حقوق تطبیقی

دو فصلنامهٔ علمی حقوق تطبیقی
دوره دوازدهم، شمارهٔ یک، بهار و تابستان ۱۴۰۴
شماره پیاپی ۲۳، صص ۲۵۳-۲۷۰
مقالهٔ پژوهشی

Law
Comparative

The Journal of Comparative Law
Semi-annual, Vol. 12, No. 1, Spring and Summer 2025
Issue 23, pp. 253-270
Original Article

مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری؛ مطالعهٔ تطبیقی رویهٔ بین‌المللی و اسناد ملی ایران

رخساره وزیری گودرزی*
محمد عرب طاط**
فاطمه زیبائی‌نژاد***

DOI: https://doi.org/10.22096/law.2026.2089138.2374
[تاریخ دریافت: ۱۴۰۵/۰۳/۰۵ تاریخ پذیرش: ۱۴۰۵/۰۴/۲۳]

چکیده

گسترش بی‌سابقهٔ حملات سایبری و ابهام در انطباق قواعد سنتی حقوق بین‌الملل بر این پدیدهٔ نوین، چالش‌های بنیادینی را در نظام مسئولیت بین‌المللی دولت‌ها ایجاد کرده است. چالش اصلی در این میان، مبنای انتساب است؛ یعنی دشواری احراز پیوند حقوقی میان یک حملهٔ سایبری که غالباً توسط بازیگران غیردولتی و با استفاده از زیرساخت‌های متعدد جهانی صورت می‌گیرد، با یک دولت مشخص. پژوهش حاضر با هدف واکاوی ابعاد حقوقی این پدیده و با روشی توصیفی-تحلیلی، به مطالعهٔ تطبیقی رویهٔ بین‌المللی، ازجمله طرح مواد مسئولیت دولت‌ها و اسناد راهبردی و قوانین ملی جمهوری اسلامی ایران می‌پردازد. یافته‌ها نشان می‌دهد که اگرچه دکترین «کنترل مؤثر» همچنان مبنای اصلی انتساب در حقوق بین‌الملل است، اما ماهیت پنهان و فرامرزی عملیات سایبری، بحث بر سر لزوم توسعهٔ معیارهای تکمیلی مانند «تکلیف به مراقبت» را ضروری ساخته است. بررسی اسناد ملی ایران نیز حاکی از اتخاذ رویکردی دفاع‌محور و مبتنی‌بر صیانت از زیرساخت‌های حیاتی است. نتایج این واکاوی تطبیقی بیانگر آن است که نظام حقوقی ایران، ضمن همسویی کلی با اصول عام بین‌المللی، نیازمند تدوین قواعد شفاف‌تری در زمینهٔ معیارهای انتساب و چهارچوب قانونی اقدامات متقابل سایبری است تا بتواند شکاف‌های هنجاری موجود را مرتفع ساخته و راهبردهای حقوقی فعالانه‌تری را در عرصهٔ بین‌المللی اتخاذ نماید.

واژگان کلیدی: مسئولیت بین‌المللی؛ حملات سایبری؛ مبنای انتساب؛ حقوق بین‌الملل؛ نظام حقوقی ایران؛ اقدامات متقابل.

* دانشجوی دکتری حقوق بین‌الملل، دانشکده حقوق، واحد قم، دانشگاه آزاد اسلامی، قم، ایران. (نویسنده مسئول)
Email: rokhsarehvazirig@gmail.com
** دانشجوی دکتری حقوق بین‌الملل، دانشکده حقوق، واحد دامغان، دانشگاه آزاد اسلامی، دامغان، ایران.
Email: mohamadarabtat1997@gmail.com
*** دانشجوی دکتری حقوق بین‌الملل، دپارتمان حقوق، دانشگاه مفید، قم، ایران.
Email: Zibaeinejad@mofidu.ac.ir

۱. مقدمه

توسعهٔ فناوری اطلاعات و ارتباطات وابستگی دولت‌ها به زیرساخت‌های سایبری را به‌طور چشمگیری افزایش داده است. در کنار مزایای این تحول، حملات سایبری به یکی از مهم‌ترین تهدیدات امنیتی تبدیل شده‌اند. برخلاف حقوق بین‌الملل سنتی که توسل به زور و نقض حاکمیت عمدتاً ازطریق ابزارهای فیزیکی صورت می‌گرفت، ماهیت فرامرزی و پنهان عملیات سایبری، مفاهیمی چون حاکمیت، عدم مداخله و مسئولیت بین‌المللی دولت‌ها را با چالش مواجه ساخته است.[۱] یکی از مسائل اساسی در این زمینه، انتساب حملات سایبری به دولت‌هاست. استفاده از هویت‌های جعلی، سرورهای واسط و مسیرهای ارتباطی پیچیده، شناسایی منشأ واقعی حملات را دشوار می‌کند. افزون‌بر انتساب فنی، انتساب حقوقی نیز مستلزم اثبات کنترل یا هدایت مؤثر یک دولت بر عاملان حمله است؛ امری که در فضای سایبر، با دشواری‌های فراوان همراه بوده و مسئولیت‌پذیری دولت‌ها را با ابهام روبه‌رو کرده است.[۲] اگرچه منشور ملل متحد و طرح مواد مسئولیت بین‌المللی دولت‌ها، مصوب ۲۰۰۱، چهارچوب کلی مسئولیت دولت‌ها را فراهم کرده‌اند، ویژگی‌های خاص فضای سایبر موجب شده است تلاش‌هایی نظیر تدوین «راهنمای تالین» برای تبیین قواعد حاکم بر عملیات سایبری صورت گیرد.[۳] بااین‌حال، هنوز اجماع روشنی دربارهٔ معیارهای انتساب و مسئولیت دولت‌ها در این حوزه وجود ندارد. جمهوری اسلامی ایران نیز به‌دلیل مواجهه با حملات سایبری علیه زیرساخت‌های حیاتی خود، نیازمند بهره‌گیری از ظرفیت‌های حقوق بین‌الملل و تقویت چهارچوب‌های حقوقی داخلی است.[٤] باوجود اهمیت این موضوع، پژوهش‌های پیشین عمدتاً بر ابعاد بین‌المللی یا کیفری جرایم سایبری متمرکز بوده و بررسی تطبیقی میان حقوق بین‌الملل و نظام حقوقی ایران کمتر مورد توجه قرار گرفته است.[۵] براین‌اساس، پژوهش حاضر با روش توصیفی-تحلیلی و رویکرد تطبیقی، چالش‌های انتساب و احراز مسئولیت دولت‌ها در قبال حملات سایبری را در حقوق بین‌الملل و نظام حقوقی ایران بررسی می‌کند.

---

1. Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 3-15.

2. James A. Green, *Cyber Warfare: A Multidisciplinary Analysis* (London: Routledge, 2015), 41-58.

3. Schmitt, *Tallinn Manual 2.0 on the International*, Rules 14-19.

٤. شورای عالی فضای مجازی، *سند راهبردی جمهوری اسلامی ایران در فضای مجازی*، شماره ثبت ۱۰۳۵۵۴ (تهران: مرکز ملی فضای مجازی، ۱۴۰۱)، بخش اهداف کلان، بندهای ۳، ۴، ۸ و ۹.

5. Majid Yar and Kevin F. Steinmetz, *Cybercrime and Society*, 3rd edition (London: Sage Publications, 2019), 221-230.

۲. واکاوی حقوقی حملهٔ سایبری و مبنای انتساب

برای احراز مسئولیت بین‌المللی یک دولت، ابتدا باید مشخص شود که آیا عمل رخ‌داده، از منظر حقوقی، یک تخلف بین‌المللی حملهٔ سایبری محسوب می‌شود و سپس، آیا این عمل قابل‌انتساب به آن دولت است یا خیر. این بخش به واکاوی این دو رکن اساسی می‌پردازد.

۲-۱. تبیین گسترهٔ مفهومی حملات سایبری در حقوق بین‌الملل معاصر

در حقوق بین‌الملل سنتی، مفهوم «حمله» غالباً با استفاده از نیروی مسلحانه فیزیکی موضوع بند ۴ مادهٔ ۲ و مادهٔ ۵۱ منشور ملل متحد گره خورده است. با ظهور فضای سایبر، تطبیق این مفاهیم با پدیده‌های نوظهور، به یک چالش اساسی تبدیل شد. امروزه در دکترین حقوقی و رویهٔ تفسیری دولت‌ها، با اتکا بر «رویکرد اثرمحور»، هرگونه عملیات سایبری که آثار مخرب آن مرگ، جراحت، یا تخریب فیزیکی اموال معادل یک حملهٔ مسلحانه سنتی باشد، تحت‌عنوان حملهٔ سایبری شناسایی می‌شود.[۶]

بااین‌حال، مفهوم‌شناسی موسع اقتضا می‌کند که عملیات‌های سایبری فروآستانه‌ای و ترکیبی، نظیر مداخله در انتخابات، جاسوسی سایبری مخرب و از کار انداختن زیرساخت‌های حیاتی بدون تخریب فیزیکی نیز مورد توجه قرار گیرند .این اقدامات اگرچه ممکن است نقض بند ۴ مادهٔ ۲ منشور یا همان اصل عدم توسل به زور نباشند، اما می‌توانند ناقض اصل عدم مداخله یا حاکمیت ملی دولت‌ها تلقی گردند و موجب مسئولیت بین‌المللی شوند؛ به‌ویژه آنکه در رویه و ادبیات حقوقی اخیر (۲۰۲۴-۲۰۲۵)، اثر تجمعی این سلسله عملیات‌های فروآستانه‌ای می‌تواند درمجموع، به‌عنوان نقض فاحش حاکمیت سایبری یا حتی معادل توسل به زور ارزیابی گردد.[۷]

۲-۲. چالش‌های احراز هویت: از موانع فنی تا مرحلهٔ اثبات حقوقی

انتساب یک عملیات سایبری به یک بازیگر خاص، یکی از پیچیده‌ترین گره‌های حقوق

---

6. Michael N. Schmitt and Anusha S. Pakkam, "Cyberspace and the Jus ad Bellum: The State of Play," *International Law Studies* 103 (2024): 194-229.

7. Michael N. Schmitt, "Big Data: International Law Issues Below the Armed Conflict Threshold," in *Big Data and Armed Conflict: Legal Issues Above and Below the Armed Conflict Threshold*, eds. Laura A. Dickinson and Edward W. Berg (Oxford: Oxford University Press, 2024), 29-54.

بین‌الملل سایبری است. این چالش دارای دو لایهٔ مجزا اما درهم‌تنیده است: لایهٔ فنی و لایهٔ حقوقی. در سطح فنی، مهاجمان سایبری با استفاده از تکنیک‌هایی نظیر جعل نشانی اینترنتی، مسیریابی ازطریق سرورهای نیابتی در کشورهای ثالث و استفاده از شبکه‌های آلوده، هویت و مکان واقعی خود را پنهان می‌کنند. علاوه‌براین، استفاده از عملیات پرچم دروغین و پیچیدگی تهدیدات مستمر پیشرفته رهگیری فنی را با ابهام مضاعف مواجه ساخته است.

حتی اگر انتساب فنی با موفقیت انجام شود، گذر از مرحلهٔ اثبات حقوقی چالش دیگری است. دیوان بین‌المللی دادگستری (ICJ) در رویهٔ خود، استانداردهای اثباتی مختلفی را مطرح کرده است، اما در فضای سایبر که ادله غالباً ماهیت دیجیتال و فرّار دارند، رسیدن به استاندارد ادلهٔ روشن و متقاعدکننده و یا با استاندارد سخت‌گیرانهٔ ادلهٔ کاملاً قاطع که دیوان در قضیه نسل‌کشی بوسنی مطرح کرد، برای انتساب یک حمله به یک دولت خارجی بسیار دشوار است. به همین دلیل، دکترین حقوقی جدید به‌سمت پذیرش استانداردهای منعطف‌تر یا انتساب مبتنی‌بر شواهد قرینه‌ای در فضای سایبر متمایل شده است.[۸]

صرف اینکه یک حمله از زیرساخت‌های یک کشور نشئت گرفته باشد، برای انتساب حقوقی آن عمل به دولتِ میزبان آن زیرساخت کفایت نمی‌کند. در چنین بن‌بست‌های اثباتی، استناد به نقض تکلیف به مراقبت مقتضی می‌تواند خلأ انتساب مستقیم را تا حدودی جبران نماید؛ بدین معنا که دولت میزبانِ زیرساخت، نه به‌دلیل انجام خود حمله، بلکه به‌سبب کوتاهی در اتخاذ تدابیر پیشگیرانه و صیانت از قلمرو سایبری خود، دارای مسئولیت بین‌المللی شناخته می‌شود.[۹]

۲-۳. دکترین کنترل موثر و قابلیت انتساب رفتار بازیگران غیردولتی سایبری به دولت‌ها

دولت‌ها برای فرار از مسئولیت بین‌المللی، غالباً حملات سایبری خود را ازطریق گروه‌های هکری مستقل، هکتیویست‌ها یا بازیگران غیردولتی که امروزه تحت‌عنوان نیروهای نیابتی سایبری یا گروه‌های تهدید مستمر پیشرفته با حمایت دولتی شناخته می‌شوند[۱۰] انجام می‌دهند. براساس مادهٔ ۸ طرح مواد کمیسیون حقوق بین‌الملل درخصوص مسئولیت دولت‌ها، رفتار شخص یا گروهی از اشخاص، درصورتی به دولت منتسب می‌شود که آن شخص یا گروه،

8. Nicholas Tsagourias and Michael Farrell, "Cyber Attribution: Technical and Legal Approaches and Challenges," *European Journal of International Law* 31, no. 3 (2020): 941-967.
9. Tsagourias and Farrell, "Cyber Attribution: Technical and Legal".
10. Tsagourias and Farrell, "Cyber Attribution: Technical and Legal".

درواقع، تحت هدایت یا کنترل مؤثر آن دولت عمل کرده باشد.

دیوان بین‌المللی دادگستری، در قضیهٔ نیکاراگوئه، معیار کنترل مؤثر را برای انتساب اعمال گروه‌های مسلح به دولت‌ها تثبیت کرد. در فضای سایبر، این معیار به این معناست که صرف حمایت مالی، فنی یا ایدئولوژیک از یک گروه هکری، برای انتساب حملات به دولت کافی نیست و باید کنترل مؤثر بر عملیات‌ها اثبات شود؛ امری که به‌دلیل ماهیت پنهان سایبری، بار اثباتی سنگینی بر دوش دولت زیان‌دیده قرار می‌دهد.[۱۱] در مقابل، برخی دکترین‌های نوین، با اشاره به قضیهٔ تادیچ، معیار کنترل کلی را منعطف‌تر می‌دانند و پیشنهاد می‌کنند برای جلوگیری از فرار دولت‌های حامی، این استاندارد در فضای سایبر مورد توجه قرار گیرد.[۱۲]

۳. ساختار حقوقی دفاع سایبری: بازخوانی اسناد بین‌المللی در کنار موازین ملی ایران

درک مسئولیت بین‌المللی سایبری مستلزم بررسی ساختار دفاع سایبری در حقوق بین‌الملل و نظام حقوقی ایران در سه محور است.

۳-۱. هنجارگذاری بین‌المللی: از راهنمای تالین تا مجمع عمومی سازمان ملل متحد

نظام حقوق بین‌الملل، در مواجهه با فضای سایبر، مسیر پرچالشی را برای انطباق قواعد سنتی با واقعیت‌های فناوری طی کرده است. در این راستا، راهنمای تالین نسخه‌های ۱ و ۲ و روند جاری تدوین نسخهٔ ۳ که بر رویهٔ عملی دولت‌ها تمرکز دارد،[۱۳] راهنمای تالین به‌عنوان مهم‌ترین تلاش نظری در تفسیر حقوق بین‌الملل سایبری، حاکمیت دولت‌ها را در فضای سایبر قابل‌اعمال می‌داند و نقض زیرساخت‌های حیاتی را نقض حاکمیت تلقی می‌کند. دربارهٔ ماهیت حقوقی حاکمیت سایبری اختلاف‌نظر وجود دارد، اما رویهٔ اخیر دولت‌ها و گزارش‌های سازمان ملل نشان‌دهندهٔ گرایش به پذیرش آن به‌عنوان قاعده‌ای مستقل است.

یکی از مفاهیم کلیدی در هنجارگذاری بین‌المللی سایبری، بسط اصل تکلیف به مراقبت است که ریشه در رویهٔ قضایی دیوان بین‌المللی دادگستری در قضیهٔ کانال کورفو ۱۹۴۹ دارد.

---

11. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, I.C.J. Reports 1986, p. 14, paras. 109 and 115.

12. Prosecutor v. Duško Tadić. Case No. IT-94-1-A. Judgment (Appeals Chamber). International Criminal Tribunal for the Former Yugoslavia, 15 July 1999, paras. 117-145.

13. Michael N. Schmitt and Liis Vihul, "Sovereignty in Cyberspace: Lex Lata Vel Non?" *American Journal of International Law* 111, no. 4 (2017): 213-218.

براساس این اصل، هیچ دولتی حق ندارد اجازه دهد از قلمرو آن برای اقداماتی استفاده شود که حقوق سایر دولت‌ها را نقض می‌کند. گروه کارشناسان دولتی سازمان ملل متحد، در گزارش سال ۲۰۱۵ خود که به تأیید و اجماع اعضا رسید، این اصل را وارد فضای سایبر کردند و مقرر داشتند که دولت‌ها نباید آگاهانه اجازه دهند قلمرو سایبری آن‌ها بستر ارتکاب اعمال متخلفانهٔ بین‌المللی قرار گیرد.[۱۴] اعمال اصل مراقبت در فضای سایبر، با چالش‌های فنی و تعارض با حریم خصوصی روبه‌روست. بنابراین، تعهد دولت‌ها در این حوزه، تعهد به وسیله است و در دکترین جدید، متناسب با ظرفیت کشورها تفسیر می‌شود.[۱۵]

تفکیک میان مداخلهٔ غیرقانونی، توسل به زور و حملهٔ مسلحانه در فضای سایبری، براساس آستانهٔ شدت و گستردگی ارزیابی می‌شود. درصورت ایجاد آثار مخرب جدی مانند تخریب فیزیکی یا تلفات جانی، عملیات سایبری می‌تواند معادل حملهٔ مسلحانه تلقی شود و حق دفاع مشروع را برای دولت قربانی ایجاد کند.

اما امروزه یکی از اصلی‌ترین چالش‌ها در ساختار حقوقی دفاع سایبری، نحوهٔ واکنش به عملیات‌های موسوم به مادونِ آستانه و یا فروآستانه‌ای است. این عملیات‌ها که در منطقهٔ خاکستری قرار می‌گیرند، عامدانه به‌گونه‌ای طراحی می‌شوند که ازحیث شدت و آثار، پایین‌تر از معیار حملهٔ مسلحانه طبقه‌بندی شوند و درنتیجه، حق دفاع مشروع را برای دولت قربانی ایجاد نکنند. حملاتی مانند باج‌افزارها یا مداخله در انتخابات که اگرچه به آستانهٔ حملهٔ مسلحانه نمی‌رسند، اما ثبات بین‌المللی را به‌شدت تهدید می‌کنند و تنها حق توسل به اقدامات متقابل غیرمسلحانه را برای دولت متضرر ایجاد می‌نمایند.[۱۶] برای مقابله با این خلأ راهبردی، دکترین حقوقی اخیراً به‌سمت استفاده از رویکرد اثرمحور و یا ضابطهٔ پیامدمحور و همچنین ارزیابی اثر تجمعی حملات مستمر گرایش یافته است تا عملیات‌های پایین‌تر از حدنصاب حملهٔ مسلحانه که موجب فلج سیستمی اقتصاد یا بهداشت یک کشور می‌شوند را نیز هم‌سنگ توسل به زور ارزیابی کند.[۱۷]

---

14. United Nations General Assembly, 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, 2015.

15. Russell Buchan and Nicholas Tsagourias (eds.), *Research Handbook on International Law and Cyberspace* (Cheltenham: Edward Elgar Publishing, 2021), 180-195.

16. François Delerue, *Cyber Operations and International Law* (Cambridge: Cambridge University Press, 2020), 224-226.

17. Delerue, *Cyber Operations and International Law*.

۳-۲. چهارچوب‌های هنجاری و اسناد راهبردی ایران: حاکمیت سایبری و دکترین دفاع مشروع

نظام حقوقی و ساختار دفاعی جمهوری اسلامی ایران، در واکنش به تهدیدات سایبری، دستخوش تحول شده است. نهادهایی مانند شورای عالی فضای مجازی و سازمان پدافند غیرعامل، مسئول سیاست‌گذاری و دفاع از زیرساخت‌های حیاتی هستند. اسناد کلان نیز بر مصون‌سازی، تاب‌آوری و بازدارندگی فعال تأکید دارند. اما مهم‌ترین سندی که رویهٔ عملی و دیدگاه حقوقی ایران را به‌صراحت در عرصهٔ بین‌المللی بازتاب می‌دهد، «بیانیهٔ ستاد کل نیروهای مسلح درخصوص حقوق بین‌الملل فضای مجازی»، مصوب مرداد ۱۳۹۹ است.[۱۸] این سند، در مقایسه با راهنمای تالین، رویکردی حاکمیت‌محور و دفاعی ازسوی ایران را نشان می‌دهد. ایران برخلاف برخی کشورهای غربی، حاکمیت سایبری را قاعده‌ای الزام‌آور می‌داند و هرگونه مداخلهٔ بدون رضایت را نقض حاکمیت تلقی می‌کند. این رویکرد با مواضع کشورهای درحال‌توسعه، در نشست‌های اخیر سازمان ملل همسو است.[۱۹]

در عرصهٔ ملی و در تبیین ساختار حقوقی دفاع سایبری، اسناد راهبردی جمهوری اسلامی ایران ازجمله بیانیهٔ ستاد کل نیروهای مسلح، نشان‌دهندهٔ پویایی و همسویی با رویه‌های درحال تکامل جهانی است. دکترین حقوقی داخلی نیز اخیراً توجه ویژه‌ای به چالش‌های ناشی از عملیات سایبریِ پایین‌تر از سطح آستانهٔ توسل به زور معطوف داشته است. همان‌طور که در ادبیات اخیر حقوقی ایران تأکید شده است، تحول مفهوم توسل به زور، در پرتو این دسته از حملات سایبری عملیات‌های فروآستانه‌ای، نیازمند اتخاذ پاسخ‌های متناسب و مبتنی‌بر حقوق بین‌الملل دفاعی است تا بازدارندگی لازم در برابر تهدیدات منطقهٔ خاکستری تأمین گردد.[۲۰] علاوه‌براین، در مقابله با عملیات‌های سایبری پراکنده که زیرساخت‌های حیاتی را هدف قرار می‌دهند، استناد به اصل عدم مداخله در امور داخلی و صیانت از حاکمیت سایبری، به‌عنوان قواعدی مستقل و بنیادین در اسناد راهبردی ایران جایگاهی محوری یافته است؛ رویکردی که نشان‌دهندهٔ گذار دکترین دفاعی کشور به‌سمت استفادهٔ حداکثری از

---

۱۸. ستاد کل نیروهای مسلح جمهوری اسلامی ایران، بیانیه درخصوص حقوق بین‌الملل فضای مجازی، مرداد ۱۳۹۹.

19. Keir Giles, and Andrew Monaghan, *Legality in Cyberspace: An Adversary View* (Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press, 2014) 45-67.

20. United Nations General Assembly, Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/75/816, 18 March 2021.

ظرفیت‌های حقوقی، برای مقابله با طیف متنوعی از مداخلات سایبری متخاصمانه است.

در بخش مربوط به توسل به زورِ بیانیهٔ ستاد کل نیروهای مسلح، این نهاد نظامی راهبردی به‌صراحت رویکردی منطبق بر موازین منشور ملل متحد اتخاذ کرده است و اعلام می‌دارد که اگر حملات سایبری ازنظر مقیاس و آثار، به‌گونه‌ای باشد که خسارات مادی یا انسانی شدیدی به زیرساخت‌های حیاتی مانند تأسیسات هسته‌ای، شبکه‌های توزیع آب و برق، یا سیستم‌های ناوبری هوایی وارد کند، مشمول مادهٔ ۵۱ منشور ملل متحد تلقی می‌شود و جمهوری اسلامی ایران حق ذاتی خود را برای پاسخ متقابل ازطریق دفاع مشروع، خواه به‌صورت سایبری و خواه فیزیکی، با رعایت اصول ضرورت و تناسب، محفوظ می‌داند.[۲۱]

همچنین، درخصوص اصل تکلیف به مراقبت مقتضی، ایران رویکردی واقع‌گرایانه و مشروط اتخاذ کرده است. بیانیهٔ مذکور تصریح می‌کند که انتساب یک حملهٔ سایبری به یک دولت، صرفاً به‌دلیل آنکه حمله از زیرساخت‌های آن کشور نشئت گرفته، غیرقابل‌قبول است، مگر آنکه آگاهی و کنترل مؤثر آن دولت بر عملیات اثبات شود. پذیرش تعهد به مراقبت مقتضی ازسوی ایران، منوط به توانمندی‌های فنی، برخورداری از زیرساخت‌های لازم و دریافت ادلهٔ روشن ازسوی دولت متضرر شده است که این امر نشان‌دهندهٔ آگاهی تدوین‌کنندگان سند از چالش‌های فنی انتساب و تلاش برای جلوگیری از انتساب‌های بی‌اساس علیه ایران است.

۳-۳. رویکرد کیفری و بازدارنده: تقاطع صلاحیت ملی و رویه‌های عملی دولت‌ها

علاوه‌بر الزامات حقوق بین‌الملل عمومی و مسئولیت مدنی دولت‌ها، ساختار دفاع سایبری نیازمند بازوهای اجرایی قدرتمندی در حوزهٔ حقوق کیفری است که بتواند بازدارندگی ایجاد نماید. در نظام حقوقی ایران، قانون جرایم رایانه‌ای مصوب ۱۳۸۸ به‌عنوان قانون خاص، و قانون مجازات اسلامی مصوب ۱۳۹۲ به‌عنوان قانون عام، چهارچوب کیفری برخورد با حملات سایبری را ترسیم کرده‌اند.

یکی از نقاط قوت نظام حقوقی ایران در برخورد با حملات سایبری فرامرزی که توسط هکرها یا گروه‌های تحت‌حمایت دولت‌های متخاصم انجام می‌شود، ظرفیت‌های قانون مجازات اسلامی در اعمال صلاحیت‌های فراسرزمینی است. براساس مادهٔ ۵ این قانون که

21. Charter of the United Nations, 1945, art. 51.

مبتنی‌بر اصل صلاحیت حمایتی است، هر فردی، اعم از ایرانی یا غیرایرانی، که در خارج از قلمرو حاکمیت ایران، مرتکب جرائمی علیه امنیت داخلی یا خارجی، یا جاسوسی علیه ساختارهای حاکمیتی شود که شامل حملات سایبری به زیرساخت‌های حیاتی و سرقت داده‌های طبقه‌بندی‌شده نیز می‌گردد، طبق قوانین جمهوری اسلامی ایران محاکمه و مجازات خواهد شد. همچنین مطابق مادۀ ۸ قانون مجازات اسلامی، ظرفیت اعمال صلاحیت جهانی برای جرایم خاص سایبری که به‌موجب تعهدات بین‌المللی جرم‌انگاری شده‌اند، فراهم می‌گردد.[۲۲]

باوجوداین، در رویۀ عملی بین‌المللی، اعمال صلاحیت کیفری علیه عاملان دولتی یا گروه‌های سایبری تحت‌حمایت دولت‌ها، با سد محکم چالش‌های فنی و مصونیت‌های سیاسی روبه‌رو است. دولت‌ها غالباً از استرداد هکرهای خود امتناع می‌ورزند و احراز هویت فردی مجرمان در دادگاه‌های کیفری، به‌دلیل استفاده از تکنیک‌های پیچیدۀ جعل آدرس و شبکه‌های پنهان دارک‌وب، با استانداردهای بالای ادلۀ اثبات دعوای کیفری، عملاً غیرممکن و یا بسیار دشوار است.[۲۳]

در پاسخ به این بن‌بست حقوقی، رویۀ عملی دولت‌ها در سال‌های اخیر، به‌سمت استراتژی انتساب هماهنگ سیاسی و استفاده از ابزارهای بازدارندۀ غیرکیفری گرایش یافته است. در این استراتژی که در پرونده‌های مشهوری نظیر بدافزارهای شامون، واناکرای و نات‌پتیا مشاهده شد، ائتلافی از دولت‌ها، به‌صورت مشترک و خارج از چهارچوب محاکم بین‌المللی، یک دولت خاص را به‌عنوان عامل حمله معرفی می کنند.[۲۴] متعاقب این انتساب سیاسی، رژیم‌های تحریمی مستقلی، نظیر چهارچوب تحریم‌های سایبری اتحادیۀ اروپا، برای مسدود کردن اموال، ممنوعیت سفر و اعمال فشارهای اقتصادی بر افراد، نهادها و سازمان‌های اطلاعاتی دخیل در حملات سایبری فعال می‌شود.[۲۵]

---

۲۲. قانون مجازات اسلامی، مصوب ۱۳۹۲، ماده ۸.

23. Kubo Mačák, "Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors," *Journal of Conflict and Security Law 21*, no. 3 (2016): 405-428.

24. Florian J. Egloff and Myriam Dunn Cavelty, "Attribution and Knowledge Creation Assemblages in Cybersecurity Politics," *Journal of Cybersecurity* 7, no. 1 (2021).

25. Erica Moret and Patryk Pawlak, *The EU Cyber Diplomacy Toolbox: Towards a Cyber Sanctions Regime?* Brief No. 24 (Paris: European Union Institute for Security Studies (EUISS), 2017), 112-135.

در نبود معاهدهٔ جامع سایبری، دولت‌ها با ترکیب حقوق کیفری داخلی، دیپلماسی اجبارآمیز و تحریم‌های هدفمند، به‌دنبال تقویت بازدارندگی و جبران خلأهای انتساب در فضای سایبر هستند.

۴. واکاوی تطبیقی مسئولیت سایبری: هم‌گرایی‌ها، شکاف‌ها و الزامات راهبردی

ورود به عصر دیجیتال، دولت‌ها را با چالشی جدی در حوزهٔ مسئولیت بین‌المللی مواجه کرده است. فضای سایبری به‌دلیل ماهیت فرامرزی، سرعت بالا و پیچیدگی داده‌ها، چهارچوب‌های سنتی حقوق بین‌الملل مبتنی‌بر مرزهای سرزمینی را با مشکل مواجه می‌کند. جمهوری اسلامی ایران نیز به‌عنوان بازیگری فعال و هدف تهدیدات سایبری، با این چالش‌ها روبه‌روست. این بخش به‌صورت تطبیقی به بررسی رویکردهای ایران و رویه‌های بین‌المللی در این زمینه می‌پردازد.

۴-۱. تقابل معیارهای انتساب: نص‌گرایی کیفری داخلی، در برابر رویکرد چندوجهی بین‌المللی

نخستین و دشوارترین چالش در مسئولیت‌پذیری حملات سایبری، مسئلهٔ انتساب است. در فضای سایبری، تفکیک میان انتساب فنی و اثبات ارتباط اقدام با دولت بسیار پیچیده است. در این زمینه، شکافی میان رویکرد حقوق داخلی ایران و رویهٔ در حال تحول بین‌المللی وجود دارد.

الف) رویهٔ بین‌المللی: از کنترل مؤثر تا مراقبت مقتضی و انتساب سیاسی

در سطح بین‌المللی، انتساب یک حملهٔ سایبری به یک دولت، فرایندی صرفاً فنی نیست، بلکه امری کاملاً حقوقی و سیاسی است. معیار کلاسیک و سخت‌گیرانهٔ حقوقی وجود ضابطهٔ کنترل مؤثر است که توسط دیوان بین‌المللی دادگستری، در قضیهٔ نیکاراگوئه تبیین شد.[۲۶] برای انتساب اقدامات گروه‌های غیردولتی مانند هکرها به یک دولت، باید کنترل مستقیم آن دولت بر عملیات مشخص اثبات شود. این امر در فضای سایبری بسیار دشوار است، زیرا گروه‌های نیابتی می‌توانند با استقلال عمل کنند و اثبات ارتباط دولت‌ها پیچیده است. حتی معیار کنترل کلی در قضیهٔ تادیچ نیز به‌تنهایی پاسخ‌گو نیست. ازاین‌رو، گرایش به معیارهای تکمیلی افزایش

26. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, I.C.J. Reports 1986, p. 14, paras. 109 and 115.

یافته است. مهم‌ترینِ این معیارها، اصل مراقبت مقتضی است.[۲۷] این اصل که ریشه در قضیهٔ تنگهٔ کورفو دارد و در گزارش‌های گروه کارشناسان دولتی سازمان ملل متحد در سال ۲۰۱۵ نیز صراحتاً مورد تأیید قرار گرفته، بیان می‌دارد که دولت‌ها مکلف‌اند تمام اقدامات ممکن و معقول را برای پیشگیری، توقف و تحقیق دربارهٔ حملات سایبری که از قلمروشان یا ازطریق زیرساخت‌های آن‌ها نشئت می‌گیرد، به کار گیرند. در همین راستا، ادبیات حقوقی اخیر تأکید دارد که تعهد به مراقبت مقتضی، دیگر صرفاً یک اصل توصیه‌ای نیست، بلکه به‌عنوان یک عرف نوظهور، در مسئولیت ثانویهٔ دولت‌ها در قبال عملیات‌های سایبری فرامرزی تثبیت شده است.[۲۸] کوتاهی در انجام این تکلیف، مستقل از اینکه حمله توسط چه کسی انجام شده باشد، خود موجد مسئولیت مستقل بین‌المللی برای دولت میزبان، به‌دلیل نقض تعهد پیشگیری یا همان عدم اجرای اصل مراقبت مقتضی است.

علاوه‌بر الزامات حقوقی، شاهد ظهور پدیدهٔ نهادینه‌شدهٔ انتساب سیاسی هماهنگ هستیم. در این سازوکار، گروهی از دولت‌ها، اغلب هم‌پیمانان غربی، به‌صورت مشترک، علنی و رسانه‌ای، یک دولت دیگر را مسئول یک حمله سایبری معرفی می‌کنند.[۲۹] این نوع انتساب، هرچند غالباً ادلهٔ قضایی، فنی و متقنِ محکمه‌پسند را منتشر نمی‌کند تا منابع اطلاعاتی خود را حفظ نماید، اما با ایجاد ائتلاف، اعمال فشار سنگین دیپلماتیک و مشروعیت‌بخشی به اقدامات متقابل، کارکردی تعیین‌کننده در رویهٔ دولت‌ها یافته است. دکترین نوین سایبری، این انتساب‌های هماهنگ را نه‌تنها یک اقدام سیاسی، بلکه گامی استراتژیک در جهت شکل‌دهی به حقوق عرفی بین‌المللی و تسهیلِ استناد به اقدامات متقابل جمعی ارزیابی می‌کند.[۳۰]

ب) رویکرد حقوق داخلی ایران: تمرکز بر مسئولیت کیفری فردی و محدودیت‌های بین‌المللی

در مقابل این رویکرد شبکه‌ای و چندوجهی، نظام حقوقی ایران، به‌ویژه در ساختار قانون جرایم رایانه‌ای مصوب ۱۳۸۸، رویکردی کاملاً مبتنی‌بر نص‌گرایی کیفری و احراز مسئولیت فردی اتخاذ کرده است. این قانون، با جرم‌انگاری طیف وسیعی از اقدامات مخرب سایبری از دسترسی غیرمجاز و شنود تا تخریب داده‌ها و جاسوسی رایانه‌ای، صرفاً بر شناسایی، تعقیب و

27. International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, in Yearbook of the International Law Commission, 2001, vol. II (Part Two), Articles 4, 8 and Commentary to Article 8.

28. Schmitt, *Tallinn Manual 2.0 on the International*, 45-68.

29. Egloff and Cavelty, "Attribution and Knowledge Creation".

30. Tsagourias and Farrell, "Cyber Attribution: Technical and Legal," 941-967.

مجازات شخص حقیقی یا حقوقیِ مرتکب جرم تمرکز دارد. دایرهٔ شمول صلاحیت دادگاه‌های کیفری ایران نیز براساس اصولی چون صلاحیت سرزمینی، مبتنی‌بر تابعیت و به‌ویژه اصل صلاحیت حمایتی تعریف شده است. این اصل که در مادهٔ ۵ قانون مجازات اسلامی مصوب ۱۳۹۲ تجلی یافته، به جرایم علیه امنیت داخلی و خارجی کشور، فارغ از محل وقوع جرم و تابعیت مرتکب تسری می‌یابد.[۳۱]

این رویکرد کیفری، هرچند برای مقابله با جرایم سایبری داخلی و هکرهای مستقل کارآمد است، اما در برخورد با حملات سایبریِ سازمان‌یافته با منشأ دولتی، با یک شکاف مفهومی و راهبردی مواجه است. قانون جرایم رایانه‌ای، چهارچوب و ابزاری برای مسئول ساختن دولت‌ها به‌عنوان تابعان اصلی حقوق بین‌الملل ارائه نمی‌دهد. درحالی‌که رویهٔ بین‌المللی به‌دنبال ایجاد مسئولیت مدنی و بین‌المللی برای حاکمیت‌ها، ازطریق مفاهیمی چون مراقبت مقتضی است، حقوق داخلی ایران صرفاً بر انتساب عنصر مادی و روانی جرم به یک فرد خاص تأکید دارد. این خلأ قانونی باعث می‌شود ظرفیت کشور برای بهره‌گیری سیستماتیک از ابزارهای حقوق بین‌الملل، جهت طرح دعوا یا اعمال فشار بر دولت‌های حامی حملات سایبری محدود بماند. مطالعات اخیر داخلی نیز با تأیید این شکاف، پیشنهاد می‌کنند که نظام حقوقی ایران باید علاوه‌بر به‌روزرسانی صلاحیت‌های کیفری، چهارچوب‌های مشخصی برای اعمال دیپلماسی حقوقی و طرح مسئولیت بین‌المللی دولت‌ها، براساس موازین نوین حقوق بین‌الملل سایبری تدوین نماید.

۴-۲. آستانهٔ توسل به زور و دفاع مشروع: هم‌گرایی دکترینال بر محور پیامد

یکی از حیاتی‌ترین و بحث‌برانگیزترین حوزه‌ها در حقوق بین‌الملل سایبری، تعیین خط مرزی یا نقطه‌ای است که در آن، یک عملیات متخاصمانهٔ سایبری، به‌مثابهٔ حملهٔ مسلحانه تلقی می‌شود و حق ذاتی دفاع مشروع نظامی موضوع مادهٔ ۵۱ منشور ملل متحد را برای دولت قربانی فعال می‌سازد. در این زمینهٔ خاص، برخلاف حوزهٔ انتساب، شاهد هم‌گرایی قابل‌توجهی میان دکترین نظامی و اعلامی ایران با موازین جهانی هستیم.

با توجه به ماهیت غیرفیزیکی غالب حملات سایبری که ازطریق کدهای مخرب اعمال می‌شوند، جامعهٔ بین‌المللی به‌سرعت دریافت که معیارهای سنتی و ابزارهای متداول و معمول دیگر پاسخ‌گو نیستند. ازاین‌رو، گرایش غالب به‌سمت ارزیابی حملات سایبری براساس نتایج

۳۱. قانون مجازات اسلامی، ماده ۵.

و میزان تخریب آن رفت؛ آنچه مهم است میزان تخریب است، نه ابزاری که برای حمله استفاده شده است. راهنمای تالین، به‌عنوان جامع‌ترین و معتبرترین تلاش آکادمیک برای تبیین حقوق بین‌الملل در فضای سایبری، در قاعدهٔ ۷۱ خود صراحتاً بیان می‌کند که مقیاس و آثار یک عملیات سایبری، تنها عامل تعیین‌کننده برای تصور آن به‌عنوان استفاده از زور یا حملهٔ مسلحانه است.[۳۲] درواقع، دکترین حقوقی معاصر تأکید دارد که رویکرد مبتنی‌بر آثار، اکنون از یک پیشنهاد نظری عبور کرده و به‌عنوان یک رویهٔ عرفیِ درحال ظهور، توسط اکثر قدرت‌های سایبری در ارزیابی توسل به زور پذیرفته شده است.[۳۳] عواملی که برای ارزیابی این مقیاس در نظر گرفته می‌شوند عبارت‌اند از شدت، فوریت، مستقیم بودن، تهاجمی بودن و قابل‌سنجش بودن اثرات.

براین‌اساس، یک حملهٔ سایبری که منجر به تلفات انسانی گسترده، آتش‌سوزی در تأسیسات صنعتی، سقوط هواپیما، یا از کار افتادن کامل و طولانی‌مدت خدمات ضروری دولتی مانند شبکهٔ برق یا سیستم بانکی شود، فارغ از اینکه ابزار آن یک موشک بوده یا یک بدافزار، از حدنصاب حملهٔ مسلحانه عبور کرده است. علاوه‌براین، رویهٔ بین‌المللی درحال پذیرش نظریهٔ تجمیع حوادث است؛ به این معنا که مجموعه‌ای از حملات سایبریِ مستمر و کوچک که هریک به‌تنهایی حملهٔ مسلحانه نیستند، درصورت تجمیع آثار، می‌توانند حق دفاع مشروع را ایجاد کنند. گزارش‌های راهبردی اخیر ناتو و نهادهای بین‌المللی نیز بر این نکته صحه گذاشته‌اند که آستانهٔ توسل به زور می‌تواند ازطریق عملیات‌های سایبری ترکیبی و جمعی که زیرساخت‌های حیاتی را به‌صورت فرسایشی مختل می‌کنند، نقض گردد.[۳۴]

دکترین رسمی و اعلامی جمهوری اسلامی ایران، به‌طور شگفت‌انگیزی، با این رویکرد پیشرو حقوقی هم‌گرایی دارد. در بیانیهٔ ستاد کل نیروهای مسلح درخصوص تبیین اصول و چهارچوب‌های عملیاتی در فضای سایبری مصوب ۱۳۹۹، به‌صراحت اعلام شده است که حملات سایبری، درصورتی‌که منجر به آسیب انسانی یا تخریب شدید زیرساخت‌های حیاتی کشور شوند، از منظر جمهوری اسلامی ایران، به‌مثابهٔ تجاوز و حملهٔ نظامی تلقی شده و متعاقباً حق پاسخ متقابل و دفاع مشروع را براساس حقوق بین‌الملل، برای کشور ایجاد می‌نماید.

32. Schmitt, *Tallinn Manual 2.0 on the International*, Rule 71 and accompanying commentary.
33. Schmitt, *Tallinn Manual 2.0 on the International*.
34. Delerue, *Cyber Operations and International Law*, 224-226.

این موضع‌گیری رسمی، با گذار از ابزار فیزیکی و تمرکز مستقیم بر اثرات و پیامدهای مخرب، عملاً همان شاخص اثرسنجی راهنمای تالین را به‌عنوان مبنای تصمیم‌گیری برای پاسخ نظامی و سایبری به رسمیت می‌شناسد. این همسویی راهبردی، یک نقطهٔ قوت بسیار مهم محسوب می‌شود، زیرا موجب می‌گردد که اقدام احتمالی نظامی یا سایبری متقابل ایران، در شرایط بحرانی، در قالب دفاع مشروع، بر مبنایی استوار شود که از منظر ادبیات نوین حقوق بین‌الملل، منطقی، متناسب و کاملاً قابل‌دفاع است.

تحلیلگران حقوقی داخلی نیز اخیراً تصریح کرده‌اند که هم‌گرایی دکترین نظامی ایران با ضابطهٔ اثرمحور، ظرفیت حقوقی کشور را برای استناد به دفاع مشروعِ متناسب در برابر تهدیدات نوین زیرساختی، به شکل قابل‌توجهی ارتقا داده است.

۴-۳. دایرهٔ شمول اقدامات متقابل: سازوکار دیپلماتیک در برابر محدودیت‌های ساختاری

سومین و آخرین حوزهٔ تطبیق، بررسی سازوکارهای در دسترس دولت‌ها برای پاسخ به عملیات‌های سایبری متخلفانه‌ای است که به سطح حملهٔ مسلحانه نمی‌رسند؛ عملیات‌هایی که اصطلاحاً در«منطقهٔ خاکستری» رخ می‌دهند، نظیر جاسوسی اقتصادی سایبری، مداخله در انتخابات یا اختلالات موقت اینترنتی. در این بخش، واگرایی عمیقی میان وسعت رویهٔ بین‌المللی و محدودیت‌های ساختار موجود در ایران دیده می‌شود.

دولت‌ها در سطح بین‌المللی، با آگاهی از اینکه استفاده از زور نظامی در برابر حملات سایبری پایین‌تر از سطح حملهٔ مسلحانه ممنوع است، سازوکارهای حقوقی و دیپلماتیک خود را برای پاسخ توسعه داده‌اند. این سازوکارها، براساس مواد طرح کمیسیون حقوق بین‌الملل دربارهٔ مسئولیت دولت‌ها، تابع شرایط دقیقی چون لزوم اخطار قبلی و رعایت اصل تناسب هستند و شامل موارد زیر می‌شوند:

الف) اقدامات متقابل غیرخصمانه شامل رفتارهایی است که فی‌نفسه غیردوستانه هستند، اما نقض حقوق بین‌الملل محسوب نمی‌شوند، مانند اخراج دیپلمات‌های کشور متخاصم، لغو یک‌جانبهٔ معاهدات تجاری دوجانبه، یا اعمال تعرفه‌های گمرکی محدودکننده به‌عنوان یک واکنش سیاسی به حملات سایبری.

ب) اقدامات متقابل که در ذات خود اعمالی غیرقانونی‌اند، مانند مسدود کردن دارایی‌های دولت خارجی یا انجام عملیات سایبری متقابل برای از کار انداختن سرورهای مهاجم، اما

درصورتی‌که منحصراً با هدف وادار کردن دولت متخلف به توقف حمله و جبران خسارت، و با رعایت اصل تناسب انجام شوند، وصف متخلفانهٔ آن‌ها زایل شده و مشروعیت می‌یابند.[۳۵] در سال‌های اخیر، دکترین حقوقی و رویهٔ برخی دولت‌ها به‌سمت پذیرش مفهوم اقدامات متقابل جمعی یا تلافی‌جویانه حرکت کرده است؛ به این معنا که کشورهای ثالث نیز می‌توانند به درخواست دولت قربانی، دست به اقدامات متقابل سایبری علیه دولت متخلف بزنند.[۳۶]

ج) پاسخ‌های جمعی و دیپلماسی قهرآمیز: این رویکرد شامل اقداماتی است که به‌صورت شبکه‌ای، توسط نهادهای بین‌المللی اعمال می‌شود. «جعبه‌ابزار دیپلماسی سایبری اتحادیهٔ اروپا» نمونهٔ بارز این سازوکارها است که در نسخه‌های به‌روزرسانی‌شدهٔ اخیر خود، بر بازدارندگی تحریمی هوشمند تأکید دارد و به کشورهای عضو اجازه می‌دهد تحریم‌های مالی هدفمند، مسدودسازی دارایی‌ها و ممنوعیت سفر را علیه افراد، نهادها و سازمان‌های اطلاعاتی خارجیِ دخیل در حملات سایبری اعمال کنند. در کنار این، دیپلماسی قهرآمیز به‌عنوان ابزاری برای تهدید معتبر، جهت دگرگونی در برآوردهای هزینه و دستاورد دولت مهاجم به کار می‌رود.

در نقطهٔ مقابل، ساختار حقوقی و نهادی ایران فاقد یک ساختار مشخص، مدون و تخصصی برای اعمال اقدامات متقابل غیرنظامیِ دولت‌محور در پاسخ به مداخلات سایبری است. همان‌طور که پیش‌تر تحلیل شد، تمرکز قوانین داخلی نظیر قانون جرایم رایانه‌ای، بر تعقیب قضایی فردی متمرکز است که در مواجهه با سرویس‌های اطلاعاتی متخاصم خارجی یا گروه‌های تحت‌حمایت آن‌ها، ابزاری ذاتاً ناکارآمد و سست است. در نتیجهٔ این خلأ حقوقی، پاسخ به حملات سایبری با شدت کمتر در ایران، عمدتاً از مجاری دیپلماتیک یا حقوقی پیگیری نمی‌شود، بلکه منحصراً در حیطهٔ وظایف و اختیارات نهادهای امنیتی، اطلاعاتی و فنی نظیر سازمان پدافند غیرعامل یا نهادهای نظامی تعریف می‌شود. هرچند اتخاذ رویکرد امنیتی و ارتقای تاب‌آوری فنی برای بازدارندگی و دفع حملات کاملاً ضروری است، اما تکیهٔ صرف بر آن، کشور را از ظرفیت‌های بسیار گستردهٔ دیپلماسی سایبری، و همچنین از بهره‌گیری از ابزارهای نبرد حقوقی برای مشروعیت‌بخشی به پاسخ‌های خود، و نیز از ساختارهای حقوق بین‌الملل و قابلیت اعمال فشارِ هماهنگ بین‌المللی محروم می‌سازد.

35. International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, Yearbook of the International Law Commission, 2001, vol. II (Part Two), UN Doc. A/CN.4/SER.A/2001/Add.1 (Part 2), arts. 22, 49-54.

36. Tsagourias and Farrell, “Cyber Attribution: Technical and Legal,” 941-967.

فقدان اسناد کلان که به‌طور جامع و شفاف، حدود و مرزهای قانونی اعمال اصل تناسب و مبانی حقوقی اقدامات متقابل سایبری را ازسوی ایران مشخص کند، دو پیامد منفی به همراه دارد: نخست، منجر به شکل‌گیری واکنش‌های مقطعی، موردی و فاقد انسجام راهبردی بلندمدت می‌شود؛ و دوم، در عرصهٔ بین‌المللی و در مجامع حقوقی، موضع جمهوری اسلامی ایران را در توجیه اقدامات واکنشی خود تضعیف نموده و امکان اتهام‌زنی‌های متقابل ازسوی کشورهای غربی را تسهیل می‌نماید. تدوین یک ساختار جامع برای استفاده از سازوکارهای حقوق بین‌الملل در اعمال متقابل، نیازی فوری در ساختار امنیت ملی سایبری کشور به شمار می‌رود.

۵. نتیجه‌گیری

فضای سایبر با ماهیت پراکنده، بی‌مرز و پویای خود، چالش‌های بنیادینی را در برابر مفاهیم سنتی حقوق بین‌الملل، به‌ویژه در حوزه‌های انتساب مسئولیت و احراز حدود حملهٔ مسلحانه ایجاد کرده است. همان‌طور که در این پژوهش تبیین شد، دشواری‌ها و شکاف‌های موجود میان انتساب فنی و انتساب حقوقی، دولت‌ها را ناگزیر به بهره‌گیری از سازوکارهای نوینی چون انتساب سیاسی هماهنگ و توسل به اصل صلاحیت حمایتی برای حراست از زیرساخت‌های حیاتی و منافع امنیت ملی خود کرده است.

علاوه‌براین، ناکارآمدی رویکردهای مبتنی‌بر نص قانون در مواجهه با عملیات‌های سایبریِ خفیف‌تر از توسل به زور یا در منطقهٔ خاکستری، ضرورت گذار به ضابطهٔ نتیجه‌محور را بیش از پیش نمایان می‌سازد. ارزیابی تهدیدات پیشرفته و مستمر براساس میزان تخریب و پیامدهای واقعی آن‌ها، به دولت‌ها اجازه می‌دهد تا با استفاده از یک ساختار جامع از اقدامات متقابل حقوقی و دیپلماتیک، پاسخی متناسب به این حملات ارائه دهند. در این راستا، هدف غایی هرگونه اقدام تقابلی، باید موجب اثرگذاری بر دستگاه محاسباتی دولت‌های متخاصم جهت ایجاد بازدارندگی مؤثر باشد. درنهایت، دستیابی به ثبات و امنیت پایدار در عرصهٔ سایبری و جلوگیری از بی کیفرمانی، در گرو همسویی نظری و هم‌گرایی مفهومی میان تابعان حقوق بین‌الملل است. تا زمانی که یک ساختار جهان‌شمول و الزام‌آور سایبری شکل نگیرد، توسعهٔ رویه‌های دولت‌ها برمبنای تفاسیر پیشرو از قواعد موجود، تنها راهکار عملی برای مقابله با بی‌کیفرمانی در فضای سایبر و تضمین مسئولیت‌پذیری بین‌المللی دولت‌ها خواهد بود.

سیاههٔ منابع

الف- منابع فارسی:

ستاد کل نیروهای مسلح جمهوری اسلامی ایران، بیانیه درخصوص حقوق بین‌الملل فضای مجازی، مرداد ۱۳۹۹.

شورای عالی فضای مجازی. *سند راهبردی جمهوری اسلامی ایران در فضای مجازی*. شماره ثبت ۱۰۳۵۵۴. تهران: مرکز ملی فضای مجازی، ۱۴۰۱.

ضیایی بیگدلی، محمد رضا. حقوق بین الملل بشر دوستانه. چاپ ششم، تهران: انتشارات گنج دانش، ۱٤۰۱.

قانون مجازات اسلامی، مصوب ۱۳۹۲.

کمیسیون حقوق بین‌الملل سازمان ملل متحد. *مسئولیت بین المللی دولت؛ متن و شرح مواد کمیسیون حقوق بین الملل*. ترجمه علیرضا ابراهیم گل. تهران: شهر دانش، ۱۳۹۸.

موسی زاده، رضا، و احمدرضا آذرپندار. *حقوق بین الملل بشردوستانه* و فناوری‌های نوین. تهران: میزان، ۱٤۰۳.

ب- منابع لاتین:

Buchan, Russell, and Nicholas Tsagourias (eds.). *Research Handbook on International Law and Cyberspace*. Cheltenham: Edward Elgar Publishing, 2021.

Charter of the United Nations, 1945.

Delerue, François. *Cyber Operations and International Law*. Cambridge: Cambridge University Press, 2020.

Delerue, François. *Cyber Operations, Sub-threshold Threats, and International Law*. Cambridge: Cambridge University Press, 2024.

Egloff, Florian J., and Myriam Dunn Cavelty. "Attribution and Knowledge Creation Assemblages in Cybersecurity Politics." *Journal of Cybersecurity* 7, no. 1 (2021). 10.1093/cybsec/tyab002

Giles, Keir, and Andrew Monaghan. *Legality in Cyberspace: An Adversary View*. Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press, 2014.

Green, James A. *Cyber Warfare: A Multidisciplinary Analysis*. London: Routledge, 2015.

International Law Commission. Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, Yearbook of the International Law Commission, 2001.

Mačák, Kubo. “Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors.” *Journal of Conflict and Security Law* 21, no. 3 (2016): 405-428.

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, I.C.J. Reports 1986. https://www.icj-cij.org/case/70

Moret, Erica, and Patryk Pawlak. *The EU Cyber Diplomacy Toolbox: Towards a Cyber Sanctions Regime?* Brief No. 24. Paris: European Union Institute for Security Studies (EUISS), 2017. DOI 10.2815/399444

Prosecutor v. Duško Tadić, Case No. IT-94-1-A, Judgment (Appeals Chamber), International Criminal Tribunal for the Former Yugoslavia, 15 July 1999. https://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf

Schmitt, Michael N. (ed.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.

Schmitt, Michael N. “Big Data: International Law Issues Below the Armed Conflict Threshold,” In *Big Data and Armed Conflict: Legal Issues Above and Below the Armed Conflict Threshold*. edited by Laura A. Dickinson and Edward W. Berg, 29-54. Oxford: Oxford University Press, 2024. https://doi.org/10.1093/oso/9780197668610.003.0003

Schmitt, Michael N., and Anusha S. Pakkam. “Cyberspace and the Jus ad Bellum: The State of Play.” *International Law Studies* 103 (2024): 194-229.

Schmitt, Michael N., and Liis Vihul. “Sovereignty in Cyberspace: Lex Lata Vel Non?” *American Journal of International Law* 111, no. 4 (2017): 213-218.

Tsagourias, Nicholas, and Michael Farrell. “Cyber Attribution: Technical and Legal Approaches and Challenges.” *European Journal of International Law* 31, no. 3 (2020): 941-967. https://doi.org/10.1093/ejil/chaa057

United Nations General Assembly. 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, 2015.

United Nations General Assembly. Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/75/816, 18 March 2021.

Yar, Majid, and Kevin F. Steinmetz. *Cybercrime and Society*. 3rd edition, London: Sage Publications, 2019.