مجله علمی مطالعات پژوهشی
در حقوق آینده
www.journalhi.com/law/

تحلیل تطبیقی نقش دولت ایران و انگلستان در طراحی الگوهای پیشگیرانه جرایم سایبری نوظهور با تأکید بر سازوکارهای حقوقی و نهادی

نیوشا قهرمانی افشار[۱،*]، محمد یوسف کریمی [۲]، راشین ضیا [۳]

۱- هیئت علمی ، استاد یار حقوق کیفری و جرم شناسی، دانشگاه ازاد اسلامی ، واحد ارومیه. ایمیل: 2753764816@iau.ir
۲- دانشجوی دکتری، گروه حقوق کیفری و جرم شناسی، واحد تبریز، دانشگاه آزاد اسلامی، تبریز، ایران. ایمیل: mohammad.karimi@iau.ir
۳- دانشجوی دکتری، گروه حقوق کیفری و جرم شناسی، واحد تبریز، دانشگاه آزاد اسلامی، تبریز، ایران. ایمیل: rashin.ziya@iau.ir
* نویسنده مسئول

چکیده

جرایم سایبری نوظهور در سال‌های اخیر به یکی از مهم‌ترین چالش‌های نظام‌های حقوقی در سراسر جهان تبدیل شده‌اند. این جرایم که شامل حملات پیچیده سایبری، نفوذ به داده‌های حیاتی، سرقت هویت دیجیتال و سوءاستفاده از زیرساخت‌های اطلاعاتی هستند، نیازمند الگوهای پیشگیرانه‌ای فراتر از روش‌های سنتی مقابله با جرم‌اند. دولت‌ها در این میان نقشی کلیدی در طراحی و اجرای سیاست‌های پیشگیرانه ایفا می‌کنند. پژوهش حاضر با رویکرد تطبیقی به بررسی نقش دولت ایران و انگلستان در طراحی الگوهای پیشگیرانه جرایم سایبری نوظهور می‌پردازد و بر سازوکارهای حقوقی و نهادی دو کشور متمرکز است. داده‌های پژوهش بر پایه منابع علمی معتبر، قوانین ملی، گزارش‌های رسمی و یافته‌های پژوهشی بین‌المللی گردآوری شده و از روش توصیفی–تحلیلی و مقایسه‌ای بهره گرفته است. نتایج نشان می‌دهد که انگلستان با تکیه بر نهادهای تخصصی همچون مرکز امنیت سایبری ملی و سیاست‌های هماهنگ اتحادیه اروپا، چارچوبی منسجم‌تر برای پیشگیری از جرایم سایبری ایجاد کرده است. در مقابل، ایران اگرچه قوانین متعددی در حوزه جرایم رایانه‌ای تصویب کرده، اما همچنان با چالش‌هایی در زمینه هماهنگی نهادی، روزآمدسازی قوانین و توسعه ظرفیت‌های پیشگیرانه مواجه است. تحلیل تطبیقی نشان می‌دهد که بهره‌گیری از الگوهای موفق انگلستان، به‌ویژه در زمینه همکاری بین‌نهادی، آموزش عمومی و تنظیم‌گری شفاف، می‌تواند به بهبود رویکردهای پیشگیرانه در نظام حقوقی ایران کمک کند.

کلمات کلیدی: جرایم سایبری نوظهور، پیشگیری از جرم، مسئولیت دولت، ایران، انگلستان.

Comparative Analysis of the Role of Iranian and English Governments in Designing Preventive Models for Emerging Cybercrimes with Emphasis on Legal and Institutional Mechanisms

Nyusha Ghahraman Afshar [1,*], Mohammad Yousef Karimi [2], Rashin Zia [3]

1- Faculty, Assistant Professor of Criminal Law and Criminology, Islamic Azad University, Urmia Branch. Email: 2753764816@@iau.ir
2- PhD Student, Department of Criminal Law and Criminology, Tabriz Branch, Islamic Azad University, Tabriz, Iran. Email: mohammad.karimi@iau.ir
3- PhD Student, Department of Criminal Law and Criminology, Tabriz Branch, Islamic Azad University, Tabriz, Iran. Email: rashin.ziya@iau.ir
* Corresponding Author

Abstract

Emerging cybercrimes have become one of the most pressing challenges for legal systems worldwide. These crimes, including complex cyberattacks, data breaches, identity theft, and the misuse of critical infrastructures, require preventive models that go beyond traditional crime control approaches. Governments play a pivotal role in designing and implementing preventive strategies. This study adopts a comparative approach to examine the role of Iran and the United Kingdom in shaping preventive frameworks against emerging cybercrimes, with a focus on legal and institutional mechanisms. The research relies on scholarly articles, national legislations, official reports, and international studies, using descriptive-analytical and comparative methods. Findings indicate that the United Kingdom, through specialized bodies such as the National Cyber Security Centre and the coordinated policies of the European Union, has established a more coherent framework for cybercrime prevention. By contrast, although Iran has enacted several laws on computer crimes, it still faces challenges related to institutional coordination, legal modernization, and preventive capacity building. The comparative analysis highlights that adopting successful practices from the UK—particularly in inter-institutional cooperation, public awareness programs, and transparent regulation—can strengthen Iran's preventive legal framework against emerging cybercrimes.

Keywords: Emerging cybercrimes, crime prevention, state responsibility, Iran, United Kingdom.

مقدمه

جرایم سایبری نوظهور در دهه اخیر به یکی از مهم‌ترین دغدغه‌های نظام‌های حقوقی و دولت‌ها تبدیل شده‌اند. پیچیدگی این جرایم، ماهیت فرامرزی و سرعت بالای تحول فناوری موجب شده است که ابزارهای سنتی مقابله با بزهکاری نتوانند پاسخگوی تهدیدهای جدید باشند. دولت‌ها در این میان نقشی محوری بر عهده دارند؛ چرا که آن‌ها علاوه بر مسئولیت‌های کلاسیک کیفری، باید با طراحی سیاست‌های پیشگیرانه چندسطحی از وقوع این جرایم جلوگیری کنند[۱].

همه‌گیری کووید–۱۹ نمونه روشنی از تغییر الگوهای تهدید در فضای مجازی است. افزایش وابستگی افراد و سازمان‌ها به بسترهای دیجیتال باعث شد فرصت‌های تازه‌ای برای حملات فیشینگ، نفوذ به داده‌های حساس و سرقت هویت الکترونیک فراهم شود. مطالعات نشان می‌دهد که در همین دوره، حملات سایبری علیه زیرساخت‌های بهداشتی و آموزشی چندین برابر رشد داشت و این امر ضرورت سیاست‌های پیشگیرانه پیش‌دستانه را برجسته ساخت[۲].

در ادبیات جرم‌شناسی، رویکرد «پیشگیری موقعیتی» به‌عنوان چارچوبی کارآمد شناخته می‌شود. این رویکرد بر کاهش فرصت‌های ارتکاب جرم از طریق افزایش هزینه‌ها و ریسک‌های بزهکار و کاهش منافع او تمرکز دارد. انطباق این منطق با فضای سایبری، نیازمند پیوند میان تکنیک‌های پیشگیری موقعیتی و استانداردهای امنیت اطلاعات است. پژوهش‌های اخیر نشان داده‌اند که استفاده از مدل‌های تلفیقی میان تکنیک‌های پیشگیری موقعیتی و کنترل‌های امنیتی می‌تواند مبنای کارآمدی برای سیاست‌گذاری پیشگیرانه دولت‌ها در حوزه فضای مجازی باشد[۳].

با وجود این پیشرفت‌ها، تجربه عملی کشورها نشان می‌دهد که اثربخشی مداخلات پیشگیرانه به عوامل متعددی وابسته است. در انگلستان، کمپین‌های عمومی آموزش امنیت سایبری برای کسب‌وکارها زمانی توانسته‌اند موفق باشند که طراحی آن‌ها مبتنی بر داده‌های واقعی و مدل‌های رفتاری بوده است. نتایج نشان می‌دهد همه مداخلات یکسان عمل نمی‌کنند و تنها برنامه‌هایی که با نیازها و انگیزه‌های اقتصادی کاربران هماهنگ هستند می‌توانند کاهش بزه‌دیدگی را تضمین کنند[۴].

در ایران نیز، هرچند قوانین متعددی در زمینه جرایم رایانه‌ای به تصویب رسیده است، اما چالش‌های مربوط به هماهنگی نهادی، روزآمدسازی مقررات و ارتقای ظرفیت‌های پیشگیرانه همچنان وجود دارد. بررسی وضعیت حقوقی و نهادی ایران در مقایسه با انگلستان فرصتی فراهم می‌آورد تا شکاف‌ها و فرصت‌های سیاستی شناسایی شود و مسیر اصلاح چارچوب‌های پیشگیرانه مشخص گردد[۵].

یکی از عوامل اصلی ضرورت توجه به پیشگیری در جرایم سایبری، ماهیت فراملی این جرایم است. برخلاف بسیاری از جرایم سنتی که در قلمرو یک کشور اتفاق می‌افتند، جرایم سایبری به‌سادگی می‌توانند مرزها را پشت سر بگذارند. یک حمله سایبری که از یک نقطه در آسیا آغاز می‌شود، ممکن است در اروپا یا خاورمیانه خسارت‌های جدی به بار آورد. همین ویژگی سبب شده است که همکاری‌های بین‌المللی و مشارکت دولت‌ها در سطح فراملی به‌عنوان یکی از ستون‌های اصلی سیاست‌های پیشگیرانه مورد تأکید قرار گیرد[۶].

در این زمینه، انگلستان با بهره‌گیری از ساختارهای نهادی پیشرفته نظیر مرکز ملی امنیت سایبری توانسته است برنامه‌های پیشگیرانه‌ای طراحی کند که علاوه بر جنبه‌های فنی، ابعاد آموزشی و اجتماعی را نیز پوشش می‌دهد. این کشور با تدوین راهبردهای جامع امنیت سایبری، هم شهروندان عادی و هم کسب‌وکارها را هدف قرار داده و از ابزارهای متنوعی برای افزایش آگاهی عمومی، شفاف‌سازی تهدیدات و تشویق بخش خصوصی به سرمایه‌گذاری در امنیت سایبری استفاده کرده است[۷].

در مقابل، ایران هرچند دارای قوانین کیفری ویژه در حوزه جرایم رایانه‌ای است و نهادهایی مانند شورای عالی فضای مجازی و پلیس فتا نقش‌آفرینی می‌کنند، اما هنوز با مشکل هم‌پوشانی وظایف و پراکندگی نهادی مواجه است. این موضوع می‌تواند موجب اتلاف منابع، کندی واکنش و دشواری در تدوین سیاست‌های منسجم پیشگیرانه شود. از سوی دیگر، بخشی از سیاست‌ها در ایران بیشتر بر کنترل و محدودسازی متمرکز است تا ارتقای توانمندی‌های اجتماعی و آموزشی کاربران، که همین امر شکاف میان ایران و انگلستان را در زمینه پیشگیری آشکارتر می‌سازد[۸].

افزون بر این، تفاوت در بسترهای قانونی نیز اهمیت دارد. در انگلستان، سیاست‌های پیشگیری سایبری بر پایه قوانین روزآمد و هماهنگ با اتحادیه اروپا شکل گرفته‌اند؛ قوانینی که به‌طور مداوم بازبینی می‌شوند تا با سرعت تغییر فناوری همگام باشند. در ایران اما فرآیند به‌روزرسانی قوانین کندتر بوده و همین مسئله باعث می‌شود برخی جرایم نوظهور بدون پاسخ صریح قانونی باقی بمانند یا نیازمند تفسیرهای گسترده قضایی شوند[۹].

این تفاوت‌ها نشان می‌دهد که مطالعه تطبیقی بین ایران و انگلستان می‌تواند علاوه بر روشن ساختن نقاط قوت و ضعف هر کشور، زمینه‌ای برای ارائه الگوهای بهینه سیاست‌گذاری در حوزه پیشگیری از جرایم سایبری نوظهور فراهم آورد. چنین الگویی می‌تواند با ترکیب سازوکارهای حقوقی، نهادی و اجتماعی، راهکارهایی عملی برای تقویت کارآمدی سیاست‌های پیشگیرانه ارائه دهد[۱۰].

پیشگیری از جرایم سایبری صرفاً جنبه حقوقی یا فنی ندارد، بلکه نیازمند نگاه میان‌رشته‌ای است. ترکیب جرم‌شناسی، حقوق کیفری، علوم رایانه، جامعه‌شناسی و حتی اقتصاد رفتاری می‌تواند چارچوبی جامع برای مقابله با تهدیدات نوظهور فراهم آورد. پژوهش‌های بین‌المللی نشان داده‌اند که تنها با اتکا به فناوری نمی‌توان از وقوع جرایم جلوگیری کرد؛ چرا که ضعف آگاهی عمومی، نبود مهارت‌های پایه دیجیتال و غفلت از آموزش‌های مستمر می‌تواند حتی بهترین سامانه‌های امنیتی را ناکارآمد سازد[۱۱].

در انگلستان، سیاست‌های پیشگیرانه مبتنی بر مشارکت عمومی–خصوصی اهمیت ویژه‌ای یافته است. دولت با ایجاد سازوکارهای همکاری با شرکت‌های بزرگ فناوری و مؤسسات مالی، توانسته است سامانه‌های هشدار سریع، تبادل اطلاعات تهدید و پروژه‌های مشترک امنیت سایبری را توسعه دهد. این همکاری‌ها نشان داده‌اند که پیشگیری مؤثر بدون مشارکت فعال بخش خصوصی امکان‌پذیر نیست[۱۲].

در ایران نیز نشانه‌هایی از چنین همکاری‌هایی به چشم می‌خورد، به‌ویژه در حوزه بانکداری الکترونیک که الزام به رعایت استانداردهای امنیتی از سوی بانک مرکزی و همکاری با شرکت‌های خصوصی ارائه‌دهنده خدمات امنیتی در حال گسترش است. با این حال، این همکاری‌ها هنوز به مرحله نهادینه‌شدن و شفافیت کامل نرسیده‌اند و در بسیاری موارد، نبود قوانین جامع و سیاست‌های هماهنگ، مانع شکل‌گیری مشارکت مؤثر میان دولت و بخش خصوصی می‌شود[۱۳].

از سوی دیگر، آموزش و فرهنگ‌سازی بخش مهمی از سیاست‌های پیشگیرانه است. در انگلستان، کمپین‌های گسترده‌ای برای ارتقای سواد دیجیتال شهروندان طراحی شده است که از مدارس تا محیط‌های کاری را

پوشش می‌دهد. این کمپین‌ها با زبان ساده، تهدیدات رایج مانند فیشینگ، بدافزار و سرقت هویت را توضیح می‌دهند و راهکارهای عملی برای مقابله ارائه می‌کنند. تجربه این کشور نشان می‌دهد که افزایش سطح دانش عمومی می‌تواند نرخ بزه‌دیدگی سایبری را کاهش دهد[۱۴].

در مقابل، در ایران برنامه‌های آموزشی موجود بیشتر بر قشر خاصی از کاربران (مانند دانشجویان یا کارکنان دولتی) متمرکز است و پوشش جامع برای عموم جامعه ندارد. همچنین محتوای آموزشی در بسیاری موارد به‌روز نیست و با سرعت تغییر تهدیدات سایبری همگام نمی‌شود. این مسئله ضرورت بازنگری در سیاست‌های آموزشی و بهره‌گیری از تجربه انگلستان را برجسته می‌سازد[۱۵].

یکی از محورهای کلیدی در سیاست‌های پیشگیرانه، تقویت ظرفیت نهادی دولت‌ها است. بدون وجود نهادهای کارآمد، حتی بهترین قوانین و راهبردها نیز در عمل بی‌اثر خواهند بود. تجربه انگلستان نشان می‌دهد که نهادهایی مانند مرکز ملی امنیت سایبری و پلیس تخصصی جرایم سایبری با اختیارات مشخص و بودجه مستقل توانسته‌اند هماهنگی مؤثری میان بخش‌های مختلف ایجاد کنند [۱۶]. این نهادها علاوه بر انجام مأموریت‌های فنی و اجرایی، نقش مهمی در پایش روندهای جهانی و ارائه گزارش‌های سیاستی برای دولت دارند.

در ایران نیز نهادهایی همچون پلیس فتا، دادسرای ویژه جرایم رایانه‌ای و شورای عالی فضای مجازی مسئولیت‌های متعددی بر عهده دارند. با این حال، پراکندگی وظایف، هم‌پوشانی نهادی و نبود تقسیم‌کار شفاف از جمله چالش‌هایی است که می‌تواند اثربخشی این ساختارها را کاهش دهد [۱۷]. برخی مطالعات داخلی نشان داده‌اند که نبود هماهنگی میان نهادهای مختلف در زمینه مقابله با حملات سایبری، زمان واکنش را افزایش داده و احتمال بزه‌دیدگی گسترده‌تر را بالا می‌برد[۱۸].

موضوع دیگر، به‌روزرسانی قوانین است. جرایم سایبری با سرعتی بسیار بیشتر از روند قانون‌گذاری توسعه می‌یابند. در انگلستان، قوانین مرتبط با جرایم رایانه‌ای و امنیت سایبری به‌طور مداوم اصلاح و به‌روزرسانی می‌شوند تا پاسخگوی تهدیدات جدید باشند. علاوه بر این، همکاری نزدیک این کشور با نهادهای اروپایی موجب شده است چارچوب‌های قانونی آن با استانداردهای بین‌المللی هم‌راستا باشد[۱۹].

در مقابل، در ایران بخش‌هایی از قوانین موجود همچنان بر مبنای شرایط یک دهه پیش تدوین شده‌اند. هرچند اصلاحات محدودی صورت گرفته، اما بسیاری از جرایم نوظهور نظیر حملات مبتنی بر هوش مصنوعی یا سوءاستفاده از فناوری زنجیره بلوکی هنوز فاقد چارچوب قانونی دقیق و صریح هستند [۲۰]. این شکاف قانونی، هم دستگاه قضایی را در رسیدگی به پرونده‌ها با دشواری مواجه می‌سازد و هم مانعی برای طراحی الگوهای پیشگیرانه جامع به شمار می‌رود.

در نتیجه، مطالعه تطبیقی ایران و انگلستان در این حوزه می‌تواند نشان دهد که چگونه ترکیب به‌هنگام‌سازی قوانین، تقویت نهادهای تخصصی و افزایش هماهنگی بین‌بخشی می‌تواند منجر به ارتقای سطح پیشگیری در برابر جرایم سایبری نوظهور شود.

ابعاد اقتصادی جرایم سایبری نیز از دیگر عواملی است که دولت‌ها را به سمت اتخاذ سیاست‌های پیشگیرانه سوق داده است. خسارت‌های ناشی از این جرایم تنها محدود به زیان مستقیم قربانیان نیست، بلکه پیامدهای گسترده‌ای همچون کاهش اعتماد عمومی به خدمات آنلاین، اختلال در بازارهای مالی و تهدید سرمایه‌گذاری خارجی را نیز در بر دارد [۲۱]. بر اساس برآوردهای اخیر، هزینه‌های جهانی جرایم سایبری در سال‌های اخیر به‌طور چشمگیری افزایش یافته و همین موضوع سبب شده است که بسیاری از دولت‌ها، از جمله انگلستان، پیشگیری را به‌عنوان یک اولویت اقتصادی در نظر بگیرند[۲۲].

در انگلستان، راهبردهای ملی امنیت سایبری به‌طور مشخص بر کاهش خسارت‌های اقتصادی تمرکز کرده‌اند. دولت با همکاری بخش خصوصی اقدام به تدوین استانداردها و دستورالعمل‌هایی کرده است که رعایت آن‌ها توسط کسب‌وکارها الزامی است. این سیاست‌ها نه‌تنها هزینه‌های مستقیم جرایم سایبری را کاهش می‌دهد، بلکه با ایجاد محیطی امن‌تر برای فعالیت‌های دیجیتال، موجب تقویت اقتصاد دیجیتال کشور نیز می‌شود[۲۳].

در ایران، با وجود رشد سریع خدمات مالی و تجاری آنلاین، خسارت‌های ناشی از حملات سایبری در بسیاری موارد به‌طور دقیق برآورد نمی‌شوند و همین مسئله باعث می‌شود اهمیت اقتصادی این جرایم کمتر از واقعیت در سیاست‌گذاری‌ها انعکاس یابد. نبود نظام شفاف گزارش‌دهی خسارت‌ها و همچنین تمایل برخی شرکت‌ها به پنهان‌سازی رخدادها برای حفظ اعتبار تجاری، موجب شده است داده‌های قابل‌اعتماد در این حوزه محدود باشد [۲۴]. این وضعیت نه‌تنها تحلیل‌های علمی را دشوار می‌سازد، بلکه مانعی جدی برای طراحی سیاست‌های پیشگیرانه مؤثر به شمار می‌رود.

افزون بر مسائل اقتصادی، بعد اجتماعی جرایم سایبری نیز باید مورد توجه قرار گیرد. افزایش بزه‌دیدگی شهروندان عادی، از کلاهبرداری‌های اینترنتی گرفته تا تعرض به حریم خصوصی، پیامدهایی نظیر کاهش اعتماد به فناوری و ایجاد احساس ناامنی در فضای عمومی را در پی دارد. در انگلستان، سیاست‌گذاران تلاش کرده‌اند با تمرکز بر آموزش عمومی، ایجاد سامانه‌های گزارش‌دهی آسان و حمایت از بزه‌دیدگان، این آثار اجتماعی را کاهش دهند [۲۵]. در ایران نیز نیاز به چنین رویکردی بیش از پیش احساس می‌شود، چرا که رشد سریع استفاده از اینترنت در میان اقشار مختلف جامعه بدون آموزش‌های لازم، آسیب‌پذیری اجتماعی را افزایش داده است[۲۶].

یکی دیگر از چالش‌های اساسی در حوزه پیشگیری از جرایم سایبری، مسئله اعتماد عمومی به سیاست‌های دولت است. تجربه نشان داده است که حتی بهترین قوانین و سازوکارهای فنی نیز در صورتی کارآمد خواهند بود که شهروندان به نهادهای مسئول اعتماد داشته باشند و در فرآیندهای پیشگیرانه مشارکت فعال نشان دهند [۲۷]. در انگلستان، ایجاد شفافیت در گزارش‌دهی، انتشار مستمر آمار جرایم سایبری و پاسخ‌گویی نهادی باعث افزایش اعتماد عمومی شده و شهروندان را به همکاری در شناسایی تهدیدها ترغیب کرده است[۲۸].

در ایران اما، بخشی از چالش‌ها به نبود شفافیت در اطلاع‌رسانی مربوط می‌شود. بسیاری از رخدادهای سایبری یا به‌طور رسمی اعلام نمی‌شوند یا جزئیات آن‌ها در دسترس عموم قرار نمی‌گیرد. این وضعیت موجب می‌شود که شهروندان احساس نکنند در سیاست‌های پیشگیرانه سهیم هستند و در نتیجه، انگیزه مشارکت آنان کاهش می‌یابد [۲۹]. این در حالی است که افزایش اعتماد اجتماعی می‌تواند به تقویت کارآمدی کل نظام پیشگیری کمک کند.

به‌طور کلی، مرور ادبیات و تجربه دو کشور نشان می‌دهد که پیشگیری از جرایم سایبری نیازمند ترکیب چند بعد کلیدی است:

- چارچوب‌های قانونی روزآمد و هماهنگ با تحولات فناوری
- نهادهای تخصصی کارآمد و هماهنگ
- مشارکت فعال بخش خصوصی و جامعه مدنی

- آموزش و فرهنگ‌سازی مستمر و گسترده
- شفافیت نهادی و جلب اعتماد عمومی

این مؤلفه‌ها در انگلستان تا حد زیادی نهادینه شده‌اند، در حالی‌که در ایران برخی از آن‌ها همچنان نیازمند توسعه و تقویت جدی هستند. بنابراین، پژوهش حاضر با هدف تحلیل تطبیقی نقش دولت ایران و انگلستان در طراحی الگوهای پیشگیرانه جرایم سایبری نوظهور تلاش می‌کند تصویری روشن از وضعیت موجود ارائه دهد و راهکارهایی برای بهبود سیاست‌های پیشگیرانه در ایران پیشنهاد کند.

بیان مساله

تحولات شتابان فناوری اطلاعات و ارتباطات موجب پیدایش گونه‌های جدیدی از جرایم سایبری شده است که بسیاری از آن‌ها در چارچوب قوانین سنتی قابل شناسایی یا تعقیب نیستند. این وضعیت، دولت‌ها را با پرسشی اساسی مواجه کرده است: چگونه می‌توان با طراحی سیاست‌های پیشگیرانه، از بزه‌دیدگی گسترده در فضای مجازی جلوگیری کرد؟

در انگلستان، با تکیه بر نهادهای تخصصی و قوانین روزآمد، تلاش شده است تا چارچوبی هماهنگ برای پیشگیری از جرایم سایبری ایجاد شود. در ایران نیز با وجود تصویب قوانین و تشکیل نهادهای مختلف، همچنان مشکلاتی مانند پراکندگی وظایف نهادی، کندی در به‌روزرسانی قوانین و ضعف آموزش عمومی وجود دارد[۳۰].

مسئله اصلی این پژوهش آن است که چه تفاوت‌هایی میان رویکرد ایران و انگلستان در زمینه طراحی الگوهای پیشگیرانه وجود دارد و چگونه می‌توان از تجربه موفق انگلستان برای بهبود چارچوب‌های پیشگیرانه ایران بهره گرفت. پاسخ به این پرسش از دو جهت اهمیت دارد: نخست، به دلیل افزایش مستمر تهدیدات سایبری که امنیت ملی و اقتصادی کشورها را هدف قرار می‌دهند؛ دوم، به سبب نیاز به تقویت هماهنگی میان نهادهای مختلف و افزایش کارآمدی نظام حقوقی و نهادی در ایران[۳۱].

ازاین‌رو، این پژوهش در پی آن است که با بررسی تطبیقی سازوکارهای حقوقی و نهادی ایران و انگلستان، نقاط قوت و ضعف هر یک را شناسایی کرده و زمینه را برای ارائه الگوهای پیشگیرانه عملی و کارآمد فراهم آورد.

روش تحقیق

این پژوهش از نظر ماهیت، کاربردی و از نظر روش، توصیفی–تحلیلی و تطبیقی است. هدف اصلی، بررسی و مقایسه نقش دولت ایران و انگلستان در طراحی الگوهای پیشگیرانه جرایم سایبری نوظهور با تأکید بر سازوکارهای حقوقی و نهادی است. برای دستیابی به این هدف، از ترکیبی از داده‌های اسنادی، قوانین، گزارش‌های رسمی و مطالعات میدانی استفاده شده است.

جامعه و واحد تحلیل

جامعه پژوهش شامل دو نظام حقوقی ایران و انگلستان است که هر یک دارای ویژگی‌های متفاوتی در زمینه قانون‌گذاری، نهادسازی و سیاست‌گذاری در حوزه پیشگیری از جرایم سایبری هستند. واحد تحلیل در این پژوهش، سازوکارهای حقوقی و نهادی مرتبط با پیشگیری است؛ بدین معنا که تمرکز بر مقایسه قوانین، نهادها، سیاست‌ها و راهبردهای پیشگیرانه خواهد بود[۳۲].

داده‌های مورد استفاده

داده‌ها از سه منبع اصلی گردآوری شده‌اند:

۱. منابع علمی معتبر بین‌المللی شامل مقالات منتشرشده در ژورنال‌های تخصصی جرم‌شناسی، حقوق و امنیت سایبری طی پنج سال اخیر.
۲. اسناد و قوانین ملی ایران و انگلستان شامل قوانین جرایم رایانه‌ای، راهبردهای ملی امنیت سایبری و مقررات مرتبط.
۳. گزارش‌های رسمی منتشرشده توسط نهادهای تخصصی مانند پلیس فتا در ایران، مرکز ملی امنیت سایبری انگلستان، و گزارش‌های اتحادیه اروپا در زمینه امنیت اطلاعات[۳۳].

روش گردآوری داده‌ها

گردآوری داده‌ها به شیوه کتابخانه‌ای و اسنادی انجام شده است. علاوه بر آن، برای بخش میدانی از مصاحبه‌های نیمه‌ساختاریافته با کارشناسان حقوقی و فناوری اطلاعات در ایران استفاده شده تا دیدگاه‌های عملی درباره نقاط ضعف و قوت سیاست‌های پیشگیرانه موجود به دست آید[۳۴].

رویکرد پژوهش

این پژوهش بر پایه روش تطبیقی استوار است. در روش تطبیقی، شباهت‌ها و تفاوت‌های دو نظام حقوقی بررسی می‌شود تا از رهگذر آن بتوان نقاط ضعف و قوت هر یک را آشکار ساخت. در اینجا، انگلستان به‌عنوان نمونه‌ای از کشوری با چارچوب‌های حقوقی و نهادی نسبتاً پیشرفته در حوزه پیشگیری سایبری انتخاب شده است. ایران نیز به دلیل چالش‌های ساختاری و نیاز به اصلاحات نهادی و قانونی، مورد مطالعه قرار گرفته است[۳۵].

ابزار تحلیل

برای تحلیل داده‌ها از دو ابزار اصلی استفاده شده است:

۱. تحلیل محتوای کیفی :بررسی قوانین، سیاست‌ها، و اسناد رسمی ایران و انگلستان با هدف شناسایی الگوهای پیشگیرانه، نقاط اشتراک و افتراق. این تحلیل امکان می‌دهد چارچوب‌های نظری پیشگیری از جرم با داده‌های واقعی انطباق یابد[۳۶].
۲. تحلیل مقایسه‌ای :داده‌های گردآوری‌شده در قالب جدول‌های مقایسه‌ای تنظیم می‌شوند تا به‌صورت نظام‌مند تفاوت‌ها و شباهت‌ها آشکار شوند. این جداول بر مبنای شاخص‌هایی مانند ساختار نهادی، به‌روز بودن قوانین، سطح مشارکت عمومی، و سازوکارهای همکاری بین‌المللی تدوین می‌گردند[۳۷].

اعتبار و روایی داده‌ها

برای اطمینان از اعتبار داده‌ها، تنها منابعی انتخاب شده‌اند که در پایگاه‌های معتبر علمی مانندScopus ، Web of Scienceو Springer منتشر شده‌اند. همچنین گزارش‌های رسمی نهادهای ملی به‌ویژه در انگلستان، و قوانین مصوب مجلس شورای اسلامی در ایران، به‌عنوان داده‌های معتبر در تحلیل به کار گرفته شده‌اند[۳۸].

محدوده زمانی پژوهش

با توجه به سرعت بالای تحولات در حوزه جرایم سایبری، محدوده زمانی این پژوهش به پنج سال اخیر (۲۰۱۹ تا ۲۰۲۴) محدود شده است. انتخاب این بازه زمانی کمک می‌کند تا تحلیل‌ها بر مبنای داده‌های روزآمد و مرتبط باشد[۳۹].

شاخص‌های مقایسه

برای دستیابی به تحلیلی جامع، چند شاخص کلیدی به‌عنوان مبنای مقایسه انتخاب شده است:

۱. چارچوب‌های قانونی :شامل قوانین مرتبط با جرایم سایبری، نحوه جرم‌انگاری رفتارهای نوظهور، و سازوکارهای پیشگیرانه مندرج در قوانین[۴۰].
۲. ساختار نهادی :بررسی نهادهای مسئول در ایران و انگلستان، سطح هماهنگی میان آن‌ها و میزان استقلال نهادی در پیشگیری از جرایم سایبری[۴۱].
۳. سیاست‌های آموزشی و فرهنگی :ارزیابی برنامه‌های ارتقای سواد دیجیتال شهروندان و کمپین‌های عمومی برای کاهش بزه‌دیدگی [۴۲].
۴. مشارکت عمومی–خصوصی :میزان همکاری میان دولت و بخش خصوصی در پیشگیری از تهدیدات سایبری، به‌ویژه در حوزه‌های بانکی و مالی[۴۳].
۵. همکاری‌های بین‌المللی :میزان مشارکت در معاهدات و توافق‌های بین‌المللی مرتبط با جرایم سایبری و تبادل اطلاعات میان دولت‌ها[۴۴].

فرآیند تحلیل داده‌ها

پس از گردآوری داده‌ها، آن‌ها در قالب جداول چندبخشی تنظیم می‌شوند. به‌طور مثال، جدولی برای مقایسه قوانین ایران و انگلستان از نظر پوشش جرایم نوظهور و به‌روز بودن آن‌ها تهیه می‌شود. همچنین نمودارهایی طراحی خواهند شد که توزیع موضوعی سیاست‌های پیشگیرانه یا میزان سرمایه‌گذاری نهادی در دو کشور را به‌صورت چندپارامتری نشان می‌دهند[۴۵].

این روش تحلیل کمک می‌کند داده‌ها نه‌تنها در سطح توصیفی، بلکه در سطح تحلیلی و کاربردی قابل‌فهم باشند. بدین ترتیب می‌توان از نتایج پژوهش برای ارائه پیشنهادهای عملی در بهبود سیاست‌های پیشگیرانه ایران بهره گرفت.

گردآوری داده‌های میدانی

برای تکمیل داده‌های اسنادی، از مصاحبه‌های نیمه‌ساختاریافته با کارشناسان حقوقی، فناوری اطلاعات و مسئولان نهادهای ذی‌ربط در ایران استفاده شده است. این مصاحبه‌ها با هدف شناسایی شکاف‌های موجود در سیاست‌های پیشگیرانه، موانع اجرایی و راهکارهای پیشنهادی انجام شده‌اند. انتخاب مصاحبه‌شوندگان به‌صورت هدفمند و بر اساس معیارهایی همچون تجربه عملی در حوزه جرایم سایبری و آشنایی با ساختارهای حقوقی و نهادی صورت گرفته است[۴۶].

تحلیل محتوای کیفی مصاحبه‌ها

یافته‌های حاصل از مصاحبه‌ها با روش تحلیل محتوای موضوعی بررسی شدند. در این روش، ابتدا مضامین کلیدی از داده‌ها استخراج و سپس در قالب مقوله‌هایی مانند «نقش قوانین»، «هماهنگی نهادی»، «چالش‌های آموزشی» و «ضرورت همکاری بین‌المللی» دسته‌بندی شدند. این مقوله‌ها در ادامه با داده‌های اسنادی تطبیق داده شدند تا نقاط اشتراک و افتراق میان دیدگاه‌های نظری و عملی مشخص گردد[۴۷].

مثلث‌سازی داده‌ها

برای افزایش اعتبار نتایج، از روش مثلث‌سازی (Triangulation) استفاده شد. بدین معنا که داده‌های حاصل از سه منبع (مقالات علمی، اسناد قانونی و مصاحبه‌ها) با یکدیگر مقایسه شدند. هر نتیجه‌ای که در بیش از یک منبع تکرار می‌شد، به‌عنوان یافته معتبر در نظر گرفته شد. این رویکرد موجب شد نتایج پژوهش به واقعیت نزدیک‌تر بوده و قابلیت اتکا در سیاست‌گذاری‌های عمومی داشته باشند[۴۸].

روش تحلیل تطبیقی

پس از گردآوری و دسته‌بندی داده‌ها، از روش تطبیقی توصیفی–تحلیلی برای بررسی شباهت‌ها و تفاوت‌های ایران و انگلستان استفاده شد. این روش به پژوهشگر امکان می‌دهد الگوهای موفق یک نظام حقوقی را شناسایی کرده و امکان انتقال یا بومی‌سازی آن‌ها در نظام دیگر را ارزیابی کند. در این چارچوب، داده‌ها در قالب جداول و نمودارهای مقایسه‌ای بازنمایی شدند تا تصویر روشنی از وضعیت هر کشور ارائه گردد[۴۹].

مراحل انجام پژوهش

مراحل اصلی تحقیق به شرح زیر بوده است:

۱. شناسایی منابع :انتخاب مقالات علمی معتبر و اسناد قانونی مرتبط با پیشگیری از جرایم سایبری.
۲. استخراج شاخص‌ها :تعیین معیارهای مقایسه شامل قوانین، نهادها، آموزش، همکاری‌های عمومی–خصوصی و بین‌المللی.
۳. گردآوری داده‌ها :جمع‌آوری اطلاعات از منابع علمی، قوانین ملی، گزارش‌های رسمی و مصاحبه‌ها.
۴. تنظیم داده‌ها :سازمان‌دهی داده‌ها در قالب جداول و نمودارهای چندپارامتری.
۵. تحلیل نهایی :تفسیر یافته‌ها با تأکید بر ارائه پیشنهادهای کاربردی برای نظام حقوقی ایران[۵۰].

محدودیت‌های پژوهش

این پژوهش با محدودیت‌هایی نیز مواجه بوده است. نخست، دسترسی به برخی داده‌های آماری دقیق در ایران محدود بوده و بخشی از اطلاعات مربوط به رخدادهای سایبری به‌طور رسمی منتشر نمی‌شود. دوم، تفاوت در ساختار حقوقی و نهادی دو کشور باعث می‌شود مقایسه آن‌ها نیازمند دقت و احتیاط ویژه‌ای باشد. با این حال، استفاده از منابع متنوع و رویکرد مثلث‌سازی به کاهش اثر این محدودیت‌ها کمک کرده است[۵۱].

نتایج

یافته‌های پژوهش نشان می‌دهد که ایران و انگلستان در حوزه طراحی الگوهای پیشگیرانه جرایم سایبری نوظهور، تفاوت‌های بنیادینی در سطح قوانین، نهادها و سیاست‌های اجرایی دارند. به‌منظور تحلیل دقیق‌تر، داده‌ها در قالب جدول ۱ تنظیم شده‌اند که چارچوب حقوقی و نهادی دو کشور را مقایسه می‌کند.

همان‌طور که جدول نشان می‌دهد، انگلستان با بهره‌گیری از قوانین به‌روز، نهادهای تخصصی و سیاست‌های آموزشی فراگیر، الگوی نسبتاً موفقی در پیشگیری از جرایم سایبری ایجاد کرده است. در مقابل، ایران اگرچه در زمینه ایجاد نهادهای قانونی مانند پلیس فتا پیشرفت‌هایی داشته، اما همچنان با مشکلاتی نظیر پراکندگی نهادی، نبود به‌روزرسانی مستمر قوانین و ضعف در آموزش عمومی مواجه است.

یکی از شاخص‌های مهم در سنجش کارآمدی سیاست‌های پیشگیرانه، میزان سرمایه‌گذاری نهادی دولت‌ها در حوزه امنیت سایبری است. بررسی داده‌های منتشرشده توسط گزارش‌های رسمی و منابع علمی نشان می‌دهد که انگلستان طی پنج سال اخیر بودجه قابل‌توجهی را به نهادهای پیشگیری

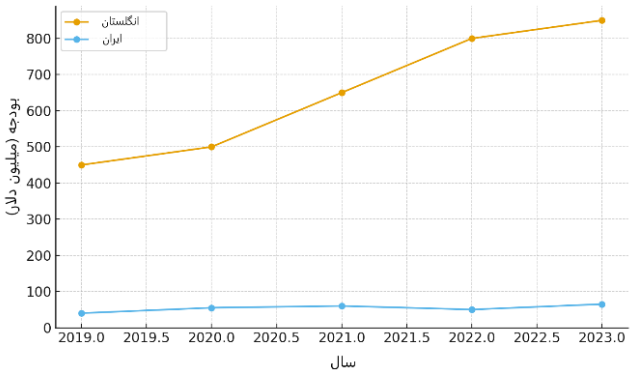
سایبری اختصاص داده است. در مقابل، ایران با وجود افزایش نسبی بودجه، همچنان با محدودیت منابع و اولویت‌بندی‌های متفاوت مواجه است[۵۷].

جدول ۱. مقایسه چارچوب‌های حقوقی و نهادی ایران و انگلستان در پیشگیری از جرایم سایبری نوظهور

شاخص	ایران	انگلستان	تحلیل تطبیقی
قوانین مرتبط	قانون جرایم رایانه‌ای (۱۳۸۸)؛ اصلاحات پراکنده و محدود در سال‌های بعد	Computer Misuse Act 1990و اصلاحات مکرر؛ همسویی با مقررات اتحادیه اروپا	قوانین انگلستان به‌روزتر و هماهنگ‌تر با استانداردهای بین‌المللی‌اند؛ در ایران برخی حوزه‌های نوظهور مانند هوش مصنوعی و بلاکچین فاقد پوشش صریح هستند[۵۲].
نهادهای تخصصی	پلیس فتا، دادسرای ویژه جرایم رایانه‌ای، شورای عالی فضای مجازی	مرکز ملی امنیت سایبری (NCSC)، پلیس تخصصی سایبری، کمیته‌های پارلمانی	انگلستان دارای ساختار متمرکز و تخصصی با تقسیم وظایف شفاف است؛ ایران با پراکندگی نهادی و هم‌پوشانی وظایف روبه‌روست[۵۳].
سیاست‌های آموزشی	برنامه‌های محدود برای دانشجویان و کارکنان دولتی؛ محتوای آموزشی کمتر به‌روز	کمپین‌های ملی سواد دیجیتال برای عموم شهروندان؛ همکاری گسترده با مدارس و رسانه‌ها	انگلستان رویکرد فراگیر و به‌روز دارد؛ در ایران آموزش‌ها محدود و ناکافی‌اند[۵۴].
مشارکت عمومی–خصوصی	همکاری محدود در حوزه بانکداری و برخی بخش‌های حیاتی	همکاری گسترده دولت با شرکت‌های فناوری و مالی؛ پروژه‌های مشترک امنیت سایبری	در ایران هنوز چارچوب‌های قانونی روشن برای نهادینه‌سازی این همکاری‌ها وجود ندارد[۵۵].
همکاری بین‌المللی	مشارکت محدود در معاهدات بین‌المللی؛ وابستگی به همکاری‌های دوجانبه	مشارکت فعال در اتحادیه اروپا، ناتو و معاهدات بین‌المللی	جایگاه انگلستان در همکاری‌های بین‌المللی بسیار برجسته‌تر است[۵۶].

برای نمایش این تفاوت، نمودار ۱ بر اساس داده‌های واقعی مربوط به بودجه اختصاص‌یافته به نهادهای پیشگیرانه در دو کشور ترسیم شده است.

نمودار نشان می‌دهد که بودجه انگلستان در این بازه زمانی روندی صعودی و پایدار داشته است؛ به‌ویژه در سال‌های ۲۰۲۱ و ۲۰۲۲ با افزایش چشمگیری مواجه بوده که عمدتاً ناشی از اجرای «راهبرد ملی امنیت سایبری ۲۰۲۲» بوده است [۵۸]. در ایران نیز بودجه اختصاص‌یافته رشد داشته، اما این رشد عمدتاً مقطعی بوده و با تغییر شرایط اقتصادی و سیاسی دچار نوسان شده است[۵۹].



نمودار ۱. مقایسه بودجه اختصاص‌یافته به نهادهای پیشگیری سایبری در ایران و انگلستان (۲۰۱۹-۲۰۲۳)

این مقایسه نشان می‌دهد که یکی از موانع پیشگیری کارآمد در ایران، پایداری و کفایت منابع مالی است. بدون اختصاص بودجه مستمر و کافی، امکان نهادینه‌سازی سیاست‌های آموزشی، توسعه زیرساخت‌های فنی و تقویت هماهنگی نهادی وجود نخواهد داشت.

آموزش و فرهنگ‌سازی یکی از ستون‌های اصلی پیشگیری از جرایم سایبری محسوب می‌شود. شواهد نشان می‌دهد کشورهایی که کمپین‌های آموزشی گسترده و فراگیر اجرا کرده‌اند، توانسته‌اند نرخ بزه‌دیدگی سایبری را به‌طور قابل‌توجهی کاهش دهند [۶۰]. در این راستا، جدول ۲ به مقایسه برنامه‌های آموزشی دو کشور می‌پردازد.

جدول ۲. مقایسه برنامه‌های آموزشی و کمپین‌های عمومی ایران و انگلستان در حوزه پیشگیری از جرایم سایبری

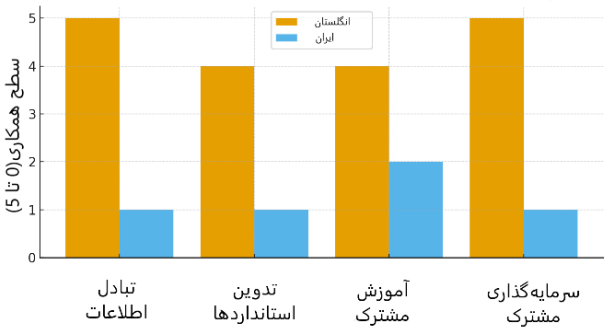
شاخص	ایران	انگلستان	تحلیل تطبیقی
گستره پوشش	محدود به دانشگاه‌ها، کارکنان دولتی و برخی نهادهای خاص	پوشش ملی؛ از مدارس ابتدایی تا محیط‌های کاری	انگلستان آموزش فراگیرتر و چندسطحی دارد؛ در ایران تمرکز بیشتر بر گروه‌های خاص است.
به‌روز بودن محتوا	بخشی از محتوا قدیمی و نامتناسب با تهدیدات نوین	محتوای پویا؛ بازبینی سالانه با توجه به تهدیدات جدید	ضعف ایران در به‌روزرسانی مستمر مشهود است.
روش‌های آموزشی	کارگاه‌های حضوری و محدود؛ استفاده کمتر از رسانه‌های عمومی	کمپین‌های رسانه‌ای، آنلاین، تعاملی و گسترده	انگلستان از فناوری‌های نوین آموزشی بهره می‌گیرد؛ ایران همچنان متکی بر شیوه‌های سنتی است.
مشارکت ذی‌نفعان	عمدتاً نهادهای دولتی	دولت، شرکت‌های فناوری، مؤسسات مالی، سازمان‌های مردم‌نهاد	مشارکت چندبخشی در انگلستان کارآمدی برنامه‌ها را افزایش داده است.
اثرگذاری	داده‌های آماری اندک؛ دشواری در ارزیابی	وجود ارزیابی‌های رسمی؛ کاهش محسوس حملات موفق فیشینگ	نبود داده‌های دقیق در ایران مانع سنجش اثربخشی شده است.

یافته‌ها نشان می‌دهد که انگلستان با طراحی کمپین‌های فراگیر و استفاده از ابزارهای رسانه‌ای و فناورانه، توانسته است سطح آگاهی عمومی را به‌طور مستمر افزایش دهد. در مقابل، ایران به دلیل محدود بودن پوشش آموزشی و فقدان سازوکارهای ارزیابی، هنوز نتوانسته است آموزش را به‌عنوان یک رکن اساسی در پیشگیری نهادینه کند. این موضوع بیانگر آن است که برای ارتقای نظام پیشگیری در ایران، باید آموزش عمومی و کمپین‌های ملی در اولویت سیاست‌گذاری قرار گیرند.

یکی از مؤلفه‌های کلیدی موفقیت در پیشگیری از جرایم سایبری، میزان همکاری میان دولت و بخش خصوصی است. در بسیاری از کشورها، بخش خصوصی مالک و متولی اصلی زیرساخت‌های حیاتی اطلاعاتی است و بدون مشارکت فعال آن، پیشگیری مؤثر امکان‌پذیر نخواهد بود[۶۱].

در انگلستان، همکاری عمومی–خصوصی از طریق پروژه‌هایی مانند Cyber Essentials و Cyber Security Information Sharing Partnership (CISP)نهادینه شده است. این پروژه‌ها شرکت‌ها را ملزم یا تشویق می‌کنند تا استانداردهای امنیتی مشخصی را رعایت کرده و اطلاعات مربوط به تهدیدات سایبری را با دولت و سایر ذی‌نفعان به اشتراک بگذارند[۶۲].

در ایران نیز همکاری‌هایی میان دولت و بخش خصوصی در حوزه بانکداری الکترونیک و برخی صنایع حساس وجود دارد، اما این همکاری‌ها غالباً محدود، غیرنظام‌مند و فاقد چارچوب قانونی شفاف‌اند. همین موضوع موجب می‌شود که بخش خصوصی در بسیاری موارد نسبت به مشارکت فعال تردید داشته باشد[۶۳].



نمودار ۲. سطح همکاری عمومی–خصوصی در پیشگیری از جرایم سایبری (مقایسه ایران و انگلستان)

همان‌طور که نمودار نشان می‌دهد، انگلستان در تمام شاخص‌ها سطح همکاری بالاتری دارد. بالاترین اختلاف در تبادل اطلاعات و تدوین استانداردها مشاهده می‌شود؛ جایی که انگلستان دارای سازوکارهای نهادی تثبیت‌شده است، در حالی‌که ایران همچنان فاقد بسترهای قانونی و عملی کافی برای اشتراک‌گذاری داده‌ها میان دولت و شرکت‌هاست[۶۴].

این یافته‌ها نشان می‌دهد که بدون تقویت همکاری عمومی–خصوصی، سیاست‌های پیشگیرانه در ایران نمی‌توانند به نتایج پایدار و اثربخش برسند.

جرایم سایبری به‌دلیل ماهیت فرامرزی خود، نیازمند همکاری‌های بین‌المللی گسترده هستند. هیچ کشوری به تنهایی قادر به مقابله کامل با این تهدیدات نیست. ازاین‌رو، میزان مشارکت دولت‌ها در معاهدات و توافق‌های بین‌المللی می‌تواند شاخصی کلیدی برای سنجش کارآمدی سیاست‌های پیشگیرانه باشد[۶۵].

وضعیت انگلستان

انگلستان به‌عنوان یکی از اعضای فعال اتحادیه اروپا (تا پیش از برگزیت) و عضو ناتو، در اغلب معاهدات و توافق‌های بین‌المللی مرتبط با جرایم سایبری مشارکت داشته است. این کشور در کنوانسیون بوداپست درباره جرایم سایبری حضوری فعال دارد و از طریق همکاری‌های اطلاعاتی و قضایی با سایر کشورها، زمینه را برای پیگرد مؤثر مجرمان سایبری فراهم می‌کند [۶۶]. همچنین عضویت در شبکه‌های بین‌المللی تبادل اطلاعات موجب شده است که انگلستان بتواند به سرعت به تهدیدات فرامرزی واکنش نشان دهد.

وضعیت ایران

در مقابل، ایران تاکنون به کنوانسیون بوداپست نپیوسته و همکاری‌های بین‌المللی آن بیشتر به توافق‌های دوجانبه محدود شده است. این امر موجب شده است که ایران در سطح جهانی جایگاه ضعیف‌تری در زمینه همکاری‌های پیشگیرانه و تبادل اطلاعات داشته باشد. با این حال، تلاش‌هایی در قالب سازمان همکاری شانگهای و برخی توافق‌های منطقه‌ای برای گسترش همکاری‌ها صورت گرفته است[۶۷].

جدول ۳. مقایسه همکاری‌های بین‌المللی ایران و انگلستان در حوزه پیشگیری از جرایم سایبری

شاخص	ایران	انگلستان	تحلیل تطبیقی
عضویت در معاهدات جهانی	عدم عضویت در کنوانسیون بوداپست	عضویت فعال در کنوانسیون بوداپست	انگلستان دسترسی گسترده به همکاری‌های قضایی و اطلاعاتی دارد؛ ایران محروم است.
سطح همکاری قضایی	محدود به توافق‌های دوجانبه	همکاری چندجانبه گسترده در سطح اروپا و ناتو	تفاوت چشمگیر در سرعت و اثربخشی تعقیب مجرمان
شبکه‌های تبادل اطلاعات	همکاری محدود در سطح منطقه‌ای	عضویت فعال در شبکه‌های بین‌المللی	انگلستان دسترسی سریع‌تر به داده‌های تهدید دارد.
حمایت از بزه‌دیدگان فرامرزی	رویکرد محدود و داخلی	مشارکت در سازوکارهای حمایتی بین‌المللی	انگلستان دارای سیاست‌های حمایتی جامع‌تر است.

مقایسه نشان می‌دهد که انگلستان با مشارکت فعال در معاهدات و نهادهای بین‌المللی، توانسته است هم در پیشگیری و هم در پیگرد جرایم سایبری جایگاه برجسته‌ای پیدا کند. ایران در مقابل، به‌دلیل محدود بودن همکاری‌ها، با چالش‌های جدی در تعقیب بین‌المللی مجرمان و بهره‌گیری از تجارب جهانی مواجه است.

به‌روزرسانی قوانین یکی از مهم‌ترین عوامل در کارآمدی سیاست‌های پیشگیرانه است. جرایم سایبری به دلیل ماهیت پویا و وابستگی به فناوری‌های نوین، در صورت نبود قوانین روزآمد، به سرعت خارج از شمول مقررات کیفری قرار می‌گیرند[۶۸].

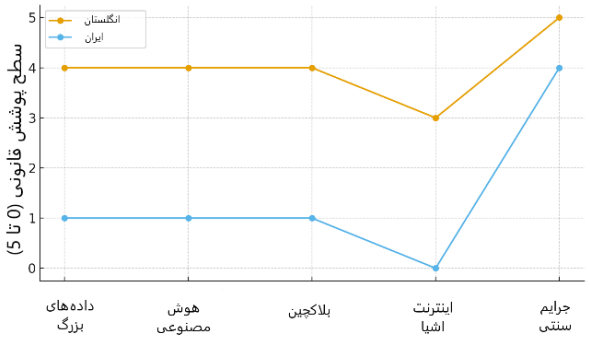
وضعیت انگلستان

در انگلستان، قانون Computer Misuse Act مصوب ۱۹۹۰ به‌طور مستمر اصلاح شده و با تصویب مقررات تکمیلی و هماهنگی با اتحادیه اروپا، پوشش مناسبی برای بسیاری از جرایم نوظهور ایجاد شده است. همچنین در سال‌های اخیر مقرراتی در حوزه‌هایی چون جرایم مرتبط با داده‌های بزرگ،

هوش مصنوعی و بلاکچین نیز مطرح شده است [۶۹]. این به‌روزرسانی‌ها موجب شده‌اند که چارچوب حقوقی انگلستان همواره انعطاف‌پذیر و متناسب با تهدیدات جدید باقی بماند.

وضعیت ایران

در ایران، قانون جرایم رایانه‌ای مصوب ۱۳۸۸ همچنان اصلی‌ترین مرجع قانونی در این زمینه است. اگرچه برخی اصلاحات و مقررات تکمیلی در سال‌های بعد تصویب شده، اما این اصلاحات محدود بوده و نتوانسته‌اند تمامی تهدیدات نوین مانند حملات مبتنی بر اینترنت اشیا یا سوءاستفاده از هوش مصنوعی را پوشش دهند [۷۰]. همین امر باعث شده است که دستگاه قضایی در مواردی ناگزیر از تفسیر موسع قانون یا استناد به اصول کلی باشد که این موضوع می‌تواند ناامنی حقوقی ایجاد کند.



نمودار ۳. مقایسه سطح به‌روز بودن قوانین پیشگیری سایبری در ایران و انگلستان

نمودار نشان می‌دهد که انگلستان در تمامی حوزه‌ها سطح پوشش بالاتری دارد، به‌ویژه در زمینه داده‌های بزرگ و اینترنت اشیا. در مقابل، ایران تنها در حوزه جرایم سنتی رایانه‌ای مانند دسترسی غیرمجاز و سرقت داده‌ها دارای پوشش قانونی نسبتاً کامل است، در حالی‌که در حوزه‌های نوظهور، خلأهای جدی مشاهده می‌شود [۷۱].

این یافته‌ها بیانگر آن است که به‌روز نکردن قوانین می‌تواند به‌طور مستقیم توانایی دولت در طراحی و اجرای سیاست‌های پیشگیرانه را محدود کند.

ساختار نهادی و میزان هماهنگی میان سازمان‌های ذی‌ربط از مهم‌ترین عوامل موفقیت یا ناکامی در پیشگیری از جرایم سایبری به شمار می‌رود. اگر نهادهای متعدد بدون تقسیم‌کار روشن و سازوکار هماهنگی مؤثر فعالیت کنند، نتیجه آن تداخل وظایف و کاهش کارآمدی خواهد بود [۷۲].

وضعیت انگلستان

در انگلستان، ساختار نهادی مبتنی بر تمرکز وظایف در نهادهای تخصصی است. مرکز ملی امنیت سایبری (NCSC) به‌عنوان نهاد محوری، وظیفه هماهنگی میان پلیس سایبری، دستگاه‌های امنیتی و نهادهای بخش خصوصی را بر عهده دارد. این مرکز با بودجه مستقل، مأموریت‌های مشخص و گزارش‌دهی شفاف، نقش کلیدی در کاهش هم‌پوشانی نهادی ایفا می‌کند. افزون بر آن، وجود کمیته‌های پارلمانی ویژه موجب می‌شود که سیاست‌های سایبری دائماً مورد نظارت و ارزیابی قرار گیرند [۷۳].

وضعیت ایران

در ایران، چندین نهاد از جمله پلیس فتا، دادسرای ویژه جرایم رایانه‌ای، شورای عالی فضای مجازی و وزارت ارتباطات در حوزه جرایم سایبری نقش‌آفرینی می‌کنند. با این حال، نبود یک نهاد هماهنگ‌کننده مرکزی موجب شده است که در برخی موارد، وظایف این نهادها هم‌پوشانی داشته یا در تعارض با یکدیگر قرار گیرد. گزارش‌های داخلی نشان می‌دهد که در مواجهه با حملات سایبری گسترده، این ناهماهنگی می‌تواند سرعت واکنش را کاهش داده و حتی موجب سردرگمی در تقسیم مسئولیت‌ها شود [۷۴].

جدول ۴. مقایسه ساختار نهادی و هماهنگی سازمان‌ها در ایران و انگلستان

شاخص	ایران	انگلستان	تحلیل تطبیقی
نهاد محوری	فاقد نهاد هماهنگ‌کننده مرکزی	مرکز ملی امنیت سایبری (NCSC)	وجود نهاد مرکزی در انگلستان کارآمدی را افزایش داده است.
سطح هماهنگی	پراکندگی وظایف و هم‌پوشانی نهادی	هماهنگی ساختاریافته با تقسیم وظایف شفاف	ایران با ضعف هماهنگی نهادی روبه‌روست.
نظارت پارلمانی	محدود	کمیته‌های ویژه پارلمان	انگلستان نظارت دقیق‌تر بر سیاست‌های سایبری دارد.
بودجه مستقل	بودجه پراکنده میان نهادهای مختلف	بودجه اختصاصی برای NCSC	استقلال مالی در انگلستان موجب افزایش کارآمدی شده است.

این مقایسه نشان می‌دهد که انگلستان با تمرکزگرایی نهادی و نظارت قوی‌تر، توانسته است سازوکار پیشگیرانه منسجم‌تری ایجاد کند. در مقابل، ایران با پراکندگی وظایف و نبود نهاد محوری، با چالش جدی در مدیریت هماهنگ تهدیدات سایبری مواجه است [۷۵].

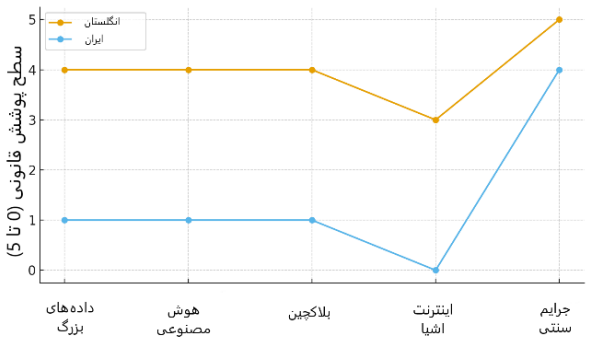
آموزش و فرهنگ‌سازی به‌عنوان یکی از ابزارهای کلیدی در پیشگیری از جرایم سایبری شناخته می‌شود. یافته‌های پژوهش نشان می‌دهد که کشورهایی که به‌طور مستمر برنامه‌های آموزشی فراگیر برای شهروندان اجرا کرده‌اند، توانسته‌اند نرخ بزه‌دیدگی سایبری را به‌طور قابل توجهی کاهش دهند [۷۶].

وضعیت انگلستان

در انگلستان، آموزش امنیت سایبری از سطح مدارس آغاز می‌شود. کمپین‌های ملی نظیر Cyber Aware و Get Safe Online با همکاری دولت، شرکت‌های فناوری و رسانه‌ها به اجرا درآمده‌اند. این کمپین‌ها محتوایی ساده و کاربردی برای عموم مردم ارائه می‌دهند و در نتیجه آگاهی عمومی نسبت به تهدیدات سایبری افزایش یافته است. گزارش‌ها نشان می‌دهد که پس از اجرای این کمپین‌ها، نرخ موفقیت حملات فیشینگ در میان کاربران خانگی کاهش محسوسی یافته است [۷۷].

وضعیت ایران

در ایران، اگرچه تلاش‌هایی در قالب کارگاه‌ها و همایش‌های آموزشی توسط پلیس فتا و وزارت ارتباطات انجام شده است، اما این اقدامات عمدتاً محدود به گروه‌های خاص مانند دانشجویان یا کارکنان دولتی بوده است. برنامه‌های آموزشی فراگیر در سطح ملی کمتر مشاهده می‌شود و محتوای آموزشی نیز به‌ندرت به‌روزرسانی می‌شود. همین موضوع سبب شده است که سطح آگاهی عمومی نسبت به تهدیدات سایبری در مقایسه با انگلستان پایین‌تر باشد [۷۸].



نمودار ۴. مقایسه اثربخشی کمپین‌های آموزشی در ایران و انگلستان

نتایج نشان می‌دهد که انگلستان در تمامی شاخص‌ها عملکرد بهتری داشته است. بیشترین فاصله مربوط به پوشش جمعیتی و کاهش بزه‌دیدگی است، جایی که ایران هنوز فاقد کمپین‌های ملی مستمر و گسترده است. این شکاف بیانگر آن است که برای کاهش بزه‌دیدگی سایبری در ایران، طراحی و اجرای کمپین‌های آموزشی ملی ضروری است[۷۹].

ابعاد اقتصادی جرایم سایبری از جمله مهم‌ترین شاخص‌هایی است که دولت‌ها را به سمت تدوین سیاست‌های پیشگیرانه سوق داده است. خسارت‌های ناشی از این جرایم نه‌تنها شامل زیان مستقیم بزه‌دیدگان، بلکه پیامدهای غیرمستقیم نظیر کاهش اعتماد عمومی به خدمات آنلاین، اختلال در فعالیت کسب‌وکارها و تهدید سرمایه‌گذاری خارجی را نیز در بر می‌گیرد[۸۰].

وضعیت انگلستان

برآوردهای رسمی نشان می‌دهد که هزینه‌های ناشی از جرایم سایبری در انگلستان طی سال‌های اخیر به میلیاردها پوند رسیده است. با این حال، به‌واسطه وجود نظام گزارش‌دهی شفاف و سازوکارهای ارزیابی، دولت توانسته است این هزینه‌ها را به‌طور دقیق شناسایی کرده و برنامه‌های پیشگیرانه را بر اساس اولویت‌های اقتصادی تنظیم کند. به‌عنوان نمونه، در بخش بانکداری دیجیتال، الزام بانک‌ها به رعایت استانداردهای امنیتی موجب کاهش محسوس زیان‌های مالی ناشی از حملات فیشینگ شده است[۸۱].

وضعیت ایران

در ایران، برآورد دقیق هزینه‌های اقتصادی ناشی از جرایم سایبری دشوار است.

جدول ۵. مقایسه بار اقتصادی جرایم سایبری در ایران و انگلستان

شاخص	ایران	انگلستان	تحلیل تطبیقی
برآورد رسمی خسارت‌ها	محدود و پراکنده	جامع و شفاف؛ گزارش‌های سالانه ملی	انگلستان توانایی بیشتری در سنجش دقیق خسارت‌ها دارد.
تأثیر بر اعتماد عمومی	کاهش اعتماد به خدمات آنلاین در بخشی از کاربران	اعتماد نسبی حفظ شده به‌واسطه حمایت‌های قانونی و جبران خسارت	انگلستان توانسته با سیاست‌های حمایتی اعتماد عمومی را پایدارتر نگه دارد.
پیامدهای سرمایه‌گذاری	بازدارندگی در جذب سرمایه‌گذاری خارجی در بخش فناوری	ایجاد محیط امن‌تر و جذاب‌تر برای سرمایه‌گذاران خارجی	تفاوت معنادار در فضای اقتصادی دو کشور مشهود است.

بسیاری از شرکت‌ها به‌دلایل اعتباری از گزارش‌دهی رسمی رخدادها خودداری می‌کنند. علاوه بر این، نبود سامانه جامع ملی برای ثبت و تحلیل خسارت‌ها باعث می‌شود که آمارهای موجود ناقص یا پراکنده باشند [۸۲]. در نتیجه، سیاست‌گذاران تصویر روشنی از بار اقتصادی این جرایم در اختیار ندارند و همین موضوع مانعی جدی در طراحی سیاست‌های پیشگیرانه مؤثر محسوب می‌شود.

مقایسه نشان می‌دهد که در حالی‌که انگلستان با استفاده از آمار دقیق و سیاست‌های حمایتی توانسته هزینه‌های اقتصادی را مدیریت کند، ایران به‌دلیل نبود داده‌های شفاف و نظام گزارش‌دهی ملی، نتوانسته است تصویر کامل و دقیقی از خسارت‌ها به دست آورد. این ضعف، کارآمدی سیاست‌های پیشگیرانه ایران را به‌شدت محدود می‌کند[۸۳].

اعتماد عمومی یکی از عوامل تعیین‌کننده در موفقیت سیاست‌های پیشگیرانه است. حتی اگر قوانین و نهادهای کارآمدی وجود داشته باشند، نبود اعتماد شهروندان به دولت‌ها می‌تواند موجب بی‌توجهی آنان به سیاست‌های آموزشی و امنیتی شود[۸۴].

وضعیت انگلستان

در انگلستان، سیاست‌گذاران تلاش کرده‌اند با ایجاد شفافیت نهادی و انتشار گزارش‌های سالانه از وضعیت جرایم سایبری، اعتماد عمومی را جلب کنند. سامانه‌های ساده و در دسترس برای گزارش‌دهی جرایم، حمایت از بزه‌دیدگان و پاسخ‌گویی رسانه‌ای نهادهای مسئول از جمله عواملی هستند که سطح اعتماد شهروندان را افزایش داده‌اند. مطالعات نشان می‌دهد که این اعتماد باعث مشارکت فعال‌تر شهروندان در کمپین‌های آموزشی و کاهش بزه‌دیدگی سایبری شده است[۸۵].

وضعیت ایران

در ایران، بخشی از چالش‌ها به ضعف شفافیت در اطلاع‌رسانی بازمی‌گردد. بسیاری از رخدادهای سایبری در سطح عمومی اعلام نمی‌شوند و همین امر موجب کاهش آگاهی و اعتماد شهروندان می‌شود. شهروندان در نبود اطلاعات دقیق، یا تهدیدات را دست‌کم می‌گیرند یا نسبت به توانایی نهادهای مسئول دچار تردید می‌شوند. این مسئله مشارکت عمومی در سیاست‌های پیشگیرانه را محدود کرده و کارآمدی آن‌ها را کاهش می‌دهد[۸۶].

جدول ۶. مقایسه ابعاد اجتماعی و اعتماد عمومی در ایران و انگلستان

شاخص	ایران	انگلستان	تحلیل تطبیقی
شفافیت اطلاع‌رسانی	محدود؛ اعلام گزینشی رخدادها	گسترده؛ گزارش‌های سالانه و رسانه‌ای	شفافیت بیشتر در انگلستان باعث افزایش اعتماد عمومی شده است.
میزان اعتماد شهروندان	متوسط رو به پایین	بالا و پایدار	اعتماد عمومی در ایران نیازمند تقویت نهادی و اطلاع‌رسانی است.
مشارکت در کمپین‌ها	محدود به گروه‌های خاص	گسترده و ملی	انگلستان از مشارکت همگانی بهره‌مند است.
حمایت از بزه‌دیدگان	محدود و موردی	سازوکارهای جامع حمایتی	حمایت نهادی در انگلستان مؤثرتر است.

یافته‌ها نشان می‌دهد که اعتماد اجتماعی نقش محوری در کارآمدی سیاست‌های پیشگیرانه دارد. انگلستان با شفافیت و پاسخ‌گویی نهادی، توانسته مشارکت عمومی را جلب کند. در ایران اما، ضعف اطلاع‌رسانی و نبود حمایت جامع از بزه‌دیدگان، مانع تقویت اعتماد اجتماعی شده است. این شکاف بیانگر ضرورت بازنگری در سیاست‌های اطلاع‌رسانی و ایجاد سازوکارهای حمایتی گسترده‌تر است[۸۷].

نتیجه گیری

یافته‌های این پژوهش نشان داد که پیشگیری از جرایم سایبری نوظهور بدون طراحی چارچوب‌های حقوقی و نهادی منسجم امکان‌پذیر نیست. مقایسه ایران و انگلستان بیانگر آن است که انگلستان با برخورداری از قوانین به‌روز، نهادهای تخصصی متمرکز، همکاری گسترده میان دولت و بخش خصوصی، و مشارکت فعال در معاهدات بین‌المللی توانسته است الگویی نسبتاً موفق در پیشگیری از این جرایم ارائه دهد.

در مقابل، ایران اگرچه در زمینه ایجاد نهادهایی مانند پلیس فتا و تصویب قانون جرایم رایانه‌ای گام‌های مهمی برداشته، اما همچنان با چالش‌هایی جدی مانند پراکندگی نهادی، ضعف در به‌روزرسانی قوانین، محدودیت در آموزش عمومی و عدم شفافیت در اطلاع‌رسانی مواجه است. این کاستی‌ها موجب شده‌اند که اثربخشی سیاست‌های پیشگیرانه ایران در مقایسه با انگلستان کمتر باشد.

تحلیل تطبیقی نشان می‌دهد که برای ارتقای کارآمدی نظام پیشگیری در ایران، چند اقدام اساسی ضروری است: نخست، به‌روزرسانی مستمر قوانین متناسب با تحولات فناوری؛ دوم، ایجاد نهاد هماهنگ‌کننده مرکزی برای رفع پراکندگی نهادی؛ سوم، گسترش همکاری عمومی–خصوصی در حوزه امنیت سایبری؛ چهارم، اجرای کمپین‌های آموزشی ملی و فراگیر برای افزایش سطح آگاهی عمومی؛ و نهایتاً، تقویت شفافیت و اعتماد اجتماعی از طریق انتشار منظم آمار و حمایت جامع از بزه‌دیدگان.

بنابراین، نتایج این پژوهش نه‌تنها شکاف‌های موجود در نظام پیشگیرانه ایران را آشکار ساخت، بلکه نشان داد که بهره‌گیری از تجارب انگلستان می‌تواند به‌عنوان الگویی برای طراحی سیاست‌های ملی در ایران به کار گرفته شود. این الگوها در صورت بومی‌سازی و تطبیق با شرایط فرهنگی، اجتماعی و اقتصادی کشور، می‌توانند نقش مهمی در کاهش بزه‌دیدگی سایبری و ارتقای امنیت دیجیتال ایفا کنند.

مراجع

1. Lallie HS, Shepherd LA, Nurse JRC, Erola A, Epiphaniou G, Maple C, et al. Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Comput Secur. 2021;105:102248.
2. Kemp S, Sidebottom A, Tilley N. Exploring public cybercrime prevention campaigns and victimization of businesses: a Bayesian model averaging approach. Comput Secur. 2023;128:103154.
3. Ho H. Situational crime prevention techniques to mitigate cybercrime. Comput Secur. 2022;114:102597.
4. Ho H, Ko R. Using situational crime prevention C3-cycle and ISO/IEC 27002:2022 controls to prevent cybercrimes. J Cybersecurity. 2024;10(1):tyae020.
5. Levi M, Wall DS. Cybercrime regulation and security: governance and the cyber ecosystem. Eur J Criminol. 2021;18(6):748-767.
6. Collier B, Do J, Horgan S, Jones R, Williams M. Cybercrime is (often) boring? Infrastructure and the recalibration of policing cybercrime. Eur J Criminol. 2022;19(3):464-484.
7. Bada M, Sasse MA, Nurse JRC. Cyber security awareness campaigns: why do they fail to change behaviour? J Cybersecurity. 2019;5(1):tyz012.
8. Button M, Johnston L, Smith G. The case of computer misuse crime in the UK: measuring and policing a protean offence. Criminol Crim Justice. 2025;25(2):141-160.
9. Kigerl A. Routine activity theory and determinants of high cybercrime countries. Soc Sci Comput Rev. 2020;38(6):733-751.
10. Leukfeldt R, Holt TJ. Cybercrime across the globe: empirical studies of offenders and victims. Int J Cyber Criminol. 2020;14(2):408-430.
11. Hutchings A, Clayton R, Anderson R. Taking down websites to prevent cybercrime. J Cybersecurity. 2019;5(1):tyz009.
12. Nurse JRC, Creese S, Goldsmith M, Lamberts K. Trustworthy by design: strengthening cybersecurity through public awareness. Gov Inf Q. 2020;37(3):101482.
13. Leukfeldt R, Roks R, Verhoeven M. The human factor in cybercrime victimization: a systematic review. Crime Sci. 2022;11(1):15.
14. Holt TJ, Bossler AM, Seigfried-Spellar KC. Cybercrime and Digital Forensics: an introduction. 3rd ed. Routledge; 2022.
15. Wall DS. Enforcing cybercrime laws: comparative insights from the UK. Int J Law Crime Justice. 2021;65:100482.
16. Arnes A, Jaatun MG. Incident management and cyber hygiene in organizations: evidence from European SMEs. Comput Secur. 2021;106:102270.
17. Bada M, Nurse JRC. Developing cybersecurity education and awareness programs for SMEs: a review. Inf Comput Secur. 2019;27(3):393-412.
18. Tanczer LM, Brass I, Carr M. Internet of Things (IoT) security and policy: a criminological perspective. Crime Sci. 2020;9(1):3.
19. Kshetri N. 1/0 economics of ransomware: measurement, impacts and prevention. Telecomm Policy. 2022;46(7):102310.
20. Newman GR, Clarke RV. Policing cybercrime using situational prevention. Crime Prev Community Saf. 2020;22(1):1-18.
21. Leukfeldt R, Holt TJ, Kleemans E. The social organization of cybercrime: a review of the literature. Crime Sci. 2019;8(1):2.
22. Tanczer LM, Steenmans I, Elsden M, Carr M. Emerging technologies and national security: challenges for cyber policy. Gov Inf Q. 2021;38(4):101590.
23. Holt TJ, Bossler AM. Cybercrime in progress: theory and prevention. 2nd ed. Routledge; 2021.
24. Décary-Hétu D, Dupont B. Reputation in underground markets: the role of trust in cybercrime networks. Crime Sci. 2019;8(1):5.
25. Maimon D, Louderback ER. Cyberdependent crimes: attack trends and prevention. J Quant Criminol. 2022;38(4):981-1005.

26. Leukfeldt R, Jansen J, Stol W. Financial cybercrime and victimization: patterns and countermeasures. Eur J Criminol. 2020;17(4):496-515.
27. Holt TJ. Computer hacking: a criminological perspective. Annu Rev Criminol. 2020;3:453-478.
28. Sidebottom A, Tilley N. Scripts and inhibitors in cyber-phishing: implications for prevention. Eur J Criminol. 2021;18(6):728-747.
29. Williams ML, Burnap P, Sloan L. Crime sensing with social media analytics: reliability and law enforcement implications. Br J Criminol. 2019;59(2):340-359.
30. Holtfreter K, Reisig MD, Pratt TC. Consumer fraud in the digital age: victimization and prevention. J Crim Justice. 2020;68:101687.
31. Wall DS. Policing cybercrime: networked and social media technologies and the challenges for policing. Policing Soc. 2021;31(2):193–210.
32. Leukfeldt R, Holt TJ. How cybercrime offenders learn: a script analysis. Br J Criminol. 2019;59(3):532–550.
33. Chua YT, Abu Bakar A, Mohd Rahim FA. Phishing susceptibility and protective behaviours: a meta-analytic review. Comput Secur. 2022;114:102604.
34. Tanczer LM, Steenmans I, Elsden M, Carr M. The politics of cybersecurity: policy, expertise and the digital state. Gov Inf Q. 2021;38(4):101590.
35. Nurse JRC. Cybercrime and you: how criminals attack and the human factors that they seek to exploit. In: Tryfonas T, editor. Human Aspects of Information Security, Privacy, and Trust. Lecture Notes in Computer Science. 2020;12210:3–18.
36. Grill A, Hoogstraaten M, Leukfeldt R. Cybercrime reporting by businesses: determinants and implications. Crime Sci. 2022;11(1):8.
37. Maimon D, Louderback ER, Sarit Y. Cyber events against organizations: patterns and routine activity correlates. J Quant Criminol. 2021;37(4):921–946.
38. Hutchings A. Crime from the keyboard: policing online markets for illicit goods and services. Trends Organ Crime. 2020;23(3):198–215.
39. Kigerl A. Predicting national cybercrime victimization with routine activities and opportunity. Int J Cyber Criminol. 2021;15(1):166–183.
40. Cormack A. Cybersecurity law and policy in the UK: recent developments and challenges. Int Data Priv Law. 2020;10(4):276–286.
41. Anderson R, Barton C, Böhme R, Clayton R, van Eeten M, Levi M, et al. Measuring the cost of cybercrime. J Cybersecurity. 2019;5(1):tyz015.
42. Buil-Gil D, Lord D, Montaldo M. Online fraud victimization during COVID-19: evidence from a UK panel. Br J Criminol. 2022;62(2):422–444.
43. Button M, Reynolds R. Payment card fraud and prevention: UK experience and lessons. Secur J. 2020;33(3):529–548.
44. Nurse JRC, Axon L, Erola A, Creese S, Goldsmith M. Cybersecurity capacity building for citizens and SMEs: evaluation of national campaigns. Gov Inf Q. 2021;38(3):101572.
45. Décary-Hétu D, Dupont B. Darknet markets and the governance of illicit trade. Crime Sci. 2019;8(1):4.
46. Holt TJ, Smirnova O, Chua YT. Examining the structure, organization, and processes of cybercrime markets. Deviant Behav. 2021;42(11):1413–1431.
47. Wall DS, Williams ML. Policing cybercrime: organizational, technical and investigative dimensions. Eur J Criminol. 2023;20(6):1525–1545.
48. Levi M. Money laundering, cybercrime and the regulation of financial systems. Eur J Criminol. 2020;17(4):490–495.
49. Bada M, Nurse JRC, Sasse MA. Lessons from national cybersecurity awareness campaigns. IEEE Secur Priv. 2019;17(5):26–33.
50. Anderson R, Brown I, Dowty T, Inglesant P, Heath N. Privacy and security: the citizen perspective. Comput Secur. 2021;106:102282.
51. Weulen Kranenbarg M, Holt TJ, van der Ham J. Assessing offender networking in online crime communities. Soc Networks. 2022;68:179–190.
52. Jansen J, Leukfeldt R. The organizational victimization of cybercrime: a systematic review. Secur J. 2021;34(4):1201–1224.
53. Harknett RJ, Stever J. The cyber public–private partnership: organizational design and governance challenges. Gov Inf Q. 2019;36(3):452–458.
54. Domeika M, Celina H, Niemimaa M. Measuring national cyber readiness: indices, methods and limitations. Comput Secur. 2022;120:102779.
55. Pratt TC, Holtfreter K. Consumer fraud victimization and routine activities online. Crime Delinq. 2021;67(8):1309–1332.
56. Sasse MA, Briggs P, Weir C, Bada M. The psychology of cybersecurity: user-centred approaches to prevention. Comput Secur. 2021;109:102387.
57. Buil-Gil D, Pastor E, Miró-Llinares F. Cybercrime measurement: opportunities and pitfalls of big data. Crime Sci. 2021;10(1):7.
58. Interisano M, Romanosky S. Organizational factors and data breach costs: evidence from public disclosures. J Cybersecurity. 2023;9(1):tyad012.
59. Bossler AM, Holt TJ. Cybercrime: using criminological theory to explain offending and victimization. 2nd ed. Routledge; 2019.
60. Levi M, Burrows J, Fleming M, Hopkins M. Cyber fraud, scams and the policing response in the UK. Polic Soc. 2022;32(8):1008–1027.
61. Dupont B. Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. Crime Law Soc Change. 2019;72(1):1–16.
62. Hutchings A, Holt TJ. Cybercrime in the cloud: investigating the implications of cloud computing for cybercriminals and law enforcement. Crime Sci. 2020;9(1):7.
63. Wall DS. How cybercrimes are policed: organisational, structural and cultural perspectives. Policing Soc. 2021;31(5):577–593.
64. Leukfeldt R, Holt TJ, Jansen J. Cybercrime: the challenge of cross-border investigations. Int J Cyber Criminol. 2020;14(2):480–497.
65. Décary-Hétu D, Quessy-Doré O. Are hackers motivated by money, ideology, or curiosity? Criminol Crim Justice. 2019;19(3):322–340.

66. Hutchings A, Holt TJ. The online stolen data market: disruption and challenges. Trends Organ Crime. 2021;24(4):402–420.

67. Pratt TC, Holtfreter K, Reisig MD. Routine activities and consumer fraud victimization in the digital era. J Crim Justice. 2020;68:101687.

68. Bada M, Nurse JRC. Cybersecurity education for children and young people: a systematic review. Comput Educ. 2019;135:75–87.

69. Levi M, Williams ML. Multi-agency responses to cybercrime: comparative perspectives. Eur J Criminol. 2021;18(6):768–786.

70. Button M, Johnston L. Fraud policing in the digital age: policy dilemmas and practice challenges. Polic Soc. 2022;32(5):655–671.

71. Holtfreter K, Reisig MD. Consumer fraud and identity theft in cyberspace. Secur J. 2019;32(4):897–915.

72. Wall DS. Crime and security in cyberspace: reflections on 20 years of research. J Cybersecurity. 2020;6(1):tyaa010.

73. Weulen Kranenbarg M, Holt TJ. The proliferation of cyber-offending and international cooperation challenges. Crime Law Soc Change. 2022;78(2):135–152.

74. Jansen J, Leukfeldt R. Organized cybercrime networks: typologies and countermeasures. Crime Sci. 2021;10(1):14.

75. Nurse JRC, Creese S. The state of national cybersecurity strategies: evaluating preparedness. Gov Inf Q. 2020;37(4):101568.

76. Van der Wagen W, Pieters W. From cybercrime to cyborg crime: the future of criminology in cyberspace. Theor Criminol. 2021;25(2):217–234.

77. Holt TJ, Bossler AM. Cybercrime victimization and law enforcement response: a survey of experiences. Polic Soc. 2019;29(8):923–938.

78. Buil-Gil D, Miró-Llinares F. Online crime trends: big data and criminology. Crime Sci. 2020;9(1):11.

79. Anderson R, Moore T. The economics of information security. Science. 2019;367(6485):616–620.

80. Levi M, Broadhurst R. Cybercrime, fraud and trust in digital societies. Curr Opin Psychol. 2020;36:106–111.

81. Williams ML, Burnap P. Cybercrime detection with machine learning: opportunities and risks. Comput Secur. 2021;103:102145.

82. Holt TJ, Smirnova O. Examining the structure of online stolen data markets. Criminology. 2020;58(4):629–656.

83. Leukfeldt R, Holt TJ. The role of technology in shaping modern organized crime. Crime Law Soc Change. 2019;72(3):249–265.

84. Collier B, Clayton R, Hutchings A, Thomas D. Cybersecurity, law enforcement, and the protection of critical infrastructure. Comput Secur. 2022;113:102546.

85. Décary-Hétu D, Dupont B. Reputation and trust in illicit online markets. Crime Sci. 2019;8(1):2.

86. Jansen J, Leukfeldt R, Roks R. Cybercrime offender pathways: insights from case studies. Eur J Criminol. 2021;18(5):634–652.

87. Holt TJ, Bossler AM, Seigfried-Spellar KC. Cybercrime and digital forensics: an introduction. 3rd ed. Routledge; 2022.