University of Tehran Press

Comparative Law Review

Homepage: https://jcl.ut.ac.ir

Online ISSN: 2423-3404

Volume: 15, Issue: 2
Autumn & Winter
2024-2025

Background element of cyber war crimes arising from disruptive cyber warfares in the light of The Tallinn Manual

Bagher Shamloo[1] | **Mahdi Hosseini**[2]✉

1. Department of Criminal Law and Criminology, Faculty of Law, Shahid Beheshti University, Tehran, Iran. Email: b_shamloo@sbu.ac.ir
2. Corresponding Author; Department of Criminal Law and Criminology, Faculty of Law, Shahid Beheshti University, Tehran, Iran. Email: Hosseini.mhdi@gmail.com

Article Info

Article Type:
Research Article

Received:
2024/06/05
Received in revised form:
2024/08/12
Accepted:
2024/10/04
Published online:
2024/12/21

Keywords:
Cyber war crime, disruptive cyber war, The Tallinn Manual, cyber armed conflict, Severity criterion.

Abstract

The increase of cyber wars has made the application of criminal war regulations on them inevitable, and this is while the said regulations have been established in accordance with traditional wars and it is challenging to apply these regulations to cyber wars. The aforementioned challenges are proportionately greater for disruptive warfare that does not create physical effects -versus destructive cyber warfare-. Based on this, how to determine the background element necessary for the occurrence of a war crime, that is, "occurrence of cyber armed conflict", is necessary and is the main question of this research. To answer this question, by collecting data through library sources, descriptive-analytical method is used in the research. The opinions of the opponents of the implementation of cyber armed conflict through disruptive cyber warfare are analyzed and answered. The Tallinn Manual as the most important non-binding international document for the application of international law regulations in the cyberspace, is the subject of a comparative study. The result of this research is that the emphasis of the Tallinn Manual on the necessity of creating physical effects as a result of cyber wars to fulfill the Severity criterion, causes the impunity of a large number of disruptive cyber wars whose effects are not necessarily less than destructive cyber wars. on this basis, it is suggested that, while emphasizing the criteria of the Tallinn Manual, the International Criminal Court to follow the severity criterion, regardless of the need to create physical effects, in line with modern approaches And to verify it, use the micro-indicators of scale, nature, method of committing, influence, disturbance in vital infrastructures and circumstances of committing.

How To Cite

Shamloo, Bagher; Hosseini, Mahdi (2024). Background element of cyber war crimes arising from disruptive cyber warfares in the light of The Tallinn Manual. *Comparative Law Review*, 15 (2), 601-636. DOI: https://doi.com/10.22059/jcl.2024.377469.634640

DOI

10.22059/jcl.2024.377469.634640

Publisher

The University of Tehran Press

شاپا الکترونیکی: ۳۴۰۴-۲۴۲۳

مطالعات حقوق تطبیقی

دوره: ۱۵، شماره: ۲
پاییز و زمستان ۱۴۰۳

Homepage: https://jcl.ut.ac.ir

University of Tehran Press

عنصر زمینه‌ای جنایات جنگی سایبری ناشی از رایاجنگ‌های مختل‌کننده در پرتو سند مقررات تالین

باقر شاملو[۱] | مهدی حسینی[۲]✉

۱. گروه حقوق جزا و جرم‌شناسی، دانشکدهٔ حقوق، دانشگاه شهید بهشتی، تهران، ایران.
رایانامه: b_shamloo@sbu.ac.ir

۲. نویسندهٔ مسئول؛ گروه حقوق جزا و جرم‌شناسی، دانشکدهٔ حقوق، دانشگاه شهید بهشتی، تهران، ایران.
رایانامه: Hosseini.mhdi@gmail.com

اطلاعات مقاله

نوع مقاله: پژوهشی

تاریخ دریافت:
۱۴۰۳/۰۳/۱۶

تاریخ بازنگری:
۱۴۰۳/۰۵/۲۲

تاریخ پذیرش:
۱۴۰۳/۰۷/۱۳

تاریخ انتشار برخط:
۱۴۰۳/۱۰/۰۱

کلیدواژه‌ها:
جنایت جنگی سایبری، رایاجنگ مختل‌کننده، سند مقررات تالین، مخاصمهٔ مسلحانهٔ سایبری، معیار شدت.

چکیده

افزایش رایاجنگ‌ها کاربست مقررات کیفریِ جنگ بر آنها را ناگزیر ساخته و این درحالی است که مقررات یادشده متناسب با جنگ‌های سنتی وضع شده‌اند و اعمال این مقررات بر رایاجنگ‌ها چالش‌برانگیز است. این چالش‌ها در تناسب با رایاجنگ‌های مختل‌کننده– که آثار فیزیکی ایجاد نمی‌کنند– در برابر رایاجنگ‌های تخریب‌گر، بیشتر است. بر این اساس، چگونگی احراز عنصر زمینه‌ای لازم برای وقوع جنایت جنگی، یعنی «وقوع مخاصمهٔ مسلحانهٔ سایبری»، ضروری است و پرسش اصلی این پژوهش است. برای پاسخ به این سؤال، با گردآوری داده‌ها از طریق منابع کتابخانه‌ای، از روش توصیفی–تحلیلی در پژوهش استفاده شده است. در این نوشتار دیدگاه‌های مخالفانِ تحقق مخاصمهٔ مسلحانهٔ سایبری از طریق رایاجنگ‌های مختل‌کننده، مورد واکاوی و پاسخ قرار می‌گیرد. سند مقررات تالین به‌عنوان مهم‌ترین سند بین‌المللی غیرالزام‌آور برای کاربست مقررات حقوق بین‌الملل در فضای سایبر، موضوع این مطالعهٔ تطبیقی است. برآمدِ این پژوهش آن است که تأکید سند مقررات تالین بر لزومِ ایجاد آثار فیزیکی در نتیجهٔ رایاجنگ‌ها برای تحقق معیار شدت، موجب بی‌کیفرمانیِ تعداد بسیاری از رایاجنگ‌های مختل‌کننده می‌شود که آثار آنها لزوماً کمتر از رایاجنگ‌های تخریب‌گر نیست و بر این اساس، پیشنهاد می‌شود که ضمن تأکید بر معیارهای سند مقررات تالین، دیوان کیفری بین‌المللی همسو با رویکردهای روزآمد، تفسیر معیار «شدت» را فارغ از لزومِ ایجاد آثار فیزیکی دنبال کند و برای احراز آن از ریزشاخص‌های مقیاس، ماهیت، روش ارتکاب، تأثیرگذاری، اختلال در زیرساخت‌های حیاتی و اوضاع و احوال ارتکاب استفاده نماید.

استناد

شاملو، باقر؛ حسینی، مهدی (۱۴۰۳). عنصر زمینه‌ای جنایات جنگی سایبری ناشی از رایاجنگ‌های مختل‌کننده در پرتو سند مقررات تالین. *مطالعات حقوق تطبیقی*، ۱۵ (۲)، ۶۰۱-۶۳۶.
DOI: https://doi.com/10.22059/jcl.2024.377469.634640

DOI 10.22059/jcl.2024.377469.634640

ناشر مؤسسه انتشارات دانشگاه تهران.

۱. مقدمه

همسو با تعداد فزایندهٔ رایاجنگ‌ها[۱]، 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 (عباسی و مرادی، ۱۳۹۴: ۳۹). رشد فزایندهٔ رایاجنگ‌ها تا آنجا پیش رفته که در سال ۲۰۲۳، خود دیوان کیفری بین‌المللی نیز مورد تهاجم واقع شده است[۲]. آنگاه که حملات در قامتِ جنگ‌های سایبری تجلی می‌یابند، نیازمند تنظیم‌گری شده، وضع محدودیت‌های حقوقی بر آنها ضروری می‌نماید؛ زیرا نادیده گرفتن واقعیت رایاجنگ‌ها، مشابه نادیده گرفتن تانک‌ها، بمب‌افکن‌ها و راکت‌های مورد استفاده به‌عنوان ابزارهای اصلی جنگ در طول جنگ جهانی دوم است (Scheffer, 2022). تنظیم‌گری حقوقی جنگ‌ها که در چارچوب حقوق بشردوستانه و حقوق مخاصمات مسلحانه انسجام می‌یابد، اساساً برای جنگ‌های فیزیکیِ سنتی وضع شده و کاربست آنها در ساختار و زمینهٔ رایاجنگ‌ها محل پرسش است.

تا سال ۲۰۲۳، هیچ موقعیتی مربوط به یک رایاجنگ مورد تجزیه و تحلیل دادستان کیفری بین‌المللی قرار نگرفته است؛ وانگهی در سال ۲۰۲۳، دادستان دیوان کیفری بین‌المللی در یک اظهار نظر مهم و مکتوب، به‌صراحت اعلام نمود، درحالی که هیچ ماده‌ای از اساسنامهٔ رم مشخصاً به حملات سایبری اختصاص ندارد، چنین رفتاری ممکن است به‌طور بالقوه عناصر بسیاری از جنایات بین‌المللی، همچون جنایات جنگی را که قبلاً تعریف شده است، برآورده کند (Khan, 2023) و دفتر دادستانی دیوان نیز آن را به‌عنوان موضع رسمی و کنونی دیوان کیفری بین‌المللی تأیید نمود (Greenberg, 2023). دادستان دیوان این مهم را با برگزاری «همایش رسیدگی به جرایم سایبری در چارچوب اساسنامهٔ رم» که با مشارکت فعال شرکت مایکروسافت برگزار می‌شد، در ابتدای سال ۲۰۲۴ آغاز نمود و در آن دادستان مجدداً بر نکتهٔ خود در خصوص قابلیت تعقیب حملات سایبری به‌عنوان جنایت جنگی در چارچوب اساسنامهٔ رم سخن گفت[۳]. در پرتو این راهبرد، پیش از عناصری که به‌طور خاص به جنایات جنگی ارتکاب‌یافته مربوط می‌شود، دادستان مکلف است وجود عنصر زمینه‌ایِ «وقوع مخاصمهٔ مسلحانه» برای ارتکاب جنایت را نیز ثابت کند (Saxon, 2016: 558). توضیح آنکه سند عناصر جنایات یادشده در اساسنامهٔ رم (Preparatory Commission for the International Criminal Court, 2000:

---

۱. «رایاجنگ» واژهٔ 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.

3. "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.

para. 18) در خصوص مادهٔ ۸ اساسنامهٔ رم، مقرر می‌دارد که «جنایت جنگی ضرورتاً در چارچوب و با مشارکت در یک مخاصمهٔ مسلحانه انجام می‌شود». از سوی دیگر، جنایت جنگی در یک وجه، نقض حقوق بشردوستانهٔ بین‌المللی دانسته شده و پیش‌شرط قابلیت اجرای قواعد حقوق بشردوستانهٔ بین‌المللی نیز وجود یک مخاصمهٔ مسلحانه است (برادران و حبیبی، ۱۳۹۸: ۱۴۳). بر این اساس، بررسی آستانهٔ شدت وصول به مخاصمهٔ مسلحانهٔ سایبری، موضوعی مهم است که متفاوت با مفهوم آستانهٔ شدت یادشده در بند نخست مادهٔ ۱۷ اساسنامهٔ رم به‌عنوان شاخص قابلیت پذیرش دعوا نزد دیوان کیفری بین‌المللی (صابر و صادقی، ۱۳۹۴: ۶۲۸) بوده، در این پژوهش مورد بررسی است.

به‌منظور بررسی امکان «عنصر زمینه‌ایِ وقوع جنایت جنگی سایبری ناشی از رایاجنگ‌های مختل‌کننده»، یعنی مخاصمهٔ مسلحانهٔ سایبری ناشی از رایاجنگ‌های مختل‌کننده، می‌بایست میان عملیات سایبری که آثار فیزیکی مشابه جنگ‌های سنتی ایجاد می‌کنند و عملیاتی که فقط تأثیرات غیرفیزیکی (تخریب داده‌ها یا اختلال در برنامه‌های رایانه‌ای) را موجب می‌شوند، تمایز قائل شد. بر اساس نظر اکثر صاحب‌نظران، عملیات سایبری که به خسارت فیزیکی یا جراحت منجر می‌شوند، توسل به زور تلقی می‌گردند (Schmitt, 2011: 573; Schmitt, 1999: 17; Joyner, Lotrionte, 2001: 850; Creekman, 2001: 166; Silver, 2002: 85; Duncan, 2008: 7; Hoisington, 2009: 447; Kerschischnig, 2012: 135; Dinniss, 2012: 74; Schmitt (A), 2013: 48; Radziwill, 2015: 131) و موجدِ مخاصمهٔ مسلحانه دانسته می‌شوند. برعکس، احتساب عملیات سایبری بدون آثار فیزیکی- که صرفاً ایجاد اختلال می‌نمایند- به‌عنوان توسل به زور سایبری و ایجادگرِ مخاصمهٔ مسلحانهٔ سایبری، محل بحث بیشتر واقع شده، دارای مخالفان جدی است (Barkham, 2001: 84-85; Lin, 2010: 73)؛ هرچند برخی دیگر تحت شرایط خاصی، از چنین نظری حمایت می‌کنند (Hoisington, 2009: 447; Silver, 2002: 85; Schmitt, 1999: 913). این در حالی است که عملیات سایبری که فقط آثار غیرفیزیکی ایجاد می‌کنند، قادر به ایجاد تأثیرات در مقیاس بزرگ نیز هستند (Lin, 2010: 74) و می‌توانند دارای پیامدهای مستقیم یا غیرمستقیمِ مخاطره‌آمیز برای بقای دولت مورد هدف باشند.

منظور از عملیات سایبری مختل‌کننده[1]، اقداماتی است که «جریان اطلاعات یا عملکرد سیستم‌های اطلاعاتی را بدون ایجاد آسیب یا خسارت فیزیکی، قطع می‌کنند» (Brown, Tullos, 2012). اگر از این عملیات 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» (Kilovaty, 2016: 116). استدلال می‌شود که عملیات سایبری مختل‌کننده این قابلیت را دارند که بحران‌آفرین

1. disruptive cyber operations (DCOs).

باشند، زیرا هرچه بیشتر زندگی ما به صورت آنلاین پیش می‌رود، عملیات سایبری مختل‌کننده به یک حوزهٔ مهم از استراتژی نظامی تبدیل خواهند شد. با این توضیح، این پژوهش می‌کوشد که به این پرسش پیچیده و بحث‌برانگیز (Schmitt, 2013 (A): 56) پاسخ دهد که آیا به سبب وقوع رایاجنگ‌های مختل‌کننده، امکان وقوع مخاصمهٔ مسلحانهٔ سایبری به‌عنوان مهم‌ترین عنصر عمومی و زمینه‌ای برای وقوع جنایات جنگی سایبری وجود دارد یا خیر؟ برای این منظور، ضمن شناسایی آثار ناشی از رایاجنگ‌های مختل‌کننده برای تبیین اهمیت آنها، آستانهٔ وقوع مخاصمهٔ مسلحانهٔ بین‌المللی مورد واکاوی قرار می‌گیرد و سپس با واکاوی نظر مخالفانِ تحقق مخاصمهٔ مسلحانهٔ سایبری از طریق رایاجنگ‌های مختل‌کننده و پاسخ به هریک از آنها، رویکرد سند مقررات تالین به‌عنوان مهم‌ترین سند بین‌المللی غیرالزام‌آور در خصوص کاربست مقررات حقوق بین‌الملل در فضای سایبر، به آستانهٔ وقوع مخاصمهٔ مسلحانه از رهگذرِ رایاجنگ‌ها، بررسی و تحلیل انتقادی می‌شود. در نهایت، کاربرد ریزشاخص‌هایی جهت سنجش دقیق‌تر معیار «شدت»، تحقق توسل به زور از رهگذرِ رایاجنگ‌های مختل‌کنندهٔ شدید، اتخاذ رویکردی پویا و آستانهٔ مطلوبِ عنصر زمینه‌ایِ یادشده، به دیوان کیفری بین‌المللی پیشنهاد می‌شود.

۲. آثار ناشی از رایاجنگ‌های مختل‌کننده

برخی از آثار ایجادشده از سوی رایاجنگ‌های مختل‌کننده نشان می‌دهند که چگونه می‌توان از عملیات سایبری مختل‌کننده که مانند حملات سنتی یا برخی دیگر از عملیات سایبری، آثار فیزیکی ایجاد نمی‌کنند، برای ایجاد اختلال در زیرساخت‌های اطلاعاتی ملی، زیرساخت‌های حیاتی ملی و زیست خصوصی شهروندان استفاده کرد و مانع از ارائهٔ خدمات ضروری، جلوگیری از دسترسی غیرنظامیان به نیازهای اساسی و مداخله در حقوق اساسی بشر شد. بنابراین، در صورت سوءاستفاده در چارچوب یک مخاصمهٔ مسلحانه، عملیات سایبری مختل‌کننده می‌توانند منجر به یک بحران بشردوستانهٔ جدی شوند.

۲. ۱. اختلال در زیرساخت‌های اطلاعاتی ملی

چندین رویداد در چند دههٔ گذشته نشان داده است که تداخل در عملکرد زیرساخت‌های اطلاعاتی ملی می‌تواند تهدیدی جدی برای شهروندان غیرنظامی باشد. به ترتیب در سال‌های ۲۰۰۷ و ۲۰۰۸، استونی و گرجستان هر دو متحمل حملات سایبری تهاجمی DDoS[1] شدند که وب‌سایت‌های دولتی آنها ازبین رفت (Miller, 2014: 222-224). در مورد اولی، خطوط ارتباط اضطراری برای مدت کوتاهی از دسترس خارج

1. Distributed Denial of Service.

شد (Bussolati, 2015: 102). ممکن است حملات DDoS به گرجستان و استونی در مقایسه با تخریب‌هایی که می‌تواند از طریق روش‌های جنگی متعارف ایجاد شود، نسبتاً بی‌اهمیت به‌نظر برسد، ولی برخی معتقدند که عملیات سایبری لزوماً و حتماً در گذر زمان پیچیده‌تر می‌شوند و می‌توانند عواقبی بحران‌آفرین را در آینده ایجاد کنند (Ophardt, 2010 :10). قبلاً نیز چندین حملهٔ سایبری زیرساخت‌های اطلاعاتی دولت و به‌ویژه زیرساخت‌های مربوط به بهداشت و درمان را هدف قرار داده بودند که درنتیجه جمعیت شهروندان غیرنظامی در معرض خطر واقع شدند. برای مثال، حملهٔ باج‌افزار واناکرای[1] در سال ۲۰۱۷، تأثیر شدیدی بر خدمات درمانی ملی انگلستان[2] گذاشت. گزارش شده است که شیوع واناکرای «تنها در انگلستان کامپیوترها را در بیش از ۸۰ سازمان خدمات درمانی ملی خاموش کرد و به لغو تقریباً ۲۰۰۰۰ وقت ویزیت منجر شد، ۶۰۰ جراح مجبور به بازگشت به قلم و کاغذ شدند و در پنج بیمارستان، آمبولانس‌ها از مسیر اصلی منحرف شدند و بیمارستان‌ها قادر به رسیدگی به هیچ مورد اضطراری دیگر نبودند» (Hern, 2017). به‌عنوان یک نمونهٔ جدیدتر، 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. این دسته از عملیات، داده‌های پزشکی بیمار را در معرض خطر قرار داده، مانع از انتشار اطلاعات بااهمیت برای مردم شده و «مستقیماً در ارائهٔ مراقبت‌ها، تدارکات پزشکی و تحقیقات لازم برای مبارزهٔ مؤثر با ویروس و گسترش آن، مداخله داشته است» (Milanovic, Schmitt, 2020: 1).

۲. ۲. اختلال در زیرساخت‌های حیاتی ملی

نمونه‌های دیگر از عملیات سایبری مختل‌کننده که زیرساخت‌های حیاتی ملی را هدف قرار داده‌اند، عبارت‌اند از: حمله به شبکهٔ برق اوکراین در دسامبر ۲۰۱۵ و حمله به یک نیروگاه هسته‌ای در هند در سپتامبر ۲۰۱۹. چنانچه ذکر شد، در مورد اول، مهاجمان باعث قطعی برق بین یک تا شش‌ساعتهٔ نواحی آسیب‌دیده در این کشور شدند و آنها را به‌گونه‌ای تحت تأثیر قرار دادند که نتوانند به فرمان‌های از راه دورِ اپراتورها پاسخ دهند و موجب شدند تا ماه‌ها، کارگران موج‌شکن‌ها را به‌صورت دستی کنترل کنند (Zetter, 2016). در مورد دوم، هیچ نشانه‌ای مبنی بر به‌خطر افتادن کنترل و بهره‌برداری از نیروگاه وجود نداشت[3] و در عوض، هدف جمع‌آوری اطلاعات به‌نظر می‌رسید (Porup, 2019). در هر دو مورد- برخلاف حملات

1. WannaCry.
2. UK's National Health Service (NHS).
3. 'Assessment of Reported Malware Infection at Nuclear Facility', Dragos, 1 November 2019, available in: https://www.dragos.com/blog/industry-news/assessment-of-reportedmalware-infection-at-nuclear-facility/.

استاکس نت[1] در سال ۲۰۱۰– هیچ آسیب فیزیکی به تجهیزات وارد نشد؛ اما با وجود این، عملیات یادشده باعث اختلال در زیرساخت‌های حیاتی دولت‌های مورد هدف گردید. حملاتی از این دست از نظر فراوانی و شدت افزایش می‌یابند، زیرا زیرساخت‌های حیاتی ملی بیشتر و بیشتر به صورت‌های آنلاین منتقل می‌شوند و وابستگی آنها روزبه‌روز به فناوری اطلاعات و بستر آنلاین افزوده می‌شود.

۲. ۳. اختلال در زیست خصوصی شهروندان

تنها زیرساخت‌های دولتی نیستند که ممکن است مورد هدف قرار گیرند، عملیات سایبری مختل‌کننده دارای قابلیت تأثیرگذاری بر زیست شهروندان غیرنظامی در سطح شخصی نیز هستند. کمیتهٔ بین‌المللی صلیب سرخ[2] در گزارش خود در خصوص هزینهٔ انسانی عملیات سایبری اشاره کرد که رشد تصاعدی فضای سایبر از طریق اینترنت اشیا یا IoT (Morgan, 2014)، فرصت‌های حملات سایبری را افزایش داده است. این گزارش هشدار می‌دهد که «هر دستگاه متصل می‌تواند به هدف یا بخشی از یک عملیات سایبری تهاجمی تبدیل شود (مثلاً یک ربات در یک روبوشبکه[3]) و این دیگر صرفاً بهره‌برداری از آسیب‌پذیری‌های سیستم‌عامل نیست. اکنون، دستگاه‌هایی مانند ضربان‌ساز و اتومبیل‌ها تا حدودی به هم متصل می‌شوند» (Gisel & Olejnik, 2019: 14-15). بر این اساس، فارغ از خرابکاری فیزیکی، خطر تداخل حتی موقت با سیستم‌عامل دستگاه‌هایی مانند ضربان‌ساز و خودروها وجود دارد که می‌تواند بحران‌های اجتماعی را سبب شود.

عملیات سایبری مختل‌کننده همچنین می‌توانند برای دسترسی به داده‌های شخصی یا دستکاری آن و تضعیف حق بر حریم خصوصی استفاده شوند. اشاره شده است که در دنیای دیجیتال امروز، «اقدام به حمله به حیثیت شخص، پاک کردن هویت، تحقیر کردن و ازبین بردن دفاع انسانی را می‌توان به‌صورت الکترونیکی انجام داد تا فیزیکی» (Lubin, 2021: 3). همچنین می‌توان تصور کرد که چگونه می‌شود از داده‌های شخصی در چارچوب یک مخاصمهٔ مسلحانه بهره‌برداری کرد: «یک بازجوی نظامی را در حال جمع‌آوری اطلاعات از نمایه‌های آنلاینِ زندانی، تلفن فیزیکی و داده‌های ذخیره‌شده در فضای ابری تصویر کنید که می‌تواند برای عذاب، تحقیر و شرمسار کردن زندانی کافی باشد» (Lubin, 2021: 4).

---

1. Stuxnet.
2. International Committee of the Red Cross (ICRC).
۳. botnet که با ترکیبی از کلمات "robot" و "network" به‌وجود آمده است، شبکه‌هایی هستند که با دراختیار گرفتن مجموعه‌ای از کامپیوترها که بات (bot) نامیده می‌شوند، تشکیل می‌شوند. این شبکه‌ها از سوی یک یا چند مهاجم که botmasters نامیده می‌شوند با هدف انجام فعالیت‌های مخرب کنترل می‌گردند. به عبارت بهتر، ربات‌ها کدهای مخربی هستند که بر روی کامپیوترهای میزبان اجرا می‌شوند تا امکان کنترل آنها را از راه دور برای botmaster ها فراهم نمایند و آنها بتوانند این مجموعه را وادار به انجام فعالیت‌های مختلف کنند.

۳. آستانهٔ وقوع مخاصمهٔ مسلحانهٔ بین‌المللی به‌عنوان عنصر زمینه‌ای جنایات جنگی

حسب رأی دادگاه کیفری بین‌المللی برای یوگسلاوی سابق[1] در قضیهٔ *تادیچ*[2] 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...» (ICTY Rep, 1995: 70). با توجه به اینکه تاکنون 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 و هر تلاشی برای قاعده‌بخشی به رایاجنگ‌ها «در معرض عدم قطعیت، مجادله، عدم شفافیت و عدم تأییدپذیری» بوده است (Waxman, 2011: 443)، بحث‌های این پژوهش نیز نظری و مبتنی بر رویهٔ فعلی حقوق بین‌الملل در خصوص عملیات سایبری است.

دادگاه بین‌المللی دادگستری و منشور سازمان ملل متحد آستانهٔ «زور» ممنوع‌شده در بند ۴ مادهٔ ۲ منشور ملل متحد را مشخص نکرده‌اند. آستانه‌ای که تا آن میزان توسل به زور با ممنوعیت مندرج در بند ۴ مادهٔ ۲ مغایرت ندارد، از سوی پژوهشگرانی استنباط شده است که رویهٔ دولت‌ها را از زمان تصویب منشور سازمان ملل متحد، تجزیه و تحلیل کرده‌اند (Corten, 2012: 52-92). وجود چنین آستانه‌ای از چندین پرونده استنباط شده که در آنها توسل به زور با شدت کم به‌عنوان توسل به زور از سوی 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 (ICJ Rep, 1949: 35). برخی از محققان این رویکرد را به‌عنوان استدلالی برای حمایت از وجود آستانه تحلیل می‌کنند (O'Connell, 2013: 102-105). این مجادلهٔ نظری در کمیسیون حقیقت‌یاب بین‌المللی در خصوص جنگ علیه گرجستان نیز مطرح و این‌گونه بیان شد: «ممنوعیت توسل به زور تمامی زور مادی را که از حداقل آستانهٔ شدت فراتر می‌رود، شامل می‌شود» (Max Planck Institute for Comparative Public Law and International Law, 2009: 242). در مقابل، برخی دیگر از محققان ادعا می‌کنند که چنین آستانه‌ای وجود ندارد و مستثنی شدن «توسل‌های حداقلی به زور» از محدودهٔ بند ۴ مادهٔ ۲ را رد می‌کنند (Ruys, 2014: 159-210; Hoogh, 2009).

اگر هر قضیه‌ای جداگانه درنظر گرفته شود، ممکن است تعیین وجود آستانه دشوار باشد؛ وانگهی اگر همهٔ قضایا و پرونده‌ها با هم درنظر گرفته شوند، ممکن است مبانی کافی را برای تعیین آستانه فراهم کنند. نمونه‌های قانع‌کننده‌تر از وجود آستانه را می‌توان خارج از رویهٔ قضایی دیوان بین‌المللی دادگستری

1. International Criminal Tribunal for the former Yugoslavia (ICTY).
2. Tadic´.

و آن‌گونه که برخی از محققان (Corten, 2012: 52-92; O'Connell, 2013: 102-107) برای دفاع از وجودِ آستانهٔ مخاصمهٔ مسلحانه به آن اشاره کرده‌اند، یافت.

در خصوص راه تعیین آستانهٔ وقوع مخاصمهٔ مسلحانه و توسل به زور در رایاجنگ‌ها، نظریات مختلفی مطرح شده است. در ادبیات نظری مشهور، سه رویکرد اصلی را می‌توان در این راستا شناسایی نمود: رویکرد مبتنی بر هدف، رویکرد مبتنی بر ابزار یا روش، و رویکرد مبتنی بر پیامد یا اثر (Ambos, 2015: 122; Droege, 2012: 533-546). رویکردهای سه‌گانهٔ پیش‌گفته مبتنی بر هنجارهای معاهداتی و چارچوب‌های قانونی فعلی هستند که منع توسل به زور را مقرر می‌نمایند. تحلیل تحقق مخاصمهٔ مسلحانه از منظر هریک از روش‌های یادشده، واجد آثار متفاوت است که ذیل معیارهای مورد پیشنهاد برای تحقق مخاصمهٔ مسلحانه از سوی رایاجنگ‌های مختل‌کننده، مورد استفاده قرار خواهند گرفت.

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 (Roscini, 2014: 55).

یک روش خلاقانه در سال ۲۰۲۱ از سوی محققان پروژهٔ آکسفورد در خصوص حمایت‌های حقوق بین‌الملل در فضای سایبر ارائه شد (Akande & Hollis, 2020)[1]. 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 (Hollis & Benthem, 2021) و این همان رویکردی است که در ادامهٔ این پژوهش در خصوص رایاجنگ‌های مختل‌کننده، دربارهٔ آن بحث می‌شود و از شیوهٔ سند مقررات تالین تبعیت نمی‌نماید.

۴. چالش‌های تحقق مخاصمهٔ مسلحانهٔ سایبری از رهگذرِ رایاجنگ‌های مختل‌کننده

تلقیِ رایاجنگ‌های مختل‌کنندهٔ بدون آثار فیزیکی به‌عنوان توسل به زور سایبری و ایجادگرِ مخاصمهٔ مسلحانهٔ سایبری، دارای مخالفان جدی است که در این قسمت، مورد به مورد، ضمن بیان چالش‌های

---

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

مدنظر مخالفان، تلاش می‌شود تا پاسخ به هریک از آنها نیز تبیین گردد. البته لازم به ذکر است که این موضوع همچنان محل اختلاف است و اعضای شورای مشاوران[1] نیز در خصوص تحقق توسل به زور از طریق رایاجنگ‌های مختل‌کننده، با نشان دادن عدم توافق فعلی، به جمع‌بندی برای ارائهٔ راهبرد مشخص نرسیده و دیدگاه‌های متعددی را ارائه‌کرده‌اند (Permanent Mission of Liechtenstein to the United Nations, 2021: 13-14). برخی از مشاوران بر این نظر بوده‌اند که ناتوانی یا ازدست دادن عملکرد بدون تخریب فیزیکی نیز می‌تواند برای تحقق «نقض آشکار» کافی باشد (Hathaway, 2022)؛ در هر حال، همچنان اختلافات قابل‌توجهی میان کارشناسان در این زمینه وجود دارد.

۴. ۱. دشواری تفکیک رایاجنگ‌های مختل‌کننده از اجبار اقتصادی یا سیاسی

یکی از دلایل مخالفت با تلقیِ رایاجنگ‌های مختل‌کننده به‌عنوان توسل به زورِ موجدِ مخاصمهٔ مسلحانه، این نگرانی است که در این صورت، امکان نظریِ تفکیک میان رایاجنگ‌های مختل‌کننده از گونه‌های مختلف اجبار اقتصادی یا سیاسی دشوار خواهد بود (Barkham, 2001: 84). به عبارت بهتر، مبتنی بر این نظر، درحالی که مقدمات تدوین منشور ملل متحد حاکی از آن است که اجبار اقتصادی یا سیاسی را نمی‌توان به‌عنوان توسل به زور تلقی نمود، تلقیِ رایاجنگ‌های مختل‌کننده به‌عنوان توسل به زور را می‌توان گونه‌ای راهبرد دوگانه نسبت به دو موضوع با ماهیت مشابه دانست؛ زیرا رایاجنگ‌های مختل‌کننده نیز همچون اجبار اقتصادی یا سیاسی موجدِ آثار فیزیکی نیستند و بر این اساس، امکان تفکیک میان این دو ماهیت برای تلقیِ برخی به‌عنوان توسل به زور و عدم تلقیِ برخی دیگر، دشوار خواهد بود.

در پاسخ باید گفت که اولاً تلقیِ دشواری در تفکیک میان دو ماهیت یادشده به‌سبب توجهِ صرف به آثار و نتایج هریک از آنها و عدم توجه به معیارهای دیگر برای وصول به آستانهٔ مخاصمهٔ مسلحانه وجود دارد. معیارهای چندگانه‌ای که برای تشخیص توسل به زور از اجبار اقتصادی یا سیاسی در رایاجنگ‌ها مورد پیشنهاد قرار گرفته است، دقیقاً احتراز از توجهِ صرف به نتیجهٔ رایاجنگ‌ها را پی می‌گیرد. مبتنی بر این نظر که در سند مقررات تالین بر آن تکیه شده است و در گفتار بعدی نیز تشریح خواهد شد، برای ارزیابی یک عملیات سایبری به‌عنوان توسل به زور، به‌جای توجهِ صرف بر آثار رایاجنگ‌ها که شائبهٔ تداخل آنها با اجبار اقتصادی یا سیاسی را ایجاد می‌کند، معیارهای هشت‌گانه‌ای پیشنهاد می‌شوند. پژوهشگران مختلف

---

۱. گزارش شورای مشاوران سازمان ملل متحد دربارهٔ امکان‌سنجی اعمال اساسنامهٔ رم دادگاه کیفری بین‌المللی در جنگ‌های سایبری است. این گزارش بر اساس نشست‌های گروهی شامل پانزده وکیل بین‌المللی، سه کارشناس فنی، یک نماینده از کمیتهٔ بین‌المللی صلیب سرخ و یک نماینده از دفتر دادستانی دیوان کیفری بین‌المللی در ماه‌های اکتبر و دسامبر سال ۲۰۱۹ و ژانویهٔ سال ۲۰۲۰ تنظیم شده است.

معیارهای یادشده را شرح داده‌اند (محقق هرچقان و همکاران، ۱۴۰۱، ۲۸۹-۲۸۷) و برخی دیگر از پژوهشگران نیز این معیارها را برای تعیین آستانهٔ توسل به زور، مفید دانسته‌اند (Trahan, 2022: 138).

از سوی دیگر، چنانچه برخی از پژوهشگران نیز اشاره کرده‌اند (Sharp, 1999: 86)، می‌توان اظهار داشت که هرچند بند ۴ مادهٔ ۲ منشور ملل متحد شامل آن دسته از اجبارهای اقتصادی یا سیاسی نیست که با هدف تأثیرگذاری بر سیاست‌ها یا اقدامات یک کشور دیگر اعمال می‌شوند، لکن می‌توان آن را شامل آن دسته از اجبارهای سیاسی یا اقتصادی دانست که شدت آنها موجب تهدید تمامیت ارضی یا استقلال کشور دیگر خواهد شد. بر این اساس، تفکیک رایاجنگ‌های مختل‌کننده از اجبار اقتصادی یا سیاسی لزوماً غیرممکن نیست. مبتنی بر همین رویکرد، گفته شده است (Sharp, 1999: 117)، بعضی از رایاجنگ‌های مختل‌کنندهٔ نظام اقتصادی کشور، همچون حملات سایبری مختل‌کنندهٔ طولانی‌مدتِ بورس نیویورک، ممکن است تا سطح یک حملهٔ مسلحانه نیز برسند.

برخی از مخالفانِ تلقیِ رایاجنگ‌های مختل‌کننده به‌عنوان توسل به زور نیز در شرایط خاص، تحقق مخاصمهٔ مسلحانه از طریق رایاجنگ‌های مختل‌کننده را ممکن می‌دانند. برای مثال، گفته شده که ممکن است آن دسته از رایاجنگ‌های مختل‌کننده که سبب ایجاد بحران‌های اقتصادی نابودگر نظام اقتصادی برای کشورهای هدف می‌شوند، موجد مخاصمهٔ مسلحانه تلقی شوند (Silver, 2002: 86-91). برای نمونه، اگر کشوری از ابزارهای فیزیکی غیرنظامی همچون اعزام مأموران اطلاعاتی به کشور هدف برای قطع کابل فیبر نوری کشور هدف، استفاده کند که اطلاعات مالی ضروری و ملی آن کشور بر روی آن مخابره می‌شود، دور است که بتوان در تلقیِ آن به‌عنوان توسل به زور تردید نمود. با این رویکرد، درصورتی که یک کشور برای ایجاد همان سطح از اختلال مالی ملی در کشور هدف از طریق رایاجنگ‌های مختل‌کننده همچون جعل سفارش‌های تجاری در مقیاس بزرگ یا انتشار گستردهٔ اطلاعات نادرست مالی استفاده نماید، می‌توان وصول به آستانهٔ توسل به زور را محقق دانست.

۴. ۲. وجود فاصلهٔ زمانی میان وقوع رایاجنگ‌های مختل‌کننده تا ایجاد آثار

دلیل دیگر برای تلقیِ رایاجنگ‌های مختل‌کننده به‌عنوان توسل به زور را وجود فاصلهٔ زمانی بین ارتکاب رفتار تا ایجاد نتیجه دانسته‌اند (Barkham, 2001: 86; Silver, 2002: 84). مبتنی بر این نظر، اگر زمان لازم برای ایجاد آثار جهت تلقیِ یک رفتار به‌عنوان توسل به زور افزایش داده شود، احتمالاً بسیاری از اجبارها و تحریم‌های اقتصادی و بسیاری دیگر از گونه‌های سلاح‌ها نیز می‌توانند در دامنهٔ آن قرار گیرند؛ زیرا در طولانی‌مدت بسیاری از زیرساخت‌های کشور را تحت تأثیر قرار می‌دهند و در این صورت راهی برای مستثنی کردنِ آنها از توسل به زور وجود نخواهد داشت. برای مثال، سلاح‌های بیولوژیکی نیز همیشه

موجب آثار فوری نمی‌شوند؛ به‌ویژه اگر بیماری گسترش یافته، دارای دورهٔ نهفتگی طولانی‌مدت باشد و این درحالی است که هیچ‌گاه نمی‌توان این‌گونه سلاح‌ها را توسل به زور تلقی نمود (Barkham, 2001: 87).

در پاسخ به دیدگاه پیش‌گفته باید گفت که اولاً تأخیر در ایجاد آثار به رایاجنگ‌های مختل‌کننده محدود نیست و رایاجنگ‌های تخریب‌گر نیز ممکن است با تأخیر زمانی سبب ایجاد آثار فیزیکی شوند و این درحالی است که تأخیر در ایجاد آثار در خصوص رایاجنگ‌های تخریب‌گر به‌عنوان عاملی برای عدم احتساب به‌عنوان توسل به زور دانسته نشده است. ثانیاً برخی از پژوهشگران (Schmitt, 1999: 913; Brownlie, 1963: 362) قائل به امکان تلقیِ استفاده از سلاح‌های شیمیایی و بیولوژیک به‌عنوان توسل به زور هستند و ثالثاً علت عدم احتساب سلاح‌های شیمیایی و بیولوژیک به‌عنوان توسل به زور را نباید در تأخیر آنها در ایجاد آثار دانست و مخالفت‌ها در پذیرش چنین سلاح‌هایی به‌عنوان توسل به زور بیشتر معطوف به ماهیت غیرنظامی آنها بوده است که در تلقیِ آنها به‌عنوان «سلاح» تشکیک می‌شده است. توضیح آنکه در خصوص تعریف «زور» که توسل به آن منع شده است، اتفاق نظر وجود ندارد. برخی از محققان از تفسیر وسیع مفهوم زور طرف‌داری می‌کنند (Olivier, 2012: 52) و گفته شده است که «ممانعت از به‌کارگیری زور بین‌دولتی محدود به جلوگیری از کاربرد تسلیحات شیمیایی، بیولوژیکی یا هسته‌ای نیست و جای تردید نیست که عملیات سایبری نیز قابل تطبیق با سلاح‌های دیگر هستند» (عباسی، مرادی، ۱۳۹۴: ۵۶). دیوان بین‌المللی دادگستری در نظر مشورتی خود در پروندهٔ *سلاح‌های هسته‌ای*، اشاره کرد که این ممنوعیت «در خصوص هرگونه استفاده از زور، صرف‌نظر از سلاح‌های به‌کاررفته، اعمال می‌شود» (ICJ Reports, 1996: 39)[1]. بنابراین، به‌نظر می‌رسد که ضرورتی وجود ندارد که تسلیحات مورد استفاده لزوماً دارای آثار انفجاری بوده یا برای اهداف تهاجمی ساخته شده باشد (فقیه حبیبی، ۱۳۹۵: ۱۲۸). هرچند واضح است که مفهوم زور هر نوع از زور را دربر نمی‌گیرد (Kelsen, 2001: 57)، لکن نمی‌توان عبارت «سلاح» را به سبب تأخیر در ایجاد آثار، محدود به سلاح‌های سنتی و غیرمدرن دانست و حقوق بشردوستانهٔ بین‌المللی را صرفاً در محدودهٔ استفاده از سلاح‌های سنتی، جاری نمود. در این صورت، توسل به سلاح‌های اتمی، زیستی و همهٔ سلاح‌های مدرن، مانند سلاح‌های سایبری، با چالش مواجه شده، مخاطره‌ای جدی برای حیات بشری محسوب خواهد شد.

---

۱. تصریح دیوان بین‌المللی دادگستری در این خصوص شایان توجه است:

"These provisions do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed. The Charter neither expressly prohibits, nor permits, the use of any specific weapon, including nuclear weapons. A weapon that is already unlawful per se, whether by treaty or custom, does not become lawful by reason of its being used for a legitimate purpose under the Charter".

۴. ۳. چالش تحقق توسل به زور با ایجاد اختلال در داده‌های رایانه‌ای

این نظر بر آن است که با توجه به عدم وجود خشونت در هنگام اختلال در داده‌های رایانه‌ای در نتیجهٔ ارتکاب یک رایاجنگ مختل‌کننده، حتی اگر اختلال در داده‌ها را بتوان دارای آثار اقتصادی مشابهی با تخریب یک کارخانهٔ بزرگ ارزیابی کرد، نمی‌توان آن را به‌عنوان توسل به زور تلقی نمود (Barkham, 2001: 88). مبتنی بر این رویکرد و بر اساس تحلیل سنتی از مفهوم «زور» در بند مادهٔ ۴ منشور ملل متحد- که شرح آن در قسمت پیشین گذشت- به این سبب که هنگام اختلال در داده‌های رایانه‌ای هیچ سلاحی استفاده نمی‌شود و هیچ مالی ازبین نمی‌رود، نمی‌توان اختلال در داده‌های رایانه‌ای ناشی از رایاجنگ‌های مختل‌کننده را به‌عنوان توسل به زور دانست (Bond, 1996: 95-96).

در پاسخ باید گفت که فارغ از بحث‌های پیشینِ مربوط به عدم محدودیت مفهوم «زور» به زور مسلحانهٔ نظامی و امکان شمول مفهوم «زور» بر انواع رایاجنگ‌ها، با توجه به اینکه پیشرفت‌های فناورانه موجب افزایش جدی اهمیت راهبردی صنعت اطلاعات و داده‌ها شده است، معادل‌سازیِ داده‌های رایانه‌ای با دارایی‌ها و اموال، دارای موافقان جدی است (Schmitt, 1998: 1063)[1]. بر این اساس، دلایل پیش‌گفته برای عدم شمول اختلال در داده‌ها ذیل مفهوم توسل به زور را نمی‌توان موجه دانست. یک عملیات سایبری مختل‌کننده که زیرساخت‌های حیاتی ملی را غیرفعال می‌کند، می‌تواند به همان اندازه خشونت‌آمیز باشد که یک رایاجنگ منجر به تخریب فیزیکی خشونت‌آمیز است.

برخی از پژوهشگران وجه شمول اختلال در داده‌ها از طریق رایاجنگ‌ها ذیل مفهوم توسل به زور را از این منظر دانسته‌اند که اختلال در داده‌های رایانه‌ای، همچون داده‌های ماهواره‌ای، می‌تواند موجب ضربه به امنیت ملی و تضعیف دولت هدف برای استفاده‌های آتی مهاجم شود و از این منظر مفهوم توسل به زور را شامل رایاجنگ‌های مختل‌کنندهٔ داده‌های رایانه‌ای نیز می‌دانند (Bond, 1996: 88-93). البته ممکن است گفته شود که حقوق بین‌الملل هر اقدامی را که موجب اثرگذاری بر امنیت کشور دیگر شود، توسل به زور تلقی نمی‌کند (Barkham, 2001: 94) که صحت آن روشن است؛ لکن در رویکرد اخیر، ایجاد بحران ملی و تضعیف دولت هدف برای حملات آتی مهاجم از طریق رایاجنگ‌های مختل‌کننده، در کنار سایر عوامل و شاخص‌های تحقق توسل به زور است که موجب احتساب آن به‌عنوان توسل به زور می‌شود که شرح معیارهای پیشنهادی جهت تحقق توسل به زور مسلحانهٔ سایبری از طریق رایاجنگ‌های مختل‌کننده خواهد گذشت.

---

۱. کمیتهٔ بین‌المللی صلیب سرخ «داده‌های غیرنظامی» را به‌عنوان «اشیای غیرنظامی» و تحت حمایت حقوق بشردوستانهٔ بین‌المللی تلقی می‌نماید (Horowitz, 2020: 54). برای مطالعهٔ اختلاف نظرهای موجود در خصوص اینکه آیا داده‌ها باید تحت حمایت حقوق بشردوستانهٔ بین‌المللی و به‌عنوان «شیء» درنظر گرفته شوند یا خیر، قابل ملاحظه است:

Biller J.T. & Schmitt M.N. (2019). Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare: *International Law Studies*, 95, p. 181.

۴. ۴. افزایش ارتکاب توسل به زور در سطح بین‌المللی

یکی از ادلهٔ مخالفت با تلقیِ رایاجنگ‌های مختل‌کننده به‌عنوان توسل به زور، آن است که در صورت گسترش مفهوم آن به رایاجنگ‌های مختل‌کننده، به آن سبب که در راستای گسترش استفاده از فناوری اطلاعات به‌عنوان یکی از حوزه‌های جنگ، بسیاری از کشورها چنین اقداماتی را به‌عنوان بخشی از برنامهٔ دفاعی خود درنظر گرفته‌اند، نقض ممنوعیت توسل به زور به‌عنوان یک اقدام متخلفانهٔ بین‌المللی گسترش پیدا خواهد کرد و می‌تواند دامنهٔ تنش‌های بین‌المللی را افزایش دهد (Barkham, 2001: 94-95; Silver, 2002: 86). بر اساس این نظر، «در صورت توسل به این رویکرد، صلح به‌صورت چشم‌گیری در معرض خطر قرار خواهد گرفت» (شایگان و صفوی کوهساره، ۱۳۹۷: ۴۲۳).

نظر مصلحت‌سنجانهٔ پیش‌گفته را نمی‌توان مانع قانونی برای تلقیِ رایاجنگ‌های مختل‌کننده به‌عنوان توسل به زور تصور نمود. توضیح آنکه هرچند تا امروز در خصوص معیار توسل به زور سایبری، حتی نسبت به رایاجنگ‌های تخریب‌گر، اجماعی وجود ندارد (شریفی طرازکوهی و برمکی، ۱۳۹۹: ۱۳۳)، اما همان‌گونه که استفاده از سلاح، ابزار و روش جنگی در مخاصمات مسلحانه از سوی حقوق بشردوستانهٔ بین‌المللی تنظیم‌گری شده و از اصول و قواعد آن پیروی می‌نماید[۱]، توسل به عملیات سایبری نیز می‌تواند به‌عنوان یک مخاصمهٔ مسلحانه واجد شرایط دانسته شده، مشمول حقوق بشردوستانهٔ بین‌المللی قرار گیرد (Schmitt, 2013 (B): 269) و تشخیص‌های مصلحت‌سنجانه را نمی‌توان مؤثر در تحلیل قانونی موضوع دانست. حتی با شیوهٔ مصلحت‌سنجانه نیز در صورت عدم شمول مقررات مربوط به ممنوعیت توسل به زور بر رایاجنگ‌های مختل‌کننده، تنظیم‌گری رایاجنگ‌های مذکور با چالش جدی مواجه شده، نتیجه با همهٔ اصول حقوق بشردوستانهٔ جاری در حقوق مخاصمات مسلحانه که بر همهٔ اَشکال جنگ و انواع سلاح‌های جنگی در گذشته، حال و آینده حاکم است، در تعارض خواهد بود (International Committee of the Red Cross, 2011: 36-37; International Committee of the Red Cross, 2015: 40; International Committee of the Red Cross, 2019: 2).

۴. ۵. نبود معیار عینی برای تشخیص رایاجنگ‌های مختل‌کنندهٔ ایجادگر مخاصمهٔ مسلحانه

ازجمله علل مخالفت با تلقیِ رایاجنگ‌های مختل‌کننده به‌عنوان توسل به زور را نبود معیار عینی و مشخص برای تعیین آستانهٔ وقوع مخاصمهٔ مسلحانه در موارد وقوع چنین رایاجنگ‌هایی دانسته‌اند (Silver, 2002: 84). به عبارت بهتر، در رایاجنگ‌های تخریب‌گر به‌سبب ایجاد آثار فیزیکی، امکان

---

۱. در این خصوص مادهٔ ۳۶ پروتکل اول الحاقی به کنوانسیون‌های ژنو در خصوص حمایت از قربانیانِ مخاصمات مسلحانهٔ بین‌المللی، شایان ملاحظه است.

تشخیص وقوع مخاصمهٔ مسلحانه به‌راحتی ممکن است؛ لکن با توجه به اینکه در نتیجهٔ ارتکاب رایاجنگ‌های مختل‌کننده، نتیجهٔ عینی و ملموس پدید نمی‌آید، تعیین وقوع یا عدم وقوع مخاصمهٔ مسلحانه با چالش مواجه خواهد بود.

این نظر را می‌توان از نتایج رویکرد اثرمحورِ صرف دانست که– چنان‌که گذشت– مورد انتقاد جدی واقع شده است. در همین راستا، برخی دیگر از پژوهشگران (کیهانلو و رضادوست، ۱۳۹۴: ۲۰۱) بر آن‌اند که «تسری نظر دیوان بین‌المللی دادگستری در قضیهٔ *نیکاراگوئه* به حملات سایبری به این معنا که این حملات نیز در صورت داشتن آثار زیاد، به استناد رأی مذکور، حملهٔ مسلحانه تلقی شوند، قابل انتقاد به‌نظر می‌رسد و توجه به اثر تا زمانی می‌تواند موجه باشد که با اصول اولیهٔ مورد پذیرش، تداخل نکند؛ در غیر این صورت، توالیِ این غایت‌انگاری افراطی، به نتایجی غیرمعقول و ناخواسته منتهی می‌شود که به‌صورت قطعی، مدنظر طراحان نظامِ منشوری توسل به زور نبوده است».

در پاسخ به ایراد نبود معیار عینی، باید گفت که اولاً در رایاجنگ‌های تخریب‌گر، ایجاد آثار فیزیکی در جهان خارجی الزاماً موجب تلقیِ یک رایاجنگ تخریب‌گر به‌عنوان توسل به زور نمی‌شود و نمی‌توان صرفِ ایجاد آثار فیزیکی را به‌عنوان شاخص الزامی برای تحقق توسل به زور دانست. به‌طور مثال، ارتکاب یک عملیات سایبری علیه یک گوشی همراه هوشمند در کشور دیگر که موجب افزایش حرارت و تخریب فیزیکی واحد پردازش مرکزی گوشی یادشده می‌شود، هیچ‌گاه به‌عنوان توسل به زور دانسته نخواهد شد. سند مقررات تالین نیز بر آن نظر است که «یک عملیات سایبری که تنها باعث آسیب، تخریب، جراحت یا مرگ محدود شود، لزوماً مخاصمهٔ مسلحانهٔ بین‌المللی محسوب نمی‌شود» (Schmitt & Vihul, 2017: 383-384). در غیر از رایاجنگ‌ها و در چارچوب جنگ‌های سنتی نیز ایجاد آثار فیزیکی محدود را نمی‌توان به‌عنوان معیار در تحقق توسل به زور دانست (O'Connell, 2013: 102-105; Olivier, 2012: 69-70). بر این اساس، با عنایت به اینکه الزاماً ایجاد آثار فیزیکی از سوی رایاجنگ‌های تخریب‌گر به‌مثابهٔ تحقق توسل به زور دانسته نمی‌شود، در رایاجنگ‌های مختل‌کننده نیز نمی‌توان به صرفِ عدم ایجاد آثار فیزیکی حکم بر عدم تحقق توسل به زور صادر نمود.

ثانیاً عدم احتساب رایاجنگ‌های مختل‌کننده به‌عنوان توسل به زور می‌تواند منجر به سطحی از مشروعیت‌بخشی به ارتکاب آنها ذیل مقررات مربوط به حقوق بین‌الملل باشد. این درحالی است که مشروعیت‌بخشی به چنین اقداماتی به صرفِ عدم ایجاد آثار فیزیکی با تردید جدی مواجه است؛ زیرا چنین اقداماتی می‌تواند تمام ارتباطات داخل و خارج از کشور هدف را مختل کند، جریان تجارت و نظام اقتصادی کشور هدف را با تعطیلی مواجه نماید و زیرساخت‌های اطلاعاتی کشور هدف را به‌طور کلی ناکارآمد سازد (Barkham, 2001: 91). مجوز ایجاد چنین بحران‌هایی در کشور هدف را نمی‌توان صرفاً به‌سبب عدم

ایجاد آثار فیزیکی، موجه نمود. خارج نمودنِ رایاجنگ‌های مختل‌کننده به‌صرفِ نبود معیار عینی برای ارزیابی آنها در تحقق توسل به زور در حالی ناموجه است که رایاجنگ‌های یادشده می‌توانند به‌صورت‌های بحران‌آفرین، صلح و امنیت بین‌الملل را مورد خدشه قرار دهند و جواز دادن به آنها به‌سببِ نبود معیار عینی، موجب نقضِ غرضِ حقوق بین‌الملل است که هدف آن تضمین صلح و امنیت بین‌الملل خواهد بود. نگارندگان ضمن عدم پذیرش دلیلِ مخالفت یادشده، بر این باورند که با تعیین معیارهایی برای تشخیص توسل به زور در نتیجهٔ ارتکاب رایاجنگ‌های مختل‌کننده، می‌توان از وقوع آنها جلوگیری نمود.

ثالثاً در راستای تقویت این نظر می‌توان به شرط مارتنس[1] 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 است و برگرفته از خرد جمعی، قرار خواهند گرفت (International Committee of the Red Cross, 1977: 1125).

رابعاً آن‌گونه که احتساب رایاجنگ‌های تخریب‌گر به‌عنوان توسل به زور صرفاً بر اساسِ معیارِ ایجاد آثار فیزیکی مورد انتقاد قرار گرفته و معیارهای دیگری نیز برای تحقق توسل به زور سایبری پیشنهاد شده است (Schmitt, Vihul, 2017: 333-337)، در تلقیِ رایاجنگ‌های تخریب‌گر نیز ضروری است که معیارهای دیگری نیز برای تحقق یا عدم تحقق توسل به زور مورد ارزیابی قرار گیرند. معیارهای یادشده را می‌توان نخست در رویکرد سند مقررات تالین مشاهده نمود که در بخش بعدیِ این نگاشته بررسی خواهد شد و دیگر اینکه به‌منظور رفع کاستی‌های استنباط‌شده از معیارهای ارائه‌شده از سوی سند مقررات تالین جهت شمول بر رایاجنگ‌های مختل‌کننده، نگارندگان می‌کوشند ریزمعیارهایی را جهت سنجش «شدت» رایاجنگ‌های مختل‌کننده به‌عنوان یکی از معیارهای سند مقررات تالین برای ارزیابی توسل به زور، پیشنهاد نمایند.

۵. رویکرد سند مقررات تالین به آستانهٔ وقوع مخاصمهٔ مسلحانه از طریق رایاجنگ‌های مختل‌کننده

قاعدهٔ ۱۱ نسخهٔ نخست و قاعدهٔ ۶۸ نسخهٔ دوم سند مقررات تالین[2] اشاره می‌کند که تحت برخی شرایط،

---

1. Martens Clause

۲. سند مقررات تالین به بررسی حقوق حاکم بر جنگ‌های سایبری پرداخته و به‌طور کلی، دربرگیرندهٔ حقوق بر جنگ (حقوق بین‌الملل حاکم بر توسل به زور از سوی کشورها به‌عنوان ابزار سیاست ملی) و حقوق در جنگ (حقوق بین‌الملل تنظیم‌کنندهٔ رفتار در مخاصمات مسلحانه که به‌عنوان حقوق مخاصمات مسلحانه یا حقوق بشردوستانهٔ بین‌المللی نیز شناخته می‌شود) است. این سند که از سوی متخصصان و محققان حقوق بین‌الملل طرح‌ریزی و در دو نسخه در سال‌های ۲۰۱۳ و ۲۰۱۷ تدوین شده، به‌دنبال تسری هنجارهای حقوقی و قانونی موجود به جنگ‌های نوین است. سند نخست به حقوق بین‌الملل مربوط به جنگ سایبری می‌پردازد و نسخهٔ دوم آن در سال ۲۰۱۷ که از سوی گروه متنوعی

رایاجنگ‌ها ممکن است بند ۴ مادهٔ ۲ را نقض کنند، اما هرگز ادعا نمی‌کند که قانون بدون ابهامی در این خصوص وجود دارد (Schmitt, 2013 (A): 47-52; Schmitt & Vihul, 2017: 333-337). 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. این آزمونِ دشوار شامل ارزیابی این موارد است: شدت[۱]، فوریت[۲]، مستقیم بودن[۳]، تهاجمی بودن (مداخله‌آمیز بودن)[۴]، قابل اندازه‌گیری بودن آثار[۵]، ماهیت نظامی داشتن[۶]، سطح مشارکت دولت[۷] و مشروعیت احتمالی[۸]. فارغ از هفت معیار دیگر که از سوی برخی از پژوهشگران مورد بررسی تفصیلی قرار گرفته‌اند (Barkham, 2001: 85-86; Hoisington, 2009: 452)، معیار «شدت» مقبولیت بیشتری در ادبیات رایج حقوق بین‌الملل یافته و چنین گفته شده است که «با درنظر گرفتن اینکه معیارهایی که برای تشخیص توسل به زور سایبری ارائه شده‌اند، قابل اعتماد به‌نظر نمی‌رسند، تنها معیاری که باقی می‌ماند، آستانهٔ شدت است» (Silver,

---

از کارشناسان تشکیل شد[۲]، 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.

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

۲. چگونگی وقوع با سرعت آسیب پس از حمله: مدت زمان بین عملیات سایبری و وقوع پیامدهای آن. آن دسته از عملیاتی که فوری‌ترین پیامدها را دارند، به احتمال زیاد واجد شرایط عنوان توسل به زور هستند.

۳. طول زنجیرهٔ میان حمله و آسیب: این معیار ارتباط علّی 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.

۴. درجه‌ای که حمله به قلمرو کشور مورد هدف نفوذ می‌کند: 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.

۵. درجه‌ای که آسیب را می‌توان اندازه‌گیری کرد: درجهٔ سهولت لازم برای شناسایی پیامدها است. هرچقدر که آثار عملیات سایبری قابل پیش‌بینی و شناسایی باشد، امکان شناسایی آن به‌عنوان توسل به زور آسان‌تر است.

۶. وجود پیوند میان عملیات سایبری و عملیات نظامی: این معیار از پیوند میان عملیات سایبری و عملیات نظامی استفاده می‌کند تا احتمال توصیف به‌عنوان توسل به زور را افزایش دهد.

۷. نزدیکی و آشکار بودن پیوند میان یک دولت و عملیات سایبری: 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.

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

2002: 89-92). 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، عملیات سایبری ایجادگرِ آثار فیزیکی را می‌توان به‌عنوان توسل به زور و موجدِ مخاصمهٔ مسلحانه محسوب نمود.

سند مقررات تالین اشاره می‌کند که حتی در زمینهٔ مخاصمات فیزیکی نیز در خصوص این موضوع اختلاف نظر وجود دارد. کمیتهٔ بین‌المللی صلیب سرخ بر این عقیده است که «هر اختلافی که بین دو کشور به‌وجود می‌آید و به مداخلهٔ نیروهای مسلح منجر می‌شود، یک مخاصمهٔ مسلحانه است ... فرقی نمی‌کند که مخاصمه چقدر طول بکشد یا چقدر کشتار اتفاق بیفتد» (International Committee of the Red Cross, 2016: 32). 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» (International Committee of the Red Cross, 2016: 236; Office of General Counsel, 2016). 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 (Greenwood, 2008: 57; Levie, 1991: 243-244). سند مقررات تالین به هر دو تفسیر احتمالی از آستانه در زمینهٔ سایبری اشاره کرده که اولی مبتنی بر یک تخمین پایین از آستانه در حوزهٔ فضای سایبری است؛ مانند «عملیات سایبری که باعث آتش‌سوزی در یک تأسیسات نظامی کوچک می‌شود» که می‌تواند برای ایجاد یک مخاصمهٔ مسلحانهٔ بین‌المللی کافی باشد (Schmitt & Vihul, 2017: 383) و در دومی اگر آستانه‌ای بالاتر درنظر گرفته شود، کارشناسان نتیجه می‌گیرند که «یک حادثهٔ سایبری که تنها باعث آسیب، تخریب، جراحت یا مرگ محدود شود، لزوماً آغازگر یک مخاصمهٔ مسلحانهٔ بین‌المللی محسوب نمی‌شود» (Schmitt & Vihul, 2017: 383-384).

بنابراین می‌توان دید که استنباط از قاعدهٔ شمارهٔ ۸۲ در خصوص سطح شدت موردنیاز برای ایجاد یک مخاصمهٔ مسلحانهٔ بین‌المللی در فضای سایبری تاحدودی مبهم است. اگرچه به‌نظر می‌رسد کارشناسان موافق هستند که عاقلانه است آستانهٔ یک مخاصمهٔ مسلحانهٔ بین‌المللی را نسبتاً پایین تلقی کنیم (Schmitt & Vihul, 2017: 384)؛ با این حال، قابل توجه است که سند یادشده قائل به برآوردهای پایینی از آستانه در شرایط جنگ سنتی فیزیکی است، اما به عملیات سایبری که به خسارات نامشهود محض منجر می‌شود، در تفسیر این قاعده هیچ اشاره‌ای نشده است که از آن می‌توان این‌گونه

استنباط نمود که برای کارشناسان تدوین‌گر سند مقررات تالین، عملیات سایبری مختل‌کننده به آستانهٔ لازم برای تحقق توسل به زور مسلحانه نمی‌رسند. وانگهی، با فرض اینکه عدم اشاره را نتوان حمل بر عدم امکان تصور توسل به زورِ سایبری با استفاده از عملیات سایبری مختل‌کننده دانست، ناگزیر می‌بایست به رویکرد سند یادشده در عملیات سایبری تخریب‌گر متوسل شد که بر آثار فیزیکی در ارزیابی یک عملیات سایبری به‌عنوان توسل به زور، تمسک می‌جوید.

این تمرکز بر آثار فیزیکی در ارزیابی تحقق «توسل به زور مسلحانه»، در نتیجه‌گیری سند مقررات تالین در خصوص توسل به زور در فضای سایبری منعکس شده است. تفسیر قاعدهٔ ۶۹ سند پیش‌گفته 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» (Schmitt & Vihul, 2017: 330). این سند فهرستی از عوامل متعدد را که ممکن است به این ارزیابی مرتبط باشند، ارائه می‌کند که شرح آنها گذشت (Schmitt & Vihul, 2017: 334-336). کارشناسان، شدت را به‌عنوان اولین نیاز، «مهم‌ترین عامل در تجزیه و تحلیل» می‌دانند (Schmitt & Vihul, 2017: 334). تفسیر موجود در خصوص این عامل تأکید زیادی بر حملات سایبری‌ای دارد که منجر به آسیب فیزیکی به افراد یا اشیا می‌شوند و اشاره دارد که «پیامدهایی شامل خسارت فیزیکی به افراد یا اموال» از آستانهٔ شدت عبور می‌کنند (Schmitt & Vihul, 2017: 334). چنان‌که ذکر شد، تفسیر قاعدهٔ شمارهٔ ۶۹ به‌صراحت این احتمال را که عملیات سایبری مختل‌کننده می‌توانند به‌عنوان 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 به‌عنوان فعالیت‌هایی اشاره می‌شود که به‌طور بالقوه می‌توانند این معیار خاص را برآورده سازند (Schmitt & Vihul, 2017: 335). با این حال، لحن کلی این قاعده نشان می‌دهد که برای حمله به دارایی‌های نامشهود یا عملیاتی که تنها به اختلال منجر 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 بشردوستانهٔ بین‌المللی- 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 مخاصمات و حقوق بشردوستانهٔ بین‌المللی در فضای سایبر را بررسی می‌کردند، اجماع کافی در مورد وضعیت آسیب‌های دیجیتال وجود نداشت و عملیات سایبری مختل‌کننده به رشد کمی و کیفیِ کنونی نرسیده بود.

در همین راستا گفته می‌شود معمولاً سرقت اطلاعات، حتی اگر اطلاعات حساس نظامی باشد، با

توجه به اینکه منجر به تلفات جانی یا جراحتی یا خسارت یا تخریب اموال نمی‌شود، به سطح حملهٔ مسلحانه نمی‌رسد. سرقت، به‌خودی خود، پیامد کافی برای تحقق معیار «آثار» نیست. اکثر مفسران این دیدگاه را دارند (Schmitt, 2013 (A): 55; Roscini, 2014: 71)؛ علی‌رغم برخی دیدگاه‌های مخالف که استدلال می‌کنند سرقت اطلاعات برای امنیت ملی حیاتی است و بنابراین، احتمالاً به‌عنوان یک حملهٔ مسلحانه قابل شناسایی است[۱]. وانگهی، به‌نظر می‌رسد عملیات سایبری که پیامدهای غیرفیزیکی شدیدی را به‌همراه دارند، به آن سبب که در حال حاضر، ارتش‌ها و جمعیت‌های غیرنظامی به‌طور یکسان به توانایی انتقال سریع اطلاعات حیاتی از طریق اینترنت وابسته هستند (Gisel & Olejnik, 2019). از نظر تئوری، در برخی شرایط بسیار محدود، می‌توانند با توسل به زور و حتی با یک حملهٔ مسلحانه برابر باشند؛ زیرا جنگ مدرن در حال تطبیق با جهانی است که به‌طور فزاینده بر فناوری و انتقال داده تکیه می‌کند. اگرچه عملیات سایبری مختل‌کننده به هیچ آسیب یا خسارت فیزیکی منجر نمی‌شود، اما می‌تواند به اندازهٔ حملات سایبری تخریب‌گر که آثار فیزیکی ایجاد می‌کنند، خطرناک باشد.

۶. معیارهای تشخیص تحقق مخاصمهٔ مسلحانه از طریق رایاجنگ‌های مختل‌کننده

دولت‌ها به‌طور روزافزون این دیدگاه را بیان می‌کنند که حقوق بشردوستانهٔ بین‌المللی انواع خاصی از عملیات سایبری مختل‌کننده را ممنوع می‌سازد (Georgia, 2020: 214). کمیتهٔ بین‌المللی صلیب سرخ نیز دیدگاه مخالف با سند مقررات تالین را اتخاذ می‌کند و 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» (Dörmann, 2004). 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 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

---

۱. آقای Christopher C Joyner و خانم Catherine Lotrionte معتقدند که ماهیت اطلاعات دزدیده‌شده یا به‌خطر افتاده نیز به تعیین اینکه آیا یک اقدام به سطحی که از نظر قانونی «حمله» تلقی شود، می‌رسد یا خیر، کمک می‌کند. اگر داده‌های خاصی برای امنیت ملی حیاتی تلقی شوند (یعنی اطلاعاتی که «طبقه‌بندی‌شده» هستند)، ممکن است تحت رژیم دفاع مشروع، حفاظت‌های ویژه‌ای برای آن اطلاعات درنظر گرفته شود. برای مثال، اگر یک دولت خارجی به پایگاه‌های اطلاعاتی رایانه‌ای وزارت امور خارجه یا وزارت دفاع یک دولت دیگر حمله کند و اطلاعات طبقه‌بندی‌شدهٔ مربوط به مکان سربازان در طول یک مخاصمهٔ مسلحانه یا کدهای ابزار پرتاب سلاح‌های هسته‌ای را به سرقت ببرد، چنین اقداماتی می‌تواند به‌عنوان «حملات مسلحانه» تلقی گردد؛ حتی اگر هیچ تلفات جانی یا تخریبی فوری نداشته باشد (Joyner & Lotrionte, 2001: 855).

بشردوستانهٔ بین‌المللی که از جمعیت غیرنظامی و اشیای غیرنظامی محافظت می‌کند، قرار نگیرد. تطبیق چنین درکِ بیش‌ازحد محدودکننده‌ای از مفهوم حمله با موضوع و هدف قواعد حقوق بشردوستانهٔ بین‌المللی در مورد ارتکاب مخاصمات دشوار خواهد بود» (International Committee of the Red Cross, 2019: 8). عبارات اخیر کمیتهٔ بین‌المللی صلیب سرخ، دور از تفسیر بیان‌شده از معیار «شدت» در سند مقررات تالین، حرکت به سمت درک منطقی از مفهوم حمله و توسل به زور را نشان می‌دهد که «ازدست دادن موقت عملکرد» را نیز شامل می‌شود.

ازآنجا 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 حمله، تابع مقررات مربوط به حقوق بشردوستانهٔ بین‌المللی واقع شود، شایسته است که دیوان کیفری بین‌المللی نیز در تفسیر کیفری خود از تفسیرهای متناظر اخیر پیروی کند. در این راستا، به‌منظور ارائهٔ معیار جهت تشخیص رایاجنگ‌های مختل‌کننده‌ای که به آستانهٔ مخاصمهٔ مسلحانه می‌رسند، شایان ذکر است که معیارهای هشت‌گانهٔ ارائه‌شده از سوی سند مقررات تالین مورد تأیید و تأکید نگارندگان قرار دارد. لکن با عنایت به اینکه از منظر سند یادشده، از یک سو، شاخص «شدت» از اولویت و اهمیت بیشتر برخوردار است و از سوی دیگر، سند یادشده نسبت به شمولیت شاخص «شدت» بر «رایاجنگ‌های مختل‌کننده» با گونه‌ای ابهام یا احتمالِ عدمِ شمول مواجه است- که شرح آن گذشت-، نویسندگان مقاله در این بخش می‌کوشند به‌منظور دقیق‌تر ساختنِ شاخص «شدت» از میان شاخص‌های هشت‌گانهٔ سند مقررات تالین، نسبت به پیشنهاد ریزمعیارهایی برای رایاجنگ‌های مختل‌کنندهٔ شدید که به آستانهٔ مخاصمهٔ مسلحانه می‌رسند، اقدام نمایند. البته برای ارزیابی این موضوع، هر عملیات سایبری به دلیل ماهیت متفاوت و آثار آن که ممکن است نوع و شدت متفاوتی داشته باشد، باید به‌صورت موردی بررسی شود (Silver, 2002: 85; Radziwill, 2015: 139).

رویهٔ قضایی 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 (Roscini, 2022). برای مثال، دادستان در تصمیم خود مبنی بر عدم شروع تحقیقات در خصوص حادثهٔ کشتی ماوی مرمره به دلیل شدت ناکافی، از عوامل پیش‌گفته استفاده کرده است (Buchan, 2014: 497-498; ICC, 2014: para. 138). این عوامل دارای اهمیتی ثابت نیستند و باید به‌صورت موردی ارزیابی شوند (Schabas, 2008: 740). برای برآورده شدنِ همهٔ آنها به‌صورت تجمیعی نیز ضرورتی وجود ندارد (O'Brien, 2012: 543). فرانسه نیز از این موضع حمایت کرده است که «در غیاب خسارت فیزیکی، یک عملیات سایبری ممکن است بر اساس معیارهای متعدد، ازجمله شرایط حاکم

در زمان عملیات، مانند منشأ عملیات و ماهیت محرک عملیات (نظامی یا غیرنظامی)، میزان نفوذ، آثار واقعی یا موردنظر عملیات یا ماهیت هدف موردنظر، توسل به زور تلقی شود» (Ministry of the Armies, 2019).

اعلامیه‌های دولت‌ها و ملاحظات پژوهشی نشان می‌دهد که حقوق عرفی در خصوص توسل به زور در فضای سایبری به سمتی پیش می‌رود که بیشتر شامل خسارت‌های دیجیتال و غیرفیزیکی شود. در این راستا، ریزمعیارهای پیشنهادیِ نگارندگان جهت ارزیابی شاخص «شدت»، علاوه بر توجه به یافته‌های پژوهشی، اظهار نظرهای رسمی دولت‌ها و رویهٔ قضایی فوق از دیوان کیفری بین‌المللی در این خصوص را نیز مورد استنباط قرار می‌دهد.

۶. ۱. مقیاس رایاجنگ

حملات سایبری به‌طور بالقوه می‌تواند آسیب فیزیکی یا غیرفیزیکی قابل‌توجهی به اشخاص، اشیا یا داده‌ها وارد کند و ممکن است در مقیاس کوچک یا وسیع انجام شود. برآورد شدت هر رایاجنگ در ارزیابی آن به‌عنوان یک مخاصمهٔ دارای شدت لازم، تأثیرگذار خواهد بود. شاخص «مقیاس» را می‌توان شامل این موارد دانست: «تعداد خسارت‌دیدگان مستقیم و غیرمستقیم ناشی از حملهٔ سایبری، میزان خسارات ناشی از حملهٔ سایبری یا گستردگی جغرافیایی یا زمانی آنها (شدت بالای جنایات در یک مدت کوتاه یا شدت کم جنایات در زمانی طولانی)» (The Office of the Prosecutor, 2013: para. 62). یک رایاجنگ ممکن است گستردگی جغرافیایی قابل‌توجهی داشته باشد، اما همچنان به خسارات فیزیکی منجر نشود. برای مثال، حملات بندآوری خدمات توزیع‌شده[1]، اغلب از جانب میلیون‌ها روبوشبکه[2] در چندین کشور انجام و از سوی یک یا چند ربات مهاجم[3] کنترل می‌شوند. اما این حملات تنها با خاموش کردن سرورها و سیستم‌هایی که مورد رجوع بسیار هستند، منجر به آسیب موقت و برگشت‌پذیر به آنها می‌شود و این آسیب ممکن است به قطع موقت و گستردهٔ خدمات بینجامد، اما آسیب فیزیکی به افراد یا اموال را موجب نمی‌شود. با توجه به اینکه بسیاری از خسارات غیرفیزیکی ممکن است حتی در داوری عرفی نیز دارای زیان بیشتری نسبت به آثار فیزیکی تلقی شوند، به‌نظر می‌رسد که فارغ از فیزیکی یا غیرفیزیکی بودنِ آثار و زیان‌های ایجادشده، توجه به مقیاس آثار ناشی از رایاجنگ‌ها، به‌صورت مورد به مورد، ضروری است.

---

1. DDoS
2. Botnet
3. Botmaster

۶. ۲. ماهیت رایاجنگ

شاخص «ماهیت» به‌طور ویژه، «به عناصر خاص جرایمی اشاره دارد که در آنها نوعی ... تحمیل شرایط نابودکنندهٔ زندگی بر یک گروه وجود دارد» (The Office of the Prosecutor, 2013: para. 63). این بدان معناست که برخی از جرایم به‌گونه‌ای از نظر ماهیتی، شدیدتر از سایرین دانسته می‌شوند. آنگاه که یک رایاجنگ مختل‌کننده با ایجاد اختلال در زیرساخت‌های مربوط به سلامت عمومی یک کشور، باعث تحمیل شرایط نابودکنندهٔ زندگی بر یک ملت یا گروهی از آنان می‌شود، می‌توان تاحدی از تحقق معیار ماهیت برای تحقق شاخصِ شدت هم سخن گفت. حملات متعدد به زیرساخت‌های درمانی که در طی شیوع کووید-۱۹ روی داده‌اند، شاهدی از اتخاذ رویکرد توجه به ماهیت رایاجنگ است که نظام سلامت جامعه را مورد هدف قرار داده است. به‌دلیل شدت همه‌گیری و مقیاس تأثیرات ویروس در سراسر جهان، دولت‌ها تمایل بیشتری دارند تا عملیات 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 قابل‌توجه و مستقیم در توزیع اطلاعات ضروری سلامت عمومی دخالت دارد، از سوی 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» (Milanovic, Schmitt, 2020: 12).

۶. ۳. روش ارتکاب رایاجنگ

برخی از معیارهایی که به‌وسیلهٔ آنها می‌توان نسبت به ارزیابی وجود این شاخص اقدام کرد، شامل موارد زیر است: «ابزاری که برای ارتکاب جرم به‌کار می‌رود، میزان مشارکت مرتکب در ارتکاب جرم و قصد مرتکب (اگر در این مرحله قابل تشخیص باشد)، میزان سازمان‌یافتگی یا وجود برنامهٔ پیشینی در ارتکاب جنایت، ارتکاب جنایت در نتیجهٔ سوءاستفاده از قدرت یا ظرفیت رسمی یا وجود عناصر ویژه از ارتکاب ظلم مانند آسیب‌پذیر بودنِ بزه‌دیدگان» (The Office of the Prosecutor, 2013: para. 64). بر این اساس، برخی از عملیات سایبری مختل‌کننده را می‌توان به‌طور مشخص ظالمانه توصیف کرد؛ برای مثال، چنانچه یک عملیات سایبری داده‌های پزشکی بیماران را به‌طوری که آنها درمان اشتباه، دردناک یا غیرضروری را دریافت کنند، تغییر دهد، به‌طور یقین ظالمانه بوده، از منظر روش ارتکاب جرم، جنایت را از نظر شدت به آستانهٔ لازم می‌رساند. همچنین وجود سازمان‌یافتگی یا وجود برنامهٔ پیشینی را نیز می‌توان از معیارهایی دانست که در خصوص برخی از رایاجنگ‌های مختل‌کننده قابل تصور و تحقق بوده، با احراز وصف «شدت»، تلقیِ آن به‌عنوان توسل به زور را ممکن می‌سازد.

گفته شده است که پیش‌زمینهٔ تجاوزکارانهٔ یک جنگ نیز یک عامل تشدیدکننده در ارزیابی شدت است (Schabas, El Zeidy, 2016: 815) و برای این وضعیت، گروه جاسوسی سایبری Fancy Bear مثال زده و ادعا می‌شود که با دستور روسیه نرم‌افزاری را آلوده کرده است که به نیروهای روسی اجازه می‌دهد به ارتباطات تلفنی و داده‌های موقعیت محلی نظامیان اوکراینی دسترسی داشته باشند و در نتیجه به آنها حمله کنند (Roscini, 2019: 267). در مثال دیگر که گونه‌ای جنایت جنگی علیه غیرنظامیان محسوب می‌شود، جریان حملات رژیم اسرائیل علیه غزه در سال ۲۰۲۳ است که رژیم اسرائیل مکان‌یابیِ تجمعات انسانی را به‌جای ترور فرماندهان نظامی در دستور کار قرار داده و بر اساس پردازش داده‌های خامی که با ثبت نام همهٔ جمعیت نوار غزه در نرم‌افزار همراهِ Lavender جمع‌آوری شده است، کشتار یا خودداری از آن را تجویز می‌کند (Frankel, 2024). در همین راستا گفته شده است ارتکاب رایاجنگ‌های مختل‌کننده‌ای که با سابقهٔ تجاوز نظامی از سوی مرتکب انجام می‌شوند، می‌تواند زمینهٔ برشماریِ آنها باعنوان توسل به زور را فراهم آورد (Silver, 2002: 85-86). البته دیوان کیفری بین‌المللی تاکنون از این دیدگاه حمایت نکرده است که یک جنگ تجاوزکارانه می‌تواند یک عامل تشدیدکننده در ارزیابی شدت محسوب شود.

۶. ۴. تأثیرگذاری رایاجنگ

آثار واقع‌شده در نتیجهٔ ارتکاب رایاجنگ می‌تواند در موارد زیر ارزیابی شود: «رنج‌های متحمل‌شده از سوی بزه‌دیدگان و افزایش آسیب‌پذیری [فیزیکی یا غیرفیزیکی] آنها، سپس وحشت ایجادشده در نتیجهٔ رنج‌ها و آسیب‌های اجتماعی، اقتصادی و زیست‌محیطی که بر جوامع آسیب‌دیده وارد می‌شود» (The Office of the Prosecutor, 2013: para. 65). برخی از رایاجنگ‌ها ممکن است بر اقتصاد یک کشور تأثیرات بحران‌آفرینی را برجای گذارند؛ مانند حملات DDoS در سال ۲۰۰۷ علیه استونی. چنان‌که ذکر شد، با شیوع ویروس کووید-۱۹ و پی بردن به اهمیت داده‌های رایانه‌ایِ حوزهٔ سلامت عمومی و پزشکی، پژوهشگران قائل به استثنا شده، حمله به داده‌های یادشده را برآورندهٔ آستانهٔ توسل به زور دانستند (Trahan, 2021: 1145)؛ این درحالی است که بدیهی است که صرفِ داده‌های پزشکی نیستند که واجد اهمیت تلقی می‌شوند و می‌توان از برخی گونه‌های دیگر از داده‌های رایانه‌ای، همچون داده‌های مربوط به زیرساخت‌های حیاتی، داده‌های مربوط به زیرساخت‌های اطلاعاتی مانند نیروگاه‌های برق و شبکه‌های توزیع آب، داده‌های مربوط به زندگی خصوصی شهروندان و داده‌های هویتی غیرنظامیان نام برد که ارتکاب رایاجنگ علیه آنها را بدون ایجاد آثار فیزیکی و با ایجاد خسارات غیرفیزیکی شدید می‌توان واجد وصف شدت لازم برای تحقق توسل به زور تلقی کرد.

به‌طور کلی، آن دسته از رایاجنگ‌های مختل‌کننده که زیرساخت‌های حیاتی یا اطلاعاتی ملی را هدف قرار می‌دهند و در نتیجه، ارائهٔ خدمات ضروری به جامعهٔ آن کشور را مختل می‌کنند، دارای تأثیرات قابل‌توجه بر جامعه محسوب می‌شوند؛ به‌ویژه اگر آثار آنها بلندمدت باشد. در چارچوب این شاخص، آسیب‌های بحران‌آفرین اجتماعی و اقتصادی را نیز باید در این زمینه درنظر گرفت. در این راستا، به‌نظر می‌رسد که با توجه به اهمیت زیرساخت‌های حیاتی یا اطلاعاتی ملی یک کشور، ایجاد اختلال گسترده در آنها از طریق رایاجنگ‌های مختل‌کننده، می‌تواند مستقلاً به‌عنوان معیار برآورندهٔ شاخص «شدت» و شاید مهم‌ترین و ملموس‌ترین شاخص دانسته شود.

۶. ۵. اختلال در زیرساخت‌های حیاتی یا اطلاعاتی

این واقعیت که هدف یک رایاجنگ مختل‌کننده، زیرساخت حیاتی یا اطلاعاتی است، عامل تشدیدکننده‌ای است که می‌تواند موجب شناسایی آن به‌عنوان توسل به زور شود. رایاجنگی که آثار فیزیکی ایجاد نمی‌کند، اما یک زیرساخت حیاتی یا اطلاعاتی را هدف قرار می‌دهد، چنین هدفی یک عنصر تعیین‌کننده برای تغییر شناسایی عملیات به‌عنوان توسل به زور یا عدم آن است که عموماً تحت شرایطی توسل به زور دانسته می‌شود. اگر رایاجنگی فقط آثار غیرفیزیکی ایجاد کند که بر زیرساخت‌های حیاتی کشور موردنظر تأثیری نداشته باشد، بعید است که این رایاجنگ واجد شرایط توسل به زور دانسته شود (Roscini, 2014: 58). برای مثال، یک رایاجنگ با آثار مخرب محدود به شبکهٔ رایانه‌ای یک کتابخانهٔ شهری به‌وضوح به‌منزلهٔ توسل به زور نخواهد بود؛ برعکس، اگر شبکهٔ مختل‌شده یک زیرساخت حیاتی یا اطلاعاتی حیاتی باشد یا برای عملکرد یک زیرساخت حیاتی یا اطلاعاتی ضروری باشد، رایاجنگ یادشده به احتمال زیاد به‌عنوان توسل به زور شناخته می‌شود؛ علی‌رغم اینکه صرفاً آثار دیجیتالی داشته باشد (Roscini, 2019: 245). ماهیت هدف که ممکن است زیرساخت‌های حیاتی یک کشور باشد، از جمله شرایط خاصی است که برخی از مخالفانِ احتسابِ رایاجنگ‌های مختل‌کننده به‌عنوان توسل به زور را نیز قانع می‌سازد تا در آن شرایط خاص، نظر بر تحقق توسل به زور داشته باشند (Hoisington, 2009: 448). گفته شده است اگر عملیات سایبری مختل‌کننده به اندازهٔ کافی شدید باشد که امنیت دولت را با اثرگذاری بر زیرساخت‌های حیاتی، تحت تأثیر قرار دهد، باید به معنای توسل به زور دانسته شود (Roscini, 2014: 245; Ziolkowski, 2010: 73-75).

در همین راستا فرانسه نیز این موضع را اتخاذ می‌کند که عملیاتی که به زیرساخت‌های نظامی برای تضعیف قابلیت‌های دفاعی فرانسه نفوذ می‌کند، حتی اگر آثار فیزیکی نداشته باشد، «توسل به زور» محسوب می‌شود (Schmitt, 2019) و به‌طور مشابه، هلند این دیدگاه را بیان کرده است که «نمی‌توان

رد کرد که یک عملیات سایبری با تأثیر بر زیرساخت‌های مالی یا اقتصادی بسیار جدی ممکن است به‌عنوان توسل به زور تلقی شود» (Letter from the Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace, 2019: 4) و حتی تا آنجا پیش رفته که گفته است «اگر یک حملهٔ سایبری کل سیستم مالی هلند را هدف قرار دهد ... یا اگر دولت را از انجام وظایف اساسی مانند نظارت یا أخذ مالیات بازدارد ... به‌عنوان یک حملهٔ مسلحانه تلقی می‌شود و بنابراین باعث می‌شود که یک دولت حق دفاع مشروع را حتی با توسل به زور، داشته باشد» (Bijleveld, 2018). این دیدگاه‌ها نشان می‌دهد حقوق عرفی از رویکرد تمرکز بر آثارِ لزوماً فیزیکیِ دور شده، به این رویکرد نزدیک می‌شود که خسارات غیرفیزیکی نیز می‌توانند به‌اندازهٔ خسارات فیزیکی زیان‌بار باشند.

اصطلاح زیرساخت‌های حیاتی به زیرساخت‌ها، دارایی‌ها یا سیستم‌هایی اشاره می‌کند که یک دولت آنها را برای حفظ عملکردهای حیاتی اجتماعی ضروری می‌داند. اگر زیرساخت‌های حیاتی آسیب ببینند، تخریب شوند یا مختل شوند، بر امنیت کشور تأثیر منفی می‌گذارند. تهدیدهای سایبری برای زیرساخت‌های حیاتی، چالشی مهم برای امنیت ملی و بین‌المللی هستند (Myjer, 2015: 287-290). بیشتر تعاریف در میان بخش‌های خدمات دولتی و عمومی، موضوعاتی چون امنیت، غذا، آب، حمل و نقل، انرژی، بهداشت، مالی و بانک را به‌عنوان زیرساخت‌های حیاتی درنظر می‌گیرند (Tsagourias, 2012: 231)؛ با این حال، هیچ تعریف پذیرفته‌شدهٔ جهانی از آنچه بخش‌های حیاتی را تشکیل می‌دهند، وجود ندارد (Roscini, 2014: 56).

در حال حاضر در ایالات متحده زیرساخت‌های حیاتی شامل فهرستی از شانزده بخش حیاتی می‌شود؛ ازجمله شیمیایی، تسهیلات تجاری، ارتباطات، تولیدات حیاتی، سدها، پایگاه‌های صنایع دفاعی، خدمات اضطراری، انرژی، خدمات مالی، غذا و کشاورزی، تسهیلات دولتی، بهداشت و سلامت عمومی، فناوری اطلاعات، رآکتورهای هسته‌ای و مواد و پسماندهای آن، سامانه‌های حمل و نقل، و سامانه‌های آب و فاضلاب (US White House, 2013). فرانسه نیز دوازده بخش از زیرساخت‌های حیاتی را شناسایی کرده است که به سه دسته به شرح زیر تقسیم می‌شوند: ۱. حاکمیت (فعالیت‌های غیرنظامی دولت، فعالیت‌های نظامی دولت، فعالیت‌های قضایی، فضا و تحقیقات)؛ ۲. حفاظت از جامعه (سلامت، تأمین آب، تأمین غذا)؛ ۳. بخش‌های اقتصادی و اجتماعی (انرژی، اطلاعات، سمعی و بصری و ارتباطات الکترونیکی، حمل و نقل، مالی و صنعت) (Delerue, 2020: 301). در سطح بین‌المللی نیز مجمع عمومی سازمان ملل متحد در سال ۲۰۰۳، قطعنامه‌ای را دربارهٔ «ایجاد فرهنگ جهانی امنیت سایبری و حفاظت از زیرساخت‌های اطلاعاتی حیاتی» به‌تصویب رساند و مقرر نمود که زیرساخت‌های حیاتی عموماً به «تولید، انتقال و توزیع انرژی، حمل و نقل هوایی و دریایی، خدمات بانکی و مالی، تجارت الکترونیک،

تأمین آب، توزیع مواد غذایی و بهداشت عمومی» مربوط است. این یک فهرست قطعی نیست و قطعنامه چنین مقرر نموده است که «هر کشور زیرساخت‌های اطلاعاتی حیاتی خود را تعیین خواهد کرد» (UNGA Res, 2003). بنابر تعاریف پیش‌گفته، روشن است که علی‌رغم اختلاف جزئی در تعاریف کشورها، فهرست‌ها بسیار شبیه به یکدیگرند. زیرساخت‌های حیاتی امروزی به‌طور اساسی به سامانه‌ها و شبکه‌های رایانه‌ای وابسته‌اند؛ بنابراین، به‌ویژه در برابر رایاجنگ‌های مختل‌کننده آسیب‌پذیر هستند (Shackelford, 2009: 199).

مشخصاً زیرمجموعه‌ای از زیرساخت‌های حیاتی که به‌طور خاص به شبکه‌ها و سامانه‌های رایانه‌ای مربوط می‌شود، به‌عنوان «زیرساخت‌های اطلاعاتی حیاتی»[1] شناخته می‌شود. زیرساخت‌های اطلاعاتی حیاتی، شبکه‌ها و سامانه‌های رایانه‌ای هستند که اختلال در آنها به‌طور جدی بر سلامت، ایمنی، امنیت یا رفاه اقتصادی شهروندان یا عملکرد مؤثر دولت یا اقتصاد تأثیر می‌گذارد (European Union, 2009). به عبارت دیگر، زیرساخت‌های اطلاعاتی حیاتی نتیجهٔ اتکای فزاینده بر زیرساخت‌های حیاتی و به‌طور کلی‌تر نتیجهٔ این است که جوامع و اقتصادهای ما شدیداً و به‌طور فزاینده، به شبکه‌ها و سیستم‌های رایانه‌ای متکی هستند (UNGA Res, 2003). از این رو، تعداد قابل‌توجهی از سامانه‌ها و شبکه‌های رایانه‌ای ممکن است به‌عنوان زیرساخت‌های اطلاعاتی حیاتی درنظر گرفته شوند. رایاجنگ‌ها و حملات بندآوری خدمات توزیع‌شده که در سال ۲۰۰۷ استونی را هدف قرار داد، سامانه‌ها و شبکه‌های رایانه‌ای حیاتی را مختل و حیات دولت را با چالش مواجه ساخت.

بر این اساس، آنگاه که رایاجنگ‌های مختل‌کننده موجب ایجاد اختلال در زیرساخت‌های حیاتی یا زیرساخت‌های اطلاعاتی کشور هدف شده، یکی از نظامات اساسیِ آن را با چالش جدی مواجه می‌سازند، می‌توان از تحقق معیار شدت برای وصول به آستانهٔ مخاصمهٔ مسلحانهٔ سایبری از رهگذرِ یک رایاجنگ مختل‌کننده سخن گفت.

۶. ۶. شرایط و اوضاع و احوال ارتکاب رایاجنگ

شرایطی که یک رایاجنگ مختل‌کننده در آن رخ می‌دهد، ممکن است در تعیین اینکه معیارهای توسل ممنوع به زور را برآورده می‌سازد یا خیر، بسیار کارساز باشد. شرایط و اوضاع و احوال مختلف ممکن است بر ارزیابی یک رایاجنگ تأثیر بگذارد؛ برای مثال، روابط بین دولت‌های درگیر ممکن است یک عامل تعیین‌کننده باشد. در زمینهٔ روابط صلح‌آمیز بین دو دولت، آستانهٔ یادشده برای تحقق شرایط توسل به زور سایبری ممکن است بالاتر باشد. در مقابل، در چارچوب تنش فزایندهٔ بین دو دولت، یک عملیات سایبری

1. critical information infrastructures (CII).

ممکن است به‌راحتی توسل به زور محسوب شود؛ با این حال، دولت‌ها نیز ممکن است برای جلوگیری از ارتقای دامنهٔ جنگ، از کاربرد این طبقه‌بندی خودداری کنند.

از شرایط و اوضاع و احوال دیگر این است که آیا رایاجنگِ ارتکاب‌یافته یک اقدام واحد (منفرد) بوده است یا بخشی از یک وضعیت پیچیده‌تر شمرده می‌شده است. توضیح آنکه یک اقدام واحد (منفرد) کمتر به‌عنوان توسل به زور شناخته می‌شود و گفته شده است که «یک حادثهٔ واحد (منفرد) عموماً از سوی دولت‌ها به‌عنوان ممنوعیت توسل به زور مذکور در منشور درنظر گرفته نمی‌شود» (Olivier, 2012: 76). از سوی دیگر، یک عملیات سایبری که در کنار سایر عملیات انجام می‌شود، می‌تواند زمینهٔ وصول به آستانهٔ توسل به زور سایبری محسوب گردد.

۷. مواجههٔ دیوان کیفری بین‌المللی با رایاجنگ‌های مختل‌کننده

هدف اصلی حقوق کیفری بین‌المللی «پایان دادن به بی‌کیفرمانی» برای «جدی‌ترین جنایات مربوط به جامعهٔ بین‌المللی» است[۱]. بر این اساس، بررسی این موضوع برای دیوان کیفری بین‌المللی ضروری است که آیا مادهٔ ۸ اساسنامهٔ رم می‌تواند عملیات سایبری مختل‌کننده را که در چارچوب هیچ مخاصمهٔ مسلحانهٔ ازپیش موجود رخ نداده است، به‌عنوان مخاصمهٔ مسلحانه محسوب کند و در محدودهٔ صلاحیتی خود قرار دهد یا خیر؛ هرچند چنین پیشرفت‌های فناوری در زمان تدوین آن پیش‌بینی نشده است. برای این منظور، اگر دیوان کیفری بین‌المللی به نتیجه‌گیری سند مقررات تالین مبنی بر عدم تحقق معیار «شدت» از رهگذرِ رایاجنگ‌های مختل‌کننده تکیه کند، این امر می‌تواند به مستثنی کردن رایاجنگ‌های یادشده از محدودهٔ صلاحیتی دیوان کیفری بین‌المللی بینجامد. این درحالی است که عملیات مختل‌کنندهٔ سایبری می‌تواند منجر به بحران‌های اجتماعی شود و با افزایش روزافزونِ وابستگی به فناوری، اختلال در سیستم‌های اطلاعاتی قادر است به اندازهٔ توسل به زورِ منجر به آثار فیزیکی، موجب ورود خسارت شود (Kilovaty, 2016: 127) و ایجاد آثار فیزیکی همیشه دارای شدت بیشتر و آسیب بزرگ‌تر تلقی نمی‌شود. بر این اساس، می‌توان از ردّ 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 هیچ نوع از نمود تخریب فیزیکی منجر نمی‌شوند، قائل به موضوعیت شد؛ زیرا غفلت از خسارت دیجیتال می‌تواند به نادیده گرفته شدن اشکال جدیدی از ظلم منتهی شود که از آنها به‌عنوان عملیات سایبری مختل‌کننده یاد می‌شود.

در مواردی که برخی از عبارات اساسنامهٔ رم قابلیت تفسیر داشته باشند، می‌بایست در چارچوب

---

۱. آن‌گونه که در مقدمهٔ اساسنامهٔ رم مورد اشاره قرار گرفته است.

رویکردی پویا مورد تفسیر واقع شوند و منعکس‌کنندهٔ تحولات فناورانه در جنگ و گفتمان در حال توسعه در خصوص آسیب دیجیتال باشند که در جامعهٔ بین‌المللی رخ می‌دهد؛ به‌گونه‌ای که رایاجنگ‌های مختل‌کننده را در محدودهٔ صلاحیتی مادهٔ ۸ قرار دهد و اطمینان حاصل کند که نقض دیجیتال حقوق بشردوستانهٔ بین‌المللی بی‌کیفر نخواهد ماند. ضمن تأکید بر اصل قانونی بودنِ جرم و مجازات مستنبط از مادهٔ ۲۲ اساسنامهٔ رم، رویهٔ قضایی دیوان نشان داده است که رویکرد هدفمند و غایت‌نگر به مادهٔ ۸ را می‌توان در مواردی اتخاذ کرد و درغیر این صورت، موضوع و هدفِ اساسنامه دیوان را تضعیف می‌کند؛ اساسنامه‌ای که مستنبط از مقدمه و مواد ۱ و ۵ آن، چیزی جز تضمین این نیست که جدی‌ترین جنایات نگران‌کننده برای جامعهٔ بین‌المللی به‌عنوان یک کل، دیگر بی‌کیفر باقی نمی‌ماند (ICC Rep, 2007: 281). همچنین باید به یاد 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 خواهند یافت. آثار غیرفیزیکی حملات سایبری «می‌تواند تأثیرات فاجعه‌باری بر جامعهٔ مدنی داشته باشد» (Li, 2013: 188). استفاده از رایاجنگ‌های مختل‌کننده در جنگ می‌تواند به حملات مکرر علیه غیرنظامیان نسبت به جنگ‌های متعارف منتهی شود؛ مگر اینکه به‌دقت مورد تنظیم‌گری قرار گیرند، زیرا چنین عملیاتی می‌تواند بدون ایجاد آسیب فیزیکی مستقیم بر روی اشیای غیرنظامی انجام شود و در نتیجه، هزینهٔ سیاسی کمتری داشته باشد (Kelsey, 2008: 1439-1441). به این دلایل، دیوان کیفری بین‌المللی باید رویکرد «ضرورت ایجاد آثار فیزیکی» را در 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 دنبال نماید.

۸. نتیجه‌گیری

استفاده از رایاجنگ‌های ناقض حقوق بشردوستانهٔ بین‌المللی میان دولت‌ها و آسیب به غیرنظامیان و زیرساخت‌های حیاتی ملی کشورها، تنظیم‌گریِ رایاجنگ‌ها و وضع محدودیت‌های کیفری مربوط به جنایات جنگی بر آنها را ناگزیر ساخته است تا آنجا که دادستان دیوان کیفری بین‌المللی در سال ۲۰۲۳، به‌صراحت از امکان تعقیب برخی رفتارهای ارتکاب‌یافته در چارچوبِ رایاجنگ‌ها با عنوان جنایت جنگی سخن گفته است. بر این اساس، پیش از تطبیق عناصر جنایات جنگی سنتی بر رایاجنگ‌های مدرن در چارچوب اساسنامهٔ رم، امکان‌سنجی وقوع عنصر زمینه‌ای جنایات جنگیِ سایبری، یعنی وقوع مخاصمهٔ

مسلحانه در نتیجهٔ ارتکاب رایاجنگ، ضرورت می‌یابد؛ زیرا در سند عناصر جنایات در صلاحیت دیوان کیفری بین‌المللی، «وجود مخاصمهٔ مسلحانه» به‌عنوان عنصر زمینه‌ای لازم برای وقوع جنایات جنگی دانسته می‌شود.

سند مقررات تالین، به‌عنوان معتبرترین سند غیرالزام‌آور بین‌المللی در خصوص کاربست مقررات حقوق بین‌الملل در فضای سایبر، در خصوص شرایط وقوع مخاصمهٔ مسلحانهٔ سایبری اظهار نظر کرده و هشت معیار مشتمل بر معیارهای شدت، فوریت، مستقیم بودن، تهاجمی بودن (مداخله‌آمیز بودن)، قابل اندازه‌گیری بودن آثار، ماهیت نظامی داشتن، سطح مشارکت دولت و مشروعیت احتمالی را ارائه نموده است؛ لکن هم از منظر سند یادشده و هم از نگاه سایر پژوهشگران، مهم‌ترین معیار در تعیین وقوع مخاصمهٔ مسلحانهٔ سایبری، تحقق معیار «شدت» است. سند پیش‌گفته ایجاد آثار فیزیکیِ مشابه با جنگ‌های سنتی را به‌عنوان مهم‌ترین شاخص برای ارزیابی معیار شدت، شناسایی کرده است. با عنایت به اینکه رایاجنگ‌ها به دو گونهٔ رایاجنگ‌های تخریب‌گر و رایاجنگ‌های مختل‌کننده تقسیم می‌شوند و ایجاد آثار فیزیکی در اولی موجود و در دومی غیرموجود است، استفادهٔ از معیار سند مقررات تالین برای تحلیل رایاجنگ‌های مختل‌کننده با چالش جدی مواجه است. بهره‌برداریِ دیوان کیفری بین‌المللی از رویکرد سند مقررات تالین نیز می‌تواند موجب بی‌کیفرمانیِ مرتکبانِ بسیاری از رایاجنگ‌های مختل‌کننده شود که جنایت آنها لزوماً دارای آثاری با شدت کمتر از رایاجنگ‌های تخریب‌گر نیست. بسیاری از رایاجنگ‌های مختل‌کننده موجب ورود خسارت عمده به زیرساخت‌های حیاتی و اطلاعاتی یک کشور می‌شوند و هیچ آثار فیزیکیِ مشابه با حملات سنتی در جهان خارج ایجاد نمی‌کنند. بنابراین، درحالی که ایجاد آثار فیزیکی لزوماً به‌معنای شدتِ بیشترِ آثارِ ایجادشده نیست و بسیاری از اختلال‌های ایجادشده در نتیجهٔ رایاجنگ‌های مختل‌کننده می‌توانند بسیار شدیدتر از آثار فیزیکیِ ناشی از برخی حملات سایبری تخریب‌گر ارزیابی شوند. بر این اساس، به‌جای اتخاذ رویکرد مبتنی بر آثار فیزیکی، می‌توان برخی معیارهای دیگر را برای ارزیابی شدت رایاجنگ‌های مختل‌کننده مورد توجه قرار داد و از این رهگذر، قائل به امکان وقوع مخاصمهٔ مسلحانه در نتیجهٔ وقوع رایاجنگ‌های مختل‌کننده شد. نگارندگان این پژوهش ضمن تأیید و تأکید بر معیارهای هشت‌گانهٔ سند مقررات تالین، بر آن‌اند که جهت ارزیابی مهم‌ترین معیار معرفی‌شدهٔ این سند، یعنی معیار «شدت»، باید به ارزیابی ریزشاخص‌های دیگر رایاجنگ، یعنی مقیاس، ماهیت، روش ارتکاب، تأثیرگذاری آن، اختلال رایاجنگ در زیرساخت‌های حیاتی و اوضاع و احوال ارتکاب آن، توجه نمود. تحقق هریک از ریزشاخص‌های یادشده می‌تواند یاری‌رسانِ یک رایاجنگ مختل‌کننده برای وصول به آستانهٔ توسل به زور باشد.

هدف اصلی تشکیل دیوان کیفری بین‌المللی در چارچوب اساسنامهٔ رم، پایان دادن به بی‌کیفرمانیِ

جدی‌ترین جنایات مربوط به جامعهٔ بین‌المللی است. این درحالی است که در صورت اتخاذ رویکرد مشهور مبنی بر اهمیتِ آثار فیزیکیِ صرف، حملات سایبری مختل‌کننده به‌سبب عدم وصول به آستانهٔ مخاصمهٔ مسلحانه، از شمول صلاحیت دیوان کیفری بین‌المللی خارج می‌شوند. در چنین شرایطی، اتخاذ رویکردی پویا و استفاده از ریزشاخص‌های نامبرده از سوی دیوان کیفری بین‌المللی جهت تحقق معیار شدت برای وصول به آستانهٔ وقوع مخاصمهٔ مسلحانهٔ سایبری برای شمول رایاجنگ‌های مختل‌کننده تحت عنوان جنایت جنگی، پیشنهاد می‌شود.

منابع

الف) فارسی

۱. برادران، نازنین و حبیبی، همایون (۱۳۹۸). قابلیت اعمال قواعد حقوق بین‌الملل بشردوستانه در جنگ‌های سایبری. *مطالعات حقوق عمومی*، ۴۹ (۱)، ۱۳۹-۱۵۸.

۲. شایگان، فریده و صفوی کوهساره، سیدحامد (۱۳۹۷). عملیات سایبری به‌مثابهٔ توسل به زور. *مطالعات حقوق عمومی*، ۴۸ (۲)، ۴۱۹-۴۴۱.

۳. شریفی طرازکوهی، حسین و برمکی، جعفر (۱۳۹۹). چالش‌های حقوقی قابلیت‌های فضای سایبری در پرتو مادهٔ ۳۶ پروتکل یکم الحاقی ۱۹۷۷. *مجلهٔ حقوقی بین‌المللی*، (۶۲)، ۱۱۹-۱۴۴.

۴. صابر، محمود و صادقی، آزاده (۱۳۹۴). بررس معیار آستانهٔ شدت برای تعقیب جنایات در دیوان کیفری بین‌المللی؛ با نگاهی بر دیگر دادگاه‌های بین‌المللی. *مطالعات حقوق تطبیقی*، ۶ (۲)، ۶۲۷-۶۵۰.

۵. عباسی، مجید و مرادی، حسین (۱۳۹۴). جنگ سایبر از منظر حقوق بین‌الملل بشردوستانه. *مجلس و راهبرد*، ۲۲ (۸۱)، ۳۷-۶۸.

۶. فقیه حبیبی، علی (۱۳۹۵). جنگ مدرن و تخاصمات سایبری در چارچوب فضای بین‌الملل. *جستارهای سیاسی معاصر*، ۷ (۱۹)، ۱۱۵-۱۴۴.

۷. کیهانلو، فاطمه و رضادوست، وحید (۱۳۹۴). حملات سایبری به‌مثابهٔ توسل به زور در سیاق منشور سازمان ملل متحد. *تحقیقات حقوقی*، (۶۹)، ۱۹۳-۲۰۸.

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

ب) انگلیسی

- Books

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

2. Ambos, Kai (2015). International Criminal Responsibility in Cyberspace. in *Research Handbook on International Law and Cyberspace*. Edited by Nicholas Tsagourias & Russell Buchan. Cheltenham: Edward Elgar.
3. Bond, James (1996). *Peacetime Foreign Data Manipulation As One Aspect of Offensive Information Warfare: Questions of Legality Under the United Nations Charter Article 2(4)*. Naval war college.
4. Brownlie, Ian (1963). *International Law and the Use of Force by States*. Oxford: Oxford University Press.
5. Bussolati, N. (2015). The Rise of Non-State Actors in Cyberwarfare. in *Cyberwar: Law and Ethics for Virtual Conflicts*. Edited by JD Ohlin, K Govern and C Finkelstein. Oxford: Oxford University Press.
6. Corten, Olivier (2012). *The Law against War - The Prohibition on the Use of Force in Contemporary International Law*. Oxford: Hart Publishing.
7. Delerue F (2020). *Cyber Operations and International Law*: Cambridge University Press.
8. Dinniss, H. Harrison (2012). *Cyber Warfare and the Laws of War*. Cambridge: Cambridge University Press.
9. Droege, C. (2012). *Get Off My Cloud: Cyber Warfare, International Humanitarian Law and the Protection of Civilians*. IRRC: Volume 94.
10. Greenwood, C. (2008). Scope of Application of Humanitarian Law. in *The Handbook of International Humanitarian Law*. edited by D Fleck. 2nd edn: Oxford University Press.
11. Hollis, Duncan B. (2008). New Tools, New Rules: International Law and Information Operations. In *THE MESSAGE OF WAR: INFORMATION, INFLUENCE AND PERCEPTION IN ARMED CONFLICT*. Edited by G. David and T. McKeldin: Temple University Legal Studies Research Paper.
12. Kerschischnig, Georg (2012). *Cyberthreats and International Law*. Hague: Eleven International Publishing.
13. Lubin, A. (2021). The Rights to Privacy and Data Protection Under International Humanitarian Law and Human Rights Law. In *Research Handbook on Human Rights and Humanitarian Law: Further Reflections and Perspectives*. Edited by R Kolb, G Gaggioli and P Kilibarda: Edward Elgar, Cheltenham.
14. Myjer, Eric (2015). Some Thoughts on Cyber Deterrence and Public International Law. in: *Research Handbook on International Law and Cyberspace*. Edited by Nicholas Tsagourias and Russell Buchan. Edward Elgar Publishing.
15. O'Connell, Mary Ellen (2013). 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.
16. Radziwill, Yaroslav (2015). *Cyber-Attacks and the Exploitable Imperfection of International Law*. Leiden: Brill & Martinus Nijhoff Publishers.
17. Roscini, Marco (2014). *Cyber Operations and the Use of Force in International Law.* Oxford: Oxford University Press.
18. Schabas, William A. and El Zeidy, Mohamed M. (2016). 'Article 17'. in: *The Statute of the International Criminal Court, A Commentary.* Edited by Otto Triffterer and Kai Ambos, 3rd ed. Oxford: Oxford University Press.
19. Schmitt, Michael N. (A) (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.
20. Schmitt, Michael N. and Vihul, Liis (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd edn. Cambridge: Cambridge University Press.
21. Sharp, Walter Gray (1999). *Cyberspace and the Use of Force*. Virginia: Aegis Research Corp.

- **Articles**
22. Barkham, Jason (2001). Information Warfare and International Law on the Use of Force. *New York University Journal of International Law and Politics.* 34 (57), 57-113.
23. Bijleveld, A. (2018). Keynote Address, Diplomacy and Defence in Cyber Space. *cyber seminar in Hague.* 20 June 2018, accessed 2 May 2024. https://english.defensie.nl/downloads/speeches/2018/06/21/keynote-address-by-the-minister-of-defence-ms.-ank-bijleveld-marking-the-firstanniversary-of-the-tallinn-manual-2.0-on-the-20th-of-june-2018.
24. Biller J.T. and Schmitt, M.N. (2019). Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare: *International Law Studies*, 95.
25. Brown G. and Tullos O. (2012). On the Spectrum of Cyberspace Operations: *Small Wars Journal*, 12 Nov. 2012, accessed 2 May 2024. https://papers.ssrn.com/sol3/papers.cfm ?abstract_id=2400536.
26. Buchan, R.J. (2014). The critical comments of Russell Buchan, 'The Mavi Marmara Incident and the International Criminal Court': *Criminal Law Forum,* 25.
27. Coleman, C. (2003). Securing Cyberspace – New Laws and Developing Strategies. *Computer Law and Security Review*. 19 (2), 131-136. https://doi.org/10.1016/S0267-3649(03)00208-5.
28. Creekman, Daniel M. (2001). A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China. *American University International Law Review*. 17 (3), 641-681.
29. Duncan, Hollis B. and Benthem, Tsvetelina van (2021). What Would Happen If States Started Looking at Cyber Operations as a "Threat" to Use Force?: *LAWFARE*, 30 March 2021, accessed 2 May 2024. https://www.lawfaremedia.org/article/what-would-happen-if-states-started-looking-cyber-operations-threat-use-force.
30. Frankel, Simon (2024). When AI Decides Who Lives and Dies, The Israeli military's algorithmic targeting has created dangerous new precedents: *Foreign Policy*. https://foreignpolicy.com/2024/05/02/israel-military-artificial-intelligence-targeting-hamas-gaza-deaths-lavender/.
31. Georgia, Beatty (2020). 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), 209-239. https://doi.org/10.4337/mllwr.2020.02.17.
32. Greenberg, A. (2023). The International Criminal Court Will Now Prosecute Cyberwar Crimes: *Wired*, 7 September 2023, accessed 2 May 2024. https://www.wired.com/story/icc-cyberwar-crimes/.
33. Hathaway, Oona A. (2022). To What Extent and Under What Conditions Might Cyber Operations or Cyberwarfare Constitute Crimes Specified in the Rome Statute?: *ICC Forum*. https://iccforum.com/cyberwar#Hathaway.
34. Hern, A. (2017). WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017: *The Guardian*. 30 December 2017. https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware.
35. Hoisington, Matthew (2009). Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense. *International & Comparative Law Review.* 32, 439-454.
36. Hoogh, André (2009). Georgia's Short-Lived Military Excursion into South Ossetia: The Use of Armed Force and Self-Defence: *ejiltalk*. 9 December 2009, accessed 2 May 2024. www.ejiltalk.org/georgia's-short-lived-military-excursion-into-southossetia-the-use-of-armed-force-and-self-defence/.
37. Horowitz, J. (2020). Cyber Operations under International Humanitarian Law: Perspectives from the ICRC: *American Society of International Law*, 24, 19 May 2020.

38. Joyner, Christopher C. and Lotrionte, Catherine (2001). Information Warfare as International Coercion: Elements of a Legal Framework. *European Journal of International Law*. 12 (5), 525-565, https://doi.org/10.1093/ejil/12.5.825.
39. Karim A.A. Khan (2023). Technology Will Not Exceed Our Humanity: *digitalfrontlines*, 20 August 2023, accessed 2 May 2024. https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity/.
40. Kelsen, Hans (2001). Collective Security under International Law: *International Law Studies, Naval War College and The Lawbook Exchange*.
41. Kelsey, J. (2008). Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare. *Michigan Law Review*. 106 (7), 1427-1452.
42. Kilovaty, I. (2016). Virtual Violence – Disruptive Cyberspace Operations as "Attacks" Under International Humanitarian Law. *Michigan Telecommunications and Technology Law Review*. 23 (1), 113-147.
43. Levie, HS. (1991). The Status of Belligerent Personnel "Splashed" and Rescued by a Neutral in the Persian Gulf Area". *Virginia Journal of International Law.* 31, 239-245.
44. Li, S. (2013). When Does Internet Denial Trigger the Right of Armed Self-Defense?. *Yale Journal International Law*. 38, 179-216.
45. Lin, Herbert S (2010). Offensive Cyber Operations and the Use of Force. Cybersecurity Symposium: National Leadership, Individual Responsibility. *Journal of National Security Law & Policy*. 4(1), 63-86.
46. Milanovic, Marko and Schmitt, Michael N. (2020). Cyber Attacks and Cyber (Mis)information Operations during a Pandemic. *Journal of National Security Law & Policy*. 11, 247-284.
47. Miller, K. (2014). The Kampala Compromise and Cyberattacks – Can There Be an International Crime of Cyber-Aggression?. *Southern California Interdisciplinary Law Journal*. 23, 217-260.
48. O'Brien, Melanie (2012). Prosecutorial Discretion as an Obstacle to Prosecution of United Nations Peacekeepers by the International Criminal Court: *Journal of International Criminal Justice*, 10.
49. Ophardt, J. (2010). Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield. *Duke Law & Technology Review*. 9 (3), 1-28.
50. Roscini, M. (2019). Gravity in the Statute of the International Criminal Court and Conduct that Constitutes, Instigates or Facilitates International Crimes: *Criminal Law Forum*, 30 (3), 247–272.
51. Roscini, M. (2022). Cyber Operations Can Constitute War Crimes Under the ICC Jurisdiction Without Need to Amend the Rome Statute: *ICC FORUM*, 7 March 2022.
52. Ruys, Tom (2014). 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), 159-210.
53. Saxon, Dan (2016). Violations of International Humanitarian Law by Non-State Actors during Cyberwarfare: Challenges for Investigations and Prosecutions. *Journal of Conflict and Security Law*. 21 (8), 555-574. https://doi.org/10.1093/jcsl/krw018.
54. Schabas, William A. (2008). Prosecutorial Discretion v. Judicial Activism at the International Criminal Court: *Journal of International Criminal Justice*, 6.
55. Scheffer, David (2022). Amending the Rome Statute to Cover Cyberwarfare as Aggression: *ICC Forum*, 7 Mar. 2022, accessed 2 May 2024. https://iccforum.com/cyberwar#Scheffer.
56. Schmitt, Michael N (1998). Bellum Americanum: The U.S. View of TwentyFirst Century War and Its Possible Implications for the Law of Armed Conflict: *Michigan Journal of International Law*, Vol. 19.
57. Schmitt, Michael N (2011). Cyber Operations and the Jus Ad Bellum Revisited. *Villanova Law Review*. 56, 569-605.
58. Schmitt, Michael N (B) (2013). The Law of Cyber Warfare: Quo Vadis?: *Stanford Law & Policy Review*, 25, 269-299.

59. Schmitt, Michael N. (1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*. 37, 885-937.
60. Shackelford, Scott (2009). From Nuclear War to Net War: Analogizing Cyber Attacks in International Law: *Berkley Journal of International Law*, 27.
61. Silver, Daniel B. (2002). Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter. *International Law Studies.* 76, 73-97.
62. Trahan, J. (2022). Contributing to Cyber Peace by Maximizing the Potential for Deterrence: Criminalization of Cyberattacks under the International Criminal Court's Rome Statute. In: *Cyber Peace*, 131-153.
63. Trahan, J. (2022). The Criminalization of Cyber-operations Under the Rome Statute: *Journal of International Criminal Justice*, 19 (5), 1133–1164.
64. Tsagourias, Nicholas (2012). Cyber Attacks, Self-Defence and the Problem of Attribution: *Journal of Conflict and Security Law*, 17.
65. Waxman, Matthew C. (2011). Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4). *Yale Journal of International Law*. 36, 421-459.
66. Ziolkowski, Katharina (2010). Computer Network Operations and the Law of Armed Conflict: Military Law and Law of War Review, 49.

- Documents

67. Dörmann, K. (2004). *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, 19 November 2004, accessed 2 May 2024. https://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf.
68. Gisel, L. and Olejnik, L. (2019). The Potential Human Cost of Cyber Operations: *ICRC*, 29 May 2019, accessed 2 May 2024. https://www.icrc.org/en/document/potential-human-costcyber-operations.
69. ICC Decision (2007). The Prosecutor v. Thomas Lubanga Dyilo, ICC-01/04-01/06, Decision on the Confirmation of Charges, PTC I, 29 Jan. 2007.
70. ICJ Reports (1949). Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania), ICJ Reports 4.
71. ICJ Reports (1996). Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion), ICJ Reports 226.
72. Int'l. Crim. Trib. for the Former Yugoslavia (1995). Prosecutor v. Tadić, Case No. IT-۱-۹۴-l, Decision on the Defense Motion for Interlocutory Appeal on Jurisdiction, 2 Octoer ۱۹۹۵.
73. International Committee of the Red Cross (1977). Additional Protocol I to the Geneva Convention of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, 12 December, 1977.
74. International Committee of the Red Cross (2011). International Humanitarian Law and the challenges of contemporary armed conflicts: ICRC position paper.
75. International Committee of the Red Cross (2015). International Humanitarian Law and the challenges of contemporary armed conflicts: ICRC position paper.
76. International Committee of the Red Cross (2016). 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.
77. International Committee of the Red Cross (2019). International Humanitarian Law and the challenges of contemporary armed conflicts: ICRC position paper.
78. International Committee of the Red Cross (2019). International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC position paper. November 28, 2019, accessed 2 May

2024. https://www.icrc.org/en/document/ international-humanitarian-law-and-cyber-operations-during-armed-conflicts.
79. Letter from the Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace (2019), Appendix, July 5, 2019, accessed 2 May 2024. https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-theparliament-on-the-international-legal-order-in-cyberspace.
80. Max Planck Institute for Comparative Public Law and International Law (2009). Report of the International Fact-Finding Commission on the Conflict in Georgia: *ceiig*, accessed May 2, 2024. www.ceiig.ch/Report.html.
81. Ministry of the Armies (2019). International Law Applied to Operations in Cyberspace: Ministère des Armées, 19 March 2019, accessed 2 May 2024. https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf.
82. Morgan, J. (2014). A Simple Explanation of the Internet of Things: *Forbes*, 13 May 2014, accessed 2 May 2024. https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#69481bd01d09.
83. Office of General Counsel (2015). United States Department of Defense Law of War Manual, 12 June 2015, updated December 2016, accessed May 2, 2024. https://www.hsdl.org/?abstract&did=797480.
84. Permanent Mission of Liechtenstein to the United Nations (2021). The Council of Advisers' Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare.
85. Porup, JM. (2019). How a nuclear plant got hacked: *CSO Online*, 9 December 2019, accessed 2 May 2024. https://www.csoonline.com/article/3488816/how-a-nuclear-plant-got-hacked.html.
86. Preparatory Commission for the International Criminal Court (2000). Report of the Preparatory Commission for the International Criminal Court, Addendum, add. Part II Finalized draft text of the Elements of Crimes, U.N. Doc. PCNIC/2000/1/Add.2.
87. Rome Statute of the International Criminal Court (1998). 17 July 1998, 2187 U.N.T.S. 90.
88. Schmitt, Michael N. (2019). France's major statement on international law and cyber: an assessment. *Just Security*, 16 September 2019, accessed 2 May 2024. www.justsecurity.org/66194/frances-major-statement-on-international-law-and-cyber-an-assessment/.
89. UN General Assembly Resolutions Tables (2003). Creation of a global culture of cybersecurity and the protection of critical information infrastructures, UNGA Res 58/199, 23 December 2003.
90. US White House, 'Presidential Policy Directive -- Critical Infrastructure Security and Resilience', 2013, Presidential Policy Directive/PPD-21, available in: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidentialpolicy-directive-critical-infrastructure-security-and-resil.
91. Zetter, K. (2016). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid: *Wired*, 3 March 2016, accessed 2 May 2024. https://www.wired.com/2016/03/inside-cunning-unprecedentedhack-ukraines-power-grid/