آستانه توسل به زور سایبری در جنایات جنگی ناشی از رایاجنگ

مهدی حسینی (نویسنده مسئول)

دکترای حقوق کیفری و جرم‌شناسی، دانشکده حقوق، دانشگاه شهید بهشتی، تهران، ایران.

hosseini.mhdi@gmail.com

امیرحسین کرمی خلیل‌آبادی

کارشناسی ارشد حقوق کیفری و جرم‌شناسی، دانشکده حقوق، دانشگاه شهید بهشتی، تهران، ایران.

amirhosseinkarami110@gmail.com

قابل انتشار در دوره ۲۶ شماره ۶۹ (بهار ۱۴۰۶) نشریه پژوهشهای حقوقی

چکیده

تهدید ناشی از رشد روزافزون رایاجنگ‌های بین‌المللی برای صلح و امنیت بین‌الملل، وضع محدودیت‌های حقوق جنگ بر آن‌ها را ناگزیر ساخته است. یکی از ضمانت اجراهای ناشی از نقض مقررات مربوط به حقوق جنگ، جرم‌انگاری بین‌المللی آن‌ها تحت عنوان جنایت جنگی است. این در حالی است که احراز عناصر جنایات جنگی در رایاجنگ‌های مدرن، با ابهام‌هایی مواجه است. برای این منظور، احراز عنصر زمینه‌ای لازم برای ارتکاب جنایت جنگی، یعنی وقوع توسل به زورِ موجدِ وضعیت مخاصمه در رایاجنگ‌ها، ضروری است. بر این اساس، پرسش اصلی این پژوهش آن است که آستانهٔ تحقق توسل به زور سایبری چگونه است؟ برای پاسخ به این سؤال، در این نوشتار با استفاده از روش توصیفی-تحلیلی و با گردآوری داده‌ها از طریق منابع کتاب‌خانه‌ای، اولاً دو گونهٔ تخریب‌گر و مختل‌کننده از حملات سایبری بازشناسی شده، ثانیاً، رویکرد غالب در خصوص تأکید بر ضرورت ایجاد آثار فیزیکیِ صرف برای تحقق توسل به زور سایبری مورد تحلیل انتقادی قرار می‌گیرد و نهایتاً، ضمن پیشنهاد آستانهٔ شدت مشخص برای وقوع توسل به زور سایبری در هر یک از گونه‌های آن، با استناد به مواد اساسنامهٔ رم، ضرورت اتخاذ تفسیر پویا از سوی دیوان کیفری بین‌المللی برای شمول بر همهٔ گونه‌های رایاجنگ، تبیین می‌شود.

کلیدواژگان: توسل به زور سایبری، جنایت جنگی سایبری، رایاجنگ، آستانهٔ شدت، سند مقررات تالین.

درآمد

در دو دهۀ گذشته، تعداد قابل توجهی از رایاجنگ‌ها[۱] در اَشکال مختلف واقع شده است. این حملات تا آن‌جا پیش رفته که در سال ۲۰۲۳، خود دیوان کیفری بین‌المللی را نیز مورد تهاجم واقع ساخته است[۲]. همسو با تعداد فزایندۀ رایاجنگ‌ها، برخی از کارشناسان نظامی و استراتژیست‌ها تا آن‌جا پیش می‌روند که فضای سایبر را به‌عنوان «پنجمین حوزه» برای عملیات نظامی، پس از زمین، دریا، هوا و فضا، توصیف می‌کنند[۳]. افزایش روزافزونِ رایاجنگ‌ها، نگرانی دولت‌ها و سازمان‌های بین‌المللی را برای تنظیم‌گریِ حملات مذکور شدت بخشیده است و با عنایت به دشواری در خلقِ سازوکارهای بین‌المللی نو در مقابله با حملات مذکور، در پهنۀ حقوق کیفری، در ساختارهای موجود نزد دیوان کیفری بین‌المللی که یکی از آن‌ها جنایت جنگی است، دنبال می‌شود[٤].

جنایت جنگی، وفق حقوق بین‌الملل، نقض شدید مقررات و عرف‌های جنگ است که در مخاصمات مسلحانه صورت می‌گیرد[٥]. مطابق با مادۀ ۸۴ سند مقررات تالین[٦]، اقدامات ارتکابی به‌وسیلۀ ابزارهای سایبری می‌توانند جنایات جنگی به‌شمار آیند و در نتیجه، موجب بروز مسئولیت کیفری فردی در معنای حد فاصل فعل مجرمانه و تحمیل واکنش جامعه[۷] در سطح بین‌المللی شوند[۸]؛ زیرا حقوق مخاصمات مسلحانه بر ابزارها و روش‌های نوین جنگی که در زمان پدیدار شدن قاعده‌ای از حقوق عرفی منظور نشده‌اند، اعمال می‌گردد[۹]. هرچند، تغییرات عمده در شیوه‌های جنگیدن ناشی از فناوری‌های نوین که برخی مانند فضای سایبر در حال حاضر

---

[۱]. «رایاجنگ» واژۀ مصوب فرهنگستان زبان و ادبیات فارسی برای عبارت «جنگ سایبری» است.

[2]. "Measures taken following the unprecedented cyber-attack on the ICC", international criminal court, accessed May 2, 2024, https://www.icc-cpi.int/news/measures-taken-following-unprecedented-cyber-attack-icc.

[۳]. مجید عباسی و حسین مرادی، «جنگ سایبر از منظر حقوق بین‌الملل بشردوستانه»، مجلس و راهبرد، ۸۱، (۱۳۹۴): ۳۹.

[٤]. علیرضا محقق هرچقان و دیگران، «حقوق بین‌الملل سایبری و توسعۀ صلاحیت دیوان کیفری بین‌المللی (با تأکید بر مذاکرات تالین ۲۰۱۷ میلادی)»، فصلنامۀ مطالعات حقوق عمومی، ۵۳، ۳ (۱۴۰۲): ۱۵۵۵.

[٥]. هیبت‌الله نژندی‌منش، حقوق بین‌الملل کیفری در رویۀ قضایی (تهران: خرسندی، ۱۳۹۴)، ۲۳۱.

[٦]. سند مقررات تالین به بررسی حقوق حاکم بر جنگ‌های سایبری پرداخته و به‌طور کلی، دربرگیرندۀ حقوق بر جنگ (حقوق بین‌الملل حاکم بر توسل به زور از سوی کشورها به‌عنوان ابزار سیاست ملی) و حقوق در جنگ (حقوق بین‌الملل تنظیم‌کنندۀ رفتار در مخاصمات مسلحانه که به‌عنوان حقوق مخاصمات مسلحانه یا حقوق بشردوستانۀ بین‌المللی نیز شناخته می‌شود) است. این سند که توسط متخصصین و محققان حقوق بین‌الملل طرح‌ریزی شد، در دو دو نسخه و در سال‌های ۲۰۱۳ و ۲۰۱۷ تدوین شد و به دنبال تسری هنجارهای حقوقی و قانونی موجود به جنگ‌های نوین است. سند نخست به حقوق بین‌الملل مربوط به جنگ سایبری می‌پردازد. نسخۀ دوم سند در سال ۲۰۱۷ که توسط گروهی متنوع‌تر از کارشناسان تشکیل شد[٦]، به عملیات سایبری به‌طور گسترده‌تر، هم در حین و هم در خارج از مخاصمات مسلحانه می‌پردازد و برای گنجاندن حقوق بین‌الملل حاکم بر فعالیت‌های سایبری در زمان صلح به‌روزرسانی شده است.

[۷]. علیرضا محقق هرچقان، مسئولیت کیفری از منظر جرم‌شناسی (تهران: دادگستر، ۱۳۹۰)، ۳۱۹.

[۸]. علیرضا محقق هرچقان، محمدعلی اردبیلی و ابراهیم بیگ‌زاده، «صلاحیت دیوان کیفری بین‌المللی و رسیدگی به جنایات بین‌المللی سایبری در عرصه‌های انسانی حقوق بین‌الملل»، پژوهشهای حقوق جزا و جرم‌شناسی، ۱۱، ۲۱ (۱۴۰۲): ۳۲۱.

[۹]. همان، ۳۱۶.

به‌کار می‌روند و برخی دیگر مانند نانوفناوری و فناوری فضایی در حال توسعه هستند[۱۰]، انعطاف گسترده را ضروری می‌نماید[۱۱] و موجب طرح مناقشات بسیار میان حقوق‌دانان بین‌المللی شده است[۱۲].

هرچند تا سال ۲۰۲۳، هیچ موقعیت مربوط به رایاجنگ‌ها مورد تجزیه و تحلیل دادستان کیفری بین‌المللی قرار نگرفته بود؛ وانگهی در سال ۲۰۲۳، دادستان دیوان کیفری بین‌المللی در یک اظهارنظر مهم مکتوب، صراحتاً اعلام نمود که یک رایاجنگ ممکن است به‌طور بالقوه عناصر بسیاری از جنایات بین‌المللی، همچون جنایات جنگی، را برآورده کند؛ هرچند هیچ ماده‌ای از اساسنامهٔ رم مشخصاً به حملات سایبری اختصاص ندارد[۱۳]. دفتر دادستانی دیوان نیز آن را به‌عنوان موضع رسمی و کنونی دیوان کیفری بین‌المللی تأیید نمود[۱۴]. طی برگزاری «همایش رسیدگی به جرایم سایبری در چارچوب اساسنامهٔ رم» که با مشارکت فعال شرکت مایکروسافت در آغاز سال ۲۰۲۴ برگزار شد، دادستان دیوان مجدداً بر نکتهٔ خود در خصوص قابلیت تعقیب حملات سایبری به‌عنوان جنایت جنگی در چارچوب اساسنامهٔ رم سخن گفت[۱۵]. در پرتو این راهبرد، تطبیق عناصر عمومی و اختصاصی «جنایات جنگی» بر «رایاجنگ‌ها» ضرورت می‌یابد؛ لکن پیش از عناصری که به‌طور خاص به جنایات جنگی ارتکاب‌یافته مربوط می‌شود و طرح مباحث مربوط به حقوق بشردوستانهٔ بین‌المللی و حقوق در جنگ را ضروری می‌نماید، دادستان مکلف است وجود یک عنصر زمینه‌ای برای ارتکاب جنایت را نیز ثابت کند؛ زیرا سند عناصر جنایات مذکور در اساسنامهٔ رم[۱۶] در خصوص مادهٔ ۸ اساسنامهٔ رم مقرر می‌دارد که «جنایت جنگی ضرورتاً در چارچوب و با مشارکت در یک مخاصمهٔ مسلحانه انجام می‌شود». این الزام زمینه‌ای موجب می‌شود که برای جنایت جنگی دانستنِ یک رایاجنگ، لازم باشد که عملیات سایبری ضرورتاً از رهگذرِ وقوع توسل به زور سایبری انجام شود. بر همین اساس است که گفته شده است برای اعمال حقوق توسل به زور بر فعالیت سایبری، باید میان آن فعالیت و وضعیت مخاصمه، گونه‌ای پیوند وجود داشته باشد[۱۷].

در این پژوهش تلاش می‌شود تا به‌منظور بررسی امکان وقوع توسل به زور سایبری، به‌عنوان مهم‌ترین عنصر عمومی و زمینه‌ای برای وقوع جنایات جنگی سایبری، به این سؤال پاسخ داده شود که «آستانهٔ توسل به زور سایبری» چگونه است؟ ضمن تأکید بر افتراق کامل موضوع پژوهش حاضر در خصوص «آستانهٔ شدت وصول به توسل به زور سایبری» از موضوع پژوهش‌های سابق مبنی

---

[۱۰]. حسین شریفی طرازکوهی و جعفر برمکی، «چالش‌های حقوقی قابلیت‌های فضای سایبری در پرتو مادهٔ ۳۶ پروتکل یکم الحاقی ۱۹۷۷»، مجلهٔ حقوقی بین‌المللی، ۳۷، ۶۲ (۱۳۹۹): ۱۲۱.

[۱۱]. حسین شریفی طرازکوهی، حقوق بشردوستانهٔ بین‌المللی (تهران: میزان، ۱۳۹۵): ۱۹۲.

[۱۲]. مونا خلیل‌زاده، مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری (تهران: مجمع علمی و فرهنگی مجد، ۱۳۹۳)، ۶۰.

[13]. Karim A.A. Khan, "Technology Will Not Exceed Our Humanity", August 20, 2023, https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity/ (accessed May 2, 2024).

[14]. Andy Greenberg, "The International Criminal Court Will Now Prosecute Cyberwar Crimes". Wired, September 7, 2023, accessed May 2, 2024, https://www.wired.com/story/icc-cyberwar-crimes/.

[15]. "Statement by ICC Prosecutor Karim A.A. Khan KC on conference addressing cyber-enabled crimes through the Rome Statute system", international criminal court, accessed May 2, 2024, https://www.icc-cpi.int/news/statement-icc-prosecutor-karim-aa-khan-kc-conference-addressing-cyber-enabled-crimes-through.

[16]. Preparatory Commission for the International Criminal Court, Report of the Preparatory Commission for the International Criminal Court, Addendum, add. Part II Finalized draft text of the Elements of Crimes, 2000, U.N. Doc. PCNIC/2000/1/Add.2, at 18.

[۱۷]. علیرضا محقق هرچقان، محمدعلی اردبیلی و ابراهیم بیگ‌زاده، پیشین، ۳۱۱.

بر «آستانهٔ شدت رسیدگی دیوان کیفری بین‌المللی» که موضوع پژوهش برخی از صاحب‌نظران قرار گرفته است[۱۸]، برای پاسخ به سؤال پژوهش، ضمن شناسایی گونه‌های مختلف حملات سایبری، یعنی حملات تخریب‌گر و مختل‌کننده، به تحلیل آستانهٔ توسل به زور در هر یک از گونه‌های مذکور پرداخته می‌شود و با ارائهٔ تحلیل انتقادی از رویکرد مبتنی بر آثارِ فیزیکیِ صرف، اتخاذ رویکردی پویا از سوی دیوان کیفری بین‌المللی برای آستانهٔ شدت توسل به زور سایبری، پیشنهاد می‌شود.

حسب رأی دادگاه کیفری بین‌المللی برای یوگسلاوی سابق در قضیهٔ تادیچ[۱۹] که معمولاً برای تعریف مخاصمهٔ مسلحانهٔ بین‌المللی به آن استناد می‌شود، «مخاصمهٔ مسلحانه زمانی وجود دارد که بین دولت‌ها (در موارد بین‌المللی) توسل به زور مسلحانه وجود داشته باشد...»[۲۰]. با توجه به این‌که تا کنون، هیچ عملیات سایبری رسماً و به‌صورت عمومی و فراگیر، به‌عنوان توسل به زور شناخته نشده است و با عنایت به این‌که هیچ اجماع بین‌المللی در خصوص چگونگی تعریف و ارزیابی توسل به زور سایبری وجود ندارد، بحث‌های این پژوهش نظری و مبتنی بر رویهٔ فعلی حقوق بین‌الملل در خصوص عملیات‌های سایبری است.

۱. وجود آستانه برای تحقق توسل به زور

معیار شکل‌گیری وضعیت مخاصمهٔ مسلحانه را در وقوعِ توسل به زور دانسته‌اند؛ وانگهی نه دادگاه بین‌المللی دادگستری و نه منشور سازمان ملل متحد، آستانهٔ شدت را برای «زور» ممنوع‌شده در بند ۴ مادهٔ ۲ منشور ملل متحد، مشخص نکرده‌اند. آستانهٔ شدتی که تا آن میزان توسل به زور با ممنوعیت مندرج در بند ۴ مادهٔ ۲ مغایرت ندارد، توسط محققینی استنباط شده است که رویهٔ دولت‌ها را از زمان تصویب منشور سازمان ملل متحد، تجزیه و تحلیل کرده‌اند[۲۱]. وجود چنین آستانه‌ای از چندین پرونده استنباط شده است که در آن‌ها توسل به زور با شدت کم به‌عنوان توسل به زور توسط دولت‌ها شناخته نشده است. مثلاً در پروندهٔ تنگهٔ کورفو، دیوان مقرر نمود که مداخلهٔ کشتی‌های جنگی بریتانیا در آب‌های آلبانی نقض حاکمیت آلبانی است؛ اما آن را نقض ممنوعیت توسل به زور یا تهدید به آن توصیف نکرد[۲۲]. برخی از محققان این رویکرد را به‌عنوان استدلالی برای حمایت از وجود آستانهٔ شدت تحلیل می‌کنند[۲۳]. این مجادلهٔ نظری توسط کمیسیون حقیقت‌یاب بین‌المللی در خصوص جنگ علیه گرجستان نیز مطرح شد که بیان کرد: «ممنوعیت

---

[۱۸]. محمدهادی ذاکرحسین، آیین پیش‌دادرسی دیوان کیفری بین‌المللی، دفتر نخست: فرایند گزینشگری قضایا (تهران: شهر دانش، ۱۳۹۹): ۱۹۱؛ محمود صابر و آزاده صادقی، «بررسی معیار آستانهٔ شدت برای تعقیب جنایات در دیوان کیفری بین‌المللی؛ با نگاهی بر دیگر دادگاه‌های بین‌المللی»، مطالعات حقوق تطبیقی، ۶، ۲ (۱۳۹۴): ۶۳۷-۶۳۳؛ علیرضا محقق هرچقان و دیگران، پیشین، ۱۵۴۷.

[19]. Tadic´.

[20]. Prosecutor v. Tadić, Case No. IT-۱-۹۴-I, Decision on the Defense Motion for Interlocutory Appeal on Jurisdiction, Int'l. Crim. Trib. for the Former Yugoslavia, 2 Octoer ۱۹۹۵, p. ۷۰.

21. Olivier Corten, The Law against War - The Prohibition on the Use of Force in Contemporary International Law (Oxford: Hart Publishing, 2012), 52-92.

22. Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania), ICJ Reports 4, 1949, p. 35.

23. Mary Ellen O'Connell, "The Prohibition of the Use of Force" in Research Handbook on International Conflict and Security Law: Jus ad Bellum, Jus in Bello and Jus post Bellum, Edited by Christian Henderson and Nigel White (London: Edward Elgar Publishing, 2013), 102-105.

توسل به زور شامل تمامی زور مادی که از حداقل آستانهٔ شدت فراتر می‌رود، می‌شود»[۲۴]. در مقابل، برخی دیگر از محققان[۲۵] ادعا می‌کنند که چنین آستانه‌ای وجود ندارد و مستثنی شدن «توسل‌های حداقلی به زور» از محدودهٔ بند ۴ مادهٔ ۲ را رد می‌کنند.

اگر هر قضیه جداگانه در نظر گرفته شود، ممکن است تعیین وجود آستانهٔ شدت دشوار باشد؛ وانگهی اگر همهٔ قضایا و پرونده‌ها با هم در نظر گرفته شوند، ممکن است مبانی کافی را برای تعیین آستانهٔ شدت فراهم کنند. نمونه‌های قانع‌کننده‌تر از وجود آستانهٔ شدت را می‌توان خارج از رویهٔ قضائی دیوان بین‌المللی دادگستری و آن‌گونه که برخی از محققان[۲۶] برای دفاع از وجودِ چنین آستانه‌ای از شدت به آن اشاره کرده‌اند، یافت.

۲. آستانهٔ شدت توسل به زور سایبری

به نظر می‌رسد که در مفهوم ممنوعیت توسل به زور، ضرورتی وجود ندارد که تسلیحات مورد استفاده لزوماً دارای آثار انفجاری بوده یا برای اهداف تهاجمی ساخته شده باشد[۲۷]. اظهارنظر دیوان بین‌المللی دادگستری در قضیهٔ اختلافات ناوبری و حقوق مرتبط کاستاریکا علیه نیکاراگوئه در سال ۲۰۰۹ میلادی، این رویکرد را تأیید می‌نماید که به عبارات مندرج در معاهدات قدیمی، می‌توان معنای امروزین بخشید[۲۸]. بر این اساس و این‌که عملیات‌های سایبری ارتکاب‌یافته در چارچوب رایاجنگ‌ها می‌توانند به‌مثابهٔ سلاح‌های سایبری تلقی شوند[۲۹]، باعث نیاز به بررسی ماهیت این‌گونه حملات در قالب قواعد موجودِ حقوق توسل به زور، حقوق بشردوستانهٔ بین‌المللی[۳۰] و حقوق کیفری بین‌المللی شده است.

عملیات‌های سایبری بسیار ناهمگن و با مقیاس متفاوت هستند و اثرات مختلفی، از جمله تخریب داده‌ها، ایراد خسارت و از دست دادن جان افراد، را ایجاد می‌کنند. عملیات‌های سایبری به‌صورت بالقوه و به‌تنهایی، توانایی عبور از آستانهٔ توسل به زور را دارا هستند[۳۱]. توسل به آستانهٔ شدت، تمایز بین اَشکال مختلف عملیات سایبری و شناسایی ناقضان ممنوعیت توسل به زور را ممکن می‌سازد. در خصوص راه تعیین آستانهٔ شدت توسل به زور در رایاجنگ‌ها، نظریات مختلفی مطرح شده است؛ اما اجماعی در این خصوص حاصل نشده است. در ادبیات نظری مشهور، سه رویکرد اصلی را می‌توان در این راستا شناسایی نمود: رویکرد مبتنی بر

---

24. Max Planck Institute for Comparative Public Law and International Law, "Report of the International Fact-Finding Commission on the Conflict in Georgia", vol II, 2009: 242, available in: www.ceiig.ch/Report.html (accessed May 2, 2024).

۲۵. به‌عنوان مثال، تحلیل‌های تفصیلی مذکور در منبع ذیل، شایان توجه است:

Tom Ruys "The Meaning of "Force" and the Boundaries of the Jus Ad Bellum: Are "Minimal" Uses of Force Excluded from UN Charter Article 2(4)?", American Journal of International Law 108, 2 (2014): 159-210.

26. Olivier Corten, The Law against War - The Prohibition on the Use of Force in Contemporary International Law (Oxford: Hart Publishing, 2012), 52-92; O'Connell, op. cit., 102-107.

۲۷. علی فقیه حبیبی، «جنگ مدرن و تخاصمات سایبری در چارچوب فضای بین‌الملل»، جستارهای سیاسی معاصر، ۷، ۱۹ (۱۳۹۵): ۱۲۸.

۲۸. همایون حبیبی و وحید بذار، «حملات سایبری و ممنوعیت توسل به زور»، تعالی حقوق، ۳، ۲ (۱۳۹۶): ۱۶۰.

۲۹. حسین شریفی طرازکوهی و جعفر برمکی، پیشین، ۱۳۶-۱۳۲.

۳۰. پرستو اسمعیل‌زاده ملاباشی، «حملهٔ سایبری به‌مثابهٔ جنایت تجاوز و بررسی صلاحیت دیوان کیفری بین‌المللی در رسیدگی به آن»، پژوهش‌های حقوق جزا و جرم‌شناسی، ۱۰ (۱۳۹۶): ۴۴.

۳۱. علیرضا محقق هرچقان، محمدعلی اردبیلی و ابراهیم بیگ‌زاده، پیشین، ۳۱۲.

هدف، رویکرد مبتنی بر ابزار یا روش و رویکرد مبتنی بر پیامد یا اثر[۳۲]. رویکردهای سه‌گانهٔ مذکور مبتنی بر هنجارهای معاهداتی و چارچوب‌های قانونی فعلی هستند که منع توسل به زور را مقرر می‌نمایند. روشی دیگر که تحت آموزه‌های نظری حقوق بین‌الملل پیشنهاد شده، این است که اگر اختلال ایجادشده در نتیجهٔ عملیات سایبری به‌اندازهٔ کافی مهم باشد و امنیت دولت را تحت تأثیر قرار دهد، عملیات سایبری ایجادکنندهٔ اختلال نیز تحت شمول بند ۴ مادهٔ ۲ منشور ملل متحد قرار خواهد گرفت[۳۳].

یک روش خلاقانه در سال ۲۰۲۱، توسط محققان پروژهٔ آکسفورد در خصوص حمایت‌های حقوق بین‌الملل در فضای سایبر پیشنهاد شد[۳۴]. آن‌ها پیشنهاد می‌کنند که تمرکز صرفاً بر روی تأثیرات عملیات سایبری، این احتمال را نادیده می‌گیرد که حتی عملیات سایبری فاقد تأثیرات خاص نیز ممکن است با ایجاد تهدید به توسل به زور، بند ۴ مادهٔ ۲ را نقض کند[۳۵] و این همان رویکردی است که در ادامهٔ این پژوهش، در خصوص رایاجنگ‌های مختل‌کننده، در خصوص آن بحث می‌شود و از شیوهٔ سند مقررات تالین تبعیت نمی‌نماید.

روش دیگر مربوط به سند مقررات تالین است. قاعدهٔ ۱۱ نسخهٔ نخست و قاعدهٔ ۶۸ از نسخهٔ دوم سند مقررات تالین اشاره می‌کند که تحت برخی شرایط، فعالیت‌های سایبری ممکن است بند ۴ مادهٔ ۲ را نقض کنند؛ اما هرگز ادعا نمی‌کند که قانون بدون ابهامی در این خصوص وجود دارد[۳۶]. در عوض، سند مقررات تالین یک آزمایش پیچیدهٔ هشت قسمتی را برای تعیین این‌که آیا یک عملیات سایبری خاص توسل به زور محسوب می‌شود یا خیر، پیشنهاد می‌کند که برخی از پژوهشگران آن‌ها را به «ضوابط و معیارهای تعیینی نظری در شدت آستانه» دانسته‌اند[۳۷]. این آزمونِ دشوار شامل ارزیابی موارد ذیل است: شدت[۳۸]، فوریت[۳۹]، مستقیم بودن[۴۰]، تهاجمی بودن

---

32. Kai Ambos, "International Criminal Responsibility in Cyberspace" in Research Handbook on International Law and Cyberspace, edited by Nicholas Tsagourias & Russell Buchan (Cheltenham: Edward Elgar, 2015), 122.

33. Marco Roscini, Cyber Operations and the Use of Force in International Law (Oxford: Oxford University Press, 2014), 55.

34. Dapo Akande and Duncan Hollis, "The Oxford Process on International Law Protections in Cyberspace", Oxford Institute for Ethics, Law and Armed Conflict (2020). available in: https://www.elac.ox.ac.uk/the-oxford-process/.

پروژهٔ آکسفورد که توسط محققان معتبر حقوق بین‌الملل، یعنی Dapo Akande و Duncan Hollis، برگزار شده بود، توسط مؤسسهٔ اخلاق، حقوق و مخاصمات مسلحانهٔ آکسفورد، دولت ژاپن و شرکت مایکروسافت حمایت می‌شد. بدان‌سبب که اکثر قریب به اتفاق زیرساخت‌های سایبری متعلق به شرکت‌های خصوصی است، مشارکت بخش خصوصی برای تضمین موفقیت در ایجاد یک چارچوب هنجاری، ضروری است و این یک چالش منحصر به فرد دیگر در اعمال مقررات حقوق بین‌الملل در فضای سایبر است.

35. Duncan B. Hollis & Tsvetelina van Benthem, "What Would Happen If States Started Looking at Cyber Operations as a "Threat" to Use Force?", LAWFARE, March 30, 2021, accessed May 2, 2024, https://www.lawfaremedia.org/article/what-would-happen-if-states-started-looking-cyber-operations-threat-use-force.

36. Michael N. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare, (Cambridge: Cambridge University Press, 2013), 47–52; Michael N Schmitt and Liis Vihul, eds., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd edn (Cambridge: Cambridge University Press, 2017) 333–337.

۳۷. علیرضا محقق هرچقان و دیگران، «اثربخشی دستورالعمل تالین ۲۰۱۷ میلادی بر صلاحیت دیوان کیفری بین‌المللی در ایجاد صلح و امنیت سایبری بین‌المللی»، آموزه‌های حقوق کیفری، ۱۹، ۲۳ (۱۴۰۱): ۲۸۹-۲۸۷.

۳۸. این معیار بر پیامدها تمرکز دارد و درجهٔ خسارت یا آسیب را ارزیابی می‌کند. شدیدترین عملیات‌های سایبری - یعنی آن‌هایی که منجر به خسارت، تخریب، جراحت یا مرگ می‌شوند - به احتمال زیاد به‌مثابهٔ توسل به زور، واجد شرایط هستند.

۳۹. مدت زمان بین عملیات سایبری و وقوع پیامدهای آن. آن دسته از عملیات‌هایی که فوری‌ترین پیامدها را دارند، به احتمال زیاد به‌عنوان توسل به زور واجد شرایط هستند.

۴۰. این معیار ارتباط علی بین عملیات سایبری و خسارت یا آسیب را ارزیابی می‌کند و اگر رابطهٔ علت و معلولی روشن باشد، امکان ارزیابی به‌عنوان توسل به زور را آسان‌تر می‌کند.

(مداخله‌آمیز بودن)[۴۱]، قابل اندازه‌گیری بودن اثرات[۴۲]، ماهیت نظامی داشتن[۴۳]، سطح مشارکت دولت[۴۴] و مشروعیت احتمالی[۴۵]. فارغ از هفت معیار دیگر که توسط برخی از پژوهشگران مورد بررسی تفصیلی قرار گرفته‌اند [۴۶]، معیار «آستانهٔ شدت» مقبولیت بیشتری در ادبیات رایج حقوق بین‌الملل یافته و چنین گفته شده است که «با در نظر گرفتن این‌که معیارهایی که برای تشخیص توسل به زور سایبری ارائه شده‌اند، قابل اعتماد به‌نظر نمی‌رسند، تنها معیاری که باقی می‌ماند، آستانهٔ شدت است»[۴۷]. معیار «شدت» مطرح‌شده در سند مقررات تالین، اساساً مبتنی بر مقایسهٔ میان پیامدهای عملیات سایبری و پیامدهای مرتبط با توسل به زور است. از این منظر، قاعدهٔ ۶۹ نسخهٔ دوم سند مقررات تالین بیان می‌کند که «با توجه به قاعدهٔ عدم اعتبار آثار قابل اغماض، اَعمال دارای پیامدهایی شامل آسیب فیزیکی به اشخاص حقیقی یا اموال، به‌عنوان توسل به زور تلقی می‌شوند». بنابراین، در رویکرد سند مقررات تالین، عملیات‌های سایبری ایجادگرِ آثار فیزیکی را می‌توان به‌عنوان توسل به زور محسوب نمود.

این تمرکز بر آثار فیزیکی در ارزیابی تحقق «توسل به زور»، در نتیجه‌گیری سند مقررات تالین در خصوص توسل به زور در فضای سایبر، منعکس شده است. تفسیر قاعدهٔ ۶۹ سند مذکور اشاره می‌کند که فعالیت سایبری می‌تواند به توسل به زور تبدیل شود، «زمانی که مقیاس و اثرات آن با عملیات غیرسایبری که به سطح توسل به زور می‌رسد، قابل مقایسه باشد»[۴۸]. این سند فهرستی را از عوامل متعدد که ممکن است به این ارزیابی مرتبط باشند، ارائه می‌کند که شرح آن‌ها گذشت[۴۹]. کارشناسان، شدت را به‌عنوان اولین نیاز، «مهمترین عامل در تجزیه و تحلیل» می‌دانند[۵۰]. تفسیر موجود در خصوص این عامل تأکید زیادی بر حملات سایبری‌ای دارد که منجر به آسیب فیزیکی به افراد یا اشیا می‌شوند و اشاره می‌کند که «پیامدهایی شامل خسارت فیزیکی به افراد یا اموال» از آستانهٔ شدت عبور می‌کنند[۵۱].

---

۴۱. این معیار میزان نفوذ یا نقض حاکمیت کشور مورد هدف را ارزیابی می‌کند. هرچه عملیات سایبری تهاجمی‌تر باشد، امکان شناسایی عملیات به‌عنوان توسل به زور آسان‌تر است.

۴۲. درجهٔ سهولت لازم برای شناسایی پیامدها است. هر چقدر که اثرات عملیات سایبری قابل پیش‌بینی و شناسایی باشد، امکان شناسایی به‌عنوان توسل به زور آسان‌تر است.

۴۳. این معیار از پیوند بین عملیات سایبری و عملیات نظامی استفاده می‌کند تا احتمال توصیف به‌عنوان توسل به زور را افزایش دهد.

۴۴. این معیار پیوند بین یک دولت و عملیات سایبری را ارزیابی می‌کند. یک دولت می‌تواند به‌تنهایی یا از طریق کنشگران دیگر، درگیر عملیات شود. هرچه که این پیوند نزدیک‌تر باشد، صلاحیت ارزیابی به‌عنوان توسل به زور بیشتر است.

۴۵. این معیار به‌دنبال ارزیابی این است که آیا یک عملیات سایبری می‌تواند به دسته‌های دیگری از اقدامات حقوق بین‌الملل تعلق داشته باشد که آن را مشروع سازد یا خیر. به‌عنوان مثال، اجبار اقتصادی و سیاسی ظاهراً نقض ممنوعیت توسل به زور نیست.

۴۶. برای ملاحظهٔ تحلیل و بررسی تفصیلی شاخص‌های مذکور، قابل ملاحظه است:

Jason Barkham "Information Warfare and International Law on the Use of Force", New York University Journal of International Law and Politics 34, (2001): 85–86; Matthew Hoisington "Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense", International & Comparative Law Review 32, (2009): 452.

47. Daniel B Silver "Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter", International Law Studies 76, (2002): 89-92.

48. Michael N Schmitt and Liis Vihul, eds., op. cit., 330.

49. Ibid., 334-336.

50. Ibid., 334.

51. Ibid..

۲/۱. تحقق توسل به زور از ره‌گذرِ حملات سایبری تخریب‌گر

در موقعیت‌هایی که ابزارها و روش‌های سایبری جنگ برای دستیابی به نتیجهٔ فیزیکی مشابه یک حملهٔ نظامی واقعی، استفاده شوند[۵۲]، احتمالاً در خصوص وصول به آستانهٔ شدت توسل به زور و ایجاد وضعیت مخاصمه برای وقوع جنایت جنگی، اختلاف کمی وجود داشته باشد[۵۳]؛ زیرا بر اساس نظر اکثر مفسران، حملات سایبری که منجر به این‌گونه آثار فیزیکی می‌شوند، توسل به زور تلقی می‌گردند[۵۴]. بر همین اساس گفته شده است که «گرچه حملات سایبری در کنوانسیون‌های چهارگانهٔ ژنو و پروتکل‌های الحاقی آن به‌عنوان مخاصمات مسلحانه شناسایی نشده‌اند، اگر حملات سایبری از حیث آثار با حملات فیزیکی برابری و همانندی کنند، می‌توانند از منظر حقوق بین‌الملل بشردوستانه، بخشی از مخاصمات مسلحانه تلقی شوند»[۵۵]. هرچند دولت آسیب‌دیده ممکن است تصمیم بگیرد که آن‌ها را به‌عنوان دارندهٔ شرایط توسل به زور محسوب ننماید. در پروندهٔ استاکس‌نت[۵۶] که ویروس استاکس‌نت منجر به خسارت فیزیکی به سانتریفیوژهای متعلق به برنامهٔ هسته‌ای ایران شد[۵۷] و اکثر محققان بر آن نظر بودند که نوعی توسل به زور تلقی می‌گردید، هیچ‌گاه توسط دولت ایران یا در اعلام رسمی هیچ کشور دیگری توسل به زور دانسته نشد[۵۸].

پرسش مهم آن است که آیا وقوع هرگونه خسارت، تخریب اموال، جراحت یا تلفات جانی برای واجد شرایط بودنِ یک عملیات سایبری به‌عنوان یک توسل به زور سایبری، کافی است یا خیر. سند مقررات تالین این موضع را اتخاذ می‌کند که «اعمالی که باعث جراحت یا کشتن افراد یا آسیب فیزیکی یا تخریب اشیا می‌شود» به‌معنای «توسل به زور» است[۵۹]. در نگاه نخست، رویکرد مبتنی بر آثار اتخاذشده توسط سند مقررات تالین، در رابطه با حملات انجام‌شده از طریق فضای سایبر، مناسب به‌نظر می‌رسد. حملات سایبری می‌توانند منجر به تخریب فیزیکی گستردهٔ افراد و اشیا شوند که اگر تخریب‌های مذکور با ابزارهای مکانیکیِ سنتی انجام شوند، مطمئناً به عنوان توسل به زور تلقی خواهند شد. بر این اساس، غیرمنطقی خواهد بود که همین وضعیت برای حملات سایبری رد شده و صرفاً به این دلیل که آسیب از طریق سوءاستفاده از فضای سایبر، به‌جای استفاده از تسلیحات متعارف سنتی، ایجاد شده است، آستانهٔ شدت لازم غیرمحقق دانسته شود[۶۰]. این رویکرد با درک مدرن از توسل به زور نیز که به سلاح‌های به‌کاررفته بستگی ندارد، سازوار است.

---

52. Michael N Schmitt and Liis Vihul, eds., op. cit., 391–396.

مثال ارائه‌شده در صفحهٔ ۳۹۳ ارجاع اخیر شامل استفاده از عملیات سایبری برای انفجار تنها خط لولهٔ گاز طبیعی است که سوخت را به یک شهر می‌رساند و در نتیجه، به‌دلیل شرایط آب و هوایی سخت، باعث مرگ قابل پیش‌بینی غیرنظامیان می‌شود و در صفحهٔ ۳۹۳ نیز مثال مربوط به آلوده کردن هواپیماهای تجاری یک کشور دشمن به بدافزاری است که باعث سقوط آن‌ها می‌شود.

53. Ibid.

54. Michael N Schmitt "Cyber Operations and the Jus Ad Bellum Revisited", Villanova Law Review 56, (2011): 573; Michael N Schmitt "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", Columbia Journal of Transnational Law 37, (1999): 17; Yaroslav Radziwill, Cyber-Attacks and the Exploitable Imperfection of International Law (Leiden: Brill & Martinus Nijhoff Publishers, 2015), 131.

۵۵. علیرضا رنجبر و علی گرشاسبی، «موانع بنیادین فراروی تدوین حقوق بین‌الملل حاکم بر حملهٔ سایبری»، مجلهٔ حقوقی بین‌المللی، ۶۳ (۱۳۹۹): ۲۴۵.

56. Stuxnet case.

۵۷. حسین شریفی طرازکوهی و جعفر برمکی، پیشین، ۱۲۷.

58. Harrison Dinniss, Cyber Warfare and the Laws of War (Cambridge: Cambridge University Press, 2012), 37-75; Kim Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon (New York: Crown, 2014).

59. Michael N Schmitt and Liis Vihul, eds., op. cit., 332.

60. Ibid., 415-446.

۲/۲. تحقق توسل به زور از رهگذرِ حملات سایبری مختل‌کننده

منظور از عملیات‌های سایبری مختل‌کننده[۶۱] یا عملیات‌های سایبری دارای پیامدهای غیرفیزیکیِ صرف، اقداماتی است که «جریان اطلاعات یا عملکرد سیستم‌های اطلاعاتی را بدون ایجاد آسیب یا خسارت فیزیکی، قطع می‌کنند»[۶۲]. اگر از این عملیات‌ها به‌عنوان سلاح جنگی استفاده شود، می‌توانند پیامدهای مخربی را برای جمعیت غیرنظامی داشته باشند؛ زیرا اتکا به فضای سایبر و انتقال داده‌ها «تقریباً در هر جامعه‌ای ضروری شده است»[۶۳]. به‌طور مثال، حملهٔ باج‌افزار واناکرای[۶۴] در سال ۲۰۱۷، تأثیر شدیدی بر خدمات درمانی ملی انگلستان[۶۵] گذاشت[۶۶]. همچنین در طول شیوع کووید-۱۹، تعداد زیادی عملیات سایبری و کمپین‌های اطلاعات نادرست علیه مراکز پزشکی، فعالیت‌های درمانی عمومی و حتی سازمان بهداشت جهانی اجرا شده است[۶۷]. حملات مذکور «مستقیماً در ارائهٔ مراقبت‌ها، تدارکات پزشکی و تحقیقات لازم برای مبارزهٔ مؤثر با ویروس و گسترش آن، مداخله داشته است»[۶۸]. نمونه‌های دیگر از عملیات‌های سایبری مختل‌کننده که زیرساخت‌های حیاتی را هدف قرار می‌دهند، عبارت هستند از حمله به شبکهٔ برق اوکراین در دسامبر ۲۰۱۵ و حمله به یک نیروگاه هسته‌ای در هند در سپتامبر ۲۰۱۹. همهٔ این مثال‌ها و ده‌ها نمونهٔ واقعی دیگر نشان می‌دهند که چگونه می‌توان از عملیات‌های سایبری مختل‌کننده که مانند حملات سنتی یا برخی دیگر از عملیات‌های سایبری، آثار فیزیکی ایجاد نمی‌کنند، برای ایجاد اختلال در ارائهٔ خدمات ضروری، جلوگیری از دسترسی غیرنظامیان به نیازهای اساسی و مداخله در حقوق اساسی بشر، استفاده کرد. بنابراین، در صورت سوءاستفاده از آن‌ها و وصول به آستانهٔ توسل به زور و شکل‌گیری وضعیت مخاصمه، عملیات‌های سایبری مختل‌کننده می‌توانند منجر به یک بحران بشردوستانهٔ جدی شوند که در این صورت، جالب توجه دیوان بین‌المللی کیفری خواهد بود و مقتضی رسیدگی آن است.

احتساب عملیات‌های سایبری که هیچ اثری در دنیای واقعی ایجاد نمی‌کنند به‌عنوان توسل به زور سایبری، محل بحث بیشتر واقع شده است و قائلان به آن حداقل تا وقوع حملات سایبری مختل‌کننده علیه اوکراین، اندک بودند. برخی از نویسندگان به‌شدت با شناسایی آن‌ها به‌عنوان توسل به زور مخالف هستند؛ در حالی که برخی دیگر تحت شرایطی خاص، از چنین نظری حمایت می‌کنند[۶۹].

---

61. disruptive cyber operations (DCOs).
62. G Brown and O Tullos, "On the Spectrum of Cyberspace Operations", Small Wars Journal, 2012. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2400536 (accessed May 2, 2024).
63. I Kilovaty, "Virtual Violence – Disruptive Cyberspace Operations as "Attacks" Under International Humanitarian Law", Michigan Telecommunications and Technology Law Review 23, 1 (2016): 116.
64. WannaCry.
65. UK's National Health Service (NHS).
۶۶. حسین شریفی طرازکوهی و جعفر برمکی، پیشین، ۱۳۰.
۶۷. برای مطالعهٔ تفصیلی در خصوص این حملات و نحوهٔ اعمال حقوق بین‌الملل بر عملیات‌های سایبری و اطلاعات نادرست در چارچوب شیوع یک بیماری همه‌گیر، قابل ملاحظه است:
Marko Milanovic and Michael N Schmitt, "Cyber Attacks and Cyber (Mis)information Operations during a Pandemic", Journal of National Security Law & Policy 11, 27 (2020).
68. Ibid., 1.
69. Matthew Hoisington, op. cit., 447; Daniel B Silver, op. cit., 85; Michael N Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", op. cit., 913.

کمیتهٔ بین‌المللی صلیب سرخ بر این عقیده است که «هر اختلافی که بین دو کشور به وجود می‌آید و به مداخلهٔ نیروهای مسلح منجر می‌شود، یک مخاصمهٔ مسلحانه است ... فرقی نمی‌کند که مخاصمه چه‌قدر طول بکشد یا چه‌قدر کشتار اتفاق بیفتد»[۷۰]. همچنین «هیچ الزامی وجود ندارد که استفاده از نیروی مسلح بین طرفین قبل از این‌که بتوان گفت مخاصمهٔ مسلحانه وجود دارد، به سطح معینی از شدت برسد»[۷۱]. سایر اقوال و تفسیرها آستانه را بالاتر می‌گذارند و استدلال می‌کنند که درجاتی از مدت زمان و شدت، قبل از وقوع یک مخاصمهٔ مسلحانهٔ بین‌المللی مورد نیاز است[۷۲]. در هر حال، هرچند که با اذعان کمیتهٔ بین‌المللی صلیب سرخ، آستانه‌ای ویژه برای وقوع مخاصمه وجود نداشته باشد، لکن بدیهی است که طرح آستانهٔ شدت برای وقوع توسل به زور، ناگزیر است.

چنان‌چه ذکر شد، تفسیر قاعدهٔ شمارهٔ ۶۹ به صراحت این احتمال را که عملیات‌های سایبری مختل‌کننده می‌توانند به عنوان توسل به زور محسوب شوند یا نشوند، مقرر نمی‌دارد. این امکان در تفسیر عامل «قابل سنجش بودن آثار» ذکر شده است که ذیل آن، به اختلال در داده‌ها، غیرفعال کردن سرورها و نفوذ در فایل‌های محرمانه به عنوان فعالیت‌هایی اشاره می‌شود که به‌طور بالقوه می‌توانند این معیار خاص را برآورده کنند (Schmitt, Vihul, 2017 : 335). با این حال، لحن کلی این قاعده نشان می‌دهد که برای حمله به دارایی‌های نامشهود یا عملیاتی که تنها منجر به اختلال می‌شود، بسیار دشوار خواهد بود که بتوان آن را توسل به زور تلقی کرد. ریشهٔ این رویکرد را شاید بتوان با توجه به این نکته یافت که زمانی که بسیاری از قوانین حقوق توسل به زور –به‌عنوان مبنای تحلیل‌های سند مقررات تالین– تدوین می‌شدند، غیرقابل تصور بود که مخاصمه در جایی غیر از قلمرو فیزیکی رخ دهد. همچنین شایان توجه است در زمانی که گروه کارشناسان سند مقررات تالین مسائل مربوط به کاربست حقوق توسل به زور در فضای سایبر را بررسی می‌کردند، اجماع کافی در مورد وضعیت آسیب‌های دیجیتال وجود نداشت و عملیات‌های سایبری مختل‌کننده به رشد کمی و کیفیِ کنونی نرسیده بودند.

به‌نظر می‌رسد که می‌توان گفت عملیات‌های سایبری که پیامدهای غیرفیزیکی شدیدی را به همراه دارند، بدان‌سبب که در حال حاضر، ارتش‌ها و جمعیت‌های غیرنظامی به‌طور یکسان به توانایی انتقال سریع اطلاعات حیاتی از طریق اینترنت وابسته هستند[۷۳]، از نظر تئوری، در برخی شرایط بسیار محدود، می‌توانند برابر با توسل به زور باشند؛ زیرا جنگ مدرن در حال تطبیق با جهانی است که به طور فزاینده‌ای بر فناوری و انتقال داده متکی می‌شود. اگرچه عملیات‌های سایبری مختل‌کننده به هیچ آسیب یا خسارت فیزیکی منجر نمی‌شوند، اما می‌توانند به همان اندازهٔ حملات سایبری تخریب‌گر که اثرات فیزیکی ایجاد می‌کنند، خطرناک باشند.

---

[70]. International Committee of the Red Cross, Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 2016, p. 32.

[71]. Ibid., 236; Office of General Counsel, 'United States Department of Defense Law of War Manual', 12 June 2015, updated December 2016. https://www.hsdl.org/?abstract&did=797480 (accessed May 2, 2024).

در ارجاعات فوق، چنین اشاره شده است که آستانهٔ شدت به‌عنوان هر موقعیتی توصیف می‌شود که در آن، میان نیروهای مسلح دو طرف، صرف‌نظر از مدت، شدت یا دامنهٔ درگیری، یک مخاصمه وجود داشته باشد.

[72]. C Greenwood, "Scope of Application of Humanitarian Law" in The Handbook of International Humanitarian Law, edited by D Fleck, 2nd edn (Oxford: Oxford University Press, 2008), 57; HS Levie, "The Status of Belligerent Personnel "Splashed" and Rescued by a Neutral in the Persian Gulf Area", Virginia Journal of International Law 31, (1991): 243-244.

[73]. L. Gisel and L. Olejnik, "The Potential Human Cost of Cyber Operations", May 29, 2019, https://www.icrc.org/en/document/potential-human-costcyber-operations (accessed May 2, 2024).

از سوی دیگر، ماهیت هدف معطوف به یک زیرساخت اطلاعاتی حیاتی نیز ممکن است بر این‌که یک حملهٔ سایبری مختل‌کننده شدید دانسته شده و به‌عنوان توسل به زور سایبری شناسایی شود تأثیر بگذارد[۷۴]. برعکس، اگر عملیات سایبری فقط اثرات غیرفیزیکی ایجاد کند که بر زیرساخت‌های حیاتی کشور مورد نظر تأثیری نداشته باشد، بعید است که این عملیات سایبری واجد شرایط توسل به زور دانسته شود[۷۵]. اتکای فزاینده بر زیرساخت‌های حیاتی به این معنی است که یک عملیات سایبری مختل‌کننده که زیرساخت‌های حیاتی ملی را غیرفعال می‌کند، می‌تواند به همان اندازه شدید باشد که یک حملهٔ سایبری منجر به تخریب فیزیکی، شدید است. در چارچوب حقوق کیفری بین‌المللی، الزام به ایجاد خسارات فیزیکی از سوی عملیات‌های سایبری، به‌دلایل عمده مشکل‌ساز است و شاید همین موضوع باعث شده است که بتوان ادعا کرد نتیجه‌گیریِ سند مقررات تالین در خصوص این موضوع، بیان‌کنندهٔ یک اجماع نبوده و تا کنون نیز موجب ایجاد اجماع نشده است. تا آن‌جا که چنان‌چه اشاره شد، برخی از دولت‌ها و اندیشمندان دیدگاه مخالف را اتخاذ کرده‌اند[۷۶].

حملات متعدد به زیرساخت‌های درمانی که در طی شیوع کووید-۱۹ روی داده‌اند، بحث‌های دوباره در مورد ماهیت توسل به زور در فضای سایبر و این‌که آیا نیازمند عواقب فیزیکی است یا خیر، موجب شده است. پژوهشگران بر آن نظر هستند که به‌دلیل شدت همه‌گیری و مقیاس تأثیرات ویروس در سراسر جهان، دولت‌ها تمایل بیشتری دارند تا عملیات‌های سایبری مختل‌کننده را که سیستم‌های مراقبت‌های درمانی آن‌ها را هدف قرار می‌دهد، به‌عنوان توسل به زور توصیف کنند. استدلال شده است که: «... عملیاتی که یک بیمارستان بزرگ را تعطیل می‌کند یا به شکلی قابل توجه و مستقیم در توزیع اطلاعات ضروری سلامت عمومی دخالت می‌کند، توسط دولت‌ها می‌تواند به‌عنوان توسل به زور دانسته شود؛ حتی اگر آسیب مستقیمی به جان انسان‌ها یا سلامتی آن‌ها وارد نکند و حتی اگر در زیرساخت‌ها یا تجهیزات به‌طور دائم مداخله ننماید»[۷۷]. این اعلامیه‌های دولت‌ها و ملاحظات پژوهشی نشان می‌دهد که حقوق عرفی در خصوص توسل به زور در فضای سایبر به سمتی پیش می‌رود که روزاروز، بیشتر شامل خسارت‌های دیجیتال و غیرفیزیکی می‌شود.

در راستای تقویت این نظر می‌توان به شرط مارتنز نیز استناد کرد که بر اساس آن، در جایی که موافقت‌نامهٔ بین‌المللی وجود نداشته باشد، نظامیان و غیرنظامیان همچنان زیر لوای حمایتی اصول حقوق بین‌الملل که در عرف مقرر، اصل انسانیت و آن‌چه از خرد جمعی ناشی می‌شود، ریشه دارد، قرار خواهند گرفت[۷۸].

---

74. Marco Roscini, "Cyber Operations as a Use of Force" in Research Handbook on International Law and Cyberspace, edited by Nicholas Tsagourias and Russell Buchan (Massachusetts: Edward Elgar Publishing, 2014), 245.

75. Marco Roscini, Cyber Operations and the Use of Force in International Law, op. cit., 58.

76. Marco Roscini, Cyber Operations as a Use of Force, op. cit., 245; K Ziolkowski, "Computer Network Operations and the Law of Armed Conflict", The Military Law and the Law of War Review 49, (2010): 73–75.

77. Marko Milanovic and Michael N Schmitt, op. cit.,12.

۷۸. علیرضا محقق هرچقان، محمدعلی اردبیلی و ابراهیم بیگ‌زاده، پیشین، ۳۱۱؛ پریسا دهقانی، محمدحسین رمضانی قوام‌آبادی و محمدرضا علی‌پور، «شرط مارتنس در حقوق کیفری بین‌المللی، ماهیت و کارکردهای تفسیری»، آموزه‌های حقوق کیفری، ۲۳ (۱۴۰۱): ۱۴۰.

۳. آستانهٔ شدت توسل به زور سایبری نزد دیوان کیفری بین‌المللی

چنان‌چه گفته شد، دیوان کیفری بین‌المللی برای رسیدگی به حملات سایبری تخریب‌گر، با چالش جدی مواجه نیست؛ لکن در خصوص حملات سایبری مختل‌کننده، با عنایت به این‌که هدف اصلی حقوق کیفری بین‌المللی «پایان دادن به بی‌کیفرمانی» برای «جدی‌ترین جنایات مربوط به جامعهٔ بین‌المللی» است[۷۹]، بررسی این موضوع ضروری است که آیا مادهٔ ۸ اساسنامهٔ رم می‌تواند عملیات‌های سایبری مختل‌کننده را نیز در سطح توسل به زور محسوب و در محدودهٔ صلاحیتی یک وضعیت مخاصمه‌آمیز برای رسیدگی خود قرار دهد یا خیر؛ هرچند چنین پیشرفت‌های فناوری در زمان تدوین آن پیش‌بینی نمی‌شده است.

هرچند که برخی از صاحب‌نظران از ضرورت تهیهٔ معاهده‌ای نو در رابطه با جنگ سایبری، به‌سبب عدم شمول مقررات موجود بر همهٔ گونه‌های عملیات سایبری سخن گفته‌اند[۸۰]، دولت‌ها ناگزیر و به‌طور روزافزون، این دیدگاه را بیان می‌کنند که حقوق توسل به زور انواع خاصی از عملیات‌های سایبری مختل‌کننده را ممنوع می‌سازد[۸۱]. کمیتهٔ بین‌المللی صلیب سرخ نیز به این نتیجه می‌رسد که «صرف غیرفعال کردن یک چیز مانند خاموش کردن شبکهٔ برق بدون تخریب آن نیز باید به‌عنوان یک حمله شناخته شود»[۸۲]. آن‌گونه که کمیتهٔ بین‌المللی صلیب سرخ اشاره کرده است: «اگر مفهوم حمله تنها به‌عنوان اشاره به عملیاتی باشد که منجر به مرگ، جراحت یا آسیب فیزیکی شود، یک عملیات سایبری که هدف آن ناکارآمد کردن یک شبکهٔ غیرنظامی (مانند برق، بانک یا ارتباطات) است یا انتظار می‌رود که اتفاقاً باعث ایجاد چنین آثاری شود، ممکن است تحت پوشش مقررات ضروری حقوق بشردوستانهٔ بین‌المللی که از جمعیت غیرنظامی و اشیای غیرنظامی محافظت می کند، قرار نگیرد. تطبیق چنین درک بیش از حد محدودکننده‌ای از مفهوم حمله با موضوع و هدف قواعد حقوق بشردوستانهٔ بین المللی در مورد ارتکاب مخاصمات دشوار خواهد بود»[۸۳]. عبارات اخیر کمیتهٔ بین‌المللی صلیب سرخ حرکتی به سمت درک منطقی از مفهوم حمله و توسل به زور را نشان می‌دهد که «از دست دادن موقت عمل‌کرد» را نیز شامل می‌شود؛ هرچند نگارندگان مؤثر در نظریهٔ ۲۰۲۴ کمیتهٔ بین‌المللی صلیب سرخ، در مقاله‌ای تأکید داشته‌اند که «در مورد این‌که آیا عملیات سایبری فقط با ایجاد اختلال یا غیرفعال کردن عمل‌کرد زیرساخت‌های دیجیتال نیز توسل به زور را موجب می‌شود یا خیر، هنوز اجماع یا مقررهٔ متقنی وجود ندارد»[۸۴].

از آن‌جا که جامعهٔ بین‌المللی شروع به تشخیص این موضوع کرده است که رایاجنگ‌ها حتی اگر صرفاً در حوزهٔ دیجیتال و بدون آثار فیزیکی اتفاق بیفتد، می‌تواند به‌عنوان یک حملهٔ واصل به آستانهٔ توسل به زور، تلقی شود، شایسته است که دیوان کیفری بین‌المللی نیز در تفسیر کیفری خود از متناظر تفسیرهای اخیر پیروی کند. در این راستا، به‌منظور ارائهٔ معیار جهت تشیص رایاجنگ‌های مختل‌کننده‌ای که به آستانهٔ توسل به زور می‌رسند، لازم به تأکید است که معیارهای هشت‌گانهٔ ارائه‌شده توسط سند مقررات تالین مورد تأیید و تأکید نگارنده قرار دارند؛ لکن با عنایت به این‌که از منظر سند مذکور، از یک سو، شاخص «شدت» از اولویت و اهمیت

---

[۷۹]. آن‌گونه که در مقدمهٔ اساسنامهٔ رم مورد اشاره قرار گرفته است.

[۸۰]. پوریا عسکری، «حقوق بشردوستانه در جنگ سایبری» در: دانشنامهٔ رفتار سایبری، به‌کوشش باقر شاملو (تهران: میزان، ۱۴۰۱): ۲۴۳.

[81]. Beatty, Georgia, "War crimes in cyberspace: prosecuting disruptive cyber operations under Article 8 of the Rome Statute", The Military Law and the Law of War Review 58, 2 (2020): 214.

[82]. K Dörmann, "The Applicability of the Additional Protocols to Computer Network Attacks: An ICRC Approach". Stockholm: International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, November 19, 2004. https://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf (accessed May 2, 2024).

[83]. International Committee of the Red Cross. "International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC position paper". November 28, 2019, p. 8. https://www.icrc.org/en/document/ international-humanitarian-law-and-cyber-operations-during-armed-conflicts (accessed May 2, 2024).

84. D'Cunha, Samit, Ferraro, Tristan and Maurice, Thomas de Saint, "Defining armed conflict: some clarity in the fog of war", Humanitarian Law & Policy Blog, May 2, 2024. https://blogs.icrc.org/law-and-policy/2024/05/02/defining-armed-conflict-some-clarity-in-the-fog-of-war/. (accessed March 30, 2025).

بیشتر برخوردار است و از سوی دیگر، سند مذکور نسبت به شمولیت شاخص «شدت» بر «رایاجنگ‌های مختل‌کننده» با گونه‌ای ابهام یا احتمالِ عدمِ شمول مواجه است -که شرح آن گذشت-. به‌نظر می‌رسد که بنا بر مراتب فوق، می‌بایست از ضرورت شمول شاخص «شدت» بر رایاجنگ‌های مختل‌کنندهٔ شدید که به آستانهٔ توسل به زور می‌رسند، سخن گفت. برای سنجش این شاخص، رویهٔ قضائی دیوان کیفری بین‌المللی نشان داده است که ارزیابی معیار «شدت» یک رفتار باید بر اساس عوامل کمی و کیفی همچون مقیاس، ماهیت، شیوهٔ ارتکاب جنایات و همچنین تأثیرات آن‌ها، صورت گیرد[۸۵]. فرانسه نیز از این موضع حمایت کرده است که: «در غیاب خسارت فیزیکی، یک عملیات سایبری ممکن است بر اساس معیارهای متعدد، از جمله شرایط حاکم در زمان عملیات، مانند منشاء عملیات و ماهیت محرک عملیات (نظامی یا غیرنظامی)، میزان نفوذ، اثرات واقعی یا مورد نظر عملیات یا ماهیت هدف مورد نظر، توسل به زور تلقی شود»[۸۶].

اعلامیه‌های دولت‌ها و ملاحظات پژوهشی نشان می‌دهد که حقوق عرفی در خصوص توسل به زور در فضای سایبر به سمتی پیش می‌رود که بیشتر شامل خسارت‌های دیجیتال و غیرفیزیکی شود. بر این اساس، می‌توان از ردِ ملاکِ لزوم ایجاد آثار فیزیکی برای تحقق معیار «شدت» برای وصول به توسل به زور سخن گفت و می‌بایست برای تأثیرات حملاتی که صرفاً در حوزهٔ دیجیتال رخ می‌دهند و به هیچ‌گونه نمودهای تخریب فیزیکی منجر نمی‌شوند، قائل به موضوعیت شد؛ زیرا غفلت از خسارت دیجیتال، می‌تواند منجر به نادیده گرفته شدن اشکال جدیدی از ظلم شود که از آن‌ها به‌عنوان عملیات‌های سایبری مختل‌کننده یاد می‌شود.

در مواردی که برخی از عبارات اساسنامهٔ رم قابلیت تفسیر داشته باشد، می‌بایست در چارچوب رویکردی پویا مورد تفسیر واقع شود و منعکس‌کنندهٔ تحولات فناورانه در جنگ و گفتمان در حال توسعه در خصوص آسیب دیجیتال باشد که در جامعهٔ بین‌المللی رخ می‌دهد؛ به‌گونه‌ای که رایاجنگ‌های مختل‌کننده را در محدودهٔ صلاحیتی ماده ۸ قرار دهد و اطمینان حاصل کند که نقض دیجیتال حقوق بشردوستانهٔ بین‌المللی در نتیجهٔ نقض حقوق توسل به زور، بی‌کیفر باقی نمی‌ماند. ضمن تأکید بر اصل قانونی بودنِ جرم و مجازات مستنبط از مادهٔ ۲۲ اساسنامهٔ رم، رویهٔ قضائی دیوان نشان داده است که رویکرد هدفمند و غایت‌نگر به مادهٔ ۸ را می‌توان در مواردی اتخاذ کرد و در غیر این صورت، موضوع و هدف اساسنامهٔ دیوان را تضعیف می‌کند؛ همچنین باید به خاطر داشت که دیوان کیفری بین‌المللی مستند به مادهٔ ۲۱ اساسنامهٔ رم، موظف است «در صورت اقتضا، ... اصول تثبیت‌شدهٔ حقوق بین‌الملل در خصوص مخاصمات مسلحانه» را اعمال کند و قانون را به‌گونه‌ای تفسیر نماید که «منطبق با حقوق بشر شناخته‌شدهٔ بین‌المللی» باشد که هر دوی این موارد به‌طور طبیعی در طول زمان و در پاسخ به توسعهٔ فناوری‌های جدید تکامل خواهد یافت. استفاده از رایاجنگ‌های مختل‌کننده در جنگ می‌تواند منجر به حملات مکرر علیه غیرنظامیان نسبت به جنگ‌های متعارف شود، مگر این‌که به‌دقت مورد تنظیم‌گری واقع شوند؛ زیرا چنین عملیات‌هایی می‌تواند بدون ایجاد آسیب فیزیکی مستقیم بر روی اشیای غیرنظامی، انجام شود و در نتیجه، هزینهٔ سیاسی کمتری داشته باشد[۸۷]. به این دلایل، دیوان کیفری بین‌المللی باید رویکرد «ضرورت ایجاد آثار فیزیکی» را در

---

85. Marco Roscini, "Cyber Operations Can Constitute War Crimes Under the ICC Jurisdiction Without Need to Amend the Rome Statute", March 7, 2022, https://iccforum.com/cyberwar (accessed May 2, 2024).

86. Ministry of the Armies. "International Law Applied to Operations in Cyberspace". March 19, 2019, https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf (accessed May 2, 2024).

87. J Kelsey, "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare", Michigan Law Review 106, 7 (2008): 1439–1441.

تفسیر خود از مادهٔ ۸ اساسنامه، رد کند و پیشنهاد می‌شود که در ارزیابی تحقق معیار «شدت» برای سنجش وقوع یا عدم وقوع توسل به زور، ریزمعیارهای دیگری همچون اختلال در زیرساخت‌های حیاتی یا اطلاعاتی را پی نماید.

برآمد

افزایشِ روزافزونِ توسل به حملات سایبری و رایاجنگ‌ها از سوی دولت‌ها و سواستفاده از قابلیت‌های هولناکِ آن‌ها برای ورود آسیب به سایر کشورها، تنظیم‌گریِ رایاجنگ‌ها و وضع محدودیت بر آن‌ها را ناگزیر ساخته است تا آن‌جا که دادستان دیوان کیفری بین‌المللی در سال ۲۰۲۳، صراحتاً از امکان تعقیب برخی رفتارهای ارتکاب‌یافته در چارچوبِ رایاجنگ‌ها با عنوان جنایت جنگی سخن گفته است. بر این اساس، پیش از تطبیق عناصر عمومی و اختصاصی جنایات جنگی سنتی بر جنایات جنگی سایبری در چارچوب اساسنامهٔ رم، امکان‌سنجی وقوع عنصر زمینه‌ای جنایات جنگیِ سنتی، یعنی وجود توسل به زور برای شکل‌گیری وضعیت مخاصمه، در رایاجنگ‌ها و آستانهٔ شدت لازم برای وقوع آن در جنگ‌های سایبری ضرورت می‌یابد.

با عنایت به رأی دادگاه کیفری بین‌المللی برای یوگسلاوی سابق، بررسی آستانهٔ توسل به زورِ سایبری ضروری است. تفاوت میان دو گونهٔ متفاوت از حملات سایبری، یعنی حملات سایبری تخریب‌گر و مختل‌کننده، ارائهٔ دو تحلیل متفاوت از آستانهٔ شدت توسل به زور سایبری را موجب شده است. توضیح آن‌که بیشتر تحلیل‌های ارائه‌شده از سوی پژوهشگران، همسو با رویکرد سند مقررات تالین، ایجاد آثار فیزیکیِ مشابه با حملات سنتی در نتیجهٔ حملات سایبری را برای احراز وقوع توسل به زور ضروری می‌دانند و در این راستا، امکان وقوع توسل به زور در اثر حملات سایبری تخریب‌گر را تأیید نموده و در مقابل حملات سایبری مختل‌کننده، نظر منفی ارائه می‌دهند. این در حالی است که تحلیل انتقادی ارائه‌شده در این پژوهش روشن می‌کند که ایجاد آثار فیزیکی لزوماً به‌معنای شدتِ بیشترِ آثارِ ایجادشده نیست و بسیاری از اختلال‌های ایجادشده در زیرساخت‌های اطلاعاتی حیاتی یک کشور که در نتیجهٔ عملیات‌های سایبری مختل‌کننده واقع می‌شوند، می‌توانند بسیار شدیدتر از آثار فیزیکیِ ناشی از برخی حملات سایبری تخریب‌گر ارزیابی شوند. بر این اساس، می‌توان به‌جای اتخاذ رویکرد مبتنی بر آثار فیزیکی، توجه به جدیتِ آثارِ ایجادشده در نتیجهٔ حملات سایبری را که لزوماً به‌معنای آثار فیزیکیِ صرف نیست، مورد توجه قرار داد و از این ره‌گذر، قائل به امکان وقوع توسل به زور در نتیجهٔ وقوع هر دو گونه از حملات سایبری شد.

مستند به اساسنامهٔ رم، هدف اصلی تشکیل دیوان کیفری بین‌المللی، پایان دادن به بی‌کیفرمانیِ جدی‌ترین جنایات مربوط به جامعهٔ بین‌المللی» است. این در حالی است که در صورت اتخاذ رویکرد مشهور مبنی بر اهمیتِ آثار فیزیکیِ صرف، حملات سایبری مختل‌کننده به‌سبب عدم وصول به آستانهٔ توسل به زور، وضعیت مخاصمه‌گونه را شکل نداده و در نتیجه، از شمول صلاحیت دیوان کیفری بین‌المللی خارج می‌شوند. بر این اساس، اتخاذ رویکردی پویا از آستانهٔ شدت وقوع توسل به زور سایبری از سوی دیوان کیفری بین‌المللی برای شمول همهٔ گونه‌های حملات سایبریِ شدید تحت عنوان جنایت جنگی، پیشنهاد می‌شود. تحولات فناورانه در جنگ و گفتمان در حال توسعه در خصوص آسیب دیجیتال که در جامعهٔ بین‌المللی در حال وقوع است، اتخاذ رویکرد پویای مذکور از سوی

دیوان را ناگزیر می‌سازد؛ به‌گونه‌ای که عملیات‌های سایبری مختل‌کننده را در محدودهٔ صلاحیتی ماده ۸ قرار دهد و اطمینان حاصل کند که نقض دیجیتال حقوق توسل به زور بی‌کیفر باقی نمی‌ماند.

فهرست منابع:

الف) منابع فارسی

کتب:

- ذاکرحسین، محمدهادی. آیین پیش‌دادرسی دیوان کیفری بین‌المللی، دفتر نخست: فرایند گزینشگری قضایا. تهران: شهر دانش، ۱۳۹۹.
- خلیل‌زاده، مونا. مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری. تهران: مجمع علمی و فرهنگی مجد، ۱۳۹۳.
- شریفی طرازکوهی، حسین. حقوق بشردوستانهٔ بین‌المللی. چاپ دوم. تهران: میزان، ۱۳۹۵.
- محقق هرچقان، علیرضا. مسئولیت کیفری از منظر جرم‌شناسی. تهران: دادگستر، ۱۳۹۰.
- نژندی‌منش، هیبت‌الله، حقوق بین‌الملل کیفری در رویهٔ قضایی. چاپ نخست. تهران: خرسندی، ۱۳۹۴.

مقالات:

- اسمعیل‌زاده ملاباشی، پرستو. «حملهٔ سایبری به‌مثابهٔ جنایت تجاوز و بررسی صلاحیت دیوان کیفری بین‌المللی در رسیدگی به آن». پژوهش‌های حقوق جزا و جرم‌شناسی، ۱۰ (۱۳۹۶): ۶۵-۴۳.
- حبیبی، همایون و وحید بذار، «حملات سایبری و ممنوعیت توسل به زور»، تعالی حقوق، ۳، ۲ (۱۳۹۶): ۱۷۸-۱۵۵.
- دهقانی، پریسا، محمدحسین رمضانی قوام‌آبادی و محمدرضا علی‌پور، «شرط مارتنس در حقوق کیفری بین‌المللی، ماهیت و کارکردهای تفسیری»، آموزه‌های حقوق کیفری، ۲۳ (۱۴۰۱): ۱۵۶-۱۲۳.

DOI: 10.30513/cld.2022.3988.1634

- رنجبر، علیرضا و علی گرشاسبی، «موانع بنیادین فراروی تدوین حقوق بین‌الملل حاکم بر حملهٔ سایبری»، مجلهٔ حقوقی بین‌المللی، ۶۳ (۱۳۹۹): ۲۶۴-۲۳۷.
- شریفی طرازکوهی، حسین و جعفر برمکی. «چالش‌های حقوقی قابلیت‌های فضای سایبری در پرتو مادهٔ ۳۶ پروتکل یکم الحاقی ۱۹۷۷». مجلهٔ حقوقی بین‌المللی، ۳۷، ۶۲ (۱۳۹۹): ۱۴۶-۱۲۱.

DOI: 10.22066/cilamag.2019.84640.1491

- صابر، محمود و آزاده صادقی. «بررسی معیار آستانهٔ شدت برای تعقیب جنایات در دیوان کیفری بین‌المللی؛ با نگاهی بر دیگر دادگاه‌های بین‌المللی». مطالعات حقوق تطبیقی، ۶، ۲ (۱۳۹۴): ۶۵۰-۶۲۷.
- عباسی، مجید و مرادی، حسین. «جنگ سایبر از منظر حقوق بین‌الملل بشردوستانه»، مجلس و راهبرد ۸۱، (۱۳۹۴): ۳۷-۶۸.
- عسکری، پوریا. «حقوق بشردوستانه در جنگ سایبری» در: دانشنامهٔ رفتار سایبری، به‌کوشش باقر شاملو. تهران: میزان، ۱۴۰۱.
- فقیه حبیبی، علی. «جنگ مدرن و تخاصمات سایبری در چارچوب فضای بین‌الملل». جستارهای سیاسی معاصر، ۷، ۱۹ (۱۳۹۵): ۱۴۴-۱۱۵.
- محقق هرچقان، علیرضا، محمدعلی اردبیلی و ابراهیم بیگ‌زاده. «صلاحیت دیوان کیفری بین‌المللی و رسیدگی به جنایات بین‌المللی سایبری در عرصه‌های انسانی حقوق بین‌الملل». پژوهشهای حقوق جزا و جرم‌شناسی، ۱۱، ۲۱ (۱۴۰۲): ۳۲۷-۳۰۳.

DOI: 10.22034/jclc.2023.389750.1827

- محقق هرچقان، علیرضا، محمدعلی اردبیلی، ابراهیم بیگ‌زاده و محمدعلی مهدوی ثابت. «اثربخشی دستورالعمل تالین ۲۰۱۷ میلادی بر صلاحیت دیوان کیفری بین‌المللی در ایجاد صلح و امنیت سایبری بین‌المللی»، آموزه‌های حقوق کیفری، ۱۹، ۲۳ (۱۴۰۱): ۲۹۶-۲۶۹.

DOI: 10.30513/cld.2022.3192.1502

- محقق هرچقان، علیرضا، محمدعلی اردبیلی، ابراهیم بیگ‌زاده و محمدعلی مهدوی ثابت. «حقوق بین‌الملل سایبری و توسعهٔ صلاحیت دیوان کیفری بین‌المللی (با تأکید بر مذاکرات تالین ۲۰۱۷ میلادی)». فصلنامهٔ مطالعات حقوق عمومی، ۵۳، ۳ (۱۴۰۲): ۱۵۵۹-۱۵۳۷.

DOI: 10.22059/jplsq.2022.329515.2869

ب) منابع خارجی

Books:

- Ambos, Kai. "International Criminal Responsibility in Cyberspace" in *Research Handbook on International Law and Cyberspace*, edited by Nicholas Tsagourias & Russell Buchan, 118-143. Cheltenham: Edward Elgar, 2015.
- Corten, Olivier. *The Law against War - The Prohibition on the Use of Force in Contemporary International Law*. Oxford: Hart Publishing, 2012.

- Dinniss, Harrison. *Cyber Warfare and the Laws of War.* Cambridge: Cambridge University Press, 2012.
- Greenwood, C. "Scope of Application of Humanitarian Law" in *The Handbook of International Humanitarian Law*, edited by D Fleck, 2nd edn. Oxford: Oxford University Press, 2008.
- O'Connell, Mary Ellen. "The Prohibition of the Use of Force" in *Research Handbook on International Conflict and Security Law: Jus ad Bellum, Jus in Bello and Jus post Bellum*, Edited by Christian Henderson and Nigel White. London: Edward Elgar Publishing, 2013.

- Radziwill, Yaroslav. *Cyber-Attacks and the Exploitable Imperfection of International Law*. Leiden: Brill & Martinus Nijhoff Publishers, 2015.
- Roscini, Marco. "Cyber Operations as a Use of Force" in *Research Handbook on International Law and Cyberspace*, edited by Nicholas Tsagourias and Russell Buchan, 297-316. Massachusetts: Edward Elgar Publishing, 2014.
- Roscini, Marco. *Cyber Operations and the Use of Force in International Law*. Oxford: Oxford University Press, 2014.
- Schmitt Michael N. and Vihul Liis. eds.. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd edn. Cambridge: Cambridge University Press, 2017.
- Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013.
- Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown, 2014.

Articles:

- Akande, Dapo and Hollis Duncan. "The Oxford Process on International Law Protections in Cyberspace". Oxford Institute for Ethics, Law and Armed Conflict (2020). available in: https://www.elac.ox.ac.uk/the-oxford-process/.
- Barkham, Jason. "Information Warfare and International Law on the Use of Force". New York University Journal of *International Law and Politics 34*, (2001): 57-113.
- Brown G. and O Tullos. "On the Spectrum of Cyberspace Operations". Small Wars Journal, 2012. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2400536 (accessed May 2, 2024).
- D'Cunha, Samit, Ferraro, Tristan and Maurice, Thomas de Saint, "Defining armed conflict: some clarity in the fog of war", Humanitarian Law & Policy Blog, May 2, 2024. https://blogs.icrc.org/law-and-policy/2024/05/02/defining-armed-conflict-some-clarity-in-the-fog-of-war/. (accessed March 30, 2025).
- Duncan B. Hollis & Tsvetelina van Benthem. "What Would Happen If States Started Looking at Cyber Operations as a "Threat" to Use Force?". *LAWFARE*, March 30, 2021. accessed May 2, 2024. https://www.lawfaremedia.org/article/what-would-happen-if-states-started-looking-cyber-operations-threat-use-force.
- Georgia, Beatty. "War crimes in cyberspace: prosecuting disruptive cyber operations under Article 8 of the Rome Statute". *The Military Law and the Law of War Review 58*, 2 (2020): 209-239.
- Gisel, L. and L Olejnik. "The Potential Human Cost of Cyber Operations". May 29, 2019, https://www.icrc.org/en/document/potential-human-costcyber-operations (accessed May 2, 2024).
- Greenberg, Andy. "The International Criminal Court Will Now Prosecute Cyberwar Crimes". *Wired*, September 7, 2023. accessed May 2, 2024. https://www.wired.com/story/icc-cyberwar-crimes/.
- Hoisington, Matthew. "Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense". *International & Comparative Law Review 32*, (2009): 439-454. DOI: 10.2139/ssrn.1542223.

- international criminal court. "Measures taken following the unprecedented cyber-attack on the ICC". accessed May 2, 2024. https://www.icc-cpi.int/news/measures-taken-following-unprecedented-cyber-attack-icc.
- international criminal court. "Statement by ICC Prosecutor Karim A.A. Khan KC on conference addressing cyber-enabled crimes through the Rome Statute system". accessed May 2, 2024. https://www.icc-cpi.int/news/statement-icc-prosecutor-karim-aa-khan-kc-conference-addressing-cyber-enabled-crimes-through.
- J Kelsey. "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare". *Michigan Law Review 106*, 7 (2008): 1427–1451.
- K Dörmann. "The Applicability of the Additional Protocols to Computer Network Attacks: An ICRC Approach". Stockholm: International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, November 19, 2004. https://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf (accessed May 2, 2024).
- Karim A.A. Khan, "Technology Will Not Exceed Our Humanity", August 20, 2023, https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity/ (accessed May 2, 2024).
- Kilovaty, I.. "Virtual Violence – Disruptive Cyberspace Operations as "Attacks" Under International Humanitarian Law". *Michigan Telecommunications and Technology Law Review 23*, 1 (2016): 113-151.
- Levie, HS. "The Status of Belligerent Personnel "Splashed" and Rescued by a Neutral in the Persian Gulf Area". *Virginia Journal of International Law 31*, (1991): 239-245
- Marco Roscini, "Cyber Operations Can Constitute War Crimes Under the ICC Jurisdiction Without Need to Amend the Rome Statute", March 7, 2022, https://iccforum.com/cyberwar (accessed May 2, 2024).
- Milanovic, Marko and Michael N Schmitt. "Cyber Attacks and Cyber (Mis)information Operations during a Pandemic". *Journal of National Security Law & Policy 11*, 27 (2020): 247-284.
- Ruys, Tom. "The Meaning of "Force" and the Boundaries of the Jus Ad Bellum: Are "Minimal" Uses of Force Excluded from UN Charter Article 2(4)?". American Journal of International Law 108, 2 (2014): 159-210. DOI: 10.5305/amerjintelaw.108.2.0159.
- Schmitt, Michael N. "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework". *Columbia Journal of Transnational Law 37*, (1999): 3-48.
- Schmitt, Michael N. "Cyber Operations and the Jus Ad Bellum Revisited". *Villanova Law Review 56*, (2011): 569-606.
- Silver, Daniel. "Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter". *International Law Studies 76*, (2002): 73-97.
- Ziolkowski, K. "Computer Network Operations and the Law of Armed Conflict". *The Military Law and the Law of War Review 49*, (2010).

Documents:

- Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania), ICJ Reports 4, 1949.
- International Committee of the Red Cross, Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 2016.
- International Committee of the Red Cross. "International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC position paper". November 28, 2019, p. 8. https://www.icrc.org/en/document/ international-humanitarian-law-and-cyber-operations-during-armed-conflicts (accessed May 2, 2024).
- Max Planck Institute for Comparative Public Law and International Law, "Report of the International Fact-Finding Commission on the Conflict in Georgia", vol II, 2009: 242, available in: www.ceiig.ch/Report.html (accessed May 2, 2024).
- Ministry of the Armies. "International Law Applied to Operations in Cyberspace". March 19, 2019, https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf (accessed May 2, 2024).
- Office of General Counsel, 'United States Department of Defense Law of War Manual', June 12, 2015, updated December 2016. https://www.hsdl.org/?abstract&did=797480 (accessed May 2, 2024).
- Preparatory Commission for the International Criminal Court, Report of the Preparatory Commission for the International Criminal Court, Addendum, add. Part II Finalized draft text of the Elements of Crimes, 2000, U.N. Doc. PCNIC/2000/1/Add.2.
- Prosecutor v. Tadić, Case No. IT-١-٩٤-l, Decision on the Defense Motion for Interlocutory Appeal on Jurisdiction, Int'l. Crim. Trib. for the Former Yugoslavia, 2 Octoer ١٩٩٥.
- Rome Statute of the International Criminal Court, 17 July 1998, 2187 U.N.T.S. 90, art. 8.