The University of Tehran Press

Public Law Studies Quarterly

Homepage: http://jplsq.ut.ac.ir

Online ISSN: 2423-8139

Volume: 55, **Issue:** 4
Winter 2026

European Union Actions in Combating Cyber Terrorism

Maryam Zabihi[1]✉ | Elham Aminzadeh[2]

1. Corresponding Author; MA in International Law, Faculty of Law and Political Science, University of Tehran, Tehran, Iran. Email: maryam.zabihi@ut.ac.ir
2. Prof., Department of Public Law, Faculty of Law and Political Science, University of Tehran, Tehran, Iran. Email: eaminzadeh@ut.ac.ir

Article Info

Article Type:
Research Article

Pages: 2439-2458

Received:
2023/06/16
Received in Revised form:
2023/12/23
Accepted:
2024/05/06
Published online:
2025/12/22

Keywords:
European Union, cyber security, cyber terrorism, cyber warfare, Council of Europe.

Abstract

Today, with the advancement of technology and its close integration with people's daily lives, terrorism has extended its activities into cyberspace to exploit its unique characteristics for the expansion of its operations. In contrast, since states have not reached a consensus on a unified definition of terrorism, and consequently cyber terrorism, there exists a gap in effective and comprehensive criminal laws, especially at the international level. As a result, countries have currently turned to drafting laws of a protective and preventive nature to counter these attacks. At the regional level, particularly in Europe, significant measures have been undertaken that can serve as models for replication and expansion at the international level. Analysis of these actions indicates that the creation of specialized organizations and teams, development of military and security capabilities, cooperation with other countries and engagement with the private sector, specialized training, and the deployment of advanced equipment are among the measures implemented to confront and prevent cyber-terrorist attacks, yielding positive results.

How To Cite

Zabihi, Maryam; Aminzadeh, Elham (2026). European Union Actions in Combating Cyber Terrorism. *Public Law Studies Quarterly*, 55 (4), 2439-2458.
DOI: https://doi.com/10.22059/jplsq.2024.360920.3335

DOI

10.22059/jplsq.2024.360920.3335

Publisher

The University of Tehran Press.

انتشارات دانشگاه تهران

فصلنامه مطالعات حقوق عمومی

Homepage: http://jplsq.ut.ac.ir

شاپا الکترونیکی: ۸۱۳۹-۲۴۲۳
دوره: ۵۵، شماره: ۴
زمستان ۱۴۰۴

اقدامات اتحادیهٔ اروپا در مقابله با تروریسم سایبری

مریم ذبیحی[۱]✉ | الهام امین‌زاده[۲]

۱. نویسندهٔ مسئول؛ دانش‌آموختهٔ کارشناسی ارشد حقوق بین‌الملل، دانشکدهٔ حقوق و علوم سیاسی، دانشگاه تهران، ایران.
رایانامه: maryam.zabihi@ut.ac.ir

۲. استاد، گروه حقوق عمومی، عضو هیأت علمی دانشکدهٔ حقوق و علوم سیاسی دانشگاه تهران، ایران. رایانامه: eaminzadeh@ut.ac.ir

اطلاعات مقاله

نوع مقاله: پژوهشی

صفحات: ۲۴۳۹-۲۴۵۸

تاریخ دریافت:
۱۴۰۲/۰۳/۲۶

تاریخ بازنگری:
۱۴۰۲/۱۰/۰۲

تاریخ پذیرش:
۱۴۰۳/۰۲/۱۷

تاریخ انتشار برخط:
۱۴۰۴/۱۰/۰۱

کلیدواژه‌ها:
اتحادیهٔ اروپا، امنیت سایبری، تروریسم سایبری، جنگ سایبری، شورای اروپا.

چکیده

امروزه با پیشرفت فناوری و ارتباط تنگاتنگ آن با زندگی مردم، تروریسم نیز گسترهٔ فعالیت خویش را به فضای سایبر کشانده تا از خصوصیات ویژهٔ آن در راستای گسترش فعالیت‌های خویش بهره‌مند شود. در مقابل از آنجا که دولت‌ها نتوانستند بر سر تعریف واحد از تروریسم و به‌تبع آن تروریسم سایبری به اجماع برسند؛ ازاین‌رو دچار خلأ قوانین کیفری کارامد و جامع به‌خصوص در سطح بین‌المللی هستیم؛ ازاین‌رو کشورها جهت مقابله با این حملات در حال حاضر به تدوین قوانینی با ماهیت حفاظتی و پیشگیری‌کننده روی آورده‌اند. در سطح منطقه‌ای به‌طور اخص در اروپا اقدامات زیادی انجام شده است که با مداقه در این اقدامات می‌توان از آنها الگوبرداری کرد و گامی در جهت گسترش و تعمیم آن در سطح بین‌المللی برداشت. تحلیل اقدامات حاکی از آن است که ایجاد سازمان‌ها و تیم‌های ویژه، توسعهٔ توانمندی‌های نظامی و امنیتی، همکاری با سایر کشورها و تعامل با بخش خصوصی، آموزش‌های متخصصانه و تجهیزات پیشرفته، از جمله اقداماتی هستند که در راستای این رویارویی و جلوگیری از حملات تروریستی سایبری انجام شده که نتایج مثبتی در بر داشته است.

استناد

ذبیحی، مریم؛ امین‌زاده، الهام (۱۴۰۴). اقدامات اتحادیهٔ اروپا در مقابله با تروریسم سایبری. *مطالعات حقوق عمومی*، ۵۵ (۴)، ۲۴۳۹-۲۴۵۸.
DOI: https://doi.com/10.22059/jplsq.2024.360920.3335

DOI 10.22059/jplsq.2024.360920.3335

ناشر مؤسسهٔ انتشارات دانشگاه تهران.

۱. مقدمه

اگر سدهٔ بیست‌ویکم به‌درستی قرن انفجار اطلاعات نامیده شده است، وجه تسمیهٔ این نامگذاری تا حدود زیادی مرهون تشکیل فضای سایبر و به‌طور اخص، ظهور اینترنت است. اگرچه جامعهٔ جهانی، تمایلی به اعمال حاکمیت ملی هر کشور بر فضای سایبری در دسترس شهروندان خود نداشت (ملکوتی، ۱۳۹۸: ۲۴۰)، اما اهمیت تأمین امنیت شهروندان و حاضران این فضا، مورد اجماع همهٔ کشورهای عضو سازمان ملل متحد است (ضیایی، ۱۳۹۶: ۲۲۹). انقلاب تکنولوژیک علی‌رغم مزایای فراوانی که عصر فناوری در تسهیل زندگی انسان‌ها ارائه می‌دهد، به محیطی مناسب برای تروریست‌ها تبدیل شده است تا ایدئولوژی افراطی خود را گسترش دهند (Alshargawi *et al*., 2023: 24). حقوقدانان و پژوهشگران هر کدام بنا به درک خود از مفهوم تروریسم، آن را به‌گونه‌ای متفاوت تعریف کرده‌اند (نجفی ابرندآبادی و هاشم بیگی، ۱۳۹۳: ۱۴). با این حال، تروریسم به‌عنوان یک روش برای تحقق اهداف ایدئولوژیک یا سیاسی با استفاده از خشونت یا تهدید به خشونت، برای منتشر کردن وحشت شناخته می‌شود (Naqvi *et al*., 2022: 54). عصر دیجیتال به پیامدهای مثبت و منفی برای همهٔ فعالان در داخل و خارج از حوزهٔ سایبری منجر شده و شبکه‌های مجازی و رسانه‌های دیجیتال به شمشیرهای دولبه برای گسترش رفاه یا انجام جرم تبدیل شده است (Monshipouri *et al*., 2018: 37). فناوری سایبری توسط تروریست‌ها برای برقراری ارتباط، تبلیغ، آموزش یا برنامه‌ریزی و رادیکال کردن، استخدام یا تأثیرگذاری بر مردم استفاده می‌شود که به‌دلیل چندجانبه بودن می‌تواند به‌عنوان ابزاری مدرن برای جنگ استفاده شود (Zerzri, 2017: 4). در حال حاضر هیچ توافقنامه بین‌المللی به‌طور خاص برای تنظیم رفتار دولت در فضای سایبری وجود ندارد. بنابراین، رویهٔ دولتی و اعلامیه‌های ملی در خصوص نحوهٔ تفسیر دولت‌ها از قوانین بین‌المللی قابل اجرا در عملیات سایبری برای افزایش اطمینان و شفافیت حقوقی ارزشمند است (Osula *et al*., 2022: 89). افزایش جرایم سایبری و حملات سایبری بزرگ نشان داد که خطرها و تهدیدات جدی در فضای سایبری در حال تکامل هستند (Naqvi *et al*., 2022: 53) و اجرای قانون نتوانسته است به‌طور مؤثر پاسخگوی تهدیداتی که از کامپیوتر برای ارتکاب جرایم استفاده می‌کنند، باشد (کتانچی و پورقهرمانی، ۱۳۹۸: ۳۲).

بحث دربارهٔ حقوق بین‌المللی قابل اجرا در عملیات سایبری از سؤال آیا حقوق بین‌المللی بر فضای سایبر اعمال می‌شود؟ به سؤال چگونه اعمال می‌شود؟، تغییر یافته است. اخیراً، اتحادیهٔ اروپا در تدوین راهبرد جدید امنیت سایبری خود، بحث توسعهٔ موقعیت مشترک اتحادیه در خصوص اعمال حقوق بین‌المللی در فضای سایبر را مطرح کرده است. به‌عنوان بخشی از یک چشم‌انداز گسترده در تلاش برای رهبری در استانداردها، نرم‌افزارها و چارچوب‌های نظارتی در فضای سایبر، این ارتباط مشترک بر لزوم اتخاذ موضع فعال‌تر در بحث‌های مطرح‌شده در سازمان ملل متحد و دیگر ارگان‌های بین‌المللی مربوطه

تأکید کرده است.[1] با این حال، کمتر از نیمی از کشورهای عضو اتحادیهٔ اروپا بیانیهٔ عمومی دربارهٔ تفسیر حقوق بین‌المللی در فضای سایبری را صادر کرده‌اند و ازاین‌رو، به‌نظر می‌رسد به‌دست آوردن توافق دربارهٔ تفسیر مفاهیم مربوط به حقوق بین‌المللی به چالشی تبدیل شده است و کشورها راهبرد ملی امنیت سایبری خود را بر اساس درک خود از امنیت سایبری تدوین می‌کنند. آنچه برای یک کشور خطر شایان توجهی است، ممکن است در خصوص کشور دیگر صدق نکند (Osula *et al*. ,2022: 89).

۲. فضای سایبری و ویژگی‌های آن

این بستر مجموعه‌ای عظیم از صفر و یک‌هایی است که داده‌های الکترونیکی را تشکیل می‌دهند و آنها نیز در قالب‌های مختلف، مفاهیم را به شکل الکترونیکی منعکس می‌کنند (احمدی، ۱۳۹۷: ۵۲). به‌طور کلی بنا به تعاریف، فضای سایبری دارای ویژگی‌های ذیل است:

- این فضا جهانی و فرامرزی است: به‌عبارت دیگر هر فرد در هر نقطه از جهان می‌تواند از طریق آن به‌آسانی، به جدیدترین اطلاعات دست یابد (Lord *et al*., 2011: 15)؛
- دستیابی آسان به آخرین اطلاعات: فضای مجازی یا سایبری، امکان دسترسی آسان و سریع را به آخرین اطلاعات دنیا فراهم کرده است (Naqvi *et al*., 2022: 55)؛
- جذابیت و تنوع رسانه‌ها: از فیلم، عکس، متن و یا هر هنر دیگری برای جذاب کردن خویش به‌کار می‌گیرند (Naqvi *et al*., 2022: 50)؛
- آزادی اطلاعات و ارتباطات: معنای واقعی آزادی اطلاعات، در فضای سایبری محقق شده است. به‌طوری‌که شما هر نوع اطلاعاتی را که بخواهید، بدون محدودیت‌های حاکم بر دیگر رسانه‌ها، در فضای سایبری قابل دسترسی است (Naqvi *et al*., 2022: 51).

۳. تروریسم سایبری و ویژگی‌های آن

تروریسم سایبری به معنای استفاده غیرقانونی از کامپیوترها، شبکه‌ها و فناوری برای ترساندن یا وادار کردن دولت یا مردم برای به‌دست آوردن منافع اقتصادی، سیاسی یا اجتماعی است. تروریسم سایبری به دو روش استدراک می‌شود؛ طبق رویکرد اول، تروریسم سایبری فقط با استفاده از فناوری اطلاعات برای انجام حمله تمایز داده می‌شوند، درحالی‌که رویکرد دوم بر روی سیستم‌های کامپیوتری به‌عنوان هدف حملات و نه ابزار برای اجرای آنها تمرکز دارد. به‌نظر می‌رسد تعریف درست از ترکیب هر دو رویکرد به‌وجود خواهد آمد (Oleksiewicz, 2016: 135). در ذیل به برخی ویژگی‌های آن خواهیم پرداخت:

1. European Council Conclusion Draft EU, council conclusion.2021.p.1

- پایین بودن احتمال تنبیه یا بازخواست اقدام‌های مجرمانه در فضای سایبری: احتمال تنبیه یا بازخواست اقدام‌های مجرمانه در فضای سایبری پایین است (خلیلی‌پور رکن‌آبادی و نورعلی وند، ۱۳۹۱: ۱۷۱)؛
- تأثیرگذاری شگرف: ماهیت خاص فضای سایبری شرایطی را به‌وجود آورده است که بروز هر اختلال یا وقفه می‌تواند تأثیرات و پیامدهای به‌مراتب بیشتری از حادثهٔ اولیه در پی داشته باشد (Lord *et al*., 2011: 17)؛
- تعدد بازیگران در فضای سایبری: تقریباً هر کسی می‌تواند به این فضا وارد شود (Charney, 2009: 5)؛
- ناشناس ماندن بازیگران و عدم قابلیت ردیابی: اینترنت به‌عنوان سیستم نامتمرکز طراحی شده و کاربران آن، اغلب شناخته‌شده نیستند (عظیمی و خشنودی، ۱۳۹۵: ۱۶۰)؛
- مشکل شدید انتساب: برای شناسایی مجرمان حملات و همچنین درک نیت و توانایی آنها و ارتباطات آنها با دیگر کشورها یا سازمان‌ها، نیاز به تحلیل اطلاعات است. تعیین مسئولیت در حملات سایبری، نه‌تنها مربوط به فناوری‌هاست، بلکه با سیاست‌ها نیز ارتباط دارد (Katagiri, 2021: 7)؛
- امکان وارد آوردن خسارت مالی، بدون رساندن آسیب‌های جسمی: اصولاً آسیب‌های جانی، به‌ویژه اگر با مرگ همراه باشد، حساسیت و واکنش‌های زیادی را علیه تروریست‌ها برمی‌انگیزند. ازاین‌رو اگر تروریست‌ها بتوانند بدون جریحه‌دار کردن احساسات مردم، لطمهٔ مالی بسیاری به کشورها وارد آورند، به موفقیت بزرگی دست یافته‌اند (کدخدایی و ساعد، ۱۳۹۰: ۸۴)؛
- انجام بهینهٔ فعالیت‌های پولی و بانکی: گروه‌های جنایتکار سازمان‌یافته و تروریست‌ها نیازمند مبادلات مالی‌اند و مجبورند درآمدهای مالی خود را تطهیر کنند تا بتوانند از آنها استفاده کنند. همچنین امکان جذب کمک‌های مالی از سوی هواداران و حامیان نیز بسیار آسان شده است (کدخدایی و ساعد، ۱۳۹۰: ۸۴).

۴. امنیت سایبری[1]

امنیت در لغت، به معنای در امان بودن و مصون بودن از هرگونه ترس و تهدید است (رزونا و همکاران، ۱۳۹۰: ۸۸). فضای سایبر، دارای گستره‌های جهانی و بدون مرز، پوشیده و پنهان، ناهنجارمند و کنترل‌ناپذیر است. ارزش‌ها و هنجارهای این فضا شاید از حیث عنوان با آنچه در فضای فیزیکی می‌بینیم، یکی باشد، ولی از حیث کیفیت و ماهیت متفاوت است. یکی از برجسته‌ترین این ارزش‌ها امنیت است. امنیت فضای سایبر بر دو گونه است: امنیت درونی که متضمن حفظ استانداردهای حاکم بر فضای تبادل اطلاعات است و امنیت بیرونی که متضمن نبود تهدید برای اشخاصی است که از شبکه‌های رایانه‌ای و اینترنتی بهره می‌گیرند. در کنار امنیت فضای سایبری، شاید تبادل و آزادی اطلاعات یکی از مهم‌ترین ارزش‌ها در فضای

1. Cyber Security

سایبر است. فضای سایبر ماهیتاً برای آزادی گردش اطلاعات شکل گرفته و محدودیت در این فضا معنا ندارد (پاکزاد، ۱۳۹۰: ۲۳). اولویت‌ها برای راهبردهای امنیت سایبری ملی، کشور به کشور متفاوت خواهد بود. در برخی کشورها، ممکن است تمرکز بر حفاظت از ریسک زیرساخت‌های حیاتی باشد، درحالی‌که سایر کشورها ممکن است بر حفاظت از مالکیت معنوی تمرکز کنند و هنوز، برخی دیگر ممکن است بر بهبود آگاهی امنیت سایبری در ارتباط‌های جدید تمرکز کنند (Odebade *et al*., 2023:3).

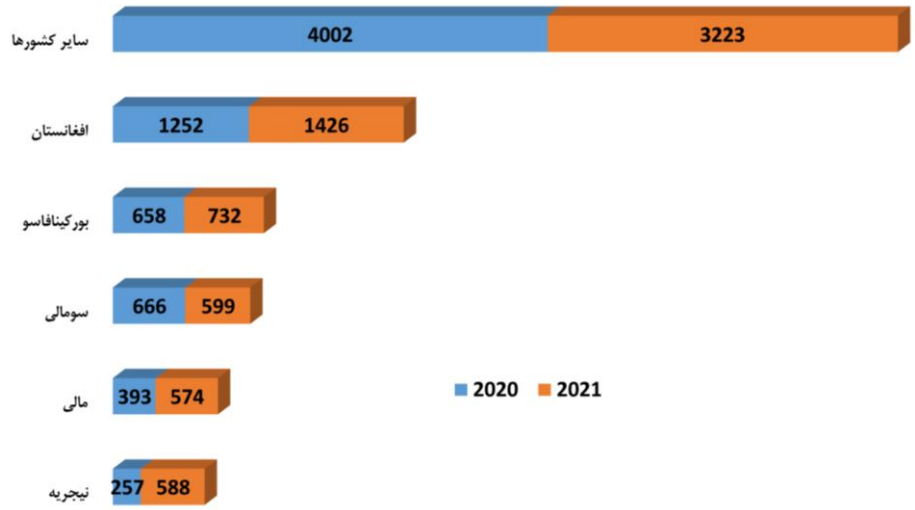
در حال حاضر تحقیقات محدودی دربارهٔ امنیت سایبری و پیامدهای آن در اتحادیهٔ اروپا انجام شده است. طبیعت بین‌الدولی اتحادیهٔ اروپا دربارهٔ فضای سایبری نقش پررنگی دارد (Lord *et al*., 2011: 16). تهدیدات و مزایای فضای سایبری سبب شده است که فضاهای سایبری از سیاست‌های پایین‌دستی به سیاست‌های با اولویت بالا منتقل شوند و از امنیت سایبری تا تروریسم سایبری یک تهدید نوظهور برای اروپا به‌وجود آید. به همین دلیل دولت‌ها به موضوع امنیت سایبری با جدیت زیادی نگریسته‌اند و به‌جز ایالات متحده، سازمان‌های بین‌المللی مانند ناتو، سازمان ملل و اتحادیهٔ اروپا نیز راهبردهای مبارزه با تهدید حملات سایبری و تروریسم سایبری را تدوین کرده‌اند (Naqvi *et al*., 2022: 53). برای درک تهدیداتی که اتحادیهٔ اروپا در فضای سایبری دارد و راهبردهای پاسخگویی به این تهدیداتی که برای مقابله با آنها اتخاذ شده است، در این مقاله اسناد سیاستی رسمی اتحادیهٔ اروپا و آژانسی که برای امنیت سایبری شکل گرفته، تحلیل شده است.

۵. اقدامات اتحادیهٔ اروپا در زمینهٔ امنیت و تروریسم سایبری

امروزه تروریسم آنچنان در سطح بین‌المللی گسترش پیدا کرده است که دیگر نمی‌توان از نقض امنیت یک کشور خاص صحبت کرد؛ بلکه بزه‌دیدهٔ تروریسم، به‌طور مستقیم یا غیرمستقیم، جامعهٔ بین‌المللی است و شرایط جدید تروریسم را به پدیدهٔ فرامرزی تبدیل کرده است (بزرگمهری، ۱۳۹۰: ۱۹۲).

تروریسم سایبری، به قدری پویاست که ارائه یک قانون و راهکار ملی، نمی‌تواند برای مدت طولانی کارامد باشد (خلیل‌زاده، ۱۳۹۳: ۴۳). اتحادیهٔ اروپا و کشورهای عضو آن با تهدیدات امنیتی جدید و پیچیده روبه‌رو هستند و برجسته شدن نیاز به شراکت و همکاری بیشتر بین کشورها و سازمان‌های بین‌المللی در همهٔ سطوح به‌وضوح آشکار است. امروزه، بسیاری از تهدیدات امنیتی، ناشی از آسیب‌پذیری کشورهای مجاور اتحادیهٔ اروپا و تغییرات سریع در شکل استفاده از خشونت، افراطی‌گری و تروریسم است. تهدید افراطی‌گری و تروریسم به‌صورت بین‌المللی در حال تبدیل شدن به یک تهدید گسترده است و از مرزها و قلمروهای کشورها عبور می‌کند. برای مقابله با این تهدیدات، پاسخی متحد و مؤثر نیاز است که از همکاری تمامی کشورها از جمله کشورهای عضو اتحادیهٔ اروپا به‌دست آید.[1]

1. https://ec.europa.eu/homeaffairs/what-we-do/policies/organized-crime-and-humantrafficking/cybercrime_en



نمودار ۱. آمار قربانیان تروریسم در سال‌های ۲۰۲۰ و ۲۰۲۱[1]

تاکنون، تعداد کمی از سازمان‌های بین‌المللی در زمینهٔ جنبه‌های حقوق بین‌الملل و فضای سایبری (مانند سازمان ملل و ناتو) با موفقیت در میان اعضای خود به اجماع دست یافته‌اند. بسیاری دیگر صرفاً حمایت کلی خود را از کاربرد قوانین بین‌المللی در فضای سایبری ابراز کرده‌اند (Osula *et al.*, 2022: 90). نهمین گزارش سالیانهٔ شاخص جهانی تروریسم[2] در مارس ۲۰۲۲ منتشر شد، که گزارشی جامع و مختصر از روندها و الگوهای مهم جهانی تروریسم در دههٔ گذشته را ارائه می‌دهد. این گزارش توسط مؤسسهٔ اقتصاد و صلح[3] با بهره‌مندی از پایگاه داده‌ها و اطلاعات موجود[4] و سایر منابع تهیه می‌شود. داده‌ها نشان‌دهندهٔ تغییر در پویایی رفتار تروریسم است که بیشتر در مناطق و کشورهایی که از بی‌ثباتی و درگیری داخلی سیاسی رنج می‌برند متمرکز بوده است؛ مثل کشورهای منطقه ساحل، افغانستان و میانمار و جنگ‌های داخلی خشونت‌آمیز،عامل اصلی تروریسم بوده است. تمامی ده کشوری که بیشترین تأثیر را از تروریسم در سال ۲۰۲۱ داشته‌اند، درگیر حملات مسلحانهٔ داخلی در سال ۲۰۲۰ بوده‌اند؛ ازاین‌رو راهبرد مبارزه با تروریسم اتحادیهٔ اروپا شامل همکاری دیگر کشورها مانند آمریکای شمالی، خاورمیانه، آسیا، آفریقا و نهادهای بین‌المللی است و بر پایهٔ چهار ستون زیر استوار است:

1. https://www.start.umd.edu/gtd/
2. Global Terrorism Database
3. The Institute of Economics and Peace (IEP)
4. https://www.dragonflyintelligence.com/intelligence/terrorismtracker/

- پیشگیری به‌منظور جلوگیری از فرایند رادیکال شدن و جذب گروه‌های تروریستی با توجه به علل آنها؛
- محافظت به‌منظور کاهش آسیب‌پذیری زیرساخت‌ها و شهروندان با حفاظت آنها از حملات تروریستی؛
- پیگیری به‌منظور محدود کردن قابلیت‌های تروریست‌ها، از راه‌هایی مانند تقویت قابلیت‌های ملی، به اشتراک‌گذاری اطلاعات و همکاری بین بخش قضایی و پلیس؛
- محدود کردن منابع مالی تروریستی و محروم کردن آنها از وسایل و حمایتی که با آنها فعالیت‌های تروریستی را انجام می‌دهند (Naqvi *et al*., 2022: 45).

در زمینهٔ حمایت از سیاست‌های ضد تروریستی اتحادیهٔ اروپا نظرسنجی «یورو بارومتر» که در سال ۲۰۱۶ به‌منظور سنجش درک و انتظارات شهروندان اروپایی از اقدامات اتحادیهٔ اروپا علیه تروریسم و افراط‌گرایی انجام شده است، مبین این است که ۸۲ درصد شهروندان اروپایی خواهان افزایش اقدامات و مداخلات اتحادیهٔ اروپا در زمینهٔ مبارزه با تروریسم و افراط‌گرایی هستند. شهروندان اروپایی مبارزه با تأمین مالی تروریسم، مبارزه علیه ریشه‌های تروریسم و افراط‌گرایی، کنترل بیشتر مرزهای خارجی اتحادیهٔ اروپا، افزایش همکاری‌های پلیسی و اطلاعاتی میان کشورهای عضو و مبارزه با قاچاق اسلحه را از مهم‌ترین اولویت‌های اتحادیهٔ اروپا برای مبارزه با تروریسم و افراط‌گرایی برشمرده‌اند. همچنین ۶۱ درصد شهروندان اروپایی مبارزات فراملی در سطح جهانی و منطقه‌ای علیه تروریسم را اثربخش دانسته‌اند (صباغیان و سروستانی، ۱۳۹۷: ۱۶۲).

در سال ۲۰۰۱ کمیسیون اروپا توصیه‌نامه‌ای با عنوان «ایجاد جامعه اطلاعاتی ایمن‌تر از طریق بهبود امنیت زیرساخت‌های اطلاعاتی و مبارزه با جرایم مرتبط با رایانه»[1] صادر کرد که در آن مشکلات ناشی از جرایم سایبری را تجزیه‌وتحلیل و به لزوم انجام اقدامات مؤثر برای مقابله با تهدیدات نسبت به صحت، دسترسی و قابلیت اعتماد سامانه‌ها و شبکه‌های اطلاعاتی اشاره کرد (پورنقدی و بختیاری، ۱۳۹۲: ۴۲).

۶. کنوانسیون بوداپست و پیمان لیسبون

شورای اروپا[2] نقش فعالی در مواجهه با چالش‌های مرتبط با جرایم سایبری داشته است. شروع این فعالیت‌ها به سال ۱۹۷۶ میلادی برمی‌گردد که شورا، کمیته‌ای از کارشناسان با عنوان کمیتهٔ اروپایی بررسی مشکلات ناشی از جنبه‌های حقوقی جرایم رایانه‌ای تشکیل داد. از جمله اقدامات مهم این کمیته

1. Communication from the Commision to the Council, The European Parliament, The Economic & Social Committee & The Committee of Regions, 2001.
2. Council of Europe محسوب نمی‌شود و مقر این سازمان در استراسبورگ قرار دارد و بخشی از اتحادیهٔ اروپایی ۴۷ عضو دارد.

تـدوین متن کنوانسیون شورای اروپا در خصوص جـرایم سـایبری و پروتکـل الحـاقی آن اسـت.[۱] ایـدهٔ تدوین این کنوانسیون که ۴۸ ماده و ۴ فـصل دارد، در سـال ۱۹۹۶ مـیلادی توسـط کمیته مطرح و متن آن در ۲۳ نوامبر سـال ۲۰۰۱ مـیلادی بـرای امـضای اعـضای شـورا مفتـوح شـد. در حـال حاضـر کنوانسیون به‌عنوان یک سند حقـوقی لازم‌الاجرا نقـش مهمی را در راستای مقابله با جـرایم سـایبری ایفـا کـرده و مـورد حمایـت بـسیاری از سازمان‌های بین‌المللی از جمله سـازمان همکـاری و توسـعهٔ اقتـصادی[۲] و اینتر پل است[۳] (Sieber, 2012: 543).

پس از آن پیمان لیسبون که معاهدهٔ اصلاحات نیز نامیده می‌شود، در سـال ۲۰۰۹ بـه اجـرا درآمـد و راهبرد اتحادیهٔ اروپا را درباره مسائل امنیت سایبری وحدت بخشید و برای نخستین بار، وظـایف و حـوزه فعالیت ثابت و مشخص را در زمینه جرایم رایانه‌ای برای اتحادیه اروپـا تعریـف کـرد. در بنـد ۱ مـادهٔ ۸۳ جرایم رایانه‌ای به‌طور مشخص به‌عنوان یکی از حوزه‌های مرتبط جرم ذکر شده است. از آنجـا کـه جـرم سایبری گسترده‌تر از جرم رایانه‌ای است، این تفاوت به اتحادیه اروپا اجازه می‌دهد تا به قاعـده‌مندسـازی هر دو حوزه بپردازد (قدیر و کاظمی‌فروشانی، ۱۳۹۸: ۲۵۳). پیش از این پیمان، سیاسـت امنیـت سـایبری اتحادیهٔ اروپا به‌دلیل وجود سه ستون مسئولیت که بین سیستم سیاسی اروپایی تقسـیم شـده بـود، بسـیار پراکنده بود. این ستون‌ها شامل دادگستری و امور داخلی، جوامع و سیاسـت مشـترک خـارجی و امنیتـی[۴] بودند. تفاهم‌نامهٔ لیسبون این رویکرد را لغو کرد و آن را به رویکـرد راهبـردی یکپارچـه تبـدیل کـرد. در نتیجه، این تفاهم‌نامه به توسعهٔ ابزارهایی برای مبارزه با جـرایم سـایبری کمـک کـرد (Naqvi *et al*., 2022: 50). در پایان دورهٔ برنامهٔ اسـتکهلم در سـال ۲۰۱۴، از راهبـرد امنیـت سـایبری اتحادیـهٔ اروپـا[۵] رونمایی شد. از جمله اهداف این راهبرد، اجرایی کردن یک دورهٔ دوسالهٔ قانونگذاری در اتحادیه اروپـا، در زمینه‌های امنیت و جرایم سایبری بود. در همین زمینه، کارگروهی تحت عنوان «کارگروه مشترک امنیت و جرایم سایبری اتحادیهٔ اروپا–ایالات متحده»[۶] به‌منظور پیگیری قاعده‌مندسـازی جـرایم سـایبری درون اتحادیه تشکیل شد (Elain, 2014: 2).

---

۱. این کمیته ۱۵ عضو داشت و نمایندگانی از کانادا، ژاپن، آمریکا و سـازمان ملـل متحـد بـر آن نظـارت داشتند.

2. Organization for Economic Cooperation and Development
3. International Criminal Police Organization – INTERPOL
4. Common Foreign And Security Policy (CFSP)
5. EU Cyber Security Strategy: An Open, Safe and Secure Cyberspace 2013
6. EU-US Cybercrime and Cyber Security Working Group (WGCC)

۷. آژانس امنیت سایبری اتحادیهٔ اروپا[1]

کشورهای مختلف در دههٔ گذشته با توسعهٔ راهبردهای امنیت سایبری، وضع قوانین امنیت سایبری و اطمینان از اقدامات حفاظتی برای محافظت از داده‌های مشتریان، گام‌هایی را برای مقابله با چالش‌های تهدیدات سایبری برداشته‌اند (Dedeke & Masterson, 2019: 373). حملات سایبری حمایت‌شده توسط دولت–ملت ها پس از سال ۲۰۰۸ به افزایش در توسعهٔ راهبردهای امنیت سایبری منجر شد (Shafqat, 2016: 133). در سال ۲۰۰۴، سازمانی با نام انیسا (ENISA)[2] در زمینهٔ امنیت سایبری توسط اتحادیهٔ اروپا ایجاد شده است. تمامی کشورهای عضو اتحادیهٔ اروپا و کمیسیون اروپا نمایندگانی را در هیأت مدیره دارند. نقش اصلی هیأت مدیره، ایجاد راهبرد و همکاری در توسعه و تصویب اسناد برنامه‌ریزی (برنامه‌های کاری) است. با این حال، طبق داده‌های جمع‌آوری‌شده توسط انیسا، تنها ۱۵ کشور عضو اتحادیهٔ اروپا دارای راهبرد امنیت سایبری ملی محکم هستند و بقیهٔ ۱۲ کشور راهبرد امنیت سایبری قوی ندارند و به همین دلیل اگر به آن نیاز پیدا کنند، ترجیح می‌دهند راهبرد امنیت ملی خود را اجرا کنند (Sliwinski, 2014: 476). راهبرد امنیت سایبری اتحادیهٔ اروپا پنج اولویت راهبردی را برجسته می‌کند که باید با مسائلی که از فضای سایبری ناشی می‌شود، مبارزه شود:

- دستیابی به انعطاف‌پذیری سایبری؛
- کاهش چشمگیر جرایم سایبری؛
- توسعهٔ سیاست‌ها و قابلیت‌های دفاعی مرتبط با سیاست مشترک امنیتی و دفاعی[3] (CSDP) ؛
- توسعهٔ منابع صنعتی و فناوری مورد نیاز برای امنیت سایبری؛
- تعیین سیاست جامع بین‌المللی در فضای سایبری برای اتحادیهٔ اروپا و ترویج ارزش‌های اتحادیهٔ اروپا (Naqvi *et al*., 2022: 49).

۸. دستورالعمل امنیت شبکه و اطلاعات (NIS)[4]

دستورالعمل ۱۱۴۸۱/۲۰۱۶ در خصوص امنیت شبکه و سیستم‌های اطلاعاتی، اولین دستورالعملی است که در سطح اتحادیهٔ اروپا برای حفاظت از شبکه و سیستم‌های اطلاعاتی مصوب شده است. این موضوع در سال ۲۰۱۳ توسط کمیسیون و نمایندهٔ عالی اتحادیهٔ امور خارجه و سیاست امنیتی در راهبرد امنیت

1. The European Union Agency for Cybersecurity
2. www.enisa.europa.eu
3. Developing defiance policy and capabilities related to the Common Security and Defense Policy (CSDP)
4. Network and Information Security (NIS)

سایبری اتحادیهٔ اروپا دنبال شد. از سال ۲۰۱۳ تا ۲۰۱۵ کمیسیون، شورا و پارلمان پیش‌نویس لایحه مطرح‌شده را به‌شدت مورد بحث قرار دادند و این بحث‌ها منجر به تدوین دستورالعمل نیس شد که در اوت ۲۰۱۶ به اجرا درآمد. این دستورالعمل متشکل از ۲۷ ماده است. مواد ۱ – ۶ دامنه و تعاریف اصلی آن، از جمله شفاف‌سازی بیشتر در زمینهٔ شناسایی اپراتورهای خدمات ضروری و همچنین معنی اثر مخرب را تعیین کرده‌اند. مواد ۷ – ۱۰ چارچوب‌های ملی مورد نیاز هر کشور عضو در امنیت شبکه و سیستم‌های اطلاعاتی را توصیف می‌کنند. این چارچوب‌ها عبارت‌اند از: تعهد کشورهای عضو برای معرفی یک راهبرد ملی و تعیین مقامات ذی‌صلاح ملی و تیم‌های واکنش حادثه امنیتی کامپیوتری و نیز ایجاد گروه همکاری. مکانیسم همکاری در فصل سوم و به‌ویژه در مواد ۱۱ تا ۱۳ ارائه شده است. موادی که در ادامه آمده است (۱۴ – ۱۸) به‌ترتیب نیازهای امنیتی و اطلاع‌رسانی حادثه را برای اپراتورها و ارائه‌دهندگان خدمات دیجیتال تعریف می‌کند. پذیرش استانداردها و روند اطلاع‌رسانی در مواد ۱۹ و ۲۰ بررسی می‌شود. در نهایت، مواد ۲۱ – ۲۷ شامل آخرین مفاد بخشنامه می‌شوند (Markopoulou *et al*., 2019: 2). بیانیهٔ نیس در جولای ۲۰۱۶ منتشر شد. این دستورالعمل ریشه در کمیسیون سال ۲۰۰۹ دارد که بر پیشگیری و آگاهی تمرکز دارد و برنامهٔ اقدام فوری برای تقویت امنیت و اعتماد در جامعهٔ اطلاعاتی را تعریف می‌کند (Naqvi *et al*., 2022: 54).

در دسامبر ۲۰۲۰ کمیسیون اروپایی در واکنش به سرعت تحولات جامعهٔ دیجیتال به‌خصوص با بروز بیماری کووید ۱۹ بازبینی «دستورالعمل سیستم‌های شبکه و اطلاعات» را با در نظر گرفتن موارد زیر پیشنهاد کرد: ۱. تقویت تعهدات امنیتی شرکت‌ها؛ ۲. افزایش امنیت زنجیره‌های عرضه؛ ۳. افزایش اقدامات نظارتی برای مقامات ملی[1] که این اقدام در راستای ارائهٔ نامه مشترک توسط کمیسیون و نمایندهٔ عالی اتحادیه در امور خارجه و سیاست امنیتی، با عنوان «راهبرد امنیت سایبری اتحادیهٔ اروپا برای دههٔ دیجیتال»[2] به پارلمان و شورای اروپا با هدف افزایش تاب‌آوری جمعی اروپا در مقابل تهدیدات سایبری و افزایش بهره‌مندی شهروندان و مشاغل و شرکت‌ها از خدمات الکترونیک و دیجیتال با توجه به تحولات و تهدیدات اخیر بود.[3]

نقش «آژانس امنیت سایبری اتحادیهٔ اروپا» در افق پیش رو در دسامبر ۲۰۱۸، کمیسیون اروپا، پارلمان اروپا و شورای اتحادیهٔ اروپا به توافق سیاسی در خصوص قانون امنیت سایبری رسیدند و در مارس ۲۰۱۹، پارلمان اروپا «قانون امنیت سایبری»[4] را تصویب کرد.[5] شورای اتحادیهٔ اروپا ظرف ۲۰ روز

1. www.consilium.europa.eu/en/policies/cybersecurity,2021
2. European Union Cybersecurity Strategy for the Digital Decade
3. European Council Conclusion Draft EU, council conclusion.2021.p.1
4. Cyber security law
5. https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en

این قانون را تصویب کرد و سپس در نشریهٔ رسمی اتحادیهٔ اروپا منتشر شد. راهبرد انیسا برای سال‌های ۲۰۱۶ – ۲۰۲۰ شامل اولویت‌های زیر است:

(الف) پشتیبانی از کشورهای عضو در مواجهه با چالش‌های امنیتی در زمینهٔ شبکه و اطلاعات؛

(ب) ارتقای امنیت شبکه و اطلاعات به‌عنوان اولویت اصلی سیاست اتحادیهٔ اروپا؛

(ج) پشتیبانی از کشورهای عضو در حفظ ظرفیت‌های نیس؛

(د) تقویت جامعهٔ نوظهور اروپا.

در عین حال، انیسا فعالانه با انتصاب نمایندهٔ خود در گروه همکاری و با تشکیل «تیم واکنش سریع حملات سایبری»[1] به مقامات ذی‌صلاح کمک می‌کند. در مادهٔ ۳۶ بیان شده است که با ارائهٔ تخصص باید به کشورهای عضو و کمیسیون کمک کند و هم کشورهای عضو و هم کمیسیون باید بتوانند با انیسا مشورت کنند. همچنین بخش ۳۸ به مسئولیت سازمان برای کمک به گروه همکاری و مشارکت در توسعهٔ دستورالعمل‌ها اشاره دارد. در نهایت، با توجه به بخش ۶۹ کمیسیون باید در هنگام اتخاذ اقدامات اجرایی با انیسا مشورت کند. نقش افزایش‌یافتهٔ انیسا نیز در برخی از مواد دستورالعمل مشهود است (Markopoulou *et al*., 2019: 13).

۹. مرکز مبارزه با تروریسم اروپا[2]

«مرکز ضد تروریسم اروپا» موسوم به ای سی تی سی در پی یک سری حملات تروریستی که در سال ۲۰۱۵ در اروپا به‌وقوع پیوست، تأسیس شد. این حملات به افزایش بی‌سابقهٔ همکاری بین کشورهای عضو اتحادیهٔ اروپا و شرکا و به ایجاد مرکز اختصاصی ضدتروریسم در یوروپل منجر شد. در سال ۲۰۱۶، حملات تروریستی در شهرهای نیس و برلین سبب شد که اتحادیهٔ اروپا با تهدیدات جدیدی از جمله ظهور پدیدهٔ گرگ‌های تنها[3] مواجه شود. این تهدیدات باعث شدند که ارزیابی تهدیدات نسبت به شهروندان اروپایی و زندگی روزمرهٔ آنها تغییر کند و افراد بیشتری مسلح شوند. برای جلوگیری از حوادث تروریستی در اتحادیهٔ اروپا، سیاست‌هایی مانند محدودیت مهاجرت جنگجویان و مصادرهٔ پاسپورت‌ها به‌وجود آمد.

هدف از تجربه و تخصص «مرکز ضدتروریسم اروپا» در تمام زمینه‌های پدیده‌های تروریستی، ارائهٔ پاسخی جامع به تهدید پیوسته در حال تغییر تروریسم در اتحادیهٔ اروپاست. با توجه به این موضوع، این

1. Cyber Security Incident Response Team (CSIRT)
2. European Counter Terrorism Centre (ECTC)
3. Loan wolf در تئوری گرگ تنها، یک فرد به‌واسطهٔ آموزش با شبکه‌های اجتماعی به یک تروریست انفرادی در جامعه تبدیل می‌شود.

مرکز در سال‌های اخیر حمایت خود را از کشورهای عضو اتحادیهٔ اروپا و شرکای خارجی در مقابله با افراط‌گرایی خشونت‌آمیز جناح راست و چپ و همچنین تروریسم با انگیزهٔ مذهبی گسترش داده است. این مرکز برای افزایش توانایی‌های مقامات مبارزه با تروریسم، ابزارهایی را برای رفع نیازهای نوظهور مبارزه با تروریسم ایجاد و توسعه می‌دهد. «مرکز ضدتروریسم اروپا» همچنین ارتباط مقامات ذی‌صلاح در کشورهای عضو اتحادیهٔ اروپا را از طریق پلتفرم‌های مبارزه با تروریسم یوروپل تسهیل می‌کند که سهمی ارزشمند در مبارزه با تروریسم است و تمامی این اقدامات از طریق بستر فضای مجازی صورت می‌گیرد (Kaunert *et al*., 2022: 151).

۱۰. «نهاد هماهنگ‌کنندهٔ مبارزه با تروریسم» در اتحادیهٔ اروپا[1]

پس از حملات تروریستی در مادرید در ۱۱ مارس ۲۰۰۴، رهبران اتحادیهٔ اروپا بیانیه‌ای را در خصوص مبارزه با تروریسم تصویب کردند. از جمله اقدامات دیگر، آنها این بود که با تعیین «نهاد هماهنگ‌کنندهٔ مبارزه با تروریسم اتحادیهٔ اروپا» موافقت کردند. وی نقشی کلیدی در پیشبرد اولویت‌های اتحادیهٔ اروپا در مبارزه با تروریسم مورد توافق وزرای امور داخلی اتحادیهٔ اروپا ایفا خواهد کرد. در ژوئیهٔ ۲۰۲۱، ایلکا سلمی[2] به‌عنوان هماهنگ‌کنندهٔ مبارزه با تروریسم اتحادیهٔ اروپا برای یک دورهٔ پنج‌ساله منصوب شد. او کار خود را با سرفصل‌های ذیل در ۱ اکتبر ۲۰۲۱ آغاز کرد[3]:

- هماهنگی کار شورا در مبارزه با تروریسم؛
- پیشنهاد و ارائهٔ توصیه‌ها و اولویت‌های مربوط به سیاست‌ها به شورا؛
- نظارت بر اجرای راهبرد مبارزه با تروریسم اتحادیهٔ اروپا؛
- نگه‌داشتن یک دید کلی از تمام ابزارهای اتحادیهٔ اروپا، ارتباط با شورا و بازبینی تصمیمات شورا؛
- همکاری با بدنه‌های پیش‌آمادهٔ مرتبط شورا، «کمیسیون و خدمات خارجی اتحادیهٔ اروپا»؛[4]
- تضمین اینکه اتحادیهٔ اروپا نقش مهم خود را در مبارزه با تروریسم ایفا می‌کند؛
- توسعه و بهبود ارتباطات بین اتحادیهٔ اروپا و سایر کشورها (Naqvi *et al*., 2022: 48).

۱۱. «راهبرد امنیت سایبری اتحادیهٔ اروپا در دههٔ دیجیتال» تا سال ۲۰۳۰

کمیسیون اروپا در ۹ مارس ۲۰۲۱ طی قطعنامه‌ای سند چشم‌انداز خود در حوزهٔ دیجیتال تا سال ۲۰۳۰ را

1. EU Counter-Terrorism Coordinator
2. Ilkka Salmi
3. https://www.consilium.europa.eu/en/policies/fight-against-terrorism/counter-terrorism-coordinator/
4. European External Action Service (EEAS)

ارائه داد. در این قطعنامه با عنوان «راهبرد امنیت سایبری اتحادیهٔ اروپا در دههٔ دیجیتال»[1]، موارد زیر به‌عنوان اهداف مطرح شده‌اند[2]:

- حمایت از کشورهای عضو در ایجاد و تقویت مراکز عملیاتی در حوزهٔ امنیت سایبری[3]؛
- راه‌اندازی تیم‌های پاسخگویی به حوادث امنیت سایبری[4] در سطوح ملی و منطقه‌ای؛
- ایجاد مراکز اشتراک‌گذاری و تجزیه‌وتحلیل اطلاعات ملی یا اروپا[5] به‌عنوان بخشی از یک شبکه مؤثر مشارکت امنیت سایبری در اتحادیهٔ اروپا در حوزه‌هایی چون هوش مصنوعی؛
- توسعهٔ یک سیستم اتصال ایمن، مبتنی بر زیرساخت‌های ارتباطی کوانتومی اروپا[6] و ارتباطات ماهواره‌ای دولتی اتحادیهٔ اروپا[7] برای در برگرفتن کل زیرساخت‌های ارتباطات الکترونیکی مانند فضا، زمین و دریا؛
- تقویت مهارت‌های دیجیتال به‌وسیلهٔ افزایش تعداد متخصصان فناوری اطلاعات گسترش بهره‌مندی افراد از مهارت‌های پایهٔ دیجیتال[8]؛
- تسهیل دسترسی به اینترنت جهانی و نیز ارائهٔ یک سرویس جایگزین اروپایی؛
- توسعهٔ طرح‌های صدور گواهینامهٔ امنیت سایبری اتحادیهٔ اروپا؛
- تسریع پذیرش استانداردهای کلیدی اینترنت؛
- تأکید بر تقویت امنیت سایبری جی ۵؛
- پیوند دادن ابتکارات، ساختارها و رویه‌های موجود در اتحادیهٔ اروپا.[9]

به‌منظور نیل به اهداف مذکور، اتحادیهٔ اروپا در حال حاضر سه ساختار جمعی مرتبط به درک تهدید و کنش مشترک در حوزهٔ سایبری دارد:

- «مجمع بین‌المللی امنیت سایبری»[10] که این مجمع هر ساله در شهر لیل فرانسه برگزار می‌شود و سیزدهمین دورهٔ آن در سال ۲۰۲۱ برگزار شد. آخرین راهبرد این سازوکار توسط وزارت امور خارجهٔ

1. The EU's Cybersecurity Strategy for the Digital Decade
2. https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf
3. Security Operation Center (SOC)
4. Cyber Security Incident Response Team (CSIRT)
5. Information Sharing and Analysis Centers (ISAC)
6. European Quantum Communication Infrastructure (EuroQCI)
7. European Union Governmental Satellite Communications (GOVSATCOM)
8. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_fr
9. European Parliament resolution of 10 June 2021 on the EU's Cybersecurity Strategy for the Digital Decade (2021/2568(RSP)) https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_EN.html#ref_1_1
10. Forum international de la cybersécurité (FIC)

فرانسه در دسامبر ۲۰۱۷ ارائه شد که بخشی از پروژهٔ فرانسه در راستای حاکمیت دیجیتال اروپاست؛

- رژیم تحریم‌های سایبری مصوب ۱۷ مه ۲۰۱۹، در ۷ می ۲۰۱۹ شورای اتحادیهٔ اروپا قانونی را تحت عنوان رژیم تحریم‌های سایبری تصویب کرد که شکل تکامل‌یافته «چارچوب پاسخ دیپلماتیک مشترک به فعالیت‌های مخرب سایبری» است که در ۱۹ ژوئن ۲۰۱۷ توسط شورا تصویب شد و هدف آن مقابله با تهدیدهای امنیتی در فضای مجازی در سطح اتحادیهٔ اروپاست؛
- بازار واحد دیجیتال اتحادیهٔ اروپا[1] که در سال ۲۰۱۵ راه‌اندازی شده است.[2]

با توجه به مباحث مذکور مشخص شد که اتحادیهٔ اروپا از تمامی راهکارها اعم از استفاده از نهادهای قانونگذاری جهت به‌روز کردن قوانین، افزایش سطح امنیت، بالا بردن بحث نظارت، استفاده از آموزش‌های تخصصی و گسترش تعاملات بین‌المللی برای پیشگیری هرچه بیشتر و مقابله با تروریسم سایبری استفاده کرده و در این زمینه با انعطاف و روزآمدی بیشتری عمل کرده است.

۱۲. نتیجه

تروریسم سایبری، به‌حدی پویاست که ارائهٔ یک قانون و راهکار ملی و بین‌المللی، نمی‌تواند برای مدت طولانی کارامد باشد. در حال حاضر، اتحادیهٔ اروپا سیاست ساختاردهی انعطاف‌پذیری دارد. همان‌طورکه در گزارش سال ۲۰۲۰ بانک اطلاعاتی جهانی تروریسم[3] ملاحظه شد عواقب وقوع ناآرامی و حملات تروریستی تنها یک کشور را درگیر نمی‌کند، بلکه به‌دلیل وجود فضای مجازی همسایگان و حتی متحدان یک کشور در آن سوی کرهٔ خاکی با وجود هزاران کیلومتر فاصله تحت تأثیر آن حملات خواهند بود؛ ازاین‌رو اروپا دریافته است بهترین روش برای ایجاد امنیت، همکاری هرچه بیشتر و ساختن اعتماد میان دولت‌های عضو است. ازین رو آژانس امنیت سایبری اتحادیهٔ اروپا برای تأمین امنیت اقتصادی، سیاسی و ملی برای کشورهای عضو و شهروندان آنان، تاکنون چندین قانون تصویب کرده و ویرایش و به‌روزرسانی سالانه و گاه ماهانهٔ قوانین و دستورالعمل‌ها و قطعنامه‌های کمیسیون و شورا را در دستور کار خود قرار داده است. آخرین گزارش‌های منتشرشده توسط بانک اطلاعات جهانی تروریسم حاکی از آن است که با اقدامات صورت‌گرفته طی دو سال گذشته حملات در منطقهٔ اروپا کاهش یافته و در خاورمیانه شدت گرفته است؛ اما با این حال نقایص ذیل در بررسی‌های صورت‌گرفته قابل ذکر است:

- اگرچه در حال حاضر مرکز مبارزه با تروریسم اروپا دامنهٔ فعالیت‌های خود را گسترش داده و اتحادیه اختیارات بیشتری به انیسا تفویض کرده است، اما با این حال در این سیاست‌ها نقاط

1. EU digital single market
2. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_EN.html
3. Global Terrorism Database (GTD)

ضعف بسیاری وجود دارد. برای مثال، بیشتر کشورها در جهان از رتبه‌بندی کنوانسیون در مورد جرایم سایبری امتناع می‌کنند، زیرا قانون موجود برای اجرا روشن نیست و به کاهش انتشار نرم‌افزارهای مخرب یا تنظیم رفتار کشورها کمک چندانی نمی‌کند؛

- دستورالعمل تالین فی‌الواقع یک قانون نرم بوده و الزام‌آور و قابل اجرا نیست؛
- اروپا اگرچه اقدام به تشکیل سازمان‌های تخصصی مختلفی همچون مرکز مبارزه با تروریسم اروپا، آژانس امنیت سایبری اتحادیهٔ اروپا و .. کرده اما باز در عمل به اجماع مطلوبی دست پیدا نکرده است؛ به‌طوری‌که طبق داده‌های جمع‌آوری‌شده توسط انیسا، تنها ۱۵ کشور عضو اتحادیهٔ اروپا دارای راهبرد امنیت سایبری هستند و بقیهٔ کشورها اگر به آن نیاز پیدا کنند، ترجیح می‌دهند راهبرد امنیت ملی خود را اجرا کنند؛
- از دیگر نقاط ضعف قابل اشاره این است که دولت‌ها نمی‌توانند تشخیص دهند که حریفشان قانون را رعایت می‌کند یا خیر، بنابراین نمی‌توانند بدانند که آیا از محدودیت خود سود می‌برد یا نه.

به‌طور خلاصه، نبود قوانین ملزم‌کننده برای ادارهٔ رفتار در فضای سایبری یک مسئلهٔ فعلی در حقوق بین‌الملل است که سبب می‌شود دولت‌ها گزینه‌های کمی برای پاسخ و جلوگیری از رفتارهای بدخواهانهٔ سایبری داشته باشند که به بیشتر شدن تناقض‌ها و تضادها منجر می‌شود. اما در نهایت با وجود همهٔ نقایص مذکور، گسترش همین اقدامات ملی و منطقه‌ای می‌تواند رفته‌رفته زمینه‌ساز اجماع‌های بین‌المللی باشد. ازاین‌رو اقدامات ذیل جهت دسترسی به اجماع جهانی توصیه می‌شود:

- الگوبرداری دیگر کشورها و پیاده‌سازی قوانین موجود به‌منظور درک نقاط ضعف و قوت قوانین موجود در جهت توسعهٔ آن؛
- صدور نظریات مشورتی و تفاسیر قانونی بر اساس قوانین موجود از مراجع قانونی و قضایی بین‌المللی؛
- اتخاذ سیاست‌های کیفری اصولی و یکسان جهت واکنش سریع دولت‌ها به حوادث تروریستی؛
- افزایش صلاحیت مراجع قانونی موجود در رسیدگی به جرائم تروریسم سایبری و همچنین تشکیل و تأسیس مراجع جدید جهت رسیدگی قانونی به موضوعات؛ زیرا بیش از هر زمان دیگری، خلأها و نقایص قانون‌ها در مقام رسیدگی قضایی به پرونده‌ها نمود پیدا می‌کند.

منابع

۱. فارسی

الف) کتاب‌ها

۱. ملکوتی، رسول (۱۳۹۸). بررسی وضعیت حقوقی حاکمیت دولت در فضای مجازی. *مجموعه مقالات همایش*

جنبه‌های حقوقی فناوری اطلاعات و ارتباطات ایران. چ دوم، تهران: دانشگاه علم و فرهنگ.
۲. نجفی ابرندآبادی، علی‌حسین؛ هاشم بیگی، حمید (۱۳۹۳). *دانشنامهٔ جرم‌شناسی*، تهران: گنج دانش.
۳. بیابانی، غلامحسین؛ هادیان‌فر، سیدکمال (۱۳۸۴). *فرهنگ توصیفی علوم جنایی*. چ اول، تهران: انتشارات مرکز تحقیقات کاربردی کشف جرایم و امنیت معاونت آگاهی ناجا.
۴. کدخدایی، عباسعلی؛ ساعد، نادر (۱۳۹۰). *تروریسم و مقابله با آن*. مجمع جهانی صلح.
۵. پاکزاد، بتول (۱۳۹۰). *تروریسم سایبری تهدیدی نوین علیه امنیت ملی*، تهران: معاونت آموزشی دانشگاه آزاد.

ب) مقالات

٦. ضیایی، سیدیاسر؛ شکیب‌نژاد، احسان (۱۳۹۶). قانونگذاری در فضای سایبر: رویکرد حقوق بین‌الملل و حقوق ایران. *دوفصلنامهٔ مجلهٔ حقوقی بین‌المللی*، ۳۴(۵۷)، ۲۲۷ ـ ۲۴۷.
۷. امین‌زاده،الهام (۱۳۸۰). تفاوت تروریسم و تلاش برای دستیابی به حق تعیین سرنوشت. *ژرفنا*، (۲۱)، ۸۳-۹۰.
۸. ملکوتی، رسول؛ خلیل‌زاده، مونا (۱۴۰۰). راهکار حقوقی تأمین امنیت سایبری. *فصلنامهٔ مطالعاتی و تحقیقاتی وسایل ارتباط جمعی*، (۱)، پیاپی ۱۲۶، ۶۹-۹۷.
۹. کتانچی، الناز؛ پورقهرمانی، بابک (۱۳۹۸). سیاست‌های نمادین معاهدهٔ جرایم سایبری شورای اروپا، *فصلنامهٔ مطالعات بین‌المللی*، ۱۶ (۲) ۶۲، ۳۱-۴۷.
۱۰. امین‌زاده، الهام،(۱۳۷۸). نگاهی اجمالی به ابعاد حقوقی – سیاسی تروریسم بین‌المللی و نهضت‌های رهایی‌بخش. *مجلهٔ سیاست خارجی*، ۱۳(۴)، ۱۲۶۳-۱۲۷۵.
۱۱. احمدی، نجمه، (۱۳۹۷). خصیصه‌های حقوقی تروریسم سایبری، مجله فقه، حقوق و علوم جزا، شماره ۷،صص ۴۸-۵۸
۱۲. خلیلی‌پور رکن‌آبادی، علی؛ نورعلی وند، یاسر (۱۳۹۱). تهدیدات سایبری و تأثیر آن بر امنیت ملی، *فصلنامهٔ مطالعات راهبردی*، ۱۵(۲)، شمارهٔ مسلسل ۵۶، ۱۶۷-۱۹۶.
۱۳. عظیمی، فاطمه؛ خشنودی، هادی (۱۳۹۵). نقش تروریسم سایبری در تهدید علیه امنیت ایران و راه‌های پیشگیری از آن. *فصلنامهٔ مطالعات سیاسی*، ۹(۳۴)، ۱۵۹-۱۷۴.
۱۴. یزدانی، عنایت‌الله؛ مرادی، فرزانه؛قنواتی، طیبه (۱۳۹۳). سایبر تروریسم شکل نوینی از ترور علیه منافع ملی.. *فصلنامهٔ پژوهش‌های روابط بین‌الملل*، ۱(۱۳)، ۹-۳۶.
۱۵. بزرگمهری، مجید (۱۳۹۰). مبارزه با تروریسم در سازمان ملل متحد، تحلیلی از تعریف تروریسم و راه‌های مقابله با آن در کنوانسیون‌های مصوب مجمع عمومی. *مجلهٔ رهیافت‌های سیاسی و بین‌المللی*، (۸۲)، ۱۸۱-۲۰۴.
۱۶. صباغیان، علی؛ سروستانی، عباس (۱۳۹۷). سیاست‌های ضد تروریستی اتحادیهٔ اروپا روندها، کارامدی و چشم‌انداز. *فصلنامهٔ مطالعات راهبردی*، ۲۱(۱)، شمارهٔ مسلسل ۷۹، ۱۳۹-۱۶۴.
۱۷. پورنقدی، بهزاد و ارشد بختیاری؛ تروریسم سایبری و اهمیت آن در برهم زدن امنیت بین‌المللی، مطالعات بین‌المللی پلیس، ۴(۱۴)، تابستان، ۲۹-۴۶.

۱۸. قدیر، محسن؛ کاظمی فروشانی، حسین (۱۳۹۸). بررسی تطبیقی حقوق کیفری ایران با اسناد بین‌المللی در زمینهٔ مقابله و پیشگیری از وقوع تروریسم سایبری. *مجله حقوقی بین‌المللی*، (۶۰) ۲۳۷-۲۶۷.

۲. انگلیسی

A) Books

1. Christian K., Alex MacKenzie, & Sarah Léonard, (2022). *The European Union as a Global Counter-Terrorism Actor,* Institutions in EU counter-terrorism, DOI: https://doi.org/10.4337/9781782548287.
2. Evan, T., Leverett, E., Ruffle, S. J., Coburn, A. W., Boudreau, J., Gunaratna, R., & Ralph, D. (2017). *Cyber Terrorism: Assessment of the Threat to Insurance; Cambridge Risk Framework series; Centre for Risk Studies,* University of Cambridge.
3. Renard, T. (2017). *Terrorism and Counterterrorism in Continental Europe*. in: Jacinta Carroll, Counterterrorism. The Australian Strategic Policy Institute.
4. Sieber, U. (2012). *Information Technology Crim Carl HeymannsVerlag KG,576*.
5. Spaaij, R. (2011). *Understanding Lone Wolf Terrorism: Global Patterns, Motivations and Prevention*. Springer Science & Business Media.
6. Thomas C. Wingfield, The Law of Information Conflict: National Security Law in Cyberspace, Aegis Research Corp., Falls Church, VA (2000); ISBN: 0-9670326-I-X
7. Walace, H., Pollack, M. A. & Young, A. R. (2021). *Policy-Making in the European Union.* Seventh Edition, Oxford University Press.
8. Wingfield, T. (2000). *The Law of Information Conflict: National Security Law in Cyberspace*, Aegis Research Corporation, ISBN 096703261X, 9780967032610, Length

B) Articles

9. Aldalbeeh, A., & Alsharqawi, A. (2023). Cyber terrorism and its role in the outbreak of international crisis. *International Journal of Electronic Security and Digital Forensics* 15.1 , 24-32.
10. Chertoff, M. (2008), The cybersecurity challenge. Regulation & Governance, (2), 480-484. https://doi.org/10.1111/j.1748-5991.2008.00051.x
11. Dedeke, A., Masterson, K., (2019). Contrasting cybersecurity implementation frameworks (CIF) from three countries. Information & Computer Security 27, (3), 373–392. https://doi.org/10.1108/ICS-10-2018- 0122.
12. Dimitra Markopoulou, Vagelis Papakonstantinou, Paul de Hert (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review*, 35(6), 1-11/ https://doi.org/10.1016/j.clsr.2019.06.007
13. DOI:10.1017/S1867299X00002944
14. Dunn Cavelty, M. & Smeets, M. (2023). Regulatory cybersecurity governance in the making: The formation of ENISA and its struggle for epistemic authority. *Journal of European Public Policy*, 1-23.
15. Elain, F. (2014). The EU Cybercrime & Cyber – Security Rule-Making: Maping the Internal & External Dimensions of EU Security. *European Journal of Risk Regulation* ,

5(1), 46 – 60.
16. Goldsmith, J. (2013). How Cyber Changes the Laws of War. *European Journal of International Law,* 24(1), 129-138.
17. Katagiri, N. (2021). Why international law and norms do little in preventing non-state cyber-attacks. *Journal of cybersecurity*, 7(1-9).
18. Lord, Kristin M. & Sharp, T. (2011). America's Cyber Future Security and Prosperity in the Information Age, *Center for a New American Security*, (I), 12-19.
19. Monshipouri, M., & Prompichai, T. (2018). Digital Activism in Perspective: Palestinian Resistance via social media, *International Studies Journal* (ISJ) 14(4), 37 – 57.
20. Naqvi, A. A, Javaid, A., & Jalal, I.(2022) From Cyber Security to Cyber-terrorism: A New Emerging threat for Europe and the challenges for EU. *Journal of Politics and International Studies*, 8(2), 45–57.
21. Odebade, A., & Elhadj, B. (2023). A Comparative Study of National Cyber Security Strategies of ten nations. *Cornel University,* 1-19 DOI: 10.48550/arXiv.2303.13938.
22. Oleksiewicz, I. (2016). Dilemmas and challenges for EU anti-cyber-terrorism policy: The example of the United Kingdom. *Politechnika Rzeszowska*, 135-146.
23. Osula, A.M., Kasper, A. & Kajander, A., (2022), EU Common Position on International Law and Cyberspace, Masaryk University Journal of Law and Technology, 16(1), pp.89-123.
24. Schaap, A.J, (2009). Cyber Warfare Operations: Development and Use under International law. *Air Force law review*, (64), 123-142,
25. Shafqat, N., & Masood, A., Z. (2016). Comparative Analysis of Various National Cyber Security Strategies. *International Journal of Computer Science and Information Security*, 129-136.
26. Sliwinski, K. F. (2014). Moving beyond the European Union's Weakness as a Cyber-Security Agent. In *Contemporary Security Policy*, 35(3), Taylor & Francis, 468-486.
27. Spper, D. (2000). Redefining borders, The challenges of cyber-crime. Marquette university. *Political science department. Crime. Law & Social change*. 24- 34.
28. Tabansky, L. (2011). Basic Concepts in Cyber Wafare. *Military and Strategic Affairs,* 3(1), 75-92.
29. Zerzri, M. (2017). The Threat of Cyber Terrorism and Recommendations for Countermeasures. *Center of Applied Perspective on Tunisia*, (4), 1-6.

C) Documents

30. D'Agostino, D. M. (2011). Defense Department Cyberefforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities. United States: DIANE Publishing Company
31. Holloway, Michael. (2015). Stuxnet Worm Attack on Iranian Nuclear Facilities. California: Stanford University
32. Joint statement by the EU home affairs ministers on the recent terrorist attacks in Europe/ Council of the EU Press release 13 November 2020
33. Ozeren, Suleyman (2005)" Global Response to Cyber terrorism And Cybercrime: A Matrix for International Cooperation and Vulne ability Assessment", University of North Texas
34. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10

March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance), as amended by Regulation (EC) No 1007/2008 and amended by Regulation (EC) No 580/2011.
35. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation
36. Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.
37. Wesseling, M. (2016). An EU Terrorist Finance Tracking System. London: Royal United Services Institute for Defence and Security Studies

D) Websites

38. http://large.stanford.edu/courses/2015/ph241/holloway1
39. http://www.eurica.ir/?p=26434
40. https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf
41. https://ec.europa.eu/homeaffairs/what-we-do/policies/organized-crime-and-humantrafficking/cybercrime_en
42. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_fr
43. https://www.consilium.europa.eu/en/policies/fight-against-terrorism/counter-terrorism-coordinator
44. https://www.consilium.europa.eu/en/press/press-releases/2020/11/13/joint-statement-by-the-eu-home-affairs-ministers-on-the-recent-terrorist-attacks-in-europe/
45. https://www.dragonflyintelligence.com/intelligence/terrorismtracker/
46. techopedia.com
47. www.merriam-webster.com