امنیت سایبری اتحادیه اروپا: تهدیدات، فرصت‌ها و اقدامات (از آغاز تا سال ۲۰۲۱)

(مقاله علمی-پژوهشی)

روح‌الله رهامی*

امیرحسین اژدری**

تاریخ دریافت: ۱۴۰۱/۰۵/۲۸ تاریخ پذیرش: ۱۴۰۱/۰۹/۲۷

چکیده

با رشد فناوری‌های نوین، فضای سایبر از اهمیت چندانی برخوردار شد. از این رو، بازیگران سیاسی در نظام بین‌الملل، فضای سایبر را به عنوان فضایی که از اهمیت بسزایی برخودار است و در کنار فرصت‌ها، تهدیدات به‌خصوص خود را دارد، در نظر گرفته‌اند و بر اساس آن در حوزهٔ سایبری اقدام به سیاست‌گذاری می‌کنند. یکی از این بازیگران سیاسی، اتحادیه اروپاست که به دنبال حضوری فعال و منسجم در حوزهٔ سایبری در نظام بین‌الملل است. این پژوهش به دنبال بررسی تهدیدات اتحادیه اروپا در حوزهٔ سایبر و اقدام اتحادیه در برابر این تهدیدات است و میزان انسجام میان مؤسسات، نهادها و آژانس‌های مرتبط با حوزهٔ سایبر و نقش آنها به منظور مقابله با این تهدیدات را بررسی می‌کند. سؤال اصلی این مقاله آن است که چگونه و با چه سازوکاری فرایند سیاست‌گذاری امنیت سایبری اروپا در حال شکل‌گیری است؟ با توجه به سؤال اصلی، این فرضیه مطرح می‌شود که سه عامل دشمن بیرونی، رقابت نهادی درونی و تعارض میان قواعد حقوقی (به عنوان متغیر مستقل) در تعیین سازوکار سیاست‌گذاری امنیت سایبری در اروپا (متغیر وابسته) تأثیرگذارند. به منظور راستی‌آزمایی فرضیه، از روش ردیابی فرایند تاریخی- تحلیلی استفاده شده است. در این پژوهش نشان داده می‌شود که پس از حملهٔ سایبری به زیرساخت‌های استونی، اقدامات اتحادیه اروپا چه از لحاظ کمّی و چه از لحاظ کیفی، افزایش یافته است که نشان از عزم اتحادیه اروپا در راستای تبدیل به یک بازیگر منسجم در حوزهٔ سایبر در سطح بین‌الملل است.

کلید واژگان:

امنیت سایبری، اتحادیه اروپا، ENISA، تاب‌آوری سایبری، انسجام.

---

* استادیار، دانشکده حقوق و علوم سیاسی، دانشگاه تهران (نویسنده مسئول) rrahami@ut.ac.ir

** دانشجوی دکتری روابط بین‌الملل، دانشکده حقوق و علوم سیاسی، دانشگاه تهران amirh.ajdari@ut.ac.ir

مقدمه

امروزه شاهد پیشرفت علم و فناوری و رشد چشمگیر وسایل ارتباطی و اطلاعاتی مبتنی بر هوش مصنوعی هستیم. اتکا به فضای سایبر و وسایلی همچون کامپیوترها، تبلت‌ها و تلفن‌های همراه به‌گونه‌ای است که وقفه در کارکرد آنها مشکلات بیشماری را به‌وجود می‌آورد. همین اتکای بیش از حد باعث شده است که مفهوم امنیت به حوزهٔ سایبری نیز وارد شود؛ چرا که وجود داده‌ها و اطلاعات مهم و بیشمار در این فضا باعث شده است که مقولهٔ امنیت سایبری از جایگاه ویژه‌ای برخوردار شود. ایجاد اختلال در سیستم‌های حمل و نقل عمومی، سایت‌های دولتی و غیر دولتی، زیرساخت‌های حیاتی و مواردی از این دست، مشکلات بیشماری را به‌وجود خواهد آورد.

موضوع قابل توجه این است که در به‌چالش‌کشیدن امنیت برخلاف موارد پیشین که دولت‌ها نقش بسزایی در آن داشتند، در مورد امنیت سایبری، بازیگران و افراد غیردولتی به اندازهٔ دولت‌ها می‌توانند اثرگذار باشند. وابستگی بیش از حد دنیای امروز به سیستم‌های فناوری و اطلاعاتی باعث شده است که دولت‌ها و بازیگران مختلف به تمهیداتی در راستای مدیریت فضای سایبری بیندیشند. از جملهٔ این بازیگران اتحادیه اروپاست که تا به امروز نسبت به امنیت سایبری اقدامات متعددی انجام داده است. حملهٔ سایبری علیه زیرساخت‌های عمومی و خصوصی استونی در سال ۲۰۰۷، بُعد جدیدی در استفاده از شبکه‌های اطلاعاتی را به‌وجود آورد. این حمله ضربهٔ سنگینی به حاکمیت استونی وارد کرد و موجب تصمیم‌ها، مذاکرات و موافقت‌نامه‌های بعدی از سوی اروپا شد.

امروزه یکی از اولویت‌های راهبردی اتحادیه اروپا توسعهٔ ظرفیت‌های دفاع سایبری، سیاست‌گذاری و همکاری بخش‌های مختلف اروپا مانند جامعه مدنی، ناتو، سازمان امنیت همکاری اروپا، کمیسیون اروپایی و در سطح فراتر از آن همچون سازمان ملل متحد، سازمان‌های منطقه‌ای و سایر کشورهاست. طی سالیان اخیر و با توجه به اهمیت فضای سایبر اقداماتی از سوی اتحادیه اروپا در ابعاد سیاسی و حقوقی انجام شده است که مهم‌ترین آنها راهبرد امنیت سایبری اروپا در سال‌های ۲۰۱۳[1] (بازبینی شده در سال ۲۰۱۷)[2] و ۲۰۲۰، [3] چارچوب

1. European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN (2013) 1 final, 7 February 2013.
2. EUROPEAN COMMISSION, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation -(EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), 2017/0225, 13 September 2017.
3. European Council conclusions Draft EU Council conclusions.2021.

سیاست‌گذاری دفاعی در ۲۰۱۴[1] (بازبینی شده در۲۰۱۸)،[2] جعبه ابزار دیپلماسی در سال ۲۰۱۷،[3] دستورالعمل امنیت شبکه و اطلاعات در سال ۲۰۱۶[4] و بازبینی آن در ۲۰۲۰[5] و فرمان امنیت سایبری در ۲۰۱۹ [6] هستند. می‌توان سال ۲۰۱۶ را یک نقطه‌عطف به‌سوی محیط سایبری امن برای اروپا دانست. اعلامیه مشترک میان اتحادیه اروپا و ناتو زمینهٔ همکاری اساسی این دو سازمان را فراهم کرد و نقش امنیت سایبری در سیاست‌گذاری را برجسته نمود. اقدام مهم دیگر تصویب بخشنامه امنیت و شبکه اطلاعات از سوی پارلمان و شورای اروپایی در سال ۲۰۱۳ بود.[7] به‌نظر می‌رسد، امنیت سایبری نقش قابل ملاحظه در سیاست‌گذاری‌های اتحادیه اروپا و کشورهای اروپایی دارد. شمار متعدد نهادها (اعم از دولتی و غیردولتی) و میزان اثرگذاری در تعیین سیاست‌گذاری و خط‌مشی‌ها خود موضوعی است که باید آن را مد نظر قرار داد.

تاکنون بیشتر مباحث مطرح‌شده در زمینهٔ امنیت سایبری مربوط به جنبهٔ فنی بوده است و حجم آثاری که از بعد سیاست‌گذاری به امنیت سایبری پرداخته‌اند، به نسبت اهمیت داده‌ها و اطلاعات در دنیای امروزی کم است. از طرفی اکثر آثار نوشته‌شده در حوزهٔ امنیت سایبری، مفاهیم پایه و کلی را به همراه تکنیک‌ها پوشش داده‌اند و کمتر اثری به‌خصوص در میان آثار فارسی اقدامات و تجربه‌های منطقه‌ای خاص در این حوزهٔ موضوعی را بررسی کرده است.

سؤال اصلی این مقاله آن است که چگونه و با چه سازوکاری فرایند سیاست‌گذاری امنیت سایبری اروپا در حال شکل‌گیری است؟ و در ذیل آن تهدیدات، فرصت‌ها و اقدامات انجام‌شده از سوی اروپا در زمینهٔ امنیت سایبری و بازیگران اثرگذار در سیاست‌گذاری امنیت سایبری اروپا بررسی خواهند شد. در این پژوهش منظور از بازیگران، نهادهای مرتبط درون اتحادیه است.

1. EU Cyber Defence Policy Framework , 15585/14, 18 November 2014.
2. EU Cyber Defence Policy Framework (2018 update), 14413/18, 19 November 2018.
3. Council of the European Union, Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), 9916/17, 19 June 2017.
4. THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, concerning measures for a high common level of security of network and information systems across the Union (NIS Directive), 2016/1148, 6 July 2016.
5. www.consilium.europa.eu/en/policies/cybersecurity, 2021 .
6. THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, REGULATION on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (Cybersecurity Act), 2019/ 881, 17 April 2019.
7. REGULATION (EU) No 526/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 21 May 2013.

فرضیهٔ این پژوهش بر آن است که سه عامل دشمن بیرونی، رقابت نهادی درونی و تعارض میان قواعد حقوقی (به عنوان متغیر مستقل) در تعیین سازوکار سیاست‌گذاری امنیت‌سایبری در اروپا (متغیر وابسته) تأثیرگذارند. در این پژوهش از روش ردیابی فرایند تاریخی- تحلیلی استفاده شده است. این روش امکان بررسی مکانیسم‌های علّی و تغییرات را می‌دهد و به کمک آن می‌توان سیر اتفاقات و روابط میان متغییر مستقل و وابسته را در طول زمان ارزیابی کرد. هدف اصلی در این روش این است که مشخص کند چگونه یک علت یا علل بالقوه بر تغییر یا مجموعه خاصی از تغییرات اثرگذار بوده است. در این پژوهش از منابع اینترنتی، گزارش، اسناد و مقالات برای گردآوری مطالب استفاده شده است. در بخش اول، مبانی نظریهٔ این پژوهش که نظریهٔ انسجام است، توضیح داده می‌شود و در بخش بعد ضمن ارائهٔ تعریفی از تهدید سایبری، حالت‌های مختلف شامل حوادث، جرائم و حملهٔ سایبری بررسی می‌شوند. بخش بعد شامل معرفی و بررسی وظایف و عملکرد مهم‌ترین بازیگران مرتبط است و سپس اقدامات صورت‌گرفته توسط اتحادیه به عنوان یک بازیگر بین‌المللی در حوزهٔ امنیت سایبری تبیین شده‌اند. در انتها، بر اساس مطالب گفته‌شده یک نتیجه‌گیری صورت گرفته است.

۱. نظریه انسجام

مفهوم انسجام[1] از مدت‌ها قبل به ادبیات سیاسی و حقوقی راه پیدا کرده است. انسجام توانایی گردهم‌آوردن لایه‌های مختلف سیاست و افرادی است که مسئولیت مدیریت آن لایه‌ها را بر عهده دارند و به طور کلی، قادر به کنش در برابر تلاش‌های بیرونی برای بهره‌برداری در درون است.[2] انسجام را می‌توان به عنوان خروجی سیستمیک[3] و فرایند نهادی[4] در نظر گرفت. خروجی سیستمیک از این نظر که دوام و ماهیت سیاست‌گذاری‌های متفاوت به‌وسیلهٔ بخشی که خود جزئی از یک کل منسجم است، به‌وجود می‌آیند و فرایند نهادی یعنی درجه‌ای که سازمان فرایند

1. Coherence
2. Thaler, Philipp. Shaping EU Foreign policy towards Russia: Improving coherence in external relations. Edward Elgar Publishing, 2020,p.31.
3. Systemic Output
4. Institutional Process

منسجم را بررسی و در نهایت اقدام به تصمیم‌گیری می‌کند.[1] نظریهٔ انسجام به دنبال این است که مطمئن شود اهداف و نتایج یک سیاست منجر به تضعیف سیاست دیگر نشود.[2]

اتحادیه اروپا از ۲۷ کشور عضو تشکیل شده است و دارای ارکان و نهادهای مختلفی از جمله شورای وزیران، کمیسیون و پارلمان است. با توجه به تعدد حضور دولت‌ها در اتحادیهٔ اروپا دنبال کردن سیاستی واحد و منسجم از جمله در حوزهٔ خارجی نیازمند سازوکاری دقیق است و براساس نظریهٔ انسجام می‌توان مدل سازمان بین دولتی برای اتحادیه اروپا متصور بود. در این مدل اتحادیه اروپا به عنوان یک سازمان بین دولتی در نظر گرفته و فرض می‌شود مشکلاتی که اعضا به تنهایی قادر به حل آنها نیستند، مورد توجه قرار می‌گیرند.

۲. تهدید سایبری

تهدید (Threat) عبارت است از هر آنچه که امنیت را مورد خدشه قرار دهد. حال تهدید سایبری[3] عبارت است از هر اقدامی که بتواند امنیت شبکه و سیستم را به منظور هدفی خاص مورد خدشه قرار دهد. اهداف تهدید سایبری به سه سطح تقسیم می‌شوند: در سطح اول، معمولاً افراد مورد هدف قرار می‌گیرند و اقداماتی از قبیل سرقت هویت یا دسترسی غیرمجاز به اطلاعات شخصی به‌منظور باج خواستن از فرد قربانی را که بیشتر رنگ و بوی مالی دارند، شامل می‌شود. سطح دوم دولت‌ها هستند که هدف، آسیب رساندن به زیرساخت‌های حیاتی یا جاسوسی از آنها با انگیزه‌های سیاسی است. در سطح سوم شرکت‌های بزرگ غیردولتی قرار دارند که هدف از آن ترکیبی از سطح اول و سطح دوم است. تهدیداتی که در سطح فردی صورت می‌گیرند، در بیشتر مواقع در دسته جرائم سایبری[4] قرار می‌گیرند. اما تهدیداتی که در سطح دوم و سوم قرار می‌گیرند، جنبهٔ حمله سایبری[5] دارند. این تهدیدات در قالب حوادث[6] که صورت فنی دارند، از حالت بالقوه به حالت بالفعل در می‌آیند. در ادامه ابتدا حوادث معمول سایبری را معرفی کرده و

1. Portela, C., and K. Raube. "Revisiting Coherence in EU Foreign Policy." *Hamburg Review of Social Sciences* 3, no. 1 (2008),p.2.
2. Koff, Harlan, Antony Challenger, and Israel Portillo. "Guidelines for operationalizing policy coherence for development (PCD) as a methodology for the design and implementation of sustainable development strategies." *Sustainability 12*, no. 10 (2020): 4055,p.1.
3. Cyberthreat
4. Cybercrime
5. Cyberattack
6. Incidents

سپس تهدیدات رایج همانند جرائم سایبری و حمله سایبری در سطح اتحادیه اروپا را مورد بررسی قرار می‌دهیم.

۲.۱. حوادث سایبری

همان‌طورکه در بخش قبل گفته شد، تهدیدات در قالب حوادث از حالت بالقوه به حالت بالفعل در می‌آیند. آژانس امنیت سایبری اتحادیه اروپا پانزده حادثهٔ مربوط به حوزهٔ امنیت سایبری را در سال ۲۰۲۰ بررسی کرده است که عبارت‌اند از: بدافزار، حملات بر پایه وب، فیشینگ، حملات برنامه‌های وب، هرزنامه، حملات محروم سازی از سرویس توزیع شده، سرقت هویت، نقض داده، تهدید داخلی، بات‌نت‌ها، دستکاری فیزیکی/ آسیب/ سرقت/ ضرر، نشت اطلاعات، باج افزار، جاسوسی سایبری و سرقت رمز ارز.[۱]

۲.۲. جرائم سایبری

عموماً جرائم سایبری به طیف گسترده‌ای از فعالیت‌های جنایی مختلف اشاره دارد که در آن رایانه‌ها یا سیستم‌های اطلاعاتی به عنوان ابزار اصلی یا هدف اصلی درگیرند.[۲] مرکز جرائم سایبری اروپایی[۳] جرائم سایبری را به سه دسته جرائم وابسته به سایبر،[۴] بهره‌برداری جنسی از کودکان به‌صورت برخط[۵] و کلاهبرداری برخط تقسیم می‌کند.[۶]

۲.۳. حمله سایبری

حمله سایبری یک حمله IT به یک یا چند سیستم IT دیگر به منظور آسیب‌رساندن به آن در فضای سایبر است.[۷] طیف حملات سایبری از اقداماتی همچون هک‌کردن سایت‌های دولتی و بانک‌ها تا زیرساخت‌های حیاتی همچون نیروگاه‌های اتمی را شامل می‌شود. در سال ۲۰۰۷ مجموعه‌ای از حملات سایبری در استونی رخ داد. هکرها رشته‌ای از حملات انکار سرویس را آغاز کردند که با درخواست‌های پی‌درپی سرورهای آنها به طور موقت از کار افتادند و

1.https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/
2. European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN (2013) 1 final, 7 February 2013.
3. European Cybercrime Centre
4. Cyber-dependent crime
5. Online child sexual exploitation
6. european-cybercrime-centre-ec3, 2021.
7. Federal Ministry of the Interior ,Cyber Security Strategy for Germany, 2011,p.14.

سیستم‌های اطلاعاتی بانک‌ها، خبرگزاری‌ها و سازمان‌های دولتی تحت فشار قرار گرفتند.[1] در سال ۲۰۱۷، باج‌افزاری به عنوان برنامه بروزرسانی نرم‌افزار M.E.Doc که اکثر مشاغل در اوکراین مجبور بودند از آن برای استفاده در پرونده‌های مالیاتی استفاده کنند، پخش شد. در این حمله نه تنها رایانه‌های مشاغل اوکراین آلوده شده بودند، بلکه تعداد قابل توجهی از رایانه‌های شرکت‌های دارای شعبه یا دفاتر در اوکراین نیز آلوده شده‌اند. حدود ۲۰٪ از رایانه‌های آلوده اوکراینی نبودند؛ به عنوان مثال، حدود ۹٪ از کل رایانه‌های آلوده در آلمان بودند که پس از اوکراین با این حمله شدیدترین آسیب را دید.[2] NotPety دو هزار کاربر در سرتاسر جهان را تحت تأثیر قرار داد و تخمین زده می‌شود که نزدیک به ۲/۱ میلیارد دلار به شرکت‌ها ضرر رسانده است.[3] باج‌افزار WannaCry در طی حملهٔ گسترده به چندین کشور در سال ۲۰۱۷ مشاهده شد. براساس چندین گزارش از متخصصان امنیت شبکه، در مجموع ۳۰۰۰۰۰ سیستم در بیش از ۱۵۰ کشور به شدت آسیب دیدند. این حمله دامنهٔ گسترده‌ای از بخش‌ها از جمله بهداشت، دولت، ارتباطات از راه دور و انرژی را شامل شد.[4] در انگلستان ۸۰ سرویس بهداشت ملی[5] به طور موقت قطع شدند و وقت‌های ملاقات برخط پزشکی نیز به مدت یک هفته به تعویق افتادند. پرونده‌های پزشکی آلوده و از دسترس خارج شدند. اگرچه WannaCry به طور خاص سیستم‌های کنترل صنعتی را هدف قرار نداده بود، تعدادی از سیستم‌های کنترل صنعتی تحت تأثیر قرار گرفتند. شرکت‌های مختلف در صنایع مختلف کنترل فرایندهای صنعتی خود را از دست دادند که شرکت فرانسوی رنو نمونه‌ای از آن است.[6] این سه مورد از مهم‌ترین حملات سایبری بوده که در سال‌های اخیر در سطح اتحادیه اروپا رخ داده‌اند؛ درحالی‌که تعداد حملات سایبری در اروپا سال به سال در حال افزایش است؛ به عنوان مثال در سال ۲۰۲۰، ۷۵۶ مورد حمله سایبری اتفاق افتاده است؛ درحالی‌که این رقم در سال ۲۰۱۹، ۴۳۲ مورد بوده است.[7]

1. Camino Mortera-Martinez. *Game over? Europe's cyber problem*. CENTRE FOR EUROPEAN REFORM, 2018,p3.
2. Team GAIT ELEC-E7470 – Cybersecurity,2017, p.4.
3. Camino Mortera-Martinez. *Game over? Europe's cyber problem*. CENTRE FOR EUROPEAN REFORM, 2018,p5.
4. Akbanov, Maxat, Vassilios G. Vassilakis, and Michael D. Logothetis. "WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms." *Journal of Telecommunications and Information Technology*, 2019,p114.
5. National Health Service (NHS)
6. eucyberdirect.eu/2017-wannacry.
7. https://www.bbc.com/news/technology-57583158

۳. بازیگران مؤثر

در سطح اتحادیه اروپا آژانس‌ها، مؤسسات و نهادها با توجه به ماهیت خود به ایفای نقش در زمینهٔ امنیت سایبری می‌پردازند و اتحادیه از طریق آنها آن دسته از اقداماتی را که به منظور مقابله با تهدیدات سایبری وضع کرده است، اعمال می‌کند. نزدیک به ۲۲ نهاد مرتبط در اتحادیه اروپا وجود دارند که به‌صورت مستقیم و غیرمستقیم در حوزهٔ امنیت سایبری فعالیت می‌کنند و در ادامه فقط مهم‌ترین آنها را بررسی می‌کنیم.

۳.۱. آژانس دفاع اتحادیه اروپا (EDA[1])

آژانس دفاع اتحادیه اروپا بر اساس اقدام مشترک شورای وزیران در ۱۲ جولای ۲۰۰۴ تشکیل شد. مأموریت‌های آژانس عبارت‌اند از:

- پشتیبانی از توسعهٔ توانایی‌های دفاعی و همکاری نظامی میان دولت‌های عضو اتحادیه اروپا؛
- بازیابی فناوری و تحقیق دفاعی و تقویت صنایع دفاعی اروپایی؛
- اقدام به عنوان رابط نظامی با سیاست‌گذاری‌های اتحادیه اروپا.

آژانس دفاع اتحادیه اروپا به‌عنوان یک کاتالیزور عمل می‌کند. همکاری‌ها را تقویت می‌کند، ابتکارات جدیدی راه‌اندازی می‌کند و راه‌حل‌هایی به منظور توسعه دفاع معرفی می‌کند.[2]

۳.۲. آژانس امنیت سایبری اتحادیه اروپا(ENISA[3])

آژانس امنیت سایبری اتحادیه اروپا به منظور رسیدن به سطح بالای امنیت سایبری در اروپا به‌وجود آمده است. این آژانس در سال ۲۰۰۴ تشکیل شد و به‌وسیلهٔ فرمان امنیت سایبری اتحادیه اروپا تقویت گردید.[4] آژانس در سیاست‌گذاری سایبری اتحادیه مشارکت می‌کند، قابلیت اطمینان محصولات، خدمات و فرایندهای ICT را با صدور گواهینامه افزایش می‌دهد، با نهادها و دولت‌های عضو اتحادیه همکاری می‌کند و برای آمادگی در برابر چالش‌های آینده سایبری کمک می‌کند. از طریق به اشتراک گذاشتن دانش، ظرفیت‌سازی و افزایش آگاهی، آژانس به همراه

1. European Defence Agency
2.https://eda.europa.eu/what-we-do/all-activities/activities-search/cyber-defence,2021.
3. European Union Agency for Cybersecurity
4. THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, REGULATION on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (Cybersecurity Act), 2019/ 881, 17 April 2019.

شرکای کلیدی خود به منظور افزایش اعتماد در اقتصاد بهم پیوسته همکاری می‌کند تا تاب‌آوری زیرساخت‌های اتحادیه تقویت و سرانجام جامعه و شهروندان اروپایی در دنیای دیجیتال ایمن شوند. از جمله کارکردهای آژانس امنیت سایبری اتحادیه اروپا می‌توان به تقویت جوامع، سیاست‌گذاری در زمینهٔ امنیت سایبری، همکاری عملیاتی، ظرفیت‌سازی، ارائهٔ راه‌حل‌های قابل اطمینان، آینده‌نگری و اتکا به دانش نام برد.[1]

۳.۳. سرویس اقدام خارجی اروپایی(EEAS)[2]

سرویس اقدام خارجی اتحادیه اروپا، سرویس دیپلماتیک اتحادیه اروپا است که در ۱ دسامبر ۲۰۱۰ تأسیس شده است و به نمایندهٔ عالی اتحادیه اروپا در امورخارجی و سیاست‌گذاری امنیتی کمک می‌کند. جنبهٔ کلیدی کارکرد EEAS توانایی همکاری نزدیک با وزارتخانه‌های دفاع و خارجه دولت‌های عضو اتحادیه اروپا و سایر نهادهای اتحادیه از جمله کمیسیون، شورا و پارلمان اروپایی و همچنین سازمان ملل متحد و سایر سازمان‌های بین‌المللی است.[3] در ۱۴ مارس ۲۰۱۷، سرویس اقدام خارجی اتحادیه اروپا و کمیسیون اروپایی سند واکنش مشترک دیپلماتیک اتحادیه در برابر عملیات سایبری را (جعبه ابزار دیپلماسی سایبری)[4] منتشر کردند. این جعبه ابزار شامل اقدامات دیپلماتیک درون اتحادیه اروپا در زمینهٔ سیاست خارجی و امنیتی مشترک است که در برابر عملیات‌های مخرب سایبری به کار گرفته می‌شوند. تفسیر شورا از اینکه در عمل جعبه ابزار شامل چه چیزهایی است مشخص نیست، اما بیان می‌کند که در صورت لزوم، اقدامات می‌توانند محدودکننده باشند. همچنین عنوان شده است که پاسخ متناسب با محدوده، مقیاس، مدت زمان، شدت، پیچیدگی و تأثیر فعالیت سایبری خواهد بود. اصطلاحاتی که به کار رفته، نشان می‌دهد که این ابزارهای دیپلماتیک می‌توانند چیزی بین اظهارات محکوم‌کننده تا موارد قهری مانند اعمال تحریم‌ها باشند. سند چارچوب واکنش مشترک دیپلماتیک اتحادیه اروپا از دولت‌های عضو، سرویس اقدام خارجی اروپایی و کمیسیون می‌خواهد در توسعهٔ چارچوب واکنش مشترک دیپلماتیک اتحادیه در برابر فعالیت‌های مخرب، اثرگذاری کامل داشته باشند و در این زمینه

1. https://www.enisa.europa.eu/about-enisa,2021.
2. European External Action Service
3. https://eeas.europa.eu/headquarters/headquarters-homepage/82/about-european-external-action-service-eeas_en,2021.
4. Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")

مجدداً تعهد خود را برای ادامه کار در این چارچوب با همکاری کمیسیون، EEAS و سایر طرف‌های ذی‌ربط از طریق تنظیم دستورالعمل‌های اجرایی، از جمله اقدامات مقدماتی و روش‌های ارتباطی و آزمایش آنها از طریق اقدامات مناسب، تأیید می‌کند.[1]

۳.۴. تیم واکنش سریع رایانه‌ای اتحادیه اروپا (CERT-EU)

نهادهای اتحادیه اروپا در ۱۱ سپتامبر ۲۰۱۲ تصمیم به ایجاد یک تیم واکنش سریع رایانه‌ای به طور دائم برای نهادها، آژانس‌ها و بخش‌های اتحادیه گرفتند. این تیم متشکل از کارشناسان امنیت فناوری نهادهای اصلی اتحادیه اروپا (کمیسون اروپایی، دبیرخانه شورا، پارلمان اروپایی، کمیته مناطق و کمیته اقتصادی و اجتماعی) است و با سایر بخش‌های عمومی و خصوصی در زمینهٔ امنیت فناوری اطلاعات همکاری نزدیکی دارد. CERT-EU براساس الزامات مؤسسان خود و با در نظر گرفتن صلاحیت‌ها، منابع و مشارکت‌های موجود خدمات خود را به تدریج گسترش می‌دهد[2]مأموریت CERT-EU کمک به زیرساخت امنیت فناوری اطلاعات و ارتباطات[3] تمام مؤسسات و آژانس‌های اتحادیه اروپا به‌وسیله پیشگیری، تشخیص، کاهش و پاسخ به حملات سایبری است. CERT-EU به‌عنوان مرکز تبادل امنیت سایبری اطلاعات و هماهنگی واکنش به حوادث برای تمام مؤسسات و نهادهای اتحادیه اروپا است و در صورت ضرورت اطلاعاتی پیرامون تهدید، آسیب‌پذیری و حوادث برای مؤسسان جمع‌آوری می‌کند.

فعالیت‌های CERT-EU شامل پیشگیری، تشخیص، واکنش و بازیابی است. تیم واکنش سریع رایانه‌ای براساس ارزش‌های کلیدی زیر عمل می‌کند:

- بالاترین استانداردهای اخلاقی؛[4]
- درجه بالایی از ارائهٔ خدمات و آمادگی عملیاتی؛
- واکنش مؤثر در برابر حوادث و شرایط اضطرار و تعهد حداکثری نسبت به حل مشکلات؛
- ساخت و تکمیل قابلیت‌های موجود؛
- فراهم کردن تبادل روش‌ها میان اعضا و مؤسسات همتا.[5]

1. https://ccdcoe.org/uploads/2018/11/EU-170607-CyberDiplomacyToolbox-1.pdf.2018.
2. cert_about.html//cert.europa.eu.2021.
3. information and communication technology
4. Ethical Integrity
5. Bada, Maria, Sadie Creese, Michael Goldsmith, Chris Mitchell, and Elizabeth Phillips. "Computer Security Incident Response Teams (CSIRTs): An Overview." The Global Cyber Security Capacity Centre(2014).

۳.۵. مرکز جرائم سایبری اروپایی(EC3)

نوآوری فنی را به همان اندازه که می‌توان برای خیر عمومی استفاده کرد، برای اهداف ناپسند نیز می‌توان مورد استفاده قرار داد. امروزه جرائم اینترنتی بیش از هر نوع جرم دیگری وجود دارند و به همین دلیل آژانس اتحادیه اروپا برای همکاری در اجرای قانون(EUROPL)[1] و سازمان‌های همتای آن با این جرائم مبارزه می‌کنند. جرم سایبری یک مشکل روبه‌رشد برای کشورها از جمله دولت‌های عضو اتحادیه اروپا است که دارای زیرساخت‌های اینترنت توسعه‌یافته و سیستم پرداخت برخط می‌باشد. نه تنها داده‌های مالی بلکه به طور عمومی‌تر، داده‌ها هدف جرائم سایبری هستند. شمار نقض و رخنه به داده‌ها در حال افزایش است که این امر منجر به کلاهبرداری می‌شود.

EC3 بر سه حوزهٔ اصلی متمرکز است که عبارت‌اند از: جرائم سایبری که توسط گروه‌های سازمان‌یافته انجام می‌شوند (به‌خصوص گروه‌هایی که سودهای بزرگ جنایی ایجاد می‌کنند، همانند کلاهبرداری برخط)؛ جرائم سایبری که صدمات جدی به قربانیان وارد می‌کند (مانند بهره‌برداری جنسی از کودکان) و جرائم سایبری که زیرساخت‌های حیاتی و سیستم‌های اطلاعاتی اتحادیه اروپا را تحت تأثیر قرار می‌دهند (مانند حملات سایبری). EC3 به عنوان مرکز اصلی اطلاعات عمل می‌کند و با استفاده از تجزیه و تحلیل عملیاتی، هماهنگی و تخصص از عملیات و تحقیقات کشورهای عضو پشتیبانی کرده، تحلیل‌های راهبردی متنوعی ارائه می‌دهد. علاوه بر این، EC3 از آموزش و ظرفیت‌سازی پشتیبانی می‌کند و جامعهٔ ضابطین قضایی اتحادیه اروپا در حوزه‌های منافع مشترک همانند تحقیق و توسعه، الزامات، حکمرانی اینترنت و توسعه سیاست‌گذاری را نمایندگی می‌کند.[2]

۴. اقدامات

اتحادیه اروپا به منظور مقابله با تهدیدات و چالش‌های امنیت سایبری اقداماتی انجام داده است که این اقدامات در ذیل مواردی همچون افزایش تاب‌آوری سایبری، مقابله با جرائم

1. The European Union Agency for Law Enforcement Cooperation
2. Thygesen Vendius, Trine. "Europol's Cybercrime Centre (EC3), its Agreements with Third Parties and the Growing Role of Law Enforcement on the European Security Scene|." EJPS 3, no. 2 (2015), p 151.

سایبری، تقویت دیپلماسی سایبری، دفاع سایبری، تحقیق و نوآوری و حفاظت از زیرساخت‌های حیاتی بوده است. در ادامه اقدامات صورت‌گرفته را در حوزهٔ امنیت سایبری توسط اتحادیه اروپا بررسی می‌کنیم. اما قبل از آن توضیح مختصری در مورد قانون‌گذاری در اتحادیه اروپا و انواع آن ارائه می‌کنیم.

هر اقدامی که اتحادیه اروپا انجام دهد، بر اساس معاهدات است. این توافقنامه‌های الزام‌آور میان دولت‌های عضو اتحادیه اروپا اهداف اتحادیه اروپا، قوانین مربوط به نهادهای اتحادیه اروپا، نحوهٔ تصمیم‌گیری و روابط بین اتحادیه اروپا و اعضای آن را مشخص می‌کند. معاهدات نقطه شروع حقوق اتحادیه اروپا هستند و در اتحادیه اروپا به عنوان حقوق اولیه[1] شناخته می‌شوند. مجموعه حقوقی که از اصول و اهداف معاهدات ناشی می‌شود، حقوق ثانویه نامیده می‌شوند و شامل مقررات،[2] دستورالعمل‌ها،[3] تصمیمات،[4] توصیه‌ها[5] و نظرات[6] است.

معاهدات اهداف اتحادیه اروپا، قوانین نهادهای اتحادیه اروپا، نحوهٔ تصمیم‌گیری و روابط بین اتحادیه اروپا و دولت‌های عضو آن را تعیین می‌کند. گاهی معاهدات اتحادیه اروپا برای اصلاح نهادهای اتحادیه اروپا و ایجاد مسئولیت‌های جدید به آن اصلاح می‌شوند. این معاهدات توسط همه کشورهای اتحادیه اروپا مورد مذاکره و توافق قرار می‌گیرند و سپس توسط پارلمان‌های آنها تصویب می‌شود. از سوی دیگر مقررات، قوانین حقوقی هستند که به محض لازم‌الاجرا شدن بدون نیاز به انتقال به قوانین ملی، به طور خودکار و یکنواخت برای همه کشورهای اتحادیه اروپا اعمال می‌شوند. آنها به طور کامل برای همه کشورهای اتحادیه اروپا لازم‌الاجرا هستند. دستورالعمل‌ها، کشورهای اتحادیه اروپا را ملزم می‌کنند که به نتیجهٔ مطمئنی برسند، اما آنها را در انتخاب نحوهٔ انجام این کار آزاد می‌گذارند. کشورهای اتحادیه اروپا باید به منظور دستیابی به اهداف تعیین‌شده در دستورالعمل، اقداماتی را برای وارد کردن آنها به قوانین ملی انجام دهند و مقامات ملی باید این اقدامات را به کمیسیون اروپا اعلام کنند. تصمیمات در کل لازم‌الاجرا هستند؛ اما تصمیمی که مشخص‌کنندهٔ کسانی است که برای آنها منظور شده، فقط برای آنها

1. primary law
2. regulations
3. directives
4. decisions
5. recommendations
6. opinions

لازم‌الاجرا است. توصیه‌ها به نهادهای اتحادیه اروپا اجازه می‌دهند تا دیدگاه‌های خود را اعلام کنند و بدون اعمال هیچ‌گونه تعهد قانونی به کسانی که خطاب به آنها خط مشی را پیشنهاد می‌دهند، این کار را انجام دهند. توصیه‌ها جنبهٔ الزام‌آور ندارند. نظر ابزاری است که به نهادهای اتحادیه اروپا اجازه می‌دهد بدون ارائهٔ هیچ گونه تعهد قانونی به موضوع نظر، اظهارنظر کنند. یک نظر فاقد جنبهٔ الزام آور است.[1]

۴.۱. افزایش تاب‌آوری سایبری

۴.۱.۱. راهبرد امنیت سایبری ۲۰۱۳

اتحادیه اروپا در ۷ فوریه ۲۰۱۳ اولین راهبرد امنیت سایبری را منتشر کرد که مهم‌ترین گام در زمینهٔ سیاست‌گذاری امنیت سایبری در آن زمان به‌شمار می‌آمد. شعار این راهبرد فضای سایبر باز، ایمن و امن است. در این راهبرد بر حفاظت از حقوق بنیادی، دموکراسی و حاکمیت قانون در فضای سایبر اشاره شده است. از این رو نیاز است که از فضای سایبر در برابر حوادث و فعالیت‌های مخرب حفاظت شود. دولت‌ها در جهت فضای سایبر ایمن و امن نقش اصلی و وظایف متعددی دارند که از جمله آنها می‌توان به دسترسی مطمئن و باز، رعایت و حمایت از حقوق اساسی به‌صورت برخط و حفظ قابلیت اطمینان و همکاری اینترنت اشاره کرد. در کنار حکومت، بخش خصوصی نیز نقش مهمی در فضای سایبر دارد.[2]

در مقدمهٔ راهبرد به منافع بی‌شمار جهان دیجیتال اشاره شده است که درکنار آن، آسیب‌پذیری نیز با خود به همراه دارد. به عنوان مثال، اقتصاد اتحادیه اروپا به‌وسیلهٔ فعالیت‌های جرائم سایبری آسیب دیده است. اینترنت بدون مرز و چندلایه به یکی از قدرتمندترین ابزار برای پیشرفت جهانی بدون نظارت و مقررات دولتی تبدیل شده است؛ درحالی‌که بخش خصوصی باید به نقش پیشتاز خود برای مدیریت سازنده اینترنت ادامه دهد، نیاز به الزامات شفافیت، پاسخگویی و امنیت بیش از پیش از اهمیت برخوردار می‌شوند. راهبرد ۲۰۱۳ اصولی را که باید در سیاست‌گذاری امنیت سایبری در سطح اتحادیه اروپا و بین‌المللی لحاظ شوند، مشخص می‌کند. این اصول عبارت‌اند از:

1. www.ec.europa.eu/ law/law-making-process.2021.
2. European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN (2013) 1 final, 7 February 2013,p.2.

- ارزش‌های اصلی اتحادیه اروپا در دنیای دیجیتال به اندازه دنیای فیزیکی کاربرد دارند و قابل اعمال هستند؛
- حفاظت از حقوق بنیادین، آزادی بیان و داده‌های شخصی و خصوصی؛
- دسترسی برای همه؛
- حکمرانی دموکراتیک و کارآمد؛
- مسئولیت مشترک جهت اطمینان از امنیت.[1]

براساس راهبرد ۲۰۱۳ پنج اولویت راهبردی عبارت‌اند از: دستیابی به تاب‌آوری سایبری، کاهش (چشمگیر) جرائم سایبری، توسعه سیاست‌ها و ظرفیت‌های مربوط به سیاست‌گذاری دفاعی و امنیتی مشترک، تقویت منابع صنعتی و فناوری مرتبط با امنیت سایبری و تشکیل سیاست‌گذاری بین‌المللی فضای سایبر منسجم برای اتحادیه اروپا و ترویج ارزش‌های حیاتی اتحادیه.[2]

۴.۱.۲. بازبینی راهبرد امنیت سایبری ۲۰۱۷

در سپتامبر۲۰۱۷ و به منظور توسعه حفاظت از زیرساخت‌های حیاتی اروپایی و تقویت اعتبار دیجیتالی اروپا نسبت به سایر نقاط جهان، بازبینی در راهبرد امنیت سایبری ۲۰۱۳ صورت گرفت. [3]در این بازبینی طرح پیشنهادی برای مقررات فرمان امنیت سایبری، تقویت مأموریت ENISA و اطمینان از واکنش‌های مؤثر دولت‌های عضو در برابر حملات مورد بحث قرار گرفته‌اند. بر اساس متن منتشرشده، مقررات پیشنهادی مجموعه‌ای جامع از اقدامات را ارائه می‌دهند که بر اساس اقدامات قبلی ایجاد شده و اهداف خاصی را تقویت می‌کنند.

۴.۱.۳. راهبرد امنیت سایبری ۲۰۲۰

در ۱۶ دسامبر ۲۰۲۰، کمیسیون و نماینده عالی اتحادیه در امور خارجه و سیاست امنیتی، نامه مشترک خود را با عنوان «راهبرد امنیت سایبری اتحادیه اروپا برای دهه دیجیتال»[4] به پارلمان و

1. European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN (2013) 1 final, 7 February 2013, pp3-4.
2. European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN (2013) 1 final, 7 February 2013,p p4-5.
3. Bendiek, Annegret, Raphael Bossong, and Matthias Schulze. "The EU's revised cybersecurity strategy: half-hearted progress on far-reaching challenges." (2017): 7,p.1
4. The EU's Cybersecurity Strategy for the Digital Decade

شورای اروپا منتشر کردند. هدف از راهبرد جدید امنیت سایبری تقویت تاب‌آوری جمعی اروپا در برابر تهدیدات سایبری و اطمینان از این که همه شهروندان و مشاغل می‌توانند از خدمات و ابزارهای دیجیتالی قابل اعتماد بهره‌مند شوند، است.[1]

این راهبرد از چهار قسمت تشکیل شده است که در ادامه هریک از آنها را بررسی می‌کنیم. قسمت اول مقدمه راهبرد است و مشکلات موجود در حوزهٔ امنیت سایبری در اتحادیه اروپا را مطرح می‌کند. به طور کلی این مشکلات عبارت‌اند از:

- اتکای بخش‌های حمل و نقل، انرژی، سلامت، مخابرات، مالیه، امنیت، فرایندهای دموکراتیک، فضایی و دفاعی به سیستم‌های شبکه و اطلاعاتی که به طور روزافزون به یکدیگر وابسته می‌شوند؛
- ترکیب چشم‌انداز تهدید با تنش‌های ژئوپلیتیکی بر سر اینترنت جهانی و باز و کنترل فناوری‌ها در کل زنجیره تأمین؛
- هدف قرار دادن مخرب زیرساخت‌های حیاتی به عنوان یک خطر بزرگ جهانی؛
- نگرانی در مورد امنیت به عنوان عامل مهمی برای استفاده از خدمات برخط؛
- نقش پررنگ فضای دیجیتال در انواع جرائم؛
- پایین بودن سطح آمادگی و آگاهی سایبری در بین مشاغل و افراد با وجود اینکه خدمات دیجیتالی و بخش دارایی یکی از شایع‌ترین اهداف حملات سایبری هستند؛
- فقدان آگاهی موقعیتی جمعی از تهدیدات سایبری در اتحادیه اروپا.

قسمت دوم تحت عنوان جهانی فکر کن و اروپایی عمل‌کن[2] است. این قسمت به سه بخش تاب‌آوری، حاکمیت فناورانه و رهبری، ایجاد ظرفیت عملیاتی جهت پیشگیری، بازدارندگی و واکنش و پیشبرد فضای سایبر جهانی و باز تقسیم شده‌اند و هر کدام از این بخش‌ها دارای زیر بخش‌های متعددی است. شایان ذکر است، اتحادیه اروپا متعهد است از این راهبرد به عنوان بخشی از سیاست‌های جدید فناوری و صنعتی از طریق سرمایه‌گذاری بی‌سابقه در انتقال دیجیتال

1. European Council conclusions Draft EU Council conclusions.2021,p.1.
2. THINKING GLOBAL, ACTING EUROPEAN

اتحادیه اروپا طی هفت سال آینده حمایت کند.[1] امنیت سایبری در مؤسسات، نهادها و آژانس‌های اتحادیه اروپا قسمت سوم راهبرد ۲۰۲۰ را تشکیل می‌دهد. مؤسسات، نهادها و آژانس‌های اتحادیه اروپا با توجه به مشخصات سیاسی، مأموریت‌های مهم برای هماهنگی موضوعات بسیار حساس و ایفای نقش در مدیریت منابع کلان مالی، هدف دائمی حملات سایبری، به ویژه جاسوسی سایبری هستند. با این‌حال، میزان تاب‌آوری سایبری و توانایی تشخیص و پاسخ به فعالیت‌های سایبری مخرب از نظر رشد در این واحدها به طور قابل توجهی متفاوت است. بنابراین لازم است که سطح کلی امنیت سایبری از طریق قوانین سازگار و همگن ارتقا داده شود. در زمینهٔ امنیت اطلاعات، پیشرفت‌هایی در راستای سازگاری بیشتر قوانین حفاظت از اطلاعات طبقه‌بندی‌شده اتحادیهٔ اروپا و اطلاعات حساس غیر طبقه‌بندی شده صورت گرفته است. با این‌حال، قابلیت همکاری سیستم‌های اطلاعات طبقه‌بندی شده همچنان محدود است و از انتقال یکپارچه اطلاعات بین نهادهای مختلف جلوگیری می‌کند. به منظور اجرای رویکردی بین نهادی به منظور رسیدگی به اطلاعات طبقه‌بندی‌شده اتحادیه اروپا و اطلاعات غیر طبقه‌بندی‌شدهٔ حساس، باید پیشرفت‌های بیشتری صورت بگیرد. از سوی دیگر، تقویت CERT-EU با مکانیزم بودجه بهبودیافته برای افزایش توانایی آن در کمک به مؤسسات، نهادها و آژانس‌های اتحادیه اروپا برای اعمال قوانین جدید امنیت سایبری و ارتقای تاب‌آوری سایبری آنها ضروری است.[2]

در انتهای راهبرد۲۰۲۰(قسمت چهارم)، نتیجه‌گیری شده است که اجرای متمرکز این سند به دهه دیجیتالی ایمن سایبری اتحادیه اروپا، دستیابی به امنیت اتحادیه و تقویت موقعیت جهانی اتحادیه اروپا کمک خواهد کرد. از طرفی، اتحادیه اروپا به منظور راه‌حل‌های جهانی و استانداردهای امنیت سایبری سرویس‌های ضروری و زیرساخت‌های حیاتی باید استانداردها و هنجارهایی را پیش ببرد. کمیسیون و نماینده عالی در راستای صلاحیت‌های خود اقداماتی از قبیل نظارت بر پیشرفت‌های ذیل راهبرد، توسعهٔ معیارها و ضوابط برای ارزیابی، تداوم ارتباط با دولت‌های عضو برای شناسایی اقدامات عملی به منظور اتصال چهار جامعهٔ امنیت سایبری شامل

1. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade.2020, p4-5. JOIN/2020/18 final

2. Ipid, p24. JOIN/2020/18 final.

زیرساخت‌های حیاتی و بازار داخلی، مجریان قضا و قانون، دیپلماسی سایبری و دفاع سایبری و تعامل با جامعهٔ ذی‌نفعان را انجام خواهند داد.[1]

۴.۱.۴. فرمان امنیت سایبری اتحادیه اروپا

در بخش‌های پیشین به این نکته اشاره شد که در بازبینی راهبرد امنیت سایبری اتحادیه اروپا (۲۰۱۷)، طرحی بر پایهٔ افزایش مأموریت و اختیارت ENISA و صدور گواهینامه در سراسر اتحادیه اروپا پیشنهاد شد که در سال ۲۰۱۹ تحت عنوان فرمان امنیت سایبری اتحادیه اروپا لازم‌الاجرا گردید. این فرمان از ۶ فصل، ۴ عنوان و ۶۹ ماده تشکیل شده است و بخش دوم فرمان به تقویت نقش و اختیارات ENISA اختصاص یافته است.[2]

۴.۱.۵. دستورالعمل سیستم‌های شبکه و اطلاعات(۲۰۱۶)

در سال ۲۰۱۶ به منظور افزایش همکاری میان دولت‌های عضو پیرامون مسائل مهم امنیت سایبری، دستورالعمل سیستم‌های شبکه و اطلاعات به عنوان اولین اقدام قانون‌گذاری در سراسر اروپا منتشر شد. این دستورالعمل تعهدات امنیتی برای اپراتورهای خدمات حیاتی در بخش‌های مهم مانند انرژی، حمل و نقل، بهداشت و مالی و ارائه‌دهندگان سرویس‌های دیجیتال مانند بازارهای برخط، موتورهای جستجو و خدمات ابری تعیین کرده است. هدف از این دستورالعمل افزایش و هماهنگ‌سازی سطح امنیت سایبری در میان دولت‌های عضو است. به منظور توسعهٔ کارکرد بازار داخلی به‌وسیلهٔ اعتمادسازی، دولت‌های عضو باید بتوانند با بازیگران اقتصادی همکاری مؤثری داشته باشند و بر اساس آن این همکاری را ساختاربندی کنند.[3]

این دستورالعمل از ۷ فصل و ۲۷ ماده به همراه ۳ ضمیمه تشکیل شده است و براساس آن سه گروه باید از آن پیروی کنند؛ این سه گروه عبارت‌اند از: دولت‌های عضو اتحادیه اروپا، اپراتورهای خدمات حیاتی و ارائه‌دهندگان سرویس‌های دیجیتال. اپراتورهای خدمات حیاتی شرکت‌هایی هستند که در زمینه‌هایی همچون انرژی، حمل و نقل، بانکداری، زیرساخت بازار

1. Ipid, p25. JOIN/2020/18 final.
2. THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, REGULATION on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (Cybersecurity Act), 2019/ 881, 17 April 2019.
3. THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, concerning measures for a high common level of security of network and information systems across the Union (NIS Directive), 2016/1148, 6 July 2016.

مالی، بخش بهداشت، تأمین و توزیع آب آشامیدنی و بخش‌های زیرساخت دیجیتال فعالیت می‌کنند. درحالی‌که ارائه‌دهندگان سرویس‌های دیجیتال مشاغل دیجیتالی هستند که در مورد امنیت سایبری از اهمیت عمومی برخوردارند و از جملهٔ آنها می‌توان به موتورهای جستجو و خدمات رایانش ابری اشاره کرد.

۴.۱.۶. طرح پیشنهادی بازبینی دستورالعمل سیستم‌های شبکه و اطلاعات (۲۰۲۰)

در دسامبر۲۰۲۰، کمیسیون اروپایی بازبینی دستورالعمل سیستم‌های شبکه و اطلاعات را پیشنهاد کرد. طرح پیشنهادی جدید در واکنش به تکامل چشم‌انداز تهدیدات و در نظر گرفتن تحول دیجیتالی جامعه است که با وجود بحران کرونا نیز سرعت پیدا کرده است. قوانین جدید شامل مواردی از جمله:

- تقویت تعهدات امنیتی برای شرکت‌ها؛
- تأکید بر امنیت زنجیره‌های عرضه؛
- معرفی اقدامات نظارتی بیشتر برای مقامات ملی؛
- افزایش به اشتراک گذاشتن اطلاعات و همکاری خواهند بود.[1]

این طرح پیشنهادی بر اساس چندین حوزهٔ اصلی سیاست‌گذاری شده است که به هم مرتبط‌اند و هدف آنها افزایش سطح امنیت سایبری در اتحادیه است.

۴.۲. مقابله با جرائم سایبری

۴.۲.۱. مقابله با کلاهبرداری در پرداخت غیرنقدی[2]

کلاهبرداری و تقلب با ابزارهای پرداخت غیرنقدی تهدیدی جدی برای امنیت اتحادیه اروپا بوده و درآمد قابل توجهی برای جرائم سازمان‌یافته ایجاد می‌کند. علاوه بر این، این نوع تقلب بر اعتماد مصرف‌کنندگان به امنیت فناوری‌های دیجیتال تأثیر می‌گذارد. در آوریل ۲۰۱۹، اتحادیه اروپا قوانین جدیدی را برای مبارزه با تقلب در پرداخت غیرنقدی تصویب کرد که دولت‌های عضو باید قوانین جدید را در سال ۲۰۲۱ اجرا کنند. این بخشنامه قوانین موجود را به‌روز می‌کند تا اطمینان حاصل شود که یک چارچوب حقوقی روشن، قوی و خنثی از فناوری وجود دارد.

1. www.consilium.europa.eu/en/policies/cybersecurity, 2021
2. Tackling non-cash payment fraud

همچنین از موانع عملیاتی که مانع تحقیقات و تعقیب می‌شوند، جلوگیری می‌کند و اقداماتی را برای افزایش آگاهی عمومی از تکنیک‌های کلاهبرداری مانند فیشینگ یا اسکیمینگ پیش‌بینی می‌نماید. هدف این دستورالعمل این است که فناوری–خنثی[1] باشد و نه تنها پرداخت‌های غیرنقدی سنتی مانند کارت‌های بانکی یا چک‌ها را شامل شود، بلکه روش‌های جدیدی برای پرداخت که در سال‌های اخیر ظاهر شده‌اند، مانند کیف پول الکترونیکی، پرداخت تلفن همراه و ارزهای مجازی را در برگیرد.

۴.۲.۲. عدالت و اجرای قانون

قوانین و سیاست‌های اتحادیه اروپا با ابعاد عدالت و اجرای قانون در مبارزه با جرائم سایبری و جرائم به طور کلی مانند دسترسی به شواهد الکترونیکی، رمزگذاری و نگهداری داده‌ها سر و کار دارد. در مورد دسترسی به شواهد الکترونیکی، مجرمان از فناوری دیجیتال برای ارتکاب جرائم و پنهان کردن فعالیت‌های غیرقانونی سوءاستفاده می‌کنند. بنابراین مقامات انتظامی و قضایی برای تحقیقات و تعقیب جنایی خود بیشتر به شواهد الکترونیکی مانند پیامک‌ها، ایمیل‌ها یا برنامه‌های پیام‌رسانی تکیه می‌کنند. از سوی دیگر، اتحادیه اروپا برای تسهیل دسترسی فرامرزی به شواهد الکترونیکی به منظور رسیدگی به پرونده‌های مجرمانه، در حال مذاکره برای دستیابی به توافق با ایالات متحده به عنوان کشوری است که بیشتر ارائه‌دهندگان خدمات در آن مستقرند.

از سوی دیگر، اتحادیه اروپا در تلاش است تا یک بحث فعال با صنعت فناوری ایجاد کند تا تعادل مناسبی میان اطمینان از استفاده مستمر از فناوری رمزگذاری قوی و تضمین اختیارات مجریان قانون و قوه قضائیه برای کار با شرایط مشابه در دنیای آفلاین برقرار شود. در دسامبر ۲۰۲۰، شورا قطعنامه‌ای را در مورد رمزگذاری تصویب کرد[2] که نیازهای امنیت به‌وسیلهٔ رمزگذاری و امنیت با وجود رمزگذاری[3] را برجسته می‌کند.

به منظور مبارزهٔ مؤثر با جرائم امروزی، مهم است که ارائه‌دهندگان خدمات، داده‌های خاصی را که می‌توانند تحت شرایط سخت برای مقابله با جرم و جنایت افشا شوند، حفظ کنند. با این حال، حفظ داده‌ها می‌تواند حقوق اساسی افراد، به ویژه حقوق حفظ حریم خصوصی و حفاظت از

1. technology-neutral
2. Council Resolution on Encryption - Security through encryption and security despite encryption, 24 November 2020.
3. security through encryption and security despite encryption

اطلاعات شخصی را نقض کند. شورا تفاسیری را در خصوص حفظ داده‌های ارتباطات الکترونیکی به منظور مبارزه با جرم و جنایت تصویب کرد. شورا کمیسیون را موظف کرد تا اطلاعات بیشتری را جمع‌آوری کرده و مشاوره‌های هدفمند را به عنوان بخشی از یک مطالعهٔ جامع در مورد راه‌حل‌های احتمالی برای حفظ داده‌ها، از جمله در نظر گرفتن ابتکار قانون‌گذاری آینده، سازماندهی کند.

۴.۳. تقویت دیپلماسی سایبری

اتحادیه اروپا و دولت‌های عضو آن از فضای سایبری باز، آزاد، با ثبات و امن که در آن حقوق بشر، آزادی‌های اساسی و حاکمیت قانون برای ثبات اجتماعی، رشد اقتصادی، رفاه و یکپارچگی جوامع آزاد و دموکراتیک کاملاً رعایت می‌شوند، حمایت می‌کنند. اتحادیه اروپا تلاش زیادی برای محافظت از خود در برابر تهدیدات سایبری از سوی کشورهای ثالث انجام می‌دهد، یکی از این تلاش‌ها «جعبه ابزار دیپلماسی سایبری»[1] است. این جعبه ابزار شامل همکاری و گفتگوی دیپلماتیک، اقدامات پیشگیرانه در برابر حملات سایبری و تحریم است.

۴.۳.۱. جعبه ابزار دیپلماسی

از آنجا که یک رویکرد مشترک و جامع توسط اتحادیه اروپا برای دیپلماسی سایبری می‌تواند به پیشگیری از درگیری، کاهش تهدیدات امنیت سایبری و ثبات بیشتر در روابط بین‌المللی کمک کند، شورای اتحادیه اروپایی در تاریخ ۱۹ ژوئن ۲۰۱۷، جعبه ابزار دیپلماسی را منتشر کرد.

اتحادیه اروپا و دولت‌های عضو آن به اهمیت مشارکت مداوم دیپلماسی سایبری اتحادیه و ضرورت انسجام بین ابتکارات سایبری اتحادیه اروپا به منظور تقویت تاب‌آوری سایبری اشاره می‌کنند و تشویق می‌شوند تا تلاش‌های خود را در زمینهٔ گفتگوهای سایبری در چارچوب همکاری مؤثر اهمیت ظرفیت سازی سایبری در کشورهای ثالث ادامه دهند.[2] از این رو، اتحادیه اروپا بر توسعهٔ یک چارچوب برای پاسخ دیپلماتیک مشترک به فعالیت‌های سایبری مخرب، با رعایت اصول اصلی زیر کار خواهد کرد:

1. cyber diplomacy toolbox
2. Council of the European Union, Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), 9916/17, 19 June 2017, p.2.

- خدمت به حفظ یکپارچگی و امنیت اتحادیه اروپا، دولت‌های عضو و شهروندان آنها؛
- در نظر گرفتن زمینه گسترده‌تر روابط خارجی اتحادیه اروپا با دولت‌های مربوطه؛
- احترام به قوانین بین‌المللی قابل اجرا و عدم نقض حقوق و آزادی‌های اساسی؛
- دستیابی به اهداف CFSP مطابق با معاهده اتحادیه اروپا و روش‌های مربوطه برای دستیابی به آنها.

۴.۳.۲. تحریم علیه حملات سایبری

در ۱۷ مه ۲۰۱۹، شورا چارچوبی را ایجاد کرد که بر اساس آن به اتحادیهٔ اروپا اجازه می‌دهد در مواردی که اقدامات محدودکننده برای دستیابی به اهداف سیاست خارجی و امنیت مشترک ضروری تلقی می‌شود، اقدامات محدودکنندهٔ هدفمند را به منظور جلوگیری و پاسخ به حملات سایبری که تهدید خارجی برای اتحادیه اروپا یا دولت‌های عضو آن هستند، شامل حملات سایبری علیه کشورهای ثالث یا سازمان‌های بین‌المللی اعمال کند. حملات سایبری که در محدودهٔ این رژیم تحریم جدید قرار دارند، حملاتی هستند که تأثیر قابل توجهی دارند و ریشهٔ آنها خارج از اتحادیه اروپا است و با پشتیبانی شخص یا نهادهای فعال در خارج از اتحادیه اروپا انجام می‌شوند. برای اولین بار این چارچوب به اتحادیه اروپا مجوز وضع تحریم علیه افراد یا نهادهایی را می‌دهد که برای حمله یا تلاش برای حملهٔ سایبری مسئول هستند. افرادی که پشتیبانی مالی، فنی یا مادی برای چنین حملاتی فراهم کرده‌اند. اقدامات محدودکننده شامل ممنوعیت سفر افراد به اتحادیه اروپا و مسدود شدن دارایی‌ها برای اشخاص و نهادها است. علاوه بر این، اشخاص و نهادهای اتحادیه اروپا از قرار دادن وجوه در اختیار افراد فهرست شده ممنوع‌اند.[1]

۴.۴. پیشبرد دفاع سایبری

فضای سایبر به عنوان پنجمین بُعد جنگ در نظر گرفته شده است. این بُعد شامل شبکه‌های اطلاعات و ارتباطات، زیرساخت و داده‌هایی که پشتیبانی می‌کنند، سیستم‌های کامپیوتری،

1. www.consilium.europa.eu/en/policies/cybersecurity, 2021.

پردازشگرها و کنترلرهاست. اتحادیهٔ اروپا در زمینهٔ دفاع در فضای سایبر از طریق فعالیت‌های آژانس دفاعی اروپا (EDA), ENISA و Europol همکاری می‌کند.

هرچند در زمینهٔ دفاع سایبری ناتو از نقش بیشتری برخوردار است، این حوزه از چشم اتحادیه اروپا دور نمانده و اقداماتی از طریق چارچوب سیاست‌گذاری دفاعی در سال ۲۰۱۴ و بازبینی در سال ۲۰۱۸ انجام داده است که هرکدام به‌طور جداگانه بررسی خواهند شد.

۴.۴.۱. چارچوب سیاست‌گذاری دفاع سایبری اتحادیه اروپا(۲۰۱۴)

این سند برای سیاست‌گذاری دفاعی و امنیتی مشترک اولویت‌ها را مشخص می‌کند و نقش بازیگران مختلف را نیز شفاف می‌سازد[1]. تمرکز اصلی این چارچوب سیاست‌گذاری بر توسعهٔ قابلیت‌های دفاع سایبری است که توسط دولت‌های عضو برای اهداف CSDP[2] و همچنین حفاظت از شبکه‌های ارتباطی و اطلاعاتی وضع شده‌اند. در زمینهٔ آموزش، تأکید بر توسعهٔ برنامه‌هایی برای مخاطبان مختلف در زنجیرهٔ فرماندهی CSDP است. از آنجا که فضای سایبری حوزه‌ای است که به سرعت در حال توسعه می‌باشد و در آن قابلیت‌های دوگانه نقش اساسی ایفا می‌کنند، لازم است همکاری نظامی و غیرنظامی و هم‌افزایی با سیاست‌های سایبری اتحادیه اروپا برای مقابله با چالش‌های جدید ایجاد شود.[3]

چارچوب سیاست‌گذاری دفاع سایبری اتحادیه اروپا از پنج اولویت تشکیل شده است که عبارت‌اند از: توسعهٔ قابلیت‌های دفاع سایبری دولت‌های عضو، افزایش حفاظت از شبکه‌های ارتباطی CSDP، ارتقای همکاری‌های نظامی- غیرنظامی[4] و هم‌افزایی با سیاست‌های سایبری اتحادیه اروپا، نهادها و آژانس‌های مرتبط اتحادیه و بخش خصوصی، بهبود فرصت‌های آموزشی و رزمایش و افزایش همکاری با شرکای بین‌المللی است.

۴.۴.۲. بازبینی چارچوب سیاست‌گذاری دفاع سایبری اتحادیه اروپا (۲۰۱۸)

در سال ۲۰۱۸ به منظور توسعهٔ بیشتر سیاست دفاع سایبری اتحادیه اروپا، چارچوب سیاست‌گذاری دفاع سایبری اتحادیه اروپا(۲۰۱۴) بروزرسانی شد. در چارچوب سیاست‌گذاری دفاع سایبری بازبینی شده شش موضوع اولویت‌دار مشخص شده است. تمرکز اصلی این چارچوب

1. EU Cyber Defence Policy Framework , 15585/14, 18 November 2014, p.2.
2. Common Security and Defence Policy
3. EU Cyber Defence Policy Framework , 15585/14, 18 November 2014, p.3.
4. civil-military

سیاست توسعهٔ قابلیت‌های دفاع سایبری و همچنین حفاظت از شبکه‌های ارتباطی و اطلاعات CSDP اتحادیه اروپا است. سایر زمینه‌های دارای اولویت عبارت‌اند از: آموزش و رزمایش، تحقیق و فناوری، همکاری نظامی- غیرنظامی و همکاری بین‌المللی. در زمینهٔ آموزش، تأکید بر ارتقای آموزش دفاع سایبری دولت‌های عضو و آموزش آگاهی سایبری از زنجیرهٔ فرماندهی CSDP است. همچنین مهم است که ابعاد سایبری در رزمایشات به اندازه کافی مورد بررسی قرار گیرند تا بتوانند با بهبود روش‌های تصمیم‌گیری و در دسترس بودن اطلاعات، اتحادیه اروپا را در واکنش به بحران‌های سایبری بهبود ببخشند. فضای سایبر حوزه‌ای است که به سرعت در حال توسعه است و پیشرفت‌های فناوری جدید باید در حوزه‌های غیرنظامی و نظامی مورد حمایت قرار گیرند. همکاری نظامی- غیرنظامی در زمینهٔ سایبری برای اطمینان از پاسخ منسجم به تهدیدات سایبری کلیدی است. همچنین، افزایش همکاری با شرکای بین‌المللی می‌تواند به افزایش امنیت سایبری در داخل اتحادیه اروپا و فراتر از آن و ارتقای اصول و ارزش‌های اتحادیه اروپا کمک کند.[1]

۴.۵. امنیت سایبری زیرساخت‌های حیاتی

۴.۵.۱. حفاظت از شبکه‌های 5G

شبکه‌های 5G نه تنها برای ارتباطات دیجیتالی بلکه برای بخش‌های مهمی مانند انرژی، حمل و نقل، بانکداری و سلامت بسیار مهم هستند. بنابراین اطمینان از تاب‌آوری شبکه‌های 5G برای اتحادیه اروپا ضروری است. با توجه به درآمدهای جهانی 5G در سال ۲۰۲۵ که ۲۲۵ میلیارد یورو تخمین زده شده است، 5G یک دارایی کلیدی برای رقابت اروپا در بازار جهانی می‌باشد و امنیت سایبری آن برای اطمینان از خودمختاری راهبردی اتحادیه بسیار مهم است. در ژانویه ۲۰۲۰ ، اتحادیه اروپا جعبه ابزاری[2] برای شناسایی مجموعه اقدامات احتمالی مشترک برای کاهش خطرات اصلی امنیت سایبری شبکه‌های 5G و ارائه راهنمایی، منتشر کرد.[3]

هدف جعبه ابزار اتحادیه اروپا در زمینه امنیت سایبری 5G، ایجاد یک رویکرد اروپایی هماهنگ بر اساس مجموعه‌ای از اقدامات مشترک است که با هدف کاهش خطرات اصلی امنیت

1. EU Cyber Defence Policy Framework (2018 update), 14413/18, 19 November 2018, p.8.
2. **EU toolbox on 5G**
3. www.consilium.europa.eu/en/policies/cybersecurity, 2021.

سایبری شبکه‌های 5G انجام می‌شود. این جعبه ابزار قصد دارد راهنمایی در انتخاب و اولویت‌بندی اقداماتی که باید بخشی از برنامه‌های کاهش خطر ملی و اتحادیه اروپا باشد، ارائه دهد. هدف نهایی، ایجاد یک چارچوب قوی و عینی از اقدامات امنیتی است که از طریق رویکردهای هماهنگ بین دولت‌های عضو سطح کافی امنیت سایبری شبکه‌های 5G در سراسر اتحادیه اروپا را تضمین نماید. رویکرد اتخاذ شده به باز بودن بازار واحد اتحادیه اروپا احترام می‌گذارد و یک رویکرد مبتنی بر ریسک می‌باشد که صرفاً بر اساس دلایل امنیتی است.[1]

۴.۵.۲. ایمن‌سازی دستگاه‌های متصل

دستگاه‌های متصل از جمله ماشین‌ها، حسگرها و شبکه‌های تشکیل دهندهٔ اینترنت اشیا نقش مهمی در شکل‌گیری بیشتر آینده دیجیتال اروپا خواهند داشت. در دسامبر۲۰۲۰، شورا سندی منتشر کرد که افزایش استفاده از محصولات مصرفی و دستگاه‌های صنعتی به اینترنت و ریسک‌های جدید مربوط به حریم شخصی، امنیت اطلاعات و امنیت سایبری را به رسمیت شناخت. این سند اولویت‌هایی را برای رسیدگی به این موضوع مهم و افزایش رقابت جهانی صنعت اینترنت اشیای اتحادیه اروپا با اطمینان از بالاترین استانداردهای تاب‌آوری، ایمنی و امنیت، مشخص می‌کند.[2]

1. https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127, 2021.
2. Council Conclusions on the cybersecurity of connected devices, 2 December 2020, p.3.

نتیجه‌گیری

امروزه فضای سایبر نقش پررنگی در زندگی بشری دارد. از کارهای روزمره همانند پرداخت‌های بانکی، آموزش‌های مجازی و خریدهای برخط گرفته تا مدیریت نیروگاه‌ها و بخش‌های دفاعی- امنیتی هر یک به فضای سایبر وابسته‌اند. این وابستگی دو وجه دارد؛ به همان اندازه که استفاده از این فضا، تسهیلاتی برای کاربران آن به‌وجود آورده است، تهدیداتی نیز همراه با خود دارد. از این رو کاربران سعی می‌کنند با این تهدیدات مبارزه کنند. کاربران کلان فضای سایبر دولت‌ها هستند و با توجه به وابستگی و اهمیت آن، تهدیدات نشأت گرفته از فضای سایبر برای دولت‌ها، به راحتی می‌تواند مخاطرات امنیتی به بار آورد. یکی از این کاربران کلان، اتحادیه اروپا است. باید خاطرنشان کرد، از آنجایی‌که تاکنون سیاست‌گذاری واحدی در سطح جهانی در زمینهٔ امنیت سایبری به‌وجود نیامده است، اتحادیه اروپا به عنوان یک بازیگر مهم بین‌المللی در تلاش است به تدریج در امنیت سایبری به یک بازیگر پیشرو تبدیل شود. فعالیت‌های صورت‌گرفته در اتحادیه اروپا حاکی از آمادگی آن برای گسترش در مقیاس جهانی و تبدیل به یک کنشگر مهم بین‌المللی است. رسیدن به چنین جایگاهی بستگی به موفقیت فعالیت‌های حال حاضر اتحادیه دارد. با افزایش ماهیت سیاسی امنیت سایبری، میان دولت‌های عضو، نهادها و مؤسسات این اجماع به‌وجود آمده است که اتحادیه به سمت یک بازیگر منسجم حرکت کند. برای تبدیل شدن به یک بازیگر منسجم در زمینهٔ امنیت سایبری اتحادیه اروپا با چالش‌هایی از جمله تعدد بازیگران، نهادها و مؤسسات و احتمال تضاد منافع میان آنها مواجه است. با وجوداین، اتحادیه با انتشار راهبردها، دستورالعمل‌ها و مقررات سعی کرده است تا این تعدد بازیگران خللی در رویکرد اتحادیه بوجود نیاورد. اما شایان توجه است که تنها انتشار راهبردها، دستورالعمل‌ها و مقررات کافی نیست؛ بلکه وجود شفافیت، مشارکت و پاسخگویی نیز لازم است. اتحادیه اروپا با تعریف عوامل اثرگذار در زمینهٔ امنیت سایبری علاوه بر انتشار اسناد، دستورالعمل‌ها و مقررات، با تشکیل نهاد، مؤسسه، آژانس جدید و یا ایجاد بخشی مربوط به سایبری در مؤسسات و نهادهای موجود در تلاش برای عملیاتی کردن اهداف خود بوده است. هرچند هر یک از بازیگران از کارویژه خاصی برخوردارند، همان‌طور که اشاره شد، اتحادیه با انتشار راهبردها، دستورالعمل‌ها و مقررات سعی در هماهنگ‌سازی آنها با یکدیگر دارد. با بررسی فعالیت دولت‌های عضو اتحادیه متوجه می‌شویم که هر یک از آنها در سطح ملی سازمانی با

کارکرد یکسان نهادهای بررسی شده دارند و از طرفی با بررسی این نهادها با سایر نهادهای اتحادیه اروپا به این نکته پی می‌بریم که از نظر بودجه و تعداد افراد در رده‌های پایین قرار دارند. اگر انسجام درونی به عنوان پیش‌شرط تبدیل به یک بازیگر مهم جهانی در زمینهٔ امنیت سایبری باشد، برای رسیدن به این مهم، اتحادیه اروپا باید به عنوان مرکز اصلی سیاست‌گذاری امنیت سایبری در اروپا تبدیل شود به گونه‌ای که دولت‌های عضو این سیاست‌ها را نسبت به سیاست‌های ملی در اولویت قرار دهند، در چنین شرایطی لازم است آن دسته از نهادهای اروپایی در زمینه امنیت سایبری که نهادهای مشابه در سطح ملی دارند، تقویت و گسترش یابند.

با توجه به مطالب گفته شده می‌توان نتیجه‌گیری کرد که تصمیم‌گیری منسجم در حوزهٔ امنیت سایبری در اتحادیه اروپا هم باعث و هم نمودی از انسجام در اتحادیه اروپا به عنوان بازیگر سیاسی می‌شود و از طرف دیگر انسجام اروپا موجب انسجام بیشتر در تصمیم‌گیری خواهد شد. به عنوان مثال، از اقداماتی که پس از حمله سایبری به استونی در سطح اتحادیه اروپا صورت گرفت (مخصوصاً از سال ۲۰۱۳ به بعد) می‌توان نوعی انسجام در تصمیم‌گیری را مشاهده کرد که از جملهٔ آن انتشار سه راهبرد، دو دستورالعمل، دو چارچوب سیاست‌گذاری دفاعی، جعبه ابزار دیپلماسی، تأسیس مؤسسات، نهادها و آژانس‌ها یا افزایش اختیار مؤسسات، نهادها و آژانس‌های پیشین را می‌توان نام برد که نتیجهٔ آن تبدیل اتحادیهٔ اروپا به یک بازیگر منسجم در زمینهٔ امنیت سایبری بوده است.

تصمیم‌گیری منسجم اتحادیه اروپا در حوزه امنیت سایبری ⟺ انسجام اتحادیه اروپا به عنوان بازیگر سیاسی در حوزه امنیت سایبری.

فهرست منابع

الف) منابع انگلیسی

Articles

1. Akbanov, Maxat, Vassilios G. Vassilakis, and Michael D. Logothetis. "*WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms*." Journal of Telecommunications and Information Technology (2019).
2. Bada, Maria, Sadie Creese, Michael Goldsmith, Chris Mitchell, and Elizabeth Phillips. *"Computer Security Incident Response Teams (CSIRTs): An Overview."* The Global Cyber Security Capacity Centre (2014).
3. Bendiek, Annegret, Raphael Bossong, and Matthias Schulze. *"The EU's revised cybersecurity strategy: half-hearted progress on far-reaching challenges."* (2017).
4. Camino Mortera-Martinez. *"Game over? Europe's cyber problem."* CENTRE FOR EUROPEAN REFORM, 2018.
5. -Koff, Harlan, Antony Challenger, and Israel Portillo. *"Guidelines for operationalizing policy coherence for development (PCD) as a methodology for the design and implementation of sustainable development strategies."* Sustainability 12, no. 10 (2020).
6. Portela, C., and K. Raube. *"Revisiting Coherence in EU Foreign Policy." Hamburg Review of Social Sciences* 3, no. 1 (2008).
7. Thaler, Philipp. *"Shaping EU Foreign policy towards Russia: Improving coherence in external relations.*" Edward Elgar Publishing, 2020.
8. Thygesen Vendius, Trine. *"Europol's Cybercrime Centre (EC3), its Agreements with Third Parties and the Growing Role of Law Enforcement on the European Security Scene|."* EJPS 3, no. 2 (2015.

Electronic resources

9. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder.
10. www.europol.europa.eu/european-union-serious-and-organised-crime-threat-assessment/ 2021.
11. Team GAIT ELEC-E7470 – Cybersecurity,2017.
12. eucyberdirect.eu/2017-wannacry.

13. https://www.bbc.com/news/technology-57583158.
14. https://eda.europa.eu/what-we-do/all-activities/activities-search/cyber-defence,2021.
15. https://www.enisa.europa.eu/about-enisaccdcoe.org/uploads/2018/11/EU-170607, 2021.
16. https://www.enisa.europa.eu/about-enisaccdcoe.org/uploads/2018/11/EU-170607, 2021.
17. https://eeas.europa.eu/headquarters/headquarters-homepage/82/about-european-external-action-service-eeas_en,2021.
18. https://ccdcoe.org/uploads/2018/11/EU-170607-CyberDiplomacyToolbox-1.pdf.2018.
19. cert_about.html// cert.europa.eu.2021.
20. europol www.europol.europa.eu/ about-europol/ EC3,2021.
21. www.ec.europa.eu/ law/law-making-process,2021.
22. www.consilium.europa.eu/en/policies/cybersecurity, 2021.
23. www.europa.eu/horizon-europe_en, 2021.
24. www.consilium.europa.eucompetence-centre, 2021.
25. www.ec.europa.eu/commission, 2021.
26. https://www.enisa.europa.eu/about-enisa, 2021.

Cases

27. Federal Ministry of the Interior ,Cyber Security Strategy for Germany, 2011.
28. REGULATION (EU) No 526/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 21 May 2013.
29. European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN (2013) 1 final, 7 February 2013.
30. Cyber Security Strategy for Germany, 2011.
31. European Council conclusions Draft EU Council conclusions.2021.
32. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade JOIN/2020/18 final.
33. THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, REGULATION on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (Cybersecurity Act), 2019/ 881, 17 April 2019.

34. Council Resolution on Encryption - Security through encryption and security despite encryption, 24 November 2020.
35. Council of the European Union, Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), 9916/17, 19 June 2017.
36. THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, concerning measures for a high common level of security of network and information systems across the Union (NIS Directive), 2016/1148, 6 July 2016.
37. EU Cyber Defence Policy Framework, 15585/14, 18 November 2014.
38. EU Cyber Defence Policy Framework (2018 update), 14413/18, 19 November 2018.
39. https://digital-strategy.ec.europa.eu/en/activities/digital-programme, 2021.
40. https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127, 2021.
41. Council Conclusions on the cybersecurity of connected devices, 2 December 2020.