

Interpol's role in fighting cybercrime

Z.Hosseini¹ , A.Ansarimahyari^{2*} , M.Raei³ 

¹ PhD student in International Law, Najafabad Branch, Islamic Azad University, Najafabad, Iran. zahra.hosseini00@yahoo.com

² Assistant Professor, Department of Law, Najafabad Branch, Islamic Azad University, Najafabad, Iran (*Correspondence: alirezaansari50@iaui.ac.ir)

³ Professor, Department of Law, Najafabad Branch, Islamic Azad University, Najafabad, Iran. masoudraei@yahoo.com

ARTICLE INFO

Article history:

Article Type: Research paper

Received: 04 January 2026

Revised: 20 February 2026

Accepted: 25 February 2026

Available online: 11 April 2026

Keywords:

Cybercrime
Interpol
Cybersecurity

ABSTRACT

Technological developments have led to the emergence of new types of previously unknown crimes, especially cybercrime. The big world we knew has now become a small village, and this has caused crimes to cross geographical borders. Criminals have taken advantage of the opportunities created by technology and developed cybercrime, which differs from traditional crimes in terms of the skills of the perpetrators. Rapid growth, the desire to gain wealth, abundant opportunities to commit crime and the increase in organized crime are among the factors that have led to the spread of cybercrime and the increase in the number of victims. These factors threaten the security of data and the well-being of victims, which in turn requires the urgent attention of the International Criminal Police Organization (INTERPOL). Interpol, one of the most well-known organizations in the world, considers its main goal to be international cooperation to combat cybercrime, which is developing rapidly and cybercriminals are using the latest technological developments to make it more difficult to catch them. Using the staff and equipment at its disposal, Interpol has a significant ability to combat these crimes. The results of the study indicate that, Interpol considers the need for international cooperation, education and increasing public awareness about cyber threats essential and pursues improvements in strategies and technologies in order to create a safer cyber environment.

Cite this article: Z, Hosseini , A. Ansarimahyari, M .Raei. (2026). Interpol's role in fighting cybercrime. *Electronic and Cyber Defense*,14(1),53-68. DOI: <https://dor.isc.ac/dor/20.1001.1.23224347.1405.14.1.4.6>



OPEN  ACCESS

© Author(s) retain the copyright and full publishing rights

Publisher: Imam Hossein University.

نقش اینترپل در مبارزه با جرایم سایبری

زهرا سادات حسینی^۱، علیرضا انصاری مهیاری^{۲*}، مسعود راعی^۳

^۱ دانشجوی دکترا حقوق بین الملل، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران. hamidreza.yazdani@gmail.com
^۲ استادیار، گروه حقوق، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران (نویسنده مسئول): alirezaansari50@iaui.ac.ir
^۳ استاد گروه حقوق، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران. rnnasiri@ihu.ac.ir

چکیده	مشخصات مقاله
توسعه‌های فناوری منجر به شکل‌گیری انواع جدیدی از جرایم ناشناخته قبلی، به‌ویژه جرایم سایبری شده است. دنیای بزرگی که می‌شناختیم اکنون به دهکده‌ای کوچک تبدیل شده است و این امر باعث شده که جرایم از مرزهای جغرافیایی عبور کنند. مجرمان از فرصت‌های به وجود آمده در فناوری استفاده کرده و جرایم سایبری را که از نظر مهارت مرتکبان با جرایم سنتی تفاوت دارد، توسعه داده‌اند. رشد سریع، تمایل به کسب ثروت، فرصت‌های فراوان برای ارتکاب جرم و افزایش جرایم سازمان‌یافته از عواملی هستند که باعث گسترش جرایم سایبری و افزایش تعداد قربانیان شده‌اند. این عوامل، ایمنی داده‌ها و رفاه قربانیان را تهدید می‌کنند که به نوبه خود نیازمند توجه فوری سازمان بین‌المللی پلیس جنایی (اینترپل) است. اینترپل که یکی از شناخته‌شده‌ترین سازمان‌های جهان است، هدف اصلی خود را همکاری بین‌المللی برای مقابله با جرایم سایبری می‌داند که به سرعت در حال توسعه هستند و مجرمان سایبری از آخرین پیشرفت‌های فناوری استفاده می‌کنند تا دستگیری آن‌ها را دشوارتر کنند. اینترپل با استفاده از کارکنان و تجهیزاتی که در اختیار دارد، توانایی قابل توجهی برای مقابله با این جرایم دارد. نتایج پژوهش حاکی از این است که اینترپل با توجه به چالش‌های موجود، نیاز به همکاری بین‌المللی، آموزش و افزایش آگاهی عمومی در مورد تهدیدات سایبری را ضروری می‌داند و در راستای ایجاد یک محیط سایبری امن‌تر، بهبود راهبردها و فناوری‌ها را دنبال می‌کند.	تاریخچه مقاله: نوع مقاله: علمی پژوهشی دریافت: ۱۴۰۴/۱۰/۱۴ بازنگری: ۱۴۰۴/۱۲/۰۱ پذیرش: ۱۴۰۴/۱۲/۰۶ ارائه آنلاین: ۱۴۰۵/۰۱/۲۲ کلید واژه‌ها: جرایم سایبری اینترپل امنیت سایبری

استناد: زهرا سادات حسینی، علیرضا انصاری مهیاری، مسعود راعی. (۱۴۰۵). نقش اینترپل در مبارزه با جرایم سایبری. پدافند الکترونیک و سایبری، ۱۴(۱)، ۶۸-۵۳. <https://dor.isc.ac/dor/20.1001.1.23224347.1405.14.1.4.6>

© نویسندگان حق نشر و حقوق کامل انتشار را برای خود محفوظ می‌دارند.

ناشر: دانشگاه جامع امام حسین(ع)

مقدمه

خلق و تولید اطلاعات جدید در دنیای مدرن به یکی از ضروری‌ترین عوامل توسعه و پیشرفت در تمامی ابعاد زندگی انسان تبدیل شده است. با حجم انبوه داده‌هایی که به واسطه‌ی فناوری‌های نوین و گسترده شدن دسترسی به فناوری جمع‌آوری می‌شوند، پردازش این اطلاعات به کاری دشوار و گاهی غیرممکن بدل شده است. درک سازوکارها و استفاده از نتایج فناوری نیازمند صرف زمان و تلاش فراوان است، به‌ویژه اگر هدف تسهیل و نظم‌بخشی به زندگی باشد. تولید اطلاعات در دنیای امروز با سرعتی بی‌سابقه ادامه دارد، به‌طوری که هر نوآوری در حوزه‌های مختلف به دنبال پیشی‌گرفتن از دیگری است. رایانه‌ها ابتدا به‌عنوان ابزاری شخصی وارد زندگی شدند، و اینترنت که در آغاز تنها به گروهی محدود دسترسی داشت، اکنون به دلیل پیشرفت‌های تکنولوژیک در اختیار همه افراد، بدون در نظر گرفتن محدودیت‌های سنی یا دیگر عوامل، قرار گرفته است. این گستردگی دسترسی، علاوه بر مزایای فراوان، زمینه‌ای برای ظهور جرائم سایبری نیز فراهم کرده است. جرائم سایبری به‌عنوان یکی از چالش‌های مدرن، قابلیت انجام بدون ردیابی در فضای مجازی را دارند. اینترنت بستری فراهم کرده که افراد یا گروه‌های سازمان‌یافته بتوانند از آن برای اعمال غیرقانونی استفاده کنند. در این میان، سازمان‌های بین‌المللی نظیر اینترپل نقش مهمی در مقابله با این تهدیدات ایفا می‌کنند. اینترپل با ارائه تجهیزات پیشرفته، روش‌های علمی، و تخصص‌های لازم، کشورهای عضو را در شناسایی و مبارزه با مجرمان سایبری یاری می‌دهد و به افزایش آگاهی عمومی در این زمینه کمک می‌کند. محققان در این پژوهش به بررسی مشارکت اینترپل در مبارزه با جرائم سایبری پرداخته و سؤال اصلی که مطرح می‌شود این است که اینترپل چگونه در مقابله با جرائم سایبری مشارکت داشته است؟ در پاسخی کوتاه می‌توان این‌چنین بیان نمود که اینترپل با انجام اقدامات و عملیات‌هایی نظیر عملیات رصد در جلوگیری از جرائم سایبری نقش مهمی داشته و در این زمینه با همکاری دیگر نهادها و ایجاد فرصت برای آموزش و مهارت‌یابی در زمینه مقابله با این‌گونه جرایم، به کاهش جرایم سایبری کمک نموده است. اینترپل به‌عنوان یکی از نهادهای کلیدی در هماهنگی و تقویت همکاری‌های پلیسی بین کشورها، نقش حیاتی در مبارزه با جرایم سایبری ایفا می‌کند و با ایجاد شبکه‌ای از متخصصان امنیت سایبری، تسهیل تبادل اطلاعات و ارائه آموزش‌های تخصصی، به کشورهای عضو کمک می‌کند تا توانایی خود را در شناسایی، ردیابی و مقابله با مجرمان سایبری افزایش دهند.

روش تحقیق

پژوهش حاضر با رویکرد توصیفی - تحلیلی و بر پایه‌ی مطالعات کتابخانه‌ای و اسنادی انجام شده است. در این تحقیق، ابتدا

مفاهیم پایه‌ای مرتبط با جرایم سایبری و ساختار سازمان بین‌المللی پلیس جنایی (اینترپل) از منظر حقوق بین‌الملل و حقوق فناوری اطلاعات تبیین می‌شود. سپس، با تحلیل محتوای اسناد رسمی، کنوانسیون‌ها، گزارش‌های سالانه و بیانیه‌های صادره از سوی اینترپل و نهادهای وابسته به آن، نقش و کارکرد این سازمان در پیشگیری، کشف و مقابله با جرایم سایبری بررسی می‌گردد. داده‌ها از طریق بررسی منابع علمی معتبر، مقالات پژوهشی، گزارش‌های رسمی، اسناد اجلاس‌های بین‌المللی و منابع حقوقی به زبان‌های فارسی و انگلیسی گردآوری شده است.

تحلیل داده‌ها بر مبنای استدلال حقوقی و سیاست‌گذاری بین‌المللی انجام شده و تلاش شده است تا باتکیه بر اصول حقوق بین‌الملل، میزان اثرگذاری، محدودیت‌ها و چالش‌های حقوقی و اجرایی اینترپل در مقابله با جرایم سایبری شناسایی شود. در این پژوهش تمرکز بر تحلیل محتوایی، استنباط منطقی و تبیین حقوقی عملکرد اینترپل در چارچوب همکاری‌های بین‌المللی است.

۱. چارچوب مفهومی

در عصر حاضر، با رشد فزاینده کاربرد رایانه‌ها و گسترش قلمرو فضای سایبری، به‌موازات آن، مخاطرات این حوزه نیز با افزایش چشمگیری مواجه شده است. این شرایط، ضرورت فراگیری دانش تخصصی در این محیط‌ها را به‌صورت امری اجتناب‌ناپذیر مطرح می‌سازد [۱]. بسیاری از فرایندهای حقوق بین‌الملل با ورود رایانه و سایبر در حال تغییر هستند و حقوق نیز از این تغییرات بی‌بهره نبوده و برای پایداری در این عرصه می‌بایست از روش‌ها و علوم نوین بهره‌مند باشند [۲]. انقلاب ارتباطات و اطلاعات، وسایل جدیدی برای بشر فراهم کرده است که زندگی را نسبت به گذشته آسان‌تر کرده است. با این حال، این انقلاب همچنین راه را برای ظهور رفتارهای انحرافی اجتماعی هموار کرده است که در گذشته امکان‌پذیر نبوده‌اند [۳]. مانند دزدی اطلاعات و نقض داده‌های محرمانه ذخیره شده در پایگاه‌های داده؛ بنابراین با رشد فناوری جرایم به اشکال جدیدی درآمده‌اند؛ زیرا دیگر همانند گذشته تهدیدآمیز نیستند. این جرایم به دنیای اطلاعات گسترش یافته‌اند که اکنون به طور بین‌المللی به‌عنوان جرایم یقه‌سفید شناخته می‌شوند. مجرمان مدرن قادر به ارتکاب جنایات هولناکی هستند بدون آنکه قطره‌ای خون بریزند [۴]. در واقع، دیگر جرایم با حرکت فیزیکی به مکان‌ها انجام نمی‌شود؛ بلکه این جرایم در امنیت و آرامش ارتکاب می‌یابند. تنها با فشردن یک کلید در صفحه‌کلید، ویرانی و تخریب بر اقتصاد شرکت‌های بزرگ وارد می‌کنند. این نوع جرایم محدود به یک منطقه یا کشور خاص نیست؛ بلکه، یک مشکل جهانی است.

۱-۱. اینترپل

اینترپل یک نهاد بین‌المللی است که به منظور مقابله با جرایم فراملی و تقویت امنیت عمومی در میان کشورهای عضو ایجاد شده است. این سازمان در سال ۱۹۲۳ میلادی در شهر وین، اتریش، تأسیس شد [۵]. مقر اصلی این سازمان در شهر لیون فرانسه قرار دارد و وظیفه اصلی آن تسهیل همکاری میان کشورها و هماهنگی میان نهادهای قضایی برای مبارزه با جرایم سازمان‌یافته و فرامرزی است. اینترپل که با مشارکت ۱۳۳ کشور فعالیت می‌کند، بزرگ‌ترین سازمان پلیسی بین‌المللی در جهان محسوب می‌شود [۶]. نقش کلیدی این سازمان، هماهنگی نیروهای پلیس کشورها برای مقابله با تهدیدات جهانی و ایجاد امنیت در سراسر جهان است. با وجود چالش‌های پیچیده و روزافزون اینترپل با بهره‌گیری از زیرساخت‌های پیشرفته و حمایت‌های عملیاتی توانسته است نقش مؤثری در پیشگیری و مقابله با جرایم ایفا کند.

۱-۱-۱. تاریخچه اینترپل

در سال ۱۹۱۴، به دعوت آلبرت اول، شاه موناکو، اولین همایش بین‌المللی بررسی مسائل پلیسی با حضور ۱۸۸ افسر بلندپایه پلیس و حقوق‌دان از ۲۴ کشور جهان در موناکو برگزار شد. این همایش به عنوان نخستین گام رسمی در راستای ایجاد سازمانی برای همکاری بین‌المللی در مسائل پلیسی به شمار می‌رفت. قرار بود جلسه بعدی در سال ۱۹۱۶ در بخارست برگزار شود، اما وقوع جنگ جهانی اول این برنامه را تا سال ۱۹۲۳ به تعویق انداخت. در سپتامبر ۱۹۲۳، دومین همایش بین‌المللی پلیس جنایی در شهر وین، اتریش به مدت پنج‌روز برگزار شد [۷]. در این همایش، رؤسای پلیس کشورهای مختلف از جمله اتریش، بلژیک، مصر، آلمان، فرانسه، یونان، مجارستان، هلند، ایتالیا، لهستان، رومانی، سوئد، سوئیس، آمریکا و یوگسلاوی حضور یافتند و به بحث در مورد مسائل پلیسی و ضرورت ایجاد نهادی بین‌المللی برای همکاری پرداختند. نتیجه این همایش، تأسیس "گروه بین‌المللی پلیس جنایی" بود که اساسنامه آن تدوین و مقر مرکزی آن در وین تعیین شد. در سال ۱۹۵۶، نام گروه به "سازمان بین‌المللی پلیس جنایی" تغییر یافت و اساسنامه آن بازنگری شد. در نهایت، در سال ۱۹۸۹، مقر اصلی این سازمان از سنت کلود فرانسه به محل کنونی آن در لیون انتقال پیدا کرد [۸]. طی سال‌ها، اینترپل گام‌های مهمی در ارتقای همکاری‌های بین‌المللی برداشته است. برای مثال، در سال ۱۹۴۹، سازمان ملل، اینترپل را به عنوان یک سازمان غیردولتی تأیید کرد [۹]. همچنین، ایجاد ایستگاه‌های رادیویی در سال ۱۹۵۳ و برگزاری اجلاس‌های عمومی در خارج از اروپا در دهه ۱۹۶۰، نشان‌دهنده گسترش فعالیت‌های این سازمان بود. اینترپل همچنان به عنوان یکی از مهم‌ترین نهادهای جهانی در مقابله با جرایم فرامرزی فعالیت می‌کند.^۱

۱-۲. اصول بنیادین سازمان اینترپل

سازمان اینترپل فعالیت‌های خود را بر اساس اصولی کلیدی و غیرقابل تغییر بنا نهاده است که به حفظ استقلال، بی‌طرفی و اثربخشی آن در سطح جهانی کمک می‌کند [۱۰]. این اصول عبارت‌اند از: ۱. عدم مداخله در امور سیاسی، نظامی، مذهبی یا نژادی؛ اینترپل هیچ‌گونه دخالتی در جرایمی که ماهیت سیاسی، نظامی، مذهبی یا نژادی دارند، ندارد و از همکاری با کشورهای عضو در این حوزه‌ها خودداری می‌کند. این اصل تضمین‌کننده بی‌طرفی و تمرکز سازمان بر جرایم عمومی است [۱۱]. ۲. احترام به حاکمیت ملی و تمامیت ارضی کشورها؛ اینترپل در تمامی فعالیت‌های خود احترام به استقلال و حاکمیت کشورها را به عنوان یک اصل اساسی رعایت می‌کند [۱۱]. ۳. تمرکز بر پیشگیری از جرایم عمومی و اجرای قانون؛ دامنه فعالیت اینترپل به جرایم عمومی محدود است و اقدامات آن در این حوزه تنها با توافق کشورهای عضو انجام می‌شود. ۴. جهانی بودن همکاری‌ها؛ اینترپل به عنوان یک سازمان بین‌المللی، همواره تلاش می‌کند همکاری‌هایی گسترده و جهانی میان کشورهای عضو برقرار سازد [۱۲]. ۵. برابری میان کشورهای عضو؛ تمامی کشورهای عضو، فارغ از اندازه یا قدرت سیاسی، در تعاملات و همکاری‌ها از جایگاه برابری برخوردارند [۱۳]. ۶. توسعه همکاری‌ها با سایر نهادها و نمایندگی‌ها؛ اینترپل همکاری‌های خود را با کشورهای عضو و دیگر سازمان‌ها گسترش داده و تلاش می‌کند منافع همه طرف‌های علاقه‌مند به مقابله با جرایم عمومی را تأمین کند [۱۴]. ۷. انعطاف‌پذیری در روش‌های اجرایی؛ سازمان، رویکردهای عملیاتی خود را بر اساس شرایط و نیازهای متنوع کشورهای عضو تنظیم می‌کند [۱۵].

این انعطاف‌پذیری به کاهش تشریفات اداری، حفظ انسجام و بهبود کارایی کمک می‌کند. این اصول، چارچوبی محکم برای عملکرد اینترپل فراهم می‌کنند و به سازمان امکان می‌دهند تا در مقابله با جرایم فرامرزی و ارتقای امنیت جهانی نقشی مؤثر ایفا کند.

۱-۱-۳. اهداف کلیدی سازمان اینترپل

سازمان اینترپل دارای سه هدف اساسی است [۱۶]: اولاً، این سازمان وظیفه تقویت همکاری‌های بین‌المللی میان ادارات پلیس کشورهای عضو را دارد. به عبارت دیگر، سازمان اینترپل باهدف ایجاد هماهنگی و تعامل میان نیروهای پلیس جنایی کشورهای

۱۹۴۱ برگزاری اولین کنگره پلیس قضایی در موناکو با حضور ۲۳ کشور؛ ۱۹۲۳ تشکیل کمیسیون بین‌المللی پلیس جنایی در وین؛ ۱۹۴۶ اصلاح سازمان در پاریس، یک سال پس از جنگ جهانی دوم، ایجاد سیستم اعلان ها و صدور اولین اعلان های قرمز، ۱۹۵۶ نامگذاری سازمان به سازمان بین‌المللی پلیس جنایی - اینترپل؛ ۱۹۷۱ رسمیت یافتن سازمان از سوی سازمان عنوان یک سازمان بین‌المللی؛ ۱۹۸۹ انتقال دبیرخانه کل از کلود به لیون؛ ۲۰۰۴ موافقت و راه اندازی نمایندگی اینترپل در سازمان ملل واقع در نیویورک؛

^۱. سال های کلیدی در تاریخ اینترپل

قاجاق آثار هنری و میراث فرهنگی، تروریسم بین‌المللی و آدم‌ربایی، مقابله با تروریسم، هواپیمارمایی و آدم‌ربایی، جرایم رایانه‌ای و سازمان‌یافته، مبارزه با جرایم اینترنتی و جرایم سازمان‌یافته، مدرن‌سازی شبکه‌های ارتباطی، ایجاد و تقویت شبکه‌های ارتباطی بین کشورهای عضو در سطح منطقه‌ای و بین‌المللی.

۲-۱. جرایم سایبری

جرایم سایبری به‌موازات فرصت‌هایی که از طریق افزایش سریع استفاده اینترنت برای تجارت الکترونیک و در کشورهای درحال‌توسعه ایجاد می‌شود تکامل یافته‌اند دلیل اصلی رشد جرایم سایبری از اواسط دهه ۲۰۰۰ به گسترش بات‌نت‌ها به‌عنوان ابزارهای انبوه برای سوءاستفاده از رایانه و تقویت این فعالیت‌ها نسبت‌داده‌شده است [۲۴]. جرایم سایبری بر اساس زمان‌های مختلف و تحولات در زمینه اطلاعات و فناوری به طور متمایز تعریف شده است. برخی از تعاریف، جرم‌شناسی سایبری را به تقلب‌های مالی سایبری، برنامه‌ها و اطلاعات محدود می‌کنند [۲۵]. این تعریف تنها به اطلاعات مالی و حساس در رایانه مالک یا زمانی که هدف جرم یک رایانه باشد، اشاره دارد. فضای اینترنت مضاف بر ابعاد روشن و در دسترس برای همگان، دارای ابعادی تاریک نیز بوده که بستری برای انجام جرایم سایبری و آزادی مجرمین هستند. مجرمین حوزه سایبر از تفاوت‌های موجود در ظرفیت‌های پیشگیری، کشف، تحقیق و تعقیب جرایم این حوزه سوءاستفاده نموده و اهداف خود را از طریق این فضا انجام می‌دهند [۲۶]. تعاریف وسیع‌تر شامل رفتارهای غیرقانونی است که با استفاده از یک رایانه انجام می‌شوند که جرایم سایبری را در ارتباط با یک شبکه از زمینه‌ها قرار می‌دهد، به‌طوری که شامل تمام اعمال مجرمانه‌ای می‌شود [۲۷]. برخی دیگر آن را به‌عنوان تمامی اعمال مجرمانه‌ای که با استفاده از یک رایانه انجام می‌شود به‌شرط آنکه نقش رایانه مهم باشد، تعریف می‌کنند و بیان می‌کنند جرایم سایبری یعنی استفاده آسان به‌طوری که مجرمان از دستگاه‌ها استفاده می‌کنند [۲۸] و پاک‌سازی آسان شواهد درحالی‌که ردیابی مرتکب دشوار است [۲۹]. جرایم سایبری به مهارت و دانش خاصی نیاز دارد و نیازمند حرفه است. جرایم سایبری می‌توانند به‌سرعت انجام شوند؛ زیرا مجرمان از جدیدترین فناوری‌ها استفاده می‌کنند [۳۰] و توسط اینترنت به دلیل ابزارها و شبکه‌هایی که استفاده می‌کنند با دقت زیاد انجام می‌شوند [۳۱]. مبهم هستند و ردیابی و تحقیق در مورد آن‌ها دشوار است، مشابه جرایم سنتی [۳۲]. جرم سایبری یک پدیده جهانی است؛ زیرا تمام دنیا به هم متصل است؛ بنابراین، کل آن به‌صورت مجازی درآمده است؛ بنابراین، تمام دنیا به یک حوزه برای جرایم سایبری تبدیل شده است [۳۳]. این جرایم معمولاً گزارش نمی‌شوند؛ زیرا یا قربانی از خسارت آگاه نبوده است یا از افشاشدن ترس دارد. به هر دلیلی، جرایم سایبری تنها به طور

عضو فعالیت می‌کند [۱۷]. این همکاری‌ها در چارچوب قوانین ملی هر کشور و با رعایت اصول اعلامیه جهانی حقوق بشر صورت می‌گیرد. ایجاد و توسعه نهادهای پیشگیرانه برای مقابله با جرایم عمومی؛ یعنی اینترنت به تأسیس و گسترش مؤسساتی می‌پردازد که هدف آنها پیشگیری از وقوع جرایم عمومی است تا از افزایش جرایم در سطح جهانی جلوگیری کند [۱۸]. عدم مداخله در موضوعات سیاسی، نظامی، مذهبی و نژادی از دیگر اهداف این سازمان است. بر اساس ماده ۳ اساسنامه اینترنت، این سازمان و کشورهای عضو از هرگونه ورود به امور مرتبط باسیاست، مذهب، نژاد یا فعالیت‌های نظامی منع شده‌اند. این اصل تضمین می‌کند که تمرکز سازمان صرفاً بر مقابله با جرایم عمومی باقی بماند. این اهداف بنیادین، جهت‌گیری اصلی اینترنت را در راستای ارتقای امنیت جهانی و پیشگیری از جرایم فراملی مشخص می‌کنند.

۴-۱-۱. وظایف اصلی سازمان اینترنت

سازمان اینترنت به‌عنوان سازمان بین‌المللی که در جهت امنیت عمومی فعالیت می‌کند دارای وظایفی است از جمله، انجام فعالیت‌های پلیسی در سطح بین‌المللی، اینترنت مسئولیت انجام فعالیت‌های پلیسی در تمامی کشورهای عضو را بر عهده دارد [۱۹]. [تهیه و مدیریت بانک‌های اطلاعاتی، سازمان اطلاعات و داده‌های مربوط به مجرمان بین‌المللی، خودروهای مسروقه، آثار فرهنگی دزدیده شده، روش‌های ارتکاب جرم و سایر موضوعات مرتبط را از کشورهای عضو جمع‌آوری کرده و در بانک‌های اطلاعاتی نگهداری می‌کند] [۲۰]. از دیگر وظایف این سازمان، برگزاری همایش‌ها و اجلاس‌های بین‌المللی است. اینترنت به سازماندهی رویدادهایی در زمینه‌های تخصصی و فنی پلیسی پرداخته تا تبادل اطلاعات و به‌روزرسانی شیوه‌های مقابله با جرم را تسهیل کند [۲۱]. تدوین و صدور دستورالعمل‌ها از دیگر وظایف این سازمان است که سازمان اینترنت قوانین و دستورالعمل‌های تخصصی در خصوص جرایم بین‌المللی را تدوین و صادر می‌کند. همکاری با مراجع قضائی بین‌المللی، از دیگر وظایف این سازمان است. اینترنت در خصوص مجرمان فراری از یک کشور به کشور دیگر با مراجع قضائی همکاری می‌کند و در زمینه استرداد مجرمان فعالیت دارد. همچنین اینترنت با تمرکز بر کشت، تولید، قاجاق و مسیرهای ترانزیت مواد مخدر، به مبارزه با این معضل جهانی می‌پردازد؛ علاوه بر این به کشف جعل مدارک مختلف از جمله گذرنامه، روادید و سایر اسناد رسمی می‌پردازد. از وظایف مهم اینترنت می‌توان به تعقیب مجرمان بین‌المللی اشاره نمود. اینترنت مجرمان را در سطح جهانی تحت تعقیب قرار می‌دهد و تلاش می‌کند تا آنها را به عدالت بسپارد [۲۲]. علاوه بر وظایف عمومی، اینترنت دارای وظایف تخصصی نیز است از جمله، جرایم زیست‌محیطی، آلوده‌سازی محیط‌زیست، قاجاق گونه‌های نادر و کمیاب [۲۳] و مواد پرتوزا، پول‌شویی و قاجاق آثار هنری، مبارزه با پول‌شویی و

ارگان‌های خاص برای اهداف غیرمستقیم صورت می‌گیرند، به‌طوری که از داده‌های هک‌شده برای ارتکاب جرایم استفاده می‌شود.

۲- مرور ادبیات

- پریوتیش گانگولی (۲۰۲۵) در مقاله‌ای تحت عنوان «پلیس دیجیتال: استفاده از نظارت بر رسانه‌های اجتماعی برای مقابله با جرایم سایبری» به این موضوع پرداخته است. یافته‌های این مقاله حاکی از این است که در عصر تحول دیجیتال، جرایم سایبری به تهدیدی پیچیده و بدون مرز تبدیل شده‌اند. رسانه‌های اجتماعی که زمانی صرفاً بستری برای ارتباطات بودند، اکنون به میدان نبرد و هم‌زمان ابزاری برای پیشگیری از جرم مبدل گشته‌اند. پلیس دیجیتال از طریق نظارت بر رسانه‌های اجتماعی، یک استراتژی نوظهور است که به نهادهای اجرای قانون امکان می‌دهد تهدیدات سایبری را به‌صورت زنده شناسایی، پیشگیری و مقابله کنند. با بهره‌گیری از هوش مصنوعی (AI)، یادگیری ماشین (ML) و تحلیل داده‌ها، مقامات قادر به ردیابی فعالیت‌های مشکوک، شناسایی مجرمان سایبری و کاهش ریسک‌ها قبل از تشدید جرایم هستند [۴۲].

- بوکاج و تاچی (۲۰۲۵) در مقاله‌ای تحت عنوان «تنظیم مقررات جهانی جرایم سایبری از طریق حقوق بین‌الملل و کنوانسیون‌های سایبری» به این موضوع پرداخته است. یافته‌های این مقاله حاکی از این است که پیشرفته‌تر شدن تهدیدات سایبری، همکاری بین‌المللی قوی را ضروری ساخته است. اداره جرایم سایبری اینترپل افزایش ۷۲ درصدی جرایم مبتنی بر هوش مصنوعی را از سال ۲۰۲۱ به‌ویژه در حوزه کلاهبرداری‌های مالی و تبلیغات دیپ‌فیک ثبت کرده است. این روند، نیاز فوری به ایجاد چارچوب‌های حقوقی هماهنگ و اشتراک اطلاعات لحظه‌ای بین کشورهای عضو را برجسته می‌سازد [۴۳].

-مرتضی جویبان و سوده حسینی (۱۴۰۳) در مقاله‌ای تحت عنوان «بهبود امنیت شبکه‌های سایبری مبتنی بر شناسایی انجمن‌ها با استفاده از الگوریتم خوشه‌بندی طیفی» به این موضوع پرداخته‌اند. یافته‌های این مقاله حاکی از این است که سازمان‌های جهانی دارای شبکه‌های سایبری بزرگی هستند که برای ذخیره و انتقال داده‌ها مورد استفاده قرار می‌گیرند. بیشتر این داده‌ها محرمانه است که شامل اطلاعات شخصی مشتریان و کارمندان، اسناد تجاری محرمانه و یا مالکیت معنوی سازمان‌ها است. درحالی‌که اتصال بالای شبکه‌ها و دستگاه‌های سایبری مدرن باعث پیشرفت‌های زیادی در عملکرد و کارایی سیستم‌های شبکه‌ای، فناوری‌های ارتباطی و توسعه سیستم اطلاعاتی شده و تمامی افراد جامعه و سازمان‌ها را درگیر ساخته است، اما از طرف دیگر منجر به افزایش آسیب‌پذیری آن‌ها در برابر حمله یا نفوذ شده است. فضای سایبری در برابر بسیاری از حملات و خطرات آسیب‌پذیر بوده و امنیت اطلاعات اصلی‌ترین چالش در این شبکه‌ها است [۴۴].

تصادفی یا پس از مدتی کشف می‌شوند. می‌توان گفت که جرایمی که فاش نشده‌اند، از آن‌هایی که فاش شده‌اند، شدیدتر هستند. فاصله بین تعداد واقعی جرایم سایبری و تعداد اعلام شده نگرانی جدی ایجاد می‌کند [۳۴]. دامنه واقعی خسارت‌های جرایم سایبری برای آشکارشدن نیاز به تخصص فنی آگاهانه دارد [۳۵] و درخواست جبران خسارت برای آسیب‌های وارد شده به قربانیان دشوار است [۳۶].

۱- ۲- ۱. اهداف جرایم سایبری

با پیشرفت فناوری، فضای سایبری به‌عنوان حوزه پنجم در حقوق بین‌الملل شناخته شده است. این قلمرو نوین افق‌های جدیدی در تعاملات بشری گشوده است، شیوه‌های ارتباطات انسانی را دگرگون ساخته است و چالش‌های حقوقی و حاکمیتی بی‌سابقه‌ای ایجاد نموده است [۳۷]. یکی از فعالیت‌های روزانه مردم دنیا در هر زمان و مکانی استفاده از فضای مجازی است. در دنیای امروزی، فضای مجازی نقشی مهم و اثرگذاری را در زندگی اشخاص ایفا می‌کند. اگرچه استفاده از فضای مجازی دارای محاسنی است و سبب راحت‌تر شدن زندگی اشخاص گردیده، اما عدم کاربرد صحیح از آن باعث ایجاد آسیب‌های بسیاری شده است که نگرانی‌هایی را در این رابطه ایجاد کرده است [۳۸]. هدف اصلی ارتکاب جرایم سایبری، به‌دست‌آوردن اطلاعات سایبری است که می‌تواند یا در سیستم‌های رایانه‌ای ذخیره شده باشد یا از طریق اینترنت منتقل شود. با این حال، این بدان معنا نیست که جرایم دیگری وجود ندارد که اهدافی غیر از به‌دست‌آوردن اطلاعات داشته باشند. جرایم سایبری بسیاری وجود دارند که به‌منظور کسب اطلاعات به‌خودی‌خود ارتکاب می‌یابند، به‌طوری که اطلاعات ذخیره شده یا تغییر داده شوند یا به طور کامل حذف شوند. بیشتر این جرایم به دنبال منافع اقتصادی به‌عنوان هدف هستند. جنگ اقتصادی همانند جنگ نظامی از اهمیت و جذابیت برخوردار است، با این تفاوت که نبردهای اقتصادی در یک زمینه متفاوت برگزار می‌شود [۳۹]. هدف اصلی به‌دست‌آوردن اطلاعات (از طریق اقداماتی مانند جعل کارت‌های اعتباری، هک کردن وبگاه‌ها و غیره) در اعمال اخاذی و اختلال در اخلاق کاری نهادهای عمومی نهفته است. مجرمان در ازای این اقدامات، منافع مالی یا سیاسی غیرقانونی به دست می‌آورند [۴۰]. جرایم سایبری ممکن است از فناوری برای کمک به تروریست‌ها و افراطی‌ها یا تبلیغ ایده‌های کفر استفاده کنند. زمانی که هدف جرایم سایبری رایانه‌ها باشند، هدف معمولاً واردآوردن آسیب کامل به آن‌هاست. در غیر این صورت، هدف این است که دستگاه‌ها را با استفاده از ویروس‌ها برای مدت طولانی از کار ببنداند [۴۱]. جرایم سایبری ممکن است به‌صورت فردی یا گروهی ارتکاب یابند. این جرایم معمولاً برای اهداف مستقیم مانند اخاذی، رشوه‌گیری یا افشاگری انجام می‌شوند [۴۰]. در مواقع دیگر، جرایم سایبری به‌منظور استخراج اطلاعات از افراد، نهادها یا

۴- دارایی‌های عملیاتی اینترنت

اینترنت همواره تلاش کرده است تا با انواع مختلف جرایم در سطح جهانی، از جمله جرایم سایبری، مبارزه کند. اینترنت اقداماتی برای تقویت تلاش‌ها انجام داده و مؤسسه‌ای را برای مبارزه با جرایم سایبری با استفاده از فناوری‌های پیشرفته و تیم‌های مختلف تأسیس کرده است [۵۰]. یکی از مراکز تازه تأسیس شده توسط اینترنت، مرکز جرایم سایبری چندرشته‌ای است که کارشناسان اینترنتی از نهادهای اجرای قانون و بخش صنعتی برای جمع‌آوری و تجزیه و تحلیل اطلاعات موجود در مورد فعالیت‌های مجرمانه در فضای سایبر گرد هم می‌آورد و اطلاعاتی را به کشورهای عضو ارائه می‌دهد [۵۱]. مرکز عملیات و هماهنگی در سال ۲۰۰۳ تأسیس شد تا به عنوان یک هاب ارتباطی میان دبیرکل اینترنت و دفاتر مرکزی کشورهای عضو عمل کند. این مرکز به کارگروه شورای امنیت کمک می‌کند و وظایف مهمی را از جمله پاسخ‌دهی و رسیدگی به درخواست‌های فوری و هماهنگی تبادل اطلاعات مربوط به عملیات مهم که شامل چندین کشور است، انجام می‌دهد [۵۲]. علاوه بر این، مرکز نوآوری که در مجموعه جهانی اینترنت برای نوآوری در سنگاپور قرار دارد، به تحقیق و توسعه ابزارها و روش‌های جدیدی می‌پردازد که در مبارزه با جرایم سایبری به کار می‌روند. این مرکز که شامل دانشگاهیان، تحلیلگران، کارکنان اجرای قانون و متخصصان فناوری است، برای همکاری در پیشرفت‌های امنیت فناوری اطلاعات و تلاش‌های ضد جرایم سایبری گرد هم می‌آورد [۵۳]. این مرکز بر پیش‌بینی تحقیقات و توسعه استراتژی‌های جدید متمرکز است. هدف آن برجسته‌سازی سازمان‌دهی مناسب نهادهای اجرای قانون، درک تأثیر ابزارهای تکنولوژیکی مدرن بر جرم، ایجاد استانداردهای جهانی برای کار پلیس بر اساس نیازهای کشورهای عضو و ارائه راه‌حل‌های فنی مانند شواهد دیجیتال قانونی به طور خاص برای نیازهای کشورهای عضو است. علاوه بر این، این مرکز بهترین خدمات ارائه شده توسط شبکه جهانی را شناسایی کرده و آن‌ها را در دسترس نهادهای اجرای قانون در سراسر جهان قرار می‌دهد. یکی از تیم‌های تخصصی برجسته در چارچوب مبارزه اینترنت با جرایم سایبری، تیمی است که به تارکینت و ارزش‌های دیجیتال اختصاص دارد. این تیم مسئول تهیه یک طبقه‌بندی جهانی از ارزش‌های دیجیتال است که دسته‌بندی‌های خاص داده‌ها را که باید در رابطه با تراکنش‌های مشکوک جمع‌آوری شوند، مشخص می‌کند [۵۴]. این می‌تواند شامل فعالیت‌هایی مانند تبادل ارزش و نوع خاص جرمی باشد که با تراکنش مرتبط است.

این دسته‌بندی‌ها به طور دیجیتالی به هر تراکنش رمزگذاری شده افزوده می‌شود، مشابه نحوه اضافه‌شدن داده‌های مربوط به مکان، تاریخ ثبت و تجهیزات استفاده شده به یک تصویر دیجیتال [۵۴].

محمد اختری و همکاران (۱۳۹۸) در مقاله‌ای تحت عنوان «مقایسه تطبیقی مدل‌های بلوغ امنیت سایبری و امنیت اطلاعات و احصای شاخص‌های امنیت سایبری مشترک» به این موضوع پرداخته‌اند. یافته‌های این مقاله حاکی از این است که حملات سایبری می‌تواند پیامدهای ناگواری را در شبکه‌های نظامی و همچنین زیرساخت‌های شبکه‌ای غیرنظامی ایجاد کنند. با مدل‌سازی حملات سایبری، تحلیلگران این حوزه با دانستن انواع مختلف حملات و فنون به کاررفته به ارزیابی اثرات هر کدام از حملات پرداخته و خود را برای دفاع در مقابل آنها آماده می‌کنند [۴۵].

۳- راهبردهای اینترنت برای مبارزه با جرایم سایبری

سازمان پلیس جنایی بین‌المللی در سال ۲۰۰۴ واحد ویژه‌ای برای جرایم سایبری تأسیس کرد. اینترنت با همکاری گروه^۱ یک طرح راهبردی برای مبارزه با جرایم سایبری طراحی کرد [۱۹] که شامل موارد زیر است؛ ایجاد مراکز تماس امن که به طور ۲۴ ساعته و ۷ روز هفته برای پلیس کشورهای عضو فعالیت می‌کنند [۴۶]؛ ارائه راهنمایی به پلیس محلی کشورهای عضو ICPO در مورد نحوه مبارزه با جرایم سایبری و آموزش و تحقیق در این زمینه. اینترنت هماهنگی میان کشورهای عضو را فراهم کرده و اطلاعات لازم را بین واحدهای تحقیقاتی برای کمک به مبارزه با جرایم سایبری ارائه می‌دهد [۴۷]. همچنین به ارتقای مهارت‌ها، دانش و توانمندی‌های فنی در زمینه امنیت سایبری کمک می‌کند. برنامه‌های آموزشی، ابزارها، پلتفرم‌های آموزشی و غیره، مهارت‌ها را در زمینه امنیت سایبری تقویت می‌کنند [۳۶]؛ پلتفرم‌های امنی برای تبادل داده‌ها و تحلیل‌ها فراهم می‌آورد تا دامنه تهدیدات و آسیب‌پذیری‌ها برای افراد و نهادها کاهش یابد، آن‌ها را پیش‌بینی کند و از آن‌ها جلوگیری نماید [۴۸]؛ اینترنت نیروی تخصص پلیس را فراهم کرده و هماهنگی‌های لازم برای اجرای اقدامات قانونی بین کشورهای عضو را انجام می‌دهد؛ اینترنت در یک شبکه وسیع فعالیت می‌کند که به آن کمک می‌کند تا میان بخش‌های خصوصی و عمومی هماهنگی ایجاد کرده و اجرای قانون را تسهیل نماید؛ پویش‌هایی را سازمان‌دهی می‌کند که بر روی اشکال مختلف جرایم سایبری روشنی می‌اندازد و توصیه‌هایی برای امنیت سایبری ارائه می‌دهد؛ اطلاعاتی که به تحلیل و تخصص فنی در زمینه جرایم سایبری می‌پردازد، به اشتراک می‌گذارد و به پیش‌بینی این نوع جرایم کمک می‌کند؛ قوانین و مقررات مربوط به امنیت سایبری و جرایم سایبری را توسعه داده و به اجرا درمی‌آورد؛ داده‌ها را تجزیه و تحلیل کرده و قوانین مربوطه را صادر می‌کند تا از وقوع و کاهش جرایم سایبری جلوگیری نماید [۴۹].

۱. (G8).

خود قرارداده که راه‌حل‌های لازم را برای حداقل رساندن خسارات ناشی از این نوع تهدیدات و حفظ امنیت بین‌المللی می‌طلبد [۵۹].

اینترپل برای مقابله با جرایم پیچیده و جهانی، همکاری‌های گسترده‌ای با شرکت‌های فناوری پیشرفته انجام می‌دهد [۵۶]. این همکاری‌ها بر استفاده از فناوری‌های نوین برای شناسایی، پیشگیری و کاهش جرایم متمرکز است.

۱-۲-۵. جرایم سایبری و امنیت دیجیتال

اینترپل با شرکت‌هایی مانند میکروسافت، سیسکو، کاسپرسکی همکاری می‌کند تا ابزارها و فناوری‌های پیشرفته‌ای برای مقابله با حملات سایبری، بدافزارها و باج‌افزارها توسعه دهد [۶۰]. این همکاری‌ها شامل اشتراک اطلاعات، تحلیل تهدیدات سایبری و پیشگیری از حملات دیجیتال است.

۲-۲-۵. استفاده از هوش مصنوعی و تحلیل داده

شرکت‌هایی مانند گوگل^۵ و آمازون^۶ در ارائه زیرساخت‌های پردازش و ابزارهای هوش مصنوعی به اینترپل نقش کلیدی دارند [۶۱]. این فناوری‌ها به تجزیه و تحلیل داده‌های بزرگ^۷ کمک می‌کنند و شناسایی الگوهای جرایم را سریع‌تر و دقیق‌تر می‌سازند.

۳-۲-۵. مبارزه با قاچاق انسان و دارو

اینترپل در همکاری با پلتفرم‌هایی مانند فیس‌بوک^۸ و توییتر^۹ تلاش می‌کند تا تبلیغات غیرقانونی قاچاق انسان یا فروش داروهای تقلبی در فضای مجازی را شناسایی و حذف کند [۶۲].

۴-۲-۵. حفاظت از کودکان در فضای آنلاین

با همکاری شرکت‌هایی مانند میکروسافت^{۱۰} و تورن^{۱۱}، اینترپل ابزارهای پیشرفته‌ای برای شناسایی و مبارزه با سوءاستفاده از کودکان در فضای مجازی توسعه داده است [۶۳]. این ابزارها شامل فناوری تشخیص تصویر و تحلیل محتوای غیرقانونی است.

۵-۲-۵. استفاده از فناوری بلاک‌چین

اینترپل در حال بررسی همکاری با شرکت‌هایی است که در حوزه فناوری بلاک‌چین فعالیت دارند تا شفافیت بیشتری در تراکنش‌های مالی ایجاد کند و پول‌شویی و جرایم مالی مرتبط را کاهش دهد [۶۴]. این همکاری‌ها به اینترپل کمک می‌کند تا توان عملیاتی خود را در مواجهه با چالش‌های فناوری مدرن افزایش دهد و امنیت بین‌المللی را تقویت کند.

این طبقه‌بندی که به صورت عمومی و آنلاین در دسترس است، حول سه دسته اطلاعاتی می‌چرخد: افراد، سازمان‌ها و موجودیت‌های دیجیتال [۵۵]. این دسته‌ها شامل خدماتی مانند بازارهای تاریک نت و صرافی‌های ارز دیجیتال، همچنین نهادهایی که تسهیل‌کننده تبادل پیام‌ها و سایر ارائه‌دهندگان خدمات مرتبط با تراکنش هستند، است [۵۶]. انواع جرایم، فعالیت‌های غیرقانونی مرتبط با تراکنش را نشان می‌دهند، مانند فروش داروها یا سلاح‌های غیرقانونی آنلاین. طبقه‌بندی نهایی جهانی، یک راهنمای استاندارد شده را فراهم می‌آورد که می‌تواند توسط نهادهای اجرای قانون، بخش خصوصی و محافل دانشگاهی برای اضافه کردن دسته‌بندی‌ها به ارزش‌های دیجیتال استفاده شود.

۵- اقدامات اینترپل در زمینه جرایم سایبری

اینترپل در سال‌های اخیر اقدامات چشمگیری در مقابله با جرایم سایبری داشته است که در ادامه به برخی از این اقدامات خواهیم پرداخت:

۱-۵. عملیات مخفی

عملیات مخفی اینترپل شامل مجموعه‌ای از تلاش‌ها و اقدامات محرمانه برای شناسایی، تعقیب و دستگیری مجرمان بین‌المللی است که اغلب در جرایم سازمان‌یافته، قاچاق مواد مخدر، جرایم سایبری، تروریسم و سایر فعالیت‌های فراملی مشارکت دارند. این عملیات معمولاً شامل همکاری گسترده میان نیروهای پلیس کشورهای عضو، استفاده از ابزارهای پیشرفته تحلیل داده، و هماهنگی در سطح جهانی است [۵۷]. از جمله نمونه‌های بارز این عملیات می‌توان به موارد زیر اشاره کرد: عملیات پانگه^۱، مقابله با فروش غیرقانونی داروهای تقلبی آنلاین، عملیات اینفرا^۲، تمرکز بر دستگیری فراریان بین‌المللی که به جرایم سنگین متهم شده‌اند. عملیات ماشه^۳، مبارزه با قاچاق سلاح‌های غیرقانونی، عملیات لیبرترا^۴، تمرکز بر شناسایی و نجات قربانیان قاچاق انسان و مهاجرت غیرقانونی [۵۸]. این عملیات به دلیل ماهیت جهانی اینترپل و توانایی آن در ایجاد ارتباط سریع میان کشورهای مختلف، در دستیابی به نتایج موفقیت‌آمیز مؤثر بوده‌اند. هدف این اقدامات تقویت امنیت جهانی از طریق کاهش جرایم بین‌المللی است.

۲-۵. همکاری با شرکت‌های فناوری

با گسترش فضای سایبری، عرصه جدیدی از تهدیدات برای دولت‌ها در قالب تهدیدات سایبری ایجاد شده است و جنبه‌های مختلف امنیت ملی از جمله امنیت اجتماعی، اقتصادی، نظامی و سیاسی و همچنین امنیت بین‌المللی و منطقه‌ای را تحت تأثیر

⁵. Google.

⁶. Amazon.

⁷. Big Data.

⁸. Meta.

⁹. Twitter.

¹⁰. Microsoft.

¹¹. Thorn.

¹. Pangea.

². Infra.

³. Trigger.

⁴. Libberterra.

۳- ۵. عملیات رصد

اینترپل به عنوان بزرگترین سازمان پلیس بین‌المللی، نقش بسیار مهمی در هماهنگی تلاش‌های پلیس کشورهای عضو در راستای مبارزه با جرایم بین‌المللی ایفا می‌کند [۶۵]. یکی از فعالیت‌های کلیدی این سازمان، عملیات رصد است که به منظور ردیابی و شناسایی مجرمان، گروه‌های تبهکار و فعالیت‌های غیرقانونی در سطح بین‌المللی انجام می‌شود.

۱- ۳- ۵. اهداف عملیات رصد اینترپل

اینترپل از طریق عملیات رصد به دنبال آن است که جرایم ارتكابی را کنترل نماید و در همین راستا اهدافی را نیز دنبال می‌کند. از جمله اهداف اینترپل در عملیات رصد می‌توان به موارد زیر اشاره نمود: شناسایی مجرمان متواری^۱، ردیابی شبکه‌های جنایی^۲، جمع‌آوری اطلاعات^۳، پیش‌بینی جرایم^۴ [۶۶].

۲- ۳- ۵. روش‌های مورد استفاده در عملیات رصد

اینترپل در اجرایی کردن عملیات خود از روش‌های استفاده می‌کند. اینترپل از یک پایگاه داده جامع و به روز استفاده می‌کند که اطلاعات مربوط به مجرمان، پرونده‌های جنایی و اشیاء مسروقه را در خود جای داده است. همچنین این سازمان با صدور انواع مختلف اعلان‌های بین‌المللی (مانند اعلان قرمز، آبی، زرد و بنفش) به پلیس کشورهای عضو در مورد افراد تحت تعقیب، افراد گمشده، اشیاء مسروقه و روش‌های جدید مجرمان اطلاع‌رسانی می‌کند [۶۷]. علاوه بر این، اینترپل با همکاری نزدیک با پلیس کشورهای عضو، اطلاعات را به اشتراک می‌گذارد، عملیات مشترک را برنامه‌ریزی می‌کند و از تجربیات یکدیگر بهره می‌برد و با استفاده از فناوری‌های نوین مانند هوش مصنوعی، تحلیل داده‌های بزرگ و بیومتریک برای بهبود کارایی عملیات رصد استفاده می‌کند.

۳- ۳- ۵. اهمیت عملیات رصد اینترپل

عملیات رصد اینترپل به کاهش جرایم بین‌المللی، افزایش امنیت شهروندان و تقویت همکاری بین‌المللی در مبارزه با جرایم کمک می‌کند این سازمان با شناسایی و دستگیری مجرمان، به اجرای عدالت کمک کرده و به قربانیان جرایم اطمینان می‌دهد که مجرمان به سزای اعمال خود خواهند رسید. اینترپل نقش مهمی در مبارزه با تروریسم بین‌المللی ایفا می‌کند و با ردیابی و دستگیری تروریست‌ها،

از وقوع حملات تروریستی جلوگیری می‌کند [۶۸]. به صورت کلی، عملیات رصد اینترپل یک ابزار قدرتمند برای مبارزه با جرایم بین‌المللی است که به لطف همکاری گسترده پلیس کشورهای عضو و استفاده از فناوری‌های نوین، روز به روز کارآمدتر می‌شود.

۴- ۵. برنامه‌های آموزشی

اینترپل به عنوان بزرگترین سازمان پلیس بین‌المللی، نقش مهمی در مقابله با جرایم سایبری ایفا می‌کند. یکی از راه‌های مقابله با این جرایم، آموزش و ارتقای آگاهی نیروهای پلیس کشورهای عضو در حوزه امنیت سایبری است [۶۹]. جرایم سایبری به سرعت در حال تکامل هستند و برای مقابله با آن‌ها، نیاز به دانش و مهارت‌های تخصصی در حوزه فناوری اطلاعات وجود دارد. این جرایم مرز نمی‌شناسند و برای مقابله با آن‌ها، همکاری بین‌المللی و تبادل اطلاعات ضروری است [۷۰]. علاوه بر آن، بسیاری از زیرساخت‌های حیاتی مانند شبکه‌های برق، حمل و نقل و بانکداری به صورت آنلاین فعالیت می‌کنند و در معرض حملات سایبری قرار دارند.

۱- ۴- ۵. برنامه‌های آموزشی سایبری اینترپل

اینترپل برنامه‌های آموزشی متنوعی را برای نیروهای پلیس کشورهای عضو ارائه می‌دهد که شامل مواردی می‌شود. از جمله، دوره‌های آموزشی آنلاین که این دوره‌ها به صورت خودآموز و تعاملی طراحی شده‌اند و به شرکت‌کنندگان امکان می‌دهد در هر زمان و مکانی به آن‌ها دسترسی داشته باشند. کارگاه‌های آموزشی حضوری که این کارگاه‌ها به صورت حضوری برگزار می‌شوند و فرصتی برای تبادل تجربیات و دانش بین کارشناسان مختلف فراهم می‌کنند [۷۱]. اینترپل به طور مرتب هم‌اندیشی‌ها و اجلاس‌هایی را در سطح بین‌المللی برگزار می‌کند که در آن‌ها آخرین تحولات در حوزه امنیت سایبری مورد بحث و بررسی قرار می‌گیرد و با تبادل کارشناسان بین کشورهای عضو، به ارتقای سطح دانش و مهارت‌های نیروهای پلیس کمک می‌کند. همچنین اینترپل پایگاه‌های داده‌ای را در اختیار نیروهای پلیس قرار می‌دهد که حاوی اطلاعات مفیدی در مورد آخرین تهدیدات سایبری، ابزارهای مقابله با آن‌ها و بهترین روش‌های تحقیقات سایبری است.

۲- ۴- ۵. حوزه‌های آموزشی

برنامه‌های آموزشی اینترپل معمولاً بر روی حوزه‌های زیر تمرکز دارند: تحقیقات سایبری: روش‌های جمع‌آوری، تحلیل و حفظ شواهد دیجیتال، پاسخگویی به حوادث سایبری: نحوه واکنش به حملات سایبری و مدیریت بحران، جرایم سایبری علیه کودکان: مقابله با جرایم سایبری علیه کودکان مانند کودک‌آزاری آنلاین و سوءاستفاده از کودکان، کلاهبرداری‌های سایبری: شناسایی و مقابله با انواع مختلف کلاهبرداری‌های سایبری [۷]. جرایم سایبری سازمان‌یافته: مقابله با گروه‌های تبهکاری که از فضای سایبری برای انجام فعالیت‌های مجرمانه استفاده می‌کنند.

^۱. اینترپل با استفاده از پایگاه داده‌های گسترده خود و همکاری با پلیس کشورهای عضو، به دنبال شناسایی و دستگیری مجرمانی است که از کشور خود گریخته‌اند؛

^۲. این سازمان تلاش می‌کند تا شبکه‌های جنایی سازمان‌یافته را شناسایی کرده و فعالیت‌های آن‌ها را مختل کند؛

^۳. عملیات رصد به اینترپل امکان می‌دهد تا اطلاعات مهمی در مورد انواع مختلف جرایم، روش‌های ارتكاب جرم و روندهای نوظهور جرم و جنایت جمع‌آوری کند؛

^۴. با تحلیل اطلاعات جمع‌آوری شده، اینترپل می‌تواند به پیش‌بینی وقوع جرایم و اتخاذ تدابیر پیشگیرانه کمک کند

۳-۴-۵. مزایای برنامه‌های آموزشی اینترپل

برنامه‌های آموزشی اینترپل باعث ارتقای سطح دانش و مهارت می‌شود. این برنامه‌ها به نیروهای پلیس کمک می‌کنند تا دانش و مهارت‌های خود را در حوزه امنیت سایبری ارتقا دهند. همچنین این برنامه‌ها فرصتی برای همکاری و تبادل اطلاعات بین نیروهای پلیس کشورهای مختلف فراهم می‌کنند و باعث بهبود مقابله با جرایم سایبری می‌شوند و با ارتقای سطح دانش و مهارت نیروهای پلیس، می‌توان به طور مؤثرتر با جرایم سایبری مقابله کرد و به این وسیله با افزایش امنیت سایبری، می‌توان از شهروندان در برابر تهدیدات سایبری محافظت کرد [۷۳].

برنامه‌های آموزشی سایبری اینترپل نقش مهمی در ارتقای امنیت سایبری در سطح جهانی ایفا می‌کند. با سرمایه‌گذاری در آموزش و ارتقای آگاهی نیروهای پلیس، می‌توان به طور مؤثرتر با جرایم سایبری مقابله کرد و دنیای سایبری را به مکانی امن‌تر تبدیل کرد.

۶- شیوه‌های نوین اینترپل در مبارزه با جرایم سایبری با کمک الگوریتم‌های یادگیری ماشین

اینترپل با ترکیب روش‌های فناوری‌های رایانه‌ای و سایبری، به یک نهاد توانمند در کشف و پیشگیری از جرایم سایبری جهانی تبدیل شده است. این روش‌ها علاوه بر کارایی فنی، نیازمند چارچوب‌های حقوقی شفاف، همکاری بین‌المللی، و توجه به حریم خصوصی کاربران نیز هستند.

۶-۱. روش‌های یادگیری ماشین توسط اینترپل

یادگیری عمیق به سرعت در حال رشد است و به نتایج انقلابی در حوزه‌های تشخیص گفتار، پردازش تصویر، تشخیص الگو و بسیاری از حوزه‌های کاربردی دیگر دست یافته است. در پی این موفقیت‌ها، بسیاری از فن‌های تحلیل خودکار داده‌ها در حال تبدیل شدن به رویه‌های متداول در سازمان‌های اجرای قانون نیز هستند [۷۴]. در مبارزه با جرایم سایبری، اینترپل می‌تواند از روش‌های یادگیری ماشین برای پیش‌بینی، کشف و تحلیل تهدیدات سایبری استفاده کند. این روش‌ها عبارت‌اند از یادگیری با ناظر، یادگیری بدون ناظر، یادگیری نیمه‌نظارتی و یادگیری تقویتی که در ادامه به این موارد پرداخته خواهد شد.

۶-۱-۱. یادگیری با ناظر

امروزه به طور معمول در حوزه‌های مختلف از روش‌های یادگیری ماشینی توسط سازمان‌های گوناگون استفاده می‌شود. اینترپل که یکی از سازمان‌هایی است که از این روش‌ها استفاده می‌کند، می‌تواند از یادگیری با ناظر^۱ برای تشخیص خودکار ایمیل‌ها یا پیام‌های

فیشینگ استفاده کند و با تحلیل محتوای دیجیتال کشف‌شده از مجرمان سایبری و استفاده از مدل آموزش‌دیده برای شناسایی محتوای مشابه در سطح بین‌المللی این تهدیدات را کاهش دهد [۷۵]. در این روش، مدل‌های هوش مصنوعی با استفاده از داده‌های برچسب خورده (مانند هزاران نمونه ایمیل فیشینگ و ایمیل سالم) آموزش می‌بینند تا الگوهای حمله را شناسایی کنند. پس از آموزش، سیستم می‌تواند پیام‌های جدید را بررسی و دسته‌بندی کند.

۶-۱-۲. یادگیری بدون ناظر

یادگیری بدون ناظر^۲ در مواقعی است که داده‌های جرایم جدید یا بدون سابقه در دسترس هستند. اینترپل می‌تواند از خوشه‌بندی یا تشخیص ناهنجاری استفاده کند و شبکه‌های ناشناخته یا تازه‌تأسیس جرایم سایبری که هنوز الگوهای مشخصی ندارند را کشف کند [۷۶]. برای مثال، بررسی تراکنش‌های بانکی ناشناس یا رفتارهای غیرعادی کاربران در شبکه‌های دارکوب. مدل بدون ناظر می‌تواند رفتارهایی را که از الگوی طبیعی خارج هستند شناسایی کرده و به تحلیلگران هشدار دهد.

۶-۱-۳. یادگیری نیمه‌نظارتی

یادگیری نیمه‌نظارتی^۳ نوعی از فن‌های یادگیری ماشین است که حالت میانی بین یادگیری با ناظر و بدون ناظر محسوب می‌شود. در این روش مجموعه داده‌ها به صورت نیمه برچسب خورده هستند. در رابطه با جرایم سایبری که اغلب داده‌های دیجیتال مرتبط تنها بخشی برچسب‌گذاری شده‌اند این یادگیری مفید است [۷۷]. مثلاً وقتی فقط بخشی از حساب‌های مشکوک در شبکه‌های اجتماعی مشخص‌اند، مدل می‌تواند با استفاده از اطلاعات محدود برچسب‌دار، بر کل داده‌ها اعمال تحلیل کند و روابط پنهان را کشف کند و اینترپل از این طریق به شناسایی گروه‌های مجرمانه سایبری با استفاده از داده‌های جزئی به دست آمده از همکاری با کشورهای مختلف می‌پردازد.

۶-۱-۴. یادگیری تقویتی

پیشرفت‌های اخیر در شبکه‌های عصبی عمیق یادگیری تقویتی^۴ را به یکی از مهم‌ترین و کاربردی‌ترین فناوری‌های حال حاضر تبدیل کرده است. این روش یادگیری مبتنی بر تعامل یک عامل نرم‌افزاری با یک محیط ناشناخته است [۷۸]. این یادگیری زمانی مورد استفاده قرار می‌گیرد که سامانه دفاع سایبری اینترپل وظیفه دارد از سیستم‌های اطلاعاتی بین‌المللی در برابر حملات دفاع کند. یادگیری تقویتی به مدل اجازه می‌دهد تا با دریافت پاداش و مجازات، رفتار دفاعی خود را بهینه کند. مثلاً چگونه به حملات مختلف واکنش نشان دهد یا الگوی فایروال‌ها را تغییر دهد. اینترپل از طریق این

^۲ Unsupervised Learning.

^۳ Semi-Supervised Learning.

^۴ Reinforcement Learning

^۱ Supervised Learning.

باشند، نیاز به متخصصین فنی برای تطبیق الگوریتم‌ها با ساختار جرایم سایبری بین‌المللی [۷۹].

۶-۳. تحلیل عددی و امکان‌سنجی سایبری اینترنت

باتوجه به پیچیدگی و فرامولی بودن جرایم سایبری، ارزیابی نقش نهادهای بین‌المللی مانند اینترنت تنها به صورت نظری کافی نیست. برای سنجش اثرگذاری واقعی این نهاد، بررسی آماری و عددی عملکرد آن ضرورت دارد. بررسی گزارش‌های رسمی اینترنت نشان می‌دهد که از سال ۲۰۱۹ تا ۲۰۲۳ بیش از ۱۲۰ هشار جهانی در حوزه جرایم سایبری صادر شده و عملیات منجر به بازداشت هزاران مجرم سایبری در قالب همکاری میان بیش از ۷۰ کشور شده است. همچنین آمار منتشرشده توسط یورپول و اینترنت حاکمی از آن است که میزان تبادل داده‌های سایبری میان کشورها در این مدت به طور متوسط ۲۰ درصد در سال رشد داشته است [۸۰]. باوجود این داده‌ها، امکان انجام ارزیابی عددی دقیق و بومی‌سازی مدل همکاری اینترنت برای کشورهایمانند ایران، به دلیل محدودیت‌های زیر، با چالش‌هایی مواجه است: عدم دسترسی به داده‌های محرمانه عملیاتی اینترنت و ملاحظات امنیتی در انتشار جزئیات، تفاوت در تعاریف حقوقی جرایم سایبری میان کشورها که مانع مقایسه‌های کمی مستقیم می‌شود، نبود بانک داده عمومی و ساخت‌یافته درباره عملکرد داخلی کشورهای عضو در اجرای همکاری‌ها. بااین‌حال، استفاده از الگوهای آماری منطقه‌ای و تطبیقی و شبیه‌سازی مدل‌های همکاری (مانند تحلیل تعداد پرونده‌های باز در سطح ملی با مشارکت پلیس بین‌الملل)، می‌تواند بستری مناسب برای تحلیل‌های آینده‌پژوهانه و طراحی نظام همکاری مؤثرتر در مبارزه با جرایم سایبری فراهم آورد.

۶-۳. چالش‌های استفاده از الگوریتم‌های هوشمند

با اینکه اینترنت از یادگیری ماشین برای مقابله با جرایم سایبری استفاده می‌کند، اما در حوزه فنی و ادبیات یادگیری ماشین، با چالش‌های متعددی مواجه است از جمله؛ دقت پایین^۱. بسیاری از مدل‌ها در شناسایی الگوهای پیچیده حملات سایبری مثلاً حملات فیشینگ‌های هدفمند (عملکرد ضعیفی دارند، به خصوص زمانی که داده‌ها ناقص یا غیرهمگن باشند). زمان اجرای بالا؛^۲ الگوریتم‌هایی مثل Random Forest یا Deep Learning در داده‌های حجیم زمان زیادی برای آموزش و پیش‌بینی نیاز دارند که در عمل ممکن است به تأخیر در پاسخ منجر شود [۸۰].

اوابستگی به نوع حمله^۳ برخی مدل‌ها تنها برای دسته خاصی از تهدیدات (مثلاً شناسایی باتنت یا بدافزار خاص) آموزش‌دیده‌اند و در مسائل دیگر دقت پایین دارند. مسائل دائمی یا مقطعی؛ مشکل

روش به توسعه سیستم‌های هوشمند واکنش سریع که بتوانند در برابر تهدیدات نوظهور، تصمیم‌گیری مستقل و مؤثر داشته باشند می‌پردازد.

جدول (۱): روش‌های یادگیری ماشین و کاربرد آن در جرایم سایبری

نوع یادگیری	روش یادگیری	نوع داده	نوع عمل	نوع چالش
یادگیری نظارت‌شده	دستورالعمل‌های ارجحی	داده‌های برچسب‌دار	یادگیری	یادگیری
یادگیری نظارت‌شده	دستورالعمل‌های ارجحی	داده‌های برچسب‌دار	یادگیری	یادگیری
یادگیری نظارت‌شده	دستورالعمل‌های ارجحی	داده‌های برچسب‌دار	یادگیری	یادگیری
یادگیری نظارت‌شده	دستورالعمل‌های ارجحی	داده‌های برچسب‌دار	یادگیری	یادگیری
یادگیری نظارت‌شده	دستورالعمل‌های ارجحی	داده‌های برچسب‌دار	یادگیری	یادگیری
یادگیری نظارت‌شده	دستورالعمل‌های ارجحی	داده‌های برچسب‌دار	یادگیری	یادگیری
یادگیری نظارت‌شده	دستورالعمل‌های ارجحی	داده‌های برچسب‌دار	یادگیری	یادگیری
یادگیری نظارت‌شده	دستورالعمل‌های ارجحی	داده‌های برچسب‌دار	یادگیری	یادگیری
یادگیری نظارت‌شده	دستورالعمل‌های ارجحی	داده‌های برچسب‌دار	یادگیری	یادگیری
یادگیری نظارت‌شده	دستورالعمل‌های ارجحی	داده‌های برچسب‌دار	یادگیری	یادگیری

۶-۲. پیچیدگی زمانی، حافظه و محدودیت‌های

اجرای روش‌های یادگیری ماشین توسط اینترنت

اجرای مدل‌های یادگیری ماشین در تحلیل داده‌های سایبری، بسته به نوع الگوریتم، میزان داده و نوع یادگیری، هزینه‌ها و چالش‌های متفاوتی دارد.

جدول (۲): اجرای مدل‌های یادگیری ماشین

نوع یادگیری	نوع داده	نوع عمل	نوع چالش
یادگیری نظارت‌شده	داده‌های برچسب‌دار	یادگیری	یادگیری
یادگیری نظارت‌شده	داده‌های برچسب‌دار	یادگیری	یادگیری
یادگیری نظارت‌شده	داده‌های برچسب‌دار	یادگیری	یادگیری
یادگیری نظارت‌شده	داده‌های برچسب‌دار	یادگیری	یادگیری
یادگیری نظارت‌شده	داده‌های برچسب‌دار	یادگیری	یادگیری
یادگیری نظارت‌شده	داده‌های برچسب‌دار	یادگیری	یادگیری
یادگیری نظارت‌شده	داده‌های برچسب‌دار	یادگیری	یادگیری
یادگیری نظارت‌شده	داده‌های برچسب‌دار	یادگیری	یادگیری
یادگیری نظارت‌شده	داده‌های برچسب‌دار	یادگیری	یادگیری
یادگیری نظارت‌شده	داده‌های برچسب‌دار	یادگیری	یادگیری

به صورت کلی محدودیت‌های اینترنت در این زمینه عبارت‌اند از؛ نیاز به داده‌های بزرگ، پاک‌سازی شده و امن، هزینه‌بر بودن آموزش مدل‌ها از نظر زمان و توان پردازشی، پیچیدگی پیاده‌سازی در فضای حقوقی یا پلیسی که داده‌ها ممکن است طبقه‌بندی شده یا محرمانه

^۱. Low Accuracy.

^۲. High Computational Time.

^۳. Domain Specificity.

دقت پایین یا زمان بالا، همیشگی نیست، اما در حملات جدید و پیچیده، دائماً باید مدل‌ها بازآموزی شوند تا مؤثر باقی بمانند.

۷ - چالش‌های اینترنت در زمینه جرایم سایبری

اینترنت، به‌عنوان یک سازمان بین‌المللی پلیس، با چالش‌های متعددی در مقابله با جرایم سایبری مواجه است. این چالش‌ها می‌توانند به طور قابل‌توجهی بر توانایی اینترنت در شناسایی و دستگیری مجرمان سایبری تأثیر بگذارند. یکی از موانع مهم در اجرای مؤثر اقدامات اینترنتی چالش‌های حقوقی در همکاری‌های بین‌المللی است که مورد بحث ما است. چالش‌های حقوقی در همکاری‌های بین‌المللی اینترنتی برای مقابله با جرایم سایبری از مهم‌ترین موانع در اجرای مؤثر اقدامات این سازمان به شمار می‌روند. این چالش‌ها به دلایل مختلفی از جمله تفاوت در قوانین داخلی کشورها، محدودیت‌های حقوقی برای تبادل اطلاعات و عدم هماهنگی در اجرای قوانین بین‌المللی بروز پیدا می‌کنند^۱ [۸]. از دیگر چالش‌های حقوقی می‌توان به حاکمیت ملی و استقلال قضایی اشاره نمود. بسیاری از کشورها به دلیل حساسیت به حاکمیت ملی، از اشتراک‌گذاری اطلاعات حیاتی با سایر کشورها خودداری می‌کنند. این مسئله به‌ویژه در مواقعی که یک کشور محل اقامت مجرم است؛ اما قربانی در کشور دیگری حضور دارد، پیچیدگی بیشتری ایجاد می‌کند.

عدم وجود معاهدات بین‌المللی جامع نیز از دیگر چالش‌های حقوقی است. نبود معاهدات حقوقی جامع و الزام‌آور بین کشورها، مبارزه با جرایم سایبری را دشوارتر می‌کند. برخی کشورها ممکن است از پذیرش درخواست‌های استرداد مجرمان سایبری به دلیل فقدان معاهده یا مسائل سیاسی خودداری کنند.

۸ - دستاوردهای اینترنت در زمینه سایبری

اینترنت در زمینه سایبری دستاوردهایی داشته از جمله، عملیات‌های مختلف، تأثیر بر امنیت سایبری، دستگیری مجرمان سایبری، دستگیری هک‌های کلاهبرداری آنلاین، دستگیری اعضای باند رانسوم‌ویر، شناسایی و دستگیری هکر روسی و دستگیری مجرمان سرقت داده‌ها که در ذیل به بررسی آنها پرداخته می‌شود.

۸-۱. موفقیت‌های عینی اینترنت

اینترنت موفقیت‌های قابل‌توجهی را در زمینه سایبری به ثبت رسانده است. این دستاوردها نشان‌دهنده اثربخشی همکاری‌های بین‌المللی و اقدامات سازمان در مقابله با تهدیدات پیچیده سایبری

است. به طور مثال، در سال ۲۰۱۸، اینترنتی عملیات‌های^۲ را در سطح جهانی راه‌اندازی کرد که موفق به شناسایی و دستگیری چندین مجرم بزرگ در زمینه کلاهبرداری‌های اینترنتی شد. این عملیات به توقف چندین شبکه کلاهبرداری که در کشورهای مختلف فعال بودند، منجر شد. این دستاورد نه تنها امنیت کاربران اینترنتی را بهبود بخشید، بلکه به کاهش کلاهبرداری‌های مالی در سطح جهانی کمک کرد. همچنین در همکاری با شرکت‌های فناوری و نهادهای دولتی، اینترنتی توانست چندین گروه مهاجم سایبری را که در حملات فیشینگ دخیل بودند، شناسایی و تحت تعقیب قرار دهد. این حملات به سرقت اطلاعات حساس کاربران اینترنتی، از جمله اطلاعات بانکی و شناسنامه‌ای، منجر می‌شد. تلاش‌های اینترنتی در شناسایی و ازبین‌بردن این تهدیدات، منجر به کاهش قابل‌توجه کلاهبرداری‌های آنلاین شد [۶]. علاوه بر این، اینترنتی یک شبکه جهانی برای تبادل اطلاعات بین نیروهای پلیس کشورهای مختلف ایجاد کرده است. این شبکه به پلیس‌ها اجازه می‌دهد تا به‌سرعت به اطلاعات مربوط به مجرمان سایبری، روش‌های آن‌ها و آخرین تهدیدات دسترسی پیدا کنند.

۸-۲. تأثیر اینترنت بر امنیت سایبری

اینترنت تأثیرات قابل‌توجهی بر امنیت سایبری در سطح جهانی داشته است. از طریق همکاری‌های بین‌المللی و اشتراک‌گذاری اطلاعات، این سازمان توانسته است تهدیدات سایبری را شناسایی و با آن‌ها مقابله کند. اینترنتی به‌عنوان یک شبکه جهانی، همکاری‌های بین کشورهای مختلف را در مبارزه با جرایم سایبری تسهیل می‌کند. این همکاری‌ها شامل اشتراک‌گذاری اطلاعات در مورد حملات سایبری، مجرمان و تهدیدات است. این همکاری‌ها منجر به تسریع شناسایی مجرمان و مقابله با حملات در سطح جهانی می‌شود. اینترنتی در مقابله با کلاهبرداری‌های سایبری مانند فیشینگ، سرقت هویت و کلاهبرداری‌های بانکی نقش‌برجسته‌ای ایفا کرده است [۲۵]. با استفاده از روش‌های پیشرفته و تحلیل داده‌ها، اینترنتی توانسته است بسیاری از گروه‌های سایبری را شناسایی و دستگیر کند. این سازمان به طور مرتب اقدام به برگزاری همایش‌ها، کارگاه‌ها و برنامه‌های آموزشی برای نیروهای پلیس و متخصصان سایبری می‌کند. این برنامه‌ها به افزایش آگاهی و مهارت‌های مقابله با تهدیدات سایبری در سطح جهانی کمک می‌کند. همچنین به کمک ابزارهای پیشرفته، تهدیدات سایبری را پیش‌بینی و از وقوع بسیاری از حملات سایبری جلوگیری می‌کند. این سازمان همچنین بر شناسایی آسیب‌پذیری‌ها و نقاط ضعف در سیستم‌های مختلف تمرکز دارد تا قبل از وقوع حملات، اقدامات پیشگیرانه انجام دهد.

۸-۳. دستگیری مجرمان سایبری

^۱. درخصوص تفاوت در قوانین کشورها می‌توان گفت که هر کشور چارچوب‌های قانونی و تعاریف خاص خود را از جرایم سایبری دارد. این تفاوت‌ها می‌توانند مانع ایجاد یک رویکرد یکپارچه برای همکاری بین‌المللی شوند. برخی کشورها جرایم خاصی مانند هک یا استفاده از نرم‌افزارهای مخرب را به‌عنوان جرم نمی‌شناسند یا در قوانین خود شفافیت کافی ندارند.

^۲. Haechi.

معمولاً شامل همکاری میان مقامات قضائی و پلیس‌های ملی و بین‌المللی است تا روند دستگیری و پیگرد قانونی مجرمان سریع‌تر و مؤثرتر انجام شود. همچنین، دستگیری اعضای باندهای رانسوم ویر به تقویت امنیت سایبری در سطح جهانی کمک می‌کند و پیام روشنی به سایر مجرمان ارسال می‌کند که اقدامات سایبری مجرمانه به‌هیچ‌عنوان مصون از پیگرد نخواهد بود.

۸-۳-۳. دستگیری مجرمان سرقت داده‌ها

سرقت داده‌ها که معمولاً شامل دسترسی غیرمجاز به اطلاعات حساس و محرمانه از شرکت‌ها، نهادهای دولتی، یا افراد می‌شود، یکی از جرایم پیچیده و فرامرزی است که به‌سرعت در حال گسترش است. این نوع جرایم معمولاً باهدف سرقت اطلاعات مالی، هویتی، تجاری یا حتی اطلاعات حساس دولتی انجام می‌شود. اینترنت به‌عنوان یک سازمان بین‌المللی پلیس، نقش مهمی در هماهنگی عملیات دستگیری مجرمان سرقت داده ایفا می‌کند. در این عملیات، پلیس کشورهای عضو اینترنت همکاری نزدیکی با یکدیگر دارند و اطلاعات مربوط به مجرمان سایبری را به اشتراک می‌گذارند. در بیشتر موارد، این نوع جرایم به‌صورت جهانی انجام می‌شود و مجرمان در کشورهای مختلف حضور دارند، بنابراین شناسایی و دستگیری آنها نیاز به همکاری پیچیده و چندجانبه دارد [۸۳]. عملیات دستگیری مجرمان سرقت داده معمولاً با استفاده از فناوری‌های پیشرفته و متخصصان امنیت سایبری انجام می‌شود. اینترنت با ردیابی فعالیت‌های مجرمان، شناسایی مکان‌های مخفی آنها و برقراری ارتباط با مراجع قضائی کشورهای مختلف، اقدام به دستگیری افراد مظنون می‌کند. در برخی موارد، عملیات‌ها به‌طور هم‌زمان در چندین کشور انجام می‌شود تا مجرمان سریعاً دستگیر شوند و اطلاعات به‌دست‌آمده از فعالیت‌های آنها برای جلوگیری از جرایم بیشتر مورد استفاده قرار گیرد. این اقدامات نه‌تنها به کاهش میزان جرایم سایبری و سرقت داده‌ها کمک می‌کند، بلکه پیامی قوی به مجرمان سایبری ارسال می‌کند که دستگیری آنها به‌طور جدی پیگیری می‌شود.

۸-۳-۴. شناسایی و دستگیری هکر روسی

شناسایی و دستگیری هک‌های روسی یکی از عملیات برجسته و پیچیده اینترنت است که نشان‌دهنده همکاری بین‌المللی در مبارزه با جرایم سایبری است. در بسیاری از موارد، هک‌های روسی به دلیل مهارت‌های بالا در حملات سایبری و فعالیت‌های مجرمانه فرامرزی شناخته می‌شوند. اینترنت برای مقابله با تهدیدات ناشی از چنین هک‌هایی، به‌طور مداوم با کشورهای عضو خود همکاری می‌کند و اطلاعات را به اشتراک می‌گذارد تا مجرمان سایبری را شناسایی و دستگیر کند. یک نمونه بارز از عملیات موفق اینترنت در شناسایی و دستگیری هک‌های روسی مربوط به یک پرونده بزرگ در سال‌های اخیر است که در آن یک هکر معروف روسی به نام "الکسی سیلوا" به اتهام حملات سایبری به سرورهای دولتی و

باتوجه به افزایش هک‌های اینترنتی و استفاده از اینترنت برای انجام جرایم سایبری، اینترنت تلاش‌های زیادی را برای شناسایی و دستگیری افرادی که از این فناوری‌ها برای پول‌شویی و سایر جرایم سایبری استفاده می‌کنند، انجام داده است [۸۲]. عملیات مختلف اینترنت منجر به شناسایی شبکه‌های پیچیده‌ای از مجرمان سایبری در سطح جهانی شد.

۸-۳-۱. دستگیری هک‌های کلاهبرداری آنلاین^۱

این عملیات به‌عنوان یکی از بزرگ‌ترین و موفق‌ترین تلاش‌ها برای مبارزه با جرایم سایبری در سطح جهانی شناخته می‌شود. هدف از این عملیات شناسایی و دستگیری مجرمان سایبری بود که به کلاهبرداری‌های آنلاین، سرقت هویت و دیگر جرایم سایبری مشغول بودند. این عملیات با همکاری نیروهای پلیس از ۲۴ کشور مختلف انجام شد. این کشورها شامل ایالات متحده، کانادا، کشورهای اروپایی و کشورهای آسیایی بودند. در مجموع، بیش از ۲۴۰ مظنون دستگیر شدند. این افراد به جرایم متنوعی از جمله کلاهبرداری‌های مالی، فروش اطلاعات شخصی و سرقت هویت متهم شدند. در این عملیات اینترنت از فناوری‌های نوین و ابزارهای تحلیل داده برای شناسایی و ردیابی مجرمان استفاده کرد. این ابزارها به نیروهای پلیس کمک کردند تا الگوهای رفتاری مجرمان را شناسایی کنند. در طول عملیات، اینترنت کارگاه‌هایی برای آموزش نیروهای پلیس کشورهای شرکت‌کننده برگزار کرد تا به آنها در شناسایی و مقابله با جرایم سایبری کمک کند [۸۳]. این عملیات نه‌تنها به دستگیری مجرمان کمک کرد، بلکه به افزایش آگاهی عمومی در مورد خطرات جرایم سایبری و روش‌های پیشگیری از آنها نیز انجامید. عملیات "مخفی" ۲۰۱۹ نشان‌دهنده تلاش‌های مداوم اینترنت در مبارزه با جرایم سایبری و اهمیت همکاری‌های بین‌المللی در این زمینه است. این عملیات به‌عنوان یک الگو برای سایر تلاش‌های جهانی در مبارزه با تهدیدات سایبری مورد استفاده قرار گرفته است.

۸-۳-۲. دستگیری اعضای باند رانسوم ویر

دستگیری اعضای باند رانسوم ویر توسط اینترنت، به‌عنوان یک اقدام جهانی برای مقابله با جرایم سایبری و تهدیدات آنلاین، نمونه‌ای از تلاش‌های این سازمان در مبارزه با جرم‌های پیچیده و بین‌المللی است. این باندها معمولاً به‌وسیله حملات باج‌افزار اقدام به نفوذ به سیستم‌های رایانه‌ای می‌کنند و داده‌ها را قفل کرده و از قربانیان خود برای بازگشایی آنها درخواست باج می‌کنند. اعضای این باندها معمولاً در کشورهای مختلف حضور دارند و فعالیت‌های آنها به‌صورت فرامرزی رخ می‌دهد. اینترنت با همکاری پلیس کشورهای عضو، تلاش می‌کند که مجرمان سایبری را شناسایی و دستگیر کند [۸۴]. در چنین عملیات، اطلاعات بین کشورهای عضو به اشتراک گذاشته می‌شود و با کمک فناوری‌های پیشرفته، ردیابی مجرمان شناسایی و اقدام به دستگیری آنها می‌شود. این عملیات

^۱. این عملیات، به‌عنوان عملیات مخفی ۲۰۱۹ شناسایی می‌شود.

زمینه؛ بنابراین، یافته‌های این مطالعه توصیه می‌کند که نقش اینترپل در هماهنگی واحدهای امنیتی جهانی که در زمینه جرایم سایبری مختلف تخصص دارند، برای مقابله استراتژیک و مؤثر تقویت شود. همچنین، پیشنهاد می‌شود واحدهای اجرای قانون با ارائه فناوری و آموزش‌های لازم برای تحقیقات در انواع مختلف جرایم سایبری حمایت شوند. همچنین، تقویت معاهدات بین‌المللی نظیر کنوانسیون بوداپست و تشویق کشورهای بیشتری به عضویت و هماهنگی بیشتر بین کشورهای عضو اینترپل برای استانداردسازی قوانین مربوط به جرایم سایبری و ایجاد چارچوب‌های مشترک برای اشتراک‌گذاری امن و قانونی اطلاعات مرتبط با جرایم سایبری از دیگر پیشنهادهای است. در نهایت، توصیه می‌شود آموزش‌های مستمر در زمینه جرایم سایبری برای مأموران امنیتی ارائه شود تا بتوانند با پیشرفت‌های جدید در این حوزه همگام شوند. همچنین، تأسیس یک سازمان جهانی برای مبارزه با جرایم سایبری به‌اندازه‌ای که ضرورت ایجاد می‌کند، به‌منظور تسهیل وظایف مأموران تخصصی پیشنهاد می‌شود.

منابع

1. S. H. Sheen. "A Study on the Operational and Legal Challenges of INTERPOL Red Notices and Diffusions". Master's Thesis, Dept. Law. South Korea, Seoul National University International Cooperation Major, 2024.
2. K. Shoushian, A.J. Rashidi, A. J., & A. Mirghadri. "Probabilistic modeling of fuzzy multi-stage cyber attacks". Journal of Electronic & Cyber Defense, 8(2), 61–73, 2020.
3. M. Stalcup, "Interpol and the Emergence of Global Policing. In Policing and Contemporary Governance: The Anthropology of Police in Practice", ed. William Garriott, 231–261. New York: Palgrave Macmillan.
4. L. Yanping, T. Minghai, S. Yanming (eds.). "Cybercrimes and Financial Crimes in the Global Era. Intl J Legal Discourse 2023; 8(1): 153–161, Switzerland: Springer. 342 pp. ISBN: 978-981-19-3188-8(hbk); ISBN: 978-981-19-3189-5 (eBk). <https://doi.org/10.1007/978-981-19-3189-5>, 2023
5. INTERPOL. Global Policing Goals. <https://www.interpol.int/Who-we-are/Strategy/Global-Policing-Goals>. 2017.
6. E. Lemon, Weaponizing Interpol. Journal of Democracy, 30 (2): 15–29, 2019.
7. INTERPOL Statement Delivered by Odd Reidar Humlegård, Special Representative of INTERPOL to the UN Special Meeting of the Counter-Terrorism Committee Commemorating the 20th Anniversary of the Adoption of Security Council Resolution 1373 (2001) and the Establishment of the Counter-Terrorism Committee. 4 November 2021.
8. INTERPOL. GUIDELINES FOR DIGITAL FORENSICS FIRST RESPONDERS. Best practices for search and seizure of electronic and digital evidence, 2021.
9. P. De Hert, J. Sajfert. "Police, Privacy and data protection from a comparative legal perspective". In Comparative Policing from a Legal Perspective, ed. Boer de Monica. Broadheath: Edward Elgar, 2018.
10. European Parliament -Directorate-General for External Policies. Misuse of Interpol's Red Notices and impact on human rights – recent developments [http://www.europa.europa.eu/RegData/etude/s/STUD/2019/603472/EXPO_STU\(2019\)603472_EN.pdf](http://www.europa.europa.eu/RegData/etude/s/STUD/2019/603472/EXPO_STU(2019)603472_EN.pdf). 2019

شرکت‌های بزرگ در سراسر جهان دستگیر شد. اینترپل با همکاری با نهادهای امنیتی روسیه و سایر کشورهای عضو، اطلاعات مربوط به فعالیت‌های این هکر را جمع‌آوری کرد و با استفاده از پایگاه‌های داده و ابزارهای ردیابی پیشرفته، محل مخفیگاه او را شناسایی کرد. در نهایت، این هکر در یکی از کشورهای ثالث بازداشت شد و به مراجع قضائی تحویل داده شد. دستگیری هکرهای روسی توسط اینترپل معمولاً به دلیل پیچیدگی‌های حقوقی و جغرافیایی به‌خصوص در زمینه جرایم سایبری فرامرزی نیازمند هماهنگی دقیق بین‌المللی است [۸۴]. این عملیات نشان می‌دهند که همکاری‌های بین‌المللی برای مبارزه با جرایم سایبری و حمایت از امنیت دیجیتال در سطح جهانی اهمیت حیاتی دارد.

۹. تجزیه تحلیل و نوآوری

اینترپل در سال‌های اخیر نقش مهمی در هماهنگی میان کشورهای برای مقابله با جرایم سایبری ایفا کرده است. فعالیت‌های این سازمان بیشتر بر سه محور متمرکز است: تبادل اطلاعات میان پلیس‌های ملی، آموزش و ارتقای ظرفیت فنی کشورها، و اجرای عملیات مشترک بین‌المللی. با این حال، عملکرد اینترپل با چالش‌هایی روبه‌روست؛ از جمله نبود صلاحیت الزام‌آور قضایی، وابستگی به همکاری داوطلبانه دولت‌ها، و تعارض میان امنیت سایبری و حفظ حریم خصوصی داده‌ها. همچنین، تفاوت نظام‌های حقوقی داخلی و ضعف در هماهنگی با نهادهایی مانند یورو پل و سازمان ملل، کارایی اقدامات اینترپل را محدود کرده است. از همین رو می‌توان بیان داشت که نوآوری این پژوهش در آن است که با رویکردی تحلیلی و تطبیقی، نقش حقوقی و ساختاری اینترپل در حکمرانی جهانی فضای سایبری را بررسی کرده و علاوه بر تحلیل چالش‌ها، راهکارهایی برای افزایش کارآمدی همکاری بین‌المللی ارائه داده است. از جمله این راهکارها می‌توان به ایجاد پروتکل‌های مشترک تبادل داده، تعریف صلاحیت‌های فراملی و تقویت شفافیت در سازوکارهای درون‌سازمانی اشاره کرد.

۱۰. نتیجه‌گیری

سازمان بین‌المللی پلیس جنایی (اینترپل) از طریق اجرای استراتژی مبارزه با جرایم سایبری و تکیه بر سازوکارهای مختلف برای کاهش این جرایم، سهم قابل‌توجهی در دستیابی به امنیت سایبری داشته است. این مطالعه نتیجه‌گیری می‌کند که اینترپل یکی از سازمان‌های جهانی است که کارایی خود را در مقابله با جرایم سایبری به اثبات رسانده است. علاوه بر این، این سازمان موفق شده است ترس را در میان مجرمان سایبری ایجاد کند؛ به‌طوری که نام اینترپل یکی از نام‌های ترسناک برای آن‌ها به شمار می‌رود. وظیفه اصلی اینترپل عمدتاً در هماهنگ‌سازی و همکاری با پلیس کشورهای عضو سازمان خلاصه می‌شود. جرایم مالی سایبری نیز در حوزه علاقه‌مندی این سازمان قرار دارد، به‌ویژه به دلیل استفاده از فناوری پیشرفته در این

29. T. A. Bromund. Interpol CCF's Latest Annual Report Highlights Fundamental Flaw in The System. Forbes <https://www.forbes.com/sites/tedbromund/2019/03/31/interpol-ccfs-latest-annual-report-highlights-fundamental-flaw-in-the-system/#185e9b043a11>, 2019.
30. C. Mouwer Singh, & T.B. Musikavan. "Narrative Review on Enhancing Cybersecurity in Higher Education Institutions: The Role of Continuous Training and Awareness". Expert Journal of Business and Management, Volume 12, Issue 2, pp.67-73, 2024.
31. M.C. Bassiouni. "International extradition: United States law and practice". Oxford: Oxford University Press. doi.org/10.1093/law/9780199917891.001.0001, 2014.
32. A.E. Bottoms & J. Tankebe. "Police Legitimacy and the Authority of the State. In Criminal Law and the Authority of the State, ed. Du Bois-Pedain, Antje, Magnus Ulväng, and Petter Asp". Oxford: Hart Publishing, 2017.
33. B.H. Arunga. "Countering Cybercrime in Kenya: Our Shared Responsibility". Thesis in major of law, Faculty of Arts & Social Sciences (FoA&SS / FoL / FBM), School of Law, University of Nairobi, 2021.
34. M. Anderson. "Policing the World: Interpol and the Politics of International Police Co-operation". Oxford: Clarendon Press. 7. Springer, 2015.
35. P. Andreas & E. Avram Nadelmann. "Policing the Globe Criminalization and Crime Control in International Relations". New York: Oxford University Press, 2016
36. T.B.A, Bromund. "Russia Requests Interpol Action On Bill Browder, For Seventh Time". Forbes <https://www.forbes.com/sites/tedbromund/2019/04/30/russia-requests-interpol-action-on-bill-browder-for-seventh-time/#646609d3392e>, 2019.
37. INTERPOL. "Global Cybercrime Conference", 2023
38. Z.S. Hosseini & A. Ansari Mahyari. "Controlling Cyberspace in order to protect the right to health of individuals". Quarterly Journal of Private and Criminal Law Research. 56: 71-87. [In Persian], 2023.
39. World Economic Forum. "Partnership against Cybercrime, INSIGHT REPORT NOVEMBER 2020". Shaping the Future of Cybersecurity and Digital Trust, 2020.
40. A. Wiener, F. Anthony, K.T. Lang, M. Poiars Maduro, & M. Kumm. "Global constitutionalism: Human rights, democracy and the rule of law". Global Constitutionalism, 1 (1): 1-15. <https://doi.org/10.1017/S2045381711000098>, 2012.
41. A. Tinsley. "Echoes of Kadi: Reforms to Internal Remedies at INTERPOL. EJIL: Talk!" Blog of the European Journal of International Law, <https://www.ejiltalk.org/echoes-of-kadi-reforms-to-internal-remedies-at-interpol/>, 2017.
42. J.B. Sheptycki. "Transnational Organization, Transnational Law and the Ambiguity of Interpol in a World Ruled with Law. Brill Research Perspectives in Transnational Crime, 2-3: 65-86, 2017.
43. S. Amiri. "International Cooperation of Interpol (with Emphasis on the International Convention against Drug Trafficking and Transnational Organized Crime)". Social Health and Addiction, 08: 66-80. [In Persian], 2015.
44. N. Lebed. Serhii & V. Alla, Nazarkina. "Actuality of the implementation of international practice in proliferation of counterfeit medicines involving Interpol". Journal of Advanced Pharmacy Education & Research, Published by SPER Publication, 52-59, 2020.
45. J.N. Sheptycki. "Transnational Organization, Transnational Law and the Ambiguity of Interpol in a World Ruled with Law". Brill Research Perspectives in Transnational Crime, 2-3: 65-86. DOI: 10.1163/9789004365797_005, 2017.
11. INTERPOL. "INTERPOL reviews its rules for the international exchange of criminal data". <https://www.interpol.int/News-and-Events/News/2019/INTERPOL-reviews-its-rules-for-the-international-exchange-of-criminal-data>. 2019
12. INTERPOL. "Key Dates. <https://www.interpol.int/Who-we-are/Our-history/Key-dates>." 2020
13. INTERPOL. "GUIDE FOR CRIMINAL JUSTICE STATISTICS ON CYBERCRIME AND ELECTRONIC EVIDENCE". Global Action on Cybercrime Extended (GLACY+) Joint project of the European Union and the Council of Europe. 2020
14. INTERPOL. What is INTERPOL? <https://www.interpol.int/Who-we-are/What-is-INTERPOL>. 2020
15. INTERPOL. "General Secretariat". <https://www.interpol.int/Who-we-are/General-Secretariat>. 2020
16. INTERPOL. "International Notices system". https://www.interpol.int/content/download/625/file/GI-02_2018-03_EN_LR.pdf. 2020
17. K. A, Sheptycki. "Brand Interpol. In Trust in International Police and Justice Cooperation, ed". Saskia Hufnagel and Carole McCartney. Oxford: Hart Publishing, 2017.
18. S. L. Sheehan. "Interpol: An International Perspective on Police Training and Development". In Police Organization and Training: Innovations in Research and Practice, ed. Maria R. Haberland, Curtis A. Clarke, and Dale L. Sheehan, 169-178. New York: Springer. DOI:10.1007/978-1-4614-0745-4_11, 2012
19. INTERPOL. "About Notices". <https://www.interpol.int/How-we-work/Notices/About-Notices>. 2020
20. M. Joutsen. "International Instruments on Cooperation in Responding to Transnational Crime". In The Handbook of Transnational Crime and Justice, ed. Philip Reichel and Jay Albanese, 255-274. Thousand Oaks: Sage, 2014
21. J. Klabbers, A. Peters, and G. Ulfstein. "The constitutionalization of international law". Oxford: Oxford University Press, 2011.
22. W. C, Ling. "Policing Interpol: The Commission for the Control of Interpol's Files and the Right to a Remedy". International Organizations Law Review, 7 (2): 375-404. DOI: 10.1163/157237410X543314, 2010.
23. Combating Wildlife Crime, Linked to the Internet, Global Trends and China's Experiences, 2019.
24. A. Ansari Mahyari, Z.S. Hosseini, A. Radman. "Examining the Position of Deep Web and Dark Web in International Law". Quarterly Journal of Legal Studies in Cyberspace, 02(03): 41-53. [In Persian], 2024.
25. J. Antczak. "The impact of the covid-19 pandemic on business entity cyber security". Inżynieria Bezpieczeństwa Obiektów Antropogenicznych, 1 (2022) 7-15 <https://inzynierabezpieczenstwa.com.pl>. DOI:10.37105/iboa.128, 2022.
26. A. Ansari Mahyari, Z.S. Hosseini, A. Radman. "Examining the Position of Deep Web and Dark Web in International Law". Quarterly Journal of Legal Studies in Cyberspace, 02(03): 41-53. [In Persian], 2024.
27. N. Langille, F. Mégret. "Red Notices and transnational police practices". In International Practices of Criminal Justice, ed. Mikkel Jarle Christensen and Ron Levi, 108-130. New York: Routledge. DOI:10.4324/9781315144788, 2018.
28. N. Boister. "An Introduction to Transnational Criminal Law". Oxford: Oxford University Press. doi.: 10.1093/law/9780198795995.001.0001, 2018.

- Focusing on the Law Enforcement Practices of the Korean National Police". Graduate School of International Studies Seoul National University, Submitting a master's thesis of International Studies, International Cooperation Major, 2024.
67. O. Schlossberger. "Economic and Legal Aspects of Electronic Money". ACTA VŠFS, 1/2016, vol. 10, 47-65, 2016.
 68. M. Deflem. "Interpol. In The Encyclopedia of Crime and Punishment, ed". Wesley G. Jennings, 788–791. London: Wiley-Blackwell, 2016.
 69. H. Javadi Niakani, M.R. Hosseini, H. Shirzad, B. Aminian. "Management model for utilizing the capacities of Interpol in the fight against crimes and criminals". NAJA Strategic Studies, 05(17): 61-86. [In Persian], 2021.
 70. S. Ugelvik. "Police Cooperation and Sovereignty in the EU: Norway's Lessons for Europe". London, New York: Routledge Press, 2019.
 71. J. Abbott, D. Sheehan. "The INTERPOL Approach to Tackling Match Fixing in Football. In Match-fixing in international sports: Existing processes, law enforcement, and prevention strategies", Haberfeld, Maria R., and Dale Sheehan, 263–28, 2013.
 72. G. Calcaral. "Balancing International Police Cooperation: INTERPOL and the Undesirable Trade-off Between Right of Individuals and Global Security". Liverpool Law Review, 42:111–142. <https://doi.org/10.1007/s10991-020-09266-9>, 2021.
 73. M. Rangriz. Interpol and its role in combating international organized crimes with the approach of combating drug trafficking. Semnan Police Science, 17: 130-140. [In Persian], 2015
 74. J. Tully, L. Jeffrey, A. Dunoff, F. Lang, K. Mattias & A. Wiener. "Introducing global integral constitutionalism". Global Constitutionalism, 5 (1): 1–15. DOI: 10.1017/S2045381715000210, 2016.
 75. Z. Khajeh Sani. "The Role of Interpol in combating human rights challenges". Master's thesis, Shiraz University [In Persian], 2018.
 76. H. Zanganeh Abadi. "Examining the role of Interpol police in establishing international order". Master's thesis, Payam Noor University of Bushehr Province. [In Persian], 2021.
 77. M. Rangriz. "Interpol and its role in combating international organized crimes with the approach of combating drug trafficking". Semnan Police Science, 17: 130-140. [In Persian], 2015.
 78. H. Kaur, et al. "Interpreting interpretability: Understanding data scientists' use of interpretability tools for machine learning". Paper. P1-14, 2020.
 79. S. Naeem, A. Ali, S. Anam, M. Ahmed. "An Unsupervised Machine Learning Algorithms: Comprehensive Review". International Journal of Computing and Digital Systems, 13(1):911-921. DOI:10.12785/ijcds/130172, 2023.
 80. P. Reddy, V. Pulabaigari, E. Reddy B. "Semi-supervised learning: a brief review", International Journal of Engineering & Technology, 7(18):81. DOI:10.14419/ijet.v7i1.8.9977, 2018
 81. N. Muddasar, S.T H. Rizvi, A. Coronato. "A Gentle Introduction to Reinforcement Learning and its Application in Different Fields". January 2020 IEEE Access 8:209320-209344. DOI:10.1109/ACCESS.2020.3038605, 2020.
 82. S. Seong-Ho. "A Study on the Operational and Legal Challenges of INTERPOL Red Notices and Diffusions". Submitting a master's thesis of International Studies February 2024 Graduate School of International Studies Seoul National University International Cooperation Major, 2024.
 83. INTERPOL, Global Cybercrime Conference, 2023
 46. INTERPOL. Databases, <https://www.interpol.int/How-we-work/Databases>, 2020.
 47. A. Hedider, Amina. "Effective measures to address cybercrime in all its forms, The Hague International Model United Nations Qatar". General Assembly, 6, 01-11, 2019.
 48. THE INTERNATIONAL CRIMINAL POLICE ORGANIZATION: "Policing Online Spaces. COLLEGE OF THE CANYONS MODEL UNITED NATIONS CONFERENCE". General Assembly Background Guide, 2022.
 49. A. Hedider. "Effective Measures to Address Cybercrime in all its forms", The Hague International Model United Nations Qatar. General Assembly 6, 01-11, 2019.
 50. D. Agung. "The Role of Interpol in the Settlement of Cybercrime Cases under the Budapest Convention on Cybercrimes". International Journal of Global Community, 05, No.1, 49-56, 2022.
 51. A. Cassese. "Cassese's international criminal law". Oxford: Oxford University Press, 2019
 52. Cybercrime and Cybersecurity practices in the Middle East Construction Industry – January, 2024
 53. G.A. Calcara. "Rethinking Legal Research on Matters of International Police Cooperation: Issues, Methods and Raison d'Être". Liverpool Law Review 40 (2): 95–111, 2019.
 54. Fair Trials. Strengthening respect for human rights, strengthening INTERPOL www.fairtrials.org/wp-content/uploads/Strengthening-respect-for-human-rights-strengthening-INTERPOL4.pdf, 2013.
 55. G. Calcara. "Role of INTERPOL and Europol in the Fight against Cybercrime, with Particular Reference to the Sexual Exploitation of Children Online and Child Pornography". Masaryk University Journal of Law and Technology, 7: 19–33, 2013.
 56. Fair Trials. INTERPOL. <https://fairtrials.org/campaign/interpol>, 2020.
 57. Fair Trials. Dismantling the tools of oppression Ending the misuse of INTERPOL <https://fairtrials.org/publication/dismantling-tools-of-oppression-1>, 2018.
 58. D. Higgins & W. Rob. "Collaboration at the Front Line: INTERPOL and NGOs in the Same NEST". In Environmental crime and collaborative state intervention, ed. Rob White and Grant Pink, 101–116. New York: Palgrave Macmillan, 2016.
 59. T.M.Sadeghi, L.Raisi, A. Ansari Mahyari. "The Function of Regional Organizations in Cyberwarfare". Quarterly Journal of New Achievements in Public Law, 03(09): 74-90. [In Persian], 2024.
 60. G. Calcara. "Preventing the Misuse of INTERPOL: A Study on the Legal Safeguards of the Organization". Nordic Journal of International Law, 87 (1): 56–78. DOI:10.1163/15718107-08701001, 2018.
 61. M. Deflem. "Policing World Society: Historical Foundations of International Police Cooperation". New York: Oxford University Press, 2022.
 62. G.B. Calcara, "INTERPOL's Rules on the Processing of Data". Oxford International Organizations (OXIO) 441, 2019.
 63. I. Hurd, Ian. "International Organizations: Politics, Law, Practice". Cambridge: Cambridge University Press, 2018.
 64. G. Calcara. "A transnational police network co-operating up to the limits of the law: examination of the origin of INTERPOL". Transnational Legal Theory, 1–28. doi.org/10.1080/20414005.2020.1793282, 2020.
 65. Unicef. "DISRUPTING HARM IN TANZANIA". Evidence on online child sexual exploitation and abuse, 2022.
 66. L.Yunjeong. "A Study on the Operational and Legal Challenges of INTERPOL Red Notices and Diffusions:

Press. doi.org/10.1017/CBO9780511494451, 2016

84. K. Wellens. Remedies Against International Organisations. New York: Cambridge University