرتبط با فهم رویکرد و راهبرد امنیت سایبری در حال ظهور اتحادیه اروپا است؛ مفاهیم قدرت سایبری، منطق‌های امنیتی و حکمرانی دارای الزامات مهمی برای نوع تاب‌آور قابل‌دسترس می‌باشند. درنتیجه به بررسی عمیق‌تر تاب‌آوری و رابطه آن با حکمرانی امنیتی نیاز داریم تا بتوانیم یک چارچوب جامع برای درک مقوله‌ای که در سطح اتحادیه اروپا در حال تکامل است و شرایط لازم برای اینکه اتحادیه اروپا بتواند یک رویکرد امنیتی تاب‌آور توسعه دهد که سنگ بنای آن، ابزارها، وسایل و سازوکارهایی باشد که امکان دستیابی به یک فضای سایبری امن‌تر را برای اتحادیه فراهم سازد، تدوین نماییم.

ترکیب مفاهیم تاب‌آوری و حکمرانی امنیت برای ساخت و تثبیت یک رویکرد تاب‌آور به امنیت، اجازه خصوصیت پردازی اقدامات در حال ظهور حکمرانی امنیت در فضای امنیت سایبری اتحادیه اروپا و مهم‌تر اینکه چگونگی برابری این موضوع با دستیابی به انواع خاص تاب‌آوری را فراهم می‌سازد. بااینکه با توجه به ماهیت سازنده اکوسیستم امنیت سایبری اتحادیه اروپا (فعالیت‌هایی نظیر انتشار گزارش‌ها، انجام پژوهش، ایجاد ابتکارهای سیاستی، خلق سازوکارها، پلتفرم‌ها و نهادهای جدید)، تمرکزی قابل‌توجه بر موضوع خروجی این تحلیل‌ها وجود دارد، اما تحلیل خروجی این ارزیابی‌ها (تغییر رفتار) و تأثیر (تغییر نشانگرهای هدف نظیر کاهش در زمان سایبر) هر جا که عملی و محتمل باشد، مستثنا نخواهد شد (ن.ک. Szilecki et al. 2011, p.716).

به‌منظور توضیح بیشتر باید گفت درواقع یک راه‌حل حکمرانی که در بسیاری از گزارش‌های سیاستی ذکر شده و اقدامات نهادهای منطقه‌ای و جهانی درگیر در امنیت سایبری و جرائم سایبری را نیز شامل می‌شود، به مشارکت عمومی- خصوصی مربوط می‌شود (ن.ک. ENISA 2011d). اتحادیه اروپا برنامه مشارکت عمومی-خصوصی اتحادیه اروپا در تاب‌آوری و جایگزین آن، پلتفرم امنیت

شبکه و اطلاعات (ن.ک. فصل 6) را با اهداف مشابهی تأسیس کرد و همچنین برنامه مشارکت عمومی- خصوصی به‌عنوان یکی از چهار ستون اصلی تعاملات میان کارگروه امنیت سایبری و جرائم سایبری اتحادیه اروپا-ایالات متحده[1] نیز ایجاد شد. بااین‌حال به‌رغم اینکه رویکردهای قدرت سایبری دو مؤلفه همکاری و هماهنگی میان بازیگران مختلف را مهم ارزیابی می‌کنند، آن‌ها به‌منظور تعیین انواع مشارکت ممکن یا مطلوب یا هر آنچه می‌تواند شکل‌دهنده یک مشارکت مؤثر باشد فراتر از توضیحاتی در خصوص اعتمادسازی و همکاری‌های متقابل گام برنمی‌دارد. علاوه بر این، بااینکه تاب‌آوری به‌عنوان یک مؤلفه پیشرو در توسعه امنیت سایبری و حفاظت اطلاعات مطرح می‌شود، در رویکردهای علمی که در بخش پیش مرور شد، ظاهراً مسئله‌مند نمی‌شود[۴]. هیچ نوع مفهوم‌سازی در خصوص منطق حکمرانی امنیت و تاب‌آوری که باید درون بُعد اروپا تکامل یابد و برداشت آن‌ها از آمادگی، حفاظت، شناسایی، واکنش و بازیابی، دیده نمی‌شود. در حقیقت چنین مسئله‌مند کردن و مفهوم‌سازی در اقدامات و فعالیت های آژانس‌های سیاست‌گذاری اتحادیه اروپا نظیر آژانس امنیت شبکه و اطلاعات اتحادیه اروپا و همچنین سازمان‌های بین‌المللی نظیر سازمان همکاری اقتصادی و توسعه[2] و سازمان ملل متحد (شورای اجتماعی اقتصادی[3] و اتحادیه بین‌المللی مخابرات) مشهودتر بوده است.

آژانس امنیت شبکه و اطلاعات اتحادیه اروپا از زبان اکوسیستم‌های طبیعی با رجوع به ارتباطات متقابل اینترنتی استفاده و به مهندسی و سیستم‌های بیولوژی نیز اشاره کرده و در ادامه تاب‌آوری را «توانایی ارائه و حفظ سطحی قابل‌قبول از خدمات در شرایط خطا و چالش‌ها نسبت به شرایط فعالیت معمولی» تعریف کرده است (ENISA 2011c, p.10). نقطه شروع این کتاب که از ادبیات موجود این حوزه نیز نشئت می‌گیرد، درواقع استفاده از استعاره اکولوژیک به‌منظور درک فضای سایبری به‌عنوان اکوسیستم در حال تکامل دارای توانایی خودتنظیمی می‌باشد (Holling 1973; Walker and Cooper 2011). این مفهوم از اکولوژی بیان می‌کند که اکوسیستم‌های به‌هم‌پیوسته و به هم متصل از توانایی تغییر و انطباق در شرایط

1. EU-US Working Group on cybersecurity and Cybercrime
2. Organisation for Economic Cooperation and Development (OECD)
3. Economic and Social Council
4. International Telecommunications Union (ITU)

وارد آمدن ضربه ناگهانی برخوردار هستند (Brassett and Vaughan-Williams 2015). تاب‌آوری در اکوسیستم‌ها از طریق ادبیات نظری انتقادی موردبررسی قرار گرفته است (Lentzos and Rose 2009; Walker and Cooper 2011; Brassett and Vaughan-Williams 2015) که در پی شالوده شکنی و سؤال پیرامون چگونگی و چرایی مطرح‌شدن تاب‌آوری به‌عنوان راه‌حل برخی مسائل است و در ادامه با نوعی ادبیات پژوهشی مواجه هستیم که در پی تعمیق شناخت ما از انواع و منطق تاب‌آوری می‌باشد. هدف در اینجا نادیده گرفتن مؤلفه‌های حیاتی[۵] که شامل سؤالاتی در رابطه با انطباق‌پذیری منطق‌هایی خاص از تاب‌آوری و حکمرانی و برای مثال قرار گرفتن تاب‌آوری و انطباق‌پذیری در برابر کارایی است، نمی‌باشد. درعین‌حال، این رویکرد در درجه اول به دنبال پرداختن به گونه‌شناسی‌های کنونی از تاب‌آوری است تا بتواند نخست منطق ورای حکمرانی امنیت که ممکن است سبب تقویت آن شود را بررسی نماید و دوم ارائه ایده‌ای در رابطه با میزانی که تولید خروجی‌هایی خاص از تاب‌آوری در اتحادیه اروپا ممکن است ارائه نمایند. البته نباید تصور کرد که این نوع گونه‌شناسی‌ها ثابت، کامل و یا غیرقابل مخالفت هستند بلکه هدف، فراهم نمودن یک فهرست سیال از نشانگرهای مفهومی است که بتوان بر اساس آن ارزیابی‌هایی مرتبط با تغییرات و خروجی‌ها را انجام داد.

البته تمرکز بر فضای سایبری به‌عنوان یک اکوسیستم طبیعی، نامتناسب با ملاحظات مرتبط با سیاست‌های تاب‌آوری در حوزه امنیت سایبری نیست؛ در حقیقت استعاره اکولوژی از دو منظر علوم طبیعی و اجتماعی تکامل یافته و خود را به‌عنوان راهی برای درک تاب‌آوری در چارچوب اکولوژی یا اکولوژی تاب‌آوری (Holling 1973) مطرح ساخته است. به‌طور خاص، مفهوم تاب‌آوری اکولوژیک که به‌عنوان جایگزینی برای مفهوم تاب‌آوری مهندسی تدوین یافت، درواقع متغیری انتزاعی است که به اکولوژی ریاضی مرتبط است و نشان‌دهنده میزان زمانی (t) است که یک سیستم پس از اختلال به بالاترین شرایط ثبات خود (یا شرایطی مشابه) بازمی‌گردد. این بازگشت صرفاً به‌عنوان مفروض بوده و وضعیت تعادل به‌عنوان معادلی برای مقاومت بلندمدت در نظر گرفته می‌شود (Walker and Cooper 2011, p.146). ازنظر هولینگ [۱]، چنین رویکرد مدیریتی به موضوع

1. Holling

تاب‌آوری مسئله‌مند بود، البته صرفاً بدین خاطرنبود که بر اساس مفهوم دانش پیش‌بینی‌کننده و این مفروضه که رویدادهای آتی قابل‌انتظار هستند، استوار بود. هولینگ بجای ارائه یک تعریف ریاضی یا کمّی (Grimm and Calabrese 2011, p.7)، به دنبال برجسته‌سازی مفهومی دقیق‌تر از تاب‌آوری است که فراتر از ثبات می‌رود و به معادله بازمی‌گردد و همچنین بر پایایی روابط درون اکوسیستم تأکید دارد. نکته مهم اینجاست که هولینگ منتقد آن بخش از مفروضات رویکرد مدیریتی بود که رویدادهای آتی را قابل پیش‌بینی می‌دانست و در عوض استدلال می‌کرد که «چارچوب تاب‌آوری نیازمند ظرفیتی دقیق برای پیش‌بینی آینده نیست، بلکه تنها نیازمند ظرفیتی کیفی برای ایجاد سیستم‌هایی است که رویدادهای آتی را به هر شکل غیرمنتظره‌ای که رخ دهند جذب کرده و در خود جای دهند» (Holling 1973, p.21).

چنین برداشتی از تاب‌آوری و سهم آثار بعدی هولینگ در گسترش ادبیات مدیریت انطباقی اکوسیستم نه‌تنها طرفداران و پیروان زیادی برای وی به همراه داشت، بلکه به‌واسطه اجماع و همکاری، به شکل‌گیری ائتلاف تاب‌آوری و ارائه تعاریف دقیقی از آن بر اساس ایده‌های وی نیز انجامید (ن.ک. Brassett and Vaughan-Williams 2015). در حقیقت مفهوم تاب‌آوری اکولوژیک گسترش یافت تا نه‌تنها قدرت و استقامت سیستم‌ها را نیز در نظر بگیرد، بلکه مؤلفه‌هایی چون تاب‌آوری اکولوژیک با تمرکز بر ظرفیت انطباقی، انتقال‌پذیری، یادگیری و نوآوری را نیز شامل شود (Brand and Jax 2007; De Bruijne et al. 2010, p.19). نکته مهم و برجسته بین این رویکردها و بحث تاب‌آوری و نقطه اشتراک آن‌ها درواقع تأکید هر دو بر مفهوم اکولوژی به‌عنوان مجموعه‌ای از روابط و به‌عنوان سیستمی مشروط و مخاطره‌آمیز می‌باشد. این موضوع در بحث تحلیل امنیت سایبری و درجایی که لایه‌های فنی یا علمی و اجتماعی یا سیاسی به شکلی اجتناب‌ناپذیر با درون یک اکوسیستم مرتبط هستند و در جایی که روابط میان لایه‌ها باید به شکل دستی تقویت شود تا به تاب‌آوری انطباقی و کارآمدی دست پیدا کرد، بسیار حائز اهمیت و حیاتی است.

علاوه بر این، پیوند آشکاری میان مفهوم گسترده تاب‌آوری و مفروضات نظریه نظام پیچیده وجود دارد که بر خصوصیات نظام‌های باز و انطباقی، منطق غیرخطی، پیش‌بینی پذیری(ناپذیری)

محدود و محدودیت‌های قابل‌توجه در دانش و پیشرفت به دلیل عدم قطعیت تأکید می‌کند (Kavalski 2009, p.532). نکته مهم اینجاست که «این بسترهای سیال، مرزهای ریخت شناختی و اجتماعی کنونی را نمی‌پذیرند و ممکن است مانند گلبول‌های سفید خون از طریق دیواره‌ها به ماده اطراف خود نفوذ کرده و عواقبی غیرقابل‌پیش‌بینی در آن ایجاد نمایند». این ویژگی غیرخطی بودن به این معناست که یک فضای سیال جهانی مانند فضای سایبری نمی‌تواند به‌سادگی از هم جدا شود یا رفتار آن به‌سادگی قابل پیش‌بینی باشد و نه تماماً اجتماعی و یا صرفاً دارای دیدگاه سازوکاری مشابه فضای سایبری بوده که به میزان کافی تجربیات و فعالیت‌های آن را ضبط کرده باشد. فضای سایبری در هرزمانی برآورد مونتاژ و سرهم‌بندی بازیگران متعددی است که روابط آن‌ها به طور کامل شکل نگرفته است (Betz and Stevens 2012, p.38).

پس موضوعی که این نکات به آن اشاره می‌کنند و برای چارچوب‌بندی این پژوهش و استدلال مطرح‌شده در آن نیز مهم است، درواقع نوعی مفهوم‌سازی پیچیده‌تر از حکمرانی امنیت یا امنیت تاب‌آور است (Kavalski 2009, p.532) که نه‌تنها درصدد تعیین سازوکارهای مناسب دولتی برای امنیت سایبری می‌باشد، بلکه درکی از سازوکارها، روابط، ویژگی‌ها و فرآیندهایی که می‌توانند به تاب‌آوری کارآمد بینجامند را نیز به دست می‌دهد؛ موضوعی که در اینجا درونِ حوزه امنیت سایبری اتحادیه اروپا قرار دارد. مفاهیم حکمرانی امنیت به شکلی نزدیک با انواع تاب‌آوری گره خورده‌اند و تلاشی با هدف دوری جستن از مفاهیم حکمرانی امنیت به‌عنوان «امنیت کنترل» که صرفاً بر تغییرات درون و میان سیستم‌ها تمرکز دارد، شروع شده است (Weber et al. 2004, Webber 2007; Kirchner and Sperling 2007a, 2007b; Hal-lenberg et al. 2009) که درنتیجه احتمال ظهور اکوسیستم تاب‌آور را مستثنا می‌سازد (De Bruijne et al. 2010)؛ و نوعی از تاب‌آوری است که امکان تغییر در سیستم‌ها و ظهور رژیم‌های انطباقی جدید را میسر می‌سازد. چنین نوعی از تاب‌آوری، کنش‌گر و نه واکنش‌گر است و غیرقابل‌اجتناب بودن تغییر را در عوضِ مقاومت در برابر آن و همچنین ایجاد یک سیستم «که قادر به انطباق با شرایط و الزامات جدید باشد» می‌پذیرد. از سوی دیگر، تاب‌آوری واکنشی، بر تقویت وضع موجود و مقاومت در برابر تغییر به‌منظور دستیابی به ثبات و تداوم درون

اکوسیستم تأکید دارد (Handmer and Dovers 1996, p.494).

چنین انواعی از گونه‌شناسی هرچند که نماینده سر حدات بر روی طیف تاب‌آوری هستند، اما نقاط شروع مناسبی برای تسهیل فهم ما از اکوسیستم نوظهور حکمرانی امنیت سایبری تاب‌آور درون اتحادیه اروپا به‌شمار می‌آیند. این گونه‌شناسی‌ها می‌توانند طیفی از واکنش‌های محتمل به انواع مختلف چالش‌ها، خطرات و حملات امنیتی در فضای سایبری ارائه نمایند (کوچک‌مقیاس، متوسط و عظیم) و مهم‌تر اینکه می‌توانند به ما در تعیین خصوصیات چگونگی تکامل اکوسیستم درونی اتحادیه اروپا، الزامات آن بر مبنای نوع بازیگران، فرآیندها و سازوکارها و همچنین روابط و ساختارهای نهادی کمک نمایند. همچنین امکان ایجاد مفروضات و چارچوبی که با هدف فراهم کردن بینش، جهت، نقاط قوت و ضعف هر عملی قابل آزمون باشند را مهیا می‌سازد. هندمر[1] و داورز[2] (۱۹۹۶) به این منظور، یک طبقه‌بندی سه‌گانه از تاب‌آوری ارائه دادند که می‌تواند با توجه به اهداف مخصوص این کتاب توسعه هم بیابد: مقاومت و نگهداری (نوع اول)؛ تغییر در حاشیه‌ها (نوع دوم)؛ جریان باز و انطباق‌پذیری (نوع سوم). در حقیقت با استفاده از چنین چارچوبی و توسعه مبانی حکمرانی و امنیتی می‌توان به مفهومی موسع‌تر ازآنچه برای دستیابی به تاب‌آوری و انطباق‌پذیری لازم (نوع سوم از تاب‌آوری، ن.ک. مبحث بعدی) –فنی و سیاسی– به‌منظور پرداختن به تهدیدات غیرمنتظره لازم است، دست یافت. رویکرد اتخاذشده به‌واسطه فراهم کردن سنگ محک‌هایی که بتوان ویژگی‌های کنونی و آتی اکوسیستم امنیت سایبری اتحادیه اروپا را سنجید، می‌تواند با توجه به نوع خروجی‌های احتمالی به شکل کامل و جامع مورد تحلیل و نقد قرار گیرد.

گونه‌شناسی تاب‌آوری که توسط هندمر و داورز (۱۹۹۶) ارائه شده دارای ارتباط نزدیکی با تفاسیری است که پیش‌تر موردبررسی قرار گرفتند. این گونه‌شناسی‌ها باید موردپذیرش و تدقیق قرار گیرند تا فضای امنیت سایبری اتحادیه اروپا به‌خوبی تحلیل شود، چراکه هندمر و داورز (1996, p.495) چنین گونه شناسی‌هایی را در سطح عمومی به بحث می‌گذارند. از طرفی، هر نوع این‌چنینی از گونه‌شناسی باید به‌منظور اضافه کردن جزئیاتی به سازوکارها و فرآیندهای

1. Handmer
2. Dovers

احتمالی حکمرانی امنیتی مورد بسط و گسترش قرار گیرند؛ این موضوع باید به‌طور خاص با توجه به رابطه میان بازیگران عمومی و خصوصی به شکل مشارکت که در کنار مدیریت ریسک پیش‌بینی محور، رویکردهای جامع به فراهم کردن تاب‌آوری درون اتحادیه اروپا بوده‌اند، انجام گیرد (ENISA 2011d, p.25; Schoon 2010).

ویژگی برجسته تاب‌آوری نوع اول را باید حکمرانی، حکومت سلسله‌مراتبی، کنترل دولتی منابع و اطلاعات، مقاومت در برابر تغییر و تأکید بر حفظ وضع موجود از طریق سرمایه‌گذاری منابع و تمایل به نادیده گرفتن دانست. این بدان معناست که در مورد امنیت سایبری، آن بازیگران (دولتی یا غیردولتی) برخوردار از قدرت ممکن است این‌طور استدلال کنند که خطرات بزرگنمایی می‌شوند و بدین ترتیب خواستار شواهد بیشتری برای اثبات آن می‌شوند. علاوه بر این، چنین تاب‌آوری‌ای به دلیل تأکید آن بر ثبات و قطعیت، توانایی واکنش و انطباق با رویدادهای غیرقابل‌پیش‌بینی یا شرایط جدید را ندارد. البته این نبود تاب‌آوری می‌تواند نکات مثبت خاص خود را داشته باشد که ازجمله می‌توان به حفظ ظرفیت نهایی و ساختارهای کنونی قدرت در کوتاه‌مدت، به‌خصوص برای آن‌ها که از دست دادن قدرت برای آن‌ها مطلوب نیست، اشاره داشت. بااین‌حال سؤال اینجاست که آیا این نوع تاب‌آوری در میان‌مدت تا بلندمدت پایدار می‌ماند یا خیر؟ ممکن است ادعا شود که چنین نوعی از تاب‌آوری می‌تواند به ایجاد حکمرانی امنیتی پایدار منجر شود؛ از سویی پایدار است و می‌تواند جریان را به دست بگیرد و در صورت فروپاشی نیز می‌تواند به نظمی کاملاً نوین بینجامد. از سویی این احتمال هم وجود دارد که چنین ساختاری به ایجاد آسیب‌های غیرقابل‌بازگشت با عواقب اجتماعی، اقتصادی و سیاسی بینجامد و در بدترین سناریوی ممکن نیز سبب فروپاشی کامل یک اکوسیستم شود بدون اینکه توانمندی و ظرفیتی برای بازسازی مجدد آن باقی بماند (Handmer and Dovers 1996, p.495-499).

نوع دوم تاب‌آوری عموماً مشابه رویکردهایی است که با هدف مدیریت ریسک اتخاذ می‌شوند (که سنگ بنای آن روش سنتی خطی ارزیابی خطر است). البته به این موضوع نیز اعتراف می‌شود که مشکلاتی می‌توانند وجود داشته باشند و تغییر نیز به‌منظور پایدارتر شدن سیستم ضروری است. این روش درواقع، رویکردی حل مسئله است که مشخصه آن گفتگو و اصلاحاتی است که

به انتقال‌پذیری منجر نمی‌شوند، اما تغییراتی در سیاست‌ها ایجاد می‌نمایند که خروجی‌ها را در حاشیه‌ها تحت تأثیر قرار می‌دهند. نتیجه این موضوع این است که هیچ نوع تغییرات کلی با توجه به استانداردها و پروتکل‌های حقوقی و فنی یا قوانین و مقررات جهانی رفتار در محیط اینترنت که می‌توانند به انطباق فرهنگی اجباری (ابزاری) و نه حکایت گونه (انتقالی) منجر شوند، شکل نمی‌گیرد (Boyden 1987, p.24). بااینکه می‌توان ادعا کرد چنین رویکرد حل مسئله‌ای می‌تواند به شناسایی مشکلات و تمهیدات سیاسی برای حل‌وفصل آن‌ها بینجامد، اما عموماً توسط منطق کارایی کوتاه‌مدت و روش‌های خطی پیش می‌روند و درنتیجه هر نوع تغییر خفیفی که اتفاق می‌افتد دارای حداقل تأثیر بر علت آن است.

علاوه بر این، چنین تغییرات اندکی می‌توانند این احساس را ایجاد نمایند که موضوعی توسط بازیگران و نهادهای دخیل در اکوسیستم در حال انجام است؛ به‌خصوص به این دلیل که دستورکار (و همچنین ساختارهای قدرت) به‌رغم افزایش سازوکارهای مشارکت‌کننده، هنوز تحت کنترل دولت هستند. درعین‌حال چنین تغییرات خفیفی ممکن است تاخیراتی در برابر هر نوع تغییرات انتقالیِ بزرگ و نوآورانه که به‌خصوص برای حفظ تاب‌آوری در اکوسیستم‌های پیچیده لازم هستند، به وجود بیاورند. چنین رویکردی آشکارا توسط ساختارهای سیاسی نهادینه شده که اجزاء بومی آن‌ها به منافع کوتاه‌مدت و نه بلندمدت علاقه دارند، محدود شده است. این موضوع باعث می‌شود رویکرد تدریجی به تنها گزینه واقعی و مطلوب تبدیل شود. یک موضوع دیگر و مرتبط با تغییرات قابل‌ملاحظه‌ای که در نوع دوم تاب‌آوری رخ می‌دهد، این است که چه کسی از این تغییرات منتفع می‌شود. این سؤال در موضوع امنیت سایبری با توجه به اینکه هر نوع حمله مرتبط با امنیت سایبری یا جرائم سایبری می‌تواند نه‌تنها نخبگان بخش‌های عمومی و خصوصی، بلکه جامعه مدنی و شهروندان را تحت تأثیر قرار دهد، حائز اهمیت است. تاب‌آوری نوع دوم را شاید بتوان رایج‌ترین واکنش به تهدید و خطر دانست؛ این رویکرد را عملگرا و متوازن تصویر می‌کنند و به‌عنوان مطلوب‌ترین گزینه از جنبه اقتصادی و سیاسی معرفی می‌شود. بااینکه این موضوع بدون شک در کوتاه‌مدت سودمند است، اما این رویکرد بهره‌وری‌محور متمرکز بر بازار و انتخاب‌های فردی، ازلحاظ سیاسی دارای تضادهایی با یک راه‌حل امن، انتقالی و بلندمدت

تاب‌آوری است (Handmer and Dovers 1996, p.499-501). این تنش میان کارایی و تاب‌آوری کوتاه تا بلندمدت به‌شدت با ایجاد تاب‌آوری پایدار و مداوم در تضاد قرار می‌گیرد (ENISA 2011c, p.13).

تاب‌آوری نوع سوم با ویژگی‌هایی نظیر توانایی و آمادگی انطباق با مفروضات عملیاتی پایه‌ای و ساختارهای نهادی جدید شناخته می‌شود (Handmer and Dovers 1996, p.502)؛ از جنبه حکمرانی نیز این نوع تاب‌آوری از احتمال بیشتری برای ایجاد تغییرات قابل‌توجه در روابط قدرت، مشارکت و جامعیت برخوردار است (این رویکرد خودسازماندهی‌شده و غیرسلسله‌مراتبی است). برخلاف رویکرد اول که در برابر تغییرات مقاومت می‌کرد، بازیگران دخیل در این رویکرد ممکن است ایده‌های جدید را بپذیرند و تغییرات قابل‌توجهی را اجرایی کنند تا اکوسیستمی را ایجاد نمایند که میزان آسیب‌پذیری را کاهش دهد. در موضوع امنیت سایبری می‌توان نوعی اکوسیستم را شکل داد که متنوع و دارای ظرفیت فضایی بوده و مفروضه زیربنایی آن نیز رها کردن کارایی به نفع پیچیدگی مفروضات عملیاتی است تا بدین طریق از نقاط منفرد تهدید و شکست پرهیز شود. چنین تغییرات دارای ماهیت انتقالی از جنبه‌های عملیاتی، ساختاری یا فرهنگی به‌سادگی قابل‌دستیابی نیستند، چراکه شامل شیوه‌های جدیدی برای انجام امور و دارای الزامات و دلالت‌هایی برای منافع تثبیت‌شده و روابط میان بازیگران مختلف فضای سایبری است. این موضوع حتی با توجه به اینکه تمامی دولت‌ها (یا بازیگران غیردولتی) دارای رویکردی مشابه به مقوله امنیت سایبری هستند و اینکه تنش‌های بسیاری در فضای سایبری میان طرفداران آزادی به‌عنوان امنیت و از سوی دیگر امنیت بیشتر یا (امنیتی شدن) برای حفظ آزادی (اغلب دولت‌ها) وجود دارد، پیچیدگی‌های بیشتری نیز پیدا می‌کند. علاوه بر این در حوزه‌هایی چون حفاظت از زیرساخت‌های حیاتی اطلاعات و امنیت اسامی دامنه‌ها که اغلب نیز حوزه‌هایی هستند که منافع یا بازیگران خصوصی بر آن غالب بوده یا در اجرایی شدن فناوری‌ها یا سیستم‌های جدید صاحب نفوذ هستند و همچنین حوزه‌ای که نوعی منطق اقتصادی یا هزینه‌ای برای انجام آن وجود دارد، طرح ایده‌های واقعاً متحول کننده، بسیار دشوار است.

به‌رغم وجود موانع و محدودیت‌های بسیار بر سر راه تغییر، رویکرد تاب‌آوری نوع سوم به شکل ضمنی بیان و البته تا حدی زیادی بر آن تکیه می‌کند که ائتلاف بازیگرانی که با هم فعالیت و در قالب یک مشارکت برای ساختن نهادهای جدید و تاب‌آور و رویه‌های عملیاتی کار می‌کنند، دستورکار گفتمانی و سیاست‌ها را تعیین می‌کند. در این روش، این نوع از تاب‌آوری به‌عنوان محتمل‌ترین شیوه برای نه‌تنها پرداختن به نشانه‌ها تلقی می‌شود، بلکه دلایل ریشه‌ای مشکلات امنیت سایبری در سطوح فردی و نهادی نیز در همین قالب بررسی می‌شوند. تاب‌آوری نوع سوم ممکن است دارای جنبه‌هایی منفی چون هزینه‌ها و ناکارآمدی‌های فزاینده ناشی از تنوع نیز باشد؛ اما چنین تنوع و پیچیدگی فزاینده ناشی از آن می‌تواند این تضمین را ایجاد کند که هر نوع اکوسیستمی می‌تواند از طریق انتخاب مجموعه‌ای از گزینه‌ها و دستورالعمل‌ها تغییر کند یا با شرایط جدیدی انطباق یابد. به همین شکل، به دلیل پیچیدگی و ناتوانی این رویکرد در پیش‌بینی و برآورد تهدیدات و خطرات محتمل، امکان تغییرات غیرقابل انطباقی وجود دارند که احتمال عواقب منفی آن‌ها در کوتاه‌مدت بالا می‌باشد. در حقیقت و البته همان‌طور که ویلداوسکی[1] (۱۹۹۸) بیان می‌کند، «تصمیم‌گیران ساختار قدرت باید به شکلی فزاینده بر راهبردهای ریسک‌پذیر و تاب‌آور تصمیم‌گیری که امکان آزمون‌وخطا و یادگیری را فراهم می‌نمایند، تکیه کنند؛ چراکه ظرفیت جامعه در پیش‌بینی ریسک و خطر نمی‌تواند خود را همپای پیچیدگی و دینامیسم رو به رشد جهانی که در آن زیست می‌کنیم، به‌پیش ببرد» (De Bruijne et al. 2010, p.22). علاوه بر این، این موضوع از طریق اتخاذ طیف متنوعی از راهبردها قابل حصول است که علاوه بر کشسانی ساختاری که پیش‌تر بدان پرداختیم، شامل روابط با عملکرد بالا میان طرف‌های ذی‌نفع مرتبط و یک فرهنگ اعتمادپذیری و بهبود عملکرد نیز می‌باشد. سازمان‌ها و نهادها درصورتی‌که واقعاً خواهان افزایش ظرفیت خود در تطبیق با شرایط مختلف هستند، باید بیاموزند که چگونه یاد بگیرند (De Bruijne et al. 2010, p.23) و برخلاف نوع محدود حالات دفاعی ذیل رویکردهای سنتی پیش‌بینی ریسک، این رویکرد نیازمند دانش، ارتباطات، ثروت و ظرفیت سازمانی و منابعی است که تا چیزی را که

1. Wildavsky

می‌خواهیم برای خود بسازیم و هر جا که بدان نیاز داریم آن را به دست آوریم، هرچند که ممکن است هیچ ایده‌ای در این رابطه که آیا واقعاً بدان مقوله نیاز داریم یا خیر نیز نداشته باشیم (Widavsky 1995, p.433).

امنیت و حکمرانی

در اینجا باید این سؤال را مطرح کرد که آیا گونه شناسی مذکور می‌تواند بسترهای لازم را برای دستیابی به اهداف این کتاب که درواقع ارزیابی اکوسیستم نوظهور تاب‌آوری حکمرانی امنیتی است، فراهم سازد؟ همان‌طور که دان کاولتری(2013 , p.6)بیان می‌کند، «اگر تاب‌آوری را مفهومی مرکزی در نظر بگیریم، در این حالت امنیت به نبود خطر اشاره نمی‌کند، بلکه به توانایی یک سیستم به‌منظور سازماندهی مجدد با هدف تحدید یک رویداد بالقوه فاجعه‌آمیز اشاره دارد». در این بافت، گونه‌شناسی انواع تاب‌آوری باعث می‌شود نشانگرهای خاص امکان درک برخی ویژگی‌ها و روابط در حال ظهور را در چنین اکوسیستم‌هایی و مهم‌تر از آن، نوع تاب‌آوری ساخته‌شده را برای ما فراهم نمایند. این موضوع همچنین امکان ترسیم دقیق شرایط عمومی موردنیاز را برای ظهور سیستم‌های به‌شدت تاب‌آور امنیتی فراهم می‌سازد (کادر ۲-۱) این موضوع در بازگشت به این دلیل که قادر است نوع پدیده در حال ظهور را از جنبه‌های دقیق اشکال، روش‌ها، سازوکارها و بازیگران حکمرانی تمیز دهد، دارای اهمیت فزاینده می‌باشد. این دقیقاً جایی است که ادبیات حوزه تاب‌آوری جوابگو نیست و ادبیات گسترده‌تر حکمرانی و حکمرانی خاص امنیتی می‌تواند در توضیح انواع منطق‌های در حال ظهور امنیتی و حکمرانی در ابعاد مختلف اکوسیستم امنیتی اتحادیه اروپا، مثمر ثمر باشد.

کادر ۲-۱. شرایط دست‌یابی به امنیت تاب‌آور کارآمد در فضای سایبری

• توانایی (شامل منابع و احکام) و آمادگی برای اتخاذ تصدی‌های عملیاتی پایه‌ای و ساختارهای نهادی جدید
• پذیرش کارآمدی که به نفع پیچیدگی‌های منطق‌های حکمرانی با هدف اجتناب از نقاط تهدید و شکست منفرد، چشم‌پوشی شده بود
• ائتلاف بازیگران در قالب همکاری در «مشارکت‌ها» مبتنی بر اعتماد برای تبادل اطلاعات، ساخت نهادهای منعطف و انطباق پذیر جدید و رویه‌های عملیاتی، تعیین دستورکار و تدوین/اجرای سیاست‌ها
• همگرایی میان ذینفعان در خصوص فهم، منطق(ها)، «هنجارها، قوانین و استانداردهای «مشترک» در حوزه امنیت تاب‌آور
• تکامل فرهنگ امنیت سایبری در تمام سطوح و لایه‌ها (فنی، حقوقی، سیاستی) در میان ذینفعان (آگاهی، آموزش، یادگیری و...)
• رویکردی یکپارچه (منسجم و پیوسته در لایه‌ها، سطوح و بازیگران)

بااین‌حال مشکل رویکرد سنتی حکمرانی امنیت این است که حکمرانی را در بافت پیچیدگی توسعه نمی‌دهد (Schneider 2012, p.130) و درنتیجه دیدگاه‌هایی محدود نسبت به حکمرانی کلان[۶] روابط بازیگران عمومی و خصوصی ارائه می‌دهد (Caveltry 2008b; Shore et al. 2011). درنتیجه لازم است به معانی دقیق مشارکت در رابطه با بازیگران دخیل یا انواع گوناگون حکمرانی که می‌توان به‌واسطه آن‌ها به اشکال تاب‌آور امنیت دست یافت (سلسله‌مراتبی، غیر سلسله‌مراتبی یا سخت/نرم) پرداخته شود؛ موضوعی که با توجه به تنوع طرف‌های ذی‌نفع در فضای سایبری و مهم‌تر از آن، با توجه به مشارکت عمومی–خصوصی به‌عنوان یکی از سازوکارهای اصلی حکمرانی برای پرداختن به موضوعات امنیت سایبری با در نظر گرفتن ماهیت جهانی آن اهمیت بالایی دارد. به این نکته توجه داشته باشید که هدف در اینجا تجویز در مورد ترکیب مناسب از حکمرانی کلان برای دستیابی به شرایط امنیت تاب‌آور نیست (نوع سوم). هرچند که نوع سوم تاب‌آوری دارای برخی ویژگی‌های خاص کلی است، اما یک سؤال مجدداً تجربی برای ارزیابی اکوسیستم امنیت سایبری اتحادیه اروپا در خود دارد. در حقیقت هنوز بحث‌های فراوانی در رابطه با -اینکه چه نوع توازن عمومی–خصوصی باید برای سیستم‌های نوظهور به‌شدت تاب‌آور درون اتحادیه اروپا مناسب‌تر است، وجود دارد.

از طرف دیگر پرداختن دقیق به موضوع مشارکت‌های در حال ظهور میان بخش‌های عمومی و خصوصی و الزامات و مفهوم آن برای امنیت سایبری تاب‌آور در اتحادیه اروپا نیز برای اثر قرار

از اهمیت بالایی برخوردار است. این موضوع مستلزم حرکت ورای نظام‌های فراحکمرانی مطرح در ادبیات سنتی حکمرانی امنیت و سطوح منطقه‌ای، جهانی و جهان پساوستفالیایی است (Hallenberg 2009, p.8) تا بدین ترتیب جنبه‌هایی از ویژگی‌های شکلی و کارکردهای محتمل آن‌ها مشخص شود. هدف ارائه فهرستی خسته‌کننده از اسامی و گونه‌ها نیست، بلکه هدف فهرست از طرف دیگر پرداختن دقیق به موضوع مشارکت‌های در حال ظهور میان بخش‌های عمومی و خصوصی و الزامات و مفهوم آن برای امنیت سایبری تاب‌آور در اتحادیه اروپا نیز برای اثر حاضر از اهمیت بالایی برخوردار است. این موضوع مستلزم حرکت ورای نظام‌های فراحکمرانی مطرح در ادبیات سنتی حکمرانی امنیت و سطوح منطقه‌ای، جهانی و جهان پساوستفالیایی است (Hallenberg 2009, p.8) تا بدین ترتیب جنبه‌هایی از ویژگی‌های شکلی و کارکردهای محتمل آن‌ها مشخص شود. هدف ارائه فهرستی خسته‌کننده از اسامی و گونه‌ها نیست، بلکه هدف فهرست بندی رویکردهایی خاص و مشخصه‌های مشترک مشارکت به‌منظور کمک در درک و تدقیق به‌واسطه ارزیابی منسجم اقدامات گوناگون و سنجش اتفاقاتی است که به‌طور خاص درون اکوسیستم امنیت سایبری اتحادیه اروپا رخ می‌دهند. شوور[1] و همکاران (2011 , p.6-7) فهرستی از سه رویکرد همکاری عمومی-خصوصی ارائه می‌دهند که برای اثر حاضر حاضر مفید فایده هستند. نخست، فراحکمرانی هویت‌ها یا نیروهای بازار است. این رویکرد بستر مناسب را برای منطقی روشن به‌منظور مشارکت بخش خصوصی فراهم ساخته است. شفافیت در این مورد که کدام بازیگران خصوصی مسئول ارائه خروجی‌ها هستند و دیگر ویژگی‌های آن تعریف صریح اهداف و وظایف و شروع مشارکت همکاری جویانه میان دولت و صنعت است. یکی از نقدهای احتمالی به این رویکرد خودتنظیم کننده و صنعت خصوصی محور این است که خروجی‌های بالقوه منفی به‌خصوص، در رابطه با امنیت سایبری و درصورتی‌که منطق راهنمای بازار و سودآوری بر آن حاکم باشد، در مواقع بحران اقتصادی مورد بزرگنمایی قرار می‌گیرد. چارچوب‌بندی رویکردهایی خاص و مشخصه‌های مشترک مشارکت به‌منظور کمک در درک و تدقیق به‌واسطه ارزیابی منسجم اقدامات گوناگون و سنجش اتفاقاتی است که به‌طور خاص

1. Shore

درون اکوسیستم امنیت سایبری اتحادیه اروپا رخ می‌دهند. شوور و همکاران (2011 , p.6-7) فهرستی از سه رویکرد همکاری عمومی-خصوصی ارائه می‌دهند که برای اثر حاضر مفید فایده هستند. نخست، فراحکمرانی هویت‌ها یا نیروهای بازار است. این رویکرد بستر مناسب را برای منطقی روشن به‌منظور مشارکت بخش خصوصی فراهم ساخته است. شفافیت در این مورد که کدام بازیگران خصوصی مسئول ارائه خروجی‌ها هستند و دیگر ویژگی‌های آن تعریف صریح اهداف و وظایف و شروع مشارکت همکاری‌جویانه میان دولت و صنعت است. یکی از نقدهای احتمالی به این رویکرد خودتنظیم‌کننده و صنعت خصوصی‌محور این است که خروجی‌های بالقوه منفی به‌خصوص، در رابطه با امنیت سایبری و درصورتی‌که منطق راهنمای بازار و سودآوری بر آن حاکم باشد، در مواقع بحران اقتصادی مورد بزرگنمایی و غلو قرار می‌گیرد.

رویکرد دوم به حکمرانی کلانِ بدون مداخله بازمی‌گردد که از ویژگی‌های اصلی آن می‌توان به تأثیر غیرمستقیم بر مشارکت به‌واسطه تغییر محیط اشاره داشت. این موضوع برای مثال می‌تواند از طریق ترتیبات همکاری‌جویانه (پلتفرم‌ها، شبکه‌ها، هیئت‌های مشاوره‌ای و سازوکارهای تک منظوره)، تسهیل شرایط از طریق حمایت از مشارکت و کمک به آن‌ها به‌منظور حرکت کارآمد، از طریق چارچوب‌هایی برای تعامل یا اعطای معافیت‌هایی از قوانینی که مانع همکاری‌های خصوصی هستند و سرانجام تحریک و انگیزش که می‌تواند با هدف افزایش مشارکت خصوصی به شکل محرک‌های اجتماعی یا اقتصادی درآید و می‌تواند داوطلبانه یا غیر داوطلبانه باشد (برای مثال در نظر گرفتن مزایایی برای آن دسته از تأمین‌کنندگان که تعهدات مندرج در مشارکت‌ها را رعایت می‌کنند).

رویکرد سوم به حکمرانی کلانِ عملگرایانه بازمی‌گردد و از ویژگی‌های آن نفوذ مستقیم بیشتر از بخش عمومی است. درنتیجه نفوذ ممکن است به شکل مشارکت بخش عمومی درآید که از طریق تسهیل و اداره شبکه‌های همکاری‌جویانه اعمال می‌شود؛ در این رویکرد، تأثیرگذاری و نظارت بر فعالیت‌های بخش خصوصی از طریق سازوکارهای حقوقی و غیرحقوقی اتفاق می‌افتد؛ هزینه‌ها کاهش می‌یابند و تنش‌ها میان بازیگران خصوصی خنثی می‌شود. یکی از نقدهای جدی وارده به این رویکرد بالا به پایین را می‌توان تضاد بالقوه میان منافع دانست که می‌تواند

به ایجاد تنش بین بازیگران بخش عمومی به‌عنوان قانون‌گذاران و شاید به شکلی کاملاً آرام در امنیت سایبری نیز منجر گردد. در این رویکرد، نبود اعتماد از سوی صنعت مقاصد، فعالیت‌ها و خروجی های عمومی نیز به‌عنوان عواملی منفی تلقی می‌شوند. این سه رویکرد می‌توانند موقعیت رویکرد نوظهور اتحادیه اروپا به حکمرانی تاب‌آور امنیت سایبری را تسهیل کرده و تغییرات را میان، درون و بین آن‌ها حفظ نمایند.

علاوه بر این و در راستای مفهوم امنیت تاب‌آور و نه امنیت کنترلی، اکوسیستم نوظهور اتحادیه اروپا و اشکال مختلف سازمانی درون آن را می‌توان سیال، پویا و قابل‌تغییر دانست. به این منظور می‌توان اشکال مختلفی از مشارکت و همکاری را درون اکوسیستم اتحادیه اروپا در سطوح و ابعاد دولت (ملی، فراملی و چندجانبه) شناسایی کرد که در مقاطع مختلف زمانی می‌توانند شکل جوامع بلندمدت، سازمان یا نهاد دارای کارکردها و مسئولیت‌های مختلف، کارگروه‌های به‌خوبی تعریف شده، شبکه‌های منعطف یا به‌شدت پیوسته سیاست‌گذاری و گروه‌های پاسخ و اقدام را به خود بگیرند (ENISA 2011d, p.28). چنین شکلی می‌تواند عمومی-خصوصی، خصوصی-خصوصی یا دارای چندین طرف ذی‌نفع و یا همچنین غیررسمی باشد. تمامی این انواع مختلف با دولت‌ها به هم مرتبط بوده و امنیت تاب‌آور دارند و ثابت و پایدار نیستند. در حقیقت تنها با درک چرایی و چگونگی تعامل میان بازیگران می‌توان به شکل، کارکرد و چشم‌انداز صحیح، دست یافت. این موضوع می‌تواند در ادامه چشم‌انداز عمیق‌تری نسبت به موانع محتمل موجود بر سر راه امنیت تاب‌آور درون اکوسیستم اتحادیه اروپا فراهم سازد و همچنین سطحی که اتحادیه اروپا می‌تواند به سمت یک سیستم بسیار تاب‌آور حرکت کند را مشخص نماید.

همان‌طور که پیش از این گفته شد، تمرکز این کتاب بر امنیت تاب‌آور و نه امنیت به‌مثابه کنترل است. امنیت کنترلی ارتباط بسیاری با ادبیات سنتی مرتبط با حکمرانی امنیت دارد، به‌عبارت‌دیگر مفروضات اصلی شامل پیش‌بینی پذیری و جامعیت همان مشخصه‌های تاب‌آوری نوع اول و روش‌های سنتی خطی ارزیابی تهدید می‌باشند (نوع دوم تاب‌آوری). درنتیجه ممکن است گفته شود تضادی میان تاب‌آوری انطباقی نوع سوم و حکمرانی سنتی امنیت وجود دارد که نمی‌توان راه‌حلی برای آن یافت (Kavalski 2009, p.531-532). البته بااینکه این

موضوع ممکن است از جنبه رویکرد در سطح معرفت‌شناسی و ازنقطه‌نظر تأکید آن بر چگونگی پیچیده‌تر شدن حکمرانی امنیت درون بافت جهانی‌شدن و منطقه‌گرایی برحسب بازیگران، فرآیندها و سازوکارهای بازی، صحیح باشد. اما یقیناً مهم‌ترین مفروض این رویکرد این است که دولت‌ها دیگر مهم‌ترین و تنها فراهم‌کننده امنیت بین‌الملل نیستند و مسئولیت امنیت در دنیایی جهانی‌شده میان بازیگران دولتی و غیردولتی توزیع شده است. علاوه بر این، ساختار امنیت یا تاب‌آوری و سیالیت یک ائتلاف یک مشخصه متمایز از حکمرانی امنیت را نشان می‌دهد که درنتیجه آن همکاری‌های امنیتی اشکال متنوعی به خود می‌گیرند (Krahmann 2003, p.5). درنتیجه حکمرانی امنیت را می‌توان «مدیریت و قاعده گذاری هماهنگ مسائل توسط مقامات چندگانه و جدای از هم، مداخله توسط بازیگران عمومی و خصوصی، ترتیبات رسمی و غیررسمی، ساختارهای گفتمانی و هنجاری و جهت‌گیری هدفمند به‌سوی خروجی‌های مشخص سیاسی» (Webber et al. 2004, p.4) تعریف کرد.

سازوکارهای کاری و هماهنگی حکمرانی امنیت درون و میان حوزه‌های مسئله‌دار از اهمیت بسیاری برخوردار است. هماهنگی، مدیریت و قانون‌گذاری سه مؤلفه حکمرانی و همچنین سه ابزار برای سنجش تجربی آن هستند. به‌طور خاص، به هماهنگی به شیوه تعامل میان بازیگران و اینکه کدام‌یک در میان آن‌ها سیاست‌گذاری را رهبری و اجرایی و فرآیندها را کنترل می‌کند، می‌پردازد. مدیریت با وظایف ارزیابی ریسک مرتبط، نظارت، مذاکره، میانجیگری و تخصیص منابع مرتبط است. قانون‌گذاری نیز نتیجه سیاست‌های اجرایی، اهداف موردنظر، انگیزه‌های پیش برنده آن، تأثیرات مؤثر و ترکیب نهادی آن است (Kirchner 2007b, p.24).

عامل مرتبط با ایجاد و اضافه کردن به ابعاد حکمرانی گونه‌شناسی تاب‌آور که پیش‌تر معرفی شدند، حکمرانی امنیت به‌عنوان یک نظریه برای مفهوم‌سازی امنیت تاب‌آور در فضای سایبری و شبکه‌های نوظهور (همکاری‌جویانه) درون اکوسیستم امنیت سایبری و نه به‌عنوان یک رویکرد کلی است (Krahman 2003). در این رابطه، رویکرد حکمرانی امنیت می‌تواند درک ما را از تعاملات میان بازیگران مختلف و در صورت نیاز از ماهیت این تعاملات برحسب نوع اکوسیستم تاب‌آور امنیت سایبری در حال ظهور در اتحادیه اروپا تسهیل کند. حکمرانی امنیت، امنیت

سایبری را ذیل مقوله حفاظت طبقه‌بندی می‌کند و نهادگرایی رسمی یا غیررسمی را مهم‌ترین ابزار دولتی برای مقابله با آن می‌داند. شناسایی مفروضات فکری روابط میان بازیگران، چه توسط هنجارها یا روابط رسمی و حقوقی ساختاربندی شده باشند یا خیر، از دیگر اهداف این رویکرد است. البته موضوعی که در اینجا بدان پرداخته نمی‌شود، شکل و نوع روابط نوظهور، چرایی ظهور آن‌ها و تنش‌های محتمل میان بازیگران مختلف در اکوسیستم امنیت سایبری در بافت رسمی یا غیررسمی است.

این موضوع در بحث پیرامون کاربرد تاب‌آوری در نظام اکوسیستم نوظهور اتحادیه اروپا به کار می‌آید، چراکه امکان تمرکز و تأکید بر سیاست‌های تاب‌آوری در مقام عمل را از طریق تشریح این موضوع که چرا اشکال خاص نهادها (یا هنجارها) ساخته می‌شوند، منافعی که بازیگران خاص در تاب‌آوری دانش و امنیت دارند (به‌عنوان‌مثال چرایی مشارکت آن‌ها)، نحوه تعامل بازیگران، تعریف اهداف سیاست‌ها و اینکه چگونه عوامل فرهنگی و مادی می‌توانند زمینه‌ساز یا مانع ایجاد هر شکلی از حکمرانی امنیت منعطف درون اکوسیستم اتحادیه اروپا شوند، فراهم می‌سازد. بررسی این جنبه‌ها نه‌تنها چشم‌اندازی به موضوع جامعیت درون یک محیط ویژه و ترکیبات آن ارائه می کند، بلکه بستری برای درکی به‌مراتب پیچیده‌تر از اینکه چگونه بازیگران درون اشکال رسمی یا غیررسمی نوظهور نهادی، تاب‌آوری را درک می‌کنند و درنهایت اینکه چگونه دانش آن‌ها تعیین‌کننده نوع رویکرد به اجرای تاب‌آوری در حکمرانی امنیت است را ایجاد می‌نماید.

جمع بندی: امنیت تاب‌آور

هدف این فصل معرفی برخی علائم خاص مفهومی و نظری بود که تحلیل اکوسیستم تاب‌آور حکمرانی امنیت اتحادیه اروپا را تسهیل می‌کند. به‌رغم اینکه ادبیات رو به گسترشی در زمینه حفاظت اطلاعات و امنیت سایبری وجود دارد، اما ازلحاظ نظری هنوز شاهد فقدان یک چارچوب مناسب برای تحلیل امنیت سایبری برحسب نوع حکمرانی امنیت تاب‌آور یا شرایطی که امکان ظهور اکوسیستم‌های به‌شدت کارآمد و تاب‌آور را فراهم می‌کند، هستیم. از طرف دیگر، آثار موجود در زمینه اکوسیستم نوظهور امنیت سایبری اتحادیه اروپا نیز ازلحاظ نظری به‌ندرت فراتر

از کاربرد مؤلفه‌های قدرت سایبری گام برمی‌دارند.[۷] آنچه در این فصل به بحث گذاشته شد، این است که کمک و افزودن به ادبیات موجود در عرصه امنیت سایبری و توزیع تاب‌آوری و حکمرانی امنیت می‌تواند نگرش‌های ارزشمند نظری و عملی به موضوع اکوسیستم درحال‌تکامل امنیت سایبری اتحادیه اروپا ارائه کند. در حقیقت استفاده از مفهوم امنیت تاب‌آور و نه امنیت به‌عنوان ابزار کنترل و مهیاکردن شرایط برای ایجاد سیستم‌های به‌شدت کارآمد نه‌تنها تحلیلی ارائه می کند که جهت واقعی را نشان می‌دهد، بلکه درکی عمیق‌تر از این موضوع که چرا و چگونه اتحادیه اروپا ازنظر بازیگران، شبکه‌ها و نهادهای دخیل و اکوسیستم جهانی، در چنین جهتی گام برمی‌دارد را نیز ارائه می‌کنند. از سوی دیگر، مسئله‌مند کردن موضوع تاب‌آوری و اضافه کردن جنبه‌هایی به چگونگی درک و تعریف مفهومی آن در کنار اتخاذ یک رویکرد انتقادی به حکمرانی امنیت سایبری، نشان خواهد داد که امنیت تاب‌آور بر اساس کدام منطق‌های مشترک در حال ظهور است و از سویی مفهوم این موضوع برای اتحادیه اروپا در فضاها، سطوح، لایه‌ها و ابعاد گوناگون که باید با آن‌ها تعامل داشته باشد یا کار کند، چیست. ارزیابی اقدامات در حال تکامل اتحادیه اروپا در حوزه امنیت سایبری در فصول بعدی می‌تواند بستری برای سنجش ایجاد اقدامات تاب‌آور در اتحادیه اروپا و اقمار حکمرانی حول آن باشد. در حقیقت این موضوع زمینه را برای تعمق نظری و مفهومی با توجه به امنیت تاب‌آور در فضای سایبری فراهم می‌کند.

فصل سوم

امنیت سایبری در اکوسیستم جهانی در فضای سایبری

مقدمه : محیط بین‌الملل

به گفته استیو پرسر[1] از آژانس امنیت شبکه و اطلاعات اتحادیه اروپا، «همکاری بین‌المللی ضروری است. برقراری امنیت در داخل مرزهای ملی معنا ندارد. تمام مسائل، ارتباط جهانی با یکدیگر دارند. رویکرد اروپا تنها در صورتی معنا پیدا می کند که مطابق رویکرد شرکای بین‌المللی خود باشد»(SDA Report 2012). ازاین‌رو، ایجاد اکوسیستم امنیت سایبری اتحادیه اروپا در اکوسیستم جهانی در حال ظهور حکمرانی امنیت سایبری و درمجموع، در حکمرانی اینترنت نهادینه و محدود به آن شده است و ارتباط بسیاری نیز با آن دارد. اتحادیه اروپا در سند راهبرد امنیت داخلی (نوامبر ۲۰۱۰) و سند دستورالعمل ها و اصول تاب‌آوری اینترنت اتحادیه اروپا[2] (مارس ۲۰۱۱) بر اهمیت همکاری با شرکای جهانی به‌منظور رسیدگی به ابعاد نظامی و غیرنظامی چالش‌های امنیت سایبری تأکید کرده است. به‌هم‌پیوستگی جهانی اکوسیستم اینترنت، بدین معنا است که هر منبعی در جهان می‌تواند منشأ تهدید بوده و پرداختن به این مقوله مستلزم اتخاذ راهکارها و سیاست‌های جهانی و بدون مرز است. آسیب‌پذیری اینترنت از یک‌سو و وابستگی متقابل شبکه‌ها، سیستم‌های اطلاعاتی و افراد از سوی دیگر، این موضوع را که هر بازیگری به‌تنهایی بتواند به ارزیابی تهدیدات و مخاطرات سایبری پرداخته و نسبت به آن‌ها واکنش نشان دهد، غیرممکن می‌سازد. علاوه بر این، با توجه به همگرایی شبکه‌های الکترونیکی،

1. Steve Purser
2. European Guidelines and Principles for Internet Resilience

اقتصادی و سیاسی در سرتاسر جهان، واکنش‌های ملی به‌تنهایی کارآمد نیستند و برای تحقق آن تغییر قابل‌ملاحظه‌ای باید در جهت هماهنگی رویکردهای نزولی و صعودی و خارجی در قبال نهادها، شبکه‌ها و بازیگران فنی و سیاسی صورت گیرد تا نقشی در زمینه ایجاد امنیت تاب‌آور در چارچوب ابعاد بی‌شمار و گوناگون امنیت سایبری ایفا نمایند.

درنتیجه، نقش نهادها، شبکه‌ها و بازیگران مطرح جهانی و منطقه‌ای دخیل در امنیت تاب‌آور فضای سایبری در این فصل به‌اختصار مطرح و استدلال های مؤثر در ظهور این اکوسیستم ارزیابی می‌شوند. علاوه بر این، به‌منظور فهم بهتر سیاست امنیت سایبری مطرح‌شده در فصول پیش رو، نحوه اتخاذ «بهترین رویه» پیشنهادی دیگر کنشگران در امنیت سایبری به نحوی (از طریق دستورالعمل، رویه یا قانون) در سطوح مختلف نیز مورد ارزیابی قرار می‌گیرد. با وجود فعالیت آشکار اتحادیه اروپا در چندین مجمع و برنامه و برقراری روابط دوجانبه ازجمله حضور در گروه کارشناسان سازمان ملل متحد[1] که وظیفه ایجاد هنجارهایی برای فضای سایبری را بر عهده دارند و نیز سازمان امنیت و همکاری اروپا[2] که اقدامات اعتمادسازی را انجام داده است، در این فصل تنها به تحلیل ضمنی نقش اتحادیه اروپا در نهادهای مختلف پرداخته می شود، چراکه جزئیات این موضوع در فصول آتی در زمینه سیاست‌های خاص و رابطه آمریکا و اتحادیه اروپا بیان می شود. در اینجا هدف صرفاً ایجاد زمینه‌ای برای فهم تأثیرات احتمالی بر اکوسیستم نوظهور حکمرانی امنیت در امنیت سایبری اتحادیه اروپا از طریق ارزیابی مفهومی آگاهانه از ماهیت رویکردها (یا مباحث) نوظهور در چشم انداز اینترنت جهانی و امنیت سایبری پیچیده است. بدین منظور، به بازیگران و سازمان‌های اصلی دخیل در ایجاد اکوسیستم حکمرانی تاب‌آور برای امنیت سایبری(۱) و به‌ویژه بر ماهیت انواع منطق‌های مربوط به حکمرانی تاب‌آور نوظهور توجه می شود. درواقع، هدف اصلی این فصل بیان حدود همگرایی یا واگرایی رویکردهای موردحمایت بازیگران اصلی و معنای این مسئله برای رویکرد و راهبرد نوظهور اتحادیه اروپا در عرصه امنیت اینترنت است.

ساختار این فصل بدین ترتیب است که در بخش نخست به نهادها و مجامع فعال در حوزه

1. UN Group of Experts
2. Organisation for Security and Cooperation

بحث و طراحی اندیشه‌های سیاسی و سیاست‌گذاری در زمینه حکمرانی اینترنت پرداخته می‌شود که در امنیت سایبری نقش دارند نظیر «آیکان» که در اصل، نظام اسامی دامنه و نظام شماره‌گذاری[1] را مدیریت می‌کند حکمرانی اینترنت[2] که محصول اجلاس جهانی جامعه اطلاعاتی[3] تحت مدیریت اتحادیه بین‌المللی مخابرات[4] است. مجمع حکمرانی اینترنت که دومین مجوز پنج‌ساله خود را در سال ۲۰۱۰ از سازمان ملل دریافت کرد، مجمع سیاست‌گذاری سنتی محسوب نمی‌شود، بلکه محلی را برای گردهمایی تمام طرف‌های ذینفع فراهم می‌کند تا بتوانند پیشنهادهای خود را پیرامون طرح‌ها و ویژگی‌های مختلف حکمرانی اینترنت ازجمله امنیت ارائه دهند. در بخش دوم به مبحث مجامع چندجانبه‌ای نظیر گروه هشت، سازمان ملل متحد، اتحادیه بین‌المللی مخابرات، سازمان پیمان آتلانتیک شمالی (ناتو)، سازمان همکاری اقتصادی و توسعه و سازمان امنیت و همکاری اروپا پرداخته می‌شود که در تکامل حکمرانی تاب‌آور در برابر تهدیدهای سایبری نقش فعالی دارند و گزارش‌ها و توصیه‌های بی‌شماری را نیز در زمینه کاهش خطرات سایبری، توسعه حوزه دفاع و بازدارندگی سایبری به‌عنوان بهترین اقدام در حوزه امنیت سایبری و حفظ زیرساخت‌های حیاتی ملی و بین‌المللی ارائه می‌دهند. در بخش آخر نیز مورد منطق‌های مربوط به امنیت تاب‌آور برگرفته از چشم‌انداز جهانی و پیامدهای این مسئله در خصوص ایجاد اکوسیستم حکمرانی سازگار و تاب‌آور برای امنیت سایبری اروپا و مناطق خارج از آن ارزیابی می‌شود.

حکمرانی اینترنت و امنیت سایبری

آیکان

آیکان مسئول رسیدگی به سه کارکرد حیاتی اینترنت است: تخصیص منابع شماره پروتکل اینترنت برای رایانه‌ها و دستگاه‌های شخصی، اسامی سرویس نام دامنه مربوطه آن‌ها و تعیین دامنه‌های سطح بالا برای فهرست‌هایی که شناسه‌هایی را به کاربران شخصی و سازمان‌ها در

1. Domain Names and Numbering System
2. Internet Governance Forum (IGF)
3. World Summit on the Information Society (WSIS)
4. International Telecommunications Union (ITU)

سطح جهان اختصاص می دهند. این سه کارکرد و نحوه تکامل آن‌ها پیامدهای مهمی برای امنیت اینترنت و رویکرد حکمرانی پشتیبان اینترنت و امنیت آن دارند. نکته مهم حول حکمرانی امنیت تاب‌آور، چالش مربوط به خودتنظیمی است که رویکرد غالب در زمینه مدیریت اسامی و آدرس‌های اینترنتی از زمان تأسیس سازمان غیرانتفاعی و سهامی عام آیکان در سال ۱۹۹۸ تحت قوانین کالیفرنیا محسوب می‌شود. آیکان بر مبنای سازمان‌های فنی پیشاموجود و با هدف دسترس پذیری اینترنت در امور شخصی و تجارت خصوصی تأسیس شد (Klimburg 2011b, p.6). آیکان نیز در کنار اینترنت اغلب از طریق تأمل و بررسی داخلی و نقد و فشار بیرونی رشد و تکامل یافت. علاوه بر این، به دلیل اهمیت بسیار راهبردی مسئله اسامی دامنه، دولت های ملی و اتحادیه اروپا خواستار برخورداری از نقش فعال تری در حوزه سیاست گذاری آیکان از طریق شورای مشورتی دولت[1] شدند و تا حدی نیز به این خواسته خود دست یافتند (Christou and Simpson 2007, 2011). آن‌ها در زمینه موضوع پاسخگویی و اعمال‌نفوذ نیز بر دولت آمریکا فشار آوردند، چراکه آیکان در اصل طرف قرارداد وزارت بازرگانی آمریکا بود و این کشور نفوذ بسیاری بر سیاست و جهت گیری آن داشت. با وجود تغییر این وضعیت بر اساس انعقاد توافقی جدید در سال ۲۰۰۹، مسائلی ازجمله تأیید تعهدات، نمایندگی، نفوذ و پاسخگویی کماکان حل‌وفصل نشده اند. علاوه بر این، اهمیت راهبردی اسامی دامنه در سطح ملی باعث تقویت فهرست های ملی برای تأمین امنیت و سایر مسائل مربوط به دامنه سطح بالای کد کشور[2] شده است. این گرایش‌ها در کنار تحولات فنی روزافزون موجب ایجاد چالش‌هایی برای آیکان، به‌خصوص در حوزه امنیت شده که این شرکت به دنبال رفع آن‌ها است. شاید جای تعجب نداشته باشد که این موضوع نیز پیامدهایی برای ماهیت حکمرانی امنیت تاب‌آور ایجادشده برای اسامی و شماره‌های دامنه در بر داشته باشد (European Parliament 2011) و به‌ویژه، اصل خودتنظیمی حامی حکمرانی اینترنت را از ابتدای آغاز کار خود تضعیف نموده است، چراکه «منفعت عمومی» با مسائل امنیت سایبری پیوند خورده است.

نقش آیکان در تأمین امنیت اسامی و شماره‌های دامنه در سه مسئله اصلی در سطح فنی

1. Government Advisory Council (GAC)
2. country code Top-Level Domain (ccTLD)

و سیاست‌گذاری ملاحظه می شود: پیوست های امنیتی سامانه نام دامنه[۲]، نسخه ۶ پروتکل اینترنت (آی پی)[1] و مسئله مربوط به حریم خصوصی داده‌ها، یعنی پایگاه اطلاعاتی تعیین هویت[2]. مسئله امنیت سیستم نام دامنه پس از آن ایجاد شد که محقق امور امنیتی به نام دَن کامینسکی[3] در تابستان ۲۰۰۸ متوجه نقطه آسیب پذیر مهمی در این سیستم گردید. این سیستم در اصل اسامی دامنه‌ای را که انسان می‌تواند به خاطر بسپرد مانند «www.europa.eu» را تبدیل به شماره‌های مورداستفاده در رایانه (آدرس‌های آی پی) می‌کند تا مقصد آن را در سطوح مختلف سرویس ذخیره اطلاعات جستجو کند (هر سطح توسط ماهیت‌های متفاوتی مدیریت می‌شود و آیکان سطح نخست یا «منطقه اصلی» را مدیریت می‌کند). مورد کامینسکی بیانگر توانایی سرقت فرایند سیستم نام دامنه در هر سطح معین (اغلب تحت عنوان مسمومیت یا جعل سامانه نام دامنه) توسط هر نوع مهاجمی است. این نوع جعل امکان «کنترل کاربران، برای مثال، هدایت آن‌ها به تارنماهای جعلی خود را در اختیار مهاجمین قرار می‌دهد» (ICANN, DNSSEC, Fact Sheet 2011) که در آن کاربر کلمه عبور و اطلاعات محرمانه حساب کاربری خود را وارد می کند یا در معرض حمله بدافزاری از طریق بارگذاری ناخواسته قرار می‌گیرد. حملات جدی‌تری نیز وجود دارند که مسیر ترافیک اینترنتی را نه در سطح داخلی، بلکه در سطح جهانی تغییر می دهند. در اینجا به مورد سرور تقلبی چینی اشاره می‌شود که به ۱۰ درصد منابع اینترنت حمله و با تغییر مسیر کاربران به سمت رژیم فیلترینگ خودکار تارنماهای چین، در بخشی از جریان اطلاعات جهانی اقدام به خرابکاری کرد (Klimburg 2011b, p.10).

هدف راه‌حل پیوست‌های امنیتی سامانه نام دامنه که در جولای ۲۰۱۰ عملیاتی شد، مقابله با تهدیدهای جدی‌تری از موارد جعل بود، گرچه هر دو مورد پیامدهای مهمی برای مسائل امنیتی دارند. این راه‌حل در سطح پایه از طریق «امضای» دیجیتالی داده‌ها (نه رمزگذاری داده‌ها) عمل می‌کند تا کاربران از اعتبار آن اطمینان داشته باشند. گرچه عملکرد مؤثر این فناوری مستلزم به‌کارگیری آن در تمام سطوح فرایند جستجو از منطقه اصلی (تحت مدیریت آیکان) تا نام دامنه

1. Internet Protocol version (IPv) 6
2. WHOIS

پروتکل جستجو و واکنش است که کاربرد گسترده‌ای در جستجوی پایگاه‌های داده‌ای دارد که اسامی کاربران ثبت شده یا عوامل یک منبع اینترنتی مانند نام دامنه، آدرس آی پی یا سیستم خودکار را ذخیره می کنند. این پروتکل در حوزه‌های اطلاعاتی دیگری نیز به کار می‌رود. (م.)

3. Dan Kaminsky

(برای مثال، «.eu» تحت مدیریت سازمان ذخیره اطلاعات نام دامنه[1]) است. پس در عمل، این سیستم بر مبنای مفهوم سیستم های رمزنگاری کار می کند تا اطلاعات معتبری را در سطوح مختلف (عمومی، ملی، محلی و غیره) فراهم آورد. مشکلات نیز از همین نقطه آغاز می شوند و پیامدهایی برای حکمرانی امنیت تاب‌آور تأمین شده از جانب پیوست های امنیتی سامانه نام دامنه ایجاد می کنند.

تهدید ناشی از حملات ایجادکننده اختلال در سرور هدف توسط پیوست های امنیتی سامانه نام دامنه در سطح فنی رفع نمی شود و با توجه به اینکه سرورها با بار اضافه مواجه شده اند، احتمال دارد این مسئله باعث کارآمدی بیشتر این حملات نیز گردد (Klimburg 2011b, p.11). در ضمن، اگر محل های ذخیره اطلاعات دامنه سطح بالای کد کشور، «سیستم‌های رمزنگاری» محلی را به‌اشتباه شناسایی کنند، احتمال آلودگی سیستم از طریق اشاعه اطلاعات نادرست سیستم نام دامنه نیز وجود دارد (Scott 2010). علاوه بر این، این موضوع در سطح سیاست گذاری و حکمرانی بستگی به منطق تجاری دارد که برخی عوارض را درمان می‌کند، ولی ماهیت آن اصلاحی و نه پادزهری است. به بیان دقیق تر، به‌رغم ایجاد امکان مدیریت برخی خطرات در قالب جعل و یا موارد جدی تر سرقت از سیستم نام دامنه، این مورد نیز با توجه به مدیریت و نظارت بر ضمیمه‌های امنیتی سامانه نام دامنه، به محاسبه هزینه-فایده بستگی دارد.[۳] این موضوع به‌خصوص برای محل های ذخیره اطلاعات کوچک‌تر و ثبت کنندگان دامنه سطح بالای کد کشور و نیز محل های ذخیره اطلاعات و ثبت کنندگان در کشورهای کمتر پیشرفته مشکل ساز است، گرچه این مشکل تنها در سطح خرد مطرح نیست، چراکه پیاده‌سازی پیوست های امنیتی سامانه نام دامنه حتی در دستورکار آن‌ها قرار ندارد. (Mohan 2011; Klimburg 2011b, p.12) درواقع، شیوه مدیریت و حکمرانی آیکان در سطح کلان بر پیوست های امنیتی سامانه نام دامنه، مربوط به ایجاد منطق اقدام مشترک در کوتاه مدت نیست، زیرا که به انطباق داوطلبانه اقدام و بحران برای ایجاد انگیزه در طرف های ذینفع وابسته است. به‌رغم فقدان راه حل آنی برای این موضوع و عضویت تعداد بیشتری از ثبت کنندگان در

1. EURID

نام سازمان غیرانتفاعی‌ای بوده که توسط کمیسیون اروپا به عنوان ذخیره کننده نام دامنه تعیین شده است. (م.)

پیوست های امنیتی سامانه نام دامنه از زمان شکل‌گیری آن،[۴] حرکت به سمت اتخاذ رویکرد اجباری، رویکرد فراحکمرانی عملی تر موجب ایجاد انگیزه در طرف های ذینفع بسیار بیشتری در سطوح مختلف برای پیاده سازی پیوست های امنیتی سامانه نام دامنه می گردد. درواقع، برنامه کلی آیکان در زمینه دامنه سطح بالای عمومی[1] این کار را در محل ذخیره اطلاعات با این هدف انجام داد که باعث ایجاد انگیزه در مناطق دارای تأیید هویت با امنیت بالا برای اجرای این پروتکل در سطح دوم نیز گردد (Mohan 2011). به‌رغم وجود طرح‌های مشترک موفق (برای مثال، آیکان و جامعه اینترنت) به‌منظور به‌کارگیری محل های ذخیره اطلاعات و طرف‌های ذینفع بیشتر در طرح پیوست‌های امنیتی سامانه نام دامنه، تمامی آن‌ها در مورد کارایی یا ارزش ایجاد سیستم نام دامنه تاب‌آور متقاعد نشده‌اند و اگر لازم باشد این بازیگران فراتر از منطق تجاری رفته و از طریق اجرای پیوست‌های امنیتی سامانه نام دامنه، به منطق بلندمدت‌تر امنیت تاب‌آور پایدار فکر کنند، انگیزه‌های بیشتری باید ایجاد گردد.

مسئله انتقال از نسخه ۴ آی پی به نسخه ۶ و مسئله فهرست تعیین هویت نیز پیامدهای امنیتی مهمی برای آیکان ازنظر حکمرانی آن بر این مسائل دارد. آی پی در اصل امکان برقراری ارتباط بین دستگاه‌های مختلف شبکه در اینترنت را فراهم می‌کند و بدون شماره آی پی (شماره ۳۲ بیتی مانند «۲۰۳.۱۵۵.۱۶.۱۷۵») نمی‌توان به اینترنت متصل شد. زمانی این تصور وجود داشت که نسخه ۴ آی پی، تعداد آدرس آی پی کافی (۴.۲۹ تریلیون) را برای آینده قابل پیش‌بینی فراهم می کند، اما افزایش کاربرد اینترنت در تمام ابعاد زندگی ازجمله در امور اقتصادی، سیاسی، اجتماعی، نظامی و غیره نشان داد که آدرس های آی پی در نسخه ۴ به‌زودی تمام می شوند. نسخه ۶ آی پی (شماره ۱۲۸ بیتی) ۳۴۰ تریلیون، تریلیون، تریلیون آدرس در اختیار قرار می‌دهد. چنین انتقالی مسلماً ویژگی‌های امنیتی جدیدی را نیز با خود به ارمغان می آورد (ن.ک. http://www.ietf.org/rfc/7123.txt) و درعین‌حال، به دلیل بروز مشکلات و خطاهای احتمالی پیش‌بینی‌شده و پیش‌بینی نشده در جریان این انتقال، فرصت‌های جدیدی نیز برای هکرها و مهاجمین ایجاد می شود (Klimburg 2011b, p.8; van der Steeg 2011).

1. generic TLD (gTLD)

به‌رغم اینکه بسیاری از نهادهای تجاری و کشورهای پیشرو مانند چین برنامه مشخصی برای انتقال و عملکرد قابلیت دوگانه ایمن نسخه‌های ۴ و ۶ آی‌پی یا تجهیزات فعال نسخه ۶ دارند، سایر کشورها این مسئله را مطرح می‌کنند که اگر قرار باشد نسخه ۶، برنامه امنی برای عملکردهای کارآمد آتی فراهم کند، باید کنترل بیشتری، به‌خصوص در حوزه نظامی، بر روی آن باشد (برای مثال، ن.ک. Yannakogeorgos 2015).

مشکل آیکان ازنظر تضمین امنیت در زمان این تعویض، وابستگی آن به پذیرش داوطلبانه نسخه ۶ از سوی ارائه‌دهندگان خدمات اینترنت، مدیران دامنه سطح بالا و دامنه سطح بالای کد کشور است. درعین‌حال، آیکان مسئول اختصاص آدرس‌های نسخه ۶ آی‌پی برای دامنه‌های سطح بالای عمومی (برای مثال «.org») و جغرافیایی (برای مثال، «.uk و .de») از طریق عملکرد نهاد شماره‌های اختصاصی اینترنت[1] است و درواقع نمی‌تواند به‌هیچ‌عنوان این تعویض را اجباری نماید (Klimburg 2011b, p.8). ماهیت داوطلبانه این تعویض ازنظر حکمرانی بدین معنا است که به دلیل وابستگی نهایی دوره انتقال به تقاضا و منبع، نمی‌توان این دوره را کوتاه نمود و نسخه ۶ آی‌پی را نیز نمی‌توان در سطح بین‌المللی اجرا کرد، چراکه هر دو مورد باعث آسیب‌پذیری اکوسیستم اینترنت در برابر حملات می‌شوند. الگویی در زمینه امنیت تاب‌آور موردنیاز است که بتواند با شواهدی دال بر اینکه در صورت عدم تبعیت بازیگران خصوصی، آیکان رابطه نزدیک‌تری با دولت‌ها برای تأمین امنیت سیستم نام دامنه از طریق انجام اقدامی هماهنگ‌تر یا اتخاذ رویکرد فراحکمرانی عملی‌تر در قالب مقررات برقرار می‌کند، طرف‌های ذینفع را هرچه سریع‌تر مجاب به اجرای این تعویض کند.

مشکل اطلاعات تعیین هویت (فهرست مالکیت تارنما) نیز مسائل مشابهی را در زمینه عدم صلاحیت حکمرانی در مورد ماهیت ابزار حیاتی رسیدگی به مسائل مربوط به جرائم سایبری ایجاد می‌کند. این موضوع بدین‌جهت مشکل‌ساز است که باوجودآنکه آیکان مسئول تعریف سیاست‌گذاری کاربر برای محل ذخیره اطلاعات دامنه سطح بالای عمومی است، اما اغلب دامنه سطح بالای کد کشور اقدامات خود را با توجه به نوع اطلاعات موردنیاز کاربر برای خرید تارنما

1. Internet Assigned Numbers Authority (IANA)

تعریف می‌کند و محل‌های ذخیره اطلاعات نیز مسئول تأمین اطلاعات مربوط به تعیین هویت هستند. مسئله تفاوت بین شیوه های به کار گرفته‌شده در کشورها است که آن دسته از محل های ذخیره اطلاعات دامنه سطح بالای کد کشور که امکان ثبت‌نام مجازی به‌صورت ناشناس را ایجاد می‌کنند، به‌احتمال‌زیاد به دلیل مقاصد مجرمانه، مورد هدف قرار می‌گیرند (برای مثال، چین). پاسخ حکمرانی ساده‌ای برای این مسئله وجود ندارد، به‌خصوص که مبحث پیرامون برقراری موازنه بین حق حفظ حریم خصوصی و حق افزایش مداخله دولت‌ها تحت عنوان تأمین فضای سایبری امن‌تر، به‌واسطه افشاگری‌های ادوارد اسنودن در سال ۲۰۱۳ تشدید گردید.

مسئله مربوط به اطلاعات تعیین هویت نیز بحث‌برانگیز است، اما برای توجه جدی به آن و به حداکثر رسانی امنیت تاب‌آور، این موضوع روشن است که توافقات یا هنجارهای منسجم خاصی باید در بین طرف‌های ذینفع اصلی از طریق تسهیل و تحریک همکاری یا مقررات اجرایی ایجاد شوند که البته به نظر نمی‌رسد این هنجارها با موارد پیشنهادی هماهنگ باشند که الگوی جایگزینی را برای امنیت و حکمرانی اینترنت مطرح می‌کنند (مبحث بعدی). درمجموع، ظاهراً مسائل امنیتی مختلف، الگوی حکمرانی آیکان را در سطح سیاست‌گذاری به چالش کشانده‌اند و ازنظر برخی مفسران (Weinburg 2010; Klimburg 2011b) آیکان حضور فعالی در گفتمان پیرامون مشارکت خصوصی-عمومی و شباهت نهادی جهت ایجاد همکاری نزدیک‌تر با دولت‌ها و تثبیت خود به‌عنوان بازیگری با توانایی و شایستگی کافی برای ایجاد حکمرانی تاب‌آور کارآمد جهت تأمین امنیت اینترنت دارد. درنتیجه، این الگوی مشارکت خصوصی- عمومی تاکنون بیشتر بیانگر فراحکمرانی نظری است تا عملی و ازاین‌رو مشخص نیست تا چه حد در بازیگرانِ بی‌میل بخش خصوصی انگیزه ایجاد می‌شود که نظر خود را در مورد کاربست فناوری جدید به‌منظور ضمانت برای تأمین امنیت تاب‌آور کارآمدی برای اینترنت تغییر دهند.

مجمع حکمرانی اینترنت

مجمع حکمرانی اینترنت[۵] در فاز دوم روند اجلاس جهانی جامعه اطلاعاتی به‌عنوان مجمعی چندجانبه، دارای چند طرف ذینفع، دموکراتیک و ازنظر نهادی شفاف برای بحث پیرامون مسائل

مربوط به حکمرانی اینترنت در سال ۲۰۰۵ تأسیس گردید. در حکم این مجمع در اجلاس جهانی جامعه اطلاعاتی در تونس (۲۰۰۵) این امر تصریح شد که «[این مجمع]» فاقد هرگونه عملکرد نظارتی است و جایگزین ترتیبات، سازوکارها، نهادها یا سازمان‌های موجود نمی‌شود، ولی آن‌ها را وارد کار می‌کند و از تخصص آن‌ها بهره می‌گیرد. این مجمع همچنین به‌عنوان فرایندی بی‌طرف، غیرتکراری و غیرالزام‌آور ایجاد می‌شود» (WSIS, Tunis Agenda for the Information Society 2005). نکته مهم این است که مجمع حکمرانی اینترنت به‌عنوان نهادی تشکیل شد که مواضع خود را به‌واسطه تأمل به‌جای تصمیم‌گیری اتخاذ می‌کند و در آن مباحث پیرامون تمام موضوعات مهم در زمینه آینده حکمرانی اینترنت ازجمله مسائل مربوط به حمایت از کودکان، جرائم سایبری و امنیت سایبری به‌صورت باز، آزاد و صریح بیان می‌شوند. قدرت هنجاری این مجمع نیز در ماهیت فراگیر و از پایین به بالای آن و این واقعیت نهفته است که در پنج سال نخست فعالیت خود به عرصه‌ای برای یادگیری از طریق بحث پیرامون نظراتی تبدیل شده است که می‌توان از آن‌ها در طرح و ایجاد سیاست بهره گرفت (Christou and Simpson 2012, p.104–105).

با توجه به ماهیت نهادی و ساختار کلی بر پایه طرف‌های ذینفع مجمع حکمرانی اینترنت، ظاهراً این امر مسلم است که میزان تأکید و اهمیت منطق‌های برگرفته از این مجمع در زمینه ویژگی‌های مختلف امنیت سایبری متفاوت است. گرچه این مسئله از تحلیل نتایج کارگروه و گزارش‌های موضوعی این مجمع در سال‌های ۲۰۰۸-۲۰۱۴ (امنیت، باز بودن، حفظ حریم خصوصی) روشن می‌کند که موضوع‌ها و مباحث خاص مربوط به حکمرانی امنیت در زمینه بحث پیرامون الگوها و رویکردهای احتمالی فراگیر هستند. مباحث مهم در این حوزه عبارت‌اند از نخست، ایجاد رابطه و موازنه بین امنیت، حفظ حریم خصوصی و باز بودن و دوم، نوع الگوی حکمرانی مناسب و کارآمد برای تنظیم مسائل مربوط به امنیت سایبری در زمینه اکوسیستم جهانی اینترنت. در خصوص مسئله نخست، این بحث پیرامون ایجاد موازنه و تناسب است. از این نظر، این مبحث در مورد میزان ایجاد موازنه بین برقراری امنیت و حفظ حریم خصوصی و بین افراد به‌عنوان افراد و افراد به‌عنوان بخشی از گروهی بزرگ‌تر است. البته زمینه سیاسی و حقوقی

کلی‌تر این مورد مربوط به تضمین امنیت دولت بدون تخطی و تجاوز به حقوق و آزادی‌های فردی است که منجر به بی‌اعتمادی به اکوسیستم اینترنت در زمینه هویت و به‌خصوص، حریم خصوصی داده‌های شخصی می‌شود.

ازآنجاکه این مسئله حکمرانی تنها به رویکرد متفاوت اتخاذشده از سوی دولت‌ها و فرهنگ‌ها وابسته نیست (برای مثال، رویکردهای آمریکا و اروپا در قبال حفظ حریم خصوصی، ن.ک. فصل [۷] و در بین و میان گروه‌ها و شبکه‌هایی نیز ملاحظه می‌شود که به اصول مختلفی بر اساس هدف خود در برنامه های متفاوت اولویت می‌دهند، درنتیجه مشکل ساز و بحث برانگیز است. برای مثال، متخصصین امنیتی ناتو و جامعه فنی اظهار می‌کنند که اتخاذ رویکردی متناسب در سطح یا لایه فیزیکی و منطقی ممکن است. بااین‌حال بسیاری از فعالان حقوق بشر، حامیان حفظ حریم خصوصی و درواقع، پیشگامان اینترنت که دسترسی به اینترنت باز (بدون نظارت دولت) را به‌عنوان حق و اصلی انسانی در نظر می‌گیرند، این مسئله را مطرح می‌کنند که بُعد ناشناس بودن باید بر امنیت اولویت داشته باشد که آن را با مداخله و سانسور مرتبط می‌دانند. با توجه به حضور نمایندگی‌های مختلف از جانب صنعت، بخش دولتی، گروه‌های حقوق مدنی و غیره (Aspects of identity yearbook 2011–12, p.24–29)، دیدگاه‌های افراطی در مورد باز بودن یا امنیت معمولاً تنها از سوی گروه‌های اقلیت در داخل مجمع حکمرانی اینترنت مطرح می‌شوند، اما ظاهراً اکثریت بسیاری نیز از اصل «تناسب» حمایت می‌کند. با وجود بیان این مطالب، معنای این موضوع ازنظر وجود الگوی حکمرانی در سطح سیاست گذاری یا فنی در تمام ابعاد از روی اسناد موجود کماکان مشخص نیست، ولی ظاهراً این دیدگاه مطرح می‌شود که هر چارچوب ایجادشده باید از «تاب‌آوری کافی برای شمول انواع مختلف رویکردها در قبال حقوق و مسئولیت‌های افراد، امور تجاری و دولت‌ها در سطح جهان» برخوردار باشد (Ibid., p.28). البته افشاگری‌های اسنودن (برای جزییات بیشتر، ن.ک. فصل ۷) تنها باعث تشدید این مبحث و درواقع، خواستار اتخاذ رویکردی پاسخگو، شفاف، دموکراتیک و مبتنی بر حقوق برای تضمین امنیت فضای سایبری شده است.

در مسئله دوم، گفتمان و بحث بین طرف های ذینفع، مسیر حکمرانی تجربی را در مورد نحوه نظارت بر مسائل مربوط به امنیت سایبری و جرائم سایبری برای ایجاد امنیت تاب‌آور و کارآمد هموار می کند. از این نظر، موضوعات اصلی بسیاری از این مباحث(ن.ک. www.intgovforum.org) به نوعی «نظارت مبتنی بر همکاری» بین تمام طرف های ذینفع دولتی و خصوصی در زمان رسیدگی به مسائل مربوط به امنیت سایبری اشاره دارد. به‌رغم وجود اجماع کلی در مورد مباحث بالا پیرامون امنیت، حریم خصوصی و باز بودن، نظراتی نیز در حاشیه در مورد محتوای این همکاری مطرح شده است. ازنظر برخی افراد، این همکاری در سطح سیاسی به موضوع فراحکمرانی نظری اشاره دارد که در آن نیازی به قانون‌گذاری اولیه نیست و در عوض، وجود هماهنگی، تسهیل و تحریک برای تأثیرگذاری غیرمستقیم بر مشارکت و همکاری از طریق تغییر محیط ضرورت دارد. رویکردهای نظارت شدید یا فراحکمرانی عملی ظاهراً به دلیل ماهیت دشوار و غیرتاب‌آور خود نمی توانند خود را با تحولات و راه‌حل‌های فنی همگام سازند که این امر نیز اغلب منجر به ظهور پیامدهای ناخواسته‌ای می‌گردد. از این منظر، به دلیل اهمیت تعامل با جامعه و مصرف‌کنندگان و آموزش آن‌ها برای افزایش آگاهی نسبت به خطرات و تهدیدهای مربوط به اینترنت، رویکرد چندگانه بهترین راه‌حل را ارائه می‌کند. افراد دیگر، به‌رغم طرفداری از حضور چند طرف ذینفع، نسبت به خطرات این مورد در صورت در نظر نگرفتن نقش اصلی برای دولت‌ها هشدار می‌دهند. برای مثال، نیلی کروس[1]، کمیسیونر سابق دستورکار دیجیتال اتحادیه اروپا در مراسم افتتاحیه مجمع حکمرانی اینترنت در نایروبی در سال ۲۰۱۱ این دیدگاه را مطرح کرد که:

«این واقعیت کماکان وجود دارد که مقامات دولتی نقش ویژه‌ای دارند. درواقع، آن‌ها از تعهد خاصی برای رسیدگی به مسائل سیاست‌گذاری دولتی به‌صورت برون‌خط (آفلاین) یا برخط (آنلاین) برخوردارند و این واقعیت باید در فرایند تصمیم‌گیری ملاحظه شود. در غیر این صورت، نتیجه حضور چند طرف ذینفع این است که [افراد/کشورهای] لابی گر نقش تصمیم‌گیرنده را بر عهده می‌گیرند و منافع خصوصی، منافع بخش عمومی را زیر پا می‌گذارند و برخی نیز خود را فراتر از قانون تلقی می‌کنند. این موارد را چه در زمان حال و

1. Neelie Kroes

چه در زمان آینده نمی پذیرم.» (Kroes 2011)

این حرکت به سمت رویکرد فراحکمرانی عملی برای دستیابی به امنیت تاب‌آور مسلماً ویژگی اصلی رویکرد امنیت سایبری در حال تکامل اتحادیه اروپا محسوب می‌شود. برای مثال، طرح اتحادیه اروپا در زمینه اتخاذ راهبرد جامع امنیت اینترنت[1] برای اروپا، بر ضرورت وجود «یک یا چند ابزار قانونی و درنتیجه، انجام اقدام مهمی از رویکرد داوطلبانه کنونی به سمت رویکردی الزام‌آور» تأکید داشت (European Commission 2011) که این مورد با رویکرد اجباری در چارچوب امریه امنیت شبکه و اطلاعات[2] پیشنهادی (۲۰۱۳) پیگیری شد که در کنار راهبرد امنیت سایبری اتحادیه اروپا[۶] (۲۰۱۳) مطرح گردید. جزئیات بیشتر مربوط به پیامدهای این مسئله برای حرکت به سمت امنیت تاب‌آور در اروپا در فصول ۶ و ۷ بیان می‌شود.

سازمان‌های چندجانبه و امنیت سایبری

فراتر از نهادهای حکمرانی اینترنت، مجامع چندجانبه نیز مشارکت فعالی در دستیابی به یک حکمرانی تاب‌آور در برابر تهدیدات سایبری داشته‌اند.

کشورهای گروه هشت

از اجلاس اوکیناوا در جولای سال ۲۰۰۸ به بعد، گروه هشت مسئله امنیت سایبری را موردتوجه قرار داد. در آنجا اعضا متعهد شدند به‌منظور بهبود دسترسی فقیرترین اقشار به اینترنت و پاسداری از حقوق مالکیت معنوی، همکاری‌های خود را افزایش دهند. گروه از پیش‌نویس موافقت‌نامه تجارت ضد جعل (آکتا)[3] و از اقدامات سازمان همکاری اقتصادی و توسعه در مقابل اثرات اقتصادی جعل و تکثیر غیرمجاز حمایت کرد (French G8-G20 Presidency 2011). دیدگاه گروه هشت درباره امنیت سایبری و حکمرانی اینترنتی که در منشور جامعه اطلاعاتی اوکیناوا منعکس است (۲۰۰۰)، این بود که رهبری این کار به بخش خصوصی داده شود و دولت‌ها نیز قوانین و سیاست‌هایی را اتخاذ کنند که محیطی قابل پیش‌بینی، شفاف و

1. Comprehensive Internet Security Strategy
2. Network and Information Security Directive
3. Anti-Counterfeiting Trade Agreement (ACTA)

عاری از تبعیض را برای آنان به وجود آورد. بحث‌ها پیرامون مقررات امنیت سایبری و حکمرانی بعد از حوادث ۱۱ سپتامبر ۲۰۰۱ شدت گرفت؛ اگرچه گروه لیون[1] (گروه کارشناسان ارشد برای جرائم سازمان‌یافته فراملی سابق) در سال ۱۹۹۵ تأسیس شد و از ضرورت بازبینی قوانین گفت «تا سوءاستفاده از فناوری‌های نوین که مستحق مجازات کیفری باشد، جرم محسوب شود و موارد دادرسی، قدرت اجرایی، تحقیقات، آموزش، پیشگیری از جرم و همکاری بین‌المللی در ارتباط با این جرم‌ها به شکل مؤثری انجام شود» (P8 Senior Experts Group 1996, p.4). هارت[2] (۲۰۰۱) ادعا کرد که ازنظر حکمرانی، موفقیت گروه لیون ناشی از مشارکت بخش خصوصی است؛ گرچه، کار اصلی را نهادهای مجری قانون دولت‌های عضو گروه هشت انجام دادند. درواقع و به شکل عجیبی، گروه هشت اولیه که تنها شامل «سران» اعضا بود، به گروه امکان داد که بازیگران غیردولتی را در مباحث امنیت و دیگر مسائلی که به رویکردی چندذینفعی نیاز داشتند، دخالت دهند.

یکی از زیرگروه‌های مهمی که از گروه لیون پدید آمد، زیرگروه مقابله با جرم‌های مرتبط با فناوری پیشرفته در سال ۱۹۹۷ بود(۷) (که بعداً توسعه یافت و کشورهای غیر گروه هشت را هم شامل شد). این زیرگروه ۱۰ اصل (ن.ک. http://www.cybercrimelaw.net/G8.html) را در جنگ علیه جرائم رایانه‌ای مقرر کرد که بستری برای تضمین برخورد قانونی مناسب با مجرمان (و همین‌طور یک برنامه اقدام) است. به لحاظ حکمرانی، تمرکز بر بهبود قوانین بوده است تا با همکاری اطلاعاتی، تشریک‌مساعی و هماهنگی بین نهادها و بازیگران خصوصیِ دخیل در اجرای قوانین کیفری با جرائم سایبری مقابله شود. ازاین‌رو، این ۱۰ اصل همه امور را بر عهده بخش دولتی نگذاشته است، بلکه تصریح کرده که باید بین دولت و صنعت همکاری وجود داشته باشد و بخش صنعتی باید مسئول ایجاد استانداردهای فنی (حکمرانی) درون شبکه‌های ارتباطی باشد. بعلاوه، مسیر بخش صنعتی برای توسعه و توزیع سیستم‌های امن و روش‌ها برای ارتقای امنیت کارکنان، نگهداری مدارک الکترونیکی و اثبات موقعیت و هویت مجرمان روشن است و چارچوب‌های قانونی لازم هم آن را تسهیل می‌کنند (Communique, Justice and

1. Lyon Group
2. Hart

Interior Ministers of the Eight, 9-10 December 1997). درباره مسائل مربوط به همکاری‌های دوطرفه قانونی و استرداد مجرمان، تأکید بر بهبود همکاری و هماهنگی و خصوصاً خلق محیط قانونی بین‌المللی بوده است؛ این محیط باید به‌قدری منعطف باشد که پرونده‌های حوزه‌های قضایی مختلف را بپذیرد، محدودیت‌ها را کاهش دهد و امکان جمع‌آوری و تبادل مدارک لازم برای پیگرد مجرمان سایبری را فراهم نماید.

گفتمان جدید گروه هشت پیرامون جرائم سایبری و امنیت با صراحت بیشتری از «الگوی چندذینفعیِ حکمرانی اینترنتی ... منعطف و شفاف ... در جهت سازگاری با پیشرفت‌ها و کاربردهای سریع فناوری» حمایت می‌کند (Deauville Declaration 2011). این گفتمان بر نقش مهم دولت‌ها، سازمان‌های منطقه‌ای و بین‌المللی، بخش خصوصی و جامعه مدنی در «جلوگیری، بازداری و مجازات استفاده از فناوری‌های اطلاعات و ارتباطات در راستای اهداف تروریستی و مجرمانه» تأکید می‌کند (Ibid.).

درواقع، تأکید بر تمام ذینفعان است؛ در مورد دولت‌ها، «گسترش هنجارهای رفتاری و رویکردهای مشترک به فضای سایبری» (Ibid.) هم‌جهت با ایجاد توازن بین امنیت و حریم خصوصی/حقوق فردی است. به‌طور خاص، درباره نقش مالکیت معنوی و داده‌های شخصی، مواضع گروه هشت بازهم حاکی از منطق الگوی چندذینفعی است که در آن دولت‌ها محیط قانونی را برای اقدام و اجرا ایجاد می‌کنند و بخش خصوصی در خط مقدم پیشبرد ابتکارات است. اینجا نیز، تأکید بر همکاری بین‌المللی و رویکردی «مشترک» مبتنی بر رعایت چارچوب‌های «قانونی» ملی و توازن درست بین حقوق فردی و تسهیم داده‌های شخصی است. در چارچوب منطق چندذینفعی، گروه هشت همکاری بهتر بین تمام ذینفعان (ازجمله کاربران) را گوشزد و بر ایجاد انعطاف و شفافیت برای همگام شدن با «سرعت زیاد پیشرفت‌های فناوری و کسب‌وکار» تأکید می‌کند (Ibid.). این موضوع برای ایجاد امنیت پایدار و تاب‌آور نویدبخش است، اگرچه در عمل به نظر می‌رسد که همه بر سر این‌که چه «الگویی» مؤثرتر است، توافق ندارند.

سازمان ملل متحد

بسیاری سازمان ملل متحد را طرف صحبت و بستری ایدئال برای تقویت گفتگوها و همکاری‌ها در حوزه امنیت سایبری می‌دانند. بااین‌حال، مسئله دیگری که بحث بر سر آن فراوان است، این بوده که کدام سازمان بین‌المللی باید به مسائل سایبری –ازجمله امنیت سایبری– بپردازد. اساساً و برای ساده‌سازی بحث، بعضی کشورها مانند روسیه و چین (و برخی کشورهای عربی) ازطریق «منطق حکمرانی» با تهدید سایبری برخورد می‌کنند و می‌خواهند به واسطه سازمان ملل متحد معاهده‌ای جهانی در این خصوص تدوین نمایند. دیگران مانند اتحادیه اروپا، بریتانیا و آمریکا اظهار دارند که با توجه به ماهیت کند و دست‌وپاگیر فرایند تصمیم‌گیری و سرعت زیاد توسعه فناوری، سازمان ملل (و اتحادیه بین‌المللی مخابرات به‌عنوان نماینده آن) برای حکمرانی اینترنتی یا رهبری در حکمرانی جهانی امنیت سایبری مناسب نیست.

بااین‌حال، سازمان ملل و خصوصاً دفتر مقابله با مواد مخدر و جرم[1] این سازمان، اتحادیه بین‌المللی مخابرات و یونسکو برای افزایش آگاهی درباره مسائل امنیت سایبری و جرائم سایبری تلاش‌های زیادی داشته و توصیه‌هایی را برای افزایش تاب‌آوری سایبری کشورها به اعضا ارائه کرده‌اند. بعلاوه، گروه کارشناسان دولتی در حوزه پیشرفت‌های اطلاعاتی و مخابرات سایبری در چارچوب امنیت بین‌المللی سازمان ملل متحد[2]، گزارشی درباره امنیت سایبری در سال ۲۰۱۰ تهیه کردند که توصیه‌هایی برای کاهش خطر سایبری و محافظت از زیرساخت‌های حیاتی در سطح ملی و بین‌المللی ارائه می‌کرد. در این بین، این موارد از همه بیشتر به چشم می‌خورد: بهبود همکاری بین‌المللی بین کشورها، بهبود همکاری از طریق اقداماتی برای به اشتراک‌گذاری «بهترین روش‌ها، مدیریت حوادث، اعتمادسازی، کاهش خطر و بهبود شفافیت و ثبات»، بهبود تشریک‌مساعی بین بازیگران دولتی، بازیگران بخش خصوصی و جامعه مدنی از طریق افزایش همکاری‌ها در این زمینه و درنهایت، ایجاد ظرفیت برای کمک به بهبود امنیت دیگر کشورها به‌منظور بهبود امنیت فناوری اطلاعات و ارتباطات در سطح جهان (UN Report 2010, p.7). گزارش این سازمان درباره امنیت سایبری (۲۰۱۰) رهنمون‌های مهمی نیز درباره ارتباط

1. UN Office on Drugs and Crime (UNODC)
2. UN Group of Governmental Experts on Developments in the Field of Information and Cyber Telecommunications in the Context of International Security

مسائل جنگ سایبری با قوانین بین‌المللی فعلی (نحوه اعمال قوانین بین‌المللی بر فضای سایبری) به دست می‌دهد. علاوه بر این، در سال ۲۰۱۳ گروه کارشناسان امنیت سایبری سازمان ملل متحد[1] «برای نخستین بار در سطح سازمان ملل ... بر سر مجموعه مهمی از توصیه‌ها در حوزه هنجارها، قواعد و اصول رفتار مسئولانه کشورها در فضای سایبری به توافق رسید» (Volter 2013). بدون شک این مجموعه تغییر مهمی در شرایط موافقت‌نامه‌های بین‌المللی در موضوعات مناقشه برانگیز محسوب می‌شد که توصیه‌های مهمی در موضوعاتی از قبیل توسعه اقدامات اعتمادساز، ایجاد ظرفیت جهانی و تسهیم اطلاعات را هم شامل می‌شد. اما این‌که فضای سایبری تاب‌آور و امنی در این بستر در درازمدت شکل بگیرد، به این بستگی دارد که کشورها هنجارهای اصلی را نهادینه کنند و توافق را عملیاتی سازند. شواهد حاکی از این است که با توجه به اختلاف‌نظرهایی که هنوز بین کشورها بر سر اصول کلیدی وجود دارد، این امر محتمل نیست. افشاگری‌های اسنودن و ادامه فعالیت گروه کارشناسان در سطح سازمان ملل متحد اوضاع را بدتر نیز کرده است (Meyer 2013).

مجمع عمومی سازمان ملل متحد نیز پنج مصوبه مهم (ن.ک. ITU 2011, p.17-18) در مورد مسئله امنیت سایبری، با تأکید بر اعتمادسازی در استفاده از فناوری‌های اطلاعات و ارتباطات به‌منظور حفظ و بهبود مزایای اجتماعی-اقتصادی این فناوری‌ها برای جوامع داشته است. این مصوبه‌ها، از دیدگاه حکمرانی تاب‌آور با ارائه چارچوب‌های قانونی محکم به‌منظور مقابله با تهدیدات جرائم سایبری و حمله به زیرساخت‌های اطلاعاتی حیاتی، تأکید بر بهبود همکاری کشورها درباره این موضوعات و نیز ایجاد هماهنگی بهتر با تمام ذینفعان، گامی در جهت رویکرد چندذینفعی است.

اتحادیه بین‌المللی مخابرات

بعد از (برگزاری) اجلاس جهانی جامعه اطلاعاتی و کنفرانس تام‌الاختیار اتحادیه بین المللی مخابرات در سال ۲۰۱۰، نقش اصلی این اتحادیه ایجاد اعتماد و امنیت در استفاده از فناوری‌های

1. UN Group of Experts on Cybersecurity

اطلاعات و ارتباطات بود. در اجلاس جهانی جامعه اطلاعاتی سران کشورها، اتحادیه بین‌المللی مخابرات را برای «ایجاد اعتماد و امنیت در استفاده از فناوری‌های اطلاعات و ارتباطات» به رسمیت شناختند و وظیفه هدایت تلاش‌های بین‌المللی در حوزه امنیت سایبری را به آن سپردند. در مقابل، هامادون توره[1]، دبیرکل اتحادیه بین‌المللی مخابرات، دستورکار جهانی امنیت سایبری[2] را راه‌اندازی کرد که چارچوبی برای همکاری بین‌المللی چندذینفعی با هدف تقویت اعتماد و امنیت در جامعه اطلاعاتی است.

مبانی یا ستون‌های دستورکار جهانی امنیت سایبری عبارت‌اند از: اقدامات قانونی، اقدامات فنی و آیین‌نامه‌ای، ساختارهای سازمانی، ایجاد ظرفیت و همکاری بین‌المللی با هدف ترویج امنیت سایبری و حفظ زیرساخت‌های اطلاعاتی تاب‌آور و اتکاپذیر (ITU Report 2011, p.20–21). اتحادیه بین‌المللی مخابرات در راستای عملیاتی ساختن دستورکار جهانی امنیت سایبری، موافقت‌نامه‌ای با دفتر مشارکت چندجانبه بین‌المللی علیه تهدیدات سایبری[3] امضا کرد که دستورکار جهانی امنیت سایبری را از طریق مراکز مختلف خود[۸] پشتیبانی می‌کند تا بتواند به اهداف راهبردی (ن.ک. Ibid., p.21) ازجمله اقدامات قانونی، ساختارهای سازمانی، طراحی راهبردهایی برای خلق چارچوب جهانی برای نظارت، هشدار و پاسخ به حوادث، ایجاد ظرفیت و همکاری بین‌المللی دست یابد. بعلاوه، اتحادیه بین‌المللی مخابرات و دفتر مشارکت چندجانبه بین‌المللی علیه تهدیدات سایبری با اتخاذ «رویکرد مشارکتی» از سوی شرکایی نظیر صنایع، دانشگاه ها، سازمان‌های بین‌المللی و اتاق‌های فکر حمایت می‌شود. اتحادیه بین‌المللی مخابرات تفاهم‌نامه‌ای نیز با دفتر مقابله با مواد مخدر و جرم سازمان ملل متحد در می ۲۰۱۱ امضا کرد که به اعضای اتحادیه بین‌المللی مخابرات و سازمان ملل کمک می‌کند که خطرات ناشی از جرائم سایبری را کاهش دهند. فعالیت‌ها به‌صورت مأموریت‌های مشترک ارزیابی، کنفرانس‌ها و فعالیت‌های آموزشی در چارچوب پنج اصل دستورکار جهانی امنیت سایبری درآمده‌اند. اتحادیه بین‌المللی مخابرات در جهت ایده مشارکت عمومی–خصوصی، تفاهم‌نامه‌ای نیز با کمپانی سیمانتک[4] امضا کرده است، به‌این‌ترتیب که این شرکت برای افزایش آگاهی و

1. Hamadoun I. Touré
2. Global Cybersecurity Agenda
3. International Multilateral Partnership Against Cyber Threats
4. Symantec Corporation

هشیاری در مورد خطرات سایبری، گزارش‌های فصلی از تهدیدات امنیتی اینترنتی را به اعضای اتحادیه بین‌المللی مخابرات ارائه می‌کند. درنهایت، اتحادیه بین‌المللی مخابرات ذیل دستورکار جهانی امنیت سایبری، برنامه محافظت آنلاین کودک[1] را راه‌اندازی کرد (نوامبر ۲۰۰۸) که یک شبکه بین‌المللی مبتنی بر همکاری (بین کشورها) است و رهنمون‌هایی در مورد رفتار امن آنلاین در اختیار ذینفعان خود قرار می‌دهد.

در مسئله حکمرانی، اتحادیه بین‌المللی مخابرات یک الگوی راهبردی امنیت سایبری را پیشنهاد کرد که در آن، کشورهای عضو می‌توانند راهبردهای خود را ایجاد نمایند (ITU 2008a, 2011). تأکید این الگو بر فلسفه چندذینفعی و پیشبرد اقدامات هماهنگ در سطح محلی، ملی و جهانی است (ن.ک. ITU 2008). در این چارچوب، منطق الگو با پنج اصل پیش‌گفته برای فعالیت حمایت می‌شود: اقدامات قانونی، اقدامات فنی و آیین‌نامه‌ای، ساختارهای سازمانی، ایجاد ظرفیت و همکاری بین‌المللی. درواقع، گفته می‌شود که توجیهات چنین الگویی ماهیتاً راهبردی، اجتماعی و اقتصادی هستند، اگرچه در عمل، ممکن است بین هرکدام از این استدلال‌ها تعارض وجود داشته باشد؛ همان‌طور که در اجرای پیوست‌های امنیتی سامانه نام دامنه نیز نشان داده شد.

روشن است که در الگوی اتحادیه بین‌المللی مخابرات، دولت‌ها تسهیلگر هستند، گرچه این را هم می‌گوید که در تعیین اهداف راهبرد امنیت سایبری، دولت‌ها باید نقش رهبری را داشته باشند. به‌عبارت‌دیگر، اتحادیه بین‌المللی مخابرات بیان می‌کند که تمام ذینفعان در تولید و اجرای راهبرد (از نظام قضایی تا جامعه مدنی، فروشندگان و جامعه اطلاعاتی) نقش دارند، درحالی‌که در مرحله تعیین دستورکار، نقش محوری برای تمام ذینفعان پیشنهاد نمی‌کند. درواقع، اتحادیه بین‌المللی مخابرات توصیه می‌کند «دولت‌ها بر تعیین دستورکار و شرایط برای همکاری تمام ذینفعان» در چارچوب راهبرد توافق‌شده تمرکز کنند و سپس بستری برای همکاری در تمام سطوح فراهم آورند (ITU 2011, p.32). از منظر حکمرانی، در بررسی اثرگذاری راهبرد، این موضوع همان رویکرد کلاسیک قانون‌گذاری مستقل (توسط یک نهاد مستقل) است . این روش

1. Child Online Protection

در سطوح پایه، از رویکرد حکمرانی چندجانبه حمایت می‌کند؛ از قوانین مداخله‌گر[1] و مشوق‌های غیرمداخله‌گر[2] برای همکاری اعضا در یک راهبرد مشترک فراگیر که دولت‌های محلی ساخته‌اند، استفاده می‌شود (برای جزییات بیشتر، ن.ک. ITU 2011).(۹)

نکته جالب این رویکرد آن است که به‌منظور بیشینه‌سازی تاب‌آوری و انطباق‌پذیری قانون‌گذاری درباره جرائم سایبری و امنیت سایبری، بر هر چه کمتر کردن بروکراسی تأکید می‌کند (Ibid., p. 49–50) و برای گسترش استانداردها و راه‌حل‌های مشترک و فرهنگ امنیت سایبری، خواهان ایجاد چارچوب‌های آیین‌نامه‌ای، فنی و قانونی برای امنیت می‌شود. بعلاوه، نقش مشارکت عمومی–خصوصی در حل مسئله امنیت سایبری را با توجه به درگیری و نقش بازیگران مختلف در بخش سایبری برجسته می‌کند. درواقع، در مورد اخیر گفته می‌شود که همکاری موفق بین بخش عمومی و خصوصی نیازمند سه رکن است: الف) ارزش پیشنهادی روشن، بدین معنی که تمام ذینفعان دقیقاً می‌دانند چرا همکاری ضروری است و منافع آن چیست، ب) نقش‌ها و مسئولیت‌های کاملاً مشخص که بر اساس راهبرد کلی و اهداف و مقاصد ذینفعان بر سر آن‌ها توافق شده است و ج) اعتماد یعنی هر طرف به انگیزه‌ها و توانایی طرف‌های دیگر در انجام وظایف خود اعتماد دارد (برای مثال، برای تبادل اطلاعات و حریم خصوصی). ارکان نهایی مربوط به ایجاد ظرفیت و همکاری بین‌المللی ستون‌های موازی هستند، اما به‌هرحال برای راهبرد امنیت سایبری پایدار و مؤثر و خلق فرهنگ جهانی امنیت سایبری مبتنی بر مجموعه‌ای از هنجارهای رفتاری برای فضای سایبری مهم هستند. موضوعی که اینجا مهم بوده آن است که ظرفیت‌ها نه‌فقط برای متخصصان دخیل در فعالیت‌های امنیت سایبری، بلکه برای جامعه و نیز در تحقیق و توسعه فناوری‌ها ایجاد می‌شوند تا از راهبردهای امنیت سایبری قوی و تاب‌آور پشتیبانی کنند.

سازمان پیمان آتلانتیک شمالی (ناتو)

اولین حمله پراکنده منع سرویس، علیه تارنمای روابط عمومی ناتو در سال ۱۹۹۹ اتفاق افتاد

1. Hands-On Legislation
2. Hands-Off Incentives

(Tick 2010) و محافظت از اطلاعات و سیستم‌های ارتباطی آن رسماً در دستورکار سیاسی اجلاس سران پراگ در سال ۲۰۰۲ قرار گرفت، اما تا زمان حمله به نهادهای دولتی و خصوصی استونی در آوریل و می ۲۰۰۷ به دفاع سایبری اهمیت چندانی داده نمی‌شد. جنگ گرجستان در سال ۲۰۰۸ هم بیش‌ازپیش توان ابزارهای سایبری را به رخ کشید و ظرفیت آن‌ها برای استفاده به‌عنوان جزئی از جنگ متعارف را نشان داد. استفاده از ابزارهای سایبری به این شکل و تهدید پیش روی جامعه یوروآتلانتیک بر ضرورت و فوریت اتخاذ سیاست دفاع سایبری برای این ائتلاف به‌مثابه یک کل واحد صحه گذاشت (www.nato.int/cps/en/natolive/topics_78170.htm).

از آن زمان، ناتو برای حل مسئله حملات سایبری اقدامات بسیاری انجام داده و در مفهوم راهبردی[1] جدید خود (که در اجلاس سران لیسبون در نوامبر سال ۲۰۱۰ تصویب شد) بر این مسئله تأکید کرده است. ناتو سیاست دفاع سایبری جدیدی نیز در ژوئن ۲۰۱۱ اتخاذ کرد (که در اجلاس سران شیکاگو در سال ۲۰۱۲ دوباره مورد تأکید قرار گرفت). به‌موازات این سیاست، در خصوص یک طرح اقدام دفاع سایبری هم توافق شد که ابزاری برای تضمین اجرای مؤثر و به‌موقع این سیاست خواهد بود. این سیاست رویکردی هماهنگ به دفاع سایبری در تمام کشورهای متحد را ارائه می‌کند که تمرکز آن بر پیشگیری از تهدیدات سایبری و تاب‌آوری شبکه‌های موجود است. یکی از اهداف این سیاست تعیین اصول همکاری دفاع سایبری ناتو با کشورهای شریک، سازمان‌های بین‌المللی، بخش خصوصی و دانشگاه‌ها است (http://www.nato.int/cps/en/natolive/news_75195.htm). دیگر اهداف آن عبارت‌اند از قرار دادن تمام ساختارها ذیل یک حفاظ متمرکز، ادغام دفاع سایبری در برنامه‌ریزی دفاعی سازمان و تعیین چارچوبی که در دریافت اخبار، اشتراک اطلاعات و تعامل‌پذیری امنیتی، بر اساس استانداردهای ناتو، به متحدان کمک و با آن‌ها همکاری کند. این سیاست بر ضرورت بهبود امنیت و تاب‌آوری متحدان داخلی برای تقویت پایدار تأکید می‌کند؛ قدرت سیاست دفاع سایبری جمعی به‌اندازه ضعیف‌ترین پیوند آن است. این سیاست سازوکارهای سیاسی و عملیاتی جدیدی بنا می‌کند که با آن‌ها می‌توان این سیاست را پیش برد. این سازوکارها شامل ایجاد قابلیت

1. Strategic Concept

واکنش به حوادث رایانه‌ای ناتو[1] و واحد آگاهی از تهدید[2] برای بهبود اشتراک اطلاعات و آگاهی موقعیتی هستند. بعلاوه، در اجلاس سران ناتو در شیکاگو در می ۲۰۱۲، برای تأکید مجدد تعهد به بهبود سیاست دفاع سایبری ناتو، توافقی برای آوردن شبکه‌های نظامی و غیرنظامی تحت حفاظت متمرکز انجام شد. بر این اساس، آژانس ارتباطات و اطلاعات ناتو[3] در اول جولای ۲۰۱۲ تأسیس شد تا روند متمرکزسازی را تسهیل و قابلیت عملیاتی ناتو را بهبود بخشد.

شورای آتلانتیک شمالی، با توجه به حکمرانی نهادی بر سیاست دفاع سایبری خود، اقدام به ارائه رایزنی‌های سیاسی می‌کند و در مدیریت بحران مربوط به دفاع سایبری تصمیم می‌گیرد. در سطح اجرایی، هیئت مدیره دفاع سایبری ناتو[4] مسئول هماهنگی دفاع سایبری در تمام نهادهای نظامی و غیرنظامی است و در سطح تخصصی، صلاحدید درباره تلاش‌ها و قابلیت‌های دفاع سایبری ائتلاف را کمیته سیاست و برنامه‌ریزی دفاعی تعیین می‌کند. تفاهم‌نامه‌هایی بین هیئت مدیره دفاع سایبری ناتو و ادارات مسئول دفاع سایبری ملی برای تسهیل اشتراک اطلاعات، گفتگو و غیره و برای اطلاع‌رسانی به تیم‌های واکنش سریع ناتو درباره چگونگی پشتیبانی از کشورهای ائتلاف در بحران‌های سایبری وجود دارند. هیئت مدیره دفاع سایبری ناتو کارکنان سیاسی، نظامی، فنی و عملیاتی را در خود دارد که تحت حمایت بخش چالش‌های نوظهور امنیتی با هیئت مشاوره، فرماندهی و کنترل ناتو[5] (نهاد اصلی که در دفاع سایبری درباره جنبه‌های فنی و اجرایی با آن مشورت می‌کنند) عمل می‌کنند. درنهایت، مرجع نظامی ناتو[6] و آژانس ارتباطات و اطلاعات ناتو مسئول الزامات عملیاتی، اکتساب، اجرا و عملیات مرکز فنی قابلیت واکنش به حوادث رایانه‌ای ناتو هستند که خدمات امنیت سایبری فنی و عملیاتی را برای تمام بخش‌های این سازمان ارائه می‌کند (www.nato.int/cps/en/natolive/topics_78170.htm)[10] فراتر از این، مرکز عالی دفاع سایبری مشترک ناتو[7] که در راستای عرضه و توسعه آموزش و تعلیم در سال ۲۰۰۸ در استونی آغاز به کار کرد، درباره مسائل

1. NATO Computer Incident Response Capability (NCIRC)
2. Threat Awareness Cell
3. NATO Communications and Information Agency
4. NATO Cyber Defence Management Board
5. Consultation, Command and Control Board (NC3)
6. NATO Military Authorities
7. NATO's Cooperative Cyber Defence Centre of Excellence (CCD CoE)

قانونی و سیاستی در زمینه دفاع سایبری تحقیق می‌کند. این مرکز به فرماندهی متحد تحولات ناتو[1] متصل است و فصل مشترک مفیدی بین نهادهای نظامی ناتو، دانشگاه و بخش خصوصی است. بعلاوه، ظرفیت معاضدت بالایی ازجمله همکاری (کشورهای عضو) با اتحادیه اروپا دارد. آژانس امنیت شبکه و اطلاعات اتحادیه اروپا و مرکز عالی دفاع سایبری مشترک ناتو رویدادهای مشترکی را –مانند تبادل بهترین رویه‌ها در این زمینه– سازمان داده‌اند که در آن‌ها یک بستر یادگیری برای آمادگی در مسائل دفاع سایبری عمل می‌کند. بعلاوه، مرکز عالی دفاع سایبری مشترک ناتو بانی ایجاد دستورالعمل تالین برای قوانین بین‌المللی اطلاق پذیر بر جنگ‌های سایبری[2] (۲۰۱۳) از طریق فرایند دستورالعمل تالین بود. اساساً این دستورالعمل قواعد حاکم بر جنگ‌های سایبری در محیط قوانین بین‌المللی را تعیین می‌کند (Tallinn Manual 2013).

همه این‌ها در منطق امنیتی سیاست‌های دفاع سایبری ناتو چه معنایی دارند؟ درحالی‌که ناتو با همان مشکلات عمومی بسیاری از سازمان‌های دیگر در امنیت سایبری مواجه است، تمرکز آن بر دفاع سایبری (و درنتیجه، عمدتاً بر محافظت و بازدارندگی) به این معنی است که این سازمان در سیاست در حال تکامل خود و منطق حکمرانی این سیاست با مشکلات خاصی مواجه است. نخست، ناتو باید دقیقاً مشخص کند که چه موضوعی یک حمله، استفاده از زور و عمل جنگجویانه در فضای سایبری تلقی می‌شود. مسئله دوم، برقراری ساختار حکمرانی است که امکان اقدام به‌موقع و مؤثر علیه تهدیدات از طریق مجموعه استانداردها و قوانین مشترک را فراهم کند. سوم، خلق هنجارهای رفتاری برای اداره فضای سایبری است که نیازمند کار سخت هماهنگی راهبردهای ملی از طریق درک مشترک و تسهیل اشتراک اطلاعات و کاهش تهدید است؛ کاری که کشورهای عضو، مایل به انجام آن نیستند. در نهایت، مصالحه‌ای بین محافظت از آزادی‌های فردی و امنیت جمعی وجود دارد که کلی‌تر از این است، اما معانی خاصی برای ناتو و سیاست دفاع سایبری آن دارد (Noshiravani, 2011, p.4).

رویکرد ناتو به دفاع سایبری در نگاه اول بسیار جامع به نظر می‌رسد؛ سیاستی هماهنگ‌تر، همکارانه‌تر و فراگیرتر از قبل دارد و در مراکز ناتو برای افزایش تاب‌آوری فردی و جمعی،

1. NATO Allied Command Transformation
2. Tallinn Manual on the International Law Applicable to Cyber Warfarel

ساختارهای پشتیبانی و یادگیری را از طریق آموزش و تعلیم ایجاد کرده است؛ اما این رویکرد از نقایص مشخصی هم رنج می‌برد. به دیگر سخن، اگر بنا باشد این نهاد در حرکت به‌سوی امنیت تاب‌آور موفق باشد، باید بر موانع خاصی فائق آید.

اولین مشکل، مسئولیت بازیگران مختلف –خصوصاً در سطح کشورهای عضو– است. تأکید ناتو بر همکاری با دولت‌های ملی برای هماهنگ کردن استانداردها و تبادل اطلاعات است، اما با توجه به ماهیت مالکیت زیرساخت‌های اطلاعاتی حساس و فعالیت‌های سایبری، این سازمان بر مشارکت عمومی–خصوصی در سطح کشورها تکیه دارد. اگرچه بدون شک دولت‌ها می‌توانند رویکرد استاندارد منظمی ابداع کنند، معمولاً اهداف بلندمدت بسیار متفاوتی از بخش خصوصی دارند که با منطق اقتصادی عمل می‌کنند و هدف آن‌ها انتقال ارزش به ذینفعان است. از این نظر، بخش خصوصی اغلب از افزایش مقررات در فضای مجازی –خصوصاً با توجه به سختی‌هایی که شرکت‌های چندملیتی برای هدایت و درواقع، استانداردسازی پیچیدگی کنونی اقدامات قانونی تنظیمی در بخش‌های سایبری مختلف با آن مواجه‌اند– استقبال نمی‌کنند. البته تشویق و انگیزه بخشی به بخش خصوصی برای همکاری و هماهنگی در یک مشارکت مؤثر غیرممکن نیست (نمونه هلند در اینجا آموزنده است)، اما این اقدام به زبان مشترک و خرد جمعی و پرداختن به مسئله امنیت سایبری فراتر از مسئولیت اداره فناوری اطلاعات و ارتباطات و در سطح هیئت‌مدیره بسیاری از شرکت‌های بزرگ‌تر فناوری اطلاعات و ارتباطات است (Ibid., p.5–6; IAAC Symposium September 2012). هدف طرح پیشنهادی ناتو برای مشارکت سایبری صنعت که اعضا در اجلاس سران کاردیف[1] در سال ۲۰۱۴ بر سر آن توافق کردند، تضمین این موضوع است که برای برآوردن اهداف بلندمدت سیاست تقویت‌شده دفاع سایبری ناتو، از تخصص و نوآوریِ بخش خصوصی تا جای ممکن استفاده می‌شود.

مسئله دوم، روشن شدن آستانه‌ها و استانداردهایی است که برای سؤالات مربوط به این حوزه‌ها بکار می‌رود؛ استفاده از زور در حوزه سایبری؛ چه وقتی حمله سایبری را می‌توان حمله‌ای مسلحانه قلمداد کرد (طبق بند ۵۱ از منشور ملل متحد و بند ۵ از

1. Cardiff Summit

پیمان واشنگتن[1])؛ چه نوع اقدامی در پاسخ به حملات سایبری مجاز و چه قوانینی بر این اقدامات حاکم است. دو مسئله در این زمینه مطرح است: نخست، اگرچه بحث زیادی بر سر این موضوع وجود دارد، اجماع کلی می‌گوید که یک حمله سایبری را زمانی می‌توان حمله‌ای مسلحانه قلمداد کرد که پیامدهای فیزیکی داشته باشد –یعنی در آن مستقیم یا غیرمستقیم از زور استفاده شود. دوم، مسئله نسبت دادن تقصیرات در فضای مجازی است؛ مشکل شناسایی حمله‌کننده می‌تواند بر توانایی کشورها و سازمان در پاسخ به‌موقع و قانونی –در چارچوب قوانین بین‌المللی مربوطه– به حمله و نیز بر ماهیت پاسخ اثر بگذارد (Ibid., p.6–7). اگرچه دستورالعمل تالین تا حدی توانسته به مسائل فوق پاسخ دهد، یعنی تعریف مشترکی از حمله نظامی، نحوه اعمال قوانین بین‌المللی، تفاوت بین اهداف نظامی و غیرنظامی و روش‌های تعیین این‌که چه طرف‌هایی در جنگ‌های خاص فضای سایبری دخیل بودند یا هستند، ارائه کرده است، اما همچنان از حل برخی مسائل مهم دیگر عاجز است. برای مثال، این دستورالعمل معیارهای روشنی برای این‌که چه حمله‌ای را می‌توان حرکتی جنگ‌طلبانه تلقی کرد، به دست نمی‌دهد و در عوض استدلال می‌کند که این موضوع باید مورد به مورد بر اساس وخامت و اثرات بالقوه هر تصمیم بررسی شود. به نظر بندیک[2] (p.8 ,2014) «استفاده از قوانین بین‌المللی برای تعیین قواعدی برای جنگ سایبری فقط باعث می‌شود این نوع اقدامات انجام‌شدنی‌تر به نظر بیایند ... هیچ هنجاری برای پرداختن به درگیری‌های کمتر از آستانه تهاجم مسلحانه وجود ندارد.» به‌علاوه، حذف متخصصان غیر ناتویی از گروه‌های کارشناسی که قواعد جنگ سایبری را مقرر می‌کنند، نه‌تنها گستره، بلکه اثر بالقوه چنین قواعدی را محدود کرده است. در نهایت، به نظر برخی، دستورالعمل تالین توجه اندکی به حقوق شهروندی دارد، چراکه تعریف موسع حمله نظامی عملاً دولت‌ها را از بکارگیری اقدامات نظامی علیه گروه‌های غیردولتی یا حتی هکرهای احتمالی منع نمی‌کند. از این نظر، با کنار گذاشتن اصول اخلاقی به نفع دفاع سایبری، مرز بین عملیات پلیسی و نظامی بیش‌ازپیش مبهم می‌شود (Ibid., p.25).

1. Washington Treaty
2. Bendiek

مسئله سوم، از همکاری و تشریک‌مساعی بین‌المللی خصوصاً با اتحادیه اروپا (با توجه به عضویت همپوشان اعضای دو سازمان) ناشی می‌شود. درواقع، همکاری ناتو-اتحادیه اروپا اگر به شکل کارآمدی هماهنگ شود، قطعاً می‌تواند به شکل‌گیری امنیت تاب‌آور کمک کند. با توجه به توانایی اتحادیه اروپا در اجرای مقررات و آیین‌نامه‌ها و توانایی ناتو در انعقاد قراردادهای بین‌المللی، این دو می‌توانند در ایجاد استانداردها، قوانین و روش‌های مشترک که بر جهت و ماهیت هنجارها و اصول بین‌المللی برای امنیت سایبری اثر می‌گذارند، نقش ایفا کنند. به‌رغم این موارد، موانع زیادی بر سر راه همکاری مؤثر ناتو و اتحادیه اروپا در مسائل امنیت سایبری وجود دارد؛ مواردی نظیر تفاوت اختیارات و درنتیجه، قابلیت‌ها؛ و مسئله قبرس-ترکیه که دست‌کم باعث محدودیت‌هایی در توانایی همکاری رسمی آن‌ها می‌شود (اگرچه به‌طور غیررسمی این‌گونه نیست – ن.ک. فصل ۶). به‌علاوه، با توجه به اینکه ناتو و اتحادیه اروپا اعضای محدودی (ازنظر جغرافیایی) دارند، هرگونه همکاری مؤثر بین این دو سازمان به نیازهای جامعه «جهانی» بازیگران (که در فضای سایبری کار می‌کنند و ازاین‌رو خواهان امن کردن آن هستند) نمی‌پردازد یا ترجیحات آن‌ها را منعکس نمی‌کند. پس دست‌کم ازنظر حکمرانی، در هر هنجار یا اصلی که این دو سازمان حول آن توافق کنند، برای این‌که اثر و حوزه جهانی داشته باشد، باید دیگر ذینفعان مهم در حوزه امنیت سایبری را نیز دخیل کنند. این موضوع از طریق مجامع قدیمی یا جدید و با دخالت دادن بخش خصوصی و جامعه مدنی صورت می گیرد.

سازمان همکاری اقتصادی و توسعه

سازمان همکاری اقتصادی و توسعه ابزار مفیدی در تولید اطلاعات درباره بهترین روش‌ها در حوزه تاب‌آوری زیرساخت‌های حیاتی برای توسعه اکوسیستم‌های امنیت سایبری در اتحادیه اروپا و اعضای آن است. کارگروه امنیت و حریم اطلاعات سازمان همکاری اقتصادی و توسعه[1] گزارش‌های منظمی از ایجاد تاب‌آوری، حریم خصوصی و جامعه اطلاعاتی ارائه می‌دهد. درواقع، این گروه شبکه‌ای از متخصصان دولتی، کسب‌وکارها و جامعه مدنی را گرد هم آورده است و به

1. OECD Working Party on Information Security and Privacy (WPISP)

تسهیل تبادل اطلاعات بین ذینفعان و پایش فعالیت‌های مربوط به امنیت سایبری کمک می‌کند (European Parliament Report 2011, p.19). از این نظر، ساختار حکمرانی آن حاکی از یک مشارکت مؤثر است و حرکت آن به سمت بهترین روش‌ها، با عنایت به تهدیدات و خطرات بیشتری که پیشرفت‌های فناوری اطلاعات و افزایش ارتباطات را به همراه دارد، بر ضرورت شکل‌گیری فرهنگ امنیت سایبری تأکید می‌کند.

به همین منظور، سازمان همکاری اقتصادی و توسعه مجموعه‌ای از دستورالعمل‌های کلی (۲۰۰۲) ایجاد کرده است[11] که هدف از آن تسهیل جریان فرهنگ امنیت سایبری است. منطق بنیادین این رویکرد فراگیر این است که «هر شرکت‌کننده بازیگر مهمی برای تضمین امنیت است. شرکت‌کنندگان متناسب با نقش خود، باید از ریسک‌های امنیتی مربوط و اقدامات پیشگیرانه آگاه و مسئولیت‌پذیر بوده و نیز برای بهبود امنیت سیستم‌ها و شبکه‌های اطلاعاتی تلاش کنند.» (OECD 2002, p.8). به‌علاوه، مطابق شرایطی که در فصل دوم برای امنیت تاب‌آور کارآمد تعیین شد، بر ضرورت اتخاذ و اجرای دستورالعمل‌هایی در سیاست و عملیات تأکید می‌کند و اشعار دارد «تلاش‌هایی که برای بهبود امنیت سیستم‌ها و شبکه‌های اطلاعاتی انجام می‌شود باید با ارزش‌های جامعه دموکرات خصوصاً نیاز به جریان باز و آزاد اطلاعات و دغدغه‌های اصلی برای حریم خصوصی شخصی هماهنگ باشند» (Ibid., p.9). به‌علاوه، در این گزارش گفته شده است که عواملی مانند رهبری، خصوصاً از طرف دولت‌ها (OECD 2003) و مشارکت فراگیر تمام شرکت‌کنندگان برای خلق محیطی که امکان برنامه‌ریزی و مدیریت امنیت ایجاد و درک بهتری از نیاز به امنیت حاصل می‌شود، ضروری است (OECD 2002, p.8).

گزارش سازمان همکاری اقتصادی و توسعه می‌گوید که اصول زیربنایی دستورالعمل‌ها در پی ارائه رویکردی فراگیر برای امنیت سیستم‌ها و شبکه‌های اطلاعاتی نیستند، بلکه می‌خواهند «چارچوبی اصولی ارائه دهند که شرکت‌کنندگان چطور می‌توانند از توسعه فرهنگ امنیت منتفع شوند و نیز در آن مشارکت نمایند» (Ibid., p.14)؛ به‌عبارت‌دیگر، این اصول مجموعه‌ای از مقتضیات هستند که درصورتی‌که در سیاست‌ها، روش‌ها، اقدامات و آیین‌نامه‌ها اعمال شوند، محیطی ایجاد می‌شود که در آن، امنیت تاب‌آور، شامل پیشگیری و واکنش، در تمام سطوح

و بین تمام شرکت‌کنندگان در فضای سایبری، به شکل فردی و جمعی نهادینه می‌شود. البته می‌توان گفت که چنین اصولی اگرچه برای بیشتر مخاطبان غربی قابل‌قبول هستند (برای مثال اصل دموکراسی)، برای دیگر کشورها، سازمان‌ها و افرادی که تحت حکمرانی و خرد امنیتی دیگری کار می‌کنند، شدیداً محل مناقشه است. این موضوع در کنوانسیون جرائم سایبری شورای اروپا[1]، خود را نشان داد (که در ادامه توضیح داده می‌شود). این را هم می‌شود گفت که برخی از دستورالعمل‌ها کفایت لازم را ندارند؛ برای مثال، اصل شرایط پاسخ در رابطه با حوادث امنیت سایبری که می‌گوید: «هر جا جایز باشد، می‌تواند شامل اشتراک اطلاعات فرامرزی و عملیات مشترک بشود.» چنین تبادل اطلاعاتی، فراتر از مرزها، پیش‌نیاز امنیت تاب‌آور است –و هنجاری است که تمام بازیگران دخیل در امنیت سایبری باید برای تضمین واکنش و پاسخ کارآمد به حوادث امنیت سایبری اتخاذ و عملیاتی کنند. پس در نهایت، چنین دستورالعمل‌هایی ماهیتاً داوطلبانه هستند و اگرچه چارچوبی عام برای خلق فرهنگ امنیت سایبری فراهم می‌کنند، اصول جهانی قابل قبولی یا اصولی که تمام بازیگران آن‌ها را اتخاذ و اجرا کنند، ارائه نمی‌دهند. درواقع، جهان در سال ۲۰۱۵ از سال ۲۰۰۲ هم پیچیده‌تر شده است؛ سازمان همکاری اقتصادی و توسعه به عرضه‌کنندگان خدمات اینترنتی توصیه‌هایی برای مقابله با بات‌نت‌ها ارائه می‌دهد؛ توصیه‌هایی که ازنظر حکمرانی با ابتکارات بخش خصوصی و مشارکت عمومی–خصوصی پشتیبانی می‌شوند (OECD 2012).

شورای اروپا

مشارکت اصلی شورای اروپا در حکمرانی امنیت سایبری تصویب کنوانسیون جرائم سایبری در سال ۲۰۰۱ بود که در جولای سال ۲۰۰۴ اجرایی شد. این کنوانسیون که کنوانسیون بوداپست هم نامیده می‌شود، اهمیت سیاسی دارد و تنها توافق الزام‌آور در مسائل امنیت سایبری است که در تعیین بهترین روش در داخل و خارج از اروپا به آن استناد می‌شود. تا زمان نگارش این مطلب (مارس ۲۰۱۵)، ۴۵ کشور (ازجمله آمریکا) این کنوانسیون را امضا و تصویب کرده‌اند. ۲۴ کشور

1. Council of Europe Cyber Crime Convention

عضو اتحادیه اروپا جزء این ۴۵ کشور هستند؛[۱۲] هشت کشور دیگر نیز آن را بدون تصویب امضا کرده‌اند.[۱۳] با همه این‌ها و با توجه به درخواست این کنوانسیون از کشورها برای همکاری بین‌المللی و اشتراک اطلاعات –ازجمله همکاری فراملی و فرامرزی بین نیروهای پلیس- این موضوع محل منازعه نیز شده است. کشورهایی نظیر چین و روسیه (و چند کشور درحال‌توسعه) مخالفت صریح خود را با تصویب این کنوانسیون اعلام کرده‌اند؛ آن‌ها نگرانی از نقض حکمرانی ملی را دلیل این کار خود اعلام کرده‌اند. واضح است که با توجه به تعداد زیاد کاربران اینترنت در این کشورها و متهم بودن این کاربران در بسیاری از رخنه‌ها و حملات سایبری در سال‌های اخیر، این مسئله در دستیابی به تاب‌آوری امنیتی جهانی مشکل‌ساز است.

ازنظر حکمرانی، کنوانسیون بوداپست داوطلبانه است چراکه امضای آن برای تمام کشورها خصوصاً خارج از اروپا، اجباری نیست. بااین‌حال، هدف از آن پایه‌گذاری «سیاست کیفری مشترک با هدف محافظت از جامعه در برابر جرائم سایبری» است (Convention on Cyber-crime 2001, Preamble). برای دستیابی به این هدف، لازم است که کشورهای امضاکننده این کنوانسیون قوانین مربوط به جنبه‌های آیین‌نامه‌ای جرائم سایبری، مانند دسترسی و ردگیری غیرمجاز، سوءاستفاده از لوازم، کلاه‌برداری، جعل، تجاوز به مالکیت معنوی، مداخله در داده‌ها و سیستم‌ها و پورنوگرافی کودکان را نیز تصویب و اجرا کنند. به‌علاوه، این کنوانسیون یک چارچوب قانونی و قضایی فراملی عرضه می‌کند که از امضاکنندگان می‌خواهد قوانین مربوط به تحقیقات جرائم سایبری را تصویب کنند و از طریق استرداد مجرمین و کمک متقابل برای اجرای قانون در تحقیقات چنین جرائمی با دیگر کشورها همکاری کنند. علاوه بر کنوانسیون بوداپست، مجمع پارلمانی شورای اروپا[1] توصیه‌هایی در مورد اینترنت و قانون ارائه می‌کند و این دیدگاه را بیان می‌کند که اگرچه ماهیت اینترنت قاعده‌مند کردن آن را غیرممکن می‌کند، اصول اخلاقی اینترنت باید با ابزارهای قانونی و از طریق مرجع اروپایی اخلاق اینترنت وضع شود تا با تعیین حقوق و وظایف ابتدایی کاربران، رفتار «مدنی» در اینترنت نهادینه شود (CoE Parliamentary Assembly Recommendation 1670, 2004; O'Neill 2012, p.8).

1. CoE Parliamentary Assembly

اگرچه اتحادیه اروپا به‌وضوح کنوانسیون بوداپست را پذیرفته و به آن گردن نهاده است، موضوعی که در برنامه استکهلم[1] برای امنیت داخلی هم بازتاب یافت (p.22 ,2010)، همچنان درباره کارآمدی آن بحث‌وجدل وجود دارد؛ خصوصاً کمبود ضمانت‌های اجرایی در هنگامی‌که امضاکنندگان نمی‌توانند به تعهدات خود طبق شرایط پیمان عمل کنند. به‌علاوه، حتی در جمع اعضای اتحادیه اروپا هم ضعف‌هایی وجود دارد، زیرا با وجودی که کنوانسیون شورای اروپا «تنها ابزار قانونی بین‌المللی تا به امروز است، به دلیل پیشرفت‌های سریع جرائم سایبری ضعف‌هایی نشان می‌دهد» (European Commission 2010, p.157 final). فقدان مرجع برای نحوه مواجهه با حملات سایبری بزرگ‌مقیاس و ضعف‌های ساختاری و فرهنگی مربوط به عملکرد نقاط تماس ملی در زمینه همکاری در جرائم رایانه‌ای ازجمله این مشکلات است.

به‌طور گسترده‌تر، مسئله اصلی به ماهیت بین‌المللی جرائم سایبری برمی‌گردد؛ به این مشکل در بحث مربوط به منازعات به‌طور ضمنی اشاره شد. جرائم سایبری مشکلی جهانی هستند و اگر بنا باشد امنیت تاب‌آور منسجمی شکل بگیرد، به همکاری جهانی نیاز دارد. درنتیجه، کنوانسیون شورای اروپا، به‌عنوان ابزاری برای مقابله با جرائم سایبری، هنگامی واقعاً کارآمد می‌شود که کشورهای خارج از اروپا هم هنجارهای آن را بپذیرند.(۱۴) پروژه جهانی جرائم سایبری برای همین هدف –ترویج کنوانسیون فراتر از اروپا– ایجاد شده و تا حدی هم موفق بوده است، زیرا که بعضی کشورها در آسیا و آمریکای لاتین کنوانسیون را پذیرفته‌اند و اصلاحات قانونی لازم را بر اساس آن انجام می‌دهند.(۱۵) دیگران کماکان دیدگاه متفاوتی پیشنهاد می‌کنند که بر هنجارها و اصول دیگری بنا شده است. برای مثال کشورهای سازمان همکاری شانگهای (چین، قزاقستان، قرقیزستان، روسیه، تاجیکستان و ازبکستان) موافقت‌نامه‌ای – [با عنوان] توافق امنیت اطلاعات بین‌المللی– به امضا رساندند که بر نقش عمده امنیت ملی و نقش دولت‌ها بر کنترل فناوری اطلاعات و مدیریت خطرات و تهدیدها تأکید می‌کند. این موافقت‌نامه همچنین کشورهای غربی و تسلط آن‌ها بر فضای اطلاعاتی را تهدیدی بزرگ برای اعضا و نظام‌های اجتماعی-سیاسی و فرهنگی آن کشورها می‌داند (Goldsmith 2011, p.4). مانند هنجار و ابزارهای ابداع‌شده

1. Stockholm Programme

ی دیگر در اروپا و اتحادیه اروپا، این کنوانسیون اصول مفید زیادی برای تضمین امنیت تاب‌آور کارآمد در خود دارد، اما برای تأثیرگذاری واقعی بر جرائم سایبری، با توجه به ماهیت جهانی این جرائم، باید توافق و اجرای آن از اروپا فراتر رود.

سازمان امنیت و همکاری اروپا

بعد از حمله به سیستم‌های سازمان امنیت و همکاری اروپا در سال ۲۰۰۷، بحث‌ها در خصوص رویکردی جامع به امنیت سایبری در مجمع سال ۲۰۰۸ به ریاست استونی جدی‌تر شد. قبل از این حادثه، تلاش‌های سازمان امنیت و همکاری اروپا بر بهبود جنبه‌های مختلف امنیت سایبری، مانند جرائم سایبری، تروریسم سایبری و نیز بر تضمین «آزادی» گردهمایی، ابراز نظر و اطلاعات در اینترنت متمرکز بود. از آن زمان به بعد، فعالیت‌ها شامل جلسات و کنفرانس‌های سطح بالا درباره مسائل راهبردی امنیت سایبری و ارائه رویکردی جامع بود، اما توافق دقیقی در خصوص نقش سازمان امنیت و همکاری اروپا وجود نداشت.[۱۶] یکی از مباحث پرباری که در این زمینه شکل گرفت، توسعه هنجارهای رفتاری دولت‌ها در فضای سایبری بود؛ مفهومی که سازمان‌های چندجانبه دیگری هم به آن پرداخته‌اند (همان‌طور که پیش از این اشاره شد). یکی از کنفرانس‌های سازمان امنیت و همکاری اروپا در می سال ۲۰۱۱ نیز به این سؤالات پرداخت که اختیارات سازمان امنیت و همکاری اروپا را چگونه می‌توان برای بهبود نقش بین‌المللی آن در امنیت سایبری تقویت کرد، چگونه می‌توان سازوکارهای داخلی سازمان را در فضای سایبری توسعه بخشید و چگونه می‌توان سندی راهبردی پیرامون رویکرد جامع فضای سایبری تدوین کرد؟[۱۷]

بااین‌حال، عضویت در سازمان امنیت و همکاری اروپا که کشورهایی از آمریکای شمالی تا آسیای مرکزی و اعضای اتحادیه اروپا، ناتو و کشورهای مستقل مشترک‌المنافع را گرد هم می‌آورد، به این معنی است که دیدگاه‌های هنجاری و رویکردهای راهبردی متنوعی به امنیت تاب‌آور در فضای سایبری وجود دارد. ازاین‌رو، اگرچه در سطح سازمان امنیت و همکاری اروپا پیشرفت‌هایی در حصول توافق بر سر مجموعه اولیه‌ای از اقدامات اعتمادساز برای فضای سایبری

به دست آمده است که نشان می‌دهد تنوع اعضا می‌تواند یک مزیت و نه یک مانع برای دستیابی به توافق بر سر مسائل خاص باشد، همین تنوع و البته عدم عضویت چین در سازمان امنیت و همکاری اروپا این مزیت را از بین می‌برد (European Parliament 2011, p.20).

نمونه خوبی از این موضوع تضاد بین هنجارهای پیشنهادی بریتانیا (ن.ک. Downing 2011; Hague 2011) و آمریکا (و دیگر کشورهای غربی و سازمان‌های بین‌المللی) برای فضای مجازی ازیک‌طرف و هنجارهای روسیه و چین از طرف دیگر است. همان‌طور که انتظار می‌رفت، بین بریتانیا، آمریکا و مقامات اتحادیه بین‌المللی مخابرات همگرایی و همپوشانی وجود دارد، خصوصاً اگر تمرکز حول مسائل دسترسی جهانی، رویکردها به جرائم سایبری، مشارکت بین‌المللی و اصل پاسداری از آزادی‌ها باشد. اگر اصول ادعایی آمریکا، بریتانیا و اتحادیه بین‌المللی مخابرات را با اصول سازمان همکاری شانگهای مقایسه کنیم، می‌توانیم تفاوت منطق هرکدام از هنجارهای پیشنهادی برای رفتار دولت‌ها در فضای سایبری (Healey 2011a) و دلیل برخی همگرایی‌ها را درک کنیم. توافق سازمان همکاری شانگهای (۲۰۰۸) صراحتاً به هنجارها نپرداخته بود، اما بر «کنترل دولتی» تأکید می‌کند؛ درواقع، در پیشنهادهای قبلی روسیه، تمایل روشن و قابل‌انتظاری برای محدود کردن جریان‌های فرامرزی اطلاعات به دلیل تأثیر احتمالی بر فرهنگ امنیت وجود داشت. از آن پس پیشرفت‌هایی در کسب توافقی بسیار گسترده بین روسیه، چین، آمریکا و بریتانیا در خصوص برخی اصول و هنجارهای کلی برای اداره امنیت سایبری مانند اعتمادسازی (که در بالا اشاره شد) حاصل شد، اما در این مباحث از مسائلی نظیر کنترل محتوا و اطلاعات که بیشتر محل مناقشه هستند، پرهیز شده است (UN Group of Government Experts Report 2010).

در سپتامبر ۲۰۱۱، اعضای سازمان همکاری شانگهای (روسیه، چین، تاجیکستان و ازبکستان) پیشنهاد کردند که دبیرکل سازمان ملل متحد امکان گفتگو پیرامون پیش‌نویس طرح جدید خود یعنی مرامنامه بین‌المللی برای امنیت بین‌المللی[1] را فراهم کند. این طرح به شکل سندی رسمی در جلسه شصت و ششم مجمع عمومی سازمان ملل متحد مطرح و تأکید شد که هدف

1. International Code of Conduct for International Security

آن کمک به دستیابی به توافق بر سر هنجارهای رفتاری بین‌المللی برای اینترنت است. این مرامنامه (ن.ک. http://news.dot-nxt.com/2011/09/13/china-russia-security-code-of-conduct) یک سری اصول پایه‌ای را مطرح می‌کند که در نگاه اول از اصول آمریکا، بریتانیا و اتحادیه بین‌المللی مخابرات چندان متفاوت نیست (Healey 2011b). برای مثال، مطابق منشور سازمان ملل متحد، زیرساخت‌های بین‌المللی و تعهد به تضمین امنیت زنجیره تأمین، «هنجارهایی» هستند که با بسیاری از اصول پیشنهادی آمریکا و بریتانیا همخوانی دارند. باوجوداین، نگاهی دقیق‌تر به منطق امنیتی پشت این طرح نقاط احتمالی اشکال را برای بسیاری از افرادی که از رویکرد چندذینفعی به امنیت سایبری و پاسداری از دسترسی، ابراز نظر و اطلاعات آزاد دفاع می‌کنند، روشن می‌سازد. شکاکان بر این باورند که برای مثال، ورای تأکید بر ترویج «برقراری مدیریت بین‌المللی چندجانبه، شفاف و دموکراتیکِ اینترنت» و توقع تعهد به «... ممانعت از دولت‌ها در استفاده از منابع، زیرساخت‌های حیاتی، فناوری‌های اصلی و دیگر مزایا، برای سرکوب حقوق کشورهای دیگر ... برای کنترل مستقل فناوری‌های ارتباطات و اطلاعات یا تهدید امنیت سیاسی، اقتصادی و اجتماعی دیگر کشورها» و «همکاری در مقابله با فعالیت‌های مجرمانه و تروریستی که از فناوری‌های ارتباطات و اطلاعات، شامل شبکه‌ها و مهار افشای اطلاعاتی که تروریسم، جدایی‌طلبی، افراط‌گرایی را تحریک یا ثبات سیاسی، اقتصادی و اجتماعی کشورهای دیگر و همچنین محیط معنوی و فرهنگی آن کشورها را به خطر می‌اندازد» منطق کنترل و نه آزادی و تاب‌آوری قرار دارد.

در اولین بندهای این مرامنامه، تشویق اتحادیه بین‌المللی مخابرات به ایفای نقش اصلی در حکمرانی اینترنت که حرکتی به سمت الگوی بین دولتی سنتی است، به‌جای حکمرانی چندذینفعی می‌تواند به بالکانیزه شدن بسیاری از فضاهای اینترنتی ملی بینجامد و چین هم از طریق نظام سازمان ملل متحد، وزن و اثر بیشتری در رأی‌دهی پیدا می‌کند. در این رویکرد دولت‌محور، برساخته و تحمیل‌شده، بازیگران دیگر کنار گذاشته می‌شوند که پیامدهایی برای مفهوم امنیت تاب‌آور برای همگان و برای فرهنگ امنیت سایبری به دنبال دارد. درباره بندهای دوم و سوم این قانون، با توجه به رویه قبلی اعضای سازمان همکاری شانگهای در تحدید جریان

اطلاعات در صورت اثرگذاری بر امنیت و فرض تسلط آمریکا بر اینترنت، نگرانی‌هایی وجود دارد که این قوانین بهانه‌ای به دست رژیم‌های سرکوبگر بدهد تا آزادی بیان و دسترسی به منابع خبری خارجی مستقل را هر چه بیشتر محدود کنند –همان اتفاقی که در قیام‌های عربی در مصر و لیبی اتفاق افتاد (ن.ک. Gjelten 2010). به‌علاوه، این موضوع به بهانه تهدید امنیت ملی می‌تواند به وضع قوانین سخت‌گیرانه در دسترسی و انتشار اطلاعات منجر شود (Healey 2011b). در نهایت، نگرانی‌هایی نیز درباره موارد نامشخص در مرامنامه وجود دارد؛ برای مثال، هیچ تعهدی به کنترل هکرهای میهن‌پرست که تحت حمایت کشورهای اصلی در جنگ سایبری هستند، وجود ندارد؛ جنگی که روسیه و چین حامیان اصلی آن محسوب می‌شوند.

جمع‌بندی: امنیت تاب‌آور در اکوسیستم سایبری بین‌المللی

درباره این موضوع که دولت‌ها و سازمان‌ها چگونه می‌توانند امنیت تاب‌آور را از طریق روش‌ها، قواعد و حالت‌های حکمرانی مختلف ایجاد کنند دستورالعمل‌ها و بحث‌های زیادی در سطح بین‌المللی وجود دارد. بااین‌حال، واضح است که بین ذینفعان همچنان بحث‌های متعددی در خصوص این موضوع وجود دارد که امنیت تاب‌آور، خصوصاً در رابطه با حقوق اساسی و توازن امنیتی چگونه باید به دست آید. افشاگری‌های اسنودن تنها به تشدید بحث حول چنین توازنی انجامید و به کشورهایی که رویکرد اول امنیت ملی را بکار می‌گیرند، توجیهی برای شدیدتر کردن کنترل بر اینترنت ارائه داد. فراتر از این، بین منطق تجاری و منطق امنیت تاب‌آور (نوع ۳) نوعی تنش وجود دارد که تاکنون ازنظر مقررات فراحکمرانی به‌درستی به آن پرداخته نشده است. همچنین بین منطق استقلال در برخی کشورها و رویکرد بازِ چندذینفعی که بسیاری از کشورهای پیشرو و سازمان‌های بین‌المللی از آن حمایت می‌کنند، نیز کشمکش وجود دارد.

این اصل در جامعه جهانی پذیرفته شده که شکل‌گیری فرهنگ امنیت جهانی در فضای مجازی مستلزم هنجارهای جهانی برای اداره رفتار دولت‌ها و بازیگران آن‌ها است؛ به‌علاوه، برای اصول کلیدی یک چارچوب جهانی، دستورالعمل‌های صریح و توافقات گسترده‌ای وجود دارد. درواقع، گروه کارشناسان سازمان ملل متحد در قابلیت اجرای قوانین بین‌المللی به توفیق‌هایی

دست یافته است؛ دستورالعمل تالین منتشر و در سازمان امنیت و همکاری اروپا بر سر اقدامات اعتمادساز توافق شد. اگرچه همگرایی خاصی در اصول کلی وجود دارد، اما هنگام تحلیل منطق حکمرانی امنیت تاب‌آور (که مبنای ساخت جنبه‌های خاص‌تری از چنین اصولی هستند) و تعیین سیاستی که از آن‌ها در داخل مرزهای مختلف ناشی می‌شود، اختلافات نمایان می‌شود. درواقع، درک بازیگران بین‌المللی مختلف و سطوح مختلف از امنیت سایبری فرصت‌ها و نیز محدودیت‌هایی را برای دستیابی به امنیت تاب‌آور در مقیاس جهانی–که با توجه به ماهیت مشکلات فراوان امنیت سایبری امری حیاتی است– ایجاد می‌کند.

به‌علاوه، این موضوع اهمیت سیاست تاب‌آوری امنیت را مشخص می‌کند که در مرکز مباحث توسعه یک اکوسیستم جهانی کارآمد قرار دارد. تنش‌ها و تعارض‌ها در ماهیت منطق‌های مختلف درون (ژئو)پلیتیک فضای سایبری –که در مرامنامه‌ها، دستورالعمل‌ها، اصول و قوانین بین‌المللی مختلف بازتاب می‌یابد– همان مقوله‌ای است که اتحادیه اروپا باید به آن بپردازد، از آن بهره‌برداری کند و به شکل مؤثری با آن ارتباط برقرار کند و آن را شکل بدهد تا تلاش‌های خود را به ثمر بنشاند. دیگر واضح است که اتحادیه اروپا در ساخت مواضع کنونی خود در اکوسیستم جهانی گسترده‌تری جا گرفته است. در فصول بعد، تأثیر هنجارهای کنونی جهانی بر شکل‌گیری راهبردهای ملی و اتحادیه اروپا و تأثیر راهبردهای ملی و اتحادیه بر شکل‌گیری هنجارهای جهانی از جنبه‌های مختلف امنیت سایبری تحلیل می‌شود.

فصل چهارم

رویکردهای ملی امنیت سایبری
در اتحادیه اروپا
نمونه مطالعاتی بریتانیا

مقدمه

اتحادیه اروپا توسعه راهبرد امنیت سایبری خود را از فوریه ۲۰۱۳ سرعت بخشیده است که این موضوع مسلماً موجب بررسی بیشتر تنوع امنیت سایبری تاب‌آور و آمادگی این حوزه در کل کشورهای عضو اتحادیه شده است. طبق تحلیل مطرح‌شده از شرایط اتحادیه اروپا در فصل‌های بعد، احتمالاً میزان آمادگی اروپا در سطح ملی مهم‌ترین بعد اکوسیستم امنیت سایبری محسوب می‌شود که عدم بهبود آن تا سطح حداقل استانداردها می‌تواند تأثیر منفی بر بلندپروازی دست‌یابی به راهبرد امنیت سایبری کارآمد در این اتحادیه داشته باشد. درواقع، راهبرد امنیت سایبری اتحادیه اروپا برای تسهیل تأمین امنیت سایبری تاب‌آور کشورهای عضو این اتحادیه و با این آگاهی ایجاد شد که در وهله نخست دولت‌های ملی باعث پیشرفت و تحول اکوسیستم امنیت سایبری اروپا می‌شوند.

باوجوداینکه بررسی اجمالی اعضای اتحادیه اروپا طرح روشنی را از شرایط نوظهور امنیت سایبری تاب‌آور در کل این اتحادیه در اختیار ما قرار می‌دهد، اما تحقیقات جامع اندکی در این زمینه در سطوح و لایه‌های مختلف میزان آمادگی امنیت سایبری صورت گرفته است و آخرین مورد (در زمان نگارش این کتاب) توسط آژانس امنیت شبکه و اطلاعات اتحادیه اروپا در سال ۲۰۰۸ انجام (ENISA 2008) و در سال ۲۰۱۰ به‌روزرسانی شد (ENISA 2010). چنین تحقیقاتی در مورد میزان آمادگی کشورها ازنظر [مقابله با] جرائم سایبری، حملات

سایبری و تاب‌آوری شبکه بیانگر تنوع و اختلافات بی‌شمار موجود در کل اروپا –یعنی کشورهای عضو اتحادیه اروپا و کشورهای منطقه اقتصادی اروپا (ایسلند، لیختن‌اشتاین و نروژ)– ازلحاظ تبادل اطلاعات و شیوه‌ها و سازوکارهای همکاری و مدیریت و گزارش‌دهی رویدادهای امنیتی، مدیریت مخاطرات و خطرهای نوظهور، تاب‌آوری شبکه، حفظ حریم خصوصی و افزایش اعتماد و آگاهی است (ENISA, Key security actors, strategies, & good practices in Europe mapped 2010).

برخورداری ۱۸ کشور عضو اتحادیه اروپا از راهبرد امنیت سایبری[۱] در مقایسه با معدود کشورهایی که در پنج سال آتی راهبرد خود را تدوین می کنند، بیانگر اختلاف موجود در اروپا و نیز پیشرفت بسیاری از کشورها در مدت‌زمان کوتاهی است. درواقع روند کلی گزارش‌های کشوری آژانس امنیت شبکه و اطلاعات اتحادیه اروپا[۲]، روند یادگیری تدریجی در چارچوب تنوع موجود است که به‌واسطه انتشار شیوه‌های مناسب موجود در کشورهای عضو پیشرو تسهیل می شود. این امر به معنای همگرایی عملی کشورهای عضو نیست، بلکه به معنای ایجاد درک مشترک از حداقل استانداردهای موردنیاز برای تأمین امنیت تاب‌آور کارآمد است.

از این نظر و گذشته از این گزارش‌ها، مسلماً کشورهای مطرح خاصی (برای مثال، بریتانیا و هلند) در حوزه رویه مناسب امنیت سایبری وجود دارند. برخی کشورها (برای مثال، مالت، پرتغال و اسلوونی) نیز بنا به دلایلی –منابع، اندازه، دانش، فرهنگ و سایر موارد– با سرعتی کندتر سیر تحول خود را طی می‌کنند (Interviews, ENISA 2012; EEAS 2013; European Commission 2013/2014). صرف‌نظر از اینکه کشورها ازنظر توانمندی و میزان آمادگی امنیت سایبری پیشرو بوده یا اخیراً وارد این حوزه شده باشند، تمام کشورهای عضو از دغدغه‌های تاریخی، اجتماعی، اقتصادی و امنیتی متفاوتی در مبحث امنیت سایبری تاب‌آور برخوردارند و درنتیجه، برداشت‌ها و نیازهای آن‌ها نیز با یکدیگر متفاوت است. این موضوع تأمین امنیت تاب‌آور کارآمد را پیچیده می‌سازد. در صورت ایجاد شرایط لازم در کل اروپا و خارج از آن، این مسئله به دلیل ماهیت جهان‌شمول آن درنهایت تنها در بلندمدت تحقق می یابد (ن.ک. فصل ۳).

ازآنجاکه بررسی جامع کشورهای عضو اتحادیه اروپا در یک فصل (احتمالاً حتی در یک جلد) امکان‌پذیر نیست، در اینجا به تحلیل دقیق مطالعه موردی یکی از اعضای مطرح اتحادیه اروپا[۳] می‌پردازیم که این مورد احتمالاً نمونه هایی از رویه مناسب را برای سایر کشورهای اروپا مطرح می کند. باوجود اشاره به‌جا به دیگر کشورهای عضو در این فصل برای انجام مقایسه تطبیقی، تحلیل و ارزیابی اصلی در مورد اقدامات بریتانیا با هدف تأمین امنیت سایبری تاب‌آور –نقاط قوت و ضعف رویکرد بریتانیا و تجربیات فراگرفتنی از سیاست‌ها و اقدامات این کشور در اروپا– صورت می گیرد. این فصل درمجموع به دنبال ارائه تصویر روشنی از جایگاه توسعه امنیت تاب‌آور کارآمد بریتانیا و نحوه ارتباط آن با تکامل و اجرای سیاست و راهبرد امنیت سایبری اتحادیه اروپا است. در بخش نخست، زمینه درک تکامل رویکرد بریتانیا در قبال امنیت سایبری مطرح می شود. در بخش دوم، راهبرد امنیت سایبری بریتانیا و به‌خصوص، مسئله حدود تأثیرگذاری اقدامات صورت گرفته برای دستیابی به اهداف اصلی آن بر تجربیات به‌دست‌آمده از طریق رویه و شیوه مناسب (و شاید نه‌چندان مناسب) مورد ارزیابی قرار می‌گیرند. در بخش نهایی این فصل، مسئله پیامدهای رویکرد بریتانیا برای امنیت سایبری تاب‌آور آن و انتقال یا انتشار احتمالی این شیوه مناسب در کل اروپا مطرح می‌شود.

روایت در حال تکامل بریتانیا از امنیت سایبری

امنیت سایبری بریتانیا در پنج سال اخیر تحت تأثیر چند منطق بوده است: نخست، تهدید مشاهده شده در حوزه امنیت ملی و احتمال ایجاد اختلال در فعالیت‌های نظامی و امنیتی شبکه دیجیتال و دوم، پیامدهای اقتصادی، سیاسی و اجتماعی گسترده‌تر مربوط به تهدیدهای امنیت سایبری ایجادشده به دلیل افزایش اتکای بسیاری از افراد، واحدهای تجاری و تأمین کنندگان زیرساخت‌های حیاتی به سیستم‌های فناوری اطلاعات و ارتباطات سایبری. مبنای این استدلال‌ها روایتی است که در راهبردهای تضمین اطلاعات بریتانیا[۱]، راهبرد های امنیت ملی و سند راهبردی بازنگری سیاست دفاعی و امنیتی[۲] شکل گرفته است. این روایت در راهبرد امنیت

1. UK's Strategies for Information Assurance
2. Strategic Defence and Security Reviews (SDSR)

سایبری به‌روزرسانی شده آن (CSSUK 2011)[۴] به اوج خود رسید که با ذکر برخی جزئیات، ابعاد اصلی برنامه ملی امنیت سایبری[۱] دولت بریتانیا را تشریح کرد.

برای مثال، تهدید صورت گرفته از جانب ابزارهای غیرنظامی با توجه خاص به تهدیدات دولتی علیه بریتانیا از طریق حملات سایبری یا جاسوسی سایبری در همان مراحل اولیه شناسایی شد (NSS 2008, p.16). توجه این روایت اولیه به حوزه های دفاع سایبری و جرائم سایبری روبه رشد در حملات سایبری ذیل حمایت دولت بود که تا حد زیادی تحت تأثیر حمله سایبری سال ۲۰۰۷ به سیستم‌ها و زیرساخت‌های خصوصی و دولتی کشور استونی و حملات سایبری به زیرساخت‌های گرجستان در سال ۲۰۰۸ در طول حمله نظامی روسیه (با تسلیحات متعارف) به این کشور قرار داشت. گرچه، مسلماً معنای موسع‌تر تهدید سایبری درک شده بود و عملکرد کارآمد فضای سایبری در بعد دفاعی و ازنظر توانایی بهره‌برداری شهروندان، واحدهای تجاری و دولت از فرصت‌هایی ضروری‌ای بود که فضای سایبری در حوزه‌های اقتصادی، اجتماعی، فرهنگی و سیاسی ایجاد می کند (Cyber Security Strategy of the UK 2009; Digital Britain 2009).

بدین ترتیب، تضمین امنیت تاب‌آور کارآمدتر در بریتانیا مستلزم ایجاد و توسعه اقدامات و ساختارهای نهادی جدید بود. برای مثال، راهبرد امنیت سایبری بریتانیا[۲] (p.3 ,2009) مسئله ضرورت اتخاذ «رویکردی منسجم در قبال امنیت سایبری» را مطرح می کند که «دولت، سازمان‌های کل بخش‌ها، عموم مردم و شرکای بین‌المللی همگی در آن نقش دارند». البته سازمان‌های دیگری نیز وجود داشتند که وظیفه آن‌ها مقابله با تهدیدات سایبری بود که مهم ترین آن‌ها عبارت‌اند از: گروه امنیتی ارتباطات الکترونیک[۳] (بخشی از ستاد ارتباطات دولتی بریتانیا[۴]) که اداره تیم واکنش اضطراری رایانه‌ای بریتانیا[۵] را بر عهده داشت که از طرف بخش دولتی برای هشداردهی و ارائه کمک در حل‌وفصل رویدادهای جدی فناوری اطلاعات عمل

1. National Cyber Security Programme (NCSP)
2. Cyber Security Strategy in the UK (CSSUK)
3. Communications-Electronics Security Group (CESG)
4. Government Communication Headquarters (GCHQ)
5. Computer Emergency Response Team (Gov-CertUK)

می کرد و سازمان ملی فنی برای تضمین اطلاعات[1] را ایجاد کرد؛ مرکز حفاظت از زیرساخت‌های ملی[2] که نقشی مشابه تیم واکنش اضطراری رایانه‌ای بریتانیا اما در حوزه واحدهای تجاری و تأمین کنندگان زیرساخت‌های حیاتی بریتانیا بر عهده داشت و وزارت کشور، آژانس جرائم مهم سازمان‌یافته[3] و پلیس (تأسیس واحد مرکزی جرائم سایبری پلیس در سال ۲۰۰۸) از طریق ابتکارهایی نظیر راهبرد جرائم اینترنتی انجمن رؤسای پلیس[4] با یکدیگر در زمینه جرائم سایبری همکاری کردند (ن.ک. مبحث بعد). گرچه، احساس می‌شد تأمین امنیت تاب‌آور کارآمدتر مستلزم وجود توانمندی امنیت سایبری مرکزی بود و این توانمندی برای نخستین بار در بریتانیا[(5)] از طریق تأسیس سازمان‌های زیر ایجاد شد: دفتر امنیت سایبری[5] (تشکیل در دفتر کابینه) با هدف ایجاد انسجام و رهبری راهبردی بیشتر در دولت، مرکز عملیات‌های امنیت سایبری[6] در ستاد ارتباطات دولتی بریتانیا برای نظارت و هماهنگسازی واکنش‌دهی به رویدادها و درک بهتر حملات علیه شبکه‌ها و کاربران این کشور و ارائه مشاوره و اطلاعات بهتر در مورد خطرات پیش روی واحدهای تجاری و مردم (Ibid., p.5).

گذشته از این موضوع، اصول اساسی مطرح‌شده در راهبرد امنیت سایبری بریتانیا (p.9–11 ,2009) مسلماً به درک شرایط لازم برای ایجاد اکوسیستم امنیت سایبری تاب‌آور در بریتانیا اشاره داشتند. برای مثال، بر تعامل با تمام طرف‌های ذینفع از طریق مشارکت و حفظ توانمندی‌های کارآمد، متعادل و تاب‌آور و نیز همکاری با شرکای بین‌المللی تأکید گردید تا ایجاد محیط جهانی و قاعده‌مندی برای رسیدگی به مسائل امنیت سایبری تضمین شود. ساختارها و اصول سایبری جدید به‌عنوان عوامل اصلی دست‌یابی به جریان‌های کاری تلقی می‌شدند که موجب ایجاد تغییرات آتی برای تأمین امنیت تاب‌آور بهتر می‌شدند. این مورد تنها شامل افزایش میزان آمادگی و حفاظت و بهبود محیط حقوقی، نظارتی و سیاست‌گذاری در سطح داخلی و بین‌المللی نمی‌شد، بلکه افزایش آگاهی و تغییر فرهنگی را نیز به همراه داشت. درواقع، ایجاد

1. National Technical Authority for Information Assurance
2. The Center for the Protection of National Infrastructure (CPNI)
3. Serious Organised Crime Agency (SOCA)
4. Association of Chief Police Officers (ACPO)
5. Office of Cyber Security
6. Cyber Security Operations Centre

تغییرات لازم در فرهنگ سایبری و «نهادینه‌سازی امنیت سایبری در ابعاد وسیع‌تر تدوین سیاست» از اهداف مهم این جریان کاری محسوب می‌شدند. علاوه بر این، مشخص بود که رفع شکاف‌های مهارتی مستلزم افزایش مهارت‌ها و آموزش، تدوین راهبرد صنعتی برای امنیت سایبری و وجود انسجامی فراتر از بریتانیا برای امنیت سایبری که مسئله جهان‌شمولی محسوب می‌شد و درک بهتر مسئله ماهیت توانمندی‌ها و حکمرانی برای تضمین امنیت تاب‌آور کارآمد بود (Ibid., p.18–20).

دولت وقت حزب کارگر بریتانیا برنامه اولیه و اصول ایجاد امنیت تاب‌آور کارآمد را ایجاد کرد و نسبت به شرایط لازم برای دستیابی به سطح تاب‌آوری کامل در بریتانیا نیز آگاهی عملی داشت. گرچه، در عمل به‌رغم کسب دستاوردهای خاص (برای مثال، در زمینه جرائم اینترنتی)، نقاط ضعف جدی برای ایجاد چنین شرایطی در ساختارهای موجود –ازلحاظ مهارت، تخصص، رهبری و منابع لازم برای ایجاد اکوسیستم تاب‌آور و درواقع، فرهنگ تفاهم، همکاری و هماهنگی موردنیاز در دولت، بین دولت و سایر طرف‌های ذینفع و بین دولت و شرکای بین‌المللی آن– وجود داشت.

ازاین‌رو، چالش اصلی پیش روی دولت ائتلافی بریتانیا (محافظه‌کار/ لیبرال دموکرات) که در مه ۲۰۱۰ به قدرت رسید تکیه به این رویکرد، ارتقای مشخصات امنیت سایبری (Downing 2011, p.9) و ارائه منابع و روایتی بود که تمام طرف‌های ذینفع را متقاعد نماید که امنیت سایبری باید تبدیل به یکی از اولویت‌های امنیت ملی شود. درواقع، به نظر می‌رسد که باوجود بلندپروازی و درک برخی عناصر دولت از ایجاد رویکردی منسجم‌تر با هدف تأمین امنیت سایبری تاب‌آور، کماکان باید کار بسیاری در سطح فرهنگی برای متقاعدسازی برخی وزارتخانه‌های دولتی فراتر از وزارت دفاع و ستاد ارتباطات دولتی بریتانیا و نیز بخش خصوصی مبنی بر این صورت می‌گرفت که تهدید سایبری باید در معنای وسیع‌تری (اقتصادی و اجتماعی) درک شود که این کار مستلزم مداخله طیف وسیعی از طرف‌های ذینفع است (Neville-Jones and Phillips 2012, p.32)[۶]. علاوه بر موارد عدم مهارت و تخصص، کمبود منابع به‌عنوان مانع اصلی پیش روی ایجاد واکنش‌های کارآمدتر، به‌خصوص در حوزه جرائم اینترنتی مورد تأکید قرار گرفت

(Downing 2011, p.10). برداشت خاصی نیز در مورد سازوکار ناموفق و نامنسجم واکنش‌دهی مرکزی و این مسئله وجود داشت که اشتراک اطلاعات بین بازیگران دولتی و خصوصی باید ازلحاظ کیفی و کمی بهبود می‌یافت. برخی شواهد حاکی از این است که رویکرد بریتانیا به‌اندازه لازم جامع نبود و تضمین امنیت تاب‌آور کارآمدتر مستلزم تغییر فرهنگی بخش‌های عمومی و خصوصی بود (Cornish et al. 2011, p.viii)[۷].

اولویت‌بندی سریع امنیت سایبری به نحوی به دست آمد که برخی محققان آن را امنیتی‌سازی (عدم)امنیت سایبری می‌نامند (برای مثال، برای مورد بریتانیا ن.ک. Dunn Cavelty 2008a). در این مورد نمونه‌های به‌دقت انتخاب‌شده میزان فزاینده تأثیرگذاری جرائم اینترنتی بر وزارتخانه‌های دولتی مانند وزارت کار و امور بازنشستگان[1] و به‌طور گسترده‌تر، سرقت مالکیت معنوی مانند اطلاعات مربوط به طراحی و عملکرد جنگنده مشترک اف۳۵ را نشان می‌دادند (Neville-Jones and Phillips 2012, p.32). این موارد در سند راهبردی بازنگری سیاست دفاعی و امنیتی برای متقاعدسازی وزارتخانه‌های دولتی در مورد ضرورت رسیدگی به مسئله امنیت سایبری مورد استناد قرار گرفتند و موجب شد در اکتبر ۲۰۱۰ امنیت سایبری به خطر شماره یک راهبرد امنیت ملی بریتانیا تبدیل شود و در اولویت امنیت ملی قرار گیرد. بدین منظور «حملات خصمانه علیه فضای سایبری بریتانیا از جانب کشورهای دیگر و جرائم اینترنتی گسترده» به‌عنوان یکی از خطرات دارای اولویت در کنار بحران‌های نظامی، رویدادهای مهم و خطرات طبیعی و تروریسم دسته‌بندی شد (UKNSS, p.27). این اولویت‌ها بازتاب اولویت‌های راهبردی اتحادیه اروپا برای امنیت داخلی خود نیز محسوب می‌شدند (The EU Internal Security Strategy 2010). درنهایت بودجه جدیدی –مبلغ ۶۵۰ میلیون پوند در طی پنج سال– در سند راهبردی بازنگری سیاست دفاعی و امنیتی (تنها) برای حوزه امنیت سایبری اختصاص داده شد. درواقع، به‌عنوان بخشی از بررسی مخارج سال ۲۰۱۳، مبلغ ۲۱۰ میلیون پوند دیگر به طرح‌های امنیت سایبری جدید و موجود اختصاص یافت –افزایش کل بودجه برای این برنامه به ۸۶۰ میلیون پوند رسید (صرف بودجه در مارس ۲۰۱۶).

1. Department for Work and Pensions (DWP)

راهبرد امنیت سایبری بریتانیا: ایجاد امنیت تاب‌آور کارآمد؟

در اینجا این پرسش‌ها مطرح می‌شوند که اهداف اصلی راهبرد تدوین‌شده دولت ائتلافی بریتانیا برای بهبود امنیت سایبری تاب‌آور در بریتانیا چه بود؟ چگونه برنامه امنیت سایبری بریتانیا برای ایجاد شرایط لازم و سازوکارهای حکمرانی برای امنیت سایبری تاب‌آور عملاً شکل گرفت؟ و چه مواردی از تجربه و شیوه رو به تکامل بریتانیا را می‌توان در سایر کشورهای اروپا اجرا کرد؟

همان‌طور که اشاره شد، راهبرد امنیت سایبری بریتانیا (UKCSS 2011) در سال ۲۰۱۱ با چشم‌اندازی واحد و اولویت‌هایی با چهار هدف اصلی بازبینی شد. این چشم‌انداز بازتاب منطق‌های غالب و محرک بود و هدف آن «کسب ارزش اقتصادی و اجتماعی کلانی از فضای سایبری پویا، تاب‌آور و امنی بود که در آن اقدامات ما تحت هدایت ارزش‌های اصلی در زمینه آزادی، عدالت، شفافیت و حکمرانی قانون موجب گسترش رفاه، امنیت ملی و جامعه قدرتمند می گردند». مؤلفه آشکار بخش های عمومی و خصوصی نیز در راهبردهای اولویت‌دار زیر ملاحظه گردید (UKCSS 2011, p.8):

۱. اقدام بریتانیا برای مقابله با جرائم سایبری و تبدیل آن به یکی از امن‌ترین کشورهای جهان با هدف تجارت در فضای سایبری

۲. تاب‌آوری بیشتر بریتانیا در برابر حملات سایبری و بهبود توانایی آن در حفاظت از منافع بریتانیا در فضای سایبری

۳. مشارکت بریتانیا در شکل‌گیری فضای سایبری باز، باثبات و پویا که از جوامع باز حمایت می‌کند و مردم بریتانیا نیز می‌توانند با خاطری آسوده از آن استفاده کنند

۴. برخورداری بریتانیا از دانش، مهارت و توانمندی با هدف تحقق تمام اهداف امنیت سایبری

درمجموع، راهبرد امنیت سایبری بریتانیا (۲۰۱۱) بیانگر تغییر قابل‌ملاحظه‌ای ازنظر نهادی و منابع رسیدگی به مسائل امنیت سایبری بود. به‌علاوه، این تصور نیز وجود داشت که عواملی نظیر رهبری و هماهنگی مرکزی حائز اهمیت بودند، چراکه مسئولیت امنیت سایبری از معاون امنیتی وزارت کشور به مسئول دفتر کابینه و امنیت سایبری[1] انتقال پیدا می‌کرد.[۸] علاوه بر این، موضوع

1. Minister for the Cabinet Office and Cyber Security

مشارکت و همکاری مؤثر در چند بعد شناسایی و اولویت‌بندی شد: از افزایش حمایت از بخش خصوصی و محافل دانشگاهی تا طراحی مشترک سیاست‌های معتبر، ایجاد برنامه‌هایی برای اشتراک مؤثرتر و لحظه‌ای داده‌ها برای امکان‌پذیری واکنش‌های سریع‌تر به حملات سایبری، تضمین به‌کارگیری استانداردهای مناسب (رژیم‌های مدیریت خطر) در بخش‌های عمومی و خصوصی، ایجاد ارتباطات بین‌المللی مؤثر با توجه به ماهیت جهانی و بدون مرز امنیت سایبری و درنهایت، تضمین ایجاد برنامه‌های ارتقای مهارت و آموزش ضروری برای گسترش تخصص در بسیاری از ابعاد امنیت سایبری تا توانایی رسیدگی به مشکلات امنیت سایبری در کوتاه، میان و بلندمدت (برای مثال، جرم‌شناسی، نظارت و جاسوسی، تضمین اطلاعات و غیره) ایجاد گردد.

ازنظر افزایش سطح آگاهی شهروندان و توانمندسازی آن‌ها به بهره‌گیری از اینترنت امن‌تر و شناسایی و به‌کارگیری آسان‌تر سازوکارهای گزارش‌دهی امنیت سایبری، عنصر فردی نیز در این بُعد آموزشی در نظر گرفته شد. از دیدگاه حکمرانی، درمجموع، دولت بریتانیا بر فراحکمرانی نظری، یعنی ایجاد انگیزه در بخش خصوصی به‌جای وضع مقررات اجباری تأکید دارد که با رویکرد آن در قبال مقررات اینترنت نیز همخوانی بیشتری دارد (Telephone Interview, UK cybersecurity official, October 2014). درواقع، به نظر یکی از مقامات، بریتانیا «درصدد ایجاد بازاری خودکفا در حوزه امنیت سایبری است» که تنها در مواردی مداخله مستقیم را مجاز می داند که توجیهی برای این کار در صورت نارسایی بازار وجود داشته باشد (Telephone Interview, Cabinet Office official, October 2014). این موضوع در تضاد کامل با این طرح مبنای دستورالعمل امنیت شبکه و اطلاعات پیشنهادی اتحادیه اروپا قرار دارد که تمام بخش‌های مالک زیرساخت‌های حیاتی را ملزم به ارائه گزارش اجباری می‌کند (برای جزئیات بیشتر ن.ک. فصل ۶).

جرائم سایبری و تأمین امنیت فضای سایبری برای واحدهای تجاری در بریتانیا: نوآوری نهادی و مشارکت بهبودیافته؟

ازلحاظ تاریخی، نخستین واکنش نهادی نسبت به جرائم اینترنتی در بریتانیا از جانب واحد جرائم ملی فناوری پیشرفته[1] در سال ۲۰۰۱ صورت گرفت و در کنار آن ۴۳ واحد جرائم محلی فناوری پیشرفته در سطح نیروی پلیس تأسیس شدند. گرچه با ادغام واحد جرائم ملی فناوری پیشرفته در آژانس جرائم مهم سازمان‌یافته (۲۰۰۶)، این واکنش برای رسیدگی مستقیم به جرائم اینترنتی عمر چندانی نداشت. درنتیجه، این امر موجب ایجاد شکاف و کاهش توجه در بخش خدمات ملی پلیس ازنظر [رسیدگی به] مسائل پیشگیری از وقوع جرائم اینترنتی گردید و سازوکار هماهنگ‌کننده اصلی مربوط به منابع جرائم الکترونیکی نیز حذف شد. علاوه بر این، توانمندی بررسی گسترده جرائم اینترنتی در حوزه هایی کاهش یافت که تحت مسئولیت آژانس جرائم مهم سازمان‌یافته قرار نداشتند (ACPO e-crime strategy 2009, p.1).

اهمیت جرائم اینترنتی منجر به ایجاد مجموعه اسناد جرائم اینترنتی انجمن رؤسای پلیس و بودجه ۳/۵ میلیون پوندی وزارت کشور برای تأسیس واحد جرائم اینترنتی پلیس مرکزی[2] در سال ۲۰۰۸ تحت هدایت خدمات پلیس کلان شهرها[3] شد[۹]. علاوه بر این، برنامه ملی جرائم اینترنتی[4] (۲۰۰۹) جهت هماهنگ سازی تعداد بی شمار طرح‌های جرائم اینترنتی برگرفته از مجموعه اسناد جرائم اینترنتی انجمن رؤسای پلیس ایجاد شد و راهبرد جرائم اینترنتی انجمن رؤسای پلیس برای برقراری ارتباط با رویکرد راهبردی خدمات پلیس کلان شهرها در قبال جرائم اینترنتی اتخاذ گردید. به‌رغم تصدیق موفقیت نسبی واحد مرکزی جرائم اینترنتی پلیس در رسیدگی به این نوع جرائم (Interview, former PCeU official, August 2014) و ایجاد الگوهای شیوه مناسب برای اشتراک اطلاعات با واحدهای تجاری (از طریق نیروی کار مجازی جهانی، برای مثال، ن.ک. Cornish et al. 2011, p.19)، مسلماً مسئله محدودیت منابع و نبود آموزش استاندارد در کل نیروهای پلیس و تخصص لازم برای مقابله با مجرمان

1. National High-Tech Crime Unit (NHTCU)
2. Police Central e-crime Unit (PCeU)
3. Metropolitan Police Service (MPS)
4. National e-crime Programme

سایبری (Interview, former PCeU official, August 2014; Downing 2011, p.10) و نیز «عدم انسجام» سازمان‌های تأسیس‌شده برای رسیدگی به مسائل امنیت سایبری (Hopkinson cited in Shah 2012)[۱۰] مطرح بود.

راهبرد امنیت سایبری بریتانیا (۲۰۱۱) و برنامه ملی امنیت سایبری مطرح‌شده با آن به دنبال بررسی دقیق رویکرد اتخاذشده در قبال جرائم اینترنتی جهت رسیدگی به نقاط ضعف اصلی مشخص‌شده و تمرکز، هماهنگی و اثربخشی راهبردی و عملیاتی بیشتر در زمینه مسئله مقابله با جرائم سایبری بودند. درنتیجه آژانس مقابله با جرائم ملی با چهار محورِ اقدام تأسیس شد: جرائم سازمان‌یافته، کنترل مرزها، جرائم اقتصادی و بهره برداری از کودکان و مرکز حفاظت آنلاین به همراه واحد ملی تازه تأسیس جرائم سایبری (تأسیس در اکتبر ۲۰۱۳) مستقر در آژانس مقابله با جرائم ملی[۱] که ارکان اصلی را پوشش می‌دهد. در اصل، واحد ملی جرائم سایبری جایگزین واحد مرکزی جرائم اینترنتی پلیس شد و بدین ترتیب، جرائم سایبری به‌عنوان نوعی جرم و ابزاری برای اجرای دیگر جرائم شناخته شد (The National Crime Agency 2011).

علاوه بر این، ۹ واحد منطقه‌ای جرائم سازمان‌یافته[۲] در سرتاسر کشور با حضور گروه‌های سایبری در هر یک از آن‌ها به‌منظور تسهیل مقابله با جرائم اینترنتی تأسیس شد. آن‌ها تحقیقاتی را انجام دادند و به واحدهای تجاری و مردم در مناطق خود ارائه مشاوره و کمک کردند.

با اینکه به گفته رئیس واحد ملی جرائم سایبری، این ساختار جدید منجر به رهبری راهبردی کارآمدتری ازنظر بهره برداری از مهارت‌ها و مشارکت‌ها در دولت، پلیس و صنعت در بریتانیا و نیز در سطح بین‌الملل شد و باعث انجام مجموعه عملیات‌های موفقیت‌آمیزی گردید (The National Security Strategy, Our Forward Plans 2013, p.5)، اما کماکان مشکلات بی شماری در زمینه ایجاد شرایط مؤثر برای تأمین امنیت تاب‌آور در حوزه جرائم اینترنتی وجود دارند. برای مثال، گزارش سازمان ملی حسابرسی[۳] (Update on the National Cyber Security Programme 2014, p.11) به کمبود کارکنان واجد شرایط و توانمندی فنی در واحد ملی جرائم سایبری و گروه‌های سایبری مستقر در واحدهای منطقه‌ای جرائم سازمان‌یافته

1. National Crime Agency (NCA)
2. Regional Organised Crime Units (ROCU)
3. National Audit Office Report

برای مقابله با میزان (افزایش) جرائم اینترنتی مشاهده‌شده، اشاره می‌کند. باوجود طرح این استدلال که با سرمایه‌گذاری بیشتر بر آموزش‌های تخصصی و افزایش ظرفیت ازنظر پشتیبانی خط مقدم می توان به این مسائل رسیدگی نمود و آن‌ها را تحت نظارت ملی انجمن رؤسای پلیس هماهنگ کرد (The National Security Strategy, Our Forward Plans 2013, p.5)، اما دیگران کماکان مشکلات مربوط به فقدان استانداردسازی چنین آموزش‌هایی و نبود آموزش سایبری متداول که اساس آموزش عمومی افسران پلیس است را مطرح می‌کنند. درواقع، توجه رهبر مرکزی به این مورد، مسئله محل «خرید» آموزش توسط رهبر منطقه‌ای را حل نمی کند و درنتیجه، این امر تضمین نمی گردد که مجموعه مهارت‌های مناسب در کل ابعاد مربوط به جرائم اینترنتی –پیشگیری، شناسایی، تحقیق و پیگرد قضایی– کسب می‌شوند. علاوه بر این، درصورتی‌که هدف نهادینه سازی و رواج فرهنگ امنیت سایبری در تمام سطوح عملیاتی باشد، راه‌حلی باید برای این مسئله پیدا کرد و رویکرد جامع‌تری نیز نسبت به آموزش باید اتخاذ شود (برای مثال، ن.ک. Tightening the Net 2015).

گذشته از این موضوع، دولت بریتانیا به دنبال تعامل مؤثرتر با طرف های ذینفع مربوطه در سطح داخلی و بین‌المللی برای رفع تهدید جرائم اینترنتی است. در داخل کشور، بخش مشارکت در کاهش جرائم سایبری وزارت کشور[1] تأسیس شد که درصدد ایجاد همکاری میان دولت، صنعت، دانشگاه و نهادهای مجری قانون –به رهبری وزارت کشور و وزارت کسب‌وکار، نوآوری و مهارت[2]– برای هماهنگی اقدامات صورت گرفته در زمینه جرائم سایبری و به‌خصوص، به دنبال فرصت هایی برای مشارکت جهت ارائه کمک‌های عملی به شرکت‌های کوچک و متوسط و شهروندان و احتمالاً حذف جرائم سایبری است. در بعد بین‌المللی نیز بریتانیا در ایجاد ترتیبات نوآورانه مشترک –تک موردی و نهادینه‌تر– برای مقابله با انواع جرائم اینترنتی پیشرو بوده است (اقدام موردی). برای مثال، در راه مقابله با بدافزار سرقت از بانک و به‌خصوص، برای مقابله با تروجان شایلاک[3] (۱۱)، آژانس مقابله با جرائم ملی شرکایی ازجمله اداره تحقیقات فدرال آمریکا

1. Home Office Cyber Crime Reduction Partnership (CCRP)
2. Department of Business, Innovation and Skills (BIS)
3. Shylock Trojan

(اف بی آی)، یوروپل، موسسه مشاوره‌ای هوش کاربردی سیستم‌های بی‌اِی‌ئی[1]، ستاد ارتباطات دولتی بریتانیا، شبکه‌های امن دل[2]، آزمایشگاه کسپرسکی[3] و پلیس فدرال آلمان را گرد هم آورد. عملیات ها از واحد عملیات در مرکز مقابله با جرائم اینترنتی اروپا و از دیدگاه امنیت تاب‌آور انجام می شد که امکان همکاری مؤثر بین محققان سایبری را با هماهنگی آژانس مقابله با جرائم ملی و پشتیبانی شرکای کشوری سازمان یافته ضروری مربوطه فراهم می آورد (UK leads international partnership to fight cybercrime, 2013).

در رهبری نهادینه‌تر این ترتیبات، کارگروه اقدام مشترک علیه جرائم اینترنتی در سپتامبر ۲۰۱۴ در مرکز مقابله با جرائم سایبری اروپا به سرپرستی اندی آرچیبالد[4]، معاون واحد ملی جرائم سایبری بریتانیا، تأسیس شد. این کارگروه به‌رغم اینکه نسبتاً تازه تأسیس است، به موفقیت‌های عملیاتی دست یافت و حتی مسائل مهمی را برای بریتانیا و دیگر کشورهای عضو اتحادیه اروپا (و نیز کشورهای غیر عضو) آشکار ساخت که در صورت ایجاد شرایط لازم برای مشارکت و همکاری کارآمد در فضای سایبری اروپا باید به آن‌ها رسیدگی شود. یکی از این موارد مربوط به لایه حقوقی و نحوه امکان دسترسی لحظه‌ای به مدارک است. در برخی کشورهای عضو اتحادیه اروپا (که به‌مانند بریتانیا تمایل دارند تحت رهبری پلیس باشند)، برای مثال، دسترسی به آدرس‌های آی‌پی تقریباً به‌سرعت انجام می‌شود(۱۲)، اما در سایر کشورها که افسران پلیس باید قبل از دسترسی به آی‌پی از دادستان حکم قضائی دریافت کنند، زمان باارزش برای اخلال در کار مجرمان سایبری عملاً از دست می‌رود (Interview, EC3 official, September 2014; see also UK-led cybercrime taskforce proving its worth, 2014). موضوع دیگر مربوط به اشتراک اطلاعات، به‌ویژه با شرکای غیر عضو اتحادیه اروپا و شرکت‌های خصوصی است. در اینجا کارگروه اقدام مشترک علیه جرائم اینترنتی نیز در حال طراحی سیستم رمزنگاری است که به مسائل مربوط به حریم خصوصی می‌پردازد و درعین‌حال، تضمین می‌کند که اطلاعات به اشتراک گذاشته‌شده مختص یک کار یا تحقیق موردی به‌خصوص (به‌جای تبادل

1. BAE Systems Applied Intelligence
2. Dell Secure Networks
3. Kaspersky Lab
4. Andy

حجم انبوه اطلاعات) است. بااینکه این کار در بهترین حالت روند تکوینی دارد، اما در صورت موفقیت می‌توان آن را به‌عنوان الگوی شیوه مناسب در کل اروپا و خارج از آن انتشار داد (Ibid.) و به دنبال راهی برای رسیدگی به مسئله موازنه بین حفظ حریم خصوصی و تأمین امنیت بود بحثی که در سال ۲۰۱۳ با افشاگری‌های ادوارد اسنودن تشدید و این مسئله نیز افشا شد که ستاد ارتباطات دولتی بریتانیا در جمع‌آوری گسترده اطلاعات از شهروندان مشارکت داشته است. درواقع، گرچه جمع‌آوری داده‌های انبوه بدین نحو با هدف تأمین امنیت در بریتانیا بحث‌برانگیز است، اما دولت ادامه این شیوه را با تصویب قانون جدیدی در سال ۲۰۱۴ –قانون حفظ داده‌ها و اختیارات تحقیق[1] – تضمین کرده است. شایان‌ذکر است که بنا به حکم دیوان دادگستری اتحادیه اروپا که دستورالعمل حفظ داده‌ها (۲۰۰۶) را در آوریل ۲۰۱۴ بی‌اعتبار اعلام کرد، چنین اقدامی غیرقانونی است، چراکه موجب مداخله بیش‌ازحد در امور شهروندان و نقض حقوق آن‌ها در زمینه حفاظت از اطلاعات و حریم خصوصی می‌شود. تنش موجود در بریتانیا بین منطق امنیت ملی آن(۱۳) که موجب اجرای چنین شیوه‌ای است و طرح‌های آن برای تأمین امنیت تاب‌آور از طریق مجموعه گسترده‌تر اهداف امنیت سایبری باید رفع شود (ن.ک. فصل ۷).

تأمین امنیت فضای سایبری برای واحدهای تجاری: مشارکت، اشتراک اطلاعات و استانداردها

بخش اصلی رویکرد بریتانیا در قبال امنیت سایبری، همکاری با بخش خصوصی جهت ارتقای استانداردها، آگاهی و ایجاد انگیزه برای اشتراک اطلاعات است که تمام این موارد شرایط لازم برای تأمین امنیت تاب‌آور کارآمد محسوب می‌شوند. با توجه به مورد دوم، مشارکت در اشتراک اطلاعات در امنیت سایبری[2] برنامه عمومی–خصوصی اصلی (راه‌اندازی در مارس ۲۰۱۳) برای دست‌یابی به این مورد است. با ادغام تیم واکنش اضطراری رایانه‌ای بریتانیا در نهاد دولتی جدید (تأسیس در آوریل ۲۰۱۴ - ن.ک. مبحث بعد)، این طرح از هدفِ برخورداری از ۵۰۰ عضو فراتر رفته است و قصد دارد اعضای بیشتری را از واحدهای تجاری، آموزشی و دیگر بخش‌ها

1. Data Retention and Investigatory Powers Act
2. Cyber Security Information Sharing Partnership (CISP)

جذب کند. طرح اصلی این مشارکت ایجاد محیط مبتنی بر اعتماد است که دولت و صنعت بتوانند داده‌های خود در مورد تهدیدات، رویدادها و نقاط آسیب‌پذیری سایبری را در آن به‌طور لحظه‌ای به اشتراک گذارند. این اطلاعات توسط اعضا فراهم می‌شود و گروه اصلی متشکل از تحلیل‌گران امور دفاعی شبکه دولت و صنعت به بررسی داده‌ها می‌پردازد و داده‌های مناسبی را در اختیار اعضای این طرح مشارکت قرار داده و به آن‌ها مشاوره می‌دهد. بااینکه ابتدا توجه این گروه به بعد فنی بود، اما افزایش اعضا به معنای این است که این طرح مشارکت اطلاعات کلی‌تری را نیز برای ارتقای سطح آگاهی در زمینه مسائل امنیت سایبری در اختیار [شرکای آن] قرار می‌دهد.

نظریه مطرح‌شده در اینجا این است که برنامه این طرح مشارکت امکان اقدام فعالانه بیشتر را به اعضا برای حفاظت از خود در برابر تهدیدات سایبری و امکان اشتراک اطلاعات به‌صورت علنی یا ناشناس می‌دهد که مورد دوم به دلیل تأثیر احتمالی اقتصادی اشتراک اطلاعات بر رویدادها به‌خصوص برای افراد شکاک حائز اهمیت است. درواقع، نقاط به سبک این مشارکت در رویدادهای مختلفی ازجمله نشست سران ناتو در کاردیف (۲۰۱۴) و بازی‌های کشورهای مشترک‌المنافع در گلاسکو (۲۰۱۴) به‌کار رفته‌اند و با بازتاب الگوی واحدهای منطقه‌ای جرائم سازمان‌یافته، نقاط این مشارکت نیز به‌طور منطقه‌ای در بریتانیا گسترده می‌شوند تا اعضاء بتوانند «روابط مبتنی بر اعتماد بیشتری را با شرکایی که از قبل می‌شناسند ایجاد کنند» (Gibsoncited in UK cyber threat sharing ahead of target, 2014)[۱۴]. طبق فصل ۵، آشنایی و اعتماد اجزای اصلی ایجاد بسترها و سازوکارهای اشتراک مؤثر و مشارکتی اطلاعات محسوب می‌شوند.

با ذکر این مطلب، مسئله احتمالی که باقی می‌ماند نحوه اشتراک اطلاعات و مسیر آن است. برخی مفسران به نبود جریان اطلاعات از ستاد ارتباطات دولتی بریتانیا به صنعت اشاره کرده‌اند[۱۵] و درواقع، این استدلال را مطرح می‌کنند که سازوکارهایی که به‌وسیله آن‌ها اطلاعات دریافتی سرویس‌های اطلاعاتی به‌طور لحظه‌ای مورداستفاده و اشتراک قرار می‌گیرند باید برای جلوگیری از تهدیدهای سایبری و حفاظت در برابر آن‌ها یکپارچه و اصلاح شوند (Interview,Anonymous, August 2014). درواقع، نظرسنجی مؤسسه تحقیقاتی اینفوسک[۱] در سال ۲۰۱۴ نشان داد که به نظرِ ۶۷

درصد از متخصصان امور امنیت اطلاعات، اطلاعات به نحو کارآمدی بین دولت و صنعت به اشتراک گذاشته نمی‌شود (cited in Update on the National Cyber Security Programme 2014, p.12). همچنین طبق اذعان مدیر تیم واکنش اضطراری رایانه‌ای بریتانیا، به‌رغم افزایش تصاعدی عضویت در این طرح مشارکت، کماکان باید مسیر طولانی‌ای به دلیل ایجاد موازنه در تعداد اعضا –تعداد معدود نمایندگان شرکت‌های کوچک و متوسط– طی شود. درصورتی‌که هدف تکامل رویکرد جامع‌تری به امنیت سایبری در بریتانیا باشد، ایجاد انگیزه همکاری در شرکت‌های کوچک و متوسط بسیار حائز اهمیت است.

یکی دیگر از ویژگی‌های اصلی رویکرد دولت بریتانیا به ایجاد ساختارهای بازاری برای تأمین امنیت تاب‌آور کارآمد، ایجاد انگیزه برای توسعه استاندارد سازمانی صنعت محور برای واحدهای تجاری به‌منظور شفاف‌سازی ماهیت شیوه مناسب برای شرکت‌ها و وجه تمایز آن در بازار است. در این زمینه، دولت بریتانیا استاندارد «الزامات سایبری»[۱۶] را تدوین کرده است که بر اساس آن وزارت دفاع تأمین‌کنندگان خود را ملزم به رعایت آن به‌عنوان بخشی از فرآیند استاندارد انعقاد قرارداد می‌سازد. درواقع، هدف دولت بریتانیا اجباری ساختن این استاندارد در کل تدارکات دولت در زمان مناسب برای عدم تحمیل هزینه‌های بیشتر بر واحدهای تجاری، به‌خصوص شرکت‌های کوچک و متوسط است.

علاوه بر این، یکی دیگر از انگیزه‌های دولت بریتانیا ایجاد بازار بیمه سایبری این کشور در کنار صنعت بیمه است تا اصلاحاتی در حوزه مدیریت خطرات سایبری صورت گیرد. بااینکه در زمان نگارش این کتاب، این موضوع صرفاً در حد توافق در زمینه اهداف کلی است، اما این موضوع رویکرد حکمرانی نظری کلی دولت بریتانیا در قبال ایجاد انگیزه در صنعت و آگاه سازی مصرف‌کنندگان را در کنار ارائه طرح‌هایی مانند گواهینامه کیفیت محصولات و خدمات و صدور گواهینامه (برای محصولات، خدمات و تخصص‌ها) و نیز طرح‌های راهنمایی (ن.ک. کادر ۴-۱) تکمیل می‌کند که هدف آن‌ها افزایش آگاهی و تسهیل حرکت به سمت تأمین امنیت تاب‌آور کارآمدتر از طریق تغییر رفتار طرف‌های ذینفع در حوزه امنیت سایبری است.

1. InfoSec

ارائه راهنمایی خاص برای مخاطبان مختلف، تجربه اصلی به‌دست‌آمده دولت بریتانیا در تکامل راهبرد امنیت سایبری خود است –بازخورد اولیه نشان می‌دهد که شرکت‌های کوچک و متوسط به‌خصوص به راهنمایی بیشتری متناسب با الگوهای تجاری و امکانات منابع خاص خود نیاز داشتند و اقدام دولت در جهت ایجاد تغییر در رفتار این نوع شرکت‌ها کمترین تأثیر را در مقایسه با دیگر طرف-های ذینفع داشت (Update on the National Cyber Security Programme 2014, p.15–16). درواقع، راهنمای واحدهای تجاری کوچک با توسعه طرح اقدام سایبری برای این واحدها با همکاری صنعت به‌روزرسانی (ژانویه ۲۰۱۵) و تکمیل شد که هدف آن کمپین‌های تبلیغاتی در زمینه اطلاعات و راهنمایی و احتمالاً در قالب نوآورانه‌تر، طرح سند نوآوری[1] امنیت سایبری به ارزش ۵ هزار پوند برای واحدهای تجاری کوچک و متوسط با هدف ایجاد انگیزه در آن‌ها برای سرمایه‌گذاری در ارتقای امنیت سایبری و افزایش ظرفیت رشد خود بود (UKCSS: Report on Progress and Forward Plans, Cabinet Office December 2014, p.6).

کادر ۴-۱. راهنمای امنیت سایبری برای کسب وکارها

برنامه «۱۰ قدم» برای امنیت سایبری	راهنمایی برای مدیران اجرایی و اعضای هیئت مدیره در خصوص حفظ ارزشمندترین دارای‌های خود ازجمله داده‌های شخصی، خدمات برخط و مالکیت معنوی
کسب‌وکارهای کوچک: درچه‌موضوعاتی در خصوص امنیت سایبری نیاز به اطلاع دارند؟	راهنمایی مبتی بر برنامه «۱۰ قدم» و مناسب‌سازی شده برای بنگاه‌های بسیار کوچک، کوچک و متوسط
مسئولیت برای اطلاعات	یادگیری مجازی برای بنگاه‌های بسیار کوچک، کوچک و متوسط، دسترسی رایگان و نقش‌محور برای کارمندان، صاحبان و مدیران دارایی‌های اطلاعات یا صاحبان کسب‌وکارها
امنیت سایبری برای مشاغل حقوقی و حسابداری	یادگیری مجازی برای کمک به وکلا و حسابداران با هدف حمایت از خود، موکلان و مشتریان و اطلاعات حساسی که از این افراد در اختیار دارند
امنیت سایبری برای مدیران غیراجرایی	راهنمایی برای حمایت از مدیران غیراجرایی که می توانند در حوزه امنیت سایبری توصیه‌هایی در اختیار شرکت‌ها قرار داده و آن‌ها را نسبت به مدیریت مطلوب مخاطرات سایبری تشویق کنند
امنیت سایبری در امور مالی شرکتی	راهنمایی از سوی صنایع با هدف کمک به برخورد با تهدیدات سایبری در خصوص ادغام، مالکیت و واگذاری شرکت و نیز سرمایه‌گذاری مخاطره‌آمیز

Source: UKCSS: Report on Progress and Forward Plans, Cabinet Office (2014, p.4)

1. Innovation Voucher Scheme

طرح اجرای استاندارد الزامات سایبری و ایجاد انگیزه در این زمینه، باعث تضمین پذیرش این استاندارد توسط تمام طرف‌های ذینفع مربوطه نمی‌شود. این امر به‌خصوص در مورد ماهیت جهانی تجارت و دسترس‌پذیری استانداردها و مقررات صنعتی خاص و سایر استانداردهای بین‌المللی صدق می‌کند. این موضوع نیز مسئله سازگاری استانداردها برای شرکت‌های بزرگ بین‌المللی را مطرح می‌سازد که در سراسر و داخل سایر حوزه‌های قضایی فعالیت می‌کنند (Neville-Jones and Phillips 2012, p.39)، گرچه، شواهدی از همکاری سازمان‌های استاندارد مختلف با یکدیگر و با صنعت برای حل این مسئله جهت دست‌یابی به هم‌افزایی و شناخت متقابل وجود دارد (EU NIS Cyber Security meeting, Brussels June 2014). علاوه بر این و به نظر برخی نمایندگان صنایع، به‌رغم قابل‌ستایش بودن طرح استاندارد صنعت محور، این امر تنها یک حداقل محسوب می‌شود و شرکت‌ها باید کار بسیار بیشتری برای تضمین امنیت داده‌ها و تأمین امنیت تاب‌آور انجام دهند (UK cyber security progress welcomed, 2013).

درنهایت، هدف اصلی دولت بریتانیا از بهبود امنیت سایبری تاب‌آور خود به حداکثررسانی فرصت‌هایی است که این امر در اختیار صادرات بخش امنیت سایبری قرار می‌دهد و به‌خصوص، دستیابی به هدف دولت در زمینه افزایش سهم بازار جهانی خود تا ۲ میلیارد پوند تا سال ۲۰۱۶ است. برای نیل به این هدف، طرح مشارکت رشد سایبری[1] مشترک (دولت و صنعت) همراه با انجمن تجارت فناوری[2] (نماینده ۸۵۰ سازمان فناوری بریتانیا) راه‌اندازی شد که وظیفه آن ارتقای طرح تأمین امنیت سایبری دولت[1] (۱۷) هماهنگ‌سازی کمپین‌های صادرات و همکاری با دولت برای تدارک آموزش و تعلیم در حوزه امنیت سایبری با هدف حمایت از رشد بخش امنیت سایبری بریتانیا است (The National Cyber Security Policy 2013, p.4).

بااینکه ارزیابی جامع اثربخشی این مشارکت در زمان نگارش این مطلب خیلی زود است، اما شواهد حاکی از این است که طرف‌های دخیل، در سطح گروه‌های تجاری منطقه‌ای تأسیس‌شده و حاضر در طرح تأمین امنیت سایبری دولت (بیش از ۳۵ شرکت انگلیسی) از نظرات مطرح‌شده در مورد محصولات، راهنمایی و آموزش امنیت سایبری منتفع می‌شوند. علاوه بر این، ستاد

1. Cyber Growth Partnership
2. TechUK

ارتباطات دولتی بریتانیا رویکرد جامع‌تری در مورد شرکت‌های کوچک و متوسط در قراردادهای غیرمحرمانه‌ای دارد که قبلاً نادیده گرفته شده بودند. چنین رویکرد فراگیری ازلحاظ تاب‌آوری و به‌خصوص به دلیل انتقادات سازمان ملی حسابرسی (Update on the National Cyber Security Programme 2014, p. 17) از این مسئله حائز اهمیت است که وزارت تجارت و سرمایه‌گذاری بریتانیا[۲] که وظیفه آن پشتیبانی از تجارت و صادرات در حوزه امنیت سایبری از طریق سازمان دفاع و امنیت[۳] خود است در اصل به معاملات بزرگ با پیمانکاران امور دفاعی و دریایی و شرکت‌های تأسیس‌شده توجه دارد. گذشته از این، ترتیبات حکمرانی جدید در قالب مرکز نوآوری در گلاسترشر[۴] برای تسهیل همکاری در امور تحقیقاتی، آزمایش و توسعه قوانین بین کارکنان و صنعت با برنامه‌هایی برای شمول واحدهای تجاری کوچک و متوسط و شرکت‌های استارتاپ و گسترش آن به سطح ملی مطرح شده‌اند (UKCSS: Report on Progress and Forward Plans, Cabinet Office December 2014, p.8–10).

حملات سایبری و تاب‌آوری

توسعه شبکه بخش دولتی[۵] جدید به‌عنوان الگوی امنیتی برای اشتراک خدمات در کل سازمان‌های دولتی، یکی از ابعاد هدف دولت بریتانیا در تاب‌آوری بیشتر این کشور در برابر حملات سایبری، یعنی حفاظت از سیستم‌های خود و تاب‌آور سازی بیشتر آن‌ها از طریق ایجاد استانداردهای مشترک، نظارت بر امنیت و انطباق و تأمین تاب‌آوری بهتر شبکه بوده است. به‌رغم پیشرفت حاصله در این حوزه، با حضور تمام مقامات و شوراهایی که بخشی از شبکه دولتی محسوب می‌شوند، این مورد درباره تمام تأمین‌کنندگان و وزارتخانه‌های دولت مرکزی صدق نمی‌کند. گرچه، هدف گسترش این مورد و فرآیند تبعیت از استانداردهای فنی و امنیتی مناسب اعتباردهی در کل شبکه دولتی تا پایان سال ۲۰۱۵ است. دولت بریتانیا نیز اقداماتی را در این

1. Cyber Security Supplier to Government Scheme (CSSGS)
2. UK Trade and Investment (UKTI) Department
3. Defence and Security Organisation (DSO)
4. Gloucestershire
5. Public Sector Network (PSN)

زمینه –برای مثال، سیستم تضمین هویت طراحی‌شده توسط سرویس دیجیتال دولت بریتانیا[1] و سایر ابزارهای فنی و مشاوره– برای تضمین امنیت خدمات آنلاین دولتی انجام داده است. دوره آموزش اینترنتی نیز با حضور پانصد هزار نفر از کارکنان دولت در کنار آموزش مستقیم ۳۶۰۰ نفر از کارکنان دارای پست‌های مهم برگزار شد.

مسائل مختلفی در مورد رویکرد دولت بریتانیا در قبال تضمین تاب‌آوری سیستم‌های آن مطرح شده است. نخستین مسئله، مربوط به تأثیر آموزش تکمیل‌شده و تأثیرگذاری احتمالی آن بر فرهنگ تاب‌آوری کارکنانی است که در این دوره شرکت کرده‌اند. بنا به اظهار سازمان ملی حسابرسی، ارزیابی تأثیر بسیاری از طرح‌های دولتی در حوزه امنیت سایبری دشوار است (Update on the National Cyber Security Programme 2014, p.22–24) اما در صورت ظهور فرهنگ امنیت کارآمد، انجام این کار ازنظر تأثیر آموزش بر رفتار کارکنان و درواقع، بر کاربران خدمات دولتی ضروری است.

مسئله دوم به پیچیدگی رویکرد دولت بریتانیا در قبال ادغام سیستم‌های جدید و قدیمی و به‌خصوص تأمین امنیت شبکه ابری دولت مربوط می‌شود. به‌خصوص، ازنظر نویل جونز[2] و فیلیپس[3] (2012, p.36–37)، مبنای این رویکرد منطق امنیت محیطی است که به‌تنهایی عمل نمی‌کند و با امنیت سایبری کارآمد لایه‌ای سازگار است. ازنظر آن‌ها، حتی رویکرد جامع‌تری به امنیت سایبری باید اتخاذ گردد و کار بیشتری برای طراحی معماری امنیتی منسجم صورت گیرد تا یکپارچگی بیشتر توسعه نرم‌افزاری و سخت‌افزاری در تمام مراحل در لایه‌های مختلف تضمین شود. این استدلال نیز مطرح شد که دولت مسیری را برای رسیدگی به چنین مسائلی با تعیین حداقل استانداردهای لازم برای قراردادهای خود در زمان مناسب طی کرده و مشوق‌هایی را در اختیار صنعت قرار داده است تا چنین استانداردهایی را اتخاذ نماید و مشخصات عمومی قابل‌دسترس۷۵۴ [4] را برای کدگذاری ماهیت مهندسی نرم‌افزار مناسب (برای مثال، کمک به

1. GOV.UK Verifyp
2. Neville-Jones
3. Phillips
4. Publicly Available Specification 754 (PAS 754)

به معنای انسجام و جامعیت بیشتر این رویکرد نیست.

درنهایت، مسئله منابع ازنظر ارتقای سیستم‌ها و انتقال به شبکه دولتی و حفظ و ارتقای معیارها و سیستم‌ها پس از انتقال مطرح است. بعید به نظر می‌رسد دفتر کابینه، سطح مخارج امنیت سایبری را بیشتر از بودجه اختصاص داده شده در سال‌های ۲۰۱۶-۲۰۱۵ و پیش از انتخابات عمومی بریتانیا در مه ۲۰۱۵ اعلام کند. اگر سطح کنونی مخارج حفظ نگردد، این امر به معنای این است که بخشی از بار انتقال پس‌ازاین دوره توسط بودجه وزارتخانه‌ها پوشش داده خواهد شد. اثربخشی سیستم جدید به حفظ امنیت سایبری در اولویت کل بخش دولتی پس‌ازاین دوره و درواقع ایجاد تحولی بنیادین در فرهنگ امنیت سایبری برای تضمین وقوع این موضوع بستگی دارد که البته تحقق آن حتمی نیست. وجود منابع بیشتر فراتر از انتقال در صورتی ضروری خواهد بود که میزان اعتبار و تاب‌آوری سیستم‌های دولتی بیشتر از چرخه عمر برنامه حفظ شود.

بعد دوم مربوط به حفاظت و تاب‌آوری زیرساخت‌های حیاتی بخش خصوصی بریتانیا است که مرکز حفاظت از زیرساخت‌های ملی[1] و تیم واکنش اضطراری رایانه‌ای بریتانیا که در مارس ۲۰۱۴ تشکیل شدند نقش حیاتی در آن ایفا می‌کنند. پیش‌ازاین، هیچ تیم واکنش اضطراری رایانه‌ای واحدی وجود نداشت، بلکه دو تیم ابتدایی واکنش اضطراری رایانه‌ای برای رسیدگی به امور گروه‌های مختلف سازمانی وجود داشتند که عبارت‌اند از: تیم واکنش حوادث امنیتی رایانه‌ای بریتانیا[2]، به‌عنوان بخشی از مرکز حفاظت از زیرساخت‌های ملی که به شرکت‌هایی خدمات ارائه می‌کند که زیرساخت‌های حیاتی ملی را تشکیل می‌دهند و تیم واکنش اضطراری رایانه‌ای بریتانیا[3] که خدمات واکنش‌دهی را به دولت و سازمان‌های دولتی گسترده‌تر ارائه می‌دهد. علاوه بر این، وزارت دفاع نیز گروه واکنش سریع رایانه‌ای اختصاصی خود را دارد که مسئول شبکه‌های وزارت دفاع است (ن.ک. Pritchard 2013). آخرین گزارش آژانس امنیت شبکه و اطلاعات اتحادیه اروپا (۲۰۱۳) در مورد فعالیت تیم واکنش اضطراری رایانه‌ای نشان می‌دهد که

1. Centre for the Protection of National Infrastructure (CPNI)
2 . Computer Security Incident Response Team in UK (CSIRTUK)

بریتانیا درمجموع دارای ۲۲ تیم واکنش اضطراری رایانه‌ای دولتی و خصوصی(۱۹)، به‌استثنای تیم واکنش اضطراری رایانه‌ای بریتانیا است.

تا سال ۲۰۰۷، نقش تیم واکنش حوادث امنیتی رایانه‌ای و تیم واکنش اضطراری رایانه‌ای در عمل در تیم واکنش اضطراری رایانه‌ای بریتانیا ترکیب شده بود که بخشی از مرکز حفاظت از زیرساخت‌های ملی[1]، یعنی مرکز هماهنگی زیرساخت‌های ملی ، محسوب می شد و طرح یکپارچه گزارش دهی و هشدار حوادث[2] –مرکزی برای گزارش حوادث از بخش های دولتی و خصوصی با تأکید بر زیرساخت‌های حیاتی و برای اعلام هشدارها و اطلاعات در مورد حوادث و تهدیدهای سایبری– را اجرا می‌کرد. این مرکز واحد گزارش‌دهی در زمان تشکیل مرکز حفاظت از زیرساخت های ملی به‌رغم افزایش تصاعدی پیچیدگی تهدید امنیت سایبری در سال‌های [انتقال عملکرد بین دو مرکز] از دست رفت؛ درنتیجه سیستم بریتانیا برای گزارش‌دهی حوادث به‌صورت غیریکپارچه باقی ماند. هدف تیم واکنش اضطراری رایانه‌ای بریتانیا، رفع این فاصله به‌عنوان نخستین تیم واکنش اضطراری رایانه‌ای دولتی مسئول مدیریت رویدادهای سایبری، رسیدگی به رویدادهای سایبری مربوط به ائتلاف اطلاعات شبکه‌ای[3]، توسعه و تبادل میزان آگاهی برحسب موقعیت از تهدیدهای سایبری و ارائه مرکز تماس بین‌المللی در زمینه مسائل امنیت سایبری بود. این امر به معنای انحلال دیگر تیم‌های واکنش اضطراری رایانه‌ای موجوددر بریتانیا نیست، بلکه به معنای این است که تیم واکنش اضطراری رایانه‌ای بریتانیا که مورد توصیه و حمایت آژانس امنیت شبکه و اطلاعات اتحادیه اروپا قرار دارد که حداقل الزامات پایه را برای آن تعریف کرده است، تبدیل به نخستین تیمی می‌شود که احتمالاً وظیفه آن هماهنگ سازی واکنش دهی به حوادث سایبری است.

از دیدگاه امنیت تاب‌آور، تیم واکنش اضطراری رایانه‌ای، حداقل ازلحاظ نظری نهاد ضروری جدیدی برای تسهیل هماهنگی مؤثرتر واکنش دهی و اشتراک اطلاعات در داخل بریتانیا و در خارج، ازنظر ایجاد مرکز تماس و ارتباط برای شرکای بین‌المللی در زمینه واکنش‌دهی به

1. National Infrastructure Coordination Centre (NISCC)
2. Unified Incident Reporting and Alert Scheme
3. Coalition for Networked Information (CNI)

حوادث فرامرزی محسوب می‌شود. در مورد دوم، این امر نیز تضمین می‌شود که اعتماد به‌واسطه عضویت و برقراری تماس منظم با دیگر تیم‌های واکنش اضطراری رایانه‌ای اروپا از طریق گروه هایی ازجمله مجمع تیم‌های واکنش و امنیت حوادث[1] و تیم واکنش اضطراری رایانه‌ای دولت های اروپایی ایجاد می شود. همان طور که در فصول بعدی نیز ملاحظه خواهد شد، اعتمادسازی مؤلفه مهم ایجاد مشارکت مؤثر و امنیت تاب‌آور محسوب می‌شود. این امر حاکی از این است که بریتانیا مایل به تغییر شیوه رسیدگی به رویدادهای سایبری به‌جای تغییر صرف سیاست در حاشیه است.

باوجود انجام اقدامات اولیه‌ای که بیانگر نقش موفق آن –برای مثال، از طریق ارائه اطلاعات و مشاوره در زمینه کاهش موارد آسیب پذیری باگ های هارت بلید[2] و شل شاک[3] و همکاری با اعضای مرکز حفاظت و اشتراک اطلاعات سایبری برای حمایت از بازی های کشورهای مشترک المنافع و نشست ناتو (ن.ک.CERT-UK Quarterly Report 2014a, 2014b)– است، برخی میزان ارزش‌افزوده به موارد موجود و ماهیت اقدامات صورت گرفته در بریتانیا برای مثال، ازنظر میزان آگاهی برحسب موقعیت، مدیریت رویدادها و تحلیل تهدید توسط مرکز محاسبات ملی[4] و مرکز حفاظت از زیرساخت های ملی و دیگر تیم‌های واکنش اضطراری رایانه‌ای را زیر سؤال برده‌اند (Jeffray 2014). بااینکه دستورالعمل‌های گزارش حوادث خاص نقش تیم واکنش اضطراری رایانه‌ای بریتانیا و تیم دولتی واکنش اضطراری رایانه‌ای را مشخص و تعریف می کنند (Bada et al. 2014؛ CESG https://www.cesg.gov.uk)، اما این مورد جامع نیست و موضوعی مستلزم همکاری مؤثرتر با بخش-های مربوطه و تیم‌های واکنش اضطراری رایانه‌ای موجود در این بخش ها برای جلوگیری از دوباره‌کاری و تضمین انسجام است. به‌رغم گزارش مستقیم بسیاری از حوادث به تیم واکنش اضطراری رایانه‌ای بریتانیا از طریق بخش های مختلف، مواردی که از طریق مرکز حفاظت و اشتراک اطلاعات سایبری گزارش شده‌اند در تحلیل آماری تیم واکنش اضطراری رایانه‌ای بریتانیا از حوادث گنجانده نشده است که این

1. Forum of Incident Response and Security Teams (FIRST)
2. Heartbleed
3. Shellshock
4. National Computing Centre (NCC)

موضوع منجر به حضور نمایندگان معدود برخی بخش‌ها [در امر رسیدگی به] انواع حوادث و مشکلات پیش روی آن‌ها و ازاین‌رو، درک موارد در خطر و واکنش‌دهی مناسب به حوادث (از طریق مرکز حفاظت و اشتراک اطلاعات سایبری یا تیم واکنش اضطراری رایانه‌ای بریتانیا) می شود. در صورت ایجاد شرایط لازم برای تأمین تاب‌آوری کارآمد در بخش‌های مختلف، مشارکت بیشتر با این بخش‌ها برای افزایش آگاهی در مورد مسائل پیش روی آن‌ها حیاتی است.

نکته سوم و نهایی، مسئله امنیت سایبری و امور دفاعی است که مرکز مشارکت حفاظت از دفاع سایبری[1] که به زنجیره تأمین توجه دارد در این زمینه شکل گرفت تا نقشی مشابه مرکز حفاظت و اشتراک اطلاعات سایبری برای بهبود همکاری و اشتراک اطلاعات بین دولت و صنعت و توجه به بهترین اقدام، میزان آگاهی و استانداردهای متناسب داشته باشد. مرکز مشارکت حفاظت از دفاع سایبری همچنین درصدد برخورداری از عضویت فراگیرتر در این مرکز است. ازاین‌رو، در کنار پیمانکاران امور دفاعی مهم (۱۳ پیمانکار در زمان نگارش این مطلب)، اتحادیه‌های تجاری مانند گروه تجاری ای‌دی‌اس[2] و انجمن تجارت فناوری که نماینده واحدهای تجاری کوچک هستند نیز عضو این مرکز محسوب می شوند. بااینکه کار در مرکز مشارکت حفاظت از دفاع سایبری کماکان روند تکوینی خود را طی می کند، این مرکز همکاری مؤثری با وزارت کسب‌وکار، نوآوری و مهارت و ستاد ارتباطات دولتی بریتانیا در زمینه شناسایی نحوه اجرای الزامات سایبری در زنجیره تأمین و موارد نظارت بیشتر (فراتر از الزامات سایبری) با –ابعاد فنی (بررسی موارد آسیب‌پذیری، ارزیابی خطر)، سازمانی (سیاست، نقش و مسئولیت در حوزه امنیت اطلاعات)، حقوقی (متابعت) و آموزشی (امنیت/ آموزش مردم)– دارد که باید توسط شرکت‌های حاضر در زنجیره تأمین به نحوی متناسب اجرا شود. در زمان نگارش این مطالب، موارد نظارت و استانداردهای مرکز مشارکت حفاظت از دفاع سایبری توسط وزارت دفاع انجام می شود –و در صورت عملکرد موفق آن‌ها، این موارد در قراردادهای وزارت دفاع از آوریل ۲۰۱۵ (Defence Cyber Protection Partnership 2015) با ایجاد انگیزه برای پذیرش چنین استانداردها و موارد نظارتی در عین تضمین ایجاد شرایط لازم برای همگرایی در زمینه

1. Defence Cyber Protection Partnership (DCPP)
2. ADS

استانداردها، موارد نظارت و درک مشترک از تهدید سایبری و درنتیجه تأمین امنیت تاب‌آور الزامی می‌شوند.

تأثیرگذاری بر سطح بین‌الملل

ماهیت جهانی و بدون مرز فضای سایبری به این معنا است که دولت بریتانیا باید به توسعه و تأمل پیرامون راهبردهایی برای کنترل مشارکت بین‌المللی در زمینه همکاری، هماهنگی و تشریک‌مساعی با هدف تضمین تأمین امنیت تاب‌آور در بریتانیا می پرداخت. این امر در قالب تعامل دوجانبه و چندجانبه صورت گرفته و از طریق «فرآیند لندن» و میزبانی رویدادهای بین‌المللی در حوزه فضای سایبری بر مباحث بین‌المللی تأثیر گذاشته و در توسعه هنجارهای مربوط به رفتار دولت مسئول در فضای سایبری و ظرفیت‌سازی نقش داشته است تا شمول طیف گسترده‌تر کشورها و تقویت توانایی‌ها و دانش آن‌ها در برخورد با مسائل مربوط به امنیت سایبری تضمین گردد.

تعدادی از تفاهم‌نامه‌ها (کره، اسرائیل) و موافقت‌نامه‌ها در زمینه گفتمان سایبری (سنگاپور، ژاپن، چین) به‌صورت دوجانبه، به‌خصوص در زمانی که یکی از طرفین چین است، نوشته شده‌اند که در این موارد کانال رسمی گفتمانی به‌موازات گفتمان تحت هدایت اتاق فکر برای بهبود تفاهم و درواقع تعامل با بازیگر اصلی در فضای سایبری وجود دارد. علاوه بر این و شاید به‌عنوان نمونه ای از شیوه مناسب مورد الگوبرداری در کل اتحادیه اروپا در صورت پیشرفت کشورهای دارای رویکردی متفاوت به امنیت سایبری (ن.ک. Bersick et al. 2015)، بریتانیا رابطه مستقیمی بین آژانس مقابله با جرائم ملی بریتانیا و نهاد مجری قانون چین با ایجاد مراکز تماس ۲۴ ساعته در طول هفته برای مقابله با جرائم سایبری در حال وقوع بین دو کشور برقرار کرده است (Brewster 2014). درواقع، چنین ترتیبات حکمرانی از وجه رسمی کمتری در سمینارهای برگزارشده در چین برای سازمان‌های مجری قانون سایبری بریتانیا و چین برخوردارند و نیز بازدیدهای چین از آژانس مقابله با جرائم ملی می‌توانند در اعتمادسازی و تسهیل ایجاد همکاری مؤثرتر و اشتراک اطلاعات در زمینه تهدیدهای سایبری سودمندتر باشند.

بریتانیا به‌طور چندجانبه درگیر تأثیرگذاری بر قوانین اولیه‌ای است که از سوی اتحادیه اروپا در حوزه امنیت سایبری و بر اساس راهبرد امنیت سایبری منتشره این اتحادیه در سال ۲۰۱۳ وضع شده‌اند (برای تحلیل دقیق‌تر، ن.ک. فصول ۵ و ۶). شایان‌ذکر است که بریتانیا به دنبال نمایش رهبری خود در اتحادیه اروپا در حوزه امنیت سایبری و درواقع ترویج رویکرد خود به امنیت سایبری، یعنی فراحکمرانی نظری هویت‌ها است که این امر در تضاد با رویکرد عملی‌تر مطرح‌شده در دستورالعمل امنیت شبکه و اطلاعات پیشنهادی است (ن.ک. فصل ۶). درواقع، موضع بریتانیا در مورد محتوای این دستورالعمل بیانگر رویکرد داوطلبانه و بازارمحور آن در تقاضا برای کاهش هزینه های مربوط به دامنه پیشنهادی (تنها شامل تأمین کنندگان زیرساخت‌های حیاتی بدون حضور ارائه‌دهندگان خدمات جامعه اطلاعاتی) و ایجاد شفافیت در نحوه دقیق همکاری در زمینه اشتراک اطلاعات است (Informal meeting, UKREP February 2014).

به‌خصوص نگرانی در مورد نحوه اعتمادسازی از طریق تحمیل گزارش‌دهی برخلاف ترتیبات غیررسمی وجود دارد که هدف آن‌ها ایجاد آشنایی و اعتماد به‌مرورزمان از طریق برقراری روابط کاری کارآمد است. از این نظر، بریتانیا و دیگر کشورهای عضو اتحادیه اروپا با برخورداری از سطوح امنیت سایبری پیشرفته‌تر و تاب‌آورتر خواستار طرح موارد جایگزینی برای گزارش‌دهی اجباری بوده‌اند. درواقع، بریتانیا اولویت خود در مورد [تشکیل] «دو گروه مجزا ... یکی در سطح فنی/ رسمی برای صحبت پیرامون اجرای این امریه و ... جنبه‌های راهبردی امنیت سایبری ... و دیگری گردهمایی جمعی از تیم‌های واکنش اضطراری رایانه‌ای کشورهای عضو ... به‌طور داوطلبانه ... برای آغاز فرآیند اشتراک اطلاعات ... و طرح برنامه آتی برای همکاری» را عنوان داشته است (Telephone Interview, UK cybersecurity official, October 2014). با توجه به اختلافات موجود در مورد امریه پیشنهادی امنیت شبکه و اطلاعات و تضعیف آن از جانب طرف‌های مختلف (ن.ک. فصول ۶ و ۷)، مسلماً اگر هدف دستیابی به توافق نهایی در زمینه دامنه و محتوای آن باشد، کماکان توافقات بسیار بیشتری باید صورت گیرد. این امر به‌ویژه از دیدگاه بریتانیا به دلیل «رویکرد تماماً تجارت محور» آن به امنیت سایبری و از دید سایر کشورهای اروپا به دلیل اینکه مؤثرترین شیوه ایجاد شرایط لازم برای دست‌یابی به امنیت

سایبری تاب‌آور محسوب می‌شود، حائز اهمیت است.

بریتانیا مشارکت خود در ناتو را با عضویت کامل در مرکز عالی همکاری های دفاع سایبری ناتو[1] بیشتر کرده است و نقش مهمی در پذیرش سیاست ارتقایافته ناتو در زمینه دفاع سایبری ایفا می‌نماید. درواقع، بریتانیا طرحی را نیز برای همکاری جدید –مشارکت سایبری صنعتی ناتو[2] – با هدف تضمین بهره‌وری هر چه بیشتر از تخصص و نوآوری بخش خصوصی جهت دست‌یابی به اهداف سیاست دفاع سایبری ارتقایافته پیشنهاد داد. پس مسلماً اولویت بریتانیا در حوزه دفاع سایبری، ناتو، به‌جای اتحادیه اروپا، به‌عنوان سازمانی بین‌دولتی است، چراکه بر این اساس که «دفاع سایبری» مسئله‌ای مربوط به امنیت و صلاحیت ملی تلقی می‌شود، این کشور دیگر در اقدامات این اتحادیه از طریق آژانس دفاع اتحادیه اروپا شرکت نمی کند. گرچه، با توجه به منافع مشترک و نیاز مبرم کل اتحادیه اروپا به افزایش توانمندی های حوزه دفاع سایبری و ضرورت محو خطوط بین زیرساخت‌های نظامی و خصوصی برای عملیات‌های نظامی، چنین استدلالی می‌تواند به ضرر تأمین امنیت سایبری تاب‌آور در بریتانیا و اروپا باشد.

درنهایت، بریتانیا اقدام به تأثیرگذاری بر هنجارهای بین‌المللی برای حکمرانی بر اینترنت و رفتار کشورها در فضای سایبری با هدف ایجاد درک مشترک و ترویج رویکردی منسجم به تهدیدهای سایبری خارج از بریتانیا کرده است. براساس مباحث فصل سوم، به دلیل وجود دیدگاه‌های متناقض یا حتی کاملاً متضاد کشورها و سازمان‌های اصلی، انجام این کار دشوار است. بااینکه بریتانیا این مبحث را از طریق کنفرانس‌های برگزارشده در لندن، بوداپست و سئول (از طریق فرآیند لندن) پیش برده است، اما ازنظر برخی کشورها این فرایند باعث دستیابی به توافق یا اجماع مشخصی در مسیر پیش رو نشده است. درواقع، به نظر برخی، این کنفرانس‌ها صرفاً محلی برای «گفتگو» است. گذشته از این، حتی زمانی که اجماعی در مورد برخی اصول حاکم بر رفتار از طریق مجامعی مانند گروه کارشناسان دولتی سازمان ملل[1] (مبنی بر قابل‌اجرا بودن حقوق بین الملل موجود در فضای سایبری)[۳۰] ظاهراً به دست می آید؛ طبق فصل سوم

1. NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE)
2. NATO Industry Cyber Partnership

این کتاب، اجماع در مورد هنجارها و اصول کلی لزوماً به معنای وجود درک مشترک از حکمرانی اینترنت یا امنیت سایبری نیست. ازاین‌رو، بریتانیا به‌طور فعال در حال ترویج این مبحث در سطح بین‌المللی با انجام اقدامات و دستورالعمل های اعتمادسازی از طریق سازمان‌هایی مانند سازمان امنیت و همکاری اروپا و سازمان همکاری اقتصادی و توسعه و تشویق افزایش مشارکت از طریق تأمین بودجه طرح‌هایی مانند اعطای بورسیه تحصیلی خارج از کشور برای محققان امنیت سایبری، مؤسسه بین المللی فناوری اطلاعات و ارتباطات برای صلح[۲] و مرکز امنیت سایبری جهانی[۳] است. گرچه، باید در مورد مسئله نحوه ارتباط این طرح‌ها با تعامل، همکاری و گفتمان غیررسمی سطح پایین‌تر بیشتر تأمل نمود، چراکه در اینجا است که تغییر درک از طریق عمل بیشترین نفع را ایجاد می کند

دانش، مهارت و توانمندی

بریتانیا مسلماً یکی از پیشرفته ترین کشورهای عضو اتحادیه اروپا در زمینه ارائه طرح‌های آموزشی و مهارتی برای توسعه توانمندی محسوب می‌شود. در دو سال اخیر برنامه جامع طرح‌های ابتکاری (ن.ک. کادر ۴-۲) در کل بخش های صنعت و دانشگاه برای تضمین ایجاد سطح دانش، مهارت و تخصص لازم جهت تأمین امنیت تاب‌آور در سطوح مختلف ازجمله سطح اجتماعی ایجاد گردید. این رویکرد مداخلات هدفمندی را در دانشگاه‌ها از طریق تحصیلات تکمیلی و با کمک گروه های کارشناسی (موسسه مشارکت فناوری[۴]، انجمن رایانه بریتانیا[۵] مؤسسه مهندسی و فناوری[۶]، مؤسسه متخصصان امنیت اطلاعات و چالش امنیت سایبری[۷]) انجام داده است.

گرچه، بُعد مهارت‌ها و آموزش سایبری در ایجاد تاب‌آوری مسلماً چندوجهی و پیچیده است.

1.UN Group of Governmental Experts (UNGGE)
2. ICT4Peace
3. Global Cyber Security Centre
4.Tech Partnership)
5. British Computer Society
6. Institute of Engineering and Technology
7. Institute of Information Security Professionals and Cyber Security Challenge

به‌رغم وجود مجموعه گسترده‌تری از استعدادها در طرح‌هایی (برای مثال، دو مورد) مانند چالش امنیت سایبری و تربیت افراد متخصص در مراکز آموزش دکترا در میان‌مدت و بلندمدت، برخی طرف های ذینفع نگران عدم تأمین تقاضا برای مهارت‌های تخصصی در کوتاه مدت، به ویژه در بخش خصوصی هستند. گزارش سازمان ملی حسابرسی به این نکته اشاره دارد که «بخش دولتی کارکنان مهم خود را از دست می دهد و افراد متخصص کافی برای جایگزینی آن‌ها نیز وجود ندارد» (Update on the National Security Programme 2014, p.21). به رغم اذعان به اینکه طرح سایبری احتیاطی در ظرفیت سازی وزارت دفاع نقش دارد، این گزارش بر این موضوع نیز تأکید دارد که مشکل گسترده‌تر جذب و حفظ کارشناسان و مشاوران در دولت که درک مناسبی از مسائل امنیت سایبری دارند، کماکان باقی می‌ماند.

درنتیجه، بااینکه مسلماً بریتانیا به دنبال اتخاذ رویکردی چندجانبه به توسعه آموزش و مهارتها در کشور خود است، اما بسیاری از این منافع احتمالاً تنها در میان‌مدت و بلندمدت به دست می‌آید. به‌رغم وجود عناصر رویه مناسب که در جای دیگری می‌توان از آن‌ها الگوبرداری کرد، اما بریتانیا کماکان قادر به بهبود اقدامات خود برای آموزش و جذب نیرو در کوتاه‌مدت، برای مثال، در حوزه پژوهشهای میانرشتهای در آموزش امنیت سایبری است. مورد دوم منحصر به کشور بریتانیا نیست و این مشکل گریبانگیر کل اروپا است و اگر هدف درک جامعتر مسائل و راهکارهای امنیت سایبری باشد، این مسئله باید رفع گردد. علاوه بر این، انجام این کار برای درک مشترک تهدیدات سایبری در کل لایه‌ها و سطوح مختلف امنیت سایبری و درنتیجه ظهور فرهنگ امنیت سایبری ضروری است.

کادر ۴-۲. دانش، مهارت و توانمندی امنیت سایبری

مدارس	یادگیری و آموزش موضوعات در سطح دیپلم، موضوعات جدید برای سطح ۳ (سنین ۱۱-۱۴ سال) در سال ۲۰۱۵ منتشر خواهد شد؛ مداخلات کنونی در تمامی سطوح نظام آموزشی
آموزش و کارآموزی	۲۰۰ شغل جدید مرتبط با امنیت سایبری ازطریق مشارکت‌ها و کارفرمایان فناوری، اضافه کردن بیش از ۱۲۰ کارآموز در ستاد ارتباطات دولتی بریتانیا به‌اضافه کارآموزان تحلیلگر اختلالات سایبری در سال ۲۰۱۵
آموزش عالی	چهار آکادمی آموزش عالی پژوهانه‌های مرتبط با توسعه آموزش عالی در حوزه برنامه ملی امنیت سایبری دریافت خواهند کرد، دوره‌های مربی‌گری و «کمپ‌های سایبری» برای مقاطع تحصیلات تکمیلی و پایین تر از آن
تحصیلات تکمیلی	ستاد ارتباطات دولتی بریتانیا شش مدرک ارشد در حوزه امنیت سایبری صادر کرده است، دو مرکز برای ترتیبت ۶۶ فارغ‌التحصیل دکترای دیگر از سال ۲۰۱۷ در صدر برنامه دکترای ستاد ارتباطات دولتی بریتانیا قرار دارد
حمایت‌های گسترده‌تر آموزشی	اوپن یونیورسیتی بریتانیا دوره‌های گسترده مجازی با عنوان «مقدمه‌ای بر امنیت سایبری» تعریف کرده است – نزدیک به ۲۴/۱۲۷ هزار درخواست در اولین مرحله ثبت شد و ارائه اپلیکیشن جدید «کریپتوی» از سوی ستاد ارتباطات دولتی بریتانیا در خصوص کدگذاری ستاد ارتباطات دولتی بریتانیا ۱۱ مرکز عالی آکادمیک که بازتاب‌دهنده استاندارد بالای تحقیقات سایبری بود را به رسمیت شناخته است.
چالش امنیت سایبری	۱۸/۸۰۰ درخواست برای دوره‌های ارشد ثبت شده است؛ ۸۰۰ مدرسه در رقابت‌های مداری شرکت کرده‌اند؛ بیش از ۲۲/۰۰۰ هزار جوان از منابع آموزشی استفاده کرده‌اند

Source: UKCSS: Report on Progress and Forward Plans, Cabinet Office (2014, p.22)

درنهایت، بریتانیا در طرح‌های مختلفی سرمایه‌گذاری کرده و برنامه‌های گوناگونی را برای آموزش شهروندان و افزایش آگاهی آن‌ها در مورد تهدیدات سایبری ایجاد کرده است. بر اساس طرح برخورداری از اینترنت امن[1] بخش‌های عمومی–خصوصی (راه‌اندازی در سال ۲۰۰۵)، طرح هایی مانند اینترنت هوشمند[2] (راه‌اندازی در سال ۲۰۱۳) با پشتیبانی طیف وسیعی از سازمان‌ها

1. Get Safe Online' scheme
2. Cyber Streetwise

(بانک‌ها، مؤسسه ارتباطات تجاری[1]، فیس‌بوک، شرکت امنیت فناوری اطلاعات سوفوس[2]، سازمان‌های تجاری)، بنابه گفته وزارت کشور بریتانیا در مرحله اول عملکرد خود تأثیر مثبتی ازنظر تغییر شیوه عمل شهروندان داشته‌اند. با توجه به آمار آن‌ها، ۶۵ درصد از شهروندان اکنون حداقل ۱۰ مورد از رفتارهای امنیت سایبری توصیه‌شده –برای مثال، استفاده از کلمات عبور مناسب‌تر یا بررسی نشانه تأیید تارنماهای امن در زمان خرید آنلاین– را انجام می‌دهند (Update on the National Security Programme 2014, p.16). مسلماً این نقطه آغاز افزایش سطح آگاهی مردم و آموزش عمومی در حوزه امنیت سایبری است و برای تغییر رفتار در حوزه فرهنگ امنیت سایبری، رویکردهای هدفمندتر و متمایزتری باید برای مخاطبان گوناگون و به‌خصوص افراد برخوردار از مهارت اندک در زمینه فناوری اطلاعات و ارتباطات و آن دسته از افراد متعلق به گروه‌های اجتماعی- اقتصادی پایین‌تر در نظر گرفته شود (The UK Cyber Security Strategy: Landscape Review 2013, p.28).

جمع بندی: امنیت تاب‌آور در بریتانیا

مبنای رویکرد دولت بریتانیا در قبال امنیت سایبری، منطق حکمرانی نظری بازار است که به دنبال اشاعه آن در کل و بین ارکان مورد هدف راهبرد امنیت سایبری خود با بهره گیری از انواع مؤسسات، سازوکارها و ابزارها و از همه مهم تر، تعداد زیادی از طرف های ذینفع مربوطه است. در این زمینه پیشرفت بسیاری ازلحاظ ایجاد پیش‌شرط‌های تأمین امنیت تاب‌آور کارآمد صورت گرفته است و بریتانیا در مقایسه و در کنار سایر کشورهای عضو اتحادیه اروپا می‌تواند خود را حداقل ازنظر طرح ها و تفکر پیرامون نحوه تضمین امنیت فضای سایبری پیشرفته تلقی کند.

در عمل، بریتانیا آمادگی خود را در حوزه سرمایه‌گذاری در منابع مالی و ایجاد شبکه‌ها و نهادهای جدید بخش دولتی و سازمان‌ها و برنامه هایی برای مقابله با حملات و جرائم سایبری نشان داده است. موضوع مشارکت‌محور رویکرد بریتانیا –از طریق مشارکت در زمینه اشتراک

1. Business Telecommunications (BT)
2. Sophos

اطلاعات در حوزه امنیت سایبری و تیم واکنش اضطراری رایانه‌ای بریتانیا یا اینترنت هوشمند، برای مثال، در داخل کشور و از طریق ترتیبات رسمی و غیررسمی مربوط به تعامل بین‌المللی برای ایجاد درک مشترک از امنیت سایبری– و ایجاد استانداردهایی محسوب می شود که امکان توسعه فرهنگ امنیت تاب‌آور مشترک را در بریتانیا و حتی در خارج از آن فراهم می‌سازد. درواقع، بخش اعظم نوآوری رویکرد بریتانیا در حکم منبع فکری برای آن دسته از کشورهای اروپایی است که از آمادگی امنیت سایبری چندان پیشرفته‌ای برخوردار نیستند.

شایان‌ذکر است که با توجه به تنوع، تازگی و تعداد طرح‌های راهبرد امنیت سایبری بریتانیا، این راهبرد کماکان از بسیاری جهات روند تکوینی را در اجرا و تأثیرگذاری خود طی می کند و ارزیابی دقیق آن در کل لایه‌ها، سطوح و طرف های ذینفع هدف آن دشوار است. کماکان کارهای زیادی باید در داخل و کل دولت و نیز بین دولت و سایر طرف های ذینفع پیش از دستیابی به درک مشترکی از تأمین امنیت سایبری با توجه به تهدید [کنونی/آتی] و راهکارهای پیشگیرانه و فعال انجام شود. به‌رغم افزایش آشکار آگاهی و علاقه از بخش صنعتی گرفته تا سطح فردی، مسائل مربوط به بهبود آموزش، تربیت و مهارت‌های سایبری و ایجاد فرهنگ امنیت سایبری باقی می ماند که امکان تأمین امنیت تاب‌آور کارآمدتر و منسجمی را در کوتاه‌مدت و میان‌مدت فراهم می کند.

بخش ضروری این فرهنگ، اعتمادسازی و اشتراک اطلاعات است که از منظر بریتانیا با اتخاذ رویکردی داوطلبانه به بهترین نحو به دست می آید. در اینجا تضاد آشکاری در منطق های مبنای امریه امنیت شبکه و اطلاعات پیشنهادی اتحادیه اروپا ملاحظه می شود که خواستار اتخاذ رویکردی اجباری است. در آینده مسلماً هرگونه سازش موردتوافق موجب ایجاد تنش بین رویکردهای اتحادیه اروپا و بریتانیا می‌شود، مگر اینکه این امریه از تاب‌آوری کافی برای پذیرش هر دو منطق برخوردار باشد. نتیجه عملی کار (اجرا)، احتمالاً موجب ایجاد نگرانی در مورد تأثیرگذاری بر ایجاد فرهنگ کارآمد اشتراک اطلاعات می گردد. گذشته از این، بریتانیا باید به تعامل سازنده با اتحادیه اروپا در زمینه راهبرد امنیت سایبری آن ادامه دهد و اگر هدف این کشور مشارکت مؤثر در تکامل شیوه مناسب در این عرصه فراتر از مرزهای خود و درنهایت،

تکامل توانمندی دفاع سایبری کشورهای عضو اتحادیه اروپا باشد، این راهبرد شامل بُعد دفاعی نیز می‌شود.

درمجموع، بریتانیا مسلماً در حال حرکت به سمت اکوسیستمی بوده که با توجه به راهبرد امنیت سایبری خود به دنبال ادغام است. یکی از مشکلات پیش رو، حفظ شتاب کار در چرخه برنامه امنیت سایبری بعدی است که این موضوع درنهایت به تضمین این مسئله بستگی دارد که حداقل درک مشترکی از تهدید امنیت سایبری در میان تمام طرف های ذینفع وجود داشته باشد. این موضوع موجب تضمین تداوم تکامل مشارکت، برنامه ها، استانداردها و مهارت های مؤثر است. علاوه بر این، دولت بریتانیا باید اطمینان یابد که طرح‌های بی شمار و رویکرد نظری آن برای ایجاد رویکرد منسجم داخلی به یکدیگر می پیوندند و ازلحاظ بین‌المللی نیز تعامل این کشور امکان صادرات شیوه مناسب آن (برای مثال، کارگروه اقدام مشترک علیه جرائم اینترنتی) (و همچنین واردات شیوه مناسب از کشورهای دیگر) و تکامل فرایندهای تکراری یادگیری را فراهم می‌کند که باعث ایجاد درک مشترک و شیوه‌های مؤثر –حداقل در سطح عملیاتی اگر نه در سطح هنجاری– با شرکای خارج از بریتانیا می‌شود. با توجه به مشارکت ستاد ارتباطات دولتی بریتانیا در اقدامات نظارت و جاسوسی جمعی و جاسازی نقاط آسیب‌پذیر و برنامه های پنهانی برای جمع‌آوری اطلاعات، این کشور باید رویکرد خود به دفاع و جرائم سایبری را با هدف تأمین امنیت تاب‌آور کارآمد در بریتانیا تطبیق دهد (ن.ک. فصل ۷).

فصل پنجم

اتحادیه اروپا و
جرائم سایبری

مقدمه

رویکرد اتحادیه اروپا در قبال امنیت سایبری، دارای پنج حوزه مربوط به اولویت‌ها (Cybersecurity Strategy 2013) و به‌طور اساسی سه ویژگی کانونی است. ویژگی نخست، به حفاظت [از این اتحادیه] در برابر جرائم سایبری و مقابله با این‌گونه جرائم ارتباط دارد و ویژگی دوم، به امنیت شبکه و اطلاعات، حفاظت از زیرساخت‌های حیاتی[1] و حفاظت از زیرساخت‌های حیاتی اطلاعات توجه می‌کند و ویژگی سوم که توسعه چندانی نیافته، مربوط به حوزه دفاع سایبری است. در این فصل، ویژگی نخست مطرح می‌شود (در مورد دو ویژگی دیگر ن.ک. فصل ۶)، گرچه باید به این مسئله نیز توجه کرد که در زمان تحلیل امنیت تاب‌آور مبنای این ویژگی‌ها در محیط نهادی اتحادیه اروپا، هم‌پوشانی بین آن‌ها دیده می‌شود. به‌خصوص آگاهی از این مطلب در شرایط وجود اصول و دستورالعمل‌های اتحادیه اروپا در تاب‌آوری و ثبات اینترنت (۲۰۱۱) و ایجاد راهبرد امنیت سایبری اتحادیه اروپا (EUCSS 2013) حائز اهمیت است. ساختار نهادی اتحادیه اروپا کماکان بازتاب جدایی سیاست‌گذاری از اداره کل مهاجرت و امور داخلی کمیسیون اروپا در زمینه مؤلفه‌های قانون کیفری، اداره کل شبکه‌های ارتباطات، محتوا و فناوری در زمینه امنیت و تاب‌آوری شبکه و دفاع سایبری تحت حکمرانی سیاست امنیتی و دفاعی مشترک است. بااین‌وجود، اتحادیه اروپا درحال‌توسعه ساختارهای کاری یکپارچه‌ای برای

1. Critical Infrastructure Protection (CIP)

تسهیل اتخاذ رویکردی منسجم در قبال راهبرد امنیت سایبری خود است.

با توجه به رشد اینترنت و اهمیت آن در زندگی اقتصادی و اجتماعی، جرائم سایبری[۱] در بازار جهانی به مسئله مهمی تبدیل شده است. بر اساس اعلام مرکز آمار اتحادیه اروپا (یورواستات) (۲۰۱۰)، ۸۰ درصد از جوانان اروپایی از طریق شبکه‌های اجتماعی به‌صورت آنلاین با یکدیگر ارتباط برقرار می‌کنند و حجم تراکنش‌های صورت گرفته از طریق تجارت الکترونیک مجموعاً به حدود ۸ هزار میلیارد دلار می‌رسد. افزایش به‌کارگیری اینترنت با گسترش اقدامات در حوزه جرائم سایبری همراه شده است که دامنه آن از سرقت هویت گرفته تا فروش کارت‌های اعتباری مسروقه و سوءاستفاده جنسی از کودکان، گسترده است. گزارش‌ها حاکی از این است که روزانه در سطح دنیا بیش از یک میلیون نفر قربانی جرائم سایبری می‌شوند (Norton Cybercrime Report 2013) و هزینه جهانی تنها برای حوزه جرائم سایبری حدود ۱۱۳ میلیارد دلار و این هزینه برای اروپا ۱۲ میلیارد دلار است (Norton Cybercrime Report 2013) که این موضوع دلالت بر این دارد که جرائم سایبری بیش از تجارت غیرقانونی مواد مخدر سودآور است. به دلیل تنوع موجود در تعریف حوزه جرائم سایبری و در نتیجه هزینه گزارش‌شده (صرف‌نظر از دستورکار گزارشگران) باید با این ارقام و اطلاعات در زمینه جرائم سایبری با احتیاط برخورد کرد، اما بدیهی است که این مسئله تأثیر مخربی بر شهروندان، دولت‌ها و واحدهای تجاری در اروپا دارد و فعالیتی محسوب می‌شود که خطرات اندک و سودآوری بالایی برای مجرمان سایبری به ارمغان می‌آورد. درمجموع، اگر این مسئله از طریق تأمین امنیت تاب‌آور مناسب و کارآمدی مورد رسیدگی قرار نگیرد، می‌تواند مانع از اجرای برنامه‌های اتحادیه اروپا در زمینه رشد اقتصادی گردد که در راهبرد اروپا ۲۰۲۰ (۲۰۱۰) و دستورکار دیجیتال اروپا در نظر گرفته شده‌اند (European Commission 2010; European Commission 2012).

سیاست جرائم سایبری در اتحادیه اروپا تحت تأثیر و مورد پشتیبانی راهبرد امنیت اینترنت در حال تکوین آن (۲۰۱۰) و در خارج از اتحادیه تحت تأثیر و مورد پشتیبانی کنوانسیون اروپایی جرائم سایبری[1] (۲۰۰۱) است که ازاین‌پس با عنوان کنوانسیون بوداپست از آن یاد می‌شود.

1. European Convention on Cybercrime

برنامه استکهلم[1] (۲۰۱۰) که اولویت‌های اتحادیه اروپا در زمینه توسعه حوزه مربوط به عدالت، آزادی و امنیت (۲۰۱۰-۲۰۱۴) را تنظیم می‌کند بر این موضوع تأکید دارد که کشورهای عضو اتحادیه اروپا باید در اسرع وقت «کنوانسیون جرائم سایبری شورای اروپا[2] در سال ۲۰۰۱ را تصویب کنند» و آن را به‌عنوان «چارچوب حقوقی اصلی و مرجع مقابله با جرائم سایبری در سطح جهان» در نظر گیرند (p.22 ,2010). این برنامه بر نقش محوری آژانس پلیس اروپا (یوروپل) به‌عنوان مرجع اصلی برای اروپا و اتحادیه اروپا تأکید دارد که می‌تواند به‌عنوان پایگاهی برای ارائه داده‌ها و شناسایی مهاجمان و حملات و همچنین به‌عنوان پشتیبان تبادل بهترین رویه‌ها در بین کشورهای عضو اتحادیه اروپا از طریق برقراری ارتباط و همکاری با سیستم‌های هشداردهنده ملی عمل نماید. بدین منظور مرکز مقابله با جرائم سایبری اتحادیه اروپا که در اول ژانویه ۲۰۱۳ تأسیس شد به‌عنوان شاخه اصلی مقابله با جرائم سایبری اقدام به گردآوری متخصصان و اطلاعات، پشتیبانی از تحقیقات جنایی، پیشبرد راه‌حل‌ها در سطح اروپا و افزایش آگاهی پیرامون جرائم سایبری در این اتحادیه می‌کند. جرائم سایبری و امنیت سایبری در صدر فهرست اولویت‌های برنامه بعدی –برنامه رم[3] (۲۰۱۹-۲۰۱۵)– قرار دارند. درواقع، بازنگری برنامه استکهلم از سوی مجلس اعیان بریتانیا این مسئله را مشخص کرد که جرائم سایبری و امنیت سایبری باید در زمان اجرای این برنامه جدید موردتوجه بیشتری قرار گیرند. این مجلس به‌خصوص رویکرد راهبردی‌تری را توصیه کرده و بر ضرورت همکاری نزدیک‌تر بخش خصوصی و دولتی نیز تأکید دارد (House of Lords, EU Committee 13th Report 2014, p.16–17).

از این گذشته، اتحادیه اروپا ابتکارهای دیگری را نیز با هدف رسیدگی به ابعاد مختلف جرائم سایبری ارائه کرده است. برای مثال، این مورد شامل امریه مربوط به مقابله با سوءاستفاده جنسی آنلاین از کودکان و پورنوگرافی کودکان (۲۰۱۱) و امریه مربوط به حملات به سیستم‌های اطلاعاتی با توجه به مجازات در نظر گرفته‌شده برای سوءاستفاده از ابزارهای جرائم سایبری، به‌خصوص بات‌نت‌ها[۲] (۲۰۱۰) می‌شود. جرائم سایبری کماکان اولویت سیاسی اصلی اتحادیه

1. Stockholm Programme
2. Council of Europe Convention on Cybercrime
3. Rome Programme

اروپا بوده و یکی از هشت اولویت چرخه سیاست گذاری اتحادیه اروپا در مورد جرائم جدی بین‌المللی سازمان‌یافته محسوب می‌شود. به نظر کمیسیون اروپا (2012, p.3)، «[حوزه جرائم سایبری] بخش مهمی از اقدامات صورت‌گرفته در جهت طرح راهبرد اصلی اتحادیه اروپا به‌منظور تقویت امنیت سایبری را شامل می‌شود». اتحادیه اروپا مسلماً با شناخت ماهیت جهانی تهدید جرائم سایبری درصدد همکاری با شرکای بین‌المللی خود و کارگروه اتحادیه اروپا-آمریکا در حوزه امنیت سایبری و جرائم سایبری، دارای اولویت بالا است (ن.ک. فصل ۷). پیشبرد کنوانسیون بوداپست (۲۰۰۱) و افزایش مشارکت‌های خصوصی-عمومی با هدف اشتراک بهترین راهکارها در زمینه مسائلی مانند بات‌نت‌ها جزو اهداف اصلی مشارکت محسوب می‌شوند. هدف دوم که مربوط به ایجاد و تقویت مشارکت‌های خصوصی-عمومی است، نیز، در برنامه استکهلم مطرح شده است (2010, p.23). قوانین حقوقی روشنگری که مروج همکاری در زمینه تحقیقات بین المللی در مورد جرائم سایبری هستند، نیز در این برنامه لحاظ شده‌اند. درنهایت، راهبرد امنیت سایبری اتحادیه اروپا (2013, p.9-11) نحوه عملکرد اتحادیه اروپا در تسهیل حرکت به سمت کسب توانمندی بیشتر در جهت مقابله با جرائم سایبری و بهبود همکاری میان بازیگران اصلی در اروپا و جهان را دقیق‌تر بیان می‌کند.

بسیاری از طرح های فوق ازجمله ایجاد مرکز اروپایی مقابله با جرائم سایبری، به دلیل وجود موانع در سر راه برخورد مؤثر با جرائم سایبری ازجمله «حدود اختیارات، توانمندی ناکافی برای تبادل اطلاعات، بروز مشکلات فنی در ردیابی سوابق مجرمان سایبری، توانمندی تحقیقاتی و قانونی متفاوت، کمبود کارکنان آموزش‌دیده و همکاری ناهماهنگ با سایر طرف های ذینفع مسئول برقراری امنیت سایبری» مطرح شده اند (European Commission 2012, p.3). هدف این فصل ارزیابی این مسئله است که اتحادیه اروپا تا چه حد به اهداف خود در زمینه اکوسیستم در حال ساخت برای جرائم سایبری دست پیدا کرده است و مهم تر از آن، این اهداف تا چه حد در رفع این موانع و ایجاد شرایط لازم برای برقراری امنیت تاب‌آور کارآمد در ابعاد مختلف جرائم سایبری ازجمله ابعاد حقوقی، اقتصادی، سیاسی، فرهنگی، عملیاتی و راهبردی نقش داشته‌اند. ساختار این فصل برای دستیابی به هدف خود بدین قرار است: در بخش

نخست، شرایط درک تکامل سیاست جرائم سایبری در اتحادیه اروپا و تحلیل و ارزیابی انتقادی از رویکرد آن در قبال حکمرانی امنیت در حوزه جرائم سایبری مطرح می‌شود. در بخش دوم، عملکرد اتحادیه اروپا در اتخاذ رویکردهای مربوط به جرائم سایبری و پیشبرد آن‌ها با توجه ویژه به اقدامات پیشنهادی راهبرد امنیت سایبری اتحادیه اروپا (۲۰۱۳) ارزیابی می شود.[۳] سپس در بخش نهایی و نتیجه‌گیری، ارزیابی‌ای از میزان پیشرفت اتحادیه اروپا در زمینه تأمین امنیت تاب‌آور کارآمد برای اروپا ارائه شده و همچنین چالش‌هایی مطرح می‌شود که کماکان پابرجا هستند.

حکمرانی بر جرائم سایبری در اتحادیه اروپا

رویکردهای اتحادیه اروپا در قبال جرائم سایبری، به‌موازات راهبردهای جامعه اطلاعاتی آن نظیر طرح اروپای الکترونیک[۱] (European Commission 1999) به‌منظور تقویت به‌کارگیری و برخورداری از منافع فناوری دیجیتال به شیوه غیرانحصاریِ اجتماعی توسعه یافته است. به دلیل افزایش تمایل اتحادیه اروپا برای تبدیل‌شدن به جامعه اطلاعاتی، اقدامات آن برای حفظ مزایای حاصله در برابر فعالیت مجرمانه نیز افزایش یافته است. در این شرایط، طرح اروپای الکترونیک با برنامه اقدام اروپای الکترونیک موردتوافق در ژوئن ۲۰۰۰ در نشست شورای اتحادیه اروپا در فیرا[۲] دنبال شد که در آن بر اهمیت رسیدگی به مسائل مربوط به امنیت شبکه و مقابله با جرائم سایبری تأکید گردید. رویکردهای پیشنهادشده در این مرحله، از هر دو ماهیت سیاست گذاری و فنی برخوردار بودند. برای ارتقای امنیت اینترنت، در کنار تصدیق بخش صنعتی به‌عنوان مسئول اصلی این امر (European Commission 1999, p.11)، مسئله تکامل رابطه بخش‌های عمومی–خصوصی در این صنعت نوپا نیز مطرح گردید، اما بخش عمومی به‌عنوان محرکی تلقی شد که نقش طرح‌های خصوصی را پررنگ‌تر می‌کند و مسیر مشخصی به سمت رویکرد فراحکمرانی نظری برای تقویت اقدامات تحت تأثیربخش خصوصی وجود

1. eEurope

ابتکار سیاسی برای اطمینان از بهره‌مندی کامل نسل‌های آینده اتحادیهٔ اروپا از مزایای تغییرات صورت گرفته در جامعهٔ اطلاعاتی. (م.)

3. Feira

داشت. بر طرح اقدام در زمینه توسعه همکاری و هماهنگی بهتر نیز تأکید گردید که مربوط به بحث کنوانسیون بوداپست در مجامع مختلف بین‌المللی است. در سطح فنی، به‌کارگیری بیشتر از کارت‌های هوشمند «به‌عنوان فناوری توانمندی که می‌تواند سطح اعتماد و حفظ حریم خصوصی را در خدمات جامعه اطلاعاتی افزایش دهد» پیشنهاد شد (Ibid.). طرح کارت هوشمند، مورد پشتیبانی صد میلیون یورویی بودجه تحقیقاتی قرار داشت و این بودجه در امتیاز کارت هوشمند به اوج خود رسید که در دسامبر ۲۰۰۲ معرفی شد.

گزارش نهایی در مورد طرح اروپای الکترونیک (۲۰۰۳)، به پیشرفت‌هایی در حوزه امنیت اینترنت و درعین‌حال به این مسئله اشاره داشت که کاربرد امریه های ارائه‌شده (Electronic Signatures, 2001)[۴] کماکان محدود بود. بااین‌وجود، طرح اروپای الکترونیک، مبنای رویکرد جامع تر اتحادیه اروپا در قبال امنیت شبکه و اطلاعات را ایجاد کرد. در ژوئن ۲۰۰۱، دو سند مشابه توسط کمیسیون اروپا منتشر شد که طرح کلی این رویکرد جامع را ترسیم می‌کردند که هدف آن رسیدگی به جرائم صورت گرفته در فضای سایبری بود. نخستین سند، ابلاغیه‌ای (European Commission 2001a) با عنوان ایجاد جامعه اطلاعاتی امن‌تر با اصلاح امنیت زیرساختارها و مقابله با جرائم رایانه‌ای، مجموعه مفاد قانونی ماهوی و رویه‌ای و اقدامات غیرحقوقی را جهت رسیدگی به فعالیت‌های مجرمانه داخلی و فراملی مطرح کرد و درعین‌حال، بر ضرورت حفظ موازنه بین امنیت و رعایت حقوق اساسی افراد نیز تأکید داشت (2001a, p.2).

برای مثال، در حوزه قانون ماهوی، بر توافق در زمینه تعاریف مشترک از جرائم سایبری و اتهامات و تحریم‌های مشترک و معرفی سازوکارهای اجرایی اتحادیه اروپا بر مبنای کنوانسیون بوداپست تأکید می‌شد که هدف آن اتخاذ اقدامی کارآمد در زمینه مسائلی مانند پورنوگرافی کودکان، نژادپرستی و بیگانه هراسی آنلاین بود (Ibid., p.14–15). ازنظر رویه‌ای، توجه اصلی همسو با قانون اتحادیه اروپا بر قانون کیفری بود و جهت حرکت نیز در مسیر بهبود همکاری بین قانون و سایر نهادهای مجری قانون (از طریق شناسایی متقابل و بهبود سازوکارها) برای تسهیل واکنش‌ها و درخواست‌های کارآمدتر مطرح‌شده از جانب کشورهای دیگر در حوزه جرائم سایبری بود (Ibid., p.16–24).

یکی از ابعاد مهم حکمرانی امنیت، همکاری در سطح بین‌المللی و وضع قوانین شفاف در مورد جستجو و توقیف فرامرزی بود. درنهایت، عنصر غیرحقوقی بیشتر بر اقدامات یا شرایط عملی بسیار هماهنگ با طرح اقدام ۱۰ بندی گروه هشت توجه داشت (ن.ک. فصل ۳) که ازنظر موضوعات کلی شامل این موارد می‌شد: تشکیل واحدهای پلیس متخصص جرائم سایبری در سطح ملی (با حضور کارکنانی از قوای مجریه و قضاییه) در محل‌هایی که چنین واحدهایی نداشتند، بهبود همکاری بین طرف‌های ذینفع، یعنی نهادهای مجری قانون، صنعت، نمایندگان مصرف‌کنندگان و مقامات مسئول حفاظت از داده‌ها و حمایت از طرح‌های مناسب ارائه‌شده از جانب صنعت و جامعه. در میان این موضوعات و در ارتباط با لایه سیاست‌گذاری و فنی، به آزادسازی ابزار رمزنگاری در حوزه قانون جامعه و توسعه تخصص و آموزش فنی، قوانین مشترک برای نگهداری سوابق و اطلاعات (جهت اشتراک اطلاعات)، همکاری بین بازیگران اتحادیه اروپا و اقدام از جانب صنعت، به‌خصوص از طریق تحقیق و توسعه توجه گردید (Ibid., p.24).

سند دوم، با عنوان ابلاغیه امنیت شبکه و اطلاعات: طرح پیشنهادی برای رویکرد سیاست‌گذاری اروپا (European Commission 2001b) بر مسائلی نظیر سرقت هویت، حملات سایبری و زیرساختی تأکید و توصیه‌هایی در زمینه نحوه تقویت امنیت تاب‌آور درون لایه‌های فنی، حقوقی و سیاست-گذاری ارائه شده است. این سند از پشتیبانی منطق حکمرانی امنیت نیز برخوردار بود که بر اساس آن «نیروهای بازار باعث ایجاد انگیزه برای سرمایه‌گذاری کافی در حوزه فناوری امنیت یا اقدام امنیتی نمی‌شوند» و در نتیجه «اقدامات سیاست‌گذاری می‌توانند موجب تقویت فرایند بازار و درعین‌حال، بهبود کارکرد چارچوب حقوقی شوند» (2001b, p.14). ازاین‌رو، نشانه روشنی از حرکت از فراحکمرانی هویت‌ها به سمت شیوه‌های نظری (تسهیلات، انگیزه‌ها) و عملی حکمرانی امنیت (چارچوب حقوقی) جهت حفاظت از بازار داخلی برای ارائه خدمات اطلاعاتی و ارتباطی و «کسب منفعت از راه‌حل‌های مشترک» و توانایی «انجام اقدام مؤثری در سطح جهان» ملاحظه گردید (Ibid., p.15).

ابزارها و اقدامات اصلی پیشنهادی بدین قرار بود: افزایش سطح آگاهی و انجام اقدامات آموزشی برای تمام طرف‌های ذینفع، اشتراک بهترین شیوه‌های امنیتی در میان کشورهای

عضو، و تقویت همکاری تیم‌های واکنش اضطراری رایانه‌ای اتحادیه اروپا جهت تضمین تبادل مؤثر اطلاعات پیرامون تهدیدات احتمالی و قریب‌الوقوع. علاوه بر این، جهت‌گیری تأثیرگذاری به سمت «تقویت همکاری بخش‌های خصوصی-عمومی در حوزه وابستگی به زیرساخت‌های اطلاعاتی» (Ibid., p.17) در شرایط طرح اقدام اروپای الکترونیک، سرمایه‌گذاری در امنیت شبکه و اطلاعات که کمتر از حد مطلوب تلقی می‌شد و لحاظ امنیت در چارچوب برنامه‌های تحقیقاتی کمیسیون جهت تسهیل این مورد، تضمین قابلیت همکاری در حوزه امنیت، به معنی بهبود راه‌حل‌ها از طریق استانداردسازی و صدور گواهینامه (تضمین به‌کارگیری استانداردهایی که در برنامه‌های مختلف اجرا می‌شوند) از طریق پشتیبانی از راه‌حل‌های کاربرپسند و تقویت استانداردهای موردتوافق بین‌المللی و حمایت از مشارکت طرف‌های ذینفع در سازمان‌ها و اقدامات استانداردسازی در سطح اروپا و بین‌الملل کمیته استانداردسازی الکتروتکنیک اروپا[1]، مؤسسه استانداردهای مخابراتی اروپا[2]، کارگروه مهندسی اینترنت[3]، کنسرسیوم جهانی وب[4]، اقدامات حقوقی[(5)] به دنبال مشابه‌سازی قوانین کیفری ملی مربوط به جرائم سایبری و امنیت سایبری و اقدامات با هدف ایجاد درکی مشترک از پیامدهای حقوقی امنیت در حوزه ارتباطات الکترونیک و پشتیبانی از دسترسی به محصولات رمزنگاری در سرتاسر اروپا وجود داشت. درنهایت، با توجه به ماهیت بدون مرز جرائم سایبری و امنیت، بر تداوم اقدامات صورت‌گرفته جهت پشتیبانی و همکاری در توسعه اقدامات بین‌المللی برای مقابله با جرائم سایبری و برقراری امنیت تأکید گردید (Ibid., p.17–22).

اتحادیه اروپا با تکیه بر موارد بالا، درصدد تقویت رویکرد جامع خود از طریق به‌کارگیری تصمیمات مختلف ساختاری و ارتباطات بود. تصمیم‌گیری ساختاری درباره حملات به سیستم‌های اطلاعاتی (Council Framework decision 2005/222/JHA, p.1) در اصل باعث ایجاد محیط یا لایه حقوقی قدرتمندتری برای انجام تحقیقات می‌شد و به‌خصوص هدف آن «بهبود همکاری میان مقامات امور قضایی و سایر مقامات ذی‌صلاح ... از طریق

1. European Committee for Electrotechnical Standardization (Cenelec)
2. European Telecommunications Standards Institute (ETSI)
3. Internet Engineering Task Force (IETF)
4. World Wide Web Consortium (W3C)

مشابه‌سازی احکام مربوط به قوانین کیفری در کشورهای عضو» بود. این تصمیم‌گیری ساختاری تعاریف مشترکی از حملات سایبری با توافق کشورهای عضو در زمینه تعاریف درباره ماهیت اقدامات مجرمانه ارائه داد که عبارت‌اند از: «دسترسی غیرقانونی به سیستم‌های اطلاعاتی، مداخله غیرقانونی در سیستم‌ها و داده‌ها»[۶] (Ibid., p.2-3). تصمیم‌گیری ساختاری درشورای جداگانه‌ای با هدف مشابه، حرکت به سمت ایجاد محیط حقوقی مشترک در زمینه مسئله سوءاستفاده جنسی از کودکان و پورنوگرافی کودکان موردتوافق قرار گرفت (JHA/2004/68) و مقرراتی برای جلوگیری از تبادل اینترنتی پورنوگرافی کودکان در آن در نظر گرفته شد. گرچه این تصمیم‌گیری ساختاری، تنها به الزامات حداقلی ازنظر مشابه‌سازی قانون در کشورهای عضو می‌پرداخت و در نتیجه، باعث ایجاد مشکلاتی در زمینه تعقیب مجرمین در داخل و خارج از کشور گردید. منطق امنیت تاب‌آور، مبنای این موارد تصمیم‌گیری ساختاری ایجاد تسهیل در همکاری و هماهنگی میان مسئولان دولتی ذی‌ربط حتی به‌رغم وجود محدودیت‌های عملی بود، چراکه فرهنگ امنیت واقعی از آن حمایت نمی‌کرد. مورد فقدان «فرهنگ» در بیانیه کمیسیون اروپا در زمینه ترسیم «راهبرد جامعه اطلاعاتی امن» (۲۰۰۶) و به دنبال آن راه‌اندازی طرح آی۲۰۱۰ [۱]- جامعه اطلاعاتی اروپا برای رشد و اشتغال[۲] مطرح گردید که بر مسئله اعتبار و امنیت شبکه‌ها و سیستم‌های اطلاعاتی (European Commission 2005) برای جامعه و اقتصاد تأکید داشت. به‌خصوص، هدف این بیانیه «طرح راهبرد جهانی پویایی در اروپا بر پایه فرهنگ امنیت بود که بر اساس گفتمان، مشارکت و توانمندسازی ایجاد شد.» (2006, p.3) کمیسیون اروپا متوجه این امر شد که باید به همگرایی و انسجام در رویکرد تابه‌حال چندجانبه‌ای دست پیدا کند تا امنیت جامعه اطلاعاتی تضمین گردد که شامل موارد مقابله با جرائم سایبری و انجام اقدامات خاص در زمینه امنیت شبکه و اطلاعات و دستیابی به چارچوب قانونی در مورد ارتباطات الکترونیکی مربوط به مسائل حفاظت از حریم خصوصی و داده‌ها است.

1. i2010

طرح اتحادیهٔ اروپا در زمینه شکاف‌زدایی الکترونیکی که جنبشی اجتماعی با هدف رفع شکاف رقمی موجود در زمینه دسترسی به فناوری‌های نوین اطلاعاتی بین جوامع مختلف است. (م.)

2. A European Information Society for Growth and Employment

درواقع، به‌رغم انجام اقدامات قبلی برای رسیدگی به جرائم سایبری در سطوح اروپایی، ملی و بین‌المللی، چند مسئله مهم باقی ماند که مستلزم توجه سیاسی و قانونی بیشتری بود. نخستین مسئله، مربوط به انگیزه ارتکاب جرائم سایبری بود که از ایجاد اختلالی ساده به تمایل به سودجویی تغییر کرده بود. این موضوع با افزایش تعداد ابزار مخرب در دسترس مجرمان سایبری برای دستیابی به اهداف خود ازجمله هرزنامه ها، نرم‌افزارهای جاسوسی و فیشینگ[1] و وابستگی روزافزون سرورها و رایانه‌های در معرض خطر برای توزیع آن‌ها مواجه شده بود(2006, 4.p). سرویس‌های شبکه تلفن همراه و دستگاه های هوشمند برخوردار از پشتیبانی فناوری شبکه و رایانه (هوش محدوده‌ای)، مشکلات دیگری برای انسجام و امنیت اینترنت مانند برنامه‌هایی که فرصت‌های جدیدی را برای حمله مجرمان سایبری فراهم می‌کردند، ایجاد می‌کنند. شایان‌ذکر است که رویکرد موردحمایت کمیسیون اروپا به‌طور صریح‌تر بیانگر حرکت به سمت «رویکردی جامع» است که از طریق فراحکمرانی نظری (حمایت از مشارکت و هماهنگی) و عملی (قانون‌گذاری برای افزایش شفافیت حقوقی و بهبود همکاری بین نهادهای مجری قانون)،(۷) با امنیت تاب‌آور باز، انطباق پذیر و جامع هماهنگ بود. به‌علاوه، این رویکرد بیانگر درک این مطلب بود که اگر قرار باشد فرهنگ امنیت سایبری پدید آید که علاوه بر نشانه ها، به علل اصلی مشکلات امنیت سایبری در سطوح فردی و نهادی (بخش‌های خصوصی و دولتی) نیز بپردازد، وجود رویکرد چندذینفعی و افزایش دانش در مورد مشکلات ضرورت خواهد داشت. کمیسیون اروپا همچنین در این سند نشان داد که این نوع رویکرد مکمل فعالیت آن در زمینه حمایت از حفظ زیرساخت های حیاتی است که آژانس امنیت شبکه و اطلاعات اتحادیه اروپا که در سال ۲۰۰۴ به خاطر آن تأسیس شده بود، نقش اصلی را در شناخت بهترین شیوه، افزایش آگاهی و ایجاد مشارکت مبتنی بر اعتماد در میان تمام طرف های ذینفع ایفا نمود (Ibid.,, p.6–9). به‌خصوص، این آژانس در حکم اولیه خود (۲۰۰۵) موظف به حمایت از گروه‌های ملی واکنش اضطراری رایانه‌ای اتحادیه اروپا شده بود که به این دلیل، برنامه تیم واکنش اضطراری رایانه‌ای اتحادیه اروپا و کارگروه همکاری و پشتیبانی این گروه ایجاد شده بود. این کار شامل

1. Phishing

کسب اطلاعات شخصی مانند نام کاربری، گذرواژه، اطلاعات حساب بانکی و سایر موارد از طریق جعل تارنمای اینترنتی، آدرس ایمیل و غیره. (م.)

شناخت توانمندی‌های گسترده پایه و تحلیل شکاف در حوزه ملاحظات عملیاتی و عوامل حقوقی و قانونی و اخیراً (مبحث بعد) کار بر روی شیوه مناسب مربوط به ویژگی‌های امنیت شبکه و اطلاعات حوزه جرائم سایبری می‌شود (ENISA 2012).

ازاین‌رو، حتی در این مرحله اولیه نیز این مسئله مشخص است که اتحادیه اروپا، حداقل در سند و گفتمان رسمی خود، شرایط لازم برای تأمین امنیت تاب‌آور کارآمد را تشخیص می‌دهد. بُعد فراحکمرانی عملی در ابلاغیه کمیسیون اروپا، پیرامون سیاست‌گذاری عمومی در زمینه مقابله با جرائم سایبری بیشتر مطرح گردید (European Commission 2007) که در آن هدف بهبود همکاری و هماهنگی میان نهادهای پلیسی در سطح راهبردی و عملیاتی و میان کشورهای عضو اتحادیه اروپا در سطح سیاسی بود. به‌علاوه، این ابلاغیه موجب پیشبرد همکاری حقوقی و سیاسی با کشورهای ثالث شد و تأکید ویژه‌ای بر تداوم یادگیری در شرایط ظهور امنیت تاب‌آور با بیان نیازهای آموزشی مربوط به مسائل جرائم سایبری برای مقامات بخش‌های مجریه و قضاییه، داشت و درواقع، پیوند و همبستگی بین برنامه‌های آموزشی مقامات مربوطه را جهت دستیابی به همکاری بهتر، افزایش داد.

علاوه بر این، با توجه به نقش مهم بخش خصوصی در انواع امنیت تاب‌آور کارآمد، بهبود ویژگی خصوصی- عمومی سیاست جرائم سایبری کمیسیون اروپا از طریق تقویت سازوکارهای گفتمان مورد تأکید قرار گرفت.[۸] موارد چنین شیوه مناسبی شامل اقدامات مربوط به مقابله با پورنوگرافی کودکان می‌شد که در آن همکاری مؤثر میان شرکت‌های کارت اعتباری و آژانس‌های مجری قانون به پلیس و نهادهایی مانند گروه کارشناسان پیشگیری و مقابله با تقلب[1] در ردیابی خریداران پورنوگرافی کودکان به‌صورت آنلاین کمک می‌کرد. علی‌رغم این مسئله، چالش موجود بهبود همکاری عملیاتی در اروپا با توجه به عدم تعهد قانونی شرکت‌های خصوصی به اشتراک اطلاعات در حوزه جرائم سایبری با مقامات دولتی و منطق اقتصادی حاکم بر این شرکت‌ها است که اولویت آن‌ها الگوی تجاری و در نتیجه، رازداری و نه تبادل علنی اطلاعاتی است که احتمال دارد شهرت و منافع آن‌ها را به خطر اندازد (Interview, ENISA, July 2012).

1. Fraud Prevention Expert Group

قوانین اتحادیه اروپا در زمینه حفظ حریم خصوصی داده‌ها، حفظ و حفاظت از اطلاعات شخصی محور بهبود تبادل اطلاعات بین بخش‌های گوناگون به شمار می‌آید که شرط اصلی تأمین امنیت تاب‌آور است. در اینجا امریه حفظ اطلاعات[1] (۲۰۰۶)[۹] برای دستیابی به فرهنگ اشتراک اطلاعات و چارچوب و رویکردی یکپارچه بسیار حائز اهمیت است چراکه بر اساس آن تمام کشورهای عضو باید قانونی را اجرا می‌کردند که به‌موجب آن شرکت‌های ارائه‌دهنده خدمات اینترنت و مخابرات باید سوابق ترافیک کاربران (ارتباطات نه محتوا) را به مدت شش ماه تا دو سال نگهداری کنند. باوجوداینکه بسیاری از شرکت‌های مخابرات این رویه را اجرا می‌کردند، بسیاری از ارائه‌دهندگان خدمات اینترنت این کار را انجام نمی‌دادند. در کنار این مسائل، اختلافات بی‌شمار حقوقی و فنی در مورد قانون ملی حفظ اطلاعات نیز مورد دیگری است که موجب ناکارآمدی اقدامات صورت‌گرفته در زمینه مقابله با جرائم سایبری ازنظر فنی و در سطح سیاست‌گذاری شد.

این امریه درصدد اصلاح این وضعیت بود که البته این اقدام آن بحث‌برانگیز شد، چراکه بسیاری از گروه‌های مدافع حقوق دیجیتال از عدم شفافیت حوزه به‌کارگیری اطلاعات جمع‌آوری‌شده و امکان سوءاستفاده احتمالی از آن‌ها انتقاد داشتند.[۱۰] پارلمان اروپا نیز این مسئله را مطرح می‌کند که این موضوع باعث ایجاد جامعه نظارتی و تضعیف حقوق بنیادین می‌شود. به‌علاوه، این امریه ابلاغ‌شده به اکثر کشورهای عضو موضوع معضل حقوقی در سطح ملی و اروپایی (دیوان دادگستری اتحادیه اروپا) شده بود و گزارش کمیسیون اروپا از ارزیابی این امریه (۲۰۱۱) نشان می‌داد که موارد تناقض بسیاری در نحوه اجرای آن و هویت مقاماتی وجود داشت که امکان دسترسی به این اطلاعات را دارند. علاوه بر این، ناظر حفاظت از اطلاعات اتحادیه اروپا[2] این مسئله را مطرح نمود که کمیسیون اروپا ثابت نکرده است که این امریه ضروری و متناسب است که این امر بر اساس منشور حقوق بنیادین اتحادیه اروپا مندرج در معاهده لیسبون غیرقانونی به‌حساب می‌آید (European Frontier Foundation 2011).

در نتیجه، تنش واقعی میان تضمین تأمین امنیت و حفظ حریم خصوصی اطلاعات شخصی وجود دارد که علاوه بر بعد حقوقی، در ابعاد فرهنگی و سیاسی اتخاذ سیاست امنیت

1. The Directive on Data Retention
2. European Data Protection Supervisor (EDPS)

تاب‌آور نیز گنجانده شده است. کمیسیون اروپا در بازنگری قوانین حفاظت از داده‌ها که طی چند سال گذشته انجام داده است، به‌رغم تأکید بر اعتبار اصول محوری مبنای رویکرد (برگرفته از امریه اصلی ۱۹۹۵) آن –حفاظت از حقوق و آزادی‌های اساسی افراد شامل حفاظت از داده‌ها و درعین‌حال، تضمین جریان آزاد اطلاعات– تصدیق می‌کند که فناوری نوین مشکلات جدیدی را در زمینه تضمین بهترین استانداردها برای حفاظت از داده‌ها در داخل اتحادیه اروپا و در سطح جهان ایجاد می‌کند؛ گرچه، تنش بین امنیت و حقوق هنوز گسترش نیافته است. درواقع، افشای برنامه ابزار برنامه‌ریزی برای ادغام، هماهنگ‌سازی و مدیریت منابع توسط ادوارد اسنودن در سال ۲۰۱۳، تنها موجب تشدید این تنش شد که پیامدهایی نیز در سطوح و لایه‌های مختلف جرائم سایبری داشت (جهت کسب اطلاعات بیشتر، ن.ک. فصل ۷). حتی پیش از افشاگری‌های اسنودن، تردید بسیاری در مورد موازنه بین برقراری امنیت و حفظ حریم خصوصی افراد وجود داشت[11] و گروه‌های جامعه مدنی خواستار نظارت بیشتر بر تأثیر این امریه بر حریم خصوصی شهروندان بودند و شواهدی مبنی بر این ارائه دادند که این برنامه در آینده به نحوی طراحی می‌شود که به حریم خصوصی افراد بیشتر نفوذ می‌کند. در ارزیابی صورت‌گرفته از جانب سازمان حقوق دیجیتال اتحادیه اروپا (April 2011, p.20) چنین نتیجه‌گیری شد که:

> «گزارش ارزیابی کمیسیون اروپا و گزارش در سایه (موازی) سازمان حقوق دیجیتال اتحادیه اروپا نشان می‌دهد که این امریه عملکرد ناموفقی در تمام سطوح دارد و نتوانسته است به حقوق اساسی شهروندان اروپا احترام گذارد و در هماهنگ‌سازی بازار واحد، عملکرد ناموفقی داشته و در مقابله با جرائم جدی نیز وجود آن ضرورت چندانی نداشته است.»

کمیسیون اروپا در گذشته متوجه پیچیدگی دستیابی به موازنه از طریق اقدامات خود شده و اغلب دیدگاه عمل‌گرایانه‌ای در زمینه این موضوع اتخاذ کرده است که حق ناشناس ماندن (حفظ حریم خصوصی) و پاسخگویی (دسترسی) در زمان رسیدگی به جرائم آنلاین موضوعات ناسازگاری نیستند (Interview, DG Home, November 2011). برای مثال، این رویکرد در طرح پیشنهادی مربوط به اتخاذ «رویکردی جامع در قبال حفاظت از داده‌های شخصی در اتحادیه

اروپا»(2010,p14) لحاظ شد که در آن این موضوع مطرح می‌شود که «باید این مسئله در نظر گرفته شود اعمال حقوق خاص حفاظت از اطلاعات توسط فرد تا چه حد موارد پیشگیری، بازرسی، تشخیص یا پیگرد جرائم کیفری یا اجرای مجازات کیفری در پرونده خاصی را به خطر می‌اندازد» و اینکه این مورد، «تأثیر مستقیمی بر احتمال اعمال حقوق حفاظت از داده‌ها یا افراد در این حوزه دارد» (Ibid.).

ازاین‌رو، چارچوب حقوقی جامع جدید پیشنهادی، جایگزین ابزارهای حقوقی بخشی در حوزه همکاری پلیس و دادگستری در مسائل کیفری نمی‌شود که حاکم بر کارکرد نهادهایی مانند یوروپل و دادگستری اتحادیه اروپا (یوروجاست)[۱۲] است. این نهادها یا زیر نظر رژیم‌های حفاظت از داده‌های خاص خود کار می‌کنند یا به‌طورمعمول، از ابزار حفاظت از داده‌ها در شورای اروپا بهره می‌گیرند. ازاین‌رو، با توجه به اینکه بر اساس رأی دادگاه عدالت اتحادیه اروپا در آوریل ۲۰۱۴ امریه حفظ داده‌ها به این دلیل بی‌اعتبار اعلام شد که حق حریم خصوصی و حفاظت از اطلاعات افراد را نقض می‌کند، وظیفه اتحادیه اروپا هماهنگ‌سازی قوانین ویژه حفاظت از داده‌ها و چارچوب کلی‌تر حقوقی حفاظت از داده‌ها[۱] و درمجموع، تبیین این مسئله است که «محدودیت‌های هماهنگ‌شده» برخی قوانین حفاظت از داده‌ها برای تأمین آن دسته از حقوق و آزادی‌های آنلاین افراد سودمند هستند. با توجه به بحث گسترده پیرامون حفظ حریم خصوصی و برقراری امنیت و تفاسیر بی‌شمار مطرح‌شده از قوانین اتحادیه اروپا در زمینه حفاظت از اطلاعات توسط طرف‌های ذینفع ازجمله مرجع ملی حفاظت از داده‌ها، این وظیفه ساده‌ای نیست. در شرایط حکمرانی امنیت تاب‌آور، تفسیر، کارکرد یا اجرای واحدی از این قوانین وجود ندارد، در نتیجه تضمین همکاری و هماهنگی کارآمد در حوزه جرائم سایبری بسیار دشوارتر می‌شود.

این مقررات (چارچوب کلی اتحادیه اروپا برای حفاظت از داده‌ها[۲])[۱۳] و امریه (در زمینه حفاظت از داده‌های شخصی مربوط به فعالیت‌های کیفری و قضایی)[۱۴] که در سال ۲۰۱۲ مطرح شدند[۱۵]، درصدد یافتن راهی از طریق این مسائل جهت اتخاذ رویکردی هماهنگ و

1. National Data Protection Authorities
2. General EU Framework for Data Protection

جامع در قبال حفاظت از داده‌ها بودند. این چارچوب جدید (مقررات و امریه)، تغییر آشکار قابل‌ملاحظه‌ای در زمینه فراحکمرانی عملی‌تر در این حوزه محسوب می‌شود. این مقررات به دنبال طرح حقوق بیشتر، برای افراد نگران افشای آنلاین داده‌های شخصی و ایجاد اطمینان حقوقی برای واحدهای تجاری است، اما هدف این امریه تبیین رابطه میان حفاظت از داده‌های شخصی و پردازش آن‌ها با هدف همکاری با پلیس و دستگاه قضایی است. عملکرد امریه قبلاً تحت پوشش تصمیم‌گیری ساختاری قرار داشت (JHA/977/2008)، اما قدرت اجرایی را در اختیار اتحادیه اروپا قرار نداده بود و به فعالیت‌های پردازش بین مرزی محدود می‌شد که این امر باعث ایجاد مشکلات عملی حائز اهمیتی در اجرای آن به علت ابهام در مورد تعیین زمان و نحوه شمول، پردازش و به‌کارگیری اطلاعات داخلی در تحقیقات می‌شد (ن.ک. Implementation Report on the Framework Decision (COM (2012)12)). در نتیجه ازلحاظ نظری، این چارچوب جدید باعث تسهیل ایجاد برخی شرایط مهم برای برقراری امنیت تاب‌آور کارآمد در این حوزه از طریق تقویت اعتماد بین بازیگران فراملی مربوطه (پلیس و دستگاه قضایی) می گردد و درعین‌حال، همکاری را بهبود می‌بخشد و تبادل اطلاعات برون‌مرزی در حوزه تحقیقات جرائم سایبری را نیز آسان تر می سازد. برای مثال، هر دو مورد امریه و مقررات احتمالاً برای برخی تیم‌های واکنش اضطراری رایانه‌ای اتحادیه اروپا و نهادهای مجری قانون، ازنظر ایجاد قوانین اساسی مشترک سودمند هستند که در مشروعیت‌بخشی به فعالیت‌های آن‌ها در تحقیقات و رویدادهای حوزه جرائم سایبری نقش داشتند (ENISA, 2012b, p.5). گرچه در عمل باید ملاحظه کرد تا چه حد منطق و اقدامات مشخص انجام‌شده در چارچوب کلی به نحو مناسبی در مفاهیم مربوط به حفظ حریم خصوصی و برقراری امنیت ادغام می‌شود، چراکه به اعتقاد برخی مفسران این مقررات کماکان از پشتیبانی «دیدگاه امنیت کلاسیک و تضاد بین حقوق و امنیت» برخوردار است (Porcedda 2012, p.71)[۱۶].

بهره‌برداری از دنیای آنلاین با هدف سوءاستفاده از کودکان

با توجه به تحولات صورت‌گرفته در محیط فناوری اطلاعات و کاربرد روزافزون اینترنت در ابعاد مختلف زندگی، یکی از مشکلات فزاینده در حوزه جرائم سایبری بهره‌برداری از دنیای آنلاین با هدف سوءاستفاده از کودکان است. به‌رغم اجرای قوانینی در اتحادیه اروپا از سال ۲۰۰۴ به‌منظور رسیدگی به مسئله سوءاستفاده جنسی و بهره‌برداری از کودکان و پورنوگرافی آنان[۱۷]، این قانون دقیقاً به‌جهت وقوع این تحولات جدید و فرصت‌هایی که برای مجرمان فراهم می‌آورد موردبازنگری قرار گرفت. تصمیم‌گیری ساختاری سال ۲۰۰۴ از جهات مختلف ناکافی تلقی می‌شد؛ دلیل آن صرفاً این نبود که این تصمیم‌گیری فقط مشابه‌سازی قانونی حداقلی را در بین دولت‌های عضو مطرح می‌کرد که همکاری و هماهنگی بین مقامات و نهادهای ملی در تحقیقات را دشوار می‌ساخت. علاوه بر این، با توجه به آنکه این قانون از سال ۲۰۰۴ اجرایی شده بود، اشکال جدیدی از سوءاستفاده جنسی و بهره‌برداری از طریق اینترنت (برای مثال، تماس جنسی با کودکان و پورنوگرافی) به‌عنوان جرم تلقی نشده بودند. طرح بازنگری شده کمیسیون اروپا که در سال ۲۰۱۰ پیشنهاد شد و در سال ۲۰۱۱ موردتوافق قرار گرفت به دنبال این بود که فراتر از قانون حداقلی و به سمت فراحکمرانی عملی‌تری ازلحاظ دامنه و جوهر در حوزه‌هایی نظیر مجازات سوءاستفاده جنسی و بهره‌برداری از کودکان (حقوق کیفری ماهوی)، تحقیقات حوزه‌های قضایی متفاوت، اقدامات و پرونده‌ها و پیشگیری از وقوع جرائم، برای مثال، سازوکارهای ملی مسدودسازی دسترسی به تارنماهای دارای محتوای پورنوگرافی کودکان رود.

ویژگی دوم نیز بحث‌برانگیز بوده است، چراکه بار دیگر وارد بحث حقوق دیجیتال و حقوق بشر گردید و پیامدهایی نیز برای نوع حکمرانی لازم به‌منظور تأمین امنیت تاب‌آور کارآمد در حوزه جرائم سایبری داشت. در اصل، در طرح اولیه کمیسیون اروپا مسئله «مسدودسازی اجباری [تارنماهای] پورنوگرافی کودکان»، یعنی در نظر گرفتن نقش مستقیم‌تری برای دولت در این موارد پیشنهاد شده بود (Interview, DG Home, November 2011). در پیش‌نویس بعدی نیز، تأکید بیشتری بر توانمندسازی مقامات پلیس و قضایی برای اجرای عملیات مسدودسازی محتوای پورنوگرافی گردید، یعنی اقدامی به دور از تضعیف قضایی

(European Parliament, Draft Report January 2011) که برخی لابی‌گرها آن را خودتنظیمی درونی[1] می نامند در جهت شکلی از حکمرانی عملی بیشتر واگذارشده که بعضی آن را خودتنظیمی خارجی[2] یا واگذاری اجرای قانون می نامند، صورت گرفت (European Digital Rights 2011, p.6). پارلمان اروپا پیشنهاد اولیه مبنی بر مسدودسازی اجباری [تارنماها] را رد کرد و در متن موردتوافق، گزینه حکمرانی انتقالی را از این نظر مطرح کرد که «کشورهای عضو می‌توانستند با مناسب‌ترین ابزار مدنظر خود اقدام به مداخله فوری جهت توقف مشاهده و دانلود به منظور جلوگیری از آسیب بیشتر قربانی نمایند» (European Parliament, Draft Report January 2011, p.14). در نتیجه، پیامد حاصله این است که بازیگران مختلف، تحت تأثیر منطق‌های اساساً متفاوتی در مورد مسئله کارایی مقابله با جرائم سایبری قرار می گیرند. این تنها یک نمونه از تنش موجود بین لایه‌های حقوقی، قانونی و سیاست گذاری محسوب می‌شود که پیامدهایی نیز برای موارد به کار گرفته‌شده در لایه فنی جهت مقابله با بهره‌برداری و سوءاستفاده آنلاین از کودکان (برای مثال، به‌کارگیری فناوری نظارت و ردیابی) دارد.

طرح‌های بیشتر مرتبط با اهداف کلی طرح اقدام جهت اجرای راهبرد هماهنگی برای مقابله با جرائم سایبری (۲۰۱۰) ازنظر بهبود اعتماد، همکاری و هماهنگی بین بازیگران بخش خصوصی و دولتی به‌منظور برخورد با سوءاستفاده آنلاین از کودکان در داخل و خارج از اروپا مطرح شده اند. برای مثال، کمیسیون اروپا به‌عنوان بخشی از برنامه اینترنت امن‌تر[3](۱۸)، مرکز پشتیبانی از شبکه سازمان‌های غیردولتی راه‌اندازی‌شده به‌صورت هات‌لاین [خط ارتباطی نقطه‌به‌نقطه] در کشورهای عضو اتحادیه اروپا است که گزارش‌هایی پیرامون تارنماهای مرتبط با سوءاستفاده از کودکان را جمع‌آوری می‌کند تا آن‌ها را حذف کند یا در مورد آن‌ها تحقیق نماید. محتوای سوءاستفاده از کودکان مرتبط با جرائم آنلاین اساساً توسط یوروپل مورد رسیدگی قرار می‌گیرد، ولی کمیسیون اروپا از طرح هایی نظیر ائتلاف مالی اتحادیه اروپا[4] (۱۹) میان ارائه دهندگان خدمات اینترنت، بانک‌ها و ارائه‌دهندگان سیستم پرداخت، سازمان های غیردولتی، شرکت‌های

1. Internal Self-Regulation
2. External Self- Regulation
3. Safer Internet Programme
4. European Financial Coalition (EFC)

مخابرات و همچنین نهادهایی مانند یوروپل، یوروجاست و مقامات قضایی و پلیس در اروپا (برای مثال، ن.ک. The Digital Economy 2014) نیز حمایت می‌کند. اتحاد جهانی علیه سوءاستفاده جنسی آنلاین از کودکان[1] در سطح جهانی و با اهداف عملیاتی مشابه طرح اقدام کلی جهت اصلاح چارچوب حقوقی، همکاری مشترک در حوزه‌های قضایی، آموزشی و حمایت از نقش بیشتر بخش خصوصی در دسامبر ۲۰۱۲ راه‌اندازی شد. در اصل این اتحاد با شیوه هماهنگی باز[2] و با هدف اشتراک بهترین اقدامات از طریق گزارش‌دهی مستمر عمل می‌کند. با وجود طرح مسئله اصلاح اکوسیستم اروپا و جهان در این نوع طرح‌ها برای مقابله با جرائم سایبری در میان‌مدت، ارزیابی کارایی آن‌ها در عمل کماکان زود است، گرچه گزارش‌های اولیه حاکی از پیشرفت چهار هدف اصلی سیاست‌گذاری موردتوافق و وجود موانعی بر سر راه آن‌ها است (Report of the Global Alliance 2013، برای کسب اطلاعات بیشتر در مورد طرح مشترک اروپا و آمریکا ن.ک. فصل۷).

درنهایت، اداره کل شبکه های ارتباطات، محتوا و فناوری (جامعه اطلاعاتی سابق) به دنبال تقویت فرهنگ امنیت از طریق طرح شاخص خود با عنوان راهبرد اینترنت بهتر برای کودکان اتحادیه اروپا[3] (۲۰۱۲) در سطوح فردی و جمعی است. این طرح به‌واسطه نگرانی درباره تقویت امنیت از طریق این موارد پشتیبانی می‌شود: «افزایش تولید برنامه‌های آنلاین با محتوای خلاقانه و آموزشی برای کودکان، افزایش سطح آگاهی و تدریس ایمنی آنلاین در تمام مدارس اروپا به‌منظور افزایش سواد دیجیتالی و رسانه‌ای و خود مسئولیتی کودکان؛ ایجاد محیطی امن برای کودکان که در آن ابزار لازم برای تضمین حفاظت آنلاین آن‌ها در اختیار والدین و کودکان قرار می‌گیرد مانند طراحی سازوکارهای آسانی برای گزارش محتوا و رفتار زیان آور آنلاین، وجود تنظیم‌های پیش‌فرض مشخص مناسب سن یا نظارت کاربرپسند ویژه والدین و جلوگیری [از انتشار/اشاعه] مطالب آنلاین در مورد سوءاستفاده جنسی از کودکان از طریق ارتقای بخش تحقیق در این رابطه و به‌کارگیری راه‌حل‌های مبتکرانه فنی در تحقیقات پلیس.»

ارزیابی‌های اولیه صورت گرفته در مورد میزان پیشرفت آگاهی از چهار رکن عنوان شده این

1. Global Alliance against Child Sexual Abuse
2. Open Method of Coordination (OMC)
3. European Strategy for a Better Internet for Children

راهبرد و در نتیجه، از شرایط مختلف برقراری امنیت تاب‌آور کارآمد محدود و ناچیز است، چراکه این راهبرد از می ۲۰۱۲ اجرایی شد و ارزیابی‌های موجود نیز تصویری مبهم را ارائه می‌دهند. برای مثال، تحقیقی در بریتانیا (Livingstone 2013) نشان می‌دهد که به‌رغم وجود ارزیابی مثبتی در کل از محتوای با کیفیت بالای در دسترس کودکان (ازنظر ۵۶ درصد از کودکان انگلیسی محتوای مطالب اینترنتی «بسیار خوب» و ازنظر متوسط ۴۴ درصد کودکان اروپا این محتوا «خوب» است)، اما ازنظر آگاهی و توانمندی این ارزیابی چندان مثبت نیست، چراکه تغییر چندانی در دامنه شاخص‌های مهم از زمان اتخاذ این راهبرد، صورت نگرفته است. برای تبیین این موضوع، «یک‌سوم افراد ۱۲-۱۵ ساله اعتبار تارنماهای جدیدی که استفاده می‌کنند را بررسی نمی‌کنند (آماری که طی شش سال گذشته تغییر ناچیزی داشته است)» و بر اساس شبکه تحقیقاتی چندملیتی کودکان اتحادیه اروپا[1] ، این مسئله مشخص شد که:

> «تنها ۵۹ درصد از کودکان ۶-۱۱ ساله بریتانیا می‌توانند تنظیمات خصوصی شبکه اجتماعی خود را تغییر دهند و صرفاً ۵۸ درصد از آن‌ها این مسئله را عنوان می‌کنند که می‌توانند در مورد اعتبار تارنماهای اینترنتی خود قضاوت کنند. در ضمن، نیمی از آن‌ها (۵۱ درصد) این مطالب را بیان می‌کنند که به دلیل صرف زمان خود در اینترنت، زمان کمتری را با دوستان و خانواده خود نسبت به زمانی که باید با آن‌ها سپری کنند، می‌گذرانند. (بسیار بیشتر از میانگین ۳۵ درصدی اروپا).»

به‌رغم وجود شواهدی دال بر انجام اقدام مناسب از سوی صنایع و سازمان‌های غیردولتی، در مورد تأثیر افزایش سطح آگاهی هیچ نوع ارزیابی‌ای وجود ندارد و منابع دولتی نیز در این حوزه در نظر گرفته نشده‌اند.[۲۰] البته این نوع مسائل نشانه برخی مشکلات گسترده‌تر پیش روی ایجاد فرهنگ امنیت کارآمد در سطح اروپا و جهان و بیانگر وجود موانع قابل‌توجهی در سر راه ایجاد چنین شرایطی در کوتاه‌مدت است، به‌خصوص اگر منابع لازم در دسترس نباشد.

1. EU Kids online

راهبرد امنیت سایبری اتحادیه اروپا: جرائم سایبری

باوجوداین که بر اساس امریه حفظ حریم خصوصی الکترونیکی (۲۰۰۹) آلوده کردن رایانه‌ها و تبدیل آن‌ها به بات‌نت ممنوع شده است، تحولات فناورانه و استفاده روزافزون مجرمان از روش‌های حمله پیچیده ضرورت انجام اقدامات بیشتر در جهت کاهش این تهدید رو به رشد را مطرح می‌ساخت. امریه مربوط به حملات صورت گرفته علیه سیستم‌های اطلاعاتی (۲۰۱۰) بر مبنای بازنگری اجرای[۳۱] امریه پیشین[۳۲]، مطرح گردید و در میان سایر موارد، عدم هماهنگی چارچوب حقوقی اتحادیه اروپا را به‌عنوان مانع اصلی بر سر راه تأمین امنیت تاب‌آور کارآمد در حوزه جرائم سایبری شناسایی کرد. درواقع، این امریه بیانگر تغییر قابل‌ملاحظه‌ای در چارچوب حکمرانی کاهش جرائم اینترنتی و به‌ویژه استفاده از بات‌نت‌ها بود. این امریه در سال ۲۰۱۰ مطرح شد، اما به دلیل بروز اختلافات داخلی بین شورا و پارلمان اروپا بر سر شنگن، توافق در مورد آن تا مدت زیادی به تأخیر افتاد و سرانجام در چهارم جولای ۲۰۱۳ پارلمان اروپا آن را با اهداف کلی زیر تصویب کرد

۱. حرکت به سمت اتخاذ رویه‌ها و قوانین کیفری یکپارچه تر در حوزه حملات مجرمانه علیه سیستم‌های اطلاعاتی کشورهای عضو

۲. تقویت و بهبود هماهنگی، همکاری و تبادل اطلاعات در میان بازیگران ذی‌ربط کشورهای عضو اتحادیه اروپا و بین مؤسسات اتحادیه اروپا، مؤسسات کشورهای عضو آن و نهادهای بین‌المللی مربوطه

۳. تسهیل همکاری بین مقامات دولتی، بخش خصوصی و جامعه مدنی

رویکرد اتحادیه اروپا در قبال جرائم سایبری یکپارچه نیست، یعنی طبق تحلیل فوق، به‌جای چارچوبی جامع، مجموعه ابزارهای نظارتی و حقوقی هم‌پوشان وجود دارد. درواقع، اتخاذ رویکردی جامع تر در قبال جرائم سایبری و به‌روزرسانی کنوانسیون بوداپست ازنظر ارزیابیِ تأثیر برای امریه مربوط به حملات علیه سیستم‌های اطلاعاتی (۲۰۱۰) گزینه های مدنظر اتحادیه اروپا محسوب می‌شدند، اما در عمل ممکن نبودند. در عوض اتحادیه اروپا راهبردی را تعریف کرد که ابتدا در طرح پیشنهادی برای امنیت اینترنت (۲۰۱۱) مطرح شد و سپس به‌صورت دقیق تر در راهبرد امنیت سایبری اتحادیه اروپا (۲۰۱۳) با پنج اولویت مشخص مطرح گردید که یکی

از آن‌ها «کاهش شدید جرائم سایبری» است. در این اولویت، به بُعد حقوقی (ملی، منطقه‌ای و جهانی) و لایه عملیاتی و هماهنگی در بین و میان تمام سطوح مربوط به حوزه جرائم سایبری توجه می شود.

این عناصر متفاوت، در اصل به‌طور مستقیم بیانگر پیش‌شرط‌های لازم –در لایه‌های عملیاتی و حقوقی– برای تأمین امنیت تاب‌آور کارآمد (ن.ک. کادر ۵-۱) و به‌خصوص معیار ایجاد فرهنگ امنیت سایبری در بین و درون ابعاد مختلف اکوسیستم امنیت سایبری در حال ظهور است. در ادامه مطالب این بخش، تحلیلی از پیشرفت عملی صورت گرفته در ارتباط با اهداف مشخص در راهبرد امنیت سایبری[۲۳] ارائه می شود و موانع احتمالی بر سر راه پیشرفت در جهت امنیت تاب‌آور کارآمد و فرصت‌های کسب موفقیت در زمینه سیستم در حال ظهور اتحادیه اروپا مطرح می شوند.

کادر ۵-۱. دانش، مهارت و توانمندی امنیت سایبری

ابعاد	بازیگران/نهادهای اصلی
حقوقی	همچنین اداره کل مهاجرت و امور داخلی کمیسیون اروپا / اداره کل عدالت، مصرف‌کنندگان و برابری جنسیتی دولت‌های ملی شورای اروپا (کنوانسیون بوداپست)
عملیاتی (و فنی)	یوروپل / مرکز مقابله با جرائم سایبری اتحادیه اروپا
	واحدها و نهادهای بین‌الملل/ملی مقابله با جرائم سایبری یوروجاست دانشکده پلیس اتحادیه اروپا
هماهنگی و اشتراک اطلاعات	مرکز مقابله با جرائم سایبری یوروپل / آژانس امنیت شبکه و اطلاعات اتحادیه اروپا / یوروجاست / دانشکده پلیس اتحادیه اروپا / واحدها و نهادهای بین‌الملل/ملی مقابله با جرائم سایبری شبکه‌ها/ابتکارهای فراملی بخش/صنعت خصوص

بُعد حقوقی

در بعد حقوقی، ابتدا بر روند امضاء، تصویب و اجرای کنوانسیون بوداپست به‌منظور تضمین وجود برنامه قانونی مشترکی با هدف مقابله با جرائم سایبری تأکید می شود (ن.ک. فصل ۳). پیش نویس کنوانسیون بوداپست دقیقاً به این دلیل مطرح شد که مشکلاتی در نظارت و حکمرانی بر جرائم سایبری، به‌خصوص در زمینه مسائل مربوط به تعریف جرائم سایبری، تعریف استانداردهای مشترک برای رسیدگی به جرائم سایبری و جلوگیری از وقوع آن‌ها و طرح چارچوب همکاری، گردآوری مدارک و انجام تحقیقات در نهادهای مجری قانون ذی ربط وجود داشت.[۲۴] گرچه به‌رغم پیشرفت اتحادیه اروپا در داخل به‌واسطه کمیسیون اروپا و در خارج توسط سرویس اقدام خارجی اتحادیه اروپا برای پیشبرد این کنوانسیون به‌عنوان ابزار اصلی گزینش و درواقع به‌عنوان الگوی مقابله با جرائم سایبری در سطح ملی کشورهای عضو اتحادیه اروپا، تنها ۲۴ کشور از بین اعضای اتحادیه اروپا آن را تصویب کردند.[۲۵] دلایل متفاوتی در مورد این مقوله: از انگیزه سیاسی و مخالفت مبتنی بر آزادی بیان آنلاین، اصول مدیریت و حفاظت از داده‌ها تا نبود ظرفیت نهادی و انسانی (مهارت‌ها) در سطح ملی، مباحث مربوط به پویایی این کنوانسیون و اختلافات مربوط به تفسیر حقوقی و فرهنگی که منجر به اجرای نامتقارن این کنوانسیون شده است، مانند مورد قانون مربوط به اشتراک و حفظ اطلاعات (Yannakogeorgos and Lowther 2013, p.253) مطرح شده است. برای مثال، برخی کشورها مانند ایرلند کنوانسیون را در سال ۲۰۱۲ امضاء کردند، ولی نتوانستند قانونی را برای تصویب آن ارائه کنند. ازاین‌رو، به نظر می‌رسد که برخی کشورها در داخل و خارج از اروپا این کنوانسیون را «به‌صورت تشریفاتی» امضاء کرده‌اند، اما «به‌صورت کامل آن را نپذیرفته‌اند» (Hilley 2005, p.171)؛ درواقع، تفاسیر متفاوت از جرائم سایبری حتی در عمل باعث اجرای قوانین حقوقی هماهنگ یا همگرایی فرهنگی در زمینه نحوه برخورد با جرائم سایبری نشده است.

صرف نظر از دلایل مطرح شده، این واقعیت که تمام کشورهای عضو اتحادیه اروپا کنوانسیون را تصویب نکرده و اجرا نمی‌کنند (این کنوانسیون اجباری نیست) موجب تضعیف اقدامات مربوط به تأمین امنیت تاب‌آور کارآمد شده است که بر اساس اعتمادسازی، اشتراک اطلاعات و اخبار و

همکاری و مشارکت بین بازیگران خصوصی و دولتی دخیل در گردآوری مدارک و پیگرد مجرمان آنلاین انجام می‌شوند. به‌علاوه، این مسئله مانع از دستیابی به همگرایی در ارائه تعریف و آگاهی مشترک از جرائم سایبری و رویه‌های لازم برای تضمین اجرای کارآمد قانون برون‌مرزی جهت جلوگیری از ایجاد پناهگاهی امن برای مجرمان سایبری می‌شود. از این گذشته، اگر چارچوب حقوقی و رویه‌ای هماهنگ یا مشترک مناسبی وجود نداشته باشد، این امر در عمل مانع از ایجاد هماهنگی سیاست گذاری و انجام تحقیقات در سطح جهان می شود. در صورت عدم وجود توافق متعارفی درباره ماهیت داده‌های به اشتراک گذاشته‌شده در مورد مجرمان سایبری، نحوه جمع‌آوری و استفاده از مدارک و [آگاهی از] ماهیت جرائم سایبری در کشورهای مختلف اتحادیه اروپا در سطح پایه، موانع بسیار جدیدی بر سر راه بازیگران ذی ربط برای برقراری امنیت تاب‌آور به وجود می آید. این مسئله بدین معنا نیست که در صورت تصویب و اجرای این کنوانسیون توسط تمام کشورهای عضو اتحادیه اروپا، تمام مشکلات حل می‌شد –جرائم سایبری معضلی جهانی است و این کنوانسیون به دلیل محدودیت‌های بسیار مقررات آن و به‌جای آنکه اقدامی واقعی در جهت رسیدگی به مسائل حقوقی ایجادشده به‌واسطه جرائم و مجرمان سایبری بین‌المللی باشد، بیانگر «قانونی نمادین» است، موردانتقاد بسیاری قرار گرفته است (Marion 2010, p.699). برای مثال، این کنوانسیون قوانینی در زمینه ذخیره سازی امن اطلاعات به‌دست‌آمده ندارد، اما تحقیقات صورت می‌گیرند، بدین معنا که اطلاعات ازنظر قانونی ذخیره‌شده توسط تیم واکنش اضطراری رایانه‌ای اتحادیه اروپا در یکی از کشورهای عضو احتمالاً مطابق الزامات حقوقی کشور عضو دیگر نیست. این موضوع نیز پیامدهایی برای این مسئله دارد که چه نوع اطلاعاتی را می‌توان در تحقیقات مربوط به جرائم سایبری و مجازات مجرمان سایبری به‌عنوان مدرک تلقی کرد (ENISA, A Flair for Sharing 2011, p.39).

صرف نظر از محدودیت‌های این کنوانسیون و همان‌طور که مقام ارشد اداره کل مهاجرت و امور داخلی کمیسیون اروپا در شرایط اتخاذ راهبرد اتحادیه اروپا برای ارتقای آن فراتر از مرزهای اروپا متوجه این امر شده است «اگر تمام کشورهای عضو این کنوانسیون را تصویب نکنند، کنار گذاشتن آن دشوار خواهد بود...» (Interview, DG Home, March 2013).

ازاین‌رو، تصویب و اجرای آن در داخل اتحادیه اروپا حداقل تضمین می کند که برنامه‌ای برای ایجاد فرهنگ امنیت سایبری بر اساس چارچوبی مشترک که الزاماً هماهنگ نیست و رویکردی منسجم، یعنی پیش‌نیازهای لازم برای ایجاد اکوسیستمی وجود دارد که امنیت تاب‌آور را در بین و داخل لایه‌ها و سطوح مختلف نهادینه می سازد. علاوه بر این، این موضوع اعتبار اتحادیه اروپا، در طرح مباحث خود را بیشتر می‌کند تا بتواند کشورهای خارج از اتحادیه را مجاب به امضاء و تصویب این کنوانسیون نماید. البته همان‌طور که ذکر شد، این بدین معنا نیست که کنوانسیون ابزاری کامل در چنین اکوسیستمی محسوب می شود، بلکه منظور این است که مسلماً از سازگاری و انعطاف بیشتری از مطالب عنوان شده توسط منتقدین برخوردار است و بیانگر انجام اقدامی مناسب در ابعاد مختلف مقابله با جرائم سایبری است. ازاین‌رو، بااینکه تصویب و اجرای کنوانسیون بوداپست مسلماً از منظر امنیت تاب‌آور –در داخل اتحادیه اروپا و در سطح جهان– مشکل ساز است، اما حداقل برنامه پایه‌ای را برای ایجاد شرایط ضروری فراهم می‌کند تا بتواند عملکرد کارآمدتری به‌خصوص در زمینه همکاری داشته باشد، چه‌بسا این همکاری بین بازیگران خصوصی-عمومی، تصمیم‌گیرندگان سیاسی، سازمان‌های بین‌المللی یا کارشناسان فنی و حقوقی باشد.

امریه مربوط به مقابله با سوءاستفاده و بهره‌برداری جنسی از کودکان (European Parliament and the Council 2011/93/EU) و امریه مربوط به حملات علیه سیستم‌های اطلاعاتی (European Parliament and the Council 2013/40/EU)، سایر موارد اصلی حقوقی قلمداد می شوند که درواقع از داخل اتحادیه اروپا نشئت می‌گیرند. امریه نخست در بخش بالا، کاملاً موردبحث قرار گرفت. در زمان نگارش این مطالب، کمیسیون اروپا در حال ارزیابی مسئله انتقال آن به کشورهای عضو اتحادیه اروپا و پیروی این کشورها از آن است. امریه دوم تا ۴ سپتامبر ۲۰۱۵ اجرایی نخواهد شد. بعد از تعیین جرائم سایبری به‌عنوان موضوع دور هفتم ارزیابی متقابل، هر دو امریه مورد ارزیابی دبیرخانه کل شورای اتحادیه اروپا قرار خواهند گرفت. این دور به بررسی اجرای عملی سیاست‌های اتحادیه اروپا در زمینه جرائم سایبری در سه حوزه خاص حملات سایبری، سوءاستفاده جنسی از کودکان یا پورنوگرافی کودکان به‌صورت

آنلاین و تقلب آنلاین در کارت برای تبیین ابعاد حقوقی و عملیاتی و مسائل مربوط به همکاری و هماهنگی برون‌مرزی در بین و میان نهادهای ملی، بین‌المللی و نهادهای ذی‌ربط اتحادیه اروپا می پردازد (Council of the EU, REV1, Limite, GENVAL 3, CYBER3).

ابعاد همکاری، تشریک‌مساعی و عملیاتی

راهبرد امنیت سایبری اتحادیه اروپا بر مسئله همکاری و تشریک‌مساعی به‌خصوص ازنظر گرد هم آوردن طرف های ذینفع مختلف ازجمله مقامات قضایی، نهادهای مجری قانون، تیم های واکنش اضطراری رایانه‌ای اتحادیه اروپا و طرف های ذینفع دولتی و خصوصی تأکید دارد که باید در راه مقابله با جرائم سایبری با یکدیگر همکاری نمایند. در این میان، عملکرد مرکز مقابله با جرائم سایبری اتحادیه اروپا به‌عنوان نقطه کانونی تسهیل انسجام عملیاتی کارآمدتر و نقش دانشکده پلیس اتحادیه اروپا[1] و یوروجاست در ارائه آموزش و اطلاعات لازم با هدف ایجاد فرصت رسیدگی کارآمد به جرائم سایبری برای طرف های ذینفع را نیز باید در نظر گرفت. مسئله همکاری و تشریک‌مساعی بازیگران مربوطه نیز تحت تأثیر دستورکار دیجیتال اروپا، ابلاغیه حفاظت از زیرساخت‌های اطلاعاتی حیاتی[2] (European Commission 2009) و گزارش پیشرفت در حفاظت از زیرساخت‌های اطلاعاتی حیاتی قرار دارد (European Commission 2011) که مورد نخست به این مسئله می پردازد که همکاری بین تیم های واکنش اضطراری رایانه‌ای اتحادیه اروپا و نهادهای مجری قانون (ENISA, 2012b, p.7) و راهبرد امنیت داخلی اتحادیه اروپا ضرورت داشت(2010, p.2)[۴۶].

این ویژگی، شامل بعد تأثیرگذار بین المللی است که چند بخش دارد. بخش نخست، همکاری با آیکان برای اجرای استانداردهای حداقلی (اتحادیه اروپا) جهت تضمین شناسایی مالکان تارنماهای ثبت‌شده توسط اداره ثبت اسامی بر اساس قوانین حفاظت از داده های اتحادیه اروپا است. سطح بالای استانداردهای حفاظت از داده ها حائز اهمیت است، «چراکه پیروی کامل از اصول حفاظت از داده ها مسئله مهمی در مبارزه کارآمد علیه جرائم سایبری محسوب می شود» و

1. European Police College (CEPOL)
2. Communication on Critical Information Infrastructure Protection

این مسئله مهم است که این امر مبنای طرح اکوسیستم ضروری برای ایجاد فرهنگ اشتراک بین کشورهای عضو و انتقال اخبار مربوطه به مرکز مقابله با جرائم سایبری به‌حساب می‌آید (Drewer and Ellerman 2012, p.2-3). بخش دوم، مربوط به طرح‌های انجام‌شده با همکاری شرکای بین‌المللی است؛ نمونه مناسب این مورد اتحاد جهانی علیه سوءاستفاده جنسی آنلاین از کودکان است که در سال ۲۰۱۲ و با مشارکت ۴۸ کشور کار خود را آغاز کرد (۵۴ عضو در زمان نگارش این مطلب – ن.ک. فصل ۷) (EU-US Joint Statement 7-8 June 2012).

یکی از مهم‌ترین جنبه‌های همکاری و تشریک‌مساعی برون‌مرزی، اشتراک لحظه‌ای داده‌ها است (ENISA, A Flair for Sharing 2011)، ولی این موضوع زمانی انجام می‌شود که اکوسیستمی طراحی شود که بتواند موانع قانونی (نظارتی)، فنی و عملیاتی را رفع کند و امکان رشد اعتماد بین طرف‌های ذینفع مختلف –بین بازیگران خصوصی و دولتی یا میان آن دسته که نگران برقراری موازنه مناسب بین حفظ حقوق و تأمین امنیت در زمان تبادل اطلاعات هستند– را فراهم نماید. با توجه به پیچیدگی و تنوع موجود در عرف‌های کاری (فرهنگ)، هنجارها و درواقع، مقررات قانونی در خصوص اشتراک داده‌ها و تشریک‌مساعی، دستیابی به سطحی از هماهنگی حائز اهمیت است که امکان رشد سیاست-گذاری کارآمد و مؤثری را در حوزه جرائم سایبری ایجاد می‌کند.

ازاین‌رو، تحقیقات صورت‌گرفته تاکنون به چندین مسئله و چالش مشکل‌ساز و راه‌حل‌های احتمالی بهبود همکاری و تشریک‌مساعی بین طرف‌های ذینفع اشاره می‌کنند، یعنی ایجاد مشارکت مبتنی بر اعتماد که امکان اشتراک اطلاعات و سیستم‌ها و فرآیندهای هماهنگ در سطح عملیاتی را فراهم می‌کند که پیش‌نیاز اصلی تأمین امنیت تاب‌آور است. آژانس امنیت شبکه و اطلاعات اتحادیه اروپا از این نظر در خط مقدم مطالعات صورت‌گرفته در مورد وضعیت عرف‌های کاری میان تیم‌های واکنش اضطراری رایانه‌ای اتحادیه اروپا و بین این گروه‌ها و نهادهای مجری قانون و نحوه تکامل این شیوه‌ها در طی پنج سال گذشته بوده است (ENISA 2012a, 2012b). یافته‌های اصلی مطالعات این سازمان اشاره به مسائل اصلی متعددی دارد که جهت تضمین همکاری و تشریک‌مساعی کارآمدتر باید به آن‌ها رسیدگی کرد. نخستین

مسئله که مربوط به حکمرانی و سطح عملیاتی است، مسئله اعتماد و عرف‌های کاری است. این موضوع برای همکاری بین تیم‌های واکنش اضطراری رایانه‌ای اتحادیه اروپا[۲۷] و میان تیم‌های واکنش اضطراری رایانه‌ای اتحادیه اروپا و نهادهای مجری قانون حائز اهمیت است.

در مورد همکاری بین تیم‌های واکنش اضطراری رایانه‌ای اتحادیه اروپا، این نتیجه به دست آمد که «در اصل، همکاری و تشریک‌مساعی به شیوه‌ای عملی و غیررسمی بین عاملانی صورت می‌گیرد که دارای رابطه‌ای مبتنی بر اعتماد به‌جای توافق حقوقی کاملاً رسمی [بین خود] هستند» (ENISA, A Flair for Sharing 2011, p.28). ازاین‌رو، تنش اصلی ایجادشده به دلیل همکاری برون‌مرزی تیم واکنش اضطراری رایانه‌ای اتحادیه اروپا نتیجه انجام تعهدات قانونی بدون تضعیف عملکرد مجاری کارآمد غیررسمی همکاری بین اعضای این گروه در سرتاسر اروپا است. این مسئله نیز مطرح شده است که چنین روابط غیررسمی مبتنی بر اعتماد بر اساس عوامل متعددی ایجاد می‌شوند که برای درک سایر مشارکت‌های عمومی–خصوصی نیز اهمیت دارند. این عوامل عبارت‌اند از: الف) اعتبار، به‌ویژه ازنظر فنی (یعنی آیا طرف دیگر از دانش کافی برخوردار است و از موضوع موردبحث اطلاع دارد)؛ ب) تعداد برخوردها، به‌خصوص ایجاد تعامل از طریق جلسات شخصی که باعث برقراری روابط «مبتنی بر اعتماد» می‌شود و ج) شناسایی و اشتراک نیات مشترک در زمان همکاری متخصصان امنیت سایبری در زمینه اهداف مشترک بسیار مهم است (Ibid., p.28).

در خصوص همکاری بین تیم واکنش اضطراری رایانه‌ای اتحادیه اروپا و نهادهای مجری قانون، گزارش شده است که وجود سازوکارهای غیررسمی در ایجاد مشارکت کارآمد و مبتنی بر اعتماد و رسیدگی به مسائل یا مشکلات خاصی نظیر بات‌نت‌ها نیز در تحکیم همکاری مؤثر است (ENISA, 2012b, p.20). بدین منظور، آژانس امنیت شبکه و اطلاعات اتحادیه اروپا نقش مهمی در دو حوزه گردهم‌آیی تیم واکنش اضطراری رایانه‌ای اتحادیه اروپا و نهادهای مجری قانون جهت ایجاد همکاری و ارائه آموزش و بهترین راهنمایی در خصوص ابعاد مختلف جرائم سایبری –مربوط به مسائل فنی و سیاست‌گذاری– بر عهده داشت.

(برای مثال، ن.ک. 8th ENISA workshop 'CERTs in Europe' 2013; ENISA, A Good Practice Guide for CERTs Directive on attacks against information systems 2013; ENISA Baseline Capability Policy Recommendation Report for national/government CERTs 2011; ENISA Work Programme 2012; Improving Information Security through Collaboration 2012).

اعتماد به شیوه های مختلف دیگری نیز ایجاد شده است که ازجمله نمونه‌های مناسب این مورد می توان به انتقال موقت کارکنان نهادهای مجری قانون به تیم های واکنش اضطراری رایانه‌ای اتحادیه اروپا اشاره کرد (برای مثال، این مورد در مرکز اطلاعات امنیت کاتالونیا[1] و گروه ملی واکنش اضطراری رایانه‌ای کشور رومانی روی داد). اگرچه، در زمان مقابله با جرائم سایبری، اعتماد تنها در صورتی شکل می گیرد و به نحو کارآمدی به کار می رود که مقررات مناسب و محیط حقوقی (حکمرانی)، به‌خصوص مقررات مربوط به تبادل اطلاعات و داده‌ها وجود داشته باشند.

اهمیت چنین گردهمایی‌های غیررسمی و اغلب تک کاربردی طرف‌های ذینفع دارای شبکه مربوطه با هدف رسیدگی به مسئله جرائم سایبری –خصوصی یا عمومی– در روابط مبتنی بر اعتماد را نمی توان از منظر دیدگاه امنیت تاب‌آور حکمرانی و اقدامات صورت گرفته جهت رسیدگی به مسئله بات‌نت‌هایی نظیر کرم کانفیکر[2]، بات‌نت بردولاب[3] و بات‌نت ماریپوسا[4] نادیده گرفت (ENISA 2012b, p.22–25). گرچه، تجربیات فراگرفته شده از مورد کرم کانفیکر بیانگر ضرورت وجود نوعی چارچوب همکاری پایدار و مقیاس پذیر با ترکیبی از مجاری رسمی و در صورت بروز رویداد های پیچیده تری که زمان واکنش به آن‌ها طولانی‌تر است بتوان شفافیت، انسجام و دقت در تبادل اطلاعات را حفظ کرد (Ibid., p.26).

دومین مسئله مربوط به شفافیت نقش، عملکرد، تعاریف، رویه‌ها و توانمندی‌های بازیگران دخیل ازجمله آموزش نحوه درک و رسیدگی کارآمد به ابعاد رویه‌ای، حقوقی و فرهنگی تحقیقات در مورد جرائم سایبری است. به دلیل وجود انواع مختلف بی‌شمار –عمومی و خصوصی،

1. Centre de Seguretat de la Informació de Catalunya (CESICAT)
2. Conficker
3. Bredolab
4. Mariposa

این مورد برای تیم های واکنش اضطراری رایانه‌ای اتحادیه اروپا از اهمیت بسیاری برخوردار است و این گروه ها در کشورهای مختلف باید با چارچوب ها و زمینه های حقوقی متفاوتی برخورد کنند تا نوع اطلاعات به اشتراک گذاشته‌شده با غیررسمی ارتباطات جهت واکنش به رویدادهای جهانی است تا در صورت بروز رویداد های پیچیده تری که زمان واکنش به آن‌ها طولانی تر است بتوان شفافیت، انسجام و دقت در تبادل اطلاعات را حفظ کرد (Ibid., p.26).

دومین مسئله مربوط به شفافیت نقش، عملکرد، تعاریف، رویه ها و توانمندی های بازیگران دخیل ازجمله آموزش نحوه درک و رسیدگی کارآمد به ابعاد رویه‌ای، حقوقی و فرهنگی تحقیقات در مورد جرائم سایبری است. به دلیل وجود انواع مختلف بی شمار – عمومی و خصوصی–، این مورد برای تیم های واکنش اضطراری رایانه‌ای اتحادیه اروپا از اهمیت بسیاری برخوردار است و این گروه‌ها در کشورهای مختلف باید با چارچوب‌ها و زمینه های حقوقی متفاوتی برخورد کنند تا نوع اطلاعات به اشتراک گذاشته‌شده با سایر طرف‌های ذینفع در مقابله با جرائم سایبری تعیین گردد. در حوزه همکاری تیم واکنش اضطراری رایانه‌ای اتحادیه اروپا و نهادهای مجری قانون این مسئله مشخص شد که اختلافات «فرهنگی» مشکلات قابل ملاحظه‌ای را در برابر همکاری بین دو جامعه به دلیل توجه و نقش خود ایجاد می کنند (ن.ک. کادر ۵-۲). با انجام تحقیقات بیشتر و در تحقیق آژانس امنیت شبکه و اطلاعات اتحادیه اروپا، این موضوع در راستای مطالعه پیشین (A Flair for Sharing 2011) روشن شد که مشکلات حقوقی اصلی مربوط به اختلاف‌نظر در مورد آگاهی از مقررات ملی مربوطه در مقایسه با چارچوب حقوق بین‌المللی نظیر کنوانسیون بوداپست یا امریه‌ها و مقررات اتحادیه اروپا است. به بیان دقیق‌تر، آگاهی از مقررات ملی نسبت به حقوق بین‌الملل، به‌خصوص به دلیل اختلاف دانش در مورد حقوق بین‌الملل در زمینه حریم خصوصی و حفاظت از داده‌ها بسیار بیشتر بود. درواقع، این موضوع دومین دلیل مهم ارائه‌شده برای عدم ارائه اطلاعات، مبنای قوانین مربوط به امنیت ملی، محسوب می‌شد که به‌ویژه گروه‌های ملی/بین المللی واکنش اضطراری رایانه‌ای اتحادیه اروپا اطلاعات بسیاری در مورد آن داشتند.

کادر ۵-۲. دانش، مهارت و توانمندی امنیت سایبری

	تیم‌های واکنش اضطراری رایانه‌ای اتحادیه اروپا	نهادهای مجری قانون
تمرکز بر معانی متفاوت جرائم/حملات سایبری	حوادث غیرمترقبه؛ تهاجم به محرمانگی، دسترس‌پذیری و یکپارچگی فناوری اطلاعات	جایی که شواهد یا سوءظن نسبت به وقوع جرم که شامل جعل یا جرائمی که محرمانگی، دسترس‌پذیری و یکپارچگی فناوری اطلاعات تحت تاثیر قرار نگیرد
فرهنگ شخصیتی/کاری هریک از جوامع	مبتنی بر حل مسئله غیررسمی	رویه‌ای، قانون‌محور
اهداف هریک از جوامع	اصلاح	پیگرد قانونی
مسیر درخواست	درونی (احتمال بیشتر در پاسخ به درخواست‌ها	بیرونی (احتمال بیشتر در انتقال درخواست‌ها)

Source: UKCSS: ENISA (2012b, p.2)

این خلأ دانش بین قوانین حقوقی ملی و بین المللی، تردید بسیاری پیرامون اشتراک و تبادل اطلاعات ایجاد می کند، گرچه راه حل های احتمالی، شامل تدوین بیشتر آن‌ها در قالب اجباری کردن اشتراک اطلاعات نمی شود، اما شامل طراحی «چارچوب هایی برای همکاری است که سطح تحمل خطای بالایی دارند که در آن‌ها خطاهای کوچک لزوماً منجر به پیامدهای (حقوقی) قابل‌ملاحظه‌ای نمی‌گردد. ازاین‌رو، فرصت‌های بیشتری برای یادگیری فراهم می‌شود» (ENISA 2012b, p.51). سایر مشکلات شناسایی‌شده مربوط به دامنه و حوزه تیم‌های واکنش اضطراری رایانه‌ای اتحادیه اروپا و تعاریف ارائه‌شده از جرائم سایبری –در حوزه سوءاستفاده از رایانه و شبکه– است (ENISA 2012, p.2-3). درواقع، مشکل دیگر پیش روی تیم‌های واکنش اضطراری رایانه‌ای اتحادیه اروپا –جدا از موانع حقوقی و نظارتی بر سر راه همکاری کارآمد آن‌ها با نهادهای مجری قانون– تعداد کل طرف‌های ذینفعی است[۲۸] که انتظار می‌رود با آن‌ها تعامل برقرار کنند؛ تمام آن‌ها سطح انتظار متفاوتی در مورد نوع اطلاعاتی

دارند که تیم‌های واکنش اضطراری رایانه‌ای اتحادیه اروپا (ملی/عمومی یا خصوصی) می‌توانند در هر لحظه ارائه دهند.

در خصوص بُعد عملیاتی، تعدادی از عواملی شناسایی شدند که بر سر راه تبادل اطلاعات و همکاری بین نهادهای مجری قانون و تیم‌های واکنش اضطراری رایانه‌ای اتحادیه اروپا مانع ایجاد می‌کنند. نخستین مانع ازنظر فرایند (رد درخواست)، مربوط به ارائه جزئیات ناکافی/ نامناسب مسائل پیرامون صلاحیت امنیتی و مجرا/مخاطب نادرست است. همین دلایل با تردید بیشتر (و حذف صلاحیت امنیتی) در مورد رد درخواست نیز بیان شده‌اند. علاوه بر این مسئله، در وهله نخست مسائل مربوط به نقش و پارامترهای همکاری و پس از آن «نگرانی درباره ظهور دیوان‌سالاری از رویه‌ها و سیاست‌گذاری‌های مختلف/ناشناخته، فقدان استانداردهای مشترک و عدم شفافیت عملکرد طرف دیگر در مورد به‌کارگیری اطلاعات دریافتی»، جزو مسائل حکمرانی تلقی می‌شدند (Ibid). نتیجه مهم به‌دست‌آمده از این تحقیق این است که اهمیت این عوامل در چرخه حیات نهاد (برای مثال، تیم‌های واکنش اضطراری رایانه‌ای اتحادیه اروپا) متفاوت بود –احتمال دارد منابع و درک چارچوب‌های حقوقی در آن در مرحله ابتدایی نسبت به زمان توسعه کامل‌تر و کسب تجربه بیشتر در امر هدایت تبادل اطلاعات برون‌مرزی و چارچوب‌های حقوقی مربوطه برای رویدادها و تحقیقات مربوط به جرائم سایبری، کمتر تثبیت شوند (Ibid).

به‌ویژه قوانین مربوط به حفاظت از داده‌ها و حریم خصوصی، مشکلاتی را در لایه‌های حقوقی و نظارتی برای تبادل اطلاعات و داده‌ها ایجاد می‌کنند. این قوانین در مورد نحوه و زمان به‌کارگیری داده‌های شخصی در داخل و خارج از اتحادیه اروپا در زمان ارتباط با فعالیت‌های مجرمانه آنلاین، بسیار غیرمنعطف هستند. برای مثال، تیم‌های واکنش اضطراری رایانه‌ای اتحادیه اروپا به رسیدگی و پردازش داده‌های شخصی احتمالی نظیر آدرس‌های آی‌پی یا ورود و خروج کاربران و در برخی مواقع ضروری، در صورت نیاز، به نظارت بر داده‌های بسته (محتوای ترافیک) رویداد خاصی می‌پردازند. برای انجام این کار، تیم‌های واکنش اضطراری رایانه‌ای اتحادیه اروپا باید برای «اجتناب از پنهان‌سازی احتمالی هرگونه مدرک به نادرستی جمع‌آوری‌شده که بنا است در دادگاه ارائه شود و همچنین اجتناب از هرگونه مسئولیت کیفری و مدنی»، اطمینان یابند که

از مقررات حقوقی مربوطه در سطح ملی و اروپایی/بین‌المللی پیروی می‌کنند[۲۹] (ENISA, Flair for Sharing 2011, p.31). مسلماً با توجه به مسئله تبادل اطلاعات با طرف‌های ذینفع گوناگون در روند تحقیقات و پیگرد قانونی، این فرایند اشتراک، پیچیده‌تر می‌شود. این فرآیند مستلزم برخورداری از دانش تخصصی در مورد اصول حقوقی است که تیم‌های واکنش اضطراری رایانه‌ای اتحادیه اروپا که تخصص آن‌ها بیشتر در حوزه فنی است و به دنبال حل مسائل هستند، از آن بی‌بهره‌اند. ایجاد نوعی چارچوب برای انطباق داده‌ها و تبادل اطلاعات، مبنای حقوقی مشخص‌تری را برای اشتراک کارآمد اطلاعات از طریق چرخه حیات هرگونه تحقیق فراهم می‌کند.

مسلماً مشکلات عملیاتی و نظارتی (حقوقی) بی‌شماری در زمینه همکاری و تشریک‌مساعی بین مؤسسات مربوطه درون و بین کشورهای اروپایی و نیز در سطح جهان وجود دارند.[۳۰] این مشکلات باعث طرح پرسش‌های مهمی در مورد ایجاد اکوسیستمی کارآمد می‌شوند که در آن امنیت تاب‌آور با هدف مقابله با جرائم سایبری برقرار می‌شود. این مشکلات به‌ضرورت انجام اقدام بیشتر در کوتاه‌مدت، میان‌مدت و بلندمدت برای دستیابی به این امر در رابطه با تغییر عرف‌های حقوقی و رویه‌ای، ابزارهای عملیاتی و ظرفیت، آموزش، فرهنگ‌های کاری و سازوکارهای حکمرانی نیز اشاره دارند. در بلندمدت، ایجاد محیط کاری منسجم‌تر با بهره‌گیری از تخصص‌های موردنیاز –حقوقی، فنی و عملیاتی– مسلماً باعث ایجاد شفافیت رویه‌ای و روابط مبتنی بر اعتماد از طریق برقراری تعاملات منظم‌تر بین طرف‌های ذینفع اصلی در مقابله با جرائم سایبری می‌شود.[۳۱] به گفته یکی از مقامات ارشد کمیسیون اروپا، طرف‌های ذینفع «باید ارزش‌افزوده اشتراک اطلاعات را درک کنند ... و باید این اشتراک را تا سطح عملیاتی پیش برده و محیط اعتماد مناسبی را ایجاد نماییم» (Interview, DG Home, March 2013).

برخی از این مسائل در راهبرد امنیت سایبری اتحادیه اروپا ذکر شده است. برای مثال، بر توانمندی کشورهای عضو و توسعه ابزارهای قانونی از طریق حمایت از مراکز تحقیقات مشترک کمیسیون اروپا[1] توجه می‌شود. به همین دلیل، ۱۰ مرکز عالی مقابله با جرائم سایبری توسط

1. European Commission's Joint Research Centres (JRCs)

اداره کل مهاجرت و امور داخلی با سرمایه پلیس صندوق امنیت داخلی[1] (مرکز پیشگیری و مقابله با جرم[2] سابق) در کشورهای یونان، فرانسه، استونی، جمهوری چک، بلغارستان، بلژیک، رومانی، بریتانیا، اسپانیا و هلند تأسیس شدند که وظیفه آن‌ها توسعه ابزارهای قانونی، طراحی برنامه‌های آموزشی در زمینه مقابله با جرائم سایبری و انجام تحقیقات عملی در مورد مسائل تأثیرگذار بر شهروندان اتحادیه اروپا (کلاه‌برداری آنلاین، کلاه‌برداری مخابراتی، امنیت سایبری زیرساخت‌های حیاتی ملی) است. علاوه بر این، بودجه‌ای نیز از طرف اتحادیه اروپا برای آکادمی حقوق اتحادیه اروپا[3] (۲۰۱۲-۲۰۱۵) با هدف طراحی برنامه‌های آموزشی در زمینه ابعاد حقوقی و فنی جرائم سایبری (آموزش ۵۰۰ قاضی و دادستان) در نظر گرفته شد. وظیفه سایر طرح‌ها نظیر گروه آموزش و تعلیم مقابله با جرائم سایبری اتحادیه اروپا[4]، ظرفیت‌سازی نهادهای مجری قانون اروپا برای مقابله با جرائم سایبری است. بسته‌های آموزشی کامل شدند و برای آموزش بیش از ۱۵۰۰ نفر از بازرسان جرائم سایبری در حوزه قوانین رایانه‌ای و جمع‌آوری مدارک به کار می‌روند. این اقدام با امضای موافقت‌نامه تجدیدنظرشده (۲۰۱۳) بین مرکز مقابله با جرائم سایبری اتحادیه اروپا، دانشکده پلیس اتحادیه اروپا و گروه آموزش و تعلیم مقابله با جرائم سایبری اتحادیه اروپا با هدف به‌روزرسانی برنامه‌های آموزشی صورت گرفت. علاوه بر این، مرکز مقابله با جرائم سایبری اتحادیه اروپا (مبحث بعدی) آموزش‌های جدی را برگزار کرده است، برای مثال ارائه آموزش کارشناسی در خصوص دستگاه‌های اسکیمر، تحقیق آنلاین در مورد سوءاستفاده جنسی از کودکان و همکاری با آکادمی حقوق اتحادیه اروپا و آژانس امنیت شبکه و اطلاعات اتحادیه اروپا جهت ارائه آموزش در زمینه ابعاد مختلف تحقیقات مربوط به جرائم سایبری. وجود این طرح‌های بی‌شمار باعث ایجاد مسائل همپوشان، کارکرد و درنهایت انسجام سیاست‌گذاری –حدود همکاری آن‌ها با سایر برنامه‌های کاری سازمان‌های اتحادیه اروپا، پذیرش و کفایت آموزش مربوطه (و چگونگی سازگاری آن با آموزش‌های داخلی/محلی) و تأثیرات واقعی آن در میان‌مدت تا بلندمدت بر طرف‌های ذینفع مربوطه در اتحادیه اروپا– شده است.[۳۲] بنا

1. ISF (Internal Security Fund) Police
2. Prevention of and Fight against Crime (ISEC)
3. European Academy of Law (ERA)
4. European Cybercrime Training and Education Group (ECTEG)

به اظهارات یکی از مقامات آژانس امنیت شبکه و اطلاعات اتحادیه اروپا، «روابط [بین نهادهای مختلف] کماکان روند تکوینی خود را طی می‌کند» (Interview, ENISA official, August 2014) و برای حداکثرسازی موارد همکاری و دوری از همپوشانی باید بیشتر توسعه یابد.

براساس چارچوب بالا، راهبرد امنیت سایبری اتحادیه اروپا بر اهمیت نقش عملیاتی یوروپل (مرکز مقابله با جرائم سایبری اتحادیه اروپا) در هماهنگ‌سازی تحقیقات ملی کشورهای عضو در حوزه جرائم سایبری، به‌خصوص در حوزه‌های مربوط به سوءاستفاده جنسی از کودکان، کلاه‌برداری در پرداخت، بات‌نت‌ها و مداخله تأکید دارد. به‌علاوه، مرکز مقابله با جرائم سایبری اتحادیه اروپا مسئول تضمین هماهنگی فعالیت‌های عملیاتی با سیاست‌گذاری مربوطه اتحادیه اروپا و ایجاد هماهنگی و همکاری با سایر مؤسسات اتحادیه اروپا نظیر یوروجاست و دانشکده پلیس اتحادیه اروپا برای تضمین رسیدگی کارآمد به حوزه‌های دارای اولویت شناسایی‌شده از طریق چرخه سیاست‌گذاری پلتفرم چندزمینه‌ای علیه تهدیدات جرائمی اتحادیه اروپا[1] است. این موارد شامل آموزش، ظرفیت‌سازی، توسعه، تحلیل راهبردی و پشتیبانی فنی است (ن.ک.EC3 First Year Report 2014). در اصل، این چرخه سیاست‌گذاری توسط شورای اتحادیه اروپا در سال ۲۰۱۰ با هدف بهینه‌سازی هماهنگی بین طرف‌های ذینفع مربوطه –کشورهای عضو، نهادها و مؤسسات اتحادیه اروپا و همچنین کشورها و سازمان‌های ثالث– برای مقابله با تهدیدات مجرمانه شناسایی‌شده در ارزیابی جرائم و تهدیدهای جدی و سازمان‌یافته یوروپل[2] ایجاد شد. در گزارش سال ۲۰۱۳، این ارزیابی (SOCTA Threat Assessment 2013) در کنار اهداف راهبردی و برنامه‌های اقدام عملیاتی، مواردی نظیر تقلب در کارت‌های پرداخت آنلاین، سوءاستفاده جنسی آنلاین و حملات سایبری علیه سیستم‌های اطلاعاتی و زیرساخت‌های حیاتی به‌عنوان مهم‌ترین تهدیدات و اهداف راهبردی شناسایی شدند و بازیگران و مؤسسات مربوطه اتحادیه اروپا نیز طرح‌های اقدام عملیاتی را جهت رسیدگی تا چهار سال آینده مشخص کردند.

مرکز مقابله با جرائم سایبری اتحادیه اروپا در نخستین سال کار خود با مشکلاتی مواجه شد، اما عملکرد گروه‌های کانونی مختلف[۳۳] آن در کمک به مؤسسات مجری قانون کشورهای عضو

1. European Multidisciplinary Platform Against Criminal Threats (EMPACT)
2. Europol Serious and Organised Crime and Threat Assessment (SOCTA)

برای ایجاد اختلال در شبکه‌های جرائم سایبری دستاوردهایی نیز برای این مرکز به ارمغان آورد. درواقع، درمجموع به نظر می‌رسد که ازنظر سایر مؤسسات اتحادیه اروپا «همکاری روزانه مناسبی بین آن‌ها برقرار است» (Senior Commission Official, DG Home, 2013). در خصوص دانشکده پلیس اتحادیه اروپا نیز:

> «هماهنگی برای ایجاد همکاری ساختاری صورت گرفت و توافقاتی در زمینه ترتیبات کاری واحد همکاری قضایی اتحادیه اروپا (یوروجاست) ازجمله مداخله افسر رابط آن‌ها به دست آمد و کنفرانس سالانه مشترکی با آژانس امنیت شبکه و اطلاعات اتحادیه اروپا برگزار شد که محور [مباحث] آن بهبود همکاری تیم‌های واکنش اضطراری رایانه‌ای اتحادیه اروپا و نهادهای مجری قانون بود» (EC3, First Year Report 2014, p.13).

رابطه بین آژانس امنیت شبکه و اطلاعات اتحادیه اروپا و مرکز مقابله با جرائم سایبری اتحادیه اروپا، محور یادگیری و همکاری متقابل در حوزه تبادل تخصص در ابعاد خرد و کلان جرائم و امنیت سایبری، در عین تضمین این موضوع محسوب می‌شود که هماهنگی و سازگاری بین اهداف سازمان‌ها وجود دارد (Telephone Interview, ENISA official, August 2014). بدین منظور رؤسای آژانس امنیت شبکه و اطلاعات اتحادیه اروپا و یوروپل، موافقت‌نامه همکاری راهبردی‌ای را در ژوئن ۲۰۱۴ جهت تسهیل همکاری نزدیک‌تر و تبادل تخصص در حوزه مقابله با جرائم سایبری امضا کردند (ENISA Press Release 2014). درنهایت، ساختارهای جدیدی نظیر کارگروه اقدام مشترک علیه جرائم اینترنتی[1] با حضور کشورهای اروپایی و غیراروپایی با هدف گسترش توانمندی همکاری عملیاتی در مقابله با جرائم سایبری در اروپا و سطح جهان ایجاد گردید. همان‌طور که در فصل چهار اشاره شد، این ترتیب نیمه‌رسمی ازنظر عملیاتی عملکرد موفقی داشت، اما درصورتی‌که بنا باشد چنین ترتیباتی عملکرد کارآمدی داشته باشند، به برخی مشکلات مهم نیز در آن‌ها اشاره می‌شود.

باوجوداینکه عملیات مرکز مقابله با جرائم سایبری اتحادیه اروپا جهت رفع باتنت زیرو

1. Joint Cybercrime Action Taskforce (J-CAT)

اکسس[1] یکی از نمونه‌های مناسب (ن.ک.EC3, First Year Report 2014, p.13) در مورد نحوه همکاری در عملیات موفق چند حوزه قضایی محسوب می‌شود، اما باعث بروز مشکلات خاصی در زمینه آغاز کار و هماهنگی مؤثر در حوزه جرائم سایبری به دلیل توانایی مرکز مقابله با جرائم سایبری اتحادیه اروپا در دست‌یابی به مدارک و اطلاعات مهم از صنایع خصوصی شده است. مسئله اصلی، عدم گزارش جرائم سایبری به نهادهای مجری قانون از ترس این است که از منظر کاری و تحت تأثیر منطق اقتصادی امکان دارد گزارش‌دهی موارد نقض قانون مهم موجب خدشه‌دار شدن برند تجاری گردد و بر سود حاصله تأثیر منفی به‌جای بگذارد. اگرچه نتیجه این کار، عدم دسترسی نیروهای پلیس و دادستانی به پایگاه مدارک جامع و تصویر روشنی از تحولات و روندهای صورت‌گرفته در حوزه جرائم سایبری است که پیامد آن عدم اشتراک لحظه‌ای تهدیدات به اشتراک گذاشته‌شده توسط سایرین در صنایع غیردولتی برای حفاظت از واحدهای تجاری است. یکی از موضوعات مربوط به گزارش اطلاعات از جانب شرکت‌های چندملیتی، به‌ویژه در مورد اطلاعات شخصی، مربوط به فرایند خودگزارش‌دهی است. اطلاعات دریافتی یوروپل باید از مسیر واحدهای مربوطه کشورهای عضو مسئول جرائم سایبری به دست آید، ولی احتمال دارد اطلاعات بسیاری از شرکت‌های چندملیتی مربوط به کشورهای محل حضور خود نباشد و درنتیجه گزارش‌های بی‌شماری ارائه شوند که درواقع به مرجع ملی ذی‌صلاح[2] آن کشور مربوط نیستند. این امر، باعث افزایش حجم کار حقوقی (مسئولیت‌پذیری و مالکیت داده‌ها) مقامات ملی ذی‌صلاح می‌شود که در عمل مانعی برای جریان مؤثر اطلاعات از صنایع خصوصی به یوروپل و درواقع به نهادهای مجری قانون در کشورهای عضو ایجاد می‌کند (EC3, First Year Report 2014, p.14).

این موضوع باعث طرح مسئله جالب حالت‌های حکمرانی و عرف مناسب و به‌ویژه مسئله نحوه ایجاد انگیزه در صنایع غیردولتی، برای ارائه اطلاعات و نحوه به‌کارگیری از رویه‌های مناسب گزارش‌دهی و ارائه اطلاعات مربوطه به یوروپل می‌شود. دستورالعمل پیشنهادی امنیت شبکه و اطلاعات باعث اجباری شدن گزارش برای بخش‌های مربوطه شده است، اما این موضوع باعث

1. ZeroAccess
2. National Competent Authority (NCA)

حل مشکل پیش روی شرکت‌های چندملیتی یا درواقع، رسیدگی کافی به مسئله محتوای دقیق گزارش –نوع اطلاعات و هدف از گزارش آن– نمی‌شود (Informal Discussion on NIS Directive, Brussels, February 2014; Telephone Interview, senior official EC3, September 2014). این مسئله که گزارش‌دهی اجباری در صنایع غیردولتی انگیزه مشارکت سازنده‌تر را ایجاد کند، نیز مشخص نیست. یوروپل و آژانس امنیت شبکه و اطلاعات اتحادیه اروپا در کنار سایر صنایع و مقامات دولتی خواستار مشارکت اصولی‌تر بخش خصوصی برای تأمین اولویت‌های مدنظر برای حوزه‌های امنیت سایبری و جرائم سایبری شده‌اند. نمونه مناسب این مورد را می‌توان در شیوه حکمرانی مناسب کشور بریتانیا ملاحظه نمود که در صورت نیاز، از متخصصان بخش خصوصی به‌صورت داوطلبانه می‌خواهند سوگند رازداری یاد کنند. سایر نمونه‌ها (گرچه ساختاری‌تر) شامل برگزاری جلسات سه‌ماهه بین واحد مقابله با جرائم سایبری کشور بلژیک و بانک‌های صادرکننده کارت بانکی این کشور یا مراکز اشتراک و تحلیل اطلاعات[1] برای بخش مالی کشورهای آمریکا و هلند است (House of Lords, EU committee, 13th Report of Session 2013–2014, p.15–17; Cybercrime @IPA, Special cybercrime units November 2011, p.38). درواقع، این مسئله مطرح شده است که چنین رویکرد نظری، باعث ایجاد انگیزه‌های مشخصی برای حضور صنایع در مقابله با جرائم سایبری و مشارکت مؤثرتر و منعطف‌تر آن‌ها در کنار فرآیندها و اعتماد لازم برای حمایت از آن‌ها می‌شود. علاوه بر این، چنین مشارکت‌های مؤثری امکان بهره‌گیری از تخصص‌های مربوط به سیستم‌ها، داده‌ها و دانش موجود در صنایع را فراهم می‌آورد که نهادهای مجری قانون، فاقد آن‌ها هستند، اما از ضرورت وجود آن‌ها آگاه‌اند (Interview, e-crime expert, July 2014).

یکی از پیش‌نیازهای اصلی تأمین امنیت تاب‌آور، وجود توانایی و آمادگی لازم برای پذیرش مفروضات عملیاتی جدید و سازوکارهای نهادی است. مرکز مقابله با جرائم سایبری اتحادیه اروپا با توجه به‌حکم یکی از پیش‌نیازهای اصلی تأمین امنیت تاب‌آور، وجود توانایی و آمادگی لازم برای پذیرش مفروضات عملیاتی جدید و سازوکارهای نهادی است. مرکز مقابله با جرائم سایبری

1. Information Sharing and Analysis Centres (ISAC)

اتحادیه اروپا با توجه به‌حکم خود، در نخستین سال فعالیت، این موضوع را به‌خوبی اجرا نمود، ولی بااین‌حال، نگرانی‌های جدی در مورد حدود پیشرفت کارآمد این مرکز با توجه به منابع محدود در اختیار آن وجود دارد (مورد مشابهی در زمان تفصیل حکم آژانس امنیت شبکه و اطلاعات اتحادیه اروپا مطرح می‌شود). راب وین‌رایت[1]، رئیس یوروپل، خواهان حمایت شفاف برنامه بعدی امور قضایی و داخلی اتحادیه اروپا از مرکز مقابله با جرائم سایبری اروپا است تا بتواند به نحو کارآمدتری به وظیفه خود عمل کند (House of Lords, EU committee, 13th Report of Session 2013–2014, p.15–17).

حتی پیش از آغاز کار آن، به دلیل وقوع بحران مالی تردید بسیاری در مورد وجود منابع بیشتر برای یوروپل (مرکز جرائم سایبری اروپا) جهت اجرای حکم خود وجود داشت این تصمیم اتخاذ شده بود که هیچ کارمند یا بودجه اضافه‌ای در سال نخست کار این مرکز در اختیار آن قرار نگیرد (۲۰۱۳). مرکز مقابله با جرائم سایبری اتحادیه اروپا تنها با جابه‌جایی وجوه از بودجه داخلی موجود، توانست به برخی اهداف اصلی خود دست یابد این اقدام به معنای ناتوانی آن در حوزه طراحی سازوکارها و ابزارهایی برای مقابله با جرائم سایبری بود که هدف اصلی تأسیس آن محسوب می‌شد. به‌رغم افزایش ۱/۷ میلیون یورویی بودجه یوروپل در سال ۲۰۱۴ و افزایش بیشتر بودجه حوزه منابع فناوری اطلاعات در سال ۲۰۱۵، این مشکل که آیا این منابع برای اجرای کارآمد مرکز مقابله با جرائم سایبری اتحادیه اروپا کافی است، کماکان باقی می‌ماند– به‌خصوص درصورتی‌که موفقیت بیشتر آن باعث تقاضای بیشتر طرف‌های ذینفع گردد. این دغدغه اصلی مطرح‌شده در ارزیابی عملکرد این مرکز در نخستین سال فعالیت این است:

> «به دلیل دستاوردهای تاکنون به‌دست‌آمده، منابع کنونی انسانی و مالی در حال تحدید پیشرفت تحقیقات است. با توجه به حجم تحقیقات مهم ارجاعی از تابستان ۲۰۱۳، مرکز مقابله با جرائم سایبری اتحادیه اروپا نمی‌تواند به تمام آن‌ها رسیدگی کند. تمام موارد افزایش منابع، کارایی، رویکردهای مبتکرانه برای همکاری و همچنین ظرفیت‌سازی در طیف وسیعی از شرکا را باید برای حداکثرسازی تأثیر بر حوزه جرائم سایبری و مجرمانی

1. Rob Wainwright

در نظر گرفت که از آن سود می‌برند» (EC3, First Year Report 2014, p.32).

ازاین‌رو، مسئله واقعی تضمین پایداری عملیات‌ها و سازوکارهای کنونی و دستیابی به پیشرفت ازنظر ایجاد روش‌ها، ابزارها و فرآیندهای کاری نوآورانه‌تری برای تثبیت اهمیت مرکز مقابله با جرائم سایبری اتحادیه اروپا و توانایی این مرکز در اجرای حکم خود و رسیدگی کارآمد به مشکلات آتی ایجادشده در حوزه جرائم سایبری است (Interview, Senior Official EC3, September 2014).

پیشنهاد جدید این کمیسیون در مورد طرح مقرراتی جهت افزایش نقش یوروپل و ایجاد آژانس مجری قوانین اتحادیه اروپا[1] (European Commission 2013) اقدامی در جهت رسیدگی به مشکلات موجود در حوزه تبادل اطلاعات و مسائل مربوط به منابع و هزینه‌ها (برای مثال، از طریق آموزش، ادغام دانشکده پلیس اتحادیه اروپا در یوروپل و غیره) و مسئله حقوقی و رویه‌ای به‌روزرسانی قوانین پیرامون یوروپل بر اساس معاهده لیسبون (۲۰۰۹) است. با توجه به اینکه این مسئله پیامدهایی برای منابع دارد و اساساً رابطه بین یوروپل و کشورهای عضو را تغییر می‌دهد و مشکلات خاصی را در عمل به وجود می‌آورد، درنتیجه، پیامدهای مهمی نیز برای اقدامات مرکز مقابله با جرائم سایبری اتحادیه اروپا خواهد داشت.

نخست، بدون هیچ استثنایی، حتی اگر این موضوع با امنیت ملی یا امنیت افراد و یکپارچگی تحقیقات در حال انجام داخلی مرتبط با جرائم سایبری در تضاد باشد، تغییر قابل ملاحظه‌ای از نظر حکمرانی ایجاد می‌شود و مقررات، تعهد بیشتری را در قبال ارائه داده‌ها به یوروپل مطرح می‌کنند. این موضوع احتمالاً مطلوب کشورهای عضوی نیست که نسبت به مشارکت اتحادیه اروپا در حوزه دارای حساسیت و منافع ملی تردید دارند. دوم، تغییر قابل‌ملاحظه‌ای ازنظر بعد حقوقی –فراحکمرانی عملی اتحادیه اروپا– صورت می‌گیرد. به‌رغم اینکه یوروپل می‌تواند از کشورهای عضو درخواست اجرای تحقیقاتی را داشته باشد، اما در مقررات جدید تعهداتی برای کشورهای عضو جهت توجیه و ارائه دلیل خود در صورت عدم انجام عملیات در نظر گرفته شده

1. European Union Agency for Law Enforcement

است که ارائه چنین دلایلی در دیوان دادگستری اتحادیه اروپا مشکل‌ساز می‌شود. از یک جهت، این مسئله را می‌توان تغییر مثبتی در جهت مسئولیت‌پذیری و کارایی تلقی کرد، ولی از دیدگاه کشورهای عضو، این موضوع خطری برای استقلال و اولویت‌بندی عملیات داخلی، به‌ویژه در زمینه جرائم سایبری تعبیر می‌شود (UK Home Office July 2013). ادغام پیشنهادی دانشکده پلیس اتحادیه اروپا و یوروپل احتمالاً باعث تقویت همکاری و پیوند شرایط آموزشی و عملیاتی می‌شود و ازاین‌رو، در رفع اختلاف فرهنگی بین طرف‌های ذینفع مختلف نقش دارد و درعین‌حال کارایی مقررات را بیشتر می‌نماید (Improvements proposed for Europol 2013). بااین‌حال، شواهد حاکی از این است که دستیابی به چنین توافقی دشوار است، چراکه بسیاری از کشورهای عضو به‌رغم وجود منطقی روشن برای ادغام ابعاد آموزشی و عملیاتی در مرکز مقابله با جرائم سایبری اتحادیه اروپا، کماکان خواستار حفظ شرایط موجود هستند (Interview, Senior Official EC3, September 2014).

جمع‌بندی: امنیت تاب‌آور و جرائم سایبری در اتحادیه اروپا

تحلیل فوق ازنظر تکامل امنیت تاب‌آور چه معنایی دارد؟ این مسئله چه پیامدهایی برای حکمرانی جرائم سایبری در اتحادیه اروپا می‌تواند به همراه داشته باشد؟ از تحلیل فوق این مسئله مشخص می‌شود که مشکلاتی مشابه ۱۰ سال قبل در مورد ایجاد و بهینه‌سازی پیش‌شرط‌های برقراری امنیت تاب‌آور کارآمد برای مقابله با جرائم سایبری در اتحادیه اروپا وجود دارند. بازیگران، فرآیندها، سطوح، لایه‌ها و ابعاد بی‌شمار دخیل در ایجاد اکوسیستمی کارآمد باعث می‌شوند این موضوع پیچیده شود و با توجه به اهمیت و محوریت تبدیل «فرهنگ‌ها» شیوه‌های تفکر و اجرا در رسیدگی به مشکلات پویای جرائم سایبری، چنین اکوسیستمی تنها از طریق تغییر فزاینده به دست می‌آید. این موضوع نیز روشن است که جرائم سایبری –در واقعیت– جدا از مشکلات کلی‌تر، مربوط به امنیت سایبری نیستند.

البته این موضوع بدین معنا نیست که پیشرفتی صورت نگرفته است. بدیهی است که ازنظر طراحی سازوکارها و فضاهایی برای ایجاد درک بهتر نحوه تفکر و اقدام بازیگران مختلف مانند

نهادهای مجری قانون و تیم‌های واکنش اضطراری رایانه‌ای اتحادیه اروپا در خصوص جرائم سایبری پیشرفت حاصل شده است. علاوه بر این، کشورهای عضو بسیار بیشتری نسبت به ۱۰ سال قبل کنوانسیون بوداپست را امضاء، تصویب و اجرا کرده‌اند که این مسئله حداقل مبنایی برای هماهنگی و همکاری برون‌مرزی ایجاد می‌کند که امریه‌ها و مقررات اتحادیه اروپا که به‌طور مستقیم و غیرمستقیم به جرائم سایبری رسیدگی می‌کنند مکمل آن محسوب می‌شوند. آگاهی از این مطلب نیز حائز اهمیت است که ساختارهای نهادی جدید آژانس امنیت شبکه و اطلاعات اتحادیه اروپا و مرکز مقابله با جرائم سایبری اتحادیه اروپا به‌عنوان بهترین نمونه‌های آن– جهت رسیدگی به مسئله جرائم سایبری ازنظر، به ترتیب، تسهیل هماهنگی بین طرف‌های ذینفع در بین و میان کشورهای عضو و ابعاد عملیاتی همکاری در زمینه جرائم سایبری از تحقیقات گرفته تا پیگرد قانونی ایجاد شده‌اند. در سطح اتحادیه اروپا نیز راهبرد امنیت سایبری اتحادیه اروپا (۲۰۱۳) فهرستی از اولویت‌های مربوط به جرائم سایبری و سایر ابعاد امنیت سایبری را منتشر کرده است و تغییر قابل‌ملاحظه‌ای نیز در قانون‌گذاری و حکمرانی جرائم سایبری ملاحظه می‌شود که به دنبال ایجاد شفافیت حقوقی در مسائلی نظیر تعریف جرائم سایبری، اشتراک داده‌ها و اطلاعات، حفظ حریم خصوصی، تحقیقات و پیگرد قانونی است.

تحولات فقط در ابعاد حقوقی و رسمی روی نداده است. شبکه‌ها، برنامه‌ها، اتحادها و راهبردهایی نظیر ارائه اینترنت امن‌تر برای کودکان و راهبرد اینترنت بهتر برای کودکان اتحادیه اروپا نیز تکامل یافته‌اند. نقش مشارکت‌های مؤثر عمومی–خصوصی از اهمیت برخوردار است، ائتلاف مالی اتحادیه اروپا نمونه مناسبی در این زمینه محسوب می‌شود. این امر نیز واضح است که شواهد و نظرات حاکی از اهمیت مشارکت غیررسمی در عملکرد کارآمد مقابله با جرائم سایبری است. چنین ترتیباتی، به‌ویژه در زمانی که به خاطر مسئله‌ای مطرح می‌شوند (برای مثال، مقابله علیه بات‌نت‌ها) مسلماً تاب‌آوری و انگیزه لازم را در طرف‌های ذینفع –خصوصی یا عمومی– برای همکاری در جهت بهینه‌سازی منابع و تخصص‌ها با هدف مقابله با جرائم سایبری به وجود می‌آورند. باوجوداین که طرح کارگروه اقدام مشترک علیه جرائم اینترنتی از این نظر بیانگر اقدام برای (شبه)رسمی سازی چنین ترتیباتی در ساختارهای مرکز مقابله با جرائم سایبری اتحادیه

اروپا است، اما نحوه گسترش چنین الگویی برای همکاری اصولی در اروپا و جهان جهت ارائه ساختار اصلی و پایدارتری در زمینه همکاری عمومی-خصوصی در میان‌مدت تا بلندمدت مشخص نیست.

با وجود بیان این مطالب، این مسئله واضح است که پیش‌شرط‌های مربوط به امنیت تاب‌آور کارآمد در اروپا و اتحادیه اروپا ایجاد نشده‌اند –ابعاد جهانی و محلی، تکامل فرهنگ امنیت تاب‌آور سایبری را پیچیده‌تر می‌سازند. در سطح ابتدایی، عدم تقارن موجود بین کشورهای عضو و منابع در اختیار آن‌ها (مالی، حقوقی، مهارت‌ها و سایر موارد) جهت مقابله با جرائم سایبری بیانگر مانع بزرگی ازنظر میزان آمادگی، هماهنگی، شناسایی متقابل و همگرایی است. روابط بین طرف‌های ذینفع و سازمان‌های مختلف در حال تکوین و تکامل است ازاین‌رو، به‌رغم همگرایی در زمینه آگاهی از موارد موردنیاز، در عمل موانع اساسی فرهنگی، رفتاری، حقوقی و سیاسی پیش روی همکاری، تشریک‌مساعی و هماهنگی مؤثر قرار دارد. علاوه بر این، با وجود طرح‌های بی‌شمار اتحادیه اروپا برای مقابله با جرائم سایبری، چگونگی تلفیق این طرح‌ها با یکدیگر و درواقع، نوع تأثیر آن‌ها ازنظر ابعاد عملیاتی، حقوقی و نظارتی، فنی، آموزشی و فرهنگی طرف‌های ذینفع مهم است. بر اساس شواهد موجود و اینکه تمام مسائل مهم در این فصل مطرح نشده‌اند، می‌توان به این نتیجه رسید که امنیت تاب‌آور در حوزه جرائم سایبری اتحادیه اروپا در مرحله تکوین تدریجی قرار دارد-این امنیت کماکان به درجه‌ای از یکپارچگی لازم جهت مبارزه کارآمد علیه جرائم سایبری در اروپا و اتحادیه اروپا دست نیافته است. برای تحقق این موضوع در میان‌مدت تا بلندمدت، موانع بین جوامع طرف‌های ذی‌نفع مربوطه همچنان باید رفع شده و روابط کاری و مشارکت‌های منظم و پایداری بر اساس اصطلاحات رایج ایجاد شوند. تنها در این صورت است که اتحادیه اروپا می‌تواند توسعه اکوسیستمی برای رسیدگی به مشکلات جرائم سایبری را تضمین نماید و امنیت سایبری نیز امکان محافظت از سیستم‌ها و شبکه‌های اروپا در برابر مجرمان سایبری را ایجاد و طراحی برنامه ایمنی برای رشد اقتصادی در عرصه اقتصاد دیجیتال را تضمین می‌کند.

فصل ششم

امنیت شبکه و اطلاعات و دفاع سایبری در اتحادیه اروپا

مقدمه

در این فصل ویژگی‌های اصلی راهبرد امنیت سایبری اتحادیه اروپا (EUCSS 2013)، یعنی راهبردهای امنیت شبکه و اطلاعات و دفاع سایبری بررسی می‌شوند. به‌رغم ایجاد ساختارهای مشارکتی در زمینه امنیت سایبری در محیط نهادی اتحادیه اروپا، این دو حوزه مربوط به سیاست امنیت سایبری تحت تأثیر دو حکم متفاوت بوده و ازاین‌رو، فرآیندها و بازیگران بسیار متفاوتی هستند. به‌علاوه، آن‌ها در مراحل توسعه مختلفی قرار دارند؛ امنیت شبکه و اطلاعات بیش از ده سال است که بخشی از دستورکار اتحادیه اروپا شده است، اما دفاع سایبری تنها به‌عنوان اولویت خاص امنیت سایبری در راهبرد امنیت سایبری اتحادیه اروپا مطرح شده است. ازاین‌رو، با وجود عدم تقارن مشخص موازنه تحلیلی که در ادامه اشاره خواهد شد، این تحلیل به مسئله تکامل این دو ویژگی در زمینه ایجاد تاب‌آوری و مسئله امور دفاعی پیش از انتشار راهبرد امنیت سایبری اتحادیه اروپا توجه دارد و ارزیابی مقدماتی را از نحوه سوق اتحادیه اروپا به سمت اتخاذ رویکرد امنیت تاب‌آور کارآمد در آینده نزدیک توسط تدابیر ذکرشده در این راهبرد ارائه می‌کند. ذکر این نکته در اینجا حائز اهمیت است که با وجود تحلیل جداگانه این دو ویژگی در این فصل، آن‌ها مطالب بسیار مرتبطی هستند و دفاع سایبری عامل بسیار مهمی در تأمین امنیت سیستم‌ها و زیرساخت‌ها در برابر حملات سایبری محسوب می‌شود. گرچه این دو بعد، «تحت حکمرانیِ» دو حکم و درنتیجه پویایی بسیار متفاوتی قرار دارند که با وجود هم‌پوشانی

اکوسیستم آن‌ها، پیامدهای متنوعی برای موضوع تکامل سایبری به همراه دارند.

منطق‌های مختلفی مبنای رویکرد اتحادیه اروپا در قبال امنیت شبکه و اطلاعات هستند. مورد نخست، منطق اقتصادی برای ترغیب و ایجاد انگیزه برای توسعه جامعه اطلاعاتی امن برای همگان است. دوم، منطق امنیتی است که تحت تأثیر و بسیار مرتبط با [ضرورت] حفاظت از زیرساخت‌های حیاتی، در برابر حملات تروریستی است. رویکرد اتحادیه اروپا ازنظر منطق‌های حکمرانی نیز تحول یافته است به‌طوری‌که به‌واسطه امریه پیشنهادی در زمینه امنیت شبکه و اطلاعات (۲۰۱۳) که در کنار راهبرد امنیت سایبری اتحادیه اروپا مطرح گردید و تا حدود زیادی بخشی از آن محسوب می‌شود، از رویکردی نسبتاً نظری به رویکردی عملی و نظارتی‌تر مبدل شده است. باوجوداینکه مسئله تأمین امنیت و مهم‌تر از آن تعهدات گزارش‌دهی در زمینه تأمین‌کنندگان ارتباطات الکترونیکی در چارچوب امریه ارتباطات الکترونیکی[1] (2009a) برای تأمین‌کنندگان مخابرات و کنترل‌کنندگان داده‌ها الزامی شده است، امریه امنیت شبکه و اطلاعات، بیانگر تغییر قابل‌ملاحظه آشکاری در خصوص منطق حکمرانی برای تمام دارندگان زیرساخت‌های حیاتی بود. بدین معنا که، این امریه مسئله شمول تمام بازیگران خصوصی و دولتی ذی‌ربط در امر الزام گزارش‌دهی در مورد حوادث سایبری مهم را مطرح کرد تا در مجموع تأمین امنیت سایبری تاب‌آور ازجمله همکاری و مشارکت کارآمد و هماهنگ به‌خصوص در زمینه اشتراک اطلاعات موثق بهبود یابد (Proposal for an NIS Directive, 2013a, p.3).

گذشته از این مسئله، آژانس امنیت شبکه و اطلاعات اتحادیه اروپا در سال ۲۰۰۴، در کنار طرف‌های ذی‌نفع مربوطه در بخش‌های دولتی و خصوصی با هدف طرح پیشنهادها و توصیه‌هایی در زمینه انجام اقدام مناسب در مورد امنیت اطلاعات و تسهیل همکاری و مشارکت و اجرای قانون مربوطه اتحادیه اروپا در خصوص امنیت شبکه و اطلاعات تأسیس شد. درواقع، حکم آژانس امنیت شبکه و اطلاعات اتحادیه اروپا در سال ۲۰۱۳ بازنگری شد تا این آژانس مشارکت مستقیمی در تأمین امنیت سایبری تاب‌آور و توسعه منابع فناورانه و صنعتی برای امنیت سایبری داشته باشد (اهداف ۱ و ۴ راهبرد امنیت سایبری اتحادیه اروپا).

1. Framework Directive for Electronic Communications

دفاع سایبری در مقایسه با هر دو مورد جرائم سایبری و امنیت شبکه و اطلاعات مسلماً پدیده نسبتاً جدیدی ازنظر توانمندی و ظرفیت نهادی اتحادیه اروپا محسوب می‌شود. اگرچه، اقدام اتحادیه اروپا در این حوزه، به‌خصوص در چارچوب سرویس اقدام خارجی اتحادیه اروپا و تیم امنیت سایبری آن ناشی از آگاهی فزاینده از این مسئله است که «دفاع سایبری رکن ضروری تمام راهبردهای امنیت سایبری به شمار می‌آید» (Interview, EEAS, senior official, Cyber Security team, February 2013). در اصل، مبنای این موضوع منطقی، امنیتی است که بر ضرورت توجه به شناسایی، واکنش و بازیابی[1] برای افزایش تاب‌آوری سیستم‌های ارتباطی و اطلاعاتی در سرتاسر اتحادیه اروپا تأکید دارد. علاوه بر این، با فرض ماهیت چندوجهی تهدیدهای سایبری، راهبرد امنیت سایبری اتحادیه اروپا بر «موارد هم‌افزایی رویکردهای نظامی و غیرنظامی به حفاظت از منابع سایبری حیاتی» با این استدلال تأکید دارد که این موارد هم‌افزایی باید به شیوه‌های متعددی ازجمله تحقیق و توسعه و همکاری مؤثر بیشتر بین طرف‌های ذی‌نفع مربوطه افزایش یابد (EUCSS 2013, p.11). به‌علاوه، کشورهای عضو اتحادیه اروپا از سال ۲۰۱۱ دفاع سایبری از طریق برنامه توسعه توانمندی‌های اتحادیه اروپا[1] را در اولویت قرار داده‌اند و در سال ۲۰۱۲، پیرامون مفهوم دفاع سایبری اتحادیه اروپا[2] در عملیات‌های تحت رهبری این اتحادیه توافق کردند. از آن زمان، آژانس دفاع اتحادیه اروپا در کنار کارکنان نظامی اتحادیه اروپا و سرویس اقدام خارجی اتحادیه اروپا، کمیسیون اروپا و کشورهای عضو اتحادیه به‌عنوان بازیگران اصلی در توسعه توانمندی‌های دفاع سایبری نقش داشته‌اند که این مورد بعد خارجی را نیز در برمی‌گیرد و با اقداماتی همراه است که توجه آن‌ها بر سیاست‌های کنونی ناتو و نقش اتحادیه اروپا در تکمیل این سیاست‌ها و اجتناب از تکرار آن‌ها است.

ساختار این فصل برای ارزیابی حدود عملکرد اتحادیه اروپا در حوزه امنیت شبکه و اطلاعات و دفاع سایبری –به‌خصوص ارزیابی حدود پیشرفت یا پسرفت اتحادیه اروپا در کسب امنیت تاب‌آور کارآمد به‌واسطه تحولات صورت‌گرفته– بدین ترتیب است: بخش نخست، به مسئله راهبرد امنیت سایبری اتحادیه اروپا می‌پردازد و با ارزیابی پیشنهادهای مطرح‌شده برای بهبود،

1. EU's Capability Development Plan
2. EU Concept for Cyber Defence

امنیت سایبری تاب‌آور را ارائه می‌کند. با توجه به اینکه پوشش کامل تمام موارد در این فصل غیرممکن است، ازاین‌رو، صرفاً نقش آژانس امنیت شبکه و اطلاعات اتحادیه اروپا و پیشنهادی برای امریه امنیت شبکه و اطلاعات (۲۰۱۳)، مطرح می‌گردد که در زمان نگارش این سطور (مارس ۲۰۱۵) کماکان در شورای وزیران اتحادیه اروپا مورد مذاکره بوده است. بخش دوم نیز به مسئله دفاع سایبری و به‌خصوص اهداف دفاع سایبری تعیین‌شده در راهبرد امنیت سایبری اتحادیه اروپا و طرح‌های مصوب شورای سران اتحادیه اروپا در دسامبر ۲۰۱۳ می‌پردازد که پنج حوزه کاری مربوط به دفاع سایبری را مشخص می‌کند. در بخش آخر نیز نتایج اولیه شیوه حرکت اتحادیه اروپا به سمت امنیت تاب‌آور کارآمد در چارچوب این ویژگی‌های مهم امنیت سایبری مطرح می‌شود.

حکمرانی بر امنیت شبکه و اطلاعات در اتحادیه اروپا

مانند مورد فصل گذشته در زمینه جرائم سایبری، منطق اقتصادی تا حدی مبنای رویکرد اتحادیه اروپا در قبال امنیت شبکه و اطلاعات به‌عنوان بخشی از برنامه جامعه اطلاعاتی گسترده‌تر محسوب می‌شود. ازاین‌رو، طرح اروپای الکترونیک (۱۹۹۹) و ارتباطات امنیت شبکه و اطلاعات اتحادیه اروپا: طرحی برای رویکرد سیاسی اروپا (European Commission 2001) بر اهمیت حفاظت از زیرساخت‌های اطلاعاتی تأکید دارد و مورد دوم، توصیه‌هایی در مورد نحوه افزایش امنیت تاب‌آور در چارچوب لایه‌های سیاسی، حقوقی و فنی ارائه می‌کند. در ابتکار آی ۲۰۱۰[1] (۲۰۰۵) نیز بر اهمیت امنیت فضای اطلاعاتی واحد اروپا[2] توجه گردید که بر «اعتبار و امنیت سیستم‌های شبکه و اطلاعات» و ارتباطات کمیسیون اروپا به‌عنوان یک «راهبرد برای جامعه اطلاعاتی امن»[۲] تأکید داشت (European Commission 2006) که دستورکار دیجیتال گسترده‌تری را برای طرح اروپا دنبال می‌کرد (European Commission 2010). مورد سوم، مجموعه اقدامات جامعی را برای رسیدگی به مسائل پیشگیری، شناسایی و واکنش به مشکلات ناشی از مسئله امنیت شبکه و اطلاعات انجام می‌داد.

1. i2010 initiative
2. Single European Information Space

ارتباطات به‌ضرورت ایجاد ابعاد مهم امنیت تاب‌آور، نظیر فرهنگ امنیت سایبری برای اتحادیه اروپا اشاره داشت که در آن امنیت شبکه و اطلاعات و چارچوب نظارتی ارتباطات الکترونیک دو مورد از سه رکن تمام راهبردهای ازاین‌دست را تشکیل می‌دهند (رکن سوم جرائم سایبری است، ن.ک. فصل ۵). هدف طرح‌های اصلی در این ارتباطات، تقویت گفتمان از طریق تشویق سطح‌بندی و اشتراک بهترین اقدام در میان بخش‌های مدیریت دولتی (شیوه باز به‌جای شیوه اجباری) با این انتظار است که این موضوع منجر به افزایش آگاهی‌بخش خصوصی گردد. آژانس امنیت شبکه و اطلاعات اتحادیه اروپا از این نظر تشویق می‌شد تا نقش فعالی را در این گفتمان و تسهیل تبادل بهترین اقدامات، داشته باشد. طرح دوم به اشتراک اطلاعات از طریق مشارکت راهبردی معتبر با هدف ایجاد سیستم اشتراک اطلاعات و هشدار اروپا می‌پردازد تا واکنش‌دهی کارآمد به تهدیدهای صورت گرفته علیه سیستم‌های شبکه و اطلاعات تسهیل گردد (European Commission Communication 2006a, p.8). به‌علاوه، این بیانیه حامی ایجاد تنوع در فناوری به‌عنوان عامل مهم تأمین امنیت در کنار قابلیت همکاری و توانایی صنعت اروپا، برای تضمین تأمین محصولات و خدمات امنیت شبکه و اطلاعات بود (Ibid., p.9).

این طرح‌ها در چارچوب این ابعاد برای تکمیل اهداف ترسیم‌شده در برگه سبز کمیسیون در زمینه برنامه اروپا برای حفاظت از زیرساخت‌های حیاتی[1] طراحی شده بودند (European Commission Green Paper, EPCIP 2005) که مبنای آن رویکرد بخشی[۳] و منطق امنیت بود که برای بخش فناوری اطلاعات و ارتباطات به معنای تقویت امنیت تاب‌آور سیستم‌های شبکه و اطلاعات از طریق رویکرد گفتمان چندجانبه بود. نظرات مطرح‌شده در برگه سبز کمیسیون اروپا، در بیانیه‌ای پیرامون برنامه اروپا برای حفاظت از زیرساخت‌های حیاتی بیشتر تشریح گردید (European Commission 2006b). این بیانیه به وابستگی و ارتباط متقابل زیرساخت‌های حیاتی و اهمیت تضمین امنیت تاب‌آور فناوری اطلاعات و کاهش تهدیدهای دیگر (تروریسم، بلایای طبیعی و غیره) اشاره می‌کند. از این نظر، هدف برنامه اروپا برای حفاظت از زیرساخت‌های حیاتی به حداقل‌رسانی نقاط آسیب‌پذیری در سطح اروپا که،

1. European Programme for Critical Infrastructure Protection (EPCIP)

احتمالاً به دلیل اختلال در سرویس‌های مهم ایجاد می‌شوند و بهبود و کارآمدترسازی حفاظت و تاب‌آوری زیرساخت‌های حیاتی در اتحادیه اروپا بود. ابعاد محوری (چارچوب) این برنامه بر ضرورت فرایند شناسایی و تعیین زیرساخت‌های حیاتی «اروپا» و درنتیجه اقدامات مربوط به حفاظت از آن‌ها، اقدامات رویه‌ای برای تسهیل اجرای برنامه، ایجاد شبکه اطلاعاتی هشدار در مورد زیرساخت‌های حیاتی[1] جهت تبادل امن بهترین رویه، پشتیبانی بیشتر از کشورهای عضو در زمینه حفاظت از زیرساخت‌های حیاتی ملی و مدیریت بحران و پیشامدهای غیرمترقبه تأکید داشت. اقدامات مختلفی نیز برای تضمین اجرای برنامه پیش‌بینی شده بود که عبارت‌اند از تشکیل گروه تماس حفاظت از زیرساخت‌های حیاتی[2] جهت تسهیل همکاری بین کشورهای عضو و بین گروه‌های تخصصی برای اعتمادسازی و تسهیل هماهنگی و تبادل اطلاعات بین تمام طرف‌های ذینفع. این برنامه ازنظر حکمرانی، بازتاب فراحکمرانی نظری به‌واسطه ایجاد برنامه‌های هماهنگ‌کننده و اشتراک اطلاعات بود.

محصول کار امریه برای مرحله نخست شناسایی و طراحی زیرساخت‌های حیاتی اروپا[3] بود (Council Directive 2008/114/EC)[۴]. این امریه بر حوزه‌های انرژی و حمل‌ونقل توجه داشت و به دنبال تعیین رویه‌ها، سازوکارها و برنامه‌های ملموس‌تری برای شناسایی و تعیین زیرساخت‌های حیاتی اروپا و تسهیل گزارش‌دهی، هماهنگی و حفاظت از زیرساخت‌های حیاتی اروپا در این بخش‌ها بود.[۵] البته منطق مبنای آن فراگیری از این مسئله و نحوه به‌کارگیری آن در سایر بخش‌ها با تأکید بر فناوری اطلاعات و ارتباطات به‌عنوان بخش دارای اولویت به شمار می‌آمد. مسلماً کمیسیون اروپا به دلیل حملات صورت‌گرفته به استونی در سال ۲۰۰۷ و بر اساس تصمیم‌گیری ساختاری در زمینه حمله به سیستم‌های اطلاعاتی (و بازنگری برنامه‌ریزی‌شده آن)، بیانیه‌ای را درخصوص حفاظت از زیرساخت‌های اطلاعاتی حیاتی تنظیم کرد (European Commission 2009b) که در آن به برخی مسائل مربوط به تأمین امنیت تاب‌آور تأکید و طرح اقدامی نیز برای رسیدگی به مشکلات اصلی پیشنهاد شد.

1. Critical Infrastructure Warning Information Network (CIWIN)
2. CIP Contact Group
3. European Critical Infrastructures (ECI)

این طرح‌های پیشنهادی به‌موازات و تحت برنامه اروپا برای حفاظت از زیرساخت‌های حیاتی و طرح‌های پیشنهادی برای بازنگری چارچوب نظارتی ارتباطات الکترونیکی اتحادیه اروپا[1] (مبحث بعد) قرار داشت. این مسائل، به موضوع عدم دستیابی به معیارهای اساسی ضروری برای تأمین امنیت تاب‌آور ازجمله عدم هماهنگی و همکاری بین کشورهای عضو اتحادیه اروپا (برتری رویکردها و فرهنگ‌های ملی) و توزیع نابرابر دانش (تخصص) و منابع، معضل حکمرانی فراتر از مرزهای ملی و مشارکت خصوصی- عمومی به‌عنوان الگوی مرجع، به‌کارگیری فرایندها و اقدامات متفاوت برای نظارت و گزارش حوادث امنیتی شبکه و اشتراک اطلاعات در بین کشورهای عضو (با الزامات اساسی مانند وجود تیم واکنش اضطراری رایانه‌ای در سطح ملی/دولتی که در اتحادیه اروپا به چشم نمی‌خورد)، و عدم وجود هماهنگی و توافق جهانی بر سر حکمرانی و حفاظت از اینترنت می‌پرداختند.

با توجه به تضمین استانداردسازی گزارش تخلف‌های امنیت شبکه و اطلاعات، هدف چارچوب بازنگری‌شده ارتباطات الکترونیکی (European Parliament and Council 2009) افزودن بعد فراحکمرانی عملی، یعنی شمول قوانینی در زمینه الزام (ماده ۱۳a) گزارش تخلف‌های امنیتی سیستم‌های شبکه و اطلاعات به اداره ملی مقررات بود. این تغییر قابل‌ملاحظه، حرکت مهمی در عدم اتخاذ رویکرد داوطلبانه بود که برای مثال، ویژگی بیانیه ۲۰۰۶ محسوب می‌شد. آژانس امنیت شبکه و اطلاعات اتحادیه اروپا وظیفه حمایت از کشورهای عضو برای اجرای ماده ۱۳a را از طریق ایجاد روش و سازوکار استانداردی برای گزارش حوادث برعهده داشت (ENISA, Technical Guidelines on Incident Reporting 2013). سند تنظیم‌شده توسط این آژانس «راهنمایی لازم را در اختیار اداره ملی مقررات درخصوص اجرای دو نوع گزارش حوادث مطرح‌شده در ماده ۱۳a می‌گذارد: ارائه خلاصه گزارش سالیانه حوادث مهم به آژانس امنیت شبکه و اطلاعات اتحادیه اروپا و کمیسیون اروپا و اعلام موردی حوادث به سایر مقامات نظارت ملی در مورد حوادث فرامرزی.» این سند دامنه گزارش حوادث، پارامترها و حدود حوادث را تعیین می‌کند.

1. EU's Regulatory Framework for Electronic Communications
2. National Regulatory Authority (NRA)

در متن بالا، حفاظت از زیرساخت‌های اطلاعاتی حیاتی (European Commission 2009a, p.7-11) پنج رکن اصلی اقدام را مطرح می‌کند: آمادگی و پیش‌گیری (برای تضمین میزان آمادگی در تمام سطوح) با حضور طرف‌های ذینفع که سه ویژگی اصلی همکاری و آمادگی را تعیین می‌کنند:

۱. تعریف مجموعه حداقل توانمندی‌ها و خدمات پایه‌ای که تیم واکنش اضطراری رایانه‌ای در سطح ملی/دولتی برای کارکرد کارآمد خود با حمایت آژانس امنیت شبکه و اطلاعات اتحادیه اروپا به آن‌ها نیاز دارد؛ ۲. مشارکت خصوصی- عمومی اروپا در امنیت تاب‌آور[1] برای تقویت همکاری بین بخش عمومی و خصوصی با هدف توسعه اهداف تأمین امنیت تاب‌آور، الزامات اساسی و اقدام مناسب و ۳. مجمع اروپایی کشورهای عضو[2] برای اشتراک اقدام مناسب و اطلاعات مربوط به امنیت تاب‌آور زیرساخت‌های اطلاعاتی حیاتی؛ شناسایی و واکنش برای ایجاد سازوکارهای هشدار اولیه مناسب با محوریت توسعه سیستم هشدار و اشتراک زودهنگام اطلاعات[3] با کمک آژانس امنیت شبکه و اطلاعات اتحادیه اروپا؛ کاهش [حملات] و بازیابی [سیستم پس از حملات] (جهت تقویت سازوکارهای دفاعی اتحادیه اروپا برای زیرساخت‌های اطلاعاتی حیاتی) شامل اقدامات سه‌جانبه مرتبطی می‌شود:

۱) طراحی برنامه‌های ملی مربوط به حوادث غیرمترقبه و سازماندهی مانورهای منظم برای واکنش به حوادث امنیت گسترده شبکه و بازیابی شبکه؛ ۲) طراحی مانورهای اروپایی در خصوص حوادث امنیت اینترنت به‌عنوان محلی برای شرکت در مانورهای بین‌المللی، برای مثال، طوفان سایبری آمریکا[4] و ۳) تقویت همکاری بین تیم‌های واکنش اضطراری رایانه‌ای در سطح ملی/دولتی از طریق مجامع تشکیل‌شده‌ای نظیر تیم‌های واکنش اضطراری رایانه‌ای (http://www.egc-goup.org)؛ همکاری بین‌المللی (برای پیشبرد اولویت‌های اروپا) که اساساً شامل طرح اولویت‌های اروپا در زمینه تاب‌آوری و ثبات اینترنت و تعریف اصول و دستورالعمل‌هایی در این زمینه در سطوح جهانی و اروپایی است؛ معیارهایی برای بخش فناوری اطلاعات و ارتباطات

1. European Public Private Partnership for Resilience (EP3R)
2. European Forum for Member States (EFMS)
3. Early Information Sharing and Alert System
4. US Cyber Storm

(جهت پشتیبانی از امریه شناسایی و تعیین زیرساخت‌های حیاتی اروپا) که هدف آن تداوم توسعه معیارهایی برای شناسایی زیرساخت‌های حیاتی اروپا برای بخش فناوری اطلاعات و ارتباطات از طریق تحقیقات و پژوهش در این زمینه است.

تصویر مبهمی در مورد حدود نقش عملی این تحولات در ایجاد شرایط لازم برای تأمین امنیت تاب‌آور وجود دارد. در بازنگری طرح حفاظت از زیرساخت‌های اطلاعاتی حیاتی (۲۰۱۱) از سوی کمیسیون اروپا، به دستاوردهای مربوط به هر رکن اشاره می‌شود که این موضوع در سطح مقدماتی ما را به این نتیجه می‌رساند که در مانور در جریان و پویا چیزی بیش از موفقیت حاشیه‌ای به دست آمد.[۶] این مورد شامل موارد زیر است: تشکیل تیم واکنش اضطراری رایانه‌ای در سطح ملی/دولتی در ۲۰ کشور عضو اتحادیه اروپا[۷] با هدف ایجاد این گروه برای نهادهای اتحادیه اروپا[۸]؛ مشارکت خصوصی- عمومی اروپا در حوزه امنیت تاب‌آور و مجمع اروپایی کشورهای عضو؛ طراحی راهنمای پیشرفته‌ای برای پیاده‌سازی سیستم هشدار و اشتراک اطلاعات اروپا[۹]؛ تثبیت برنامه‌های ملی مربوط به حوادث غیرمترقبه در ۱۲ کشور عضو (در پایان سال ۲۰۱۰) و طراحی راهنمای اقدام مناسب در زمینه مانورهای ملی و هدایت نخستین مانور با رویکرد اروپایی تحت عنوان اروپای سایبری[1] ۲۰۱۰ -توسط آژانس امنیت شبکه و اطلاعات اتحادیه اروپا؛ افزایش همکاری تیم‌های واکنش اضطراری رایانه‌ای در سطح ملی/دولتی؛ تثبیت اصول و دستورالعمل‌های اروپا در مورد اقدامات اینترنتی صورت‌گرفته در مجمع اروپایی کشورهای عضو؛ مشارکت هفت کشور عضو[۱۰] در مانور سایبری آمریکا با عنوان طوفان سایبری ۳ با حضور آژانس امنیت شبکه و اطلاعات اتحادیه اروپا و کمیسیون اروپا به‌عنوان ناظر؛ مباحث فنی پیرامون معیارهای بخش فناوری اطلاعات و ارتباطات در مجمع اروپایی کشورهای عضو که به طرح پیش‌نویس معیارهایی برای ارتباطات تلفن ثابت و همراه و اینترنت منجر می‌شود.

بااین‌وجود شواهد حاکی از این است که برخی طرح‌ها نسبت به سایر طرح‌ها عملکرد موفق‌تری ازنظر تقویت شرایط لازم برای تأمین امنیت تاب‌آور، به‌خصوص ازنظر ایجاد محل دائمی برای تعامل و همکاری کارآمد بخش‌های عمومی و خصوصی داشته‌اند. برای مثال،

1. Cyber Europe 2010

مشارکت خصوصی- عمومی امنیت تاب‌آور اتحادیه اروپا، مانوری آموزشی بود، ولی درنهایت منجر به کسب نتایج ملموسی در مورد ایجاد محل دائمی برای بازیگران خصوصی و عمومی جهت بحث و یافتن راه‌حل مشکلات واقعی نشد. به‌رغم صراحت طرح ارائه‌شده در کنفرانس تالین سال ۲۰۰۹، برنامه مشارکت خصوصی- عمومی امنیت تاب‌آور اتحادیه اروپا[۱۱] در دو سال نخست کار خود، بازیگران بخش‌های عمومی و خصوصی را گرد هم آورد که توجه کاملی به مسائلی که باید موردبحث قرار می‌گرفتند و حل می‌شدند و درواقع، به تأثیر عملکرد کارگروه‌های گوناگون تشکیل‌شده بر سیاست کلی‌تر اتحادیه اروپا در زمینه امنیت شبکه و اطلاعات، نداشتند. از دیدگاه یکی از ناظران، «ارتباط واقعی بین طرح‌ها وجود نداشت و توجه کاملی بر آن‌ها مبذول نشد؛ حدود وظایف و اختیارات بسیار گسترده و موضوعات مختلفی را پوشش می‌داد» (Interview, Anonymous, July 2012). درنهایت، انگیزه‌های مناسب و درواقع، مسائل و فرایندهای واقعی متناسب با تخصص بخش‌های خصوصی جهت کسب نتایج تأثیرگذار بر تحولات سیاست-گذاری اتحادیه اروپا در اختیار آن‌ها قرار نگرفت.

در بررسی داخلی آژانس امنیت شبکه و اطلاعات اتحادیه اروپا در مورد فرایندهای مقدماتی مبنای مشارکت خصوصی- عمومی امنیت تاب‌آور اتحادیه، این نقاط ضعف شناسایی شدند که این موضوع منجر به ظهور حوزه‌های موضوعی مشخص‌تری برای کارگروه‌ها و بیانیه رسالت و درنهایت دستورکاری گردید که بسیار دقیق و هدفمند بود. مضامین کارگروه‌ها شامل این موارد است: ۱. منابع و کارکردهای اصلی برقراری مستمر و امن ارتباطات الکترونیک در کشورهای مختلف؛ ۲. الزامات اساسی تأمین امنیت تاب‌آور ارتباطات الکترونیک و ۳. نیازها و سازوکارهای مربوط به هماهنگی و همکاری برای آمادگی و واکنش‌دهی به اختلالات گسترده مؤثر بر ارتباطات الکترونیک (توجه به مقابله علیه بات‌نت‌ها). گرچه، این موضوع موجب توجه بیشتر به اهداف و نتایج احتمالی مشارکت خصوصی- عمومی امنیت تاب‌آور اتحادیه اروپا گردید، اما «به نتایج عینی قابل انتقالی دست نیافت». درواقع، مشارکت خصوصی- عمومی امنیت تاب‌آور اتحادیه اروپا به دلیل عدم ایجاد شرایط لازم برای اعتمادسازی طرف‌های ذینفع با مشکل روبرو شد، چراکه آن‌ها از منطق و دیدگاه‌های متفاوتی برخوردار بودند و این امر، موجب عدم دست‌یابی

به نتایج عینی گردید (Interview, DG Connect official, June 2013, Interview ENISA official, July 2012). به دلیل نبود ارتباط مشخص بین کار مشارکت خصوصی- عمومی امنیت تاب‌آور اتحادیه اروپا با اهداف سیاست و قوانین اتحادیه، انگیزه لازم در طرف‌های ذینفع خصوصی و عمومی برای شرکت در این فعالیت با هدف مشخصی ایجاد نشد.(۱۲) طرح مشارکت خصوصی- عمومی امنیت تاب‌آور اتحادیه اروپا پس از انتشار راهبرد امنیت سایبری اتحادیه اروپا با طرح جدیدی با عنوان پلتفرم امنیت شبکه و اطلاعات عمومی- خصوصی[1] پیگیری شد تا به مسئله نقاط ضعف تجربه مشارکت خصوصی- عمومی امنیت تاب‌آور اتحادیه اروپا پرداخته شود. پلتفرم امنیت شبکه و اطلاعات عمومی- خصوصی کاملاً با راهبرد امنیت سایبری اتحادیه اروپا(۱۳)، امریه امنیت شبکه و اطلاعات و برنامه تحقیقاتی افق ۲۰۲۰(۱۴) مرتبط است و در زمان نگارش این کتاب (مارس ۲۰۱۵) این طرح کماکان مراحل نهایی [تصویب] اهداف اصلی خود را می‌گذراند و درنتیجه ارزیابی کاربرد و پایداری آن به‌عنوان برنامه دشوار است. شایان‌ذکر است که برخی پیشرفت این برنامه موقت در زمینه اعتمادسازی لازم و تعامل منظم برای همکاری، هماهنگی و تشریک‌مساعی بخش‌های دولتی- خصوصی در بلندمدت را زیر سؤال برده‌اند (Interview, Anonymous, September 2014).

پس از برنامه مشارکت خصوصی- عمومی امنیت تاب‌آور اتحادیه اروپا، مجمع اروپایی کشورهای عضو که جهت تقویت همکاری و هماهنگی دولت‌های ملی برای تأمین امنیت تاب‌آور زیرساخت‌های حیاتی ایجاد شده بود به موفقیت مورد انتظار از آن دست پیدا نکرد. از یک نظر، پاسخ دولت بریتانیا به گزارش چهارم کمیته اتحادیه اروپای مجلس اعیان این کشور در مورد طرح اقدام حفاظت از زیرساخت‌های اطلاعاتی حیاتی با عنوان این مطلب که «مجمع اروپایی کشورهای عضو دستاورد موفقی به شمار می‌آید و به نیاز واقعی سیاست‌گذاران برای ایجاد فرصت تبادل تجربیات دست یافته است»، این است که کاملاً از این برنامه حمایت می‌کند (UK government House of Lords 2010–2011, p.8). درواقع، این مجمع نقش مهمی در طرح اصول و امریه‌های اتحادیه اروپا در مورد تأمین امنیت تاب‌آور اینترنت ایفا می‌کند

1. NIS Public Private Platform (NISP)

(ن.ک. مبحث بعد). اگرچه، برخی افراد از این موردحمایت نکرده‌اند و توانایی تسهیل تبادل اقدام مناسب یا اطلاعات این مجمع را زیر سؤال برده‌اند. برای مثال، بعضی آن را به محفلی بدون نتایج عینی و محلی برای حضور مقامات دون‌پایه تشبیه کرده‌اند که جلسات نامنظم آن، تنها سه جلسه در سال، چندان تأثیری بر اعتمادسازی و تبادل کارآمدتر اطلاعات و اقدام مناسب ندارد. ازنظر برخی نیز اهمیت این مجمع به‌اندازه مجامع سطح ملی و هماهنگی حفاظت از زیرساخت‌های اطلاعاتی حیاتی ملی نیست (Interviews, EEAS and ENISA, February 2013/ July 2012; Interview, UK cybersecurity official, October 2014). از آن مهم‌تر اینکه، مجمع اروپایی کشورهای عضو ابزار سودمندی ازنظر ایجاد شرایط لازم برای تشریک‌مساعی، همکاری و هماهنگی تلقی می‌شود، اما لزوماً ابزاری برای ایجاد محلی دائمی، قابل‌اعتماد و کارآمد برای بحث و تبادل اطلاعات و اقدام مناسب محسوب نمی‌شود. به‌عبارت‌دیگر، به‌رغم ایجاد فرصت تبادل تجربیات و طرح اصول مهمی برای سیاست‌گذاران، نتیجه این فرصت برای رسیدگی کارآمد و پایدار به مسائل مربوط به حفاظت از زیرساخت‌های اطلاعاتی حیاتی در داخل و سرتاسر اروپا به‌اندازه کافی روشن یا شفاف نیست.

مانورهای سایبری برگزارشده در سطح جهان و اروپا که مورد استقبال دولت‌های ملی قرار دارند، به‌عنوان ابزاری مثبت برای تقویت برنامه‌ریزی حوادث غیرمترقبه و توانمندی کشورهای عضو اتحادیه اروپا در حوزه امنیت سایبری تلقی می‌شوند. از ابتدا مسئولیت مانورهای سایبری برعهده آژانس امنیت شبکه و اطلاعات اتحادیه اروپا گذاشته شد که تاکنون بر دو مانور با رویکرد اروپایی (۲۰۱۰ و ۲۰۱۲)[۱۵] و مانورهای مشترک انجام‌شده با ایالات‌متحده آمریکا (ن.ک. فصل ۷) و سایر کشورهای ثالث نظارت داشته و موجب تسهیل آمادگی و انجام مانورهای ملی کشورهای عضو شده است. مانورهای سایبری در ابتدا نشان‌دهنده عدم تناسب در میزان آمادگی کشورهای عضو اتحادیه اروپا در مقابله با حملات به سیستم‌های اطلاعاتی و زیرساخت‌های حیاتی و عدم وجود چارچوب مشترکی در اروپا قوانین، هنجارها و روش کار برای واکنش‌دهی در برابر این نوع حملات و بازیابی سیستم پس از آن بود. یکی از مقامات آژانس امنیت شبکه و اطلاعات اتحادیه اروپا که جزو افراد مسئول آماده‌سازی این مانورها است درخصوص نخستین

مانور چنین می‌گوید:

«توانمندی‌ها و انتظاراتی در این زمینه وجود داشت ... که بزرگترین مشکل پیش روی کشورها .... تجربه بیش‌ازحد بعضی کشورها و بی‌تجربگی برخی دیگر بود .... درنتیجه، انتظارات متفاوتی در مورد خواسته این کشورها از این مانورها وجود داشت ... و [عدم برخورداری] تمام کشورها از [میزان تجربه مشابه] .... مشکل بزرگی است» (Interview, ENISA official, July 2012).

با اشاره به این موضوع روشن است که مانورهای سایبری در حکم ابزار آموزشی هستند، بدین معنی که آمادگی انجام این مانورها به معنای ایجاد ساختارها، نهادها و محیط لازم (برای مثال، تیم واکنش اضطراری رایانه‌ای، برنامه‌ریزی حوادث غیرمترقبه و غیره) جهت مشارکت و درنتیجه واکنش‌دهی عملی است (Ibid). آژانس امنیت شبکه و اطلاعات اتحادیه اروپا با حمایت مرکز تحقیقات مشترک کمیسیون اروپا[1] سازماندهی و اجرای مانورها را تسهیل کرده است. بدین منظور، این آژانس دستورالعمل‌هایی را منتشر کرده[۱۶] و سمینارهایی را جهت شفاف‌سازی کل عملکرد این مانور برای کشورهای عضو، برگزار کرده است. ازاین‌رو، مانورهای سایبری محل یادگیری دائمی محسوب می‌شوند که در آن‌ها مشکلات هر مانوری بررسی می‌گردند. ولی نکته مهم‌تر این است که تجربیاتی در مورد نحوه افزایش میزان آمادگی و واکنش‌دهی در سطح ملی، جهانی و اروپایی نیز به دست می‌آید. بدیهی است که این موضوع تنها در مورد بهبود فنی در سطوح مختلف نبود، بلکه در مورد تقویت ابعاد سیاسی، عملیاتی، فنی و راهبردی برای کسب توانایی واکنش‌دهی کارآمد به شیوه‌ای تاب‌آور در برابر حملات سایبری نیز بود. درنتیجه، در ارزیابی نخستین مانور با رویکرد اروپایی که در آن تنها نهادهای دولتی شرکت داشتند[۱۷]، مشکلات مربوط به مسائلی نظیر برنامه‌ریزی و سازماندهی مانور سایبری اعتمادسازی، افزایش تفاهم میان بازیگران مربوطه؛ نقاط تماس در موارد حمله (نقاط واحد در برابر چند نقطه) و برقراری ارتباط و تبادل کارآمد داده‌ها بود.

1. Joint Research Centre of the European Commission (JRC)

برای مثال، گزارش مذکور این موضوع را در خصوص اعتمادسازی بیان می‌کرد که «این واقعیت که نمایندگان (افراد میانجی) کشورهای عضو به‌طور منظم با یکدیگر ملاقات کرده و همکاری داشتند احتمالاً مهم‌ترین اقدام در جهت اعتمادسازی در این مانور محسوب می‌شد» (ENISA, 2011a, p.32). نکته مهم در اینجا این بود که این محل نقطه آغاز مهمی برای تبادل اطلاعات و دیدگاه‌ها از نظر افزایش تفاهم و همین‌طور از نظر اعتمادسازی به‌حساب می‌آمد و درواقع، جلسات متعدد برگزارشده این افراد برای اعتمادسازی و افزایش تفاهم میان کشورهای عضو در مورد نحوه رسیدگی به حوادث سایبری اهمیت بسیاری داشت (Ibid., p.33). در مجموع، به‌رغم اینکه توصیه‌های مربوط به مسائل آمادگی، طرح و سازماندهی پیش از مانور (برای مثال، در مورد نحوه شمول بخش خصوصی در مانورهای آتی) از منظر امنیت تاب‌آور تأکید بر این نکته داشتند که «رویه‌های مربوط به نحوه رسیدگی به حوادث سایبری کماکان در سطح رویکرد اروپایی وجود ندارند» (ENISA, 2011a, p.9)، این مانور که با هدف اعتمادسازی، درک و تبادل اطلاعات انجام می‌شد، گام مهمی برای انجام اصلاحات آتی تلقی می‌گردید. به گفته یکی از مقامات آژانس امنیت شبکه و اطلاعات اتحادیه اروپا، این مانور «سودمندی واقعی خود برای همگان را نشان داد، [به‌واسطه انجام این مانور مشترک بود که] شناخت کاملی از یکدیگر در اروپا به دست آوردیم» (Interview, ENISA official, July 2012).

دومین مانور امنیت سایبری، در اصل از تجربیات اصلی فراگرفته‌شده از نخستین مانور، به‌خصوص از مورد شمول بخش خصوصی بهره برد. این موضوع بدین معنا بود که در کنار کشورهای عضو اتحادیه اروپا، کشورهای عضو انجمن تجارت آزاد اروپا[1] (۲۹ کشور) و مشارکت نهادی اتحادیه اروپا، ۳۳۹ سازمان [در این مانور] در کنار بازیگران خصوصی و دولتی در سطح ملی و همکاری بین‌المللی بازیگران دولتی شرکت داشتند (ENISA 2012c, p.4). تمام بازیگران حاضر (۸۸ درصد) این مانور را تجربه مثبتی قلمداد کردند، اما این مانور چند مسئله مهم برای تقویت امنیت تاب‌آور در درون و سرتاسر اروپا و در سطح بین‌المللی را نیز نشان داد. برای مثال، با وجود همکاری مناسب بازیگران دولتی و خصوصی در سطح ملی در طی برگزاری

1. European Free Trade Association (EFTA)

مانور، اما این همکاری به دلیل وجود سازماندهی و رویه‌های متفاوت کشورها دشوار بود. در ضمن بازیگران دولتی برای برخورد با موقعیت‌های بحرانی (برای مثال، انتخاب مسائلی که در سطح راهبردی باید مطرح شوند) باید در مورد مسائلی تصمیم می‌گرفتند. بااینکه اعتماد بین مشارکت‌کنندگان اصلی مربوطه در سطح همکاری بین‌المللی ایجاد گردید، مسائلی پیرامون ارتقای دانش در مورد رویه‌های عملیاتی جهت همکاری کارآمدتر با آن‌ها، نحوه شمول بخش خصوصی به‌صورت اصولی‌تر، مقیاس‌پذیری و اثربخشی سازوکارهای موجود و جریان اطلاعات برای همکاری و شمول و مشارکت سایر بازیگران مهم اروپایی در رسیدگی به وضعیت‌های بحرانی (برای مثال، حمل‌ونقل) مطرح شدند (Ibid., p.9-10). در مجموع، این مانور سودمند تلقی می‌شد، مانوری کارآمد به‌عنوان محل تقویت یادگیری در سطوح راهبردی، عملیاتی، سیاسی (نهادی) و فنی که باید کماکان به‌عنوان ابزار اصلی تقویت دانش، تفاهم و اعتمادسازی میان طرف‌های ذینفع به کار رود.

درنهایت، اتحادیه اروپا سندی را در مارس ۲۰۱۱ در مورد تعریف اصول و دستورالعمل‌ها در زمینه تاب‌آوری و ثبات اینترنت منتشر کرد که حاصل بحث و مشورت در مجمع اروپایی کشورهای عضو بود. این نتیجه بازتاب ابعاد مثبت و منفی چنین مجمعی است؛ بدین معنی که این مجمع کارکرد ارزشمندی در زمینه ارائه بیانیه‌های کلی درباره اصول امنیت و تاب‌آوری سایبری دارد، اما احتمالاً در زمینه عناصر خرد مربوط به همکاری و تشریک‌مساعی کارآمد طرف‌های ذینفع یا مسائل خاصی نظیر تبادل اخبار و اطلاعات، از ارزش کمتری برخوردار است. از دید مثبت، این سند دستورالعمل‌ها و اصول مشخصی را تعریف می‌کند که بر مبنای هنجاری سیاست اتحادیه اروپا در زمینه تاب‌آوری و ثبات اینترنت تأکید دارد، اما به شیوه‌های فنی، راهبردی و عملیاتیِ دستیابی به آن نمی‌پردازد که در راهبرد امنیت سایبری اتحادیه اروپا مطرح شده است. این سند بیانیه سیاسی روشنی در مورد بایدها و نبایدهای ماهیت اینترنت و حکمرانی لازم برای تأمین امنیت آن به شمار می‌آید. ازاین‌رو، اتحادیه اروپا اینترنت جهانی را به‌عنوان خیری همگانی یا جمعی تلقی می‌کند که باید در دسترس همگان باشد. دیدگاه هنجاری مبنی بر این وجود دارد که کاربرد اینترنت نباید برای هیچ شهروندی ممنوع و محدود

باشد، تنها مورد استثنا اقدامات و ابزارهای به‌کاررفته برای جلوگیری از آسیب‌رسانی به دیگران است. علاوه بر این، بدیهی است ارزش‌ها، قوانین و هنجارهای اصلی اتحادیه اروپا محور اقدامات برخط و برون‌خط در حوزه امنیت سایبری محسوب می‌شوند و «امنیت سایبری تنها در صورتی جامع و کارآمد به شمار می‌آید که بر اساس حقوق و آزادی‌های بنیادی باشد که در منشور حقوق اساسی اتحادیه اروپا لحاظ شده است...» (EUCSS 2013, p.4).

گذشته از این موضوع، اتحادیه اروپا طرح بسیار روشنی در مورد الگوی حق انتخاب حکمرانی برای اینترنت و سیاست امنیت سایبری دارد که چندجانبه‌گرایی است (ن.ک. European Commission 2009b; and EUCSS). البته این الگو نیز بحث‌برانگیز است. با اینکه دیدگاه چندجانبه به دلیل پیچیدگی اینترنت ازنظر حضور بازیگران بی‌شمار دخیل در موضوع مدیریت و به‌کارگیری آن ایجاد شده است و این دیدگاه در کشورهای غربی بسیاری (برای مثال، آمریکا، ژاپن، کانادا و استرالیا) ملاحظه می‌شود، اما کشورهای زیادی (برای مثال، ایران، روسیه، چین و هند) نیز مخالف آن هستند، چراکه ازنظر این کشورها: الف) آمریکا قدرت بیش‌ازحدی در مدیریت اینترنت دارد؛ ب) آن‌ها نقش چندانی در نهادهای حکمرانی اینترنت جهانی کنونی ندارند و خواستار مداخله دولتی بسیار بیشتری در فضای سایبری از طریق اتحادیه بین‌المللی مخابرات، یعنی اتخاذ رویکرد فراحکمرانی عملی سنتی به‌جای رویکرد چندجانبه هستند (ن.ک. فصل ۳).

به‌علاوه، اهمیت مشارکت تمام طرف‌های ذینفع در اصل مسئولیت مشترک اتحادیه اروپا برای تأمین امنیت سایبری کارآمد، نیز ملاحظه می‌شود. از این نظر، این اصل در تمام اصول و دستورالعمل‌های دیگر ازجمله بهبود آموزش و افزایش آگاهی، همکاری و کمک متقابل داخلی در اتحادیه اروپا، ایجاد صنعت فناوری اطلاعات و ارتباطات قدرتمندی در اروپا (تضمین تنوع محصولات)، مدیریت مناسب خطرات و ساخت و پذیرش استانداردهای باز در کنار تأمین امنیت و حریم خصوصی ایجادشده از مرحله طراحی است که اتحادیه اروپا آن‌ها را به‌عنوان اصول مهمی برای تاب‌آوری و ثبات اینترنت مطرح می‌کند (European Principles and Guidelines 2011). تأکید اتحادیه اروپا بر زمینه جهانی و همکاری بین‌المللی نیز حائز اهمیت است. اتحادیه اروپا از این امر کاملاً آگاهی دارد

که اصول آن در زمینه تأمین امنیت سایبری جدا از اصول دیگر نیست و بدون همکاری و تشریک‌مساعی با شرکای بین‌المللی دولتی و خصوصی برای ایجاد اصول جهانی منطبق با ارزش‌های اتحادیه اروپا، اقدامات این اتحادیه برای اتخاذ سیاست امنیت سایبری تاب‌آور خاص خود و همچنین ثبات و قابلیت همکاری اینترنت اساساً تضعیف می‌شود.

برای مثال، مخالفت و اعتراض جهانی نسبت به نقش استانداردهای فنی، حفاظت از داده‌ها و حریم خصوصی که باید بر اینترنت کنترل و نظارت داشته باشند و علیه کنوانسیون‌ها و پروتکل‌های حقوقی مناسب برای مقابله با جرائم سایبری و حملات سایبری می‌تواند هر اقدام صورت‌گرفته برای ایجاد فضای سایبری امن و تاب‌آور برای همگان را تضعیف نماید. به‌رغم حمایت اساسی اتحادیه اروپا از رویکرد چندجانبه برای حکمرانی جهان سایبری، مسلماً مقامات دولتی نقش مهمی در ارائه چارچوب حقوقی و هنجاری فعالیت‌های تمام طرف‌های ذینفع ایفا می‌کنند. به‌عبارت‌دیگر، اتحادیه اروپا از نوع خاصی مشارکت عمومی- خصوصی در چارچوب چندجانبه‌گرایی حمایت می‌کند که در آن مقامات دولتی باید (با مشاوره طرف‌های ذینفع مربوطه) در مورد شیوه‌ها و اشکال حکمرانی و نظارت (برای مثال، انگیزه‌ها) تصمیم بگیرند و بخش خصوصی نیز نقش روزمره مهمی در مدیریت اینترنت و امنیت آن دارد (European principles and guidelines 2011; EUCSS 2013, 3). از این نظر، اتحادیه اروپا به‌خصوص در دوره پس از افشاگری‌های اسنودن از حضور پررنگ‌تر کمیته مشورتی دولت در آیکان، برای تفویض نقش تصمیم‌گیری مهم‌تری به آن در زمینه سیاست‌های مربوط به حکمرانی اینترنت حمایت کرده است.[۱۸]

امنیت شبکه و اطلاعات در راهبرد امنیت سایبری اتحادیه اروپا: دستیابی به تاب‌آوری سایبری؟

دیدگاه فوق در مورد دست‌یابی به تاب‌آوری، کاملاً در طرح پیشنهادی برای امریه امنیت شبکه و اطلاعات بازتاب یافته است که منضم به راهبرد امنیت سایبری اتحادیه اروپا می‌باشد. درواقع، این امریه تصریح می‌کند که این تغییر قابل‌ملاحظه‌ای (European Commission 2013a 4),

از رویکرد فراحکمرانی نظری به موضع الزام‌آور عملی‌تری در قبال بهبود توانایی مقابله با حوادث مهم سایبری و مدیریت خطرات و گزارش آن‌ها محسوب می‌شود. این امریه برخلاف چارچوب امریه ارتباطات الکترونیکی (۲۰۰۹)، تنها برای تأمین‌کنندگان مخابرات و بخش کنترل‌کنندگان داده‌ها نیست، بلکه برای تمام بخش‌های مالک زیرساخت‌های حیاتی (انرژی، بانکداری، حمل‌ونقل، بورس، مدیریت دولتی) الزام‌آور است. همان‌طور که در راهبرد امنیت سایبری اتحادیه اروپا (۲۰۱۳) آمده است، به‌رغم دستیابی به پیشرفت در توافقی داوطلبانه‌تر در زمینه ایجاد فرهنگ امنیت سایبری، «اختلافات اتحادیه اروپا باقی ماند» و بازیگران خصوصی از «انگیزه کافی برای ارائه داده‌های موثق در مورد وجود یا تأثیر حوادث مربوط به امنیت شبکه و اطلاعات، پذیرش فرهنگ مدیریت خطرات یا سرمایه‌گذاری در راه‌حل‌های امنیتی برخوردار نیستند» (EUCSS 2013, 5). طرح پیشنهادی امریه امنیت شبکه و اطلاعات (European Commission 2013a, 3) به‌روشنی مؤید این موضوع است که «وضعیت کنونی اتحادیه اروپا تاکنون بیانگر اتخاذ رویکرد کاملاً داوطلبانه بوده است که امنیت شبکه و اطلاعات را در برابر حوادث و خطرات در اتحادیه اروپا به‌اندازه کافی تأمین نمی‌کند.»

امریه امنیت شبکه و اطلاعات و رویکرد نظارتی (حکمرانی) اتخاذشده در آن به‌عنوان مناسب‌ترین گزینه[۱۹] برای ایجاد انگیزه در دولت‌ها و واحدهای تجاری، با هدف به‌کارگیری روش‌هایی ایجاد شد که منجر به تأمین امنیت تاب‌آور کارآمدتری از طریق الزام کشورهای عضو به تضمین کسب میزان آمادگی نهادی کافی مانند [تعیین] مقامات ذی‌صلاح برای تأمین امنیت شبکه و اطلاعات و [تشکیل] تیم کارآمد واکنش اضطراری رایانه‌ای در سطح ملی/دولتی؛ ایجاد سازوکارهای پیشگیری، شناسایی، کاهش [جرائم سایبری] و واکنش‌دهی برای ایجاد امکان اشتراک اطلاعات و کمک متقابل در میان مقامات ملی ذی‌صلاح امنیت شبکه و اطلاعات و در مورد دوم، تضمین همکاری گسترده اتحادیه اروپا بر اساس طرح اقدام امنیت شبکه و اطلاعات اتحادیه اروپا جهت واکنش‌دهی به حوادث مربوط به امنیت شبکه و اطلاعات برون‌مرزی و افزایش تعهد و آمادگی بخش خصوصی به‌واسطه موظف سازی آن به گزارش حوادث مهم مربوط به امنیت شبکه و اطلاعات به مقامات ملی ذی‌صلاح امنیت شبکه و اطلاعات تلقی می‌شد

(European Commission 2013a; EUCSS 2013). این فرض مبنای منطق کلی این امریه است که «موظف سازی» کشورهای عضو به آماده‌سازی و برخورداری از توانایی و موظف‌سازی بازیگران خصوصی و بخش‌های مدیریت دولتی مربوطه به گزارش رویدادها به نحو بهتری موجب ایجاد فضای اعتماد متقابل و ازاین‌رو، همکاری و مشارکت کارآمدتری در داخل و بین بخش‌های خصوصی و دولتی می‌گردد. یعنی، این موضوع عملکرد بهتری در تسهیل و ایجاد شرایط لازم برای تأمین امنیت تاب‌آور دارد. درعین‌حال، این کمیسیون کاربرد و سودمندی دائمی مجاری اشتراک اطلاعات غیررسمی و موثق بین طرف‌های ذی‌نفع مربوطه را برای بهبود امنیت و تبادل اطلاعات و اقدام مناسب تأیید و تشویق می‌کند.

احتمالاً این مسئله جای تعجب ندارد که امریه امنیت شبکه و اطلاعات از حمایت عمومی در مورد اصل حفاظت از امنیت شبکه و اطلاعات در برابر تهدیدها برخوردار است، اما با انتقادات بسیاری نیز در مورد جزئیات نحوه اجرای آن روبه‌رو شده است. این انتقادات تنها از جانب صنایع خصوصی مطرح نشده‌اند، بلکه دولت‌ها و دیگر نهادهای اتحادیه اروپا، به‌خصوص پارلمان اروپا نیز آن‌ها را مطرح کرده‌اند و این موضوع موجب انجام بازبینی اساسی و حتی می‌توان ادعا کرد، تضعیف عامدانه این امریه گردید. برای مثال، هدف امریه اصلی، شمول تمام بخش‌ها و بازیگران دخیل در حفاظت از زیرساخت‌های حیاتی بود. اگرچه، به نظر برخی کشورهای عضو، امریه امنیت شبکه و اطلاعات برگرفته از حکم بازار داخلی، مبنای قانونی مناسبی برای بخش‌های مدیریت دولتی به دلیل توجه آن به مسائل احتمالاً «ازنظر امنیتی حساس» نبود. به‌خصوص آلمان اصرار بر حذف بخش‌های مدیریت دولتی از فهرست بازیگران تحت حکمرانی امریه امنیت شبکه و اطلاعات داشت که موفق به انجام آن نیز گردید. به گفته یکی از اعضای کمیته حمایت از بازار داخلی و مصرف‌کنندگان[1] پارلمان اروپا، به دنبال نگرانی‌های مطرح‌شده در مورد دامنه [این امریه] و فقدان جزئیات درباره نحوه اجرای آن، این کمیته نیز «درصدد اتخاذ راهبرد برای مبهم سازی آن بود» (Informal meeting, Brussels, February 2013). به‌خصوص، اعضای این کمیته با حذف «فعال‌کنندگان اینترنت»[۲۰] از فهرست موجب تقلیل این دامنه با

1. Internal Market and Consumer Protection (IMCO) Committee

این استدلال شدند که این مورد غیرضروری و چالش‌برانگیز است و توجیه کاملی نیز ندارد (برای مثال، دلیل شمول فعال‌کنندگان اینترنت و عدم شمول تولیدکنندگان نرم‌افزار/سخت‌افزار) و ازنظر حکمرانی، ایجاد روابط مبتنی بر اعتماد داوطلبانه سودمندتر از اتخاذ رویکردی الزام‌آور است.

جدا از این ابعاد خاص، کماکان اختلافاتی میان و بین صنایع و دولت‌ها در خصوص الگوی حکمرانی اتخاذشده برای تأمین امنیت سایبری تاب‌آور وجود دارد. این مسئله ابعاد گوناگونی دارد. نخست، موضوع هزینه مطرح است که از منطق اقتصادی کاربردی حاکم بر بخش‌های مربوطه ناشی می‌شود. این موضوع به پیامدهای مالی مدیریت سیستم گزارش‌دهی اجباری و مسائلی نظیر حدود گزارش‌دهی، اطلاعات در زمینه اختیارات مقامات ملی ذی‌صلاح و پیامدهای ناخواسته دیگر مربوط می‌شود که مهم‌ترین آن‌ها عبارت است از: ترویج فرهنگ اطاعت و حسابرسی محدود به‌جای ترویج فرهنگ امنیت سایبری کارآمدتر و مؤثرتر. بر اساس گزارش واکنش‌ها نسبت به امریه امنیت شبکه و اطلاعات در بریتانیا، «طرف‌های ذی‌نفع بر این امر تأکید داشتند که گزارش‌دهی اجباری به فرهنگ اطاعتی می‌انجامد و این امر منجر به کاهش اشتراک داوطلبانه اطلاعات و منابع احتمالاً تخصیص‌یافته در توسعه توانمندی امنیت سایبری می‌شود که در استخدام گروه‌های حقوقی برای تحلیل هر رویداد، مجدداً اختصاص می‌یابند» (UK Department of Business Innovation and Skills Report September 2013, p.23). مورد دوم و مرتبط با آن، ترس از تأثیر منفی امریه امنیت شبکه و اطلاعات بر فرهنگ گفتمان بخش‌های دولتی و خصوصی است. برخی آن را دور شدن از گفتمان و همکاری در جهت تعهد از بالا به پایین به گزارش‌دهی اجباری تلقی می‌کنند که می‌تواند مسیر منابع را از اقدامات امنیتی مؤثر منحرف نماید و منافع شرکت‌ها را از تبادل [اطلاعات] (غیررسمی) دوطرفه داوطلبانه کاهش دهد که این موضوع منجر به بهبود درک تهدیدهای جدید و واکنش به حوادث می‌شود. این استدلال نیز مطرح است که در صورت دشواری گزارش‌دهی اجباری، این موضوع باعث کاهش اعتماد درزمانی می‌شود که اشتراک لحظه‌ای اطلاعات و واکنش‌دهی جمعی حیاتی است. این مقوله در دوره پس از افشاگری‌های اسنودن اهمیت بیشتری یافته است، چراکه اعتماد

و اطمینان چندانی در خصوص اشتراک اطلاعات از بخش خصوصی به دولتی وجود ندارد.

استدلال بالا مهم است، چراکه امریه امنیت شبکه و اطلاعات بر مبنای این فرض اصلی است که رویکرد عملی اجباری از طریق الزام و محدودسازی موجب تأمین امنیت تاب‌آور با بیشترین کارآمدی می‌گردد. این فرض که به نظر کمیسیون، موردحمایت بخش قابل‌توجهی از افرادی است که در مورد سودمندی الزام گزارش‌دهی و ایجاد توانمندی مورد مشورت قرار گرفتند (ن.ک. European commission 2013b) نیز زیر سؤال رفته است. شاید یکی از دلایل این مسئله این باشد که تنها بخش کوچکی از این پاسخگویان (تقریباً ۱۵ درصد) واقعاً در بخش‌های تحت تأثیر این امریه مشغول به کار بودند (UK Department of Business Innovation and Skills Report September 2013, p.14). ازاین‌رو، به‌رغم پشتیبانی اکثر پاسخ‌دهندگان از تقویت توانمندی‌های امنیت شبکه و اطلاعات در سرتاسر اروپا و انجام اقداماتی نظیر تشکیل تیم واکنش اضطراری رایانه‌ای و [تعیین] مقامات ذی‌صلاح امنیت شبکه و اطلاعات، ظاهراً اجماع چندانی در میان بخش‌هایی که مستقیماً تحت تأثیر این امریه قرار گرفتند، در مورد اینکه آیا گزارش‌دهی اجباری موجب تأمین امنیت تاب‌آور کارآمدتری می‌شود یا خیر، وجود ندارد. ازاین‌رو، مدارک ارائه‌شده در این زمینه کافی نیست، گرچه، بعضی بخش‌های صنعتیِ برخی اعضای اتحادیه اروپا استدلال محکمی را مبنی بر این مطرح می‌کنند که رویکرد داوطلبانه و خاص از پویایی بسیار بیشتری برخوردار است و مبنای آن نیز رابطه‌ای غیررسمی و مبتنی بر اعتماد است. از این نظر، نقطه تقابل استدلال مطرح‌شده در این زمینه در دستورالعمل امنیت شبکه و اطلاعات این است که چنین ترتیبی باید از طریق اتخاذ رویکرد ترکیبی (نظارتی و داوطلبانه) اصولی‌تر گردد تا شاهد بهبود توانمندی‌ها و گزارش‌دهی در سرتاسر اروپا باشیم (Interview, UK official, October 2014).

درنهایت، مسائل گسترده‌تر دیگری نیز بر حدود نقش این امریه در بهبود امنیت تاب‌آور اروپا تأثیر می‌گذارند. نخستین مورد، مربوط به گروه‌های واکنش اضطراری رایانه‌ای است. در حال حاضر، بیش از صد گروه –خصوصی و عمومی– واکنش اضطراری رایانه‌ای در کل اروپا وجود دارد و امریه امنیت شبکه و اطلاعات به‌منظور بهبود توانمندی، همکاری و مشارکت، تمام

کشورهای عضو اتحادیه اروپا را ملزم به تشکیل تیم واکنش اضطراری رایانه‌ای دولتی یا ملی با عملکرد مناسبی کرده است. همچنین پیشنهادی در موردبررسی امکان تشکیل چنین تیمی برای سیستم‌های کنترل صنعتی مطرح شده است. اگرچه، برخلاف چنین پیشرفتی، مسئله نقش امریه امنیت شبکه و اطلاعات در رسیدگی به کیفیت این گروه ایجاد شده و به‌خصوص نحوه ایجاد انگیزه در آن برای ایفای نقشی فعال به‌جای منفعل کماکان مشخص نیست. ازنظر آژانس امنیت شبکه و اطلاعات اتحادیه اروپا «متداول‌ترین رویکرد تیم واکنش اضطراری رایانه‌ای برای رسیدگی به حوادث امنیتی، انتظار برای گزارش حوادث بعدی و سپس «پرداختن» به تأثیرات حملات و نه لزوماً به «علت» آن‌ها است. بدین ترتیب، حادثه از قبل رخ داده و احتمالاً بر محیط تولید تأثیر گذاشته است» (ENISA 2011b).

مشکلات دیگری نیز در مورد رفتار منفعلانه گروه‌های واکنش اضطراری رایانه‌ای وجود دارد که باید به آن‌ها رسیدگی شود تا این گروه‌ها عملکرد کارآمدتری داشته باشند. این مشکلات عبارت‌اند از: عدم به‌کارگیری تمام اطلاعات در دسترس این گروه‌ها از منابع خارجی، عدم جمع‌آوری داده‌های مربوط به حوادث از حوزه‌های دیگر و کیفیت پایین داده‌های جمع‌آوری‌شده و مشکلات قانونی مانند موارد نظارت بر حفاظت از حریم خصوصی و داده‌ها که می‌توانند مانع از تبادل اطلاعات مربوطه شوند. این موضوع، مسلماً، در مورد اهداف دستورالعمل امنیت شبکه و اطلاعات در دوره پس از افشاگری‌های اسنودن، به‌خصوص درباره مسئله اختلاف‌نظر احتمالی در مورد قانون اصلاح‌شده حفاظت از داده‌های اتحادیه اروپا مطرح شده است. بی‌شک تبادل اطلاعات به‌عنوان بخشی از یکی از شرایط لازم برای کسب امنیت تاب‌آور کارآمد حیاتی است که این موضوع صرفاً در مورد گروه‌های واکنش اضطراری رایانه‌ای صدق نمی‌کند، بلکه در مورد کل طیف‌ها، لایه‌ها و بازیگران مختلف دخیل در تأمین امنیت سایبری تاب‌آور، صادق است. حدود توانایی اتحادیه اروپا و آژانس امنیت شبکه و اطلاعات اتحادیه اروپا در ترغیب این گروه‌ها از طریق راهبرد امنیت سایبری اتحادیه اروپا و امریه امنیت شبکه و اطلاعات به اعمال تغییرات لازم و ظرفیت‌سازی جهت برخورداری از عملکرد کارآمدتر مشخص نیست.

دوم، امریه امنیت شبکه و اطلاعات در زمینه مسائلی نظیر گزارش‌دهی در اکوسیستم پیچیده‌تر

محاسبات ابری چنان شفاف نیست. درواقع، این امریه مسئولیت گزارش تخلفات در حیطه کنترل را برعهده مقامات ملی ذی‌صلاح و بازیگران دولتی و خصوصی مربوطه می‌گذارد، حتی اگر آن‌ها خارج از اتحادیه اروپا باشند و این موضوع زمانی پیچیده‌تر می‌شود که برای مثال، کشوری سرویس مورداستفاده آن‌ها را تأمین کند که از استانداردهای اروپا پیروی نمی‌کند. در این صورت، مقامات ملی ذی‌صلاح مربوطه یا بازیگران دولتی و/یا خصوصی از این دستورالعمل تبعیت نمی‌کنند، چراکه هیچ الزامی برای امضای موافقت‌نامه چارچوبی بین نهاد اتحادیه اروپا و شرکت‌های تأمین‌کننده خدمات در دیگر کشورها وجود ندارد. این مسئله که تمام کشورها چارچوب جهانی (مانند کنوانسیون بوداپست) را برای مقابله با جرائم سایبری (شامل حملات سایبری به سیستم‌های اطلاعاتی) امضا نکرده‌اند، این مشکل را تشدید می‌کند. سوم، مسئله ایجاد استانداردی مشترک برای گزارش‌دهی و ضرورت اجرای هماهنگ دستورالعمل جهت جلوگیری از تفرقه مطرح است. در اینجا آژانس امنیت شبکه و اطلاعات اتحادیه اروپا نقش اصلی در تسهیل اجرای کارآمد و برقراری و تضمین استقرار و عملکرد سیستم گزارش‌دهی مشترک طبق ماده ۱۳a امریه مخابرات و ماده ۴ امریه حریم خصوصی الکترونیک ایفا می‌کند. بااین‌وجود، کماکان نگرانی‌هایی درباره ویژگی‌های اشتراک اطلاعات موردنیاز این دستورالعمل، به‌خصوص محتوای اطلاعات به اشتراک گذاشته‌شده، نحوه به‌کارگیری اطلاعات و تأثیر این موضوع بر اشتراک داده‌های موجود و جمع‌آوری اطلاعات وجود دارد (Informal meeting, Brussels, February 2013).

درنهایت، مسئله حدود اختلاف رویکرد حکمرانی اتخاذشده توسط دستورالعمل امنیت شبکه و اطلاعات و رویکرد داوطلبانه آمریکا به‌رغم اقدامات انجام‌گرفته جهت تصویب قانون امنیت سایبری موردحمایت دولت در نوامبر ۲۰۱۲ مطرح است که این موضوع با مخالفت شدید گروه‌های تجاری مواجه گردید که از نظارت بیش‌ازحد شکایت داشتند. پیامد اصلی این مسئله این است که برخلاف همکاری کارگروه‌های اتحادیه اروپا و آمریکا در زمینه جرائم، امنیت و گفتمان سایبری طرفین (ن.ک. فصل ۷)، مسلماً قوانین متفاوتی در اروپا و ایالات‌متحده در خصوص الزام گزارشدهی وجود دارد. این مسئله باعث ایجاد اختلاف در آن دسته از شرکت‌هایی

می‌شود که در هر دو حوزه قانونی قرار دارند. در این میان، پیامدها و عواقبی نیز ازنظر اعتماد و همکاری ایجاد می‌گردد. این امر مانع مهمی بر سر راه مذاکرات پیرامون تجارت آزاد بین اروپا و آمریکا در آینده نزدیک محسوب می‌شود.

دفاع سایبری اتحادیه اروپا: در دست ساخت؟

در بازبینی راهبرد امنیت سایبری اتحادیه اروپا توسط این اتحادیه پس از نخستین سال طرح آن، بعد دفاع سایبری، بیشتر در قالب «در حال ایجاد» ارزیابی شد. با توجه به اولویت پایین حوزه دفاع سایبری که البته برای تأمین امنیت تاب‌آور کارآمد اروپا، حوزه ضروری محسوب می‌شود، هدف از شمول این بعد در راهبرد امنیت سایبری اتحادیه اروپا توانمندسازی این اتحادیه به اتخاذ رویکردی «فراگیر» یا «در کل اتحادیه» در قبال امنیت سایبری بود. بدیهی است که عملکردها، فرآیندها و اقدامات حیاتی نظامی وابسته به حوزه سایبری و به‌خصوص به زیرساخت‌ها و فرآیندهای حیاتی غیرنظامی هستند. این موضوع در کنار رشد پایدار و سریع شبکه‌های پیچیده و مرتبط، به معنای وجود موارد آسیب‌پذیری و تهدیدات جدیدی بود که باید مورد رسیدگی قرار گیرند تا ارزش عملکرد روزانه مطمئن و کارآمدی داشته باشد. بدین منظور، دفاع سایبری حوزه‌ای با ۱۰ اولویت مهم در طرح توسعه توانمندی آژانس دفاع اتحادیه اروپا[1] در سال ۲۰۱۱ محسوب می‌شد که برای ایجاد این حوزه، چند وظیفه ازجمله انجام مطالعات با چشم‌انداز دفاع سایبری، توسعه برنامه آموزشی دفاع سایبری، ارزیابی امکان تأسیس مرکز اروپایی دفاع سایبری[2] و پیگیری پژوهش‌ها و اقدامات آموزشی مربوطه برای آن تعیین گردید (Cirlig 2014; Roehrig 2014). کشورهای عضو اتحادیه اروپا در مورد مفهوم اتحادیه اروپا از دفاع سایبری در عملیات‌های تحت رهبری این اتحادیه در سال ۲۰۱۲ به توافق رسیدند که این مسئله به فرماندهان عملیاتی اجازه می‌دهد آگاهی سایبری بر حسب موقعیت را خلق و حفظ کنند. شورای سران اتحادیه اروپا نیز در جلسه دسامبر ۲۰۱۳ (European Council Conclusions December 2013) در مباحث خود در زمینه دفاع سایبری، بر ضرورت

1. EDA Capability Development Plan (CDP)
2. European Cyber Defence Centre (ECDC)

تداوم و تحول کار در پنج حوزه اصلی تأکید کرد:

۱. ارتقای توسعه توانمندی‌ها، پژوهش‌ها و فناوری‌های دفاع سایبری اتحادیه اروپا از طریق برنامه دفاع سایبری آژانس دفاع اتحادیه اروپا

۲. ایجاد چارچوب سیاست‌گذاری دفاع سایبری جهت حفاظت از شبکه‌های پشتیبان نهادها، مأموریت‌ها و عملیات‌های سیاست امنیتی و دفاعی مشترک

۳. بهبود آموزش، تعلیم و [ایجاد] فرصت‌های مانور سایبری برای کشورهای عضو

۴. تقویت همکاری با ناتو و سایر سازمان‌های بین‌المللی، بخش خصوصی و محافل دانشگاهی

۵. ایجاد سازوکارهای واکنش‌دهی و هشدار زودهنگام و ایجاد هم‌افزایی بین بازیگران امنیت سایبری مربوطه در اروپا

در همان جلسه، به کاترین اشتون[1]، نماینده عالی وقت اتحادیه اروپا، وظیفه همکاری با کمیسیون اروپا و آژانس دفاع اتحادیه اروپا جهت ایجاد چارچوب سیاست‌گذاری دفاع سایبری اتحادیه اروپا محول شد که اقدامات فوق در آن اجرا می‌شد. نقش آژانس دفاع اتحادیه اروپا در این مورد بسیار حائز اهمیت بود: توجه به تعلیم، افزایش آگاهی سایبری بر حسب موقعیت، بهبود همکاری بین بخش‌های نظامی و غیرنظامی، حفاظت از دارایی‌های اتحادیه اروپا در طول مأموریت‌ها و عملیات‌ها و ابعاد فناورانه.

شایان‌ذکر است که منظور از دفاع سایبری در اتحادیه اروپا، توسعه توانمندی تهاجمی سایبری (مانند مورد آمریکا) نیست، بلکه منظور «خودحفاظتی سایبری و تضمین دسترسی به فضای سایبری برای انجام اقدامات نظامی معمول است» (Roehrig and Smeaton 2013, 24). نقطه آغاز اصلی درک اقدامات در زمینه دفاع سایبری، دستیابی به فهمی بهتر از توانمندی‌های کل اروپا بود. جهت تحقق این امر، آژانس دفاع اتحادیه اروپا دستور انجام پژوهشی را صادر کرد که ۲۰ کشور عضو اتحادیه اروپا (آژانس دفاع اتحادیه اروپا) را پوشش می‌داد.[۲۱] این پژوهش

1. Catherine Ashton

به تحلیل توانمندی‌های دفاع سایبری در سطح ملی و در سطح سازمان‌های اروپایی فعال در امور دفاع سایبری در مأموریت‌های سیاست امنیتی و دفاعی مشترک اتحادیه اروپا[۲۲] پرداخت (Cyber Defence Fact Sheet 2013). از منظر امنیت تاب‌آور، این یافته‌ها حاکی از این است که به‌رغم تأمین حتمی شرایط اصلی، کماکان مشکلات بسیاری وجود دارد. برای مثال، این مسئله مطرح می‌شود که در سطح اتحادیه اروپا توانمندی تحلیل تهدید و جمع‌آوری اطلاعات در حال ظهور است و ساختار سازمانی پیچیده (یعنی آژانس دفاع اتحادیه اروپا، سرویس اقدام خارجی اتحادیه اروپا، دبیرخانه عمومی شورای سران اتحادیه اروپا، شورای وزیران، کمیسیون اروپا، آژانس امنیت شبکه و اطلاعات اتحادیه اروپا، مرکز مقابله با جرائم سایبری اتحادیه اروپا و تیم واکنش اضطراری رایانه‌ای) باید واکنش مناسب‌تری در سطح عملیاتی نسبت به حوادث نشان دهند. به‌علاوه، این مسئله مشخص شد که دانش و درک چندانی در مورد استانداردها و ابزارهای خاص نظامی وجود ندارد و فرهنگ اقدام مناسب امنیت سایبری، باید ایجاد شود تا آن را کارآمدتر سازد (Cyber Defence Fact Sheet 2013).

در سطح کشورهای عضو اتحادیه اروپا، این تصویر بیانگر میزان آمادگی کلی حوزه امنیت سایبری است. بدین معنی که به‌رغم پیشرفت ۲۰ کشور عضو مورد ارزیابی در اروپا، کماکان توانمندی بسیار متنوع و ازاین‌رو، جای پیشرفت زیادی وجود دارد. در این پژوهش توانمندی در شش حوزه اصلی[۲۳] بررسی شد که عبارت‌اند از: رهبری، کارکنان، قابلیت همکاری، دکترین، سازمان‌دهی، آموزش و امکانات. در مجموع، نتایج نشان می‌دهد کشورهای عضو برخوردار از تصمیم‌گیرندگان باتجربه در مورد امنیت سایبری، به پیشرفت بیشتری نیز در زمینه توانمندی دفاع سایبری دست یافته‌اند. به‌ویژه، این پژوهش این مسئله را نیز نشان داد که قدرت این ۲۰ کشور عضو در حوزه‌های رهبری، کارکنان و قابلیت همکاری قرار داشت و شایان‌ذکر است که گزارش هیچ یک از کشورها حاکی از سطح پایین آشنایی تصمیم‌گیرندگان اصلی نظامی با مسائل دفاع سایبری نبود. اگرچه، سطوح درک و تجربه در حوزه‌های دکترین، سازمان‌دهی و آموزش، پایین‌تر بود. احتمالاً دلیل این تفاوت این است که در مورد دوم به ساختارها و فرآیندهای سازمانی بلندمدت‌تر و پیچیده‌تری نیاز است. گزارش‌ها در زمینه امکانات، حاکی از

این بود که این حوزه چندان توسعه نیافته و عملاً در بسیاری از موارد پیشرفتی در آن صورت نگرفته است (Cyber Defence Fact Sheet 2013; Robinson et al. 2013).

برای تشریح بیشتر این موضوع، باید بیان کرد که کشورهای شرکت‌کننده از اتحادیه اروپا- در این پژوهش مسلماً با مشکلاتی در مورد ابعاد دکترینی نقش ارتش در دفاع از فضای سایبری برخورد کرده‌اند. آن‌ها درخصوص عملکرد ارتش در حوزه دفاع سایبری و رابطه بین راهبردهای امنیت سایبری ملی کلی‌تر و دکترین‌های دفاع سایبری ارتش اطلاعات چندانی ندارند یا این اطلاعات حداقل برای آن‌ها چندان واضح نیست. گذشته از این، برخی کشورهای اتحادیه اروپا فرانسه و هلند – که دارای تفکر امنیت سایبری پیشرفته‌ای تلقی می‌شوند، گروه‌های نظامی واکنش اضطراری رایانه‌ای را تشکیل داده‌اند و با توجه به عملکرد سازمان‌های دفاع سایبری پویاتر، در مراحل گوناگون ارزیابی و اجرا قرار دارند (Robinson 2014, p.2). اعضای اتحادیه اروپا و درواقع خود اتحادیه اروپا در سطح پیشرفته‌ای ازنظر طرح دکترین دفاع سایبری قرار ندارند و ترغیب به بهبود این وضعیت با همکاری نزدیک با دیگر اعضا و نهادهای اتحادیه اروپا میسر می‌شود.

کماکان اقدامات بسیاری باید در حوزه تعلیم و آموزش دفاع سایبری انجام شود تا نقص خاص شناسایی‌شده در سطوح عملیاتی و فرماندهان ارشد برطرف شود. مسائلی در خصوص ایجاد فرهنگ امنیت سایبری در سطح اتحادیه اروپا وجود دارد که یکی از راه‌حل‌های رفع آن‌ها احتمالاً تشکیل نیروی وظیفه اروپایی جهت انجام اقدام مناسب، افزایش آگاهی و ارائه آموزش در زمینه مسائل دفاع سایبری است. درواقع، شناسایی موارد هم‌افزایی و توسعه بیشتر الگوی همکاری با بازیگران اتحادیه اروپا که در امر ارائه آموزش دخیل هستند –مانند مرکز مقابله با جرائم سایبری اروپا، گروه آموزش و تعلیم مقابله با جرائم سایبری اتحادیه اروپا، آژانس امنیت شبکه و اطلاعات اتحادیه اروپا و دانشکده دفاع و امنیت اروپا[1]– موجب بهبود توانمندی آموزشی و اطلاعاتی می‌شود. آژانس دفاع اتحادیه اروپا برای تسهیل توسعه آموزش دفاع سایبری، تحلیل نیازهای آموزشی دفاع سایبری را بر اساس دوره‌های آموزشی موجود در اتحادیه اروپا و کشورهای

1. European Security and Defence College (ESDC)

عضو آن و با همکاری نزدیک با مرکز عالی همکاری‌های دفاع سایبری ناتو[1] در تالین انجام داد.

اهداف اصلی این تحلیل، تهیه نظام آموزشی تعریف‌شده و هدفمند روشن‌تری است که سطوح مختلف (مخاطبان هدف تعریف‌شده)، انواع آموزش دفاع سایبری (مناسب هر سطح) و الزامات کارکردی (ابزارهای پشتیبانی و آموزش) را تبیین می‌کرد. درواقع، اقداماتی در این حوزه انجام شده بود[۲۴] که مهم‌ترین آن‌ها طرح موردی آژانس دفاع اتحادیه اروپا در مورد محدوده‌های سایبری (برای آزمایش توانمندی‌های دفاع سایبری) بود که هدف آن افزایش دسترس‌پذیری محدوده‌های سایبری؛ افزایش بازده محدوده‌های سایبری موجود؛ ایجاد شبکه محدوده‌های سایبری و بهبود مانورها و آزمایش‌های آموزشی دفاع سایبری در سطح اروپا در میان‌مدت بود (Roehrig 2013). در داخل و سرتاسر اتحادیه اروپا فرصت‌هایی برای تأثیرگذاری بیشتر، به‌خصوص در زمینه مانورهای مشترک –دوجانبه و جمعی (آژانس امنیت شبکه و اطلاعات اتحادیه اروپا، ناتو)– و آموزش و ایجاد ساختارهای آموزشی و تعلیمی ضروری جدید وجود دارند. مسلماً اگر هدف، برقراری امنیت تاب‌آور کارآمدتر در اکوسیستم دفاع سایبری است، اقدامات بیشتری باید به دلیل وجود عدم تقارن در اروپا صورت گیرد. توافق وزرای دفاع اروپا در سال ۲۰۱۲ در زمینه شمول حوزه دفاع سایبری، در دستورکار ادغام و اشتراک [اطلاعات] موجب تسهیل همکاری مشترک بیشتر در زمینه آموزش و تعلیم شده و امکان بررسی موارد هم‌افزایی بیشتر را در اختیار آژانس امور دفاعی اروپا قرار داده است که در افزایش ظرفیت این حوزه ازجمله در رشد و حفظ متخصصان سایبری خبره در ارتش نقش دارد.

به نظر برخی مفسران، افزایش حفاظت از شبکه‌های ارتباطات و اطلاعات برای نهادها، مأموریت‌ها و عملیات‌های سیاست امنیتی و دفاعی مشترک منجر به ایجاد مسائل پیچیده‌ای می‌شود، چراکه اتحادیه اروپا درواقع مالک منابع نظامی خود نیست (Roehrig and Smeaton 2013, p.24; Robinson 2014, p.2). به‌علاوه، پرسش‌هایی در زمینه نحوه ادغام مسئولیت‌های کشورهای عضو در قبال حفاظت از زیرساخت‌های حیاتی در کشور خود و نحوه مشارکت با مالکان خصوصی زیرساخت‌های حیاتی مربوطه مطرح می‌شود (Robinson 2014, p.3).

1. Cooperative Cyber Defence Centre of Excellence (CCDCoE)

ازاین‌رو، این مسئله که عملیات‌های نظامی اتحادیه اروپا تا حد زیادی به زیرساخت‌های حیاتی خصوصی و بازیگران غیرنظامی وابسته است، مسائل همکاری و هم‌افزایی بین این دو مورد و نحوه دستیابی به آن به کارآمدترین نحو را مطرح می‌کند. به‌ویژه، این مسئله پرسش‌هایی را در مورد رویکردهای فرهنگی در قبال مدیریت خطرات و حفاظت ازجمله رویکردهای مربوط به تضمین و درواقع، استانداردهای امنیتی مطرح می‌کند. اتحادیه اروپا از ظرفیت سازمانی لازم برای رسیدگی به این مسائل برخوردار است –برای مثال، کارکنان نظامی اتحادیه اروپا[1] و شورای وزیران همواره در حال ارتقای توانمندی‌های امنیت اطلاعاتی و ارتباطی خود هستند و تیم واکنش اضطراری رایانه‌ای اتحادیه اروپا ازنظر تجربه و توانایی پیشرفت کرده است.

اگرچه، مسائل فرضی نیز در مورد شمول امنیت سایبری در مدیریت بحران مربوط به فرایندهای پیچیده برنامه‌ریزی سیاست امنیتی و دفاعی مشترک و به‌ویژه، مراحل گوناگون مأموریت‌ها، یعنی مرحله ارزیابی راهبردی و مرحله تولید نیرو وجود دارد. هر فرمانده عملیاتی باید شیوه مشخصی درخصوص نحوه ارزیابی و درک نقاط بهره‌برداری احتمالی امنیت سایبری برای هر مأموریت فرضی (ارزیابی راهبردی[۳۵]و نحوه ایجاد موازنه بین منابع سازمان‌دهی‌شده در زمینه عملیاتی و توانمندی‌های دفاع سایبری کشورهای عضو عرضه‌کننده منابع برای هر مأموریت خاص (تولید نیرو) داشته باشد. در توسعه چارچوب سیاست پیشنهادی دفاع سایبری، نحوه تصمیم‌گیری، ارزیابی و عملیاتی کردن خطرات سایبری در هر مأموریت، باید شفاف باشد تا حوزه دفاع سایبری حضور کارآمدی در ساختارهای سیاست امنیتی و دفاعی مشترک داشته باشد (Ibid.). درنهایت، این نقاط بسیار به هم پیوسته‌اند تا همکاری نظامی-غیرنظامی در اقدام عملیاتی و آموزشی برای درک بهتر خطرات و اقدامات مشترک لازم جهت رسیدگی به آن‌ها در حوزه دفاع سایبری (برای مثال، حضور گروه‌های نظامی واکنش اضطراری رایانه‌ای در مانورهای مدیریت بحران غیرنظامی ملی و چندملیتی یا تیم‌های واکنش اضطراری رایانه‌ای دولتی در مانورهای نظامی ملی و چندملیتی) بهبود یابد.

آخرین حوزه اقدام –تقویت همکاری با ناتو و دیگر بازیگران خصوصی و دولتی بین‌المللی

1. EU Military Staff (EUMS)

مربوطه– محل پیشرفت کنونی اتحادیه اروپا و ارتقای حتمی مشارکت‌های کارآمد است. همکاری اتحادیه اروپا–ناتو در سطح غیررسمی از سال ۲۰۱۰ آغاز شده است و طرفین در مورد زمینه‌های مشترک مورد نگرانی، مانند افزایش آگاهی درباره امنیت سایبری و توسعه آموزش و توانمندی در حوزه امنیت سایبری تاب‌آور به توافق رسیده‌اند. به‌رغم تحول هویتی ایجادشده در ناتو در چند سال اخیر، [این سازمان] سیاست خود را گسترش داده و طرح اقدامی برای توسعه توانمندی دفاع سایبری برای رسیدگی به مسائل هر دو بعد نظامی و غیرنظامی ایجاد کرده است. سیاست بهبودیافته با اولویت بالای «حفاظت از سیستم‌های ارتباطی تحت مالکیت و مدیریت کشورهای متحد» در نشست سپتامبر ۲۰۱۴ ناتو در ولز تصویب شد (NATO 2014).

گذشته از این موضوع، این سیاست بر تسهیل اقدامات متحدان ناتو (۲۲ کشور عضو اتحادیه اروپا و ناتو) در حوزه دفاع سایبری، بهبود ظرفیت و توانمندی نهادی خود و همکاری با شرکا و صنایع تأکید داشت. ازنظر نهادی، ناتو اقدام به تشکیل تیم‌های واکنش سریع دفاع سایبری[1]، جهت ایجاد توانمندی واکنش‌دهی به حوادث رایانه‌ای[2] برای حفاظت از شبکه‌های خود نمود که با اداره مدیریت دفاع سایبری[3] آن همکاری می‌کنند، یعنی فرآیند برنامه‌ریزی دفاعی که «اهدافی را برای به‌کارگیری توانمندی‌های ملی کشورهای متحد در حوزه دفاع سایبری تعریف می‌کند.» دفاع سایبری نیز در ابتکار دفاع هوشمند[4] ناتو گنجانده شده است که کشورها را قادر به همکاری با یکدیگر برای توسعه توانمندی‌های دفاع سایبری می‌کند –آن‌ها به‌تنهایی نمی‌توانستند این کار را انجام دهند[۲۶] (Ibid.). گذشته از ساختارهای رسمی دفاع سایبری ناتو، مرکز عالی همکاری‌های دفاع سایبری ناتو در تالین، گروه فعالی در حوزه آموزش و تعلیم دفاع سایبری و تحقیق و توسعه محسوب می‌شود. درواقع، این مرکز سند مهمی –راهنمای تالین (ن.ک. فصول ۳ و ۷)– را در زمینه تفسیر قانون جنگ مسلحانه منتشر کرد که مربوط به حوزه دفاع سایبری است.

ازاین‌رو، وظیفه اتحادیه اروپا در بررسی طرح چارچوب سیاسی برای دفاع سایبری و تأمین

1. Rapid Reaction Teams for Cyber Defence
2. Computer Incident Response Capability
3. Cyber Defence Management Authority
4. Smart Defence Initiative

امنیت تاب‌آور کارآمدتر در این حوزه، بررسی نحوه ایجاد همکاری و مشارکت با اجتناب از تکرار و به‌کارگیری کامل منابع اشتراک و جمع‌آوری [اطلاعات] در هر زمان ممکن است. به‌رغم وجود موانع بی‌شمار بر سر راه این مورد ازنظر قانونی، فرآیندها و توافقات مشابه موارد مطرح‌شده در زمینه توانمندی‌ها و منابع «دفاع» مشترک، مسیر احتمالی برای جلب همکاری طرفین محسوب می‌شوند. گذشته از ناتو، پیشرفته‌ترین مشارکت بین‌المللی اتحادیه اروپا با آمریکا از طریق کارگروه امنیت سایبری و مقابله با جرائم سایبری اتحادیه اروپا-آمریکا صورت می‌گیرد، اما این مسئله بُعد دفاعی روشنی ندارد (ن.ک. فصل ۷). اتحادیه اروپا با هند، برزیل و چین نیز توافقاتی امضا کرده است و برنامه گفتگوی سایبری با آن‌ها دارد (برای مثال، تشکیل نیروی وظیفه امنیت سایبری چین- اتحادیه اروپا) و در کنفرانس‌های دیپلماتیک سطح بالای بسیاری (ازجمله کنفرانس‌های لندن ۲۰۱۱، بوداپست ۲۰۱۲ و سئول ۲۰۱۳) شرکت کرده و با هدف تأمل پیرامون هنجارها و قوانین حکمرانی فضای سایبری جهانی، این کنفرانس‌ها را سازماندهی کرده است. اگرچه برنامه‌های رسمی مطرح‌شده در مورد دوم به‌رغم کارآمدی در زمینه تقویت پیام‌های اصلی هنجارهای موردنظر برای اینترنت، منجر به ایجاد مشارکت کارآمدی در حوزه دفاع سایبری نشدند و تعداد آن‌ها به حدی اندک است که توافق عملی در زمینه اقدام و درک مشترک از مشکلات دفاع سایبری به دست نیامد.

جمع‌بندی

این فصل به ارزیابی دو ویژگی دارای اولویت در راهبرد امنیت سایبری اتحادیه اروپا می‌پردازد. همان‌طور که در مقدمه به‌خصوص در بحث ذیل امنیت شبکه و اطلاعات اتحادیه اروپا اشاره شد، این کتاب با توجه به دامنه گسترده این موضوع جامع نیست و مسائل مهمی نظیر امنیت شبکه‌های ابری و تلفن همراه، شبکه‌های هوشمند، سیستم‌های کنترل صنعتی مجهز به فناوری اطلاعات، همکاری در زمینه فرآیند استانداردسازی و موارد دیگر در آن مطرح نشده‌اند. علاوه بر این، پیامدهای کلی و خاص‌تر مهمی برای تأمین امنیت تاب‌آور اتحادیه اروپا در حوزه دفاع سایبری و امنیت شبکه و اطلاعات ایجاد می‌شوند.

الگوهای متفاوتی در خصوص امنیت شبکه و اطلاعات در کشورهای عضو ازنظر توانمندی و همکاری وجود دارند و این موضوع ظاهراً بیانگر عدم تمایل آن‌ها به گزارش رویدادها و بهبود ظرفیت‌های نهادی جهت تأمین امنیت سایبری تاب‌آور در نظام داوطلبانه است. ازنظر کمیسیون اروپا، انگیزه لازم در بخش‌های دولتی یا خصوصی برای بهبود توانمندی‌ها ایجاد نمی‌شود که این مسئله منجر به طرح پیشنهادی امنیت شبکه و اطلاعات گردید؛ قانون اصلی، که در کنار راهبرد امنیت سایبری اتحادیه اروپا مطرح شد که حاکی از تغییر قابل‌ملاحظه در حکمرانی امنیت شبکه و اطلاعات به رویکرد فراحکمرانی عملی بود. اجماع کلی در مورد اهداف اصلی امریه پیشنهاد ی امنیت شبکه و اطلاعات برای بهبود امنیت سایبری تاب‌آور وجود داشت، اما مسائل و مشکلات بسیاری نیز به چشم می‌خورد که احتمال دارد موجب محدودسازی ایجاد شرایط لازم برای تأمین امنیت تاب‌آور کارآمد ازنظر ارتقای همکاری، مشارکت و تشریک‌مساعی و فرهنگ امنیت سایبری ازنظر مشارکت‌های مبتنی بر اعتماد لازم برای تبادل و اشتراک اطلاعات بین طرف‌های ذی‌نفع مربوطه گردند. اجماع کلی در مورد توانمندی مبنی بر این وجود دارد که ظرفیت‌سازی نهادی حداقلی، اقدامی مثبت تلقی می‌شود، گرچه، تضمین کیفیت نهادها و عملکرد آن‌ها احتمالاً بسیار دشوارتر است. امنیت شبکه و اطلاعات مسلماً روند تدریجی را در ایجاد شرایط لازم برای تأمین امنیت سایبری تاب‌آور طی می‌کند (موارد عملکرد خوب بسیارند)، اما از وضعیت مطلوب فاصله بسیاری دارد.

شایان‌ذکر است که شرایط تأمین امنیت تاب‌آور در حوزه دفاع سایبری در بهترین حالت، روند تکوینی را طی می‌کند. کسب چنین نتیجه‌ای با توجه به‌تازگی حوزه دستورکار سایبری اتحادیه اروپا تعجب‌برانگیز نیست، اما تحولات با رهبری آژانس دفاع اتحادیه اروپا بر حوزه‌های اولویت‌دار مهم، به‌سرعت شتاب می‌گیرند. طرح روشن‌تری از این چشم‌انداز در خصوص توانمندی دفاع سایبری در سطح اتحادیه اروپا و در کشورهای عضو حاضر در آژانس دفاع اتحادیه اروپا مطرح شد، اما اتحادیه اروپا در این حوزه با مشکلاتی نیز برای دستیابی به اهداف اصلی و توسعه چارچوبی جامع و کارآمد برای دفاع سایبری روبرو است. مسلماً آگاهی، درک، ظرفیت سازمانی و نهادی چندانی در اتحادیه اروپا وجود ندارد و تصویر مبهمی در مورد عدم انسجام و ناکارآمدی

حوزه دفاع سایبری کشورهای عضو ملاحظه می‌شود.

برنامه‌ها در حال ایجاد هستند و روند پیشرفت ازنظر حرکت به سمت رژیمی تاب‌آورتر و کارآمدتر کُند بوده، ولی در جریان است. مواردی نظیر آموزش و تعلیم پیشرفت بسیار بیشتری نسبت به موارد دیگر در سطح اتحادیه اروپا داشته‌اند و طرح‌های موردی توسط آژانس دفاع اتحادیه اروپا برای افزایش دانش و توانمندی عملیاتی شده‌اند. اگرچه، مسائل در مورد ساخت تسهیلات، سازمان‌ها و دکترین‌های لازم برای توسعه دفاع سایبری برای بسیاری از کشورهای عضو کماکان [حل‌نشده] باقی می‌مانند. به‌رغم وجود احتمال تکامل مشارکت بین‌المللی کارآمدتر برای رسیدگی به مسائل دفاع سایبری، در اینجا نیز پیشرفت به‌واسطه پیچیدگی فرآیند رسمی –به‌خصوص در ارتباط با ناتو– حتی با وجود موارد هم‌افزایی آشکار محدود شده است. علاوه بر این، تمام اعضای اتحادیه اروپا در رکن دفاع سایبری موردحمایت سیاست امنیتی و دفاعی مشترک، حضور ندارند و این امر ایجاد درک و رویکردهای مشترک در سطح اتحادیه اروپا در آینده نزدیک را دشوار می‌سازد.

فصل هفتم

همکاری فراآتلانتیک در امنیت سایبری
همگرایی در امنیت تاب‌آور

مقدمه

امنیت سایبری، چالش بین‌المللی محسوب می‌شود (ن.ک. فصل ۳) که رسیدگی کارآمد به آن مستلزم تشریک‌مساعی و مشارکت بین‌المللی با بازیگران و سازمان‌های کلیدی است. در این زمینه، یکی از اولویت‌های راهبرد امنیت سایبری اتحادیه اروپا، ایجاد سیاست بین‌المللی منسجمی برای فضای سایبری و ترویج و بیان ارزش‌های اصلی اتحادیه اروپا در این فضا است. در این راهبرد، آمده است که هدف سیاست بین‌المللی فضای سایبری اتحادیه «مشارکت بیشتر و ایجاد روابط محکم‌تر با شرکا و سازمان‌های بین‌المللی اصلی و جامعه مدنی و بخش خصوصی» است و «همکاری با ایالات‌متحده آمریکا در سطح دوجانبه اهمیت بسیاری دارد» «و به‌خصوص در چارچوب کارگروه آمریکا- اتحادیه اروپا در امور امنیت سایبری و جرائم سایبری[1] افزایش می‌یابد» (European Commission 2011; EU Cybersecurity Strategy 2013, p.15). درواقع، هدف از تشکیل این کارگروه، «مقابله با تهدیدهای جدید پیش روی شبکه‌های جهانی است که امنیت و سعادت و رفاه جامعه آزاد ما بیش‌ازپیش به آن‌ها وابسته شده است» (Joint Statement of the EU–US Summit 2010).

می‌توان این استدلال را مطرح کرد که روابط با آمریکا نه‌فقط ازنظر امنیت و جرائم سایبری، بلکه ازنظر حیاتی و در کل، ازلحاظ جریان تجارت فراآتلانتیکی و مذاکرات در زمینه پیمان مشارکت

1. EU-US Working Group on Cyber-Security and Cyber-Crime

تجاری و سرمایه‌گذاری فراآتلانتیک[1] برای اروپا نیز ارزشمند است. این مسائل به دلیل وجود سازوکارهای اشتراک لحظه‌ای داده‌ها و اطلاعات دیجیتالی –برای مقاصد تجاری یا تحقیقات جنایی برخط یا برون‌خط– پیوند اجتناب‌ناپذیری با یکدیگر دارند. همکاری فراآتلانتیک در زمینه مسائل سایبری و مشارکت تجاری و سرمایه‌گذاری فراآتلانتیک، تا حد زیادی تحت تأثیر افشاگری‌های ادوارد اسنودن در مورد نظارت و جاسوسی جمعی از شهروندان و نخبگان اروپا توسط آژانس‌های اطلاعاتی آمریکا قرار گرفتند که این موضوع اعتماد بین آمریکا و اتحادیه اروپا در حوزه اقدامات همکاری‌جویانه را بسیار خدشه‌دار کرد. به‌علاوه، این مورد بیانگر اختلاف‌نظر آن‌ها در زمینه برقراری موازنه صحیح بین حفاظت از داده‌ها و حریم خصوصی و اشتراک (و جمع‌آوری) اطلاعات با هدف تضمین برقراری امنیت سایبری تاب‌آور کارآمد بود.

این مسئله، بدین معنا نیست که آمریکا و اتحادیه اروپا در مورد مسائل مربوط به مشارکت و تشریک‌مساعی و همکاری در زمینه امنیت سایبری و جرائم سایبری ازلحاظ فرهنگی با یکدیگر کاملاً ناسازگارند. مسلماً چنین نیست، چراکه آن‌ها کماکان نظرات مشابهی درخصوص حکمرانی جهانی اینترنت –اینترنت آزاد، باز، امن و قابل‌دسترس برای همگان– و در مورد ضرورت طراحی سازوکارهای کارآمدی برای مقابله با جرائم سایبری و حفاظت و تولید زیرساخت‌های اطلاعاتی حیاتی صنایع تاب‌آور دارند. به‌علاوه، مجامعی برای همکاری نزدیک‌تر اتحادیه اروپا و آمریکا در زمینه جرائم سایبری و امنیت سایبری مانند کارگروه تشکیل‌شده در نوامبر ۲۰۱۰ با محورهای: الف) مدیریت حوادث سایبری؛ ب) مشارکت بخش‌های عمومی- خصوصی؛ ج) افزایش آگاهی و د) جرائم سایبری ایجاد شده‌اند که یکی از نتایج آن ایجاد اتحاد جهانی علیه سوءاستفاده جنسی آنلاین از کودکان (دسامبر ۲۰۱۲) بود. در دوره پس از افشاگری‌های اسنودن و احتمالاً با کاهش خشم اولیه در مورد جاسوسی جمعی آمریکا از شهروندان اروپا، گفتگو بین اتحادیه اروپا و آمریکا در مورد موضوعات فی‌مابین و مربوط به سیاست خارجی از سر گرفته شد (مارس ۲۰۱۴) و گفتگوی جامعه اطلاعاتی[2] با محوریت مسائل گسترده‌تر مربوط به امنیت سایبری ازجمله سیاست‌گذاری و حکمرانی اینترنت صورت گرفت.

1. Information Society Dialogue
2. Information Society Dialogue

بااین‌حال، با وجود پیشرفت حاصله در دوره پس از افشاگری‌های اسنودن، مسلماً افشاگری‌های انجام‌شده در مورد اقدامات جاسوسی آژانس امنیت ملی آمریکا[1] تأثیر نامطلوبی بر تکامل و پیشرفت مشارکت فراآتلانتیک و فرهنگ امنیت سایبری و امنیت تاب‌آور مبتنی بر اعتماد و درک مشترک از مسائل و راه‌حل مربوط به منطق و قوانین امنیت سایبری داشته است. در همین زمینه، این فصل به تحلیل رابطه اتحادیه اروپا و ایالات‌متحده و پیامدهای این رابطه برای اتحادیه ازنظر توسعه بُعد فراآتلانتیکی راهبرد و اکوسیستم امنیت سایبری آن می‌پردازد. به‌ویژه، این فصل شباهت‌ها و تفاوت‌های موجود بین منطق امنیتی طرفین در مورد مسائل مختلف مربوط به امنیت فضای سایبری را تحلیل می‌کند. در بخش نخست، تحلیل دقیقی از پیامدهای افشاگری اسنودن و رویکردهای آمریکا و اروپا در قبال همکاری سایبری (فرهنگ‌های امنیت سایبری) و معنای این مورد برای تأمین امنیت تاب‌آور کارآمد فراآتلانتیک ارائه می‌شود. در بخش دوم، پیشرفت حاصله به‌واسطه توافقات رسمی و غیررسمی به‌دست‌آمده بین آمریکا و اتحادیه اروپا در زمینه مقابله با جرائم سایبری و ایجاد امنیت سایبری تاب‌آور کارآمد فراآتلانتیک ارزیابی می‌گردد. در بخش آخر نیز میزان تأثیرگذاری مشارکت طرفین بر ایجاد شرایط لازم برای برقراری امنیت تاب‌آور کارآمد بین این دو بازیگر اصلی در جهان و درمجموع، برای تکامل اکوسیستم امنیت سایبری تاب‌آور جهان بررسی می‌شود.

حکمرانی بر فضای سایبر

اتحادیه اروپا و ایالات‌متحده آمریکا مواضع هنجاری مشابهی در زمینه اینترنت و نحوه حکمرانی بر آن دارند، اگرچه از نظر تاریخی و پس از افشاگری‌های اسنودن، در مواردی نیز با یکدیگر اختلاف‌نظر و مشاجره داشته‌اند، چراکه اتحادیه اروپا خواستار فراگیری و شفافیت بیشتر مجامع جهانی –به‌ویژه آیکان(ICANN)– است که بر اینترنت نظارت دارند. آن‌ها هر دو بر اساس اصل اینترنت جهانی عمل می‌کنند که اساسا، یک خیر عمومی و جمعی است که بر مبنای آن اینترنت باید برای همه شهروندان قابل دسترسی و قابل استفاده باشد. بدین ترتیب، آن‌ها دیدگاه هنجاری

1. National Security Agency (NSA)

مشترکی درخصوص اینترنتِ بدون محدودیتی دارند که تنها مورد استثناء این قانون، به‌کارگیری ابزارهایی برای جلوگیری از آسیب‌رسانی آنلاین به دیگران است (Christou 2014).

اتحادیه اروپا و آمریکا نظرات مشابهی در مورد الگوی نظارت بر اینترنت دارند تا تضمین کنند که در فضای برخط، حقوق افراد محفوظ و اینترنت امن و قابل دسترس است تا از این رهگذر مزایای اقتصادی به حداکثر برسد. چنین الگوی چندجانبه‌ای از فرایندی طولانی، بحث‌برانگیز و متضادی –در اجلاس جهانی جامعه اطلاعات سازمان ملل (WSIS 2002–2005)– متولد شد که در آن کنترل یکجانبه امریکا بر اینترنت به چالش کشیده شد. چنین چالشی از جانب اتحادیه اروپا مطرح شد که خواستار نظارت بین دولتی بیشتری در چارچوب آیکان، یعنی ایجاد تغییر در ماهیت رابطه عمومی- خصوصی بود که ابتدا شکل گرفت (Christou and Simpson 2007, p.154–156). این مسئله همچنین از جانب کشورهایی نظیر روسیه، چین، عربستان سعودی و ایران به نحو آشکارتری مطرح گردید که الگوی چند کشوری را ترجیح می‌دادند و خواستار گذار کامل از الگوی «تمام طرف‌های ذینفع» به الگوی کنترل دولتی حکمرانی و نظارت اینترنت از طریق سازمان ملل با هدف تضعیف کنترل آمریکا بودند (Laprise 2014).

کارگروه حکمرانی اینترنت[1] که توسط کوفی عنان[2]، دبیرکل وقت سازمان ملل متحد، با هدف تعریف حکمرانی اینترنت و ساختارها و مسئولیت‌های بازیگران در آن تشکیل گردید، به‌رغم امتناع آمریکا از صرف‌نظر از کنترل و مالکیت اینترنت، درنهایت از ایجاد انجمنی درراستای ارائه «فضایی برای گفتمان تمام طرف‌های ذینفع با برخورداری از جایگاه برابر در مورد مسائل مربوط به حکمرانی اینترنت» حمایت کرد (WGIG 2005, p.10). این مسئله در طرح مجمع حکمرانی اینترنت به اوج خود رسید که گرچه تحت حمایت سازمان ملل متحد شکل گرفت، اما نهادی محسوب می‌شد که امکان گردهمایی طرف‌های ذینفع برای مباحثه، تأمل و یافتن راه‌حل‌هایی در مورد تمام مسائل مربوط به حکمرانی اینترنت را فراهم می‌کرد.

از آن زمان، الگوی چندجانبه‌ای که در آیکان و مجمع حکمرانی اینترنت و همچنین در نهادهای نظارتی و واضع استاندارد نظیر کارگروه مهندسی اینترنت[3] لحاظ شده است، با توجه به

1. Working Group on Internet Governance (WGIG)
2. Kofi Annan
3. Internet Engineering Task Force (IETF)

ماهیت اینترنت و تأثیر احتمالی آن بر انواع طرف‌های ذینفع، به‌عنوان الگوی هنجاری مناسبی برای حکمرانی اینترنت ازجمله مسئله امنیت موردتوجه قرار گرفته است. درواقع، شواهدی از بهترین روش‌های موردبحث در مجمع حکمرانی اینترنت در سیاست داخلی ملاحظه می‌شود (Christou and Simpson 2012)، ساختارها و برنامه‌های آیکان نحوه رفع مسائل عملی در فرایند فراگیر آن را نشان می‌دهند و درمجموع، رویکرد چندجانبه، حفظ اینترنت آزاد و رایگان را تضمین می‌کند که عامل شکوفایی نوآوری و تنوع است (Bendiek 2014, p.8).

البته این الگو (ن.ک. فصل ۳) بحث‌برانگیز است و در هر فرصتی از جانب دولت‌هایی به چالش کشیده شده است که خواستار اعمال کنترل دولتی بیشتر و اتخاذ رویکرد بین دولتی مؤثرتر بر حکمرانی اینترنت هستند و نگرانی خود را درخصوص کنترل و نظارت ایالات‌متحده بر مدیریت اینترنت (آیکان) ابراز کرده‌اند. به‌عنوان‌مثال، در کنفرانس جهانی ارتباطات بین‌المللی[1] (۲۰۱۲) که با هدف اصلاح مقررات مربوط به مخابرات اینترنتی تشکیل گردید، پیشنهادی از جانب روسیه، چین، عربستان، الجزایر و سودان مبنی بر گسترش حوزه‌های قضایی مقررات مربوط به مخابرات اینترنتی، یعنی کنترل دولتی مستقل بر تمام ابعاد حکمرانی اینترنت ازجمله ابعاد امنیتی مطرح گردید. اگرچه این پیشنهاد درنهایت پس گرفته شد، اما اتحادیه بین‌المللی مخابرات، قطعنامه غیرالزام‌آور مصالحه‌آمیزی (قطعنامه ۳) را تصویب کرد که در متن نهایی مقررات مربوط به مخابرات اینترنت لحاظ شده است که به نحو کارآمدی زبان بین‌حکومت‌گرایی و کنترل بیشتر دولت بر توسعه فنی اینترنت و مسائل سیاست‌گذاری دولتی مربوطه را در بر داشت (Kruger 2013, p.12). درنتیجه این امر، آمریکا از امضای معاهده نهایی به دلیل پیامدهای این موضوع برای مفاد بعدی مقررات مربوط به مخابرات اینترنتی در مورد امنیت سایبری و جرائم اینترنتی امتناع ورزید. اما همان‌طور که کلیمبرگ این مسئله را مطرح می‌کند «پیامدهای گسترده سند [نهایی] را می‌توان «جایگاه معنایی» برای انتقاد بیشتر از مسئله چندجانبه‌گرایی تلقی کرد» (2012, p.4).

مسلماً مجامعی مانند اتحادیه بین‌المللی مخابرات و کنفرانس جهانی ارتباطات بین‌المللی در

1. World Conference on International Communications (WCIT)

سال ۲۰۱۳ شاهد مشکلات مشابهی برای الگوی چندجانبه‌گرایی بودند که اتحادیه اروپا و آمریکا (و اتحادی از دیگر کشورهای غربی) همواره از آن و اصول اینترنت رایگان و آزاد دفاع کرده‌اند. اگرچه، انتشار اسناد محرمانه آمریکا در تابستان ۲۰۱۳ توسط ادوارد اسنودن که نشان‌دهنده گستره فعالیت‌های نظارت بر اطلاعات آمریکا بود، لحظه‌ای بود که همبستگی در چارچوب اتحاد غرب –به‌ویژه بین اتحادیه اروپا و آمریکا– زیر سؤال رفت و این مسئله پیامدهای خاصی برای همکاری سایبری فراآتلانتیک داشت. حتی پیش از افشاگری‌های اسنودن، اتحادیه اروپا همواره خواستار پاسخ‌گویی و شفافیت بیشتر و ایفای نقش برابرتری در شورای مشورتی دولت در مورد نظارت و عملکرد آیکان بود (European Commission 2009) و درعین‌حال، ظاهراً از چندجانبه‌گرایی حمایت می‌کرد (Christou and Simpson 2011). اگرچه آمریکا از طریق [سند] تأیید تعهدات[1] (۲۰۰۹) که از جانب آیکان و وزارت بازرگانی آمریکا امضا شده بود، تعهد خود در قبال بررسی دوره‌ای چهار هدف اصلی آیکان ازجمله پاسخ‌گویی، شفافیت و منافع کاربران اینترنت جهانی را نشان داد، اما این موضوع منجر به کاهش نظارت یک‌جانبه آمریکا بر عملکرد آیکان و نهاد شماره‌های اختصاصی اینترنت[2](آیانا) نگردید. ازاین‌رو، پس از افشاگری‌های اسنودن، اتحادیه اروپا گام دیگری برداشت و خواستار مشارکت بیشتر کشورهای دموکراتیکی نظیر برزیل و هند شد و قدرت یک‌جانبه نظارت آمریکا در آیکان را نیز به‌شدت به چالش کشید.

بدین منظور، کمیسیون اروپا –به رهبری اداره کل شبکه‌های ارتباطات، محتوا و فناوری– مرکز نظارت جهانی بر سیاست اینترنت[3] را با هدف ایجاد برنامه فنی جامع و شفاف برای مشارکت در حکمرانی اینترنت تأسیس کرد. این مرکز با همکاری کشورهای همفکری نظیر برزیل، هند و سوئیس و سازمان‌های منطقه‌ای مانند اتحادیه آفریقا و برخی سازمان‌های غیردولتی تأسیس شد. هدف از تأسیس این مرکز، اطمینان از این مسئله بود که تمام طرف‌های ذینفع –حتی طرف‌های برخوردار از منابع محدود– بتوانند از طریق راه‌حل فناورانه به فرایندهای سیاست‌گذاری، اطلاعات و بحث در زمینه حکمرانی اینترنت دسترسی و در آن‌ها مشارکت

1. Affirmation of Commitments
2. Internet Assigned Numbers Authority (IANA)
3. Global Internet Policy Observatory (GIPO)

بیشتری داشته باشند.(۲) هدف این مرکز جایگزین کردن مجامع و برنامه‌های موجود برای مباحث مربوط به حکمرانی اینترنت نیست، بلکه اعطای حق اظهارنظر و نفوذ بیشتر به آن دسته از قدرت‌های دموکراتیک نوظهور و سازمان‌های منطقه‌ای است که می‌خواهند کنترل آمریکا بر عملکرد اینترنت را به چالش بکشند (Interview, DG Connect official, March 2013).

علاوه بر این، اتحادیه اروپا در جلسه چندجانبه برگزارشده در مورد آینده حکمرانی اینترنت (نت ماندیل[1]) در سائوپائولو برزیل (آوریل ۲۰۱۴) و جلسه مجمع حکمرانی اینترنت (سپتامبر ۲۰۱۴) بر تعهد خود در قبال شفافیت و جامعیت تأکید کرد. درواقع، هدف طرح مشترک و منسجم و پیام نیلی کروز[2]، معاون پیشین کمیسیون اروپا و عضو کمیته عالی چندجانبه نت ماندیل، تضمین جهانی‌شدن آیانا و آیکان و تقویت مجمع حکمرانی اینترنت و اصلاح الگوی چندجانبه‌ای برای حکمرانی اینترنت بود. کروز، منطق مبنای این موضع را به‌وضوح بیان می‌کند: «افشاگری‌های اخیر در مورد جاسوسی گسترده، مدیریت آمریکا در زمینه حکمرانی اینترنت را زیر سؤال برده است ... با توجه به الگوی آمریکا، محور کنونی حکمرانی اینترنت، مذاکره درخصوص گذار آسان به الگوی جهان‌شمول‌تر و درعین‌حال، حفظ ارزش‌های اصلی حکمرانی چندجانبه باز ضروری است ... فعالیت‌های نظارتی و اطلاعاتی گسترده باعث عدم اعتماد به اینترنت و ترتیبات حکمرانی کنونی آن شده است» (Kroes cited in Traynor 2014). درنهایت، نت ماندیل، سندی را تهیه کرد که اصول و ارزش‌های مشترک چارچوب حکمرانی فراگیر، چندجانبه و در حال تکاملی برای اینترنت–با راهنمایی برای چگونگی دستیابی به این مورد که اتحادیه اروپا و آمریکا هر دو به دنبال دستیابی به آن هستند، را تعیین کرد (Press release, 1st EU–US Cyber dialogue 2014).

در این زمینه، آمریکا در مارس ۲۰۱۴، قصد خود مبنی بر ایجاد فرایندی جهت حذف عملکرد نظارتی سازمان ملی مخابرات و اطلاعات آمریکا[3] بر آیکان را با دو شرط مهم اعلام کرد: ۱. الگوی چندجانبه‌ای که تحت سلطه دولت‌ها نیست، جایگزین نظام نظارت کنونی شود؛ ۲. سیستم و ساختارهای کنونی پشتیبان آن، تا زمان توافق در مورد سازوکارهای حکمرانی جدید توسط

1. NETmundial
2. Neelie Kroes
3. National Telecommunications and Information Administration (NTIA)

جامعه اینترنت باقی بمانند. این موارد از تأثیر دوگانه‌ای برخوردار است: دلجویی از طرف‌هایی مانند اتحادیه اروپا و کشورهای عضو آن به دلیل «نظارت و جاسوسی» با هدف تأمین «امنیت» که با افشاگری‌های اسنودن و مسائل بعدی مربوط به کنترل آمریکا بر اینترنت برای منافع راهبردی خود مطرح شد و درعین‌حال، مسئله حفظ توافق میان دولت‌ها و سازمان‌های همفکر (سازمان‌های غیردولتی، سازمان‌های منطقه‌ای و غیره) در مورد ارزش‌های مبنای حکمرانی اینترنت –و مهم‌تر از آن، مجموعه گسترده بازیگرانی که باید در چنین فرایندهایی شرکت کنند– تضمین گردید. بدین ترتیب، دیدگاه مبتنی بر «استقلال» حکمرانی اینترنت که توسط دولت‌هایی مانند روسیه و چین بیان شده بود، حداقل به‌طور موقت، بی‌اعتبار شد و سازوکارهای «انتقالی» احتمالاً فراگیرتری محور اصلی مباحث صورت‌گرفته در مجامع بین‌المللی بعدی بودند. این امر بدین معنا نیز است که اتحادیه اروپا و سایر کشورهای دموکراتیک نوظهور همفکر – حتی بااینکه در زمان نگارش این مطالب دولت آمریکا کماکان کنترل عملکرد اصلی اینترنت را در دست دارد– مبنایی برای تحت‌فشار گذاشتن دولت آمریکا جهت تحقق این مورد و ایجاد ساختارهای مشخصی برای حکمرانی جامع‌تر اینترنت در اختیار داشتند.

امنیت، حریم خصوصی و حفاظت از داده‌ها

چالش فرهنگی ایجادشده به‌واسطه تعامل در چنین حوزه قانونی و فنی پیچیده‌ای، مانع اصلی پیش روی همکاری در حوزه امنیت سایبری محسوب می‌شود. این استدلال مطرح شده است که هدف برنامه‌های پایش و نظارت جمعی نظیر ابزار برنامه‌ریزی برای ادغام، هماهنگ‌سازی و مدیریت منابع (یا موارد دیگری نظیر برنامه بال‌ران[1]، اپ‌استریم[2] و سایر موارد) که توسط آمریکا و آژانس‌های اطلاعاتی آن اجرا می‌شوند، تضعیف رویکردهای مختلف اتخاذشده از طرف اتحادیه اروپا و ایالات‌متحده برای تأمین امنیت فضای سایبری و بدین ترتیب، مانع‌تراشی در سر راه همکاری فی‌مابین و درعین‌حال، تسهیل فرایند بازتابی برای احیای کارآمد این همکاری است.

1. Bullrun
2. Upstream

منطق و رویکردهای اتحادیه اروپا و ایالات‌متحده آمریکا

تنش بین آمریکا و اتحادیه اروپا بر سر برقراری موازنه بین تأمین امنیت و حفظ حریم خصوصی داده‌ها از این واقعیت نشئت می‌گیرد که سیاست امنیت سایبری آن‌ها تحت تأثیر منطق‌های متفاوتی است. مشخصه رویکرد اتحادیه اروپا، توجه قانونی به جرائم سایبری و تأکید بر دفاع سایبری و توانمندی‌های قدرت نرم است (Bendiek 2014; Christou 2014). درواقع، برخی حتی اتحادیه اروپا را قدرت سایبری غیرنظامی می‌نامند (Dunn Cavelty 2013). طبق فصول پیشین، توجه این اتحادیه در اصل، بر ایجاد اکوسیستم تاب‌آوری است که امکان حفاظت از طریق ظرفیت‌سازی و توانایی بازگشت و ترمیم [اکوسیستم] پس از حملات سایبری را به وجود می‌آورد. علاوه بر این، مفهوم امنیت تاب‌آور (به‌خصوص نوع سوم - ن.ک. فصل ۲) در رویکرد اتحادیه اروپا لحاظ شده است که در آن امنیت به معنای توانایی ایجاد توانمندی تهاجمی و دفاع از محیط سایبری نیست، بلکه مقوله امنیت به مفاهیم خلق سیستم‌های انطباق‌پذیر، تاب‌آور و قدرتمند و محیط نظارتی پیچیده‌ای توجه دارد که مشخصه اصلی آن وجود مسئولیت مشترک و حضور چندذینفع است. ازاین‌رو، ایجاد تاب‌آوری می‌تواند محرکی برای تضمین تأمین امنیت سایبری کارآمدتر در اروپا باشد و چنین رویکردی –حداقل در سطح اتحادیه اروپا، اگرنه در تمام کشورهای عضو این اتحادیه– تحت تأثیر منطق امنیتی‌ای نیست که بدون توجه به پیامدهای سوءاستفاده از قدرت، حقوق مدنی و درنهایت، امنیت شهروندان، اولویت را به جمع‌آوری داده‌ها با هدف برقراری امنیت، دهد (Ibid., p.8; Bigo et al. 2013; Bowden et al. 2013; Coaffee and Fussey 2015).

در مقابل، رویکرد آمریکا در قبال امنیت سایبری، حول محور مفاهیم بازدارندگی و دفاع نظامی است (برخوردار از جنبه تهاجمی برخلاف اتحادیه اروپا) (Lewis 2014; Sofaer et al. 2010) و شامل طیف وسیعی از اصول و اولویت‌ها است (ن.ک. کادر ۷-۱).

کادر ۷-۱. اولویت‌های امنیت سایبری ایالات‌متحده آمریکا

اولویت‌ها

۱. حفاظت از زیرساخت‌های حساس کشور مهم‌ترین سیستم‌های اطلاعات در برابر حملات سایبری.

۲. ارتقای توانایی در تشخیص و گزارش حوادث سایبری، بطوریکه بتوان به بهترین وجه پاسخ داد.

۳. تعامل با شرکای بین‌المللی برای ترویج آزادی اینترنت و حمایت از فضای سایبری باز، تعاملی، امن و قابل‌اتکا

۴. ایمن‌سازی شبکه‌های فدرال از طریق تعیین اهداف امنیتی مشخص و پاسخگو دانستن آژانس‌ها در تحقق آن اهداف

۵. ایجاد نیروی کار آگاه به موضوعات سایبری و فراتر رفتن از وضعیت کنونی در مشارکت یا بخش خصوصی

اصول

۱. رویکرد تمام دولتی

۲. اول دفاع از شبکه

۳. صیانت از حریم خصوص و آزادی‌های مدنی

۴. مشارکت عمومی-خصوصی

۵. همکاری و تعامل بین‌المللی

Source: http://www.whitehouse.gov/issues/foreign-policy/cybersecurity

اگرچه، چنین اولویت‌هایی تحت تأثیر این برداشت غالب قرار دارند که امنیت سایبری تهدیدی برای امنیت ملی تلقی می‌شود؛ تهدیدی که با افزایش قدرت سخت آمریکا در فضای سایبری از طریق به‌کارگیری ابزارهای نظامی به بهترین نحو رفع می‌گردد (Bendiek 2014, p.17; Stevens 2012)[۳]. برای مثال، کمیسیون امنیت سایبری مرکز مطالعات راهبردی و بین‌الملل[1] در گزارش خود (۲۰۰۸)، امنیت سایبری را «مسئله امنیت ملی مهمی» برای آمریکا توصیف کرد. در پی آن، بازبینی دقیق رئیس‌جمهور باراک اوباما از سیاست امنیت سایبری آمریکا، منجر

1. Center for strategic and International Studies (CSIS)

به سازماندهی مجدد توانمندی و راهبرد دفاع سایبری توسط وزارت دفاع آمریکا گردید که این اقدام تا حد زیادی امنیت سایبری را در جایگاهی معادل امنیت نظامی قرار داد که شامل حملات پیش‌دستانه نیز می‌شد.

بازتاب این اقدام در زمان پیوستن کارگروه‌های پیشین به ستاد فرماندهی سایبری آمریکا[1] که تحت فرمان ستاد فرماندهی راهبردی آمریکا[2] قرار دارد، در نهاد مسئول دفاع سایبری نیز ملاحظه شد (Porcedda 2012, p.48). وظایف اصلی ستاد فرماندهی سایبری آمریکا شامل دو مورد می‌شد: ۱) دفاع از شبکه‌های رایانه‌ای (جهت هماهنگی عملیات‌های دفاعی در برابر حملات سایبری)؛ ۲) عملیات علیه حملات سایبری (جهت ایجاد و تقویت توانمندی تهاجمی در برابر حملات سایبری). درواقع، با توجه به بروز خطرات سایبری شدیدتری از جانب بازیگران خارج از آمریکا (به‌عنوان‌مثال، جاسوسی سایبری چین)، راهبرد بین‌المللی فضای سایبری آمریکا[3] (۲۰۱۱) در مورد دوم، این مسئله را به‌صراحت بیان می‌کند که «آمریکا در زمان مقتضی نسبت به اقدامات خصمانه صورت‌گرفته در فضای سایبری به‌مانند هر تهدید دیگر [علیه این کشور]، واکنش نشان خواهد داد.» این نکته حائز اهمیت است که راهبرد دفاع و بازدارندگی ایالات‌متحده بر اساس توانایی ایجاد جو وحشت در میان دشمنان سایبری خود، از طریق افزایش نظامی‌سازی (توانمندی و قدرت) بوده است. این مسئله به‌رغم این واقعیت است که هر منطق بازدارندگی نیز به معنای خطوط «استناد» مشخص و به‌تبع آن اقدام متقابل است که به دلیل تضمین حدودی از گمنامی برای کاربران از جانب پروتکل‌های فنی، این موضوع همواره در فضای سایبری ممکن و عملی نیست. درواقع، حتی در صورت پیچیدگی کمتر استناد، مسئله اقدام متقابل مناسب و متناسب در واکنش به حملات سایبری کماکان بسیار بحث‌برانگیز است. اگرچه، قوانین جنگ سایبری در کتاب راهنمای تالین (۲۰۱۳) مطرح شده است.

علاوه بر تغییر نهادی، منابع مالی و انسانی قابل‌توجهی نیز برای تحقق اهداف ستاد فرماندهی سایبری آمریکا فراهم شده است. به‌عنوان‌مثال، رییس ستاد فرماندهی سایبری و آژانس امنیت

1. US Cyber Command (USCYBERCOM)
2. US Strategic Command
3. US International Strategy for Cyberspace

ملی آمریکا، ژنرال کیث الکساندر[1]، در دو سال گذشته، مشغول آماده‌سازی ۴۰ گروه مأمور سایبری جدید بوده است که ۱۳ گروه از آنها به حملات سایبری تهاجمی صورت‌گرفته علیه کشورهای دیگر و دشمنان سایبری رسیدگی می‌کنند. درمجموع، ژنرال الکساندر آن‌ها را گروه‌های «مدافع ملت» می‌نامد که «مشابه گردان‌ها در نیروی زمینی و تفنگداران دریایی یا گردان‌های هوایی حاضر در نیروی دریایی و هوایی هستند ... آن‌ها با برخورداری از مجموعه مهارت‌های عملیاتی و اطلاعاتی و ترکیبی از کارکنان نظامی و غیرنظامی، در مدت‌زمان کوتاهی می‌توانند عملیات خود را به‌طور مستقل اجرا کنند» (Pentagon creates 13 offensive cyber teams 2013). تعداد نیروهای به کار گرفته‌شده در ستاد فرماندهی سایبری آمریکا نیز از زمان تأسیس آن تاکنون چهار برابر شده است (نزدیک به ۵ هزار نفر) و منابع مالی امنیت سایبری نیز برای حمایت از اقدامات دولت آمریکا سالیانه افزایش یافته است. به‌عنوان‌مثال، در سال ۲۰۱۳ بودجه امنیت سایبری ۵۲/۶ میلیارد دلار - به‌اضافه ۱۴ میلیارد دلار دیگر درخواست‌شده برای سال مالی ۲۰۱۶ - بود (Obama seeks $14 billion to boost US cybersecurity defences 2015). دوسوم این بودجه از سال ۲۰۱۳ توسط سازمان اطلاعات مرکزی آمریکا (سیا)[2]، آژانس امنیت ملی آمریکا و دفتر ملی شناسایی[3]، درخواست و هزینه شده است (Bendiek 2014, p.16)، درواقع، پنتاگون به‌تنهایی ۵/۵ میلیارد دلار برای بودجه سال ۲۰۱۶ درخواست کرد (این مقدار در سال ۲۰۱۴ برابر با ۴/۷ میلیارد دلار بود).

اقدامات نشئت‌گرفته از این منطق تهاجمی و منابع پشتیبان آن به بُعد اطلاعاتی نیز سرایت کرده‌اند و پیامدهای جدی ازنظر نحوه جمع‌آوری و بهره‌گیری دولت ایالات‌متحده و آژانس‌های اطلاعاتی آن از داده‌ها جهت مقابله با تهدید ملی ناشی از مسائل امنیت سایبری دارند. به‌عنوان‌مثال، جامعه اطلاعاتی آمریکا به‌طور منظم در عملیات‌های سایبری تهاجمی شرکت می‌کند - بنا به اسناد افشاشده (ویکی لیکس)، درمجموع ۲۱۳ مورد در سال ۲۰۱۱ - و سایر طرح‌های بودجه‌بندی‌شده نیز با هدف نفوذ به شبکه‌های خارجی از طریق جاسازی بدافزارهای پیچیده در رایانه‌ها، مسیریاب‌ها و فایروال‌ها به کار می‌روند

1. Keith Alexander
2. Central Intelligence Agency (CIA)
3. National Reconnaissance Office (NRO)

(Gellman and Na kashima 2013). طرح‌هایی نیز در مرحله بعد عملیات‌های سایبری تهاجمی آژانس‌های جاسوسی آمریکا برای به‌کارگیری سیستم خودکاری به نام توربین[1] وجود دارند که می‌تواند جاسازی میلیون‌ها بدافزار برای جمع‌آوری اطلاعات و حمله به دستگاه‌ها را مدیریت کند (Chan 2013). به‌علاوه، این استدلال مطرح گردید که آژانس امنیت ملی آمریکا «موارد آسیب‌پذیری روز صفر[2]» را خریداری و در سیستم‌عامل‌ها و سخت‌افزارهای کنونی جاسازی کرده است تا بدافزارهای خود را به نقاط حساس متعددی در زیرساخت اینترنت وارد کند (Dunn Cavelty 2014; Greenwald and MacAskill 2013). به‌علاوه، این مسئله نیز مشخص شد که منابع مورداستفاده دولت آمریکا برای رمزگشایی استانداردهای رمزنگاری موجود، بیشتر موجب آسیب‌پذیری چنین سیستم‌های رمزنگاری شده است. (Dunn Cavelty 2014; Clarke et al. 2013)

این استدلال نیز مطرح می‌شود که چنین فعالیت‌هایی پیامدهای جدی برای تأمین امنیت تاب‌آور دارند و در تضاد کامل با منطق مبنای امنیت سایبری اتحادیه اروپا (البته نه لزوماً برخی کشورهای اتحادیه اروپا) هستند. آن‌ها بازار (و مشوقی) برای تولید و فروش چنین نقاط آسیب‌پذیری ایجاد می-کنند و این برنامه‌های پنهانی[3] و خفته[4] را می‌توان در هر زمان و برای مقاصد متفاوتی (اختلال، نظارت و سایر موارد) به کار برد که این موضوع درنهایت منجر به ناامنی و آسیب‌پذیری بیشتر می‌شود و درعین‌حال، تأثیر منفی نیز بر اعتماد به فضای سایبری می‌گذارد. به نظر دان کاولتی (2013, p.9) ، کشورهایی که برنامه‌های پنهانی را در سیستم‌های رایانه‌ای تعبیه می‌کنند، نمی‌توانند کنترل مستمر خود بر آن‌ها را تضمین کنند و درنتیجه، این نقاط آسیب‌پذیر عملاً مورد بهره‌برداری همان مجرمان سایبری، هکرها و تروریست‌هایی قرار می‌گیرند که چنین تدابیری به دنبال مقابله با آن‌ها هستند. چنین اقداماتی که تحت تأثیر منطق امنیت ملی قرار دارند می‌توانند موجب افزایش تهدید سایبری برای دولت‌ها و شهروندان به یک

1. TURBINE
2. Zeroday Vulnerabilities
نقاط آسیب‌پذیر ناشناخته‌ای در نرم‌افزارهای رایانه‌ای که هکر می‌تواند با شناسایی آن‌ها به هدف خود آسیب وارد کند. (م.)
3. Backdoor
راه مخفی به سیستم رایانه‌ای (م.)
4. Sleeper Program
برنامه رایانه‌ای که مدت زیادی بدون شناخته شدن در سیستم هدف، باقی می‌ماند و در هنگام مناسب برای ضربه زدن به سیستم مورداستفاده قرار می‌گیرد. (م.)

نسبت شوند و تأثیر منفی بر تاب‌آوری اکوسیستم‌ها از طریق ایجاد مستقیم یا غیرمستقیم نقاط آسیب‌پذیر داشته باشد.

امنیت شبکه و اطلاعات: حفاظت از زیرساخت‌های حیاتی

با وجود تفاوت اساسی منطق‌های اتحادیه اروپا و ایالات‌متحده آمریکا در مورد دفاع سایبری، در زمینه مسئله امنیت شبکه و اطلاعات و به‌ویژه حفاظت از زیرساخت‌های حیاتی حداقل نوعی همگرایی در مورد ضرورت نظارت و وجود فراحکمرانی عملی‌تری در مورد گزارش‌دهی، حتی به‌رغم مخالفت اتحادیه اروپا (برای کسب اطلاعات بیشتر ن.ک. فصل ۶) و آمریکا با اتخاذ رویکردی الزام‌آور، وجود دارد.

آژانس امنیت شبکه و اطلاعات اتحادیه اروپا در گزارش چشم‌انداز تهدید سالانه خود (ENISA Threat Landscape 2013, 2014) کماکان بر خطرات مرتبط و پیامدهای احتمالی حملات سایبری به زیرساخت‌های حیاتی تأکید دارد.[۴] امریه امنیت شبکه و اطلاعات (ن.ک. فصل ۶) پس از تصویب در پارلمان اروپا در مارس ۲۰۱۴، در زمان نگارش این کتاب، کماکان در شورای وزیران اتحادیه اروپا در جریان بحث و بررسی بوده است. اگرچه، صرف‌نظر از توافق صورت‌گرفته در این شورا، توجه کمتری در توافق نهایی به بخش‌ها و عاملان بازار ازنظر گزارش‌دهی الزام‌آور حوادث می‌شود که علت اصلی آن انجام اصلاحاتی از جانب کمیته حمایت از بازار داخلی و مصرف‌کنندگان[1] پارلمان اروپا است (Pearse et al. 2015; Long 2014). علاوه بر این، احتمال دارد دولت‌های عضو، از اختیارات بسیار بیشتری در زمینه گنجاندن مدیریت دولتی تحت این دستورالعمل برخوردار باشند و بدین ترتیب امکان بیشتری برای وضع ترتیبات داوطلبانه بین دولت و بخش خصوصی فراهم کنند. ازاین‌رو، باوجوداینکه مسلماً دستورالعمل امنیت شبکه و اطلاعات زمینه استقرار مقامات ذی‌صلاح امنیت شبکه و اطلاعات را در دولت‌های عضو اتحادیه اروپا فراهم می‌کند که بر پیروی از این دستورالعمل نظارت دارند، راهبرد امنیت شبکه و اطلاعات را ترویج می‌کنند و اطلاعات مربوط به حملات و تهدیدهای

1. Internal Market and Consumer Protection Committee (IMCO)

امنیت سایبری را دریافت و سازمان‌دهی کرده و به اشتراک می‌گذارند، اما تاب‌آوری تفسیر و تقلیل حوزه این دستورالعمل ممکن است تأثیر نامطلوبی بر کیفیت نهادهای ایجادشده و انسجام و اشتراک اطلاعات معتبر داشته باشد.

در ایالات‌متحده آمریکا، تیم واکنش اضطراری سایبری سیستم‌های کنترل صنعتی[1] و سازمان‌هایی مانند شورای ملی پژوهش[2] گزارش‌هایی درخصوص افزایش تعداد حملات سایبری بر زیرساخت‌های حیاتی داده‌اند و تأثیر احتمالی آن‌ها را تا حد زیادی در نظر گرفته‌اند. ازنظر برخی محققان، این مسئله موجب تشدید احساس ضرورت بعضی نهادهای دولتی آمریکا برای انجام فعالیت بیشتر، با هدف ایجاد تدابیری جهت حفاظت از زیرساخت‌های حیاتی ملی، به‌ویژه در رابطه با بخش خصوصی شده است (Titch 2013, p.3). واحدهای تجاری، طرفداران حقوق مدنی و مدافعان حریم خصوصی در اینترنت و بخش‌های مختلف دولت آمریکا مخالفت بسیاری با قوانین پیشنهادی داشته‌اند (ن.ک. مبحث بعدی) که نتیجه آن در آمریکا اعتماد به «بازار» داوطلبانه و رویکرد فراحکمرانی «نظری» به اشتراک اطلاعات بین دولت و تأمین‌کنندگان زیرساخت‌های حیاتی ملی، به‌رغم اقدامات صورت گرفته برای طرح گزارش‌دهی الزام‌آور بوده است.

برای تبیین بیشتر این موضوع، ذکر این نکته لازم است که در موارد متعددی در طی چند سال گذشته لوایحی به کنگره فرستاده شده است که می‌تواند موجب تسهیل اشتراک الزام‌آور اطلاعات در زمینه تهدیدها و حملات سایبری بین دولت آمریکا و تأمین‌کنندگان زیرساخت‌های بخش خصوصی مربوطه گردد. به‌عنوان‌مثال، قانون حفاظت و اشتراک اطلاعات سایبری[3] در ۳۰ نوامبر ۲۰۱۱ (با حضور ۱۱۱ حامی مشترک) مطرح گردید. اگرچه این قانون با اکثریت آراء در آوریل ۲۰۱۲ در مجلس نمایندگان تصویب شد، اما در مجلس سنا رأی نیاورد. دلیل اصلی این موضوع نیز ترس از این مسئله بود که درنهایت کاخ سفید این قانون را به دلیل فقدان تدابیر امنیتی کافی در حوزه آزادی‌های مدنی و امور محرمانه و عدم ایجاد انگیزه لازم در

1. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
2. National Research Council (NRC)
3. Cyber Intelligence Sharing and Protection Act (CISPA)

بخش خصوصی برای پذیرش استانداردها و پروتکل‌های امنیت سایبری وتو نماید. افراد بسیاری این پرسش را مطرح کرده‌اند که چنین لایحه‌ای تا چه حد با قوانین مربوط به تدابیر امنیتی مطرح‌شده نظیر قانون حفظ حریم خصوصی ارتباطات الکترونیکی[1] همخوانی دارد (Titch 2013, p.4–10). با وجود ارائه مجدد این لایحه در سال‌های ۲۰۱۳، ۲۰۱۴ (مانند قانون اشتراک اطلاعات امنیت سایبری[2]) و ۲۰۱۵، نتیجه خاصی به دست نیامد و در زمان نگارش این مجلد (مارس ۲۰۱۵)، این لایحه برای ارزیابی ضرورت طرح آن در مجلس نمایندگان برای رأی‌گیری مجدد، به کمیته اطلاعات ارجاع داده شد.

به دلیل عدم تصویب لایحه فوق، فرمان اجرایی ۱۳۶۳۶ در فوریه ۲۰۱۳ توسط باراک اوباما، رئیس‌جمهور آمریکا، صادر شد که یکی از اهداف اصلی آن ایجاد چارچوب و راهنمای داوطلبانه‌ای برای ارتقای سطح حفاظت از زیرساخت‌های حیاتی ملی بود(۵)، یعنی وضع قوانینی که بتواند هدایت اشتراک اطلاعات بین دولت آمریکا و صاحبان و عاملان زیرساخت‌های حیاتی را بر عهده بگیرند و موجب تسهیل و ترغیب اجرای استانداردهای حداقلی امنیت سایبری شوند. مؤسسه ملی استاندارد و فناوری[3] مسئول ایجاد این چارچوب در فوریه ۲۰۱۴ و توسعه روش مقرون‌به‌صرفه‌ای «برای کاهش خطرات سایبری برای زیرساخت‌های حیاتی» بود (Pearse et al. 2015). به‌علاوه، این مؤسسه در کنار وزارت امنیت داخلی[4] و وزارت دفاع وظیفه مشارکت با صاحبان و عاملان زیرساخت‌های حیاتی ملی و ایجاد چارچوب امنیت سایبری را بر عهده داشت:

- روش جدید اشتراک اطلاعات، جهت ارائه اطلاعات محرمانه و غیرمحرمانه در مورد تهدیدها و حملات به شرکت‌های آمریکایی
- برنامه داوطلبانه‌ای برای ترویج به‌کارگیری این چارچوب
- بازبینی قوانین موجود درخصوص امنیت سایبری
- حفاظت شدید از حریم خصوصی و آزادی‌های مدنی بر اساس اصول به‌کارگیری منصفانه اطلاعات[5] (EO 13636: Improving Critical Infrastructure Cybersecurity 2014)

1. Electronic Communications Privacy Act (ECPA)
2. Cybersecurity Information Sharing Act
3. National Institute for Standards and Technology (NIST)
4. Department of Homeland Security (DHS)
5. Fair Information Practice Principles

همانند دستورالعمل اولیه امنیت شبکه و اطلاعات پیشنهادی کمیسیون اروپا، دامنه چارچوب عملکرد ایالات‌متحده آمریکا [در حوزه امنیت سایبری] گسترده است و شامل طیف وسیعی از بخش‌ها و درواقع مشوق‌هایی برای به‌کارگیری این چارچوب در بخش‌هایی مانند تضمین امنیت سایبری و کمک‌های مالی و تحقیقات در زمینه امنیت سایبری است. این طرح‌های مربوط به سیاست‌گذاری، در راهبرد سایبری اتحادیه اروپا و به نحو متفاوتی در راهبردهای کشورهای عضو مطرحی مانند بریتانیا نیز ملاحظه شده است. بر این اساس، رویکرد دولت اوباما و اتحادیه اروپا ازنظر تمایل به اجرای استانداردهای امنیت سایبری حداقلی و ایجاد انگیزه برای به‌کارگیری این استانداردها و اشتراک اطلاعات مشابه است. در ضمن، توافقی نیز در این زمینه وجود دارد که رویکرد اتخاذشده باید مبتنی بر قوانین و نظارت باشد. باوجوداینکه مجلس سنای آمریکا و افراد مهم دیگری از این کشور همواره مخالف این موضوع بوده‌اند، اما تعهد الزام‌آور به گزارش‌دهی (به‌رغم تردید کشورهای عضو مطرح) در متن دستورالعمل امنیت شبکه و اطلاعات اتحادیه اروپا گنجانده شده است، حتی اگر متن نهایی آن موجب کاهش دامنه و نفوذ آن گردد. بااینکه این امر بیانگر همگرایی طرفین در زمینه تأمل پیرامون موضوع چگونگی افزایش امنیت سایبری تاب‌آور بین آن‌ها ازنظر حفاظت از زیرساخت‌های حیاتی است، این استدلال نیز مطرح است که اگر این رویکردها در عمل منجر به ایجاد اقدامات متفاوتی گردند، این امر باعث ایجاد تناقضاتی در گزارش‌دهی و به‌تبع آن واکنش نسبت به تهدیدات سایبری احتمالی، با توجه به ماهیت جهان‌شمول جرائم سایبری نیز می‌شود. علاوه بر این، بحث در آمریکا پیرامون اتخاذ رویکردی الزام‌آور به اشتراک اطلاعات، بیانگر حساسیت چنین موضوعی ازنظر حقوق شهروندان این کشور است و از طرف دیگر، بیانگر اختلافات احتمالی بین آمریکا و اتحادیه اروپا، در زمینه رابطه بین حفظ حریم خصوصی، آزادی و تأمین امنیت با توجه به منطق‌های مبنای رسیدگی به این مسائل است.

حریم و حفاظت از داده‌ها

برخی، گفتگوها بین اتحادیه اروپا و آمریکا در مورد حفظ حریم خصوصی داده‌ها را با توجه

به دیدگاه، فرهنگ و سیستم قانونی متفاوت آن‌ها «دشوار» تلقی می‌کنند، به‌خصوص که این اختلافات بر اثر افشاگری‌های اسنودن تشدید نیز شده است (Kerry 2014; see also Bygrave 2013). به همین ترتیب، گفتگو بین اعضای اتحادیه اروپا در مورد رابطه بین برقراری امنیت و حفظ حریم خصوصی داده‌ها نیز به همان اندازه دشوار است. برخی کشورها مانند بریتانیا (ستاد ارتباطات دولتی)، در اقدامات نظارتی و جاسوسی آژانس امنیت ملی آمریکا همدست بوده‌اند که این امر بیانگر اختلافات درونی اتحادیه اروپا در مورد زمان و نحوه جمع‌آوری، ذخیره‌سازی و بهره‌گیری از داده‌ها برای مقاصد امنیتی و ضد تروریستی است.

چنین اقداماتی در گزارش کمیته آزادی‌های مدنی پارلمان اروپا در زمینه نظارت و جاسوسی جمعی مطرح و محکوم شدند. درواقع، انتقاداتی نیز در مورد نظارت و جاسوسی جمعی و به‌خصوص عدم صلاحیت کمیته‌های نظارتی کشورهای اتحادیه اروپا برای پاسخ‌گویی در سطح سیاسی (مشروعیت دموکراتیک) یا فنی (جاسازی برنامه‌های پنهانی و عدم‌اصلاح نقاط آسیب‌پذیر) از جانب بریتانیا، آمریکا و حتی فرانسه، آلمان و سوئد مطرح گردید (European Parliament 2013; see also Bigo et al. 2013). کمیسیون اروپا و به‌خصوص ویوین ردینگ[1]، قائم‌مقام این کمیسیون و کمیسیونر امور دادگستری، حقوق اساسی و شهروندی، در هنگام افشاگری اسنودن (ژوئن ۲۰۱۳)، در پیامی صریح اعلام کرد که «چنین اقداماتی پیامدهای بسیار نامطلوبی برای حقوق اساسی شهروندان اتحادیه اروپا دارند» (Reding 2013) و بیان کرد هیچ مصالحه‌ای در مورد استانداردهای حفاظت از داده‌های شهروندان اروپا انجام نمی‌شود. بااینکه ردینگ این مسئله را پذیرفت که امنیت ملی موضوعی مربوط به کشورهای عضو اتحادیه اروپا است، اما مورد اسنودن نشان داد که ایجاد چارچوب قانونی مشخصی برای حفاظت از داده‌های شخصی مسئله بی‌موردی محسوب نمی‌شود، بلکه، موضوعی کاملاً ضروری و حق اساسی تمام شهروندان اتحادیه اروپا است (cited in Watt 2013). البته، ردینگ مسئله حمایت از توسعه ابر[2] اروپا(۶)، به‌عنوان گزینه جایگزین برای تضمین امنیت داده‌های اروپا را نیز

1. Vivienne Reding
2. Cloud

شبکه خدمات پردازشی و تبادل اطلاعات که به‌عنوان بستری برای فعالیت‌های مبتنی بر فناوری اطلاعات به کار می‌رود. (م.)

مطرح کرد (ن.ک. Venkatraman 2013).

اقدامات نظارت و جاسوسی جمعی آژانس امنیت ملی آمریکا با مجوز دولت این کشور به‌واسطه منطق «امنیت ملی» و مجموعه قوانین آمریکا توجیه می‌شد که مبنای رویکرد آمریکا به امنیت سایبری بود. گزارش کارگروه موردی اتحادیه اروپا-آمریکا در حفاظت از داده‌ها (۲۰۱۳) بر مبنای قانون آمریکا تأکید داشت که اقدامات نظارتی بر اساس آن صورت می‌گرفت. دو عنصر اساسی این مبنای قانونی، اجازه جمع‌آوری داده‌های شخصی را در اختیار آژانس‌های اطلاعاتی آمریکا قرار می‌داد: نخست، بخش دوم قانون نظارت بر امور خارجی[1] و دوم، بخش ۲۱۵ قانون میهن‌پرستی ۲۰۰۱ آمریکا[2]. مجوز و نظارت بر جمع‌آوری اطلاعات توسط دادگاه ناظر بر اعمال قانون نظارت بر امور خارجی، تحت این قوانین انجام می‌شود. قوانین دیگری نیز امکان جمع‌آوری اطلاعات خارجی را ایجاد می‌کنند –مانند فرمان اجرایی ۱۲۳۳۳– که هیچ‌گونه نظارت قضایی بر آن‌ها وجود ندارد، اما اقدامات صورت‌گرفته تحت این «فرمان نباید قانون اساسی آمریکا یا قوانین موضوعه مربوطه را نقض کنند» (Ibid). در این مورد قانون اساسی آمریکا از شهروندان این کشور در برابر جمع‌آوری داده‌ها تحت متمم چهارم محافظت می‌کند که در آن «جستجو و توقیف بی‌دلیل» ممنوع اعلام شده است و بر اساس آن، حکم جلب باید بر مبنای «شواهد و ادله کافی» صادر گردد. گرچه، این حفاظت شامل اتباع غیرآمریکایی نمی‌شود، مگر اینکه جزئی از جامعه آمریکا شده باشند که این موضوع مسئله میزان حفاظت از داده‌های شهروندان اروپایی در زمان به‌کارگیری سرویس‌های برخط آمریکا را مطرح می‌کند.(۷) اشتراک و به‌کارگیری داده‌های شخصی شهروندان در آمریکا به‌واسطه مجموعه قوانین بخش‌های مختلف نیز، حفاظت می‌شود که این قوانین را کمیسیون فدرال تجارت[3] در صورتی اجرا می‌کند که شرکت‌ها سیاست‌های مربوط به حفظ حریم خصوصی را نقض کنند (Kerry 2014, p.2).

افشاگری‌های صورت‌گرفته درخصوص عملکرد آژانس امنیت ملی آمریکا، مسائل اخلاقی و قانونی در مورد برقراری موازنه بین حفظ حریم خصوصی و حقوق –در آمریکا و اتحادیه اروپا– و البته، ضرورت و تناسب حدود اختیارات نظارتی آمریکا در مورد شهروندان و سران کشورهای

1. Foreign Affairs Surveillance Act (FISA)
2. USA Patriot Act
3. Federal Trade Commission

اروپایی برای منافع امنیت ملی را مطرح کرد (European Commission 2013e; Bendiek 2014, p.20). به‌عبارت‌دیگر، افشای این اقدامات مسئله سازگاری «فرهنگ‌های» امنیت سایبری طرفین در زمان جمع‌آوری داده‌های شخصی و به‌کارگیری آن‌ها برای اهداف امنیتی را با توجه به منطق زیربنای رویکردهای اتخاذشده مطرح کرد. این مسئله نیز باعث تحرک بیشتری در اصلاحات جاری در حوزه حفظ حریم خصوصی و حفاظت از داده‌ها در اتحادیه اروپا (the EU's 1995 Data Protection Directive) و در آمریکا (the Consumer Privacy Bill of Rights) گردید و موجب تسهیل موارد بازنگری جدید قوانین موجود و توافقات فراآتلانتیک در زمینه جریان داده‌هایی شد که باید حقوق شهروندی را بازگردانده و تضمین می‌کردند و اعتماد طرفین را نیز مجدداً جلب می‌نمودند.

ازجمله این توافقات می‌توان به توافق بندرگاه امن[1] اشاره کرد (European Commission 520/2000/EC) که با هدف تضمین حفاظت کافی از انتقال داده‌های شخصی از اتحادیه اروپا اجرایی شده بود (European Commission 2013d, p.2). این توافق در اصل اصولی را (ن.ک. کادر ۷-۲) برای حفاظت از حریم خصوصی مطرح می‌کرد که شرکت‌های آمریکایی عامل انتقال داده‌ها در مورد شهروندان اتحادیه اروپا باید از طریق خودتصدیقی به آن پایبند باشند. بااینکه امضای چنین ترتیباتی داوطلبانه بود، پایبندی به قوانین آن، در صورت امضای آن، داوطلبانه نبود. بازنگری توافق بندرگاه امن که در سال ۲۰۱۳ توسط کمسیون اروپا انجام شد، این مطلب را نشان داد که تعداد بی‌شماری از ۳۲۴۶ شرکتی که این توافق را امضا کرده بودند، تعهدات آن را رعایت نمی‌کردند (Ibid., p.4) و گزارش‌های مستقل دیگر نیز مؤید افزایش موارد نقض این اصول به‌مرورزمان بود (ن.ک. Bendiek 2014, p.21). اگرچه با توجه به درخواست‌های اولیه پارلمان اروپا برای تعلیق توافق بندرگاه امن و سخنان ویوین ردینگ مبنی بر تبدیل توافق بندرگاه امن به روزنه احتمالی برای تضعیف قوانین حفاظتی اتحادیه اروپا، اصلاحات پیشنهادی کمیسیون اروپا در این زمینه چندان جدی نبودند (Alden 2014).

1. Safe Harbour agreement

کادر ۷-۲. بندرگاه امن: اصول اساسی اصلی

۱. شفافیت پایبندی به سیاست‌های حریم خصوصی شرکت‌ها

۲. ادغام اصول بندرگاه امن در سیاست‌های حریم خصوصی شرکت‌ها

۳. انجام، از طریق مراجع عمومی

Source: European Commission (2013d, p.2)

محورهای توصیه‌های اصلی برای تقویت اصول حریم خصوصی بندرگاه امن در این زمینه عبارت بودند از: دسترس‌پذیری بیشتر افراد به مورد حل اختلاف؛ تضمین حفاظت از داده‌ها در زمان انتقال آن‌ها به پردازشگر ثالث؛ شفافیت بیشتر قوانین حریم خصوصی شرکت‌های عضو توافق بندرگاه امن و بررسی امکان جمع‌آوری داده‌ها تحت قوانین و مقررات آمریکا [از این شرکت‌ها] و توسعه فرایندها و ابزارهایی برای اجرای اصول این توافق (European Commission 2013d, p.14–19). با توجه به اهمیت این توافق و مقررات کافی آن در زمینه جریان داده‌ها و حریم خصوصی برای انجام مذاکرات مشابه پیرامون توافق مشارکت تجاری و سرمایه‌گذاری فراآتلانتیک، نارسایی این توصیه‌ها موردانتقاد برخی قرار گرفته است، اما کمیسون اروپا آن‌ها را برای «بهبود عملکرد توافق بندرگاه امن کافی» می‌داند (Reding cited in Saran 2014). از دیدگاه ایالات‌متحده، جریان داده‌ها موضوعی قابل‌مذاکره در موافقت‌نامه مشارکت تجاری و سرمایه-گذاری فراآتلانتیک است، اما از منظر اتحادیه اروپا، این مورد به دلیل اینکه حفاظت شدید از داده‌ها و حقوق حریم خصوصی در این توافقنامه غیرقابل‌مذاکره هستند، از دستورکار [مذاکرات] حذف شده است که در صورت عدم کسب توافق در زمینه همکاری در مورد سیستم‌های حفاظت از حریم خصوصی و داده‌ها، این موضوع مسلماً مانعی در برابر همکاری‌های آتی ایجاد خواهد کرد.

باوجوداینکه بندرگاه امن، توافقی خاص ابعاد اقتصادی و تجاری جریان داده‌ها و حفاظت از آن‌ها محسوب می‌شود، اما با توجه به مسئله میزان دسترسی دولت آمریکا به داده‌های ذخیره‌شده توسط شرکت‌های خصوصی که بسیاری از آن‌ها در سطح بین‌المللی فعالیت می‌کنند، پیامدهای آن (یعنی همکاری در زمینه امور کیفری) بسیار گسترده‌تر است. این موضوع در مورد

پیش‌نویس پیشنهادی اتحادیه اروپا درباره مقررات کلی حفاظت از داده‌ها[1] نیز صدق می‌کند که هدف آن گسترش و هماهنگ‌سازی استانداردهای حفاظت از داده‌ها در کل اتحادیه اروپا و افزایش تدابیر امنیتی، حقوق و روش‌های اجرای قانون در زمان به‌کارگیری داده‌های اروپا در داخل یا خارج از اتحادیه اروپا است[۸] (GDPR 2014). مقررات کلی حفاظت از داده‌ها و مذاکرات آن بحث‌برانگیز بود، چراکه پارلمان اروپا بند ضد قانون نظارت بر امور خارجی (در دوره پس از اسنودن) (Bendiek 2014, p.21) و ماده ۴۲ را مطرح کرد که می‌توانست در حکم پایان کار توافق بندرگاه امن باشد (Kerry 2014, p.4).

باوجوداینکه این موارد در نسخه نهایی موردتوافق پارلمان اروپا در مارس ۲۰۱۴ مطرح نشدند،[۹] لابی‌گری شدید حاکم بر پارلمان بدین معنا بود که ۳۹۹۹ اصلاحیه از جانب کمیته آزادی‌های مدنی، امور کشور و دادگستری[2] در پیشنهاد اولیه کمیسیون (ژانویه ۲۰۱۲) اعمال گردید. نسخه موردتوافق در زمان نگارش این سطور (مارس ۲۰۱۵) در شورای وزیران موردبحث قرار دارد و موضوعات مهمی نظیر حق حذف، رضایت آگاهانه و انتقال داده‌ها به کشورهای ثالث باید کماکان حل‌وفصل شوند. چنین مسائلی –مانند مسئله انتقال داده‌ها به اشخاص یا کشورهای ثالث که پس از لابی‌گری شدید دولت آمریکا از طرح پیشنهادی اولیه کمیسیون حذف شد و پارلمان اروپا مجدداً آن را در نسخه نهایی گنجاند– در طول فرایند مذاکرات، بحث‌برانگیز هستند. کشورهای عضو تاکنون این رویکرد را در نسخه خود وارد نکرده‌اند و حذف آن می‌تواند حقوق شهروندان اروپا را ازنظر به‌کارگیری و انتقال داده‌ها تا حد زیادی تضعیف نماید. در موضوع رضایت آگاهانه نیز به‌رغم تأکید کمیسیون و نسخه نهایی پارلمان اروپا بر رضایت صریح، یعنی موافقت یا مخالفت آگاهانه افراد از به‌کارگیری و انتقال داده‌های خود [توسط دولت‌ها]– کشورهای عضو کماکان بر مفهوم مبهم‌تر رضایت «غیرمبهم» تکیه دارند که ازنظر برخی احتمال دارد «بهانه ساده‌ای در اختیار کنترل‌کنندگان داده‌ها» قرار دهد تا رضایت کاربران را در این زمینه جلب نکنند و درنتیجه، سطح حفاظت از داده‌ها از سطح مدنظر کاهش یابد (Albrecht 2015).

1. General Data Protection Regulation (GDPR)
2. Civil Liberties, Justice and Home Affairs Committee (LIBE)

علاوه بر این، اتحادیه اروپا و ایالات‌متحده آمریکا توافقات خاصی نیز در زمینه به‌کارگیری و انتقال داده‌ها در حوزه امور پلیسی و قضایی دارند و مذاکراتی نیز در زمینه «توافق چتری»[1] در این حوزه در حال انجام است که هدف آن «تضمین حفاظت شدید از داده‌ها در راستای مجموعه مقررات حقوقی داخلی اروپا در زمینه حفاظت از داده‌های اتحادیه اروپا برای شهروندانی است که داده‌های آن‌ها به آمریکا منتقل می‌شود و بدین ترتیب، همکاری بین اروپا و آمریکا در مقابله علیه جرائم و تروریسم» نیز بیشتر تقویت می‌گردد (European Commission 2013e). مباحث و اختلافاتی در مورد سطوح حفاظت از داده‌های خصوصی قبل و به‌خصوص بعد از افشاگری‌های اسنودن در موردتوافق ثبت‌نام و مشخصات مسافران در خطوط هوائی (انتقال اطلاعات پرواز)، برنامه ردیابیمالی تروریست‌ها[2] (تبادل داده‌های مالی از طریق سیستم سوئیفت) و موافقت‌نامه همکاری دوجانبه حقوقی[3] (تسهیل تبادل اطلاعات و مدارک در تحقیقات جنایی برون‌مرزی) مطرح شدند. در اصل، مذاکرات پیرامون توافق چتری ازنظر اتحادیه اروپا مستلزم تضمین همان سطح حفاظت از داده‌های مدنظر مقررات کلی حفاظت از داده‌ها، برای انتقال داده‌ها در حوزه همکاری پلیسی و قضایی در زمینه امور کیفری بود (European Commission 2013d).

مسئله برخورداری شهروندان اروپایی غیرمقیم در آمریکا از حق جبران حقوقی و تدابیر امنیتی مشابه شهروندان آمریکایی، موضوع اصلی این مذاکرات است. در فضای افزایش تردید عمومی در ایالات‌متحده و پیامدهای اقتصادی نظارت و جاسوسی جمعی با هدف تأمین امنیت، دولت اوباما «گام بی‌سابقه‌ای در جهت گسترش برخی موارد حفاظت از ... مردم آمریکا به اروپاییان» برداشت (Kerry 2014, p.10) که طبق آن قانون حفظ حریم خصوصی آمریکا[4] (۱۹۷۴) باید بازبینی گردد تا شامل اتباع غیرآمریکایی نیز شود. اگرچه، در عمل، این تعهد دولت اوباما هنوز منجر به اتخاذ راه‌حل عملی از طریق قانون‌گذاری در کنگره نشده است. علاوه بر این، حتی در صورت یافتن سازوکار مناسبی برای اعطای جبران حقوقی به شهروندان اروپایی مقیم آمریکا، ازنظر بعضی «این امر به معنای پایان کار یا حتی شفافیت موارد نقض کلی حقوق شهروندان

1. Umbrella Agreement توافق بین دو طرف در مورد قوانین اعمال‌شده به توافقات خاص بین طرفین. م
2. Terrorist Finance Tracking Program (TFTP)
3. Mutual Legal Assistance Agreement (MLA)
4. US Privacy Act

اروپا توسط برنامه‌های جاسوسی جمعی بسیار محرمانه آمریکا نیست»، چراکه قانون حفظ حریم خصوصی سال ۱۹۷۴ دارای موارد استثنا است و شامل داده‌های جمع‌آوری‌شده برای آژانس امنیت ملی آمریکا و سایر برنامه‌های امنیت ملی نمی‌شود (Micek and Masse 2014). به‌علاوه، توافقی در مورد موضوع بسیار مهم محدودسازی انتقال داده‌ها بنا به اهداف خاص مربوط به اجرای قانون برای پردازش این داده‌ها فقط برای این اهداف حاصل نشده است (European Commission 2014).

بااین‌وجود، به دلیل بازبینی مورد درخواست رئیس‌جمهور اوباما از فناوری اطلاعات و ارتباطات[1] (در مورد این گزارش، ن.ک. Clarke et al 2013)، اصلاحاتی ازجمله «انتشار تصمیمات دادگاه ناظر بر اعمال قانون نظارت بر امور خارجی و سایر مطالب اطلاعاتی و امنیتی» انجام شده است که ازنظر برخی، شفافیت بیشتری در مورد جمع‌آوری اطلاعات خارجی توسط آمریکا ایجاد کرده است (Kerry 2014, p.10). تدابیر دیگر شامل اعمال محدودیت‌هایی بر جمع‌آوری و به‌کارگیری داده‌ها با افزایش آزادی مدنی و حفاظت از حریم خصوصی تحت بخش ۲۱۵ قانون میهن‌پرستی آمریکا و بخش ۷۰۲ قانون نظارت بر امور خارجی و ایجاد سازوکارهای بیشتر برای حفاظت از افشاگران است (Office of the Director of National Intelligence 2015). به‌علاوه، کارگروه داده‌های حجیم[2] به ریاست جان پودستا[3]، مشاور اوباما، تشکیل شد که تعهداتی در قبال پیشرفت قانون حفظ حریم خصوصی مصرف‌کنندگان[4] در آمریکا داشته و اجرای آن‌ها توسط کمیسیون فدرال تجارت را قانونی کرده است تا با «ایجاد مجموعه گسترده‌ای از اصول برای واحدهای تجاری و مصرف‌کنندگان»، مبنای محکم‌تری برای اعتماد را فراهم نماید (Ibid., p.17).

پیشرفت‌هایی در اروپا و آمریکا در زمینه اصلاح سیستم‌های حفاظت از حریم خصوصی و داده‌ها صورت گرفته است– و به‌رغم عدم اختلاف ظاهری اتحادیه اروپا و آمریکا درخصوص ارزش‌های اصلی مربوط به حکمرانی اینترنت، کماکان اقداماتی باید در مورد ابعاد فرهنگی و قانونی امنیت سایبری صورت گیرد. باوجوداینکه منطق اصلی امنیت سایبری اتحادیه اروپا امکان

1. Intelligence and Communication Technology
2. Big Data Working Group
3. John Podesta
4. Consumer Privacy Bill of Rights

اتخاذ رویکرد قانونی‌تر، نظارتی و مبتنی بر حقوق در سطح اروپا را می‌دهد، بعضی کشورهای عضو (بریتانیا، آلمان، فرانسه و سوئد) در کنار آمریکا به‌روشنی رویکرد اولویت «امنیت ملی» را در مورد موضوع جمع‌آوری داده‌ها برای امور جنایی اتخاذ می‌کنند که این مسئله رابطه بین حفظ حقوق شهروندان و تأمین اهداف امنیتی دولت‌ها در اروپا و آمریکا را در زمان ایجاد امنیت تاب‌آور فراآتلانتیک کارآمد مشکل‌ساز می‌کند. حتی قوانین اتحادیه اروپا نظیر دستورالعمل حفظ حریم خصوصی الکترونیکی (۲۰۰۹) امکان به‌کارگیری داده‌های شخصی برای «پیشگیری از جرم» و دستیابی به اهداف دیگر را فراهم می‌کند و ازاین‌رو، چارچوب ضعیفی برای حفاظت از داده‌های افراد در زمان اولویت‌بخشی به منطق امنیت ملی، ایجاد می‌نماید (Bendiek 2014, p.23). درواقع، بااینکه دیوان دادگستری اتحادیه اروپا امریه حفظ داده‌ها (۲۰۰۶) را به دلیل «مداخله جدی آن در ... حقوق حفظ حریم خصوصی و حق حفاظت از داده‌های خصوصی» در آوریل ۲۰۱۴ نامعتبر اعلام کرد (Villalon cited in Hern 2014)، اما بریتانیا کماکان این امریه را برای تضمین دسترسی به داده‌های ارتباطی اجرا می‌کنند[۱۰] (Ibid.). علاوه بر این، چنین قضاوتی بر ماهیت جمع‌آوری داده‌ها در چارچوب سازوکارهای موجود اتحادیه اروپا و آمریکا مانند ثبت‌نام و مشخصات مسافران در خطوط هوائی و برنامه ردیابی مالی تروریست‌ها و به‌ویژه بر روش انتقال داده‌های حجیم مشابه به مقامات آمریکایی، یعنی داده‌های افراد غیرمشکوک نیز، تأثیر می‌گذارد که سرنخ روشنی از اینکه تهدید امنیت عمومی باشند در دست نیست. این مسئله نیز پیامدهایی برای حقوق اساسی این افراد و روش جمع‌آوری اطلاعات اتحادیه اروپا و آمریکا برای مقاصد امنیتی دارد (ن.ک. Boehm and Cole 2014). درنهایت، تنش‌ها بین حقوق فردی و منطق امنیتی به سطح بین‌المللی نیز کشیده می‌شود که در آن کنوانسیون بوداپست (جرائم سایبری) و کتاب راهنمای تالین (جنگ سایبری) مطالب روشنی در زمینه حفاظت از داده‌های خصوصی و حقوق افراد مطرح نمی‌کنند (Bendiek 2014, p.23).

بسترهای همکاری و تشریک‌مساعی اتحادیه اروپا و آمریکا در امنیت و جرائم سایبری

گزاره برگ آمریکا- اتحادیه اروپا (۲۰۱۴) در مورد همکاری دوجانبه سایبری بیانگر «حدود همکاری طرفین بر اساس ارزش‌های مشترک، علاقه به اینترنت آزاد و با ارتباط سازگار و تعهد طرفین در قبال حکمرانی اینترنت چندجانبه، آزادی در اینترنت و حفاظت از حقوق بشر در فضای سایبری است. تحولات فضای بین‌المللی سایبری محور سیاست خارجی و امنیتی گسترده‌تر و عناصر اصلی مشارکت راهبردی طرفین محسوب می‌شود.» اگرچه، با توجه به موارد ذکرشده، این پرسش مسلماً مطرح می‌شود که چگونه موارد اختلاف و تشابه اتحادیه اروپا و آمریکا در مورد اشکال مختلف امنیت سایبری و جرائم سایبری در عمل منجر به ایجاد برنامه‌های کارآمدی برای همکاری و هماهنگی شده است؟ مهم‌تر از آن، درک حدود تأثیرگذاری این موضوع بر تأمین امنیت تاب‌آور کارآمد در اقدامات مشترک صورت گرفته، بسیار مهم است.

مسلماً در پنج سال گذشته کمبودی ازنظر طرح‌های مطرح‌شده در زمینه توسعه اقدامات در این حوزه وجود نداشته است. نخستین مورد این طرح‌ها در نشست سران اتحادیه اروپا و آمریکا در ۲۰ نوامبر ۲۰۱۰ در لیسبون با هدف «گسترش طرح‌های مربوط به امنیت سایبری و جرائم سایبری و مقابله با تهدیدات امنیت سایبری جهان» ارائه شد. کارگروه امنیت سایبری و جرائم سایبری مجموعه اهداف و حوزه‌های دارای اولویت مشخص و اقلام قابل تحویل خاصی را با هدف گزارش‌دهی سالانه درخصوص پیشرفت انجام‌شده در هر مورد تعیین کرد. چهار حوزه اصلی عبارت‌اند از: مدیریت حوادث سایبری، مشارکت بخش‌های عمومی- خصوصی، افزایش آگاهی و جرائم سایبری (EU–US Working Group, Concept Paper 2011). به‌رغم روشنی این مسئله که افشاگری‌های اسنودن تأثیر منفی بر بسیاری از ابعاد کاری این کارگروه و زیرگروه‌های تخصصی (برای رسیدگی به هر یک از حوزه‌های اصلی بالا) گذاشت، اما تا حدی پیشرفت و نتایج ملموسی نیز حاصل شد (Interviews, European Commission, June 2013).

برای مثال، کارگاه‌های آموزشی عمومی- خصوصی که در زمینه سیستم‌های کنترل صنعتی با میزبانی و مشارکت هر دو طرف تشکیل شده است باعث ترویج «ماه آگاهی از سایبر ملی»[1]

1. National Cyber Awareness Month

در آمریکا و اتحادیه اروپا شده است (US-EU fact sheet 2014). آمریکا و اروپا مانور امنیت سایبری فراآتلانتیک را نیز در کنار سازماندهی تبادل اطلاعات پیرامون مانورهای سایبری ملی و منطقه‌ای انجام دادند. این مانور، دورمیزی[1] دوجانبه با عنوان امنیت سایبر آتلانتیک[2] در نوامبر ۲۰۱۱، با هدف شناسایی نحوه همکاری کارآمد بین اتحادیه اروپا و آمریکا انجام شد (برای اهداف این مانور، ن.ک. کادر ۷ ۳-). این نخستین و (تنها) مانور مشترک طرفین بود و درنتیجه، ماهیتی اکتشافی داشت. بااین‌حال، بیش از ۶۰ شرکت‌کننده از ۱۶ کشور عضو اتحادیه اروپا به همراه نمایندگانی از دولت آمریکا در این مانور شرکت کردند و آژانس امنیت شبکه و اطلاعات اتحادیه اروپا و وزارت امنیت داخلی آمریکا نیز از برگزاری آن حمایت کردند. متأسفانه، به دلیل حساسیت این موضوع، هیچ مستنداتی در مورد تجربیات آموخته‌شده و نتایج این مانور منتشر نشده است و ظاهراً سیاست اسنودن و نیز مشارکت و همکاری دوجانبه جداگانه کشورهای عضو اتحادیه اروپا با آمریکا به معنای روند پیشرفت بسیار کند برنامه مدیریت حوادث سایبری به سرپرستی کمیسیون اروپا است (Interview, ENISA official, March 2015).

کادر ۷-۳. اهداف سایبر آتلانتیک (۲۰۱۱)

- بررسی و بهبود روشی که از طریق آن اعضای اتحادیه اروپا با فعالیت‌های مدیریت بحران سایبری ایالات‌متحده تعامل داشته باشند
- بررسی و شناسایی موضوعات با هدف بهبود روشی که از طریق آن ایالات‌متحده با فعالیت‌های مدیریت بحران سایبری اعضای اتحادیه تعامل داشته باشد و از رویه‌های مطلوب خود استفاده کند
- تبادل رویه‌های مناسب در خصوص رویکردها، به همکاری بین‌المللی در پی بحران‌های سایبری، به‌عنوان نخستین قدم به‌سمت تشریک‌مساعی کارآمد

Source: ENISA, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-atlantic/cyber-atlantic2011-

1. Table Top Exercise
جلسات مباحثه که در آن اعضای گروه در محیطی غیررسمی در مورد نقش خود در شرایط اضطراری و واکنش خود نسبت به وضعیت اضطراری خاصی بحث می‌کنند. (م.)
2. Cyber Atlantic

علاوه بر مانورهای سایبری، اتحاد جهانی علیه سوءاستفاده جنسی آنلاین از کودکان که در دسامبر ۲۰۱۲ آغاز به کار کرد، محصول موفق فعالیت کارگروه اتحادیه اروپا و آمریکا محسوب می‌شود (Interview, European Commission, June 2013). این مشارکت همکاری‌جویانه بین‌المللی ۵۴ کشوری[۱۱] (A Global Alliance against Child Sexual Abuse Online 2015) چهار سیاست مشترک (کادر ۷ -۴) را با هدف مقابله با تهدید فزاینده آنلاین کودکان تعیین کرد. بدین منظور، پیشرفت مثبت بسیاری در زمینه دستیابی به این اهداف ایجاد گردید، اما کماکان موانع و مشکلات بسیاری پیش روی ایجاد ابعاد عملیاتی، قانونی، فنی و فناورانه امنیت تاب‌آور کارآمدتر وجود دارند (Report of the Global Alliance 2013, p.3; Ministerial Declaration 2014). ازاین‌رو، کشورهای امضاکننده این توافق برنامه‌هایی را مطرح کردند که بیانگر تعهد آن‌ها در قبال دستیابی به اهداف تعیین‌شده و بهبود سازوکارها و ابزارهای هماهنگ‌کننده، همکاری‌جویانه و فناورانه و گسترش مهارت‌ها، برنامه‌های آموزشی و نهادی است که زمینه مقابله با سوءاستفاده جنسی آنلاین از کودکان را بیش‌ازپیش فراهم می‌کند.

کادر ۷-۴. اتحاد جهانی علیه سوءاستفاده جنسی آنلاین از کودکان: اهداف سیاستی مشترک

۱. بهبود تلاش‌ها در شناسایی قربانیان و تضمین آنکه این قربانیان کمک‌ها، حمایت‌ها و حفاظت‌های ضروری را دریافت خواهند کرد

۲. بهبود تلاش‌ها در بررسی پرونده‌های سواستفاده جنسی آنلاین از کودکان و شناسایی و پیگرد قانونی مجرمان

۳. افزایش آگاهی در بین کودکان، والدین، مربیان و جوامع در خصوص مخاطرات

۴. کاهش دسترسی به پورنوگرافی کودکان در فضای مجازی و قربانی‌شدن مجدد کودکان

Source: European Commission http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/index_en.htm.

بعضی موارد مرتبط با این موضوع عبارت‌اند از طرح‌هایی برای بهبود کاربرد و محتوای پایگاه داده‌های اینترپل در مورد بهره‌برداری جنسی بین‌المللی از کودکان از طریق گسترش دسترسی کشورهای عضو اتحاد جهانی علیه سوءاستفاده جنسی آنلاین از کودکان و مشارکت آن‌ها در این زمینه. ازنظر آمریکا و فنلاند، مشارکت بیشتر شامل جمع‌آوری تصاویر تهیه‌شده توسط

سازمان‌های غیردولتی موردبررسی (به‌عنوان‌مثال، مرکز ملی رسیدگی به امور کودکان گمشده و مورد بهره‌برداری[1] در آمریکا) است. کشورهای دیگر (به‌عنوان‌مثال، نیوزیلند، هلند، آلمان، مولداوی، بلژیک و اسلوونی) کماکان در حال طراحی برنامه‌های نرم‌افزاری و ایجاد توانمندی‌های قانونی (بریتانیا) برای تسهیل تحلیل و تبادل داده‌ها در پایگاه داده‌های بهره‌برداری جنسی بین‌المللی از کودکان در مورد نخست و شناسایی تصاویر جدید سوءاستفاده جنسی از کودکان در مورد دوم هستند. علاوه بر این، بریتانیا و آمریکا کارگروهی برای مقابله با بهره‌برداری آنلاین از کودکان با هدف یافتن راه‌حل‌های فناورانه بر اساس تخصص دانشگاه‌ها و بخش خصوصی تشکیل داده‌اند (Report of the Global Alliance 2013, p.7–18).

ازلحاظ توانایی تحقیقاتی، باوجوداینکه الزامات قانونی در داخل اتحادیه اروپا در امریه مقابله با سوءاستفاده و بهره‌برداری جنسی از کودکان و پورنوگرافی کودکان اتحادیه اروپا (European Parliament and Council 2011) مشخص شده‌اند (ن.ک. فصل ۵)، اما در اروپا و در سطح جهان انسجام و سازگاری کافی ازنظر قانون ماهوی اجرایی در کشورهای عضو اتحاد جهانی علیه سوءاستفاده جنسی آنلاین از کودکان وجود ندارد. ازاین‌رو، سوئیس، به‌عنوان‌مثال، در حال بازبینی قانون کیفری خود برای ارائه مقررات جدیدی در مورد تعریف «کودک» و تصویب قطعنامه‌هایی برای محافظت از کودکان در سطح سازمان ملل است، اما کشورهای دیگر (اسلوونی، گرجستان، آلمان) بر بهبود بُعد رویه‌ای چارچوب قانونی خود از طریق شیوه‌های مختلف ازجمله قانون‌گذاری برای تسهیل اجرای حقوق بین‌الملل و سازوکارهای حکمرانی تاب‌آورتر برای همکاری مستقیم مقامات مجری قانون توجه دارند.

درواقع، ضرورت ایجاد هماهنگی بهتر به‌عنوان موضوع اصلی در گزارش اتحاد جهانی مورد تأکید قرار گرفته است (2013, p.13) و بیانیه وزیران در مورد پیشرفت این اتحاد که در سپتامبر ۲۰۱۴ صادر شد نیز مشکلات «فرایندها و چارچوب‌های کاملاً داخلی و چندجانبه را مشخص می‌کند ... که اغلب مانع از دسترسی مناسب به اطلاعات و مدارک لازم برای رسیدگی و پیگرد کارآمد جرائم مربوط به بهره‌برداری آنلاین از کودکان می‌شوند» (Ministerial Declaration2014).

1. National Center for Missing and Exploited Children

بدین منظور، ایالات‌متحده به دنبال ایجاد برنامه جهانی جدیدی برای امکان‌پذیری و تسهیل انجام تحقیقات مشترک با اینترپل است، اما برخی کشورها به دنبال پیوستن به کارگروه مجازی جهانی[1] هستند که در پی ایجاد مشارکت بین نهادهای مجری قانون، سازمان‌های غیردولتی و صنایع برای گسترش همکاری‌های عملیاتی و راهبردی است (Report of the Global Alliance 2013, p.14). این مسئله نیز پذیرفته شده است که باید کارهای بیشتری فراتر از چارچوب قانونی، برای تسهیل همکاری بین طرف‌های ذینفع عمومی-خصوصی، تقویت گفتگوها و گسترش روابط مبتنی بر اعتماد و همکاری عملیاتی انجام شوند. درنهایت، موضوع بهبود همکاری با بخش خصوصی از طریق قانون‌گذاری (فراحکمرانی عملی) برای افزایش میزان پاسخ‌گویی ارائه‌دهندگان خدمات اینترنتی و نظیر به نظیر و از طریق اصول اخلاقی و رفتاری (فراحکمرانی نظری) نیز مطرح است که مستلزم توجه کامل و حذف رویه‌ها است (Ibid., p.20).

اتحاد جهانی، گرچه بیانگر عملکرد موفق فعالیت مشترک اتحادیه اروپا و آمریکا در دو سال نخست کار خود است، اما هنوز کارهای بسیاری برای ریشه‌کنی بهره‌برداری آنلاین از کودکان باید صورت گیرد. هرچند ماهیت پیشرفت کار، تاکنون بیانگر ضرورت دستیابی به شرایط لازم در مشارکت برای تأمین امنیت تاب‌آور کارآمد به‌ویژه با توجه به ابعاد قانونی و عملیاتی مقابله با سوءاستفاده جنسی آنلاین از کودکان است. بدیهی است رهبری اتحادیه اروپا- آمریکا برای تکامل بیشتر این اتحاد ضرورت دارد و ازاین‌رو، آن‌ها باید راه‌هایی برای رفع کلی اختلافات قانونی، عملیاتی و راهبردی خود در زمان هماهنگی، همکاری و مشارکت در زمینه مسائل امنیت سایبری پیدا کنند تا این اتحاد به برنامه موفقی در سطح جهان مبدل گردد. درواقع، رهبری اتحادیه اروپا- آمریکا فراتر از این اتحاد و برای ترویج چارچوب قانونی مشترک مقابله با جرائم سایبری (هم‌اکنون کنوانسیون بوداپست) و استانداردهای امنیت سایبری در محافل بین‌لمللی مربوطه، با هدف تضمین شرایط تأمین امنیت تاب‌آور کارآمد، ضروری است.

درنهایت، گفتگوی سایبری بین طرفین در نشست اتحادیه اروپا- آمریکا در مارس ۲۰۱۴ با هدف ارتقاء و گسترش همکاری در زمینه مسائل سایبری و «طرح برنامه‌ای برای تقویت

1. Global Virtual Task Force

مبادلات بین اتحادیه اروپا و آمریکا در زمینه مسائل سایبری فی‌مابین، تحولات اصلی بین‌المللی و مسائل مربوط به سیاست خارجی» برگزار شد (EU–US fact sheet 2014). گفتگوی جامعه اطلاعاتی نیز با این هدف انجام شد که اتحادیه اروپا بتواند مشارکت بیشتری در مباحث پیرامون سیاست‌گذاری و حکمرانی اینترنت و فناوری اطلاعات و ارتباطات داشته باشد. بااینکه هر دو برنامه امکان مشارکت بیشتر اتحادیه اروپا و آمریکا در موضوعات حیاتی را فراهم می‌کنند، اما کارآمدی آن‌ها تنها در حد تأیید مجدد تعهدات مشترک، هنجارهای موردتوافق و اهداف راهبردی و تضمین تحرک در زمینه موضوعات حیاتی مربوط به امنیت سایبری است. البته، شواهد موجود در جلسه افتتاحیه مذاکرات سایبری این مسئله را تأیید می‌کند که هر دو طرف تعهدات خود را در قبال حکمرانی چندجانبه و اینترنت «فراگیر، شفاف، پاسخگو و با کیفیت فنی مناسب» بازگو کردند (Press Release, 1st EU–US Cyber Dialogue) و بر پیشرفت حاصل‌شده در کارگروه اتحادیه اروپا- آمریکا، تعهد آن‌ها نسبت به حقوق بشر در فضای سایبری و ظرفیت‌سازی سایبری جهانی تأکید نمودند. با توجه به برگزاری سالانه این نشست‌ها، مسلماً آن‌ها اهداف راهبردی را به‌ویژه در ترتیبات رسمی و غیررسمی تعیین‌شده در سطح کارگروه و از طریق همکاری تاکتیکی و عملیاتی منظم‌تر دنبال می‌کنند –اما فعالیت مربوط به درک و واکنش مشترک قطعاً در جای دیگری انجام می‌شود (به‌عنوان‌مثال، مذاکرات اداره تحقیقات فدرال آمریکا و مرکز مقابله با جرائم سایبری اتحادیه اروپا در زمینه مقابله با باتنت‌ها - ن.ک. فصول ۴ و ۵ یا مانورهای امنیت سایبری آتی).

جمع‌بندی: همگرایی در امنیت تاب‌آور؟

در این فصل مطالبی در مورد وجود مصادیق و الگوهای واگرایی و اختلاف و نیز همگرایی و موارد مشترک بین اتحادیه اروپا و ایالات‌متحده آمریکا در زمینه مسائل مختلف مربوط به امنیت سایبری ازجمله حکمرانی اینترنت، امنیت شبکه و اطلاعات و حفاظت از حریم خصوصی و داده‌ها مطرح شد. ارتباط این ابعاد و پیچیدگی حاصل از آن پیامدهایی برای هماهنگی، همکاری و مشارکت طرفین در زمینه امنیت سایبری و مهم‌تر از آن بر همگرایی رویکرد مشترک امنیت

تاب‌آور کارآمد دارد. به‌خصوص، در صورت وجود موانع قابل‌توجهی ازنظر توسعه و گسترش مشارکت مبتنی بر اعتماد (به‌عنوان‌مثال، نحوه اشتراک اطلاعات) و اختلاف فرهنگ امنیت سایبری (امنیت ملی در برابر رویکرد امنیت تاب‌آور) تا حدی که درک مشترکی از مشکلات و به‌تبع آن توافقی در مورد راه‌حل‌ها وجود نداشته باشد، ایجاد شرایط لازم برای تأمین امنیت تاب‌آور کارآمد دشوار می‌گردد. به دلیل عدم انسجام داخلی اتحادیه اروپا و نیز بین اتحادیه اروپا و آمریکا در زمینه مسائل خاص و ایجاد موازنه صحیح بین حفظ حریم خصوصی و تأمین امنیت در زمان پیگرد مجرمان سایبری و پیشگیری از حملات سایبری، چنین مشکلاتی تشدید نیز شده است.

مسلماً این موانع و اختلافات رفع می‌شوند. اتحادیه اروپا و آمریکا در مورد دستیابی به اینترنت باز، آزاد و قابل‌دسترس از طریق الگوی چندجانبه تا حد بسیاری همگرا و متعهد هستند. این همگرایی امکان مشارکت کارآمد آن‌ها در محافل بین‌المللی برای پیگیری دیدگاه خود درخصوص اینترنت و حکمرانی اینترنت را ایجاد کرده است. بااینکه افشاگری‌های اسنودن باعث ایجاد تنش‌هایی در این مشارکت گردید، اما فضای تحقق روایت فراگیرتر، پاسخ‌گوتر و چندجانبه‌ای را نیز در مورد حکمرانی اینترنت ایجاد کرد. در چنین فضایی آمریکا چاره‌ای جز مشارکت برای دلجویی از اتحادیه اروپا و سایر کشورهای دموکرات و طرف‌های ذینفع در حکمرانی اینترنت و هماهنگ ماندن با ارزش‌های مدنظر مشارکت اتحادیه اروپا و ایالات‌متحده در مورد اینترنت، حکمرانی و امنیت آن نداشت. اعلام تمایل به چندجانبه‌سازی کنترل بر اینترنت باید اکنون در عمل به‌صورت دوجانبه و مهم‌تر از آن در محافل چندجانبه با حضور چند ذینفع، بدون توجه به تنش حاصل از آن برای رویکرد امنیت ملیِ فرهنگ امنیت سایبری آمریکا دنبال شود. درواقع، به دلیل اتخاذ چنین رویکردی از جانب دولت‌های اقتدارگرا برای ایجاد مرزهایی کارآمد در فضای سایبری تحت عنوان امنیت سایبری است که اتحادیه اروپا و آمریکا باید اختلافات خود را رفع کنند و رویکرد اینترنت امن و آزاد را برای همگان اتخاذ نمایند.

رویکرد آمریکا و اتحادیه اروپا ازنظر به‌کارگیری پارامترها و سازوکارهای رسیدگی به مسائل مربوط به امنیت شبکه و اطلاعات و به‌طور دقیق‌تر، حفاظت از زیرساخت‌های اطلاعاتی حیاتی

ملی مشابه است. درواقع، چارچوب امنیت سایبری آمریکا و دستورالعمل امنیت شبکه و اطلاعات اتحادیه اروپا با ایجاد انگیزه برای پذیرش این استانداردها و بهبود اشتراک اطلاعات مربوط به حملات و تهدیدهای سایبری بین بخش‌های خصوصی و دولتی بیانگر به‌کارگیری استانداردهای حداقلی امنیت سایبری است. از این نظر، همگرایی و فرصت‌های [همکاری] بی‌شماری برای طرفین از طریق انجام مانورهای امنیت سایبری مدیریت‌شده، کارگاه‌های آموزشی، جلسات و برنامه‌ها (به‌عنوان‌مثال، برگزاری کارگاه آموزشی مقدماتی برای بحث پیرامون این موضوع در نوامبر ۲۰۱۴) در راستای مباحثه حول ایجاد رویکردهای مشترک و اقدامات مناسب در رابطه با حفاظت از زیرساخت‌های حیاتی وجود دارد. گرچه، تفاوت اصلی دو رویکرد اتخاذشده – یکی داوطلبانه (آمریکا) و دیگری نظارتی (اتحادیه اروپا)– احتمال دارد، باعث تضعیف اقدامات صورت‌گرفته برای ایجاد «تشابه» و ازاین‌رو، تأمین عملی امنیت تاب‌آور کارآمد در حوزه گزارش‌دهی، تبادل و پردازش اطلاعات و واکنش‌های لحظه‌ای احتمالی گردد. شایان‌ذکر است که مباحثه درخصوص اتخاذ رویکرد الزام‌آور در برابر رویکرد داوطلبانه، کماکان در اتحادیه اروپا و ایالات‌متحده در جریان است. به‌رغم وجود رویکرد نظارتی در اتحادیه اروپا و رویکرد داوطلبانه در آمریکا، کارایی هر یک از این دو رویکرد باید با جمع‌آوری مدارک کافی در اتحادیه اروپا و آمریکا مشخص گردد. درواقع، اختلاف‌نظرهایی در مورد این موضوع در میان اعضای اتحادیه و بین طرف‌های ذینفع خصوصی و دولتی آمریکا وجود دارد. نحوه عملکرد دو رویکرد در عمل، در کنار اصلاحات صورت‌گرفته در مورد حقوق حفاظت از حریم خصوصی و داده‌ها، درک عمیق‌تری را درباره حدود ایجاد رویکردی مشترک و ماهیت اقدامی مناسب با توجه به اختلافات فرهنگی و قانونی دو طرف در حوزه مسائل سایبری ایجاد می‌کند.

حفاظت از حریم خصوصی و داده‌ها، مسلماً بیشترین تنش را ایجاد کرده و بیانگر مهم‌ترین تفاوت رویکردهای آمریکا و اتحادیه اروپا در قبال امنیت سایبری است. درواقع، افشاگری‌های اسنودن، مسئله سازگاری فرهنگ‌های امنیت سایبری آمریکا و اتحادیه اروپا در زمان جمع‌آوری و به‌کارگیری داده‌های شخصی برای اهداف امنیتی با توجه به منطق مبنای رویکردهای. اتخاذشده را مطرح کرده است. اتحادیه اروپا رویکرد تأثیرگذار حقوقی را در قبال اصلاح قوانین

در زمینه حفاظت از داده‌ها برای شهروندان اروپا اتخاذ کرده است که پیامدهایی برای امنیت سایبری و مسائل مربوط به تجارت و به‌کارگیری رسانه‌های اجتماعی در فضای فراآتلانتیک دارد. باوجوداینکه آمریکا نیز اصلاح حقوق شهروندان خود و اتباع غیرآمریکایی و قوانین مربوط به جمع‌آوری داده‌ها برای اهداف امنیتی را آغاز کرده است، کماکان مسائل حل‌نشده‌ای مانند چگونگی جمع‌آوری، فیلترسازی و به‌کارگیری داده‌های حجیم وجود دارند که بر توافقات موجود نظیر ثبت‌نام و مشخصات مسافران در خطوط هوائی و پروتکل انتقال فایل تأثیر می‌گذارند برای دستیابی به پیشرفت در زمینه حذف موانع قانونی و بازسازی اعتماد بین دو طرف و نیز بین شهروندان و دولت‌های اتحادیه اروپا و ایالات‌متحده، این مسائل باید در بالاترین سطح مشارکت و همین‌طور در سطوح عملیاتی و کاری بین اتحادیه اروپا و آمریکا اولویت‌بندی شوند. با توجه به روابط نزدیک بین بخش خصوصی، جمع‌آوری داده‌ها توسط دولت‌ها و آژانس‌های اطلاعاتی و ماهیت بدون مرز فضای سایبری، این مسئله، برای ایجاد شرایط لازم برای تأمین امنیت تاب‌آور در مسائل سایبری و مسائل مشابهی نظیر موافقت‌نامه مشارکت تجاری و سرمایه‌گذاری فراآتلانتیک اهمیت دارد.

اگر امنیت تاب‌آور کارآمد هدف واقعی همکاری فراآتلانتیک در امنیت سایبری و جرائم سایبری باشد، آمریکا و اتحادیه اروپا برخی اعضای اتحادیه اروپا– باید در کوتاه‌مدت مذاکره جدی در مورد منطق مبنای رویکردهای خود داشته باشند و در این زمینه با یکدیگر به توافق برسند. درواقع، مهم‌ترین مانع در سر راه همگرایی اتحادیه اروپا و آمریکا در زمینه تأمین امنیت تاب‌آور، موارد آسیب‌پذیری و ناامنی ایجادشده به دلیل پذیرش منطق اولویت امنیت ملی مبتنی بر بازدارندگی است. با وجود تأکید منطق اتحادیه اروپا بر امنیت تاب‌آور به‌جای تهاجم و بازدارندگی، برخی کشورهای عضو این اتحادیه (ازجمله بریتانیا) اولویت را به تهاجم و بازدارندگی می‌دهند که این موضوع در عمل موجب ایجاد تناقضاتی شده است. بااینکه احتمال دارد این مسئله فرصت‌هایی را برای همکاری دوجانبه بین بعضی اعضای اتحادیه و آمریکا ایجاد کند، درمجموع، این مسئله موجب تضعیف اقدامات صورت‌گرفته با هدف ایجاد رویکردی مشترک بین اتحادیه اروپا و آمریکا بر اساس ارزش‌های موردتوافق در زمینه حکمرانی اینترنت و امنیت

تاب‌آور کارآمد می‌گردد. به‌علاوه، این موضوع از اعتبار اقدامات مشترک طرفین برای ترویج چنین ارزش‌هایی در حوزه امنیت سایبری در میان کشورهای غیردموکراتیک می‌کاهد که اولویت آن‌ها امنیت ملی برای حفاظت از فضای سایبری خود است.[۱۲] بدون چنین توافقی، همگرایی در زمینه تأمین امنیت تاب‌آور واقعی و کارآمد بین شرکای فراآتلانتیک تنها در حاشیه و نه به‌صورت جامع و متحول‌کننده‌ای به دست می‌آید.

فصل هشتم

جمع‌بندی: به‌سوی امنیت تاب‌آور کاآمد در اتحادیه اروپا

مقدمه

یکی از اهداف اصلی این کتاب تحلیل و ارائه درکی عمیق‌تر از اکوسیستم در حال تکامل اتحادیه اروپا در حوزه امنیت سایبری است. به علاوه، این کتاب نشان داد که اتحادیه اروپا تا چه حد در زمینه ایجاد و تثبیت شرایط لازم برای ظهور امنیت تاب‌آور کارآمد در اروپا و خارج از آن پیش رفته است. در کنار این مطلب، مسائلی نظیر رابطه بین شیوه‌های مختلف اِعمال حکمرانی امنیت سایبری و انواع امنیت سایبری تاب‌آور در حال تکامل موردبررسی قرار گرفت و به‌ویژه رابطه و تنشی که اغلب بین رویکرد عملی و رویکردهای نظری و مبتنی بر بازار در حوزه امنیت سایبری موجود است، به‌دقت واکاوی شد. جهت یافتن پاسخ پرسش‌های زیر که در ابتدای کتاب نیز مطرح شد، ارکان اساسی راهبرد امنیت سایبری اتحادیه اروپا در سطح ملی و جهانی را مورد ارزیابی قرار داد:

- چگونه می‌توان اکوسیستم در حال تکامل حکمرانی امنیت سایبری اتحادیه اروپا را درک و توصیف کرد؟
- اتحادیه اروپا تا چه حد توانسته است رویکردی جامع و تاب‌آور در حوزه امنیت سایبری در این اکوسیستم در حال تکامل اتخاذ نماید؟
- ماهیت این اکوسیستم تاب‌آور در حال ظهور در اتحادیه اروپا چیست؟

این استدلال در سرتاسر کتاب مطرح شد که به‌کارگیری مفهوم امنیت تاب‌آور به‌جای امنیت کنترلی، جهتی را در راستای رویکرد اتحادیه اروپا به روابط در حال ایجاد و شکل‌گیری آن و همچنین درکی عمیق‌تر از این مسئله را ایجاد می‌کند که با توجه به حضور بازیگران و نهادهای فعال و اکوسیستم جهانی محل عملکرد این بازیگران، اتحادیه اروپا به چه دلیل و چگونه در چنین جهتی سیر می‌کند. به‌علاوه، این مطلب نیز مطرح شد که به دلیل برخورد با موضوع امنیت تاب‌آور به‌عنوان مسئله‌ای مستلزم یافتن راه‌حل و افزودن نکات ظریفی در نحوه تعریف و ادراک مفهومی این موضوع و نیز اتخاذ رویکردی انتقادی در قبال مقوله حکمرانی امنیت، امکان ارزیابی دقیق‌تر استدلال(های) مشترک مربوط به پدیده نوظهور حکمرانی امنیت تاب‌آور و درک معنای این مسئله در فضاها و سطوح مختلف تعامل عملی اتحادیه اروپا ایجاد گردید.

در این کتاب این مسئله نیز مطرح شد که نوع مناسب و منعطف امنیت تاب‌آور باید محرک اتحادیه اروپا در رویکرد آن نسبت به امنیت سایبری باشد و این اتحادیه باید از طریق سازوکارهای حکمرانی مناسب بر ایجاد شرایط لازم برای تأمین امنیت سایبری تاب‌آور کارآمد توجه نماید تا بتواند به بازیگری تأثیرگذار در فضای سایبری تبدیل گردد و با توجه به شیوه‌های صحیح به‌کاررفته در حوزه امنیت سایبری و ابعاد مختلف بی‌شمار آن، بتواند نقش رهبری را نیز در این حوزه ایفا کند. باید توجه داشت که در اینجا هدف، فی‌نفسه شرح حکمرانی نیست بلکه جستجوی مسیر تکامل امنیت تاب‌آور کارآمد و سازوکارهای حکمرانی نوظهوری است که برای دستیابی به این نوع امنیت در ابعاد مختلف امنیت سایبریِ مورد ارزیابی، انتخاب شدند. درمجموع، رویکرد امنیت تاب‌آور بر مبنای ادبیات مفهومی موجود در زمینه موضوع کلی‌تر امنیت سایبری و ادبیات اندک پیرامون اتحادیه اروپا، ایجاد و اضافه گردید (Klimburg and Tiirma Klaar 2011; Dunn Cavelty 2013).

با تلفیق بخش‌های تجربی و مفهومی کتاب در فصل آخر این مجلد، به موضوع یافته‌های اصلی برای راهبردها و سیاست‌های در حال تکامل اتحادیه اروپا پرداخته می‌شود. در این فصل، پیامدهای رویکرد اروپا نسبت به امنیت شبکه و اطلاعات و دفاع سایبری و همچنین پیامدهای نقش این رویکرد در دولت‌های عضو اتحادیه و در سطح بین‌الملل –به‌ویژه همکاری‌های آتی

بین اتحادیه اروپا و ایالات‌متحده آمریکا– مورد ارزیابی قرار می‌گیرد. در اینجا باید به این مورد محدودیت نیز اشاره کرد که نتایج قابل‌تعمیم و ملموسی در مورد به‌کارگیری امنیت تاب‌آور در کل کشورهای عضو اتحادیه اروپا به دست نیامده است. اگرچه، تحلیل داده‌های موجود (ن.ک. فصل ۴) و بررسی بریتانیا به‌عنوان مطالعه موردی، حداقل امکان تأمل پیرامون یکی از اعضای اصلی اتحادیه اروپا و یادگیری مواردی از شیوه‌های مناسب به‌کاررفته در این کشور را فراهم می‌کند. در این فصل تجربیات کلی‌تر فراگرفته‌شده مطرح می‌شوند، پیرامون امنیت تاب‌آور و مقوله حکمرانی تأمل صورت می‌گیرد و با فرض حرکت آتی این اتحادیه به سمت رویکرد امنیت تاب‌آور کارآمدتر، توصیه‌هایی درباره جهت‌گیری آتی راهبردها و سیاست‌های اتحادیه اروپا مطرح می‌شود.

کادر ۸-۱. شرایط کلی: امنیت تاب‌آور کارآمد

- توانایی (شامل منابع و احکام) و آمادگی برای اتخاذ تصدی‌های عملیاتی پایه‌ای و ساختارهای نهادی جدید
- پذیرش کارآمدی که به نفع پیچیدگی‌های منطق‌های حکمرانی با هدف اجتناب از نقاط تهدید و شکست منفرد مورد چشم‌پوشی قرار گرفته بود
- ائتلاف بازیگران در قالب همکاری در «مشارکت‌ها» برای تبادل اطلاعات، ساخت نهادهای منعطف و انطباق پذیر جدید و رویه‌های عملیاتی، تعیین دستورکار و تدوین/اجرای سیاست‌ها
- همگرایی میان ذینفعان در خصوص منطق(ها)، «هنجارها»، قوانین و استانداردهای «مشترک» در حوزه امنیت تاب‌آور
- تکامل فرهنگ امنیت سایبری در تمام سطوح در میان ذینفعان (آگاهی، آموزش، یادگیری و...)
- رویکردی یکپارچه (منسجم و پیوسته در لایه‌ها، سطوح و بازیگران)

اکوسیستم نوظهور در اتحادیه اروپا: امنیت تاب‌آور؟

رویکرد اتحادیه اروپا در قبال امنیت سایبری که تا فوریه ۲۰۱۳ اعلام نشده بود از ماهیت سازنده‌ای برخوردار است و هر حوزه اولویت‌مند آن در مرحله توسعه متفاوتی قرار دارد. در این زمینه، حوزه جرائم سایبری پیشرفته‌ترین بخش به شمار می‌آید و پس از آن حوزه امنیت شبکه و اطلاعات و درنهایت، حوزه دفاع سایبری قرار دارد که در مقایسه با سایر حوزه‌ها، از تاریخچه نسبتاً کوتاهی برای توسعه در چارچوب راهبرد کلی امنیت سایبری اتحادیه اروپا برخوردار

است. اگرچه هدف از ایجاد این راهبرد خلق رویکردی منسجم بود، اما بدیهی است کماکان باید همکاری بسیاری بین نهادها، شبکه‌ها و مؤسسات مسئولیت‌پذیر ملی، منطقه‌ای و بین‌المللی صورت گیرد تا این امر تحقق یابد. درواقع، اتحادیه اروپا باید بر روی ابعاد مختلف سیاست‌های خود کار کند تا مسئولیت‌های مشترک را حذف و کار مؤثر بر روی مسائل موردعلاقه طرفین را تضمین نماید. علاوه بر این، کار بسیاری در جهت حفظ منابع و ایجاد اکوسیستمی برای تأمین .شرایط ضروری رویکرد امنیت تاب‌آور نیز باید صورت گیرد

اگرچه جنبه حقوقی بیشترین اهمیت را در خلق چارچوبی مشخص برای همکاری در زمینه تبادل اطلاعات، انجام تحقیقات و پیگردهای قضایی در حوزه جرائم سایبری –چه از طریق امریه‌ها و مقررات اتحادیه اروپا و چه به‌واسطه تصویب و اجرای کنوانسیون بوداپست– دارد، اما تغییر موانع فرهنگی و سیاسی در سطوح مختلف و ضروری دشوارتر است. به‌رغم ایجاد تغییر قابل‌ملاحظه‌ای در شرایط حکمرانی در مورد رویکرد فراحکمرانی عملی‌تری در حوزه امنیت شبکه و اطلاعات، اجماع مشخصی در میان طرفین ذینفع در اتحادیه اروپا مبنی بر این امر وجود ندارد که این مورد کارآمدترین رویکرد ازنظر ایجاد روابط مبتنی بر اعتماد موردنیاز برای ظهور همکاری‌های کارآمد به‌حساب می‌آید. باوجوداینکه کمیسیون اروپا با ارزیابی گزینه‌های دستورالعمل مربوط به امنیت شبکه و اطلاعات چنین رویکردی را برگزید، بسیاری از کشورهای عضو و رهبران اصلی واحدهای تجاری فعال در حوزه امنیت سایبری در مورد این مسئله تردید دارند که این رویکرد بتواند اعتمادسازی لازم برای اشتراک مؤثر اطلاعات و تاب‌آوری و سازگاری لازم برای رشد امنیت تاب‌آورتر در میان طرفین ذینفع اصلی را ایجاد نماید. با توجه به حساسیت موضوع دفاع سایبری برای دولت‌های عضو اتحادیه اروپا، تاکنون بر موارد همکاری تشویقی در زمینه گسترش برنامه‌های تعلیمی، آموزشی و مهارتی برای مخاطبان ضروری (نظامی و غیرنظامی) و ازاین‌رو، بر فراحکمرانی مربوط به هماهنگی از طریق کانال‌های همکاری رسمی و غیررسمی تأکید شده است.

با این توصیف، اتحادیه اروپا تا چه حد در زمینه تسهیل ظهور و ایجاد شرایط لازم برای امنیت تاب‌آور پیشرفت کرده است؟

جرائم سایبری

اگرچه سیاست‌گذاری جرائم سایبری را می‌توان کامل‌ترین رکن چارچوب راهبرد امنیت سایبری اتحادیه اروپا در نظر گرفت، اما با توجه به مقابله با جرائم سایبری در اتحادیه اروپا، چالش‌های اساسی در پیش روی تأمین شرایط امنیت تاب‌آور کارآمد وجود دارد. وجود بازیگران، فرایندها، سطوح، لایه‌ها و ابعاد بی‌شمار دخیل در ایجاد اکوسیستمی کارآمد باعث پیچیدگی این موضوع شده است و با توجه به اهمیت و محوریت ایجاد تحول در «فرهنگ‌ها» –شیوه‌های تفکر و عمل– برای رسیدگی به مشکل پویای جرائم سایبری، تنها از طریق تغییر فزاینده می‌توان به چنین اکوسیستمی دست یافت. بدیهی است جرائم سایبری درمجموع جدا از مشکلات امنیت سایبری در نظر گرفته نمی‌شوند. در ضمن، موارد افشاگری اسنودن، موجب تشدید بحث در مورد موضوع حفظ حریم خصوصی در برابر برقراری امنیت و پیچیده‌تر شدن محیط حقوقی و فرهنگی شده است که سیاست‌گذاری در زمینه جرائم سایبری و مجرمان سایبری در آن به اجرا درمی‌آید. درواقع، ابزار برنامه‌ریزی برای ادغام، هماهنگ‌سازی و مدیریت منابع موجب تسهیل روند تحول در ابعاد حقوقی اتحادیه اروپا و آمریکا با ایجاد تغییر فرهنگی غالبی در اروپا شده است تا حمایت از حقوق فردی در قوانین اتحادیه اروپا در برابر نظارت جمعی ذیل مقوله امنیت تضمین گردد. مفهوم اصلی شرایط امنیت تاب‌آور درواقع همان مفهوم منطق حکمرانی پیچیده و متعارض و به‌ویژه مفهوم تطبیق‌دهنده بُعد حقوقی با ابعاد عملیاتی و راهبردی مربوط به بررسی قضایی و پیگرد مجرمان سایبری است.

در حوزه جرائم سایبری، به‌رغم موانع موجود قطعاً پیشرفت‌هایی نیز حاصل شده است. سال‌های متمادی است که ایجاد فرهنگ امنیت سایبری، محور اقدامات اتحادیه اروپا برای دستیابی به امنیت در جامعه اطلاعاتی با آگاهی از این موضوع بوده است که رسیدگی به علل و نه فقط علائم جرائم سایبری مستلزم اتخاذ رویکردی مشارکتی با حضور چند ذی‌نفع و نیز درک مشترک این مشکل (تعریف) و فرایندهای موردنیاز است. در خصوص موضوع اولویت‌دار «کاهش شدید جرائم سایبری» در راهبرد امنیت سایبری اتحادیه اروپا بر بُعد حقوقی در سطح ملی، منطقه‌ای و جهانی و نیز لایه‌های عملیاتی و هماهنگی بین و درون تمام سطوح مربوط به جرائم

سایبری توجه می‌شود. این عناصر مختلف به‌طور مستقیم به شرایط لازم در لایه‌های حقوقی و عملیاتی برای تأمین امنیت تاب‌آور کارآمد و به‌ویژه به معیار ایجاد فرهنگ امنیت سایبری در درون و بین ابعاد مختلف اکوسیستم در حال ظهور امنیت سایبری می‌پردازند.

در این شرایط، برنامه‌ها، کنوانسیون‌های حقوقی، فضاهای کاری، روابط و سازوکارهایی با هدف پرورش محیطی همگرا برای درک و «انجام» جرائم سایبری در داخل اروپا و خارج از آن ایجاد شده است. به‌عنوان‌مثال، اکثر کشورهای عضو اتحادیه اروپا کنوانسیون بوداپست را امضا و تصویب کرده‌اند. اگرچه این کنوانسیون بدون اشکال و انتقاد نیست، اما عرصه‌ای برای ظهور فرهنگ امنیت سایبری در سطوح حقوقی و عملیاتی بر اساس مجموعه مشترک –نه کاملاً هماهنگی– از حداقل استانداردها، تعاریف و پروتکل‌ها را به وجود آورده است. مسلماً محدودیت‌های کنوانسیون بوداپست در اتحادیه اروپا و در خارج از آن در میان‌مدت باید با افزودن دامنه و شفافیت بیشتر به قوانین و مقررات به‌عنوان‌مثال، مربوط به بررسی و ذخیره‌سازی اطلاعات به‌دست‌آمده در نظر گرفته شوند. تمام اعضای اتحادیه اروپا موظف به تصویب و اجرای سریع این کنوانسیون برای تضمین برخی هنجارهای حقوقی حداقلی برای هماهنگ‌سازی و ترغیب کشورهای خارج از اتحادیه اروپا به بهره‌گیری از این کنوانسیون از طریق مشارکت دوجانبه مستقیم و حضور در مجامع چندجانبه مربوطه هستند، چراکه این کنوانسیون در زمان رسیدگی به جرائم سایبری نقش کارآمدی دارد. در این شرایط، دستورالعمل‌ها و مقررات اتحادیه اروپا که به‌طور مستقیم و غیرمستقیم بر رسیدگی به جرائم سایبری مربوط می‌شوند باید بیشتر مکمل کنوانسیون بوداپست باشند تا اینکه فراتر از ساختارهای تشویقی روند که حداقل ظرفیت سازی لازم درون و بین کشورهای اتحادیه اروپا (نهادها، منابع، مهارت‌ها و سایر موارد) را ایجاد می‌کند. اتحادیه اروپا باید در سطح بین‌المللی پیشرفت نماید و اعتبار بیشتری نیز در زمینه سیاست‌گذاری سایبری بین‌المللی و اقدامات خود در جهت تسهیل ظرفیت‌سازی در کشورهای درحال‌توسعه کسب کند. اقدامات این اتحادیه در سطوح دیپلماتیک و همچنین عملیاتی باید به علت مشارکت با آن دسته از کشورهایی انجام گیرند که از امضای هرگونه کنوانسیون به این دلیل طفره می‌روند که «امنیت ملی» آن‌ها نسبت به جرائم سایبری و امنیت سایبری در

اولویت قرار دارد. ایجاد توافق و اعتمادسازی میان انواع مشارکت عملیاتی در سطوح پایین‌تر مسلماً می‌تواند موجب تسهیل رفع موانع پیش روی همکاری‌ها گردد و انعقاد موافقت‌نامه‌های سیاست‌گذاری کلی‌تر در میان‌مدت تا بلندمدت را شتاب بخشد.

آگاهی از این نکته نیز حائز اهمیت است که ساختارهای نهادی جدید و شبکه‌ها، برنامه‌ها، اتحادها و راهبردهایی در سطح اتحادیه اروپا برای ارتقای مشارکت، ایجاد اعتماد و محیط یکپارچه برای رسیدگی به جرائم سایبری ایجاد شده است. بدین منظور، سازمان‌هایی نظیر مرکز مقابله با جرائم سایبری اتحادیه اروپا و آژانس امنیت شبکه و اطلاعات اتحادیه اروپا ایجاد شدند که وظیفه آن‌ها رسیدگی به جرائم سایبری به ترتیب ازنظر ویژگی‌های عملیاتی و راهبردی جرائم سایبری از بررسی قضایی تا پیگرد و تسهیل هماهنگی بین طرفین ذینفع درون و بین کشورهای عضو است. در راهبرد امنیت سایبری اتحادیه اروپا (۲۰۱۳)، فهرستی از اولویت‌های مربوط به جرائم سایبری و سایر ابعاد امنیت سایبری منتشر شده است و تغییر قابل‌ملاحظه‌ای نیز در قانون‌گذاری و حکمرانی جرائم سایبری با هدف ایجاد شفافیت حقوقی در مسائلی نظیر تعریف جرائم سایبری، اشتراک داده‌ها و اطلاعات، حفظ حریم خصوصی، بررسی قضایی و پیگرد قانونی صورت گرفته است. طرح‌های اتحادیه اروپا در زمینه جرائم سایبری نیز شاهد ظهور برنامه‌هایی نظیر اینترنت امن‌تر برای کودکان و راهبرد اتحادیه در ارائه اینترنت بهتر برای کودکان بوده است. در طرح اتحاد جهانی علیه سوءاستفاده جنسی آنلاین از کودکان، دستاوردهای به‌دست‌آمده در سطح بین‌المللی در زمان همکاری فعالان با یکدیگر برای نیل به اهداف خاصی نشان داده شده است، اما اقدامات بیشتری باید در جهت هماهنگ‌سازی چارچوب-های قانونی، تقویت گفتمان و گسترش روابط مبتنی بر اعتماد و هماهنگی عملیاتی بین طرفین امضاکننده صورت گیرد.

در بین تمام این تحولات، این نقش مشارکت مؤثر و روابط کاری قابل‌اعتماد بوده که حائز اهمیت است –ائتلاف مالی اتحادیه اروپا مورد مناسبی در این حوزه به شمار می‌آید. این مسئله نیز مشخص گردید که شواهد و نظرات بیانگر اهمیت مشارکت غیررسمی کشورها (ازنظر حکمرانی) در ایجاد تأثیر کارآمد مقابله با جرائم سایبری است. چنین ترتیباتی، به‌ویژه در زمانی که تحت تأثیر مسئله‌ای ایجاد می‌شوند، تاب‌آوری و انگیزه همکاری لازم جهت بهینه‌سازی

منابع و تخصص‌ها در مقابله با جرائم سایبری را در طرفین اصلی –خصوصی و عمومی– به وجود می‌آورند. به‌رغم وجود رویه‌های مناسب در ترتیبات رسمی (مرکز جرائم سایبری اتحادیه اروپا و کارگروه اقدام مشترک علیه جرائم اینترنتی)، نیمه‌رسمی (مراکز اشتراک و تحلیل اطلاعات) و غیررسمی (همکاری‌های موردی، به‌عنوان‌مثال، مقابله با بات‌نت‌ها) بین بازیگران اصلی (سازمان‌های مجری قانون، سازمان‌های اطلاعاتی، نهادهای دولتی، صنایع خصوصی، گروه‌های واکنش اضطراری رایانه‌ای اتحادیه اروپا و سایر موارد) در اتحادیه اروپا و در سطح جهان، اقدام بیشتری باید در زمینه شفاف‌سازی امور حقوقی و رویه‌ای، بهبود منابع عملیاتی، ابزارها، ظرفیت‌ها و آموزش، هماهنگی فرهنگ‌های مختلف کاری طرفین ذینفع و نهادینه‌سازی سازوکارهای حکمرانی تاب‌آور جهت تضمین ظهور سیستم یکپارچه در میان‌مدت تا بلندمدت صورت گیرد. در اینجا شواهد دلالت بر این موضوع دارد که الگوهای رویه مناسب باید گسترش یابند تا با برخورداری از عملکردی اصولی در اروپا و در سطح جهان، ساختار اصلی و پایدارتری برای همکاری عمومی–خصوصی ایجاد نمایند. ایجاد محیط کاری یکپارچه‌تر با بهره‌گیری از تخصص‌های موردنیاز –حقوقی، فنی، عملیاتی، راهبردی و سیاست‌گذاری– مسلماً باعث ایجاد شفافیت رویه‌ای و روابط مبتنی بر اعتماد از طریق انجام تعاملات منظم‌تر بین طرفین اصلی در مقابله با جرائم سایبری می‌شود.

علاوه بر این، عدم تقارن موجود بین کشورهای عضو و منابع و نهادهای در اختیار آن‌ها (مالی، حقوقی، مهارتی، تخصصی و...) برای مقابله با جرائم سایبری، بیانگر وجود مانعی بزرگ با توجه به میزان آمادگی، هماهنگی، شناسایی متقابل و همگرایی است. روابط بین طرفین ذینفع و سازمان‌های مختلف –درون و بین کشورها– سازنده و در حال تکامل است. به همین دلیل، به‌رغم وجود توافق نظر درباره آگاهی از موارد موردنیاز، در عمل کماکان موانع اساسی بر سر راه همکاری و هماهنگی کارآمد وجود دارند. علاوه بر این، به‌رغم این موضوع که اتحادیه اروپا طرح‌های بی‌شماری برای مقابله با جرائم سایبری در اختیار دارد، چگونگی تلفیق این طرح‌ها با یکدیگر و مسئله تأثیر واقعی آن‌ها با توجه به ویژگی‌های عملیاتی، حقوقی و نظارتی، فنی، آموزشی و فرهنگی کماکان مطرح است. بر اساس شواهد موجود در این کتاب می‌توان به این

نتیجه رسید که گرچه امنیت تاب‌آور به درجه‌ای از یکپارچگی لازم جهت مقابله کارآمد با جرائم سایبری در اتحادیه اروپا دست نیافته است، اما شرایط لازم برای تأمین آن در حوزه جرائم سایبری این اتحادیه به‌تدریج در حال شکل‌گیری است. برای تحقق این موضوع در میان‌مدت تا بلندمدت، موانع بین جوامع ذی‌نفع مربوطه باید کماکان حذف شوند و روابط کاری و مشارکت‌های پایداری بر اساس اصطلاحات مشترک ایجاد گردند. تنها در این صورت است که اتحادیه اروپا می‌تواند این مسئله را تضمین نماید که اکوسیستمی که برای رسیدگی به مشکلات جرائم سایبری در حال شکل‌گیری است، امکان محافظت از سیستم‌ها و شبکه‌های اروپا در برابر مجرمان سایبری را در اختیار این قاره قرار می‌دهد و وجود محیطی امن برای رشد اقتصادی در عرصه اقتصاد دیجیتال نیز تضمین می‌گردد.

امنیت شبکه و اطلاعات

رویکرد اتحادیه اروپا در قبال امنیت شبکه و اطلاعات ازنظر حکمرانی، به‌تدریج از رویکردی نظری و فراحکمرانی و اختیاری، به مسئله اشتراک اطلاعات و گزارش رویدادهای مهم که موردحمایت چند برنامه نظیر مجمع اروپایی کشورهای عضو، برنامه مشارکت عمومی–خصوصی اتحادیه اروپا در تاب‌آوری و آژانس امنیت شبکه و اطلاعات اتحادیه اروپا به‌عنوان تسهیل‌کننده اصلی همکاری و ظرفیت‌سازی قرار دارد به رویکرد عملی و الزام‌آور پیشنهادی دستورالعمل‌امنیت شبکه و اطلاعات، تبدیل شده است (۲۰۱۳) که البته در مذاکرات نهادهای اتحادیه اروپا، توافقی پیرامون شکل نهایی آن به دست نیامد (ن.ک. فصل ۶).

در این کتاب تجربیاتی در زمینه چگونگی ترغیب موارد همکاری عمومی–خصوصی و برنامه‌ها به تسهیل این موضوع آموخته شد. در این میان عامل اصلی، تضمین این مسئله است که هر یک از این برنامه‌ها اهداف مشخصی در مورد موضوعات تعریف‌شده ارائه می‌دهد و هر اقدامی نتیجه واضحی در این خصوص دارد که چگونه می‌تواند نقشی در دستورکار حقوقی و تحقیقاتی در حال تکامل اتحادیه اروپا در حوزه امنیت سایبری ایفا کند. از این نظر، مشارکت عمومی–خصوصی اتحادیه اروپا در زمینه امنیت تاب‌آوری به پلتفرم امنیت شبکه و اطلاعات تبدیل شد و بخشی

از آن گردید و ثابت نمود که کارآمدی بیشتری ازنظر تولید محصولاتی دارد که در تحقق اهداف تحقیقاتی مربوط به راهبرد امنیت سایبری اتحادیه اروپا و برنامه افق ۲۰۲۰ تأثیرگذار هستند. بااین‌حال، این مسئله کماکان پرسش‌هایی را در مورد پایداری همکاری‌های عمومی-خصوصی در سطح اروپا مطرح می‌کند. ازاین‌رو، اتحادیه اروپا باید در مورد نحوه پیشبرد چنین برنامه‌ای در میان‌مدت تا بلندمدت برای ایجاد و حفظ فراگیری، اعتماد و تعاملات معمول موردنیاز برای همکاری و هماهنگی کارآمد بین بخش‌های عمومی- خصوصی به‌دقت تأمل نماید.

مجمع اروپایی کشورهای عضو، به‌خوبی توانسته است اسناد اصلی اتحادیه اروپا (اصول و دستورالعمل‌های اروپا در زمینه تاب‌آوری و ثبات اینترنت) را تولید نماید، اما تا زمانی که دولت‌های عضو آن را جدی‌تر نگیرند، این اسناد در حکم برنامه‌ای نمادین به‌جای برنامه‌ای کارآمد برای اشتراک اطلاعات و تبادل شیوه‌های مناسب خواهد بود. تشکیل جلسات در زمینه موضوعات مهم به‌صورت منظم‌تر و غیررسمی در سطوح کاری مختلف احتمالاً در اعتمادسازی لازم برای ایجاد تعاملات مثمر ثمر در میان‌مدت سودمندتر است. همچنین امکان دارد در زمان نهایی شدن امریه امنیت شبکه و اطلاعات و توافق بر سر آن، مسئله ملموسی مطرح گردد که با توجه به رویه‌های اجرا و پیامدهای آن، مقامات به آن می‌پردازند. تجربیات مهم دیگری نیز از اجرای مانورهای امنیت سایبری در اروپا و بین اتحادیه اروپا و آمریکا به دست آمد که ارزشمندترین آن‌ها این مورد است که این برنامه به‌عنوان محلی برای ارتقای یادگیری در سطوح فنی، سیاسی (نهادی)، عملیاتی و راهبردی از عملکرد کارآمدی برخوردار بود و کماکان باید به‌عنوان ابزار اصلی ارتقای دانش، درک و اعتماد بین طرفین اصلی به کار گرفته شود. درواقع، منابع باید گسترش یابد تا تعداد چنین مانورهایی در سطح کلان (در اروپا یا در سطح بین‌الملل) و در سطح خرد (در بین برخی بازیگران عمومی و خصوصی) افزایش پیدا کند و تعامل و آگاهی از فرهنگ‌های کاری مختلف و مهارت‌ها و ظرفیت‌های موردنیاز طرفین ذینفع برای اطمینان از ایجاد نهادها، همکاری‌ها و رویه‌های کاری مشترک کارآمد بیشتر گردد. به‌عبارت‌دیگر، این موضوع به معنای اطمینان از این موضوع است که فرهنگ امنیت تاب‌آور در سراسر اکوسیستم اروپا نهادینه می‌شود و بدین ترتیب چرخه مطلوب یادگیری از طریق انجام کارها در سطوح

مختلف و در سطح بین‌المللی ایجاد می‌گردد.

امریه پیشنهادی برنامه امنیت شبکه و اطلاعات –قانون اصلی ضمیمه راهبرد امنیت سایبری اتحادیه اروپا– از یک سو به اجماع عمومی در زمینه ضرورت ایجاد حداقل ظرفیت‌ها و توانمندی‌ها در تمام کشورهای عضو اتحادیه اروپا (به‌عنوان‌مثال، تیم واکنش اضطراری رایانه‌ای اتحادیه اروپا) دست یافته است تا امنیت سایبری تاب‌آور با توجه به موارد تمایز و عدم تقارن موجود تأمین گردد و از سوی دیگر، تردیدها پیرامون رویکرد مهم و فراگیر بخش زیرساخت آن موجب تضعیف دامنه اصلی این امریه از جانب پارلمان اروپا و کشورهای عضو اتحادیه اروپا شده است که این مسئله احتمالاً پیامدهایی را برای اجرا و به‌کارگیری مؤثر آن و مهم‌تر از آن، برای ایجاد شرایط لازم جهت تحقق امنیت تاب‌آور از طریق همکاری‌ها و ائتلاف‌های قابل‌اعتماد بازیگرانی خواهد داشت که «رویکرد» مشترکی را برای گزارش و تبادل اطلاعات کارآمد اتخاذ کرده‌اند. ازاین‌رو، در آخرین مرحله از مذاکرات مربوط به امریه امنیت شبکه و اطلاعات، توافقی باید در شورای وزیران به دست آید که موازنه بین گزارش‌های رسمی و اجباری و تبادل اطلاعات غیررسمی و مبتنی بر اعتماد را تضمین می‌نماید. تنها در این صورت است که فرهنگ امنیت سایبری به‌مرورزمان نهادینه می‌شود و جلوی حرکت به سمت فرهنگ محدود و حساب‌گرایانه در اروپا گرفته می‌شود که خود موانع بیشتری را بر سر راه همگرایی و همکاری کارآمد طرفین ذینفع ایجاد می‌کند.

اکوسیستم امنیت شبکه و اطلاعات به‌مانند حوزه جرائم سایبری و به نحوی بسیار مرتبط با آن در حال شکل‌گیری است. اگرچه، این شکل‌گیری از وضعیت بهینه‌ای در نهادینه‌سازی شرایط لازم برای انتشار و اجرای رویکرد کارآمد امنیت تاب‌آور در اروپا یا درواقع، از طریق همکاری‌های بین‌المللی اصلی آن برخوردار نیست. این موضوع در کوتاه‌مدت تنها در صورتی محقق می‌شود که تمام طرفین ذینفع از زمینه‌های «مشترک» کافی در مورد کارآمدترین شیوه(های) حکمرانی برای تشویق برقراری روابط کاری مؤثر در خصوص تبادل، اشتراک و پردازش اطلاعات بهره‌مند باشند. در دوره میان‌مدت تا بلندمدت نیز زمانی این مسئله روی می‌دهد که کانال‌ها و مجامع رسمی و غیررسمی، روابط پایدار و مبتنی بر اعتمادی را ایجاد نمایند که امکان شکوفایی رویه‌های مناسب و ظهور فرهنگ اصیل امنیت سایبری را فراهم می‌کنند. کمیسیون اروپا در این

برهه از زمان، معتقد است که دستورالعمل پیشنهادی امنیت شبکه و اطلاعات، برنامه لازم برای این کار یا برنامه حداقلی را برای بهبود وضعیت اروپا فراهم می‌آورد. گرچه، در عمل این مسئله کاملاً به میزان توافق نهایی (و اجرای) آن بین فرهنگ‌های ملی و حرفه‌ای امنیت سایبری درون و بین کشورهای عضو اتحادیه اروپا بستگی دارد.

دفاع سایبری

دفاع سایبری، جدیدترین بخش راهبرد امنیت سایبری اتحادیه اروپا محسوب می‌شود و به همین دلیل، کمتر از سایر بخش‌های آن توسعه پیدا کرده است. پذیرش این مسئله نیز حائز اهمیت است که برداشت اتحادیه اروپا از دفاع سایبری بر اساس منطق امنیت تاب‌آور پایه‌ریزی شده است تا بتواند در صورت لزوم از خود دفاع کند و همواره نیز به منابع نظامی و غیرنظامی مرتبطی که کاربرد نظامی دارند، دسترسی داشته باشد (رویکرد قدرت نرم). این مورد به‌عنوان‌مثال، در تضاد مستقیم با رویکرد ایالات‌متحده آمریکا است که بر اساس منطق تهاجم سایبری عمل می‌کند و سلاح‌های سایبری خود را ارتقا می‌بخشد تا برای جنگ با دشمن سایبری خود کاملاً مجهز باشد (رویکرد قدرت سخت). دلیل اصلی این موضوع آن است که اتحادیه اروپا دارای نیروی نظامی متعلق به خود نیست. برخی کشورهای عضو که از نیروی نظامی برخوردارند بر سلاح‌های سایبری سرمایه‌گذاری می‌کنند، اما دیگر کشورهای فاقد سلاح‌های سایبری در چارچوب راهبردهای ملی امنیت سایبری خود، چشم‌انداز نظامی درخصوص دفاع سایبری در نظر می‌گیرند. سایر کشورها نیز کماکان راهبرد امنیت سایبری برای خود تعریف نکرده‌اند و به‌رغم آشنایی با مسائل مربوط به دفاع سایبری، درک کاملی از آن‌ها ندارند یا به آن‌ها توجه کافی نمی‌کنند.

این تنوع و عدم تقارن موجود در دانش و آمادگی لازم در حوزه دفاع سایبری به نسبت سایر حوزه‌های موردبحث، بیشتر مشهود است، چراکه مشکلات خاص مربوط به طرح دکترین‌ها پیرامون دفاع سایبری، سازماندهی و آموزش مناسب و نیز تجهیزات لازم برای دفاع سایبری در کشورهای عضو اتحادیه اروپا شناسایی می‌شوند. نکته مثبت‌تر در اینجا این است که سطح توسعه

بسیار بالاتری در حوزه‌های مربوط به مدیریت، کارمندان و قابلیت همکاری مشاهده می‌شود. ظاهراً کشورهای عضوی که تصمیم‌گیرندگان اصلی آن‌ها به بلوغ فکری در زمینه امنیت سایبری رسیده‌اند، از پیشرفت بیشتری نیز در حوزه توانمندی دفاع سایبری برخوردارند.

توانمندی تحلیل تهدیدها و جمع‌آوری اطلاعات در اتحادیه اروپا در شرف تکوین است و واکنش جدی‌تری باید در قبال رویدادها در چارچوب ساختار سازمانی پیچیده در سطح عملیاتی صورت گیرد. علاوه بر این، شناخت و درک استانداردها و ابزارهای نظامی ویژه باید تا حد بسیاری بهبود یابد و لازم است فرهنگ به‌کارگیری شیوه مناسبی در حوزه امنیت سایبری ایجاد گردد تا کارایی آن افزایش یابد. بااین‌وجود، تحت مدیریت آژانس دفاع اتحادیه اروپا، طرح‌ها در اصل، با نیت دستیابی به اهداف مدنظر چارچوب سیاست‌های دفاع سایبری به‌سرعت توسعه یافته‌اند. بخش‌هایی مانند تعلیم و آموزش نسبت به سایر بخش‌ها در اتحادیه اروپا تکامل بیشتری پیدا کرده‌اند و طرح‌های موردی که برای افزایش دانش و توانمندی توسط آژانس دفاع اتحادیه اروپا عملیاتی شده‌اند، برنامه‌های سودمندی محسوب می‌شوند.

بااین‌وجود، کماکان چالش‌های بی‌شماری ازنظر گسترش تاب‌آوری در حوزه دفاع سایبری اتحادیه اروپا و کشورهای عضو وجود دارد. در وهله نخست، این‌گونه نیست که تمام کشورهای عضو اتحادیه اروپا در زمینه دفاع سایبری همکاری می‌کنند و عدم اجبار کشورها به مشارکت در سیاست امنیتی و دفاعی مشترک مؤید همین مطلب است. این مسئله ایجاد همکاری و در نتیجه درک و اتخاذ رویکردهای مشترک در حوزه کاملاً مشخص منافع و تهدیدات مشترک پیش روی تمام کشورهای عضو اتحادیه اروپا را دشوارتر می‌سازد. دوم اینکه، مسائلی در داخل اتحادیه اروپا و بین این اتحادیه و کشورهای عضو درباره موارد هم‌افزایی و اتخاذ رویکردهایی در پشتیبانی از عملیات‌های نظامی مطرح می‌شوند که اغلب متکی بر زیرساخت‌های حیاتی خصوصی هستند. تعاریف، دکترین‌ها، فرایندها و رویه‌های مشخصی باید جهت اطمینان از شفافیت رویکرد و ارزیابی تهدیدات امنیت سایبری در مراحل مختلف هر مأموریت مطرح شوند. علاوه بر این، از طریق برقراری تعامل بیشتر کارکنان در تیم‌های نظامی واکنش اضطراری رایانه‌ای با تیم‌های غیرنظامی واکنش اضطراری رایانه‌ای، باید دوره‌های آموزشی بیشتری برگزار شوند تا خطرات

مشترک، رویه‌ها و فرایندهای موردنیاز برای برخورد با تهدیدات سایبری در حوزه دفاع سایبری بهتر درک گردند.

باوجوداینکه آژانس دفاع اتحادیه اروپا مسلماً اقداماتی در زمینه گسترش چنین تعاملاتی از طریق برنامه‌های آموزشی مختلف انجام می‌دهد، این اقدامات باید در کوتاه‌مدت تا میان‌مدت افزایش یابد تا بازیگران و مؤسسات ملی و اروپایی به درک متقابل بیشتری از الزامات تکامل تاب‌آوری در حوزه دفاع سایبری دست یابند. آموزش و حفظ متخصصان امور سایبری برای مقاصد نظامی نیز به همین مسئله مربوط است. اتحادیه اروپا در وهله نخست باید با همکاری با کشورهای عضو، تعداد برنامه‌های آموزش نظامی سایبری هدفمند را در کوتاه‌مدت افزایش دهد و سپس سیاست‌ها و مشوق‌هایی را در زمینه حفظ متخصصان برای دوره زمانی میان‌مدت تا بلندمدت طرح‌ریزی کند تا دسترس‌پذیری به مهارت‌ها و دانش موردنیاز برای حفظ تاب‌آوری در حوزه دفاع سایبری تضمین گردد.

درنهایت، به‌رغم وجود ظرفیت ایجاد تحول در همکاری‌های بین‌المللی مؤثرتر برای رسیدگی به مسائل مربوط به دفاع سایبری و علیرغم وجود موارد هم‌افزایی مشخص، پیچیدگی فرایندهای رسمی –به‌ویژه در ارتباط با ناتو– موجب محدودیت پیشرفت در این خصوص شده است. اتحادیه اروپا کماکان باید به جستجوی راه‌حل‌های رسمی در این زمینه ادامه دهد و درعین‌حال، از روابط غیررسمی شکل‌گرفته بین مقامات امنیت سایبری اتحادیه اروپا و ناتو در سطوح مختلف کاری بهره بیشتری ببرد.

تأملاتی پیرامون حوزه‌های داخلی و بین‌المللی

همان‌طور که در فصول مختلف این کتاب اشاره شد، امنیت سایبری شامل لایه‌ها و سطوح بی‌شماری است که در زمان بحث درباره تکامل امنیت تاب‌آور، مجموعه‌ای از آن‌ها را باید موردبررسی قرار داد. بدین منظور، در زمان تحلیل میزان پیشرفت اتحادیه اروپا، درک زمینه‌های اقدام و تأثیرگذاری داخلی و بین‌المللی اتحادیه اروپا حائز اهمیت است. باوجوداینکه در این کتاب به جزئیات میزان آمادگی کشورهای عضو اتحادیه اروپا به‌استثنای بریتانیا پرداخته نشد، از

شواهد ارائه‌شده درباره سه رکن اصلی موردبحث، می‌توان به مفاهیم کلی در این مورد دست یافت. به‌علاوه، تجربه بریتانیا برداشت دقیقی را از رویه‌های به‌کاررفته در حوزه امنیت سایبری فراهم می‌آورد که می‌توان آن را به سایر عرصه‌های داخلی و مؤسسات و مجامع اروپایی نیز منتقل نمود و درعین‌حال، بر این نکته نیز تأکید کرد که حتی در کشورهای پیشرفته عضو اتحادیه اروپا، استدلال‌ها و رویکردهای متفاوت می‌توانند موانع بالقوه‌ای را بر سر راه توسعه رویکرد اروپایی و جهانی به مقوله امنیت تاب‌آور ایجاد نمایند.

درمجموع، بدیهی است که اعضای اتحادیه اروپا در مورد ارکان امنیت سایبری (جرائم سایبری، امنیت شبکه و اطلاعات و دفاع سایبری) به سطوح بلوغ متفاوتی رسیده‌اند. پیشرفت در این زمینه کند بوده است، اما این موضوع به‌زودی محقق می‌شود. یکی از نشانه‌های مهم این مسئله، تکامل راهبردهای امنیت سایبری در هجده کشور عضو اتحادیه اروپا است. گرچه این مسئله نیز بدیهی است که در دوره زمانی کوتاه‌مدت تا میان‌مدت، عدم تقارن موجود در اروپا بین اعضای اتحادیه اروپا و کشورهای منطقه اقتصادی اروپا (ایسلند، لیختن‌اشتاین و نروژ) کماکان باقی خواهد ماند. در این کشورها سطوح توسعه متفاوتی وجود دارد و فرهنگ امنیت سایبری در لایه‌های مختلف ایجاد شده است، اما درمجموع، کماکان از وضعیت بهینه امنیت تاب‌آور، چه در ارتباط با رویه‌های تبادل و همکاری در زمینه اطلاعات و چه ایجاد مؤسسات و فرایندهایی برای مدیریت و گزارش حوادث امنیتی، تاب‌آوری شبکه‌ها، چارچوب‌های حقوقی برای اطمینان از ایجاد توازن بین حفظ حریم خصوصی و تأمین امنیت یا افزایش آگاهی نسبت به این موضوعات فاصله بسیاری داریم. نتیجه‌گیری نه‌چندان مطمئن در این زمینه، بدین قرار است که در تمام کشورهای عضو اتحادیه اروپا، آگاهی و درک مشترکی از اجزای تشکیل‌دهنده اکوسیستم تاب‌آور ازنظر ضرورت وجود حداقل الزامات وجود دارد. اگرچه، برای تحقق عملی این موضوع، موانع قابل‌ملاحظه فرهنگی، نهادی، قانونی و مربوط به منابع در داخل و خارج از کشورهای عضو وجود دارد و در برخی موارد نیز میزان درک و آگاهی آن‌ها از تهدیدات سایبری بالقوه کافی نیست.

در مطالعه موردی بریتانیا که کشوری پیشرو در حوزه سیاست‌گذاری و تفکر در زمینه امنیت سایبری در اتحادیه اروپا به‌شمار می‌آید، این مسئله مشخص گردید که اکوسیستم امنیت

سایبری این کشور از طریق اتخاذ رویکردی جامع در طی چهار سال گذشته به پیشرفت بسیاری دست یافته است. هرچند، رویکرد دولت بریتانیا که بر اساس منطق اختیاری، نظری و مبتنی بر بازار است که کاملاً در تضاد با رویکرد الزام‌آور برگرفته از امریه پیشنهادی امنیت شبکه و اطلاعات است. از این نظر، تنها دولت بریتانیا نیست که اصرار می‌ورزد اتخاذ رویکرد اختیاری به‌احتمال‌زیاد منجر به اشتراک اطلاعات به‌صورت پایدار و مبتنی بر اعتماد بین طرفین ذینفع اصلی می‌گردد. درواقع، اختلاف پیش‌آمده در شورای وزیران ظاهراً بین کشورهای پیشرفته حامی این موضع و اعضای کمتر توسعه‌یافته حامی رویکرد الزام‌آور ایجاد شده است. مسلماً نمونه‌های مناسبی درخصوص عملکرد چنین رویکردی –از طریق طرح‌هایی مانند مشارکت در زمینه اشتراک اطلاعات در حوزه امنیت سایبری در بریتانیا ملاحظه می‌شود، لیکن این‌گونه طرح‌ها نیز مشکلات خود را دارند. مورد حائز اهمیت در زمینه توسعه امنیت تاب‌آور در اروپا، مسئله ظهور ناسازگاری عملی احتمالی در صورت عدم دستیابی به توافق کارآمدی درباره دستورالعمل امنیت شبکه و اطلاعات است که می‌تواند بین دو منطق اختیاری و الزام‌آور سازگاری ایجاد نماید. باید به موضعی همگرا دست یافت که ظهور فرهنگ اشتراک اطلاعات را تضمین می‌کند و از گزارش‌های رویه‌ای مربوط به حوادث فراتر می‌رود تا بیانگر پذیرش تبادل اطلاعات مؤثر و به هنگام بر پایه منافع مشترک پیرامون برخورد با تهدیدات سایبری باشد. بریتانیا باید به این موضوع نیز واقف باشد که عدم مشارکت این کشور در دوره زمانی میان‌مدت تا بلندمدت در اقدامات دفاع سایبری اتحادیه اروپا به ضرر منافع آن است و توانمندسازی خود در اروپا مطمئناً موجب افزایش امنیت تاب‌آور کشور می-گردد، به‌خصوص که معماری و منابع نظامی و غیرنظامی در چارچوب مأموریت‌های اتحادیه اروپا به‌هم‌پیوسته است.

در زمینه رویه‌های مناسب، مطمئناً می‌توان تجربیاتی را درباره همکاری‌های رسمی و غیررسمی در حوزه‌های آموزش، آگاهی و به‌ویژه درباره بعد عملیاتی جرائم سایبری آموخت و به دیگران منتقل ساخت. از این نظر، طرح کارگروه اقدام مشترک علیه جرائم اینترنتی که توسط آژانس ملی جرائم بریتانیا مطرح شد و در مرکز مقابله با جرائم سایبری اتحادیه اروپا حالت نیمه‌رسمی پیدا کرد، بیانگر این مطلب است که چگونه مشارکت چندجانبه می‌تواند عملکرد

کارآمدی به‌عنوان‌مثال، در حذف بات‌نت‌ها و شبکه‌های پورنوگرافی کودکان داشته باشد. چنین حکمرانی موردی، شناخت ارزشمندی در مورد موانع موجود بر سر راه انجام این کار در سطح بین‌المللی نظیر موانع قانونی و رویه‌ای ازنظر دسترسی به آدرس‌های آی‌پی یا دسترسی و استفاده از اطلاعات در زمان واقعی فراهم می‌کند. به‌علاوه، این حکمرانی موجب تسهیل ایجاد سازوکارهای خلاقانه‌ای نظیر سیستم‌های رمزنگاری نیز می‌شود که به مسائل مربوط به حریم خصوصی رسیدگی می‌کنند و درعین‌حال، این مسئله را نیز تضمین می‌کند که اشتراک اطلاعات مخصوص اقدامات یا تحقیقات موردی خاص و نه تبادل اطلاعات حجیم است. به‌رغم وجود روند تکوینی در چنین سازوکارهایی، آن‌ها باید مورد پشتیبانی و حمایت مالی بیشتر اتحادیه اروپا قرار گیرند، چراکه شیوه کارآمدی برای محافظت در مقابل جرائم سایبری ارائه و مشکلات را نیز پیدا می‌کنند و راه‌حل‌هایی نیز برای دستیابی به واکنش‌های کارآمد در برابر حملات و تهدیدات ارائه می‌دهند.

در محیط سایبری جهان، اعتراض و اجماع بسیاری درخصوص چگونگی مدیریت ابعاد مختلف امنیت سایبری وجود دارد. همان‌طور که در فصول سوم و هفتم اشاره شد، در جامعه بین‌الملل این موضوع به‌روشنی پذیرفته شده است که چنان چه قرار باشد فرهنگ جهانی امنیت در فضای سایبری شکل گیرد، وجود هنجارهای جهانی برای حکمرانی بر رفتار کشورها و سایر بازیگران لازم است. علاوه بر این، دستورالعمل‌ها و اجماعی کلی در مورد برخی اصول اصلی مبنای چارچوب جهانی وجود دارد. گرچه علی‌رغم وجود همگرایی مسلم در زمینه اصول و هنجارهای کلی، اتفاق‌نظری در مورد معنای این هنجارها برای حکمرانی اینترنت و همچنین معنای امنیت سایبری در کشورهای مختلف مشاهده نمی‌شود. درواقع، چند مورد تنش غالب به چشم می‌خورد که ایجاد شرایط بهینه لازم برای ظهور امنیت تاب‌آور را با اختلال روبرو می‌کنند که مهم‌ترین آن‌ها عبارت‌اند از: تنش بین منطق تجاری و منطق امنیت تاب‌آور، منطق امنیت ملی مستقل برخی کشورهای خاص و رویکرد باز و چندجانبه موردحمایت بسیاری از کشورهای مطرح «غربی» و سازمان‌های بین‌المللی و سرانجام، تنش بین حفظ حریم خصوصی و برقراری امنیت (که بسیار مرتبط با مورد قبلی است) و مبحث چگونگی دستیابی به موازنه‌ای

برای تضمین حفظ حقوق افراد در زمان جمع‌آوری اطلاعات برای تأمین امنیت فضای سایبری. گرچه این مسئله صرفاً مورد تقابل «غرب» و «بقیه دنیا» نیست و کشمکش در فضاهای مختلف به چشم می‌خورد و همواره نیز بین ائتلاف‌های گوناگون بازیگران در حال تغییر است. بدین ترتیب، باوجوداینکه اتحادیه اروپا و آمریکا مسلماً در مورد این مسئله توافق دارند که اینترنت باید آزاد، قابل‌دسترس و تاب‌آور باشد و الگوی چندجانبه‌ای را باید در مورد حکمرانی اینترنت در مقابل الگوی کشورهایی نظیر چین و روسیه به کار برد که از سیستم بین دولتی و دولت‌محور حمایت می‌کنند، اما اختلافاتی نیز بین آن‌ها بروز می‌کند که منشأ آن رویکردهای مبتنی بر منطق امنیت آن‌ها در قبال امنیت سایبری است. از این نظر، افشاگری‌های اسنودن بر اختلافات بین اتحادیه اروپا و ایالات‌متحده دامن زد و موجب بی‌اعتمادی آن‌ها به یکدیگر در حوزه مسائل مربوط به حفظ حریم خصوصی در برابر برقراری امنیت و امنیت سایبری گردید. این افشاگری‌ها دستاویزی برای توجیه رویکرد امنیت ملی کشورهای اقتدارگرا نیز ایجاد کردند که با «مرزبندی» اینترنت، به دنبال این هستند فضای سایبری داخلی خود را امن نگاه دارند.

افشاگری‌های اسنودن تا حدی موجب ایجاد تنش در روابط اتحادیه اروپا و آمریکا شد، اما دوره‌ای از تأمل، تعمق و اصلاح نیز در این روابط ایجاد نمود. این موضوع تا اندازه‌ای در احیای اعتماد طرفین نقش داشت، اما ضرورتاً منجر به همگرایی رویکردها یا رویه‌ها در ابعاد مختلف امنیت سایبری نشد. دلیل این مسئله نیز آن است که کماکان اختلافات اساسی در حوزه‌های حقوقی و فرهنگی بین اتحادیه اروپا و آمریکا وجود دارد. بااین‌حال، اگر اتحادیه اروپا و آمریکا هر دو مایل به ایجاد فرایندها و سازوکارهای کاری مشترک و کارآمدی برای پرداختن به مسائل امنیت سایبری بوده و خواستار آن هستند که به نحو متقاعدکننده‌ای از ارزش‌های اصلی حکمرانی اینترنت مطرح‌شده در عرصه بین‌المللی دفاع کنند و آن‌ها را اشاعه دهند، آن‌ها می‌توانند به توافق عملی در این حوزه دست یابند که البته این مسئله ضرورت نیز دارد. برای دستیابی به امنیت تاب‌آور کارآمد در همکاری‌های اتحادیه اروپا و آمریکا، سازمان‌های اطلاعاتی آن‌ها (به‌عنوان‌مثال آژانس امنیت ملی ایالات‌متحده آمریکا و ستاد ارتباطات دولتی بریتانیا) باید به تناقض موجود بین ارزش‌های موردحمایت و اقدامات صورت‌گرفته رسیدگی کنند. در غیر

این صورت، این تناقض پیامدهایی برای توافقات کنونی در زمینه ثبت‌نام و مشخصات مسافران در خطوط هوائی و پروتکل انتقال فایل و مسائل کلی‌تری نظیر مذاکرات موافقت‌نامه مشارکت تجاری و سرمایه‌گذاری فراآتلانتیک دارد. این مسئله پیامدهایی نیز برای قدرت نفوذ اتحادیه اروپا و آمریکا در عرصه بین‌المللی امنیت سایبری خواهد داشت. تنش‌ها و موارد تناقض موجود در محور استدلال‌های مختلف در حوزه سیاست (ژئوپلیتیک) فضای سایبری که در قالب موارد بی‌شمار اصول اخلاقی، دستورالعمل‌ها، اصول و حقوق و منشورهای بین‌الملل (که لزوماً همگرا یا مشترک نیستند) ملاحظه می‌شوند باید کماکان مدنظر اتحادیه اروپا برای تأثیرگذاری و تأثیرپذیری فعالانه باشند تا اقدامات آن بتواند موجب خلق اکوسیستم فراگیر و منعطف حکمرانی امنیت تاب‌آور گردد. اگرچه برای تحقق این امر، اتحادیه اروپا باید کماکان به بهره‌گیری از دیپلماسی کنفرانسی، اقدامات دوجانبه با کشورهای راهبردی و همکاری با نهادهای بین‌المللی مانند سازمان همکاری اقتصادی و توسعه ادامه دهد که نقش اصلی در انجام اقدامات اعتمادساز در آن‌ها داشته است. گرچه، تأمل خلاقانه‌تر پیرامون تعامل و همکاری منظم‌تر چندجانبه و عملی (نظیر تلاش‌های تحقیقاتی و عملیاتی) و منابع موردنیاز برای انجام این کار نیز حائز اهمیت است.

تأملات و سخن پایانی

این کتاب راهنمای کلی درخصوص جهت سیر اتحادیه اروپا در دستیابی به مورد مطرح‌شده در فصل دوم با عنوان امنیت تاب‌آور اجتماعی- اکولوژیک یا نوع سوم در سیاست و راهبرد امنیت سایبری این اتحادیه است. با بهره‌گیری از شرایط عمومی مطرح‌شده در ادبیات مربوط به امنیت تاب‌آور کارآمد و با بررسی انواع حکمرانی غالب به‌کاررفته در اکوسیستم در حال تکامل اتحادیه اروپا، طرح کلی از خط سیر ارکان مورد تحلیل امنیت سایبری این اتحادیه ازنظر پیشرفت داخلی و بین‌المللی ترسیم گردید. گرچه تحلیل ارائه‌شده از این ارکان جامع است، اما جنبه‌های خرد و کلان بی‌شمار دیگری نیز وجود دارند که در اینجا مجال پرداختن به آن‌ها نیست و باید در تحقیقات آتی موردبررسی قرار گیرند تا مفهوم جامع‌تری از جایگاه اتحادیه اروپا در ابعاد مختلف

راهبرد آن، مسائل و اولویت‌های مدنظر آن و بازیگران و فضاهایی به دست آید که با آن‌ها تعامل دارد. در این زمینه، توسعه شرایط لازم برای ایجاد امنیت تاب‌آور در اعضای اتحادیه اروپا، به‌صورت اساسی‌تر و کیفی‌تر در برنامه‌های تحقیقاتی سودمند آتی بررسی می‌گردد. موانع بر سر راه همکاری در زمینه امنیت سایبری و مسائل مربوط به جرائم سایبری بین طرفین ذینفع و مؤسسات اصلی در داخل و خارج از اعضای اتحادیه و بین اتحادیه اروپا و شرکای بین‌المللی و کشورهای دیگر نیز موردبررسی قرار می‌گیرند.

گذشته از محدودیت‌های مذکور، این تحلیل پرسش‌هایی را پیرامون سودمندی امنیت تاب‌آور به‌عنوان مفهوم راهنمای راهبرد امنیت سایبری و رویکرد امنیت تاب‌آور برای درک نتایج کنونی و ضروری اقدامات اتحادیه اروپا مطرح می‌کند. سه جنبه مرتبط در این خصوص وجود دارد: جنبه‌های عملی، نظری و هنجاری. در سطح عملی گرچه می‌توان به روندها و الگوهای کلی امنیت تاب‌آور اشاره کرد، اما سنجش و ارزیابی دقیق شرایط امنیت تاب‌آور –به‌ویژه ازنظر تحول فرهنگی عملی– دشوار است. در کشورهایی (به‌عنوان‌مثال، آمریکا) که این برنامه‌ها را به کار می‌گیرند، کماکان مشکلاتی در زمینه انتخاب شاخص‌ها، طرفین ذینفع مورد مشورت و کفایت داده‌های افزوده‌شده وجود دارد (Cavelty and Prior 2013, p.3). چنین مشکلات کلی در مورد سنجش میزان تاب‌آوری در حوزه‌های امنیتی، در عرصه امنیت سایبری تشدید می‌شوند، چراکه لایه‌ها، سطوح، فضاها و ابعاد چندگانه موجود نیز باید سنجیده شوند. گرچه برای اینکه مفهوم تاب‌آوری در حوزه امنیت سایبری با اتهام ابهام و عدم وضوح مواجه نشود که سال‌ها دامن‌گیر مسائل مربوط به امنیت انسانی است، متغیرهای مدنظر برای چگونگی دستیابی به تاب‌آوری به‌صورت عملی، به‌ویژه در اتحادیه اروپا و اروپا، باید به شکل خاص‌تری برای اهدافی فراتر از شرایط عمومی طراحی شوند تا اهداف و اقدامات صورت‌گرفته در حوزه‌های دارای اولویت (و عناصر خرد در این حوزه‌ها) را پوشش دهند. در اینجا تجربیات ارزشمندی را می‌توان از دستورالعمل‌های در حال تکامل برای دستیابی به امنیت تاب‌آور یکپارچه در حوزه‌های موازی مدنظر فراگرفت (به‌عنوان‌مثال، در حوزه مدیریت بحران و حوادث؛ ن.ک. Comfort et al. 2010; Chmutina et al. 2014).

مطالب ذکرشده بدین معنا نیست که امنیت تاب‌آور را باید به‌طور نسنجیده به‌عنوان راه‌حلی برای برخورداری از امنیت سایبری کارآمد پذیرفت. تحلیل اکوسیستم امنیت سایبری اتحادیه اروپا بیانگر وجود برداشت‌ها و استدلال‌های گوناگونی در مورد امنیت تاب‌آور در سطوح کاری مختلف است. لازم به ذکر است که ایجاد سازگاری بین فرهنگ‌های مختلف امنیت سایبری با هدف دستیابی به درک و طرز فکر و اقدام مشترک در این خصوص، اقدامی دشوار است. ازاین‌رو، درک نحوه ایفای نقش و تکامل این برداشت‌ها و شکل‌گیری و عملکرد امنیت تاب‌آور در عمل (در حوزه‌های سیاسی، اقتصادی، حقوقی، عملیاتی و راهبردی) برای ارتقای دانش ما در زمینه تأثیرات آن و درواقع، در زمینه تکامل این مفهوم در اتحادیه اروپا به‌عنوان روایتی راهبردی، حائز اهمیت است که می‌تواند راهنمای امنیت سایبری باشد. به همین دلیل، تحقیقات آتی باید بیشتر به مسئله نحوه عملکرد تاب‌آوری در حوزه امنیت سایبری بپردازند که در آن با رقابت و چالش مواجه شده‌اند و تأثیرات مادی و غیرمادی (فرهنگی) تاب‌آوری بر ایجاد امنیت بیشتر در فضای سایبری را نیز موردبررسی قرار دهند.

درنهایت، در جنبه هنجاری، محور استدلال ضمنی مطرح‌شده در تحلیل اکوسیستم در حال تکامل اتحادیه اروپا برای امنیت سایبری، نوع یا مفهوم خاص امنیت تاب‌آور است که اساس آن توجه به امنیت افراد در فضای سایبری است و نه امنیت ملی کشورها. این تحلیل نشان داد که در مورد آمریکا و کشورهای حاضر در سازمان همکاری شانگهای (چین، قزاقستان، قرقیزستان، روسیه، تاجیکستان و ازبکستان) و در اتحادیه اروپا (مانند بریتانیا) که اولویت رویکرد امنیت ملی، حفظ فضای سایبری از طریق تداوم جنگ سایبری و نظارت جمعی و جاسوسی است، آزادی و امنیت اینترنت، تحت تأثیر نامطلوبی قرار می‌گیرند. درواقع، بنا به نظر استادانه دان کاوتلی (۲۰۱۴)، رویکرد امنیتی ملی یا سنتی به فضای سایبری، تنها منجر به ایجاد معضل امنیتی در حوزه سایبری و آسیب‌پذیری بیشتر و نه برقراری امنیت تاب‌آور می‌گردد.

رویکرد اتحادیه اروپا تاکنون، بر اساس تعریف آن در راهبرد امنیت سایبری و در عمل، بر پایه منطق امنیت تاب‌آور، یعنی بر اساس حفاظت از خود از طریق ایجاد و نمایش قدرت نرم (دفاع حفاظتی) و نه قدرت سخت (حمله) شکل گرفته است (ن.ک. فصل ۲). به‌رغم وجود جهت‌گیری

عمومی اتحادیه اروپا، مدیریت خطرات مرتبط با فرایندهای تضمین امنیت اطلاعات و داده‌ها نیز در سیاست‌ها و برنامه‌های این اتحادیه و کشورهای عضو آن ملاحظه می‌شود. به نظر برخی مفسران، با وجود کاربرد گسترده روش‌های سنتی مقابله با خطرات (امنیت تاب‌آور نوع ۲، ن.ک. فصل ۲) در امنیت سایبری، آن‌ها با رویکرد امنیت تاب‌آور (ازلحاظ اجتماعی- اکولوژیک) سازگاری ندارند. این روش‌ها با تعریف ارائه‌شده از امنیت تاب‌آور همخوانی دارند که خطی بودن و پیش‌بینی‌پذیری را مفروض می‌دانند، اما در حوزه شبکه‌های پیچیده و خطرات، اساساً عملکرد ناقصی دارند چراکه امکان هر نوع پیش‌بینی صحیح رویدادها در آن‌ها به‌واسطه عدم قطعیت کاهش می‌یابد (Dunn Cavelty 2013). اگرچه، اتحادیه اروپا از طریق ارائه طرح‌هایی نظیر برنامه امنیت شبکه و اطلاعات و انجام اقدامات خود در جهت تشویق و خلق همکاری‌ها و سیستم‌های کاری پایدار برای اشتراک اطلاعات و گزارش‌دهی و ویژگی‌های عملیاتی جرائم سایبری، این مسئله را نشان داده است که اقدامات این اتحادیه در چارچوب منطق امنیت تاب‌آور برنامه‌ریزی و اجرا می‌گردد. از این نظر، ابعاد اکوسیستم امنیت سایبری تاب‌آور اتحادیه اروپا حالت تکوینی و درعین‌حال متغیری دارند. چالش پیش روی اتحادیه اروپا برای تضمین امنیت فضای سایبری و محافظت از ارزش‌های حکمرانی اینترنت موردحمایت، اطمینان از این مسئله است که امنیت تاب‌آور و نه رویکردهای سنتی در قبال امنیت ملی و خطرات، در خط مقدم و مرکز تکامل سیاست آن حفظ شده و توسعه می‌یابند و این مفهوم در رویه‌های مربوط به امنیت سایبری این اتحادیه به‌خوبی تثبیت و به‌روشنی تبیین شده و به نحو مؤثری نیز به اجرا درمی‌آیند. بدین ترتیب، امنیت تاب‌آور کارآمد از طریق فرایند یادگیری و اندیشه مکرر در حوزه‌های خاص و با اجتناب از تعمیم که ممکن است این مفهوم را غیرضروری سازد، تکامل پیدا می‌کند.

درنهایت، باید پیرامون موضوع فراحکمرانی امنیت سایبری در اتحادیه اروپا و رابطه آن با ایجاد رویکرد امنیت تاب‌آور در اروپا و عرصه بین‌الملل اندیشید. حکمرانی چندگانه‌ای در حوزه اولویت‌های اصلی راهبرد امنیت سایبری اتحادیه اروپا در حال تکامل است که ترکیبی از رویکردهای عملی، نظری و فراحکمرانی مربوط به هویت است. بااین‌وجود، در تحلیل سیستم در حال تکامل حکمرانی امنیت سایبری اتحادیه اروپا این موضوع مشخص شد که حرکتی به‌سوی

رویکرد عملی با هدف ایجاد شرایط لازم برای امنیت تاب‌آور در قالب گزارش‌دهی اجباری مطرح‌شده در دستورالعمل امنیت شبکه و اطلاعات یا به دلیل ضرورت وضوح قانونی و حقوقی بیشتر در حوزه جرائم سایبری در حال وقوع است. این امر به‌رغم این مسئله انجام می‌شود که همان‌طور که در بالا اشاره شد اتخاذ چنین رویکردی (یعنی گزارش‌دهی الزامی) با مخالفت‌هایی در اروپا و عرصه بین‌الملل در داخل اتحادیه اروپا و بین طرفین ذینفع عمومی و خصوصی روبرو شده است.

بدین ترتیب، تصویر روشنی از ماهیت رویکرد بهینه دستیابی به امنیت تاب‌آور در اکوسیستم اتحادیه اروپا وجود ندارد و به‌جای آن، بحثی پویا در زمینه این مسئله وجود دارد که چگونه می‌توان به بهترین نحو به روابط مبتنی بر اعتماد دست یافت که منجر به ایجاد برنامه‌های پایدار و مشارکتی می‌گردد. بااین‌وجود، تجربه اصلی به‌دست‌آمده از این تحقیق و درواقع، از رویه‌های به‌کاررفته در اتحادیه اروپا، توجه به نقش اصلی ترتیبات حکمرانی چندجانبه، غیررسمی و موردی در سطوح کاری عملیاتی است که امکان انجام اقدامی هدفمند در زمینه مسائل خاص و ترتیباتی که بیشتر حالت نیمه‌رسمی و رسمی دارند را ایجاد می‌کند که انجام تعامل منظم بین طرفین ذینفع مربوطه (به‌عنوان‌مثال، مانورهای مشترک در حوزه امنیت سایبری و اعزام موقت کارکنان) را ممکن می‌سازد. چنین ترتیبات نوظهوری متعاقباً به رشد آگاهی و درک متقابل بازیگران مربوطه منجر می‌شود و فضایی را می‌آفرینند که در آن فرهنگ‌های رویه‌های مختلف را می‌توان جهت ایجاد شرایط لازم برای توسعه امنیت تاب‌آور تعدیل نمود. بدین منظور و به دلیل ضرورت ایجاد تاب‌آوری و سازگاری در سیستم امنیت سایبری تاب‌آور اتحادیه اروپا، باید فضا و حمایت لازم برای ایجاد اشکال حکمرانی تجربی و چندگانه به همراه برنامه‌های عمومی-خصوصی پایدارتر تأمین گردد و مورد تشویق قرار گیرد. به‌ویژه این موضوع درجایی صدق می‌کند که شواهد دال بر آن است که این مورد احتمالاً خلاقانه‌ترین شیوه ایجاد روابط مبتنی بر اعتماد و ارائه راه‌حل‌هایی برای چالش‌های امنیت سایبری موجود پیش روی اتحادیه اروپا و قاره اروپا محسوب می‌شود.

یادداشت‌ها

فصل ۲. مفهوم‌سازی امنیت تاب‌آور در فضای سایبری

۱. اسلیوینسکی به تحلیل اتحادیه اروپا به عنوان کارگزار امنیت سایبری می‌پردازد، اما به رغم به-کارگیری مفهوم قدرت سایبری، این مفهوم به طور دقیق تعریف نشده است. در واقع، [این تحلیل] صرفاً این مسأله را مطرح می‌کند که اتحادیه اروپا برای تأثیرگذاری باید اشکال مختلف قدرت سایبری (اجباری، سازمانی، ساختاری و تولیدی) را توسعه دهد. گرچه، این موضوع باعث می‌شود ماهیت خاص اتحادیه اروپا به عنوان بازیگر و کارگزاری در امنیت سایبری نادیده گرفته شود (یعنی دولت متعارف محسوب نمی‌شود). همچنین ن.ک.

Christou (2014) and Miriam Dunn Cavelty (2014)

این مسأله را مطرح می‌کنند که اتحادیه اروپا باید بر اساس رویکرد تاب‌آور و ارزش‌های خود به ساخت «قدرت نرم» آن توجه نماید.

۲. در موردی که حرکت از حکمرانی به فراحکمرانی در چارچوب مورد سوئیس (حفاظت از زیرساخت‌های اطلاعاتی حیاتی) پیشنهاد شده است، ن.ک.

Dunn Cavelty (2008b)

۳. در مورد تحلیل دقیق‌تر تأمین امنیت فضای مجازی در آمریکا، ن.ک.

Dunn Cavelty (2009)

۴. اگرچه رابطه بین امنیت و تاب‌آوری به طور گسترده‌تری در این ادبیات مورد تحلیل قرار گرفته است. ن.ک.

Dunn Cavelty and Prior (2013); Coaffee and Fussey (2015)

۵. اگرچه ادعا نمی‌کند که تا حد براسه و وون- ویلیامز[1] (۲۰۱۵) پیش رفته است که مفهوم «اکولوژی‌های اجرایی» را به منظور تأکید بر سیالیت و اصل رقابت گفتمان تاب‌آور و تأکید بر تأثیرات غیرمادی آن مطرح کردند.

۶. به عنوان «شکل غیرمستقیم حکمرانی از بالا به پایین که با تأثیرگذاری بر فرایندهای خود حکمرانی از طریق حالت‌های مختلف هماهنگی انجام می‌شود» تعریف شده است. (Shore et al. 2011, p.6)

۷. اثر دان کاولتی (۲۰۱۳) یک مورد استثنا محسوب می‌شود و به طور مستقیم به بحث در این کتاب مربوط است. به منظور تحلیل سیستم امنیت سایبری در حال توسعه اتحادیه اروپا، وی تاب‌آوری و قدرت سایبری را تبیین می‌کند. گرچه، این کار در قالب مقاله اولیه کوتاهی صورت می‌گیرد و وی تحلیل جامعی از راهبرد امنیت سایبری اتحادیه اروپا و سیاست‌ها و ابتکارات اتحادیه اروپا ارائه نمی‌دهد.

فصل ۳. امنیت سایبری در اکوسیستم جهانی

۱. توجه داشته باشید که در این فصل نمی‌توان تمام سازمان‌ها را پوشش داد و از این رو، بسیاری از ابتکارها/شبکه‌های غیررسمی (برای مثال، کارگروه مهندسی اینترنت، مؤسسه مهندسان برق و الکترونیک، بنیاد مرزهای الکترونیک، انجمن گروه‌های امنیتی و واکنش‌دهی به رویداد، مؤسسه روند مریدین، طرح اقدام لندن، گروه‌های دولتی واکنش سریع رایانه‌ای اروپا و غیره) و نهادهای رسمی فعال در زمینه امنیت سایبری حذف می‌شوند. برای مرور کلی نقش این سازمان‌ها، ن.ک. پارلمان اروپا (۲۰۱۱) و گزارش اتحادیه بین‌المللی مخابرات (۲۰۱۱). همچنین ن.ک.

1. Brassett and Vaughan-Williams

www.impact-alliance.org

در مورد مناطق جنوب جهان و آسیا نیز ن.ک.

Kshetri (2013) and Deibert et al (2012)

۲. استانداردهای فنی که توسط کارگروه مهندسی اینترنت مطرح شد.

۳. علاوه بر این مورد و با [برخورداری از] اهمیت در زمینه تاب‌آوری، ضمیمه‌های امنیتی سامانه نام دامنه به طور مستقیم به مسأله حفظ دسترس‌پذیری به نام‌های دامنه نمی‌پردازد (ن.ک. Sommer and Brown 2011, p.59–60).

۴. در مورد فهرست ثبت‌کنندگان پشتیبان ضمیمه‌های امنیتی سامانه نام دامنه، ن.ک.

https://www.icann.org/resources/pages/deployment-2012-02-25-en

۵. در مورد مرور جامع و تحلیل حیاتی انجمن حکمرانی اینترنت، ن.ک.

Malcolm (2008)

۶. امریه چارچوب ارتباطات الکترونیکی (۲۰۰۹)، تعهدات گزارش‌دهی ارائه‌دهندگان ارتباطات الکترونیکی را به ارائه‌دهندگان مخابرات و کنترل‌کننده‌های داده‌ها تحمیل کرده است، اما امریه امنیت شبکه و اطلاعات بیانگر تغییر قابل ملاحظه‌ای از نظر منطق حکمرانی برای تمام مالکان زیرساخت‌های حیاتی است.

۷. این زیرگروه شبکه تمام وقتی را برای تسهیل تحقیق درباره تروریست‌ها و سایر پرونده‌های جنایی مربوط به شواهد الکترونیکی بین کشورها تأسیس کرد. این زیرگروه نقاط تماس تخصصی پیشرفته‌ای را در کشورهای حاضر (حدود ۴۵ کشور) فراهم می‌کند که مبادله اطلاعات در مورد مجرمان اینترنتی را تسهیل می‌نمایند. ن.ک.

http://www.oas.org/juridico/english/cyb20_network_en.pdf

۸. ن.ک.

www.impact-alliance.org

۹. اتحادیه بین‌المللی مخابرات در سپتامبر ۲۰۱۲ گزارشی را نیز در زمینه فهم جرایم سایبری با عنوان «درک جرایم سایبری: پدیده، مشکلات و واکنش حقوقی» منتشر کرد. قابل.

دسترسی از:

http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

۱۰. مرکز هماهنگی مرکز ملی منابع اطلاعاتی جنایی نخستین سطح این مرکز محسوب می‌شود و مسئول هماهنگی اقدامات دفاع سایبری در داخل ناتو و بین ناتو و سازمان‌های بین‌المللی (یعنی اتحادیه اروپا، سازمان ملل/ اتحادیه بین‌المللی مخابرات، سازمان امنیت و همکاری اروپا و غیره) است

۱۱. سازمان همکاری اقتصادی و توسعه برای نخستین بار دستورالعمل‌هایی را در زمینه امنیت سیستم-های اطلاعاتی در سال ۱۹۹۲ مطرح کرد. علاوه بر این موارد و دستورالعمل‌های تجدیدنظرشده مطروحه در سال ۲۰۰۲، این سازمان توصیه‌های تکمیلی در مورد دستورالعمل¬های مربوط به جامعه اطلاعاتی از جمله حفظ حریم خصوصی (۱۹۸۰) و رمزنگاری (۱۹۹۷) را مطرح کرد.

۱۲. کشورهایی که در زمان نگارش این کتاب (مارس ۲۰۱۵) آن را تصویب نکردند عبارتند از: یونان، ایرلند، لوکزامبورگ و لهستان. سوئد آن را در سال ۲۰۱۴ تصویب کرد.

۱۳. ن.ک.

http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG

۱۴. در مورد تحلیل کنوانسیون و کاربرد آن در آمریکا، ن.ک.

Weber (2014)

۱۵. ن.ک. شورای اروپا:

http://www.coe.int/t/DGHL/cooperation/economycrime/cybercrime/default_en.asp

۱۶. برای بررسی گزینه‌های سیاست‌گذاری جهت رسیدگی به مسائل امنیت سایبری، ن.ک. سخنان رئیس امور ضدتروریستی در سازمان امنیت و همکاری اروپا (Perl 2010).

۱۷. کنفرانس سازمان امنیت و همکاری اروپا در خصوص «رویکردی جامع به امنیت سایبری: بررسی آینده نقش سازمان امنیت و همکاری اروپا»، وین، هافبورگ، مه ۲۰۱۱.

فصل ۴. رویکردهای ملی امنیت سایبری در اتحادیه اروپا؛ نمونه مطالعاتی بریتانیا

۱. این مورد مطابق با [مقررات] آژانس امنیت شبکه و اطلاعات اتحادیه اروپا است. ن.ک. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cybersecurity-strate gies-in-the-world

لازم به ذکر است که این امر بدین معنا نیست که کشورهای مندرج در این فهرست لزوماً از راهبرد برخوردار نیستند - برای مثال، قبرس راهبرد دارد، اما در تارنمای اینترنتی آژانس امنیت شبکه و اطلاعات اتحادیه اروپا نیست، چرا که متن آن باید به زبان انگلیسی ترجمه شود.

۲. سایر منابع احتمالی اطلاعات در مورد میزان آمادگی ملی کشورها مانند شاخص امنیت سایبری اتحادیه بین‌المللی مخابرات در زمان نگارش هیچ نتیجه‌ای برای اروپا ندارد. ن.ک. http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx ۳. با تشخیص آژانس امنیت شبکه و اطلاعات اتحادیه اروپا و در واقع، بر اساس گزارش کمیته امور اتحادیه اروپا در مجلس اعیان (۲۰۱۰، بند ۲۴).

۴. اولین نسخه آن در سال ۲۰۰۹ تحت عنوان «راهبرد بریتانیا: ایمنی، امنیت و تاب‌آوری در فضای سایبری» منتشر شد. همچنین لازم به ذکر است که دولت بریتانیا نیز پیش از این، راهبردهای امنیت اطلاعات ملی (۲۰۰۳، ۲۰۰۷) را مطرح کرده بود که مراحل و اقدامات اولیه اطمینان از صحت، دسترس‌پذیری و محرمانه بودن سیستم‌های فناوری اطلاعات و ارتباطات و اطلاعاتی که به آنها رسیدگی می‌کنند را مشخص می‌نماید.

۵. برای کسب اطلاعات بیشتر در مورد راهبرد جرایم سایبری، ن.ک.

Cyber Crime Strategy (2010)

۶. بارونس پائولین نویل- جونز[1] وزیر سابق امنیت و ضد تروریسم (۲۰۱۱-۲۰۱۰) است. او به عنوان نماینده ویژه دولت در امور تجاری در زمینه امنیت سایبری نیز خدمت کرده است.

۷. شایان ذکر است که گزارش مؤسسه چتم هاوس توسط کورنیش و دیگران (۲۰۱۱) در زمینه مرکز ائتلاف اطلاعات شبکه‌ای و امنیت سایبری و نه تمام ابعاد امنیت سایبری تهیه شد.

۸. دفتر امنیت سایبری و تضمین اطلاعات این برنامه را با مسئول دفتر کابینه مدیریت و هماهنگ می‌کند که مسئول امور نظارتی نیز است (The UK CSS: Landscape Review 2013, p.11).

۹. با دسترسی به منابع بیشتر به واسطه ادغام واحد جرایم رایانه‌ای کنونی مستقر در واحد خدمات پلیس کلان‌شهرها در واحد مرکزی جرایم سایبری پلیس.

۱۰. نیک هاپکینسون[2] قبلاً رئیس ستاد ارتباطات دولتی بریتانیا و گروه امنیتی ارتباطات الکترونیک بود.

۱۱. این کار با تخریب زیرساختی انجام می‌شود که جنایتکاران را قادر می‌سازد از بدافزار برای حمله به حساب‌های بانکی استفاده کنند. به خصوص، این امر مستلزم توقیف سرورهای رایانه‌ای است که در حکم سیستم فرمان و کنترل تروجان هستند و کنترل دامنه‌هایی را در اختیار دارند که شایلوک برای ارتباط بین رایانه‌های آلوده از آنها استفاده می‌کند.

۱۲. لازم به ذکر است که دسترسی سریع حتی در زمان انجام تحقیقات توسط پلیس همواره تضمین نمی‌شود. این موضوع تا حد زیادی بستگی به قانون مربوطه در هر کشور دارد.

۱۳. این مسئله در بودجه مصرفی آن مشاهده می‌شود که بیشترین مقدار صرف توسعه توانمندی مستقل ملی برای شناسایی و غلبه بر تهدیدهای جدی (۸/۲۵۳ میلیون پوند در سه سال نخست و ۲/۹۳ میلیون پوند در سال چهارم) گردید. برای کسب جزئیات بیشتر، ن.ک. «به روزرسانی برنامه ملی امنیت سایبری» (2014, p.7–8)

۱۴. کریس گیبسون[3] مدیر تیم واکنش اضطراری رایانه‌ای بریتانیا است.

۱۵. همچنین در زمینه پارادوکس ستاد ارتباطات دولتی بریتانیا از نظر محرمانه بودن و

1. Baroness Pauline Neville-Jones
2. Nick Hopkinson
3. Chris Gibson

اشتراک اطلاعات، ن.ک. هرینگتون و الدریچ [1](2012, p.301) . گزارش به روزرسانی شده دسامبر ۲۰۱۴ دفتر کابینه نشان می‌دهد که این سازوکارها با ستاد ارتباطات دولتی بریتانیا گسترش می‌یابند که هدف آن «اشتراک به موقع و مناسب اطلاعات در زمینه اقدامات دولت مخاصم و جرایم سایبری با کارکنان امنیتی در بخش ارائه-دهندگان خدمات ارتباطی» است (2014, p.13). گرچه، روشن نیست این موضوع تا چه حد مسأله گسترده‌تر اشتراک لحظه‌ای اطلاعات با تمام طرف‌های ذینفع مربوطه را رفع می‌کند.

۱۶. ن.ک. برنامه الزامات سایبری (۲۰۱۴). الزامات در این لینک قابل دسترسی است:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317481/Cyber_Essentials_Requirements.pdf

۱۷. برای توانمندسازی شرکت‌هایی که محصولات و خدمات امنیت سایبری را در اختیار دولت بریتانیا قرار می‌دهند به ارجاع علنی به این مورد و اعطای اعتبار بیشتر [به آنها] در زمان پیگیری امور تجاری (برای مثال، در خارج از کشور).

۱۸. در رابطه با این طرح نرم افزار معتبر، ن.ک.
http://www.uk-tsi.org/

۱۹. ن.ک.
http://www.enisa.europa.eu/activities/cert/background/inv/certs-bycountry-interactive-map

۲۰. گرچه نحوه تعبیر آن در عمل ممکن است آن را بی اهمیت سازد.

فصل ۵. اتحادیه اروپا و جرائم سایبری

۱. در اینجا به عنوان «طیف گسترده اقدامات جنایی مختلف در زمانی تعریف شده است که کامپیوترها و سیستم‌های اطلاعاتی، ابزار اصلی یا هدف اصلی محسوب می‌شوند» (EU cybersecurity strategy 2013, p.3). جرایم سایبری شامل حملات به سیستم‌های اطلاعاتی،

1 Herrington and Aldrich

جرایم مرتبط با محتوا مانند تحریک تنفر نژادی و جرایم سنتی مانند کلاهبرداری و سرقت هویت است.

۲. بات‌نت‌ها شبکه‌هایی از رایانه‌های آلوده‌شده توسط نرم‌افزارهای مخرب هستند که از راه دور برای انجام اقدامات خاصی از جمله حملات سایبری (مانند انکار حملات به سرویس‌ها یا اسپم) فعال می‌شوند.

۳. در زمان نگارش این کتاب پیش‌بینی می‌شود که بسیاری از این اقدامات کماکان در ساختار تصمیم‌گیری اتحادیه اروپا مورد بحث باشند، از این رو، ارزیابی کامل تمام دستورالعمل‌ها/اقدامات پیشنهادی ممکن نیست.

۴. برای تسهیل اجرای این مورد، طرح استانداردسازی امضای الکترونیکی اروپا نیز راه‌اندازی شد.

۵. مسلماً اقدامات قانونی در بخش‌های سیاست‌گذاری مختلف برای حفاظت از حریم خصوصی، داده‌ها، اطلاعات مخابراتی و امنیت خدمات (ماده‌های ۴ و ۵) در چهارچوب خدمات مخابراتی اتحادیه اروپا وجود دارند که چندین مقررات را برای «امنیت مقررات شبکه» و «یکپارچگی شبکه» مطرح می‌کنند (بازگویی در چارچوب نظارتی خدمات ارتباطات الکترونیکی در سال ۲۰۰۲).

۶. با تعهد به معرفی قوانین تا سال ۲۰۰۷.

۷. به خصوص در مورد ارتباطات آن «با سیاست کلی در زمینه مقابله با جرایم سایبری» بیشتر توضیح داده شد (European Commission 2007).

۸. مجمع نوآوری پژوهشی امنیت اتحادیه اروپا[1] در سال ۲۰۰۹ در مورد چگونگی ارتباط بین بخش‌های عمومی- خصوصی از نظر امنیت کلی اروپا (از جمله امنیت سایبری و جرایم) راه‌اندازی و [کارهای آن] گزارش شد. ن.ک. گزارش نهایی مجمع نوآوری پژوهشی امنیت اتحادیه اروپا (۲۰۰۹).

۹ این مورد بر اساس امریه سال ۱۹۹۵ حفاظت از داده‌ها (European Parliament

1. European Security Research Innovation Forum

and Council 95/46/EC) و امریه سال ۲۰۰۲ در زمینه حفظ حریم خصوصی و ارتباطات الکترونیکی (European Parliament and Council 2002/58/EC) (اصلاح شده با امریه EC/2009/136) است.

۱۰. برای مثال، ن.ک.

http://www.edri.org/files/dr_letter_260911.pdf

۱۱. گرچه، برای پیشنهادها در مورد تطبیق حفاظت از حریم خصوصی/داده‌ها و امنیت از طریق رویکرد فنی به جای امنیت ملی، ن.ک.

Porcedda (2012)

+ ۱۲. ن.ک.

Drewer and Ellermann (2012)

۱۳. جایگزین امریه ۱۹۹۵/۹۵/۴۶ EC (European Parliament and Council).

۱۴. جایگزین تصمیم چارچوبی JHA (Council of the European Union/2008/977 2008).

۱۵. در زمان نگارش این کتاب (مارس ۲۰۱۵)، کماکان در شورای وزیران مورد بحث و مذاکره است - ن.ک. فصل ۷.

۱۶. پورسدا (p.63–64 ,2012) نیز این مورد را در مسائل مربوط به محاسبات ابری مطرح می‌کند.

۱۷. تصمیم چارچوبی JHA/۲۰۰۴/۶۸ در مورد مقابله با سوءاستفاده جنسی، بهره‌برداری جنسی از کودکان و پورنوگرافی کودکان (Council of the European Union 2004) و در مجموع، قبل از این مورد برای تعیین حقوق قربانیان جرایم، تصمیم چارچوبی JHA/۲۰۰۱/۲۲۰ در مورد جایگاه قربانیان در دادرسی جزایی (Council of the European Union 2001). مورد دوم نیز به روزرسانی شده و امریه EU/۲۰۱۲/۲۹ جایگزین آن گردید که حداقل استانداردها در زمینه حقوق، حمایت و حفاظت از قربانیان جرایم را تعیین می‌کند (European Parliament and the Council 2012).

۱۸. برنامه اینترنت امن‌تر در سال ۱۹۹۹ راه‌اندازی شد. ن.ک.

http://ec.europa.eu/information_society/activities/sip/policy/index_en.htm

۱۹. ائتلاف مالی اتحادیه اروپا قصد دارد با تولید، توزیع و فروش تصاویر پورنوگرافی کودکان در اینترنت مقابله کند. ن.ک.:

http://www.europeanfinancialcoalition.eu/document.php

۲۰. گرچه برخی کشورها پیشرفته‌تر از کشورهای دیگر هستند (ن.ک. فصل ۴). طرح‌هایی در سطح اروپا مانند ماه [مقابله با] جرایم سایبری اروپا –با پشتیبانی آژانس امنیت شبکه و اطلاعات اتحادیه اروپا و اداره کل شبکه‌های ارتباطات، محتوا و فناوری– راه‌اندازی شده‌اند که این طرح در اکتبر هر سال با هدف ترویج آگاهی امنیت سایبری و آموزش شهروندان صورت می‌گیرد.

۲۱. گزارش کمیسیون به شورا بر اساس ماده ۱۲ تصمیم‌گیری ساختاری شورا در ۲۴ فوریه در مورد حملات به سیستم‌های اطلاعاتی، 448(2008)COM (European Commission 2008).

۲۲. تصمیم‌گیری ساختاری شورا

222/2005/JHA (Council of the European Union 2005).

۲۳. این در حالی است که این راهبرد در فوریه ۲۰۱۳ منتشر گردید و مهم‌ترین دستورالعمل همراه آن در مورد امنیت شبکه و اطلاعات کماکان در فرایند تصمیم‌گیری اتحادیه اروپا در زمان نگارش این کتاب (مارس ۲۰۱۵) است.

۲۴. در واقع، برخی از مفاهیم و تعاریف اصلی کنوانسیون به منظور لحاظ این مورد در قانون اتحادیه اروپا و تعریف حداقل تحریم‌ها برای تخلفات جرایم سایبری تعریف شده، در تصمیم‌گیری ساختاری اتحادیه اروپا در زمینه حملات به سیستم‌های اطلاعاتی (222/2005/JHA) گنجانده شده است (Council of the European Union 2005).

۲۵. کشورهایی که در زمان نگارش این کتاب (مارس ۲۰۱۵) آن را تصویب نکردند عبارتند از یونان، ایرلند، لوکزامبورگ و لهستان. سوئد در سال ۲۰۱۴ آن را تصویب کرد.

۲۶. ترویج همکاری از طریق طرح‌هایی نظیر تیم واکنش اضطراری رایانه‌ای اروپا (http://www.egc.org) و ابتکارهایی نظیر «ترِنا» (http://www.terena.org/tf-csirt) و انجمن گروه‌های امنیتی و واکنش‌دهی به رویداد (http://www.first.org).

۲۷. گزارش آژانس امنیت شبکه و اطلاعات اتحادیه اروپا در زمینه تیم‌های دولتی یا ملی واکنش اضطراری رایانه‌ای، یعنی گروه‌هایی که به عنوان نقطه تماس ملی برای همکاری و اشتراک اطلاعات با دیگر تیم‌های ملی واکنش اضطراری رایانه‌ای در اتحادیه اروپا یا گروه‌های مسئول حفاظت از شبکه‌های مدیریت دولتی عمل می‌کنند (ENISA, Flair for Sharing ,2011 ,20.p).

۲۸. برای مثال، مراکز ملی امنیت سایبری، سایر تیم‌های واکنش اضطراری رایانه‌ای (داخلی، اتحادیه اروپا و خارج از اتحادیه اروپا)، سازمان‌های اطلاعاتی، نهادهای مجری قانون غیراروپایی، بخش خصوصی و هر نهاد بین‌المللی مربوطه (مانند اینترپل).

۲۹. آژانس امنیت شبکه و اطلاعات اتحادیه اروپا گزارش داد (ENISA, Give and Take ,2012 ,41.p) که حداقل دو کشور مواردی را مطرح کرده‌اند که در آن اقدام تیم واکنش اضطراری رایانه‌ای موجب شد آنها از طریق قوانین حفاظت از اطلاعات مسئولیت‌پذیر شوند. این نکته در مورد انواع مختلف تیم‌های واکنش اضطراری رایانه‌ای اهمیت می‌یابد، چرا که تمام آنها از مجوز مشخصی بر اساس قانون اولیه اشتراک و پردازش داده‌ها برخوردار نیستند.

۳۰. تمام این موارد را نمی‌توان در این فصل پوشش داد (برای مثال، مسائل مهمی مانند کسب شواهد و توانمندی قانونی سایبری مطرح نشده‌اند). برای تحلیل دقیق‌تر تمام مسائل، ن.ک.

http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime

۳۱. نمونه اقدام مناسبی که در مجموع می‌تواند گسترش و توسعه یابد، رویکرد یکپارچه اتخاذشده در بازی‌های المپیک لندن به امنیت سایبری است (Interview, former UK cybercrime law enforcement official, July 2014).

۳۲. مسأله‌ای که راب وین رایت، رئیس یوروپل، در اظهارات خود در مجلس اعیان بریتانیا در زمینه برنامه بعدی وزارت کشور و دادگستری بر آن تأکید کرد (House of Lords, EU committee, 13th Report of Session 2013–2014, p.17).

۳۳. در واقع، او خواستار ایجاد انسجام سیاست‌گذاری بیشتر در سیاست‌های امنیت سایبری اتحادیه اروپا گردید. . کانون‌های اصلی، گروه‌هایی در بخش عملیات‌های یوروپول هستند که به رده خاصی از جرایم و شبکه‌های جنایی توجه دارند. در حال حاضر عملیات در سه گروه کانونی انجام می‌شود: سایبورگ (جرایم پیشرفته و بدافزارها)، دوقلوها (بهره‌برداری جنسی آنلاین از کودکان) و ترمینال (کلاه‌برداری در پرداخت).

فصل ۶. امنیت شبکه و اطلاعات و دفاع سایبری در اتحادیه اروپا

۱. توجه اتحادیه اروپا بر حفاظت از خود (دفاع) است، چرا که از توانمندی‌های نظامی مستقلی فراتر از موارد ارائه شده توسط کشورهای عضو برخوردار نیست. این امر برخلاف مورد آمریکا است که در سالیان اخیر به توسعه توانمندی‌های تهاجمی سایبری خود توجه داشته است.

۲. هدف از این ارتباط، احیا و تقویت سند راهبرد اصلی سال ۲۰۰۱ کمیسیون اروپا تحت عنوان «امنیت شبکه و اطلاعات: پیشنهادی برای رویکرد سیاست‌گذاری اروپا» است.

۳. نتایج شورا در مورد «پیشگیری، میزان آمادگی و واکنش به حملات تروریستی» و «برنامه همبستگی اتحادیه اروپا در مورد پیامدهای تهدیدات و حملات تروریستی» که در دسامبر ۲۰۰۴ توسط شورا تصویب شد، از قصد کمیسیون برای پیشنهاد برنامه اروپا برای حفاظت از زیرساخت‌های حیاتی و شبکه اطلاعاتی هشدار در مورد زیرساخت‌های حیاتی حمایت می‌کند (Communication, EPCIP 2006).

۴. پس از بررسی جامع برنامه اروپا برای حفاظت از زیرساخت‌های حیاتی و امریه شورا۲۰۰۸/۱۱۴/EC ، کمیسیون اروپا (2013c) رویکرد جدیدی را برای اجرای عملی برنامه اروپا برای حفاظت از زیرساخت‌های حیاتی از طریق سه جریان کاری آن –پیشگیری، میزان آمادگی و واکنش– مطرح کرد. چنین رویکرد جدیدی به خصوص به دنبال توجه و رسیدگی به

مسأله وابستگی متقابل بین صنعت زیرساخت‌های حیاتی و بازیگران دولتی بود.

۵. این دستورالعمل از دستورالعمل‌های مدیریت ریسک عمومی («برنامه‌های امنیتی اپراتور»)، افسران رابط امنیتی و گزارش‌دهی اجباری و نیز تبادل اطلاعات حساس در میان مقامات مجری قانون حمایت می‌کرد. .

۶. همچنین ن.ک. قطعنامه پارلمان اروپا (۲۰۱۲) که مؤید ارتباطات کمیسیون است و توصیه‌های بیشتری را نیز ارائه می‌دهد که در راهبرد امنیت سایبری اتحادیه اروپا (۲۰۱۳) و امریه امنیت شبکه و اطلاعات پیشنهادی تأیید شدند (European Commission 2013a).

۷. برای ارزیابی فعالیت به‌روزرسانی‌شده تیم‌های واکنش اضطراری رایانه‌ای، ن.ک. آژانس امنیت شبکه و اطلاعات اتحادیه اروپا:

http://www.enisa.europa.eu/activities/cert

۸. این مورد به طور کامل در سپتامبر ۲۰۱۲، پس از یک دوره آزمایشی یک ساله ایجاد شد و در تمام نهادها، سازمان‌ها و مؤسسات اتحادیه اروپا به کار می‌رود. ن.ک.

http://cert.europa.eu/cert/plainedition/en/cert_about.html

۹. در مطالعه امکان‌سنجی انجام شده برای این مورد توسط آژانس امنیت شبکه و اطلاعات اتحادیه اروپا این نتیجه به دست آمد که «مؤثرترین سطح مشارکت برای اتحادیه اروپا در ایجاد و بهره‌برداری از سیستم اشتراک اطلاعات برای کاربران خانگی و شرکتهای کوچک و متوسط آن، سطح مشارکت تسهیل‌کننده، ناظر مبحث و «نگهبان اقدام مناسب»» است. روند پیشرفت تکامل و اجرای واقعی آن به دلیل وجود دیدگاه‌های مختلف افراد ذینفع در مورد ماهیت این امر کند است. برای جزئیات ن.ک.:

http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder

۱۰. فرانسه، آلمان، مجارستان، ایتالیا، هلند، سوئد و بریتانیا.

۱۱. مشارکت خصوصی-عمومی امنیت تاب‌آور اتحادیه اروپا از طریق سند غیررسمی ایجاد شد که هدف آن تعیین اهداف مشارکت خصوصی-عمومی، هدف و ساختار آن بود: ن.ک. http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/ep3r/index_en.ht.

۱۲. توجه داشته باشید که این موضوع بدین معنی نیست که مشارکت خصوصی- عمومی اتحادیه اروپا در زمینه امنیت تاب‌آور زائد بود. برای مثال، کار بر روی بات‌نت‌ها آموزنده بود و آژانس امنیت شبکه و اطلاعات اتحادیه اروپا در حال بررسی دوم مشارکت خصوصی- عمومی اتحادیه اروپا در زمینه امنیت تاب‌آور برای اطمینان از سودمندی کلی و تجربیات آموخته شده است.

۱۳. برای مثال، حوزه دارای اولویت توسعه منابع صنعتی و فناورانه برای امنیت سایبری/ترویج بازار واحد برای محصولات امنیت سایبری است.

۱۴. سه کارگروه اصلی وجود دارد: کارگروه (۱) در زمینه مدیریت خطرات؛ کارگروه (۲) در زمینه اشتراک اطلاعات/هماهنگی رویدادها و کارگروه (۳) در زمینه تحقیقات و نوآوری‌های امن فناوری اطلاعات و ارتباطات. نویسنده این کتاب عضو کارگروه ۳ بود.

۱۵. مانور سوم برای سال ۲۰۱۴ برنامه‌ریزی شده بود. به رغم انجام جنبه فنی این مانور در آوریل ۲۰۱۴ (مرحله ۱)، هیچ اطلاعاتی در مورد مراحل عملیاتی/تاکتیکی و راهبردی/سیاسی در دسترس عموم نیست. قرار بود این اطلاعات در نیمه دوم سال ۲۰۱۴، در دسترس عموم قرار گیرند. اهداف «اروپای سایبری ۲۰۱۴» عبارتند از: آزمون رویه‌های همکاری استاندارد و سازوکارهای موجود برای مدیریت بحران‌های سایبری در اروپا؛ افزایش توانمندی‌های ملی؛ بررسی همکاری‌های موجود بین بخش‌های خصوصی و دولتی؛ تحلیل فرایندهای تشدید بحران و تشنج‌زدایی (سطوح فنی، عملیاتی و راهبردی)؛ درک مسائل مربوط به امور دولتی مرتبط با حملات سایبری گسترده. ن.ک.:

http://www.enisa.europa.eu/media/press-releases/biggest-eucyber-security-exercise-to-date-cyber-europe-2014-taking-place-today

۱۶. برای مثال، راهنمای اقدام مناسب آژانس امنیت شبکه و اطلاعات اتحادیه اروپا در زمینه مانورهای ملی (۲۰۱۰).

۱۷. بر اساس گزارش آژانس امنیت شبکه و اطلاعات اتحادیه اروپا، «شرکت‌کنندگان از ۳۰ کشور (اتحادیه اروپا و انجمن تجارت آزاد اروپا) در طرح اروپای سایبری ۲۰۱۰ حضور داشتند؛

۲۲ کشور فعال بودند، اما هشت کشور به عنوان ناظر حضور داشته و به رویدادها و یافته‌های مربوط به مانور دسترسی داشتند. سازمان مرکزی کنترل مانور تحت عنوان کنترل مانور در آتن مستقر بود که وظیفه ارائه جهت‌گیری و راهنمایی‌های [لازم] برای اجرای این مانور را برعهده داشت. این سازمان شامل ناظرانی از میان کارکنان نظامی، یک نماینده از هر کشور شرکت‌کننده و مدیران این سازمان، آژانس امنیت شبکه و اطلاعات اتحادیه اروپا و مرکز تحقیقات مشترک کمیسیون اروپا بود که کنترل کلی این مانور را برعهده داشت» (ENISA, 2011a, p.6).

۱۸. کمیسیون از شمول دولت‌های دموکراتیکی مانند هند و برزیل در چنین ساختارهایی برای بهبود شفافیت و نمایندگی (ن.ک. فصل ۷) حمایت بیشتری نیز نموده است.

۱۹. ارزیابی تأثیر، انجام شد که در کنار رویکرد نظارتی اتخاذی این موارد را در نظر گرفت: ۱. حفظ وضعیت موجود از طریق رویکرد بازاری/داوطلبانه؛ ۲. رویکرد ترکیبی شامل رویکرد داوطلبانه برای کشورهای عضو با هدف بهبود توانمندی آنها و الزامات قانونی بیشتر برای بازیگران خصوصی و بخش‌های مدیریت دولتی (European Commission 2013b).

۲۰. دولت بریتانیا نیز به شدت خواستار حذف «فعال‌کنندگان اینترنت» از این دستورالعمل است.

۲۱. تمام کشورهای عضو حضور ندارند؛ بعضی از آنها در این حوزه همکاری نمی‌کنند (دانمارک)، بعضی از آنها با کمبود منابع مواجه هستند (مالت) و کشورهای دیگر به واسطه انتخاب خود حضور ندارند، چرا که معتقدند این امر در حوزه صلاحیت ملی و نه اروپا است (بریتانیا) (Interview, EDA official, September 2014).

۲۲. لازم به ذکر است که نسخه‌های محرمانه و غیرمحرمانه این گزارش وجود دارد. یافته‌های گزارش‌شده در اینجا برگرفته از گزارش غیرمحرمانه‌ای بوده که در دسترس عموم است. در گزارش محرمانه جزئیات بسیار بیشتر و تحلیل دقیقی از توانمندی دفاع سایبری اتحادیه اروپا و کارکنان نظامی این اتحادیه ذکر شده است.

۲۳. برگرفته از چارچوب نظامی معمولاً درک شده از شرکت‌کنندگان در توانمندی دفاعی معروف به خطوط توسعه دفاع (Robinson et al. 2013).

۲۴. همچنین طرح دامنه‌های سایبری که طرح آزمایشی برای آموزش و صدور گواهینامه برای دانشجویان نظامی در بخش جرم‌شناسی دیجیتال بود؛ برنامه آزمایشی با همکاری پرتغال و استونی در زمینه تصمیم‌گیری راهبردی سایبری مطرح شد و برنامه‌های موردی گوناگون دیگری نیز برای مثال، یکی در زمینه توسعه آگاهی بر حسب موقعیت برای ارائه برنامه‌ریزی دفاع سایبری استاندارد و سیستم مدیریت و دیگری برای شناسایی تهدید همیشگی پیشرفته وجود دارند.

۲۵. برای مثال، با ایجاد فرایندها و مکانیسم‌هایی برای ادغام اطلاعات مربوط به تهدید سایبری در عملیات‌های نظامی (برای این مورد، ن.ک. Roehrig 2014).

۲۶. طرح‌های دفاع هوشمند در دفاع سایبری تاکنون شامل برنامه اشتراک اطلاعات بدافزار، طرح توسعه توانمندی دفاع سایبری چندملیتی دفاع هوشمند و طرح آموزش و تعلیم دفاع سایبری چندملیتی است (ن.ک. ناتو (۲۰۱۴) http://www.nato.int/cps/en/natohq/topics_78170.htm).

فصل ۷. همکاری فراآتلانتیک در امنیت سایبری؛ همگرایی در امنیت تاب‌آور؟

۱. آیکان شرکت خصوصی و غیرانتفاعی آمریکایی است که وظایف نهاد شماره‌های اختصاصی اینترنت (آیانا) را انجام می‌دهد که از طریق آن، استانداردهایی را برای به کارگیری و حفاظت از اسامی در فضای سایبری ایجاد می‌کند.

۲. ن.ک.

https://ec.europa.eu/digital-agenda/en/global-internet-policy-observatorygipo

۳. برای دیدگاه روشنگرانه در مورد تأثیر اولیه، پیشنهادات دولت اوباما در زمینه امنیت سایبری، ن.ک. هاتاوی (۲۰۱۱).

۴. همچنین ن.ک. تحقیق ویژه انجام شده توسط آژانس امنیت شبکه و اطلاعات اتحادیه اروپا در زمینه زیرساخت‌های حیاتی:

https://www.enisa.europa.eu/activities/ResilienceandCIIPcriticalinfrastructureand- services

۵. این رویکرد داوطلبانه در قانون افزایش امنیت سایبری (S.۱۳۵۳) لحاظ گردید که توسط مجلس سنا در ۱۱ دسامبر ۲۰۱۴ تصویب و در ۱۸ دسامبر ۲۰۱۴ به قانون عمومی مبدل شد (۲۷۴-۱۱۳). ن.ک.

https://www.govtrack.us/congress/bills/113/s1353

۶. مسلماً اتحادیه اروپا پیش از اسنودن نیز راهبرد افزایش به کارگیری از ابر در اروپا را در نظر گرفته بود که در اصل تحت تأثیر بازار واحد، منطق اقتصادی قرار داشت، ن.ک. راهبرد اروپا برای محاسبات ابری – به‌کارگیری قدرت محاسبات ابری در اروپا (۲۰۱۲). همچنین ن.ک.

http://www.enisa.europa.eu/activities/Resilienceand-CIIP/cloud-computing

۷. اروپاییان غیرمقیم امریکا تحت قانون سال ۱۹۷۴ حفظ حریم خصوصی امریکا نیستند. ن.ک.

http://europa.eu/rapid/press-release_MEMO1059-13-_en.htm

۸. درباره نحوه برخورد مورد اصلاح حفاظت از داده‌های اتحادیه اروپا با مسأله نگرانی پیرامون موارد جاسوسی ن.ک.

http://europa.eu/rapid/press-release_MEMO1059-13-_en.htm

۹. برای دسترسی به متن مقررات حفاظت از اطلاعات عمومی مورد تصویب پارلمان اروپا ن.ک.

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//

EPTEXT+TA+P+-7 ۱۰. به عبارت دقیق‌تر، بریتانیا طرح پیش‌نویس لایحه ارتباطات داده‌ها (با عنوان منشور اسنوپرس مورد نظر بسیاری از گروه‌های حقوق بشر در بریتانیا) را بازسازی کرد. این طرح به عنوان قانون حفظ داده‌ها و اختیارات تحقیقاتی بازتولید شد و در تاریخ ۱۷ جولای ۲۰۱۴ به قانون تبدیل شد. ن.ک.

https://www.liberty-human-rights.org.uk/campaigning/no-snoopers-charter

۱۱. در ابتدا کار خود را با حضور ۴۸ کشور آغاز کرد.

۱۲. برای مثال، ن.ک.

Ashford (2015)

منابع

• ACPO e-crime Strategy (2009), Association of Chief Police Officers of England, Wales and Northern Ireland. Available at: http://www.acpo.police.uk/documents/crime/200908/2009CRIECS01.pdf (accessed October 2014).

• 'A Global Alliance Against Child Sexual Abuse Online' (2015), Available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/index_en.htm (accessed February 2015).

• Albrecht, P. J. (2015), 'EU General Data Protection Regulation: State of Play and 10 Main Issues', LIBE, The Greens in the European Parliament, 7 January 2015.

• Alden, E. (2014), 'How Obama's NSA Reforms Could Help TTIP', Council on Foreign Relations, 15 January 2014.

• Ashford, W. (2015), 'China and US Cross Swords Over Software Backdoors', Computerweekly.com, 5 March 2015. Available at: http://www.computerweekly.com/news/2240241750/China-and-US-cross-swords-over-software-backdoors?asrc=EM_EDA_40356910&utm_medium=EM&utm_source=EDA&utm_campaign=20150305_China20%and20%US20%cross20%swords20%over20%software20%backdoors_ (accessed March 2015).

• Aspects of Identity Yearbook 2011) 2012–2011), BCS: The Chartered Institute for IT, Identity Assurance Working Group.

• Bada, M., Creese, S., Goldsmith, M., Mitchel, C. and Phillips, E. (2014), 'Computer Emergency Response Teams (CERTs): An Overview', Global Cyber Security Capacity Centre. Available at: http://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CERTs20%An20%Overview20%.pdf (accessed December 2014).

• Bendiek, A. (2014), 'Tests of Partnership: Transatlantic Cooperation in Cyber Security, Internet Governance and Data Protection', Stiftung Wissenschaft und Politik (SWP), SWP Research Paper, Berlin, March 2014.

• Bendrath, R., Eriksson, J. and Giacomello G. (2007), 'Cyberterrorism to Cyberwar, Back and Forth: How the United States Securitized Cyberspace', in Eriksson, J. and Giacomello G. (eds.)

International Relations and Security in the Digital Age, London, Routledge, pp.82–57.
• Bendrath, R., Eriksson, J. and Giacomello, G. (2010), 'From «cyberterrorism» to «cyberwar», Back and Forth: How the United States Securitized Cyberspace', in Eriksson, J. and Giacomello, G. (eds.) International Relations and Security in the Digital Age, London and New York: Routledge.
• Benkler, Y. (1998), 'The Commons as a Neglected Factor of Information Policy'. Available at: www.benkler.org/commons.pdf (accessed June 2013).
• Benkler, Y. (2007), 'The Battle over the Institutional Ecology of the Digital Environment'. Available at: http://cyber.law.harvard.edu/wealth_of_networks/11._The_Battle_Over_the_Institutional_Ecology_of_the_Digital_Environment (accessed March 2015).
• Bersick, S., Christou, C. and Yi, S. (forthcoming 2015), 'Cyber Security and EUChina Relations', in Kirchner, Emil, Christiansen, Thomas and Dorussen, Han (eds.) Security Relations between China and the European Union: From Convergence to Cooperation? Cambridge: Cambridge University Press.
• Betz, D. and Stevens, T. (2011), Cyberspace and the State: Towards a Strategy for Cyber-Power, The International Institute for Strategic Studies, Oxon: Routledge.
• Bigo, D., Carrera, S., Hernanz, N., Jeandesboz, J., Ragazzi, F. and Scherrer, A. (2013), National Programmes for Mass Surveillance of Personal Data in EU Member States and their compatibility with EU Law, Directorate General for Internal Policies, Policy Department C: Citizen's Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs, European Parliament.
• Boehm, F. and Cole, D. M. (2014), 'Data Retention After the Judgement of the European Court of Justice of the EU', The Greens/European Free Alliance, 30 June 2014. Available at: http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_June_2014.pdf (accessed February 2015).
• Bowden, C., Bigo, D. and Scherrer, A. (2013) The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens' fundamental rights, Directorate General for Internal Policies, Policy Department C: Citizen's Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs, European Parliament.
• Boyden, S. (1987), Western Civilization in Biological Perspective: Patterns in Biohistory, Oxford: Clarendon.
• Brand, F. S. and Jax, K. (2007), Focusing the meaning(s) of resilience: Resilience as a descriptive concept and a boundary object. Ecology and Society, 23 :(1)12. [online] Available at: http://www.ecologyandsociety.org/vol12/
• Brassett, J. and Vaughan-Williams, N. (2015), 'Security and the Performative Politics of Resilience: Critical Infrastructure Protection and Humanitarian Emergency Preparedness', Security Dialogue, 50–32 ,(1)46.
• Brewster, T. (2014), 'UK Forges Closer Cyber Ties with China Despite «endemic espionage» ', The Guardian, Secure + Protect, 18 June 2014.
• Brown, I. and Marsden, C. T. (2007), 'Co-regulating Internet Security: The London Action Plan', http://essex.academia.edu/ChrisMarsden/Papers/700007/Co-regulating_Internet_security_the_London_Action_Plan (accessed October 2012).
• Bygrave, A. L. (2013), 'Transatlantic Tensions on Data Privacy', Transworld, Working Paper 19, April

2013.
• Castells, M. (1996), The Information Age: Economy, Society and Culture, vol.1: The Rise of the Network Society, Malden, MA: Blackwell.
• Castells, M. (1997), The Information Age: Economy, Society and Culture, vol.2: The Power of Identity, Malden, MA: Blackwell.
• Castells, M. (1998), The Information Age: Economy, Society and Culture, vol.3: End of Millennium, Malden, MA: Blackwell.
• Chan, C. (2013), 'Leaked Documents Detail the Cyber Operations of US Spy Agencies'. Available at: http://gizmodo.com/leaked-documents-detail-the-cyber-operations-of-us-spy1230265977- (accessed January 2015).
• Chmutina, K., Bosher, L., Coaffee, J. and Rowlands, R. (2014), 'Towards Integrated Security and Resilience Framework: A Tool for Decision-Makers', Procedia Economics and Finance, 2014/12, DOI: 10.1016/S5-00909(14)5671-2212.
• Christou, G. (2014), 'The EU's Approach to Cyber Security,' EU-China Security Cooperation: Performance and Prospects Project, Jean Monnet Multilateral Research Group'. Available at: http://privatewww.essex.ac.uk/susyd/EUSC/publications.htm (accessed January 2015).
• Christou, G. and Croft, S. (2012), European Security Governance, Oxon: Routledge.
• Christou, G., Croft, S., Ceccorulli, M. and Lucarelli, S. (2010), 'European Union Security Governance: Putting the Security back In', European Security, Special Issue, 3) 19), September 361–341 ,2010.
• Christou, G. and Simpson, S. (2012), 'The Influence of Global Internet Institutions on the EU', in Costa, O. and Jørgensen, K. E. (eds.) The Influence of International Institutions on the European Union, Houndmills, Basingstoke: Palgrave MacMillan.
• Christou, G. and Simpson, S. (2011), 'The European Union, Multilateralism and the Global Governance of the Internet', Journal of European Public Policy, 257–241 ,(2)18.
• Christou, G. and Simpson, S. (2007), The New Electronic Marketplace: European Governance Strategies in a Globalising Economy, London: Edward Elgar. China and Russia's 'International Code of Conduct for Information Security', Available at: http://news.dot-nxt.com/13/09/2011/china-russia-security-code-of-conduct (accessed October 2013).
• Cirlig, C. C. (2014), 'Cyber Defence in the EU: Preparing for Cyber Warfare?', European Parliamentary Research Service, European Parliament Briefing, October 2014.
• Clarke, A. R. and Knake, R. K. (2010), Cyber War: The Threat to National Security and What to Do About It, New York: Harper Collins.
• Clarke, A. R. et al. (2013), 'Liberty and Security in a Changing World', Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, The Whitehouse, 12 December 2013. Available at: http://www.whitehouse.gov/sites/default/files/docs/12-12-2013_rg_final_report.pdf (accessed February 2015).
• Coaffee, J. and Fussey, P. (2015), 'Constructing Resilience Through Security and Surveillance: The Politics, Practices and Tensions of Security-Driven Resilience', Security Dialogue, 14–3 ,(1)46.
• Colarik, A. M. (2006), Cyber Terrorism: Political and Economic Implications, IGI Publishing.
•Comfort, K. L., Boin, A. and Demchak, C. C. (eds.) (2010), Designing Resilience: Preparing for Extreme Events, Pittsburgh: University of Pittsburgh Press.

• Cornish, P., Livingstone, D., Clemente, D. and York, C. (2011), 'Cyber Security and the UK's Critical National Infrastructure', A Chatham House Report, Chatham House, September 2011.
• Council of the European Union (2011), 'Council Conclusions on Critical National Infrastructure Protection – 'Achievements and Next Steps: Towards Global Cyber-Security', 3093rd Transport, Telecommunications and Energy Council Meeting, Brussels, 27 May 2011.
• Council of the European Union (2008a), 'Council Directive on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection', Council Directive 114/2008/EC, 8 December 2008.
• Council of the European Union (2008b), Council Framework Decision 977/2008/JHA of 27 November 2008 on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matter.
• Council of the European Union (2005), Council Framework Decision 222/2005/JHA of 24 February 2005 on Attacks Against Information Systems.
• Council of the European Union (2004), Council Framework Decision 68/2004/JHA of 22 December 2003 on Combating the Sexual Exploitation of Children and Child Pornography.
• Council of the European Union (220/2001 ,(2001/JHA: Council Framework Decision of 15 March 2001 on the Standing of Victims in Criminal Proceedings.
• Cybercrime@IPA project of the Council of Europe and the European Union (2011), 'Specialised Cybercrime Units: Good Practice Study', Version 9 November 2011. Available at: www.coe.int/cybercrime (accessed May 2014).
• 'Cyber Crime Strategy' (2010), Home Office, CM7842, March 2010. Cyber Defence Fact Sheet (2013), 'European Defence Agency'. Available at: http://www.eda.europa.eu (accessed August 2014).
• 'Cyber Essentials Scheme: Requirements for Basic Technical Protection Against Cyber Attacks' (2014), 'HM Government', June 2014. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317481/Cyber_Essentials_Requirements.pdf (accessed October 2014).
• Cyber Security Building Resilience, Reducing Risks (2014), Chatham House, The Home of the Royal Institute of International Affairs, Conference, 20–19 May 2014.
• 'Cybersecurity Strategy of the EU: An Open, Safe and Secure Cyberspace' (2013), Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, 7 February 2013, JOIN (1 (2013 final.
• 'Cyber Security Strategy of the UK: Safety, Security and Resilience in Cyberspace' (2009), Office of Cyber Security and UK Cyber Security Operations Centre, June 2009.
• Deauville Declaration (2011). Available at: http://www.g8.utoronto.ca/summit/2011deauville/-2011 declaration-en.html (accessed March 2015).
• De Bruijne, M., Boin, A. and van Eeten, M. (2010), 'Resilience: Exploring the Concept and Its Meanings', in Comfort, L., Boin, A. and Demchal, C. (eds.) Designing for Resilience: Preparing for Extreme Events, Pittsburgh: Pittsburgh University Press.
• Defence Cyber Protection Partnership (2015), Available at: https://www.adsgroup.org.uk/pages/65757387.asp.
• Deibert, R. J., Rohozinski, R. and Crete-Nishihita, M. (2012), 'Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War', Security Dialogue, 24–3 ,(1)43.
• Deibert, R. J., Palfrey, J. G., Rohozinski, R. and Zittrain, J. (eds.) (2011), Access Contested: Security,

Identity and Resistance in Asian Cyberspace, Cambridge: MIT Press.
• DG Home Affairs (2013), Available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/child-sexual-abuse/index_en.htm (accessed March 2013).
• Di Camillo, F. and Miranda, V. (2011), 'Ambiguous Definitions in the Cyber Domain: Costs, Risks, and the Way Forward', IAI Working Papers 1126, September 2011.
• 'Digital Britain' (2009), Final Report, June 2009. Department for Culture Media and Sport and Department for Business, Innovation and Skills. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/7650/228844.pdf (accessed October 2014).
• Downing, E. (2011), 'Cyber Security – A New National Programme', Science and Environment Section, SN/SC/5832, House of Commons Library, 23 June 2011.
• Drewer, D. and Ellermann, J. (2012), 'Europol's Data Protection Framework as an Asset in the Fight Against Cybercrime', Europol, 19 November 2012. Available at: https://www.europol.europa.eu/content/publication/europolsdata-protection-framework-asset-fight-against-cybercrime1838- (accessed February 2014).
• Dunn Cavelty, M. (2014), 'Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities', Journal of Science and Engineering Ethics, DOI: 10.1007/s-014-11948 -9551y.
• Dunn Cavelty, M. (2013), 'A Resilient Europe for an Open, Safe and Secure Cyberspace', Occasional Papers, No. 23, The Swedish Institute of International Affairs.
• Dunn, M. (2010), 'Securing the Digital Age: The Challenges of Complexity for Critical Infrastructure Protection and IR Theory', in Eriksson, J. and Giacomello, G. (eds.) International Relations and Security in the Digital Age, London and New York: Routledge.
• Dunn Cavelty, M. (2008a), Cyber-Security and Threat Politics: US Efforts to Secure the Information Age, London and New York: Routledge.
• Dunn Cavelty, M. (2008b), 'Critical (Information) Infrastructure Protection: History, Trends and Concepts', Centre for Security Studies, Swiss Federal Institute of Technology.
• Dunn Cavelty, M. (2007), 'Cyber-Terror-Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate', Journal of Information Technology and Politics, 35–19 ,(1)4. •
Dunn Cavelty, M. and Prior, T. (2013), 'Resilience in Security Policy: Present and Future', CSS Analysis in Security Policy, ETH Zurich, No. 142, October 2013.
• ENISA Threat Landscape Report (2014), 'ENISA, Greece'. Available at: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape#b_start=0 (accessed January 2015).
• ENISA, Press Release (26 June 2014), Available at: http://www.enisa.europa.eu/media/press-releases/fighting-cybercrime-strategic-cooperation-agreement-signed-between-enisa-and-europol (accessed March 2014).
• ENISA (2008), 'Stock Taking of Member States', Policies and Regulations Related to Resilience of Public eCommunications Networks', ENISA, 2008.
• ENISA (8' ,(2013th ENISA Workshop «CERTs in Europe» ', Report, ENISA, Greece.
• ENISA (2012), 'On National and International Cyber Security Exercises: Survey, Analysis and Recommendations', ENISA, October 2012. Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/cyber-europe2012-/cyber-europe-

-2012key-findings-report1-.
• ENISA (2012a) 'The Fight Against Cybercrime – Cooperation Between CERTs and Law Enforcement Agencies to Fight Against Cybercrime', ENISA, February 2012.
• ENISA (2012b) 'Give and Take: Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime. Legal, Regulatory and Operational Factors Affecting CERT Co-operation with Other Stakeholders', ENISA, November 2012.
• ENISA (2012c), 'Cyber Europe 2012: Key Findings and Recommendations', ENISA, December 2012. Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/cyber-europe2012-/cyber-europe-2012-key-findings-report (accessed July 2014).
• ENISA (2011), 'A Flair for Sharing – Encouraging Information Exchange Between CERTs', ENISA, November 2011.
• ENISA (2011a), 'Cyber Europe 2010 Evaluation Report', ENISA. Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2010/ce2010report (accessed July 2014).
• ENISA (2011b), 'Proactive Detection of Network Incidents', ENISA Report.
Available at: https://www.enisa.europa.eu/activities/cert/support/proactive-detection/proactive-detection-report (accessed July 2014).
• ENISA (2011c), Inter-X: Resilience of the Internet Interconnection Ecosystem, Summary Report, ENISA April 2011.
• ENISA (2011d), Cooperative Models for Effective Public-Private Partnerships: Good Practice Guide, ENISA 2011.
• ENISA (2010), 'ENISA Good Practice Guide on National Exercises', ENISA. Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce (accessed July 2014).
• Eriksson, J. (2001), Cyberplagues, IT and Security: Threat Politics in the Information Age, Journal of Contingencies and Crisis Management, 222–211 ,(4)9. Eriksson, J. and Giacomello G. (eds.) (2010) International Relations and Security in the Digital Age, London and New York: Routledge.
• EU Kids Online Survey (2010), 'Risks and Safety for Children on the Internet: The UK Report'. Available at: http://eprints.lse.ac.uk/33730/ (accessed April 2014).
• Europe 2010) 2020), 'A Strategy for Smart, Sustainable and Inclusive Growth', European Commission, COM (3 ,2020 (2010 March 2010.
• European Commission (2014), EU-US Fact Sheet: Negotiations on Data Protection, Brussels, June 2014. Available at: http://ec.europa.eu/justice/data-protection/files/factsheets/umbrella_factsheet_en.pdf (accessed February 2015).
• European Commission (2013), 'Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement and Training (Europol) and Repealing Decisions 371/2009/JHA and 681/2005/JHA', Brussels, 27 March 2013, COM (173 (2013 final, 0091/2013 (COD).
• European Commission (2013a), 'Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Level of Network and Information Security Across the Union', Brussels 7, February 2013, COM (48 (2013 final.
• European Commission (2013b), 'Impact Assessment', Accompanying the Document Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High

Level of Network and Information Security Across the Union, Commission Staff Working Document, Strasbourg, 7 February 2013, SWD(2013) Final.

• European Commission (2013c), Commission Staff Working Document on a New Approach to the European Programme for Critical Infrastructure Protection: Making European Critical Infrastructures More Secure, SWD (318 (2013 Final, Brussels, 28 August 2013.

• European Commission (2013d), 'Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU', Brussels, 27 November 2013, COM (847 (2013 final.

• European Commission (2013e), 'Restoring Trust in EU-US Data Flows', Memo, Brussels, 27 November 2013. Available at: http://europa.eu/rapid/press-release_MEMO1059-13-_en.htm (accessed February 2015).

• European Commission (2012), Communication from the Commission to the Council and the European Parliament, 'Tackling Cybercrime in Our Digital Age: Establishing a European Cybercrime Centre', COM (140 (012 final, Brussels, 28 March 2012.

• European Commission (2011), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection 'Achievements and Next Steps: Towards Global Cyber-security', COM (163 (2011 final, Brussels, 31 March 2011.

• European Commission (2011), 'Proposal on a European Strategy for Internet Security', November 2011. Available at: http://ec.europa.eu/smart-regulation/impact/planned_ia/docs/2012_infso_003_european_internet_security_strategy_en.pdf (accessed September 2013).

• European Commission (2011), 'Cyber security: EU and US Strengthen Transatlantic Cooperation in Face of Mounting Global Cyber-Security and Cybercrime Threats', Brussels, 14 April 2011. Available at: http://europa.eu/rapid/press-release_MEMO246-11-_en.htm (accessed January 2015).

• European Commission (2010), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 'A Digital Agenda for Europe', COM (245 (2010 final/26 ,2 August 2010.

• European Commission (2009a), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, 'Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience', COM (149 (2009 final, Brussels, 30 March 2009.

• European Commission (2009b), 'Internet Governance: Next Steps', Communication from the Commission from the European Parliament and the Council, Brussels, COM (277 (2009 final, 18 July 2009.

• European Commission (2008), COM (448 (2008: Report from the Commission to the Council Based on Article 12 of the Council Framework Decision of 24 February 2005 on Attacks Against Information Systems.

• European Commission (2006a), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 'A strategy for a Secure Information Society – «Dialogue, Partnership and Empowerment» ', COM ((2006 251 Final, Brussels, 31 May 2006.

• European Commission (2006b), Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM (786 (2006 Final, Brussels, 12 December 2006.
• European Commission (2005), Green Paper on the European Programme for Critical Infrastructure Protection, COM (576 (2005 Final, Brussels, 17 November 2005.
• European Commission (2005), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 'i2010 – A European Information Society for growth and employment', COM (229 (2005 Final, Brussels, 1 June 2005.
• European Commission (2001a), 'Creating a Safer Information Society by Improving the Security of Infrastructures and Combating Computer-Related Crime', COM (26 ,890 (2000 January 2001.• European Commission (2001b), Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on Network and Information Security: Proposal for A European Policy Approach, COM (298 (2001 Final, Brussels, 6 June 2001.
• European Commission (1999), Communication of 8 December 1999 on a Commission Initiative for the Special European Council of Lisbon, 23 and 24 March 2000 – eEurope – An Information Society for All, COM (687 (1999 Final (not published in the Official Journal).
• European Council Conclusions (20–19 December 2013), Available at: https:// www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/140214.pdf (accessed July 2014).
• European Cybercrime Centre (EC3) First Year Report (2014), Europol. Available at: http://www.europol.org (accessed December 2014).
• European Digital Rights Initiative (2011), 'The Slide from «Self-Regulation» to Corporate Censorship', January 2011. Available at: http://www.edri.org/files/EDRI_selfreg_final_20110124.pdf (accessed March 2014).
• European Frontier Foundation (2011), Available at: https://www.eff.org/issues/mandatory-data-retention/eu (accessed March 2014).
• European Parliament (2013), Draft Report, 'On the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens of Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs' (2188/2013 (INI)), Committee on Civil Liberties, Justice and Home Affairs. Available at: http://www.europarl.europa.eu/meetdocs/2014_2009/documents/libe/dv/moraes_1014703_/moraes_1014703_en.pdf (accessed February 2015).
• European Parliament (2012), Report on Critical Information Infrastructure Protection – Achievements and Next Steps: Towards Global Cyber-Security', Committee on Industry, Research and Energy, RR\902472EN.doc, 16 May 2012.
• European Parliament (2011), On the Proposal for a Directive of the European Parliament and of the Council on Combating Sexual Abuse, Sexual Exploitation of Children and Child Pornography, Repealing Framework Decision 68/2004/JHA, (COM(0094(2010 – C0064/2010 – 2010/70088(COD)), Draft Report, {LIBE}Committee on Civil Liberties, Justice and Home Affairs, 24 January 2011. Available at: http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&mode=XML&language=EN&reference=PE452.564 (accessed March 2014).
• European Parliament and the Council (2013), Directive 40/2013/EU of the European Parliament and of the Council of 12 August 2013 on Attacks Against Information Systems and Replacing Council

Framework Decision 222/2005/JHA.
• European Parliament and the Council (2012), Directive 29/2012/EU of the European Parliament and of the Council of 25 October 2012 Establishing Minimum Standards on the Rights, Support and Protection of Victims of Crime, and Replacing Council Framework Decision 220/2001/JHA.
• European Parliament and the Council (2012), Directive 29/2012/EU of the European Parliament and of the Council of 25 October 2012 Establishing Minimum Standards on the Rights, Support and Protection of Victims of Crime, and Replacing Council Framework Decision 220/2001/JHA. •
European Parliament and the Council (2011), Directive 93/2011/EU of the European Parliament and of the Council of 13 December 2011 on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography, and Replacing Council Framework Decision 68/2004/JHA.
• European Parliament and Council (2009), Regulation (EC) No 2009/544 of the European Parliament and of the Council of 18 June 2009 Amending Regulation (EC) No 2007/717 on Roaming on Public Mobile Telephone Networks Within the Community and Directive 21/2002/EC on a Common Regulatory Framework for Electronic Communications Networks and Services.
• European Parliament and the Council (2002), Directive 58/2002/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications).
• European Parliament and the Council (1995), Directive 46/95/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.
• EU Prepares to Launch First Cybercrime Centre (2012), EuroActiv, 29 March 2012. Available at: http://www.euractiv.com/infosociety/eu-prepares-launch-cybercrime-ce-news511823- (accessed March 2015).
• European Principles and Guidelines for Internet Resilience and Stability (2011), Available at: http://ec.europa.eu/danmark/documents/alle_emner/videnskabelig/110401_rapport_cyberangreb_en.pdf (accessed March 2013).
• European Security Research Innovation Forum Final Report (2009), Available at: http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf (accessed March 2014).
• European Strategy for Cloud Computing – Unleashing the Power of Cloud Computing in Europe (2012), Available at: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF (accessed March 2015).
• EU-US Cooperation on Cybersecurity and Cyberspace (2014), Fact Sheet, European External Action Service, 26 March 2014.
• EU-US Working Group on Cybersecurity and Cybercrime (2011), Concept Paper, European Commission, 13 April 2011.
Flyverbom, M. (2011), The Power of Networks: Organizing the Global Politics of the Internet, Cheltenham: Edward Elgar Publishing.
• Gellman, B. and Nakashima, E. (2013), 'US Spy Agencies Mounted 231 Offensive Cyber-operations in 2011, Documents Show', Washington Post, 30 August 2013. Available at: http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/30/08/2013/d090a6ae119-e11-e-3b4cb-fd7ce041d814_story.html (accessed January 2015).

• Gjelten, T. (2010), Seeing the Internet as an 'Information Weapon', 23 September 2010, Available at: http://www.npr.org/templates/story/story.php?storyId=130052701 (accessed September ر.(2013
• Goldsmith, J. (2011), Cybersecurity Treaties: A Skeptical View, Future Challenges Essay, Hoover Institution, Stanford University.
• Greenwald, G. and MacAskill, E. (2013), Obama Orders US to Draw up Overseas Target List for Cyber Attacks, The Guardian, 7 June 2013.
• Grimm, V. and Calabrese, J. M. (2011), 'What Is Resilience? A Short Introduction', in Deffuant, G. and Gilbert, N. (eds.) Viability and Resistance of Complex Systems: Concepts, Methods and Case Studies, Springer.
• Hague, W. (2011), 'Security and Freedom in the Cyber Age – Seeking the Rules of the Road', Speech Given to the Munich Security Conference, 4 February 2011.
• Hallenberg, J., Sperling, J. and Wagnsson, C. (2009), European Security Governance: The European Union in a Westphalian World, London: Routledge.
• Handmer, J. W. and Dovers, S. R. (1996), 'A Typology of Resilience: Rethinking Institutions for Sustainable Development', Organization & Environment, 511–482 ,9.
• Hart, A. G. (2001), 'The G8 and the Governance of Cyberspace', in Fratianni, M. (ed.) New Perspectives on Global Governance: Why America Needs the G8, Aldershot: Ashgate Publishing Limited.
• Hathaway, M. (2011), 'Examining the Homeland Security Impact of the Obama Administrations Cybersecurity Proposal', Statement Before the House off Representative Committee on Homeland Security, Sub Committee on Cybersecurity, Infrastructure Protection and Security Technologies, 24 June 2011.
• Healey, J. (2011a), 'Comparing Norms for National Conduct in Cyberspace', 20th September 2011. Available at: http://www.acus.org (accessed October 2013).
• Healey, J. (2011b), 'Breakthrough or Just Broken? China and Russia's UNGA Proposal on Cyber Norms', 21 September 2011. Available at: http://www.acus.org (accessed October 2013).
• Hern, B. (2014), 'British Government «breaking law» in Forcing Data Retention by Companies', theguardian.com, 24 June 2014. Available at: http://www.theguardian.com/technology/2014/jun/24/british-government-breaking-law-in-forcing-data-retention-by-companies (accessed February 2015).
• Herrington, L. and Aldrich, R. (2012), 'The Future of Cyber-Resilience in an Age of Global Complexity', Politics, 310–299 ,(4)33.
• Hilley, S. (2005), 'Pressure Mounts on US Senate to Pass Cyber Crime Treaty', Digital Investigation, 174–171 ,2.
• Holling, C. (1973), 'Resilience and the Sustainability of Ecological Systems', Annual Review of Ecology and Systematics, 23–1 ,(1)4.
• Hosein, I. and Eriksson, J. (2010), 'International Policy Dynamics and the Regulation of Data Flows: Bypassing Domestic Restrictions', in Eriksson, J. and Giacomello, G. (eds.) International Relations and Security in the Digital Age, London and New York: Routledge.
• House of Lords, EU Committee 13th Report of Session 2014–2013, 'Strategic guidelines for the EU's next Justice and Home Affairs Programme: Steady as She Goes', HL Paper 173, House of Lords, April 2014. Available at: http://www.parliament.uk/business/committees/committees-a-z/lords-select/eu-home-affairs-sub-committee-f/inquiries/parliament2010-/rome-programme/ (accessed July 2014).
• House of Lords (2011–2010), Government and Commission Responses Session: 2010–2009,

European Union Committee, 4th Report of the 11–2010 Session, UK Government.
• House of Lords EU Committee Report (2010), 'Protecting Europe Against Large Scale Cyber Attacks', HL Paper 2010–2009 ,68, March 2010, para 24.
• Improvements Proposed for Europol (2013), Available at: http://www.eubusiness.com/topics/crime/europol27 ,2- March 2013 (accessed July 2014).
• Information Assurance Advisory Council Symposium, 'Securing the Cloud –Securing Me', Royal College of Physicians, London, 12 September 2012.
• International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World (2011), The White House, Washington DC, May 2011.
• International Telecommunications Union (ITU) (2011) National Cybersecurity Strategy Guide, ITU, September 2011.
• International Telecommunications Union (ITU) (2008) Global Cybersecurity Agenda, High level Experts Group, Global Strategic Report, ITU.
• International Telecommunications Union (ITU) (2008a) Q.1/22 Report on Best Practices for a National Approach to Cyber Security: A
• Management Framework for Organizing National Cybersecurity Efforts (2008), ITU-D Secretariat, January 2008.
• Janczewski, L. J. and Colarik, A. M. (2007), Cyber Warfare or Cyber Terrorism, USA: IGI Global.
• Janczewski, L. J. and Colarik, A. M. (2008), Cyber Warfare and Cyber Terrorism, USA: Information Science Reference, IGI Global.
• Jeffray, C. (2014), 'Five Unanswered Questions on the UK's New Computer Emergency Response Team', RUSI Analysis, RUSI, UK. Joint Statement of the EU-US Summit 20 ,2010 November 2010, Lisbon.
Available at: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/597/10&type=HTML (accessed February 2015).
• Karatzogianni, A. (ed.) (2009), Cyber Conflict and Global Politics, London and New York: Routledge.
• Karatzogianni, A. (2006), The Politics of Cyber Conflict, London and New York: Routledge.
• Kavalski, E. (2009), 'Timescapes of Security: Clocks, Clouds, and the Complexity of Security Governance', World Futures, 551–527 ,(7)65.
• Kerry, C. (2014), 'Missed Connections: Talking with Europe About Data, Privacy, and Surveillance', Center for Technology Innovation, Brookings, May 2014.
• Kirchner, J. E. and Sperling, J. (2007a), Global Security Governance: Competing Perceptions of Security in the 21st Century, London: Routledge.
• Kirchner, J. E. and Sperling, J. (2007b), European Union Security Governance, Manchester: Manchester University Press.
• Klimburg, A. (2012), 'The Internet Yalta', Commentary, Center for New American Security, 5 February 2013.
• Klimburg, A. (2011a), 'Mobilising Cyber Power', Survival, 60–41 ,(1)53.
• Klimburg, A. (2011b), 'Ruling the Domain: Self-Regulation and the Security of the Internet', Austrian Institute of International Affairs, Paper Distributed at the 11th Meeting of the ICANN Studienkreis, 29/28 April 2011.
• Klimburg, A. and Tiirmaa-Klaar, H. (2011), 'Cyber War and Cyber Security: Challenges Faced by

the EU and Its Member States', DG for External Policies, Policy Department, European Parliament, April 2011.
• Krahman, E. (2003), 'Conceptualizing Security Governance', Cooperation and Conflict, 26–5 ,(1)38.
• Kramer, F. D. Starr, S. and Wentz, K. L. (eds.) (2010), Cyber Power and National Security, Washington, DC: National Defence UP.
• Kroes, N. (2011), 'I Don't Like to Be too Diplomatic. That Is Not My Style: Neelie
•Kroes Talks Internet Governance'. Available at: http://news.dot-nxt.com/30/09/2011/kroes-interview-igf (accessed June 2013).
• Kruger, G. L. (2013), 'Internet Domain Names: Background and Policy Issues', Congressional Research Service Report, 5700–7. Available at: www.crs.gov (accessed November 2014).
• Kshetri, N. (2013), Cybercrime and Cybersecurity in the Global South, New Political Economy Series, Houndmills, Basingstoke: Palgrave Macmillan.
• Laprise, J. (2014), 'Internet Governance: The New «Great Game» ', The Centre for Global Communications Studies, University of Pennsylvania.
• Lentzos, F. and Rose, N. (2009), 'Governing Insecurity: Contingency Planning, Protection, Resilience', Economy and Society, 54–230 ,(2)38.
• Lewis, A. J. (2014), 'Liberty, Equality, Connectivity: Transatlantic Cybersecurity Norms', Strategic Technologies Program, Centre for Strategic and International Studies, Washington, DC, USA.
• Leyden, J. (2011), 'EU Parliament Suspends Webmail After Cyber-Attack', The Register, 31 March 2011. Available at: http://www.theregister.co.uk/31/03/2011/eu_parliament_hack/ (accessed March 2015).
• Libicki, M. C. (2009), Cyber Deterrence and Cyber War, Rand Corporation.
• Libicki, M. C. (2007), Conquest in Cyberspace: National Security and Information Warfare, New York: Cambridge University Press.
• Livingstone, S. (2013), 'A Better Internet for UK Children?', 23 April 2013. Available at: http://blogs.lse.ac.uk/mediapolicyproject/23/04/2013/a-better-internet-for-uk-children/ (accessed April 2014).
• Long, W. (2014), 'What to Expect from the EU's NIS Directive', Computer Weekly. Available at: http://www.computerweekly.com/opinion/What-to-expect-from-European-NIS-Directive (accessed December 2014).
• Malcolm, J. (2008), Multi-Stakeholder Governance and the Internet Governance Forum, Perth: Terminus Press.
• Marion, E. N. (2010), 'The Council of Europe's Cyber Crime Treaty: An Exercise in Symbolic Legislation', International Journal of Cyber Criminology, 4 (Combined Issue 712–699 ,(2&1.
• Mehan, J. (2008), CyberWar, CyberTerror, CyberCrime, Cambridgeshire: IT Governance Publishing.
• Meyer, P. (2013), 'Cyber Security Takes the Floor at UN', Canadian International Council, 12 November 2013. Available at: http://opencanada.org/features/the-think-tank/comments/cyber-security-takes-the-floor-at-the-un/ (accessed January 2014).
• Micek, P. and Masse, E. (2014), 'US May Grant Rights to EU Citizens Under Privacy Act', Access, 16 July 2014.
• Mohan, R. (2011), DNSSEC Baby Steps Reported at ICANN 41, CircleID Internet Infrastructure, 29 July 2011.
• Mowlana, H. (1997), Global Information and World Communication: New Frontiers in International

Relations, London: Sage.
• Mueller, M. L. (2010), Networks and States: The Global Politics of the Internet, MIT Press.
• Net Losses: Estimating the Global Cost of Cybercrime (2014), Economic Impact of Cybercrime II, Center for Strategic and International Studies, McAfee/Intel Security, June 2014. Available at: http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf (accessed March 2015).
• Neville-Jones, P. and Phillips, M. (2012), 'Where Next for UK Cyber-Security?' RUSI Journal, 6)157), Dec 40–32 ,2012.
North Atlantic Treaty Organisation (NATO) (2014), Available at: http://www.nato.int/cps/en/natohq/topics_78170.htm (accessed December 2014).
• Norton Cybercrime Report (2013), 'Symantec'. Available at: https://msisac.cisecurity.org/resources/reports/documents/b-norton-report2013-.pdf (accessed December 2014).
• Noshiravani, R. (2011), NATO and Cyber Security: Building on the Strategic Concept, 20 May 2011, Rapporteur Report, The NATO Science for Peace and Security Programme, Chatham House
• Nye, J. (2010), 'Cyber Power', Harvard Kennedy School, Belfer Center for Science and International Affairs, May 2010.
Obama seeks 14$ billion to boost US cybersecurity defences', Reuters, 15 February 2015. Available at: http://www.reuters.com (accessed January 2015).
• OECD (2012), 'Proactive Policy Measures by Internet Service Providers Against Botnets', OECD Digital Economy Papers, No.199, OECD Publishing. Available at: http://dx.doi.org/5/10.1787k98tq42t18w-en (accessed July 2013).
• OECD (2003), 'Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security', Working Party on Information Security and Privacy, DSTI/ICCP/REG(5(2003/REV1, Organisation for Economic Cooperation and Development, Paris, France.
• OECD (2002), 'OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security', Organisation for Economic Cooperation and Development, Paris, France.
• Office of the Director of National Intelligence (2015), Available at: http://icontherecord.tumblr.com/ppd2015/28-/overview.
O'Neill, M. (2012), 'Cyber Crime and Cyber Security: A Late Developer in the EU's AFSJ', Draft Paper, Presented at Cybercrime and Cyber Security Workshop, University of Abertray, Dundee, 10 September 2012.
• P8 Experts Group on Transnational Organized Crime (Lyon Group): 40 Recommendations. Available at: http://www.auswaertigesamt.de/cae/servlet/contentblob/357602/publicationFile/3516/G-8Lyon40-recomOCrime1996.pdf (accessed March 2015).
• Pearse, R. Buckenham, P. and Donnelly, N. (2015), 'EU Network and Information Security Directive', Society for Computers and Law. Available at: http://www.scl.org/site.aspx?i=ed39127 (accessed February 2015).
• 'Pentagon Creates 13 Offensive Cyber Teams for Worldwide Attacks' (2013), RT, 13 March 2013. Available at: http://rt.com/usa/alexander-cyber-command-offensive209-/ (accessed January 2015).
• Perl, R. (2010), 'Combating Terrorist Use of the Internet/Comprehensively Enhancing Cyber Security', Counter Terror Expo, 'Countering Terrorism in a Changing World', 15–14 April 2010, London, UK.

• Porcedda, G. M. (2012), Data Protection and the Prevention of Cybercrime: The EU as an Area of Security? EUI Working Papers, Law 25/2012, Department of Law. Available at: http://cadmus.eui.eu/bitstream/handle/23296/1814/LAW25-2012-.pdf?sequence=1 (accessed March 2014).
• Press Release, '1st EU-US Cyber Dialogue' (2014), Brussels, 5 December 2014.
• Pritchard, R. (2013), 'UK Cyber Response: Getting It Right Matters', RUSI Analysis, RUSI.
• Reding, V. (2013), Letter to the US Attorney General of the United States Department of Justice, 10 June 2013. Available
• Report of the Global Alliance Against Child Sexual Abuse Online (2013), European Commission, DG Home Affairs, December 2013. Available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/global_alliance_report_201312_en.pdf (accessed February 2015).
• Robinson, N. (2014), 'EU Cyber-Defence: A Work in Progress', European Union Institute for Security Studies, March 2014.
• Robinson, N. Walczak, A. Brune, S.-C. Esterle, A. Rodriguez, P. (2013), Stocktaking Study of Military Cyber Defence Capabilities in the European Union, RAND Europe Report Prepared for the European Defence Agency (UNCLASSIFIED SUMMARY REPORT).
• Roehrig, W. (2014), 'How to Integrate Cyber Threat Intelligence into EU-led Military Operations', Cyber Intelligence Europe, Brussels, 23 September 2014.
• Roehrig, W. (2013), 'Mainstreaming European Military Cyber Defence Training and Exercises', September 2 ,2013nd ENISA International Conference on Cyber Crisis Cooperation and Exercises, 24–23 September 2013.
• Roehrig, W. and Smeaton, R. (2013), 'Cyber Security and Cyber Defence in the European Union: Opportunities, Synergies and Challenges', European Defence Agency.
• Saran, C. (2014), 'European Parliament Calls to Drop Safe Harbour', ComputerWeekly.com, 16 January 2014. Available at: http://www.computerweekly.com/news/2240212616/European-parliaments-calls-to-drop-Safe-Harbour (accessed January 2015).
• Schneider, V. (2012), 'Governance and Complexity', in Levi-Faur, D. (ed.) The Oxford Handbook of Governance, Oxford: Oxford University Press.
• Schoon, I. (2010), (ed.) Risk and Resilience: Adaptations in Changing Times, Cambridge: Cambridge University Press.
Scott, M. (2010), 'With Three Months to go to DNSSEC, Someone's Fudging Root Zone Records', Betanews, March 2010. Available at: http://www.betanews.com/article/with-three-months-to-go-to-DNSSES-someones-fudging-root-zone-records/1269642342 (accessed June 2013).
• Shah, S. (2012), 'UK Cyber Security – Fragmented and Failing', Computing, 28 November 2012.
• Shore, M., Du, Y. and Zeadally, S. (2011), 'A Public-Private Partnership Model for National Cybersecurity', Policy & Internet, 2)3), Art.8.
• Sliwinski, F. K. (2014), 'Moving Beyond the European Union's Weakness as Cyber-Security Agent', Contemporary Security Policy, DOI:22) 13523260.2014.959261/10.1080 September 2014).
• Sofaer, D. A., Clarke, D. and Diffie, W. (2010), 'Cybersecurity and International Agreements', Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for US Policy. Available at: http://www.nap.edu/catalog/12997.html (accessed February 2015).
• Sommer, P. and Brown, I. (2011), 'Reducing Systemic Cybersecurity Risk', OECD/IFP Project on

'Future Global Shocks', IFP/WKP/FGS(3(2011.
at: http://www.statewatch.org/news/2013/jun/eu-usa-reding-ag.letter.pdf (accessed February 2015).
• Stevens, T. (2012), 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', Contemporary Security Policy, 170–148 ,(1)33.
• Szilecki, K. Pattberg, P. and Biermann, F. (2011), 'Explaining Variation in the Effectiveness of Transnational Energy Partnerships', Governance: An International Journal of Policy, Administration and Institutions, 736–713 ,(4)24.
• Tallinn Manual on the International Law Applicable to Cyber Warfare (2013), Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge: Cambridge University Press.
• 'The Digital Economy: Potential, Perils and Promises' (2014), A Report of the Digital Economy Task Force, March 2014.
• 'The National Crime Agency: A Plan for the Creation of a National Crime Fighting Capability' (2011), Home Office, June 2011, CM 8097.
• 'The UK Cyber Security Strategy: Report and Forward Plans' (2014), Cabinet Office, December 2014.
• 'The UK Cyber Security Strategy: Landscape Review' (2013), Report by the Controller and Auditor General, HC 890, National Audit Office, 12 February 2013.
• 'The UK Cyber Security Strategy: Report and Forward Plans' (2013), Cabinet Office, December 2013.
• 'The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World' (2011), Cabinet Office, November 2011.
• Tick, E. (2010), Global Cyber Security – Thinking About the Niche for NATO, The SAIS Review of International Affairs, Fall 2010 (pre-publication).
• Titch, S. (2013), 'US Cybersecurity Policy: Problems and Principles', Policy Brief, the Heartland Institute, August 2013.
• Traynor, I. (2014), 'Internet Governance too US-centric, Says European Commission', 12 February 2014. Available at: http://www.theguardian.com/technology/2014/feb/12/internet-governance-us-european-commission (accessed January 2015).
• 'UK Cyber Security Progress Welcomed' (2013), Computer Weekly.com. Available at: http://www.computerweekly.com (accessed December 2013).
• UK Department of Business Innovation and Skills (2013), Call For Evidence on Proposed EU Directive on Network and Information Security, Report on Summary of Responses, September 2013. Available at: https://www.gov.uk/government/consultations/eu-directive-on-network-and-information-security-call-for-evidence (accessed July 2014).
• UK Home Office (2013), 'The European Commission's Proposal for a Europol Regulation'. Available at: http://www.gov.uk/speeches/the-european-commissions-proposal-for-a-europol-regulation (accessed July 2014).
• United Nations (2010), Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/201/65, Study Series 2010 ,33.
• 'Update on the National Cyber Security Programme' (2014), Report by the Controller and Auditor

General, HC 626, National Audit Office, 10 September 2014.
• US-EU Cyber Cooperation FACT SHEET (2014), The White House, Office of the Press Secretary, 26.3.14. Available at: http://www.whitehouse.gov/the-press-office/26/03/2014/fact-sheet-us-eu-cyber-cooperation (accessed February 2015).
• Valeri, L. (2010), 'Public-private Cooperation and Information Assurance', in Eriksson, J. and Giacomello, G. (eds.) International Relations and Security in the Digital Age, London and New York: Routledge.
• Van der Steeg, D. (2011), 'IPv6 Security: Transition from IPv4 to IPv6', University of Twente, June 2011.
• Venkatraman, A. (2013), 'EC urges Europe: Become a 'trusted cloud region' in the Post-PRISM Age', Computer Weekly Europe, December 2013.
• Verton, D. (2003), Black Ice: The Invisible Threat of Cyber-Terrorism, California: McGraw-Hill Companies.
• Volter, W. (2013), 'The UN Takes a Big Step Forward on Cybersecurity', Arms Control Today. Available at: https://www.armscontrol.org/act/09_2013/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity (accessed January 2014).
• Walker, J. and Cooper, M. (2011), 'Genealogies of Resilience: From Systems Ecology to the Political Economy of Crisis Adaptation', Security Dialogue, 60–143 ,(2)42.
• Watt, N. (2013), 'Prism Scandal: European Commission to Seek Privacy Guarantees from US', theguardian.com, 10 June 2013. Available at: http://www.theguardian.com/world/2013/jun/10/prism-european-commissions-privacy-guarantees (accessed February 2015).
• Weber, M. A. (2014), 'The Council of Europe's Convention on Cybercrime', Berkeley Technology Law Journal, 1)18). Available at: http://scholarship.law. berkeley.edu/btlj/vol18/iss28/1 (accessed 30 January 2014).
• Webber, M. (2007), Inclusion, Exclusion and the Governance of European Security, Manchester and New York: Manchester University Press.
• Webber, M. Croft, S. Howorth, J. Terriff, T. and Krahmann, E. (2004), 'The Governance of European Security', Review of International Studies, 26–3 ,(3)30.
• Weinburg, J. (2010) 'Non-State Actors and Global Informal Governance – The Case of ICANN', Wayne State University Law School Research Paper No. 05-10. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1621862 (accessed March 2015).
• Wiemann, G. (2006), Cyberterrorism: How Real Is the Threat, Washington, DC: United States Institute of Peace.
• Wildavsky, A. B. (1995), But Is It True? A Citizen's Guide to Environmental Health and Safety Issues, Cambridge, MA: Harvard University Press.
• Wildavsky, A. B. (1988), Searching for Safety, New Brunswick: Transaction.
• Yannakogeorgos, P. A. (2015), 'The Rise of IPv6: Benefits and Costs of Transforming Military Cyberspace', Air and Space Power Journal, 2)29), March–April 128–103 ,2015.
• Yannakogeorgos, P. A. and Lowther, A. B. (eds.) (2013), Conflict and Cooperation in Cyberspace: The Challenge to National Security, London: CRC Press.

مرکز ملی فضای مجازی
انتشارات پژوهشگاه فضای مجازی

تردیدی نیست که گسترش فزاینده فناوری‌های ارتباطی و اطلاعاتی در سطح کشورهای اروپایی و همچنین پیگیری جدی اتحادیه اروپا در افزایش رشد و توسعه اقتصادی از بستر فضای دیجیتال و سایبر، امنیت اتحادیه را هم‌ردیف با امنیت سایبری آن کرده است؛ بدین معنی که هر عامل تهدیدزا برای امنیت سایبری اتحادیه اروپا و اعضای آن به‌مثابه تهدیدی برای امنیت سرزمینی و وجودی آن‌ها به شمار می‌آید. از همین روست که اتحادیه اروپا در دهه دوم سده جدید تلاش مضاعفی برای تدوین و اجرای سیاست‌ها و راهبردها در خصوص امنیت سایبری اتحادیه داشته است. به‌رغم اهمیت موضوع امنیت و بخصوص امنیت سایبری اتحادیه اروپا، این مقوله چندان از سوی جوامع علمی غربی و ایرانی موردتوجه قرار نگرفته است که لذا تألیف و ترجمه این اثر با هدف تکمیل این خلأ در هر دو جامعه مذکور انجام گرفته است.

ISBN:978-600-8365-50-1

قیمت : ؟