The University of Tehran Press

Public Law Studies Quarterly

Homepage: http://jplsq.ut.ac.ir

Online ISSN: 2423-8139

Volume: 55, **Issue:** 4
Winter 2026

Cyberattacks and International Law: Legal Gaps in Articles 4 (2) and 51 of the United Nations Charter

Manizheh Eskandari✉

Ph.D. in International Relations; Researcher in International Relations and International Law, Tehran, Iran. Email: esma1334@gmail.com, Manizheh.eskandari@srbiau.ac.ir

Article Info

Article Type:
Research Article

Pages: 2693-2715

Received:
2024/09/18
Received in Revised form:
2025/11/17
Accepted:
2025/02/03
Published online:
2025/12/22

Keywords:
use of force, international law, cyber attack, self-defense, cyberspace.

Abstract

Today, emerging technologies have become an inseparable part of human life. Cyberspace is a new domain from which states, individuals, and companies can derive significant benefits. At the same time, existing security threats can penetrate it, or new threats may emerge within it. As governmental, economic, and essential public service infrastructures increasingly rely on digital systems, states find themselves vulnerable to escalating cyber threats. The central question is whether international law—particularly Article 2, paragraph 4 of the United Nations Charter regarding the prohibition of the use of force, and Article 51 on the right to self-defense—can be applied to cyberattacks. In response, this study tests the hypothesis that the unique characteristics of cyberspace, which distinguish it from the physical domain, pose fundamental challenges to the application of existing international law. This research analyzes the main legal obstacles and emphasizes the necessity of establishing a binding international legal framework governing states' cyber activities. Such a comprehensive legal system should be compatible with the evolving nature of cyber operations while being sufficiently explicit and precise to effectively regulate them.

How To Cite

Eskandari, Manizheh (2026). Cyberattacks and International Law: Legal Gaps in Articles 4 (2) and 51 of the United Nations Charter. *Public Law Studies Quarterly*, 55 (4), 2693-2715.
DOI: https://doi.com/10.22059/jplsq.2025.382206.3603

DOI 10.22059/jplsq.2025.382206.3603

Publisher The University of Tehran Press.

انتشارات دانشگاه تهران

فصلنامه مطالعات حقوق عمومی

Homepage: http://jplsq.ut.ac.ir

شاپا الکترونیکی: ۸۱۳۹-۲۴۲۳
دوره: ۵۵، **شماره:** ۴
زمستان ۱۴۰۴

حملات سایبری و حقوق بین‌الملل:
شکاف‌های حقوقی بند ۲ مادهٔ ۴ و مادهٔ ۵۱ منشور ملل متحد

منیژه اسکندری✉

دانش‌آموختهٔ مقطع دکتری روابط بین‌الملل و پژوهشگر روابط و حقوق بین‌الملل، ایران. رایانامه: esma1334@gmail.com، Manizheh.eskandari@srbiau.ac.ir

اطلاعات مقاله

نوع مقاله: پژوهشی

صفحات: ۲۶۹۳-۲۷۱۵

تاریخ دریافت:
۱۴۰۳/۰۶/۲۸

تاریخ بازنگری:
۱۴۰۳/۰۸/۲۷

تاریخ پذیرش:
۱۴۰۳/۱۱/۱۵

تاریخ انتشار برخط:
۱۴۰۴/۱۰/۰۱

کلیدواژه‌ها:
توسل به زور، حقوق بین‌الملل، حملهٔ سایبری، دفاع از خود، فضای سایبری.

چکیده

امروزه فناوری‌های نوین بخش جدایی‌ناپذیری از زندگی بشر شده‌اند. فضای سایبری نیز قلمرو جدیدی است که دولت‌ها، اشخاص و شرکت‌ها می‌توانند منافع بسیاری از آن کسب کنند. در عین حال، تهدیدات امنیتی موجود می‌تواند به آن راه یابد یا تهدیدات جدیدی در آن ظهور کند. از آنجا که زیرساخت‌های حکومتی، اقتصادی و خدمات همگانی حیاتی به‌طور فزاینده به سیستم‌های دیجیتال وابسته‌اند، دولت‌ها خود را در برابر تشدید تهدیدات سایبری آسیب‌پذیر می‌یابند. پرسش اصلی این است که آیا حقوق بین‌الملل، به‌ویژه بند ۴ مادهٔ ۲ منشور ملل متحد دربارهٔ منع توسل به زور، و مادهٔ ۵۱ منشور مربوط به دفاع از خود می‌توانند در مورد حملات سایبری به‌کار آیند؟ در پاسخ، این فرضیه را به آزمون می‌گذاریم که به‌نظر می‌رسد ویژگی‌های بی‌مانند فضای سایبری که این حوزه را از قلمرو فیزیکی متمایز می‌سازد، کاربست حقوق بین‌الملل موجود را با چالش‌های اساسی مواجه کرده است. این پژوهش با تحلیل موانع اصلی حقوقی موجود، بر ضرورت ارائهٔ یک چارچوب حقوقی بین‌المللی الزام‌آور حاکم بر فعالیت‌های سایبری دولت‌ها تأکید می‌کند. نظام حقوقی فراگیری که بتواند با روند توسعهٔ عملیات سایبری سازگار گردد، و نیز به میزان کافی صریح و دقیق باشد تا به‌طور مؤثری آنها را سامان دهد.

استناد
اسکندری، منیژه (۱۴۰۴). حملات سایبری و حقوق بین‌الملل: شکاف‌های حقوقی بند ۲ مواد ۴ و ۵۱ منشور ملل متحد. *مطالعات حقوق عمومی*، ۵۵ (۴)، ۲۶۹۳-۲۷۱۵.
DOI: https://doi.com/10.22059/jplsq.2025.382206.3603

DOI
10.22059/jplsq.2025.382206.3603

ناشر
مؤسسهٔ انتشارات دانشگاه تهران.

۱. مقدمه

فضای سایبری قلمرویی است که اشخاص حقیقی و حقوقی می‌توانند منافع بسیاری در آن کسب کنند، اما می‌تواند عرصهٔ بروز تهدیدات امنیتی موجود و حتی پیدایش تهدیدات امنیتی جدید نیز باشد. در نتیجهٔ چنین تهدیداتی است که امنیت در فضای سایبر به دغدغهٔ عمومی جامعهٔ بین‌الملل تبدیل شده است (قاسمی و چهاربخش، ۱۳۹۱: ۱۱۶).

همزمان با پیشرفت فناوری‌های سایبری در سال‌های پایانی دههٔ ۱۹۸۰ و اوایل دههٔ ۱۹۹۰ و با رایج شدن دسترسی به اینترنت پرسرعت در اوایل دههٔ ۲۰۰۰، فناوری‌های جدید با فراهم کردن امکان به‌کارگیری رایانه به‌عنوان ابزار فرماندهی، کنترل، ارتباطات و اطلاعات، قلمرو نوینی را به قلمرو هوایی، زمینی، دریایی و فضایی منازعات اضافه کرد که ماهیت و شیوهٔ آن متفاوت از دیگر قلمروهاست.

از سال ۲۰۲۰ با فراگیر شدن فعالیت‌های مخرب سایبری در سطح بین‌المللی، فضای سایبری به آوردگاه جدید جنگ و تهدید جدی علیه صلح و امنیت بین‌المللی در قرن حاضر تبدیل شده است. چنانکه در هفتادوششمین اجلاس مجمع عمومی در ۲۱ سپتامبر ۲۰۲۱ آنتونیوگوترش دبیر کل سازمان ملل متحد در سخنرانی خود برای دستیابی به راهی برای جهانی بهتر و تحقق وعده‌های داده‌شده در «دستور کار مشترک ما» برای دنیایی بهتر، تأکید کرد که باید از شش شکاف عمیق از جمله شکاف دیجیتال عبور کرد. وی با اعلام اینکه رویارویی‌های بزرگ آینده با حملهٔ سایبری بزرگی آغاز خواهد شد، خواستار مشخص شدن چارچوب‌های حقوقی رسیدگی به مسائل سایبری شد (UN Secretary- General, 2021: 11).

دلیل این رویکرد، وابستگی فزایندهٔ دولت‌ها به شبکه‌های رایانه‌ای است که از زیرساخت‌های حیاتی نظیر شبکه‌های برق قوی، شبکه‌های ارتباطی راه دور، سیستم‌های بیمارستانی و نظام‌های بانکداری محافظت می‌کنند. این وابستگی احتمال حمله از طریق تهدیدات پیشرفته بی‌وقفه مانند تهدیدات هدفمند برای حصول یک هدف ویژه را به‌گونه‌ای افزایش می‌دهد که بتواند زیرساخت یک دولت را مورد حمله قرار دهد، به انهدام گسترده منجر شده و به تهدید قطعی علیه امنیت ملی دولت قربانی تبدیل شود (Mann, 2020: 10). بدین ترتیب منازعهٔ سایبری به نوبهٔ خود تهدیدی عظیم علیه صلح و امنیت بین‌المللی است.

در سراسر تاریخ، پیشرفت‌های فناورانه همواره از حوزهٔ حقوق پیش بوده است. هرچند سال‌های ابتدای دههٔ ۲۰۰۰ شاهد توسعهٔ ناچیز حقوق بین‌الملل ناظر بر جرم‌های سایبری و کنوانسیون جرم سایبری بوداپست و پروتکل الحاقی آن در رابطه با جرم‌انگاری در سیستم‌های رایانه‌ای[1] بود، اما موضوع

1. Convention on Cybercrime (also known as the Budapest Convention), Nov. 23, 2001, ETS No. 185, and the Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts Committed through Computer Systems, Jan. 28, 2003, ETS No. 189.

مهم دامنه، هدف و چگونگی اعمال حقوق بین‌الملل در قلمرو سایبری به‌ویژه فعالیت‌های سایبری بازیگران دولتی همچنان بی‌پاسخ ماند (Cherry & Pascucci, 2023: 1) . هرچه باشد هنگام تکوین هنجارهای حقوقی بین‌المللی جاری . . . افق فناوری سایبری نمایان نبود (Schmitt, 2013: 3). از همین رو انطباق حقوق بین‌الملل برای رویارویی با ابعاد دشوار و نامعلوم فضای سایبری مانند کنترل استفاده از فناوری‌های پیشرفته سایبری حائز اهمیت است.

امروز هیچ چارچوب حقوقی مشخصی که حاکم بر حوزهٔ سایبری به‌ویژه در رابطه با کاربرد زور باشد، وجود ندارد، به همین دلیل برخی پژوهشگران موارد ارتکاب دولت‌ها به حملهٔ سایبری را تحت حاکمیت حقوق بین‌الملل و حقوق جنگ[1] ناظر بر کاربرد نیروی مسلح در سطح بین‌المللی دانسته‌اند (Roscini, 2010: 90).

پس پرسش اصلی، چگونگی اعمال حقوق بین‌الملل ناظر بر کاربرد زور در حوزهٔ سایبری است و بیش از آن به‌ویژه، آیا بند ۴ مادهٔ ۲ منشور ملل متحد در مورد منع کاربرد زور و دفاع از خود ذیل مادهٔ ۵۱ منشور را می‌توان در مورد حملات سایبری[2] به‌کار گرفت. با در نظر داشتن اینکه فضای سایبری میزبان مسائل جدید و بسیار دشوار حقوقی است، فرضیه‌ای که از پاسخ به پرسش اصلی شکل می‌گیرد آن است که اعمال حقوق بین‌الملل ناظر بر کاربرد زور در فضای سایبری با تردید و محدودیت و چالش‌های مهمی همراه است.

بخش نخست نوشتار، کاربرد حقوق بین‌الملل و به‌ویژه منشور ملل متحد در فضای سایبری و در عملیات سایبری را مورد بحث قرار می‌دهد و اقدامات صورت‌گرفته در این زمینه را که به شکل‌گیری چارچوب حقوقی موجود منجر شده است مرور می‌کند. بخش دوم این مسئله را بررسی می‌کند که در چه شرایطی حملهٔ سایبری می‌تواند کاربرد «زور» موردنظر بند ۴ مادهٔ ۲ منشور ملل متحد محسوب شود. بخش سوم شرایطی را که حملات سایبری می‌توانند به‌عنوان «حملهٔ مسلحانه» درگیر حق دفاع از خود تحت مادهٔ ۵۱ منشور شوند، همچنین موضوع چگونگی انتساب حملات سایبری بازیگران غیردولتی به یک دولت را به‌منظور دفاع از خود بررسی می‌کند. موضوع استفاده دولت‌ها از حق دفاع از خود علیه حملات سایبری بازیگران غیردولتی که منتسب به یک دولت نیستند، نیز به بحث گذاشته می‌شود. بخش چهارم کاربرد دفاع از خود پیشدستانه و پیشگیرانه در فضای سایبری را ارزیابی می‌کند. بخش پنجم به ارائهٔ آخرین نمونه‌های دفاع از خود سایبری در قالب دفاع پیشتاز و دفاع سایبری خودکار می‌پردازد. در بخش پایانی چگونگی فائق آمدن بر چالش‌های به‌جامانده بررسی می‌شود.

---

1. Jus ad bellum

۲. واژهٔ حملهٔ سایبری در اینجا به‌طور عام به‌کار رفته است. اینکه یک حملهٔ سایبری می‌تواند با توسل به زور یا یک حملهٔ مسلحانه برابری کند، در بخش‌های مربوط بررسی می‌شود.

۲. حقوق بین‌الملل و فضای سایبری

موضوع تبعیت فضای سایبری از قواعد حقوقی و همانا حقوق بین‌الملل سال‌هاست که مورد بحث محافل علمی و حقوقی و تصمیم‌گیران سیاسی بوده است. ویژگی‌های خاص فضای سایبری از جمله ماهیت بدون مرز بودن و به‌هم‌پیوستگی آن، سرزمینی و عینی بودن، و توانایی ناشناس ماندن، ماهیت غیرقابل شناسایی عملیات سایبری، هزینهٔ پایین ورود و خروج از آن و سرعت عملیات سایبری می‌تواند بیانگر آن باشد که این حوزه نمی‌تواند تابع قواعد حقوقی باشد (Buchan & Tsagourias, 2021: 115). این در حالی است که گفته می‌شود فضای سایبری می‌تواند برای مقاصد شرورانه به‌کار رود، همچنان‌که استفاده شده است، و چنین رفتاری می‌تواند صلح و امنیت بین‌المللی و نیز نظام حقوقی بین‌المللی را به خطر اندازد (UN GA. A/68/98, 2013: 6).

از همین رو، موضوع قواعد حقوقی و به‌ویژه چگونگی اعمال حقوق بین‌الملل بر فضای سایبری اهمیت زیادی کسب کرده است. نخستین کوشش برای شفاف‌سازی حقوق مربوط به منازعهٔ سایبری در سال ۲۰۰۸ صورت گرفت. در آن هنگام، مرکز عالی همکاری دفاع سایبری ناتو[1] واقع در تالین استونی از گروهی از کارشناسان مستقل بین‌المللی جهت نگارش دستورالعملی در مورد قانون حاکم بر جنگ سایبری دعوت کرد. حاصل تلاش سه‌سالهٔ بیست پژوهشگر حقوق بین‌الملل تدوین دستورالعمل تالین۱ در مورد قابلیت کاربرد حقوق بین‌الملل در مخاصمات سایبری بود[2] (Schmitt, 2013).

این دستورالعمل که شامل ۹۵ قاعده در هفت فصل در سال ۲۰۱۳ منتشر شد، به ادعای تدوین‌کنندگان، بازتاب حقوق بین‌الملل قراردادی یا عرفی بود که چگونگی اعمال رژیم حقوقی آنها بر اقدامات دولتی در جنگ سایبری را توصیف می‌کرد. این کار اولیه که چارچوب مهمی ارائه می‌داد، مجموعه دیدگاه‌های افرادی بود که با صلاحیت شخصی خود کار می‌کردند و لزوماً بازتاب مواضع ناتو یا هیچ دولتی نبود (Cherry & Pascucci, 2023: 4). در هر حال، دستورالعمل تالین۱ نقطهٔ آغازین بسیار خوبی برای توافق در مورد چگونگی کاربرد حقوق بین‌الملل در فضای سایبری بود.

در سپتامبر ۲۰۱۲ هارولد که[3] مشاور حقوقی وزارت امور خارجه ایالات متحده طی سخنرانی در کنفرانس حقوقی فرماندهی سایبری ایالات متحده[4] برای نخستین بار نظر این کشور در مورد کاربست حقوق بین‌الملل موجود در فضای سایبری را برای عموم اعلام کرد (Koh, 2012). ده سال بعد این موضع از سوی اکثریت جامعهٔ بین‌الملل پذیرفته شده است.

---

1. Cooperative Cyber Defence Centre of Excellence (CCDCOE)
2. Tallinn Manual on International Law Applicable to Cyber Warfare (Tallinn Manual)
3. Harold Koh
4. U.S. Cyber Command legal conference

در سال ۲۰۱۲ مجمع عمومی ملل متحد، گروه کارشناسان دولتی توسعهٔ اطلاعات و ارتباطات راه دور در زمینهٔ امنیت بین‌المللی[1] را تشکیل داد. مأموریت این گروه بررسی امکان اعمال حقوق بین‌الملل به‌طور کلی و به‌ویژه هنجارهای بین‌الملل در فضای سایبری و چگونگی کاربست آن بود. گزارش‌های ارائه‌شدهٔ گروه حاکی از تأیید کاربرد حقوق بین‌الملل در فضای سایبری بود. به‌ویژه گزارش سال ۲۰۱۳ گروه، با تأیید قابلیت اعمال حقوق بین‌الملل به‌ویژه منشور ملل متحد در فضای سایبری، تصدیق کرد که حاکمیت دولت و هنجارهای بین‌المللی و اصولی که از حاکمیت نشأت می‌گیرد، ناظر بر رفتار دولت‌ها در فعالیت‌های فناوری اطلاعات و ارتباطات از راه دور است. افزون بر این، گروه اعلام کرد دولت‌ها بر زیرساخت‌های اطلاعات و ارتباطات راه دور مستقر در قلمرو سرزمین خود اعمال صلاحیت دارند، و باید تعهدات بین‌المللی در زمینهٔ اعمال غیرقانونی منتسب به خود را پاسخگو باشند (UN GA. A/68/98, 2013: Paras.19-20) گزارش ۲۰۱۲ همچنین حاکمیت را به‌مثابهٔ شالودهٔ حقوق و تعهدات دولت‌ها در رابطه با عملیات سایبری شناخت، اما چگونگی ملزم ساختن دولت‌ها به انجام دادن یا ندادن اقدامات ویژه را مشخص نکرد (UN GA. A/68/98, 2013: Para. 8).

سه سال پس از دستورالعمل تالین۱، در سال ۲۰۱۵ گروه کارشناسان دولتی ملل متحد بسیاری از دستاوردهای سال ۲۰۱۲ کارشناسان، از جمله کاربرد منشور ملل متحد در فعالیت سایبری دولت و صلاحیت دولت‌ها بر زیرساخت مستقر در قلمروشان را تأیید کرد. در ادامه، گزارش سال ۲۰۱۵ گروه مقرر نمود که اصول حقوقی حاکم بر منازعهٔ مسلحانه، در اقدامات دولت در فضای سایبری قابل اجراست، اما وارد جزئیات کاربرد این اصول در فعالیت‌های سایبری نشد. مهم‌تر اینکه، درک مشترک از چگونگی کاربرد حقوق بین‌الملل را در ارتقای یک محیط سایبری آزاد، امن، باثبات، قابل دسترس و صلح‌آمیز تأیید کرد (UN DOC. A/70/174, 2015, Para.13). گروه همچنین فهرستی شامل هنجارهای داوطلبانه و غیرالزام‌آور رفتار مسئولانهٔ دولت‌ها به‌همراه فهرستی از اصول حقوق بین‌الملل قابل اجرا در فضای سایبری را تدوین کرد که شامل اصول حاکمیت دولت، برابری مطلق، حل‌وفصل مسالمت‌آمیز اختلافات، اصل خودداری از تهدید یا توسل به زور در روابط بین‌الملل و اصل عدم مداخله در امور داخلی سایر دولت‌ها بود (UN GA. A/70/174, 2015: Para. 26)

در سال ۲۰۱۷ دومین ویرایش تالین۱ با عنوان دستورالعمل تالین۲ در مورد کاربرد حقوق بین‌الملل در عملیات سایبری منتشر شد.[2] این دستورالعمل شامل ۱۵۴ قاعده بود و مهم‌تر از آن، حوزهٔ تحلیل را به شمول فعالیت‌های دولت در فضای سایبری در زمان صلح گسترش می‌داد. تالین۲ نیز مانند تالین۱ بازتاب نظرهای

1. Group of Governmental Experts on Developmeats in the Field of Informaton and Telecommunications in the Context of International Security. (GEE)
2. Tallinn Manual 2.0 on International Law Applicable to Cyber Operations (Tallinn Manual 2.0)

افراد بود، هرچند دولت‌ها به‌طور انفرادی یا جمعی کاربست حقوق بین‌الملل و منشور ملل متحد از جمله قواعد مربوط به کاربرد زور و دفاع از خود را به‌صراحت اعلام کردند (Cherry & Pascucci, 2023: 5).

در ۲۹ مه ۲۰۱۹ رئیس‌جمهور استونی، کرستی کالجولید[1] طی سخنرانی خود در افتتاحیهٔ کنفرانس بین‌المللی منازعهٔ سایبری[2]، دیدگاه کشورش را در مورد کاربرد حقوق بین‌الملل در فضای سایبری ارائه کرد. وی اعلام کرد که حقوق بین‌الملل در فضای سایبری قابل اجراست و دولت‌ها به‌طور قانونی مسئول فعالیت‌های خود هستند و همچنین مسئولیت دارند مقاومت خود در برابر تهدیدات سایبری را تقویت کنند. خانم کالجولید اظهار کرد طبق حقوق بین‌الملل دولت‌ها حق نسبت دادن فعالیت‌های سایبری را دارند؛ آنها حق دارند به عملیات سایبری ستیزه‌جویانه پاسخ دهند و به حق ذاتی دفاع از خود عمل کنند، زیرا در شرایطی این عملیات ممکن است کاربرد زور یا حملهٔ مسلحانه تلقی شود (Kaljulaid, 2019) .

در سپتامبر همان سال، وزارت دفاع فرانسه نیز بیانیه‌ای مبنی بر دیدگاه فرانسه در قابل اعمال بودن حقوق بین‌الملل به اقدامات دولتی در فضای سایبری منتشر کرد. این سند جامع دیدگاه فرانسه را در شماری از موضوعات از جمله حاکمیت، مداخله، توسل به زور و دفاع از خود و حقوق بشردوستانهٔ بین‌المللی مطرح می‌کرد. شاید مهم‌ترین موضع فرانسه آن بود که حاکمیت یک قاعدهٔ اصلی حقوق بین‌الملل است و چنانچه اقدامات یک دولت در فضای سایبری به ایجاد آثار فیزیکی در سرزمین دولت دیگری بینجامد، نقض حاکمیت دولتی است (Ministry of Defence of France, 2019).

در مارس۲۰۲۰ پل نی[3]، مشاور کل وزارت دفاع ایالات متحده ملاحظاتی را در کنفرانس سالانهٔ حقوقی فرماندهی سایبری ایراد کرد که بازتاب موضع این کشور در مورد کاربرد حقوق بین‌الملل به‌ویژه حقوق مخاصمات مسلحانه و حقوق مسئولیت دولت در عملیات سایبری بود (Ney, 2020: 22). وی با تأیید موضع ایالات متحده مبنی بر کاربرد حقوق بین‌الملل در عملیات سایبری، بر اهمیت توجه به رویهٔ دولت‌ها و اجماع حقوقی[4] در تعیین چگونگی کاربست حقوق بین‌الملل در عملیات سایبری تأکید کرد (Ney, 2020: 35).

در ۱۳ جولای ۲۰۲۱ مجمع عمومی ملل متحد خلاصهٔ گزارش رسمی گروه کارشناسان را منتشر کرد (UN GA. A/76/136, 2021). این گروه که در پی صدور قطعنامهٔ ۲۰۱۸ مجمع عمومی تشکیل شده بود از دولت‌ها خواسته بود نظرهای خود را در خصوص چگونگی کاربرد حقوق بین‌الملل در فعالیت‌های سایبری ارائه کنند (UN GA Res.73/266, 2018: Para.3). هدف، پیشبرد درک مشترک حقوق

1. Kersti Kaljulaid
2. International Conference on Cyber Conflict- Cycon
3. Paul Ney
4. Opinio Juris

بین‌الملل در فضای سایبری و ترویج هنجارها و اقدامات اعتمادسازی بود. نتیجهٔ کار، گزارش کوتاه حاوی تلفیقی از نظرهای پانزده دولت بود.[۱] ورای این فرایندها و بیانیه‌ها، مقدمات تشکیل یک کنوانسیون بین‌المللی ناموفق بوده است.[۲]

در ۲۲ آوریل ۲۰۲۲ کانادا نیز طی بیانیه‌ای دیدگاه خود را در زمینهٔ حقوق بین‌الملل در فضای سایبری منتشر کرد. موضع‌گیری کانادا دال بر این بود که حاکمیت سرزمینی یک قاعدهٔ حقوق بین‌الملل است، اما این قاعده مستلزم موافقت با هر فعالیت سایبری با آثاری همچون آسیب‌رسانی به برخی از قابلیت‌های دولت دیگر نیست (National Position of Canada, 2022).

ورای این مواضع رسمی کلی، روند پیشرفت کارگروه کارشناسی مطلوب نبوده است و این تا حد زیادی به‌دلیل اختلاف‌نظر اعضای گروه در مورد چگونگی اعمال هنجارهای قطعی در فضای سایبری بود که به ناکامی در ارائهٔ گزارش کارگروه در سال ۲۰۱۷ منجر شد (UN DOC. A/72/315, 2017). از آن زمان دو گروه در ملل متحد تشکیل شده است که به موازات هم فعالیت می‌کنند: یک گروه کارشناسی جدید متشکل از ۲۵ عضو انتخابی برای سال‌های ۲۰۱۹تا ۲۰۲۱ (UN GA Res. 73/266, 2018) و یک کارگروه دائم[۳] متشکل از همهٔ اعضای علاقه‌مند برای سال‌های ۲۰۱۹ تا۲۰۲۰ (UN GA Res.73/27, 2018). این دو گروه در کنار موضوعات دیگر کاربرد هنجارها، قواعد و اصول را در فضای سایبری بررسی می‌کنند.

با در نظر گرفتن روند طی‌شده، فرض بر این است که اجماع نسبی در خصوص کاربست بند ۴ مادهٔ ۲ و مادهٔ ۵۱ منشور ملل متحد و قواعد عرفی مربوط در فضای سایبری فراهم است، اما هنوز در مورد گستره، محتوا و چگونگی کاربرد آنها تردیدهایی وجود دارد، زیرا رویهٔ دولت‌ها و قواعد عام‌الشمول نیز همواره صریح و مشخص نیستند (Sander, 2019: 361-381). با چنین رویکردی، همهٔ این موضوعات در بخش‌های زیر بررسی می‌شوند.

۳. حملات سایبری و بند ۴ مادهٔ ۲ منشور ملل متحد

تنوع فعالیت‌های سایبری نظرات متفاوتی را در مورد شمولیت آنها در حوزهٔ قواعد منع توسل به زور در

---

۱. دولت‌ها عبارت بودند از: استرالیا، برزیل، اشرفی، المان، ژاپن، قزاقستان، کنیا، هلند، نروژ، رومانی، روسیه، سنگاپور، سوئیس، بریتانیا و ایالات متحده.

۲. برای آگاهی بیشتر ر.ک: Smith,Brad (2017). The Need for a Digital Geneva Convention' https:// blogs .microsoft .com/ wp -content/ uploads/ 2017/ 03/ Transcript-of -Brad -Smiths -Keynote - Address -at -the -RSA -Conference -2017 .pdf.

3. Open-Ended Working Group

روابط بین‌الملل مطرح کرده است (Roscini, 2014: 32)، و این پرسش وجود دارد که در چه شرایطی این فعالیت‌ها می‌توانند توسل به زور ذیل بند ۴ مادهٔ ۲ منشور ملل متحد محسوب شوند؟ پاسخ به این پرسش را با این پیش‌فرض در مورد مفهوم زور و رویکرد مبتنی بر آثار محوری[1] شروع می‌کنیم که استفاده از هر ابزاری که موجب مرگ، آسیب یا خسارت اساسی و نابودی شود، می‌تواند به‌مثابهٔ «زور» موردنظر بند ۴ مادهٔ ۲ منشور تلقی شود. این رویکرد هر حملهٔ سایبری با آثاری معادل آثار زور جنبشی[2] را مشمول قاعدهٔ منع توسل به زور قرار می‌دهد، هرچند ابزار مورد استفاده نظیر کرم‌ها یا ویروس‌ها جزء سلاح به مفهوم متعارف آن نباشند (Schmitt, 2017: Rules 68-69).

این رویکرد دو پرسش در پی دارد: نخست آنکه چه آثاری باید به‌عنوان آثار عینی یک حملهٔ سایبری که می‌تواند بلافاصله نیز ظاهر نشود، محسوب گردد، و پرسش دوم آیا آستانهٔ معینی از آسیب لازم است تا ماشهٔ بند ۴ مادهٔ ۲ فعال شود.

در مورد پرسش اول باید گفت حملات سایبری اغلب آثار واکنشی ایجاد می‌کنند. با آنکه مبدأ اصلی حمله که می‌تواند یک شبکه، سرور یا داده‌های موجود باشد، نابود نمی‌شود، دچار اختلال یا دستکاری گردد و آثار عینی ثانویه به‌بار آورد. برای مثال هنگامی‌که داده‌های کنترل ترافیک هوایی دستکاری شود منجر به تصادم هواپیماها می‌شود. حقیقت امر آن است که آثار بعدی به‌طور معمول همان چیزی است که موردنظر مهاجم بوده است. به همین دلیل، برای تعیین توسل به زور صورت گرفته، باید همهٔ نتایج شامل تمام آثار اتفاقی کنترل‌نشدنی و پیامدهای پیش‌بینی‌پذیر در نظر گرفته شود، زیرا بروز این آثار می‌تواند با تأخیر همراه شود و یا عینیت یافتن آنها اغلب ممکن است به تنظیمات سیستم وابسته باشد (Bochan & Tsagourias, 2021: 119).

در خصوص پرسش دوم یعنی تعیین آستانهٔ آسیب دو استدلال وجود دارد؛ استدلال اول هر میزان کاربرد زور، فارغ از شدت آن را کافی می‌داند (Ruys, 2014: 108)، درحالی‌که بنا به استدلال دوم استفاده از زور باید به آستانهٔ مشخصی برسد تا واجد شرایط توسل به زور موردنظر بند ۴ مادهٔ ۲ منشور ملل متحد باشد (Corten, 2012: 67-76). دیدگاه نخست کاربرد قاعدهٔ منع توسل به زور را تسهیل می‌کند و به آن عینیت می‌بخشد و قابلیت اجرای آن را توسعه می‌دهد، اما دیدگاه دوم قلمرو آن را محدود ساخته و قابلیت اجرایش را پیچیده می‌کند، چون هیچ آستانهٔ مشخص و روشنی وجود ندارد. افزون بر این، تشخیص نیل به آستانهٔ موردنظر، به چگونگی ارزیابی دولت قربانی از آثار عملیات، وابسته خواهد بود. در هر حال، هر دو دیدگاه می‌تواند به تشدید تنش‌ها منجر شود، اولی با تنزل دادن آستانهٔ واکنش و دومی با مجاز کردن دولت‌ها به کاربرد زور زیر آستانهٔ قانونی. هیچ پاسخ قطعی به این پرسش که چه آستانه‌ای باید ملاک باشد

1. effected based
2. Kinetic force

وجود ندارد و نظر دیوان بین‌المللی دادگستری هم در این باره خیلی کارساز نبوده است[1] (ICJ Rep. 161, 2003: Para.72). واقعیت آن است که حملات سایبری به‌سهولت می‌توانند تکرار شوند و آسیب محدودی داشته باشند، پس تعیین یک آستانهٔ حداقلی، منطقی به‌نظر می‌رسد تا از بی‌اعتبار شدن قاعدهٔ منع توسل به زور ممانعت کند. در هر حال، باید پذیرفت که حصول آستانهٔ موردنظر موضوعی مربوط به ارزیابی خود دولت قربانی است، زیرا تنها ارزیابی کمی آثار حملهٔ سایبری موردنظر نیست، بلکه ارزیابی کیفی آن نیز مطرح است (Netherlands letter to the Parliament, 2019: 4).

این الزام که حملهٔ سایبری باید آثار و پیامدهای عینی به‌بار آورد تا مصداق توسل به زور باشد، پرسش جالبی را مطرح می‌کند، اینکه چنانچه حملات سایبری آثار عینی خارجی نداشته باشند، مانند عملیاتی که سیستم فرماندهی و کنترل یک دولت یا بورس سهام آن را از کار بیندازد، می‌تواند کاربرد زور توصیف شود؟ این حملات هیچ چیز را منهدم نمی‌کنند، اما کارکرد سیستم را از بین می‌برد. همچنین آنها ممکن است هیچ پیامد عینی مشخص بیرونی نداشته باشند، اما بتوانند بر اقتصاد، حکمرانی یا ابعاد مهم دیگری از حیات یک دولت تأثیرات جدی بگذارند. در این مورد هم یک استدلال ادعا دارد که ماهیت متفاوت عملیات سایبری ایجاب می‌کند اختلال در عملکرد و آثار غیرعینی نیز مشمول تعریف زور قرار گیرد و نظر دیگر مخالف شمول آنهاست (Schmitt, 2017: Rule 69). به‌نظر می‌رسد حملات سایبری که به‌طور جدی یک سیستم را مختل یا تضعیف می‌کند و آثار غیرمادی به‌بار می‌آورد باید توسل به زور محسوب شود (Buchan & Tsagourias, 2021:127)، زیرا حتی اگر هیچ انهدامی در کار نباشد، عملکرد سیستم و کارکردهای آن از بین می‌رود و به‌دلیل وابستگی زندگی مدرن به زیرساخت سایبری، این می‌تواند موجب خسارات غیرمادی اساسی شود. افزون بر این، میان انهدام ساختمانی که زیرساخت فرماندهی و کنترل نظامی یک دولت در آن قرار دارد یا بورس سهام در آن جای داده شده، و خنثی‌سازی دقیق کارکردهای آن با حملهٔ سایبری تفاوت کمی وجود دارد. چنین حملاتی اگر زیرساخت حیاتی ملی را هدف قرار دهند، بسیار زیانبار خواهند بود. با آنکه تعریف مشخصی از زیرساخت حیاتی ملی وجود ندارد، طبق تعریف کلی مجمع عمومی ملل متحد زیرساخت حیاتی می‌تواند شامل تولید، انتقال و توزیع انرژی، حمل‌ونقل هوایی و دریایی، بانکداری و خدمات مالی، تجارت الکترونیک، تأمین آب، توزیع غذا و بهداشت عمومی باشد و زیرساخت‌های اطلاعاتی بسیار مهم که به‌طور فزاینده‌ای به هم پیوسته‌اند و عملکرد آنها را تحت تأثیر قرار می‌دهد (UN GA. Res.58/199, 2004: 1). به همین دلیل، حملهٔ سایبری که بر زیرساخت حیاتی ملی به‌طور جدی اثر بگذارد باید مشمول تعریف زور باشد، زیرا توانمندی عملکردی دولت را به مخاطره می‌اندازد.

---

۱. دیوان بین‌المللی دادگستری در رسیدگی به قضیهٔ «سکوهای نفتی» بین ایران و ایالات متحده، اعلام کرد که حتی مین‌گذاری تنها یک کشتی نظامی می‌توانست برای اعمال «حق ذاتی دفاع از خود» کافی باشد.

یافته‌های پیشین از برخی رخدادها حاکی از آن است که چنانچه تبعات حمله، محدود، موقت و قابل کنترل باشد، توسل به زور محسوب نخواهد شد (Buchan, 2012: 218-219) مانند حملهٔ شبکه‌ای سال ۲۰۰۷ به سایت‌های حکومتی و بانکی کشور استونی که مانع توزیع خدمات به کاربرها شد. در وضعیت مشابه، حمله به سایت‌های حکومتی، رسانه‌ای و مالی گرجستان در سال ۲۰۰۸ نیز نمی‌تواند توسل به زور تلقی شود. این موارد می‌تواند نقض اصل عدم مداخله محسوب شوند (Buchan, 2012: 221-226).

باید یادآور شد که رویهٔ دولت‌ها در این باره هنوز نامعلوم است. برخی با اتخاذ رویکرد زمینه‌ای[1] در مورد توسل به زور، حملات سایبری بدون پیامدهای عینی را به‌عنوان کاربرد زور سایبری تأیید می‌کنند. برای مثال فرانسه اعلام کرده است که اقدام سایبری بدون آثار عینی هم می‌تواند به‌عنوان توسل به زور توصیف شود. در نبود خسارت مادی، عمل سایبری می‌تواند کاربرد زور علیه مقیاس برخی از ضوابط همچون شرایط حاکم در زمان اقدام، محسوب شود . . . (Ministry of Defence of France, 2019) . دولت هلند در سال ۲۰۱۹ اعلام کرد «در حال حاضر احتمال اینکه یک عمل سایبری با آثار بسیار جدی مالی یا اقتصادی توسل به زور تلقی شود، غیرمحتمل نیست». در سال ۲۰۱۸ وزیر دفاع این کشور اظهار کرد: «چنانچه یک حملهٔ سایبری کل سیستم مالی هلند را هدف قرار دهد . . . یا مانع انجام وظایف اساسی حکومت همچون حفظ نظم و آرامش یا وضع مالیات شود . . . حملهٔ مسلحانه تلقی خواهد شد» (Buchan & Tsagourias, 2021: 122). از آنجایی که همهٔ حملات مسلحانه توسل به زور هستند، این اظهارنظر بدان معناست که یک حملهٔ سایبری که خسارات جدی اما غیرعینی به‌بار آورد، می‌تواند توسل به زور محسوب شود (Schmitt, 2019). بریتانیا[2] و ایالات متحده نیز با اتخاذ رویکرد زمینه‌ای، کاربرد زور را به عملیات ویرانگر محدود نمی‌کنند، رویکردی که دامنهٔ دفاع از خود را گسترش می‌دهد (Egan, 2017: 169).

۴. حملات سایبری و دفاع از خود

در این بخش به شرایطی می‌پردازیم که در آن حملهٔ سایبری می‌تواند به‌عنوان «حملهٔ مسلحانه» توصیف شده و به‌تبع آن موجب حق دفاع از خود دولت قربانی شود. هرچند گزارش سال ۲۰۱۵ گروه کارشناسان

---

1. contextual approach

رویکرد زمینه‌ای در علوم اجتماعی به رویکردی اطلاق می‌شود که بر چگونگی تأثیرگذاری شرایط احاطه‌کننده (بیرونی) بر آگاهی، اندیشه و عمل تمرکز دارد و بر اهمیت عوامل محیطی در عملکرد تأکید می‌کند.

۲. برای آگاهی از موضع دولت بریتانیا ر.ک:

Wright, J. United Kingdom Attorney General ‘Cyber and International Law in the 21st Century’ (23 May 2018) www .gov .uk/ government/ speeches/ cyber -and -international -law -in -the -21st -century.

به حق دفاع از خود اشاره نداشت، و بنابر گزارش‌ها، گسترهٔ آن در فضای سایبری یکی از موضوعاتی بود که به ناکامی گروه کارشناسان در سال ۲۰۱۷ انجامید، حق دفاع از خود به‌عنوان بخشی از منشور ملل متحد و حقوق عرفی در فضای سایبری نیز قابل اجراست. دولت‌ها نیز تأیید کرده‌اند که حملهٔ سایبری می‌تواند موجد حق دفاع از خود شود و برخی دولت‌ها بر این موضع اصرار ورزیده‌اند (Roguski, 2020: 2). اما بحث اساسی چگونگی اعمال حق دفاع از خود هنوز باقی است و دولت‌ها در مورد جزئیات رویهٔ دولتی یا اجماع دربارهٔ قواعد این حوزه به نتیجه نرسیده‌اند (Roguski, 2020: 24).

دیوان بین‌المللی دادگستری به‌طور ضمنی پذیرفته است که استفاده از تسلیحات غیرجنبشی می‌تواند نقض در جریان بررسی پروندهٔ نیکاراگوئه، حملهٔ مسلحانه را کاربرد زور با شدت معین و با در نظر گرفتن مقیاس و آثار آن تعریف کرده است (ICJ Rep.1986: Paras.191,195). این بدان معناست که هر حملهٔ سایبری که آثار عینی شدید داشته باشد می‌تواند به‌عنوان «حملهٔ مسلحانه» با پیامد دفاع از خود رده‌بندی شود، و برای برخی دولت‌ها شامل حملهٔ سایبری با آثار شدید غیرعینی نیز می‌شود (Netherlands'Letter to the Parliament, 2019: 8-9).

در اینجا لازم است به چگونگی اثرگذاری بند ۴ مادهٔ ۲ و مادهٔ ۵۱ و آستانهٔ تعامل آنها با یکدیگر اشاره شود. به‌نظر می‌رسد بند ۴ مادهٔ ۲ منشور کاربردی از زور را ساماندهی می‌کند که بین آستانهٔ حداقلی آن و آستانهٔ شدت مقرر برای دفاع از خود قرار می‌گیرد، چون هر کاربردی از زور که شدید یا بالاتر از آستانهٔ شدت باشد در محدودهٔ مادهٔ ۵۱ قرار می‌گیرد. این در حالی است که دولت‌های خاص همچون ایالات متحده آستانهٔ متمایزی بین توسل به زور و حملهٔ مسلحانه را نمی‌پذیرند، بلکه هر توسل به زوری را مانند یک حملهٔ مسلحانه تلقی می‌کنند که موجب حق دفاع از خود می‌شود (Koh, 2012: 7).

با این حال، حتی اگر چنین آستانه‌ای پذیرفته شود، هیچ معیار روشنی برای کمک به دولت‌ها یا حقوقدانان در تعیین شدت وجود ندارد. دیوان بین‌المللی دادگستری هم در ارائهٔ هرگونه شفافیت در مورد چگونگی اندازه‌گیری شدت یک حمله ناکام بوده است. در ارزیابی شدت، عوامل جغرافیایی، موقتی و مادی، همچنین عواملی نظیر ماهیت حمله، هدف آن، شمار آنانی که تحت تأثیر واقع شده‌اند، میزان خسارت وارده و تأثیر کلی بر دولت قربانی می‌تواند در نظر گرفته شود. تنها این عوامل نیستند و باید تأکید شود که هر ارزیابی در شرایطی صورت می‌گیرد و پیش از آنکه تماماً حقوقی یا واقعی باشد، به‌شدت سیاسی است (Buchan & Tsagourias, 2021:124).

موضوع دیگر مربوط به مواردی است که حملات سایبری پایین‌تر از آستانهٔ حملهٔ مسلحانه باشد. راهکار مبتنی بر نظریهٔ انباشت رویدادها[1]، مجموع حملات سایبری جزئی را به‌مثابهٔ یک حملهٔ مسلحانه

1. the accumulation of events theory

محسوب می‌کند که موجد حق دفاع از خود است، مشروط بر آنکه عاملیت حملات واحد باشد (Schmitt, 2017: Rule 71, Para.11). مبانی نظری در حقوق بین‌الملل از این دیدگاه حمایت می‌کند و مباحثات مستدل بسیاری در جانبداری از آن وجود دارد(Gazzini, 2006: 192) . سازوکار دوم اقدام متقابل قهری است (ICJ Rep.14, 1986: Para. 249) . نمونه آن، حملهٔ سایبری سال ۲۰۱۹ ایالات متحده علیه ایران است که در پاسخ به حملات منسوب به ایران به نفت‌کش‌ها در تنگهٔ هرمز و تیراندازی و انهدام یک پهپاد تجسسی بدون سرنشین آمریکایی صورت گرفت. گزارش‌ها حاکی از آن بود که «طی این حمله یک پایگاه بسیار مهم نیروهای شبه‌نظامی ایران که مرکز طراحی حملات علیه نفت‌کش‌ها بود منهدم شد و توانایی ایران در هدف‌گیری محرمانهٔ تردد کشتیرانی در خلیج‌فارس به‌طور موقت کاهش یافت. چون اقدام منتهی به انهدام یک پایگاه مهم، می‌توانست توسل به زور تلقی شود، دولت ایالات متحده به‌صراحت اعلام کرد حمله «کاملاً پایین‌تر از آستانهٔ جنگ تنظیم شده بود» (Barnes, 2019). در این صورت، پرسش مطرح این است که آیا اقدام ایالات متحده عمل قانونی دفاع از خود بود یا یک اقدام متقابل قانونی (حتی در صورت مسلحانه بودن، نمونهٔ یک عمل تلافی‌جویانهٔ مسلحانه)؟ با توجه به گزارش متفاوت دو دولت از رویداد، پاسخ این پرسش بسته به اینکه پهپاد هنگام سقوط در حریم هوایی ایران بوده باشد یا در حریم هوایی بین‌المللی متفاوت است. چنانچه پهپاد در حریم هوایی بین‌المللی بوده باشد، حملهٔ ایران توسل به زور غیرقانونی می‌بود و اقدام ایالات متحده به‌عنوان عمل تلافی‌جویانهٔ مسلحانه توجیه‌پذیر بود. اگر موضع ایالات متحده مبنی بر عدم تمایز میان کاربرد زور و حملهٔ مسلحانه مورد توجه قرار گیرد، و پهپاد در حریم هوایی بین‌المللی سقوط کرده باشد، اقدام ایالات متحده می‌تواند به‌عنوان عمل دفاع از خود توجیه گردد. همان‌طور که گفته شد استدلال ایالات متحده آن بود که اقدامش پایین‌تر از آستانهٔ جنگ بوده و این اشاره به توصیف اقدام به‌عنوان عمل تلافی‌جویانهٔ مسلح قانونی است که به لحاظ منطقی ادعایی متناسب با شرایط بود.

موضوع قابل بررسی دیگر آن است که آیا حملات سایبری بازیگران غیردولتی، می‌تواند به دفاع از خود منجر شود و چه کسی می‌تواند هدف اقدام دفاع از خود باشد. اهمیت مسئله آن است که هر چند نمونهٔ متعارف حملهٔ مسلحانه هجوم نیروهای مسلح یک دولت به درون سرزمین دولت دیگری است، تحولات اخیر حاکی از رشد فزایندهٔ ویژگی ترکیبی یا نامتقارن جنگ و منازعات بوده است (Pangrazzi, 2021: 9). منازعات ترکیبی به‌طور معمول انواع بازیگران دولتی و غیردولتی و نیز

نظریهٔ انباشت رویدادها مفهومی است که به تجمع و تأثیرگذاری وقایع مختلف بر روند یا نتیجهٔ یک فرایند یا پدیده اشاره دارد. این نظریه توضیح می‌دهد که وقوع مجموعه‌ای از رویدادها که به ظاهر جداگانه به‌نظر می‌رسند، می‌تواند با هم جمع شده و تأثیر قابل ملاحظه‌ای بر روند یا نتیجهٔموردنظر داشته باشد (برای مطالعهٔ بیش‌تر ر.ک: احمدی‌فرد و همکاران، ۱۴۰۲: ۵۰–۷۶).

تاکتیک‌های متفاوت را در بردارد (Schroefl & Kaufman, 2014: 862). از منظر حقوق بین‌الملل، این تحولات (به‌ویژه در رابطه با پیامدهای حملات ۱۱ سپتامبر ۲۰۰۱) بحثی اساسی را مطرح کرده است که آیا مقررات دفاع از خود می‌تواند در مواجهه با حملات بازیگران غیردولتی مناسب باشد؟ در پاسخ، تمایل برخی از دولت‌ها گسترش اساسی دامنهٔ دفاع از خود بوده است (Gray, 2018: 120, 200). این تحولات به لحاظ امکانات فنی جدید حملات سایبری اهمیت ویژه‌ای می‌یابد، چون ویژگی‌های فضای سایبری فرصت‌های بیشتری برای بازیگران غیردولتی فراهم می‌سازد تا دستور کارهایشان و حمله به دولت‌ها را دنبال کنند. به دولت‌ها نیز مجال می‌دهد با بازیگران غیردولتی برای حمله به دولت‌های دیگر همکاری کرده و همزمان میزانی از انکار موجه را نیز برای خود حفظ کنند (Buchan & Tsagourias, 2021: 125). بدین ترتیب چگونگی گسترش کاربست حق دفاع از خود به حملات بازیگران غیردولتی در فضای سایبری تبعات و چالش‌های ویژه‌ای را پدید می‌آورد.

چالش نخست، قابلیت انتساب حقوقی و فنی حمله است (Tsagourias & Farrel, 2020: 941). به‌طور سنتی حملهٔ مسلحانه ذیل مادهٔ ۵۱ منشور باید از سوی یک دولت به قلمرو دولت دیگری صورت گیرد. پس، حق دفاع از خود برای یک دولت به مفهوم دفاع از خودش در برابر رفتار نظامی غیرقانونی دولت دیگر است. با این حال با تغییر چهرهٔ مخاصمات، دولت‌ها و پژوهشگران ناگزیرند هنجارهای اساسی حقوقی همچون دفاع از خود را مورد توجه مجدد قرار دهند. چنانچه حملات سایبری افراد و گروه‌های خصوصی یا فراتر از آن بازیگران غیردولتی نیاز به پاسخ نظامی داشته باشد، باید قابل انتساب به یک دولت باشد. انتساب نه‌تنها یک مفهوم حقوقی است، بلکه ابعاد فنی و سیاسی نیز دارد. جنبهٔ حقوقی آن مربوط به نسبت دادن فنی حمله به عامل تهدید از طریق تحلیل قانونی است، درحالی‌که انتساب سیاسی وابسته به آگاهی و اطلاعات دیگری است تا حملهٔ بازیگر غیردولتی را به یک دولت نسبت دهد. این جنبه‌ها در تعامل با یکدیگرند، اما اگر یک دولت تصمیم بگیرد راه حقوقی را پیش بگیرد، لازم است عوامل فنی و سیاسی طبق معیار حقوقی تفسیر شوند و معیار حقوقی انتساب باید اقناع‌کننده باشد (Tsagourias, 2012: 229).

حقوق بین‌الملل برای نسبت دادن حملات غیردولتی به دولت‌هایی که سپس هدف اقدام دفاع از خود می‌شوند از معیار انتساب حقوق مسئولیت دولت بهره می‌گیرد (Buchan & Tsagourias, 2021: 126) در هر حال، این معیارها بسیار محدود، پرمسئولیت و پرتنش هستند و مواجهه با آنها در جهان عینی دشوار است، و در فضای سایبری به‌دلیل ناشناس بودن حملات، ویژگی چندمرحله‌ای و سرعت آن‌ها و حوزه‌های مختلف درگیر در یک حملهٔ سایبری، به‌مراتب حتی دشوارتر می‌شود (Netherland letter to the Parliament, 2019: 9). نکتهٔ مهم آن است که حتی اگر بتوان وقوع حملات از یک سرزمین مشخص را به اثبات رساند، باز روشن نیست که آیا واقعاً یک دولت در پس حملات بوده و اگر

چنین باشد آیا آن دولت حقیقتاً یک دولت واقعی و برحق بوده است. حملات سایبری اغلب از سرزمین دولت‌های متعددی به‌طور همزمان بروز می‌کنند. در فضای سایبری، مهاجم معمولاً از زیرساخت یک یا چند دولت ثالث غیر درگیر استفاده می‌کند و با هک کردن نشانی پروتکل اینترنتی[1] خود داخل نشانی‌های دیگر، از آنجا اقدام به حمله می‌کند (Singer & Friedman, 2014: 33). بنابراین خودش اغلب ناشناس می‌ماند. بدیهی است چنانچه فرد حقیقی یا ملیت فردی که در پس حملات سایبری است، یافت شود، بار مسئولیت اثبات درگیر بودن دولت یا پناهگاه امن بودن برای هکرها دشوارتر نیز می‌شود. بدین ترتیب روشن نخواهد بود که اقدام دفاع از خود علیه چه دولتی صورت می‌گیرد. علاوه بر این، از آنجایی که بدافزار[2] ممکن است نه‌تنها سیستم هدف را آلوده کند، بلکه به سایر رایانه‌های سراسر جهان نیز گسترش یابد، بروز آسیب‌های جانبی در فضای سایبری بسیار واقع‌بینانه خواهد بود (Pangrazzi, 2021: 17). بدین ترتیب، اغلب نه‌تنها مهاجم مشخص نیست، بلکه مخاطب حمله نیز دقیقاً روشن نیست. پس به‌نظر می‌رسد در اتخاذ تصمیم نظامی به‌منظور شروع یک اقدام (دیجیتالی یا جنبشی) دفاع از خود، باید دست‌کم توجه داشت که حملهٔ متقابل می‌تواند به یک دولت اشتباه اصابت کند و در نتیجه به یک طرف ثالث غیردرگیر صدمه بزند و آن را وارد مناقشهٔ ناخواسته کند. چنین اقدام اشتباه قهری علیه یک دولت صلح‌جو یا غیر درگیر، به‌دلیل غیرقانونی بودن، خود می‌تواند حملهٔ مسلحانه علیه آن دولت محسوب شود. این رویداد که نخست یک دولت غیردرگیر را به طرف جدید مناقشه تبدیل می‌کند، احتمال دارد چرخه تشدید را کلید بزند و آسیب‌های جانبی بیش‌تری به‌بار آورد. بنابراین، برای قانونی بودن دفاع از خود یا هرگونه اقدام دیگر، الزامات حقوقی انتساب و مبنای شهودی آن باید کافی و قابل قبول باشد. این همه، نشان از اهمیت موضوع انتساب دارد (Tsagourias & Farrell: 2020)، به همین دلیل است که دولت‌ها انتساب را به‌عنوان بخشی از حق ویژهٔ ملی خود در نظر می‌گیرند (NATO, 2018: Para.20) .

با آگاهی از دشواری‌ها حقوقی و تکنیکی انتساب، هرچند به‌نظر می‌رسد که در حملات سایبری به‌ندرت همهٔ شرایط لازم مندرج در مادهٔ ۵۱ منشور فراهم باشد، می‌توان گفت یک دولت خواه خود مرتکب حملهٔ مسلحانه شده باشد یا به‌طور اساسی درگیر حملهٔ مسلحانه‌ای شده باشد که توسط بازیگر غیردولتی راه‌اندازی شده است می‌تواند عامل حملهٔ مسلحانه تلقی شود. همچنین یک بازیگر غیردولتی هم می‌تواند با مسئولیت خود مرتکب حملهٔ مسلحانه شود و در نتیجه، هدف دفاع از خود قرار گیرد. با این رویه، بسیاری از مسائل در خصوص موضوع انتساب تا حد زیادی مرتفع می‌شود و صرف‌نظر از اینکه عامل حملهٔ سایبری، دولت یا بازیگر غیردولتی باشد، حق دفاع از خود می‌تواند علیه آن اعمال شود (Buchan & Tsagourias, 2021: 127) .

1. IP address
2. malware

۵. دفاع از خود پیشدستانه و پیشگیرانه

طبق حقوق بین‌الملل عرفی هنگامی‌که یک دولت با حملهٔ قریب‌الوقوع مواجه باشد، مشروط به ضرورت دفاع از خود، فوریت و شدت حمله، نبودن گزینهٔ دیگر و نداشتن فرصت برای بررسی بیشتر می‌تواند اقدام دفاعی اتخاذ کند. این همان دفاع از خود پیشدستانه[1] است. در مقابل، دفاع از خود پیشگیرانه[2] زمانی است که یک دولت علیه تهدید حملهٔ مسلحانه در آینده دست به اقدام دفاعی بزند. درحالی‌که امروز دفاع از خود پیشدستانه از توجیه قانونی نسبی برخوردار است، در مورد دفاع پیشگیرانه چنین نیست (UN GA. A/59/565, 2004: Paras.188, 189-192). در خصوص حملات سایبری، چنانچه حمله قریب‌الوقوع باشد، دولت قربانی می‌تواند اقدام به دفاع از خود پیشدستانه کند و این اقدام می‌تواند سایبری یا فیزیکی باشد (Egan, 2017: 178). لیکن باید یادآور شد که اثبات قریب‌الوقوع بودن حمله در فضای سایبری اگر غیرممکن نباشد، دشوار خواهد بود (Madubuike-Ekwe, 2021: 635). در بیشتر موارد به‌دلیل سرعت حملات سایبری و آثار فوری آن، دفاع از خود پیشدستانه کاربرد نخواهد داشت، مگر در موردی که حمله معوق باشد، مانند جاگذاری کد بمب منطقی[3]درون سیستم، مانند ویروس استاکس‌نت[4]، که دیرتر فعال می‌شود. در چنین مواردی، تشخیص زودهنگام و نیز شناخت روند عملیات و قصد مهاجمان، برای اقدام به دفاع از خود دولت حائز اهمیت است (Buchan & Tsagourias, 2021:127).

چنانچه حملهٔ سایبری مقدمهٔ یک حملهٔ عینی باشد، می‌تواند موجب دفاع از خود پیشدستانه شود. نمونهٔ چنین موردی حملهٔ اسرائیل به تأسیسات هسته‌ای الکبار[5] سوریه است که پیش‌درآمد آن حملهٔ سایبری به سیستم دفاع هوایی آن کشور بود (Gill and Ducheine, 2013: 438). سوریه در این مورد می‌توانست اقدام به دفاع از خود پیشدستانه کند.

اگر دفاع از خود پیشدستانه بنا به دلایلی که اشاره شد، قابل استفاده یا اجرا نباشد، کارامدترین گزینه، اقدام پیشگیرانه است که در حقوق بین‌الملل معاصر جایز نیست. در هر حال، اگر قریب‌الوقوع بودن طبق معیارهای واقعی و کیفی و نه‌فقط برحسب شرایط زودگذر تفسیر شود، دفاع از خودپیشدستانه و پیشگیرانه کاملاً به هم نزدیک می‌شوند. در این رابطه دستورالعمل تالین۲ از آخرین روزنهٔ فرصت (Schmitt, 2017: Rule73, Para.4) نام می‌برد که نشان می‌دهد عمل دفاع از خود می‌تواند خیلی پیش از حمله اتخاذ شود.

با در نظر گرفتن آنچه گفته شد به‌نظر می‌رسد ارزیابی قریب‌الوقوع بودن بر مبنای معیارهای نامحدود عاری از اشکال نباشد. شدت حمله برحسب کمیت به‌آسانی برآورد نمی‌شود و چون حملات سایبری

1. Anticipatory Self- Defencc
2. Preventive Self- Defence
3. Logic bomb
4. Stuxnet
5. Al-Kibar

به‌طور معمول مخفیانه و ناشناس هستند، امکان آگاه شدن از حمله در شرف وقوع در بیشتر موارد وجود ندارد، بدین ترتیب تشخیص عزم و قصد مهاجم نیز دشوار است. همان‌گونه که اشاره شد ارزیابی امری ذهنی و فردی است که مستلزم اطلاعات کامل، دانش و قابلیت‌های فنی است.

۵. ۱. دفاع پیشتاز و دفاع سایبری خودکار

«دفاع پیشتاز»[1] یک راهبرد درگیری مداوم با دشمن را توصیف می‌کند که اغلب مستلزم عملیات برون‌مرزی است (Buchan & Tsagourias, 2021: 128). این مفهوم در خلاصه طبقه‌بندی‌نشدهٔ وزارت دفاع ایالات متحده به مفهوم ایجاد اختلال یا قطع فعالیت سایبری مخرب در مبدأ آن است و شامل فعالیتی است که در سطحی پایین‌تر از منازعه مسلحانه قرار می‌گیرد. در ادامهٔ این خلاصه آمده است «این وزارتخانه به‌دنبال پیشگیری، خنثی‌سازی یا بازدارندگی از فعالیت سایبری مخربی است که زیرساخت حیاتی ایالات متحده را هدف بگیرد و بتواند به یک رویداد سایبری مهم منجر شود . . . وظیفهٔ اصلی ما در مأموریت دفاع از وطن «دفاع پیشتاز» با تمرکز بر توقف تهدیدات پیش از دستیابی به اهدافشان است[2](US Department of Defense, 2018).

پرسش مطرح آن است که کاربست بند ۴ مادهٔ ۲ و مادهٔ ۵۱ منشور ملل متحد در مفهوم دفاع پیشتاز تا چه حد است. آن‌گونه که از توصیف وزارت دفاع برمی‌آید عملیات «دفاع پیشتاز» می‌تواند هم به فعالیت‌های پایین از آستانهٔ کاربرد زور و هم بالاتر از آن پاسخ دهد. همچنین بسته به عملیاتی که به آن واکنش نشان داده می‌شود، دفاع پیشتاز می‌تواند قهری یا غیرقهری باشد. چنانچه هدف عملیات دفاع، متوقف کردن حملهٔ مسلحانهٔ در جریان یا قریب‌الوقوع باشد، می‌توان با انهدام برای مثال، شبکه‌ای که حمله از آن انجام شده یا قرار است انجام شود، متوسل به زور شد. چنین عملیاتی به‌عنوان عمل دفاع از خود باید از معیار ضرورت و تناسب و نیز قریب‌الوقوع بودن خطر تبعیت کند، هرچند معیار سوم همان‌طور که پیشتر اشاره شد موضوع پیچیده‌ای است.

اگر عملیات دفاع پیشتاز واکنش به عملیات مخرب زیر آستانهٔ حملهٔ مسلحانه باشد، می‌تواند به‌عنوان اقدام تلافی‌جویانهٔ مسلحانه توجیه شود، مشروط به آنکه در پاسخ مناسب به نقض مورد مهم‌تری از حقوق بین‌الملل باشد(Buchan & Tsagourias, 2021: 129). به‌عبارت دیگر، چنین عملی به‌عنوان

---

1. Defend forward

مفهوم «دفاع پیشتاز» که برخاسته از راهبرد امنیت سایبری وزارت دفاع ایالات متحده در سال ۲۰۱۸ است، حاکی از تفکری تهاجمی بازدارنده است که به‌طور کنشی فعالیت‌های سایبری مخرب را در مراحل اولیه مختل یا متوقف می‌سازد و هزینه را برای دشمن افزایش می‌دهد. برای مطالعهٔ بیشتر در این مورد ر.ک: Jeff Kosseff, 2019, the Contours of ‘Defend Forward”, under International Law,Tallin: NATO CCD COE Publications.

دفاع از خود در چارچوب نظریهٔ انباشت رویدادها توجیه‌پذیر است، البته منوط به اینکه حملات جزئی دیگری هم صورت گرفته باشد و به یکدیگر مرتبط باشند.

در هر حال، عملیات دفاع پیشتاز لزوماً نباید قهرآمیز باشد و بدون استفاده از زور هم می‌تواند مؤثر باشد و توسط سایر قواعد حقوق بین‌الملل توجیه شود، هرچند ممکن است مسائلی در زمینهٔ نقض حاکمیت دولت قربانی پدید آید (Tsagourias, 2021: 9-31). پرسش مهمی که می‌توان در خصوص عملیات «دفاع پیشتاز» غیرقهری مطرح کرد آن است که آیا دفاع از خود نیز می‌تواند شامل اقدامات غیرقهری باشد.

نظر به آنچه گفته شد، مشکلاتی در زمینهٔ مفهوم دفاع پیشتاز وجود دارد. نخست آنکه، دشمنی که سیستم‌هایش تجسس و پایش می‌شود[1] ممکن است چنین عملیاتی را به‌مثابهٔ مقدمهٔ حملهٔ مسلحانه تفسیر کرده و اقدام به دفاع از خود کند. دوم، امکان دارد عملیات «دفاع پیشتاز» بر شبکه‌های دولت‌های ثالث تأثیر گذارد و این مسئله را مطرح کند که آیا تلقی این دولت‌ها باید استفاده از زور علیه آنها باشد یا نقض تعهدی که به آنها داشتند. به‌نظر می‌رسد مفهوم «دفاع پیشتاز» می‌تواند همانند یک شمشیر دو لبه باشد که به‌ویژه در میان دولت‌های پیشرفته فنی، به‌جای پیشگیری از برخوردها، آنها را تشدید کند. افزون براین، مفهوم «دفاع پیشتاز» می‌تواند به فراگیر شدن و تداوم دفاع از خود منجر شود و تحت این مفهوم هیچ محدودیت جغرافیایی، ظاهری، واقعی یا زمانی برای آن وجود ندارد(Buchan & Tsagourias, 2021: 129).

نوع دیگر دفاع سایبری تهاجمی فعال، «دفاع سایبری خودکار»[2] است که کاربرد رایانه‌ها و هوش مصنوعی در شناسایی حملات و اقدام به دفاع بی‌درنگ را توصیف می‌کند. با پیشرفت فناوری، امکان دارد دولت‌ها بیشتر جذب این شکل از دفاع شوند چون قادر به تأمین بازدهی مقیاس و غلبه بر وقفه‌های زمانی در دفاع است. اما پرسش‌هایی هم در خصوص چگونگی کاربرد حقوق توسل به زور پیش می‌آورد (Tsagourias & Buchan, 2017: 203). دفاع سایبری خودکار برای قانونی بودن، باید در واکنش به یک حملهٔ مسلحانه باشد. اگرچه یک رایانه می‌تواند حمله را از لحاظ اهداف موردنظر تشخیص دهد و شاید بتواند کم و کیف آن را تعیین کند، امکان ندارد بتواند به‌درستی آن را زمینه‌یابی کند تا شدت و آثار بیرونی آن را به‌درستی تعیین کند. همچنین در شرایط پیچیده و ارزیابی سریع یا گمراهی عامدانه، رایانه قادر به احراز یک حمله از غیر آن نیست. علاوه بر اینها، رایانه‌ها نمی‌توانند از عهدهٔ کار مهم نسبت دادن حمله برآیند، مگر آنکه حمله از جانب رایانه‌های دولتی با علائم قابل شناسایی سرزده باشد، حتی در این صورت هم، رایانه قادر به تشخیص عامل رایانه نخواهد بود. چنانچه دفاع از خود علیه عامل چنین حمله‌ای

---

۱. برای مطالعهٔ بیشتر در این مورد، ر.ک:

Russell Buchan, 2018, Cyber Espionage and International Law, Oxford: Hart Publishing.

2. Automatic cyber defence

صرف‌نظر از دولتی یا غیردولتی بودن آن جایز باشد، همان‌گونه‌که اشاره شد ممکن است منشأ حمله جعلی باشد که رایانه قادر به تشخیص آن نیست. سرانجام، امکان ندارد یک رایانه بتواند ضرورت عمل دفاع از خود را اثبات کند، به‌ویژه اگر شناسایی حمله با تأخیر انجام شده باشد، و تعیین تناسب اقدام علیه اهداف عملیات نیز دشوار است. در واقع، برآورد نادرست می‌تواند اقدامی را که باید دفاعی باشد، به توسل به زور یا حملهٔ مسلحانه و پیامدهای مربوط تبدیل کند (Buchan & Tsagourias, 2021: 130).

این همه حاکی از آن است که دفاع سایبری خودکار می‌تواند در شرایط بسیار محدود و در محیطی ساده و ساختارمند کارامد باشد و کاربردهای گسترده‌تر آن مستلزم وجود انسان در چرخهٔ ماشینی یا توسعهٔ ظرفیت‌های خود فراگیری است که قادر به رقابت با استدلال و قضاوت بشری باشد.

۶. نتیجه

بررسی‌ها حاکی از وجود اجماع نسبی مبنی بر اعمال حقوق بین‌الملل در فضای سایبری و عملیات سایبری است، هرچند دیدگاه‌های متعارضی دربارهٔ چگونگی کاربرد قواعد بین‌المللی کاربرد زور به‌دلیل بحث‌انگیز بودن محتوا و گسترهٔ این قواعد، وجود دارد. از سوی دیگر فضای سایبری محیط عملیاتی جدید و پویایی است و به‌سبب ویژگی‌های منحصربه‌فردی که دارد چالش‌های جدیدی را به‌مثابهٔ موضوعاتی نوین با ابعاد فنی، سیاسی و حقوقی به جامعهٔ بین‌الملل عرضه داشته است. از این منظر انتظار نمی‌رود نظام حقوق بین‌الملل و به‌ویژه مقررات مربوط به کاربرد زور، قابلیت اجرا در فضای سایبری را داشته باشند. ارزیابی پیامدهای غیرعینی به‌مثابهٔ توسل به زور یا وقوع حملهٔ مسلحانه، جایگاه و نقش بازیگران غیردولتی، تعیین زمان و شرایط قریب‌الوقوع بودن حملهٔ مسلحانه، و موضوع نسبت دادن و مسئولیت دولت، برخی از چالش‌های موجودند که مورد بحث قرار گرفت. بنابراین، حتی اگر به لحاظ نظری با توجه به برخی دیدگاه‌ها، پروتکل‌ها و آرای دیوان بین‌المللی دادگستری بتوان نتیجه گرفت که امکان اعمال حقوق بین‌الملل در فضای سایبری وجود دارد، به‌وضوح می‌توان دریافت که در عمل آسان نیست و ابهاماتی در حقوق بین‌الملل موجود در ارتباط با کاربرد زور در فضای سایبری وجود دارد. بخشی از ابهامات مربوط به خود حقوق بین‌الملل است و برخی هم زاییدهٔ ویژگی‌های قلمرو سایبری است. بنابراین، به قواعد جدید و حتی چارچوب حقوقی جدیدی نیاز است که با در نظر گرفتن این ویژگی‌ها مقررات جدید خلق کند یا حتی قوانین موجود مربوط به کاربرد زور را با قلمرو سایبری سازگار سازد.

هرچه تلاش‌های بین‌المللی در این زمینه به طول انجامد، اقدامات ملی دولت‌ها در زمینهٔ ارتقای امنیت سایبری‌شان افزایش خواهد داشت. در حال حاضر بیشتر دولت‌هایی که از منابع مالی و انسانی متبحر آموزش‌دیده برخوردارند، با سرمایه‌گذاری‌های هنگفت سعی در توسعهٔ توانمندی‌ها و ارتقای

سیستم‌های امنیت سایبری خود دارند. در بخشی از این راهبرد، آنها با ایجاد فرماندهی نظامی سایبری، آمادهٔ واکنش به خطرهای ناشی از حملات سایبری شده‌اند و به‌تبع آن از توانمندی‌های تهاجمی سایبری خود برای از هم گسستن رقبایشان نیز بهره می‌گیرند. مادامی که چنین فرآیندهایی در مواجهه با خطرها، اهمیت غیرقابل بحثی داشته باشد، تنظیم مقررات اساسی حاکم بر رفتار سایبری دولت‌ها نیز بسیار حیاتی است. به این ترتیب، در سال‌های پیش رو احتمالاً شاهد توسعهٔ عملکرد دولتی و همچنین قواعد عام‌الشمول دربارهٔ حقوق بین‌الملل و فعالیت‌های سایبری خواهیم بود. در حال حاضر دستورالعمل تالین۳ در دستور کار گروهی از کارشناسان قرار دارد و با افزایش دیدگاه‌های دولت‌ها در مورد امکان کاربست حقوق بین‌الملل در فضای سایبری، توافقات بیشتری در راه خواهد بود. در عین حال پیشرفت سریع فناوری در پیشتازی از حقوق بین‌الملل ادامه خواهد داشت. در چنین چشم‌اندازی، هرچند دستیابی زودهنگام به ثبات اصول قانونی به دلیل منافع و قابلیت‌های ناهمگون دولت‌ها دشوار است، حقوق بین‌الملل موجود می‌تواند چارچوب مقرری برای گروه‌بندی و تنظیم فعالیت‌های سایبری فراهم سازد و مباحثات میان دولت‌ها و سایر بازیگران نیز هرچند با گام‌های آهسته و تدریجی به تثبیت و تحکیم این اصول کمک کند. وگرنه، آونگ حقوق کاربرد زور همان‌گونه‌که رونالد دورکین در سال ۱۹۸۶ در کتاب *امپراتوری حقوق* گفته است «میان گذشته منسوخ اما مشروع خود، و جادوی به‌وضوح نامشروع پیشرفت» (Dworkin, 1986: 348) ، همچنان در نوسان خواهد بود و قواعد آن در میان ضرورت پایداری و اصرار برای تغییر، منسوخ خواهد ماند.

منابع

۱. فارسی

– مقالات

۱. احمدی فرد، مرتضی؛ حاتمی، مهدی؛ آزادبخت، فرید (۱۴۰۲). نظریهٔ انباشت وقایع در توسل به دفاع مشروع بین‌المللی. *مجلهٔ حقوقی بین‌المللی*، ۴۰ (۷۰) ، ۵۳-۷۶. DOI: 10.22066/CILAMAG.2023.706167

۲. قاسمی، علی؛ چهاربخش، ویکتور بارین (۱۳۹۱). حملات سایبری و حقوق بین‌الملل. *مجلهٔ حقوقی دادگستری*، ۷۶ (۷۸)، ۱۱۵-۱۴۵ DOI: https://doi.org/10.22106/jlj.2012.11057

۲. انگلیسی

A) Books

1. Buchan, R. (2018). *Cyber Espionage and International Law*. Oxford: Hart Publishing.
2. Corten, O. (2012). *The Law against War: The Prohibition on the Use of Force in Contemporary International Law.* Oxford: Hart Publishing.

3. Dworkin, R. (1986). *Law's Empire*. Cambridge*:* Harvard University Press.
4. Gazzini, T. (2006).*The Changing Rules on the Use of Force in International Law.* Manchester University Press.
5. Gray, C. (2018). *International Law and the Use of Force.* 4th ed. Oxford: Oxford University Press.
6. Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.
7. Schmitt, M. N. (ed.), (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.
8. Singer P.W., & Friedman A. (2014). *Cybersecurity and Cyberwar, What Everyone Needs to Know*. Oxford: Oxford University Press.

B) Articles

9. Barnes, J. E. (2019). U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say., *The New York Times*, 28 August 2019, www.nytimes .com/ 2019/ 08/ 28/ us/ politics/ us - iran -cyber -attack .html? action = click&module = Top %20Stories & pgtype =Homepage.
10. Buchan, R., & Tsagourias, N. (2021). Cyber Attacks, Use of Force and Self-Defense. In *Regulating the Use of Force in International Law, Stability and Change*, by Russell Buchan and Nicholas Tsagourias, Cheltenham: Edward Elgar Publishing pp. 114-130.
11. Buchan, R. (2012). Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?. *Journal of Conflict* and *Security Law* (17)2, pp.211-227. Doi:10.1093/jcs1/krs014.
12. Cherry, L. M., & Pascucci, P. P. (2023). International Law in Cyberspace, in ABA *(American Bar Association*),https://www.americanbar.org/groups/law_national_security/publications/aba-standing-committee-on-law-and-national-security-60-th-anniversary-an-anthology/international-law-in-cyberspace/
13. Convention on Cybercrime (also known as the Budapest Convention), (2001), Nov. 23, ETS No. 185, and the Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts Committed through Computer Systems, Jan. 28, 2003, ETS No. 189.
14. Egan, B. J. (2017). International Law and Stability in Cyberspace, *Berkeley J. Int'l Law* (35)1, 169-180. (DOI) http://dx.doi.org/
15. Gill, T. D., & Ducheine, P.A. L. (2013). Anticipatory Self-Defense in the Cyber Context, *International Law Studies* (89)1, 438-471.
16. Koh, H. H. (2012). International Law in Cyberspace.*Harvard International Law Journal* (54*)* 1-12. https://doi.org/10.1093/ejil/chaa057.
17. Madubuike-Ekwe, J.N. (2021). Cyberattack and the Use of Force in International Law, *Beijing Law Review*, (12), pp. 631-649. https://doi.org/10.4236/blr.2021.122034
18. Ney, P. C. Jr. (2020). Some Considerations for Conducting Legal Reviews of U.S. Military Cyber Operations. *Harvard International Law Journal* (62)2, 22-41.
19. Pangrazzi, S. (2021). Self-Defense against Cyberattacks? Digital and Kinetic Defense in Light of Article 51 UN Charter, Geneva: ICT4Peace Publishing. 1-22.
20. Ruys, T. (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. DOI: 10.5305/amerjintelaw.108.2.0159.

21. Schroefl, J., & Kaufman, S. (2014). Hybrid Actors, Tactical Variety: Rethinking Asymmetric and Hybrid War, *Studies in Conflict and Terrorism*, 37(10), 862-880. https://doi.org/10.1080/1057610X.2014.941435.
22. Tsagourias, N. (2019). The Slow Process of Normativizing Cyberspace. *American Journal of International Law* (113) Unbound 71, 71-75. https://doi.org/10.1017/aju.2019.9.
23. Tsagourias, N. (2012). Cyber Attacks, Self- Defense and the Problem of Attribution. *Journal of Conflict and Security Law,* (17)2, 229-244. https://doi.org/10.1093/jcsl/krs019.
24. Tsagourias, N., & Farrell, M. (2020). Cyber Attribution: Technical and Legal Approaches and Challenges. *European Journal of International Law* (31)3, 941-967. https://doi.org/10.1093/ejil/chaa057

C) Documents, Reports, Essays

25. ICJ International Court of Justice (1986). "Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Judgment Merits", ICJ Rep. 14, 27 Jun 1986, http://www.icj-cij.org/docket/files/70/6503.pdf.
26. ICJ International Court of Justice (2003). "Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America), Merits" ICJ Rep. 161, 6 November 2003.
27. Kaljulaid, K. (2019). President of the Republic of Estonia, *Remarks at the Opening of CyCon 2019* (May 29, 2019). https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html.
28. Kosseff, J. (2019). *The Contours of 'Defend Forward" under International Law*, Tallinn: NATO CCD COE Publications.
29. Ministry of Defense of France, (2019). *International Law Applied to Operations in Cyberspace*, Sept. 9, 2019. https://cyberlaw.ccdcoe.org/wiki/ National_position_of_France (2019)? oldid=3763.
30. National Position of Canada, (2022).*International Law in Cyberspace*. April 22, 2022. https://cyberlaw.ccdcoe.org/wiki/National_position_of_Canada_(2022)?oldid=4128.
31. NATO, (2018) 'Brussels Summit Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Brussels 11–12 July 2018', para. 20, www.nat int/ cps/en/ natohq/ official texts 156624 htm? Selected Locale = u k.
32. Netherlands Letter to the Parliament on *the International Legal Order in Cyberspace'* (2019) www .government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/ letter-to-the-parliament-on-the-international-legal-order-in-cyberspace.
33. Roguski, P. (2020). *Application of International Law to Cyber Operations: A Comparative Analysis of States'Views***,**The Hague Program for Cyber Norms Policy Brief. March 2020. https://www.thehaguecybernorms.nl › application-of-int.
34. Schmitt, M. N. (2019). '*France's Major Statement on International Law and Cyber: An Assessment'* (16 September 2019) Just Security, www .just security .org/ 66194/frances-

major -statement -on -international -law -and -cyber -an -assessment/ .
35. Talem, C. (2020). *International Law in Cyberspace: Cyber Attacks as Use of Force*, Center for Cyber Security and International Relations Studies (CCSSII). https://www.cssii.unifi.it/ls-6-cyber-security.html.
36. UN GA. A/73/266, General Assembly Resolution on Advancing Responsible State Behavior in cyberspace in the context of international security, UN Document A/73/266, 22 December 2018.
37. UN GA. A/76/136, General Assembly Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States, UN Document A/76/136, 13 July 2021.
38. UN GA. A/68/98, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Document A/68/98, June 24, 2013.
39. UN GA. A/59/565, Report of the Secretary-General's High-Level Panel on Threats, Challenges and Change, 'A More Secure World: Our Shared Responsibility', UN Doc. A/59/565, 2 December 2004.
40. UN GA. A/72/315, General Assembly Resolution on Developments in the field of information and telecommunications in the context of international security, UN Document Res. A/72/315, 11 August, 2017.
41. U.N. GA. A/70/174, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Document Res. A/70/174, 22 July 2015.
42. UN GA. 58/199, General Assembly Resolution on Creation of a global culture of cybersecurity and the protection of critical information infrastructures 30 January 2004.
43. UN GA. A/73/27, General Assembly Resolution on_Developments in the field of information and telecommunications in the context of international security, UN Document Res. A/73/27, 5 December 2018.
44. UN Secretary-General's address to the 76th Session of the UN General Assembly, 21 September 2021.
45. US Department of Defense, (2018). '*Summary, Department of Defense Cyber Strategy 2018'* (2018) 2, https:// media .defense.gov/ 2018/ Sep/ 18/ 2002041658/ -1/ -1/ 1/ CYBER_STRATEGY SUMMARY FINAL .PDF.
46. Wright, J. (2018). United Kingdom Attorney General, '*Cyber and International Law in the 21st Century'* (23 May 2018) www .gov.uk/ government/ speeches/ cyber -and -international -law -in -the -21st -century.