مطالعات فقه اقتصادی
Economic Jurisprudence Studies

Destructive Cyber Operations as an "Attack" in International Criminal Law and Economic Jurisprudence: Redefining the Threshold of the Use of Force in the Digital Age

Mahmoud Darvish Torabi[1*]

1. Department of Law, Payame Noor University, Tehran, Iran.

ARTICLE INFORMATION

Article Type: Original Research

Pages:265-278

Article history:

Received: 06 Sep 2024

Edition: 05 Nov 2024

Accepted:13 Mar 2025

Published online:25 Mar 2025

Keywords:
Destructive Cyber Operations, Use of Force, International Criminal Law, Economic Jurisprudence, Economic Security.

Corresponding Author:
Mahmoud Darvish Torabi

Address:
Iran, Tehran, Payame Noor University, Department of Law,

Orchid Code:
0000-0002-8819-3024

Tel:
09113530796

Email:
darvishtorabi@pnu.ac.ir

ABSTRACT

Background and Aims: With the transition of hostilities from the physical realm to cyberspace and the growing vulnerability of critical economic infrastructures, this study aims to redefine the threshold of the use of force and the concept of "attack" within international criminal law and Imami economic jurisprudence, thereby examining the feasibility of assessing destructive cyber operations in the absence of physical destruction.

Materials and Methods: This is a theoretical research conducted using a descriptive-analytical methodology.

Findings: The criteria for evaluating cyber operations must shift from an instrument-based to an effects-based approach, such that the paralysis of financial and critical infrastructures constitutes a clear instance of an armed attack and international crimes, including war crimes and aggression. Furthermore, in economic jurisprudence, data possess financial value (Maliyyah), and their destruction—relying on the rules of *Itlaf* (destruction), *Tasbib* (causation), *La-Zarar* (non-harm), *Ifsad fil-ard* (corruption on earth), and the conceptual expansion of weapons—warrants civil liability and criminalization.

Ethical Considerations: Throughout all stages of writing this research, the authenticity of texts, honesty, and trustworthiness have been strictly observed.

Conclusion: The results indicate that developing expansive interpretations of the *actus reus* within the International Criminal Court and drawing upon the dynamism of Imami jurisprudence provide an effective mechanism for safeguarding public livelihoods and the economic security of developing countries in the digital age.

Cite this article as: Darvishtorabi, M. ***Destructive Cyber Operations as an "Attack" in International Criminal Law and Economic Jurisprudence: Redefining the Threshold of the Use of Force in the Digital Age.*** Economic Jurisprudence Studies. 2026.

مطالعات فقه اقتصادی
Economic Jurisprudence Studies

فصلنامهٔ مطالعات فقه اقتصادی، دورهٔ هفتم، شمارهٔ اول، بهار ۱۴۰۴

عملیات‌های سایبری مخرب به‌مثابهٔ «حمله» در حقوق بین‌الملل کیفری و فقه اقتصادی: بازتعریف آستانه توسل به زور در عصر دیجیتال

محمود درویش ترابی[*1]

۱. گروه حقوق، دانشگاه پیام نور، تهران، ایران.

اطلاعات مقاله

نوع مقاله: پژوهشی

صفحات: ۲۶۵-۲۷۸

سابقهٔ مقاله:

تاریخ دریافت: ۱۴۰۳/۰۶/۱۶

تاریخ اصلاح: ۱۴۰۳/۰۸/۱۵

تاریخ پذیرش: ۱۴۰۳/۱۲/۲۳

تاریخ انتشار: ۱۴۰۴/۰۱/۰۵

واژگان کلیدی:

عملیات سایبری مخرب، توسل به زور، حقوق بین‌الملل کیفری، فقه اقتصادی، امنیت اقتصادی.

نویسندهٔ مسئول:

محمود درویش ترابی

آدرس پستی:

ایران، تهران، دانشگاه پیام نور، گروه حقوق.

تلفن:

09113530796

کد ارکید:

0000-0002-8819-3024

پست الکترونیک:

darvishtorabi@pnu.ac.ir

چکیده

زمینه و هدف: با گذار مخاصمات از عرصه فیزیکی به فضای مجازی و آسیب‌پذیری زیرساخت‌های حیاتی اقتصادی، پژوهش حاضر با هدف بازتعریف آستانه توسل به زور و مفهوم حمله در حقوق بین‌الملل کیفری و فقه اقتصادی امامیه شکل گرفته است تا امکان سنجش عملیات‌های مخرب سایبری را در غیاب تخریب کالبدی بررسی کند.

مواد و روش‌ها: این تحقیق از نوع نظری بوده روش تحقیق به صورت توصیفی تحلیلی می‌باشد.

یافته‌ها: معیار ارزیابی حملات سایبری باید از ابزارمحور به نتیجه‌محور تغییر یابد؛ به گونه‌ای که فلج‌سازی زیرساخت‌های مالی و حیاتی، مصداق بارز حمله مسلحانه و جنایات بین‌المللی مانند جنایت جنگی و تجاوز است. همچنین در فقه اقتصادی، داده‌ها دارای مالیت بوده و تخریب آن‌ها با استناد به قواعد اتلاف، تسبیب، لاضرر، افساد فی‌الأرض و توسعه مفهومی سلاح، مستوجب ضمان و جرم‌انگاری است.

ملاحظات اخلاقی: در تمام مراحل نگارش پژوهش حاضر، ضمن رعایت اصالت متون، صداقت و امانت‌داری رعایت شده است.

نتیجه: نتایج حاکی از آن است که توسعه تفاسیر موسع از عنصر مادی در دیوان کیفری بین‌المللی و بهره‌گیری از پویایی فقه امامیه، راهکاری کارآمد برای صیانت از معیشت عمومی و امنیت اقتصادی کشورهای در حال توسعه در عصر دیجیتال فراهم می‌آورد.

©تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق بشر اسلامی ایران می‌باشد.

۱. مقدمه

با گذار شتابان مخاصمات و رقابت‌های ژئوپلیتیک از میدان‌های سنتی و فیزیکی به بستر پهناور فضای رایانه‌ای، امنیت ملی و ساختار حیاتی دولت‌ها دستخوش دگرگونی بنیادینی شده است. امروزه زیرساخت‌های حیاتی جوامع اعم از شبکه‌های بانکی و مالی، سامانه‌های توزیع انرژی، خطوط ارتباطی و مراکز داده، بیش از پیش در برابر بدافزارها و سلاح‌های رایانه‌ای آسیب‌پذیرند. حملات رایانه‌ای مخرب برخلاف جنگ‌افزارهای کلاسیک، مرزهای جغرافیایی را درنوردیده و با هزینه‌ای اندک، توانایی فلج‌سازی کامل بنیان‌های اقتصادی و اجتماعی یک کشور را دارا هستند. این تحول ساختاری، ضرورت بازخوانی مفاهیم سنتی حقوق بین‌الملل را دوچندان ساخته است.

بررسی ادبیات موجود نشان می‌دهد که پژوهش‌های پیشین پیرامون این پدیده، عمدتاً یا بر ابعاد فنی و امنیت سایبری متمرکز بوده‌اند و یا مباحث حقوقی را صرفاً در چارچوب حقوق مخاصمات مسلحانه و قواعد ناظر بر جنگ‌های سنتی تحلیل کرده‌اند. این در حالی است که تسری پیامدهای این حملات به ساحت «حقوق بین‌الملل کیفری» و تبیین مسئولیت کیفری عاملان آن، به ویژه پیوند میان خسارت‌های ساختاری اقتصادی ناشی از این حملات با عناوین مجرمانه بین‌المللی، کمتر مورد توجه قرار گرفته است. از سوی دیگر، خوانش تطبیقی این پدیده در «فقه اقتصادی» اسلامی و استخراج احکام مترتب بر تخریب سامانه‌های مالی و معیشتی جامعه، همچنان یک حوزه مغفول و نیازمند واکاوی علمی است.

این پژوهش بر پایه سه پرسش کلیدی شکل گرفته است: نخست آنکه آستانه شمول یک عملیات رایانه‌ای مخرب ذیل مفاهیم «حمله» و «توسل به زور» بر پایه معیارهای مندرج در بند چهارم ماده دو و ماده پنجاه‌ویکم منشور ملل متحد و ماده چهل‌ونهم پروتکل الحاقی اول چیست؟ دوم اینکه، اثرات اقتصادی ویرانگر و فلج‌کننده یک حمله رایانه‌ای چگونه می‌تواند رکن مادی جرایم مندرج در اساسنامه دیوان کیفری بین‌المللی نظیر جنایات جنگی علیه اموال یا جنایت تجاوز را محقق سازد؟ و سوم اینکه، فقه امامیه با تکیه بر اصول فقه اقتصادی، قاعده اتلاف، تسبیب و احکام ناظر بر افساد و محاربه اقتصادی، چه سازوکارهایی برای بازتعریف و جرم‌انگاری این‌گونه حملات ارائه می‌دهد؟

فرضیه بنیادین مقاله آن است که حملات رایانه‌ای مخرب با عبور از رویکرد کالبدی‌محور و با اتکا بر رویکرد نتیجه‌گرا، ماهیت «حمله مسلحانه» را احراز کرده و با ایجاد خسارت‌های ساختاری بر زیرساخت‌های اقتصادی، ارکان مادی جرایم شدید بین‌المللی را محقق می‌سازند؛ همچنین فقه امامیه با توسعه مفاهیم مالیت داده‌ها و تسری قواعد ضمان و عناوین بازدارنده، ظرفیت بالایی در جرم‌انگاری و تقنین این پدیده دارد. نوآوری اصلی این پژوهش در ارائه یک الگوی مفهومی یکپارچه میان حقوق بین‌الملل کیفری و فقه اقتصادی برای بازتعریف آستانه توسل به زور در عصر دیجیتال نهفته است.

۲. مواد و روش‌ها

پژوهش حاضر یک مطالعه توصیفی تحلیل است. از روش کتابخانه‌ای به منظور جمع‌آوری داده‌ها و مطالب در این تحقیق استفاده شده است.

۳. ملاحظات اخلاقی

در مراحل مختلف نگارش این مقاله، ضمن رعایت اصالت متون، صداقت و امانتداری رعایت شده است.

۴. یافته‌ها

یافته‌ها حاکی از آن است که معیار ارزیابی حملات سایبری باید از ابزارمحور به نتیجه‌محور تغییر یابد؛ به گونه‌ای که فلج‌سازی زیرساخت‌های مالی و حیاتی، مصداق بارز حمله مسلحانه و جنایات بین‌المللی مانند جنایت جنگی و تجاوز است. همچنین در فقه اقتصادی، داده‌ها دارای مالیت بوده و تخریب آن‌ها با استناد به قواعد اتلاف، تسبیب، لاضرر، افساد فی‌الأرض و توسعه مفهومی سلاح، مستوجب ضمان و جرم‌انگاری است.

۵. بحث

بخش حاضر به واکاوی ابعاد بنیادین و استدلال‌های تفصیلی پژوهش در سه ساحت حقوق بین‌الملل، اسناد کیفری و مبانی فقه اقتصادی اختصاص دارد تا از این رهگذر، الگویی نوین در بازتعریف مفهوم حمله سایبری ارائه گردد.

۵-۱. مبانی نظری

شناخت دقیق ماهیت حقوقی عملیات‌های رایانه‌ای در گروی تبیین مبانی نظری و استانداردهای حاکم بر مفاهیم کلیدی چون حمله و توسل به زور است؛ از این رو، در این بخش سازوکارهای حقوق بین‌الملل بشردوستانه و چالش‌های انتساب در بستر فضای مجازی واکاوی می‌شوند.

۵-۱-۱. مفهوم حمله در حقوق بین‌الملل بشردوستانه و پیوند آن با حقوق کیفری بین‌المللی

مفهوم «حمله» در حقوق بین‌الملل بشردوستانه، نقطه اتصال میان شیوه‌های اعمال خشونت در مخاصمه و محدودیت‌های حمایتی است که برای صیانت از غیرنظامیان و اموال غیرنظامی پیش‌بینی شده‌اند. ماده ۴۹ پروتکل الحاقی اول ۱۹۷۷، حمله را «اعمال خشونت‌آمیز علیه دشمن، خواه در حالت تهاجمی و خواه دفاعی» تعریف می‌کند. اهمیت این تعریف در آن است که خشونت را به استفاده از ابزارهای متعارف جنگی یا وارد آوردن نیروی فیزیکی مستقیم فرو نمی‌کاهد؛ بنابراین، تفسیر آن باید با توجه به ماهیت رفتار و پیامدهایی صورت گیرد که بر اشخاص و اموال بر جای می‌گذارد. در محیط سایبری، تمرکز صرف بر ابزار ناموجه است؛ زیرا کد رایانه‌ای، بدافزار یا فرمان دیجیتال، با وجود فقدان نمود فیزیکی متعارف، ممکن است سامانه‌ای حیاتی را از کار بیندازد یا زنجیره‌ای از آثار زیان‌بار انسانی و مادی پدید آورد. ازاین‌رو، معیار اصلی باید قابلیت رفتار برای ایجاد آثار خشونت‌آمیز باشد، نه شکل فنی وسیله‌ای که این آثار را محقق می‌کند (Gisel, Rodenhäuser, & Dörmann, 2020: 311–312).

این برداشت، گذار از رویکرد ابزارمحور به رویکرد آثارمحور را توجیه می‌کند. بر مبنای رویکرد دوم، عملیات سایبری هنگامی در شمار حملات قرار می‌گیرد که انتظار رود موجب مرگ یا جراحت اشخاص، یا آسیب و انهدام اموال شود. راهنمای تالین نیز در تعریف حمله سایبری، بر انتظار معقول از چنین پیامدهایی تکیه می‌کند و بدین‌ترتیب، فناوری مورد استفاده را از جایگاه معیار تعیین‌کننده کنار می‌زند (Schmitt, 2017: 415–416). البته آثارمحوری به معنای آن نیست که هر نفوذ، دست‌کاری یا اختلال دیجیتال حمله محسوب شود؛ میان دسترسی غیرمجاز یا اخلال گذرا و عملیاتی که کارکرد هدف را به‌طور جدی مختل می‌کند یا به اشخاص و اموال آسیب می‌رساند، باید تفکیک کرد. همچنین، شناسایی رفتار به‌عنوان حمله در حقوق بشردوستانه، به‌خودی‌خود تحقق جرم بین‌المللی را اثبات نمی‌کند؛ مسئولیت کیفری مستلزم احراز مستقل عناصر مادی و روانی جرم، پیوند رفتار با مخاصمه و سایر شرایط مقرر در اساسنامه رم است (Trahan, 2021: 1133–1134). بر این اساس، در تحلیل عملیات سایبری، پرسش محوری نباید این باشد که آیا ابزار به‌کاررفته ماهیتی فیزیکی دارد، بلکه باید سنجید که عملیات در بستر مخاصمه چه اثری بر کارکرد هدف، امنیت اشخاص و امکان بهره‌مندی جامعه از اموال و خدمات اساسی بر جای می‌گذارد. چنین تفسیری، هم با غایت حمایتی حقوق بشردوستانه سازگارتر است و هم از توسعه بی‌ضابطه مفهوم حمله جلوگیری می‌کند؛ زیرا ارزیابی آثار باید عینی و قابل اثبات باشد.

۵-۱-۲. آستانه خشونت و مسئله «تخریب داده‌ها»

ازکارافتادن سامانه تسویه ناخالص آنی، شبکه توزیع سوخت یا بورس اوراق بهادار، حتی بدون تخریب فیزیکی تجهیزات، می‌تواند واجد آثار سنگین اقتصادی و اجتماعی باشد؛ بااین‌حال، پاسخ به این پرسش که چنین عملیاتی «حمله» یا «حمله مسلحانه» محسوب می‌شود، به تفکیک دو آستانه حقوقی وابسته است. در حقوق بین‌الملل بشردوستانه، مفهوم حمله ناظر بر اعمال خشونت‌آمیز علیه دشمن است و اختلاف اصلی آن است که آیا از دست‌رفتن کارکرد سامانه، بدون آسیب کالبدی، برای تحقق این مفهوم کفایت می‌کند یا خیر. رویکرد مضیق، تحقق حمله را به مرگ، جراحت یا خسارت فیزیکی به اموال پیوند می‌دهد؛ در مقابل، رویکرد کارکردی، اختلال جدی در کارکرد زیرساخت را نیز، به‌ویژه هنگامی که ارائه خدمات حیاتی به جمعیت غیرنظامی را مختل کند، در قلمرو حمله جای می‌دهد. بااین‌همه، هر اختلالی کافی نیست و باید از آستانه‌ای فراتر رود که صرفاً ناظر بر دشواری موقت یا مزاحمت ناچیز باشد (Biggio, 2025: 247–248).

در ارزیابی این آستانه، معیارهای اشمیت در تشخیص توسل به زور سایبری راهنمایی تحلیلی فراهم می‌کنند: شدت پیامدها، فوریت و نزدیکی اثر به رفتار، مستقیم‌بودن رابطه میان عملیات و نتیجه، میزان مداخله در قلمرو هدف، قابلیت سنجش خسارت، ماهیت نظامی رفتار و

نقش دولت در آن. اعمال این عوامل بر نمونه‌های یادشده مستلزم بررسی گستره توقف مبادلات، مدت اختلال، امکان بازیابی داده‌ها و سامانه‌ها، آثار زنجیره‌ای بر پرداخت‌ها و تأمین کالاهای ضروری و میزان وابستگی جامعه به زیرساخت هدف است. هرچه اختلال فراگیرتر، پایدارتر و پیامدهای آن برای زندگی و امنیت اقتصادی مردم شدیدتر باشد، استدلال برای عبور از آستانه‌های حقوقی قوت بیشتری می‌یابد؛ بااین‌حال، معیارهای مزبور فرمولی مکانیکی یا آزمونی قطعی نیستند و باید با توجه به اوضاع هر پرونده اعمال شوند (Haataja, 2022: 430–431). نکته تعیین‌کننده آن است که «حمله» در حقوق بشردوستانه را نباید با «حمله مسلحانه» موضوع ماده ۵۱ منشور ملل متحد یکسان گرفت. حتی اگر اختلالی حمله محسوب شود، احراز حق دفاع مشروع مستلزم اثبات شدت و آثار کافی در سطحی بالاتر است. رویه دولت‌ها درباره کفایت صرفِ ازکارافتادن کارکرد سامانه‌ها هنوز یکدست نیست؛ بنابراین، توقف سامانه بانکی یا سوخت‌رسانی به‌تنهایی پاسخ قطعی نمی‌دهد و باید آثار واقعی، دامنه و دوام آن احراز شود (Kis Kelemen, 2025: 329–330). بر این مبنا، فقدان تخریب کالبدی نباید به‌تنهایی مانع شناسایی عملیات به‌عنوان حمله باشد؛ همان‌گونه که اهمیت اقتصادی هدف نیز به‌تنهایی برای وصف حمله مسلحانه کفایت نمی‌کند. معیار نهایی، ارزیابی مستند شدت، گستره، دوام و پیامدهای انسانی و اقتصادی عملیات در پرتو آستانه حقوقی مورد بحث است.

۵-۱-۳. انتساب عملیات‌های سایبری

انتساب عملیات سایبری به دولت، صرف شناسایی منشأ فنی حمله نیست؛ بلکه مسئله‌ای حقوقی است که باید رابطه میان مرتکب، رفتار ارتکابی و ساختار قدرت دولتی را اثبات کند. پیچیدگی این فرایند از آنجا ناشی می‌شود که عملیات سایبری از مسیر چندین سامانه و واسطه عبور می‌کند و مهاجم می‌تواند با جعل هویت، استفاده از زیرساخت اشخاص ثالث یا آلوده‌سازی تجهیزات دیگران، ردپای خود را پنهان سازد. نشانی اینترنتی، محل استقرار سرور یا شباهت ابزار و شیوه حمله با عملیات پیشین نیز به‌تنهایی هویت مرتکب یا وابستگی او به دولت معینی را ثابت نمی‌کند. بنابراین، داده‌های فنی باید در کنار اطلاعات انسانی، شواهد ارتباطی، الگوهای رفتاری و قرائن مربوط به انگیزه و سازمان‌دهی ارزیابی شوند (Tsagourias & Farrell, 2020: 945–946).

در سطح حقوقی، انتساب رفتار به دولت تابع قواعد عام مسئولیت بین‌المللی دولت‌هاست. رفتار ارکان رسمی دولت اصولاً به آن منتسب می‌شود؛ اما درباره گروه‌ها و اشخاص غیردولتی، صرف برخورداری از حمایت مالی، تجهیزاتی یا سیاسی دولت کافی نیست. مطابق ماده ۸ مواد مسئولیت دولت‌ها، رفتار چنین اشخاصی هنگامی به دولت منتسب می‌شود که عمل موردنظر به دستور، هدایت یا تحت کنترل آن دولت انجام شده باشد. معیار کنترل مؤثر مستلزم اثبات رابطه‌ای مشخص میان دولت و عملیات مورد اختلاف است؛ به‌گونه‌ای که حمایت عمومی یا نفوذ کلی بر گروه، جایگزین اثبات کنترل بر رفتار معین نشود. بنابراین، حتی اگر گروهی به‌طور مستمر از منابع یک دولت بهره‌مند باشد، انتساب هر عملیات سایبری آن نیازمند احراز پیوند لازم با همان عملیات است (Delerue, 2020: 129–130).

بااین‌حال، دشواری اصلی در گردآوری و ارائه ادله‌ای است که واقعیت‌های فنی را با معیار حقوقی انتساب پیوند دهد. محرمانگی اطلاعات امنیتی، دسترسی نابرابر دولت‌ها به داده‌ها و ملاحظات سیاسی ممکن است سبب شود مسئولیت یک دولت بدون انتشار ادله کافی اعلام شود. ازاین‌رو، باید میان انتساب سیاسی، که ممکن است مبنای واکنش دیپلماتیک یا تحریم قرار گیرد، و انتساب حقوقی، که آثار مسئولیت بین‌المللی را به دنبال دارد، تمایز گذاشت (Brunner, 2025: 33–34). در نتیجه، انتساب معتبر مستلزم ارزیابی شواهد و پرهیز از نتیجه‌گیری بر پایه یک قرینه منفرد است. همچنین، انتساب رفتار به دولت را نباید با شناسایی مسئولیت کیفری فردی عاملان خلط کرد؛ هر یک تابع مبانی و عناصر اثباتی مستقل است. این تفکیک مانع از آن می‌شود که پیچیدگی فنی فضای سایبری به توسعه بی‌ضابطه مسئولیت دولت‌ها یا نسبت‌دادن شتاب‌زده عملیات به بازیگران دولتی بینجامد.

۵-۲. مسئولیت کیفری بین‌المللی ناشی از عملیات‌های سایبری مخرب

پس از تبیین آستانه ورود به قلمرو توسل به زور، مسئله اساسی تعیین ضمانت‌اجرا و انتساب کیفری به مرتکبان چنین اقداماتی است؛ از این رو، در این بخش انطباق

رفتارهای مجرمانه در فضای مجازی با ارکان مادی و معنوی جنایات جنگی، جنایت علیه بشریت و جنایت تجاوز در پرتو اسناد بین‌المللی تحلیل می‌شود.

۵-۲-۱. عملیات سایبری در قامت «جنایات جنگی»

در بررسی این عنوان باید میان دو مبنای کیفری تفکیک شود: ماده ۸(۲)(ب)(۴) اساسنامه رم ناظر بر حمله‌ای است که با علم به نامتناسب‌بودن آشکار پیامدهای مورد انتظار آن انجام می‌شود؛ درحالی‌که ماده ۸(۲)(الف)(۴) تخریب یا تصاحب گسترده اموال را، در صورت فقدان توجیه ضرورت نظامی و غیرقانونی و خودسرانه‌بودن رفتار، جرم‌انگاری می‌کند. بنابراین، صرف خسارت اقتصادی یا حذف داده‌ها برای تحقق این جرایم کافی نیست و باید عناصر اختصاصی هر عنوان جداگانه احراز شود. توصیف عملیات سایبری به‌عنوان جنایت جنگی، به وجود مخاصمه مسلحانه و ارتباط رفتار با آن وابسته است؛ ازاین‌رو، صرف مخرب‌بودن عملیات یا گستردگی زیان اقتصادی، برای تحقق مسئولیت کیفری کفایت نمی‌کند. ماده ۸(۲)(ب)(۴) اساسنامه رم، حمله‌ای را جرم می‌داند که مرتکب با علم به این امر آن را آغاز کند که تلفات اتفاقی انسانی، جراحت غیرنظامیان، خسارت به اموال غیرنظامی یا آسیب گسترده، بلندمدت و شدید به محیط زیست طبیعی، آشکارا در قیاس با مزیت نظامی مشخص و مستقیمِ مورد انتظار، بیش از اندازه خواهد بود. در عملیات سایبری، این حکم می‌تواند ناظر بر وضعیتی باشد که نفوذ به سامانه‌های انرژی، آب‌رسانی یا درمانی، پیامدهای قابل پیش‌بینی و نامتناسبی برای جمعیت غیرنظامی ایجاد کند. بااین‌حال، زیان مالی یا اختلال در بازار به‌تنهایی کافی نیست؛ باید پیوند آن با خسارت به اموال غیرنظامی، صدمه انسانی یا آسیب زیست‌محیطی و نیز علم مرتکب به نامتناسب‌بودن آشکار آثار احراز شود (Wilmshurst, Moynihan, & van Benthem, 2026: 13–14).

مسئله پیچیده‌تر، انطباق تخریب داده‌ها با ماده ۸(۲)(الف)(۴) است؛ حکمی که تخریب و تصاحب گسترده اموال را، در صورتی که ضرورت نظامی آن را توجیه نکند و رفتار به‌صورت غیرقانونی و خودسرانه انجام شده باشد، از مصادیق نقض فاحش می‌شناسد. باید میان داده به‌عنوان موضوع مستقل و داده به‌مثابه وسیله دسترسی یا بهره‌برداری از مال تفکیک کرد. حذف اطلاعات بانکی، قفل‌کردن پایگاه‌های داده یا ازکارانداختن سامانه‌های ثبت مالکیت ممکن است امکان استفاده یا اداره اموال را از بین ببرد؛ اما شمول داده‌های ناملموس در مفهوم «مال» و «موضوع» همچنان محل اختلاف تفسیری است و نمی‌توان هر حذف داده‌ای را بدون احراز تخریب مال حمایت‌شده، مشمول این عنوان دانست (McKenzie, 2021: 1173–1174).

افزون بر این، ارتکاب عملیات به‌وسیله گروه غیردولتی مانع تحقق جنایت جنگی نیست؛ مسئولیت کیفری فردی می‌تواند متوجه اعضا یا فرماندهانی شود که با تحقق عناصر جرم در آن مشارکت داشته‌اند. بااین‌حال، باید وضعیت مخاصمه، پیوند رفتار با آن، ماهیت هدف و شکل مشارکت هر شخص جداگانه اثبات شود؛ به‌ویژه آنکه قواعد مربوط به مخاصمات غیربین‌المللی در اساسنامه رم محدودیت‌ها و صورت‌بندی خاص خود را دارند (Gabrielli, 2023: 296–297). بنابراین، تحلیل کیفری عملیات سایبری باید از ارزیابی کلی شدت خسارت فراتر رود و عناصر دقیق هر جرم را جداگانه بررسی کند. رویکرد آثارمحور می‌تواند در تفسیر رفتارهای دیجیتال راهگشا باشد، اما نباید به توسعه قیاسی عناوین کیفری یا کنارگذاشتن اصل قانونی‌بودن جرم و مجازات بینجامد.

۵-۲-۲. عملیات سایبری فلج‌کننده و «جنایت علیه بشریت»

در تحلیل این عنوان، باید میان شدت آثار اقتصادی یک عملیات سایبری و تحقق عناصر حقوقی جنایت علیه بشریت تفکیک شود؛ زیرا اختلال گسترده در خدمات عمومی، هرچند می‌تواند زمینه‌ساز رنج انسانی شدید باشد، به‌تنهایی برای احراز این جنایت کفایت نمی‌کند. متن زیر این تمایز را با تمرکز بر ماده ۷(۱)(ک) اساسنامه رم لحاظ می‌کند. عملیات سایبری فلج‌کننده، هنگامی که از محدوده اخلال فنی یا زیان مالی فراتر رود و به‌طور جدی شرایط زیست و سلامت جمعیت غیرنظامی را مختل سازد، می‌تواند از منظر جنایت علیه بشریت مورد بررسی قرار گیرد. برخلاف جنایات جنگی، تحقق این عنوان به وجود مخاصمه مسلحانه وابسته نیست؛ بلکه رفتار ارتکابی باید در چارچوب حمله‌ای گسترده یا نظام‌مند علیه جمعیت غیرنظامی، با آگاهی مرتکب از آن، صورت گرفته باشد. افزون بر این، حمله مزبور باید متضمن ارتکاب مکرر اعمال ممنوع و مبتنی بر سیاست یک دولت یا سازمان

باشد. بنابراین، حملـه سـایبری منفـرد، هرچنـد خسـارت اقتصادی قابل‌توجهی ایجاد کند، لزومـاً واجـد ایـن وصـف نیست؛ مگر آنکه در پیوند با مجموعه‌ای از رفتارهای واجد شـرایط و در راسـتای سیاسـت یادشـده قـرار گیـرد (Permanent Mission of Liechtenstein to the United Nations, 2021: 52–53).

در این چـارچوب، مـاده ۷(۱)(ک) اساسـنامه رم ظرفیـت مهمی برای ارزیابی آثار انسـانی عملیـات سـایبری فـراهم می‌آورد. این ماده، سایر اعمـال غیرانسـانیِ دارای مـاهیتی مشابه با اعمال ممنوع دیگر را دربرمـی‌گیـرد، مشـروط بـر آنکه عمداً موجب رنج شدید یا صدمه جدی بـه جسـم یـا سلامت جسمی و روانی اشخاص شوند. بـر ایـن اسـاس، از کـار انـداختن سـازمان‌یافتـه سـامانه توزیـع دارو، شـبکه آب‌رسـانی یـا زیرسـاخت‌هـای مـالی در شـرایط بحرانـی، چنانچه دسترسی جمعیت غیرنظامی به نیازهای حیاتی را مختل کند و به بیماری، محرومیت شدید، اضطراب فراگیر یا آسیب جدی روانی بینجامد، ممکن است از مصادیق این عنوان تلقی شود. اهمیت موضـوع در آن اسـت کـه زیـان اقتصادی در این تحلیل، موضوع مستقل جرم نیست، بلکه از طریق پیامدهای انسانی و شدت رنجی کـه بـر اشـخاص تحمیل می‌کند، واجد وصف کیفری می‌شـود (Zarmsky, 2024: 170–171).

رویکرد دادستانی دیوان کیفری بین‌المللی نیز بـر قابلیـت اعمال مقررات اساسنامه، فارغ از ابزار ارتکاب، تأکیـد دارد؛ ازاین‌رو، استفاده از فناوری‌های دیجیتال مانع بررسی رفتار در قالـب جـرایم موجـود نخواهـد بـود (Office of the Prosecutor, 2025: 5). بااین‌حال، تفسـیر مـاده ۷(۱)(ک) نباید به توسعه نامحدود قلمرو جرم بینجامد. صرف توقـف خدمات بانکی، کاهش ارزش دارایی‌ها یا اختلال در فعالیت اقتصادی، بدون اثبات رنج شدید یا صـدمه جـدی و سـایر عناصر زمینه‌ای جنایت علیه بشریت، کافی نیسـت. معیـار تعیین‌کننـده، تبـدیل اخـتلال زیرسـاختی بـه محرومیـت انسانی شدید و هدف‌گیری جمعیـت غیرنظـامی در قالـب حمله‌ای واجد شرایط است. از این منظر، امنیت اقتصـادی هنگامی در قلمرو حمایت کیفری بین‌المللی قرار می‌گیـرد که فروپاشی کارکردهای حیاتی، مستقیماً به تهدید جـدی سلامت، کرامت و امکان زیست جمعـی انسـان‌هـا منتهـی شود.

۵-۲-۳. عملیـات سـایبری و «جنایـت تجـاوز» (Crime of Aggression):

جنایت تجاوز در ماده ۸ مکرر اساسنامه رم، صرفاً ناظر بـر کـاربرد غیرقـانونی زور نیسـت، بلکـه تحقـق آن مسـتلزم ارتکاب عمل تجاوزکارانه از سوی یک دولت و نقض آشکار منشور ملل متحد از حیث ماهیت، شدت و مقیـاس اسـت. افزون بر این، مسئولیت کیفری متوجه شخصی اسـت کـه در موقعیت رهبری سیاسـی یـا نظـامی قـرار داشـته و در طراحی، تدارک، آغاز یا اجرای آن عمل نقش داشته باشـد. قطعنامه ۳۳۱۴ مجمع عمومی نیز با برشـمردن مصـادیقی مانند تهاجم، بمباران و حمله نیروهای مسلح یک دولت به دولت دیگر، چارچوب تشخیص رفتار تجاوزکارانه را فـراهم می‌کند. بـر ایـن مبنـا، عملیـات سـایبری نیـز در صـورت برخورداری از آثار و شدت متناسب، نمـی‌توانـد صـرفاً بـه دلیل ماهیت غیرمادی ابزار ارتکاب، از قلمرو مفهوم تجـاوز خارج شود (Trahan, 2025: 77–78).

بااین‌حال، فلج‌شدن زیرساخت‌های اقتصـادی یـک کشـور، به‌تنهایی برای تحقـق ایـن جنایـت کـافی نیسـت. معیـار اساسی آن است که عملیات به دولت دیگر منتسب باشد و از حیث آثار، در سطح کاربرد نیروی مسلح و نقض آشـکار منشور قرار گیرد. ازکارانداختن شبکه بـانکی، سـامانه‌هـای انرژی یا نظام پرداخت ملی، چنانچـه صـرفاً موجـب زیـان مـالی یـا اخـتلال موقـت اقتصـادی شـود، لزومـاً چنـین آستانه‌ای را محقق نمی‌کند؛ اما اگر به مـرگ، جراحـت یـا تخریب فیزیکـی گسـترده بینجامـد، ارزیـابی حقـوقی آن متفاوت خواهد بود. سیاست دادسـتانی دیـوان نیـز امکـان ارتکاب تجـاوز از طریـق عملیـات سـایبری را مـی‌پـذیرد، هرچند ارزیابی آثار غیرمـادیِ فاقـد پیامـدهای فیزیکـی را پیچیـده‌تـر مـی‌دانـد (Office of the Prosecutor, 2025: 38–40). از سوی دیگر، استفاده از سامانه‌های هوشـمند در طراحی و اجرای عملیـات، مسـئله احـراز قصـد و انتسـاب مسئولیت به رهبران انسانی را دشوارتر می‌سازد؛ زیرا نقش تصمیم‌گیری مسـتقل فنـاوری نبایـد بـه خـلأ مسـئولیت کیفری منتهی شود (Carpenter, 2025: 69–70). بنابراین، حمله سایبری فلج‌کننده ملی تنهـا هنگـامی مـی‌توانـد در چارچوب جنایت تجاوز بررسی شود کـه آثـار آن، انتسـاب دولتی و شرایط مسئولیت رهبـری، در کنـار معیـار نقـض آشکار منشور، احراز گردد. صرف بزرگی خسارت اقتصادی

جایگزین این عناصر نیست و نمی‌توان شدت اختلال را بدون سنجش ماهیت و پیامدهای آن، معادل تجاوز دانست.

۵-۳. تبیین فقهی-اقتصادی عملیات‌های سایبری مخرب در فقه امامیه

در نظام حقوقی اسلام، صیانت از مال و انتظام معیشت عمومی در زمره ضروریات شریعت قرار دارد؛ از این رو، در این بخش با تکیه بر ظرفیت‌های فقه امامیه، ماهیت مالیت داده‌ها، قواعد عام ضمان و امکان تطبیق حملات سازمان‌یافته رایانه‌ای با عناوین مجرمانه‌ای چون اخلال در نظام و افساد فی‌الارض بررسی می‌شود.

۵-۳-۱. مالیت داده‌ها و دارایی‌های ناملموس در فقه معاصر

تحول فضای اقتصادی به محیط دیجیتال، ضرورت بازنگری در مفهوم فقهی مال و قلمرو مالکیت را آشکار ساخته است؛ زیرا ارزش اقتصادی دیگر منحصر به اشیای مادی و قابل‌قبض نیست و داده‌ها، دارایی‌های رمزنگاری‌شده و حقوق مالی ثبت‌شده در سامانه‌های الکترونیکی نیز می‌توانند موضوع مبادله و انتفاع قرار گیرند. در فقه معاصر، معیار اصلی برای شناسایی مال را باید در برخورداری از ارزش عقلایی، قابلیت اختصاص و امکان انتفاع مشروع جست‌وجو کرد، نه صرف وجود مادی. بر این اساس، داده‌های شخصی، تجاری و مالی، در صورتی که دارای ارزش اقتصادی و قابلیت بهره‌برداری مشروع باشند، می‌توانند دست‌کم در قالب مال، حق مالی یا منفعت مورد حمایت قرار گیرند؛ هرچند تعیین دقیق ماهیت فقهی آن‌ها به نوع داده و حدود اختیار دارنده وابسته است (الحربی، ۲۰۲۵: ۱۱۲۵–۱۱۲۷).

در این میان، نباید میان داده و حقی که از طریق آن بازنمایی می‌شود، خلط کرد. برای مثال، سپرده الکترونیکی بانکی خودِ داده ثبت‌شده در سامانه نیست، بلکه طلب و حق مالی صاحب حساب در برابر بانک است که اطلاعات دیجیتال، وجود و میزان آن را نشان می‌دهد. به همین ترتیب، سرقت یا انتقال غیرمجاز داده‌ها ممکن است موجب نقض حق اختصاص، محرمانگی یا منفعت اقتصادی شود، حتی اگر نسخه اصلی اطلاعات همچنان نزد مالک باقی بماند؛ ازاین‌رو، فقدان جابه‌جایی فیزیکی، لزوماً به معنای فقدان موضوع حمایت مالی نیست (بودقرزام و نوبس، ۲۰۲۵: ۱۸۴–۱۸۹).

در مورد دارایی‌های رمزنگاری‌شده نیز قابلیت مبادله، اختصاص و ارزش اقتصادی می‌تواند مبنای پذیرش مالیت قرار گیرد؛ بااین‌حال، میان رمزینه‌های دارای پشتوانه یا کارکرد مالی مشخص و ارزهای رمزنگاری‌شده فاقد شناسایی رسمی باید تفاوت گذاشت. بنابراین، مالیت این دارایی‌ها حکمی یکسان و مطلق ندارد و به ویژگی‌های هر دارایی و ضوابط اعتبار آن وابسته است ت در نتیجه، حمایت فقهی از دارایی‌های دیجیتال باید بر ماهیت واقعی حق یا منفعت استوار باشد، نه بر شکل فنی ثبت آن. چنین رویکردی امکان می‌دهد تخریب، تصاحب یا محروم‌سازی غیرمجاز از دارایی‌های دیجیتال نیز، متناسب با موضوع و آثار رفتار، در قلمرو قواعد ضمان و حمایت از اموال قرار گیرد.

۵-۳-۲. قواعد عام ضمان و مسئولیت مالی در فقه اقتصادی

قواعد ضمان در فقه اقتصادی، ظرفیت تحلیل خسارات ناشی از عملیات سایبری را حتی در مواردی که زیان بدون تخریب فیزیکی اموال پدید می‌آید، فراهم می‌کنند. بر پایه قاعده اتلاف، هرگاه رفتار مستقیم مرتکب به نابودی یا از بین رفتن قابلیت انتفاع از مال متعلق به دیگری بینجامد، اصل ضمان قابل طرح است. ازاین‌رو، حذف غیرقابل‌بازگشت اطلاعات اقتصادی، تخریب سوابق مالی یا قفل‌کردن پایگاه داده‌ها از طریق بدافزارهای اخاذی، در صورتی که موجب زوال ارزش یا محرومیت مؤثر مالک از مال و منافع آن شود، می‌تواند موضوع ضمان قرار گیرد. البته باید میان نابودی داده و محرومیت موقت از دسترسی به آن تفاوت گذاشت؛ زیرا هر اختلالی لزوماً اتلاف عین مال نیست و ممکن است صرفاً موجب ضمان منافع یا جبران خسارت ناشی از تعطیلی فعالیت اقتصادی شود (الحناوی و العموش، ۲۰۲۵: ۴۲۸–۴۲۹).

قاعده تسبیب نیز در مواردی اهمیت می‌یابد که خسارت اقتصادی، نتیجه زنجیره‌ای از آثار یک عملیات سایبری باشد. برای مثال، انتشار بدافزار در سامانه بانکی ممکن است ابتدا موجب اختلال در پردازش اطلاعات و سپس توقف پرداخت‌ها، زیان بنگاه‌ها و اخلال در زنجیره تأمین شود. در چنین وضعی، انتساب ضمان به عامل سایبری

مستلزم احراز رابطه سببیت عرفی، قابلیت پیش‌بینی پیامدها و انتساب نتیجه به رفتار متعدی است؛ به‌ویژه آنکه ورود عامل مستقل یا رفتار اشخاص دیگر می‌تواند در تعیین مسئولیت مؤثر باشد (عنانبه، ۲۰۲۳: ۲۸۸–۲۸۹). در کنار این قواعد، قاعده لاضرر و نفی حرج، ارزیابی خسارت را به زیان مستقیم مالی محدود نمی‌کند. اختلال پایدار در خدمات بانکی، آب‌رسانی یا تأمین کالاهای ضروری، ممکن است معیشت عمومی را مختل و هزینه‌های سنگینی بر جامعه تحمیل کند. بنابراین، آثار عمومی و ساختاری عملیات سایبری نیز، در صورت احراز ضرر و رابطه انتساب، در تحلیل فقهی قابل اعتناست (بوزغار، ۲۰۱۷: ۴۳۷–۴۳۸). بر این اساس، معیار ضمان در فضای دیجیتال باید بر حقیقت زیان، رابطه سببیت و میزان محرومیت از مال یا منفعت استوار باشد، نه صرفاً بر وقوع تخریب مادی و محسوس.

۵-۳-۳. جرم‌انگاری حملات سایبری در ساحت فقه جزایی و امنیت اقتصادی

در فقه جزایی، حملات سایبری سازمان‌یافته علیه زیرساخت‌های حیاتی را می‌توان از منظر عناوینی چون افساد فی‌الارض و اخلال در نظام بررسی کرد؛ به‌ویژه هنگامی که هدف، از کار انداختن شبکه بانکی، مختل‌کردن گردش کالاهای اساسی یا محروم‌سازی گسترده مردم از خدمات ضروری باشد. در چنین وضعیتی، رفتار ارتکابی صرفاً تعرض به داده یا مال معین نیست، بلکه ممکن است امنیت عمومی و بنیان معیشت جامعه را مختل سازد. بااین‌حال، صدق عنوان افساد نیازمند احراز گستره و شدت آثار، عمدی‌بودن رفتار و نقش آن در ایجاد فساد عمومی است و نباید هر نفوذ یا تخریب رایانه‌ای را بی‌درنگ مشمول این عنوان دانست (مبارکیهٔ و خلفهٔ، ۲۰۲۲: ۱۲۸–۱۲۹).

در بررسی امکان انطباق چنین رفتارهایی با محاربه، مسئله اصلی آن است که آیا می‌توان مفهوم سلاح را از ابزارهای متعارف جسمانی فراتر برد و کدهای تهاجمی را نیز، در صورت برخورداری از کارکرد ارعاب‌آمیز و ایجاد ناامنی عمومی، در تحلیل موضوع وارد کرد. از منظر کارکردی، ابزار دیجیتال ممکن است بدون تماس فیزیکی، قدرت اخلال، تهدید و سلب امنیتی هم‌سنگ برخی ابزارهای سنتی پیدا کند؛ اما توسعه مفهوم سلاح به‌تنهایی برای تحقق محاربه کافی نیست و باید عناصر خاص این عنوان، از جمله قصد ارعاب و کیفیت رفتار، جداگانه احراز شود. در غیر این صورت، رفتار می‌تواند حسب مورد ذیل تعزیر و عناوین کیفری دیگر قرار گیرد، نه حد محاربه (خضیر، ۲۰۲۳: ۶۱۱–۶۱۲؛ بومعزهٔ، ۲۰۲۰: ۱۰۶–۱۰۷).

همچنین، حمله به دارایی‌ها و زیرساخت‌های عمومی، افزون بر مسئولیت مالی، می‌تواند تعرض به حقوق جمعی و امنیت اقتصادی جامعه باشد. تعبیر «تروریسم اقتصادی» در این زمینه وصفی تحلیلی برای رفتارهای سازمان‌یافته با هدف ایجاد هراس و فروپاشی کارکردهای حیاتی است، نه عنوانی حدی و مستقل در فقه. بنابراین، مبنای جرم‌انگاری باید بر احراز دقیق عناصر شرعی هر عنوان و تناسب پاسخ کیفری استوار باشد تا حمایت از امنیت اقتصادی به توسعه نامحدود حدود و نادیده‌گرفتن اصل احتیاط در تعیین مجازات‌ها نینجامد.

۵-۴. سنتز و همگرایی تطبیقی؛ الگوی نوین بازتعریف «حمله» بر پایه امنیت اقتصادی

پیوند میان آموزه‌های فقه اقتصادی و قواعد حقوق بین‌الملل کیفری، بستری تحلیلی برای همگرایی هنجاری در بازتعریف مفهوم تجاوز و حمله پدید می‌آورد؛ از این‌رو، در این بخش با تطبیق رویکردهای کارکردی طرفین و شناسایی خلأهای تقنینی، معیاری سه‌گانه و بومی برای احراز حملات سایبری متجاوزانه با ابعاد کلان اقتصادی صورت‌بندی می‌شود.

۵-۴-۱. نقاط اشتراک

اشتراک بنیادین فقه اسلامی و حقوق بین‌الملل کیفری در مواجهه با عملیات‌های سایبری مخرب، در امکان عبور از ظاهر مادی رفتار و توجه به آثار واقعی آن بر انسان و مناسبات اجتماعی آشکار می‌شود. در هر دو نظام، حمایت حقوقی نباید صرفاً به جسم اشیا یا ابزار ارتکاب محدود بماند؛ زیرا ارزش حمایت از اموال و زیرساخت‌ها، در نهایت به نقشی بازمی‌گردد که در حفظ جان، امنیت، معیشت و کرامت انسان‌ها ایفا می‌کنند. از این منظر، تخریب یک سامانه بانکی یا مختل‌ساختن شبکه توزیع دارو، حتی اگر با انفجار، آتش‌سوزی یا آسیب کالبدی همراه نباشد، می‌تواند به سبب محروم‌ساختن اشخاص از خدمات ضروری و ایجاد زنجیره‌ای از زیان‌های انسانی، واجد اهمیت حقوقی جدی باشد. در حقوق بین‌الملل کیفری،

این رویکرد نتیجه‌محور امکان ارزیابی رفتار را بر پایه پیامدهای آن فراهم می‌کند؛ بااین‌حال، آثار زیان‌بار به‌تنهایی جایگزین عناصر قانونی جرم، رابطه رفتار با مخاصمه و شرایط مسئولیت کیفری نمی‌شوند. در فقه اسلامی نیز قواعد حمایتی و مقاصد شریعت، به‌ویژه صیانت از جان، مال و کرامت انسان، نشان می‌دهند که معیار ارزیابی نباید به صورت فیزیکی خسارت منحصر شود. توجه به غایت حمایت از غیرنظامیان و منع رفتارهایی که امنیت و زندگی آنان را به مخاطره می‌اندازد، زمینه‌ای برای فهم کارکردی زیان‌های نوپدید فراهم می‌آورد (آل رشود و صالح، ۲۰۲۵: ۲۱۲۵–۲۲۲۴؛ خنوش و مساعید، ۲۰۲۱: ۸۸–۸۹؛ الحولی، ۲۰۱۸: ۱–۲).

همگرایی این دو منظومه، در پذیرش تقدم انسان و نیازهای اساسی او بر شکل مادی وسیله یا موضوع تعرض است؛ هرچند مبانی، قلمرو و ضمانت‌اجراهای آن‌ها یکسان نیست. بنابراین، در تحلیل حملات سایبری باید پرسید چه کارکرد حیاتی از میان رفته، چه حقوقی مختل شده و چه پیامدی بر زندگی جمعی تحمیل شده است. این معیار، بدون توسعه بی‌ضابطه عناوین کیفری، امکان می‌دهد خسارت ناملموس نیز هنگامی که به تهدیدی واقعی علیه حیات، معیشت و کرامت انسانی تبدیل می‌شود، در ارزیابی حقوقی جایگاه شایسته خود را بیابد.

۵-۴-۲. خلأهای موجود در حقوق عرفی و پیشنهاد برای رویه قضایی

خلأ حقوق موجود در مواجهه با عملیات‌های سایبری، فقدان قواعد قابل اعمال نیست، بلکه دشواری انطباق مفاهیم سنتی جرم بر رفتارهایی است که آثار خود را از مسیر ناملموس پدید می‌آورند. ازاین‌رو، بازنگری در فهم عنصر مادی جرایم بین‌المللی ضرورت دارد؛ اما نباید به توسعه نامحدود عناوین مجرمانه یا کنارگذاشتن اصل قانونی‌بودن جرم و مجازات بینجامد. رفتار، نتیجه و رابطه سببیت باید با توجه به ویژگی‌های عملیات سایبری و در چهارچوب عناصر قانونی هر جرم ارزیابی شوند؛ نه آنکه فقدان تخریب فیزیکی، امکان تحقق جرم را منتفی سازد. ضرورت تدوین چارچوبی برای پاسخ کیفری به جرایم سایبری نیز از شکاف میان تحول ابزار ارتکاب و صورت‌بندی سنتی مسئولیت ناشی می‌شود (الشهری و المکی، ۲۰۲۶: ۳–۴).

در رسیدگی قضایی، گستره اختلال، وضعیت قربانیان، ماهیت زیرساخت هدف و تأثیر رفتار بر حقوق بنیادین باید در تشخیص عناصر مادی لحاظ شوند. ازکارانداختن زیرساختی حیاتی ممکن است بدون تخریب فیزیکی، دسترسی جمعیت را به خدمات ضروری مختل کند؛ بااین‌حال، این پیامد تنها هنگامی در مسئولیت کیفری مؤثر است که با رفتار ممنوع و نتیجه مقرر در عنوان مجرمانه ارتباط داشته باشد. توجه به آثار انسانی و سنجش تناسب، مانع فروکاستن ارزیابی قضایی به نمودهای کالبدی خسارت می‌شود (محمد، ۲۰۲۶: ۳۹۲–۳۹۳). سنجش شدت رفتار سایبری نیز باید ابعاد کمی و کیفی، شیوه ارتکاب و اثرگذاری آن را در برگیرد (Roscini, 2019: 259–260). الهام از قواعد حمایتی فقهی، به‌ویژه صیانت از جان و مال و نفی اضرار، در فهم غایت حمایت کیفری راهگشاست؛ اما این اصول جایگزین عناصر اساسنامه رم نیستند. در حقوق عرفی نیز تعیین دامنه قاعده باید بر بررسی رویه دولت‌ها و پذیرش حقوقی آن استوار باشد (Pomson, 2023: 1023–1024). بنابراین، راهکار مطلوب، تفسیر زمینه‌مند و آثارمحور در محدوده متن قانونی، همراه با اثبات رفتار، نتیجه، سببیت و عنصر روانی است؛ رویکردی که از بی‌کیفرمانی جلوگیری می‌کند و مانع گسترش ناموجه صلاحیت می‌شود.

۵-۴-۳. ارائه معیار سه‌گانه پیشنهادی برای احراز «حمله سایبری متجاوزانه»

بازتعریف آستانه حمله سایبری متجاوزانه مستلزم سنجشی چندبعدی است؛ زیرا نه بزرگی زیان مالی به‌تنهایی تعیین‌کننده است و نه انتخاب زیرساختی مهم، وصف تجاوزکارانه ایجاد می‌کند. معیار نخست، مقیاس اثر اقتصادی است. در این سنجش باید گستره اختلال، شمار اشخاص و بنگاه‌های متأثر، میزان توقف مبادلات، اختلال در پرداخت‌ها و آثار زنجیره‌ای بر تولید و توزیع کالا بررسی شود. عملیات علیه زیرساخت مالی، حتی بدون تخریب فیزیکی، اگر کارکرد اقتصادی جامعه را به‌طور جدی مختل کند، ممکن است از آستانه زیان فراتر رود؛ بااین‌حال، ارزیابی شدت و پیامدها باید با اوضاع هر مورد انجام شود (Spáčil, 2022: 31–32).

معیار دوم، ماهیت حیات‌بخش زیرساخت هدف است. اهمیت شبکه بانکی، انرژی، آب، حمل‌ونقل و خدمات درمانی از آن جهت است که استمرار زندگی و دسترسی به نیازهای اساسی به عملکرد آن‌ها وابسته است. بااین‌حال، حیاتی‌بودن هدف به‌تنهایی برای احراز حمله کافی نیست؛ باید نشان داد عملیات چگونه کارکرد آن را مختل کرده و چه آثار بر جمعیت غیرنظامی گذاشته است. ازکارافتادن سامانه بیمارستانی یا شبکه توزیع دارو، در شرایطی که درمان را ناممکن سازد، اهمیت این پیوند را آشکار می‌کند (Urs, Dias, Coco, & Akande, 2023: 45–46).

معیار سوم، پایداری اختلال و تأثیر آن بر حقوق بنیادین و زیست اجتماعی است. اختلال کوتاه‌مدت و قابل جبران، از حیث شدت با محرومیت طولانی‌مدت از درمان، آب، انرژی یا دسترسی به دارایی‌های مالی یکسان نیست. مدت استمرار، دشواری بازیابی، نبود جایگزین و پیامدهای انسانی باید در کنار یکدیگر سنجیده شوند؛ چنان‌که آثار غیرمادی مهم، از جمله توقف خدمات ضروری و زیان اقتصادی شدید، در ارزیابی حمایت از غیرنظامیان نادیده نماند (Biggio, 2025: 253–254). این سه معیار، در این پژوهش، چارچوبی تحلیلی مستقل برای تشخیص شدت و ماهیت عملیات فراهم می‌کنند، نه قاعده‌ای مستقل و خودکار برای احراز تجاوز. تحقق عنوان حقوقی همچنان به انتساب، زمینه وقوع و شرایط مقرر در قواعد مربوط وابسته است.

۶. نتیجه

پژوهش حاضر با هدف بازتعریف آستانه توسل به زور و مفهوم حمله در پرتو تحولات ناشی از عملیات‌های سایبری مخرب، به واکاوی پیوند میان حقوق بین‌الملل کیفری و فقه اقتصادی امامیه پرداخت. یافته‌های این بررسی نشان می‌دهد که تفسیر مضیق و کلاسیک از ماده ۵۱ و بند ۴ ماده ۲ منشور ملل متحد و نیز ماده ۴۹ پروتکل اول الحاقی، که مفهوم حمله یا توسل به زور را منحصراً به اقدامات متضمن نیروی کالبدی، حرارتی و جنبشی تقلیل می‌داد، در زیست‌بوم امنیتی معاصر کارآمدی خود را از دست داده است. پاسخ روشن به پرسش نخست آن است که آستانه ورود یک عملیات رقومی به قلمرو «حمله مسلحانه» نباید بر پایه ماهیت ابزار به‌کاررفته، بلکه باید بر مبنای مقیاس و آثار مخرّب آن سنجیده شود. بر این اساس، عملیات‌های سایبری که کارکرد سامانه‌های تسویه ناخالص آنی بانکی، شبکه‌های سوخت‌رسانی یا خدمات حیاتی سلامت را فلج می‌سازند، حتی بدون بر جای گذاشتن آوار فیزیکی، به سبب تولید همان پیامدهای ناشی از تهاجم کالبدی، ماهیتاً مصداق توسل به زور و حمله مسلحانه به شمار می‌آیند.

در پاسخ به پرسش دوم پیرامون قابلیت تحقق ارکان مادی جرایم مندرج در اساسنامه رم، تحلیل نشان داد که تخریب سیستماتیک و گسترده داده‌های زیرساختی به موجب قواعد تفسیر غایت‌گرایانه، به‌طور کامل با عناصر مادی جنایت جنگی موضوع تخریب نامتناسب اموال، جنایت علیه بشریت به جهت تحمیل رنج شدید از طریق قطع شریان‌های حیاتی زیست مدنی، و در شرایط تهاجم فلج‌کننده سراسری، با جنایت تجاوز موضوع ماده ۸ مکرر انطباق دارد؛ تفکیک سنتی میان اتلاف داده و تخریب فیزیکی در عصر وابستگی تامِ دارایی‌ها به محیط رقومی، مبنای حقوقی خود را از دست داده است. از دیگر سو، در ساحت فقه اقتصادی امامیه و در پاسخ به پرسش سوم، اثبات گردید که داده‌ها و سرمایه‌های رقومی به جهت دارا بودن مالیت عرفی و منافع عقلایی، در شمول احکام اموال محترم قرار دارند. از این‌رو، اخلال سازمان‌یافته در سامانه‌های مالی با اتکا به قواعد بنیادینی همچون اتلاف، تسبیب، لاضرر و نفی حرج، مستوجب ضمان قهری کامل است. افزون بر این، در بعد هنجارگذاری کیفری، توسعه موضوعی عناوین افساد فی‌الارض، اخلال در نظام اقتصادی و خروج مفهوم سلاح از انحصار ادوات سنتی و شمول آن بر کدهای مخرب تهاجمی، چارچوبی منسجم برای کیفرگذاری تروریسم اقتصادی فراهم می‌آورد.

بنابراین، ضروری است نظام‌های تقنینی ملی با گذر از قوانین سنتی رایانه‌ای، قوانین کیفری ماهوی ویژه‌ای را تصویب کنند که اختلال سایبری ساختاری علیه اموال عمومی و حاکمیتی را هم‌طراز جرایم علیه امنیت ملی جرم‌انگاری نماید. در عرصه بین‌المللی نیز مجمع دولت‌های عضو اساسنامه رم باید از رهگذر الحاق اسناد تفسیری به ارکان جرایم، به پذیرش صریح آثار ناملموس اما ویرانگر سایبری اقدام ورزند تا مانع گریز ناقضان از مسئولیت کیفری شوند. در نهایت، تلفیق تفاسیر پویای فقهی در مراجع داوری و معاهدات چندجانبه، ابزاری

بنیادین برای موازنه‌سازی در برابر انحصار هنجارسازی قدرت‌های بزرگ فراهم می‌آورد. چنین رویکردی که بر تقدم صیانت از معیشت عمومی، کرامت انسانی و زیست پایدار استوار است، می‌تواند به عنوان سپری هنجاری، حاکمیت اقتصادی و تاب‌آوری ملی کشورهای در حال توسعه را در نظام حقوق بین‌الملل تثبیت کند.

۷. سهم نویسندگان

نگارش متن، نظارت علمی و اصلاحات نهایی توسط نویسنده مسئول صورت گرفت.

۸. تضاد منافع

در این پژوهش هیچگونه تضاد منافعی وجود ندارد.

منابع

منابع عربی

- آل رشود، ریاض بن راشد عبد الله، و صالح، نهی الشافعی محمود. (۲۰۲۵). دراسة مقارنة بین مواد القانون الدولی الإنسانی وأحکام الشریعة الإسلامیة حول حمایة المدنیین فی النزاعات المسلحة. المجلة القانونیة، ۲۴(۵)، ۲۱۶۹–۲۲۲۴.
- البرعی، أحمد سعد علی. (۲۰۲۴). وقف الأصول الرقمیة: دراسة فقهیة قانونیة. مجلة الوقف، ۲۰۲۴(۳)، ۸۵–۱۲۹.
- بودقرزام، سامیة، ونوبس، نبیل. (۲۰۲۵). سرقة البیانات الإلکترونیة: دراسة تأصیلیة مقارنة بین الأحکام الشرعیة والقانون الجزائری. مجلة الدراسات القانونیة والاقتصادیة، ۸(۲)، ۱۸۲–۲۰۵.
- بوزغار، دلیلة. (۲۰۱۷). قاعدة «لا ضرر ولا ضرار»: نماذج تطبیقیة فی الاقتصاد الإسلامی. مجلة جامعة الأمیر عبد القادر للعلوم الإسلامیة، ۳۱(۲)، ۴۳۳–۴۵۶.
- بومعزة، إبتسام. (۲۰۲۰). موقف الشریعة الإسلامیة من الإرهاب الإلکترونی. مجلة القانون والتنمیة المحلیة، ۲(۲)، ۹۵–۱۱۲.
- الحربی، هویدا بنت بخیت حمید اللهیبی. (۲۰۲۵). المتاجرة بالبیانات الشخصیة فی ضوء الفقه الإسلامی. مجلة مداد الآداب، ۱۵(۴۱)، ۱۱۱۳–۱۱۶۴.
- الحناوی، أمجد محمد عاطف، والعموش، محمد محمود. (۲۰۲۵). قواعد الضمان فی الفقه الإسلامی، وتطبیقاتها الفقهیة والمعاصرة. مجلة جامعة أم درمان الإسلامیة للعلوم الإسلامیة والقانونیة، ۲۱(۳)، ۴۱۸–۴۴۳.
- الحولی، ماهر حامد محمد. (۲۰۱۸). حمایة المدنیین فی الشریعة الإسلامیة والقانون الدولی الإنسانی. مجلة الجامعة الإسلامیة للدراسات الشرعیة والقانونیة، ۲۶(۱)، ۱–۲۹.
- خضیر، علی عبد الفتاح بسیونی. (۲۰۲۳). الرؤیة الفقهیة والقانونیة لمدی تطبیق حد الحرابة علی الجرائم الإلکترونیة: دراسة مقارنة. مجلة الدرایة، ۲۳(۱)، ۶۱۱–۷۳۴.
- خنوش، سعید، و مساعید، عبد الوهاب. (۲۰۲۱). البعد المقاصدی لحمایة المدنیین أثناء النزاعات المسلحة، دراسة مقارنة فی الشریعة الإسلامیة والقانون الدولی الإنسانی. المجلة الجزائریة للعلوم القانونیة والسیاسیة، ۵۸(۳)، ۸۸–۱۲۶.

- الشهری، فاطمهٔ دربی سعد، و المکی، رواء غـازی. (۲۰۲۶). التنظیم الدولی للجرائم السیبرانیهٔ الدولیهٔ فی إطار القـانون الجنائی الدولی. المجلهٔ الدولیهٔ للبحوث والدراسات القانونیهٔ، ۵(۹)، ۱-۲۰.
- عنانبه، سوار أحمد. (۲۰۲۳). العلاقهٔ بین التعدی والضرر فی وجوب الضـمان فـی الفقـه الإسـلامی. المیـزان للدراسـات الإسلامیهٔ والقانونیهٔ، ۱۰(۴)، ۲۷۵–۳۰۱.
- مبارکیهٔ، مفیـدهٔ، وخلفـهٔ، عبـد الرحمـان. (۲۰۲۲). جـرائم المعلوماتیهٔ فی الفقه الإسلامی والتشـریع الجنـائی: دراسـهٔ تأصیلیهٔ مقارنهٔ [أطروحهٔ دکتوراه، جامعهٔ الأمیر عبد القـادر للعلوم الإسلامیهٔ]. المستودع الرقمـی لجامعـهٔ الأمیـر عبـد القادر للعلوم الإسلامیهٔ.
- محمد، أسامهٔ صبری. (۲۰۲۶). تطبیق مبـدأ التناسـب فـی العملیات السیبرانیهٔ: دراسهٔ فی ضوء مبادئ القانون الـدولی الإنسانی. مجلهٔ القادسیهٔ للقانون والعلـوم السیاسـیهٔ، ۱۷(۲، الجزء الأول)، ۳۶۳–۴۰۸.

منابع انگلیسی

- Biggio, G. (2025). Regulating non-kinetic effects of cyber operations: The ‘Loss of Functionality’ approach and the military necessity-humanity balance under international humanitarian law. Journal of Conflict and Security Law, 30(2), 241–263.
- Biggio, G. (2025). Regulating non-kinetic effects of cyber operations: The ‘Loss of Functionality’ approach and the military necessity-humanity balance under International Humanitarian Law. Journal of Conflict and Security Law, 30(2), 241–263.
- Brunner, I. (2025). Attributing cyber operations under international law: Political and legal aspects. Questions of International Law, 110, 27–43.
- Carpenter, Christine. (2025). Whose [crime] is it anyway? Adapting the crime of aggression to grapple with AI and the future of international crimes. Journal of International Criminal Justice, 23(1), 69–86.
- Delerue, F. (2020). Cyber operations and international law. Cambridge University Press.
- Gabrielli, G. (2023). Individual criminal responsibility of non-state actors operating in cyberspace for war crimes under the ICC Statute. EU and Comparative Law Issues and Challenges Series (ECLIC), 7, 286–315.
- Gisel, L., Rodenhäuser, T., & Dörmann, K. (2020). Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. International Review of the Red Cross, 102(913), 287–334.
- Haataja, S. (2022). Cyber operations against critical infrastructure under norms of responsible state behaviour and international law. International Journal of Law and Information Technology, 30(4), 423–443.
- Kis Kelemen, B. (2025). International armed conflicts in cyberspace. InterEULawEast: Journal for the International and European Law, Economics and Market Integrations, 12(1), 317–347.
- McKenzie, S. (2021). Cyber operations against civilian data: Revisiting war crimes against protected objects and property in the Rome Statute. Journal of International Criminal Justice, 19(5), 1165–1192.
- Office of the Prosecutor, International Criminal Court. (2025). Policy on cyber-enabled crimes under the Rome Statute.
- Office of the Prosecutor, International Criminal Court. (2025). Policy on cyber-enabled crimes under the Rome Statute.
- Permanent Mission of Liechtenstein to the United Nations. (2021). The Council of Advisers’ report on the application of the Rome Statute of the International Criminal Court to cyberwarfare.
- Pomson, O. (2023). Methodology of identifying customary international law applicable to cyber activities. Leiden Journal of International Law, 36(4), 1023–1047.

- Roscini, M. (2019). Gravity in the Statute of the International Criminal Court and cyber conduct that constitutes, instigates or facilitates international crimes. Criminal Law Forum, 30, 247–272.
- Schmitt, M. N. (Ed.). (2017). Tallinn manual 2.0 on the international law applicable to cyber operations (2nd ed.). Cambridge University Press.
- Spáčil, J. (2022). Cyber operations against critical financial infrastructure: A non-destructive armed attack? International and Comparative Law Review, 22(2), 27–42.
- Trahan, J. (2021). The criminalization of cyber-operations under the Rome Statute. Journal of International Criminal Justice, 19(5), 1133–1164.
- Trahan, Jennifer. (2025). Cyber operations and the crime of aggression. Case Western Reserve Journal of International Law, 57(1), 77–108.
- Tsagourias, N., & Farrell, M. (2020). Cyber attribution: Technical and legal approaches and challenges. European Journal of International Law, 31(3), 941–967.
- Urs, P., Dias, T., Coco, A., & Akande, D. (2023). The international law protections against cyber operations targeting the healthcare sector. Blavatnik School of Government, University of Oxford; Oxford Institute for Ethics, Law and Armed Conflict.
- Wilmshurst, E., Moynihan, H., & van Benthem, T. (2026). Securing justice for cyber-enabled international crimes: Legal foundations and practical routes to prosecution. Chatham House.
- Zarmsky, Sarah. (2024). Is international criminal law ready to accommodate online harm? Challenges and opportunities. Journal of International Criminal Justice, 22(1), 169–184.