Criminal Law Doctrines
ISSN Print: 2251- 9351 Online: 2783- 3704

Disruptive Cyberwars Targeting Critical Infrastructures as a War Crime

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

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

Article Info

Article type:
Original research

Received: 28 June 2024
Received in revised form: 27 October 2024
Accepted: 3 December 2024
Available online: 29 December 2024

Keywords
cyber warfare, critical infrastructures, war crimes, armed conflict, dual-use cyber infrastructures.

Abstract

In parallel with the expansion of cyberspace, cyber warfare has also expanded as a tool for exerting power against various countries. The imposition of legal restrictions on them has become inevitable. In the realm of international criminal law, imposing limitations of the laws of war on cyberattacks, which differ from conventional warfare, faces challenges. Because the regulations governing the laws of war and war crimes has been formulated to align with conventional warfare. Yet disruptive cyberattacks on critical infrastructure are a type of cyberwarfare that, without causing physical effects similar to conventional wars and solely through non-physical impacts on a country's vital infrastructure, are considered capable of producing consequences more severe than those of conventional wars. Employing a descriptive-analytical method and gathering materials through a library-based approach, this study addresses its central question whether under the existing framework of the Rome Statute, disruptive cyberattacks on critical infrastructure could constitute war crimes particularly Article 8 on war crimes. Ultimately, it holds the view that by adopting a dynamic interpretation of the concept of 'intensity' under existing regulations, it can be affirmed the possibility of cyber conflict and war crimes via severe disruptions to critical infrastructure. However, this approach will face challenges when dealing with critical infrastructure with dual-use.

Cite this article: Shamloo, B. & Hosseini, M. (2024). Cyberattacks Disrupting Critical Infrastructure as a War Crime. *Criminal Law Doctrines*, 21(27), 115-152. https://doi.org/10.30513/cld.2024.6134.2005

آموزه‌های حقوق کیفری
ISSN Print: 2251- 9351 Online: 2783- 3704

رایاجنگ‌های مختل‌کنندهٔ زیرساخت‌های حیاتی به‌مثابهٔ جنایت جنگی

باقر شاملو[1]، مهدی حسینی[2]

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

۲. نویسنده مسئول، دانش‌آموختهٔ دکتری حقوق کیفری و جرم‌شناسی، دانشکدهٔ حقوق، دانشگاه شهید بهشتی، تهران، ایران. رایانامه: hosseini.mhdi@gmail.com

اطلاعات مقاله

نوع مقاله: پژوهشی

تاریخ دریافت: ۱۴۰۳/۰۵/۱۶
تاریخ بازنگری: ۱۴۰۳/۸/۱۷
تاریخ پذیرش: ۱۴۰۳/۰۹/۱۳
تاریخ انتشار برخط: ۱۴۰۳/۹/۱۷

کلیدواژه‌ها

رایاجنگ، زیرساخت‌های حیاتی، جنایت جنگی، مخاصمهٔ مسلحانه، زیرساخت‌های سایبری دوگانه.

چکیده

متناظر با گسترش استفاده از فضای سایبر، رایاجنگ‌ها نیز به‌عنوان ابزاری برای اعمال قدرت علیه کشورهای مختلف گسترش یافته‌اند و اعمال محدودیت‌های حقوقی بر آن‌ها ناگزیر شده است. در پهنهٔ حقوق کیفری بین‌المللی، وضع محدودیت‌های حقوق جنگ بر رایاجنگ‌های غیرمشابه با جنگ‌های سنتی، با چالش‌هایی مواجه است، زیرا مقررات مربوط به حقوق جنگ و جنایات جنگی متناسب با جنگ‌های سنتی وضع شده‌اند. این در حالی است که رایاجنگ‌های مختل‌کنندهٔ زیرساخت‌های حیاتی گونه‌ای از رایاجنگ‌هایند که بدون ایجاد آثار فیزیکی مشابه با جنگ‌های سنتی و صرفاً با ایجاد آثار غیرفیزیکی بر زیرساخت‌های حیاتی یک کشور، یارای ایجاد آثاری شدیدتر از جنگ‌های سنتی دانسته می‌شوند. بر این اساس، این پژوهش با استفاده از روش توصیفی - تحلیلی و با گردآوری مطالب با روش کتابخانه‌ای، می‌کوشد تا به این سؤال اصلی پاسخ دهد که در چهارچوب مقررات موجود در اساسنامهٔ رم و خصوصاً مادهٔ ۸ آن در خصوص جنایات جنگی، آیا با استفاده از رایاجنگ‌های مختل‌کنندهٔ زیرساخت‌های حیاتی، امکان وقوع جنایت جنگی وجود دارد یا خیر، و نهایتاً بر این نظر است که با اتخاذ رویکردی پویا از مفهوم «شدت» در استنباط از مقررات موجود، می‌توان قائل به امکان وقوع مخاصمهٔ سایبری و جنایت جنگی از رهگذرِ ایجاد اختلال‌های شدید در زیرساخت‌های حیاتی شد، هرچند این رویکرد در مواجهه با زیرساخت‌های حیاتی سایبری با کاربرد دوگانه، با چالش مواجه خواهد بود.

استناد: شاملو، باقر؛ حسینی، مهدی. (۱۴۰۳). رایاجنگ‌های مختل‌کنندهٔ زیرساخت‌های حیاتی به‌مثابهٔ جنایت جنگی. آموزه‌های حقوق کیفری، ۲۱(۲۷)، ۱۱۵-۱۵۲.
https://doi.org/10.30513/cld.2024.6134.2005

ناشر: دانشگاه علوم اسلامی رضوی.

مقدمه

گسترش رایاجنگ‌ها[۱] نگرانی دولت‌ها و سازمان‌های بین‌المللی را برای تنظیم‌گریِ حقوقی این‌گونه از جنگ‌های نوین شدت بخشیده است. علی‌رغم دشواری‌های اثبات انتساب در فضای سایبر که موجب شده است برخی از پژوهشگران آن را خلوتگاه مناسب بزه‌کاران بنامند (پاکزاد، ۱۳۸۸، ص۳۰)، نادیده گرفتن واقعیت رایاجنگ‌ها مشابه نادیده گرفتن کاربرد تانک‌ها، بمب‌افکن‌های هواپیما و راکت‌های مورد استفاده به‌عنوان ابزارهای اصلی جنگ در طول جنگ جهانی دوم است (Scheffer, 2022). بزهکاری سایبری جنبهٔ فراملی دارد و تهدید جهانی برای کشورها و شهروندان آن‌هاست و مقابله با همهٔ گونه‌های آن نیازمند همکاری فراملی و بین‌المللی است (نجفی ابرندآبادی، ۱۳۸۸، ص۱۲۹؛ نجفی ابرندآبادی، ۱۳۹۵، ص۱۳). بر این اساس و با توجه به چالش‌ها و دشواری‌ها در خلق سازوکارهای بین‌المللی نو و این موضوع که مشخصهٔ بارز هزارهٔ سوم، سرعت در پیشرفت‌ها و نوآوری‌هاست (شاملو؛ خلیلی پاجی، ۱۴۰۰، ص۲۹)، از این منظر، بروز رایاجنگ‌ها به‌مثابهٔ سوءاستفاده از فناوری‌های روز است که منشأ اخلال در نظم و امنیت سایبری بین‌المللی بوده و با توجه به این‌که رایاجنگ نیز باید تابع قواعد حقوقی باشد و بی‌توجهی به آن از سوی هیچ طرفی در مخاصمات مسلحانه پذیرفتنی نیست (ضیایی بیگدلی، ۱۳۹۷، ص۴۸۳-۴۸۲)، ظهور ضمانت‌های کیفری را که فصل ممیز میان اخلاق و حقوق است، ناگزیر ساخته است (محقق هرچقان و دیگران «الف»، ۱۴۰۲، ص۱۵۵۵). حقوق جنگ که نقض آن‌ها منجر به جنایت جنگی می‌شود، اساساً برای جنگ‌های فیزیکیِ سنتی وضع شده‌اند و تنظیم‌گری حقوقی رایاجنگ‌ها در چهارچوب مقررات مربوط به جنایات جنگی، با چالش‌هایی مواجه است.

تا سال ۲۰۲۳، هیچ موقعیت مربوط به یک رایاجنگ مورد تحلیل دادستان دیوان کیفری بین‌المللی قرار نگرفته بود. وانگهی در سال ۲۰۲۳، دادستان در یک اظهارنظر مهم مکتوب، صراحتاً اعلام نمود که در حالی که هیچ ماده‌ای از اساسنامهٔ رم مشخصاً به حملات سایبری اختصاص ندارد، چنین رفتاری ممکن است به‌طور بالقوه عناصر جنایات جنگی را برآورده کند (Khan, 2023). دفتر دادستانی دیوان نیز آن را به‌عنوان موضع رسمی و کنونی دیوان کیفری بین‌المللی تأیید نمود (Greenberg, 2023). در پرتو این راهبرد، به سبب آن‌که سند عناصر جنایات مذکور در اساسنامهٔ رم (Preparatory Commission for the International Criminal Court, 2000, para. 18)

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

در خصوص مادهٔ ۸ اساسنامهٔ رم، مقرر می‌دارد که «جنایت جنگی ضرورتاً در چهارچوب و با مشارکت در یک مخاصمهٔ مسلحانه انجام می‌شود»، دادستان مکلف است وجود عنصر زمینه‌ایِ «وقوع مخاصمهٔ مسلحانه» برای ارتکاب جنایت جنگی را نیز ثابت کند (Saxon, 2016, p. 558). بر این اساس، احراز امکان وقوع مخاصمهٔ مسلحانه از طریق رایاجنگ‌ها به‌عنوان «مهم‌ترین عامل زمینه‌ای در تلقی یک رایاجنگ به‌عنوان جنایت جنگی» دانسته می‌شود که در صورت وقوع رایاجنگ در بستر آن و علیه اهداف محافظت‌شدهٔ غیرنظامی مذکور در مادهٔ ۸ اساسنامهٔ رم، می‌توان از تحقق جنایت جنگی سخن گفت.

به‌منظور بررسی امکان وقوع جنایات جنگی سایبری از رهگذر ایجاد مخاصمهٔ مسلحانهٔ سایبری به‌عنوان عنصر زمینه‌ایِ وقوع جنایات مذکور، پژوهشگران میان رایاجنگ‌های «تخریبگر»[2] (دارای اثرات فیزیکی مشابه جنگ‌های سنتی) و رایاجنگ‌های «مختل‌کننده»[3] (دارای آثار غیرفیزیکی همچون تخریب داده‌ها یا اختلال در برنامه‌های رایانه‌ای) تمایز قائل شده و اغلب بر آن نظرند که صرفاً رایاجنگ‌های تخریبگر می‌توانند به آستانهٔ توسل به زور و یک مخاصمهٔ مسلحانه واصل شده و جنایت جنگی را شکل بدهند (Schmitt, 2011, p. 573; Schmitt, 1999, p. 17; Joyner, Lotrionte, 2001, p. 850; Creekman, 2001, p. 166; Silver, 2002, p. 85; Duncan, 2008, p. 7; Hoisington, 2009, p. 447; Kerschischnig, 2012, p. 135; Dinniss, 2012, p. 74; Schmitt, 2013, p. 48; Radziwill, 2015, p. 131). مبتنی بر همین رویکرد، 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» (رنجبر؛ گرشاسبی، ۱۳۹۹، ص۲۴۵).

برعکس، تلقی رایاجنگ‌های مختل‌کنندهٔ بدون آثار فیزیکی که صرفاً ایجاد اختلال می‌نمایند، به‌عنوان توسل به زور سایبری و ایجادگر مخاصمهٔ مسلحانهٔ سایبری، دارای مخالفان جدی است (Barkham, 2001, p. 84-85; Lin, 2010, p. 73)، هرچند برخی نیز با آن موافقت کرده‌اند (Hoisington, 2009, p. 447; Silver, 2002, p. 85; Schmitt, 1999, p. 913). رایاجنگ‌های مختل‌کننده در برخی مواقع که در زیرساخت‌های حیاتی یک کشور ایجاد اختلال می‌کنند، قادر به

2. Destructive

3. Disruptive

ایجاد اثراتی بسیار شدیدتر از رایاجنگ‌های تخریبگر نیز هستند (Lin, 2010, p. 74) و این‌که رایاجنگ‌های دارای پیامدهای مستقیم یا غیرمستقیمِ بحران‌آفرین برای بقای دولت مورد هدف، به‌عنوان توسل به زور و ایجادگر جنایت جنگی شناسایی نشوند، غیرمنطقی به نظر می‌رسد. توضیح آن‌که، آن‌گونه که یکی از گونه‌های حملات سایبری را اقداماتی دانسته‌اند که موضوعات آن‌ها امنیت سامانه‌ها، داده‌ها یا شبکه‌هاست (نجفی ابرندآبادی، ۱۳۹۵، ص۱۲)، منظور از این‌گونه حملات سایبری و رایاجنگ‌های مختل‌کننده، اقداماتی است که «جریان اطلاعات یا عملکرد سیستم‌های اطلاعاتی را بدون ایجاد آسیب یا خسارت فیزیکی، قطع می‌کنند» (Brown, Tullos, 2012). با توجه به این‌که اتکا به فضای سایبر و انتقال داده‌ها «تقریباً در هر جامعه‌ای ضروری شده است» (Kilovaty, 2016, p. 116)، این‌گونه از رایاجنگ‌های مختل‌کننده می‌توانند پیامدهای مخربی برای جمعیت غیرنظامی داشته باشند.

اصطلاح «زیرساخت‌های حیاتی» به زیرساخت‌ها، دارایی‌ها یا سیستم‌هایی اشاره می‌کند که یک دولت آن‌ها را برای حفظ عملکردهای حیاتی اجتماعی ضروری می‌شمارد یا تهدید آن را خطر جدی بالقوه‌ای برای جامعه می‌داند (Myjer, 2015, p. 287-290). بیشتر تعاریف، در میان بخش‌های خدمات دولتی و عمومی، امنیت، غذا، آب، حمل‌ونقل، انرژی، بهداشت، مالی و بانک را به‌عنوان بخش‌های حیاتی در نظر می‌گیرند (General Assembly of the United Nations, 2003; Tsagourias, 2012, p. 231). با این حال، هیچ تعریف پذیرفته‌شدهٔ جهانی از آنچه زیرساخت‌های حیاتی را تشکیل می‌دهند، وجود ندارد (Roscini, 2014, p. 56; Focarelli, 2015, p. 268). اکثر دولت‌ها تعریف خود را از آنچه که بخش حیاتی و زیرساخت‌های حیاتی را تشکیل می‌دهد، اتخاذ می‌کنند. دولت‌ها فهرستی از بخش‌های حیاتی را شناسایی می‌کنند و سپس در داخل هر بخش، زیرساخت‌های حیاتی را مورد شناسایی قرار می‌دهند.

با این توضیح، فارغ از این پیش‌زمینه که رویکرد غالب جهانی برای تلقی یک رایاجنگ به‌عنوان جنایت جنگی، ایجاد آثار فیزیکی است، این پژوهش می‌کوشد که به این پرسش بحث‌برانگیز پاسخ دهد که «آیا به سبب وقوع رایاجنگ‌های مختل‌کننده علیه زیرساخت‌های حیاتی یک کشور، امکان وقوع جنایت جنگی از رهگذر تحقق مخاصمهٔ مسلحانهٔ سایبری، به‌عنوان مهم‌ترین عنصر عمومی و زمینه‌ای برای وقوع جنایات جنگی سایبری، وجود دارد یا خیر؟». فرض این پژوهش بر آن است که اگر هدف یک رایاجنگ، ایجاد اختلال در یک

زیرساخت حیاتی باشد، عامل تشدیدکننده‌ای است که ممکن است تحت تفسیری پویا از مفهوم «شدت»، موجب شناسایی رایاجنگ مذکور به‌عنوان توسل به زور و جنایت جنگی شود. برای پاسخ به سؤال پژوهش و ارزیابی فرضیهٔ آن، مصادیق زیرساخت‌های حیاتی و آثار ناشی از رایاجنگ‌های مختل‌کنندهٔ زیرساخت‌های حیاتی، به‌منظور تبیین اهمیت آن‌ها مورد بسط واقع شده و سپس، ضمن واکاوی شرط مبنایی وقوع جنایات جنگی سایبری، یعنی مخاصمهٔ مسلحانهٔ سایبری، به شناسایی آستانهٔ وقوع مخاصمهٔ مسلحانهٔ بین‌المللی از رهگذر رایاجنگ‌های مختل‌کنندهٔ زیرساخت‌های حیاتی پرداخته می‌شود و نهایتاً پس از طرح چالش مربوط به تلقی زیرساخت‌های حیاتی سایبری با کاربرد دوگانه به‌عنوان اهداف نظامی مشروع، مبتنی بر اتخاذ رویکردی پویا، رسیدگی به رایاجنگ‌های مختل‌کننده علیه زیرساخت‌های حیاتی نزد دیوان کیفری بین‌المللی پیشنهاد خواهد شد.

۱. آثار رایاجنگ‌های مختل‌کننده بر زیرساخت‌های حیاتی

برای شناخت اهمیت ایجاد آثار سوء بر زیرساخت‌های حیاتی کشورها از سوی رایاجنگ‌ها و درک ماهیت ویرانگر اختلال در عملکرد زیرساخت‌های حیاتی، ابتدا مصادیق زیرساخت‌های حیاتی در اسناد سازمان ملل متحد، کمیسیون اروپا و قوانین ملی، واکاوی می‌گردد و سپس به برخی آثار ناشی از رایاجنگ‌های مختل‌کننده بر چنین زیرساخت‌هایی اشاره می‌شود.

۱-۱. مصادیق زیرساخت‌های حیاتی

در سطح بین‌المللی، مجمع عمومی سازمان ملل متحد در سال ۲۰۰۳، قطعنامه‌ای را دربارهٔ «ایجاد فرهنگ جهانی امنیت سایبری و حفاظت از زیرساخت‌های اطلاعاتی حیاتی» به تصویب رساند و مقرر نمود که زیرساخت‌های حیاتی عموماً به «تولید، انتقال و توزیع انرژی، حمل‌ونقل هوایی و دریایی، خدمات بانکی و مالی، تجارت الکترونیک، تأمین آب، توزیع مواد غذایی و بهداشت عمومی» مربوط است. این فهرست قطعی نیست و قطعنامه چنین مقرر نموده است که «هر کشور زیرساخت‌های اطلاعاتی حیاتی خود را تعیین خواهد کرد» (General Assembly of the United Nations, 2003). اتحادیهٔ اروپا نیز برنامهٔ خود را برای حفاظت از زیرساخت‌های حیاتی (EPCIP)،[۴] به‌عنوان چهارچوبی برای نتیجه‌بخشی به تلاش‌های خود جهت حفاظت از زیرساخت‌های

4. European Programme for Critical Infrastructure Protection

حیاتی در اروپا، به تصویب رسانده است (European Union, 2006) و در آن، میان زیرساخت‌های حیاتی ملی و زیرساخت‌های حیاتی اروپایی تمایز قائل می‌شود که مورد دوم به زیرساخت‌های حیاتی واقع در کشورهای عضو اشاره می‌کند که اختلال یا تخریب آن تأثیر قابل‌توجهی بر حداقل دو کشور عضو خواهد داشت. دستورالعمل شناسایی و تعیین زیرساخت‌های حیاتی اروپا و ارزیابی نیاز به بهبود حفاظت از آن‌ها[5] مصوب ۲۰۰۸ نیز دو بخش از زیرساخت‌های حیاتی ملی را فهرست می‌کند که هر یک چندین زیربخش را در بر می‌گیرد: اول، انرژی (برق، نفت و گاز) و دوم، حمل‌ونقل (حمل‌ونقل جاده‌ای، ریلی، هوایی، آبراهه‌های داخلی و نیز کشتی‌رانی اقیانوسی و دریایی و بنادر) (European Union, 2008, Annex I). البته این فهرست را می‌توان نسبتاً فهرستی محدود دانست، زیرا فقط بر زیرساخت‌های حیاتیِ بااهمیت اروپایی تمرکز دارد.

در سال ۲۰۰۴، کمیسیون اروپا بیانیه‌ای را در خصوص «حفاظت از زیرساخت‌های حیاتی در مبارزه با تروریسم»[6] تصویب کرد که شامل فهرستی از زیرساخت‌های حیاتی بود که به زیرساخت‌های حیاتی اروپایی محدود نمی‌شد. بر اساس این فهرست، بخش‌هایی که شامل زیرساخت‌های حیاتی می‌شوند، عبارت‌اند از: ۱. تأسیسات و شبکه‌های انرژی؛ ۲. ارتباطات و فناوری اطلاعات (مثل مخابرات، سیستم‌های پخش، نرم‌افزار، سخت‌افزار و شبکه‌ها از جمله اینترنت)؛ ۳. امور مالی؛ ۴. زیرساخت‌های مربوط به نهادهای مراقبت از سلامت و بهداشت؛ ۵. تغذیه؛ ۶. آب (برای مثال: سدها، ذخیره‌سازی، تصفیه و شبکه‌ها)؛ ۷. حمل‌ونقل؛ ۸. تولید، نگهداری و حمل‌ونقل کالاهای خطرناک؛ ۹. حاکمیت (European Union, 2004, p. 4).

ایالات متحده نیز در طی زمان، رویکردهای مختلفی را در خصوص زیرساخت‌های حیاتی اتخاذ کرده است (Roscini, 2014, p. 56). در حال حاضر، زیرساخت‌های حیاتی شامل فهرستی از شانزده بخش حیاتی می‌شود، از جمله: ۱. شیمیایی؛ ۲. تسهیلات تجاری؛ ۳. ارتباطات؛ ۴. تولیدات حیاتی؛ ۵. سدها؛ ۶. پایگاه صنعتی دفاع؛ ۷. خدمات اضطراری؛ ۸. انرژی؛ ۹.خدمات مالی؛ ۱۰. غذا و کشاورزی؛ ۱۱. تسهیلات دولتی؛ ۱۲. بهداشت و سلامت عمومی؛ ۱۳.فناوری اطلاعات؛ ۱۴. رآکتورهای هسته‌ای، مواد و پسماندها؛ ۱۵. سامانه‌های حمل‌ونقل؛ ۱۶. سامانه‌های آب و فاضلاب (US White House, 2013).

5. Directive on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection

6. Critical Infrastructure Protection in the Fight against Terrorism

فرانسه دوازده بخش از زیرساخت‌های حیاتی را شناسایی کرده است[۷] که به سه دسته، به شرح ذیل تقسیم می‌شوند: ۱. حاکمیت (فعالیت‌های غیرنظامی دولت، فعالیت‌های نظامی دولت، فعالیت‌های قضائی، 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، حمل‌ونقل، مالی و صنعت) (Delerue, 2020, p. 301).

سه مثال از فهرست‌های بخش‌های حیاتی که در بالا ارائه شد، نشان می‌دهد که کشورها فهرست‌ها و رویکردهای متفاوتی را برای تعریف و برشماری زیرساخت‌های حیاتی اتخاذ می‌کنند، هرچند این فهرست‌ها بسیار شبیه یکدیگرند. زیرساخت‌های حیاتی امروزی به‌طور اساسی به سامانه‌ها و شبکه‌های رایانه‌ای وابسته بوده و بنابراین، به‌ویژه در برابر رایاجنگ‌های مختل‌کننده آسیب‌پذیرند (Shackelford, 2009, p. 199). مشخصاً، زیرمجموعه‌ای از زیرساخت‌های حیاتی که به‌طور خاص به شبکه‌ها و سامانه‌های رایانه‌ای مربوط می‌گردد، به‌عنوان «زیرساخت‌های اطلاعاتی حیاتی»[۸] شناخته می‌شود. زیرساخت‌های اطلاعاتی حیاتی شبکه‌ها و سامانه‌های رایانه‌ای‌اند 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). بر این اساس، دفاع حقوقی در برابر رایاجنگ‌های مختل‌کنندهٔ زیرساخت‌های مذکور را می‌توان دارای اهمیت راهبردی برای کشورها دانست. این موضوع آن‌گاه اهمیت مضاعف می‌یابد که دریافته شود که آسیب‌پذیری زیرساخت‌های حیاتی در برابر رایاجنگ‌ها دو بعد دارد: از یک سو، آسیب‌پذیری سامانه‌ها و شبکه‌های رایانه‌ای که زیرساخت‌های حیاتی بر آن‌ها تکیه دارند و از سوی دیگر، آسیب‌پذیری سامانه‌ها و شبکه‌های رایانه‌ای که خود زیرساخت‌های حیاتی را تشکیل می‌دهند.

۲-۱. آثار رایاجنگ‌های مختل‌کننده بر زیرساخت‌های حیاتی

رویدادهای مختلف در چند دههٔ گذشته، نشان داده است که تداخل در عملکرد زیرساخت‌های حیاتی، خصوصاً زیرساخت‌های اطلاعاتی حیاتی، می‌تواند تهدیدی جدی برای شهروندان غیرنظامی باشد. به‌ترتیب در سال‌های ۲۰۰۷ و ۲۰۰۸، استونی و گرجستان هر دو متحمل حملات

---

۷. در فرانسه، «زیرساخت‌های حیاتی» به «OIV (operateur d'importance vitale)» و «بخش‌های حیاتی» به «SAIV (secteurs d'activités d'importance vitale)» ترجمه می‌شود.

8. critical information infrastructures (CII)

سایبری بندآوری توزیع‌شدهٔ خدمت[9] شدند که وب‌سایت‌های دولتی آن‌ها را از بین برد (Miller, 2014, p. 222-224) و در مورد اولی، خطوط ارتباط اضطراری را برای مدت کوتاهی از دسترس خارج کرد (Bussolati, 2015, p. 102). اگرچه ممکن است حملاتِ «بندآوری توزیع‌شدهٔ خدمت» به گرجستان و استونی در مقایسه با تخریب‌هایی که می‌تواند با روش‌های جنگی متعارف ایجاد شود، نسبتاً بی‌اهمیت به نظر برسد، برخی معتقدند که رایاجنگ‌ها حتماً در گذر زمان پیچیده‌تر می‌شوند و می‌توانند عواقب ویرانگری را در آینده ایجاد کنند (Ophardt, 2010, p. 10). قبلاً نیز چندین حادثهٔ سایبری رخ داده است که زیرساخت‌های حیاتی دولت و به‌ویژه زیرساخت‌های مربوط به بهداشت و درمان را تحت تأثیر و در نتیجه، جمعیت شهروندان غیرنظامی را در معرض خطر قرار داده است. به‌طور مثال، حملهٔ باج‌افزار واناکرای[10] در سال ۲۰۱۷، تأثیر شدیدی بر خدمات درمانی ملی انگلستان[11] گذاشت. گزارش شده است که شیوع واناکرای «تنها در انگلستان کامپیوترها را در بیش از ۸۰ سازمان خدمات درمانی ملی خاموش کرد که منجر به لغو تقریباً ۲۰۰۰۰ وقت ویزیت شد، ۶۰۰ جراح پزشکی 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). برای 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 عملیات‌ها داده‌های پزشکی بیماران 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, p. 1).

نمونه‌های دیگر از عملیات‌های سایبری مختل‌کننده که زیرساخت‌های حیاتی را هدف قرار می‌دهند، عبارت‌اند از حمله به شبکهٔ برق اوکراین در دسامبر ۲۰۱۵ و حمله به نیروگاهی هسته‌ای در هند در سپتامبر ۲۰۱۹. چنان‌که ذکر شد، در مورد اول، مهاجمان باعث قطعی برق بین یک تا شش ساعتهٔ نواحی آسیب‌دیده در این کشور شدند و آن‌ها را به‌گونه‌ای تحت تأثیر قرار دادند که آن‌ها به فرمان‌های از راه دورِ اپراتورها پاسخ نمی‌دادند و موجب شدند که تا ماه‌ها کارگران، موج‌شکن‌ها

9. Distributed Denial of Service (DDoS)

10. WannaCry

11. UK's National Health Service (NHS)

را به‌صورت دستی کنترل کنند (Zetter, 2016). در مورد دوم، هیچ نشانه‌ای مبنی بر به خطر افتادن کنترل و بهره‌برداری از نیروگاه وجود نداشت (dragos, 2019) و در عوض، هدفْ جمع‌آوری اطلاعات به نظر می‌رسید (Porup, 2019). در هر دو مورد و برخلاف حملات استاکس‌نت علیه تأسیسات هسته‌ای نطنز در ایران در سال ۲۰۱۰، هیچ آسیب فیزیکی به هیچ یک از تجهیزات وارد نشد، اما با وجود این، حملات مذکور باعث نگرانی قابل توجهی شد. در سال‌های اخیر، دامنهٔ رایاجنگ‌های مختل‌کننده علیه ایران نیز افزایش داشته است که می‌توان به برخی از موارد آن، که مورد مشاهدهٔ عموم بوده است، اشاره کرد: حملات با ویروس‌های رایانه‌ای Flame،Duku و Viper علیه تأسیسات نفتی و هسته‌ای ایران در سال ۱۳۹۱ (گیوکی و دیگران، ۱۴۰۰، ص۲۷۹)، حمله به سامانهٔ سوخت و جایگاه‌های توزیع فراورده‌های نفتی در پاییز سال‌های ۱۴۰۰ و ۱۴۰۲، حمله به سامانهٔ وزارت فرهنگ و ارشاد اسلامی در فروردین ۱۴۰۱ که روند فعالیتِ برخط وزارت مذکور را مختل نمود، حمله به شبکهٔ زیرساختِ مرکز آمار ایران در خرداد سال ۱۳۹۵، حمله به شبکهٔ سازمان ثبت اسناد کشور، حمله به شبکه‌های برخط شهرداری تهران در سال ۱۴۰۱ و حمله به برخی از وب‌سایت‌های دولتی. حملات مذکور مجموعه‌ای از حملات سایبری است که هر کدام قابلیت بالقوه برای ایراد خسارات قابل توجه مالی و نرم‌افزاری یا بحران‌آفرینی اجتماعی نسبت به عموم شهروندان کشور را داشته است. این‌گونه از حملات مختل‌کننده نسبت به زیرساخت‌های حیاتی، از نظر فراوانی و شدت به‌صورت روزافزون افزایش می‌یابند، زیرا زیرساخت‌های حیاتی، بیشتر و بیشتر به صورت آنلاین منتقل می‌شوند و وابستگی روزافزونِ آن‌ها به فناوری اطلاعات و بستر آنلاین بیشتر می‌شود.

کمیتهٔ بین‌المللی صلیب سرخ در گزارش خود در خصوص هزینهٔ انسانی عملیات‌های سایبری اشاره کرد که رشد تصاعدی فضای سایبر از طریق اینترنت اشیا (Morgan, 2014) فرصت‌های حملات سایبری علیه زیرساخت‌های حیاتی را افزایش داده است و هشدار می‌دهد که «هر دستگاه متصل می‌تواند به هدف یا بخشی از یک عملیات سایبری تهاجمی تبدیل شود» (Gisel, Olejnik, 2019, p. 14–15). اشاره شده است که در دنیای دیجیتال امروز، می‌توان یک بازجوی نظامی را در حال جمع‌آوری اطلاعات از نمایه‌های آنلاینِ زندانی، تلفن فیزیکی و داده‌های ذخیره‌شده در فضای ابری تصور کرد که می‌تواند برای عذاب، تحقیر و شرمسارسازی زندانی کافی باشد (Lubin, 2021, p. 4). بر این اساس، رایاجنگ‌های مختل‌کنندهٔ زیرساخت‌های حیاتی می‌توانند برای دسترسی به یا دستکاری در داده‌های شخصی و تضعیف حق بر حریم خصوصی نیز استفاده شوند.

۲. شرط اساسی وقوع جنایت جنگی ناشی از رایاجنگ‌های مختل‌کنندهٔ زیرساخت‌های حیاتی

جنایت جنگی، وفق حقوق بین‌الملل، نقض شدید مقررات و عرف‌های جنگ است که در مخاصمات مسلحانه صورت می‌گیرد (نژندی‌منش، ۱۳۹۴، ص۲۳۱). مطابق با مادهٔ ۸۴ سند مقررات تالین، اقدامات ارتکابی به‌وسیلهٔ ابزارهای سایبری می‌توانند جنایات جنگی به شمار آیند، زیرا حقوق مخاصمات مسلحانه بر ابزارها و روش‌های نوین جنگی که در زمان پدیدار شدن قاعده‌ای از حقوق عرفی منظور نشده‌اند، اعمال می‌گردد (محقق هرچقان و دیگران، «ب»، ۱۴۰۲، ص۳۱۶). هرچند، تغییرات عمده در شیوه‌های جنگیدن ناشی از فناوری‌های نوین انعطاف گسترده را در حقوق بشردوستانهٔ بین‌المللی ضروری می‌نماید (شریفی طرازکوهی، ۱۳۹۵، ص۱۹۲) و موجب طرح مناقشات بسیار میان حقوق‌دانان بین‌المللی شده است (خلیل‌زاده، ۱۳۹۳، ص۶۰). با توجه به این‌که جنایت جنگی در یک وجه، نقض حقوق بشردوستانهٔ بین‌المللی دانسته می‌شود (برادران؛ حبیبی، ۱۳۹۸، ص۱۴۳) و پیش‌شرط قابلیت اجرای قواعد حقوق بشردوستانهٔ بین‌المللی برای وقوع جنایت جنگی، وجود شرطی مبنایی یعنی وقوع مخاصمهٔ مسلحانه است (کاسسه و دیگران، ۱۴۰۱، ص۱۱۰) و تبعاً به‌منظور وقوع جنایت جنگی سایبری، تحقق شرط اساسی وقوع مخاصمهٔ مسلحانهٔ سایبری ضروری است، بر این اساس، در این قسمت تلاش می‌شود تا در سه بخش، اولاً به‌عنوان شرط مبنایی، آستانهٔ وقوع مخاصمهٔ مسلحانهٔ سایبری از طریق رایاجنگ‌ها بررسی شود؛ ثانیاً چگونگی تشکیل مخاصمهٔ مسلحانهٔ سایبری از طریق رایاجنگ‌های مختل‌کنندهٔ زیرساخت‌های حیاتی مورد واکاوی قرار گیرد و نهایتاً، امکان تجمیع رایاجنگ‌های مختل‌کننده برای تشکیل مخاصمهٔ مسلحانه ارزیابی شود.

۲-۱. آستانهٔ مخاصمهٔ مسلحانهٔ سایبری

حسب رأی دادگاه کیفری بین‌المللی برای یوگسلاوی سابق[12] در قضیهٔ تادیچ[13] 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, p. 70). دیوان بین‌المللی دادگستری و منشور سازمان ملل متحد آستانهٔ «زور» ممنوع‌شده در بند ۴ مادهٔ ۲ منشور ملل متحد را مشخص نکرده‌اند. وجود چنین آستانه‌ای از چندین پروندهٔ مطرح نزد دیوان استنباط شده است که در آن‌ها توسل به زور با شدت کم به‌عنوان توسل به زور

12. International Criminal Tribunal for the former Yugoslavia (ICTY)

13. Tadic´

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 (ICJ Rep, 1949, p. 35). برخی از محققان، این رویکرد را به‌عنوان استدلالی برای حمایت از وجود آستانه تحلیل می‌کنند (O'Connell, 2013, p. 102-105). این مجادلهٔ نظری توسط کمیسیون حقیقت‌یاب بین‌المللی در خصوص جنگ علیه گرجستان نیز مطرح شد که بیان کرد: «ممنوعیت توسل به زور شامل تمامی زور مادی که از حداقل آستانهٔ شدت فراتر می‌رود، می‌شود» (Max Planck Institute for Comparative Public Law and International Law, 2009, p. 242)، هرچند در مقابل، برخی دیگر از محققان ادعا می‌کنند که چنین آستانه‌ای وجود ندارد و مستثنا شدن «توسل‌های حداقلی به زور» از محدودهٔ بند ۴ مادهٔ ۲ را رد می‌کنند (Ruys, 2014, p. 159-210; Hoogh, 2009).

مبتنی بر شرط مارتنس، 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 (دهقانی و دیگران، ۱۴۰۱، ص۱۴۰) و بر جریان حقوق بشردوستانه حکم خواهد شد، لکن در خصوص راه تعیین آستانهٔ وقوع مخاصمهٔ مسلحانه و توسل به زور در رایاجنگ‌ها، نظریات مختلفی مطرح شده است، هرچند اجماعی بر این‌که حمله‌ای سایبری در چه سطحی به مخاصمهٔ مسلحانه تبدیل می‌شود، حاصل نشده است (رضائی؛ جلالی، ۱۳۹۷، ص۷۰۲). یکی از روش‌های مشهور در ادبیات نظری موجود، روش ارائه‌شده در سند مقررات تالین[۱۴] است. قاعدهٔ ۱۱ از نسخهٔ نخست و قاعدهٔ ۶۸ از نسخهٔ دوم سند مقررات تالین نیز 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 (Schmitt, 2013, p. 47-52; Schmitt & Vihul, 2017, p. 333-337). برای این منظور،

۱۴. 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 را که متخصصان و محققان حقوق بین‌الملل طرح‌ریزی کردند، در 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. نسخهٔ دوم سند در سال ۲۰۱۷ که توسط گروهی متنوع‌تر از کارشناسان تشکیل شد، 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.

سند مقررات تالین آزمایش پیچیدهٔ هشت‌قسمتی را برای تعیین این‌که آیا یک عملیات سایبری خاص توسل به زور و واصل به آستانه مخاصمهٔ مسلحانه محسوب می‌شود یا خیر، پیشنهاد می‌کند که برخی پژوهشگران، آن‌ها را «ضوابط و معیارهای تعیینی نظری در شدت آستانه» دانسته‌اند (محقق هرچقان و دیگران، ۱۴۰۱، ص۲۸۷-۲۸۹). این آزمونِ دشوار شامل ارزیابی موارد ذیل است: شدت،[۱۵] فوریت،[۱۶] مستقیم بودن،[۱۷] تهاجمی بودن (مداخله‌آمیز بودن)،[۱۸] قابل اندازه‌گیری بودن اثرات،[۱۹] ماهیت نظامی داشتن،[۲۰] سطح مشارکت دولت[۲۱] و مشروعیت احتمالی.[۲۲] از میان معیارهای مذکور، معیار «آستانهٔ شدت» مقبولیت بیشتری در ادبیات رایج حقوق بین‌الملل یافته و با تضعیف هفت معیار دیگر، چنین گفته شده است که «تنها معیاری که باقی می‌ماند شدت است» (Silver, 2002, p. 89-92). معیار «شدت» مطرح‌شده در سند مقررات تالین، اساساً مبتنی بر مقایسه 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» و «زمانی که مقیاس و اثرات آن با عملیات غیرسایبری که به سطح توسل به زور می‌رسد، قابل مقایسه باشد» (Schmitt & Vihul, 2017, p. 330) و اشاره می‌کند که «پیامدهایی شامل خسارت فیزیکی به افراد یا اموال» از آستانهٔ شدت عبور می‌کنند (Schmitt & Vihul, 2017, p. 334). چنان‌که ملاحظه می‌شود، در مقررات سند مذکور، هیچ اشاره‌ای به عملیات سایبری که منجر به خسارات نامشهود محض می‌شود، نشده است. از این

۱۵. این معیار بر پیامدها تمرکز دارد و درجهٔ خسارت یا آسیب را ارزیابی می‌کند.

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

۱۷. 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.

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

۱۹. بر این اساس، هر چقدر که اثرات عملیات سایبری قابل پیش‌بینی و شناسایی باشد، امکان شناسایی به‌عنوان توسل به زور آسان‌تر است.

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

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

۲۲. این معیار به دنبال این ارزیابی است که آیا عملیات سایبری می‌تواند به دسته‌های دیگری از اقدامات حقوق بین‌الملل تعلق داشته باشد که آن را مشروع سازد یا خیر.

عدم اشاره، شاید بتوان این‌گونه استنباط نمود که برای کارشناسان تدوینگر سند مقررات تالین، عملیات‌های 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 عملیات‌های سایبری مختل‌کننده دانست، ناگزیر می‌بایست به رویکرد سند مذکور در عملیات‌های سایبری تخریبگر متوسل شد که بر آثار فیزیکی در ارزیابی یک عملیات سایبری به‌عنوان توسل به زور، تمسک می‌جوید. چنان‌که ذکر شد، تفسیر قاعدهٔ شمارهٔ ۶۹ به‌صراحت این احتمال را که عملیات‌های 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 کنند (Schmitt and Vihul, 2017, p. 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 بشردوستانهٔ بین‌المللی، به‌عنوان مبنای تحلیل‌های سند مقررات تالین، تدوین می‌شدند، تصورناپذیر 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 عملیات‌های سایبری مختل‌کننده به رشد کمّی و کیفیِ کنونی نرسیده بودند.

یک روش دیگر که تحت آموزه‌های نظری حقوق بین‌الملل پیشنهاد شده، این است که اگر اختلال ایجادشده در نتیجهٔ عملیات سایبری، به اندازهٔ 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, p. 55) که با این معیار می‌توان رایاجنگ‌های مختل‌کنندهٔ زیرساخت‌های حیاتی را در سطح آستانهٔ مذکور تلقی نمود.

یک روش خلاقانه در سال ۲۰۲۱، توسط محققان پروژهٔ آکسفورد در خصوص حمایت‌های

حقوق بین‌الملل در فضای سایبر پیشنهاد شد (Akande & Hollis, 2020)[۲۳]. بر اساس آن، تمرکز بر آثار عملیات سایبری، امکان نقض بند ۴ مادهٔ ۲ توسط عملیات‌های سایبری فاقد تأثیرات خاص را نادیده می‌گیرد (Hollis & Benthem, 2021) و این همان رویکردی است که در ادامهٔ این پژوهش، در خصوص رایاجنگ‌های مختل‌کنندهٔ زیرساخت‌های حیاتی، در خصوص آن بحث می‌شود.

۲-۲. مخاصمهٔ مسلحانهٔ سایبری از رهگذر رایاجنگ‌های مختل‌کنندهٔ زیرساخت‌های حیاتی

مبتنی بر رویکرد عمدتاً غالب، تعیین این‌که آیا یک رایاجنگ به‌منزلهٔ توسل به زور است یا خیر، اساساً به تأثیراتی که ایجاد می‌کند، بستگی دارد. به نظر می‌رسد 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 (فقیه حبیبی، ۱۳۹۵، ص۱۲۸) و شناسایی سند مقررات تالین در خصوص رایاجنگ‌هایی که فقط اثرات سایبری، دیجیتال و غیرفیزیکی ایجاد می‌کنند، مانند تخریب یا اخلال در داده‌ها، نیازمند تأمل بیشتر است. با عنایت به این‌که سند مقررات تالین نیز تأکید ویژهٔ خود را بر عامل «شدت» به‌عنوان شاخص توسل به زور، معطوف داشته و از سوی دیگر نیز عامل مذکور را به‌گونه‌ای «پیامدمحور» تحلیل می‌نماید، حتی می‌توان با تمسک به سند مقررات تالین، با توجه به پیامدهای بحران‌آفرین رایاجنگ‌های مختل‌کنندهٔ زیرساخت‌های حیاتی، از تحقق معیار «شدت» و وقوع مخاصمه در اثر ارتکاب چنین رایاجنگ‌هایی سخن گفت.

همچنین، مضاف بر این‌که ارتکاب رایاجنگ‌های مختل‌کننده علیه زیرساخت‌های حیاتی می‌تواند تحقق‌بخش معیار «شدت» تلقی شود، با این حال، با عنایت به این‌که ماهیت هدف نیز ممکن است بر این‌که یک رایاجنگ به‌عنوان توسل به زور سایبری شناسایی شود یا خیر تأثیر بگذارد، ارتکاب رایاجنگ‌های مختل‌کننده علیه زیرساخت‌های حیاتی نیز به سبب ماهیت پراهمیت هدفِ خود، یارای شناسایی به‌عنوان رفتارهای مشمول وصف توسل به زور، به نظر می‌رسند. به‌طور مثال، یک رایاجنگ با اثرات مخرب محدود به شبکهٔ رایانه‌ایِ یک کتابخانهٔ شهری به‌وضوح به‌منزلهٔ توسل به زور نخواهد بود. برعکس، اگر شبکهٔ

۲۳. 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. بدان سبب که اکثر قریب به اتفاق زیرساخت‌های سایبری متعلق به شرکت‌های خصوصی است، مشارکت بخش خصوصی برای تضمین موفقیت در ایجاد چهارچوبی هنجاری، ضروری است و این یک چالش منحصربه‌فرد دیگر در اعمال مقررات حقوق بین‌الملل در فضای سایبر است.

مختل‌شده، یک زیرساخت اطلاعاتی حیاتی باشد یا برای عملکرد یک زیرساخت اطلاعاتی حیاتی ضروری باشد، رایاجنگ مذکور به احتمال زیاد به‌عنوان توسل به زور شناخته می‌شود، علی‌رغم این‌که صرفاً اثرات دیجیتالی ایجاد می‌کند (Roscini, 2016, p. 245). رایاجنگی که اثرات فیزیکی ایجاد نمی‌کند، اما یک زیرساخت حیاتی را هدف قرار می‌دهد که چنین هدفی یک عنصر تعیین‌کننده برای تغییر شناسایی عملیات به‌عنوان توسل به زور یا عدم آن می‌باشد، عموماً تحت شرایط توسل به زور دانسته می‌شود و برعکس، اگر رایاجنگ فقط اثرات غیرفیزیکی ایجاد کند که بر زیرساخت‌های حیاتی کشور مورد نظر تأثیری نداشته باشد، بعید است که این رایاجنگ واجد شرایط توسل به زور دانسته شود (Roscini, 2014, p. 58). بنابراین، اتکای فزاینده بر زیرساخت‌های حیاتی به این معناست که یک عملیات سایبری مختل‌کننده که زیرساخت‌های حیاتی ملی را غیرفعال می‌کند، می‌تواند به همان اندازه شدید و خشونت‌آمیز باشد که یک رایاجنگ منجر به تخریب فیزیکی، شدید و خشونت‌آمیز است. بر این اساس، تمرکز سند مقررات تالین بر خسارت فیزیکی، نارسایی‌های استدلال آن را در قیاس با سلاح‌های سنتی در زمینهٔ ایجاد یک مخاصمهٔ مسلحانهٔ سایبری برجسته می‌کند. 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 قابل توجه بر جامعه محسوب می‌شوند، به‌ویژه اگر اثرات آن‌ها بلندمدت باشد. در چهارچوب این شاخص، آسیب‌های بحران‌آفرین اجتماعی و اقتصادی را نیز باید در این زمینه در نظر گرفت. در این راستا، به نظر 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.

یکی از علت‌هایی که ممکن است به‌عنوان چالش مانع برای تلقیِ رایاجنگ‌های مختل‌کنندهٔ زیرساخت‌های حیاتی به‌عنوان جنایت جنگی تلقی شود، دشواری ارزیابی و عدم وجود معیار عینی برای سنجش چنین آثاری است. این در حالی است که به نظر می‌رسد اولاً در رایاجنگ‌های تخریبگر نیز ایجاد آثار فیزیکی در جهان خارجی الزاماً موجب تلقی یک رایاجنگ تخریبگر به‌عنوان توسل به زور نمی‌شود و نمی‌توان صرف ایجاد آثار فیزیکی را

به‌عنوان شاخص الزامی برای تحقق توسل به زور دانست. به‌طور مثال، ارتکاب عملیات سایبری علیه یک گوشی همراه هوشمند در کشور دیگر که موجب افزایش حرارت و تخریب فیزیکی واحد پردازش مرکزی گوشی مذکور می‌شود، هیچ گاه به‌عنوان توسل به زور دانسته نخواهد شد. سند مقررات تالین نیز بر آن نظر است که «یک حادثهٔ سایبری که تنها باعث آسیب، تخریب، جراحت یا مرگ محدود شود، لزوماً مخاصمهٔ مسلحانهٔ بین‌المللی محسوب نمی‌شود» (Schmitt & Vihul, 2017, p. 383-384). در غیر از رایاجنگ‌ها و در چهارچوب جنگ‌های سنتی نیز ایجاد آثار فیزیکی محدود را نمی‌توان به‌عنوان معیار در تحقق توسل به زور دانست. 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 به‌صرف عدم ایجاد آثار فیزیکی، حکم به 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 در حالی است که مشروعیت‌بخشی به چنین اقداماتی به‌صرف عدم ایجاد آثار فیزیکی، با تردید جدی مواجه است، زیرا چنین اقداماتی می‌توانند تمام ارتباطات داخل و خارج از کشور هدف را مختل کنند، جریان تجارت و نظام اقتصادی کشور هدف را با تعطیلی مواجه گردانند و زیرساخت‌های اطلاعاتی کشور هدف را به‌طور کلی ناکارآمد سازند (Barkham, 2001, p. 91). جوازبخشی به ایجاد چنین بحران‌هایی در کشور هدف را نمی‌توان صرفاً به سبب عدم ایجاد آثار فیزیکی، موجه نمود. خارج نمودنِ رایاجنگ‌های مختل‌کننده به‌صرف عدم وجود معیار عینی برای ارزیابی آن‌ها در تحقق توسل به زور در حالی ناموجه است که رایاجنگ‌های مذکور می‌توانند به‌صورت‌های بحران‌آفرین، صلح و امنیت بین‌الملل را مورد خدشه قرار دهند و جوازبخشی به آن‌ها به سبب عدم وجود معیار عینی، نتیجتاً موجب نقض غرض حقوق بین‌الملل است که هدف آن، تضمین صلح و امنیت بین‌الملل می‌باشد. نگارندگان ضمن عدم پذیرش دلیل مخالفت مذکور، بر آن‌اند 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 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. رابعاً آن‌گونه که احتساب رایاجنگ‌های تخریبگر به‌عنوان توسل به زور نیز صرفاً بر اساس معیارِ ایجاد آثار فیزیکی، مورد انتقاد قرار گرفته، معیارهای دیگری برای تحقق توسل به زور سایبری پیشنهاد شده است.

در چهارچوب حقوق کیفری بین‌المللی، الزام به ایجاد خسارات فیزیکی از سوی عملیات‌های سایبری، به دلایل عمده مشکل‌ساز است و شاید همین موضوع باعث شده است که بتوان ادعا کرد نتیجه‌گیری سند مقررات تالین در خصوص این موضوع، بیان‌کنندهٔ یک اجماع نبوده و تاکنون نیز موجب ایجاد اجماع نشده است، تا آن‌جا که، چنان‌که اشاره شد، برخی دولت‌ها و اندیشمندان، دیدگاه مخالف را اتخاذ کرده‌اند و استدلال می‌کنند که اگر عملیات‌های سایبری مختل‌کننده به اندازهٔ کافی شدید باشند که امنیت دولت را خصوصاً با اثرگذاری بر زیرساخت‌های حیاتی، تحت تأثیر قرار دهند، باید به معنای توسل به زور باشند (Roscini, 2014, p. 245; Ziolkowski, 2010, p. 73–75). به‌عنوان مثال، فرانسه «این امکان را رد نمی‌کند که یک عملیات سایبری بدون اثرات فیزیکی نیز به‌عنوان توسل به زور شناخته شود» و 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 منشأ 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» (Ministry of the Armies, 2019, p. 7).

به‌طور مشابه، هلند این دیدگاه را بیان کرده است که «نمی‌توان رد کرد که عملیاتی سایبری با تأثیرات 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, Appendix, 2019, p. 4). به‌طور کلی، دولت‌هایی که زیرساخت‌های آن‌ها وابستگی بیشتری به فضای سایبر دارد و بیشتر در معرض این‌گونه حملات قرار می‌گیرند، طبیعتاً تمایل دارند هر گونه حملهٔ سایبری را تهدید و توسل به زور در چهارچوب بند ۴ مادهٔ ۲ منشور ملل متحد به حساب آورند (آهنی امینه؛ فتح‌اللهی، ۱۳۹۳، ص۱۲۳) تا بتوانند به حق دفاع مشروع متوسل شوند (کیهانلو؛ رضادوست، ۱۳۹۴، ص۲۰۴). بر همین اساس است که دولت هلند حتی تا آن‌جا پیش رفته که گفته است «اگر حمله‌ای سایبری کل سیستم مالی هلند را هدف قرار دهد ... یا

اگر دولت را از انجام وظایف اساسی مانند نظارت یا اخذ مالیات باز دارد ... به‌عنوان حمله‌ای مسلحانه تلقی می‌شود و بنابراین باعث می‌شود که یک دولت حق دفاع مشروع را حتی با توسل به زور، داشته باشد» (Bijleveld, 2018).

همچنین حملات متعدد به زیرساخت‌های حیاتی درمانی که در طی شیوع کووید-۱۹ روی داد، بحث‌های دوباره دربارهٔ ماهیت رایاجنگ‌های مختل‌کننده و این بحث را که آیا ایجاد مخاصمهٔ مسلحانه توسط آن‌ها نیازمند عواقب فیزیکی است یا خیر، موجب شد. پژوهشگران معتقدند که به دلیل شدت همه‌گیری و مقیاس تأثیرات ویروس در سراسر جهان، دولت‌ها تمایل بیشتری دارند تا رایاجنگ‌های مختل‌کننده‌ای را که زیرساخت‌های مراقبت‌های درمانی آن‌ها را هدف قرار می‌دهند، به‌عنوان مخاصمهٔ مسلحانه 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» (Milanovic & Schmitt, 2020, p. 12). این اعلامیه‌های دولت‌ها و ملاحظات پژوهشی نشان می‌دهد که حقوق عرفی در خصوص توسل به زور و ایجاد مخاصمهٔ مسلحانه و جنایت جنگی در فضای سایبر به‌سمتی پیش می‌رود که روزاروز بیشترْ شامل خسارت‌های دیجیتال و غیرفیزیکی ناشی از رایاجنگ‌های مختل‌کنندهٔ زیرساخت‌های حیاتی می‌شود.

۲-۳. تجمیع رایاجنگ‌های مختل‌کنندهٔ پایین‌تر از آستانهٔ مخاصمهٔ مسلحانه

در برخی شرایط، دولتی ممکن است قربانی برخی رایاجنگ‌های مختل‌کنندهٔ زیرساخت‌های حیاتی واقع شود که مجموعاً از آستانهٔ توسل به زور عبور می‌کنند. با این حال، هر یک به‌صورت جداگانه، در مرتبه‌ای پایین‌تر از مخاصمه‌ای مسلحانه واقع می‌گردد (Dinniss, 2012, p. 93-95). اینْ راهکاری است که اغلب مرتکبین رایاجنگ‌های مختل‌کننده علیه زیرساخت‌های حیاتی با استفاده از مجموعه‌ای از حملات با شدت خفیف‌تر از یک حملهٔ واحد شدید، به کار می‌برند (داینیس، ۱۳۹۵، ص۱۰۷). نظریهٔ «تجمیع رویدادها» که به آن نظریهٔ «خراشیدن با نوک سوزن»[۲۴] نیز گفته می‌شود، به چنین موقعیت‌هایی می‌پردازد. این نظریه استدلال می‌کند که در این شرایط،

24. pin-prick theory

هر رویدادی که به‌صورت مجزا انجام می‌شود، به‌منزلهٔ مخاصمهٔ مسلحانه نیست، اما به‌طور تجمیعی، مخاصمهٔ مسلحانه یا حتی حملهٔ مسلحانه محسوب می‌شوند. دیوان بین‌المللی دادگستری در پروندهٔ نیکاراگوئه، با طرح این سؤال، راه را برای پذیرش این نظریه هموار کرد که آیا حملات جزئیِ مشروع ممکن است در تجمیع با هم، «حملهٔ مسلحانه» تلقی شوند یا خیر (ICJ Report, 1986, p. 119-120). همچنین می‌توان رویکردی مشابه را در پروندهٔ سکوهای نفتی[۲۵] و پروندهٔ کنگو علیه اوگاندا[۲۶] نیز یافت (ICJ Report, 2003, p. 191; ICJ Report, 2005, p. 223).

در برخی شرایط، رایاجنگ‌های مختل‌کنندهٔ زیرساخت‌های حیاتی ممکن است همزمان علیه اهداف مختلف انجام شود تا اثرات آن به حداکثر برسد. برای مثال، در خصوص عملیات‌های سایبری علیه استونی در سال ۲۰۰۷، چندین نهاد دولتی و خصوصی به‌طور همزمان هدف قرار گرفتند.[۲۷] در شرایطی مانند رایاجنگ‌ها علیه استونی، نظریهٔ تجمیع رویدادها اجازه می‌دهد تا واقعیت حملهٔ در حال انجام که از چندین عملیات سایبری تشکیل شده است، در نظر گرفته شود. علاوه بر این، اکثر رایاجنگ‌های علیه زیرساخت‌های حیاتی که از آستانهٔ توسل به زور عبور می‌کنند و مخاصمه‌ای مسلحانه را تشکیل می‌دهند، ممکن است به حملهٔ مسلحانهٔ موجدِ حق دفاع مشروع تبدیل نشوند. ازاین‌رو، تجزیه و تحلیل آن‌ها در ترکیب با یکدیگر، ممکن است تنها راه موجود برای ایجاد حق دفاع مشروع برای کشور هدف باشد. با این حال، موقعیت‌هایی که در آن‌ها می‌توان به نظریهٔ تجمیع رویدادها تکیه کرد، محدودند (Roscini, 2014, p. 110).

دیوان بین‌المللی دادگستری در سال ۲۰۰۵ در خصوص شکایت جمهوری دموکراتیک کنگو علیه اوگاندا، رأی خود را در خصوص حقوق توسل به زور مرتبط با فعالیت‌های نظامی اوگاندا صادر نمود و ذیل بند ۱۴۶ این رأی، بیان می‌کند که اگر مجموعهٔ حملات صورت‌گرفته را بتوان یک‌جا در نظر گرفت و حملهٔ مسلحانه قلمداد نمود، همچنان برای کنگو قابل استناد

25. Oil Platforms case

26. Congo v. Uganda case

۲۷. عملیات سایبری علیه استونی که به‌صورت جداگانه یا جمعی، مورد تجزیه و تحلیل قرار گرفت، عموماً یک مخاصمهٔ مسلحانه دانسته نشد. برای مشاهدهٔ دیدگاه مخالف، می‌بایست به نظر Matthew Sklerov مراجعه کرد. او (۲۰۰۹) استدلال می‌کند که رایاجنگ‌های علیه استونی به‌منزلهٔ مخاصمهٔ مسلحانه‌اند و نوشته است که «حملات سایبری در سال ۲۰۰۷ علیه استونی نمونه‌ای از مجموعه‌ای هماهنگ از حملات سایبری بود که در مجموع، به سطح مخاصمه‌ای مسلحانه رسیدند. توضیح آن‌که، در حالی که برخی از حملات به استونی علیه زیرساخت‌های حیاتی آن بود و ممکن بود به‌صورت منفرد نیز مخاصمهٔ مسلحانه در نظر گرفته شوند، تأثیر جمعی آن‌ها بسیار بیشتر از آسیب واردشده در هر یک از حملاتِ جداگانه بود و مطمئناً این موضوع حملات سایبری را به درجهٔ مخاصمهٔ مسلحانه می‌رساند».

نیستند (ICJ Report, 2005, p. 146). همچنین دیوان در رأی پروندهٔ سکوهای نفتی، بدون تحلیل تفصیلی در خصوص این نظریه، به نظریهٔ تجمیع رویدادها اشاره کرده است. دیوان در رأی مذکور با اشاره به نظر نمایندهٔ دائم آمریکا در سازمان ملل که گفته بود: «حمله به کشتی «شهر جزیرهٔ دریایی» آخرین حمله از سری حملات موشکی علیه کشتی‌های دارای پرچم آمریکا و سایر کشتی‌های غیرمتخاصم (کشتی‌های غیرعراقی) بوده که برای اهداف تجاری در آب‌های کویت فعالیت می‌کردند»، بیان می‌کند که با در نظر گرفتن جمیع رویدادها و با حفظ مسئولیت ایران، به نظر نمی‌رسد که این رویدادها بتوانند حملهٔ مسلحانه علیه آمریکا تلقی شوند.

«اگر مجموع حملات انجام‌شده، فاصلهٔ زمانی بیش از اندازه نداشته باشد و عرفاً بتوان آن‌ها را یک حمله در نظر گرفت، اعمال دفاع مشروع در برابر آن‌ها می‌تواند از نظر حقوقی توجیه گردد و این تئوری در سال‌های آینده بر اثر گسترش احتمالی حملات سایبری، بیشتر از گذشته مورد استناد قرار خواهد گرفت» (نامدار؛ قاسمی، ۱۳۹۷، ص۲۱۰). بر این اساس، می‌توان گفت که با وجود آن‌که دیوان در دو رأی اخیر، به‌طور صریح، تئوری تجمیع وقایع را نه تحلیل و نه تأیید نموده است، اما عبارات آرا حاکی از آن است که احتمال این‌که انباشتی از حملات با مقیاس کوچک را بتوان حمله‌ای مسلحانه تلقی نمود و علیه آن نسبت به دفاع مشروع اقدام نمود، توسط دیوان رد نشده است.

شایان توجه است که در خصوص حملات سایبری واقع‌شده از سوی چندین رایانه، همچون حملات موسوم به «بندآوری خدمات» که دارای پیامدهایی بیش از یک مخاصمهٔ مرزی ساده‌اند، برای احتساب آن‌ها به‌عنوان یک مخاصمهٔ مسلحانهٔ تشکیل‌دهندهٔ جنایت جنگی، ضرورتی برای تمسک به رویکرد مرکب نیست و مادام که حمله از یک مرجع واحد مدیریت شود، توسل به زور و مخاصمهٔ مسلحانهٔ واحد تلقی می‌شود. این‌گونه حمله به‌مثابهٔ توسل به زوری است که توسط بمب‌افکن‌های متعدد و از سوی یک روبوشبکهٔ واحد انجام می‌پذیرد.

۳. زیرساخت‌های حیاتی سایبری با کارکرد دوگانه

با عنایت به این‌که بسیاری از زیرساخت‌های حیاتی مورد هدف در رایاجنگ‌ها، زیرساخت‌های حیاتی سایبری با کاربرد دوگانه‌اند که هم مورد بهره‌برداری نظامی و هم مورد بهره‌برداری غیرنظامی واقع می‌شوند، در صورت تحقق مخاصمه، بررسی ماهیت نظامی یا غیرنظامی آن‌ها نیز در خصوص

وقوع یا عدم وقوع جنایت جنگی نسبت به آن‌ها، به‌عنوان یکی از اهداف پرتکرار در رایاجنگ‌های حمله‌کننده به زیرساخت‌های حیاتی، مؤثر است. مطابق با تعریف موجود از اشیای نظامی، حتی تأسیسات و شبکه‌های با کاربری دوگانه نیز ممکن است از نظر قانونی، به‌عنوان اهداف نظامی شناخته شوند (Schmitt & vihul, 2017, p. 445). اگر تعریفِ پذیرفته‌شده از اهداف نظامی مندرج در بند ۲ مادهٔ ۵۲ از پروتکل الحاقی نخست به کنوانسیون‌های ژنو در این زمینه اعمال شود، طیف وسیعی از زیرساخت‌های حیاتی سایبری که اساساً ماهیت غیرنظامی دارند، به‌عنوان اهداف نظامی مشروع شناخته می‌شوند، زیرا همهٔ آن‌ها به‌واسطهٔ روشی که از آن‌ها استفاده می‌شود و این‌که انهدام یا خنثی‌سازی آن‌ها یک مزیت نظامی قطعی را مطابق با بند ۲ از مادهٔ ۵۲ پروتکل الحاقی اول موجب می‌شود، به‌عنوان اهداف نظامی قابل شناسایی هستند. علاوه بر این، کدهای نظامی که در فضای سایبر جابه‌جا می‌شوند، به بسته‌های داده‌ای مختلف تقسیم می‌شوند که معمولاً همگی از طریق سامانه‌های غیرنظامی مختلف عبور می‌کنند. بنابراین، حتی در یک حملهٔ سایبری، طیف وسیعی از زیرساخت‌های فیزیکی سایبری، یعنی سرورها، روترها، کابل‌ها یا ماهواره‌ها و نرم‌افزارها، برای کمک مؤثر به اقدام نظامی استفاده می‌شوند و بنابراین با این رویکرد، به‌عنوان اهداف نظامی قابل شناسایی‌اند. اما چنین تفسیرهایی در عصر دیجیتال منسوخ شده‌اند و تلقی مطلقِ آن‌ها به‌عنوان اهداف نظامی، اساساً با اهداف پروتکل الحاقی نخست نیز ناسازگار به نظر می‌رسد و در صورت کاربست تعریف پذیرفته‌شده از اهداف نظامی، اجزای مختلف زیرساخت‌های سایبری غیرنظامی به یک هدف نظامی مشروع تبدیل خواهند شد، زیرا در رایاجنگ‌ها، طرفین از ابزارهایی از جنگ سایبری استفاده می‌کنند که در آن‌ها بخش‌های قابل توجهی از زیرساخت‌های سایبری غیرنظامی برای کمک مؤثر به اقدامات نظامی استفاده می‌شود، لکن نامشخص است که دقیقاً کدام اجزا برای اهداف نظامی استفاده خواهند شد. به دلیل پیوستگی ماهیتی فضای سایبر، به‌سختی می‌توان با هر درجه‌ای از قطعیت پیش‌بینی کرد که در کدام ثانیه، کدام اجزای زیرساخت سایبری برای یک عملیات نظامی خاص مورد استفاده قرار گرفته یا قرار خواهد گرفت. بر این اساس و با توجه به چنین عدم قطعیتی، می‌توان ادعا نمود که همیشه می‌بایست فرض را به نفع وضعیت محافظت‌شده، یعنی وضعیت غیرنظامی، قرار داد، هرچند دور است که چنین رویکرد محدودکننده‌ای در عمل قبول گردد. بر این اساس، پیش‌بینی منطق حقوقی مؤثر برای برون‌رفت از این چالش مهم، ضروری به نظر می‌رسد.

۳-۱. مواجههٔ سنتی با زیرساخت‌های سایبری با کاربرد دوگانه

بر اساس «معیار هدف» مذکور در بند ۲ مادهٔ ۵۲ پروتکل الحاقی نخست، که معیاری مبهم است، قصد استفاده از شیئی در آینده برای اقدامی نظامی، جهت ارزیابی آن به‌عنوان هدف نظامی، کافی دانسته شده است (Sandoz and et al., 2022, p. 21). در صورت عدم وجود قطعیت در این خصوص، بند ۳ مادهٔ ۵۲ مقرر می‌دارد که در صورت تردید، - تا آن‌جا که به اشیایی که معمولاً به اهداف غیرنظامی اختصاص داده می‌شوند، مربوط است - فرض می‌شود که از اشیای مورد نظر استفادهٔ نظامی نمی‌شود. با این حال، گزارهٔ اخیر که اصل را بر غیرنظامی بودنِ سامانه‌های سایبری با قابلیت دوگانه می‌نهد، نتوانسته است وضعیت قانون عرفی را در حقوق بین‌الملل به دست بیاورد. بنابراین، اکنون هر زیرساخت سایبری غیرنظامی که به‌سختی به‌عنوان یک هدف عموماً اختصاص‌داده‌شده به اهداف غیرنظامی شناخته می‌شود، می‌تواند قاعدتاً به‌عنوان هدفی نظامی تلقی گردد. در مواردی که بند ۳ مادهٔ ۵۲ قابل اجرا نیست، به‌وضوح مشخص نیست که برای اثبات قصد و نیت دشمن در خصوص استفادهٔ آتی از یک شیء به‌عنوان شیء نظامی، به چه درجه‌ای از قطعیت یا اثبات نیاز هست (Oeter, 2008, p. 180-181). بیشتر اشیای غیرنظامی در دنیای واقعی به‌سادگی پتانسیل نظامی قابل توجهی ندارند و بنابراین هرگز به روش نظامی مورد استفاده قرار نخواهند گرفت. این یکی از جنبه‌هایی است که به نظر می‌رسد حوزهٔ سایبری اساساً در آن متفاوت است. هر ذره‌ای از ظرفیت حافظه یا قدرت رایانه‌ها، در هر کجا که باشند، همیشه قابلیت عملکرد نظامی دارد و به همین دلیل است که سیستم‌های نظامی و غیرنظامی به‌طور ذاتی به هم مرتبط‌اند. هیچ تفاوتی بین رایانهٔ نظامی و غیرنظامی وجود ندارد. هر رایانه و اساساً هر بخشی از زیرساخت سایبریِ بزرگ‌تر می‌تواند برای خدمت به ارتش و حوزهٔ غیرنظامی به‌صورت متقابل یا همزمان استفاده شود. در واقع، در حوزهٔ سایبری چنین «استفادهٔ دوگانه»ای معمولاً همزمان رخ می‌دهد. بنابراین، ۹۹ درصد از ظرفیت یک سرور ممکن است منحصراً برای انجام وظایف مهم غیرنظامی استفاده شود، درحالی‌که ۱ درصد یا حتی تنها ۰٫۱ درصد از ظرفیت آن ممکن است همزمان برای ارتباطات نظامی و سایر اهداف نظامی استفاده شود. با وجود این‌گونه کاربرد همزمان در فعالیت‌های نظامی و غیرنظامی، به نظر می‌رسد که دیدگاه پذیرفته‌شده این است که هر گونه استفادهٔ نظامی، هرچند حداقلی، شیئی غیرنظامی را به هدفی نظامی تبدیل می‌کند (Dinstein, 2010, p. 141). نتیجه این است که در هر «رایاجنگ» در آینده، علی‌رغم اصل پذیرفته‌شده برای

حفاظت از غیرنظامیان در مخاصمات مسلحانهٔ سایبری، تعریف مذکور از اهداف نظامی می‌تواند اساساً هر جزء از زیرساخت‌های سایبری را به یک هدف نظامی مشروع تبدیل کند. در این راستا، حتی اگر به نظر برسد که فضای سایبر از نظر فنی، امکان حملات بسیار دقیق و تفکیک‌گر علیه تأسیسات نظامی خاص را داراست، از نظر قانونی، در چهارچوب رویکرد فوق، بر اساس تعریف معاصر از اهداف نظامی، کل زیرساخت سایبری یک کشور به‌طور بالقوه می‌تواند به‌عنوان یک هدف نظامی، پس از درگیر شدن در مخاصمه‌ای مسلحانه، شناخته شود که حمله به آن‌ها مشمول هیچ ممنوعیت منجر به وقوع جنایت جنگی نخواهد بود. این نتیجه، خصوصاً برای دولت‌ها و جوامع مدرن که جنبه‌های مهم زندگی غیرنظامی آن‌ها به‌شدت و به‌طور فزاینده‌ای به فضای سایبر کارآمد وابسته است، نگران‌کننده است.

۳-۲. تلاش برای مواجههٔ نوین با زیرساخت‌های سایبری با کاربرد دوگانه

تعریف تثبیت‌شده از اهداف نظامی همواره توسط برخی از نویسندگان مورد انتقاد قرار گرفته است که «آن‌قدر گسترده است که می‌تواند عملاً هر چیزی را شامل شود» (Cassese, 2001, p. 993). تعریف محدودتر از اهداف نظامی می‌تواند به ایجاد تعادل مناسب‌تر بین ضرورت‌های نظامی و ملاحظات بشردوستانه در حوزهٔ سایبر و تشخیص بهتر اهداف نظامی از سیستم‌ها و تأسیسات حفاظت‌شدهٔ غیرنظامی کمک کند. یک راه‌حل، مستثنا کردنِ زیرساخت‌های سایبریِ مهم نظامی با ظرفیت استفادهٔ دوگانهٔ دارای کارکردِ عمدتاً غیرنظامی، همچون اجزای خاص زیرساخت‌های سایبری، از محدودهٔ اهداف نظامی مشروع است، مانند گره‌های اصلی تبادل اینترنت یا سرورهای مرکزی که میلیون‌ها کارکرد غیرنظامی مهم بر آن‌ها متکی است. البته این رویکرد نه جدید است و نه با قوانین بشردوستانه بیگانه است. بند۱ مادهٔ ۵۶ پروتکل الحاقی نخست، برخی از اشیا را به دلیل پیامدهای انسانی شدیدی که ممکن است حمله به این اشیا داشته باشد، حتی در مواردی که این اشیا به‌عنوان اهداف نظامی واجد شرایط‌اند، از جوازِ حمله مستثنا کرده و حمله به آن‌ها را ممنوع می‌سازد (Dinstein, 2010, p. 102). بنابراین، بند۱ مادهٔ ۵۶ اشیایی با کاربرد دوگانه را مقرر می‌دارد که تخریب آن‌ها می‌تواند بر جمعیت غیرنظامی تأثیرات سوءِ قابل توجهی بگذارد. بر اساس این استدلال، بند۱ مادهٔ ۵۱ مقرر می‌دارد که حتی سایر اهداف نظامی واقع در مجاورت چنین تأسیساتی نیز نباید هدف حمله قرار گیرند. با کاربست این نگاه در قلمرو فضای سایبر، رویکرد بند فوق می‌تواند بر تأسیسات سایبری نیز مشابه با اشیایی که در حال حاضر در مادهٔ

۵۶ پروتکل الحاقی اول فهرست شده‌اند، اعمال شود. خنثی کردن یا تخریب تأسیسات مذکور منجر به تأثیرات قابل توجه بر غیرنظامیان می‌شود که از مزایای نظامیِ حاصل‌شده معمولاً بیشتر است. در حوزهٔ فضای سایبر، این رویکرد می‌تواند به کاهش آثار سوء بر جمعیت غیرنظامی کمک کند و از این واقعیت ناشی می‌شود که اجزای اصلی زیرساخت‌های سایبری دوگانه به‌طور اجتناب‌ناپذیری همیشه در عملیات سایبری نظامی، هرچند به‌صورت حداقلی، دخیل‌اند و این در حالی است که چنین تأسیساتی عمدتاً وظایف غیرنظامی را انجام می‌دهند و ممکن است برای عملکرد کلی ترافیکِ سایبریِ غیرنظامی ضرورت داشته باشند. چنین معافیت‌هایی به‌ویژه مرتبط با ماهیت قلمرو سایبری به نظر می‌رسد، زیرا اختلال در اجزای زیرساخت‌های سایبری، از نظر جغرافیایی، نمی‌تواند محدود به کشور مورد هدف باشد و ممکن است پیامدهایی برای عملکرد فضای سایبری در سراسر جهان داشته باشد و از این منظر موجب ایجاد آثار سوء بر غیرنظامیان شود. البته ممکن است این چنین استدلال شود که قیاس با مادهٔ ۵۶ و توسیع این ماده به فضای سایبر، عملی به نظر نمی‌رسد، زیرا استثنای ارائه‌شده توسط بند نخست مادهٔ ۵۶ پروتکل الحاقی نخست، تنها بر اساس احتمال «تلفات شدید در میان جمعیت غیرنظامی» توجیه می‌شود. تأثیر غیرنظامی ناشی از حملات علیه اجزای زیرساخت‌های سایبری، هرچند احتمالاً در مقیاس بسیار بزرگ خواهد بود و باعث از بین رفتن عملکرد سایبری هزاران نفر می‌شود، اما معمولاً به سطح مشابه مذکور در مادهٔ فوق در خصوص شدت حمله، مانند آثار مخرب ناشی از تخریب تأسیسات هسته‌ای یا یک سد، نمی‌رسد.

در صورت عدم پذیرش راه‌حل فوق برای مستثنا کردنِ زیرساخت‌های حیاتی سایبری با کاربرد دوگانه از دایرهٔ اهداف نظامی مشروع، می‌بایست سایر تکالیف موجود در حقوق بشردوستانهٔ بین‌المللی مربوط به جداسازی اهداف نظامی از غیرنظامی یا رعایت احتیاط در حمله هنگام ارتکاب رایاجنگ علیه زیرساخت‌های مذکور را مورد توجه قرار داد (Jensen, 2010, p. 1552) که هیچ یک موجب آن نمی‌شود که بتوان مطلقاً زیرساخت‌های حیاتی سایبری با کاربرد دوگانه را به‌عنوان اهداف غیرنظامی محافظت‌شده محسوب نمود.

۴. رسیدگی به رایاجنگ‌های مختل‌کنندهٔ زیرساخت‌های حیاتی نزد دیوان کیفری بین‌المللی

رسیدگی

دیوان کیفری بین‌المللی برای رسیدگی به حملات سایبری تخریبگر، به سبب عدم وجود

اختلاف در خصوص وصول به آستانهٔ مخاصمهٔ مسلحانهٔ سایبری در نتیجهٔ رایاجنگ‌های تخریبگر، با چالش جدی مواجه نیست، لکن در خصوص رایاجنگ‌های مختل‌کننده، با عنایت به این‌که هدف اصلی حقوق کیفری بین‌المللی، آن‌گونه که در مقدمهٔ اساسنامهٔ رم مورد اشاره قرار گرفته، «پایان دادن به بی‌کیفرمانی» برای «جدی‌ترین جنایات مربوط به جامعهٔ بین‌المللی» است (بیگ‌زاده، ۱۴۰۲، ص۱۳۳۰)، بررسی این موضوع ضروری است که آیا مادهٔ ۸ اساسنامهٔ رم می‌تواند رایاجنگ‌های مختل‌کنندهٔ زیرساخت‌های حیاتی را نیز که در چهارچوب هیچ مخاصمهٔ دیگری رخ نمی‌دهد، مخاصمهٔ مسلحانه محسوب کند و در محدودهٔ صلاحیتی خود قرار دهد یا خیر؛ هرچند چنین پیشرفت‌های فناورانه‌ای در زمان تدوین آن پیش‌بینی نمی‌شده است. برای این منظور، اگر دیوان کیفری بین‌المللی به نتیجه‌گیری‌های سند مقررات تالین تکیه کند، این امر می‌تواند منجر به مستثنا کردن همهٔ گونه‌های رایاجنگ‌های مختل‌کننده، حتی رایاجنگ‌های مختل‌کنندهٔ زیرساخت‌های حیاتی، از محدودهٔ صلاحیتی دیوان کیفری بین‌المللی باشد. رایاجنگ‌های مختل‌کنندهٔ زیرساخت‌های حیاتی می‌توانند منجر به عواقبی ویرانگر شوند و با افزایش روزافزونِ وابستگی به فناوری، اختلال در زیرساخت‌های حیاتی می‌تواند به اندازهٔ توسل به زورِ منجر به آثار فیزیکی، موجب ورود خسارت شود (Kilovaty, 2016, p. 127). به این ترتیب، می‌بایست برای تأثیرات حملاتی که صرفاً در حوزهٔ دیجیتال رخ می‌دهند و به هیچ گونه 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 رایاجنگ‌های مختل‌کنندهٔ زیرساخت‌های حیاتی یاد می‌شود.

دولت‌ها به‌طور فزاینده‌ای این دیدگاه را بیان می‌کنند که حقوق بشردوستانهٔ بین‌المللی انواع خاصی از عملیات‌های سایبری مختل‌کنندهٔ زیرساخت‌های حیاتی را ممنوع می‌سازد (Georgia, 2020, p. 214) و مثال آن، در خصوص رویکردهای کشور فرانسه و هلند، گذشت. 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، عملیاتی سایبری که هدف آن ناکارآمد کردن شبکه‌ای 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 می‌کند، 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» (International Committee of the Red Cross, 2019, p. 8).

هرچند برخی صاحب‌نظران بر آن هستند که «کنوانسیون‌های ژنو و مقررات حقوق بشردوستانه در کل به‌طور کامل نمی‌توانند همهٔ گونه‌های عملیات سایبری را که در جنگ‌ها و غیر آن مورد استفاده قرار می‌گیرند، مورد پوشش قرار دهند و بنابراین، شایسته است دولت‌ها و سازمان‌های بین‌المللی درصدد آن بر آیند تا در قالب معاهده‌ای جدید، مقررات مربوط به جنگ سایبری را تهیه و تبیین کنند» (عسکری، ۱۴۰۱، ص۲۴۳)، لکن در مواردی که برخی از عبارات اساسنامهٔ رم قابلیت تفسیر داشته باشد، می‌بایست در چهارچوب 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 راياجنگ‌های مختل‌کننده را در محدودهٔ صلاحیتی مادهٔ ۸ قرار دهد و اطمینان حاصل کند که نقض دیجیتال حقوق بشردوستانهٔ بین‌المللی بی‌کیفر باقی نمی‌ماند. 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؛ اساسنامه‌ای که چیزی جز تضمین این نیست که جدی‌ترین جنایات نگران‌کننده برای جامعهٔ بین‌المللی به‌عنوان یک کل، دیگر بی‌کیفر باقی نمانند (ICC, 2007, p. 281)[۲۸]. همچنین باید به خاطر داشت که دیوان کیفری بین‌المللی موظف است «در صورت اقتضا، ... اصول تثبیت‌شدهٔ حقوق بین‌الملل در خصوص مخاصمات مسلحانه» را اعمال کند[۲۹] و حسب پاراگراف سوم مادهٔ ۲۱ اساسنامهٔ رم، 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. اثرات غیرفیزیکی حملات سایبری «می‌تواند اثرات فاجعه‌باری بر جامعهٔ

۲۸. در این خصوص، در رأی فوق، مقدمه و مواد ۱ و ۵ از اساسنامهٔ رم مورد ارجاع قرار گرفته است.

۲۹. این موضوع در بند «ب» از پاراگراف نخست مادهٔ ۲۱ اساسنامهٔ رم، مورد اشاره قرار گرفته است، لکن از سوی دیگر، لازم به ذکر است که بر اساس بند «الف» از پاراگراف نخستِ مادهٔ مزبور، اعمال حقوق بشردوستانهٔ بین‌المللی، در مقایسه با اعمال «اساسنامه، عناصر جرائم و قواعد دادرسی و ادله» خود دیوان کیفری بین‌المللی، در اولویت دوم قرار دارد.

مدنی داشته باشد» (Li, 2013, p. 188). استفاده از رایاجنگ‌های مختل‌کنندهٔ زیرساخت‌های حیاتی در جنگ می‌تواند منجر به حملات مکرر علیه غیرنظامیان نسبت به جنگ‌های متعارف شود، مگر این‌که به‌دقت مورد تنظیم‌گری واقع شوند، زیرا چنین جنگ‌هایی می‌توانند بدون ایجاد آسیب فیزیکی مستقیم بر روی اشیای غیرنظامی، انجام شود و در نتیجه، هزینهٔ سیاسی کمتری داشته باشد (Kelsey, 2008, p. 1439-1441). به این دلایل، علی‌رغم وجود خلأهای تقنینی در مادهٔ ۸ اساسنامهٔ رم (بیگ‌زاده، ۱۴۰۲، ص۱۳۲۷)، دیوان کیفری بین‌المللی می‌تواند رویکرد «برابری با آثار حملات سنتی فیزیکی» را در تفسیر خود از مادهٔ ۸ اساسنامه، رد کند تا امکان تعقیب جدی‌ترین تهدیدها علیه معیشت دیجیتالی غیرنظامیان و جلوگیری از مصونیت از کیفر در فضای سایبر فراهم شود.

نتیجه‌گیری

حملات سایبری به یکی از وقایع پرتکرار در جهان امروز تبدیل شده‌اند و قدرت کشورهای مختلف در استفاده از گونه‌های پیشرفتهٔ آن‌ها تا آن‌جا پیش رفته است که از رایاجنگ‌ها، به‌عنوان ابزاری نظامی، جهت نمایش یا اِعمال قدرت استفاده می‌کنند. استفادهٔ فزاینده از حملات مذکور موجب گسترش تأثیرات آن‌ها در طیفی از آثارِ فیزیکی (تخریبگر) و غیرفیزیکی (مختل‌کننده) شده و برخی رایاجنگ‌ها را پدید آورده است که مانند تمام دیگر گونه‌های جنگ، همهٔ کشورهای جهان ناگزیر از تنظیم‌گری و وضع محدودیت بر آن‌هایند. آن‌گونه که سایر گونه‌های جنگ با وضع مقررات حاکم بر جنگ که نقض آن‌ها موجب شکل‌گیری جنایات جنگی می‌شود، مورد تنظیم‌گری واقع شده‌اند، در صورت امکانِ استفاده از مقررات حاکم بر جنگ و وضع ضمانت اجرای وقوع جنایت جنگی بر رایاجنگ‌ها، این گونهٔ جدید جنگ نیز تا حدی مورد تنظیم‌گری واقع می‌شود.

رایاجنگ‌های ایجادگرِ آثار فیزیکی که از آن‌ها با عنوان «رایاجنگ‌های تخریبگر» یاد می‌شود، به سبب ایجاد آثار مشابه با جنگ‌های سنتی، بر اساس ادبیات نظری موجود، در چالش بسیار کمتری برای احتساب به‌عنوان جنایت جنگی قرار دارند، و این در حالی است که رایاجنگ‌های ایجادگرِ آثار غیرفیزیکی که «رایاجنگ‌های مختل‌کننده» نیز خوانده می‌شوند، آن‌گاه که آثار خود را بر «زیرساخت‌های حیاتی» واقع می‌سازند، علی‌رغم ایراد ضرر بسیار بر کشورِ مورد هدف، برای احتساب به‌عنوان جنایت جنگی، با چالش جدی مواجه‌اند. علی‌رغم عدم وجود تعریف واحد

میان کشورها در سطح جهان در خصوص «زیرساخت‌های حیاتی»، تعاریف موجود بسیار شبیه یکدیگرند و بر اساس هر تعریفی که پذیرفته شود، زیرساخت‌های حیاتی امروزی به‌طور اساسی به سامانه‌ها و شبکه‌های رایانه‌ای وابسته بوده و بنابراین، به‌ویژه در برابر رایاجنگ‌های مختل‌کننده آسیب‌پذیرند که این موضوع تأکیدی بر ضرورت تنظیم‌گری چنین رایاجنگ‌هایی در چهارچوب مقررات مربوط به جنایات جنگی است.

در صورتی می‌توان برخی اقدامات ارتکاب‌یافته در رایاجنگ‌های مختل‌کنندهٔ زیرساخت‌های حیاتی را به‌عنوان جنایت جنگیِ سایبری بر اساس مقررات موجود تلقی نمود که شرط زمینه‌ای برای وقوع جنایات جنگی در رایاجنگ موضوع رسیدگی وجود داشته باشد. شرط زمینه‌ای مذکور مشتمل بر آن است که در نتیجهٔ یک رایاجنگ مختل‌کنندهٔ زیرساخت‌های حیاتی، مبتنی بر آموزه‌های مرتبط با حقوق مخاصمات مسلحانه، یک مخاصمهٔ مسلحانهٔ بین‌المللی یا غیربین‌المللی واقع شده باشد. سطح وقوع یک مخاصمهٔ مسلحانه در خصوص رایاجنگ‌ها، دچار ابهام است. در ادبیات رایج حقوق بین‌الملل، به سبب شهرت اعتبار نظر سند مقررات تالین در فضای سایبر، برخی «ایجاد آثار فیزیکی» را ضرورت تشکیل مخاصمهٔ مسلحانهٔ سایبری می‌دانند و این موجب شده است که در تلقیِ رایاجنگ‌های تخریبگر به‌عنوان جنایت جنگی، هم‌نظری بیشتری میان صاحب‌نظران وجود داشته باشد و این در حالی است که به نظر می‌رسد حتی مبتنی بر سند مقررات تالین که مهم‌ترین شاخص را برای توسل به زور، وقوع «شدت» می‌داند و آن را در راستای پیامدهای ایجادشدهٔ ناشی از رایاجنگ معنا می‌بخشد، می‌توان از تحقق مخاصمه سخن گفت آن‌گاه که رایاجنگ‌های مختل‌کنندهٔ زیرساخت‌های حیاتی، موجب ایجاد بحران‌های کلان ملی در سطح یک اجتماع می‌شوند.

بر این اساس، در تحلیلی روزآمد و پویا در خصوص تحقق معیار «شدت، به‌عنوان آستانهٔ وصول به مخاصمهٔ مسلحانهٔ سایبری، آستانهٔ لازم برای وقوع توسل به زور و شکل‌گیری مخاصمهٔ مسلحانه، از یک‌سو، ضرورتاً محدود به ایجاد آثار و خسارات فیزیکی مشابه با حملات سنتی نبوده و از سوی دیگر، آن‌گونه نیست که بتوان هر گونه ایجاد اختلال در سامانه‌های رایانه‌ایِ طرف متخاصم را نیز شامل شود و به‌گونه‌ای آستانهٔ میانهٔ ایجاد آثار فیزیکیِ صرف و ایجاد آثار غیرفیزیکیِ صرف را شامل می‌شود. با این توضیح که علاوه بر شمول نسبت به حملات سایبری موجدِ آثار فیزیکی، شامل خسارت غیرفیزیکی و مختل‌کنندهٔ زیرساخت‌های حیاتی ملی نیز می‌شود.

بـر ایـن اسـاس، از منظـر عناصـر زمینـه‌ایِ لازم بـرای وقـوع جنایـات جنگـیِ سـایبری در نتیجـهٔ رایاجنگ‌هـای مختل‌کننـدهٔ زیرسـاخت‌های حیاتـی و رسـیدگی نـزد دیـوان کیفـری بین‌المللـی، نیـاز بـه اصـلاح اساسـنامهٔ رم نیسـت و مقـررات موجـود در دو حـوزهٔ حقـوق بشردوسـتانهٔ بین‌المللی و حقـوق کیفـری بین‌المللـی، بـا انعطـاف لازم، یـارای تنظیم‌گـری رایاجنگ‌هـای مختل‌کننـدهٔ زیرسـاخت‌های حیاتـی مبتنـی بـر حقـوق جنـگ، هسـتند. در پرتـو ایـن راهبـرد، دیـوان کیفـری بین‌المللی می‌توانـد رویکرد «برابری با آثار حملات سـنتی فیزیکی» را در تفسـیر خود از مادهٔ ۸ اساسـنامه، رد کند تا متعاقب ارتکاب رایاجنگ‌هـای مختل‌کننـدهٔ زیرسـاخت‌های حیاتـی، امـکان تعقیـب جدی‌تریـن تهدیدها علیه معیشـت دیجیتالـی غیرنظامیـان و جلوگیـری از مصونیـت از کیفـر در فضـای سـایبر فراهـم شـود.

فهرست منابع

۱. آهنی امینه، محمد؛ فتح‌اللهی، فاطمه‌زهرا. (۱۳۹۳ش). حقوق بین‌الملل مدرن در مواجهه با جنگی پست‌مدرن (نبرد سایبری). راهبرد، ش۷۲، ص۱۱۶-۱۴۴.

۲. برادران، نازنین؛ حبیبی، همایون. (۱۳۹۸ش). قابلیت اعمال قواعد حقوق بین‌الملل بشردوستانه در جنگ‌های سایبری. مطالعات حقوق عمومی، ۴۹(۱)، ۱۳۹-۱۵۸. https://doi.org/10.22059/jplsq.2017.228162.1478

۳. بیگ‌زاده، ابراهیم. (۱۴۰۲ش). حقوق بین‌الملل، (جلد دوم). تهران: نشر میزان.

۴. پاکزاد، بتول. (۱۳۸۸ش). تروریسم سایبری. رسالهٔ دکتری، (استاد مشاور: علی‌حسین نجفی ابرندآبادی). دانشکدهٔ حقوق دانشگاه شهید بهشتی. گروه حقوق کیفری و جرم‌شناسی. تهران.

۵. خلیل‌زاده، مونا. (۱۳۹۳ش). مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری. تهران: مجد.

۶. داینیس، هیتر هریسن. (۱۳۹۵ش). جنگ سایبری و حقوق جنگ، (ترجمهٔ سعید حکیمی‌ها و هومان شاهرخ). تهران: میزان.

۷. دهقانی، پریسا؛ رمضانی قوام‌آبادی، محمدحسین؛ علی‌پور، محمدرضا. (۱۴۰۱ش). شرط مارتنس در حقوق کیفری بین‌المللی، ماهیت و کارکردهای تفسیری. آموزه‌های حقوق کیفری، ۱۹(۲۳)، ۱۲۳-۱۵۶. https://doi.org/10.30513/org.2022.3988.1634.cld

۸. رضائی، مسعود؛ جلالی، محمود. (۱۳۹۷ش). جنگ سایبری و توسعهٔ حقوق بین‌الملل منع توسل به زور. مطالعات حقوق عمومی، ۴۸(۳)، ۶۹۷-۷۱۳. https://doi.org/10.30513/cld.2022.3988.1634

۹. رنجبر، علیرضا؛ گرشاسبی، علی. (۱۳۹۹ش). موانع بنیادین فراروی تدوین حقوق بین‌الملل حاکم بر حملهٔ سایبری. مجلهٔ حقوقی بین‌المللی، ۳۷(۶۳)، ۲۳۷-۲۶۴. https://doi.org/10.22066/cila-mag.2020.111943.1823

۱۰. شاملو، باقر؛ خلیلی پاجی، عارف. (۱۴۰۰ش). جرم‌انگاری در حوزهٔ رمزارزها. آموزه‌های حقوق کیفری، ۱۸(۲۱)، ۲۹-۶۸. https://doi.org/10.30513/cld.2021.1420.1230

۱۱. شریفی طرازکوهی، حسین. (۱۳۹۵ش). حقوق بشردوستانهٔ بین‌المللی. تهران: میزان.

۱۲. ضیایی بیگدلی، محمدرضا. (۱۳۹۷ش). حقوق جنگ؛ حقوق بین‌الملل مخاصمات مسلحانه. تهران: دانشگاه علامه طباطبائی.

۱۳. عسکری، پوریا. (۱۴۰۱ش). «حقوق بشردوستانه در جنگ سایبری»، در: دانشنامهٔ رفتار سایبری، (به‌کوشش باقر شاملو). تهران: میزان.

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

۱۵. کاسسه، آنتونیو؛ گایتا، پائولو؛ بیگ، لورل؛ فان، ماری؛ گاسنل، کریستوفر؛ ویتینگ، الکس. (۱۴۰۱ش). حقوق بین‌الملل کیفری، (ترجمهٔ حسین پیران). تهران: نشر نو.

۱۶. کیهانلو، فاطمه؛ رضادوست، وحید. (۱۳۹۴ش). حملات سایبری به‌مثابهٔ توسل به زور در سیاق منشور سازمان ملل متحد. تحقیقات حقوقی، ۱۸(۶۹)، ۱۹۳-۲۰۸.

۱۷. گیوکی، آذر؛ کفایی‌فر، محمدعلی؛ رضایی، محمدتقی. (۱۴۰۰ش). حملات سایبری و لزوم رعایت اصول اساسی حقوق بشردوستانه در آن‌ها. تحقیقات حقوقی تطبیقی ایران و بین‌الملل، ۱۴(۵۱)، ۲۲۷-۳۰۵. https://doi..

org/10.30495/alr.2021.1872408.1562

۱۸. محقق هرچقان، علیرضا؛ اردبیلی، محمدعلی؛ بیگ‌زاده، ابراهیم؛ مهدوی ثابت، محمدعلی. «الف». (۱۴۰۲ش). حقوق بین‌الملل سایبری و توسعهٔ صلاحیت دیوان کیفری بین‌المللی (با تأکید بر مذاکرات تالین ۲۰۱۷ میلادی). مطالعات حقوق عمومی، ۵۳(۳)، ۱۵۳۷-۱۵۵۹. https://doi.org/10.22059/jplsq.2022.329515.2869

۱۹. محقق هرچقان، علیرضا؛ اردبیلی، محمدعلی؛ بیگ‌زاده، ابراهیم؛ مهدوی ثابت، محمدعلی. (۱۴۰۱ش). اثربخشی دستورالعمل تالین ۲۰۱۷ میلادی بر صلاحیت دیوان کیفری بین‌المللی در ایجاد صلح و امنیت سایبری بین‌المللی. آموزه‌های حقوق کیفری، ۱۹(۲۳)، ۲۶۹-۲۹۶. https://doi.org/10.30513/cld.2022.3192.1502

۲۰. محقق هرچقان، علیرضا؛ اردبیلی، محمدعلی؛ بیگ‌زاده، ابراهیم. «ب». (۱۴۰۲ش). صلاحیت دیوان کیفری بین‌المللی و رسیدگی به جنایات بین‌المللی سایبری در عرصه‌های انسانی حقوق بین‌الملل. پژوهشهای حقوق جزا و جرم‌شناسی، ۱۱(۲۱)، ۳۰۳-۳۲۷. https://doi.org/10.22034/jclc.2023.389750.1827

۲۱. نامدار، سعید؛ قاسمی، غلامعلی. (۱۳۹۷ش). بررسی مفهوم دفاع مشروع در پرتو حملات سایبری (با تأکید بر حملهٔ استاکس‌نت به تأسیسات هسته‌ای ایران). مطالعات حقوقی، ۱۰(۱)، ۱۹۹-۲۳۵. https://doi.org/10.22099/jls.2018.23191.2178

۲۲. نژندی‌منش، هیبت‌الله. (۱۳۹۴ش). حقوق بین‌الملل کیفری در رویهٔ قضایی. تهران: خرسندی.

۲۳. نجفی ابرندآبادی، علی‌حسین. (۱۳۸۸ش). دربارهٔ بزهکاری و جرم‌شناسی سایبری. تعالی حقوق (ماهنامهٔ آموزشی دادگستری کل استان خوزستان)، ۴(۳۶).

۲۴. نجفی ابرندآبادی، علی‌حسین. (۱۳۹۵ش). «از جرم‌شناسی حقیقی تا جرم‌شناسی مجازی»، دیباچه بر: پیکا، ژرژ. جرم‌شناسی، (ترجمهٔ علی‌حسین نجفی ابرندآبادی، ویراست ۳). تهران: میزان.

25. 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/.

26. Barkham, Jason. (2001). Information Warfare and International Law on the Use of Force. *New York University Journal of International Law and Politics*, 34 (57).

27. Bijleveld, A. (2018). Keynote Address, Diplomacy and Defence in Cyber Space. *cyber seminar in Hague*. 20 June 2018. 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.

28. Brown G, and Tullos O. (2012). On the Spectrum of Cyberspace Operations. *Small Wars Journal*. 12 Nov. 2012. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2400536.

29. 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.

30. Cassese, Antonio. (2001). Terrorism is also Disrupting Some Crucial Legal Categories of International Law. *European Journal of International Law*.

31. 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*, Vol. 17 (3).

32. Delerue, F. (2020). *Cyber Operations and International Law*. Cambridge University Press.

33. Dinniss, H. Harrison. (2012). *Cyber Warfare and the Laws of War*. Cambridge. Cambridge University Press.

34. Dinstein, Yoram. (2010). *The Conduct of Hostilities under the Law of International Armed Conflict*. 2nd edn. Cambridge. Cambridge University Press.

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

36. Dragos. (2019). Assessment of Reported Malware Infection at Nuclear Facility. *Dragos*. 1 November 2019. available in: https://www.dragos.com/blog/industry-news/assessment-of-reported-malware-infection-at-nuclear-facility/.

37. 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. https://www.lawfaremedia.org/article/what-would-happen-if-states-started-looking-cyber-operations-threat-use-force.

38. European Union. (2006). *Communication from the Commission on a European Programme for Critical Infrastructure Protection*. COM/2006/0786 final.

39. European Union. (2004). *Communication from the Commission to the Council and the European Parliament – Critical Infrastructure Protection in the Fight against Terrorism*. COM/2004/0702 final.

40. European Union. (2009). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection – "Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience". COM/2009/0149 final.

41. European Union. (2008). *Directive on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection*. Council Directive 2008/114/EC., 2008, Annex I: 'List of ECI sectors'.

42. Focarelli, Carlo. (2015). Self-Defence in Cyberspace. in: *Research Handbook on International Law and Cyberspace*. Nicholas Tsagourias and Russell Buchan (eds.). Edward Elgar Publishing.

43. General Assembly of the United Nations. (2023). *Creation of a global culture of cybersecurity and the protection of critical information infrastructures*. UNGA Res 58/199. 23 December 2003.

44. Georgia, Beatty. (2021). War crimes in cyberspace: prosecuting disruptive cyber operations under Article 8 of the Rome Statute. *The Military Law and the Law of War Review*, Vol. 58 (2). https://doi.org/10.4337/mllwr.2020.02.17.

45. Gisel, L, and Olejnik, L. (2019). *The Potential Human Cost of Cyber Operations*. *ICRC*. 29 May 2019. https://www.icrc.org/en/document/potential-human-costcyber-operations.

46. Greenberg, A. (2023). The International Criminal Court Will Now Prosecute Cyberwar Crimes. *Wired*. 7 September 2023. https://www.wired.com/story/icc-cyberwar-crimes/.

47. 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/wanna-cry-petya-notpetya-ransomware.

48. Hoisington, Matthew. (2009). Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense. *International & Comparative Law Review*. Vol. 32.

49. 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.

50. Hoogh, André. (2009). Georgia's Short-Lived Military Excursion into South Ossetia: The Use of Armed Force and Self-Defence. *Ejiltalk*. 9 December 2009. www.ejiltalk.org/georgia's-short-lived-military-excursion-into-southossetia-the-use-of-armed-force-and-self-defence/.

51. ICJ Report. (2005). *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*. (Judgment). ICJ Reports 168.

52. ICJ Report. (1986). *Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.)*. Judgment. ICJ Report 14. 27 June 1986.

53. ICJ Report. (2003). *Oil Platforms (Islamic Republic of Iran v. United States of America)*. (Judgment). ICJ Reports 161, 2003.

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

55. ICJ Reports. (2005). *The Armed Activities on the Territory of the Congo Case*.

56. Inteernational Criminal Tribunal for the Former Yugoslavia. (1995). *Prosecutor v. Tadić*. Case No. IT-1-94-1. Decision on the Defense Motion for Interlocutory Appeal on Jurisdiction. 2 October 1995.

57. International Committee of the Red Cross. (2019). *International Humanitarian Law and Cyber Operations during Armed Conflicts*. ICRC position paper. November 28, 2019. https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts.

58. Joyner, Christopher C, and Lotrionte, Catherine. (2001). Information Warfare as International Coercion: Elements of a Legal Framework. *European Journal of International Law*, Vol. 12 (5). https://doi.org/10.1093/ejil/12.5.825.

59. Kelsey, J. (2008). Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare. *Michigan Law Review*. Vol. 106 (7).

60. Kerschischnig, Georg. (2012). *Cyberthreats and International Law*. Hague. Eleven International Publishing.

61. Khan, Karim A.A. (2023). Technology Will Not Exceed Our Humanity. *Digitalfrontlines*. 20 August 2023. https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity/.

62. Kilovaty, I. (2016). Virtual Violence – Disruptive Cyberspace Operations as "Attacks" Under International Humanitarian Law. *Michigan Telecommunications and Technology Law Review*. Vol. 23 (1).

63. Letter from the Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace. (2019). Appendix, 5 July 2019. https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-theparliament-on-the-international-legal-order-in-cyberspace.

64. Li, S. (2013). When Does Internet Denial Trigger the Right of Armed Self-Defense?. *Yale Journal International Law*, Vol. 38.

65. Lin, Herbert S. (2010). Offensive Cyber Operations and the Use of Force. Cybersecurity Symposium: National Leadership, Individual Responsibility. *Journal of National Security Law & Policy*, Vol. 4(1).

66. 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.

67. Max Planck Institute for Comparative Public Law and International Law. (2019). Report of the International Fact-Finding Commission on the Conflict in Georgia. *ceiig*,. www.ceiig.ch/Report.html.

68. Milanovic, Marko, and Schmitt, Michael N. (2020). Cyber Attacks and Cyber (Mis)information Operations during a Pandemic. *Journal of National Security Law & Policy*. Vol. 11.

69. Miller, K. (2014). The Kampala Compromise and Cyberattacks – Can There Be an International Crime of Cyber-Aggression?. *Southern California Interdisciplinary Law Journal*, Vol. 23.

70. Ministry of the Armies. (2019). *International Law Applied to Operations in Cyberspace* (English version). Ministère des Armées. 19 March 2019. https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf.

71. Morgan, J. (2014). A Simple Explanation of the Internet of Thing. *Forbes*. 13 May 2014. https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#69481bd01d09.

72. Myjer, Eric. (2015). Some Thoughts on Cyber Deterrence and Public International Law. in: *Research Handbook on International Law and Cyberspace*. Nicholas Tsagourias and Russell Buchan (eds.). London. Edward Elgar Publishing.

73. 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.

74. Oeter, Stefan. (2008). Methods and Means of Combat. in: *The Handbook of International Humanitarian Law*. Dieter Fleck (ed.). Oxford University Press.

75. Ophardt, J. (2010). Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield. *Duke Law & Technology Review*, Vol. 9 (3).

76. Porup, JM. (2019). How a nuclear plant got hacked. *CSO Online*. 9 December 2019. https://www.csoonline.com/article/3488816/how-a-nuclear-plant-got-hacked.html.

77. 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.

78. Radziwill, Yaroslav. (2015). *Cyber-Attacks and the Exploitable Imperfection of International Law*. Leiden. Brill & Martinus Nijhoff Publishers.

79. Rome Statute of the International Criminal Court. (1998). 17 July 1998, 2187 U.N.T.S. 90.

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

81. Roscini, Marco. (2016). Cyber Operations as a Use of Force. in: *Research Handbook on International Law and Cyberspace*. Nicholas Tsagourias and Russell Buchan (eds.). London. Edward Elgar Publishing.

82. 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,* Vol. 108 (2).

83. Sandoz, Yves, Swinarski, Christophe and Zimmermann, Bruno (eds.). (2022). *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*. International Committee of the Red Cross.

84. 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*. Vol. 21 (8). https://doi.org/10.1093/jcsl/krw018.

85. Scheffer, David. (2022). Amending the Rome Statute to Cover Cyberwarfare as Aggression. *ICC Forum*, 7 March 2022. https://iccforum.com/cyberwar#Scheffer.

86. 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.

87. 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*, Vol. 37.

88. Schmitt, Michael N. (2011). Cyber Operations and the Jus Ad Bellum Revisited', *Villanova Law Review*, Vol. 56.

89. Schmitt, Michael N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge. Cambridge University Press.

90. Shackelford, Scott. (2009). From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. *Berkley Journal of International Law*, Vol. 27.

91. Silver, Daniel B. (2002). Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter. *International Law Studies,* Vol. 76.

92. Sklerov, Matthew J. (2009). Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent. *Military Law Review*, Vol. 201.

93. The Prosecutor v. Thomas Lubanga Dyilo. (2007). ICC-01/04-01/06. Decision on the Confirmation of Charges. PTC I, 29 Jan. 2007.

94. Tsagourias, Nicholas. (2012). Cyber Attacks, Self-Defence and the Problem of Attribution. *Journal of Conflict and Security Law*, Vol. 17.

95. US White House. (2013). *Presidential Policy Directive - Critical Infrastructure Security and Resilience*. Presidential Policy Directive/PPD-21, available in: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

96. 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/.

97. Ziolkowski, K. (2010). Computer Network Operations and the Law of Armed Conflict. *The Military Law and the Law of War Review*, Vol. 49.