نوع مقاله: **پژوهشی**

تاریخ دریافت: ۱۴۰۰/۰۷/۲۵
تاریخ پذیرش: ۱۴۰۰/۱۱/۲۸
صفحه: ۱ الی ۲۳

International Legal Research
تحقیقات حقوقی بین المللی

Volume 15, Issue 55, Spring 2022

Received: 2021/10/17
Date of Acceptance: 2022/02/17
Pages: 1-23

System: alr.iauctb.ac.ir doi: 10.30495/ALR.2022.1951703.2279 Article Type: **Research**

دوره ۱۵ / شماره ۵۵ / بهار ۱۴۰۱

The necessary for a coordinated international police criminal policy in the confronting against cybercrime

Ebrahim Rajabi Taj Amir[1]

Abstract

Field and Aims: In the present era, one of the new challenges for the police is to deal with cybercrime. Given the vastness and networking of cyberspace, it must be acknowledged that tackling cybercrime will be due to the extent of the damage and the large number of victims, cross-border and the difficulty of detecting and prosecuting the perpetrator, and many other police-only characteristics.

Method: This is a qualitative and applied research in terms of purpose and in terms of collecting information by documentary method and studying international documents, sources related to the subject and the obtained information has been analyzed descriptively-analytically.

Findings and Conclusion: The criminal policy governing cybercrime in Iran relies more on government response with a focus on national security. The lack of police dynamism, the lack of international cooperation and the lack of a homogeneous police criminal policy structure at the global level have challenged the criminal policy of the Iranian police in the fight against cybercrime. Therefore, in order to achieve the desired result and facilitate international police cooperation in order to reduce the challenges ahead, as well as to build capacity in the fight against cybercrime, an effective coordinated international criminal police policy through international police cooperation mechanisms against cybercrime is necessary. And specializing in cybercrime units, providing equipment and facilities for advanced cybercrime hardware and software, adopting international frameworks for police cooperation in cybercrime, and establishing a coherent international police policy in the face of cybercrime.

Keywords: criminal policy, international cooperation, police, cybercrime.

❋Citation (APA): Rajabi Taj Amir, E. (2022). The necessary for a coordinated international police criminal policy in the confronting against cybercrime. *International Legal Research*, 15(55), 1-23. http://alr.iauctb.ac.ir/article_689315.html?lang=en

1. Assistant Professor, Department of Criminology, Faculty of Law Enforcement Sciences and Technology, Amin University of Law Enforcement Sciences, Tehran, Iran.
Email: E.rajabi.t@gmail.com

Volume 15, Issue 55, Spring 2022

Received: 2021/10/17
Date of Acceptance: 2022/02/07
Pages: 1-23

تحقیقات حقوقی بین المللی
International Legal Research

نوع مقاله: **پژوهشی**

تاریخ دریافت: ۱۴۰۰/۰۷/۲۵
تاریخ پذیرش: ۱۴۰۰/۱۱/۲۸
صفحه: ۱ الی ۲۳

Article Type: **Research**

doi: 10.30495/ALR.2022.1951703.2279

سامانه: alr.iauctb.ac.ir

دوره ۱۵ / شماره ۵۵ / بهار ۱۴۰۱

ضرورت اتخاذ سیاست جنایی هماهنگ بین‌المللی پلیس در مقابله با جرایم سایبری

ابراهیم رجبی تاج امیر[۱]

چکیده

زمینه و هدف: در عصر حاضر یکی از چالش‌های جدید پلیس، مقابله با جرایم سایبری است. با توجه به گستردگی و شبکه‌ای بودن فضای سایبر، باید اذعان داشت مقابله با جرایم سایبری به جهت گستردگی خسارت و کثرت بزه‌دیدگان، فرامرزی بودن و مشکلات کشف و تعقیب مجرم و بسیاری ویژگی‌های دیگر تنها با سیاست جنایی هماهنگ بین‌المللی پلیس میسر خواهد بود.

روش: این پژوهش کیفی و به لحاظ هدف، کاربردی و از نظرگردآوری اطلاعات به روش اسنادی و مطالعه اسناد بین المللی، منابع مرتبط با موضوع انجام شده و اطلاعات به دست آمده به صورت توصیفی-تحلیلی مورد تجزیه و تحلیل قرار گرفته است.

یافته‌ها و نتایج: سیاست جنایی حاکم بر جرایم حوزهٔ سایبر در ایران بیشتر متکی به پاسخ‌دهی از طریق دولت با محوریت قرار دادن امنیت ملی می‌باشد. عدم پویایی پلیس، عدم همکاری بین‌المللی و نبود ساختار سیاست جنایی پلیسی همگون در سطح جهانی، سیاست جنایی پلیس ایران را در مقابله با جرایم سایبری با چالش روبرو نموده است. از این رو، برای رسیدن به نتیجهٔ مطلوب و تسهیل همکاری‌های بین‌المللی پلیس به‌منظور کاهش چالش‌های پیش‌رو، همچنین ایجاد ظرفیت‌سازی در راه مبارزه با جرایم سایبری لزوم یک سیاست جنایی پلیسی مؤثر هماهنگ بین‌المللی از طریق سازوکارهای همکاری بین‌المللی پلیس در مقابله با جرایم‌سایبری، ارتقای توان علمی و تخصصی واحدهای مبارزه با جرائم‌سایبری، تهیهٔ تجهیزات و امکانات سخت‌افزاری و نرم‌افزاری پیشرفته مبارزه با جرایم‌سایبری، اتخاذ چارچوب‌های بین‌المللی همکاری پلیس در مقابله با جرایم‌سایبری و ایجاد سیاست منسجم بین‌المللی پلیس در مقابله با جرایم‌سایبری ضرورت می‌یابد.

کلیدواژه‌ها: سیاست جنایی، همکاری‌های بین‌المللی، پلیس، جرایم سایبری.

❋استناددهی (APA): رجبی تاج امیر، ابراهیم. (۱۴۰۱). ضرورت اتخاذ سیاست جنایی هماهنگ بین‌المللی پلیس در مقابله با جرایم سایبری. *تحقیقات حقوقی بین‌المللی*، ۱۵(۵۵)، ۲۳-۱.

http://alr.iauctb.ac.ir/article_686934.html

۱. استادیار گروه جرم‌شناسی دانشکده علوم و فنون انتظامی دانشگاه علوم انتظامی امین، تهران. ایران. رایانامه: E.rajabi.t@gmail.com

مقدمه

جرم شناسی در آغاز سده بیست و یکم با محیط یا فضای جدیدی روبرو شده است که فرآیند جهانی شدن را، به طور کلی و جهانی شدن بزهکاری را، به ویژه تسریع و تسهیل کرده است.

دوزیست شدن انسان‌ها «زیست حقیقی» و «زیست مجازی» یا سایبری یا دوگانه شدن فعالیت‌ها و روابط اشخاص و به تبع آنها، دوگانه شدن بزهکاری و در نتیجه، ظهور بزهکاران/ بزه‌دیدگان سایبری، جرم‌شناسان و جامعه‌شناسان جنایی را به سوی مطالعه علت‌شناختی و نظریه‌پردازی در حوزه بزهکاری سایبری سوق داده است (نجفی ابرندآبادی، ۱۳۹۵: ۲۵).

در سال‌های پیش رو، بی‌تردید شاهد گسترش مطالعات در جرم‌شناسی و بزه‌دیده‌شناسی سایبری خواهیم بود (جیشنکار[1]، ۲۰۱۱)؛ زیرا امنیت ملی کشورها و امنیت بین‌المللی جامعه جهانی بیش از پیش نه تنها از سوی بزهکاری و بزهکاران جهانی، بلکه از جانب جرایم سایبری و بزهکاران فعال در حوزه فن‌آوری ارتباطات و اطلاعات، یعنی مجرمان سایبری در معرض تهدید جدی است. در همین چهارچوب، تهدید مرتکبان جنایات بین‌المللی برای امنیت ملی جوامع دموکراتیک و نیز امنیت بین‌المللی قابل‌بررسی است.

جرایم سایبری از جمله جرایم نوظهوری است که مبارزهٔ مؤثّر با آن در پرتو راهبردهای پیشگیری از وقوع جرم، حمایت از بزه‌دیده و تعقیب کیفری مرتکب آن صورت می‌گیرد. دولت‌ها نقش مهمی در تضمین فضای مجازی آزاد و ایمن دارند تا با ایجاد سازوکارهای مناسب اجرایی به مبارزه با این نوع جرایم بپردازند. این حوزه از جرایم از مسائل جدید در نظام حقوقی ملی و فراملی بوده و در آینده‌ای نه‌چندان دور با حجم انبوهی از جرایم داخلی و برون‌مرزی در این خصوص مواجه خواهیم شد. از این رو، درباره جرایم سایبری باید در ابتدا به ماهیت فراملی آنها توجه کرد. به دلیل بین‌المللی بودن فناوری‌های سایبری، معمولا این جرم به صورت بین‌المللی محقق می‌شوند (یزدان‌پناه‌درو و کامران، ۱۳۹۳: ۶۷). به همین دلیل، پیشگیری و مبارزه با این جرم، با اقدامات مستقل کشورها محقق نخواهد شد. با توجه به تحولاتی که در قرن حاضر در عرصه‌های مختلف اتفاق افتاده است، دولت‌ها نیازمند ایجاد تشکیلات منظمی هستند تا بتوانند با همکاری و همبستگی بین‌المللی، در رسیدن به اهداف مشترک یکدیگر را یاری کنند (مشهدی و تسخیری، ۱۳۹۲: ۱۵ و ۱۶). در این میان، مبارزه با جرم توجه روزافزون سازمان‌های بین‌المللی را به خود جلب کرده است. در این شرایط باید سازمان‌های بین‌المللی، که تنها علت وجودی آنها برطرف کردن مشکلات بین‌المللی است، به جرم فراملی نیز به عنوان مسئله‌ای بین‌المللی نگریسته و برای برطرف ساختن آن تلاش کنند (زیبر، ۱۳۹۱: ۳۵۵). آنچه در این زمینه اهمیت دارد، ایجاد گفتمان مشترک بین‌المللی برای پیشگیری از جرم سایبری است. برای ایجاد این گفتمان، سازمان‌های بین‌المللی باید

1. Jaishankar

به جرم سایبری به منزله دغدغه یا مشکلی بین‌المللی بنگرند.

فضای سایبر مفاهیم سنتی قدرت جزایی و حاکمیت را که پیش از این با سرزمین و دولت-ملت گره خورده بودند، به چالش کشانده است. ماهیت پخش فضایی فضای سایبر و جرم سایبر مجموعه‌ای از چالش‌ها را برای نهادهای عدالت کیفری که سعی در کنترل پدیده دارند، ایجاد کرده است؛ به نحوی که سیستم‌های قانونگذاری مختلف برای کنترل و محاکمه موثر این پدیده با مشکل مواجه‌اند.

ماهیت غیرسرزمینی فضای سایبر و جرم سایبر چالشی نظری برای اندیشمندان جرم‌شناسی نیز می‌باشد. تئوری‌های خرده‌فرهنگ‌های سنتی، تئوری کنترل و روابط حاشیه‌نشینی با محرومیت اجتماعی با پیدایش فناوری‌های جدید به چالش کشانده شده‌اند (یار، ۱۳۹۰: ۲۵۹).

چالش‌های پلیسی‌گری در فضای سایبر که تعامل اجتماعی، محدودیت‌های فضای فیزیکی را ندارند، دوچندان شده است؛ مثل هرزه‌نگاری کودکان که مجرمان و قربانیان ممکن است در کشورهای مختلف باشند. از چالش‌های دیگر، تحقیق در خصوص محل وقوع جرم است که بخش مهمی از فرهنگ جرم‌شناسی و پلیسی‌گری محسوب می‌شود.

همچنین، رویکردهای متعددی از جمله فعالیت عادی، مناطق جرم‌خیز، پلیسی‌گری جامعه‌محور و رویکردهای مشابه همگی قدرت خود را از ایجاد رابطه میان پلیسی‌گری و سرزمین می‌گیرند. این در حالی است که پلیسی‌گری فضای سایبر، حرکتی از پلیسی‌گری سرزمین به سوی پلیسی‌گری جمعیت‌های مظنون است. و در عین حال حرکتی است از سوی نظارت به داده‌بینی. لذا، مقابله با جرایم سایبر، راهکارهای بین‌المللی را می‌طلبد، زیرا که این مسئله اساسا جهانی است. البته، با وجود کنوانسیون جرم سایبری اروپا این راهکارها در حال شکل گرفتن هستند. هدف از این کنوانسیون آن است که دولت‌ها از طریق قوانین داخلی اشکال مختلفی از جرم سایبری جرم‌انگاری کنند و آئین‌های دادرسی ضروری برای بررسی چنین جرایمی را در چارچوب صلاحیت قوانین ملی خود بگنجانند. البته، پلیسی‌گری فضای سایبر که بالقوه غیرقابل‌کنترل است، علاوه بر دخالت دولت‌ها، نیازمند انتقال مسئولیت‌پذیری به کاربران و همکاری معماران سیستم است. مفهوم پلیسی‌گری چندگانه و تقسیم وظایف انتظامی یکی از علائم حاکمیت بر فضای سایبر است. لذا، مشکلات ناشی از ماهیت فراسرزمینی فضای سایبر جنبه‌های متعددی از معیارهای در حال تغییر زمامداری جزایی معاصر را نشان می‌دهد که در آن چندپارگی و فاصله به شدت افزایش می‌یابد. بر این اساس، جرایم سایبر نیازمند همکاری‌های بین‌المللی فراوان پلیس و حجم انبوهی از کار کارشناسی است. و رویکرد مسئولیت‌پذیری و تعدد پلیسی‌گری از جنبه‌های حیاتی حاکمیت بر فضای سایبر تلقی می‌شود. به‌نظر می‌رسد در وضع کنونی، سیاست جنایی پلیس در ایران، کارایی مؤثر را برای پیشگیری از جرایم سایبری دارا نبوده و علیرغم افزایش جرایم سایبری، پلیس

نتوانسته است به‌طور مؤثر به تهدیدات مطرح شده واکنش نشان دهد و این به دلیل آماده نبودن بستر و زمینه برای سیاست هماهنگ پلیس در بُعد بین‌المللی می‌باشد. بر همین اساس، مهم‌ترین مسئله این پژوهش، پاسخ‌گویی به این پرسش اساسی است که سیاست جنایی پلیس در مقابله با جرایم سایبری چگونه باید باشد؟

۱. ادبیات نظری

۱-۱. جرایم سایبری

از دهه ۶۰ تا اواخر دهه ۸۰ میلادی، نسل نخست جرائم سایبری [1]ظهور پیدا کردند. در این برهه، بزهکاران رایانه‌های کاربران را به عنوان سیبل و هدف بزه برمی‌گزیدند و از آن به عنوان ابزاری برای ارتکاب جرائم سنّتی همچون کلاهبردار ی و سوءاستفاده‌ای مالی استفاده می‌کردند. نسل دوم جرائم سایبری[2]، از دهه ۸۰ آغاز و تا اواخر دهۀ ۹۰ ادامه داشت. ویژگی غالب این نسل را میتوان در رابط بودن بین جرائم نسل اول و سوم دانست، چراکه پیش از آنکه به عنوان یک نسل از جرائم با ویژگیهای خاص مورد توجه قرار گیرد، پل ارتباطی میان نسل اول و سوم بوده است. دلیل بارز آن هم عمر بسیار کوتاه این نسل است که به سرعت با ظهور نسل سوم منتفی شد (جلالی فراهانی، ۱۳۸۴: ۱۴۰). در این نسل، جرائم علیه داده‌ها و محتوا مورد توجه قرار گرفت و بزهکاران غالباً به داده‌های موجود در رایانه‌ها نفوذ می‌کردند. از همین رو، در این دوره توجه قانون‌گذاران داخلی و منطقه‌ای به مباحث حمایت از داده‌ها جلب شد و صیانت از محرمانگی[3] تمامیت [4] و دسترس‌پذیری[5] اطلاعات مورد توجه قرار گرفت.

نسل سوم جرائم سایبری[6]، در اواسط دهه ۹۰ شکل گرفت و با عناوینی همچون جرائم سایبری، جرائم مجازی، جرائم محیط سایبری شناخته می‌شود. این نسل از جرائم به واسطۀ ظهور فناوریهای ارتباطی که امکان ارتباط با همگان را فراهم می‌کردند، شکل گرفت. این نسل از جرائم بدون وجود اینترنت قابل‌ارتکاب نمی‌باشند و به عبارت دیگر، اینترنت شرط لازم تحقق آن‌ها است (برایانت ها[7]، ۲۰۱۴: ۳۲).

نهادهای منطقه‌ای و بین‌المللی نیز سعی در ار ائه تعریفی جامع از جرائم سایبری کرده‌اند. به عنوان نمونه، سازمان همکاری و توسعه‌ی اقتصادی، جرائم سایبری را هر عمل غیرقانونی، غیراخلاقی یا غیرمجاز نسبت به پردازش خودکار و یا انتقال داده‌ها تعریف کرده است (زیبر، ۱۳۹۰: ۱۸). از طرفی دیگر، کنوانسیون جرائم سایبری شورای اروپا نیز، جرائم سایبری را تحت

1. First generation of cybercrimes
2. Second generation of cybercrimes
3. Confidentiality
4. Integrity
5. Accessibility
6. Third generation of cybercrimes
7. Bryant

چهار گروه جرائم علیه محرمانگی، تمامیت و دسترس‌پذیری سیستم‌ها و داده‌های رایانه‌ای[1]، جرائم مرتبط با رایانه[2]، جرائم مرتبط با محتوا[3] و جرائم مرتبط با نقض حق نشر و حقوق مرتبط[4] تقسیم کرده است . لیکن، تعریفی مستقل از جرائم سایبری ارائه نداده و به تقسیم‌بندی مذکور اکتفا کرده است.

به هر رفتار غیرقانونی که با استفاده از وسایل الکترونیکی ایجاد می‌شود و امنیت سیستم‌های کامپیوتری و اطلاعات پردازش شده آنها را مورد هدف قرار می‌دهد، جرایم سایبری گفته می‌شود (برودهد، ۲۰۱۸؛ آدومی و ایگان، ۲۰۰۸). هرگونه رفتارغیرقانونی که بوسیله سیستم‌ها و شبکه‌های کامپیوتری انجام می‌شود، جرایم سایبری گفته می‌شود (چن و همکاران، ۲۰۱۴).

مهمترین چالش در خصوص جرایم رایانه‌ای، تعریف آن است. تا آنجا که در کنوانسیون جرایم سایبری ۲۰۰۱ در بوداپست نیز تعریفی از این جرایم به عمل نیامده است. طبق تعریف ارائه شده از سوی گروهی از کارشناسان همکاری و توسعهٔ اقتصادی[5] در سال ۱۹۸۳، جرایم رایانه‌ای را «هر عمل غیرقانونی، غیراخلاقی یا غیرمجاز نسبت به پردازش خودکار یا انتقال داده‌ها» عنوان کرده‌اند (ذبیح الله نژاد، ۱۳۹۶: ۱۴).

در مجموع، فضای سایبری، محیطی همه‌گیر است که جرایم ارتکابی در آن را در فضایی جهانی مطرح می‌سازد. ایجاد قاعده و نظم بین‌المللی در این فضا مستلزم ایجاد تعهد به مجموعه قواعد بسیار عام و فراگیری است که با وجود تنوع فرهنگی، سیاسی، اقتصادی و... موجب الزام جهانی و کاهش جرم سایبری شود. در این راستا، کارآمدترین سازمان بین‌المللی برای ایجاد نظم در فضای سایبری، سازمان ملل متحد است.

۱-۲. سیاست جنایی اجرایی

سیاست جنایی اجرایی سیاستی است که قوهٔ مجریه و اعضای آن از جمله پلیس برای سیاست جنایی تقنینی و به‌منظور پیشگیری از وقوع جرم یا گسترش آن در جامعه اتخاذ می‌کنند (میرخلیلی و یعقوبی، ۱۳۹۶: ۱۰۲). در عرصهٔ سیاست جنایی اجرایی از یک سو، نقش و عملکرد مجریان و ضابطان دادگستری در مرحلهٔ اولیهٔ رویارویی با پدیدهٔ جنایی، یعنی کشف جرایم و تعقیب متهمین مطرح است و از سوی دیگر، عملکرد این نهادها و به‌طورکلی عملکرد و نقش قوهٔ مجریه در مرحلهٔ پاسخ‌گویی به جرایم و انحرافات، یعنی سطوح اجرای احکام و تصمیمات و بسترسازی در راستای پیشگیری از پدیدهٔ جنایی ظاهر می‌شود؛ بر این اساس، سیاست جنایی اجرایی، قلمرو و اقتدار قوهٔ مجریه را در امور کلان جنایی انعکاس می‌بخشد که همسو با دستگاه قضا از جمله

1. Offences against the confidentiality, integrity and availability of computer data and systems
2. Computer-related offences
3. Content-related offences
4. Offences related to infringements of copyright and related rights
5. Organization for Economic Cooperation and Development (OECD)

ارکان اصلی و حقیقی تقویت مدیریت و انتظام اجتماعی در مواجهه با پدیدهٔ جنایی می‌باشند (کونانی، انصاری و مندنی، ۱۳۹۲: ۶۸). کلیهٔ سیاست‌های اجرایی نهاد پلیس باید بر پایهٔ اصل پیشگیری باشد، زیرا هزینه‌هایی که امر پیشگیری به دنبال دارد، خیلی کمتر از هزینه‌های مواجهه با جرم می‌باشد (حیدری، شهبازی و شیبانی، ۱۳۹۷: ۴۳).

۱-۳. همکاری‌های بین‌المللی

تعریف مشهوری از همکاری بین‌المللی بیان می‌کند که همکاری‌های بین‌المللی عبارت است از: مجموعه‌ای از اصول، هنجارها، قواعد و رویه‌های تصمیم‌گیری صریح و ضمنی که انتظارات بازیگران در ارتباط با آنها، در یک حوزهٔ خاص از روابط بین‌الملل همگرا بوده و نقطهٔ مشترک دارند. اگرچه دولت‌ها، بازیگران اصلی در چنین رژیم‌هایی هستند، اما آنها تنها نیستند؛ دیگر نهادهای بین‌المللی نیز در این زمینه نقش‌آفرینی خواهند نمود (کراسنر[1]، ۲۰۱۳: ۲).

۲. روش‌های همکاری بین‌المللی پلیس در مقابله با جرایم سایبری

در میان انواع سازمان‌های بین‌المللی، سازمان ملل متحد در توسعه و ایجاد همکاری‌های گسترده سیاسی و اقتصادی میان نظام‌های گوناگون اجتماعی، اقتصادی، سیاسی و حقوقی نقش چشمگیری دارد. هم‌اکنون این سازمان، به واسطه انتقال تجربه‌ها، ابتکارها و گسترش فعالیت‌هایش، کانون اصلی گردهم‌آیی‌ها و انجام مذاکره درباره صلح، امنیت و نظم بین‌المللی است (ماده ۵۵ و ۵۶ منشور). در میان جرایم فراملی، جرم سایبری یکی از بین‌المللی‌ترین مصادیق جرایم فراملی و به تبع آن، یکی از محوری‌ترین جرایم مورد توجه سازمان ملل طی دهه‌های اخیر بوده است. گرچه کشورهای عضو، در متضرر بودن از جرم سایبری، با یکدیگر هم عقیده‌اند، اما بر سر سازوکارهای پیشگیری از این جرم هرگز اتفاق‌نظری وجود ندارد. در واقع، عرصه بین‌المللی، عرصه‌ای بسیار متنوع، متعدد و واگراست. از این رو، پیش از هر چیز ایجاد وفاق بین‌المللی درباره این مسئله بین‌المللی ضرورت می‌یابد.

تفاهم‌نامه‌ای مشترک بین یوروپل، اتحادیهٔ اروپا، آژانس دفاع از شبکه و اطلاعات[2]، آژانس دفاع اروپا[3] و تیم واکنش اضطراری رایانه‌ای در سال ۲۰۱۸ امضا شده است: این تفاهم‌نامهٔ مشترک همکاری در حوزه‌هایی مانند عملیاتی کردن و اطمینان از مشارکت نیروی انتظامی و دستگاه قضایی در تمرینات شبیه‌سازی شدهٔ جرایم سایبری و درگیری زودهنگام در پاسخ به بحران‌های پیش رو می‌باشد (پلیس اتحادیهٔ اروپا و دادگستری اروپا، ۲۰۱۹: ۳۱).

1. Krasner
2. ENISA
3. EDA

نقش پلیس در اتحادیهٔ اروپا را باید در مرکز مبارزه با جرایم سایبری اروپا[1] جستجو نمود. کمیسیون اروپا بر پایهٔ مطالعات امکان‌سنجی انجام شده تصمیم به ایجاد مرکز مبارزه با جرایم سایبری در یوروپل گرفت. این مرکز نقطهٔ کانونی و مهم در اتحادیهٔ اروپا برای مبارزه با جرم‌های سایبری و حمایت از ۲۸ عضو این اتحادیه است و کمک می‌کند تا پلیس اروپا واکنش‌های سریع‌تر و دقیق‌تری را در این رابطه اتخاذ نموده و همچنین، در زمینهٔ جرایم سایبری تحقیقات بهتر و همکاری‌های بین‌المللی صورت پذیرد (پلیس اتحادیهٔ اروپا، ۲۰۲۰). یوروپل در سال ۲۰۱۳، مرکز مبارزه با جرایم سایبری اروپایی را برای تقویت اجرای قانون جهت مقابله با جرایم اینترنتی در اتحادیهٔ اروپا و همچنین، کمک به محافظت از شهروندان اروپایی، کسب و کار و دولت در قبال جرایم اینترنتی ایجاد کرد. همچنین، برای این مرکز سه وظیفه در نظر گرفته شد: اول، جرایم سایبری که توسط گروه‌های سازمان‌یافته انجام می‌شود، به‌ویژه افرادی که سودهای بزرگی از اقداماتی نظیر کلاهبرداری آنلاین به‌دست می‌آورند. دوم، جرایم سایبری که صدمات جدی به قربانیان خود وارد می‌کند، مانند سوءاستفادهٔ جنسی آنلاین کودکان. سوم، جرایم سایبری که بر زیرساخت‌های مهم و سیستم‌های اطلاعاتی تأثیر می‌گذارد. با توجه به این سه حوزهٔ فعالیت، انتظار می‌رود که این مرکز به‌عنوان قطب اصلی اطلاعات جنایی خدمت نموده و با تجزیه و تحلیل تخصصی، آموزش و ظرفیت‌سازی موجب هماهنگی عملیات و تحقیقات کشورهای عضو شود. این مرکز در سال ۲۰۱۳ علاوه بر همکاری با مقامات اجرایی قانون در مبارزه با جرایم سایبری، مشارکت‌های مهمی را با تیم‌های واکنش اضطراری[2] رایانه، شرکت‌های مهم اینترنتی و خدمات مالی، صنعت ضدبدافزار، تولیدکنندگان نرم‌افزار و دانشگاه‌ها آغاز نموده (مرکز جرایم سایبری اروپا، ۲۰۱۴: ۴) و از زمان تأسیس، سهم قابل‌توجهی در مبارزه با جرایم اینترنتی داشته است. یوروپول دارای ابزارها و منابع لازم جهت ارزیابی و شناسایی تهدیدات مختلف تا فعالیت‌های جمع‌آوری هوشمند اطلاعات و فعالیت‌های عملیاتی خود، به‌منظور ایجاد امنیت در اروپا است. فعالیت‌های یوروپل عبارت است از: اتخاذ طیف گسترده‌ای از روش‌های مبارزه با جرایم اینترنتی، تجزیهٔ و تحلیل استراتژیک، تجزیهٔ و تحلیل اطلاعات از جمله اطلاعات جنایی و فعالیت‌های اطلاعاتی سایبری، ایجاد تیم‌های مشترک تحقیقاتی و همچنین، فعالیت‌های پیشرفتهٔ بررسی جرم و آموزش و ظرفیت‌سازی آن و اجرای قانون در کشورهای عضو.

یوروپل دارای ساختار منسجم و پیشرفته‌ای است و جای خالی چنین سازمانی در پلیس ایران کاملاً احساس می‌گردد. در رویکرد استراتژی، یوروپل در دو حوزهٔ «استراتژی و توسعه» و «توسعه و مدیریت اشخاص ذی‌نفع» فعالیت می‌نماید (پلیس اتحادیهٔ اروپا، ۲۰۲۰). یکی از اهداف اصلی یوروپل، اختیار اجرای قانون اتحادیهٔ اروپا با پشتیبانی و حمایت عملیاتی در حوزه‌های متعدد

1. European Cybercrime Center = EC3
2. CERT

کیفری است که در زمینهٔ جرایم رایانه‌ای عبارت است از: حملات سایبری، تقلب در پرداخت کارت، تجارت غیرقانونی آنلاین از جمله: مواد مخدر (کوکائین، هروئین، مواد مخدر مصنوعی)، قاچاق غیرقانونی اسلحه گرم، قاچاق انسان، ارزهای مجازی، اسناد جعلی، پولشویی و تقلبی.

مرکز مبارزه با جرایم سایبری اروپا دارای یک هیئت برنامه‌ریزی است و هیئت مذکور جهت دستیابی به اهداف خود و انجام وظایف رسمی، ایجاد مشارکت، مسئولیت مشترک و همکاری با کلیهٔ اعضای هیئت مدیره را در اختیار مرکز قرار می‌دهد. هیئت مرکز مبارزه با جرایم سایبری اروپا سکوی اصلیِ فعالیت های بازیگران مختلف در زمینهٔ تقویت امنیت سایبری و مبارزه با جرایم سایبری را ترسیم کرد. هیئت مذکور دارای اعضای مختلفی است که به شرح ذیل می‌باشد: (برنامه‌های مرکز جرایم سایبری اتحادیهٔ اروپا، ۲۰۲۰): ۱- کالج پلیس اتحادیه‌ی اروپا[1]؛ ۲- تیم واکنش اضطراری (سریع) رایانه[2]؛ ۳- گروه آموزش جرایم سایبری اروپا[3]؛ ۴- آژانس دفاع اروپا[4]؛ ۵- سرویس اقدام خارجی اروپا[5]؛ ۶- آژانس امنیت شبکه و اطلاعات اروپا[6]؛ ۷- واحد همکاری قضایی اتحادیه‌ی اروپا[7]؛ ۸- کمیسیون اروپا[8]؛ ۹- شورای اروپا[9]؛ ۱۰- کارگروه سایبری اتحادیه‌ی اروپا[10]؛ ۱۱- اینترپل[11].

جرایم رایانه‌ای، مبتنی بر فناوری اطلاعات است و در جهان شبکه‌ای امروز، دیگر هیچ جزیره‌ای منزوی محسوب نمی‌شود. از این‌رو، جرایم رایانه‌ای طبع جهانی دارد و مقابله با آنها اقدامات یکسان بین‌المللی را می‌طلبد و چنانچه این جرایم در سیستم‌های قضایی کشورهای مختلف به صورت یکسان تعریف نشوند، تلاش‌های ضابطان اجرایی برای برخورد هماهنگ با این جرایم، غامض و پیچیده خواهد شد. پلیس بین‌الملل، کنوانسیون اروپایی جرایم مجازی همگی در این زمینه به دنبال ادبیات واحدی هستند. به نظر می‌رسد که قواعدی نیز باید وضع گردد تا مسئولیت رسیدگی به جرایم در سطح بین‌المللی را مشخص نماید (حیدری، شهبازی و شیبانی، ۱۳۹۷: ۴۸). باتوجه به جنبهٔ فراملی بودن جرایم رایانه‌ای در حوزهٔ پیشگیری از جرم و آئین دادرسی، کشف جرایم سایبری، تعقیب متهمان، دستگیری، انتقال محکومان، نیابت قضایی و بازجویی رویهٔ یکسانی درکشورها به‌خصوص ایران در بُعد بین‌المللی به چشم نمی‌خورد. در واقع، کشورها ناگزیر هستند در راستای گسترش همکاری‌های بین‌المللی، چهارچوب‌های حقوقی و

1. European Police College
2. Computer Emergency Response Team
3. European Cybercrime Training and Education Group
4. European Defence Agency
5. European External Action Service
6. European Network and Information Security Agency
7. European Union’s Judicial Cooperation Unit
8. European Commission
9. European Council
10. European Union Cybercrime Task Force (EUCTF)
11. INTERPOL

رویه‌های اجرایی جدیدی تعریف نمایند تا سیاست اجرایی بتواند نقش مؤثری ایفا نماید (اشرر[1]، ۲۰۱۲: ۱۳۴).

با توجه به ویژگی فرامرزی بودن برخی جرایم رایانه‌ای، قانون ایران و کنوانسیون جرایم سایبری راهکاری در خصوص جمع‌آوری موجود در خارج از مرزهای کشور ارائه نکرده‌اند و این امر به‌عنوان مهمترین چالش در پلیس سایبری کشورها مطرح شده و راهکاری در این خصوص ارائه نشده است (جلالی فراهانی، ۱۳۹۴: ۴۷). در حالی که، اگر مجرمان و اهداف در کشورهای مختلفی قرار داشته باشند، پیگرد جرم سایبری نیاز به همکاری پلیس در همهٔ کشورهای تحت تأثیر دارد؛ مجرمان نیاز به‌حضور در همان مکانی که هدف قرار گرفته، ندارند. مکان امن در کشورهایی با قانون‌گذاری ضعیف می‌تواند از محدودیت‌های نهادهای اجرایی بین‌المللی باشد (گرکی[2]، ۱۳۸۹: ۱۵۳). این عوامل تهدیدکننده، افزایش پویایی دستگاه‌های اجرایی را ضروری می‌سازد.

۳. ارتقای توان علمی و تخصصی واحدهای مبارزه با جرائم سایبری

نداشتن تخصص کافی نهادهای اجرایی همگام با پیشرفت روزافزون فناوری‌ها در راستای تعقیب و کشف جرایم رایانه‌ای نیز چالش دیگری محسوب می‌شود. تدابیر پیشگیرانه و مقابله ای در صورتی می توانند مؤثر واقع شوند که طرفین درگیر در قضیه قادر به پاسخگویی به درخواست‌های یکدیگر باشند و این امر در گام نخست، نیازمند روزآمد بودن سطح دانش هر یک از نیروهایی است که به نوعی در این فرآیند مشارکت دارند؛ چراکه صرف توان علمی بالای یکی از طرف‌های درگیری نمی‌تواند منجر به موفقیت پیشگیری از بزهکاری سایبری شود و اهمال و کاستی هر یک از طرفین می‌تواند همگان را با خسارات سهمگین سایبری مواجه کند. این شکاف، امروزه میان کشورهای توسعه‌یافته و کشورهای کمتر توسعه‌یافته یا توسعه‌نیافته به وضوح قابل‌مشاهده است. به همان میزانی که کشورهای اخیر با ضعف قوانین خود، پناهگاه‌هایی امن به شمار می‌آیند، عدم آگاهی نیروهای پلیس سایبری آن‌ها نیز بزهکاران را در انتخاب این کشورها مصمم می‌سازد (فرهادی آلاشتی و جوان جعفری بجنوردی، ۱۳۹۶: ۲۵). بدین ترتیب، به سبب عدم هماهنگی آموزشها و مهارت‌های متخصصان با یکدیگر، هر یک از روشها و شیوه‌های گوناگونی برای پاسخگویی به درخواست طرف یا طرف‌های مقابل استفاده می‌کنند و قادر به تعامل مناسب با یکدیگر نیستند و احتمال عدم موفقیت در تأمین خواسته‌های طرف مقابل وجود خواهد داشت.

نتایج سوء ناشی از عدم هماهنگی سطح دانش نیروهای پلیس در سال‌های اخیر از نظر نهادهای بین‌المللی و منطقه‌ای مسئول مبارزه با جرایم سایبری پوشیده نمانده و آنان نیز به این اجماع دست یافته‌اند که هرگونه تلاش برای ایجاد فضای امن و پیشگیری مؤثر از جرایم سایبری در گام نخست

1. Scherrer
2. Gercke

نیازمند دانش تخصصی همگام با شیوه‌های نوین ارتکاب جرم می‌باشد. در حال حاضر، ایران جز صادرکنندگان تکنولوژی رایانه‌ای در دنیا نیست و به تبع، پلیس ایران نیز در زمینه شناسایی، کشف، جمع‌آوری ادله و پی‌جویی جرایم دارای ضعف‌هایی می‌باشد، به گونه‌ای که هر ساله شاهد ورود خسارت‌های هنگفت مالی و حیثیتی به اشخاص اعم از حقیقی و حقوقی هستیم. همچنین، میزان اعتبار ادله جمع‌آوری توسط ضابطان از دیگر چالش‌های بحث است. هرچند به نظر می‌رسد ادله الکترونیکی در چهارچوب نظرات کارشناس اعتبار می‌یابد، ولی نوع نگاه مراجع رسیدگی‌کننده به جرایم سایبری و میزان تخصص و آشنایی آن‌ها با ادله الکترونیکی نقشی تعیین کننده در سرنوشت تعقیب و اثبات این جرایم دارد. جهت تقویت در این حوزه باید به آخرین نوآوری‌ها دست یافته و از طریق همکاری با اینترپل و یوروپل از تجارب آنها بهره‌مند شد. همچنین، ضرورت ایجاد یک نهاد پلیسی بین‌المللی مرتبط با جرم سایبری مانند تشکیل پلیس جهانی اینترنتی می‌تواند نقش پررنگی در مقابله با این جرایم ایفا نماید (محسنی و صوفی زمرد، ۱۳۹۶: ۱۸۰-۱۷۹).

در سالهای اخیر، نهادهای بین المللی و منطقه‌ای مبارزه با جرائم سایبری، فعالیت‌های بسیاری را به منظور ارتقای توان علمی و تخصصی واحدهای مربوطه آغاز کرده‌اند. به عنوان نمونه، مجمع عمومی پلیس بین‌الملل طی نشستی در سال ۲۰۱۰، با تأسیس انجمن جهانی نوآوری پلیس بین‌الملل[1] موافقت کرد. این انجمن اخیراً در کشور سنگاپور شروع به فعالیت کرده و مرکز جرائم دیجیتالی[2] را راه‌اندازی کرده است. یکی از اهداف این مرکز، غلبه بر چالش یاد شده است و برای نیل به این منظور، از اقداماتی همچون توسعهٔ راه‌حل‌های عملی برای همکاری بین نیروهای پلیس، آزمایشگاه‌های تحقیقاتی جرائم سایبری، مجامع دانشگاهی و بخشهای عمومی و خصوصی، ارتقای آگاهی نیروهای پلیس کشورها از طریق انجام تحقیقات مختلف و در اختیار نهادن نتایج آن در دسترس آن‌ها و همچنین، آموزش جدیدترین شیوه‌های پیشگیری از جرائم بهره می‌برد (گیرنو – هیلی[3]، ۲۰۱۳: ۲۸۲).

در اتحادیهٔ اروپا پروژه‌های پژوهشی و اجرایی ویژه‌ای به‌منظور ارتقا مهارت‌های تخصصی پرسنل انتظامی و همچنین، همکاری بین نیروی انتظامی و بخش صنعت انجام یافته، که در چهارچوب برنامه‌های ستون سوم از قبیل ایست[4]، شاهین[5]، اویزین[6] و گروتیوس[7] مورد حمایت قرار گرفته‌اند (سازمان فرهنگ و ارتباطات اسلامی، ۱۳۸۲). کشورهای اتحادیهٔ اروپا همکاری با

1. The INTERPOL Global Complex for Innovation (IGCI)
2. Digital Crime Center
3. Ghernaouti-Hélie
4. stop
5. falcon
6. OISIN
7. GROTIUS

کشورهای ثالث و تأکید ویژه بر یادگیری مداوم از طریق بیان نیازهای آموزشی در رابطه با مسائل مربوط به جرایم سایبری برای مقامات اجرایی را به‌طور جدی پیگیری می‌نمایند. در مجموع، بدنهٔ منسجم قوانین اساسی و رویه‌ای یوروپل و مرکز جرایم سایبری که در درون آن واقع شده است، به طور مؤثرتری به چالش‌های جرایم سایبری پاسخ می‌دهد (کمیسیون اروپا، ۲۰۱۲). مکانیزم‌های بررسی و تضمین کنندهٔ عملکردهای عملیاتی در مرکز جرایم سایبری، پیروی از دستورالعمل و چهارچوب‌های قانونی اتحادیهٔ اروپا با یوروپل می‌باشد (پارلمان اروپا، ۲۰۱۵: ۲۶).

۴. تهیه تجهیزات و امکانات سخت‌افزاری و نرم‌افزاری پیشرفته مبارزه با جرائم سایبری

یکی دیگر از مشکلاتی که فراروی سیاست جنایی هماهنگ بین‌المللی پلیس وجود دارد، شکاف فناورانه‌ای است که بین طرفین درگیر وجود دارد. تهیهٔ تجهیزات و امکانات سخت‌افزاری و نرم‌افزاری موردنیاز این نوع از مقابله، برای همهٔ کشورها میسر نیست. کمبود منابع مالی در برخی از کشورها سبب می‌شود که نیروهای پلیس همهٔ تجهیزاتی که برای مبارزه با جرائم سایبری نیاز است را در اختیار نداشته باشند و نتوانند خود را با استانداردهای جهانی مبارزه با جرائم سایبری هماهنگ سازند (کاشتری[1]، ۲۰۱۰: ۴۰). در واقع، فقدان تجهیزات موردنیاز پیشگیری از بزه سبب می‌شود که در بسیاری از موارد، موقعیت‌های خطر شناسایی نشوند و گمان رود که امنیت تأمین شده است و پس از بروز خسارات و گزارش بزه‌دیدگی ارتکاب جرم مسلّم شناخته شود. در اختیار داشتن ابزارهای بروز و پیشرفته مبارزه با جرائم سایبری از آن رو حائز اهمیت است که گاه برای پیشگیری از این جرائم ثانیه‌ها نیز ارزشمند هستند و هرگونه قصوری نتایج زیان‌باری را در پی خواهد داشت؛ چراکه بعضی از انواع داده‌های رایانه‌ای صرفاً برای مدت زمان کوتاهی قابل‌ذخیره شدن هستند و سپس، پاک خواهند شد. در دیگر موارد، چنانچه شواهد، به سرعت جمع‌آوری نشوند، احتمال ورود خسارات جانی یا مالی اساسی وجود خواهد داشت (شورای اروپا[2]، ۲۰۰۱: ۴۴).

همچنین، از چالش‌های دیگر می‌توان به عدم تناسب آموزش‌های تخصصی با نیازهای جامعه، امنیت پایین شبکه‌های مخابراتی، ضعف زیرساخت‌های مخابراتی و نبود استانداردهای مناسب در ارتباط با تبادل اطلاعات، کدگذاری کالا و خدمات نام برد. این چالش‌ها به سه حوزهٔ دسترسی غیرمجاز، استفادهٔ غیرمجاز و ریزش ناخودآگاه اطلاعات تقسیم می‌گردد. این چالش‌ها موجب سرقت اطلاعات، خرابکاری، از کارانداختن سیستم‌های رایانه‌ای، کلاهبرداری و جاسوسی می‌شود که از جمله تأثیرات مخرب فناوری اطلاعات برای حیات بشری است. توسعهٔ اینترنت در جوامع و

1. Kshetri
2. Council of Europe

گسترش آن حتی به درون منازل و محل کار مردم و نیز جهان‌شمول بودن و وجود خطرات بالقوهٔ آن، چالش‌های جدیدی را ایجاد نموده است (حسن بیگی، ۱۳۸۴: ۱). جرایم رایانه‌ای بیشتر مواقع ماهیتی فنی و تخصصی دارند. ارائه‌دهندگان خدمات سایبری بسیاری اوقات اشخاص حقیقی/ حقوقی غیردولتی هستند. لذا، چنانچه کشورها به‌صورت مستقل مبادرت به آموزش واحدهای فنّی خود نمایند و هماهنگی و تعامل کارآمد و اثربخش میان تمامی دست‌اندرکاران این حوزه به وجود نیاید و همچنین، یک مرکز فرماندهی واحد برای آن‌ها پیش‌بینی نشود، بیش از همه کاربران فنّاوری اطلاعات و ارتباطات یا به عبارت بهتر، شهروندان سایبری لطمه خواهند دید (جلالی فراهانی، ۱۳۸۳: ۱۱۲-۱۱۱).

اتحادیهٔ اروپا از مدت‌ها پیش از پروژه‌های تحقیق و توسعه که به‌منظور بالا بردن ضریب امنیت و اعتماد در زیرساخت‌های اطلاعاتی و مبادلات الکترونیکی به اجراء درآمده‌اند، حمایت می‌کند. همچنین، این اتحادیه اخیراً بودجهٔ مخصوص برنامهٔ مشابهی چون فناوری‌های جامعهٔ اطلاعاتی[1] را افزایش داده است (سازمان فرهنگ و ارتباطات اسلامی، ۱۳۸۲). برای برون‌رفت از چالش‌های فنی نیز می‌توان از دیوار آتش استفاده نمود که یک سری محدودیت را بین دو یا چند شبکه اعمال می‌کند و تا حد زیادی از دسترسی غیرمجاز دنیای بیرون به منابع داخلی جلوگیری می‌نماید. دیگر روش فناوری رمزنگاری می‌باشد که جهت ممانعت از دسترسی دیگران به اطلاعات خصوصی افراد مورد استفاده قرار می‌گیرد. همچنین، استفاده از نرم‌افزارهای ضدپایش می‌تواند راهگشا باشد (سایبانی و کریمی، ۱۳۹۷: ۱۳۲). رمزگذاری قوی یکی از عناصر اساسی دمکراسی‌های دیجیتالی محسوب شده و به حفاظت از امنیت دیجیتالی ما کمک می‌کند. تحقیقات مقامات اجرایی اتحادیه اروپا نشان می‌دهد که نوعی رمزگذاری به‌طور مؤثر و نامحدود اطلاعات و شواهد حیاتی و فعالیت‌های نامشروع را از اجرای قانون پنهان می‌کند. اقداماتی در یوروپل، یوروجاست و شبکه جرایم رایانه‌ای قضایی اروپا برای ارزشیابی پیشرفت‌های فنی و حقوقی و رصد رمزگذاری ارائه شده توسط مجرمان رایانه‌ای در حال انجام است. همچنین، از یوروپل برای توسعه بیشتر قابلیت رمزگشایی و ساماندهی مجموعهٔ کاملی از ابزارها، تکنیک‌ها و تخصص مورد نیاز مقابله با سوءاستفاده جنایی از رمزگذاری پشتیبانی می‌شود (گزارش مشترک یوروپل و یوروجاست، ۲۰۱۹: ۱۱-۱۰). با در نظر گرفتن اینکه اتحادیه اروپا از طریق پروژه‌های همکاری فنی به ظرفیت قانونی و عملیاتی لازم برای مقابله با جرایم رایانه‌ای دست می‌یابد و همچنین، نه تنها در اروپا، بلکه در هر کشور یا منطقه‌ای آماده همکاری در پروژه‌های مشترک در زمینهٔ جرایم رایانه‌ای است. از این‌رو، ایران نیز می‌تواند با مشارکت در چنین پروژه‌هایی از همکاری‌های فنی، اجرایی و پشتیبانی بین‌المللی در این زمینه بهره‌مند شود.

1. Information society technologies (IST)

۵. چارچوب‌های بین‌المللی همکاری پلیس در مقابله با جرایم سایبری

قطعنامه‌های مجمع عمومی سازمان ملل متحد، شورای امنیت و شورای اقتصادی- اجتماعی بر دو موضوع مهم تاکید دارند: نخست اینکه لازم است تا زیرساختهای سایبری در هر کشور مطابق با استانداردهای بین المللی باشد تا امکان دفاع در برابر عملیاتهای تروریستی در فضای سایبری ممکن گردد و دیگر اینکه اجرای سیاستهای مد نظر جز با همکاری بین‌المللی میسر نمی گردد. لذا، لازم است دولتها در تدوین سیاستهای خود در زمینه مقابله با تروریسم سایبری ضمن لحاظ نمودن استانداردهای بین‌المللی در این خصوص، زمینه‌های همکاری‌های منطقه‌ای و بین‌المللی را مهیا نمایند. لذا، در قوانین و سیاستهای خود باید شرایط انجام چنین همکاری را فراهم نمایند. همچنین، برای شناسایی فناوری‌های نوین که گروه‌های تروریستی ممکن است از آنها در اقدامات خود استفاده نمایند، لازم است تا از بخش خصوصی بالاخص شرکت‌های دانش‌بنیان کمک گرفت تا امکان اقدام بازدارنده و پیشگیرانه در زمان مناسب وجود داشته باشد.

راهکار دیگر جهت رفع برخی موانع ایجاد سازوکارهای حقوقی از جمله امضای معاهدات، کنوانسیون منطقه‌ای، انعقاد قراردادهای دو یا چندجانبه می‌باشد. کنوانسیون جرایم سایبری افزایش اهمیت همکاری بین‌المللی را در مواد ۲۳ تا ۳۵ مورد بررسی قرارداده است. اعضای کنوانسیون باید از طریق اعمال ابزارهای بین‌المللی مربوط به همکاری بین‌المللی در حوزهٔ کیفری به منظور انجام تحقیقات یا دادرسی با یکدیگر همکاری نمایند (گرکی، ۱۳۸۹: ۴۱۷-۴۱۶) در این بستر، دفتر برنامه‌ریزی جرایم سایبری به‌عنوان نهادی موثّر در زمینهٔ همانندسازی قواعد جرم‌انگاری فضای سایبر قابل بحث و بررسی است. نهاد مذکور با کارکرد ظرفیت‌سازی خود، کار کمیتهٔ کنوانسیون سایبری جرم را تکمیل نموده و از طریق آن، دولت‌های عضو از اجرای کنوانسیون بوداپست پیروی می کنند. این دفتر وظیفهٔ کمک به کشورهای سراسر جهان در راستای تقویت ظرفیت سیستم‌های حقوقی‌شان برای پاسخ‌گویی به چالش‌های ناشی از جرایم سایبری و ادلهٔ الکترونیکی بر اساس استانداردهای کنوانسیون بوداپست نسبت به جرایم سایبری را به همراه تقویت اثربخشی همکاری‌های بین‌المللی، ارتقا همکاری‌های عمومی/ خصوصی و ایجاد واحدهای تخصصی جرایم سایبری و پزشکی قانونی و بهبود همکاری‌های بین‌سازمانی بر عهده دارد.

دفتر برنامه‌ریزی جرایم سایبری در بخارست به‌عنوان دیگر نهاد مبتنی بر معاهدهٔ دبیرخانهٔ کمیتهٔ کنوانسیون جرایم سایبری دایر گردیده است. هدف این دفتر، اطمینان از اجرای پروژه‌های ظرفیت‌ساز در زمینهٔ جرایم سایبری در کلیهٔ مناطق جهان از طریق ظرفیت‌سازی در زمینهٔ جرایم سایبری، مشاوره، پشتیبانی و هماهنگی در برنامه‌ریزی، مذاکره و اجرای به موقع فعالیت‌های هدفمند در زمینهٔ جرایم سایبری، از جمله برنامه‌های مشترک با اتحادیهٔ اروپا و سایر اهداکنندگان و ایجاد مشارکت در برابر جرایم سایبری با سازمان‌های بخش دولتی و خصوصی می‌باشد. این دفتر

همچنین مسئول کمک به کشورهای جهان در تقویت ظرفیت سیستم‌های حقوقی خود برای پاسخ‌گویی به چالش‌های ناشی از جرایم اینترنتی و شواهد الکترونیکی بر اساس استانداردهای بوداپست است (شورای اروپا، ۲۰۲۰)؛ حال و در مقام تطبیق کلیهٔ موارد پیش‌گفته با فضای سیاست تقنینی جمهوری اسلامی ایران در اجرای قواعد همانندسازی، با ملاحظهٔ قانون جرایم رایانه‌ای مصوب ۱۳۸۸ و مفاد کنوانسیون بین‌المللی بوداپست مصوب ۲۰۰۱ می‌توان نتیجه گرفت که قانون‌گذار ایران در نگارش و تدوین قانون مذکور از مفاد این کنوانسیون الهام گرفته است. استفاده از سازوکارهای این نهادها به مجموعهٔ سیاست اجرایی یاری می‌رساند تا منعطف و مطابق با زمان خود باشد.

همچنین، «دستورالعمل درخصوص حملات علیه سیستم اطلاعاتی» مصوب ۲۰۱۳ با هدف مقابله با حملات سایبری در مقیاس بزرگ تدوین یافته است تا نیاز کشورهای عضو برای تقویت قوانین در حوزهٔ جرائم سایبری در سطح ملی و معرفی ضمانت اجراهای کیفری سخت‌تر را بیش از پیش مرتفع سازد. در سال ۲۰۱۷، کمیسیون گزارشی را منتشر کرده است که به موجب آن، ارزیابی می‌شود تا چه میزان کشورهای عضو اقدامات لازم را برای رعایت دستورالعمل انجام داده‌اند (مجله رسمی اتحادیه اروپا، ۲۰۱۳).

لیکن، متأسفانه ایران تاکنون به هیچ‌یک از اسناد بین‌المللی مربوط به جرایم رایانه‌ای از جمله کنوانسیون بین‌المللی جرایم سایبری بوداپست ۲۰۰۱ ملحق نشده است. این امر یکی از چالش‌های اساسی نظام کیفری ایران در برخورد با جرائم حوزهٔ سایبر به‌شمار رفته و امکان نیل به یکسان‌سازی قواعد و اصول و همسان‌سازی تدابیر اجرایی را کمتر می‌نماید.

۶. ایجاد سیاست منسجم بین‌المللی پلیس در مقابله با جرایم سایبری

در فصل سوم کنوانسیون اصول کلی مربوط به همکاری بین‌المللی از قبیل پی‌جویی‌ها یا جمع‌آوری دلایل الکترونیکی یا رسیدگی قضایی راجع به جرایم رایانه‌ای در ماده ۲۳ بیان شده است. ماده ۲۴ نیز اصول مرتبط با استرداد مجرمان را روشن ساخته است. حتی در ماده ۲۵ به اصول کلی راجع به همکاری دوجانبه اشاره شده است. در ماده ۲۶ نیز ارائهٔ اطلاعات به طور داوطلبانه حتی بدون درخواست عضو دریافت‌کنندهٔ اطلاعات برای کمک در شروع یا اجرای پی‌جویی مدنظر قرارگرفته است. همچنین، در مواد ۳۴، ۳۳، ۳۱ به همکاری دوجانبه در موارد دستیابی به داده‌های رایانه‌ای ذخیره‌شده، در زمینه جمع‌آوری داده ترافیک در زمان واقعی و همکاری در زمینه قطع و شنود داده محتوا اشاره شده است. تمامی موارد مشخص شده به لزوم همکاری بین‌المللی ذی‌نفعان اشاره دارد. در راستای تقویت بنیادین سیاست اجرایی یک جامعه، همکاری بین ذی‌نفعان و بازیگران اصلی پیشنهاد شده است که شامل همکاری و مشارکت‌های عمومی و خصوصی می‌شود. به عنوان نمونه، کشورهای حوزهٔ اتحادیهٔ اروپا در زمینهٔ استرداد مجرمان

رایانه‌ای، همکاری‌های مؤثّری با یکدیگر و سایر کشورهای جهان دارند.

اذعان نیاز به همکاری بین کشورها و بخش‌خصوصی در زمینهٔ مبارزه با جرائم سایبر و نیاز به حمایت از منافع مشروع در زمینهٔ استفاده و توسعهٔ فناوری‌های اطلاعات در چهارچوب کنوانسیون بوداپست نقشی اساسی دارد. این اعتقاد که مبارزهٔ مؤثّر با جرایم سایبر مستلزم یک همکاری گسترده، سریع و کارآمد در عرصهٔ بین‌الملل در موضوعات کیفری می‌باشد نیز امری است که ماهیتی ضروری دارد. بالاترین سطح همکاری مربوط به همکاری‌های متقابل می باشد که در چهارچوب قوانین اتحادیه اروپا ایجاد شده است. در این راستا، اقدامات مختلفی اتخاذ شده که به طور مستقیم یا غیرمستقیم مربوط به سرکوب جرایم رایانه‌ای می‌باشد. این اقدامات شامل توافق‌نامه‌های مربوط به همکاری متقابل در امور کیفری، مانند کنوانسیون ۲۰۰۰ اتحادیه اروپا در ارتباط با همکاری متقابل در امور کیفری و پروتکل ۲۰۰۱ آن است. خلاقانه‌ترین ابزارها در چهارچوب اتحادیه اروپا شامل اقدامات اجرای اصل شناخت متقابل در امور کیفری است (کالدرونی، ۲۰۱۱: ۱۰).

اتحادیه اروپا از کنوانسیون شورای اروپا به عنوان کامل‌ترین استاندارد بین‌المللی پیروی می‌نماید. رویکرد شورای اروپا در مورد جرایم رایانه‌ای از یک مثلث پویا تشکیل شده است: استانداردها، نظارت و همکاری فنی. این رویکرد منحصربه‌فرد و اثربخش است. اتحادیه اروپا ابزارهایی برای مجبور کردن کشورهای عضو برای اجرای چهارچوب حکم و بخشنامه دارد؛ به این دلیل که تعدادی از کشورهای اتحادیه اروپا با وجود اینکه کنوانسیون جرایم سایبری سال ۲۰۰۱ را امضا کرده‌اند، اما هنوز آن را به تصویب نرسانده‌اند؛ ولی چهارچوب حکم اتحادیه اروپا در حملات علیه سیستم‌های اطلاعات را با هدف بهبود همکاری بین‌المللی و سایر مراجع ذی‌صلاح، از جمله پلیس و سایر خدمات ویژه اجرای قانون کشورهای عضو اجرا نموده‌اند (گرکی، ۱۳۸۹: ۲۳۶-۲۳۵).

رویکرد اتحادیهٔ اروپا در قبال جرایم سایبری به موازات جامعهٔ اطلاعاتی خود توسعه یافته است. این رویکرد توسط اسناد امنیتی داخلی اتحادیهٔ اروپا و عدالت و برنامه‌ریزی امور داخلی، همچنین دستورکار اروپا در مورد امنیت (کمیسیون اروپا، ۲۰۱۵) و چهارچوب مشترک مقابله با تهدیدات ترکیبی، که راهنمای استراتژیک در مورد امنیت سایبری و جرایم سایبری می‌باشد، ارائه شده است (کمیسیون اروپا و سرویس اقدام خارجی اتحادیهٔ اروپا، ۲۰۱۶). در سال ۲۰۰۷ تلاش شد تا همکاری و هماهنگی در سطح عملیاتی و استراتژیک بین سازمان‌های اجرایی قانون و در سطح سیاسی صورت پذیرد. از زمان تصویب استراتژی امنیت سایبری اتحادیهٔ اروپا در سال ۲۰۱۳، کمیسیون اروپا تلاش خود را برای پیشرفت بهتر در این زمینه افزایش داد و اتحادیهٔ اروپا در سال ۲۰۱۴، ۶۰۰ میلیون یورو برای تحقیق و نوآوری در پروژهٔ امنیت سایبری در نظر گرفت. استراتژی

اتحادیهٔ اروپا دارای پنج اولویت می‌باشد: افزایش انعطاف‌پذیری سایبری، کاهش جرایم رایانه‌ای، توسعهٔ سیاست دفاع سایبری، توسعهٔ فناوری برای امنیت سایبری، ایجاد سیاست منسجم بین‌المللی فضای مجازی و ارتقا ارزش‌های اصلی اتحادیهٔ اروپا (کمیسیون اروپا، ۲۰۱۷: ۲). در راستای تسهیل همکاری‌های بین‌المللی پلیس، در اروپا «یوروپل[1]» تأسیس شده است. مرکز جرایم سایبری به‌عنوان کانون اصلی اروپا برای مبارزه با جرایم سایبری و به‌عنوان بخشی جدایی‌ناپذیر از یوروپل جهت تقویت واکنش اجرایی به جرایم رایانه‌ای در اتحادیهٔ اروپا ایجاد شده است. وظیفهٔ مرکز مبارزه با جرایم سایبری اطمینان از هماهنگی فعالیت‌های عملیاتی با سیاست مربوطهٔ اتحادیهٔ اروپا و همکاری با سایر آژانس‌های ذی‌ربط مانند: یوروجاست، امنیت شبکه و اطلاعات اروپا و آموزش اجرای قانون و همچنین، تجزیه و تحلیل و پشتیبانی فنی به‌طور مؤثر می‌باشد (مرکز جرایم سایبری اروپا، ۲۰۱۴). تیم واکنش اضطراری رایانه‌ای اتحادیهٔ اروپا نیز در سال ۲۰۱۲ با هدف پاسخ‌گویی به حوادث امنیتی اطلاعاتی و تهدیدات سایبری برای نهادها، سازمان‌های اتحادیهٔ اروپا راه‌اندازی شده بود. رویهٔ اجرایی اتحادیهٔ اروپا در زمینهٔ جرایم سایبری بیشتر بر پایهٔ همکاری بازیگران بخش دولتی و خصوصی متمرکز شده است و ادعا می‌شود ذی‌نفعان باید برای ایجاد اختلال در شبکهٔ مجرمان سایبری همکاری نمایند؛ به‌طور مثال، مشارکت بین مرکز جرایم سایبری اتحادیهٔ اروپا و مایکروسافت در این مورد از اهمیت ویژه‌ای برخوردار است (کارگروه مشترک در زمینهٔ جرایم سایبری، ۲۰۱۷: ۱۳). «جی کت»[2] نیز به‌عنوان یک سازمان شبکه‌ای سیال و یک کارگروه این امکان را دارد تا با کشورهای غیرعضو به‌طور مؤثر همکاری نماید. به دلیل بین‌المللی بودن جرایم سایبری، اغلب مجرمان در کشورهای خارج از اتحادیهٔ اروپا قرار دارند. این کارگروه می‌تواند از طریق توافق‌نامهٔ موقت همکاری کند (ریتانو[3]، اورتینگ[4] و هانتر[5]، ۲۰۱۵: ۱۴۵). «جی کت» به‌عنوان یک شکل عملیاتی در حال ظهور و در حال تکامل می‌باشد که نشان‌دهندهٔ عملکرد غیررسمی و انعطاف‌پذیرتر نسبت به یوروپل و مرکز مبارزه با جرایم سایبری به‌منظور جلوگیری از موانع موجود و اقدامات سنتی و کند می‌باشد. سرانجام، اگرچه این کارگروه به‌عنوان الگویی عملیاتی منجر به نتایج بهتری می‌شود، اما موضوعات گسترده‌تری برای مبارزهٔ مؤثر با جرایم سایبری باقی می‌ماند. همچنین، طبق مادهٔ ۲۳ کنوانسیون جرایم سایبری، اعضای کنوانسیون از طریق اعمال ابزارهای بین‌المللی مربوط به همکاری در حوزهٔ توافق‌هایی دوجانبه مبنی بر انجام تحقیقات یا دادرسی مرتبط با سامانه‌ها و داده‌های رایانه‌ای یا جمع‌آوری ادله و آثار الکترونیکی جرایم کیفری با یکدیگر همکاری می‌نمایند.

1. the European Unions law enforcement agency (Europol)
2. J-CAT
3. Reitano
4. Oerting
5. Hunter

بحث و نتیجه‌گیری

تمایل روزافزون به استفاده از فناوری‌های پیشرفته از جمله رایانه و اینترنت، شرایط و بستر مساعدی برای ظهور جرایم مجازی به‌وجود آورده است. از آنجا که این جرایم در فضای مجازی انجام می‌پذیرد و مانند سایر جرایم ملموس نیستند، پلیس برای پیشگیری از این جرایم و کشف آن‌ها با چالش‌هایی جدید مواجه هستند. مؤلفه‌هایی مانند داشتن جنبهٔ بین‌المللی، مشکل تعریف واحد از جرایم مجازی، تغییرپذیری ماهیت دلایل اثبات جرم، مسائل خاص مرحلهٔ کشف، ناهماهنگی قوانین کشورهای مختلف، فقدان همکاری‌های متقابل به‌ویژه در حوزه پیشگیری از جرم و آئین دادرسی، فقدان ساختار و رویهٔ واحد چالش‌های موجود در این فضا می‌باشند. از این رو، مداخله و مشارکت چندین کشور در فرآیند مقابله با جرم که هرکدام قوانین خاص خود را داشته و چه بسا وابسته به نظام های حقوقی متفاوتی نیز باشند، همکاری بین المللی برای مبارزه با جرائم سایبری را با مشکلات متعددی مواجه می کند. در برخی از موارد، نیروهای پلیس، سطح دانش یکسانی نداشته یا به فنّاوری های نوین پیشگیری از بزه دسترسی نداشته و نمی‌توانند درخواستهای طرف مقابل برای پیشگیری از موقعیت‌های پیش‌جنایی را فراهم آورند. بنابراین، برای رسیدن به نتیجهٔ مطلوب و مقابله با چالش‌های فراروی سیاست اجرایی می‌توان با ایجاد یک نظام منسجم همکاری با نهادهای رسمی اجرایی بین المللی همچون پلیس اتحادیهٔ اروپا اقدام به ایجاد بسترهایی برای تسهیل این نوع همکاری‌ها نمود و با بهره‌گیری از تجربه‌های موجود، آموزه‌های جهانی جرم‌شناسی سایبری و آموزش تخصصی پلیس همانند پلیس اتحادیهٔ اروپا که مرکز آموزش و عملیاتی در آن به‌طور متمرکز فعالیت می‌نمایند، آموزش همگانی، تنظیم مقررات حقوقی شفاف هماهنگ با جوامع بین‌المللی جهت مشارکت فعال بخش خصوصی که مکمل سیاست جنایی اجرایی کشور باشد، به مقابله و پیشگیری از جرایم رایانه‌ای پرداخت.

در واقع، چالش‌های ناشی از جرایم فراملی را هرگز نمی‌توان بدون وجود یک سیاست جنایی منسجم بین‌المللی پلیسی کاهش داد. کشورها علاوه بر هماهنگی قوانین اساسی و توانمندسازی اجرای قانون با اختیارات رویه‌ای مناسب، باید رژیم‌های جدیدی برای کمک به یکدیگر جهت تحقیق و تعقیب جرایم سایبری ایجاد کنند. رژیم‌های موجود در زمینه کمک حقوقی متقابل بین دولت‌ها به‌طور کلی کند بوده و تقسیم مدارک را فقط در بین دو کشور، یعنی کشور قربانی و کشور مجرم پیش‌بینی می کنند. با توجه به اینکه یک مجرم می‌تواند ارتباطات خود را از طریق چندین کشور ارسال کند و با درنظر گرفتن افزایش احتمال غیرقابل‌دسترسی یا از بین رفتن داده‌ها و شواهد، آزادی عمل برای مجرم ایجاد می‌شود. در این راستا، می‌توان از روند اتحادیه اروپا که توسعه شبکه‌های اضطراری بین‌دولتی به منظور ارتباط شبانه‌روزی محققان با سایر کارشناسان است، الگوبرداری نمود. از آنجا که همکاری مؤثر بین مقامات پلیس اغلب به داشتن حداقل

تعاریف هماهنگی از جرم بستگی دارد، اتحادیه اروپا نزدیک‌تر کردن قوانین کشورهای عضو را به عنوان یک هدف بلندمدت مدنظر قرار داده است. تلاش اتحادیه اروپا برای ایجاد یک سیستم هماهنگ از اقدامات قانونی پشتیبانی‌شده و تکمیل‌شده قابل‌ستایش است. اتحادیه اروپا کشورهای عضو را ملزم به تخصیص منابع کافی در جهت حمایت از کودکان به‌ویژه در رابطه با انواع موارد سوءاستفاده از آن‌ها و تحریک به خشونت در متن، تصاویر و بازی‌ها نموده است. علاوه بر این، افزایش حمایت مالی از ابتکارات در جهت تقویت نهادهای اجرای قانون و همچنین، آموزش بهتر مقامات انتظامی و قضائی به منظور رسیدگی به پرونده‌های جرایم اینترنتی و اقدام به هماهنگی کلیه تلاش‌های آموزش چندملیتی در این زمینه با ایجاد یک بسترآموزشی را نیز در دستورکار قرار داده است. اتحادیه اروپا همچنین به گفتگو بین کشورهای عضو با کشورهای ثالث در مورد روش‌های فنی برای مبارزه با محتوای غیرقانونی و روش‌های مسدود کردن و بستن وبسایت‌های غیرقانونی و دستیابی به توافق‌نامه‌های رسمی با کشورهای همسایه در ارتباط با این موضوع و ترویج آن توصیه نموده است. از این رو، برای رسیدن به نتیجهٔ مطلوب و تسهیل همکاری‌های بین‌المللی پلیس به‌منظور کاهش چالش‌های پیش‌رو، همچنین ایجاد ظرفیت‌سازی در راه مبارزه با جرایم سایبری، لزوم یک سیاست جنایی پلیسی مؤثر هماهنگ بین‌المللی از طریق سازوکارهای همکاری بین‌المللی پلیس در مقابله با جرایم سایبری، ارتقای توان علمی و تخصصی واحدهای مبارزه با جرائم سایبری، تهیهٔ تجهیزات و امکانات سخت‌افزاری و نرم‌افزاری پیشرفته مبارزه با جرائم سایبری، اتخاذ چهارچوب‌های بین‌المللی همکاری پلیس در مقابله با جرایم سایبری و ایجاد سیاست منسجم بین‌المللی پلیس در مقابله با جرایم سایبری ضرورت می‌یابد.

پیشنهادها

۱. بایستی با الگوبرداری از اتحادیهٔ اروپا ابتدا با همکاری در عرصهٔ بین‌المللی و سپس، با وضع قوانین جدید با تبیین سیاست اجرایی کشور و با همکاری پلیس کشورهای مختلف به‌منظور تحقیق، پیگرد، استرداد مجرمان گامی مؤثر برداشت.

۲. ویژگی فراملی بودن جرایم ارتکابی سایبری، ضرورت پیوستن به کنوانسیون‌ها و مشارکت فعال در عرصهٔ جهانی را جهت اتخاذ سیاست جنایی هماهنگ بین‌المللی پلیس در مقابله با جرایم سایبری به‌منظور برون‌رفت از چالش‌های پیش‌رو در این زمینه روشن می‌سازد.

۳. بر اساس کنوانسیون جرایم رایانه‌ای پلیس کشورهای مختلف بایستی در رابطه با هماهنگ‌سازی بین حقوق کیفری داخلی و مقررات بین‌المللی، تعقیب متهمان این جرایم و بازجویی از آن‌ها در امور مربوط به ارائهٔ دلایل جرم و اعلام دقیق محل وقوع آن، به یکدیگر یاری رسانند.

۴. کشور ما به کنوانسیون‌های بین‌المللی در جهت مقابله با مجرمان سایبری و پیگیری اموراتی از قبیل اصول کلی مربوط به همکاری بین‌المللی، استرداد مجرمان، همکاری‌های دوجانبه، نقش

مراکز غیردولتی در مبارزه با جرایم در فضای مجازی، ضمانت اجراها و... که در زمرهٔ مباحث مهم مطروحه در کنوانسیون‌ها هستند، بپیوندد.

۵. بسترسازی جهت استفاده از تجربه‌های به‌دست آمده و همکاری با پلیس کشورهای دیگر به‌ویژه اتحادیهٔ اروپا در مقابله با جرایم سایبری.

۶. ارتقای توان علمی و تخصصی واحدهای پلیسی مبارزه با جرائم سایبری.

۷. تهیهٔ تجهیزات و امکانات سخت‌افزاری و نرم‌افزاری پیشرفته پلیسی در مبارزه با جرائم سایبری.

۸. اتخاذ چهارچوب‌های بین‌المللی همکاری پلیس در مقابله با جرایم سایبری.

۹. ایجاد سیاست منسجم بین‌المللی پلیس در مقابله با جرایم سایبری.

سپاسگزاری

پژوهشگر، از عزیزانی که در فرآیند ویراستاری ادبی و صفحه‌آرایی این مقاله همکاری و راهنمایی داشتند، کمال تشکر و امتنان را دارد.

منابع

- احمدوند، علی محمد؛ عطایی جعفری، امیرمسعود. (۱۳۸۳). نقش و راهبرد فناوری اطلاعات در سیستم پلیس و فضاهای مجازی جرایم در ایران. *دو ماهنامهٔ توسعهٔ انسانی پلیس*، ۱(۳)، ۲۸-۵.
http://pod.jrl.police.ir/article_9510.html
- بیگی، جمال؛ خوشیاری، رزاق. (۱۳۹۰). جرایم رایانه‌ای و مقابله با آن در اسناد بین‌المللی. *همایش منطقه‌ای چالش‌های جرایم رایانه‌ای در عصر امروز*. دانشگاه آزاد اسلامی مراغه، ۱۳۸-۱۲۳.
https://civilica.com/doc/128777/
- پرویزی، رضا. (۱۳۸۵). *پی‌جویی جرایم رایانه‌ای*. چاپ اول. انتشارات جهان جام جم.
- تقی‌زاد، مهرداد؛ زمردی،کیوان؛ حاجیان، مهدی. (۱۳۹۶). نقش اتحادیهٔ اروپا در قاعده‌مندسازی جرائم سایبری. *فصلنامه مطالعات بین‌المللی پلیس*، ۸(۲۹)، ۱۴۳-۱۰۴.
http://interpol.jrl.police.ir/article_12920.html
- جلالی فراهانی، امیرحسین. (۱۳۸۳). پیشگیری از جرایم رایانه‌ای. *مجله حقوقی دادگستری*، (۴۷)، ۱۱۹-۸۷.
http://ensani.ir/file/download/article/20120329110338-2101-75.pdf
- جلالی فراهانی، امیرحسین. (۱۳۸۴). پیشگیری وضعی از جرائم سایبر در پرتو موازین حقوق بشر. *فقه و حقوق*، ۶(۲)، ۱۳۶-۱۳۲.
magazines.iict.ac.ir/uploads/5_51_06.07.pdf
- جلالی فراهانی، امیرحسین. (۱۳۹۴). *درآمدی بر آیین‌دادرسی کیفری جرائم سایبری*. چاپ اول. انتشارات خرسندی.
- حسن بیگی، ابراهیم. (۱۳۸۴). توسعهٔ شبکهٔ ملی دیتا، چالش‌های فراروی و تهدیدهای متوجهٔ امنیت ملّی. *فصلنامهٔ مطالعات مدیریت*، (۴۸)، ۲۸-۱.
http://ensani.ir/fa/article/54561
- حیدری، مسعود؛ شهبازی، امید؛ شیرانی، پویا (۱۳۹۷). چالش‌ها و فرصت‌های پیش روی پلیس در برخورد با جرایم سایبری. *فصلنامهٔ کارآگاه*، ۱۲(۴۵)، ۵۴-۴۱.
http://journals.police.ir/article_91542_5dc35ffa484c060819e4993eb1818270.pdf
- زیبر، اولریش. (۱۳۹۰). *جرائم رایانه‌ای*. ترجمه محمدعلی نوری، رضا نخجوانی، مصطفی بختیارون و احمد رحیمی مقدم. گنج دانش.
- ذبیح الله نژاد، وحید. (۱۳۹۶). ماهیت جرایم رایانه‌ای و مجازی (سایبری) و نقش پلیس فتا در پیشگیری و کشف این جرایم. *فصلنامهٔ دانش انتظامی پلیس پایتخت*، ۳ (۲۴)، ۲۷-۸.
http://tehran.jrl.police.ir/article_14887_c5f25516cedb24b84ac53f2086d9a860.pdf
- رضوی، محمد. (۱۳۸۶). جرایم سایبری و نقش پلیس در پیشگیری از این جرایم و کشف آنها. *فصلنامه دانش انتظامی*، (۳۲)، ۱۴۰-۱۲۰.
https://www.noormags.ir/view/fa/articlepage/275832/
- صبح خیز، رضا. (۱۳۹۴). چالش‌های حقوقی جرائم سایبری در نظام حقوق بین‌الملل و نظام حقوقی ایران. *فصلنامهٔ پژوهش های اطلاعاتی و جنایی*، ۱۰ (۳۹)، ۱۳۸-۱۱۷.
https://www.sid.ir/fa/journal/ViewPaper.aspx?ID=316390
- پرویزی، رضا. (۱۳۸۲). اروپا جامعهٔ اطلاعاتی، جرایم رایانه‌ای. *سازمان فرهنگ و ارتباطات*

اسلامی.
http://icro.ir/index.aspx?pageid=32738&p=254&showitem=5062
- سایبانی، علیرضا؛ کریمی، اصغر. (۱۳۹۷). سیاست جنایی ایران در خصوص جرایم مالی رایانه‌ای. *مطالعات علوم سیاسی، حقوق و فقه*، ۴ (۱)، ۱۴۲-۱۲۴.
https://www.noormags.ir/view/fa/articlepage/1379426/
- کونانی، سلمان؛ انصاری، جمال؛ مندنی، اسلام. (۱۳۹۲). *سیاست جنایی از گفتمان تا برساخت‌های ریزومیک شده و ناروا*. چاپ دوم. انتشارات مجد.
- گرکی، مارکو. (۱۳۸۹). *جرایم سایبری؛ راهنمایی برای کشورهای در حال توسعه*. ترجمه مرتضی اکبری. چاپ اول. انتشارات پلیس فضای تولید و تبادل اطلاعات ناجا.
- گزارش سالانهٔ مرکز جرایم سایبری اروپا (۲۰۱۳).
http://ej.uz/FirstYearReport_EC3
- مشهدی، علی و محمدصالح تسخیری. (۱۳۹۲). *بایسته‌های حقوق سازمان‌های بین‌المللی*. ویرایش ۱. نشر خرسندی.
- میرخلیلی، سیدمحمود؛ یعقوبی، تقی. (۱۳۹۶). بررسی عوامل قضایی افزایش جمعیت کیفری زندان‌ها. *فصلنامهٔ راهبرد*، ۸۲ (۲۶)، ۱۲۸-۹۹.
http://ensani.ir/file/download/article/20171017080030-9518-240.pdf
- نجفی ابرندآبادی، علی حسین. (۱۳۹۵). *جرم‌شناسی در آغاز هزاره سوم، درآمد در: دانشنامه جرم‌شناسی*. چاپ چهارم. انتشارات گنج دانش.
- یار، مجید. (۱۳۹۰). *جرم سایبر و جامعه*. ترجمه یوسف بابایی و اصلی عباسی. چاپ اول. انتشارات مجد.
- یزدان‌پناه‌درو، کیومرث و کامران، حسن. (۱۳۹۳). تروریسم در فضای مجازی و اثرات آن بر حوزه جغرافیای سیاسی. *فصلنامه جغرافیا*، ۱۳(۴۴)، ۴۵- ۲۵.
https://www.sid.ir/fa/journal/ViewPaper.aspx?id=244714

- Bryant, R. Bryant, S. (2014). *Policing Digital Crime*. England: Ashgate Publishing.
- Calderoni, Francesco. (2011). The European legal framework on cybercrime: Striving for an effective Implementation. *Crime Law and Social Change*, 54: 1-21.
https://www.researchgate.net/publication/227301292_The_European_legal_framework_on_cybercrime_Striving_for_an_effective_implementation
-Council of Europe. Explanatory Report to the Convention on Cybercrime. Budapest, 23.XI.2001. *European Treaty Series*, (85), 1 – 60.
https://rm.coe.int/16800cce5b
-Council of Europe. (2020). *Cybercrime Programme Office.*
https://www.coe.int/en/web/cybercrime
-European Commission. (2017). *Eu cybersecurity Initiatives Working towards a more secure online environment.*
https://ec.europa.eu/information_society/newsroom/image/document/20173/factsheet_cybersecurity_update_january_2017_41543.pdf (last visited on 4/5/2020).
- European Commission. (2015). *Communication from the commission to the council and the European Parliament.* The Council, The European Economic and Social Committee and The Committee of the Regions, The Agenda on European Security, Strasbourg, 28.4.2015, COM (2015) 185 final.

-European Commission and European External Action Service (EEAS). (2016). *Joint communication to the European Parliament and the Council, Joint Framework on Countering Hybrid Threats: A European Union response*. 6 April, JOIN (2016) 18 final.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018
- European Commission. (2012). Communication from the commission to the council and the European Parliament. '*Tackling Cybercrime in our Digital Age: Establishing a European Cybercrime Centre'*. COM (2012) 140 final, Brussels, 28 March 2012.
-European court of Auditors. (2019). Challenges to effective EU cybersecurity policy. *Briefing Paper*. 1-74.
https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf
-European Cybercrime Centre. (2020). *Combating crime in a digital age*. Europol, 2014.
https://www.europol.europa.eu/ec3 (last visited on 6/5/2020).
-Europol. (2020). About Europol.
https://www.europol.europa.eu/about-europol (last visited on 7/5/2020).
-Europol. (2020). *EC3 Programme Board*.
https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/ec3-programme-board (last visited on 6/6/2020).
-Europol. (2020). *Operations*.
https://www.europol.europa.eu/activities-services/europol-in-action/operations (last visited on 6/6/2020).
-European Parliament. (2015). *The law enforcement challenges of cybercrime: Are we really playing catch-up?*. Technical Report. Directorate- General for Internal Policies, Policy Department C: Citizens Rights and Constitutional Affairs, Study for the LIBE Committee, October 2015.
https://www.europarl.europa.eu/RegData/etudes/STUD/2015/536471/IPOL_STU(2015)536471_EN.pdf
- Joint Report Europol and Eurojust Public Information. (2019). *Common Challenges in Combating Cybercrime as Identified by Eurojust and Europol.*
-Krasner, Stephen. (2013). *International Regimes*. Ithaca. Cornell University Press.
-Kshetri, N (2010). *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*. Chapter2. springer.
-Official Journal of the European Union. (2013). *Directive 2013/40/EU of the European Parliament and of the Council (on attacks against information systems and replacing Council Framework Decision 2005/222/JHA).* 218, 8 – 14.
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF
-Scherrer, Joseph H., Grund, William, C. (2012). *A Cyberspace Command and Control Model*. Maxwell Paper No. 47, Air War, College.
- Ghernaouti-Hélie, S (2013). *Cyber Power: Crime, Conflict and Security in Cyberspace.* EPFL Press.