Criminal Law Doctrines of Islamic Countries
Online ISSN:3041-9964
https://diplic.qom.ac.ir

Countering Destructive and Disruptive Cyberwars Targeting Energy Infrastructure Security in International Documents; A Comparative Analysis of the Regulations of Iran and Qatar

Peyman Namamian[1]

1. Associate Professor of Criminal Law and Criminology, Faculty of Administrative Sciences and Economics, Arak University, Iran, Arak, Email: p_namamian1512@yahoo.com

Abstract

Energy infrastructures, as vital sectors of every country, are exposed to risks posed by destructive and disruptive cyberwars, such as data breaches, control system destruction, and attacks on distribution networks, with the spread of virtual technologies, which have consequences for national and economic security. Effectively combating these crimes requires the establishment of up-to-date legal frameworks, strengthening security and educational measures and utilizing international documents. However, achieving this goal necessitates extensive international cooperation and alignment of these documents' principles with the domestic legal structures of countries. In this regard, some countries, particularly Iran and Qatar, are striving to manage the response to destructive and disruptive cyberwars targeting energy infrastructure through the creation of legal and executive frameworks. In this context, Iran emphasizes national regulations and internal synergy, while Qatar prioritizes international cooperation and adherence to global standards, alongside specific institutions. Therefore, to achieve effective protection of energy infrastructures against cyberwars, adopting legal policies in coordination with international documents and strengthening internal executive capacities is an undeniable necessity.

Keywords: destructive and disruptive cyberwars, cybersecurity, energy security, energy infrastructure, international cooperation.

Received: 2/07/2025 **Revised: 05/08/2025** **Accepted: 15/09/2025**

How To Cite: Namamian, Peyman (2025). Countering Destructive and Disruptive Cyberwars Targeting Energy Infrastructure Security in International Documents; A Comparative Analysis of the Regulations of Iran and Qatar, *Criminal Law Doctrines of Islamic Countries, 2 (4), 148-177.* http://www.doi.org/10.22091/dclic.2025.13272.1092

Published by: University of Qom **Article type**: Research

آموزه‌های حقوق کیفری کشورهای اسلامی
https://diplic.qom.ac.ir
شاپا الکترونیکی: ۹۹۶۴-۳۰۴۱

مقابله با رایاجنگ‌های تخریبگر و مختل‌کنندهٔ امنیتِ زیرساخت‌های انرژی در اسناد بین‌المللی؛ با تحلیل تطبیقی مقررات ایران و قطر

پیمان نمامیان[1]

۱. دانشیار حقوق کیفری و جرم‌شناسی، دانشکده علوم اداری و اقتصاد دانشگاه اراک، ایران، اراک، رایانامه: p_namamian1512@yahoo.com

چکیده

زیرساخت‌های انرژی، به‌عنوان بخش‌های حیاتی هر کشور با گسترش فناوری‌های مجازی در معرض مخاطره‌های ناشی از رایاجنگ‌های تخریبگر و مختل‌کننده نظیر نفوذ به داده‌ها، تخریب سامانه‌های کنترل و حمله به شبکه‌های توزیع قرار گرفته‌اند که پیامدهایی برای امنیت ملی و اقتصادی دارند. مقابله مؤثر با این جرائم نیازمند ایجاد چارچوب‌های قانونی به‌روز، تقویت اقدامات امنیتی و آموزشی و بهره‌گیری از اسناد بین‌المللی است. بااین‌حال، تحقق این هدف مستلزم همکاری بین‌المللی گسترده و انطباق اصول این اسناد با ساختارهای حقوقی داخلی کشورهاست. در این راستا، برخی کشورها به‌ویژه ایران و قطر در تلاش هستند تا با ایجاد چارچوب‌های قانونی و اجرایی، مقابله با رایاجنگ‌های تخریبگر و مختل‌کننده امنیتِ زیرساخت‌های انرژی را مدیریت کنند. وفق این امر، ایران بیشتر بر مقررات ملی و هم‌افزایی داخلی تأکید دارد، درحالی‌که قطر علاوه‌بر نهادهای خاص، همکاری‌های بین‌المللی و پیروی از استانداردهای جهانی را در اولویت قرار داده است. بنابراین، برای دستیابی به حفاظت مؤثر از زیرساخت‌های انرژی در قبال رایاجنگ‌ها و اتخاذ سیاست‌های حقوقی هماهنگ با اسناد بین‌المللی و تقویت ظرفیت‌های اجرایی داخلی ضرورتی انکارناپذیر است.

کلیدواژه‌ها: رایاجنگ‌های تخریبگر و مختل‌کننده، امنیت سایبری، امنیت انرژی، زیرساخت‌های انرژی، همکاری بین‌المللی.

تاریخ دریافت: ۱۴۰۴/۰۴/۱۱ **تاریخ بازنگری:** ۱۴۰۵/۰۵/۱۴ **تاریخ پذیرش:** ۱۴۰۴/۰۶/۲۴

استناد: نمامیان، پیمان (۱۴۰۴). مقابله با رایاجنگ‌های تخریبگر و مختل‌کنندهٔ امنیتِ زیرساخت‌های انرژی در اسناد بین‌المللی؛ با تحلیل تطبیقی مقررات ایران و قطر، آموزه‌های حقوق کیفری کشورهای اسلامی، ۲ (۴)، ۱۷۷-۱۴۸. http://www.doi.org/10.22091/dclic.2025.13272.1092

ناشر: دانشگاه قم

نوع مقاله: پژوهشی

مقدمه

مسائل امنیت سایبری به دغدغه اصلی بسیاری از سازمان‌های بین‌المللی تبدیل شده است، اما کمتر توجهی به تهدیدهای ناشی از «رایاجنگ‌ها»[۱] اعم تخریبگر (فیزیکی) و مختل کننده (غیرفیزیکی) در بخش انرژی می‌شود. زیرساخت‌هایی مانند خطوط لوله، نیروگاه‌ها، پالایشگاه‌ها و شبکه‌های انتقال به‌طور بالقوه هدف رایاجنگ‌ها هستند(Kü feoğlu & Akgü n, 2024: 29-31). یک نظرسنجی در سال ۲۰۱۵ نشان داد به‌طور تقریبی بخش قابل ملاحظه‌ای از مدیران فناوری اطلاعات در ایالات‌متحده و اروپا بر این باورند گسترش رایاجنگ‌ها علیه زیرساخت‌های حیاتی در آینده می‌تواند منجر به تلفات جانی شود (DiPietro, 2015: 1).

با پیشرفت فناوری و وابستگی بیشتر این زیرساخت‌های انرژی به سامانه‌های رایانه‌ای، رایاجنگ‌ها به یکی از خطرات اصلی این بخش تبدیل شده‌اند (Abdallah, 2025: 2536). بنابراین، مقابله با این جرائم برای تضمین توسعه پایدار و قابل اعتماد این زیرساخت‌ها ضرورت دارد. ازاین‌رو، می‌توان با «پیشگیری» و «کاهش» و «بازیابی» با چنین حمله‌هایی مقابله کرد: الف. پیشگیری، اقداماتی که در عمل از وقوع و موفقیت‌آمیز بودن حمله به سامانه انرژی پیشگیری کند؛ ب. کاهش، آثار رایاجنگ‌ها بر سامانه انرژی تا حد امکان محدود شود؛ ج. بازیابی، سامانه انرژی پس از یک حمله موفقیت‌آمیز در اسرع وقت به عملکرد عادی بازگردد.[۲]

وابستگی فزاینده زیرساخت‌های انرژی به فناوری‌های سایبری آن‌ها را در قبال رایاجنگ‌ها آسیب‌پذیر کرده است. رایاجنگ‌ها مانند نفوذ به شبکه‌های توزیع انرژی و سرقت اطلاعات حساس می‌توانند امنیت ملی و تأمین انرژی را تهدید کنند.[۳] در اوایل سال ۲۰۰۰، با گسترش اینترنت و تهدیدهای ناشی از رایاجنگ‌ها، جرائم اینترنتی به یک مقوله جهانی تبدیل شد و کشورهای گوناگون شروع به تدوین قوانین خاص در قبال آن نظیر هک،[۴] دسترسی غیرمجاز، سرقت هویت و کلاهبرداری برخط کردند (Bartoli, 2025: 499). در ضمن، وفق چارچوب الزامات جهانی، در قبال این تهدیدها، ضرورت پیروی از اسناد بین‌المللی، به‌ویژه «کنوانسیون بوداپست در مورد جرائم

---

۱. «رایاجنگ» (Cyberwars)، واژه مصوب «فرهنگستان زبان و ادب فارسی» است.

2. United Nations Economic Commission for Europe, Digitalization. in Energy: Case Study on "Cyber Resilience of Critical Energy Infrastructure", December 2023, https://unece.org/info/Sustainable-Energy/pub/387073

3. https://insights.issgovernance.com/posts/cybersecurity-threats-to-critical-energy-infrastructure-business-continuity-in-a-changing-geopolitical-environment/

4. Heck

سایبری، مصوب ۲۰۰۱»،[1] مورد تأکید است که کشورهای امضا کننده را ملزم به اتخاذ مقررات داخلی در قبال رایاجنگ‌ها می‌کند.[2] با وجود اسناد بین‌المللی، بسیاری از کشورها تاکنون به‌طور کامل به آن نپیوسته‌اند یا مقررات داخلی خود را با آن تطبیق نداده‌اند. این عدم هماهنگی و فقدان چارچوب جهانی یکپارچه، همکاری‌های بین‌المللی را محدود می‌کند. برای مقابله مؤثر با رایاجنگ‌ها علیه زیرساخت‌های انرژی، ضروری است که کشورهای بیشتری به کنوانسیون بپیوندند و مقررات خود را بر اساس آن تنظیم کنند.

در این بین، ایران و قطر در قبال تهدیدهای ناشی از رایاجنگ‌ها علیه زیرساخت‌های انرژی، مقررات خاصی وضع کرده‌اند. در ایران، «قانون جرائم رایانه‌ای، مصوب ۱۳۸۸» و پروژه‌های امنیت سایبری برای محافظت از زیرساخت‌های حیاتی مانند برق و گاز ایجاد شده است. به‌علاوه، در ایران، «مرکز ملی فضای مجازی» نقش مهمی در نظارت و تدوین سیاست‌های امنیتی ایفا می‌کند. این در حالی است که قطر وفق «قانون پیشگیری جرائم سایبری قطر (قانون شماره ۱٤، مصوب ۲۰۱٤)»[3] بر حفاظت از زیرساخت‌های حیاتی تأکید دارد و از فناوری‌های نوین و همکاری‌های بین‌المللی برای تقویت امنیت سایبری بهره می‌برد. بنابراین، باید اذعان داشت قطر ازنظر همکاری‌های بین‌المللی و پیشرفت‌های فناورانه در مواجهه با تهدیدهای رایاجنگ‌ها علیه زیرساخت‌های حیاتی (به‌ویژه زیرساخت‌های انرژی) نسبت به ایران دارای سیاست تقنینی بیشتری است.

با این اوصاف، این پژوهش با رویکردی توصیفی‌تحلیلی، به بررسی رایاجنگ‌ها علیه زیرساخت‌های انرژی می‌پردازد و با سنجش اسناد بین‌المللی، در تلاش است تا با پاسخ به این پرسش که «چگونه اسناد بین‌المللی از زیرساخت‌های انرژی در قبال رایاجنگ‌ها محافظت می‌کنند؟» چارچوب‌های حقوقی موجود را تحلیل و راهکارهایی برای تقویت همکاری‌ها و اقدامات پیشگیرانه ارائه دهد. به‌علاوه، با تمرکز بر ایران و قطر به شناسایی سیاست‌ها و راهکارهای اجرایی این دو کشور و وجوه افتراق مقررات آن‌ها پرداخته و ظرفیت‌های همکاری‌های منطقه‌ای و بین‌المللی در قبال این تهدیدها را با پاسخ به این پرسش که «چارچوب حقوقی ایران و قطر در مقابله با رایاجنگ‌ها علیه زیرساخت‌های انرژی چگونه طراحی شده است؟» ارزیابی می‌کند.

---

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

2. European Convention on Cybercrime. (2001). *Convention on Cybercrime, Budapest*. Council of Europe. Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

3 . Law No. (14) of 2014 Promulgating the Cybercrime Prevention Law, https://www.cra.gov.qa/en/document/cybercrime-prevention-law-no-14-of-2014

۱. زیرساخت‌های انرژی؛ شناخت حقوقی و ظرفیت‌های بین‌المللی

در اسناد بین‌المللی، هیچ تعریف رسمی و جهانی از «زیرساخت‌های حیاتی» وجود ندارد، زیرا این مفهوم بیشتر بر اساس ارزیابی‌های ملی و نیازهای هر کشور مشخص می‌شود. به دیگر تعبیر، هر کشور به‌طور مستقل دارایی‌ها، سامانه‌ها یا قابلیت‌هایی را که به امنیت ملی خود مرتبط می‌داند، به‌عنوان زیرساخت‌های حیاتی شناسایی می‌کند.[۱] در ایالات‌متحده آمریکا، زیرساخت‌های حیاتی به این صورت تعریف می‌شود: «سامانه‌ها و دارایی‌ها، اعم از فیزیکی و غیرفیزیکی، به‌قدری برای ایالات‌متحده مهم هستند که اختلال یا نابودی آن‌ها می‌تواند تأثیرات جدی بر امنیت ملی، اقتصاد، سلامت عمومی یا ایمنی عمومی کشور بگذارد.»[۲] این تعریف در چارچوب «قانون حفاظت از زیرساخت‌های حیاتی، مصوب ۲۰۰۱»[۳] مقرر شده که تصریح می‌کند «اختلال فیزیکی یا غیرفیزیکی در عملکرد زیرساخت‌های حیاتی که تأثیرات منفی بر اقتصاد، خدمات دولتی و امنیت ملی ایالات‌متحده داشته باشد، قابل توجه است.»[۴] افزون بر این، «قانون میهن‌پرستی ایالات‌متحده آمریکا، مصوب

---

۱. در عین حال، کمیسیون اروپا در سال ۲۰۰۴ وفق «برنامه اقدام اتحادیه اروپا راجع‌به مبارزه با تروریسم»، بر تقویت همکاری‌ها و بهبود قابلیت‌های کشورهای عضو در مقابله با تروریسم و تهدیدهای امنیتی تأکید کرد و هدف آن ایجاد رویکرد یکپارچه و هماهنگ برای تقویت زیرساخت‌های قانونی، عملیاتی و اطلاعاتی بود؛

- European Council. (2004, June 11). *EU plan of action on combating terrorism*. Council of Public. https://www.eumonitor.eu/9353000/1/j4nvgs5kjg27kof_j9vvik7m1c3gyxp/vi7jgsy4c6vl/f=/10010_3_04_rev_3.pdf

2. Migration and Home Affairs: Critical Infrastructure, EUR. COMM'N, https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/criticalinfrastructure_en (last visited Dec. 26, 2019) [https://perma.cc/LF9P-DUEZ].

3. Critical Infrastructures Protection Act of 2001, https://www.congress.gov/bill/107th-congress/senate-bill/1407

۴. به‌عنوان نمونه، وزارت امنیت داخلی ایالات متحده آمریکا در حال حاضر شانزده بخش از زیرساخت‌های حیاتی مشتمل بر شیمیایی، تأسیسات تجاری، ارتباطات، تولیدات حیاتی، سدها، پایگاه صنعتی دفاعی، خدمات اضطراری، انرژی، خدمات مالی، غذا و کشاورزی، تأسیسات دولتی، بهداشت و درمان و بهداشت عمومی، فناوری اطلاعات، هسته‌ای، حمل و نقل و سامانه‌ها و تأسیسات آب و فاضلاب را مورد شناسایی قرار داده است؛

- Critical Infrastructure Sectors, U.S. Department of Homeland Security, Supra note 28, https://www.dhs.gov/critical-infrastructure-sectors

پس از حوادث ۱۱ سپتامبر ۲۰۰۱، ایالات متحده به آسیب‌پذیری زیرساخت‌های حیاتی خود پی برد و در پاسخ، در فوریه ۲۰۰۳ «راهبرد ملی حفاظت فیزیکی از زیرساخت‌های حیاتی و دارایی‌های اساسی» را منتشر کرد. هدف این راهبرد، تقویت امنیت و کاهش آسیب‌پذیری زیرساخت‌های حیاتی در قبال تهدیدهای فیزیکی و غیرفیزیکی، از جمله اقدام‌های تروریستی بود. در این سند، سیاست‌هایی برای شناسایی، ارزیابی و کاهش خطرات، با تأکید بر مقابله با رایاجنگ‌ها نیز پیش‌بینی شد. این اقدام بخشی از تلاش‌های جامع آمریکا برای افزایش تاب‌آوری ملی و حفظ عملکردهای اقتصادی، اجتماعی و امنیتی کشور به‌شمار می‌رود؛

- U.S. Department of Homeland Security, The National Strategy for the Physical Protection of Critical

۲۰۰۱»،[۱] مشابه همین تعریف را در خصوص زیرساخت‌های حیاتی ارائه داده و اعلام می‌دارد که چنین سامانه‌ها و دارایی‌ها به‌قدری برای کشور حیاتی هستند که از دست دادن آن‌ها می‌تواند بر اقتصاد ملی و ایمنی عمومی تأثیرات منفی بگذارد.[۲] وانگهی قانون مزبور نسبت در قبال تهدیدها علیه زیرساخت‌های حیاتی مشتمل بر بهبود روش‌های شناسایی و پیشگیری از رایاجنگ‌ها و جنگ‌های شیمیایی، بیولوژیک و فیزیکی تأکید دارد.

طی سال ۱۹۹۸، ایالات‌متحده آمریکا با انتشار «فرمان اجرایی شماره ٦٣»، اولین راهبرد ملی برای حفاظت از زیرساخت‌های حیاتی را تدوین کرد.[۳] این سیاست‌ها در راستای تقویت آمادگی و تاب‌آوری زیرساخت‌ها در قبال تهدیدهای گوناگون نظیر رایاجنگ‌های تخریبگر و مختل‌کننده قرار داشت. در سال ۲۰۱۳، ایالات‌متحده آمریکا با هدف تقویت تاب‌آوری زیرساخت‌های حیاتی در قبال تهدیدهای ناشی از رایاجنگ‌های تخریبگر و مختل‌کننده، «سند شماره ۲۱ سیاست راهبردی» را معرفی کرد.[٤] این سند، رویکردهایی را برای محافظت از زیرساخت‌های حیاتی کشور در قبال چنین تهدیدهایی ارائه می‌دهد.

سند نهایی اجلاس جهانی جامعه اطلاعاتی[٥] به توافقات اجلاس‌های ۲۰۰۳ و ۲۰۰۵ اشاره دارد که هدف آن‌ها استفاده بهینه از فناوری‌های اطلاعات و ارتباطات برای توسعه پایدار و تقویت امنیت جهانی در قبال رایاجنگ‌های مختل‌کننده علیه زیرساخت‌های حیاتی بود.[٦] این سند بر استفاده از فناوری‌های اطلاعات و ارتباطات برای بهبود کیفیت زندگی، تقویت حقوق بشر و دموکراسی و حفاظت از زیرساخت‌های حیاتی در مقابله

Infrastructures and Key Assets (2003), https://www. dhs.gov/xlibrary/assets/Physical_Strategy.pdf [https://perma.cc/G62A-MY6W].

1. U.S. Congress. (2001, October 26). Public Law 107–56—October 26, 2001: Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA PATRIOT Act) Act of 2001. https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

2. Public Law 107 - 56 - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, https://www.govinfo.gov/app/details/PLAW-107publ56

3. https://www.inss.org.il/wp-content/uploads/2019/04/Memo190new_e.pdf

4. White House, "Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience, Washington, DC, USA, 2013. [Online]. Available: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resi

5. World Summit on the Information Society (WSIS), https://publicadministration.un.org/wsis10/

6. International Telecommunication Union. (2003, December 12). *Declaration of principles: Building the information society: A global challenge in the new millennium*. Document WSIS-03/GENEVA/DOC/4-E. https://www.itu.int/net/wsis/docs/geneva/official/dop.html

با رایاجنگ‌ها تأکید دارد و لزوم ایجاد جامعه اطلاعاتی جهانی با تمرکز بر امنیت سایبری و حکمرانی اینترنت را مطرح می‌کند.[۱]

گروه کارشناسان دولتی در گزارشی طی سال ۲۰۱۵ ضمن تأکید بر تأثیر فناوری‌های نوین اطلاعاتی در تهدیدات امنیتی، به‌ویژه رایاجنگ‌ها علیه زیرساخت‌های انرژی، بر لزوم تقویت همکاری‌های بین‌المللی، ایجاد چارچوب‌های حقوقی منسجم و تعریف دقیق‌تر مفاهیم حقوقی و استانداردسازی مقررات راجع‌به فضای سایبری برای حفاظت از زیرساخت‌های انرژی اذعان داشتند.[۲] به‌علاوه، روزآمدسازی مقررات داخلی و بین‌المللی و افزایش توانمندی‌های تخصصی برای مقابله با این جرائم ضروری است.[۳] در ضمن، پیش‌نویس سند جامعی تحت عنوان «پیمان دیجیتال جهانی» در سال ۲۰۲۳ منتشر شد که به دنبال ایجاد توافق جهانی برای مدیریت فناوری‌های دیجیتالی و مقابله با تهدیدهای ناشی از رایاجنگ‌ها در این حوزه است.[٤] این سند بر تسهیل دسترسی به اینترنت، حمایت از حقوق دیجیتال و تأمین امنیت زیرساخت‌های غیرفیزیکی و همکاری‌های بین‌المللی در مقابله با تهدیدهای رایاجنگ‌ها تأکید دارد.[٥]

در دید کلی، زیرساخت‌های حیاتی مجموعه‌ای از سامانه‌ها و دارایی‌هایی هستند که برای حفظ امنیت، ثبات و عملکرد اقتصادی و اجتماعی کشور ضروری‌اند. این زیرساخت‌ها شامل منابع انرژی، شبکه‌های مخابراتی، سامانه‌های مالی، تأسیسات ارتباطی و مراکز نظامی و دولتی می‌شوند. هرگونه اختلال یا آسیب به این بخش‌ها می‌تواند تأثیرات جدی بر امنیت ملی و پایداری کشور داشته باشد؛ بنابراین حفاظت از این زیرساخت‌ها در قبال تهدیدهای فیزیکی و غیرفیزیکی از اهمیت قابل ملاحظه‌ای برخوردار است (معاونت پژوهش و تولید علم دانشگاه اطلاعات و امنیت ملی، ۱۳۹٦: ۸٤-۸۳).

1. https://www.itu.int/net/wsis/outcome/booklet.pdf
2. United Nations. (2015, July 22). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/70/174). General Assembly, Seventieth session, Item 93 of the provisional agenda. https://undocs.org/A/70/174
3. https://digitallibrary.un.org/record/799853?ln=en&v=pdf
4. United Nations Office for Digital and Emerging Technologies. (2024). *Global Digital Compact: A comprehensive global framework for digital cooperation and governance of artificial intelligence*. Retrieved from https://www.un.org/global-digital-compact/en
5.https://www.un.org/global-digital-compact/sites/default/files/2024-09/Global%20Digital%20Compact%20-%20English_0.pdf

وفق تعاریف فوق‌الاشاره، باید اذعان داشت «زیرساخت‌های انرژی» به مجموعه‌ای از تأسیسات، سامانه‌ها و شبکه‌هایی اطلاق می‌شود که برای تولید، انتقال، ذخیره‌سازی و توزیع انرژی طراحی شده‌اند. این زیرساخت‌ها نقش حیاتی در رشد اقتصادی، توسعه پایدار و امنیت انرژی دارند و شامل شبکه‌های برق، گاز، نفت و انرژی‌های تجدیدپذیر هستند. زیرساخت‌های انرژی به فرآیندهای تولید، انتقال، ذخیره‌سازی و توزیع انرژی اشاره دارند و شامل نیروگاه‌ها، پست‌های انتقال، خطوط انتقال و شبکه‌های توزیع می‌شوند. توسعه این زیرساخت‌ها به افزایش بهره‌وری اقتصادی، بهبود کیفیت زندگی و کاهش اثرات زیست‌محیطی کمک می‌کند (Onyeji, I, Bazilian, M, & Bronk, 2014, 53-54).

از منظر حقوقی، زیرساخت‌های انرژی نه‌تنها به‌عنوان دارایی فیزیکی، بلکه به‌عنوان مجموعه‌ای قانونی تحت نظارت مراجع دولتی، محلی و بین‌المللی شناخته می‌شوند. وفق موازین بین‌المللی، کشورهای مختلف موظف به رعایت استانداردهای خاص برای توسعه و مدیریت این زیرساخت‌ها هستند. این مقررات شامل مالکیت انرژی، قراردادهای دولتی و خصوصی و محیط‌زیست می‌شود.[1] ازاین‌رو، زیرساخت‌های انرژی تحت مقررات خاصی قرار دارند که هدف آن‌ها تضمین بهره‌گیری پایدار از منابع انرژی، پیشگیری از بحران‌های انرژی و تأمین دسترسی به انرژی برای تمامی کشورهای عضو است.[2]

در چارچوب توافق‌نامه پاریس، مصوب ۲۰۱۵،[3] کشورهای امضاکننده این توافق‌نامه متعهد به کاهش تولید گازهای گلخانه‌ای و افزایش استفاده از انرژی‌های تجدیدپذیر شده‌اند. این توافق‌نامه می‌تواند به‌مثابه چارچوبی برای توسعه پایدار زیرساخت‌های انرژی در سطح جهانی اطلاق شود.[4] وفق ساختار و محتوای کنوانسیون سازمان ملل متحد راجع‌به حقوق دریاها مصوب ۱۹۸۲،[5] کنوانسیون مبادرت به تنظیم بهره‌برداری از منابع انرژی در دریاها و اقیانوس‌ها می‌نماید و بر حقوق کشورهای ساحلی در مورد استخراج منابع انرژی از آب‌های بین‌المللی تأکید دارد (Siig, Feldtmann, & Billing, 2024: 163-164).

1. https://sustainablefutures.linklaters.com/post/102ju7t/energy-infrastructure-legal-outlook-2025
2. https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e2143
3. The Paris Agreement, https://unfccc.int/files/essential_background/convention/application/pdf/english_paris_agreement.pdf
4. https://www.britannica.com/topic/Paris-Agreement-2015
5 . United Nations Convention on the Law of the Sea, Montego Bay, 10 December 1982, https://treaties.un.org/Pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XXI-6&chapter=21&Temp=mtdsg3&clang=_en

۲. پیشینه و تحولات تهاجمی؛ آماج‌های رایاجنگ‌ها به زیرساخت‌های انرژی

زیرساخت‌های انرژی به‌عنوان ارکان حیاتی هر جامعه، نقش مهمی در تأمین انرژی برای صنایع، اماکن مسکونی و سایر بخش‌ها دارند. این زیرساخت‌ها به سامانه‌های رایانه‌ای و شبکه‌های پیچیده وابسته‌اند که آن‌ها را در قبال تهدیدهای رایاجنگ‌ها آسیب‌پذیر می‌کند (Onyeji, I, Bazilian, M, & Bronk, 2014, 53-54).

طی سال‌های اخیر، داده‌ها و منابع اطلاعاتی «سامانه‌های کنترل صنعتی»[1] در شرکت‌های انرژی، مؤسسات مالی، سازمان‌های دولتی و سرورهای رسمی به هدف اصلی آماج‌های رایاجنگ‌ها مکرر تبدیل شده‌اند. افزایش شدید این نوع از آماج‌ها حاکی از آن است که مرتکبان رایاجنگ‌ها با انگیزه‌های سیاسی، به‌طور عمده به نمایندگی از دولت‌های تحت سیطره خود، آماج‌های گسترده و نقض‌کننده‌ای را علیه نهادهای دولتی و خصوصی مرتکب که منجر به خسارات شدید مکرر شده است (ر.ک: محمودزاده و دیگران، ۱۳۹۷: ۲۶۷-۲۶۶).

پلیس طی سال ۲۰۰۰ در کوئینزلندِ استرالیا مردی را دستگیر کرد که با استفاده از رایانه و فرستنده رادیویی تلاش کرده بود، سامانه فاضلاب «ماروچی شایر»[2] را کنترل کرده و فاضلاب را به پارک‌ها و رودخانه‌ها و املاک هدایت کند.[3] بنابراین، باید تأکید داشت رایاجنگ‌ها از طریق آماج به منابع تأمین آب مشتمل بر خرابکاری عمدی سامانه تأمین آب، به‌واسطه آماج‌های شیمیایی یا بیولوژیک و خرابکاری در زیرساخت‌ها صورت می‌پذیرد.

اوکراین قربانی یکی از اولین آماج‌های رایاجنگ‌های شناخته شده علیه جمعیت غیرنظامی است که منجر به قطع برق طی سال ۲۰۱۵ شد (Zetter, 2017: 1). در ۲۳ دسامبر، یکی از توزیع کنندگان برق اوکراین، بیست‌وهفت پست برق را به‌طور ناگهانی از مدار خارج کرد و یک‌صدوسه شهر را در تاریکی و یک‌صدوهشتادوشش شهر دیگر را در تاریکی نسبی رها فروبرد. آماج رایاجنگ‌ها به شبکه برق اوکراین ماه‌ها پیش، زمانی که رایانه‌های شرکت انرژی به بدافزار آلوده شدند، آغاز شد (Blotzer, 2018: 41). البته حدود یک سال بعد، در هفدهم دسامبر ۲۰۱۶، شبکه برق اوکراین مجدد هک شد. آماج دوم حدود نیمه‌شب رخ داد و تنها یک ساعت طول کشید. مقامات اوکراینی بر این باورند که آماج اخیر از سوی همان هکرهایی ارتکاب یافت که آماج اول را مرتکب شدند. آماج دوم می‌توانست آسیب بیشتری وارد کند، اما به نظر می‌رسید که هکرها تنها می‌خواستند «توانایی‌های [خود] را به نمایش بگذارند»(Pagliery, 2016: 1).

---

1. Industrial Control Systems (ICS)
2. Mariachi Shire
3. https://fa.wikipedia.org/wiki/

شبکه انرژی در آمریکا ۷۹ مرتبه طی سال ۲۰۱٤ مورد آماج قرار گرفت، اما دولت آمریکا اطلاعات خاصی را ارائه نکرد و به‌طور صرف حوادث مربوط به روش‌های مهاجم را بیان کرد (Pagliery, 2016: 1). وزارت امنیت داخلی در سال ۲۰۱۷ به شرکت‌هایی که نیروگاه‌های هسته‌ای در ایالات‌متحده را اداره می‌کنند، نسبت به آماج‌های بدافزاری که هدف آن‌ها هکِ دستگاه‌های رایانه متعلق به کارکنان شرکت‌های هسته‌ای است، هشدار داد (Gallagher, 2017: 1).

«سازمان امنیت ارتباطات»[1] در «آژانس اطلاعاتی فدرال کانادا»،[2] آماری از «سازش‌های سامانه‌ای»[3] شناخته شده را در نوامبر ۲۰۱٦ منتشر کر د (Freeze, 2016: 1).[4] اطلاعات منتشر شده نشان می‌دهد که بخش منابع طبیعی، انرژی و محیط‌زیست کانادا به‌طور تقریبی به اندازه تمام بخش‌های دیگر مورد هدف هکرها قرار گرفته است. در سال ۲۰۱٦، این بخش ۲۰۷۸ مرتبه مورد هدف قرار گرفت، درحالی‌که به‌طورکلی ۲٤۹۳ اقدام برای هکِ سایر بخش‌ها انجام شده است (Silver, 2016: 1).

۳. چالش‌ها و تهدیدهای رایاجنگ‌ها علیه زیرساخت‌های انرژی

با گسترش فناوری‌های اطلاعاتی در زیرساخت‌های انرژی، تهدیدهای رایاجنگ‌ها افزایش یافته‌اند. رایاجنگ‌ها می‌توانند منجر به قطع خدمات، خسارات مالی و بی‌ثباتی سیاسی شوند. بنابراین، زیرساخت‌های انرژی مانند شبکه‌های برق، خطوط انتقال گاز و تأسیسات نفتی هدف جذابی برای مرتکبان رایاجنگ‌ها هستند (Ahmad et al, 2021). افزایش وابستگی به سامانه‌های کنترل صنعتی و اینترنت اشیاء صنعتی باعث شده تا این زیرساخت‌ها نسبت به رایاجنگ‌ها بسیار آسیب‌پذیر شوند. حوادثی نظیر حمله بدافزار «استاکس‌نت»(ر.ک: شاملو و حسینی، ۱٤۰۳: ۱۲٤)[5] یا رایاجنگ‌ها به شبکه برق اوکراین نمونه‌هایی از تهدیدهای واقعی و پرخطر هستند (Kushner, 2013: 52; Lee et al, 2016).

1. Communication Security Establishment (CSE)
2. Canada's Federal Intelligence Agency
3. System Compromises
4 . See generally Communications Security Establishment, https://www.cse-cst.gc.ca/en/inside-interieur/protect-protection, archived at https://perma.cc/PNY6-ETDR
5. Stuxnet

یکی از مهم‌ترین راهکارها، طراحی و اجرای ساختارهای مقاوم در قبال رایاجنگ‌ها است. این کار می‌تواند شامل استفاده از پروتکل‌های امن ارتباطی، «فایروال‌های صنعتی»،[۱] تفکیک شبکه‌ها و نظارت و پایش مستمر بر عملکرد یک سامانه بلادرنگ باشد.[۲] به‌علاوه، روزآمدسازی مداوم سامانه‌های کنترل و استفاده از نرم‌افزارهای امن، ضرورتی انکارناپذیر است. در ضمن، آموزش مستمر کارکنان درزمینهٔ امنیت سایبری و شناسایی تهدیدها و واکنش به حوادث اهمیت زیادی دارد. این آموزش‌ها باید بر اساس سطوح فنی و مدیریتی متفاوت طراحی شوند (Venkatachary et al, 2021: 18). در ضمن، فناوری‌های نوین نظیر هوش مصنوعی، یادگیری ماشین و تحلیل کلان‌داده‌ها می‌توانند در پیش‌بینی و شناسایی رایاجنگ‌ها مؤثر باشند (Ahmad et al, 2021).

تهدیدهای رایاجنگ‌ها علیه زیرساخت‌های انرژی نیاز به همکاری بین سیاست‌گذاران، متخصصان فنی، مدیران و قانون‌گذاران دارند. ترکیب راهکارهای سایبری، مدیریتی، حقوقی و آموزشی می‌تواند تاب‌آوری سایبری کشورها را افزایش داده و از فاجعه‌های بزرگ پیشگیری کند. ارتقای امنیت زیرساخت‌ها به رویکردی چندبخشی با ابعاد فنی، مدیریتی و حقوقی نیاز دارد. آموزش، مقررات‌گذاری هوشمندانه و فناوری‌های نوین از مؤلفه‌های اصلی مقابله با رایاجنگ‌ها در این حوزه هستند. همچنین، چارچوب مقررات‌گذاری پویا می‌تواند الگویی مناسب در سطح ملی و بین‌المللی باشد (حسینی، ۱۴۰۲: ۱۲۱۳).

همکاری‌های بین‌المللی، ازجمله تبادل اطلاعات و فناوری‌های امنیتی، می‌تواند به تقویت امنیت زیرساخت‌های انرژی کمک کند.[۳] برای مقابله مؤثر، کشورهای مختلف باید استانداردهای امنیتی جهانی برای محافظت از زیرساخت‌های انرژی ایجاد کنند.[۴] این همکاری‌ها به تقویت چارچوب‌های قانونی و کاهش تهدیدهای رایاجنگ‌ها کمک خواهد کرد و به ایجاد یک رویکرد جهانی و هماهنگ برای مقابله با تهدیدها ضروری است.

مقابله با رایاجنگ‌ها نیازمند مقررات جامع ملی و بین‌المللی است که مسئولیت‌ها، استانداردهای امنیتی، مجازات‌ها و همکاری‌های بین‌المللی را شامل شود. برای این امر، همکاری بین‌سازمانی و بین‌المللی ضروری

---

۱. فایروال‌های صنعتی (Industrial Firewalls) ابزارهای امنیتی هستند که برای محافظت از زیرساخت‌های صنعتی و سامانه‌های کنترل صنعتی (Industrial Control Systems "ICS")در قبال تهدیدهای سایبری طراحی شده‌اند.

2 . CISA. (2022). Cybersecurity best practices for industrial control systems. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov

3. https://levelblue.com/blogs/security-essentials/protecting-energy-infrastructure-from-cyberattacks

4. See: https://gsconlinepress.com/journals/gscarr/sites/default/files/GSCARR-2024-0237.pdf

است. نهادهایی مانند مراکز ملی سایبری باید اطلاعات و تهدیدها را بلادرنگ به اشتراک بگذارند و مشارکت در فعالیت‌ها و تدوین طرح‌ها می‌تواند آمادگی سازمان‌ها را افزایش دهد.

٤. کاربست اسناد بین‌المللی برای حفاظت از امنیتِ زیرساخت‌های انرژی در قبال رایاجنگ‌ها

زیرساخت‌های انرژی که نقش حیاتی در تأمین انرژی و ثبات اقتصادی و اجتماعی دارند، در عصر دیجیتال با تهدیدهای ناشی از رایاجنگ‌ها در این حوزه مواجه‌اند. این تهدیدها می‌توانند آسیب‌های گسترده‌ای به زیرساخت‌های انرژی نظیر شبکه‌های برق، گاز و انرژی‌های تجدیدپذیر وارد کنند. در این میان، اسناد بین‌المللی واکنش‌های قانونی مؤثری را در سطح جهانی در قبال رایاجنگ‌ها بروز داده‌اند که آن‌ها مورد تدقیق و بررسی قرار می‌گیرد.

٤-١. قطعنامه‌ها و الزامات جهانی در جرم‌انگاری‌ها

سازمان ملل متحد طی سال ۲۰۰۵، وفق چارچوب «کارگروه فناوری‌های اطلاعاتی و ارتباطی» و «مؤسسه آموزش و تحقیقات»، کتابچه‌ای تحت عنوان «عدم امنیت اطلاعات؛ راهنمای بقا در سرزمین‌های ناشناخته تهدیدهای سایبری و امنیت سایبری»[1] منتشر کرد. این کتابچه ضمن تأکید بر اهمیت اجرای سازوکارهای پیشگیری و پاسخ‌گویی به حوادث امنیتی، بر چالش‌های ناشی از فقدان امنیت اطلاعات و توسعه آگاهی نسبت به رایاجنگ‌ها در راستای حفاظت از زیرساخت‌های حیاتی تمرکز ویژه‌ای داشت.

در راستای فرایند پیشگیری از ارتکاب رایاجنگ‌ها علیه زیرساخت‌های حیاتی که وفق قطعنامه‌های ۱۳۷۳ (۲۰۰۱) و ١٥٦٦ (٢٠٠٤) وضع شده بود، شورای امنیت سازمان ملل متحد با صدور قطعنامه (۲۰۱۷)۲۳٤۱ راجع‌به حفاظت از زیرساخت‌های حیاتی، به‌عنوان نخستین سند جهانی به این قضیه به نحو ویژه‌ای پرداخت. قطعنامه اخیر از دولت‌های عضو خواست تا رایاجنگ‌ها علیه زیرساخت‌های حیاتی را به‌عنوان جرائم جنایی جدی در مقررات داخلی خود تعریف کنند و مسئولیت کیفری این جرائم، ازجمله تخریب، از کار انداختن، برنامه‌ریزی، آموزش، تأمین مالی و پشتیبانی لجستیکی را احراز کنند.[2]

1. United Nations, Information Insecurity: A Survival Guide to the Uncharted Territories of Cyber Threats and Cyber Security (Ict Task Force Series), July 1, 2005, https://unesdoc.unesco.org/ark:/48223/pf0000143889

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

قطعنامه ۲۳۴۱ شورای امنیت سازمان ملل متحد، به‌ویژه درزمینهٔ جرم‌انگاری اقدام‌های ارتکابی علیه زیرساخت‌های حیاتی مانند رایاجنگ‌ها، ویژگی متمایز خود را نشان می‌دهد. این قطعنامه وفق اسناد پیشین مانند قطعنامه ۱۳۷۳ که پس از حوادث ۱۱ سپتامبر ۲۰۰۱ صادر شد، تنظیم شده و الزامات کلی برای محاکمه مرتکبان رایاجنگ‌ها و پیشگیری از آن‌ها را برای دولت‌های عضو تعیین می‌کند. در ضمن شورای امنیت، وفق قطعنامه ۲۳۹۶(۲۰۱۷) بر اهمیت تقویت همکاری‌های ملی و منطقه‌ای و بین‌المللی با ذی‌نفعان دولتی و خصوصی در قبال تهدیدها به‌ویژه درزمینهٔ تهاجم به اماکن عمومی و استفاده از فناوری‌های نوین مانند هواپیماهای بدون سرنشین تأکید داشت.[۱]

در ژوئن ۲۰۲۱، طی هفتمین بررسی راهبرد جهانی ضد تروریسم سازمان ملل متحد، دولت‌های عضو با اجماع موافقت کردند که حفاظت از اهداف آسیب‌پذیر باید در اولویت اقدام مشترک آن‌ها علیه رایاجنگ‌ها باشد.[۲] قطعنامه ۲۹۱/۷۵ مجمع عمومی در سال ۲۰۲۱ مشتمل بر دو بند مقدماتی و چهار بند عملیاتی در این زمینه بود که بر لزوم گردهم آوردن کلیه ذی‌نفعان (اعم از دولت‌های عضو، سازمان‌های بین‌المللی و منطقه‌ای، بخش خصوصی، جامعه مدنی و دانشگاهیان)، برای مقابله مؤثر با تهدید بی‌سابقه‌ای که رایاجنگ‌ها به زیرساخت‌های حیاتی و اهداف نرم ایجاد می‌کند، تأکید کرد.[۳]

برنامه جهانی مقابله با تهدیدهای ناشی از رایاجنگ‌ها علیه اهداف آسیب‌پذیر ازجمله زیرساخت‌های حیاتی و اماکن عمومی (یا «اهداف نرم»)، به‌طور مشترک از سوی دفتر مبارزه با تروریسم، اداره اجرایی کمیته مبارزه با تروریسم،[۴] مؤسسه تحقیقات جنایی و عدالت بین منطقه‌ای سازمان ملل متحد[۵] و اتحاد تمدن‌های سازمان ملل متحد،[۶] با همکاری اینترپل، از سال ۲۰۲۱ از دولت‌های عضو در ایجاد ظرفیت‌های خود، توسعه ارتباطات بین کارشناسان و شناسایی شیوه‌های مطلوب برای حفاظت از زیرساخت‌های حیاتی حمایت می‌کند.

---

1. 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
2. https://www.un.org/counterterrorism/un-global-counter-terrorism-strategy
3. United Nations, General Assembly, A/RES/75/291, 2 July 2021, https://documents.un.org/doc/undoc/gen/n21/175/70/pdf/n2117570.pdf
4. Office of Counter-Terrorism, the Counter-Terrorism Committee Executive Directorate
5. United Nations Interregional Crime and Justice Research Institute (UNICRI)
6. United Nations Alliance of Civilizations

برنامه جهانی دفتر مبارزه با تروریسم سازمان ملل متحد در قبال رایاجنگ‌ها علیه اهداف آسیب‌پذیر به درخواست دولت‌های عضو به‌ویژه از طریق مجمع عمومی (راهبرد جهانی ضدتروریسم و قطعنامه‌های بررسی و قطعنامه ۲۹۸/۷۷[1] مصوب سال ۲۰۲۳) و شورای امنیت (قطعنامه‌های ۲۳٤۱ و ۲۳۹٦ مصوب سال ۲۰۱۷ و قطعنامه ۲٦۱۷ مصوب سال ۲۰۲۱) و «اصول راهنمای شورای امنیت راجع‌به جنگجویان خارجی: اصول راهنمای مادرید (۲۰۱۵)، با الحاقیه ۲۰۱۸»،[2] تقویت حمایت سازمان ملل متحد از دولت‌های عضو برای رسیدگی به شکاف‌ها و چالش‌ها در حفاظت از اهداف آسیب‌پذیر که شامل زیرساخت‌های حیاتی و اهداف «نرم» بود را در صدر اولویت قرار داد.[3] هدف این برنامه شناسایی و به اشتراک‌گذاری سیاست‌ها و سازوکارهای عملیاتی برای درک، پیشگیری و مقابله با تهدیدهای احتمالی رایاجنگ‌ها علیه اهداف آسیب‌پذیر بود.[4] البته تقویت ظرفیت دولت‌های عضو برای توسعه راهبردهای جامع و مشترک همچون مشارکت عمومی و خصوصی، ظرفیت‌سازی مناسب برای پیشگیری، حفاظت، کاهش، بررسی، پاسخ به رایاجنگ‌ها علیه اهداف آسیب‌پذیر مورد تأکید قرار داشت.[5]

با توجه به تهدیدهای فزاینده رایاجنگ‌ها علیه زیرساخت‌های انرژی، جامعه جهانی به چارچوب‌های قانونی و الزامات جرم‌انگاری نیاز دارد تا از این زیرساخت‌ها محافظت کند. کشورهای مختلف و سازمان‌های بین‌المللی در تلاش برای جرم‌انگاری این حملات و ایجاد الزامات قانونی هستند. این الزامات شامل بهره‌گیری از فناوری‌های پیشرفته، افزایش نظارت، همکاری‌های بین‌المللی و توجه به حقوق بشر و حریم خصوصی در رسیدگی قانونی است. درنهایت، الزامات جهانی و قطعنامه‌های مرتبط نقش مهمی در تقویت امنیت زیرساخت‌های انرژی دارند.

1 .United Nations, General Assembly, A/RES/77/298, 3 July 2023, https://documents.un.org/doc/undoc/gen/n23/189/01/pdf/n2318901.pdf

2. Security Council Guiding Principles on Foreign Terrorist Fighters: The 2015 Madrid Guiding Principles, 2018 Addendum, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/security-council-guiding-principles-on-foreign-terrorist-fig.pdf

۳. طی سال ۲۰۲۲ دفتر مبارزه با تروریسم سازمان ملل متحد مجموعه اقدامات سازوکارهای مطلوب را در مورد حفاظت از زیرساخت‌های حیاتی در قبال جرائم ارتکابی روزآمد و منتشر کرد؛

-https://www.un.org/counterterrorism/events/unoct-launches-2022-update-un-compendium-good-practices-protection-critical-infrastructure

4. https://www.un.org/counterterrorism/vulnerable-targets

5. https://www.un.org/counterterrorism/cybersecurity

۴-۲. اسناد بین‌المللی و پاسخ‌گذاری‌های کیفری: دستاوردها و چشم‌انداز

زیرساخت‌های انرژی به دلیل وابستگی روزافزون به سامانه‌های رایانه‌ای، در معرض رایاجنگ‌ها قرار دارند که می‌توانند بحران‌های انرژی و اختلالات اقتصادی و اجتماعی ایجاد کنند. در قبال این تهدیدها، اسناد بین‌المللی گوناگونی اعم از قطعنامه‌ها و کنوانسیون‌ها، شکل گرفته‌اند تا کشورهای عضو را به اتخاذ تدابیر امنیتی برای محافظت از امنیت زیرساخت‌ها ملزم کنند. این اسناد نقش قابل ملاحظه‌ای در تقویت استانداردهای امنیتی دارند، اگرچه با چالش‌هایی در تطبیق و اجرای مؤثر، مواجه هستند.

۴-۲-۱. کنوانسیون بین‌المللی راجع‌به سرکوب بمب‌گذاری‌های تروریستی

جرائم ارتکابی وفق ماده ۲ از «کنوانسیون بین‌المللی راجع‌به سرکوب بمب‌گذاری‌های تروریستی، مصوب ۱۹۹۷»[1] به سه دسته تقسیم شده است: الف. جرائم ارتکابی توسط مرتکب اصلی؛ ب. مبادرت به ارتکاب جرم؛ ج. معاونت در جرم. ماده مزبور مشتمل بر بهره‌گیری از مواد منفجره یا ادوات مرگبار در اماکن عمومی، تأسیسات دولتی، یا سامانه‌های حمل‌ونقل است.

در ارتباط با رایاجنگ‌ها علیه زیرساخت‌های حیاتی به‌ویژه زیرساخت‌های انرژی، این کنوانسیون می‌تواند بدین شرح کاربرد داشته باشد: الف. «مواد منفجره یا ادوات مرگبار» ممکن است به معنای مواد انفجاری باشد که برای ایجاد مرگ یا آسیب طراحی شده‌اند. بااین‌حال، رایانه‌ها به‌تنهایی نمی‌توانند مانند بمب عمل کنند، بلکه ممکن است برای راه‌اندازی بمب استفاده شوند؛ ب. مواد مرگبار می‌توانند شامل مواد شیمیایی، بیولوژیک یا رادیواکتیو باشند که از طریق رهاسازی یا انتشار موجبات ایجاد مخاطره‌هایی برای مردم را فراهم خواهد آورد.

کنوانسیون بین‌المللی بمب‌گذاری‌های تروریستی باید با تهدیدهای رایاجنگ‌ها تطبیق یابد. این کنوانسیون به‌طور معمول به مقابله با تروریسم فیزیکی می‌پردازد، اما با تفسیرهای انعطاف‌پذیر، می‌توان تهدیدهای رایاجنگ‌ها علیه زیرساخت‌های انرژی را نیز شامل شود.[2] وفق ماده ۲، «مواد منفجره یا ادوات مرگبار» می‌تواند به هر وسیله‌ای که منجر به ورود خسارت یا آسیب شود، اطلاق گردد. آماج‌های رایاجنگ‌ها به سامانه‌های انرژی می‌تواند خسارات مشابه حملات فیزیکی وارد کند. بنابراین، با توجه به تهدیدهای رایاجنگ‌ها روزافزون،

1. International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on 15 December 1997; entered into force on 23 May 2001; 146 parties.

2 . https://ebooks.iospress.nl/volume/the-protection-of-critical-energy-infrastructure-against-emerging-security-challenges

کنوانسیون باید تفسیرهای نوینی برای حفاظت از زیرساخت‌ها و مقابله با رایاجنگ‌ها ارائه دهد (Cohen, 2010: 24-25).

۴-۲-۲. پیش‌نویس کنوانسیون جامع مقابله با تروریسم بین‌المللی

این پیش‌نویس که در سال ۱۹۹۶ توسط هند پیشنهاد شد و پس از بازنگری‌هایی در سال ۲۰۰۲ نهایی شد، به تقویت همکاری‌های بین‌المللی در مبارزه با تروریسم پرداخته است.[1] البته باید اذعان داشت پیش‌نویس مزبور به‌صورت ویژه تهدیدهای رایاجنگ‌ها به زیرساخت‌های حیاتی نظیر تأسیسات انرژی را تحت شمول خود قرار داده بود.

یکی از چالش‌های اصلی این پیش‌نویس، چالش تعریفی درزمینهٔ اقدام‌های تروریستی در مخاصمات مسلحانه و پناه دادن به تروریست‌ها است. این چالش، پیش‌نویس گامی مهم در راستای همکاری بین‌المللی ضدتروریستی به شمار می‌رفت. اگرچه، امکان تطبیق با تهدیدهای نوین همچون تهدیدهای رایاجنگ‌ها را فراهم می‌کند؛ زیرا ماده (ب)(۱)۲ پیش‌نویس به‌طور ضمنی تهدیدهای رایاجنگ‌ها را پوشش می‌دهد و جرائم ارتکابی علیه سامانه‌های انرژی و مخابرات را به‌عنوان جرائم تروریستی شناسایی می‌کند. به‌علاوه، محدودیت تعریف تروریسم ممکن است نتواند تمامی روش‌ها و شیوه‌های نوین جرائم، به‌ویژه رایاجنگ‌ها را تحت پوشش قرار دهد.[2]

بنابراین، برای پیشگیری از شکاف‌های موجود، لازم است که اصلاحات و تفسیرهای نوینی برای شمول رایاجنگ‌ها به‌ویژه ارتکاب آن‌ها علیه زیرساخت‌های حیاتی در این پیش‌نویس اعمال شود تا این پیش‌نویس به ابزاری مؤثر در قبال تهدیدهای رایاجنگ‌ها، به‌ویژه درزمینهٔ زیرساخت‌های انرژی، تبدیل شود.[3]

1. UN Ad Hoc Committee on Terrorism, Deraft International Comprehensive Convention on International Terrorism, in Annexes to the Report of the Ad Hoc Committee Established by General Assembly Resolution 51/210 of 17 December 1996, UN GAOR, 57th sess, Supp no 37, UN Doc A/57/37 (2002).

2.https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2225521_compendium_of_good_practice_web.pdf

3 . https://carnegieendowment.org/research/2024/03/why-the-world-needs-a-new-cyber-treaty-for-critical-infrastructure?lang=en

۴-۲-۳. قانون امنیت سایبری اتحادیه اروپا

این قانون[۱] در اتحادیه اروپا طی ۱۷ آوریل ۲۰۱۹ به‌عنوان بخشی از راهبرد گسترده‌تر برای افزایش امنیت سایبری در سراسر اروپا تصویب شد.[۲] در پاسخ به افزایش فراوانی و پیچیدگی تهدیدهای رایاجنگ‌ها، این قانون چارچوبی جامع با هدف بهبود سطح کلی امنیت سایبری در اتحادیه اروپا ایجاد کرد.[۳] ریشه‌های آن به راهبرد امنیت سایبری برای اتحادیه اروپا که در سال ۲۰۱۳ تصویب شد، برمی‌گردد که منجر به ایجاد آژانس امنیت سایبری اتحادیه اروپا[۴] و توسعه یک پاسخ هماهنگ به چالش‌های امنیت سایبری شد. این قانون، اختیارات آژانس را بیشتر تقویت کرده و یک چارچوب صدور گواهینامه امنیت سایبری اروپایی را معرفی می‌کند.[۵] اتحادیه اروپا وفق ماده نخست قانون امنیت سایبری اهداف کلی این آیین‌نامه را برجسته می‌کند که شامل افزایش امنیت شبکه و اطلاعات در سراسر اتحادیه اروپا می‌شود،[۶] درحالی‌که ماده ۳ وظایف خاص آژانس، مانند حمایت از توسعه سیاست‌های امنیت سایبری و ایجاد ظرفیت در سطح اتحادیه اروپا را شرح می‌دهد.[۷]

---

1 . EU Cybersecurity Act, Regulation (EU) 2019/881, 2019 O.J. (L 151) 15, http://data.europa.eu/eli/reg/2019/881/oj.

۲. در ضمن باید تأکید داشت شورای اروپا طی سال ۲۰۰۱ «کنوانسیون جرم سایبری» را به‌منظور هماهنگ‌سازی سیاست‌های کیفری و تقویت همکاری‌های جهانی در قبال رایاجنگ‌ها وضع کرد که افزون بر جرائم اینترنتی، جرائم مرتبط با استفاده از رایانه‌ها نظیر تبلیغات نژادپرستانه را مقرر نمود؛

- Council of Europe Convention on Cybercrime, Nov. 8, 2001, E.T.S. 185. (hereinafter "*Convention on Cybercrime*").

لازم به‌ذکر است «پیش‌نویس کنوانسیون استانفورد» که در سال ۲۰۰۰ ارائه شد، وفق کنوانسیون جرم سایبری شورای اروپا، بر رایاجنگ‌ها و حفاظت از زیرساخت‌های بحرانی، به‌ویژه تأسیسات انرژی، تمرکز دارد. این پیش‌نویس به جرم‌انگاری تهدیدهای رایاجنگ‌ها و پیشنهاد ایجاد آژانس بین‌المللی امنیت سایبری پرداخته است. با این حال، پیش‌نویس نتواسته در سازمان ملل متحد پیگیری شود؛

-https://web.stanford.edu/~gwilson/Transnatl.Dimension.Cyber.Crime.2001.p.249.pdf;
https://cyberir.mit.edu/site/proposal-international-convention-cyber-crime-and-terrorism/

3. https://djilp.org/international-legal-frameworks-on-cybersecurity-and-data-protection-law/

4. European Union Agency for Cybersecurity (ENISA), https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_en

5 . The EU Cybersecurity Act, SHAPING EUROPE'S DIGITAL FUTURE, EU (Nov. 21, 2024), https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act.

6. Regulation (EU) 2019/881, art. 1, 2019 O.J. (L 151) 15.

7. Regulation (EU) 2019/881, art. 3, 2019 O.J. (L 151) 15.

ماده ٤ نقش آژانس را در ترویج و ارائه مشاوره در مورد صدور گواهینامه امنیت سایبری تعیین می‌کند.[1] علاوه‌بر این، ماده ۷ حمایت آژانس از همکاری عملیاتی در سطح اتحادیه، ازجمله تسهیل تبادل اطلاعات، مشاوره به کشورهای عضو در مورد حوادث امنیت سایبری، سازماندهی رزمایش‌ها، ارائه گزارش وضعیت فنی و کمک به واکنش به بحران‌های امنیت سایبری فرامرزی در مقیاس بزرگ را تشریح می‌کند (Bygrave, 2024: 1).[2] این سند می‌تواند نقش مؤثری در حفاظت از زیرساخت‌های انرژی در قبال رایاجنگ‌ها ایفا کند، اما موفقیت آن وابسته به اتخاذ استانداردهای امنیتی یکپارچه توسط کشورهای عضو و گسترش همکاری‌های بین‌المللی درزمینهٔ تبادل اطلاعات و فناوری‌های امنیتی است. این اقدامات موجب تقویت امنیت سایبری زیرساخت‌های انرژی و کاهش تهدیدهای رایاجنگ‌ها می‌شود (Bartoli, 2025: 502). بنابراین، برای مقابله مؤثر با تهدیدهای رایاجنگ‌ها، کشورهای عضو باید به استانداردهای یکپارچه امنیت سایبری دست یابند و همکاری‌های بین‌المللی را تقویت کنند. این مشکلات موجب شده تا برخی کشورها قادر به محافظت مؤثر از زیرساخت‌های انرژی خود نباشند (Adenekan, 2024: 1).

۴-۲-۴. مقررات عمومی حفاظت از داده‌ها

در دنیای سایبری امروزی، امنیت و حفاظت از داده‌ها به چالش‌های اصلی برای افراد، مشاغل و دولت‌ها تبدیل شده است. با ظهور تهدیدهای رایاجنگ‌ها و نگرانی‌های فزاینده در مورد حریم خصوصی داده‌ها، بسیاری از کشورها به سمت توسعه چارچوب‌های قانونی برای حفاظت از داده‌ها و ایمن‌سازی فضای مجازی حرکت کرده‌اند.[3] ازاین‌رو، مقررات عمومی حفاظت از داده‌ها[4] که از سوی اتحادیه اروپا مصوب شده است، معیارهای سختگیرانه‌ای را برای حفاظت از داده‌های شخصی در سراسر اروپا تعیین کرده است.[5] این مقررات که در ۲۵ مه ۲۰۱۸ به تصویب رسید، با هدف حفاظت از حریم خصوصی افراد در قبال تهدیدهای رایاجنگ‌ها ایجاد شده است.[6]

1. Regulation (EU) 2019/881, art. 4, 2019 O.J. (L 151) 15.
2. Regulation (EU) 2019/881, art. 7, 2019 O.J. (L 151) 15.
3. Cybersecurity Rules Saw Big Changes in 2024: Here's What to Know, *World Economic Forum* (Oct. 17, 2024), https://www.weforum.org/stories/2024/10/cybersecurity-regulation-changes-nis2-eu-2024/.
4. General Data Protection Regulation (GDPR), https://gdpr-info.eu/
5. General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, 2016 O.J. (Apr. 27, 2016).
6. https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/.

مقررات عمومی حفاظت از داده‌ها حول چندین اصل و حقوق کلیدی وضع شده که از داده‌های شخصی افراد محافظت می‌کند. ماده ۵ بر پردازش قانونی، عادلانه و شفاف تأکید دارد و جمع‌آوری داده‌ها را برای اهداف خاص و مشروع الزامی می‌کند، درحالی‌که تضمین می‌کند محدود، دقیق و به‌روز است.[۱] ماده ۶ شرایط پردازش قانونی، مانند اخذ رضایت و انجام تعهدات قانونی را تشریح می‌کند و تعهد مقررات به حفاظت از حقوق افراد را تقویت می‌کند.[۲] ماده ۳۲ بر امنیت داده‌ها تمرکز دارد و کنترل‌کنندگان و پردازنده‌های داده‌ها را ملزم می‌کند که اقدامات فنی و سازمانی مناسبی را برای محافظت از داده‌های شخصی در قبال نقض‌ها اجرا کنند.[۳] علاوه‌بر این، ماده ۲۵ «حفاظت از داده‌ها به صورت طراحی شده و پیش‌فرض» را معرفی می‌کند که سازمان‌ها را ملزم می‌کند از ابتدا اقدامات حفاظت از داده‌ها را در فرآیندهای خود ادغام کنند و درنتیجه جمع‌آوری داده‌های غیرضروری را به حداقل رسانده و حریم خصوصی کلی را افزایش دهند.[٤]

در ضمن باید اذعان شود، «آژانس همکاری عدالت کیفری اتحادیه اروپا»[٥] به‌عنوان مرکز همکاری قضایی اتحادیه اروپا در امور کیفری،[٦] وفق ماده ۸۵ «پیمان لیسبون» و آیین‌نامه آژانس برای تعیین مأموریت، ساختار حاکمیتی، نظام حفاظت از داده‌ها و چارچوب ایجاد توافق‌نامه‌ها با کشورهای غیرعضو اتحادیه اروپا و بهبود رسیدگی به جرائم جدی فرامرزی و سازمان‌یافته از طریق تحریک هماهنگی در تحقیقات و دادستانی در فوریه ۲۰۰۲ تأسیس شد که از ۱۲ دسامبر ۲۰۱۹ لازم‌الاجرا و فعالیت خود را آغاز نمود[۷] (روبو، ۱۴۰۳: ۴۷۵-۴۶۴). در ضمن، آژانس در مقابله با رایاجنگ‌ها مرتبط با زیرساخت‌های حیاتی اتحادیه اروپا از طریق تسهیل همکاری‌های بین‌المللی، پشتیبانی از تحقیقات مشترک و سنجش تهدیدها، به کشورهای عضو در شناسایی، پیشگیری و مقابله با رایاجنگ‌ها و حملات باج‌افزار، نقشی اساسی ایفا می‌کند (Hernández López, 2023: 391-934).[۸]

1. General Data Protection Regulation (EU) 2016/679, art. 5, O.J. L 119 (May 4, 2016).
2. General Data Protection Regulation (EU) 2016/679, art. 6, O.J. L 119 (May 4, 2016).
3. General Data Protection Regulation (EU) 2016/679, art. 32, O.J. L 119 (May 4, 2016).
4. General Data Protection Regulation (EU) 2016/679, art. 25, O.J. L 119 (May 4, 2016).
5. European Union Agency for Criminal Justice Cooperation (Eurojust).
6. https://www.eurojust.europa.eu/about-us/data-protection.
7. https://www.eurojust.europa.eu/about-us/organisation/eurojust-legal-framework.

۸. بر اساس ماده ۸۵ (۱) «معاهده عملکرد اتحادیه اروپا، مصوب ۱۹۵۷» و چارچوب قانونی آژانس، «سند برنامه‌ریزی واحد برای سال‌های ۲۰۲۵ تا ۲۰۲۷» (Eurojust Single Programming Document 2025-2027) با هدف حفظ امنیت سایبری و مقابله با تهدیدهای رایاجنگ‌ها، بر اهدافی نظیر تقویت دفاع در قبال تهدیدهای آن‌ها، تقویت همکاری‌های بین‌المللی، بهره‌گیری از فناوری‌های نوین برای شناسایی و پیشگیری از

با این همه حفاظت از زیرساخت‌های حیاتی انرژی در قبال رایاجنگ‌ها، به‌ویژه در حوزه داده‌های حساس نظیر اطلاعات مشتریان و تأسیسات، اهمیت ویژه‌ای دارد. آسیب به این داده‌ها درنتیجه رایاجنگ‌ها می‌تواند منجر به نقض مقررات حفاظت از داده‌ها و بروز پیامدهای امنیتی جدی شود.[۱]

۴-۲-۵. کنوانسیون بوداپست در مورد جرائم سایبری

با وجود تلاش‌های بین‌المللی برای تصویب «کنوانسیون بوداپست در مورد جرائم سایبری»، چالش‌هایی در پیاده‌سازی آن در کشورهای مختلف وجود دارد، ازجمله تفاوت‌های قانونی، عدم هماهنگی در معیارهای امنیت سایبری و کمبود منابع لازم. این مسائل مانع از مقابله مؤثر با تهدیدات رایاجنگ‌ها علیه زیرساخت‌های انرژی می‌شوند.[۲] کنوانسیون بوداپست نقش مهمی در هماهنگ‌سازی مقررات کشورها دارد و به پیشگیری، پیگرد و همکاری بین‌المللی درزمینهٔ جرائم سایبری می‌پردازد. این معاهده تبادل اطلاعات، استرداد و تحقیقات مشترک را تسهیل کرده و زمینه همکاری‌های قضائی در پیگیری رایاجنگ‌ها مرتبط با زیرساخت‌های انرژی را فراهم می‌کند (Arifi, 2020: 43-44). هم‌گرایی بین‌المللی و تعهد به اجرای کنوانسیون‌ها می‌تواند امنیت جهانی و حفاظت از زیرساخت‌های حیاتی را تضمین کند.[۳]

اصلاح و روزآمدسازی کنوانسیون بوداپست در قبال تهدیدهای نوین و تقویت همکاری بین کشورها درزمینهٔ رایاجنگ‌ها ضرورتی انکارناپذیر است. روزآمدسازی این کنوانسیون امکان پیش‌بینی تهدیدهای آینده را فراهم کرده و حفاظت از زیرساخت‌های انرژی را ایجاد می‌کند. این کنوانسیون با فراهم کردن چارچوب حقوقی برای همکاری‌های بین‌المللی، به کشورهای مختلف در مدیریت مقابله با رایاجنگ‌ها علیه زیرساخت‌های انرژی کمک می‌کند (Koki, 2024: 1).

تهدیدها علیه زیرساخت‌های حیاتی، آموزش و توانمندسازی متخصصان در حوزه امنیت سایبری و حمایت از پژوهش‌های علمی در قبال رایاجنگ‌ها تمرکز دارد. این سند در سال ۲۰۲۴ تدوین و صادر شد؛
https://www.eerstekamer.nl/bijlage/20241122/eurojust_single_programming_2/document3/f=/vmikl3f9o0b6.pdf.

1. https://www.tandfonline.com/doi/full/10.1080/13600834.2019.1573501.

2. https://dig.watch/updates/comparative-analysis-the-budapest-convention-vs-the-un-convention-against-cybercrime.

3. https://pmc.ncbi.nlm.nih.gov/articles/PMC8473297/.

۴-۲-۶. کنوانسیون سازمان ملل متحد علیه جرائم سایبری

با توجه به تحولات فزاینده در فضای سایبری، نظام حقوقی بین‌المللی نیاز به مقررات متناسب، اثرگذار و پاسخگو در این زمینه دارد. ازاین‌رو، پس از بیست سال پیش‌نویس «کنوانسیون سازمان ملل متحد علیه جرائم سایبری» برای تقویت همکاری و به اشتراک‌گذاری شواهد الکترونیکی تهیه شد. چالش‌های اصلی آن شامل صلاحیت شخصی منفعل و حفاظت از داده‌هاست. برخی کشورها ممکن است تلاش کنند مفاد کنوانسیون را با مقررات داخلی خود هماهنگ کنند و شرکت‌های فناوری نقش بیشتری در تعیین قوانین دارند (Shtodina, 2025: 110).

ازاین‌رو، تلاش‌ها برای تدوین معاهده‌ای بین‌المللی درزمینهٔ جرائم سایبری از سال ۲۰۱۰ با ابتکار روسیه آغاز شد. با وجود مخالفت‌هایی از سوی کشورهای غربی که کنوانسیون بوداپست را کافی می‌دانستند، روسیه در سال ۲۰۱۸ موفق به تصویب قطعنامه‌ای در مجمع عمومی سازمان ملل متحد شد که به صدور قطعنامه ۲۴۷/۷۴ در سال ۲۰۱۹ و تشکیل کمیته ویژه برای تدوین یک چارچوب الزام‌آور منجر گردید.[1] این روند نخستین تلاش سازمان ملل متحد برای تنظیم معاهده‌ای خاص در حوزه رایاجنگ‌ها بود که در آگوست ۲۰۲۳، پیش‌نویس کنوانسیون سازمان ملل متحد علیه جرائم سایبری به‌عنوان نخستین سند الزام‌آور در این حوزه به تصویب رسید (Hakmeh, 2024: 125-126). به‌هر روی در اوت ۲۰۲۴، پیش‌نویس نهایی آن با وجود انتقادات مربوط به نقض احتمالی حقوق بشر، با اجماع مورد توافق قرار گرفت.[2] این معاهده نقطه عطفی در مقابله بین‌المللی با رایاجنگ‌ها محسوب می‌شود، هرچند نگرانی‌هایی درباره ضعف ضمانت‌های حقوق بشری در آن وجود دارد.[3]

تصویب این کنوانسیون برای تسهیل همکاری بین‌المللی راجع‌به مسائل پیرامون جرائم سایبری طی سال ۲۰۲٤ در میان مقاومت سازمان‌های حقوق بشری از سوی مجمع عمومی، به‌عنوان یک چارچوب بین‌المللی نوین در قبال جرائم سایبری، راهبردهایی را برای حفاظت از زیرساخت‌های حیاتی، به‌ویژه زیرساخت‌های انرژی،

1. Resolution 74/247 of the United Nations General Assembly. “Countering the use of information and communications technologies for criminal purposes,” A/Res//74/247 adopted 27 December 2019; available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/440/28/PDF/N1944028.pdf?OpenElement.
2. UN. Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, [New York]: UN, 7 Aug. 2024
3. Explanation of Position of the United States on the Adoption of the Resolution on the UN Convention Against Cybercrime in UNGA's Third Committee – United States Mission to the United Nations

ارائه می‌دهد.[۱] البته کنوانسیون یک چارچوب حقوقی نوین در قبال رایاجنگ‌ها است.[۲] کنوانسیون به تأمین امنیت سایبری زیرساخت‌های حیاتی، به‌ویژه انرژی، پرداخته و کشورهای امضا کننده را به همکاری در جمع‌آوری اطلاعات و مقابله با رایاجنگ‌ها تشویق می‌کند. این سند بین‌المللی و جهانی نوظهور، مشابه کنوانسیون بوداپست است، اما در مسیر پیاده‌سازی آن چالش‌هایی مانند تفاوت در مقررات داخلی، عدم وجود استانداردهای یکپارچه امنیتی و مشکلات فنی وجود دارد.[۳]

کنوانسیون مذکور بر جرائم سایبری نظیر دسترسی غیرمجاز به داده‌ها، کلاهبرداری‌های رایانه‌ای و تهدیدات علیه زیرساخت‌های حیاتی تأکید دارد. برخی مواد آن از کنوانسیون بوداپست الهام گرفته‌اند. به علت ماهیت فراملی و ناشناس بودن مرتکبین، تعقیب قضائی این جرائم با چالش‌هایی نظیر تعارض در صلاحیت قضائی مواجه است (Fahmy, 2024: 33-35). ماده ۳۵ کنوانسیون کشورهای عضو را به همکاری بین‌المللی در جمع‌آوری و تبادل شواهد الکترونیکی ملزم می‌کند. محدودیت‌های صلاحیتی در کشورهای غیرعضو نیز مانع اجرای مؤثر آن است. مواد ۳۷ تا ۴۰ بر تقویت همکاری‌ها، روزآمدسازی مقررات و آموزش‌های قضائی تأکید دارند. درنهایت، این کنوانسیون ابزاری مؤثر برای مقابله با تهدیدات سایبری به ویژه حملات به زیرساخت‌های حیاتی است، اما تحقق اهداف آن نیازمند تقویت همکاری‌های بین‌المللی و رفع موانع حقوقی و نظارتی است (Fidler, 2025: 784).

در قبال تهدیدهای ناشی از ارتکاب رایاجنگ‌ها علیه زیرساخت‌های انرژی، کشورهای مختلف باید به این کنوانسیون ملحق شوند و تدابیر امنیتی یکپارچه‌ای را به‌کار گیرند.[۴] علاوه‌بر این، تقویت همکاری‌های بین‌المللی وتبادل اطلاعات درزمینهٔ تهدیدهای رایاجنگ‌ها و توسعه فناوری‌های امنیتی می‌تواند به کاهش تهدیدها و افزایش

---

۱. در ضمن، «پیش‌نویس کنوانسیون سازمان ملل متحد در مورد مقابله با استفاده از فناوری‌های اطلاعات و ارتباطات برای اهداف مجرمانه» با ۸۹ ماده، در ۲۹ ژوئن ۲۰۲۱ به منظور مقابله با تهدیدهای ناشی از جرائم در این حوزه و سوءاستفاده‌های مجرمانه مانند حمله‌های رایانه‌ای، جاسوسی، تروریسم، کلاهبرداری و قاچاق داده‌ها، تدوین شد (Tennant, I, & Oliveira, 2024: 221). این کنوانسیون وفق قطعنامه ۲۷۴/۷۴ مجمع عمومی سازمان ملل متحد مورخ ۲۷ دسامبر ۲۰۱۹ ایجاد گردید؛

- https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_E.pdf

2. https://www.unodc.org/unodc/en/press/releases/2024/December/un-general-assembly-adopts-landmark-convention-on-cybercrime.html

3. https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_english.pdf

4. https://law.yale.edu/yls-today/news/panel-shares-insights-drafting-new-un-cybercrime-treaty

امنیت زیرساخت‌های انرژی کمک کند.[1] افزون بر این، ایجاد استانداردهای یکپارچه و توسعه آموزش‌های مشترک برای متخصصان امنیت سایبری ازجمله راهکارهای مؤثر است.[2]

۵. سنجش رویکرد مقرراتیِ ایران و قطر

رایاجنگ‌ها علیه زیرساخت‌های انرژی تهدیدهایی پیچیده و خطرناک هستند که می‌توانند آسیب‌های اقتصادی و اجتماعی قابل توجهی به همراه داشته باشند. این زیرساخت‌ها به فناوری‌های رایانه‌ای وابسته‌اند که تهدیدهای رایاجنگ‌ها را افزایش می‌دهند. اگرچه در ایران و قطر مقرراتی در این زمینه وجود دارد، اما همچنان نیاز به سیاست‌ها و راهبردهای حقوقی بیشتر برای تقویت امنیت سایبری و حفاظت از این زیرساخت‌ها احساس می‌شود.

در حقوق ایران، قانون جرائم رایانه‌ای مصوب ۱۳۸۸ مهم‌ترین سند در مقابله با رایاجنگ‌ها است و جرائمی مانند دسترسی غیرمجاز و سرقت اطلاعات را جرم‌انگاری می‌کند. بااین‌حال، این قانون به‌طور مستقیم زیرساخت‌های انرژی و سامانه‌های کنترل صنعتی را پوشش نمی‌دهد. با وجود افزایش توجه به امنیت سایبری، فقدان مقررات تخصصی و زیرساخت‌های مناسب همچنان چالشی جدی در حفاظت از زیرساخت‌های حیاتی به شمار می‌آید (ر.ک: ملکی عزین‌آبادی و جمالی ۱۴۰۳: ۸۹-۸۸).

مقررات کیفری ایران به رایاجنگ‌ها علیه زیرساخت‌های انرژی توجه کرده، اما مشکلاتی در شناسایی و پیگیری این پدیده وجود دارد. با توجه به پیشرفت فناوری و تهدیدهای نوین، مقررات فعلی ناکافی هستند و نیاز به تدوین سیاست‌های کیفری نوین برای حفاظت از زیرساخت‌های فنی و انرژی احساس می‌شود (سلیمانی و دیگران، ۱۴۰۳: ۲۵۱). رویکرد ایران برای تنظیم مقررات فضای سایبری در سطح ملی باید مبتنی بر «پارادایم پاترنالیستی»[3] باشد و در سطح بین‌المللی از «لیبرتارینیسم»[4] تبعیت کند (حسینی، ۱۴۰۲: ۱۲۱۳). لازم به ذکر است نگرش ایران، به‌طور اساسی مبتنی بر شیوه قانون‌گذاری ملی است. ازاین‌رو، عملکرد ایران در سطح بین‌المللی، حاکی از پذیرش روش مختلط در قانون‌گذاری در فضای سایبری است (ضیایی و شکیب‌نژاد، ۱۳۹۶: ۲۲۷؛ ر.ک: فرجی‌ها و علمداری، ۱۳۹۶: ٦٤١-٦٣٩).

1. https://blog.prif.org/2024/12/09/between-a-rock-and-a-hard-place-the-un-cybercrime-convention/.
2. http://su.diva-portal.org/smash/get/diva2:1957464/FULLTEXT01.pdf.
3. Paternalistic Paradigm
4. Libertarianism

در راستای مقابله با رایاجنگ‌ها علیه زیرساخت‌های حیاتی، «طرح امن‌سازی زیرساخت‌های حیاتی در قبال حملات سایبری» به‌عنوان یک برنامه جامع به منظور حفاظت از زیرساخت‌های حساس کشور[۱] در قبال تهدیدهای رایاجنگ‌ها، توسط مرکز مدیریت راهبردی امنیت فضای تولید و تبادل اطلاعات ریاست جمهوری ایران تدوین و در سال ۱۳۹۸ به کلیه سازمان‌ها و دستگاه‌های اجرایی دارای زیرساخت‌های حیاتی کشور ابلاغ شده است.[۲] البته می‌توان به اسنادی دیگر نظیر «سیاست‌های کلی نظام در امور امنیت فضای تولید و تبادل اطلاعات و ارتباطات (افتا)، ابلاغی ۱۳۸۹»، «سند راهبردی پدافند سایبری کشور، مصوب ۱۳۹٤»، «آیین‌نامه اجرایی قانون تعیین حریم حفاظتی‌امنیتی اماکن و تأسیسات کشور، مصوب ۱۳۹۷» و «سند راهبردی جمهوری اسلامی ایران در فضای مجازی، مصوب ۱٤۰۱» اشاره داشت که امکان مقابله با آماج‌های رایاجنگ‌ها علیه امنیتِ زیرساخت‌های حیاتی کشور را فراهم می‌نماید (ر.ک: نظری‌نژاد و پورشاسب، ۱۳۹۹: ۲۹٦؛ تقی‌پور و دیگران، ۱۳۹۸: ۲۱-۱۷).

برای مقابله رایاجنگ‌ها در قطر، «قانون پیشگیری جرائم سایبری قطر (قانون شماره ۱٤، مصوب ۲۰۱٤)» وضع که وفق آن، فعالیت‌های گوناگون سایبری نظیر دسترسی غیرمجاز به سامانه‌ها و داده‌ها، کلاهبرداری و حملات به شبکه‌های اطلاعاتی جرم‌انگاری شد. بااین‌حال، مشابه با ایران، این مقررات بیشتر به ابعاد عمومی جرائم ارتکابی در فضای سایبری پرداخته و کمتر به تهدیدهای خاص علیه زیرساخت‌های انرژی توجه دارند. البته «قانون شماره ۱۳، مصوب ۲۰۱٦» موسوم به «قانون حفاظت از حریم خصوصی داده‌های شخصی»، دستورالعمل‌ها و مقرراتی را برای پردازش داده‌های شخصی در داخل کشور تعیین می‌کند.[۳] هدف این قانون محافظت از حقوق افراد برای حفظ حریم خصوصی و تضمین شفافیت، صداقت و احترام به کرامت انسانی هنگام کار با داده‌های شخصی است.[٤] به دیگر تعبیر، هدف این قانون حفاظت از حقوق افراد در حفظ حریم خصوصی

---

۱. لازم به تأکید است که وفق بند (ب-۱) از ماده نخست «نظام فنی و تخصصی حفاظت از زیرساخت‌های کشور، مصوب ۱۴۰۲» و بند هفتم از ماده نخست «طرح راهبردی حفاظت از زیرساخت‌های کشور، مصوب ۱۴۰۲» توصیف زیرساخت‌ها و نحوه حفاظت از آن‌های مورد پردازش قرار گرفته است.

2. https://amnafzar-rayka.ir/.pdf

3 . Law No. (13) of 2016 on Protecting Personal Data Privacy, https://assurance.ncsa.gov.qa/sites/default/files/library/2020-11/Law%20No.%20%2813%29%20of%202016%20%20on%20Protecting%20Personal%20Data%20Privacy%20-%20English.pdf

4. https://www.squirepattonboggs.com/~/media/files/insights/publications/2017/11/qatars-new-protection-of-personal-data-privacy-law/28492--qatars-new-protection-of-personal-data-privacy-law.pdf

و تضمین شفافیت و احترام به کرامت انسانی هنگام کار با داده‌های شخصی است. این قانون مسئولیت‌های کنترل کنندگان و پردازشگران داده‌ها را برای حفاظت از داده‌های شخصی در قبال خطرات گوناگون مشخص می‌کند و با معرفی الزامات آموزشی و اقدامات پیشگیرانه، صلاحیت پردازنده‌های داده‌ها را تضمین می‌نماید.[1] در ضمن، «راهبرد ملی امنیت سایبری قطر ۲۰۲٤-۲۰۳۰»[2] با هدف قرار دادن این کشور به‌عنوان مجری در پذیرش ایمن فناوری‌های نوظهور، همسو با چشم‌انداز ملی قطر ۲۰۳۰ تدوین شده است. این راهبرد بر رویکردی آینده‌نگر تأکید دارد و بر ادغام ایمن فناوری‌هایی نظیر هوش مصنوعی و محاسبات کوانتومی تمرکز دارد. افزون بر این، حفاظت از زیرساخت‌های حیاتی (نظیر زیرساخت‌های انرژی) و ترویج تحقیق و توسعه درزمینهٔ امنیت سایبری را در اولویت قرار می‌دهد.[3]

مطالعات تطبیقی مقررات ایران و قطر نشان می‌دهد که هر دو کشور مقررات عمومی در قبال رایاجنگ‌ها دارند، اما قطر وفق قانون پیشگیری از جرائم سایبری به مسائل زیرساخت‌های حیاتی توجه بیشتری دارد. ایران بیشتر بر مقررات داخلی متمرکز است و کمتر به امنیت زیرساخت‌های حیاتی پرداخته است. به‌علاوه، قطر به‌طور مؤثرتری درزمینهٔ همکاری‌های بین‌المللی امنیت سایبری فعالیت کرده است. این مقایسه نشان می‌دهد که چالش‌های اساسی در مقابله با رایاجنگ‌ها علیه زیرساخت‌های انرژی در هر دو کشور وجود دارد. ازاین‌رو، با توجه به مقررات موجود در ایران و قطر، چالش‌های اساسی در فرایند مقابله با رایاجنگ‌ها علیه امنیتِ زیرساخت‌های انرژی مشتمل بر موارد ذیل قابل ملاحظه است:

الف. فقدان وجود مقررات خاص برای حفاظت از زیرساخت‌های انرژی؛ ایران و قطر نیازمند روزآمدسازی و تکمیل مقررات خود برای محافظت از زیرساخت‌های انرژی در قبال تهدیدهای رایاجنگ‌ها هستند؛

ب. ضعف و نقصان همکاری‌های بین‌المللی؛ علی‌رغم پیشرفت‌های قطر در این زمینه، ایران و قطر نیازمند تقویت همکاری‌های بین‌المللی در قبال رایاجنگ‌ها و تهدیدهای جهانی هستند؛

---

1. https://assurance.ncsa.gov.qa/en/privacy/law

2 . The National Cyber Security Strategy 2024-2030, https://www.gco.gov.qa/en/media-centre/top-news/the-national-cyber-security-strategy-2024-2030-is-launched/

۳. این راهبرد در ارکان گوناگونی تدوین یافته است: ۱. تقویت ایمنی و تاب‌آوری اکوسیستم امنیت سایبری قطر؛ ۲. تدوین و اجرای قانون برای فضای سایبری امن؛ ۳. تقویت اقتصاد پررونق، داده‌محور و نوآورانه؛ ۴. ترویج تحقیق، توسعه و نوآوری در امنیت سایبری؛ ۵. ایجاد فرهنگ امنیت سایبری با ارتقای مهارت نیروی کار ملی؛ ۶. تقویت همکاری منطقه‌ای و بین‌المللی در امنیت سایبری. راهبرد ملی امنیت سایبری ۲۰۲۴-۲۰۳۰ یک چارچوب جامع، سازگار و آینده‌نگر است که برای پاسخگویی به تغییرات در حال تحول و چالش‌های روبه رشد امنیت فضای مجازیِ عصر دیجیتال طراحی شده است.

ج. توسعه فناوری‌های امنیتی؛ بهره‌گیری از فناوری‌های پیشرفته در حفاظت از زیرساخت‌های انرژی ازجمله سامانه‌های کنترل صنعتی و شبکه‌های ارتباطی ضرورتی انکارناپذیر است.

مقابله با رایاجنگ‌ها علیه زیرساخت‌های انرژی نیازمند تدابیر قانونی و امنیتی پیشرفته است. مقررات موجود در ایران و قطر در قبال تهدیدهای رایاجنگ‌ها مناسب هستند، اما برای مقابله مؤثرتر با تهدیدهای خاص علیه زیرساخت‌های انرژی، نیاز به روزآمدسازی این مقررات و اتخاذ راهبردهای نوین است. در ضمن، همکاری‌های بین‌المللی و توسعه فناوری‌های پیشرفته به‌عنوان راهکارهای مؤثر در این زمینه هستند.[۱]

نتیجه‌گیری

زیرساخت‌های انرژی به‌واسطه وابستگی به سامانه‌های رایانه‌ای، در قبال تهدیدهای رایاجنگ‌ها آسیب‌پذیر شده‌اند. رایاجنگ‌ها می‌توانند تأمین انرژی را مختل کرده و پیامدهای اقتصادی و اجتماعی به دنبال داشته باشند. اسناد مقرر همکاری‌های بین‌المللی را تسهیل کرده‌اند، اما برای افزایش اثربخشی این اسناد، ضروری است که کشورها به آن‌ها بپیوندند و تبادل اطلاعات، استانداردهای امنیتی، سرمایه‌گذاری در فناوری‌های نوین و آموزش نیروی انسانی متخصص تقویت شود.

با افزایش رایاجنگ‌ها علیه امنیتِ زیرساخت‌های انرژی، اسناد بین‌المللی توانایی ایجاد چارچوب‌های قانونی مؤثر را دارند، اما چالش‌هایی مانند افتراق مقررات ملی و عدم هماهنگی جهانی، اجرای این چارچوب‌ها را سخت کرده است. برای مقابله مؤثر، همکاری‌های بین‌المللی باید تقویت و استانداردهای امنیتی مشترک تدوین شود. امنیت پایدار نیازمند تعهد دولت‌ها به اجرای هماهنگ این ابزارها است. ازاین‌رو، برای مقابله مؤثر با رایاجنگ‌ها، می‌توان مجموعه‌ای از راهکارهای ذیل را به‌عنوان استانداردهای جهانی در اسناد بین‌المللی پیشنهاد کرد:

الف. به‌کارگیری هوش مصنوعی، یادگیری ماشین، رمزنگاری پیشرفته و سامانه‌های پایش مستمر برای شناسایی، پیشگیری و واکنش سریع به رایاجنگ‌ها؛

---

۱. لازم به ذکر است با توجه به عضویت ایران در سازمان بریکس (BRICS)، همکاری‌های بین‌المللی می‌تواند کمبودهای مقابله با رایاجنگ‌ها علیه زیرساخت‌های انرژی را جبران کند. این همکاری‌ها باید شامل تقویت امنیت سایبری، تبادل اطلاعات، آموزش نیروهای متخصص، تقویت زیرساخت‌های قانونی و ایجاد سامانه‌های مقاوم باشد. البته، سازمان بریکس باید از ظرفیت فناوری‌های نوین در قبال تهدیدهای فزاینده و پیچیده استفاده کند و به همکاری‌های منطقه‌ای و بین‌المللی ادامه دهد؛

- https://brics.br/en/news/brics-strengthens-cooperation-on-cybersecurity

ب. ایجاد سامانه‌های مقاوم، تقویت زیرساخت‌های امنیتی غیرفیزیکی، تبادل اطلاعات بین‌المللی و آموزش نیروهای متخصص برای افزایش آمادگی و تاب‌آوری؛

ج. تدوین استانداردها و چارچوب‌های قانونی بین‌المللی، تعیین مسئولیت‌ها، استرداد مرتکبان رایاجنگ‌ها و تقویت همکاری‌های قضایی از طریق اسناد بین‌المللی نظیر کنوانسیون بوداپست و حتی کنوانسیون سازمان ملل متحد علیه جرائم سایبری.

بنابراین، راهکارهای مزبور، یک چارچوب جامع برای حفاظت از زیرساخت‌های انرژی در قبال رایاجنگ‌ها را فراهم نموده و موجب ایجاد امنیت پایدار در مقیاس جهانی می‌شوند. در انتها، راجع‌به مطالعه تطبیقی مقررات ایران و قطر در قبال رایاجنگ‌ها اعم از تخریبگر و مختل کننده علیه زیرساخت‌های انرژی، اذعان می‌گردد ایران بر تقویت مقررات داخلی و بهره‌گیری از ظرفیت‌های ملی تأکید دارد، درحالی‌که قطر رویکردی بین‌المللی‌محور اتخاذ کرده و بر همکاری‌های فراملی و تبعیت از استانداردهای جهانی تمرکز دارد. در ضمن، ایران و قطر اهمیت الحاق به اسناد بین‌المللی را پذیرفته‌اند، اما قطر در اجرای مؤثر چارچوب‌های حقوقی بین‌المللی عملکرد فعال‌تری دارد.

فهرست منابع

حسینی، محمدرضا. (۱۴۰۲). «الگوهای مقررات‌گذاری در فضای سایبر: ارائهٔ چارچوب جامع تنظیم‌گری برای محیط ملی». **مطالعات حقوق عمومی**، دوره ۵۳، شماره ۳.

سلیمانی، سودابه؛ رضوی‌فرد، بهزاد و صفایی، مریم (۱۴۰۳). «سیاست‌گذاری در مورد جرائم سایبری علیه زیرساخت‌های انرژی‌های نوپدید و بازنمایی آن در نظام حقوق کیفری ایران و فرانسه». **تحولات سیاسی اجتماعی معاصر ایران**، دوره ۳، شماره ۴.

شاملو، باقر و حسینی، مهدی (۱٤۰۳). «رایاجنگ‌های مختل‌کنندهٔ زیرساخت‌های حیاتی به‌مثابهٔ جنایت جنگی». **آموزه‌های حقوق کیفری**، دوره ۲۷، شماره ۲۱.

ضیایی، سید یاسر و شکیب‌نژاد، احسان (۱۳۹۶). «قانون‌گذاری در فضای سایبر: رویکرد حقوق بین‌الملل و حقوق ایران». **مجله حقوقی بین‌المللی**، دوره ۳۷، شماره ۵۷.

فرجی‌ها، محمد و علمداری، علی (۱۳۹۶). «مطالعهٔ تطبیقی معیارهای جرم‌انگاری در فضای سایبر در نظام کیفری ایران و آلمان». **مطالعات حقوق تطبیقی**، دوره ۸، شماره ۲.

تقی‌پور، رضا و همکاران (۱۳۹۸). «الگوی راهبردی حفاظت سایبری از زیرساخت‌های اطلاعاتی حیاتی جمهوری اسلامی ایران». **امنیت ملی**، دوره ۹، شماره ۳۴.

محمودزاده، ابراهیم؛ حسنی‌اصل، حمیدرضا؛ قوچانی، محمدمهدی و نیک‌نفس، علی (۱۳۹۷). «تدوین راهبردهای امنیت سایبری سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی کشور». **مطالعات بین‌رشته‌ای دانش راهبردی**، دوره ۸، شماره ۳۱.

ملکی عزین‌آبادی، روح‌الله و جمالی، جواد (۱۴۰۳). «مطالعه مقایسه‌ای قوانین سایبری چین، ایالات‌متحده آمریکا و روسیه؛ بایسته‌ها و ضرورت‌های امنیت سایبری جمهوری اسلامی ایران». **آمار و فناوری دفاعی**، دوره ۷، شماره ۳.

معاونت پژوهش و تولید علم دانشگاه اطلاعات و امنیت ملی. (۱۳۹۶). **حفاظت سایبری از زیرساخت‌های حیاتی**. تهران: موسسهٔ چاپ و انتشارات دانشگاه اطلاعات و امنیت ملی.

نظری‌نژاد، احمدعلی و عبدالعلی‌پورشاسب، عبدالعلی (۱۳۹۹). الگوی راهبردی حفاظت سایبری از زیرساخت‌های اطلاعاتی حیاتی جمهوری اسلامی ایران. **مطالعات دفاعی استراتژیک**، دوره ۱۸، شماره ۸۲.

References

Abdallah, M. & Abdallah, A. Y. (2025). The International Legal Frameworks to Combat Cybercrime in the Era of Artificial Intelligence. *International Journal of Economic Perspectives*, 19 (5), 2534-2548.

- Adenekan, T. K. (2024). Cybersecurity Challenges and Solutions for Critical Energy Infrastructure in the Digital Age. *Research Gate*. https://www.researchgate.net/publication/385681419_Cybersecurity_Challenges_and_Solutions_for_Critical_Energy_Infrastructure_in_the_Digital_Age

- Ahmad, T, Zhang, D, Huang, C, Zhang, H, Dai, N, Song, Y, & Chen, H. (2021). Artificial Intelligence in Sustainable Energy Industry: Status, Challenges and Opportunities. *Journal of Cleaner Production, 289*, 125834.

- Arifi, D, & Arifi, B. (2020). Cybercrime: A Challenge to Law Enforcement. *South East European*

University Review, 15 (2), 42-55.
- Bartoli, L. (2025). Cybersecurity and the Fight against Cybercrime: Partners or Competitors? *European Journal of Risk Regulation*, 16 (2), 498-513.
- Bygrave, L. A. (2024). The Emergence of EU Cybersecurity Law: A Tale of Lemons, Angst, Turf, Surf and Grey Boxes. *Computer Law & Security Review*, University of Oslo Faculty of Law Research Paper No. 2024-04.
- Blotzer, P. (2018). The Threat is Real: Protecting the Energy Infrastructure From Cyberattacks. *Barry Law Review*, 24 (1), 39-58.
- DiPietro, B. (2015). *Survey Roundup: Deadly Cyberattack Worries*. *The Wall Street Journal*. http://on.wsj.com/1CVsrWK
- Cohen, A. (2010). Cyberterrorism: Are We Legally Ready? *The Journal of International Business & Law*, 4 (15), 18-32.
- Fahmy, W. (2024). The Cybercrime Acts and the Electronic Transaction in International Law. *Economics Law and Policy*, 7 (1), 18-41.
- Fidler, M. (2025). Fragmentation of international cybercrime law. *Utah Law Review*, 3 (4), 737-804.
- Freeze, C. (2016). *Hackers target Canadian Government's Energy and Resource Departments*. *The Globe & Mail*. http://www.theglobeandmail.com/news/politics/hackers-target-governments-energy-and-resource-departments/article32890960/, archived at https://perma.cc/9Z7L-RF6Y.
- Gallagher, S. (2017). *FBI-DHS "Amber" Alert Warns Energy Industry of Attacks on Nuke Plant Operators*. *ARS Technica*. https://arstechnica.com/information-technology/2017/07/dhs-fbi-warn-of-attempts-to-hack-nuclear-plants/, archived at https://perma.cc/E52M-ER7X
- Hakmeh, J. (2024). The UN Convention on Cybercrime: A Milestone in Cybercrime Cooperation? *Journal of Cyber Policy*, 9 (2), 125-130.
- Hernández López, A, & Jiménez-Villarejo Fernández, F. (2023). Eurojust. in K. Ambos & P. Rackow (Eds.), *The Cambridge Companion to European Criminal Law* (pp. 387-412). Cambridge University Press.
- Koki, S. I. (2024). Analysing the International Convention on Cybercrime and the Nigeria Cybercrimes Act 2015: An Explanatory Literature Review. *ResearchGate*. https://www.researchgate.net/publication/386552531_ANALYSING_THE_INTERNATIONAL_CONVENTION_ON_CYBERCRIME_AND_THE_NIGERIA_CYBERCRIMES_ACT_2015_AN_EXPLANATORY_LITERATURE_REVIEW
- Küfeoğlu, S, & Akgün, A. T. (2024). *Cyber Resilience in Critical Infrastructure* (pp. 29–31). Routledge Taylor & Francis.
- Kushner, D. (2013). The Real Story of Stuxnet. *IEEE Spectrum*, 50 (3), 48-53.
- Onyeji, I, Bazilian, M, & Bronk, C. (2014). Cyber Security and Critical Energy Infrastructure. *The Electricity Journal*, 27 (2), 52-60.
- Pagliery, J. (2016). *Scary Questions in Ukraine Energy Grid Hack*. *CNN Tech*. http://money.cnn.com/2016/01/18/technology/ukraine-hack-russia/, archived at https://perma.cc/975L-VD3X
- Pagliery, J. (2016). *Government Reveals Details about Energy Grid Hacks*. *CNN Tech*. http://money.cnn.com/2016/04/05/technology/energy-grid-hacks/, archived at https://perma.cc/P965-2YYH
- Siig, K, Feldtmann, B, & Billing, F. M. W. (2024). *The United Nations Convention on the Law of the Sea: A System of Regulation*. Routledge & CRC Press.
- Silver, A. (2016). *Why Do Hackers Love to Attack Canada's Energy Departments? IEEE Spectrum*. http://spectrum.ieee.org/energywise/energy/the-smarter-grid/why-do-hackers-love-to-attack-canadas-energy-environment-and-natural-resources-sector, archived at https://perma.cc/T32F-

XMFS
- Shtodina, D. D. (2025). United Nations Convention against Cybercrime, 2024 – the Outcome of «Cyber Compromise»? *Moscow Journal of International Law*, 1, 110-124.
- Tennant, I, & Oliveira, A. P. (2024). Applying the Right Lessons from the Negotiation and Implementation of the UNTOC and the UNCAC to the Implementation of the Newly agreed UN 'Cybercrime' Treaty. *Journal of Cyber Policy*, 9 (2), 221-238.
- Zetter, K. (2017). *The Ukrainian Power Grid was Hacked Again*. *MOTHERBOARD*. https://motherboard.vice.com/en_us/article/ukrainian-power-station-hacking-december-2016-report, archived at https://perma.cc/C8NY-W26X
- Venkatachary, S. K, Alagappan, A, & Andrews, L. J. B. (2021). Cybersecurity Challenges in Energy Sector (Virtual Power Plants) - Can Edge Computing Principles be Applied to Enhance Security? *Energy Informatics*, 4 (1), 1-21.

In Persian

- Deputy for Research and Science Production, National Intelligence and Security University (2017). Cyber Protection of Critical Infrastructures. Tehran: National Intelligence and Security University Printing and Publishing Institute.
- Farajiha, Mohammad; Alamdari, Ali (2017). A Comparative Study of Criminalization's Criteria in Cyberspace in the Iranian and German Penal Systems. *Comparative Law Studies*, 8 (2), 637-653.
- Hosseini, Mohammad Reza (2023). Regulation-making Patterns in Cyberspace: Providing a Comprehensive Regulatory Framework for the National Environment. *Public Law Studies*, 53 (3), 1213-1239.
- Mahmoudzadeh, Ebrahim; Hassani-Asl, Hamidreza; Ghochani, Mohammad Mehdi; and Niknafs, Ali (2018). Developing Cybersecurity Strategies for Industrial Control Systems in the Country's Critical Infrastructures. *Interdisciplinary Studies in Strategic Knowledge*, 8 (31), 253-281.
- Maleki Azinabadi, Ruhollah & Jamali, Javad (2024). A Comparative Study of Cyber Laws of China, the United States of America and Russia; The Essentials and Necessities of Cyber Security of the Islamic Republic of Iran. *Defense Equipment and Technology*, 7 (3), 77-108.
- Nazarinejad, Ahmad Ali & Abdolalipourshaseb, Abdol-Ali (2012). Strategic Model of Cyber Protection of Critical Information Infrastructures of the Islamic Republic of Iran. *Strategic Defense Studies*, 18 (82), 313-336.
- Shamloo, Baqer & Hosseini, Mehdi (2024). Cyberwars Disrupting Critical Infrastructure as a War Crime. *Criminal Law Doctrines*, 27 (21), 115-152.
- Soleimani, Sudabeh; Razavifard, Behzad; Safaei, Maryam (2024). Policy-making on Cybercrimes against Emerging Energy Infrastructures and its Representation in the Iranian and French Criminal Law Systems. *Contemporary Iranian Social and Political Developments*, 3 (4), 251-279.
- Taghipour, Reza et. al. (2019). Strategic model for Cyber Protection of Critical Information Infrastructures of the Islamic Republic of Iran. *National Security*, 9 (34), 7-48.
- Ziaei, Seyed Yaser & Shakibnejad, Ehsan (2017). Legislation in Cyberspace: An International Law and Iranian Law Approach. *International Law Journal*, 37 (57), 227-249.