Received: 10 /10/2024
Review: 04/01/2025
Accepted: 10 /04/2025
DOI: 10.22054/jocl.2025.85062.1275

Journal of Cyber Law
No(1),Vol(2), 82-94
ISSN: 0972-6934
www.jocl.ir

cyber Law and Regulatory Challenges of Hybrid Cyber Attacks Against Critical Infrastructures

Kamran Mirdamadi Asl[1]

1- PhD Candidate in Law, University of Shiraz, Shiraz, Iran

ABSTRACT

Cyber law has become a fundamental pillar of national security and the protection of critical infrastructures in the digital age. A central question in this domain is how legal and regulatory frameworks can address hybrid cyber attacks that simultaneously target technical, human, and economic aspects of critical systems. The importance of studying this issue stems from the potentially widespread destructive impacts of such attacks on national security, economy, and society, and the existing legal gaps complicating effective response. This article aims to identify the legal and regulatory challenges in countering hybrid cyber attacks against critical infrastructures and to propose mechanisms for improving governance frameworks. The research method is descriptive–analytical and based on documentary analysis, including the review of national and international laws, cybersecurity reports, and case studies of recent attacks. The findings indicate that major challenges include the lack of a harmonized legal framework, limitations in international cooperation, the complexity of defining hybrid attacks, and weaknesses in oversight and preventive capacities. Furthermore, the article presents innovative legal and policy solutions to enhance the protection of critical infrastructures against hybrid cyber threats. The results can inform the development of proactive policies and comprehensive cyber law regulations at national and regional levels, shedding light on new dimensions of governance and responses to complex cyber threats.

Keywords:
Cyber law, Hybrid attacks, Critical infrastructures, Regulation, Cybersecurity

How to Cite: mirdamadiasl, K. (2025). cyber Law and Regulatory Challenges of Hybrid Cyber Attacks Against Critical Infrastructures. Journal of Cyber Law (JOCL), 2(1), 82-94.
doi: 10.22054/jocl.2025.85062.1275

* Corresponding Author: kamran.mirdamadiasl@shirazu.ac.ir

نشریه حقوق سایبری
شماره (۱) ۸۲-۹۴
دوره ۱۴۰۴

تاریخ دریافت: ۱۴۰۳/۰۷/۲۰
تاریخ اصلاح: ۱۴۰۳/۱۰/۱۴
تاریخ پذیرش: ۱۴۰۴/۰۱/۲۲

حقوق سایبری و چالش‌های تنظیم‌گری حملات سایبری ترکیبی علیه زیرساخت‌های حیاتی

کامران میردامادی اصل[۱]

۱- دانشجوی دکترای حقوق، دانشگاه شیراز، شیراز، ایران

چکیده

حقوق سایبری در عصر دیجیتال به یکی از محورهای اساسی امنیت ملی و حفاظت از زیرساخت‌های حیاتی تبدیل شده است. یکی از مهم‌ترین پرسش‌های این حوزه، چگونگی مواجهه قانونی و تنظیم‌گری با حملات سایبری ترکیبی است که می‌توانند همزمان ابعاد فنی، انسانی و اقتصادی زیرساخت‌های حیاتی را هدف قرار دهند. اهمیت بررسی این موضوع از آنجا ناشی می‌شود که چنین حملاتی می‌توانند اثرات مخرب گسترده‌ای بر امنیت ملی، اقتصاد و جامعه داشته باشند و خلاهای قانونی موجود، پاسخ‌دهی مناسب را پیچیده می‌سازد. هدف این مقاله، شناسایی چالش‌های حقوقی و مقرراتی مرتبط با مقابله با حملات سایبری ترکیبی علیه زیرساخت‌های حیاتی و ارائه راهکارهای بهبود سازوکارهای تنظیم‌گری است. روش پژوهش در این مقاله توصیفی–تحلیلی و مبتنی بر مطالعه اسنادی است که شامل بررسی قوانین ملی و بین‌المللی، گزارش‌های امنیت سایبری و مطالعات موردی حملات اخیر می‌باشد. یافته‌های پژوهش نشان می‌دهد که اصلی‌ترین چالش‌ها شامل نبود چارچوب قانونی هماهنگ، محدودیت در همکاری‌های بین‌المللی، پیچیدگی تعریف حملات ترکیبی و ضعف در ظرفیت‌های نظارتی و پیشگیرانه است. همچنین، این مقاله با ارائه راهکارهای حقوقی و سیاست‌گذاری نوآورانه، امکان تقویت حفاظت از زیرساخت‌های حیاتی در برابر تهدیدات سایبری ترکیبی را بررسی می‌کند. نتایج پژوهش می‌تواند مبنای تدوین سیاست‌های پیشگیرانه و توسعه مقررات حقوق سایبری جامع در سطح ملی و منطقه‌ای قرار گیرد و ابعاد جدیدی از تنظیم‌گری و پاسخ به تهدیدات پیچیده سایبری را روشن سازد.

کلیدواژه‌ها:

حقوق سایبری، حملات ترکیبی، زیرساخت‌های حیاتی، تنظیم‌گری، امنیت سایبری

نحوه استناد:

میردامادی اصل, کامران . (۱۴۰۴). حقوق سایبری و چالش‌های تنظیم‌گری حملات سایبری ترکیبی علیه زیرساخت‌های حیاتی. حقوق سایبری, ۲(۱), ۸۲-۹۴

* ایمیل نویسنده مسئول: kamran.mirdamadiasl@shirazu.ac.ir

مقدمه

در دنیای امروز، توسعه فناوری اطلاعات و ارتباطات و همزمان افزایش وابستگی جوامع به زیرساخت‌های حیاتی، زمینه‌ساز بروز تهدیدات پیچیده سایبری شده است. حملات سایبری ترکیبی که می‌توانند به‌طور همزمان ابعاد دیجیتال، فیزیکی و انسانی زیرساخت‌ها را هدف قرار دهند، به یکی از مهم‌ترین چالش‌های حقوق سایبری تبدیل شده‌اند. این نوع حملات با پیچیدگی‌های تکنیکی و تعامل با سایر تهدیدات امنیتی، مدیریت قانونی و نظارتی را دشوار ساخته‌اند و نیازمند تحلیل دقیق حقوقی و تدوین سیاست‌های تنظیم‌گری مؤثر هستند (Bace, 2024,p.12).در نظام حقوقی جمهوری اسلامی ایران، قانون جرایم رایانه‌ای مصوب ۱۳۸۸ به‌عنوان چارچوب اصلی مقابله با جرایم سایبری شناخته می‌شود. ماده ۱ این قانون، دسترسی غیرمجاز، شنود، تخریب داده‌ها و سیستم‌ها و سایر اقدامات مشابه را جرایم رایانه‌ای تعریف کرده است (قانون جرایم رایانه‌ای، ۱۳۸۸، ص. ۲۳). با این حال، عدم تطابق کامل این قانون با پیچیدگی‌های حملات ترکیبی، خلاهایی در زمینه شفافیت تعاریف و هماهنگی بین نهادهای مسئول ایجاد کرده است (پورغهرامی، ۱۳۹۶، ص. ۵).مقالات اخیر نشان می‌دهند که حملات ترکیبی نه تنها تهدیدهای دیجیتال را شامل می‌شوند، بلکه می‌توانند باعث اختلال در شبکه‌های انرژی، حمل و نقل، سیستم‌های آب و درمان و حتی تهدید امنیت شهروندان شوند. میرزازاده (۱۳۹۹، ص. ۳۴) در مطالعه‌ای تحلیلی بر روی حملات ترکیبی زیرساخت‌های حیاتی، بر ضرورت بازنگری قوانین موجود و تدوین مقررات تکمیلی برای پوشش حملات چندبُعدی تأکید کرده است. او معتقد است که فقدان تعریف جامع جرم و نبود الزامات پیشگیرانه، باعث کاهش اثرگذاری حقوقی مقابله با این حملات می‌شود.همچنین شریفی (۱۴۰۰، ص. ۲۲) با تحلیل تجربیات قضایی ایران، بر اهمیت ایجاد هماهنگی میان نهادهای قضایی، امنیتی و فنی تأکید کرده است. او نشان داده است که بسیاری از پرونده‌های حملات سایبری، در نبود دستورالعمل‌های شفاف و هماهنگ، با تأخیر و نارسایی قانونی مواجه شده‌اند و پاسخ قضایی نتوانسته به‌طور کامل اثر بازدارندگی داشته باشد. شریفی پیشنهاد کرده است که قوانین موجود با تبصره‌ها و مواد تکمیلی، مسئولیت‌های سازمان‌ها و مجازات‌ها را به‌طور روشن تعیین کنند تا ضمن حمایت از زیرساخت‌ها، حقوق شهروندان نیز تضمین شود.

در سطح بین‌المللی، چارچوب‌های حقوقی مانند کنوانسیون بوداپست، قانون CISA در آمریکا و دستورالعمل NIS2 اتحادیه اروپا، نمونه‌هایی از سیاست‌های پیشگیرانه و هماهنگ در مقابله با حملات سایبری ترکیبی ارائه می‌کنند (Council of Europe, 2023, p. 12; US DHS, 2024, p. 18; European Commission, 2025, p. 21). این چارچوب‌ها نه تنها مسئولیت‌های قانونی و مجازات‌ها را تعیین می‌کنند، بلکه الزامات پیشگیرانه، گزارش‌دهی رخدادها و هماهنگی میان نهادها را نیز مشخص می‌کنند. مقایسه تجربه ایران با این استانداردها نشان می‌دهد که قوانین داخلی نیازمند بازنگری و توسعه هستند تا با تهدیدات نوظهور سازگار شوند (قدیری، ۱۴۰۱، ص. ۳۴).نتیجه‌گیری از این تحلیل، روشن می‌کند که مقابله مؤثر با حملات سایبری ترکیبی علیه زیرساخت‌های حیاتی بدون ایجاد هماهنگی میان قانون‌گذاری، رویه قضایی و استفاده از استانداردهای بین‌المللی امکان‌پذیر نیست. رویکردی ترکیبی که هم قوانین داخلی را تقویت کند و هم از تجارب جهانی بهره گیرد، می‌تواند چارچوبی امن و پایدار برای حفاظت از امنیت ملی، حقوق شهروندان و زیرساخت‌های حیاتی ایجاد نماید (Liu, 2022, p. 42; Bace, 2023, p. 26).در ادامه، پیشنهادهای عملی برای قانون‌گذاران و محاکم مطرح می‌شود: اول، اصلاح و بازنگری قانون جرایم رایانه‌ای با افزودن مواد و تبصره‌های جدید برای پوشش حملات ترکیبی. دوم، ایجاد مقررات پیشگیرانه که سازمان‌ها را ملزم به اجرای استانداردهای امنیتی

کنند. سوم، بهره‌گیری از تجربیات بین‌المللی مانند CISA و NIS2 برای تدوین سیاست‌های هماهنگ و عملیاتی. چهارم، تشویق پژوهش‌های میان‌رشته‌ای شامل حقوق، فناوری، امنیت و اقتصاد برای ارائه راهکارهای نوآورانه و کاربردی (میرزازاده، ۱۳۹۹، ص. ۳۶؛ شریفی، ۱۴۰۰، ص. ۲۸).

اهمیت پرداختن به این موضوع، به‌ویژه در شرایطی که حملات سایبری می‌توانند اثرات گسترده‌ای بر امنیت ملی، اقتصاد و جامعه داشته باشند، دوچندان می‌شود. گزارش‌های اتحادیه اروپا و ایالات متحده نشان می‌دهند که تهدیدات ترکیبی می‌توانند در مدت کوتاه خسارات جبران‌ناپذیری به زیرساخت‌های انرژی، حمل‌ونقل و بهداشت وارد کنند (European Commission, 2025.p.18; United States Department of Homeland Security, 2025,p.22). این تهدیدات، فراتر از آسیب‌های فنی، جنبه‌های حقوقی و اجتماعی گسترده‌ای دارند و پاسخ‌دهی قانونی بدون بازنگری و به‌روزرسانی چارچوب‌های موجود، ناکافی خواهد بود (Schmitt, 2024,p.7).پیشینه پژوهش‌های انجام‌شده نشان می‌دهد که این موضوع قبلاً مورد توجه محققان قرار گرفته است. پورغهرامی (۱۳۹۶) با بررسی تطبیقی استراتژی‌های حفاظت از قربانیان جرایم رایانه‌ای در ایران و اسناد بین‌المللی، بر لزوم هم‌سویی قوانین ملی با استانداردهای جهانی تأکید کرده است (ص. ۱۴). قدیری (۱۳۹۸) نیز به بررسی راهکارهای مقابله با سایبرتروریسم پرداخته و خلأهای موجود در نظام قانونی ایران را برجسته ساخته است (ص. ۸). پژوهش‌های (Bace,2024) به تحلیل چالش‌های بین‌المللی تنظیم‌گری حملات سایبری ترکیبی و ارائه مدل‌های سیاستی پرداخته‌است.همچنین تحقیقات داخلی مانند مطالعه کرمی و همکاران (۱۴۰۰) نشان می‌دهد که هماهنگی میان نهادهای مسئول، آموزش‌های تخصصی و تعریف دقیق حملات ترکیبی، از جمله مهم‌ترین موانع قانونی مقابله با تهدیدات سایبری است (ص. ۴۱). با وجود این پژوهش‌ها، هنوز خلأهای قابل توجهی در حوزه حقوق سایبری و تنظیم‌گری حملات ترکیبی علیه زیرساخت‌های حیاتی وجود دارد که نیازمند بررسی دقیق و ارائه راهکارهای عملی است.هدف اصلی این مقاله، شناسایی چالش‌های حقوقی و مقرراتی مرتبط با حملات سایبری ترکیبی و ارائه راهکارهای تقویت نظام حقوقی کشور در این زمینه است. پرسش‌های اصلی تحقیق عبارتند از: چه چالش‌های قانونی و مقرراتی در مقابله با حملات سایبری ترکیبی وجود دارد؟ و چگونه می‌توان با استفاده از راهکارهای نوآورانه، حفاظت از زیرساخت‌های حیاتی را تقویت کرد؟ برای پاسخ به این پرسش‌ها، روش پژوهش تحلیلی–توصیفی و مبتنی بر مطالعه اسنادی انتخاب شده است. در این راستا، ابتدا قوانین و مقررات موجود در ایران بررسی و با استانداردهای بین‌المللی مقایسه می‌شوند. سپس، با استفاده از مطالعات موردی و گزارش‌های بین‌المللی، چالش‌های موجود شناسایی و تحلیل می‌شوند. در نهایت، با ارائه پیشنهادهای عملی، راهکارهایی برای تقویت نظام حقوقی کشور در مقابله با حملات سایبری ترکیبی ارائه می‌شود.نتایج این پژوهش می‌تواند مبنای تدوین سیاست‌های پیشگیرانه و توسعه مقررات حقوق سایبری جامع در سطح ملی و منطقه‌ای قرار گیرد و ابعاد جدیدی از تنظیم‌گری و پاسخ به تهدیدات پیچیده سایبری را روشن سازد. این مقاله با ترکیب تحلیل‌های داخلی و بین‌المللی، امکان ارائه راهکارهای مبتنی بر شواهد و تجربه عملی را فراهم می‌آورد و خلأهای پژوهشی موجود در زمینه تنظیم‌گری حملات سایبری ترکیبی را کاهش می‌دهد.

حملات سایبری ترکیبی

به‌عنوان یکی از عناصر کلیدی امنیت سایبری و حقوق سایبری در دهه اخیر، اهمیت ویژه‌ای یافته است. این حملات، تهدیداتی پیچیده محسوب می‌شوند که به‌طور همزمان از ابزارهای دیجیتال، فیزیکی و انسانی برای ایجاد اختلال و آسیب به زیرساخت‌های حیاتی استفاده می‌کنند. آن‌ها می‌توانند سامانه‌های کنترل صنعتی، شبکه‌های داده‌ای، خدمات حمل‌ونقل،

سیستم‌های انرژی و حتی بخش‌های انسانی مرتبط با عملیات زیرساخت‌ها را مورد هدف قرار دهند. از این رو، تحلیل این حملات نیازمند دیدگاه چندبعدی و ترکیبی است که شامل فنی، حقوقی و امنیتی باشد (Liu, 2019, p. 33).در ادبیات علمی، این نوع حملات به دلیل تأثیر همزمان بر چند حوزه، چالش‌های جدیدی برای تنظیم‌گری قانونی ایجاد کرده‌اند. قوانین سنتی سایبری، غالباً محدود به اقدامات دیجیتال و نفوذ به داده‌ها هستند و به بعد فیزیکی یا انسانی حملات توجه کافی ندارند. به همین دلیل، اجرای مقررات موجود به‌تنهایی نمی‌تواند پاسخگوی تهدیدات پیچیده ترکیبی باشد (Anderson & Moore, 2020, p. 78).مطالعات اخیر نشان می‌دهند که مواجهه با چنین تهدیداتی نیازمند توسعه مقررات و سیاست‌های جامع است. نامجو (۱۳۹۸، ص. ۴۲) در مقاله‌ای تحلیلی پیرامون تهدیدات نوین سایبری، اشاره کرده است که ترکیب ابعاد مختلف حملات، باعث افزایش پیچیدگی شناسایی و پیگرد قانونی شده و نهادهای قضایی و امنیتی را با چالش‌های جدی مواجه می‌کند. او پیشنهاد کرده است که چارچوب‌های حقوقی نوین باید قابلیت انعطاف برای پوشش حملات چندبُعدی را داشته باشند و ضمن رعایت اصول حقوقی، جنبه‌های پیشگیرانه و هماهنگی میان نهادها را نیز شامل شوند.دلیر (۱۳۹۹، ص. ۳۷) در پژوهشی کاربردی، به بررسی اثرات تهدیدات ترکیبی بر امنیت اقتصادی و زیرساخت‌های حیاتی پرداخته و تأکید کرده است که فقدان دستورالعمل‌های هماهنگ و استانداردهای واحد، موجب افزایش آسیب‌پذیری سازمان‌ها در برابر حملات می‌شود. او معتقد است که سیاست‌گذاری سایبری، باید شامل ارزیابی ریسک، مدیریت بحران و تعیین مسئولیت‌های قانونی و اجرایی باشد تا ضمن کاهش خسارات اقتصادی و عملیاتی، پاسخ‌دهی به تهدیدات سریع و مؤثر انجام شود.سیادتی (۱۴۰۰، ص. ۲۹) نیز با تحلیل تطبیقی تهدیدات سایبری در محیط‌های مختلف، بر لزوم همکاری میان نهادهای قانونی، امنیتی و پژوهشی تأکید کرده است. بر اساس یافته‌های او، ترکیب رویکردهای فنی و حقوقی باعث می‌شود که کشورها بتوانند با تهدیدات نوین سازگار شوند و چارچوبی منعطف برای مقابله با حملات پیچیده ایجاد نمایند. این تحلیل نشان می‌دهد که تحلیل حملات ترکیبی صرفاً فنی نیست و بدون نگاه حقوقی و سیاست‌گذاری کارآمد، امکان مدیریت مؤثر آن‌ها محدود خواهد بود.

زیرساخت‌های حیاتی

این عبارت به سامانه‌ها، مؤسسات و خدمات کلیدی کشور اشاره دارد که عملکرد آن‌ها برای حفظ امنیت ملی، رفاه عمومی و ادامه فعالیت اقتصادی ضروری است. نمونه‌های آن شامل سیستم‌های انرژی، حمل‌ونقل، بهداشت و درمان، ارتباطات و خدمات مالی است (European Commission, 2025,p:18). حفاظت از این زیرساخت‌ها در برابر تهدیدات سایبری ترکیبی اهمیت حیاتی دارد، زیرا حمله به این بخش‌ها می‌تواند تأثیرات گسترده اقتصادی، اجتماعی و حتی سیاسی داشته باشد (Schmitt, 2024,p:14).

تنظیم‌گری سایبری

مفهومی کلیدی در حوزه حقوق فناوری اطلاعات و امنیت زیرساخت‌های حیاتی است که باید در این بخش با دقت تعریف شود. به طور کلی، تنظیم‌گری به فرآیند وضع، اجرا و نظارت بر قوانین و مقررات مرتبط با امنیت فضای مجازی و حفاظت از دارایی‌ها و داده‌ها اشاره دارد. این فرآیند، شامل تدوین سیاست‌های پیشگیرانه، نظارت مستمر بر رعایت قوانین، اعمال مجازات‌ها و ارزیابی مداوم تهدیدات سایبری است. هدف اصلی تنظیم‌گری، ایجاد چارچوبی است که بتواند تعامل میان فناوری، قانون و امنیت ملی را همسو سازد و ثبات، شفافیت و پاسخگویی را در فضای سایبری تضمین کند(پورقهرمانی ،۱۳۹۶ص۱۴). در دنیای امروز، اهمیت تنظیم‌گری سایبری با توجه به پیچیدگی حملات سایبری ترکیبی بیش از پیش

روشن می‌شود. چنین حملاتی، که به‌طور همزمان از ابزارهای دیجیتال، فیزیکی و انسانی بهره می‌برند، می‌توانند آسیب‌های گسترده‌ای به زیرساخت‌های حیاتی وارد کنند و تهدیدی جدی برای امنیت ملی و ثبات اقتصادی کشورها باشند. بدون چارچوب‌های تنظیم‌گری مؤثر، مقابله با این حملات به‌صورت پراکنده و ناکارآمد خواهد بود، زیرا قوانین سنتی سایبری اغلب محدود به اقدامات دیجیتال هستند و ابعاد فیزیکی یا انسانی را پوشش نمی‌دهند (Bace, 2024, p. 12).تنظیم‌گری سایبری همچنین نقش مهمی در تضمین پاسخگویی و شفافیت سازمان‌ها دارد. از طریق ایجاد استانداردها و دستورالعمل‌های اجرایی، نهادهای مسئول موظف به گزارش‌دهی رخدادهای امنیتی و اجرای اقدامات پیشگیرانه می‌شوند. این فرآیند، علاوه بر کاهش آسیب‌های مستقیم، زمینه را برای ارزیابی و بهبود مستمر سیاست‌های امنیتی فراهم می‌کند و باعث افزایش اعتماد عمومی و امنیت روانی جامعه نیز می‌شود (شریفی ،۱۴۰۰ص۲).

در ادبیات علمی، تنظیم‌گری سایبری به عنوان حلقه اتصال میان فناوری، قانون و امنیت ملی دیده می‌شود. میرزازاده (۱۳۹۹، ص. ۳۶) معتقد است که بدون وجود مکانیسم‌های تنظیم‌گری شفاف و جامع، قوانین سایبری قادر به پاسخگویی به تهدیدات پیچیده نیستند و اعمال مجازات‌ها و نظارت قانونی با تأخیر و ناکارآمدی مواجه می‌شود. همچنین دلیر (۱۳۹۹، ص. ۴۰) تأکید کرده است که تنظیم‌گری سایبری باید منعطف باشد و توانایی پوشش تهدیدات نوظهور و همزمان را داشته باشد، زیرا حملات ترکیبی می‌توانند همزمان بخش‌های مختلف فناوری و زیرساخت‌های انسانی را هدف قرار دهند.یکی دیگر از جنبه‌های حیاتی تنظیم‌گری سایبری، تلفیق رویکردهای پیشگیرانه و واکنشی است. سیاست‌های پیشگیرانه شامل آموزش نیروی انسانی، توسعه استانداردهای امنیتی و ایجاد سیستم‌های مانیتورینگ مداوم است، در حالی که سیاست‌های واکنشی شامل فرآیندهای پاسخ‌دهی سریع، گزارش‌دهی و پیگرد قانونی می‌شوند . ترکیب این دو رویکرد، امکان مدیریت مؤثر حملات سایبری ترکیبی را فراهم می‌کند و از خسارات مستقیم و غیرمستقیم به زیرساخت‌ها و جامعه جلوگیری می‌کند.

تنظیم‌گری سایبری نه تنها یک فرآیند قانونی یا فنی است، بلکه به عنوان ابزاری راهبردی برای امنیت ملی، حفاظت از حقوق شهروندان و حفظ ثبات اقتصادی عمل می‌کند. این مفهوم، به قانون‌گذاران و سازمان‌های اجرایی کمک می‌کند تا ضمن شناسایی نقاط ضعف، سیاست‌های جامع و هماهنگ تدوین کنند و امکان مدیریت هوشمند تهدیدات پیچیده را فراهم آورند (سیادتی ،۱۴۰۰ص۳۳)در چارچوب نظام حقوقی ایران، قانون جرایم رایانه‌ای مصوب ۱۳۸۸، محور اصلی مقابله با جرایم سایبری است. ماده ۱ این قانون، جرایم رایانه‌ای را شامل دسترسی غیرمجاز، شنود، تخریب داده‌ها و سیستم‌ها و سایر اقدامات مشابه تعریف کرده است (قانون جرایم رایانه‌ای، ۱۳۸۸، ص. ۲۳). با این حال، این قانون به‌صورت محدود، بعد فیزیکی و انسانی حملات ترکیبی را در نظر نگرفته است و همین موضوع باعث ایجاد خلاهای قانونی در مواجهه با تهدیدات نوظهور شده است (کرمی و همکاران، ۱۴۰۰، ص. ۴۱).

امنیت سایبری ملی

امنیت سایبری ملی به مجموعه اقدامات، سیاست‌ها و چارچوب‌های قانونی و اجرایی اطلاق می‌شود که دولت‌ها برای حفاظت از زیرساخت‌ها، شبکه‌های اطلاعاتی و داده‌های حیاتی کشور انجام می‌دهند. این مفهوم شامل برنامه‌ریزی استراتژیک، ایجاد استانداردهای امنیتی، تدوین مقررات پیشگیرانه و اجرای راهکارهای حفاظتی مداوم است تا کشور در برابر تهدیدات سایبری نوظهور و پیچیده، از جمله حملات ترکیبی، مقاوم باشد (قدیری، ۱۳۹۸، ص. ۸). امنیت سایبری

ملی تنها محدود به بعد فنی نیست، بلکه ابعاد حقوقی، اقتصادی و اجتماعی نیز در آن نقش دارند، زیرا اختلال در زیرساخت‌ها می‌تواند پیامدهای گسترده‌ای برای امنیت ملی، اقتصاد و رفاه شهروندان داشته باشد.

حقوق شهروندی دیجیتال

به مجموعه حقوق و آزادی‌هایی گفته می‌شود که افراد در استفاده از فناوری‌های اطلاعات و ارتباطات دارند. این حقوق شامل حفاظت از حریم خصوصی، حفظ امنیت داده‌های شخصی، دسترسی آزاد و امن به خدمات دیجیتال، و تضمین شفافیت و پاسخگویی سازمان‌ها در پردازش اطلاعات می‌شود. توجه به حقوق شهروندی دیجیتال، به‌ویژه در مواجهه با حملات سایبری ترکیبی، ضروری است، زیرا تهدیدات نوین می‌توانند علاوه بر زیرساخت‌ها، به اطلاعات و داده‌های حساس افراد نیز آسیب برسانند (Bace, 2024, p. 18).

ادبیات علمی بین‌المللی بر ضرورت ایجاد تعادل میان امنیت سایبری ملی و حقوق شهروندان تأکید دارد. استانداردهای بین‌المللی و مقررات حقوق بشر، دولت‌ها را ملزم می‌کنند که هنگام تدوین سیاست‌های امنیتی، آزادی و حریم خصوصی افراد را محترم بشمارند. به عبارت دیگر، حفظ امنیت نباید منجر به نقض حقوق اساسی شهروندان شود و برعکس، حفاظت از آزادی‌های فردی نباید امنیت ملی را تهدید کند. این تعادل، اساس شکل‌گیری چارچوب‌های حقوق سایبری پیشرفته در کشورهای توسعه‌یافته است (علیزاده ،۱۳۹۹ ،ص۱۵) همچنین در پژوهشی تحلیلی، بر اهمیت تدوین سیاست‌های جامع سایبری تأکید کرده و اشاره می‌کند که امنیت سایبری ملی و حقوق شهروندی دیجیتال نباید به‌صورت جداگانه بررسی شوند، بلکه هر دو باید در چارچوبی یکپارچه و هماهنگ مدیریت شوند. این هماهنگی باعث می‌شود که دولت‌ها بتوانند ضمن حفاظت از زیرساخت‌ها، اعتماد عمومی و مشارکت شهروندان در فضای دیجیتال را نیز تضمین کنند.رشیدی (۱۴۰۰، ص. ۲۲) نیز با تحلیل تطبیقی، تأکید کرده است که قوانین داخلی و سیاست‌های اجرایی سایبری باید مطابق با استانداردهای بین‌المللی و حقوق بشر طراحی شوند تا تضاد میان امنیت و آزادی فردی کاهش یابد. او بر ضرورت نظارت مستمر بر عملکرد نهادهای دولتی و بخش خصوصی و ایجاد مکانیسم‌های پاسخگویی مؤثر تأکید کرده است.نیکنام (۱۴۰۱، ص. ۳۰) در مطالعه‌ای دیگر، به بررسی نقش حقوق شهروندی دیجیتال در جلوگیری از سوءاستفاده از داده‌های شخصی و محافظت از حریم خصوصی پرداخته است. وی معتقد است که عدم توجه به این حقوق می‌تواند منجر به کاهش اعتماد عمومی و ایجاد آسیب‌های اجتماعی و اقتصادی شود، و این امر اهمیت تدوین سیاست‌ها و مقررات تنظیم‌گری سایبری را دوچندان می‌کند.به طور کلی، ترکیب تحلیل امنیت سایبری ملی و حقوق شهروندی دیجیتال، چارچوبی جامع برای مقابله با تهدیدات پیچیده سایبری از جمله حملات ترکیبی ارائه می‌دهد. این ترکیب به سیاست‌گذاران، قانون‌گذاران و نهادهای اجرایی کمک می‌کند تا هم زیرساخت‌های حیاتی کشور را محافظت کنند و هم حقوق اساسی شهروندان را تضمین نمایند.

از منظر فلسفی، مبانی امنیت و عدالت در فضای دیجیتال اهمیت ویژه‌ای دارند. نظریه عدالت جان رالز بر برابری فرصت‌ها و حفاظت از حقوق فردی تأکید دارد و نشان می‌دهد که جامعه موظف است حتی در فضای دیجیتال، حقوق افراد را تضمین کند (Rawls, 2001, p. 56). هابرماس نیز با تأکید بر ضرورت شفافیت و مشارکت عمومی، بیان می‌کند که تنظیم‌گری و تدوین قوانین باید در یک فرایند مشارکتی و مبتنی بر عقلانیت جمعی انجام شود تا مشروعیت قانونی و

اجتماعی داشته باشد (Habermas, 2001, p. 62). این دیدگاه فلسفی می‌تواند مبنای طراحی مقررات سایبری باشد که تعادل بین امنیت ملی و حقوق فردی را حفظ کند.

از منظر فقهی، اصولی مانند منع تجاوز به مال و حق الناس قابل تعمیم به فضای سایبری هستند. بر اساس فقه اسلامی، دسترسی غیرمجاز به اموال دیگران، تخریب یا ایجاد خسارت، از مصادیق تعدی به حق الناس است (مطهری، ۱۳۸۲، ص. ۱۰۲). این اصول می‌تواند در تحلیل حملات سایبری ترکیبی و توجیه ضرورت جرم‌انگاری اقدامات مخرب دیجیتال و فیزیکی مورد استفاده قرار گیرد. همچنین، اصل حفظ نظم و امنیت عمومی که در فقه و شریعت اسلامی مورد توجه است، با حفاظت از زیرساخت‌های حیاتی همسو است، زیرا تهدیدات ترکیبی می‌توانند نظم اجتماعی و امنیت عمومی را مختل کنند (جعفری، ۱۳۹۵، ص. ۴۵).

در بعد حقوقی، قانون اساسی ایران و قوانین جزایی مرتبط با جرایم رایانه‌ای، چارچوب نظری مهمی ارائه می‌دهند. اصل ۳ قانون اساسی ایران تصریح دارد که دولت موظف است امنیت کشور و حقوق شهروندان را تضمین کند و حفاظت از زیرساخت‌های حیاتی جزو مصادیق آن محسوب می‌شود (قانون اساسی جمهوری اسلامی ایران، ص. ۴۵). همچنین، ماده ۱ و تبصره‌های قانون جرایم رایانه‌ای مصوب ۱۳۸۸، مصادیق دسترسی غیرمجاز، تخریب داده‌ها و سیستم‌ها و اقدامات مشابه را تعریف می‌کند (قانون جرایم رایانه‌ای، ۱۳۸۸، ص. ۲۳–۲۵). اصول حقوق آمره، مانند تضمین امنیت ملی و حمایت از دارایی‌های عمومی، مبنای قانونی و الزام‌آور برای تدوین سیاست‌های پیشگیرانه و مقابله با حملات ترکیبی هستند.

از دیدگاه اقتصادی، هزینه‌های حملات سایبری ترکیبی به زیرساخت‌های حیاتی قابل توجه است. تحلیل‌های اقتصادی نشان می‌دهد که توقف خدمات انرژی، اختلال در شبکه‌های حمل‌ونقل و آسیب به سیستم‌های مالی می‌تواند هزینه‌های مستقیم و غیرمستقیم قابل توجهی ایجاد کند (Anderson & Moore, 2020, p. 78). بنابراین، تنظیم‌گری سایبری نه تنها یک الزام قانونی و امنیتی است، بلکه یک ضرورت اقتصادی نیز محسوب می‌شود. هزینه پیشگیری و حفاظت، معمولاً به مراتب کمتر از هزینه‌های ناشی از حمله است، و این نکته به‌ویژه در سیاست‌گذاری ملی اهمیت دارد (Liu, 2019, p. 33).

نظریه‌های حقوقی

نظریه‌های حقوقی در این زمینه به دو دسته اصلی تقسیم می‌شوند: نظریه‌های بین‌المللی و نظریه‌های ملی، که هر یک نقش مهمی در شناسایی مسئولیت‌ها و تدوین سیاست‌های مقابله با تهدیدات دارند.

از منظر حقوق بین‌الملل، نظریه مسئولیت دولت‌ها در مواجهه با حملات سایبری اهمیت ویژه دارد. بر اساس مفاد معاهدات بین‌المللی و اسناد حقوقی مانند کنوانسیون بوداپست، دولت‌ها مسئول اقدامات سایبری هستند که از قلمرو آن‌ها علیه دیگر کشورها انجام می‌شود (Schmitt, 2024). این دیدگاه، ضرورت تدوین قوانین داخلی منسجم و هماهنگی با استانداردهای بین‌المللی را برجسته می‌سازد و مبنای الزام‌آور برای تنظیم‌گری و پاسخگویی دولت‌ها فراهم می‌کند. همچنین، نظریه کیفری بودن حملات سایبری ترکیبی، که توسط(Bace ,2024)مطرح شده، بر لزوم مجازات مرتکبین و ایجاد مسئولیت کیفری برای اقدامات مخرب دیجیتال و فیزیکی تأکید دارد. این نظریه، چارچوب قانونی روشنی برای تحلیل و پیگرد قانونی حملات ترکیبی ارائه می‌دهد.در سطح ملی و ایران، اصول و حقوق آمره قانون اساسی، به ویژه اصل ۳ و اصل ۱۷۰، حفاظت از امنیت ملی و زیرساخت‌های حیاتی را تضمین می‌کنند. قانون جرایم رایانه‌ای مصوب ۱۳۸۸ در ماده ۱ و تبصره‌های بعدی، مصادیق مختلف جرایم سایبری را مشخص کرده و تعهدات قانونی دولت و نهادهای مسئول را

روشن می‌سازد (قانون جرایم رایانه‌ای، ۱۳۸۸، ص. ۲۳–۲۵). این چارچوب قانونی، با ادغام اصول حقوق آمره و مقررات جزایی، امکان مقابله با حملات ترکیبی و تضمین امنیت زیرساخت‌ها را فراهم می‌کند.دیدگاه‌های دکترین حقوقی نیز تنوع قابل توجهی دارند. برخی از حقوقدانان ایرانی مانند قدیری (۱۳۹۸، ص. ۱۲) و کرمی و همکاران (۱۴۰۰، ص. ۴۱) بر ضرورت هماهنگی میان نهادهای مسئول و ایجاد چارچوب‌های قانونی پیشگیرانه تأکید کرده‌اند. به باور آنان، خلأهای موجود در قوانین ایران، به ویژه در تعریف حملات ترکیبی و سازوکارهای نظارتی، باعث کاهش اثربخشی مقررات شده است. این دیدگاه با نظریه بین‌المللی مسئولیت دولت‌ها و استانداردهای کیفری بین‌المللی هم‌راستا است و ضرورت بازنگری در قوانین و تدوین سیاست‌های هماهنگ را تأکید می‌کند.نظریه‌های حقوقی دیگر شامل تحلیل حقوق آمره و الزام دولت‌ها به حفاظت از زیرساخت‌های حیاتی است. حقوق آمره، به‌ویژه در سطح ملی، الزاماتی را برای حفاظت از امنیت عمومی و جلوگیری از اقدامات مخرب تعیین می‌کند. به عنوان مثال، اصل ۳ قانون اساسی ایران تصریح دارد که دولت موظف است امنیت کشور و رفاه عمومی را تضمین کند، و اصل ۱۷۰ بر حفاظت از زیرساخت‌های حیاتی به عنوان مصادیق امنیت ملی تأکید دارد (قانون اساسی جمهوری اسلامی ایران، ص. ۴۵). این اصول حقوقی الزام‌آور، مبنای قانونی محکمی برای تدوین مقررات پیشگیرانه و پاسخ‌گویی سریع در برابر تهدیدات ترکیبی فراهم می‌کنند.

دیدگاه‌های بین‌المللی همچنین بر اصل پیشگیری و مسئولیت گسترده تأکید دارند. Schmitt ,2024)) بیان می‌کند که کشورها موظف‌اند نه تنها در پاسخ به حملات سایبری عمل کنند، بلکه اقدامات پیشگیرانه برای کاهش احتمال وقوع حملات ترکیبی نیز اتخاذ کنند. این اصل، با فلسفه حقوق و مبانی اقتصادی ترکیب می‌شود، زیرا هزینه پیشگیری معمولاً کمتر از هزینه‌های ناشی از حمله است و تحلیل اقتصادی نیز ضرورت سرمایه‌گذاری در حفاظت قانونی و فنی را تأیید می‌کند (Anderson , Moore, 2020).

لیو (۲۰۱۹)بر پیچیدگی‌های مربوط به مرزهای جغرافیایی و شناسایی مرتکب تأکید دارد، زیرا حملات ترکیبی معمولاً چندملیتی و چندبخشی هستند. در کنار آن، دکترین داخلی ایران، به ویژه نظریات کرمی و همکاران (۱۴۰۰، ص. ۴۱)، پیشنهاد می‌کنند که ایجاد نهادهای تخصصی نظارت و هماهنگی میان وزارتخانه‌ها و سازمان‌های امنیتی می‌تواند خلاهای قانونی موجود را کاهش دهد و پاسخ‌دهی سریع به حملات ترکیبی را تسهیل کند.

تحلیل و بررسی

در تحلیل حقوق سایبری و حملات ترکیبی علیه زیرساخت‌های حیاتی، بررسی قوانین داخلی کشور، به ویژه قانون جرایم رایانه‌ای مصوب ۱۳۸۸ و سایر مقررات مرتبط، نقطه شروع ضروری است. ماده ۱ این قانون، اعمالی همچون دسترسی غیرمجاز به داده‌ها، شنود غیرمجاز و تخریب سیستم‌ها را جرم دانسته و مجازات‌های کیفری متناسب با آن تعیین کرده است (قانون جرایم رایانه‌ای، ۱۳۸۸، ص. ۲۳–۲۴). با این حال، این قانون به صورت مشخص به حملات ترکیبی که ابعاد فیزیکی، دیجیتال و انسانی را به صورت همزمان هدف قرار می‌دهند، اشاره نکرده است، که نشان‌دهنده وجود خلا در مواجهه با تهدیدات نوظهور است (پورغهرامی، ۱۳۹۶، ص. ۱۴).بر اساس ماده ۲ این قانون، هرگونه اقدام برای دسترسی غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای بدون اجازه صاحب آن، جرم محسوب می‌شود. این ماده در تحلیل حملات ترکیبی اهمیت دارد، زیرا اغلب این حملات با نفوذ دیجیتال به زیرساخت‌های حیاتی آغاز می‌شوند و سپس به اقدامات فیزیکی و انسانی

تسری می‌یابند. بنابراین، ضرورت بازنگری و توسعه مواد قانونی برای پوشش تمامی ابعاد حملات ترکیبی، آشکار است (قدیری، ۱۳۹۸، ص. ۱۲).

ماده ۳ قانون جرایم رایانه‌ای نیز مسئولیت سازمان‌ها و نهادهای دولتی را در حفاظت از سیستم‌های اطلاعاتی و پیشگیری از تخلفات مشخص کرده است. این ماده می‌تواند پایه قانونی مناسبی برای الزامات امنیتی زیرساخت‌های حیاتی باشد، به ویژه وقتی با اصول حقوق آمره قانون اساسی ایران مانند اصل ۳ (تضمین امنیت ملی و حفاظت از دارایی‌های عمومی) ترکیب شود (قانون اساسی جمهوری اسلامی ایران، ص. ۴۵). ترکیب این مواد و اصول، چارچوبی ایجاد می‌کند که هم مسئولیت قانونی نهادها را روشن می‌کند و هم امکان پیگیری حقوقی حملات ترکیبی را فراهم می‌آورد.

علاوه بر قانون جرایم رایانه‌ای، قوانین مرتبط با حفاظت داده‌ها و حریم خصوصی نیز اهمیت دارند. به عنوان مثال، ماده ۵ قانون حفاظت از داده‌های شخصی مصوب ۱۳۹۷، سازمان‌ها را موظف کرده است که اقدامات پیشگیرانه برای جلوگیری از دسترسی غیرمجاز به داده‌ها انجام دهند (قانون حفاظت داده‌های شخصی، ۱۳۹۷، ص. ۱۸). این ماده به ویژه در تحلیل حملات ترکیبی کاربرد دارد، زیرا داده‌های حساس و اطلاعات زیرساخت‌ها اغلب هدف اولیه این حملات هستند. تحلیل این قوانین نشان می‌دهد که چارچوب قانونی ایران در زمینه مقابله با تهدیدات سایبری، پایه‌ای مناسب دارد اما با پیچیدگی حملات ترکیبی تطابق کامل ندارد. خلاهای قانونی، به ویژه در زمینه تعریف جامع جرم و هماهنگی میان نهادهای مسئول، نشان‌دهنده ضرورت بازنگری و به‌روزرسانی مقررات است (کرمی و همکاران، ۱۴۰۰، ص. ۴۱). نتیجه این تحلیل، تأکید بر ضرورت تدوین قوانین تکمیلی، تعریف دقیق حملات ترکیبی و الزام به اجرای الزامات امنیتی برای همه سازمان‌ها و زیرساخت‌های حیاتی است.

در ایران، رویه قضایی در زمینه حملات سایبری ترکیبی هنوز به بلوغ کامل نرسیده است، اما آراء صادره و نظریات مشورتی، مسیر روشنی برای تحلیل حقوقی ارائه می‌دهند. تجربه قضایی نشان می‌دهد که قضاوت در این حوزه نیازمند ترکیب تحلیل قانونی با دانش فنی و امنیتی است، زیرا این نوع حملات معمولاً ابعاد دیجیتال، فیزیکی و انسانی را به‌طور همزمان هدف قرار می‌دهند (کرمی و همکاران، ۱۴۰۱، ص. ۴۴).

بر اساس ماده ۲ قانون جرایم رایانه‌ای مصوب ۱۳۸۸، دسترسی غیرمجاز به داده‌ها و سیستم‌های رایانه‌ای جرم محسوب می‌شود و مجازات متناسب برای آن در نظر گرفته شده است. با استناد به این ماده، دیوان عالی کشور در رأی شماره ۳۲۱/۱۴۰۰، متهمی را که به سامانه‌های کنترل صنعتی نفوذ کرده و موجب اختلال در شبکه‌های انرژی شده بود، محکوم نمود (دیوان عالی کشور، ۱۴۰۰، ص. ۱۲). تحلیل این رأی نشان می‌دهد که قضات، گرچه قانون موجود را به‌کار گرفته‌اند، اما با توجه به ابعاد فیزیکی و انسانی حمله، ناگزیر از تعمیم مفهوم جرم به زیرساخت‌های حیاتی بوده‌اند.در موارد دیگر، نظریات مشورتی اداره حقوقی قوه قضائیه نقش راهنما را ایفا کرده‌اند. برای مثال، در نظریه مشورتی شماره ۱۴۰۱/۲۴۵، تأکید شده است که «حملات سایبری که علاوه بر تخریب داده‌ها و سامانه‌ها، موجب آسیب به جان و مال مردم شود، می‌تواند در زمره جرایم علیه امنیت ملی و نظم عمومی محسوب شود» (اداره حقوقی قوه قضائیه، ۱۴۰۱، ص. ۱۸). این نظریه، لزوم هماهنگی میان نهادهای قضایی، امنیتی و فنی را نشان می‌دهد و اهمیت تعریف دقیق جرم را برجسته می‌کند. برخی از حقوقدانان بر ضرورت بازنگری قانون جرایم رایانه‌ای تأکید دارند تا پوشش کافی برای حملات ترکیبی فراهم شود. قدیری (۱۴۰۰، ص. ۲۷) معتقد است که «تعریف محدود جرایم سایبری، مانع از برخورد قضایی مؤثر با حملات

پیچیده به زیرساخت‌های حیاتی است» و پیشنهاد کرده است که با اضافه کردن تبصره‌هایی در قانون، مسئولیت و پیگرد قانونی برای تخریب همزمان داده‌ها و سیستم‌های فیزیکی تعریف شود.

در تحلیل رویه قضایی، یکی از محورهای مهم، تطبیق مفاهیم قانونی با استانداردهای بین‌المللی است. برخی قضات با استناد به تجربیات و گزارش‌های بین‌المللی، اقدام به تعمیم ماده ۲ و ۳ قانون جرایم رایانه‌ای به حملات ترکیبی کرده‌اند (Schmitt, 2024, p. 15). این رویکرد تحلیلی نشان می‌دهد که رویه قضایی ایران، گرچه هنوز کامل نیست، اما قابلیت انطباق و توسعه را دارد و می‌تواند با به‌کارگیری نظریات مشورتی و تجربیات بین‌المللی، چارچوب قانونی جامعی برای مقابله با حملات ترکیبی ایجاد کند.

نتیجه‌گیری از تحلیل رویه قضایی ایران نشان می‌دهد که: اولاً، قضات در مواجهه با حملات ترکیبی به تفسیرهای تطبیقی روی آورده‌اند تا خلاهای قانونی موجود را جبران کنند؛ ثانیاً، نظریات مشورتی و تحلیل دکترین حقوقی به روشن شدن ابعاد جرم و مسئولیت‌ها کمک می‌کنند؛ ثالثاً، نیاز به بازنگری قانون و توسعه مقررات برای پوشش جامع حملات ترکیبی وجود دارد (Bace, 2024, p. 22; Liu, 2019, p. 37). این نتایج، محورهای اساسی برای سیاست‌گذاری و تدوین رویه قضایی هماهنگ با استانداردهای بین‌المللی را روشن می‌کند و نشان می‌دهد که تحلیل حقوقی صرفاً گزارش نیست، بلکه ابزار تصمیم‌گیری استراتژیک و پیشگیرانه فراهم می‌آورد.

در سطح بین‌المللی، حملات سایبری ترکیبی علیه زیرساخت‌های حیاتی، به عنوان تهدیدی فراگیر شناخته شده و مجموعه‌ای از قوانین و استانداردها برای مقابله با آن تدوین شده است. یکی از مهم‌ترین اسناد، کنوانسیون بوداپست علیه جرایم سایبری است که کشورهای عضو را موظف به تعریف و پیگرد قانونی اقدامات مخرب سایبری کرده است. بر اساس این کنوانسیون، حملات دیجیتال که موجب آسیب به سیستم‌ها و خدمات حیاتی می‌شوند، جرم محسوب می‌شوند و باید با مجازات متناسب پاسخ داده شوند (Council of Europe, 2023, p. 12). این استاندارد بین‌المللی، به کشورها چارچوبی می‌دهد تا قوانین داخلی خود را با تهدیدات نوین تطبیق دهند.

در ایالات متحده، قانون حفاظت از زیرساخت‌های حیاتی سایبری (CISA) و سیاست‌های مربوط به امنیت سایبری، مسئولیت شرکت‌ها و نهادهای دولتی در حفاظت از شبکه‌ها و داده‌ها را مشخص می‌کند (US DHS, 2024, p. 18). بر اساس این قانون، هرگونه نقص امنیتی که منجر به اختلال در خدمات عمومی یا اقتصادی شود، قابل پیگرد است. تجربه قضایی و اجرایی آمریکا نشان می‌دهد که تعریف دقیق مسئولیت‌ها و الزامات پیشگیرانه، باعث کاهش چشمگیر آسیب‌پذیری زیرساخت‌ها شده است (Anderson & Moore, 2021, p. 84).

در اتحادیه اروپا، دستورالعمل NIS2 و سیاست‌های حفاظت از شبکه‌ها و اطلاعات، سازمان‌ها را موظف به رعایت الزامات امنیتی و گزارش‌دهی رخدادهای سایبری می‌کند (European Commission, 2025, p. 21). این دستورالعمل، با تمرکز بر هماهنگی میان کشورهای عضو و شفافیت در اقدامات امنیتی، نمونه‌ای موفق از رویکرد تنظیم‌گری پیشگیرانه است. تحلیل این سیاست‌ها نشان می‌دهد که ترکیب الزامات قانونی و استانداردهای فنی، چارچوبی مؤثر برای مدیریت حملات ترکیبی ایجاد می‌کند و می‌تواند به عنوان الگو برای کشورهای دیگر، از جمله ایران، مورد استفاده قرار گیرد.دیدگاه دکترین حقوقی بین‌المللی نیز بر ضرورت مسئولیت گسترده دولت‌ها تأکید دارد. Schmitt ,2024, p. 20)) معتقد است که کشورها نباید تنها به پاسخ پس از حمله اکتفا کنند، بلکه موظف‌اند اقدامات پیشگیرانه، آموزش نیروی انسانی و سرمایه‌گذاری در امنیت سایبری زیرساخت‌ها را در دستور کار قرار دهند. این تحلیل نشان می‌دهد که

حقوق بین‌الملل و اسناد جهانی، چارچوبی جامع برای مقابله با تهدیدات ترکیبی فراهم می‌آورند که تنها با هماهنگی قوانین داخلی قابل پیاده‌سازی است.

مقایسه ایران با این استانداردها نشان می‌دهد که، اگرچه قانون جرایم رایانه‌ای و قانون حفاظت داده‌های شخصی، پایه‌ای مناسب فراهم کرده‌اند، اما خلاهایی همچون عدم پوشش کامل حملات ترکیبی، نبود الزامات پیشگیرانه سختگیرانه و کمبود هماهنگی میان نهادها، باعث کاهش کارایی مقابله با تهدیدات می‌شود (قدیری، ۱۴۰۱، ص. ۳۴). در مقابل، استانداردهای بین‌المللی با تعریف دقیق مسئولیت‌ها، الزام به گزارش‌دهی رخدادها و هماهنگی میان نهادها، سطح امنیت و پاسخ‌دهی به حملات ترکیبی را به شکل قابل توجهی افزایش می‌دهند.نتیجه‌گیری از این مقایسه، روشن می‌کند که ایران نیازمند بازنگری در قوانین، تعریف دقیق‌تر جرم و مسئولیت و ایجاد سیاست‌های هماهنگ با استانداردهای بین‌المللی است. اتخاذ رویکردی ترکیبی که هم از قوانین داخلی بهره ببرد و هم از تجربیات جهانی استفاده کند، می‌تواند سطح امنیت زیرساخت‌های حیاتی را ارتقا دهد و چارچوب قانونی و عملیاتی جامعی برای مقابله با حملات سایبری ترکیبی ایجاد کند (Liu, 2022, p. 42; Bace, 2023, p. 26).

بحث و نتیجه گیری

تحلیل حقوق سایبری و حملات ترکیبی علیه زیرساخت‌های حیاتی نشان می‌دهد که موضوع، پیچیدگی‌های فراوانی دارد و مواجهه مؤثر با آن نیازمند تلفیق چندین رویکرد قانونی، قضایی و اجرایی است. در بخش تحلیل و بررسی، مهم‌ترین نکات استخراج شده حاکی از آن است که قوانین داخلی ایران، از جمله قانون جرایم رایانه‌ای مصوب ۱۳۸۸ و قانون حفاظت داده‌های شخصی مصوب ۱۳۹۷، پایه قانونی اولیه‌ای برای مقابله با جرایم سایبری فراهم کرده‌اند. این قوانین، با تعریف جرم، تعیین مجازات و مشخص کردن مسئولیت سازمان‌ها، امکان پیگرد قانونی را فراهم می‌کنند، اما با ظهور حملات ترکیبی که شامل جنبه‌های دیجیتال، فیزیکی و انسانی هستند، مشخص شد که خلأهای قانونی وجود دارد که باعث کاهش اثرگذاری قوانین می‌شود (پورغهرامی، ۱۳۹۶، ص. ۱۴؛ کرمی و همکاران، ۱۴۰۱، ص. ۴۴).بر اساس تحلیل رویه قضایی، قضات ایران با استفاده از مواد قانونی موجود، مانند ماده ۲ و ماده ۳ قانون جرایم رایانه‌ای، تلاش کرده‌اند حملات سایبری ترکیبی را تحت شمول قانون قرار دهند. آراء صادره از دیوان عالی کشور نشان می‌دهد که تفسیر تطبیقی و استفاده از نظریات مشورتی، مانند نظریه مشورتی شماره ۱۴۰۱/۲۴۵ اداره حقوقی قوه قضائیه، نقش مهمی در پوشش خلاهای قانونی ایفا کرده است (اداره حقوقی قوه قضائیه، ۱۴۰۱، ص. ۱۸). این روند نشان می‌دهد که قوه قضائیه ایران، با وجود محدودیت‌های قانونی، سعی در ایجاد چارچوبی برای پاسخ‌دهی به حملات پیچیده دارد، اما هنوز نیازمند توسعه و بازنگری است.

در مقایسه با قوانین و سیاست‌های بین‌المللی، تفاوت‌های آشکاری مشاهده می‌شود. کنوانسیون بوداپست، دستورالعمل NIS2 اتحادیه اروپا و قانون CISA در آمریکا، چارچوب‌های جامع و هماهنگ پیشگیرانه برای مقابله با حملات ترکیبی ارائه کرده‌اند (Council of Europe, 2023, p. 12; US DHS, 2024, p. 18; European Commission, 2025, p. 21). این قوانین نه تنها مسئولیت و پیگرد قانونی را تعیین می‌کنند، بلکه الزامات پیشگیرانه و هماهنگی میان نهادها را نیز مشخص کرده‌اند. تجربه جهانی نشان می‌دهد که رویکردی که صرفاً واکنشی باشد، در برابر حملات پیچیده ناکارآمد است و ایجاد چارچوب حقوقی پیشگیرانه و هماهنگ، احتمال آسیب و خسارت را به حداقل می‌رساند.بر اساس بررسی‌های انجام‌شده، می‌توان نتیجه گرفت که ایران دارای پایه قانونی و رویه قضایی اولیه برای مقابله

با حملات سایبری ترکیبی است، اما این چارچوب‌ها برای مقابله با تهدیدات پیچیده و چندبُعدی کافی نیستند و نیاز به بازنگری، اصلاح و تکمیل دارند. خلأهایی که شناسایی شده، شامل موارد زیر است: عدم تعریف جامع جرم حملات ترکیبی، نبود الزامات پیشگیرانه سختگیرانه، کمبود هماهنگی میان نهادها، و فقدان سازوکارهای شفاف برای گزارش‌دهی رخدادهای سایبری. این خلاها باعث می‌شوند که مقابله قانونی با حملات ترکیبی ناقص باشد و پاسخ‌دهی قضایی و اجرایی به‌صورت پراکنده و ناکارآمد انجام شود (قدیری، ۱۴۰۱، ص. ۳۴).

آثار و پیامدهای حقوقی نتایج، در چند محور قابل بررسی است:

۱. تأثیر بر رویه قضایی:

نتایج تحلیل نشان می‌دهد که قضات در مواجهه با حملات ترکیبی نیازمند ابزارهای قانونی دقیق‌تر و آموزش‌های تخصصی هستند. استفاده از مواد قانونی محدود و تفسیر تطبیقی، در کوتاه‌مدت امکان پاسخ‌دهی فراهم می‌کند، اما در بلندمدت نیاز به چارچوب قانونی دقیق‌تر و روش‌های تحلیلی علمی برای شناسایی و پیگرد حملات پیچیده وجود دارد. این امر می‌تواند موجب ایجاد رویه قضایی هماهنگ و توسعه‌یافته برای برخورد با حملات ترکیبی شود.

۲. تأثیر بر قانون‌گذاری:

نتایج تحلیل نشان می‌دهد که اصلاح و بازنگری قوانین موجود، مانند قانون جرایم رایانه‌ای، ضروری است. ایجاد تبصره‌های جدید برای پوشش حملات ترکیبی، تعریف مسئولیت‌های سازمان‌ها، تعیین الزامات پیشگیرانه و تدوین مقررات هماهنگ با استانداردهای بین‌المللی، می‌تواند خلأهای قانونی را کاهش دهد و سطح امنیت زیرساخت‌های حیاتی را ارتقا دهد. علاوه بر این، قانون‌گذاران می‌توانند از تجربیات کشورهای پیشرفته بهره‌گیری کنند تا چارچوبی کارآمد، جامع و عملیاتی ایجاد شود (Bace, 2023, p. 26).

۳. تأثیر بر حقوق شهروندان:

حفاظت از داده‌ها، امنیت خدمات عمومی و کاهش ریسک حملات سایبری، تأثیر مستقیم بر حقوق شهروندان دارد. تضمین حفاظت از اطلاعات و کاهش احتمال آسیب به زیرساخت‌های حیاتی، اعتماد عمومی را افزایش می‌دهد و مانع از بروز خسارت‌های اقتصادی، اجتماعی و روانی به شهروندان می‌شود. این امر اهمیت تدوین قوانین و سیاست‌های پیشگیرانه را دوچندان می‌کند و نشان می‌دهد که حقوق سایبری، فراتر از مباحث فنی، به حقوق انسانی و اجتماعی نیز مرتبط است.

۴. پیشنهادها برای قانون‌گذاران، محاکم و پژوهشگران:

اصلاح و بازنگری قوانین موجود با هدف تعریف جامع جرم، مسئولیت‌ها و مجازات‌ها برای حملات ترکیبی

تصویب مقررات جدید با تمرکز بر الزامات پیشگیرانه، هماهنگی میان نهادها و گزارش‌دهی رخدادها

بهره‌گیری از تجربیات کشورهای پیشرفته و استانداردهای بین‌المللی (مانند CISA و NIS2)

توسعه مطالعات میان‌رشته‌ای شامل حقوق، فناوری، امنیت و اقتصاد برای ارائه راهکارهای نوآورانه

آموزش تخصصی قضات، کارکنان امنیتی و بخش خصوصی برای مواجهه با حملات پیچیده

نتیجه نهایی این است که مقابله مؤثر با حملات سایبری ترکیبی علیه زیرساخت‌های حیاتی، بدون ایجاد هماهنگی میان قانون‌گذاری، رویه قضایی و استانداردهای بین‌المللی، امکان‌پذیر نیست. یک رویکرد جامع، که هم قوانین داخلی را تقویت

کند و هم تجارب جهانی را به‌کار گیرد، می‌تواند چارچوبی امن و پایدار برای حفاظت از امنیت ملی، حقوق شهروندان و زیرساخت‌های حیاتی فراهم آورد.

منابع

۱. منابع فارسی

کتاب‌ها

جعفری، ح. (۱۳۹۵). فقه و امنیت عمومی: تحلیل حقوقی حفاظت از زیرساخت‌ها. تهران: انتشارات پژوهشگاه

مطهری، م. (۱۳۸۲). اصول فقه و کاربرد آن در حقوق نوین. تهران: انتشارات دانشگاه

مقالات

پورغهرامی، ب. (۱۳۹۶). مطالعه تطبیقی راهبردهای حفاظت از قربانیان جرایم رایانه‌ای در حقوق ایران و اسناد بین‌المللی با تأکید بر کنوانسیون بوداپست. پژوهش‌های حقوق کیفری، ۸(۱)، ۵–۳۶

تقی‌پور، م. (۱۳۹۸). پیشگیری و مقابله با سایبرتروریسم. مجله مطالعات امنیت سایبری، ۱۲(۲)، ۷–۲۵

دلیر، م. (۱۳۹۹). تأثیر تهدیدات سایبری ترکیبی بر امنیت اقتصادی و زیرساخت‌های حیاتی. پژوهش‌های مدیریت ریسک و امنیت سایبری، ۳(۱)، ۳۷–۵۰

رشیدی، م. (۱۴۰۰). تحلیل تطبیقی سیاست‌های سایبری و حفاظت از حقوق شهروندان. پژوهش‌های امنیت و فناوری اطلاعات، ۶(۲)، ۲۲–۳۵

سیادتی، ع. (۱۴۰۰). تحلیل تطبیقی تهدیدات نوین سایبری و چارچوب‌های قانونی. مجله حقوق فناوری اطلاعات ایران، ۵(۳)، ۲۹–۴۵

علیزاده، س. (۱۳۹۹). امنیت سایبری ملی و هماهنگی با حقوق شهروندی دیجیتال. مجله مطالعات حقوق فناوری اطلاعات، ۵(۱)، ۱۵–۲۸

کرمی، ر.، احمدی، ف.، و رضایی، س. (۱۴۰۰). تحلیل چالش‌های قانونی و نظارتی حملات سایبری ترکیبی در ایران. مجله حقوق و فناوری اطلاعات، ۵(۳)، ۳۵–۵۰

نامجو، ح. (۱۳۹۸). چالش‌های حقوقی تهدیدات نوین سایبری: تحلیل تهدیدات ترکیبی. مجله مطالعات امنیت فناوری اطلاعات، ۴(۲)، ۴۲–۵۵

نیکنام، ع. (۱۴۰۱). نقش حقوق شهروندی دیجیتال در تنظیم‌گری سایبری و حفاظت از داده‌ها. مجله حقوق و فناوری اطلاعات ایران، ۷(۳)، ۳۰–۴۴

میرزازاده، ح. (۱۳۹۹). حملات سایبری ترکیبی علیه زیرساخت‌های حیاتی: تحلیل حقوقی و سیاست‌های پیشگیرانه. مجله حقوق و فناوری اطلاعات ایران، ۵(۲)، ۳۴–۳۷

شریفی، م. (۱۴۰۰). بررسی تجربیات قضایی ایران در مواجهه با حملات سایبری ترکیبی. مجله مطالعات حقوق و امنیت فناوری، ۶(۱)، ۲۲–۳۰

اسناد

اداره حقوقی قوه قضائیه. (۱۴۰۱). نظریه مشورتی شماره ۱۴۰۱/۲۴۵ در زمینه جرایم سایبری ترکیبی. تهران: قوه قضائیه

قانون اساسی جمهوری اسلامی ایران. (۱۳۵۸). تهران: مرکز اسناد ملی

قانون حفاظت داده‌های شخصی مصوب ۱۳۹۷. تهران: مرکز پژوهش‌های مجلس

قانون جرایم رایانه‌ای مصوب ۱۳۸۸. تهران: مرکز پژوهش‌های مجلس شورای اسلامی

۲.منابع انگلیسی

Books

Habermas, J. (2001). The theory of communicative action. Boston, MA: Beacon Press

Rawls, J. (2001). Justice as fairness: A political conception. Cambridge, MA: Harvard University Press

Articles

Anderson, R., & Moore, T. (2020). The economics of cybersecurity: Cost-benefit analysis for critical infrastructures. Journal of Cybersecurity Studies, 15(2), 78–95

Bace, B. (2023). Hybrid cyber attacks on critical infrastructure: Legal challenges and regulatory frameworks. Journal of Cyber Law & Policy, 19(1), 26–42

Joseph O. Eichenhofer and Elisa Heymann and Barton P. Miller, (2017), “ InDepth Software Vulnerability Assessment of Container Terminal Systems”, 2nd NATO Conference on Cyber Security in the Maritime Domain, Souda, Crete, Greece, pp 1-17 .

Kadri Kaska and Lorena Trinberg, (2015),Regulating Cross-Border Dependencies of Critical Information Infrastructure,Nato Cooperation Cyber Defence Center of Excellence report, Tallinn Eslonia, 2015 .

KS Min, (2015), “An International Comparative Study on Cyber Security Strategy”, International Journal of Security and Its Applications Vol.9, No.2 (2015), pp 13-20. 24. L. Cazorla, C. Alcaraz, and J. Lopez, (2016), “Cyber Stealth Attacks in Critical Information Infrastructures", IEEE Systems Journal, pp. 1-15 .

Luiijf E, van Schie T, van Ruijven T, Huistra, A, (2016), good practice guide on critical information infrastructure protection for governmental policy-makers, The GFCE-MERIDIAN .

Martin Koyabe, (2015), “Critical Information Infrastructure Protection A Commonwealth Perspective”, ITU Workshop on “ICT Security Standardization for Developing Countries, pp 1-45. Bace, B. (2024). Legal implications of combined cyber-physical attacks on national infrastructure. International Journal of Cybersecurity Studies, 20(1), 12–28

Liu, H. (2019). Cross-border cyber threats and legal challenges. International Journal of Cyber Law, 12(3), 33–50

Liu, H. (2022). Legal responses to multi-dimensional cyber threats: Comparative perspectives. International Journal of Cybersecurity Law, 13(2), 37–52

Schmitt, M. N. (2024). A policy approach for addressing hybrid cyber attacks. Lieber Institute West Point, 7(1), 7–21

Official Documents and Reports

Council of Europe. (2023). Convention on Cybercrime (Budapest Convention). Strasbourg: Council of Europe Publishing

European Commission. (2025). NIS2 Directive and cybersecurity policies for EU member states. Energy & Infrastructure Security Review, 12(3), 21–33

European Commission. (2025). Protecting critical infrastructure and cybersecurity. Energy Policy Review, 12(3), 18–33

US Department of Homeland Security (DHS). (2024). Cybersecurity and Infrastructure Security Act: Guidelines for critical infrastructure protection. Washington, DC: DHS Publications