Criminalization of Cyberterrorism Against the Security of Critical Infrastructure; Feasibility of Designing a Development Model within the Jurisdictional Framework of the International Criminal Court Statute

Abstract

The commission of cyberattacks by terrorists, in addition to its growing impact on the economic, social, political, and security dimensions, poses the risk of violating the security of critical infrastructure as a strategic international target. Therefore, the International Criminal Court (ICC) should expand its jurisdiction to address such crimes, thereby enabling a response to transnational threats affecting global security. To this end, reforms in the ICC Statute and the criminalization of cyberterrorism, particularly through the development of clear criteria for identifying, prosecuting, and punishing perpetrators of these crimes, as well as strengthening international cooperation in cybersecurity, are essential. In this context, this study, using a descriptive-analytical approach, aims to answer the question: "Is it feasible to design a model for expanding the jurisdiction of the ICC to address cyberterrorism against critical infrastructure?" Accordingly, the research first examines the feasibility of expanding the ICC's jurisdiction in this area and its impact on international security, and then assesses the necessity of reforms in the ICC Statute for the criminalization of cyberterrorism and the design of the necessary legal model for identifying, prosecuting, and punishing the perpetrators of such crimes, in line with enhancing global security and facilitating international cooperation.

Keywords: International Criminal Court Jurisdiction, Cyberterrorism, Protection of Critical Infrastructure, Cybersecurity Platforms, International Cooperation.

جرم‌انگاری تروریسم سایبری علیه امنیت زیرساخت‌های حیاتی؛ امکان‌سنجی طراحی الگوی توسعه در صلاحیت قضایی اساسنامه دیوان کیفری بین‌المللی

چکیده

ارتکاب حملات سایبری از سوی تروریست‌ها، ضمن ایجاد آثار فزاینده در ابعاد اقتصادی، اجتماعی، سیاسی و امنیتی، امکان نقض امنیت زیرساخت‌های حیاتی به‌عنوان اهداف راهبردی در قلمرو نظام‌های ملی و بین‌المللی را به‌دنبال خواهد داشت. از اینرو، دیوان کیفری بین‌المللی باید صلاحیت خود را برای رسیدگی به ارتکاب چنین جرایمی توسعه دهد تا امکان پاسخ به تهدیدهای فراملی و تأثیرگذار بر امنیت جهانی را فراهم نماید. برای این منظور، اصلاحات در اساسنامه دیوان و جرم‌انگاری تروریسم سایبری به‌ویژه از طریق تدوین معیارهای روشن برای شناسایی، تعقیب و مجازات مرتکبان این جرایم و تقویت همکاری‌های بین‌المللی در زمینه امنیت سایبری، ضرورتی انکارناپذیر است. در این چارچوب، پژوهش حاضر با استفاده از روش توصیفی-تحلیلی درصدد پاسخ به این پرسش که «آیا امکان طراحی الگوی توسعه در صلاحیت قضایی دیوان برای رسیدگی به تروریسم سایبری علیه زیرساخت‌های حیاتی وجود دارد؟» است. وفق این امر، پژوهش ابتدا مبادرت به بررسی امکان‌سنجی توسعه صلاحیت دیوان در این حوزه و تأثیر آن بر امنیت بین‌المللی نموده و سپس ضرورت اصلاحات در اساسنامه دیوان را برای جرم‌انگاری تروریسم سایبری و طراحی الگوی حقوقی لازم جهت شناسایی، تعقیب و مجازات مرتکبان این‌گونه جرایم، در راستای ارتقاء امنیت جهانی و تسهیل همکاری‌های بین‌المللی، مورد سنجش قرار می‌دهد.

واژگان کلیدی: صلاحیت دیوان کیفری بین‌المللی، تروریسم سایبری، حفاظت از زیرساخت‌های حیاتی، امنیت سکوهای سایبری، همکاری‌های بین‌المللی.

مقدمه

وابستگی زیرساخت‌های حیاتی به فناوری‌های نوین، آن‌ها را در مواجهه با حملات سایبری آسیب‌پذیر کرده و این حملات به چالشی جهانی تبدیل شده‌اند. برای مقابله با این تهدیدها، دولت‌ها ضمن افزایش سطح داخلی ایمنی سامانه‌ها، با جذب نیروی انسانی متخصص،

باید مقررات سختگیرانه وضع کنند. به‌علاوه، همکاری بین‌المللی برای تدوین معاهده‌ای الزام‌آور راجع‌به ممنوعیت حملات سایبری[1] به زیرساخت‌های حیاتی، نقش مهمی در حفاظت از امنیت سایبری جهانی دارد (فرشاسعید؛ جلالی؛ گودرزی، ۱۴۰۱، ص ۱۷۳). در عین حال، با توسعه فناوری‌های دیجیتال و اینترنت، تهدیدهای نوینی، از جمله تروریسم سایبری به‌مثابه جرمی جهانی(اینارسن، ۱۴۰۲، ص ۲۴-۲۳)، شکل گرفت که در آن از فضای سایبری (*به‌مثابه پنجمین فضای مشترک، پس از زمین، دریا، هوا و فضای بیرونی*) برای حمله به زیرساخت‌های حیاتی استفاده می‌شود(Sieber, 2006, p. 431-432). رشد فضای دیجیتال به بهبود ارتباطات و تقویت زیرساخت‌های حیاتی جوامع کمک کرده است، اما تهدیدات سایبری مانند حملات تروریستی فناورانه، امنیت این زیرساخت‌ها را به خطر انداخته‌اند. این حملات شامل سرقت داده‌ها، دستکاری اطلاعات و اختلال در خدمات اساسی هستند. علیرغم اشاره‌ها به این تهدیدات در اسناد بین‌المللی، فقدان قوانین قوی برای مقابله با آن‌ها، این جرایم را تسهیل کرده است(نمامیان، ۱۴۰۳: ۲۵).

تروریسم سایبری علیه زیرساخت‌های حیاتی نشان می‌دهد که اساس‌نامه دیوان کیفری بین‌المللی [*زین‌پس «دیوان» تقریر می‌شود*]، تروریسم سایبری را به عنوان جرم بین‌المللی تعریف نکرده است. این اساس‌نامه تنها صلاحیت رسیدگی به چهار جرم عمده را شامل می‌شود: جنایات جنگی، جنایات علیه بشریت، نسل‌کشی و جنایت تجاوز(شریعت‌باقری، ۱۴۰۲، ص ۲۰۶-۲۰۵). با این حال، در صورتی که حملات سایبری گسترده و علیه زیرساخت‌های حیاتی منجر به نقض حقوق بشر و آسیب‌های انسانی شوند، ممکن است این حملات به‌طور غیرمستقیم تحت شمول جنایات علیه بشریت قرار گیرند. برای رسیدگی مؤثر به این نوع جرایم، تدوین یک تعریف جامع و معتبر از تروریسم سایبری به‌عنوان جرم بین‌المللی ضروری است(Viganò; Loi; Yaghmaei, 2020, p. 164-165). بنابراین، یکی از چالش‌های اصلی در توسعه صلاحیت دیوان برای رسیدگی به جرایم سایبری، تعریف دقیق «تروریسم سایبری» است. در حال حاضر، حقوق بین‌الملل و اساسنامه دیوان هیچ تعریف مشخصی از این جرم ندارند(Qualters, 2023, p. 1). بنابراین، لازم است که تعریف و معیارهای دقیق‌تری برای شمول حملات سایبری، به ویژه حملات به زیرساخت‌های حیاتی، ارائه شود. چالش دیگر، توسعه صلاحیت قضایی دیوان برای رسیدگی به این نوع جرایم است. دیوان تاکنون تنها به جنایات فیزیکی رسیدگی کرده است، و برای مقابله با تهدیدهای سایبری، باید صلاحیت خود را توسعه دهد. این امر نیازمند اصلاحات در اسناد بین‌المللی است(Rahman; Das, 2024, p. 986-987; Gupta; Deol, 2025, p. 12497-12498). از اینرو، حملات سایبری به دلیل ماهیت فرامرزی خود، نیازمند همکاری‌های حقوقی بین‌المللی است تا از طریق تبادل اطلاعات، هماهنگی تحقیقات و اجرای احکام، پاسخگویی مؤثری به این تهدیدها صورت گیرد(Alabbadi; Al Amaren; Aletein, 2020, p. 159-161). نهادهایی نظیر اینترپل و یوروپول می‌توانند در تسهیل این همکاری‌ها نقش مهمی ایفا کنند.[2]

به طور کلی، توسعه صلاحیت دیوان برای رسیدگی به تروریسم سایبری نیازمند اصلاحات اساسی در مقررات و همکاری‌های بین‌المللی است تا تهدیدهای نوین سایبری را پوشش داده و همزمان حقوق بشر و امنیت جهانی را تضمین کند(کالک، ۱۴۰۳، ص ۱۴۲-۱۴۱). از

---

[1] با گسترش فضای سایبر، «رایاجنگ‌ها» (یا «جنگ سایبری») به‌عنوان ابزاری برای اعمال قدرت افزایش یافته‌اند و ضرورت اعمال محدودیت‌های حقوقی بر آن‌ها احساس می‌شود. قواعد حقوق جنگ به‌طور عمده برای جنگ‌های سنتی طراحی شده‌اند و به‌کارگیری آن‌ها برای رایاجنگ‌های غیرسنتی با چالش‌هایی مواجه است. رایاجنگ‌هایی که زیرساخت‌های حیاتی را مختل می‌کنند، ممکن است آثار شدیدتری از جنگ‌های سنتی ایجاد کنند، بدون آنکه آثار فیزیکی مشابهی داشته باشند. با اتخاذ رویکردی پویا به مفهوم «شدت»، می‌توان وقوع مخاصمات سایبری و جنایات جنگی ناشی از اختلال در زیرساخت‌های حیاتی را پیش‌بینی کرد، هرچند این رویکرد در مواجهه با زیرساخت‌های سایبری با کاربرد دوگانه با چالش‌هایی همراه است(شاملو؛ حسینی، ۱۴۰۳، ص ۱۱۵).

[2] https://www.europol.europa.eu/media-press/newsroom/news/interpol-and-europol-agree-joint-initiatives-to-enhance-global-response-against-transnational-crime

اینرو، دیوان باید صلاحیت خود را برای رسیدگی به این تهدیدها علیه امنیت زیرساخت‌های حیاتی توسعه دهد.[3] اصلاح و روزآمدسازی اساسنامه دیوان و تقویت همکاری‌های بین‌المللی در مقابله با این تهدیدها، امری ضروری به نظر می‌رسد. افزون بر این، دیوان می‌بایست مقررات مؤثری را برای مقابله با آسیب به زیرساخت‌های حیاتی تدوین کرده و به‌این‌ترتیب، امنیت جهانی را حفظ و از تهدیدهای آینده پیشگیری کند(Buisman; Alfatlawi, 2025, p. 26-27).

بازنگری و توسعه مقررات موجود برای جبران نقضِ امنیت سایبری در چارچوب جنایات جنگی و جنایات علیه بشریت از اهمیت ویژه‌ای برخوردار است(Matos, 2021: 9-11). با توجه به تهدیدهای فزاینده سایبری و استفاده از آن‌ها به‌عنوان ابزار جنگ یا وسیله‌ای برای ارتکاب جنایات علیه بشریت، تدوین مقررات بین‌المللی به منظور مقابله با این تهدیدها ضرورتی انکارناپذیر است. دیوان باید صلاحیت خود را در رسیدگی به جرایم سایبری در چارچوب جنایات جنگی و علیه بشریت تقویت کرده و اصلاحاتی در اساسنامه خود اِعمال نماید؛ اصلاحاتی که مشتمل بر تعریف دقیق‌تر این جرایم و تعیین مسئولیت‌های فردی و دولتی باشد. افزون بر این، ضرورت ایجاد سازوکارهای نوین برای تحقیق، تعقیب و همکاری بین‌المللی به‌منظور تأمین امنیت سایبریِ جهانی، قابل درک است.[4]

این پژوهش با اهدافی نظیر «بررسی ظرفیت‌های دیوان در رسیدگی به تروریسم سایبری و شناخت چالش‌ها و موانع حقوقی در توسعه صلاحیت قضایی آن» و «سنجش تأثیر توسعه صلاحیت قضایی دیوان به‌مثابه طراحی الگو برای تقویت همکاری‌های بین‌المللی و امنیت سایبری به‌منظور مقابله با تهدیدهای ناشی از تروریسم سایبری علیه زیرساخت‌های حیاتی» با بهره‌گیری از مطالعه اسنادی و روش توصیفی‌تحلیلی، سعی بر آن دارد تا به این پرسش که «الگوی توسعه صلاحیت دیوان برای مواجهه با چالش‌ها و موانع حقوقی و ساختاری برای درج تروریسم سایبری در اساسنامه چیست؟» و «چگونه الگوی توسعه صلاحیت قضایی دیوان در جرم‌انگاری تروریسم سایبری، امکان حفاظت از امنیتِ زیرساخت‌های حیاتی و همکاری‌های بین‌المللی در قبال چنین تهدیدهایی اثرگذار است؟»، پاسخ دهد.

۱. از چالش‌ها و تهدیدهای نوین تا ضرورت جرم‌انگاری تروریسم سایبری

بررسی شکل‌های مختلف تروریسم به دلیل تفاوت شرایط آن‌ها ضروری نیست، اما در همه موارد، غیرقانونی‌بودن آن مشترک است. تروریسم، به‌ویژه پس از حوادث ۱۱ سپتامبر ۲۰۰۱، به یکی از نگرانی‌های اصلی جهانی تبدیل شده و دولت‌ها با تقویت اقدامات داخلی، در پی مقابله با این پدیده بین‌المللی و حفظ امنیت خود بوده‌اند. از اینرو، تروریسم، به‌ویژه از اواخر قرن بیستم، به‌عنوان یک جرم در حقوق بین‌المللی مورد توجه قرار گرفت(Guillaume, 2004, p. 539-541). پیش از آن، بیشتر توجه به مسائلی چون جنگ‌های مسلحانه، جنایات جنگی و نقض حقوق بشر معطوف بود و مفاهیم خاصی برای مقابله با تروریسم وجود نداشت. در دهه‌های بعد، به‌ویژه پس از تصویب کنوانسیون‌های بین‌المللی برای جرم‌انگاری فعالیت‌های تروریستی نظیر هواپیماربایی (کنوانسیون راجع به جرایم و دیگر اعمال ارتکابی در داخل هواپیما[5]) و سایر فعالیت‌ها، نگرش حقوق بین‌المللی به مفهوم تروریسم تغییر کرد.

---

[3] https://iccwbo.org/news-publications/policies-reports/protecting-the-cybersecurity-of-critical-infrastructures-and-their-supply-chains/

[4] برای تضمین شفافیت در مقررات مسئولیت‌پذیری کشورها در قبال حملات سایبری علیه زیرساخت‌ها، لازم است مفاهیم اساسی نظیر حمله سایبری، زیرساخت‌های حیاتی و مسئولیت کشورها به‌طور دقیق در معاهدات بین‌المللی تعریف شوند. این مقررات باید شرایط مشخصی برای تعیین مسئولیت کشورها در قبال حملات سایبری داشته باشند(Kumar, 2024, p. 25-26). ایجاد نهادهای نظارتی بین‌المللی برای پیگیری نقض‌ها و حل اختلافات در شناسایی مسئولیت‌ها ضروری است. کشورها باید با همکاری و تبادل مؤثر اطلاعات، در شناسایی و تعقیب حملات سایبری مشارکت کنند. البته روزآمدسازی معاهدات امنیت سایبری برای افزایش شفافیت قضایی و مدیریت بهتر تهدیدهای سایبری اهمیت دارد.

[5] Convention on Offences and Certain Other Acts Committed on Board Aircraft, Signed at Tokyo on 14 September 1963; https://treaties.un.org/doc/db/terrorism/conv1-english.pdf

حملات سایبری در دهه ۲۰۰۰ میلادی، به‌ویژه پس از حوادث ۱۱ سپتامبر ۲۰۰۱، ضرورت مقابله با این تهدیدها را در سطح بین‌المللی برجسته‌تر ساخت. در این راستا، دولت‌ها اقداماتی همچون تصویب مقررات ملی برای مقابله با جرایم سایبری و تقویت همکاری‌های بین‌المللی را آغاز کردند(Jayakumar, 2021, p. 884-886).[۶] از اینرو، تروریسم سایبری علیه زیرساخت‌های حیاتی حملاتی است که با استفاده از فناوری‌های دیجیتال به سامانه‌ها و شبکه‌ها حمله کرده و تهدیدی جدی برای امنیت ملی و زندگی روزمره افراد به شمار می‌آید. این نوع تروریسم به عنوان «جرایم سایبری» شناخته شده و نیازمند تدوین مقررات داخلی و بین‌المللی برای مقابله با آن است. دولت‌ها موظف به حفاظت از زیرساخت‌های حیاتی خود هستند و می‌توانند در صورت وقوع حملات، با استناد به قواعد دفاع مشروع واکنش نشان دهند(Sim, 2023, p. 226; George; Baskar; Srikaanth, 2024, p. 59-62). چنین حملاتی ممکن است حقوق بشر، به ویژه حق حریم خصوصی و حفاظت از داده‌های شخصی را نقض کنند. با توجه به پیچیدگی فضای سایبری، شناسایی مجرمان دشوار است، از اینرو، همکاری‌های بین‌المللی برای اجرای مؤثر مقررات و تسهیل اقدامات قضایی ضرورت دارد(احمدی‌مقدم؛ غلامی‌دون، ۱۳۹۸، ص ۸۶-۸۷)؛ از اینرو، به‌علت اینکه تروریسم سایبری امکان ایجاد بحران در ساختارهای اجتماعی، اقتصادی و سیاسی فراهم می‌کند، ضرورت همکاری‌های بین‌المللی در قبال این تهدیدها از اهمیت قابل ملاحظه‌ای برخوردار است (Snider; Hefetz; Shandler; Canetti, 2025, p. 16-18).

در حال حاضر، اسناد بین‌المللی هم‌چون «کنوانسیون بوداپست در مورد جرایم سایبری، مصوب ۲۰۰۱»[۷] در فرایند مقابله با تروریسم سایبری کمک می‌کنند(Girard, 2023, p. 214)، اما این اسناد تحت صلاحیت دیوان قرار ندارند (Azmi; Shabrina, 2023, p. 6-7). بنابراین، با توجه به تهدیدهای ناشی از جرایم سایبری، توسعه اساس‌نامه دیوان به‌منظور جرم‌انگاری حملات سایبری شدید علیه زیرساخت‌های حیاتی به‌عنوان جنایات جنگی یا علیه بشریت ضروری است. اصلاحات مورد نیاز باید شامل تعریف دقیق مفاهیم مرتبط، شناسایی حملات گسترده به‌عنوان جنایات بین‌المللی، تعیین مسئولیت کیفری فردی و ایجاد سازوکارهای همکاری بین‌المللی برای تعقیب عاملان باشد. این اقدامات مستلزم اراده سیاسی و اجماع جهانی به‌منظور مقابله مؤثر با تهدیدات سایبری هستند (Bartoli, 2025, p. 508).

دیوان که طی سال ۱۹۹۸ به‌عنوان مرجع قضایی برای تعقیب و رسیدگی به جنایات بین‌المللی ایجاد شده بود، تنها صلاحیت قضایی برای تعقیب جنایات جنگی، جنایات علیه بشریت و نسل‌کشی را داشت و تروریسم و جرایم سایبری به‌طور خاص در تحت شمول صلاحیت قضایی نداشت؛ اما از ابتدای دهه ۲۰۲۰ با افزایش تهدیدهای سایبری، نگرانی‌هایی راجع‌به نحوه مقابله دیوان با تروریسم سایبری مطرح شد که بر این اساس، اجرای «کنوانسیون سازمان ملل متحد علیه جرایم سایبری، مصوب ۲۰۲۴»[۸]، بر لزوم پاسخ‌گذاری به تهدیدهای سایبری و توسعه همکاری‌های بین‌المللی، به‌ویژه به شناسایی و تعقیب تروریسم سایبری، مورد تأکید قرار گرفت. کنوانسیون مزبور، بر

---

[۶] لازم به‌ذکر است، در مه ۲۰۰۷، اتحادیه بین‌المللی مخابرات دستور کار جهانی جرایم سایبری را با هدف هماهنگی واکنش‌های بین‌المللی در قبال چالش‌های فزاینده امنیت سایبری راه‌اندازی کرد. در اکتبر همان سال، گروهی از کارشناسان بین‌المللی برای تدوین پیشنهادات راهبردی به‌منظور پاسخ به این چالش‌ها تشکیل شد که طی سال ۲۰۰۸ گزارش‌هایی در زمینه امنیت سایبری و مقررات جرایم سایبری ارائه کردند. در سال ۲۰۱۰، چهار گروه کاری تأسیس گردیدند تا پیشنهادهایی برای واکنش‌های حقوقی بین‌المللی جدید در قبال جرایم سایبری ارائه دهند. به‌علاوه، در همان سال، مؤسسه شرق و غرب گروه کاری حقوقی جرایم سایبری را با هدف بررسی و تدوین معاهده‌ای جهانی در این زمینه تأسیس کرد. علاوه بر این، ایالات متحده و اتحادیه اروپا در ۲۰۱۰ گروه کاری مشترکی را برای توسعه رویکردهای یکپارچه در مسائل امنیت سایبری و جرایم سایبری تشکیل دادند. این گروه به‌ویژه بر گسترش الحاق کشورهای عضو اتحادیه اروپا به کنوانسیون شورای اروپا و حمایت از کشورهای غیرعضو برای پیوستن به آن تمرکز دارد(Schjolberg, 2012, p. 3-5).

[7] The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols, https://www.coe.int/en/web/cybercrime/the-budapest-convention

[8] https://docs.un.org/en/A/AC.291/L.15

ضمن تأکید بر اهمیت حفاظت از زیرساخت‌های حیاتی نظیر شبکه‌های برق، آب، حمل‌ونقل و خدمات بهداشت و درمان، آسیب به زیرساخت‌ها می‌تواند منجر به ایجاد بحران‌های جهانی شود.

با وجود تحولات و تهدیدات نوین سایبری، دیوان کیفری بین‌المللی تاکنون به جرایم سایبری علیه زیرساخت‌ها نپرداخته است. برای رسیدگی به این جرایم، توسعه صلاحیت دیوان از طریق اصلاحات در اساسنامه ضروری است. چالش‌های اصلی در این فرایند شامل عدم تعریف جامع از «جرایم سایبری» و نیاز به همکاری‌های بین‌المللی است که توسعه صلاحیت دیوان می‌تواند به تقویت امنیت جهانی و مدیریت تهدیدهای سایبری کمک کند(Ya, 2023, p. 1012).

۲. تقویت ساختارهای نهادی؛ از چالش‌های امنیتی سایبری تا همکاری‌های حقوقی بین‌المللی

تحولات جدید در جرایم و تروریسم سایبری، مسائل حقوقی پیچیده‌ای در حوزه‌هایی چون حقوق بشر و صلاحیت قضایی پدید آورده است(سیدناصری؛ میربد، ۱۴۰۳، ص ۱۵). ازاینرو، تروریسم سایبری به‌عنوان یک تهدید جهانی، با توجه به تأثیرات آن بر زیرساخت‌های حیاتی، چالش‌های جدی در حوزه امنیت ملی و بین‌المللی ایجاد کرده است(Adenekan, 2023, p. 12). مقابله با این تهدیدها مستلزم ایجاد چارچوب‌های حقوقی هماهنگ در سطح بین‌المللی است. یکی از چالش‌های اساسی در این راستا، عدم هماهنگی مقررات ناظر به امنیت سایبری و عدم چارچوب حقوقی جامع است که مانع از تعقیب مؤثر مرتکبان جرایم سایبری می‌شود (Fidler, 2015, p. 17). علاوه بر این، مسائل حقوق بشری و حاکمیت ملی باید به‌گونه‌ای مدیریت شود که توازن میان امنیت و حقوق فردی به‌طور مؤثر حفظ گردد. البته کشورهای در حال توسعه باید با تقویت ظرفیت‌های فنی و آموزشی، به‌طور مؤثر به مقابله با این تهدیدهای جهانی بپردازند.[9]

۲-۱. چالش‌ها و موانع درج تروریسم سایبری در صلاحیت دیوان؛ ضرورت بازنگری و همکاری‌های بین‌المللی

تروریسم سایبری در اسناد بین‌المللی به‌طور مستقیم به‌عنوان یک جرم مستقل شناسایی نشده است، اما در برخی اسناد به‌طور غیرمستقیم مورد توجه قرار گرفته است(LeChette-Danberry, 2025, p. 49). کنوانسیون بوداپست (۲۰۰۱) و قطعنامه‌های شورای امنیت و مجمع عمومی سازمان ملل متحد تهدیدهای سایبری و استفاده از آن در فعالیت‌های تروریستی را مورد بررسی قرار داده‌اند.[10] اتحادیه

---

[9] National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

[10] شورای امنیت سازمان ملل متحد در راستای پیشگیری از جرایم دیجیتال علیه زیرساخت‌های حیاتی، با صدور قطعنامه ۲۳۴۱ طی سال ۲۰۱۷ به این موضوع پرداخته و از دولت‌ها خواست تا این جرایم را به‌عنوان جرایم جدی در مقررات داخلی خود تعریف کنند؛

- Resolution 2341 (2017) / adopted by the Security Council at its 7882nd meeting, on 13 February 2017, https://docs.un.org/S/RES/2341(2017)

افزون بر این، قطعنامه ۲۳۹۶ بر اهمیت تقویت همکاری‌های ملی، منطقه‌ای و بین‌المللی در قبال تهدیدهای سایبری، به‌ویژه حملات به اماکن عمومی و استفاده از فناوری‌های نوین تأکید داشت؛

- The protection of critical infrastructures against terrorist attacks: Compendium of good practices, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf

در سال ۲۰۲۱، در هفتمین بررسی راهبرد جهانی ضد تروریسم، دولت‌ها با اجماع بر اولویت حفاظت از اهداف آسیب‌پذیر در مقابل جرایم دیجیتال توافق کردند. قطعنامه ۲۹۱/۷۵ مجمع عمومی نیز بر لزوم همکاری میان دولت‌ها، سازمان‌های بین‌المللی، بخش خصوصی و سایر ذینفعان برای مقابله با تهدیدهای سایبری و حفظ امنیت زیرساخت‌های حیاتی تأکید نمود؛

- United Nations, General Assembly, A/RES/75/291, 2 July 2021, https://documents.un.org/doc/undoc/gen/n21/175/70/pdf/n2117570.pdf

اروپا[11] بر ضرورت مقابله با تهدیدهای سایبری تأکید کرده‌اند[12]، اما برای جرم‌انگاری تروریسم سایبری در چارچوب صلاحیت دیوان، بازنگری در اساسنامه و تعریف جامع این جرم ضروری است. چالش‌هایی مانند عدم تعریف واحد، پیچیدگی‌های فنی و مخالفت برخی کشورها با محدود شدن حاکمیت ملی، مانع این روند هستند. مقابله مؤثر با تروریسم سایبری مستلزم همکاری بین‌المللی و ایجاد سازوکارهای اجرایی کارآمد است (Cristiano; Broeders; Weggemans, 2020, p. 28-29).

موانع اصلی برای درج تروریسم سایبری در صلاحیت دیوان شامل فقدان تعریف جامع و بین‌المللی از این جرم، پیچیدگی‌های فنی حملات سایبری، و عدم اراده سیاسی در میان کشورهای عضو برای اصلاح اساس‌نامه می‌باشد. تلاش‌های قبلی برای افزودن جرم تروریسم به‌عنوان یک جرم مستقل در اساس‌نامه دیوان به دلیل عدم توافق جهانی و نگرانی‌های مرتبط با حاکمیت ملی تاکنون به نتیجه نرسیده است(Asghar; Javed; Azhar, 2025, p. 419-421). در نتیجه، اساس‌نامه در وضعیت کنونی ابزار مناسبی برای رسیدگی مستقیم به تروریسم سایبری نیست. برای رفع این شکاف قانونی، بازنگری در اساس‌نامه، تدوین مقررات جدید و تقویت همکاری‌های بین‌المللی به‌ویژه در زمینه ایجاد اجماع جهانی، ضروری به نظر می‌رسد.

با توجه به عدم وجود مقررات مشخص راجع‌به تروریسم سایبری در اساس‌نامه دیوان، مواجهه با تهدیدهای فناوری‌های دیجیتال و حملات سایبری به زیرساخت‌های حیاتی، چالش‌های جدی برای حقوق بشردوستانه و حقوق بشر ایجاد می‌کند. حقوق بشردوستانه حملات سایبری به تأسیسات غیرنظامی را نقض می‌داند، در حالی که حقوق بشر با تهدیدهایی نظیر نقض حریم خصوصی، آزادی بیان، امنیت فردی و حق بر سلامت مواجه است(Alkharman; Hassan, 2023, p. 16-18). یکی از چالش‌های اصلی برای گنجاندن تروریسم سایبری در صلاحیت دیوان، فقدان تعریف جامع از «جرایم سایبری» است. برای مقابله مؤثر با این تهدیدها، بازنگری و تدوین مقررات جدید در اساس‌نامه دیوان ضروری بوده و شکاف قانونی موجود، به‌ویژه در مواجهه با پیشرفت‌های فناوری، یک مشکل جدی در حقوق بین‌الملل کیفری به‌شمار می‌آید.

۲-۲. تقویت همکاری‌های بین‌المللی در قبال تروریسم سایبریِ ناقض امنیت زیرساخت‌های حیاتی؛ ضرورت هماهنگی مقررات، تبادل اطلاعات و توسعه صلاحیت در دیوان

برای مبارزه مؤثر با تروریسم سایبری و حفاظت از زیرساخت‌های حیاتی، توسعه همکاری‌های بین‌المللی میان کشورهای عضو و نهادهایی مانند دیوان، سازمان ملل، اینترپل و اتحادیه اروپا ضروری است. این نهادها می‌توانند در تقویت امنیت سایبری جهانی و مقابله با تهدیدها سایبری نقش مهمی ایفا کنند. وفق قطعنامه ۷۴/۱۳۰(۲۰۱۹) مجمع عمومی سازمان ملل متحد، کشورها باید مقررات امنیت سایبری را هماهنگ کرده و با یکدیگر برای تعقیب تروریسم سایبری همکاری کنند.[13] دیوان باید به‌عنوان مرجع اصلی تعقیب جنایات بین‌المللی

---

[11] در این ارتباط، «آژانس همکاری عدالت کیفری اتحادیه اروپا» (European Union Agency for Criminal Justice Cooperation "Eurojust") وفق ماده ۸۵ «پیمان لیسبون» و آیین‌نامه آژانس که تعیین مأموریت، ساختار حاکمیتی، نظام حفاظت از داده‌ها و چارچوب ایجاد توافق‌نامه‌ها با کشورهای غیرعضو اتحادیه اروپارا مقرر نموده، از ۱۲ دسامبر ۲۰۱۹ لازم‌الاجرا شد و فعالیت می‌کند(روبو، ۱۴۰۳، ص ۴۷۵-۴۶۴). در ضمن، آژانس در مقابله با جرایم سایبری مرتبط با زیرساخت‌های حیاتی اتحادیه اروپا از طریق تسهیل همکاری‌های بین‌المللی، پشتیبانی از تحقیقات مشترک و تحلیل تهدیدات، به کشورهای عضو در شناسایی، پیشگیری و مقابله با حملات سایبری و حملات باج‌افزار نقشی اساسی ایفا می‌کند؛

- https://www.eurojust.europa.eu/about-us/organisation/eurojust-legal-framework

[12] https://digital-strategy.ec.europa.eu/en/news/european-union-and-nato-intensify-cooperation-addressing-cyber-threats

[13] https://docs.un.org/en/A/74/130

عمل کرده و اصلاحات در اساسنامه دیوان برای درج جرایم سایبری، به ویژه تروریسم سایبری و حملات به زیرساخت‌های حیاتی، ضروری است.[۱۴]

همکاری‌های حقوقی و اجرایی میان کشورهای عضو باید شامل توسعه استانداردهای مشترک برای شناسایی و مقابله با حملات سایبری باشد. این استانداردها باید چارچوبی شفاف برای تجزیه‌وتحلیل تهدیدها و تعیین مسئولیت‌ها فراهم کنند. تبادل اطلاعات و ایجاد سازوکارهای مؤثر برای حل‌وفصل اختلافات در مورد مسئولیت‌ها باید در اولویت قرار گیرد. همکاری با سازمان‌های بین‌المللی مانند سازمان ملل متحد، اینترپل و اتحادیه اروپا برای نظارت بر امنیت سایبری، اهمیت زیادی دارد (Sendjaja; Prastiawan; Suryani, 2024, p. 1016). در سطح بین‌المللی، همکاری میان نهادهای مختلف باید به تقویت زیرساخت‌های فنی مشترک و تبادل اطلاعات فنی و آموزش تخصصی متمرکز گردد. به‌ویژه برای کشورهای در حال توسعه، ارتقای توانمندی‌های امنیت سایبری از طریق آموزش، مشاوره فنی و تبادل تجربیات می‌تواند نقش مؤثری در کاهش تهدیدهای سایبری ایفا کند.[۱۵] نهادهایی همچون اینترپل و اتحادیه اروپا می‌توانند به‌عنوان پشتیبان‌های فنی و مشاور در زمینه اجرای استانداردهای مشترک و تبادل اطلاعات مؤثر عمل کنند.[۱۶]

نهادهای بین‌المللی باید بر اجرای مقررات و تعقیب مرتکبان جرایم سایبری نظارت داشته باشند. دیوان و سازمان‌هایی نظیر اینترپل و اتحادیه اروپا باید همکاری‌های خود را برای شناسایی تهدیدهای سایبری، مقابله با تروریسم سایبری و حفاظت از زیرساخت‌های حیاتی تقویت کرده و بر اساس یک چارچوب حقوقی منسجم و تبادل اطلاعات مؤثر عمل کنند.[۱۷] افزون بر این، ایجاد شبکه‌های آموزشی برای ارتقاء توانمندی‌های قضایی و امنیتی، به‌ویژه در کشورهای در حال توسعه، و طراحی استانداردهای مشترک با احترام به حقوق بشر و حاکمیت ملی، گامی مؤثر در مقابله با تهدیدهای سایبری جهانی خواهد بود.[۱۸]

در هر حال، توسعه همکاری‌های قضایی بین کشورها از طریق امضای توافق‌نامه‌ها و پروتکل‌های مشترک برای مقابله با تروریسم سایبری علیه زیرساخت‌های حیاتی ضروری است. این همکاری‌ها باید شامل تدوین چارچوب‌های حقوقی مشترک، تعریف دقیق جرایم سایبری و تضمین تعقیب بین‌المللی متخلفان باشد.[۱۹] به‌علاوه، همکاری با نهادهای بین‌المللی برای ایجاد سازوکارهای نظارتی و اجرایی می‌تواند به شکل‌گیری نظامی حقوقی، یکپارچه و هماهنگ برای مقابله جهانی با تهدیدهای سایبری کمک کند.

۲-۳. تقویت زیرساخت‌های جهانی مقابله با تروریسم سایبری؛ تحقیقات، پاسخگویی و آموزش

تروریسم سایبری به‌عنوان تهدیدی جهانی، ابعاد پیچیده‌ای در زمینه‌های حقوقی، بین‌المللی و امنیتی دارد که مقابله مؤثر با آن نیازمند ایجاد پاسخگویی حقوقی هماهنگ و تقویت همکاری‌های بین‌المللی است. در این راستا، تحقیقات علمی در حوزه امنیت سایبری نقش محوری

---

[14] Stimson Center. (2024, August 8). Strengthening global cyber resilience through UN Security Council initiatives: Paving the way for the United Nations Security Council to uphold global cyber peace and security. Cyber Security in the UN Security Council Project. https://www.stimson.org/2024/strengthening-global-cyber-resilience-through-un-security-council-initiatives/

[15] https://www.unodc.org/e4j/fr/cybercrime/module-8/key-issues/international-cooperation-on-cybersecurity-matters.html

[16] https://www.eucybernet.eu/wp-content/uploads/2020/08/2018-operational-guidance-for-the-eus-international-cooperation-on-cyber-capacity-building.pdf

[17] https://www.interface-eu.org/publications/navigating-the-eu-cybersecurity-policy-ecosystem

[18] https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2225521_compendium_of_good_practice_web.pdf

[19] https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unoct_law_enforecement_capabilities_web.pdf

در شناسایی تهدیدهای نوظهور و فناوری‌های پیشرفته‌ای چون هوش مصنوعی و یادگیری ماشین ایفا می‌کند (Jimmy, 2024, p. 942-943). تحقیقات باید در چارچوب‌های قانونی و با رعایت دقیق اسناد بین‌المللی مربوط به حفاظت از داده‌ها و حریم خصوصی انجام شود. همکاری‌های بین‌المللی، به‌ویژه در کشورهای در حال توسعه، باید برای تحقیق و تبادل اطلاعات علمی تسهیل گردد تا در پیشگیری از تروریسم سایبری مؤثر واقع شود. این تحولات ضرورت بازتعریف مفاهیم امنیتی در چارچوب عرف بین‌المللی و تصمیمات سازمان‌های بین‌المللی را ایجاب می‌کند. درضمن، دولت‌ها باید راهبردهای ملی برای بهره‌برداری از فضای سایبری و هوش مصنوعی و کاهش تهدیدات آن تدوین کنند(خاکزادشاهاندشتی؛ میربد، ۱۴۰۳، ص ۱۷۹).

یکی از مهم‌ترین چالش‌ها در مقابله با تروریسم سایبری، فقدان چارچوب حقوقی واحد و هماهنگ برای تعقیب و رسیدگی به جرایم سایبری در سطح بین‌المللی است. برای این منظور، توسعه سازوکارهای قضایی جهانی ضروری است تا همکاری‌های بین‌المللی تسهیل شده و مسئولیت‌های قضائی در تعقیب مرتکبان جرایم سایبری به‌طور شفاف مشخص گردد. در این راستا، دیوان و نهادهایی مانند اینترپل می‌توانند نقش مؤثری در تبادل اطلاعات و هماهنگی قضایی ایفا کنند، مشروط بر اینکه این همکاری‌ها با احترام به حاکمیت ملی و حقوق بشر انجام شود(Ilchyshyn; Brusakova; Krykun; Myroshnychenko, 2023, p. 767). در ضمن، آموزش در زمینه امنیت سایبری به‌عنوان یکی از ارکان اساسی در قبال تهدیدهای سایبری به‌شمار می‌رود. از منظر حقوقی، کشورها موظف به ارائه آموزش‌های تخصصی در زمینه امنیت سایبری به تمامی اقشار جامعه هستند. این آموزش‌ها باید شامل متخصصان، کارکنان دولتی و عموم مردم باشد و به‌ویژه در کشورهای در حال توسعه که ممکن است از منابع فنی کمتری برخوردار باشند، باید با اولویت بیشتری تعقیب شود(Nasir, 2023, p. 154-155). در این راستا، تضمین دسترسی به آموزش‌های سایبری و حفاظت از اطلاعات شخصی و امنیت زیرساخت‌های حیاتی باید به‌عنوان اولویتی حقوقی در نظر گرفته شود.[20]

توسعه همکاری‌های بین‌المللی و ایجاد مقررات مشترک برای تقویت امنیت سایبری امری ضروری است. این همکاری‌ها باید شامل تعریف دقیق جرایم سایبری، تقویت ظرفیت‌های فنی کشورهای در حال توسعه و ایجاد سازوکارهای اجرائی برای تعقیب مرتکبان باشد. در ضمن، سیاست‌های اجرایی باید در چارچوب اصول حقوقی و اخلاقی انجام شوند تا از نقض حاکمیت ملی و حقوق فردی پیشگیری کرده و امکان مقابله مؤثر با تهدیدهای سایبری فراهم شود.[21]

۳. ضرورت توسعه صلاحیت دیوان در جرم‌انگاری تروریسم سایبری علیه زیرساخت‌های حیاتی

جرم‌انگاری تروریسم سایبری علیه زیرساخت‌های حیاتی به دلیل پیشرفت فناوری‌های دیجیتال و تهدیدهای نوین، اهمیت یافته است. حملات سایبری به این زیرساخت‌ها می‌تواند تهدیدی جدی برای امنیت ملی و بین‌المللی باشد. جرم‌انگاری تروریسم سایبری به‌عنوان ابزاری بازدارنده، امکان پیشگیری از بحران‌ها را فراهم می‌آورد و به مقابله مؤثر با این چالش جهانی کمک می‌کند (Hui; Kim; Wang, 2107, p. 514-515). این تهدیدها می‌توانند نقض حقوق بشر از جمله امنیت، حریم خصوصی و سلامت را به دنبال داشته باشند. البته، فقدان چارچوب قانونی جامع، ضرورت جرم‌انگاری تروریسم سایبری را بیشتر می‌کند(Perloff-Gilest, 2018: 195-196).

---

20 https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2020/RDF2020/Post%20Forum%20Day%203/CII-Whitepaper-WK.pdf

21 https://unidir.org/files/publication/pdfs/the-role-of-regional-organizations-in-strengthening-cybersecurity-and-stability-experiences-and-opportunities-en-789.pdf

حملات سایبری به زیرساخت‌های حیاتی، پیامدهای انسانی، اقتصادی و اجتماعی گسترده‌ای دارند و می‌توانند حقوق بشر را نقض کنند. به همین دلیل، جرم‌انگاری تروریسم سایبری و قرار دادن آن تحت صلاحیت دیوان ضروری است. این اقدام نه‌تنها جنبه‌ای بازدارنده دارد، بلکه زمینه‌ساز تقویت همکاری‌های بین‌المللی و حفاظت مؤثر از حقوق بشر در قبال تهدیدهای سایبری خواهد بود (Watney, 2022, p. 321). استفاده تروریست‌ها از فضای سایبری برای سازمان‌دهی حملات، جذب نیرو و تأمین مالی، تهدیدهای فرامرزی را تشدید کرده و نیاز به همکاری بین‌المللی را ضروری می‌سازد. بنابراین، درج تروریسم سایبری به‌عنوان جرم مستقل در صلاحیت دیوان برای پیشگیری، تعقیب و رسیدگی به این جرایم ضروری است. بازنگری در اساس‌نامه دیوان و گسترش صلاحیت آن در قبال تروریسم سایبری علیه زیرساخت‌های حیاتی، اقدامی ضروری در راستای حفظ صلح، امنیت جهانی و حمایت از حقوق بشر است (Edwards, 2023, p. 1).

حملات سایبری علیه غیرنظامیان، اعم از شرایط جنگی و غیرجنگی، دارای آثار حقوقی قابل ملاحظه‌ای در چارچوب حقوق بین‌المللی بشردوستانه و حقوق بشر است. در شرایط جنگی، این نوع حملات می‌تواند مصداق «جنایات جنگی» تلقی شده و ناقض اصول اساسی چون تفکیک، تناسب و احتیاط باشد؛ بنابراین، مرتکبان آن مشمول تعقیب و مجازات در دیوان خواهند بود (Gervais, 2012, p. 73-75). در شرایط غیرجنگی، حملات سایبری ممکن است منجر به نقض شدید حقوق بشر، از جمله حق بر حریم خصوصی، امنیت فردی و سلامت عمومی شود.[۲۲] در ضمن، جرایم بین‌المللی در حوزه‌های حقوق بشر و حقوق بشردوستانه نقض موازین بین‌المللی را به همراه دارند که تهدیدی برای صلح و امنیت بین‌المللی سایبری به‌شمار می‌روند. این تهدیدها می‌توانند به جنایت جنگی سایبری و جنایت علیه بشریت سایبری منجر شوند. وفق مادۀ ۷ اساس‌نامه دیوان، نقض حقوق بشردوستانه در فضای سایبری می‌تواند منجر به جنایت علیه بشریت شود. به‌علاوه، مطابق مادۀ ۸ اساس‌نامه، نقض حقوق بشر در فضای سایبری ممکن است جنایت جنگی را در بر داشته باشد. با توجه به مسئولیت کیفری فردی در مادۀ ۲۳ اساس‌نامه، رسیدگی به این جنایات بدون مصونیت و در دیوان ممکن است(محقق‌هرچقان؛ اردبیلی؛ بیگ‌زاده، ۱۴۰۲، ص ۳۰۳).

با توجه به فقدان چارچوب حقوقی جامع برای مقابله با جرایم سایبری، به‌ویژه در حوزه تهاجم به زیرساخت‌های حیاتی، و با در نظر گرفتن ماهیت پیچیده و فرامرزی این جرایم، نیاز به تدوین و روزآمدسازی مقررات بین‌المللی بیشتر از همیشه احساس می‌شود. توسعه صلاحیت دیوان برای شامل کردن تروریسم سایبری، به‌ویژه علیه زیرساخت‌های حیاتی، می‌تواند به تقویت نظام عدالت کیفری بین‌المللی، ارتقاء همکاری‌های فراملی، افزایش بازدارندگی و تضمین تعقیب مؤثر مرتکبان این جرایم کمک کند (Arnell; Faturoti, 2023, p. 45). بنابراین، در پاسخ به تهدیدهای سایبری، «اعلامیه ۲۰۱۸ ژنو برای فضای سایبری»[۲۳] به منظور تنظیم رفتار کشورها و بازیگران غیر دولتی در سطح بین‌المللی صادر شد. اهداف آن شامل تعیین اصول امنیت سایبری جهانی، مقابله با تهدیدهای سایبری، ارتقای همکاری‌های بین‌المللی، حمایت از حقوق بشر و توسعه مقررات حقوقی در فضای سایبری است. این اعلامیه، اگرچه غیرالزام‌آور است، اما به عنوان یک مرجع اخلاقی و حقوقی می‌تواند به تقویت همکاری‌های بین‌المللی و پیشبرد امنیت سایبری کمک کند و بر حفظ حقوق بشر در فضای سایبری تاکید دارد.[۲۴]

[22] http://www.diva-portal.org/smash/get/diva2:1864503/FULLTEXT02.pdf
[23] Schjolberg, S. (2018, March 20). A Geneva Declaration for Cyberspace. Presentation at the WSIS Forum 2018, Geneva. Moderated High-Level Policy Session 7 - Building confidence and security in the use of ICTs. Retrieved from https://www.cybercrimelaw.net/documents/Presentation1.pdf
[24] https://www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/

به‌علاوه، دفتر دادستانی دیوان در تاریخ ششم مارس ۲۰۲۵، پیش‌نویس سندی را تحت عنوان «سیاست دیوان کیفری بین‌المللی در خصوص جرایم سایبری»[۲۵] ارائه کرد که به تحلیل اقدامات دادستانی دیوان در مواجهه با جرایم سایبری می‌پردازد.[۲۶] وفق این سند پیش‌نویس، جرایم سایبری می‌توانند از طریق ابزارهای سایبری ارتکاب یابند یا تسهیل شوند، حتی اگر به‌طور مستقیم در حوزه قضایی دیوان قرار نگیرند.[۲۷] علاوه بر این، سیاست مذکور بر اهمیت تعقیب دقیق و مؤثر جرایم سایبری در چارچوب صلاحیت دیوان تأکید کرده و تلاش دارد تا تطابق آن با تحولات فناوری را تضمین کند.[۲۸] این سند پیش‌نویس بر لزوم همکاری با کشورهای مختلف و تقویت تلاش‌های ملی در راستای مقابله با جرایم سایبری تأکید دارد و همکاری با سازمان‌های غیردولتی و شرکت‌های فعال در حوزه امنیت سایبری را ضروری می‌شمارد.[۲۹] دیوان در نظر دارد با تکیه بر چارچوب این سند پیش‌نویس، رویه قضایی بین‌المللی را توسعه داده و بهترین شیوه‌ها در تعقیب جرایم سایبری را معرفی کند.[۳۰] بنابراین، این سند پیش‌نویس بر اهمیت توجه به جرایم سایبری از منظر فنی و حقوقی تأکید دارد و هدف آن ایجاد یک چارچوب حقوقی جامع و کارآمد در قبال تهدیدهای سایبری در سطح جهانی است(Trahan, 2025, p. 80).

٤. ظرفیت کنوانسیون سازمان ملل متحد علیه جرایم سایبری در تقویت صلاحیت قضائی دیوان

تروریسم سایبری به‌عنوان تهدیدی پیچیده، نیازمند تقویت سازوکارهای قانونی و قضایی است. کنوانسیون سازمان ملل متحد علیه جرایم سایبری با هدف جرم‌انگاری و استانداردسازی مقررات، می‌تواند چارچوبی مؤثر برای پیشگیری، رسیدگی و همکاری بین‌المللی در مقابله با این جرایم فراهم کند.[۳۱]

دیوان می‌تواند نقش اساسی در مقابله با تروریسم سایبری ایفا کند، هرچند که صلاحیت آن در حال حاضر محدود به جرایم جنگی و جنایات ضد بشری است. توسعه صلاحیت این دیوان برای رسیدگی به جرایم سایبری، به‌ویژه تروریسم سایبری، امری ضروری است، هرچند چالش‌هایی همچون مسائل حاکمیت ملی و حفاظت از حریم خصوصی باید مد نظر قرار گیرد (Buçaj; Idrizaj, 2024, p. 3-5). توسعه صلاحیت دیوان می‌تواند همکاری‌های بین‌المللی را تقویت کرده و به اجرای اسناد جهانی کمک کند. برای مقابله مؤثر با تروریسم سایبری، تقویت کنوانسیون سازمان ملل متحد و گسترش صلاحیت دیوان در این حوزه ضروری است، مشروط بر اینکه اصول حاکمیت ملی و حقوق بشر رعایت شود.

---

[25] Office of the Prosecutor ICC. (2025, March 6). Draft policy on cyber-enabled crimes under the Rome Statute. International Criminal Court. https://www.icc-cpi.int/sites/default/files/2025-03/250306-OTP-Policy-on-Cyber-Enabled-Crimes-for-public-consultation.pdf

[26] International Criminal Court. (2025, March 7). ICC Office of the Prosecutor launches public consultation on policy on cyber-enabled crimes under the Rome Statute. The International Criminal Court. https://www.icc-cpi.int/about/the-court

[۲۷] این سند پیش‌نویس، نحوه استفاده دفتر از اختیارات خود در راستای تحقیق و تعقیب جرایم سایبری در حوزه قضایی دیوان را تعیین می‌نماید. هدف آن حمایت از تلاش‌های ملی در قبال بهره‌گیری غیرقانونی و مضر از فضای مجازی است. افزون بر این، به جرایم سایبری مرتبط با تجاوز، نسل‌کشی، جرایم علیه بشریت و جرایم جنگی می‌پردازد و مشتمل بر جنایات علیه عدالت، نظیر ارعاب شاهدان یا دستکاری شواهد دیجیتال می‌شود. به‌علاوه، به نقش ابزارهای سایبری در تسهیل ارتکاب این جرایم و مسئولیت‌های فرعی مرتبط با آن‌ها وفق اساسنامه دیوان اشاره می‌کند؛

- The Indian Society of International Law. (2025). Newsletter, Vol. 24, No. 1, January-March 2025. https://www.isil-aca.org/newsletter/2025/Newsletter-Jan-March-2025-Vol-24-No1.pdf

[28] https://www.ejiltalk.org/icc-office-of-the-prosecutor-releases-draft-policy-on-cyber-enabled-crimes/

[29] https://www.ejiltalk.org/two-weeks-in-review-24-march-6-april-2025/

[۳۰] برای مطالعه بیشتر راجع‌به این مسأله (نک: محقق‌هرچقان، اردبیلی؛ مهدوی‌ثابت، ۱۴۰۴، ص ۶۷-۶۴).

[31] United Nations Office on Drugs and Crime. (2024, December 24). UN General Assembly adopts landmark convention on cybercrime. https://www.unodc.org/unodc/en/press/releases/2024/December/un-general-assembly-adopts-landmark-convention-on-cybercrime.html

٤-١. کنوانسیون سازمان ملل متحد علیه جرایم سایبری؛ رویکردها، دستاوردها و چشم‌انداز

کنوانسیون سازمان ملل متحد در خصوص جرایم سایبری، در تاریخ ۲۴ دسامبر ۲۰۲۴، پس از پنج سال مذاکرات فشرده، با اجماع تمامی ۱۹۳ کشور عضو مجمع عمومی با هدف تقویت همکاری بین‌المللی در مبارزه با جرایم ارتکابی از طریق فناوری‌های اطلاعات و ارتباطات و تسهیل اشتراک‌گذاری شواهد الکترونیکی جرایم جدی با ۶۸ ماده و (*یادداشت‌های تفسیری راجع‌به مواد ۲، ۱۷، ۲۳ و ۳۵ کنوانسیون سازمان ملل متحد علیه جرایم سایبری برای تقویت همکاری بین‌المللی برای مبارزه با برخی جرایم ارتکابی از طریق سامانه‌های فناوری اطلاعات و ارتباطات و برای به اشتراک گذاشتن شواهد الکترونیکی جرایم جدی*) وفق قطعنامه‌های مجمع عمومی شماره (۲۰۱۹)۲۴۷/۷۴[۳۲] و (۲۰۲۱)۲۸۲/۷۵[۳۳] مورخ ۲۶ مه ۲۰۲۱، به تصویب رسید.[۳۴] این معاهده الزام‌آور، از سال ۲۰۲۵ برای امضا در شهر «هانوی»[۳۵] گشوده خواهد شد و نود روز پس از تصویب توسط حداقل چهل کشور، لازم‌الاجرا خواهد گردید.[۳۶] این کنوانسیون، بر تقویت همکاری‌های بین‌المللی در قبال جرایم سایبری نظیر دسترسی غیرمجاز به داده‌ها، کلاهبرداری‌های رایانه‌ای، و تهدیدها علیه زیرساخت‌های حیاتی و تبادل اطلاعات، حمایت از بزه‌دیدگان و رعایت موازین حقوق بشر در فضای دیجیتال تأکید دارد (De Silva De Alwis, 2025, p. 32).

مواد ۷ تا ۱۷ این کنوانسیون به جرم‌انگاری رفتارها و تبیین عناصر تشکیل‌دهنده جرایم سایبری و برخی مصادیق آن اختصاص یافته است. جرایم مقرر در مواد ۷ تا ۱۱، با الهام از مقررات کنوانسیون بوداپست، ناظر بر جرایم سایبری می‌باشند. به‌علاوه، مواد ۱۲ تا ۱۶ نیز با اقتباس از همان کنوانسیون، به سایر اشکال جرایم مرتبط با فضای سایبری می‌پردازند.[۳۷] بنابراین، در چارچوب این کنوانسیون، اصطلاح «جرایم سایبری» به اقداماتی اطلاق می‌گردد که از طریق شبکه‌های رایانه‌ای یا اینترنت به‌منظور ارتکاب جرم انجام می‌شوند، که از جمله آن‌ها می‌توان به حملات علیه داده‌ها، سامانه‌های اطلاعاتی یا نرم‌افزارهای حیاتی اشاره نمود. این نوع جرایم، به دلیل ماهیت فراملی و ناشناس بودن عاملان آن، چالش‌های جدی در تعقیب و رسیدگی قضایی ایجاد می‌کنند(Fahmy, 2024, p. 33).

یکی از مهم‌ترین چالش‌ها در مقابله با تروریسم سایبری، فقدان تعاریف دقیق، شفاف و هماهنگ در سطح بین‌المللی است که می‌تواند موجب تعارض در صلاحیت و اختلال در فرآیند تعقیب کیفری گردد. از اینرو، کنوانسیون وفق ماده ۳۵، کشورهای عضو را موظف

---

[32] https://docs.un.org/en/A/RES/74/247

[33] https://docs.un.org/en/A/RES/75/282

[34] United Nations General Assembly. (2024, December 24). Resolution adopted by the General Assembly on the report of the Third Committee (A/79/460, para. 15): 79/243. United Nations Convention against Cybercrime; Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes. https://docs.un.org/en/A/RES/79/243

[35] Hanoi

[۳۶] این کنوانسیون، که نخستین کنوانسیون جهانی در زمینه عدالت کیفری پس از بیش از بیست سال به شمار می‌رود، به‌عنوان نقطه عطفی در تلاش‌های بین‌المللی برای پیشگیری از جرایم سایبری و ارتقای همکاری‌های چندجانبه در این زمینه شناخته می‌شود. شهر هانوی پایتخت ویتنام مسئولیت میزبانی مراسم امضای کنوانسیون را در ژوئیه ۲۰۲۵ بر عهده داشت. کنوانسیون، بستری مناسب برای تقویت همکاری‌های حقوقی بین‌المللی، ظرفیت‌سازی و ایجاد فضای دیجیتال امن فراهم می‌آورد تا مجرمان در مقابل اقدام‌های خود پاسخ‌گو باشند؛

- United Nations Office on Drugs and Crime. (2025, February 19). The Road to Hanoi: Opening for signature of the UN Convention against Cybercrime. Conference Room 8, UNHQ. https://unodaweb-meetings.unoda.org/public/2025-02/Concept%20note%20The%20Road%20to%20HN%20-%20OEWG.pdf

[37] https://tokyo.mid.ru/en/novosti_posolstva/article_the_first_global_treaty_against_cybercrime_from_geopolitical_confrontation_towards_professio/

می‌سازد در چارچوب تحقیق، تعقیب کیفری، جمع‌آوری و تبادل ادله الکترونیکی مرتبط با جرایم تعریف‌شده در این کنوانسیون، همکاری‌های بین‌المللی مؤثر داشته باشند.[۳۸] در این راستا، کنوانسیون ظرفیت ایجاد یک چارچوب قانونی یکپارچه برای مقابله با تروریسم سایبری را داراست و می‌تواند موجب تقویت صلاحیت دیوان در رسیدگی به این جرایم شود. تمرکز ویژه کنوانسیون بر تهدیدها علیه زیرساخت‌های حیاتی، گامی مؤثر در راستای تأمین امنیت سایبری جهانی تلقی می‌گردد(Tropina, 2024, p. 207). از اینرو، یکی از موانع جدی در مسیر اجرای مؤثر این کنوانسیون، محدودیت‌های صلاحیتی در تعقیب کیفری مرتکبان جرایم سایبری است. این جرایم اغلب از سوی افرادی صورت می‌گیرند که در حوزه قضایی کشورهایی قرار دارند که یا به کنوانسیون ملحق نشده‌اند یا همکاری قضایی لازم را ارائه نمی‌دهند(Rakha, 2024, p. 376). این امر، نیازمند توسعه سازوکارهای حقوقی برای همکاری قضایی فراملی و اجرای مؤثر کنوانسیون در سطح جهانی است.

از جمله مزایای شاخص این کنوانسیون مواد ۳۷ تا ۴۰ است که امکان تقویت همکاری‌های بین‌المللی در حوزه تبادل اطلاعات، هماهنگی قضایی و ارتقای زیرساخت‌های امنیتی برای پیشگیری از حملات سایبری را فراهم می‌سازد. کشورها می‌توانند با بهره‌گیری از مفاد کنوانسیون، مقررات ملی خود را روزآمدسازی کرده و با ایجاد هماهنگی و همگرایی در مقررات مربوط به جرایم سایبری، شکاف‌های قانونی و تضادهای حقوقی موجود را برطرف نمایند(Fidler, 2025, p. 784). افزون بر این، برنامه‌های آموزشی، انتقال دانش فنی و تقویت ظرفیت‌های قضایی، می‌توانند بستر مناسبی برای مقابله مؤثر با تهدیدهای پیچیده‌ای همچون تروریسم سایبری فراهم آورند.

به‌طور کلی، این کنوانسیون می‌تواند ابزاری کارآمد برای مقابله با تهدیدهای فزاینده سایبری، به‌ویژه تروریسم سایبری علیه زیرساخت‌های حیاتی، محسوب شود. با این حال، تحقق اهداف آن منوط به تقویت همکاری‌های بین‌المللی، رفع موانع صلاحیتی، توسعه سازوکارهای نظارتی و تسهیل فرآیندهای شناسایی و پیگرد کیفری مرتکبان خواهد بود(Hakmeh, 2024, p. 127).

٤-۲. ضرورت‌ها و فرصت‌های توسعه صلاحیت قضایی دیوان

تروریسم سایبری با ویژگی‌هایی مانند سازمان‌یافتگی، اهداف سیاسی و حمله به غیرنظامیان یا زیرساخت‌های عمومی، قابلیت شناسایی به‌عنوان جرم بین‌المللی مستقل را دارد. در صورت وقوع خسارات عمده، این جرایم می‌توانند در چارچوب صلاحیت دیوان قرار گیرند. حملات به زیرساخت‌های حیاتی، مطابق با کنوانسیون‌های چهارگانه ژنو، نقض جدی تعهدات بین‌المللی هستند. بنابراین، جرم‌انگاری تروریسم سایبری و درج آن در صلاحیت دیوان برای ایجاد بازدارندگی و پاسخ‌گذاری مؤثر، امری ضروری است (Stockton; Golabek-Goldman, 2014, p. 234-236).

وفق مواد ۲۵ و ۲۸ اساس‌نامه دیوان، افراد در قبال ارتکاب جنایات بین‌المللی، دارای مسئولیت کیفری فردی هستند. در حوزه تروریسم سایبری، مسئولیت فرماندهی جایگاه ویژه‌ای دارد؛ به‌گونه‌ای که فرماندهان و اشخاص دارای اختیار، در صورت اطلاع از وقوع جرم و عدم اقدام برای پیشگیری یا مجازات آن، قابل تعقیب خواهند بود(Shulzhenko; Romashkin, 2021, p. 76-77). با توجه به پیچیدگی‌های فنی این جرایم، بهره‌گیری از ابزارهای دیجیتال برای شناسایی مرتکبان، امری ضروری است. در همین راستا، پیشنهاد ایجاد پایگاه داده تخصصی در دیوان و همکاری فعال با نهادهای بین‌المللی نظیر اینترپل، می‌تواند موجب ارتقای کارآمدی در تعقیب این جرایم شود.

هماهنگ‌سازی مقررات داخلی با اسناد بین‌المللی، از جمله کنوانسیون بوداپست و قطعنامه ۲۳۴۱ شورای امنیت، زمینه‌ساز جرم‌انگاری و پیگرد ملی این جرایم خواهد بود. در صورت ناتوانی دولت‌ها در رسیدگی مؤثر، امکان ارجاع پرونده به دیوان وجود دارد. درضمن،

[38] https://www.eumonitor.eu/9353000/1/j4nvhdfdk3hydzq_j9vvik7m1c3gyxp/vmp4el2lb0y6

تقویت نهادهایی مانند اینترپل و یوروپل به‌عنوان سازوکارهای مکمل، و تصویب ماده‌ای مستقل در خصوص تروریسم سایبری، می‌تواند بستر همکاری‌های قضایی و تقویت ادله کیفری در سطح بین‌المللی را فراهم آورد(Kovalčík, 2024, p. 61). از اینرو، با توجه به شکاف موجود در اساس‌نامه دیوان نسبت به جرایم سایبری، به‌ویژه تروریسم سایبری، توسعه صلاحیت دیوان مستلزم الحاق ماده‌ای مستقل در این خصوص و نیز هماهنگی اقدامات داخلی و بین‌المللی است(Wang, 2024, p. 17). این اقدام، گامی مؤثر در جهت ایجاد چارچوب نوین عدالت کیفری بین‌المللی در عصر دیجیتال تلقی می‌شود و می‌تواند پاسخ مناسبی به تهدیدات فزاینده علیه زیرساخت‌های حیاتی باشد. از اینرو، پیشنهاد می‌شود که تروریسم سایبری به‌عنوان جرم مستقل بین‌المللی در اساس‌نامه دیوان درج شود. این جرم شامل حملات سایبری سازمان‌یافته با اهداف ایجاد رعب، تضعیف حکومت‌ها یا آسیب به زیرساخت‌های حیاتی، و با انگیزه‌های سیاسی یا اعتقادی است. مصادیقی چون حمله به داده‌ها، تخریب منابع عمومی و دسترسی غیرمجاز از ویژگی‌های این جرم به شمار می‌روند. شناسایی این جرم در چارچوب اساس‌نامه دیوان، موجب تقویت بازدارندگی، ارتقای همکاری بین‌المللی، و توسعه پاسخ‌گذاری کیفری در فضای دیجیتال خواهد شد(Macidov, 2023, p. 91).

با وجود این، با بهره‌گیری از تعاریف موجود در اسناد بین‌المللی نظیر کنوانسیون بوداپست، قطعنامه‌های شورای امنیت (نظیر قطعنامه ۲۳۴۱) و پروتکل‌های الحاقی به کنوانسیون ژنو، می‌توان با الگوگیری از ساختار مواد ۷ و ۸ اساس‌نامه، در قالب ماده مستقل، پیش‌نویس ماده جدید در قالب پیوست الحاقی تحت عنوان «جرایم نوظهور [*تروریسم سایبری*]»، برای الحاق به اساس‌نامه دیوان تحت عنوان «تروریسم سایبری» را پیشنهاد داد(Shackelford, 2020, p. 147).[۳۹] بنابراین، ماده پیشنهادی، با در نظر گرفتن اصول بنیادین حقوق بین‌المللی کیفری و تحولات فناوری اطلاعات، می‌تواند گامی اساسی در جهت ارتقای پاسخ‌گذاری بین‌المللی، حمایت از غیرنظامیان و حفاظت از زیرساخت‌های حیاتی در قبال تهدیدهای نوین سایبری محسوب شود.

با این حال، افزون بر توسعه صلاحیت دیوان، برخی از صاحب‌نظران تأسیس محکمه‌ای موسوم به «دیوان کیفری بین‌المللی برای رسیدگی به جرایم سایبری» را پیشنهاد کرده‌اند که با توجه به بی‌کیفری فزاینده، ضرورت رسیدگی به جدی‌ترین حملات سایبری را فراهم می‌سازد. این صاحب‌نظران معتقدند که این دیوان باید مستقل از سازمان ملل متحد عمل کند و برای مقابله با بی‌کیفری جرایم بزرگ بین‌المللی قابلیت تأسیس داشته باشد. صلاحیت آن محدود به جرایم خاص مانند نسل‌کشی و جرایم جنگی است، اما ممکن است در قبال حملات سایبری گسترده علیه زیرساخت‌های اطلاعاتی حیاتی نیز نقش ایفا کند(Schjolberg, 2012, p. 15).

---

[۳۹] پیش‌نویس ماده جدید برای الحاق به اساس‌نامه به‌عنوان ماده ۸ مکرر تحت عنوان «تروریسم سایبری»، بدین شرح می‌توان پیشنهاد نمود: «برای اهداف این اساس‌نامه، «تروریسم سایبری» به هرگونه اقدام عمدی و سازمان‌یافته اطلاق می‌شود که از طریق فناوری‌های اطلاعاتی و ارتباطی انجام شده و دارای کلیه ویژگی‌های نظیر الف) با قصد ایجاد ترس، وحشت یا بی‌ثباتی در میان جمعیت غیرنظامی؛ ب) با هدف تحمیل دیدگاه‌های سیاسی، مذهبی یا اعتقادی، تأثیرگذاری بر تصمیم‌های سیاسی دولت‌ها یا نهادهای بین‌المللی، یا ایجاد اختلال عمده در نظم عمومی؛ ج) از طریق حمله به زیرساخت‌های حیاتی، سامانه‌های اطلاعاتی، خدمات عمومی، داده‌های حساس یا مراکز حیاتی درمانی، مالی، انرژی، ارتباطات، حمل‌ونقل یا امنیتی؛ د) به‌گونه‌ای که منجر به یکی از نتایج زیر گردد: مرگ یا آسیب شدید بدنی به افراد؛ وارد آمدن خسارات جدی و گسترده به اموال یا محیط زیست؛ ایجاد اختلال اساسی در خدمات عمومی یا اقتصادی؛ ایجاد بی‌ثباتی یا تهدید امنیت ملی یا بین‌المللی، باشد. ارتکاب یا مشارکت در هر یک از اعمال فوق، در صورتی که در چارچوب یک طرح یا سیاست عمومی، یا به‌صورت گسترده و سازمان‌یافته انجام گیرد، در صلاحیت دیوان کیفری بین‌المللی قرار خواهد گرفت. در تعیین مسئولیت کیفری فردی برای جرم تروریسم سایبری، دادگاه می‌تواند به موارد زیر توجه کند: الف) نقشه‌کشی، هدایت یا فرماندهی حمله؛ ب) ارائه پشتیبانی مالی، فنی یا اطلاعاتی؛ ج) مشارکت در طراحی یا اجرای نرم‌افزارها یا سامانه‌های تهاجمی سایبری؛ د) استفاده از افراد زیر سن قانونی در عملیات سایبری با هدف تروریستی. برای اعمال این ماده، کشورهای عضو متعهد به همکاری حقوقی و قضایی کامل با دیوان خواهند بود، از جمله: الف) استرداد، توقیف یا تعقیب فنی؛ ب) اشتراک‌گذاری داده‌ها و اطلاعات سایبری؛ ج) اجرای احکام کیفری صادره توسط دیوان.»

نتیجه‌گیری

تهدیدهای فزاینده تروریسم سایبری و ناتوانی چارچوب حقوق بین‌المللی کیفری در قبال آن، ضرورت بازنگری در صلاحیت دیوان را برجسته کرده است. تعریف تروریسم سایبری به‌عنوان جرم مستقل و اصلاح اساس‌نامه دیوان از جمله اقدامات مورد نیاز است. این امر مستلزم تقویت همکاری‌های قضائی، تقنینی و فنی میان دولت‌ها و سازمان‌های بین‌المللی می‌باشد. از اینرو، با توجه به تهدید فزاینده حملات سایبری در حوزه‌هایی مانند انرژی، بهداشت و حمل‌ونقل، توسعه صلاحیت دیوان در زمینه تروریسم سایبری راهبردی ضروری و هماهنگ با اهداف منشور ملل متحد و اصول عدالت کیفری بین‌المللی اطلاق می‌شود؛ راهبردی که می‌تواند نقشی مؤثر در پیشگیری از این تهدیدهای سایبری و حمایت از بزه‌دیدگان را ایفا کند. از اینرو، برای توسعه صلاحیت دیوان در زمینه جرم‌انگاری تروریسم سایبری علیه زیرساخت‌های حیاتی، سازوکارهای پیشنهادی ذیل قابل ملاحظه است:

الف- تقویت زیرساخت‌های ملی و بین‌المللی امنیت سایبری از طریق ایجاد سامانه‌های هشدار سریع، توسعه فناوری‌های پیشرفته در حوزه رمزنگاری، شناسایی نفوذ و افزایش تاب‌آوری سایبری، استانداردسازی بین‌المللی، و راه‌اندازی پایگاه‌های داده و سکوهای اطلاعاتی مشترک برای شناسایی تروریست‌های سایبری، ابزارها، روش و الگوهای آماج.

ب- اصلاح ساختار حقوقی اساس‌نامه دیوان از طریق تدوین و تصویب پیوست الحاقی تحت عنوان «جرایم نوظهور»، مشتمل بر تعریف جامع، دقیق و جهان‌شمول تروریسم سایبری با لحاظ عناصر مادی (نظیر نوع زیرساخت هدف و میزان خسارت) و معنوی (نظیر قصد ایجاد رعب یا اخلال در امنیت عمومی یا بین‌المللی)، و شناسایی آن به‌عنوان تهدیدی علیه صلح و امنیت بین‌المللی در سطحی هم‌تراز با جنایات چهارگانه مقرر در ماده ۵ اساس‌نامه دیوان؛

ج- انعقاد معاهدات دوجانبه و چندجانبه میان دولت‌ها در زمینه همکاری قضایی، استرداد متهمان، تبادل اطلاعات و معاضدت حقوقی؛ ایجاد نهاد تخصصی در چارچوب دیوان جهت رسیدگی فنی به جرایم سایبری؛ آموزش و تربیت قضات، دادستان‌ها و کارشناسان متخصص در زمینه ادله دیجیتال و چالش‌های مرتبط با زنجیره مراقبت؛ و تدوین پروتکل‌های بین‌المللی برای جمع‌آوری، تحلیل، اعتبارسنجی و پذیرش ادله دیجیتال در فرآیند دادرسی کیفری بین‌المللی.

به‌هر روی، مقابله با تروریسم سایبری به‌عنوان پدیده‌ای نوظهور، فراملی، پیچیده و فزاینده، مستلزم اتخاذ رویکردی جامع، هماهنگ و چندبعدی در سطوح حقوقی، فنی و اجرایی است. در فقدان چنین تدابیری، تحقق پاسخ کیفری مؤثر و بازدارنده از سوی دیوان در قبال این نوع جرایم با چالش‌های جدی مواجه خواهد بود.

منابع

احمدی‌مقدم، جواد؛ غلامی‌دون، حسین. (۱۳۹۸ش). تروریسم سایبری: ماهیت، روش‌ها و اقدامات متقابل. کنفرانس بین‌المللی ابعاد حقوقی-جرم‌شناختی تروریسم، گردآورندگان حسنعلی موذن‌زادگان و بهزاد رضوی‌فرد. چاپ اول، تهران: دانشگاه علامه طباطبایی.

اینارسن، ترج. (۱۴۰۲ش). مفهوم جرایم جهانی در حقوق بین‌الملل. ترجمه فریدون جعفری، چاپ اول. بروکسل(بلژیک): تورکل اوپسال.

خاکزاد شاهاندشتی، محسن؛ میربد، لیلا. (۱۴۰۳ش). خوانش نوین صلح و امنیت بین‌المللی در پرتو مبارزه با تروریسم سایبری. پژوهش‌های بین‌الملل، ۱۴(۳)، ۱۷۹-۲۰۴. https://doi.org/10.22034/irr.2024.463239.2557

روبو، دیدیه. (۱۴۰۳ش). حقوق کیفری بین‌المللی. ترجمه بهزاد رضوی‌فرد و محمد فرجی، چاپ دوم. تهران: بنیاد حقوقی میزان.

فرشاسعید، پرویز؛ جلالی، محمود؛ گودرزی، مهناز. (۱۴۰۱ش). ضرورت تقویت امنیت سایبری بخش انرژی توسط دولت‌ها. مطالعات حقوق انرژی، ۸(۱)، ۱۷۳-۱۹۳. https://doi.org/10.22059/jrels.2022.316656.413

سیدناصری، محمدمهدی؛ میربد، لیلا. (۱۴۰۳ ش). تروریسم و افراطی‌گری سایبر-تکنولوژیک؛ چالش‌های حقوقی و امنیتی برای نظام حقوق بین‌الملل. نشریه رویکردهای حقوق سیاسی، ۲(۱)، ۱۵-۲۷. https://doi.org/10.22084/qjpla.2025.30336.1008

شاملو، باقر؛ حسینی، مهدی. (۱۴۰۳ش). رایاجنگ‌های مختل‌کنندهٔ زیرساخت‌های حیاتی به‌مثابهٔ جنایت جنگی. آموزه‌های حقوق کیفری، ۲۷(۲۱)، ۱۱۵-۱۵۲. https://doi.org/10.30513/cld.2024.6134.2005

شریعت‌باقری، محمدجواد. (۱۴۰۲ ش). حقوق کیفری بین‌المللی. چاپ اول. تهران: گنج‌دانش.

کالک، ولفگانگ. (۱۴۰۳ش). معیارهای دوگانه: حقوق کیفری بین‌المللی و غرب. ترجمه فریدون جعفری و جلال‌الدین حسانی، چاپ اول. بروکسل(بلژیک): تورکل اوپسال.

محقق‌هرچقان، علیرضا؛ اردبیلی، محمدعلی؛ بیگ‌زاده، ابراهیم. (۱۴۰۲ش). صلاحیت دیوان کیفری بین‌المللی و رسیدگی به جنایات بین‌المللی سایبری در عرصه‌های حقوق بین‌الملل. پژوهش‌های حقوق جزا و جرم‌شناسی، ۱۱(۲۱)، ۳۲۷-۳۰۳. https://doi.org/10.22034/jclc.2023.389750.1827

محقق‌هرچقان، علیرضا؛ اردبیلی، محمدعلی؛ مهدوی‌ثابت، محمدعلی. (۱۴۰۴ش). دوگانه‌گرایی قضائی در جنایات سایبری بین المللی در حدود اختیارات دادستان دیوان کیفری بین المللی. پژوهش‌های حقوقی، ۲۴(۴۱)، ۹۰-۵۹. https://doi.org/10.48300/jlr.2023.388705.2304

نمامیان، پیمان. (۱۴۰۳ش). الزمات حقوقی جهانی حفاظت از امنیت زیرساخت‌های حیاتی کشورها در قبال جرایم تروریستی فناورانه. دولت و حقوق، ۵(۴)، ۴۶-۲۵. https://doi.org/10.48315/qgl.2025.494372.1167

Adenekan, T. K. (2023). Securing critical infrastructure: Strategies for resilience against global cyber threats. ResearchGate. https://www.researchgate.net/publication/385620316_Securing_Critical_Infrastructure_Strategies_for_Resilience_Against_Global_Cyber_Threats

Alabbadi, F. S., Al Amaren, E. M., & Aletein, S. I. (2020). International responsibility arising from cyberattacks in the light of the contemporary international law. International Journal of Cyber Criminology, 16(1), 156–169. https://doi.org/10.5281/zenodo.4766562

Alkharman, J. A., & Hassan, I. (2023). Cyberterrorism and self-defense in the framework of international law. Journal of Law and Sustainable Development, 11(8), e1430. https://doi.org/0009-0004-3056-9748

Arnell, P., & Faturoti, B. (2023). The prosecution of cybercrime – why transnational and extraterritorial jurisdiction should be resisted. International Review of Law, Computers & Technology, 37(1), 29-51. https://doi.org/10.1080/13600869.2022.2061888

Asghar, M. U., Javed, M. H., & Azhar, S. (2025). The regulation of cybercrime in international law: Discussing the legal frameworks and challenges in regulating cybercrime. Indus Journal of Social Sciences, 3(2), 417-430. https://doi.org/10.59075/ijss.v3i2.1267

Azmi, A. N., & Shabrina, S. (2023). Challenges of universal adoption of the Budapest Convention on cybercrime. The 5th International Conference on Technology, Education, and Social Science, 1(1), 1-10.

Bartoli, L. (2025). Cybersecurity and the fight against cybercrime: Partners or competitors? European Journal of Risk Regulation, 16(2), 498 - 513. https://doi.org/10.1017/err.2025.31

Buçaj, E., & Idrizaj, K. (2024). The need for cybercrime regulation on a global scale by the international law and cyber convention. Multidisciplinary Reviews, 8(1), 1-10. https://doi.org/10.31893/multirev.2025024

Buisman, C., & Alfatlawi, A. A. (2025). Cyber attacks under international criminal law: Challenges in investigation and prosecution. In The guide to understanding aggressive cyber-attacks: A study within an effective legal and political perspective (pp. 24–30). Zain Legal Publications. https://ssrn.com/abstract=4959031

Cristiano, F., Broeders, D., & Weggemans, D. (Eds.). (2020). Countering cyber terrorism in a time of ‘war on words’: Kryptonite for the protection of digital rights? The Hague: The Hague Program for Cyber Norms. https://scholarlypublications.universiteitleiden.nl/access/item%3A3069991/view

De Silva De Alwis, R. (2025). Gendering the new international convention on cybercrimes and new norms on artificial intelligence and emerging technologies. Washington Journal of Law, Technology & Arts, 20(2), 1-41. https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=1350&context=wjlta
Edwards, K. (2023). The ICC and the prosecution of global cyber war crimes. Denver Journal of International Law & Policy. Retrieved from https://djilp.org/the-icc-and-the-prosecution-of-global-cyber-war-crimes/
Fahmy, W. (2024). The cybercrime acts and the electronic transaction in international law. Economics Law and Policy, 7(1), 18–41. https://doi.org/10.22158/elp.v7n1p18
Fidler, D. P. (2015). Whither the Web?: International law, cybersecurity, and critical infrastructure protection. Maurer School of Law: Indiana University, 8-20. https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=3452&context=facpub
Fidler, M. (2025). Fragmentation of international cybercrime law. Utah Law Review, 3(4), 737–804. https://dc.law.utah.edu/ulr/vol2025/iss3/4/
Gervais, M. (2012). Cyber attacks and the laws of war. Journal of Law & Cyber Warfare, 1(1), 8–98. https://www.jstor.org/stable/26441233
George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber threats to critical infrastructure: Assessing vulnerabilities across key sectors. Partners Universal International Innovation Journal (PUIIJ), 2(1), 51–75. https://doi.org/10.5281/zenodo.10639463
Girard, R. N. (2023). The honeypot stings back: Entrapment in the age of cybercrime and a proposed pathway forward. Chicago Journal of International Law, 24(1), 187-223. https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1848&context=cjil
Guillaume, G. (2004). Terrorism and international law. The International and Comparative Law Quarterly, 53(3), 537–548.
Gupta, I. & Deol, P. (2025). The role of International Criminal Court (ICC) jurisdiction in prosecuting cyberterrorism. International Journal of Research Publication and Reviews, 6(5), 12491–12498. https://ijrpr.com/uploads/V6ISSUE5/IJRPR46404.pdf
Hakmeh, J. (2024). The UN convention on cybercrime: A milestone in cybercrime cooperation? Journal of Cyber Policy, 9(2), 125–130. https://doi.org/10.1080/23738871.2024.2441549
Hui, K.-L., Kim, S. H., & Wang, Q.-H. (2017). Cybercrime deterrence and international legislation. MIS Quarterly, 41(2), 497-524. https://www.jstor.org/stable/26629724
Ilchyshyn, N., Brusakova, O., Krykun, V., & Myroshnychenko, Y. (2023). International legal cooperation in the field of criminal justice: New challenges and ways to overcome them. Journal of Law and Sustainable Development, 11(4), 754-771. https://doi.org/10.55908/sdgs.v11i4.767
Jayakumar, S. (2021). Cyber attacks by terrorists and other malevolent actors: Prevention and preparedness. With three case studies on Estonia, Singapore and the United States. In A. P. Schmid (Ed.), Handbook of terrorism prevention and preparedness (pp. 871–930). ICCT Press Publication.
Jimmy, F. (2024). The role of artificial intelligence in predicting cyber threats. International Journal of Scientific Research and Management (IJSRM), 11(8), 935–953. https://doi.org/10.18535/ijsrm/v11i08.ec04
Kovalčík, M. (2024). Constitutional referrals by ordinary courts: A platform for judicial dialogue and another toolkit for judicial resistance? European Constitutional Law Review, 20(1), 52-81. https://doi.org/10.1017/S1574019624000087
Kumar, A. (2024). Examining cybersecurity laws: Protecting critical infrastructure against emerging threats and global cybercrimes. Journal of Law and Intellectual Property Rights, 1(1), 21–29. https://jlipr.in/doc/Vol-1-No-1-2024/3_JLIPR_Vol%201%20%20No%201_Dec%202024.pdf
LeChette-Danberry, C. A. (2025). Cyberterrorism and international laws: Need for cyber inclusion (PhD dissertation). Walden University, College of Health Sciences and Public Policy. https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=19456&context=dissertations
Macidov, S. T. o. (2023). Prosecuting cybercrimes under international legal frameworks: Challenges and innovations. Futurity Economics & Law, 3(3), 80-96. https://doi.org/0000-0003-3541-6893

Matos, L. (2021). Cyberattacks as crimes against humanity and international responsibility of states. SSRN. https://ssrn.com/abstract=3953744
Nasir, S. (2023). Exploring the effectiveness of cybersecurity training programs: Factors, best practices, and future directions. Advances in Multidisciplinary & Scientific Research Journal Publication, 2(1), 151–160. https://doi.org/10.22624/AIMS/CSEAN-SMART2023P18
Perloff-Gilest, A. (2018). Transnational cyber offenses: Overcoming jurisdictional challenges. The Yale Journal of International Law, 43, 191–227.
Qualters, M. M. (2023). Cyberwarfare: An international crime? Whether "cyberwarfare" is an issue that can be prosecuted before the ICC. Syracuse Law Review, 75. Retrieved from https://lawreview.syr.edu/cyberwarfare-an-international-crime-whether-cyberwarfare-is-an-issue-that-can-be-prosecuted-before-the-icc/
Rakha, N. A. (2024). Jurisdictional challenges of cybercrimes and the role of the International Criminal Court. Thematic Conference Proceedings, 14(3), 357–383. https://doi.org/10.1092/ejil/chy056
Rahman, M. M., & Das, T. K. (2024). Countering cyberattacks: Gaps in international law and prospects for overcoming them. Journal of Digital Technologies and Law, 2(4), 973–1002. https://doi.org/10.21202/jdtl.2024.46
Schjolberg, S. (2012). An international criminal tribunal for cyberspace (ICTC); Prosecution for the tribunal police investigation for the tribunal. Cybercrime Law. Retrieved from http://www.cybercrimelaw.net
Shackelford, S. J. (2020). Managing cyber attacks as a global collective action problem. In Governing new frontiers in the information age: Toward cyber peace (pp. 87-172). Cambridge University Press. https://doi.org/10.1017/9781108604000.004
Sieber, U. (2006). International cooperation against terrorist use of the internet. International Review of Penal Law, 77, 395-449. https://doi.org/10.3917/ridp.773.0395
Sim, S. (2023). The development of digital technologies and cyber security threats. Sungshin Women's University Center for East Asian Studies, 29(1), 197–238. https://doi.org/10.56022/ceas.2023.29.1.197
Snider, K. L. G., Hefetz, A., Shandler, R., & Canetti, D. (2025). Experimenting with threat: How cyberterrorism targeting critical infrastructure influences support for surveillance policies. Terrorism and Political Violence, 1–15. https://doi.org/10.1080/09546553.2025.2457746
Stockton, P. N., & Golabek-Goldman, M. (2014). Prosecuting cybertterrorists: Applying traditional jurisdictional frameworks to a modern threat. Stanford Law & Policy Review, 25(3), 211-268.
Trahan, J. (2025). Cyber operations and the crime of aggression. Case Western Reserve Journal of International Law, 57(1), 77-108. https://scholarlycommons.law.case.edu/jil/vol57/iss1/6/
Tropina, T. (2024). This is not a human rights convention: The perils of overlooking human rights in the UN cybercrime treaty. Journal of Cyber Policy, 9(2), 200–220. https://doi.org/10.1080/23738871.2024.2419517
Viganò, E., Loi, M., & Yaghmaei, E. (2020). Cybersecurity of critical infrastructure. In M. Christen, B. Gordijn, & M. Loi (Eds.), The ethics of cybersecurity (pp. 157–177). Springer Nature. https://doi.org/10.1007/978-3-030-29053-5_8
Wang, X. (2024). Global (re-)framing of cybercrime: An emerging common interest in flux of competing normative powers? Leiden Journal of International Law. First View, 1-27. https://doi.org/10.1017/S0922156524000402
Watney, M. (2022). Cybersecurity threats to and cyberattacks on critical infrastructure: A legal perspective. European Conference on Cyber Warfare and Security, 21(1), 319–327. https://doi.org/10.34190/eccws.21.1.196
Ya, A. (2023). Employing the responsibility to protect (R2P) to impose universal jurisdiction regarding cyber-terrorism. Journal of Digital Technologies and Law, 1(4), 994–1027. https://doi.org/10.21202/jdtl.2023.43