Cyber War Crimes through Non-International Armed Conflict Arising from Cyber Warfare

Hossein Mirmohammad Sadeghi[1], Mahdi Hosseini[2*]

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

S.D.I.L.
The SD Institute of Law Research & Study

Publisher:
Shahr-e- Danesh Research And Study Institute of Law

Article Type:
Original Research

DOI:
10.48300/jlr.2024.461397.2663

Received:
6 May 2024

Accepted:
17 July 2024

Published:
5 January 2026

ABSTRACT

Despite the increasing prevalence of cyber warfare and the need to apply the laws of armed conflict (jus in bello), existing regulations were designed for traditional physical warfare, making their application to modern cyber operations a significant challenge. A primary hurdle to prosecuting war crimes in this domain is establishing the requisite contextual element: the existence of an armed conflict. Specifically, cyber attacks by non-state armed groups can constitute war crimes only if they occur within the context of a non-international armed conflict. Consequently, this research investigates the feasibility of a non-international armed conflict arising from cyber warfare as a condition for realizing cyber war crimes. Using a descriptive-analytical method and library resources, the study concludes that the nature of cyber groups, characterized by

the physical dispersal of members, potential lack of consensus, and absence of traditional internal discipline, does not fully align with established legal criteria for an organized armed group. Therefore, only through a contemporary and dynamic interpretation of existing regulations and jurisprudence can the threshold for a non-international cyber armed conflict be met, thereby enabling the contextual element for war crimes to be satisfied.

Keywords: Cyber War Crime, Non-International Armed Conflict, Cyber Warfare, Organized Armed Group, Threshold of Violence.

Excerpted from the Ph.D. thesis entitled "Feasibility of War Crimes Occurrence in Cyber War", Faculty of Law, Shahid Beheshti University, Tehran, Iran.

Funding:

The author(s) received no financial support (funding, grants, and sponsorship) for the research, authorship, and/or publication of this article.

Author contributions:

Hossein Mirmohammad Sadeghi: Conceptualization, Data Curation, Supervision.

Mahdi Hosseini: Methodology, Software, Validation, Formal Analysis, Investigation, Resources, Writing - Original Draft, Writing - Review & Editing, Project Administration.

Competing interests: The authors declare that they have no competing interests.

Citation:
Mirmohammad Sadeghi, Hossein & Mahdi Hosseini. "Cyber War Crimes through Non-International Armed Conflict Arising from Cyber Warfare". *Journal of Legal Research*, 24, no. 64 (January 5, 2026), 7-40.

Extended Abstract

The increasing use of cyber warfare by non-state groups, and the exploitation of its disruptive capabilities to harm civilians, has rendered the regulation of such activities through the lens of international humanitarian law (IHL) both urgent and inevitable. However, despite this imperative, the laws of armed conflict, including the conditions for establishing war crimes, were formulated for traditional physical warfare, creating significant challenges for their application to modern cyber operations. Under the Rome Statute and the Elements of Crimes, the application of Article 8 (war crimes) is contingent upon both a violation of IHL and the existence of an armed conflict, as IHL applies only within that framework. Consequently, the primary legal hurdle to prosecuting cyber war crimes is establishing the requisite contextual element: proving that a cyber operation occurred within an armed conflict. Armed conflicts are categorized as international or non-international, each with distinct thresholds, and the applicable classification depends on the specific alleged crime. To date, no cyber attack has been formally recognized as constituting a non-international armed conflict (NIAC), and international consensus on defining a non-international cyber armed conflict is absent.

This research therefore addresses a central question: Can cyber attacks alone generate a non-international armed conflict and, consequently, fall under the jurisdiction of the International Criminal Court (ICC) as war crimes? Employing a descriptive-analytical method and library resources, the study investigates how a NIAC, as the contextual element for cyber war crimes, can be established through cyber warfare. It proceeds by defining armed conflict, analyzing the constitutive elements of a non-international cyber armed conflict, and assessing whether independent cyber attacks can reach the required threshold. The research focuses specifically on attacks that are not part of a pre-existing armed conflict but are freestanding. The analysis concludes that establishing a NIAC through cyber warfare hinges on fulfilling three core elements: a sufficient threshold of violence, the armed nature of the perpetrating group, and its organized nature. Regarding the threshold of violence, cyber attacks must amount to "protracted armed violence." A restrictive interpretation limiting "violence" to physical effects would exclude highly disruptive cyber operations targeting national infrastructure, necessitating instead a broad, effects-based approach that considers the severity of the consequences. Concerning the armed nature of the group, the concept of a "weapon" must evolve beyond traditional arms to include modern cyber capabilities for IHL to remain relevant. The most significant challenge lies in the criterion of the organized nature of the group. A traditional, formalistic analysis of "organization" would likely exclude loosely

structured cyber collectives. However, the absence of a conventional hierarchy does not equate to an absence of capability, as cyber groups with weak structures can still coordinate potent operations. Therefore, it is imperative for the ICC to adopt a flexible and contemporary interpretive approach to "organized armed group." Only through such a dynamic legal interpretation can this element be satisfied, thereby encompassing powerful cyber collectives within the scope of Article 8 and enabling the recognition of a non-international cyber armed conflict. This, in turn, is the essential step for the potential prosecution of cyber warfare under international criminal law.

جنایت جنگی سایبری از رهگذرِ مخاصمه مسلحانه غیربین‌المللی ناشی از رایاجنگ

حسین میرمحمدصادقی[۱]، مهدی حسینی[۲*]

۱. استاد، گروه حقوق جزا و جرم‌شناسی، دانشکده حقوق، دانشگاه شهید بهشتی، تهران، ایران.
h_sadeghi@sbu.ac.ir
۲. دکترای حقوق کیفری و جرم‌شناسی، دانشکده حقوق، دانشگاه شهید بهشتی، تهران، ایران.
*نویسنده مسئول: hosseini.mhdi@gmail.com

پژوهشکدهٔ حقوق

نوع مقاله:
پژوهشی

DOI:
10.48300/jlr.2024.461397.2663

تاریخ دریافت:
۱۷ اردیبهشت ۱۴۰۳

تاریخ پذیرش:
۲۷ تیر ۱۴۰۳

تاریخ انتشار:
۱۵ دی ۱۴۰۴

چکیده:

علی‌رغم افزایش روزافزونِ رایاجنگ‌ها و ضرورت وضع محدودیت‌های حقوق جنگ بر آنها، مقررات مربوط به حقوق جنگ متناسب با جنگ‌های فیزیکی سنتی وضع شده است و کاربست آنها در پهنه رایاجنگ‌های مدرن با چالش‌هایی مواجه است. تحقق عنصر زمینه‌ای وقوع جنایات جنگی در رایاجنگ‌ها، یعنی وجود یک مخاصمه مسلحانه، چالش اولیه وقوع جنایت جنگی از رهگذرِ رایاجنگ‌ها دانسته می‌شود. توضیح آنکه رایاجنگ‌های ارتکاب‌یافته از سوی گروه‌های غیردولتی در صورتی یارای آن هستند که به‌عنوان جنایت جنگی سایبری تلقی شوند که لزوماً در بستر یک مخاصمه مسلحانه غیربین‌المللی واقع شده باشند. بر این اساس، امکان‌سنجی وقوع مخاصمه مسلحانه غیربین‌المللیِ سایبری به‌منظور تحقق جنایات جنگی سایبری، موضوع اصلی این پژوهش است که با روش توصیفی ـ تحلیلی و با استفاده از منابع کتابخانه‌ای، تلاش می‌شود تا به آن پاسخ داده شود. برآمد این پژوهش بر آن است که ماهیت گروه‌های سایبریِ مرتکبِ رایاجنگ،

مقتضیِ وجود صفاتی همچون عدم تجمع اعضای گروه، فقدان هم‌صدایی و نبود سازکارهای انضباطی در گروه‌های مذکور است. صفات نام‌برده با ارکان مخاصمه مسلحانه غیربین‌المللی همچون «سازمان‌یافتگیِ گروه مرتکب»، در سازواری کامل قرار نمی‌گیرد. بر این اساس تنها در صورت استنباط روزآمد و پویا از مقررات و رویه قضایی موجود، امکان وقوع مخاصمات مذکور از طریق رایاجنگ و تحقق عنصر زمینه‌ای جنایات جنگی وجود دارد.

کلیدواژه‌ها:
جنایت جنگی سایبری، مخاصمه مسلحانه غیربین‌المللی، رایاجنگ، گروه مسلح سازمان‌یافته، آستانه خشونت.

برگرفته از رساله دکتری با عنوان « امکان‌سنجی وقوع جنایات جنگی در رایاجنگ»، دانشکده حقوق، دانشگاه شهید بهشتی، تهران، ایران.

حامی مالی:
این مقاله هیچ حامی مالی ندارد.

مشارکت نویسندگان:
حسین میرمحمدصادقی: مفهوم‌سازی، نظارت بر داده‌ها، نظارت.
مهدی حسینی: روش‌شناسی، استفاده از نرم‌افزار، اعتبارسنجی، تحلیل، تحقیق و بررسی، منابع، نوشتن ـ پیش‌نویس اصلی، نوشتن ـ بررسی و ویرایش، مدیریت پروژه.

تعارض منافع:
بنابر اظهار نویسندگان این مقاله تعارض منافع ندارد.

استناددهی:
میرمحمدصادقی، حسین و مهدی حسینی. «جنایت جنگی سایبری از رهگذرِ مخاصمه مسلحانه غیربین‌المللی ناشی از رایاجنگ». *مجله پژوهشهای حقوقی*، ۲۴، ش. ۶۴ (۱۵ دی ۱۴۰۴)، ۷-۴۰.

مقدمه

تعقیب و محاکمه مرتکبان نقضِ عمده حقوق بشردوستانه بین‌المللی به‌وسیله دادگاه‌های کیفری ملیِ محل وقوع نقض (مستند به صلاحیت سرزمینی) یا محل حضور متهم (مستند به صلاحیت جهانی) موضوعی ممکن و شاید سودمند دانسته شده است[۱] و دولت‌ها نیز به شناسایی درگیری‌های واقع‌شده در قلمرو سرزمینی آنها به‌عنوان «مخاصمه مسلحانه» مایل نیستند. این در حالی است که از یک سو، ظرفیت دولت‌ها برای استفاده از ارتباطات و فناوری اطلاعات برای انجام حملات سایبری به اهداف نظامی و غیرنظامی در هزاره سوم به‌شدت افزایش یافته است و از سوی دیگر، ظرفیت دولت‌ها برای پاسخ به این شکل سریع و در حال تکاملِ جنگ با فناوری پیشرفته، از توسعه انواع جدید قوای نظامی به‌ویژه فناوری‌های جدیدی مانند تسلیحات موجود در فضای سایبر و رایاجنگ‌ها، عقب مانده است.

علی‌رغم اینکه برخی از اندیشمندان در خصوص ظرفیت دادگاه‌های کیفری موقت یا دیوان کیفری بین‌المللی برای جلوگیری از جنایات ظالمانه سایبری موضع بدبینانه‌ای اتخاذ می‌کنند[۲]، تحقیقاتی وجود دارد که مؤید نقش بازدارنده دادگاه‌ها و دیوان مذکور در پیشگیری از وقوع جنایات بزرگ است[۳] و برخی مطالعات بیانگر بازدارندگی دیوان کیفری بین‌المللی نسبت به ارتکاب جنایات بین‌المللی است.[۴] بر این اساس چنانچه بتوان برخی از رایاجنگ‌ها را در چهارچوب حقوق کیفری بین‌المللی و در صلاحیت رسیدگی دیوان کیفری بین‌المللی قرار داد، به‌ویژه در مواردی که این اقدامات واجد اوصاف جرایم

---

۱. برای نمونه، نک: جمشید ممتاز و فریده شایگان، *حقوق بین‌الملل بشردوستانه در برابر چالش‌های مخاصمات مسلحانه معاصر* (تهران: مؤسسه مطالعات و پژوهشهای حقوقی شهر دانش، ۱۳۹۷)، ۱۹۳-۲۲۴.

۲. در این خصوص برخی پژوهش‌ها عوامل متعدد مربوط به وجود گسست میان مقررات تنظیم‌گر جنگ و افزایش گسترده خشونت‌های غیرقابل‌کنترل و جنگ‌های مرتبط با جنگ را واکاوی می‌کنند. در این راستا به علل زیر اشاره شده است: ۱. دولت‌ها و به‌ویژه دولت‌های قدرتمند، اجازه نمی‌دهند قوانین بین‌المللی بر منافع نظامی و امنیت ملی آنها غلبه کند. ۲. کنوانسیون‌های ژنو دارای مکانیسم اجرایی قدرتمند و دقیق برای اجرای مفاد خود نداشتند. ۳. ابهام در تعریف ماهیت یک مخاصمه مسلحانه و موضوعیت داخلی یا بین‌المللی داشتنِ مخاصمات مسلحانه. برای مطالعه بیشتر در این خصوص، نک:

Steven B. Remy, *War Crimes, Law, Politics & Armed Conflict in the Modern World* (New York: Routledge, 2023), 65-66.

3. J. R. McAllister, "Deterring wartime atrocities: Hard lessons from the Yugoslav tribunal", *International Security*, 44, (2020), 85.

4. H. Jo & B. A. Simmons, "Can the International Criminal Court deter atrocity?", *International Organization*, 70, 3(2016), 443-475; C. Hillebrecht, "The deterrent effects of the international criminal court: Evidence from Libya", *International Interactions*, 42, 4(2016), 616-643.

بزرگ‌مقیاس از قبیل نسل‌زدایی، جنایت علیه بشریت، تجاوز و جرایم جنگی باشند،[۵] تعقیب بین‌المللی آنها می‌تواند نقش مؤثری در پیشگیری از ارتکاب چنین جنایاتی ایفا نماید. در این راستا افزایش روزافزونِ رایاجنگ‌ها[۶]، رسیدگی دیوان کیفری بین‌المللی به جنایات جنگی ارتکاب‌یافته در بستر رایاجنگ‌ها را ناگزیر ساخته بود. در سال ۲۰۲۳، دادستان دیوان کیفری بین‌المللی به‌صراحت طی یک مقاله اعلام نمود: «هرچند هیچ ماده‌ای از اساسنامه رم مشخصاً به رایاجنگ‌ها اختصاص ندارد، چنین رفتاری ممکن است به‌طور بالقوه عناصر بسیاری از جنایات بین‌المللی، همچون جنایات جنگی را که قبلاً تعریف شده است، برآورده کند».[۷] دفتر دادستانی دیوان نیز آن را به‌عنوان موضع رسمی و کنونی دیوان کیفری بین‌المللی تأیید نمود.[۸] در پرتو این راهبرد، افزون بر ضرورت تطبیق عناصر عمومی و اختصاصی «جنایات جنگی» بر «رایاجنگ‌ها»، دادستان مکلف است وجود عنصر زمینه‌ای ارتکاب جنایت جنگی، یعنی وقوع مخاصمه مسلحانه را نیز ثابت کند.[۹]

توضیح آنکه در خصوص ماده ۸ اساسنامه رم[۱۰]، سند عناصر جنایات مذکور در اساسنامه[۱۱] مقرر می‌دارد که «جنایت جنگی ضرورتاً در چهارچوب و با مشارکت در یک مخاصمه مسلحانه انجام می‌شود». همچنین مستند به اساسنامه رم و عناصر جنایات مذکور در اساسنامه رم[۱۲]، کاربست ماده ۸ اساسنامه رم و وقوع جنایات جنگی، از یک سو منوط به جریان داشتنِ حقوق بشردوستانه بین‌المللی و نقض آن است[۱۳] و از سوی دیگر، جریان حقوق بشردوستانه بین‌المللی نیز لزوماً در بستر وجود یک مخاصمه

---

۵. پیمان نمامیان و نجات امیری، «امکان‌سنجی گسترش قلمرو صلاحیت دیوان کیفری بین‌المللی در قبال سلاح‌های ساخته‌شده با فناوری نانو»، *حقوق فناوری‌های نوین*، ۷، ۴(۱۴۰۲)، ۳۲.

۶. «رایاجنگ» واژه مصوب فرهنگستان زبان و ادبیات فارسی برای عبارت «جنگ سایبری» است.

7. Karim A. A. Khan, "Technology Will Not Exceed Our Humanity", 2023. Accessed May 2, 2024. Available at: https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity/

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

9. Dan Saxon, "Violations of International Humanitarian Law by Non-State Actors during Cyberwarfare: Challenges for Investigations and Prosecutions", *Journal of Conflict and Security Law*, 21, 8(2016), 558.

10. Rome Statute of the International Criminal Court, 17 July 1998, 2187 U.N.T.S. 90, art. 8.

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

12. Ibidem; Rome Statute of the International Criminal Court, Op. Cit. art. 8.

13. Kai Ambos, "International Criminal Responsibility in Cyberspace", in: *Research Handbook on International Law and Cyberspace*, edited by Nicholas Tsagourias & Russell Buchan (Cheltenham: Edward Elgar, 2015), 118-121.

مسلحانه، ممکن است. شورای مشاوران سازمان ملل متحد[۱۴] نیز به اتفاق آرا بر این نظر است که عملیات سایبری در صورتی می‌توانند به‌عنوان یک جنایت جنگی مورد تعقیب واقع شوند که نخست، در چهارچوب یک مخاصمه مسلحانه بین‌المللی یا غیربین‌المللی واقع شوند و دوم، مشمول یکی از رفتارهای مذکور در بند ۲ ماده ۸ اساسنامه رم باشند.

مخاصمات مسلحانه نیز به دو گونه بین‌المللی[۱۵] و غیربین‌المللی[۱۶] تقسیم می‌شوند و شرایط وقوع آنها با یکدیگر متفاوت است. ماده ۸ اساسنامه رم نیز در مقام برشماری انواع جنایات جنگی، جنایات جنگی قابل ارتکاب در مخاصمات مسلحانه «غیربین‌المللی» را ذیل بندهای «ج» تا «و» از پاراگراف ۲ و متفاوت با جنایات قابل ارتکاب در بستر مخاصمات مسلحانه «بین‌المللی» برشمرده است. بر این اساس مخاصمه مسلحانه مورد نیاز برای وقوع جنایت جنگی با توجه به رفتار موضوع اتهام، ممکن است بین‌المللی یا غیربین‌المللی باشد و این موضوع به جنایت جنگی خاص مورد نظر بستگی دارد.[۱۷] بر این اساس شرایط وقوع مخاصمه مسلحانه غیربین‌المللی سایبری متفاوت با گونه دیگر مخاصمات مسلحانه است.

شایان ذکر است که در صورت وقوع رایاجنگ در بستر یک مخاصمه مسلحانه غیربین‌المللیِ ازپیش‌موجود و وجود سایر شرایط لازم، می‌توان به صورت قاطع تصریح نمود که رفتار ارتکاب‌یافته به‌عنوان یک جنایت جنگی دانسته شود.[۱۸] موضوع بررسی پژوهش مربوط به بررسی رایاجنگ‌هایی است که نه در جریانِ یک مخاصمه مسلحانه ازپیش‌موجود، بلکه به‌عنوان یک وجود مستقل ارتکاب می‌یابند؛

---

۱۴. گزارش شورای مشاوران سازمان ملل متحد درباره امکان‌سنجی اعمال اساسنامه رم دادگاه کیفری بین‌المللی در جنگ‌های سایبری است. گزارش مذکور بر اساس نشست‌های گروهی از پانزده وکیل بین‌المللی، سه کارشناس فنی، یک نماینده از کمیته بین‌المللی صلیب سرخ و یک نماینده از دفتر دادستانی دیوان کیفری بین‌المللی در ماه‌های اکتبر و دسامبر سال ۲۰۱۹ و ژانویه سال ۲۰۲۰ میلادی تنظیم شده است. نک:

Permanent Mission of Liechtenstein to the United Nations, "The Council of Advisers' Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare", August 2021. Accessed May 2, 2024. Available at: https://www.regierung.li/files/medienarchiv/The-Council-of-Advisers-Report-on-the-Application-of-the-Rome-Statute-of-the-International-Criminal-Court-to-Cyberwarfare.pdf

15. International Armed Conflict

16. Non-International Armed Conflict

۱۷. جنایات جنگی مذکور در بندهای «الف» و «ب» از پاراگراف ۲ ماده ۸ لزوماً در جریان یک مخاصمه مسلحانه بین‌المللی قابلیت وقوع دارند و جنایات جنگی مذکور در بندهای «ج» تا «و» از پاراگراف ۲ ماده ۸ ناگزیر از وقوع در جریان یک مخاصمه مسلحانه غیربین‌المللی هستند.

18. Ibid. 29.

به عبارت دیگر پژوهش حاضر به این سؤال اصلی می‌پردازد که آیا رایاجنگ‌ها به‌تنهایی می‌توانند موجدِ یک مخاصمه مسلحانه غیربین‌المللی بوده و در صلاحیت دیوان کیفری بین‌المللی، به‌عنوان یک جنایت جنگی واقع گردند یا خیر. بر این اساس در این پژوهش تلاش می‌شود تا به «چگونگی وقوع مخاصمه مسلحانه غیربین‌المللی، به‌عنوان عنصر زمینه‌ای جنایات جنگی سایبری از طریق رایاجنگ‌ها»، به‌عنوان مسئله اصلی پژوهش پاسخ داده شود. برای این منظور، ابتدا به تعریف مخاصمه مسلحانه بین‌المللی پرداخته شده و سپس ارکان تشکیل مخاصمه مسلحانه غیربین‌المللی سایبری از رهگذر رایاجنگ‌ها تشریح می‌گردد و در نهایت امکان وصول رایاجنگ‌های منفرد به مخاصمه مسلحانه غیربین‌المللی سایبری بررسی می‌شود.

با توجه به این‌که تاکنون هیچ رایاجنگی به‌طور رسمی و به‌صورت عمومی و فراگیر، به‌عنوان مخاصمه مسلحانه غیربین‌المللی شناخته نشده است و هیچ اجماع بین‌المللی درباره چگونگی تعریف و ارزیابی مخاصمه مسلحانه غیربین‌المللی سایبری وجود ندارد، بحث‌های این پژوهش نظری و مبتنی بر رویه فعلی حقوق بین‌الملل در خصوص رایاجنگ‌ها است. بر همین اساس هر تلاشی برای قاعده‌بخشی به رایاجنگ‌ها «در معرض عدم قطعیت، مجادله، عدم شفافیت و عدم تأییدپذیری»[۱۹] است.

شایان ذکر است همان‌گونه که در مقدمه اساسنامه رم بیان شده است، دیوان فقط برای تحقیق و تعقیب قانونی «شدیدترین جنایات مربوط به جامعه بین‌المللی به‌عنوان یک کل» تأسیس شده است. همچنین ماده ۵ بیان می‌کند که صلاحیت دیوان محدود به «شدیدترین جنایات مربوط به کل جامعه بین‌المللی» است. در ماده ۱۷ اساسنامه دیوان کیفری بین‌المللی نیز «شدت» گونه‌ای عنصر زمینه‌ای مشترک برای همه جنایات محسوب می‌شود. در تعریف جنایات که در مواد ۶، ۷، ۸ و ۸ مکرر اساسنامه رم ذکر شده است، ارجاعات متعددی به عنصر «شدت» وجود دارد؛ بنابراین موضوع این پژوهش نیز منحصر به رایاجنگ‌های غیربین‌المللی با شدت بسیار است که عموماً خارج از محدوده توان فنی دولت‌ها نیز جهت تعقیب و رسیدگی واقع می‌شوند. سایر گونه‌های رایاجنگ همچنان در حوزه صلاحیت‌های داخلی نظام‌های حقوقی ملی باقی می‌مانند.

۱- مخاصمه مسلحانه غیربین‌المللی

علی‌رغم موضوعیت وجود «مخاصمه مسلحانه» جهت رسیدگی دیوان کیفری بین‌المللی، اساسنامه رم

19. Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)", *Yale Journal of International Law*, 36, (2011), 443.

هیچ‌گونه تعریفی را برای مخاصمات مسلحانه ارائه نمی‌دهد.[۲۰] اسناد حقوق بشردوستانه بین‌المللی نیز تعریفی از «مخاصمه مسلحانه» ارائه نمی‌دهند. برای تعریف «مخاصمه مسلحانه» معمولاً به رویه قضایی دادگاه کیفری بین‌المللی برای یوگسلاوی سابق[۲۱] در قضیه تادیچ[۲۲] استناد می‌شود. بر اساس رأی دادگاه مذکور، مخاصمه مسلحانه غیربین‌المللی زمانی وجود دارد که «خشونت مسلحانه طولانی‌مدت بین مقامات دولتی و گروه‌های مسلح سازمان‌یافته یا بین چنین گروه‌هایی در داخل یک کشور وجود داشته باشد».[۲۳] در قضیه لوبانگا[۲۴] نیز بر این معیار تأکید شده است.[۲۵] بر همین اساس است که گفته شده است «دیوان کیفری بین‌المللی نیز در تعریف مخاصمه مسلحانه غیربین‌المللی، سه معیار را ملاک قرار داده است که عبارت‌اند از وقوع درگیری در قلمرو یک کشور، وقوع درگیری میان نیروهای دولتی و گروه‌های مسلح مخالف با آنها یا با گروه‌های مسلح مخالف و در نهایت، درگیری طولانی‌مدت»[۲۶]. رویه قضایی دادگاه کیفری بین‌المللی برای یوگسلاوی سابق دو معیار اساسی، یعنی «جنگ طولانی» و «گروه‌های مسلح سازمان‌یافته» را مورد بحث و تعریف قرار می‌دهد.[۲۷] دو معیار مذکور توسط کمیته بین‌المللی صلیب سرخ نیز مورد تأکید قرار گرفته است و به‌گونه‌ای منعکس‌کننده حقوق بین‌الملل عرفی است.

در معاهدات مربوط به حقوق بشردوستانه بین‌المللی، مفهوم مخاصمه مسلحانه غیربین‌المللی در ماده ۳ مشترک کنوانسیون ۱۹۴۹ ژنو و در ماده ۱ پروتکل الحاقی دوم به کنوانسیون ۱۹۴۹ ژنو به‌گونه‌ای متفاوت بیان شده است. توضیح آنکه ماده ۳ مشترک کنوانسیون ۱۹۴۹ ژنو، طرفین مخاصمه مسلحانه غیربین‌المللی را موظف می‌کند که با افرادی که در مخاصمه مشارکت فعالی ندارند و افرادی که در «حریم جنگ» قرار گرفته‌اند، رفتاری انسانی داشته باشند. ماده مذکور در تمام موقعیت‌های

20. Ambos, Op. Cit. 228-229; Prosecutor v. Bemba, ICC-01/05-01/08-424, Decision Pursuant to Article 61(7)(a) and (b) of the Rome Statute on the Charges of the Prosecutor Against Jean-Pierre Bemba Gombo, 15 June 2009, 217.

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

22. Tadic´

23. Prosecutor v. Tadić, Case No. IT-94-1-l, Decision on the Defense Motion for Interlocutory Appeal on Jurisdiction, Int'l. Crim. Trib. for the Former Yugoslavia, 2 Octoer 1995, 70.

24. Lubanga

25. The Prosecutor v. Thomas Lubanga Dyilo, ICC-01/04-01/06, Decision on the Confirmation of Charges, PTC I, 29 Jan. 2007, 533.

۲۶. محمدرضا ضیایی بیگدلی، *حقوق بین‌الملل بشردوستانه* (تهران: گنج دانش، ۱۴۰۰)، ۵۲-۵۳.

۲۷. برای یک بحث تفصیلی در خصوص عوامل مختلفی که می‌توان هنگام ارزیابی شدت مخاصمه و سطح سازمانی گروه‌های مسلح در نظر گرفت، نک:
Prosecutor v Ljube Bos˘koski and Johan Tarc˘ulovski (Judgment), IT-04-82-T, 10 July 2008, 176–292.

Mirmohammad Sadeghi, Hossein . "Cyber War Crimes through Non-International Armed Conflict Arising from Cyber Warfare". Jour. of Legal Res. 24, no. 64 (January 5, 2026), 7-40.

مربوط به «مخاصمات مسلحانه غیربین‌المللی» اعمال می‌شود.[۲۸] طبق تفسیر ارائه‌شده از سوی کمیته بین‌المللی صلیب سرخ در خصوص ماده مذکور، «مخاصمات مسلحانه غیربین‌المللی» عبارت است از «رویارویی‌های مسلحانه طولانی‌مدت بین نیروهای دولتی و نیروهای یک یا چند گروه مسلح یا بین این گروه‌ها که در قلمرو یک دولت [طرف کنوانسیون ژنو] پدید می‌آیند. رویارویی مسلحانه باید به حداقل خشونت برسد و طرفین درگیر باید حداقل سازمان‌دهی را از خود نشان دهند».[۲۹]

با این حال ماده ۱ پروتکل الحاقی دوم به کنوانسیون ۱۹۴۹ ژنو به طیف محدودتری از مخاصمات مسلحانه غیربین‌المللی می‌پردازد؛ یعنی فقط به مخاصمات مسلحانه بین نیروهای مسلح دولت و نیروهای مسلح مخالف یا سایر گروه‌های مسلح سازمان‌یافته می‌پردازد که تحت فرماندهیِ دارای مسئولیت، کنترل بر بخشی از قلمرو کشور را اعمال می‌کنند.[۳۰] در واقع ماده ۱ پروتکل الحاقی دوم مستلزم سطح بالاتر مخاصمه و همچنین سطح سازمان‌دهی بالاتری برای «گروه‌های مسلح» نسبت به ماده ۳ مشترک است.[۳۱] علاوه بر این ماده ۱ پروتکل الحاقی دوم، این احتمال را که صرفاً نبرد طولانی‌مدت میان دو یا چند گروه مسلح سازمان‌یافته، یک مخاصمه مسلحانه غیر بین‌المللی باشد، رد می‌کند.

بر خلاف پروتکل دوم الحاقی به کنوانسیون‌های ژنو که اِعمال کنترل گروه‌های مسلح سازمان‌یافته بر بخشی از قلمرو سرزمینی را ضروری می‌داند، اساسنامه رم چنین الزامی را برای تحقق یک مخاصمه مسلحانه غیربین‌المللی قائل نیست.[۳۲] بر این اساس دامنه گسترده‌تر ماده ۳ مشترک برای مخاصمات مسلحانه غیربین‌المللی، گسترده‌ترین کاربرد ممکن را برای حقوق بشردوستانه بین‌المللی که در جنگ‌های سایبری قابل اعمال است، تجویز و تسهیل می‌نماید.[۳۳]

---

28. International Committee of the Red Cross, “Commentary to Art 1 of Geneva Convention II”, 2017, 4447 and 4453.

29. Prosecutor v. Tadić, Op. Cit. 70.

30. Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 1125 U.N.T.S. 609. 8 June 1977, Accessed May 2, 2024. Available at: www.icrc.org/applic/ihl/ihl.nsf/Article.xsp?actionopenDocument&documentId93F022B3010AA404C12563CD0051E7384

31. International Committee of the Red Cross, “Commentary to Art 1 of Geneva Convention II”, 2017, 4463 and 4470.

32. Prosecutor v. Bemba, ICC-01/05-01/08-424, Op. Cit. 236.

۳۳. همچنین بند «هـ» از پاراگراف ۲ ماده ۸ اساسنامه رم نیز که جنایات جنگی خاصی را که در جریان یک مخاصمه مسلحانه غیربین‌المللی رخ می‌دهند، تعریف می‌کند، کاربرد آن را محدود به شرایطی نمی‌کند که شامل شرایط بیان‌شده در پروتکل الحاقی دوم باشد.

۲- ارکان مخاصمه مسلحانه غیربین‌المللی سایبری

تعاریف رویه‌ایِ فوق در حالی ارائه شده‌اند که در خصوص کاربست این تعاریف در چهارچوب ماهیتی فضای سایبر، فاقد اظهارنظر هستند. «به نظر می‌رسد که رویه دولتی بر محکومیت وسیع حملات سایبری است؛ اما اجماعی بر چگونگی واکنش به آن و اینکه یک حمله سایبری در چه سطحی به مخاصمه مسلحانه تبدیل می‌شود، حاصل نشده است».[۳۴] بر این اساس برای تعریف مخاصمه مسلحانه در فضای سایبر و امکان‌سنجی وقوع آن از طریق رایاجنگ، به اسناد دیگری همچون دستورالعمل تالین استناد می‌شود. بر اساس دستورالعمل مذکور، وجود یک مخاصمه مسلحانه غیربین‌المللی به دو معیار بستگی دارد: نخست، مخاصمات باید به «آستانه خشونت» معینی برسند و دوم، حداقل یکی از طرفین باید یک گروهِ «مسلحِ» «سازمان‌یافته» باشد.[۳۵] رأی قضیه تادیچ نیز به‌طور ضمنی، دو رکن را برای شناسایی یک مخاصمه به‌عنوان مخاصمه مسلحانه غیربین‌المللی تعیین می‌کند که همین ارکان در مخاصمات سایبری نیز قابل کاربست است: اول، شدت خشونت خصومت و دوم، مشارکت یک گروه مسلحانه سازمان‌یافته. بر این اساس به‌منظور شناسایی یک رایاجنگ به‌عنوان یک مخاصمه مسلحانه غیربین‌المللی، وجود سه شرط ضروری است[۳۶]: نخست، عملیات سایبری ناگزیر می‌بایست به «آستانه شدت خشونت» مشخص برسد. دوم، گروه غیردولتی درگیر در مخاصمه می‌بایست «مسلحانه» باشد و سوم، گروه مسلحانه مذکور می‌بایست واجد سطح حداقلی از «سازمان‌یافتگی» باشد.

۲-۱- آستانه شدت خشونتِ رایاجنگی

برای اینکه رایاجنگ‌ها به‌تنهایی یک مخاصمه مسلحانه غیربین‌المللی را ایجاد کنند، باید به‌عنوان «خشونت مسلحانه مستمر» تلقی شوند.[۳۷] با توجه به الزام به وجود آستانه شدت خشونت مذکور،

---

۳۴. مسعود رضایی و محمود جلالی، «جنگ سایبری و توسعه حقوق بین‌الملل منع توسل به زور»، *فصلنامه مطالعات حقوق عمومی*، ۴۸، ۳ (۱۳۹۷)، ۷۰۲.

۳۵. این دو شرط در احکام مختلف صادرشده از سوی دادگاه کیفری بین‌المللی برای یوگسلاوی سابق مورد اشاره قرار گرفته است. برای مثال، نک:

Prosecutor v. Tadić, Case No. IT-94- 1-A, Appeals Chamber Judgment, Int'l Crim. Trib. for the Former Yugoslavia, 15 July 1999, 194; Prosecutor v. Furundžija (Judgment), ICTY, Trial Chamber IT-95-17/1-T, 1998, p. 59; Prosecutor v Zejnil Delalic´, et al, IT-96-21-T, 16 November 1998, 183.

36. Prosecutor v. Milošević, Case No. IT-02-54-T, Decision on Motion for Judgment of Acquittal, Int'l Crim. Trib. for the Former Yugoslavia, 16 June 2004, 16-17; Michael N Schmitt and Liis Vihul, eds., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd edn (Cambridge: Cambridge University Press, 2017) 387.

۳۷. این وصف در احکام مختلف صادرشده از سوی دادگاه کیفری بین‌المللی برای یوگسلاوی سابق، مورد اشاره قرار گرفته

دستورالعمل تالین[۳۸] در بررسی رویه قضایی مربوطه به دیوان کیفری بین‌المللی برای یوگسلاوی سابق، به این نتیجه می‌رسد که رایاجنگ‌های مختل‌کننده به‌تنهایی به‌ندرت به سطح خشونت مورد نیاز برای ایجاد یک مخاصمه مسلحانه غیربین‌المللی دست می‌یابند.[۳۹] نتیجه مذکور پس از تفکیک رایاجنگ‌ها به دو نوع تخریبگر (ایجادگرِ آثار فیزیکی مشابه با حملات سنتی) و مختل‌کننده (فاقد آثار فیزیکی و دارای آثار غیرفیزیکی همچون تغییر یا تخریب داده‌ها)، حاصل آمده است. به‌طور خاص این دستورالعمل بیان می‌کند که رایاجنگ‌هایی که صرفاً در فضای سایبر رخ می‌دهند، مانند «نفوذ در شبکه، حذف یا تخریب داده‌ها (حتی در مقیاس بزرگ)، تهاجم به شبکه کامپیوتری و سرقت داده‌ها» برای ایجاد مخاصمه مسلحانه غیربین‌المللی کافی نیستند.[۴۰] از سوی دیگر دستورالعمل مذکور بر قابلیت تشکیل مخاصمه مسلحانه غیربین‌المللی از سوی رایاجنگ‌های تخریبگر تأکید می‌نماید؛ بنابراین به نظر می‌رسد که دستورالعمل مذکور بر آن است که معیار خشونتی که یک مخاصمه مسلحانه غیربین‌المللی به آن نیاز دارد، مستلزم نوعی از عملیات سایبری است که به‌گونه‌ای از پیامدهای فیزیکی منجر شود. بر این اساس از منظر دستورالعمل تالین، عملیات سایبری مختل‌کننده به‌تنهایی قادر به ایجاد سطح مورد نیاز از خسارت نیستند. شورای مشاوران سازمان ملل متحد نیز همسو با دستورالعمل تالین، بر آن نظر است که اقدامات مختل‌کننده مذکور در دستورالعمل تالین یا توقف کارکردها و خدمات اینترنتی، به‌خودی‌خود موجد یک مخاصمه مسلحانه غیربین‌المللی نیستند و در این خصوص به گزارش کمیته بین‌المللی صلیب سرخ استناد می‌کند.[۴۱] در خصوص شرط «طولانی شدن خشونت» و «استمرار» آن نیز شورای

است. برای مثال، نک:

Prosecutor v. Tadić, Case No. IT-94- 1-A, Appeals Chamber Judgment, Int'l Crim. Trib. for the Former Yugoslavia, 15 July 1999, 194; Prosecutor v. Furundžija (Judgment), ICTY, Trial Chamber IT-95-17/1-T, 1998, 59; Prosecutor v Zejnil Delalic´, et al, IT-96-21-T, 16 November 1998, 183.

۳۸. دستورالعمل تالین به بررسی حقوق حاکم بر جنگ‌های سایبری پرداخته و به‌طور کلی دربرگیرنده حقوق بر جنگ (حقوق بین‌الملل حاکم بر توسل به زور از سوی کشورها به‌عنوان ابزار سیاست ملی) و حقوق در جنگ (حقوق بین‌الملل تنظیم‌کننده رفتار در مخاصمات مسلحانه که به‌عنوان حقوق مخاصمات مسلحانه یا حقوق بشردوستانه بین‌المللی نیز شناخته می‌شود) است. این دستورالعمل که توسط متخصصین و محققان حقوق بین‌الملل طرح‌ریزی شد، در دو نسخه و در سال‌های ۲۰۱۳ و ۲۰۱۷ تدوین شد و به دنبال تسری هنجارهای حقوقی و قانونی موجود به جنگ‌های نوین است. دستورالعمل نخست به حقوق بین‌الملل مربوط به جنگ سایبری می‌پردازد. نسخه دوم دستورالعمل 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.

39. Schmitt and Vihul, Op. Cit. 388.

40. Ibidem.

41. International Committee of the Red Cross, "Commentary on the Third Geneva Convention", 2020,

مشاوران بر آن است که با رایاجنگ‌های تکرارشونده (نه لزوماً مستمر) که در یک بازه زمانی به‌نسبت مشخص واقع می‌شوند، این شرط می‌تواند محقق گردد.[۴۲]

هدف اصلی حقوق کیفری بین‌المللی «پایان دادن به بی‌کیفرمانی» برای «جدی‌ترین جنایات مربوط به جامعه بین‌المللی» است.[۴۳] اگر دیوان کیفری بین‌المللی به نتیجه‌گیری‌های دستورالعمل تالین تکیه کند، ممکن است منجر به مستثنا کردن عملیات سایبری مختل‌کننده از محدوده صلاحیتی دیوان کیفری بین‌المللی باشد. عملیات مختل‌کننده سایبری می‌توانند منجر به عواقبی ویرانگر شوند. با افزایش روزافزونِ وابستگی به فناوری، اختلال در سیستم‌های اطلاعاتی می‌تواند به اندازه توسل به زورِ منجر به آثار فیزیکی، موجب ورود خسارت گردد.[۴۴] به این ترتیب می‌بایست برای تأثیرات حملاتی که صرفاً در حوزه دیجیتال رخ می‌دهند و به هیچ‌گونه نمودهای تخریب فیزیکی منجر نمی‌شوند، قائل به موضوعیت شد.

کمیته بین‌المللی صلیب سرخ نیز دیدگاه مخالف با دستورالعمل تالین را اتخاذ می‌کند و به این نتیجه می‌رسد که «صرف غیرفعال کردن یک چیز مانند خاموش کردن شبکه برق بدون تخریب آن نیز باید به‌عنوان یک حمله شناخته شود».[۴۵] آن‌گونه که کمیته بین‌المللی صلیب سرخ اشاره کرده است: «اگر مفهوم حمله تنها به‌عنوان اشاره به عملیاتی باشد که منجر به مرگ، جراحت یا آسیب فیزیکی شود، یک عملیات سایبری که هدف آن ناکارآمد کردن یک شبکه غیرنظامی (مانند برق، بانک یا ارتباطات) است یا انتظار می‌رود که اتفاقاً باعث ایجاد چنین آثاری شود، ممکن است تحت پوشش مقررات ضروری حقوق بشردوستانه بین‌المللی که از جمعیت غیرنظامی و اشیای غیرنظامی محافظت می‌کند، قرار نگیرد. تطبیق چنین درک بیش‌ازحد محدودکننده‌ای از مفهوم حمله با موضوع و هدف قواعد حقوق بشردوستانه بین‌المللی در مورد ارتکاب مخاصمات دشوار خواهد بود».[۴۶] در این راستا شایسته است که دیوان کیفری بین‌المللی نیز در تفسیر کیفری خود از متناظر تفسیرهای اخیر پیروی کند.

در مواردی که الفاظ موجود در اساسنامه رم در خصوص یک ممنوعیت کیفری، پذیرای معنای

288. Accessed May 2, 2024. Available at: https://ihl-databases.icrc.org/ihl/full/GCIIIcommentary

42. Schmitt and Vihul, Op. Cit. 389.

۴۳. آن‌گونه که در مقدمه اساسنامه رم مورد اشاره قرار گرفته است.

44. I. Kilovaty, "Virtual Violence - Disruptive Cyberspace Operations as 'Attacks' Under International Humanitarian Law", *Michigan Telecommunications and Technology Law Review*, 23, 1(2016), 117.

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

46. International Committee of the Red Cross, "International Humanitarian Law and Cyber Operations during Armed Conflicts", 2019, 8.

تفسیری جدیدی در چهارچوب نص موجود باشند، دیوان مکلف است نسبت به اتخاذ رویکردی پویا در تفسیر حقوق بشردوستانه بین‌المللی در فضای سایبر اقدام نماید. رویکرد مذکور که عملیات سایبری مختل‌کننده را در محدوده صلاحیتی ماده ۸ قرار می‌دهد، می‌تواند منعکس‌کننده تحولات فناورانه در جنگ و گفتمان درحال‌توسعه در خصوص آسیب‌های دیجیتالی باشد که در جامعه بین‌الملل رخ می‌دهند. دیوان کیفری بین‌المللی موظف است «در صورت اقتضا، ... اصول تثبیت‌شده حقوق بین‌الملل در خصوص مخاصمات مسلحانه» را اعمال کند[۴۷] و قانون را به‌گونه‌ای تفسیر نماید که «منطبق با حقوق بشر شناخته‌شده بین‌المللی» باشد.[۴۸] دو رویکرد اخیر به‌طور طبیعی در طول زمان و در پاسخ به توسعه فناوری‌های جدید تکامل خواهد یافت. اثرات غیرفیزیکی حملات سایبری «می‌تواند اثرات فاجعه‌باری بر جامعه مدنی داشته باشد».

بنا بر مراتب فوق، دیوان کیفری بین‌المللی باید رویکرد «برابری با آثار حملات سنتی فیزیکی» را در تفسیر خود از ماده ۸ اساسنامه، رد کند و معیار «آثار واقعی» را که لزوماً فیزیکی نیستند، به‌عنوان معیار شدت خشونت رایاجنگ‌ها در نظر بگیرد. در این صورت امکان تعقیب جدی‌ترین تهدیدها علیه معیشت دیجیتالی غیرنظامیان و جلوگیری از مصونیت از کیفر در فضای سایبر فراهم می‌شود.

۲-۲- «مسلحانه بودن» گروه سازمان‌یافته درگیر در مخاصمه سایبری

توسعه فناوری‌های جدید، تشخیص این را که دارنده چه ابزاری «مسلح» است، دشوارتر می‌کند. تولید سلاح‌هایی که «اثرات انفجاری» ایجاد نمی‌کنند، مانند سلاح‌های شیمیایی، باکتریایی و بیولوژیکی، رویکرد سنتی را به چالش می‌کشد. مستنبط از دستورالعمل تالین، وصف «مسلح» در خصوص آن گروهی دارای مصداق می‌شود که دارای توانایی برای اقدام به عملیات سایبری باشد.[۴۹] بر این اساس هرچند تا امروز، اجماعی در خصوص اینکه سلاح سایبری چیست حاصل نشده است[۵۰]، اما به نظر می‌رسد که نمی‌توان عبارت «سلاح» را محدود در سلاح‌های سنتی و غیرمدرن دانست و حقوق

---

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

۴۸. پاراگراف سوم ماده ۲۱ اساسنامه رم

49. Schmitt and Vihul, Op. Cit. 389.

۵۰. حسین شریفی طرازکوهی و جعفر برمکی، «چالش‌های حقوقی قابلیت‌های فضای سایبری در پرتو ماده ۳۶ پروتکل یکم الحاقی ۱۹۷۷»، *مجله حقوقی بین‌المللی*، ۶۲، ۳۷(۱۳۹۹)، ۱۳۳.

بشردوستانه بین‌المللی را صرفاً در محدوده استفاده از سلاح‌های سنتی، جاری نمود. در این صورت توسل به سلاح‌های اتمی، زیستی و همه سلاح‌های مدرن مانند سلاح‌های سایبری، با چالش مواجه شده و مخاطره‌ای جدی برای حیات بشری محسوب خواهد شد. این موضوع که سلاح‌های هسته‌ای پس از تثبیت اکثر اصول حقوق بشردوستانه قابل اعمال در مخاصمات مسلحانه اختراع شده‌اند، به معنای عدم شمول قواعد حقوق بشردوستانه نسبت به سلاح‌های مدرن اخیر نیست. در غیر این صورت، نتیجه با همه اصول حقوق بشردوستانه جاری در حقوق مخاصمات مسلحانه که بر همه اَشکال جنگ و انواع سلاح‌های جنگی در گذشته، حال و آینده حاکم است، در تعارض خواهد بود.[۵۱] در درکی نوین از مفهوم «سلاح»، مؤلفه «مسلحانه» بودن، مستلزم وجود مخاصمه‌ای است که متضمن استفاده از «ابزارها و روش‌های جنگ» باشد.[۵۲] شایان ذکر است که ابزارها و روش‌های جنگ سایبری در قاعده شماره ۱۰۳ دستورالعمل تالین تعریف شده است: ابزارهای سایبری «سلاح‌های سایبری و سیستم‌های سایبری مرتبط با آنها» هستند، در حالی که روش‌های سایبری «تاکتیک‌ها، تکنیک‌ها و رویه‌هایی سایبری هستند که مخاصمه‌ها توسط آنها انجام می‌شوند».[۵۳]

در رابطه با ابزارهای جنگ سایبری، این تفسیر بر آن است که سلاح‌های سایبری آنهایی هستند که «برای آسیب رساندن یا مرگ افراد یا ایراد خسارت یا تخریب اشیا استفاده می‌شوند یا طراحی یا در نظر گرفته شده‌اند که مورد استفاده قرار گیرند و منجر به عواقب لازم برای ارزیابی یک عملیات سایبری به‌عنوان یک حمله شوند».[۵۴] تفسیر مذکور هیچ اشاره‌ای به سلاح‌های سایبری مختل‌کننده ندارد که برای اختلال در سیستم‌های ارتباطی یا خسارات صرفاً دیجیتالی طراحی شده‌اند؛ بنابراین واضح است که کارشناسان نگارنده دستورالعمل تالین معتقدند برای اینکه یک قابلیت سایبری به‌عنوان یک سلاح ارزیابی شود، باید برای این طراحی شده باشد یا قصد شده باشد که نوعی پیامد فیزیکی ایجاد کند.

در رابطه با روش‌های جنگ سایبری، «تاکتیک‌ها، تکنیک‌ها و رویه‌های سایبری که به موجب

51. ICJ Reports, Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion), 226, 1996, 86; Terry D. Gill, "International humanitarian law Applied to Cyber-Warfare: Precautions, Proportionality and the Notion of 'Attack' Under the Humanitarian Law of Armed Conflict", in: *Research Handbook on International Law and Cyberspace*, editd by Nicholas Tsagourias & Russell Buchan (Cheltenham: Edward Elgar, 2015), 366-367; International Committee of the Red Cross, "International Humanitarian Law and the challenges of contemporary armed conflicts", 2011, 36-37; International Committee of the Red Cross, "International humanitarian law and the challenges of contemporary armed conflicts", 2015, 40; International Committee of the Red Cross, "International Humanitarian Law and Cyber Operations during Armed Conflicts", 2019, 2.

52. Schmitt and Vihul, Op. Cit. 383.

53. Ibid. 452.

54. Schmitt and Vihul, Op. Cit. 452.

آن مخاصمه‌ها انجام می‌شوند»، بیشتر حاکی از آن دسته از عملیات است که به سطح «مخاصمه» نمی‌رسند. به‌عنوان مثال نوع خاصی از عملیات سایبری که برای مداخله در توانایی دشمن برای ارتباط طراحی شده است، ممکن است به‌عنوان یک مخاصمه واجد شرایط نباشد ... اما یک روش جنگی است.[۵۵] به این ترتیب «عملیات سایبری، هنگامی که برای آسیب رساندن یا مداخله در نیروهای دشمن، اهداف نظامی، جمعیت غیرنظامی یا اشیای غیرنظامی به کار می‌رود، به‌عنوان یک روش جنگی توصیف می‌شود».[۵۶]

به نظر می‌رسد که حتی در چهارچوب تفاسیر محدود دستورالعمل تالین نیز برای تحقق یک مخاصمه مسلحانه غیربین‌المللی از طریق رایاجنگ، لازم نیست یک روش جنگ سایبری منجر به آسیب فیزیکی شود؛ زیرا «هیچ الزامی برای استفاده از ابزار جنگی هنگام درگیر شدن در یک روش جنگی وجود ندارد».[۵۷] بر این اساس عملیات سایبری مختل‌کننده را نیز می‌توان روشی برای جنگ در نظر گرفت؛ بدون توجه به اینکه آیا سیستم‌های رایانه‌ای مورد استفاده برای اجرای عملیات می‌توانند به‌عنوان ابزارهای جنگ طبقه‌بندی شوند یا خیر.

۲-۳- «سازمان‌یافتگی» گروه مسلحانه درگیر در مخاصمه سایبری

شرط دیگر برای تحقق یک مخاصمه مسلحانه غیربین‌المللی، آن است که حداقل یک گروه مسلحانه سازمان‌یافته غیردولتی نیز در میان طرفین درگیری وجود داشته باشد.[۵۸] شعبه مقدماتی دیوان کیفری بین‌المللی مقرر نمود: «مداخله گروه‌های مسلح با درجاتی از سازمان‌یافتگی و توانایی برنامه‌ریزی و اجرای عملیات نظامی مستمر باعث می‌شود که مخاصمه به‌عنوان یک مخاصمه مسلحانه غیربین‌المللی توصیف شود».[۵۹] روشن است که استفاده از عبارت «درجاتی از سازمان‌یافتگی» در نظر مذکور، امکان تفسیرپذیری و ارائه تفسیرهای متعدد را فراهم می‌کند. تفسیرهای موجود از تعیین اجزای گروه مسلحانه سازمان‌یافته را می‌توان ذیل دو رویکرد قرار داد: رویکرد نخست با اتخاذ شیوه‌ای منعطف، آستانه‌ای حداقلی را برای احتساب یک گروه به‌عنوان گروه مسلحانه سازمان‌یافته پیشنهاد می‌کند و این در حالی است که رویکرد دوم با نگاهی سخت‌گیرانه، آستانه تحقق شرط مذکور را بسیار دشوار در نظر می‌گیرد که

55. Ibid. 453.
56. Jeffrey Biller and Michael N. Schmitt, “Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare”, *International Law Studies*, 95, (2019), 218.
57. Ibid. 218–219.
58. Schmitt and Vihul, Op. Cit. 389.
59. The Prosecutor v. Thomas Lubanga Dyilo, Op. Cit. 233.

طی دو گفتار به آنها پرداخته می‌شود.

۲-۳-۱-رویکرد منعطف

مبتنی بر این رویکرد که صاحب‌نظران کمتر به آن معتقد هستند، آستانه احراز شرط گروه مسلحانه سازمان‌یافته به‌نسبت پایین است؛ زیرا شواهدی مبنی بر «مقداری از سطح سازمان‌یافتگی» در خصوص گروه، کافی است.[۶۰] در زمینه جنگ‌های سنتی فیزیکی، چند شاخص وجود دارد که به‌تنهایی یا ترکیبی برای اثبات سازمان‌دهی یک «گروه مسلح» کافی هستند: ۱- شواهدی از ساختار فرماندهی؛ ۲- شواهدی مبنی بر اینکه گروه می‌تواند عملیات هماهنگ انجام دهد؛ ۳- شواهد مربوط به قابلیت‌های لجستیکی گروه؛ ۴- شواهدی که نشان دهد گروه دارای سطحی از نظم و انضباط و توانایی اجرای تعهدات اساسی حقوق بشردوستانه بین‌المللی است و ۵- شواهدی که توانایی گروه را برای صحبت با یک صدای واحد نشان دهد.[۶۱]

با این حال زمانی که «گروه مسلح» صرفاً از بازیگران سایبری تشکیل شده است، با توجه به ویژگی‌های خاص فضای نبرد سایبری، دسته‌بندی فوق از شواهد لازم برای احراز شرط سازمان‌یافتگی یک گروه که در خصوص جنگ‌های سنتی مطرح شده است، سودمند به نظر نمی‌رسند؛[۶۲] زیرا مفهوم «سازمان‌یافتگی» ممکن است کاملاً در فضای سایبر تغییر کند. با فرض وجود کثرت اعضا، هویت گروه به‌عنوان یک «گروه» ممکن است تنها شامل تبادلات دوره‌ای داده‌های الکترونیکی باشد.[۶۳] ممکن است

60. Prosecutor v Ljube Bos˘koski and Johan Tarc˘ulovski (Judgment), Op. Cit. paras 197-198.
61. Ibid. paras 199-203.

۶۲. در بند دوم از قاعده ۲۳ از دستورالعمل تالین ذکر شده است که در غیاب عملیات‌های سنتی فیزیکی، عملیات سایبری به‌تنهایی می‌تواند منجر به یک مخاصمه مسلحانه غیربین‌المللی شود. همچنین در بند هفتم از قاعده مذکور چنین آمده است که به‌دلیل پیش‌شرط وجود خشونت طولانی‌مدت برای ایجاد یک مخاصمه مسلحانه غیربین‌المللی، «عملیات سایبری در موارد نادر است که به‌تنهایی می‌تواند منجر به مخاصمه مسلحانه غیربین‌المللی شود». با این حال چنانچه برخی از نویسندگان نیز اشاره کرده‌اند، به‌نظر می‌رسد که این نتیجه‌گیری با احتمال آسیب و خسارتی که در ذات جنگ سایبری نهفته است، ناسازگار باشد؛ زیرا اثرات احتمالی عملیات‌های سایبری خصمانه به‌عنوان آثار سهمگینِ جنگ سایبری در حقوق بشردوستانه بین‌المللی دانسته می‌شوند. نک:
Dan Saxon, *International Humanitarian Law and the Changing Technology of War* (Leiden: Martinus Nijhoff, 2013), 213.

۶۳. همچنین بر خلاف اکثر عملیاتی که در جنگ سنتی فیزیکی واقع می‌شوند، یک فرد نامرئی می‌تواند چندین حمله نامرئی را از مکان‌های سایبری مختلف انجام دهد که همین موضوع وجود یک گروه را دشوار می‌کند.

اعضای گروه تحت ویژگی گمنامی فضای سایبر، هویت خود را از یکدیگر پنهان کنند.[۶۴] اگرچه گروه سایبری ممکن است فقط تعداد کمی از اعضا را در خود جای دهد، اما توانایی آنها در ایجاد پیامدهای مضر ممکن است قابل توجه باشد. بر عکس این گروه ممکن است اعضای زیادی داشته باشد که در سرتاسر جهان پراکنده شده‌اند و به‌صورت آزاد و مجازی از طریق اینترنت به هم متصل هستند.

به‌طور مشابه از بسیاری جهات، مفهوم «قابلیت‌های لجستیکی» در زمینه عملیات سایبری بسیار کمتر شایان توجه است. برای مثال، نیازهای «تدارکاتی» گروه ممکن است فقط شامل دسترسی گاه‌به‌گاه به رایانه و اینترنت باشد. سلاح‌های آن ممکن است در ذهن یک عضو «ذخیره» شود و تنها با لمس یک دکمه منتشر شود. علاوه بر این در جنگ‌های سنتی فیزیکی، توانایی کنترل قلمرو، یک شاخص قوی از سطح سازمان‌یافتگی یک گروه مسلحانه محسوب می‌شود.[۶۵] این در حالی است که هرچند شبکه‌های سایبری بی‌گمان «سرزمین» را نیز تشکیل می‌دهند[۶۶]، اما کنترل «سرزمین» الکترونیکی مستلزم نوعی کنترل متفاوت از اقتدار دولتی است که به‌طور سنتی بر مناطق جغرافیایی توسط بازیگران دولتی و غیردولتی اعمال می‌شود. کنترل بر «سرزمین سایبری» شامل تسلط الکترونیکی بر یک محیط مجازی است که در تئوری می‌تواند توسط گروه کوچکی از افراد یا حتی یک فرد به دست آید.

این تفاوت‌های مفهومی برای دادستانی که می‌خواهد وجود یک «گروه مسلحانه سازمان‌یافته» را اثبات کند، حل‌ناپذیر نیست. لازم است که «مقداری از سطح سازمان» اعمال‌شده توسط گروه نشان داده شود.[۶۷] با این حال از سوی دیگر با توجه به کنشگران غیردولتی که عملیات سایبری را انجام می‌دهند، مهم است که این آستانه احراز شرط گروه مسلحانه سازمان‌یافته خیلی پایین نباشد؛ زیرا با توجه به فراگیر بودن و ارزان بودن نسبی فناوری و زیرساخت‌های رایانه‌ای، ممکن است تعداد مخاصمات مسلحانه

---

۶۴. طبق بند ۱۳ از ماده ۲۳ دستورالعمل تالین، این واقعیت که اعضای گروه به‌صورت حضوری یکدیگر را ملاقات نمی‌کنند، مانع از تحقق سطح کافی برای سازمان‌یافتگی نمی‌شود.

۶۵. ماده نخست از پروتکل دوم الحاقی به کنوانسیون‌های ژنو در خصوص حمایت از قربانیان مخاصمات مسلحانه غیربین‌المللی توضیح می‌دهد که پروتکل شامل گروه‌های مسلح سازمان‌یافته است که از جمله کنترل قلمرو یک دولت عضو را در اختیار دارند.

۶۶. در تفسیریه بند هفدهم از قاعده شماره ۲۳ دستورالعمل تالین چنین آمده است که «کنترل بر فعالیت‌های سایبری به‌تنهایی برای تحقق شرط کنترل قلمرو در جهت تحقق الزام مذکور در پروتکل الحاقی دوم کافی نیست؛ هرچند کنترل بر فعالیت‌های سایبری ممکن است نشان‌دهنده درجه‌ای از کنترل سرزمینی باشد که یک گروه از آن برخوردار است».

۶۷. برای مثال طبق بند سیزدهم از قاعده ۲۳ دستورالعمل تالین، «یک گروه آنلاین مجزا با ساختار رهبری که فعالیت‌های آن را هماهنگ می‌کند» ممکن است به‌عنوان یک گروه مسلح سازمان‌یافته دانسته شود.

غیربین‌المللی به‌طور تصاعدی افزایش یابند و در نتیجه موجب گسترش حق کشورها برای توسل به زور مرگبار، مطابق با قواعد حقوق بشردوستانه بین‌المللی گردد.

بنابراین برای تعیین اینکه آیا یک کنشگر غیردولتی آستانه یک گروه مسلحانه «سازمان‌یافته» را برآورده می‌کند یا خیر، باید با دقت و مورد به مورد اقدام نمود. به‌علاوه ممکن است شرایطی پیش بیاید که اثرگذاری وجود یا فقدان شواهد سطح سازمان‌دهی کنشگران غیردولتی بر تعیین اینکه آیا قوانین حقوق بشردوستانه بین‌المللی اعمال شود یا خیر و وابسته کردن دو موضوع مذکور به یکدیگر، درست نباشد. برای مثال برخی از صاحب‌نظران از تحلیل «همه شرایط» برای تعیین وجود یا نبود یک مخاصمه مسلحانه حمایت می‌کنند، نه رویکرد قانونی حاکم بر معیارهای تادیچ.[۶۸] تحت آزمون مذکور، زمانی که هرج‌ومرج و سطوح خشونتِ جاری توسط یک یا چند طرف، هویت و سازمان‌دهی گروه‌های مسلح غیردولتی را مبهم می‌کند، عقل و منطق و هدف حقوق بشردوستانه بین‌المللی ایجاب می‌کند که طرفین از رژیم حقوقی حقوق بشردوستانه بین‌المللی تبعیت کنند.[۶۹] گزارش سال ۲۰۰۸ کمیته توسل به زور انجمن حقوق بین‌الملل نیز چنین پیشنهاد کرده است: «معیارهای سازمان‌دهی و شدت خشونت به‌وضوح به هم مرتبط هستند و باید هنگام ارزیابیِ اینکه آیا یک موقعیت خاص به یک مخاصمه مسلحانه تبدیل می‌شود یا خیر، با هم در نظر گرفته شوند. به نظر می‌رسد که هر چه سطح سازمان‌یافتگی بالاتر باشد، ممکن است به‌شدت کمتری نیاز باشد و بالعکس»؛[۷۰] البته این بدان معنا نیست که معیار «سطح سازمان‌یافتگی» بی‌اهمیت است، بلکه پیشنهاد مذکور گونه‌ای راهبردی عملی است تا اطمینان حاصل شود که غیرنظامیان و سایر افراد آسیب‌دیده از حمایت‌هایی برخوردار می‌شوند که طبق حقوق بشردوستانه بین‌المللی، مستحق آن هستند.

۲-۳-۲- رویکرد سخت‌گیرانه

مبتنی بر این رویکرد، سازمان‌یافتگی کافی مستلزم یک ساختار فرماندهی مستقر و توانایی پایش عملیات نظامی است.[۷۱] وصف «سازمان‌یافتگی» زمانی محقق می‌شود که یک گروه دارای «درجاتی

68. Laurie R. Blank & Geoffrey S. Corn, "Losing the Forest for the Trees: Syria, Law, and the Pragmatics of Conflict Recognition", *Vanderbilt Journal of Transnational Law*, 46, 3(2013), 693-746.

69. Blank & Corn, Op. Cit. 696–697, 701–702, 730–731, 740–742.

70. Mary Ellen O'Connell & Judith Gardam, *Initial Report on the Meaning of Armed Conflict in International Law* (London: International Law Association, 2008)

71. Prosecutor v. Limaj, Case No. IT-03-66-T, Trial Chamber Judgment, Int'l Crim. Trib. for the Former Yugoslavia, 30 Nov. 2005, 129.

از سازمان‌یافتگی و توانایی برنامه‌ریزی و اجرای عملیات نظامی پایدار» باشد.[۷۲] رویه قضایی دادگاه‌های موقت نیز نشان می‌دهد که سازمان‌یافتگی درون گروه، لازم نیست که به سطح یک واحد نظامی منضبط متعارف برسد.[۷۳] با این حال به نظر می‌رسد که شروط اساسی شامل «ظرفیت برنامه‌ریزی و اجرای عملیات نظامی، وجود یک ساختار فرماندهی مستقر و توانایی کار کردن گروه به‌عنوان یک واحد و صحبت با یک صدای واحد» باشد.[۷۴]

با تطبیق این قواعد بر پهنه رایاجنگ‌ها، دستورالعمل تالین چنین نتیجه می‌گیرد که «یک گروه آنلاین مجزا با ساختار رهبری که فعالیت‌های خود را به‌طور مثال با تخصیص اهداف سایبری مشخص در بین خود، به اشتراک گذاشتن ابزارهای حمله، انجام ارزیابی‌های آسیب‌پذیری سایبری و انجام ارزیابی خسارت سایبری، هماهنگ می‌کند»، می‌تواند یک گروه مسلحانه سازمان‌یافته دانسته شود، زیرا آنها به‌صورت همکارانه عمل می‌کنند.[۷۵] با این حال یک گروه غیررسمی که به‌جای مشارکت در تعقیب یک هدف مشترک، با یکدیگر عمل می‌کنند، با این تعریف مطابقت ندارد. کارشناسان دستورالعمل تالین بر آن نظر هستند که «یک گروه دیجیتال فرضی که به یک وب‌سایت مشترک که حاوی ابزارها و اهداف آسیب‌پذیر است، دسترسی پیدا می‌کند، اما حملات سایبری خود را به‌هیچ‌وجه سازمان‌دهی نمی‌کند»[۷۶]، به‌اندازه کافی برای شناسایی به‌عنوان یک گروه مسلحانه سازمان‌یافته برای تحقق یک مخاصمه مسلحانه غیربین‌المللی، شایستگی لازم را ندارد.

در همین راستا شورای مشاوران سازمان ملل متحد نیز بر آن نظر بوده است که عملیات سایبری و حملات رایانه‌ای ارتکاب‌یافته توسط اشخاص خصوصی یا گروه‌هایی کوچک از هکرها که فاقد ارتباط با یکدیگر هستند، نمی‌تواند شرط «سازمان‌یافتگی» را برآورده سازد.[۷۷] البته شایان ذکر است که بررسی کفایت شرط «سازمان‌یافتگی»، موضوعی است که می‌بایست بر اساس شرایط و اوضاع و احوال و

72. The Prosecutor v. Thomas Lubanga Dyilo, Op. Cit. 233; Prosecutor v. Limaj, Op. Cit. 129; Schmitt and Vihul, Op. Cit. 389.

مستند به ارجاع اخیر از دستورالعمل تالین، زمانی می‌توان یک گروه را دارای وصف «سازمان‌یافتگی» دانست که تحت یک ساختار فرماندهی مستقر قرار داشته باشد و بتواند اقدام به انجام عملیات نظامی پایدار نماید.

73. Prosecutor v. Limaj, Op. Cit. 132-134.

74. Prosecutor v. Limaj, Op. Cit. 129; Prosecutor v Bosˇkoski and Tarcˇulovski, Op. Cit. 290; Prosecutor v Akayesu, ICTR-96-4-T, 2 September 1998, 619–627; N. Bussolati, "The Rise of Non-State Actors in Cyberwarfare", in: *Cyberwar: Law and Ethics for Virtual Conflicts*, edited by D. Ohlin, K. Govern and C. Finkelstein (Oxford: Oxford University Press, 2015), 114-115.

75. Schmitt and Vihul, Op. Cit. 390.

76. Ibidem.

77. Ibid. 389.

به‌صورت مورد به مورد انجام شود.[۷۸] در همین راستا درباره گروه‌هایی که به‌طور کامل در فضای آنلاین سازمان یافته‌اند، شورای مشاوران بر این دیدگاه تأکید دارد که احراز شرط «سازمان‌یافتگی» در خصوص این گروه‌ها، اگر نگوییم ناممکن، دست‌کم با دشواری‌های جدی مواجه است.[۷۹] از نظر شورای مذکور، اینکه گروه به‌صورت فیزیکی دیداری نداشته است، مانع از برآوردنِ شرط سازمان‌یافتگی نیست،[۸۰] بلکه صرفِ وجودِ یک گروه کاملاً مجازی، تعیین عضویت در گروه مذکور را بدون تحقیقات گسترده قضایی تقریباً غیرممکن می‌سازد، زیرا ردیابی و کشف اینکه چه کسی پشت هر یک از رایانه‌ها قرار دارد، بسیار دشوار است.[۸۱] افزون بر این موضوع، وسعت دامنه جغرافیایی اعضای یک گروه مجازی موجب می‌شود که به سبب توانایی محدود چنین گروهی برای اجرای دستورها، اجرای مؤثرِ راهبردهای گروه از سوی اعضای آن و در نتیجه، تحقق سازمان‌یافتگی بسیار دور و دشوار باشد.[۸۲] بر این اساس شورای مشاوران در نهایت بر این نظر قرار گرفته است که تصور یک گروه مجازی که بتواند شرط سازمان‌یافتگی را برای یک مخاصمه مسلحانه غیربین‌المللی فراهم کند، بعید است و بر این اساس هم‌راستا با دستورالعمل تالین، چنین اظهارنظر نمود که به سبب لزوم تحقق شروط «شدت خشونت» و «سازمان‌یافتگی»، عملیات سایبریِ صرف تنها در شرایط بسیار استثنایی یارای تحقق یک مخاصمه مسلحانه غیربین‌المللی را خواهند داشت.[۸۳]

بنا بر مراتب فوق، اگر دیوان کیفری بین‌المللی نیز رویکرد مضیق دستورالعمل تالین و شورای مشاوران را اتخاذ نماید، یک گروه سایبری تنها زمانی قادر خواهد بود که شرط «گروه مسلحانه سازمان‌یافته» بودن را برای ایجاد یک مخاصمه مسلحانه غیربین‌المللی برآورده کند که ماهیت آن بسیار سازمان‌یافته باشد و ساختار رهبری‌ای را به کار گیرد که نقش خاصی را در سلسله‌مراتب به هر یک از اعضای گروه اختصاص دهد. این احتمال وجود دارد که اکثر گروه‌های سایبری که مسئول فعالیت‌های مخرب سایبری هستند،

78. Ibidem.

79. International Committee of the Red Cross, “Commentary on the Third Geneva Convention”, 2020, 471. Accessed May 2, 2024. https://ihl-databases.icrc.org/ihl/full/GCIIIcommentary

«با این حال، برای گروهی که فقط به‌صورت آنلاین سازمان‌دهی می‌کند، ممکن است تعیین این‌که آیا این گروه از آستانه سازمان‌دهی لازم برای تبدیل شدن به یک طرف مخاصمه مسلحانه غیربین‌المللی برخوردار است یا خیر، دشوار باشد؛ هرچند قطعاً غیرممکن نیست».

80. Schmitt and Vihul, Op. Cit. 390.

81. R. Geiss, “Cyber Warfare: Implications for Non-international Armed Conflicts”, *International Law Studies*, 89, 1(2013): 636.

82. Ibid. 637.

83. Ibid. 629; Schmitt and Vihul, Op. Cit. 385-386.

نتوانند این آستانه بالا برای هماهنگی و سازمان‌یافتگی را برآورده کنند؛ بنابراین به‌منظور تعقیب بر اساس ماده ۸ اساسنامه رم، به‌عنوان یک گروه مسلحانه سازمان‌یافته واجد شرایط نخواهند بود. این به دلیل ویژگی‌های منحصربه‌فرد فضای سایبر به‌عنوان میدان نبرد است که به جنگجویان سایبری این امکان را می‌دهد تا خود را به روش‌های متفاوتی از واحدهای نظامی سنتی ساختاربندی کنند.

۲-۳-۳- بازنگری در تعریف «سازمان‌یافتگی» گروه مسلحانه درگیر در مخاصمه سایبری

شرط «گروه مسلحانه سازمان‌یافته» برای یک مخاصمه مسلحانه غیربین‌المللی، تفاوت اساسی بین مفاهیم جنگ سنتی و جنگ سایبری را برجسته می‌کند. تا به امروز، اکثر رویه حقوق بشردوستانه بین‌المللی و نظرات پژوهشگران در مورد این موضوع بر این تصور استوار بوده است که جنگ فقط توسط دولت‌ها یا سایر نهادهای بسیار سازمان‌یافته انجام می‌شود و این در حالی است که ظهور فضای سایبر منجر به پخش قدرت شده است و این فرض را تضعیف می‌کند که فقط دولت‌ها یا گروه‌های بسیار سازمان‌یافته قادر به مشارکت در خشونت مؤثر در مقیاس گسترده هستند.[۸۴] «هرکس از یک هکر در سنین نوجوانی گرفته تا یک دولت بزرگ مدرن، می‌تواند در فضای سایبر، سبب حمله شده و خسارت وارد کند».[۸۵] تنها چیزی که برای شرکت در یک حمله سایبری لازم است، «یک رایانه ارزان‌قیمت، برخی نرم‌افزارهای قابل دسترسی آسان و یک اتصال ساده به اینترنت» است.[۸۶] الزامات سهل‌الوصول مذکور می‌تواند از طرق ذیل بر یکپارچگی ساختاری یک گروه سایبری تأثیر بگذارد و آن را بی‌نیاز از یکپارچگی سازد:

- نخست، عدم اجتماع جنگجویان در یک رایاجنگ[۸۷]: به این معنی است که اجرای هر نوع سلسله‌مراتب رسمی بسیار دشوار است. به‌جای یک ساختار هرمی مرسوم در جنگ‌های سنتی که از طریق آن بتوان زنجیره‌ای از فرمان‌ها را اجرا کرد، گروه‌های سایبری تمایل دارند تا خود را در ساختاری دولایه متشکل از مدیران و کاربران وابسته، سازمان‌دهی کنند.[۸۸] مدیران بر حمله نظارت

84. S. Haataja, "Technology, Violence and Law: Cyber Attacks and Uncertainty in International Law" (Presented in Proceedings of the 12 European Conference on Information Warfare and Security), edited by R. Kuusisto and E. Kurkinen, Academic Conferences and Publishing International, 2013, 319.

85. JS. Nye, The Future of Power (New York: PublicAffairs, 2011), 132.

86. RW Barnett, "A Different Kettle of Fish: Computer Network Attack", in: *Computer Network Attack and International Law*, edited by M. Schmitt and B. O'Donnell (Newport: Naval War College, 2002), 22.

87. J. Ophardt, "Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield", *Duke Law & Tech Review*, 9, 3(2010), 50.

88. Bussolati, Op. Cit. 116-117.

و مدیریت می‌کنند و ابزارها، اهداف و مسیرهای لازم را ارائه می‌دهند؛ اما تصمیم نهایی برای انجام اقدامات مشخص معمولاً توسط خود کاربران وابسته گرفته می‌شود.[۸۹] این ساختار دوسطحی و غیررسمی در حملات سایبری به گرجستان در سال ۲۰۰۸، قابل ملاحظه است؛ حملات در درجه اول توسط یک گروه اصلی از مدیران، از طریق وب‌سایتی به نام استاپ‌جورجیا[۹۰] سازمان‌دهی شدند که فهرستی از اهداف و ابزارهایی را ارائه می‌کردند که می‌توانستند برای انجام حملات دی‌داس[۹۱] استفاده شوند.[۹۲] با این حال اجرای واقعی این حملات متکی به همکاری افرادی بود[۹۳] که اغلب به میل خود شرکت کردند و به‌جای هر فرمان صریح، با تبلیغات ملی‌گرایانه مجبور به اقدام شدند.[۹۴]

– دوم، یک گروه دیجیتال به دلیل فقدان هرگونه توافق ایدئولوژیک، قادر به اقدام واقعی به‌عنوان یک کل واحد یا صحبت با یک صدا نیست؛ اشاره شده است که «اکثریت قریب به اتفاق حملات سایبری توسط افرادی انجام می‌شود که فقط وابستگی‌های ضعیفی به یک گروه دارند».[۹۵] به همین دلیل، اعضای گروه سایبری ممکن است از نظر درجه وابستگی به گروه یا انگیزه آنها برای مشارکت، کاملاً متفاوت باشند. انگیزه‌های شرکت‌کنندگان در حمله ممکن است به‌طور قابل توجهی متفاوت از «وجه مشترک به‌حرکت‌درآورنده گروه» باشد.[۹۶] این نشان می‌دهد که اگرچه گروه‌های سایبری ممکن است اهداف مشترک مبهمی مانند از کار انداختن زیرساخت‌های ملی در ذهن داشته باشند، اما معمولاً وحدت ایدئولوژیک کافی برای تسهیل درجه لازم سازمان‌یافتگی وجود ندارد.

– سوم، گروه‌های دیجیتال معمولاً فاقد مکانیسم‌های انضباطی داخلی هستند؛ زیرا انجام عملیات سایبری به «تماس‌های شخصی کمتر و در نتیجه روابط مبتنی بر اعتماد و اجرای نظم کمتری»، نسبت به جنگ‌های متعارف نیاز دارند.[۹۷] به همین دلیل اقدامات انضباطی در یک گروه دیجیتال،

89. Ibid. 117.
90. StopGeorgia
91. DDoS
92. Ibidem.
93. E. Zuckerman, “Misunderstanding Cyberwar in Georgia”, Reuters, August 16, 2008, Accessed May 2, 2024. https://www.reuters.com/article/us-georgia-comments/misunderstanding-cyber-war-in-georgia-idUSGOR66065320080816
94. Ibidem; E. Morozov, “An Army of Ones and Zeroes”, Slate, August 14, 2008. Accessed May 2, 2024. http://www.slate.com/articles/technology/technology/2008/08/an_army_of_ones_and_zeroes.html.
95. Ophardt, Op. Cit. 46.
96. Bussolati, Op. Cit. 116.
97. Council of Europe, “Organised Crime Situation Report 2004: Focus on the threat of economiccrime”,December2005.43.AccessedMay2,2024.Availableat:https://www.coe.int/t/dg1/legalcooperation/economiccrime/organisedcrime/Report2005E.pdf

اغلب محدود به ممنوعیت یک عضو از یک سکو (پلتفرم) یا تلاش برای وادار کردن به پذیرش دستورها از طریق «تأثیر کاریزماتیک و احترام» است.[۹۸] چنین اقداماتی، طبیعتاً برای وادار کردن به پذیرش حقوق بشردوستانه بین‌المللی کافی نیست. فقدان هرگونه مکانیسم انضباطی قابل اجرا، فقدان ساختار فرماندهی در گروه سایبری را فاش می‌کند و بنابراین احتمالاً از طبقه‌بندی آن به‌عنوان یک گروه مسلحانه سازمان‌یافته جلوگیری می‌کند. به این ترتیب اگر یک رویکرد سنتی برای تجزیه و تحلیل «سازمان‌یافتگی» یک گروه مسلحانه توسط دیوان کیفری بین‌المللی اتخاذ شود، بعید است که یک عملیات سایبری مختل‌کننده هماهنگ‌شده توسط یک گروه سایبری بتواند اقتضای رسمی از یک مخاصمه مسلحانه غیربین‌المللی را برآورده کند. در همین راستا تعیین عنصر زمینه‌ای جنایت جنگی بر اساس ماده ۸ اساسنامه رم، غیرممکن می‌شود و اعضای چنین گروه‌هایی که در طول دوره درگیری مرتکب جنایات سایبری می‌شوند، نمی‌توانند تحت اساسنامه رم مورد تعقیب قرار گیرند. این موضوع نگران‌کننده است؛ زیرا با وجود این واقعیت که گروه‌های سایبری از نظر ماهیت ساختار ضعیفی دارند، هنوز هم می‌توانند آسیب‌های قابل توجهی ایجاد کنند. در فضای سایبر، فقدان ساختار هرگز به معنای فقدان قدرت نیست. در مقابل اشاره شده است که گروه‌های سایبری با همان ساختار ضعیف، قادر به هماهنگی و انجام عملیات سایبری مؤثر هستند؛ پدیده‌ای که می‌توان آن را در حملات سال ۲۰۰۸ به گرجستان[۹۹] و در فعالیت‌های گروه هکری انانیموس[۱۰۰] مشاهده کرد.[۱۰۱] مطمئناً این امکان وجود دارد که چنین گروه‌هایی به‌عنوان بخشی از یک کمپین تهاجمی سایبری مرتکب جنایات شدید شوند؛ بنابراین متوقع است که دیوان کیفری بین‌المللی بتواند رویکرد تفسیری خود را در خصوص «گروه مسلحانه سازمان‌یافته»، بر اساس رویکردی پویا و روزآمد بنا نهد. در این صورامکان این را خواهد داشت که گروه‌های سایبری قدرتمند با ساختار ضعیف را نیز در تعریف خود از یک مخاصمه مسلحانه غیربین‌المللی مطابق با ماده ۸ شامل شود.

۳- مخاصمه مسلحانه غیربین‌المللی سایبری ناشی از رایاجنگ‌های منفرد

بر اساس پروتکل دوم الحاقی به کنوانسیون‌های ژنو و بند «د» از پاراگراف ۲ ماده ۸ اساسنامه رم، وضعیت‌هایی مانند ناآرامی‌ها و شورش‌های داخلی، اعمال خشونت‌آمیز صِرف و پراکنده یا سایر اعمال

98. Bussolati, Op. Cit. 117-118.
99. Bussolati, Op. Cit. 117.
100. Anonymous
101. Ibidem; K. Miller, "The Kampala Compromise and Cyberattacks – Can There Be an International Crime of Cyber-Aggression?", *Southern California Interdisciplinary Law Journal*, 23, (2014), 254.

مشابه[۱۰۲] نمی‌توانند به آستانه لازم برای وقوع مخاصمات مسلحانه غیربین‌المللی برسند.[۱۰۳] رأی دادگاه کیفری بین‌المللی برای یوگسلاوی سابق در برشماریِ ویژگی‌های عمومی مخاصمات[۱۰۴]، شاخص‌هایی مانند شدت حملات، تکرار حملات، تعداد قربانیان، مدت‌زمان درگیری، وسعت سرزمینیِ درگیری[۱۰۵]، اسلحه مورد استفاده طرفین درگیری[۱۰۶] و این را که آیا درگیری موجب جلب توجه و اقدام شورای امنیت ملل متحد می‌شود یا خیر[۱۰۷]، برشمرده است.[۱۰۸] در میان شاخص‌های مذکور به نظر می‌رسد که بیشتر از شدت خشونت، به مدت‌زمان آن اهمیت داده شده است.[۱۰۹]

با این حال بند ۲ ماده ۱ پروتکل الحاقی به کنوانسیون‌های ژنو ۱۲ اوت ۱۹۴۹، در خصوص حمایت از قربانیان مخاصمات مسلحانه غیربین‌المللی، در ۸ ژوئن ۱۹۷۷ بیان می‌کند که پروتکل در خصوص «اقدامات منفرد و پراکنده» اعمال نمی‌شود؛ بنابراین یک حمله سایبری منفرد بدون توجه به‌شدت آن نمی‌تواند مشمول پروتکل مذکور واقع گردد.[۱۱۰] بر این اساس نفوذ به شبکه، سرقت و دست‌کاری داده‌ها و حملات بندآوریِ خدمات توزیع‌شده[۱۱۱] که توسط یک کنشگر غیردولتی انجام می‌شود، تشکیل‌دهنده یک مخاصمه مسلحانه غیربین‌المللی محسوب نمی‌شود. با همین توضیح است که حمله واناکرای[۱۱۲] را که یک حادثه مجزا بود و فقط چند ساعت طول کشید و موجب هیچ مرگ‌ومیر شناخته‌شده یا حتی آسیب فیزیکی نیز نشد، «منفرد یا پراکنده» دانسته‌اند که به آستانه خشونت لازم برای آغاز یک مخاصمه مسلحانه غیربین‌المللی نمی‌رسد.[۱۱۳] البته اثرگذاری حملات منفرد در صورتی که موجب خدشه به

---

۱۰۲. بند «د» از پاراگراف ۲ ماده ۸ اساسنامه رم.

103. Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), Op. Cit. art. 1(2); Geiss, Op. Cit. 627-632.

104. Ibid. 633; Prosecutor v. Limaj, Op. Cit. 94-134.

105. Prosecutor v. Milošević, Op. Cit. 28-29; Geiss, Op. Cit. 632-633.

106. Prosecutor v. Mrkšić, Case No. IT-95-13/1-T, Trial Chamber Judgment, Int'l Crim. Trib. for the Former Yugoslavia, 27 Sep. 2007, 407; Prosecutor v. Limaj, Op. Cit. 90; Prosecutor v. Milošević, Op. Cit. pp. 31-32; Schmitt and Vihul, Op. Cit. 388.

107. Prosecutor v. Mrkšić, Op. Cit. 421; Prosecutor v. Ntaganda, ICC-01/04-02/06-2359, Judgment, 08 July 2019, 716; Prosecutor v. Ongwen, ICC-02/04-01/15-1762-Red, Trial Judgment, 4 Feb. 2021, 2684; Prosecutor v. Haradinaj, Case No. IT-04-84bis-T, Retrial Judgment, Int'l Crim. Trib. for the former Yugoslavia, 29 Nov. 2012, 394; Schmitt and Vihul, Op. Cit. 388.

108. Geiss, Op. Cit. 627-632.

109. Ibid. 633.

110. Ibid. 634; Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 1125 U.N.T.S. 609, 8 June 1977.

111. DDoS

112. WannaCry

113. John Griffith, "Distinguishing Cyberwarfare in the Law of Armed Conflict", March 4, 2022.

زیرساخت‌های سایبری شود، می‌تواند آستانه لازم برای وقوع یک مخاصمه مسلحانه غیربین‌المللی را نیز فراهم آورد.

نتیجه‌گیری

افزایشِ روزافزونِ استفاده از رایاجنگ‌ها از سوی گروه‌های غیردولتیِ غیرمنتسب به دولت‌ها و سوءاستفاده از قابلیت‌های هولناکِ آنها برای ورود آسیب به غیرنظامیان، تنظیم‌گریِ رایاجنگ‌ها و وضع محدودیت‌های حقوق جنگ بر آنها را ناگزیر ساخته است. با عنایت به اینکه جنایات جنگی ضرورتاً در چهارچوب یک مخاصمه مسلحانه، امکان وقوع دارند، برای تحقق جنایات جنگی سایبری، احراز تحقق عنصر زمینه‌ای جنایات جنگیِ سنتی یعنی وجود مخاصمه مسلحانه در رایاجنگ‌ها نیز ضرورت می‌یابد که حسب تفاوت در شرایط وقوع مخاصمات مسلحانه بین‌المللی و غیربین‌المللی، در این پژوهش صرفاً شرایط وقوع نوع اخیر مخاصمات از رهگذرِ رایاجنگ‌ها بررسی شد.

واکاوی امکان تحقق مخاصمات مسلحانه غیربین‌المللی از رهگذرِ رایاجنگ‌ها منوط به تحقق سه شرط است که به‌عنوان ارکان مخاصمه مسلحانه غیربین‌المللی از آنها یاد می‌شود. ارکان مذکور مشتمل بر «وجود آستانه خشونت»، «مسلح بودنِ گروه مرتکب» و «سازمان‌یافتگیِ گروه مرتکب» است که تحقق آنها در یک مخاصمه مسلحانه غیربین‌المللی سایبری نیز ضروری است. در خصوص شرط «وجود آستانه خشونت»، برای اینکه رایاجنگ‌ها به‌تنهایی یک مخاصمه مسلحانه غیربین‌المللی را ایجاد کنند، باید به‌عنوان «خشونت مسلحانه مستمر» تلقی شوند. دستورالعمل تالین، آستانه وقوع چنین خشونتی را منحصر در ایجاد آثار فیزیکی و وقوع خشونت ملموس در جهان فیزیکی می‌داند. به نظر می‌رسد که چنین استنباطی از مفهوم خشونت مستمر موجب خروج بسیاری از رایاجنگ‌های مختل‌کننده از دایره تنظیم‌گری مخاصمات مسلحانه می‌شود که بدون ایجاد آثار فیزیکی، دارای آثار گاه جدی‌تر بر زیرساخت‌های ملی هستند. در همین راستا اتخاذ رویکرد موسع نسبت به مفهوم خشونت که منحصر در آثار فیزیکی نبوده و جدیتِ آثار ایجادشده را مطمح نظر قرار دهد، پیشنهاد می‌شود.

در خصوص شرط «مسلح بودن گروه مرتکب»، به نظر می‌رسد که نمی‌توان عبارت «سلاح» را محدود در سلاح‌های سنتی و غیرمدرن دانست و حقوق بشردوستانه بین‌المللی در محدوده استفاده از سلاح‌های مدرن سایبری نیز جاری است. در خصوص شرط «سازمان‌یافتگی گروه مرتکب»، اگر یک رویکرد سنتی برای تجزیه و تحلیل «سازمان‌یافتگی» یک گروه مسلحانه اتخاذ شود، بعید است که

Accessed May 2, 2024. https://iccforum.com/forum/permalink/131/38976

یک عملیات سایبری مختل‌کننده هماهنگ‌شده توسط یک گروه سایبری بتواند اقتضای رسمی از یک مخاصمه مسلحانه غیربین‌المللی را برآورده کند. این در حالی است که در فضای سایبر، فقدان ساختار، هرگز به معنای فقدان قدرت نیست و گروه‌های سایبری با همان ساختار ضعیف، قادر به هماهنگی و انجام عملیات سایبری مؤثر هستند؛ بنابراین متوقع است که دیوان کیفری بین‌المللی بتواند رویکرد تفسیری خود را در خصوص «گروه مسلحانه سازمان‌یافته»، بر اساس رویکردی منعطف و روزآمد بنا نهد. در این صورت قادر خواهد بود تا گروه‌های سایبری قدرتمند با ساختار ضعیف را نیز در تعریف خود از یک مخاصمه مسلحانه غیربین‌المللی، مطابق با ماده ۸ شامل شود.

Mirmohammad Sadeghi, Hossein . “Cyber War Crimes through Non-International Armed Conflict Arising from Cyber Warfare”. Jour. of Legal Res. 24, no. 64 (January 5, 2026), 7-40.

فهرست منابع

الف) منابع فارسی

– رضایی، مسعود و محمود جلالی. «جنگ سایبری و توسعه حقوق بین‌الملل منع توسل به زور». *فصلنامه مطالعات حقوق عمومی*، ۴۸، ۳ (۱۳۹۷)، ۶۹۷-۷۱۳.
Doi:10.22059/jplsq.2018.217523.1365

– شریفی طرازکوهی، حسین و جعفر برمکی. «چالش‌های حقوقی قابلیت‌های فضای سایبری در پرتو ماده ۳۶ پروتکل یکم الحاقی ۱۹۷۷». *مجله حقوقی بین‌المللی*، ۶۲، ۳۷(۱۳۹۹)، ۱۱۹-۱۴۴.
Doi:10.22066/cilamag.2019.84640.1491

– ضیایی بیگدلی، محمدرضا. *حقوق بین‌الملل بشردوستانه*. چاپ پنجم. تهران: گنج دانش، ۱۴۰۰.

– ممتاز، جمشید و فریده شایگان. *حقوق بین‌الملل بشردوستانه در برابر چالش‌های مخاصمات مسلحانه معاصر*. تهران: مؤسسه مطالعات و پژوهشهای حقوقی شهر دانش، ۱۳۹۷.

– نمامیان، پیمان و نجات امیری. «امکان‌سنجی گسترش قلمرو صلاحیت دیوان کیفری بین‌المللی در قبال سلاح‌های ساخته‌شده با فناوری نانو». *حقوق فناوری‌های نوین*، ۷، ۴(۱۴۰۲)، ۲۱-۳۶.
doi.org/10.22133/MTLJ.2023.357735.1116

ب) منابع خارجی

- Ambos, Kai. “International Criminal Responsibility in Cyberspace”. In: *Research Handbook on International Law and Cyberspace*. edited by Nicholas Tsagourias & Russell Buchan, 118-143. Cheltenham: Edward Elgar, 2015.

- Barnett, RW. “A Different Kettle of Fish: Computer Network Attack”. in: *Computer Network Attack and International Law*. edited by M. Schmitt and B. O’Donnell. Newport: Naval War College, 2002.

- Biller, Jeffrey and Michael N. Schmitt. “Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare”. *International Law Studies*, 95, (2019), 179-225.

- Blank, Laurie R. & Geoffrey S. Corn. “Losing the Forest for the Trees: Syria, Law, and the Pragmatics of Conflict Recognition”. *Vanderbilt Journal of Transnational Law*, 46, 3(2013), 693-746.

- Bussolati, N. “The Rise of Non-State Actors in Cyberwarfare”. in: *Cyberwar: Law and Ethics for Virtual Conflicts*. edited by D. Ohlin, K. Govern and C. Finkelstein. Oxford: Oxford University Press, 2015.

- Council of Europe. “Organised Crime Situation Report 2004: Focus on the threat of economic crime”. December 2005. Accessed May 2, 2024. https://www.coe.int/t/dg1/legal cooperation/economiccrime/organisedcrime/Report2005E.pdf

- Dörmann, K. “The Applicability of the Additional Protocols to Computer Network Attacks: An ICRC Approach”. Presented in International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law. Stockholm, November 19, 2004. Accessed May 2, 2024. Available at: https://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf

- Geiss R. "Cyber Warfare: Implications for Non-international Armed Conflicts". *International Law Studies*, 89, 1(2013), 627-645.

- Gill, Terry D. "International humanitarian law Applied to Cyber-Warfare: Precautions, Proportionality and the Notion of 'Attack' Under the Humanitarian Law of Armed Conflict". In: *Research Handbook on International Law and Cyberspace*. editd by Nicholas Tsagourias & Russell Buchan. Cheltenham: Edward Elgar, 2015.

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

- Griffith, John. "Distinguishing Cyberwarfare in the Law of Armed Conflict". March 4, 2022. Accessed May 2, 2024. https://iccforum.com/forum/permalink/131/38976

- Haataja, S. "Technology, Violence and Law: Cyber Attacks and Uncertainty in International Law". Presented in Proceedings of the 12 European Conference on Information Warfare and Security. edited by R. Kuusisto and E. Kurkinen. Academic Conferences and Publishing International, 2013.

- Hillebrecht, C. "The deterrent effects of the international criminal court: Evidence from Libya". *International Interactions*, 42, 4(2016), 616-643.

- ICJ Reports. Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion), 226, 1996.

- International Committee of the Red Cross. "Commentary on the Third Geneva Convention". 2020, 288. Accessed May 2, 2024. https://ihl-databases.icrc.org/ihl/full/GCIIIcommentary

- International Committee of the Red Cross. "Commentary to Art 1 of Geneva Convention II", 2017.

- International Committee of the Red Cross. "International Humanitarian Law and Cyber Operations during Armed Conflicts", 2019.

- International Committee of the Red Cross. "International humanitarian law and the challenges of contemporary armed conflicts", 2015.

- International Committee of the Red Cross. "International Humanitarian Law and the challenges of contemporary armed conflicts", 2011.

- *Jo, H. & B. A. Simmons. "Can the International Criminal Court deter atrocity?". International Organization, 70, 3(2016), 443-475.*

- Khan, Karim A.A. "Technology Will Not Exceed Our Humanity", 2023. Accessed May 2, 2024. Available at: https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity/

- Kilovaty, I. "Virtual Violence – Disruptive Cyberspace Operations as 'Attacks' Under International Humanitarian Law". *Michigan Telecommunications and Technology Law Review*, 23, 1(2016), 113-147.

- McAllister, J. R. "Deterring wartime atrocities: Hard lessons from the Yugoslav tribunal".

International Security, 44, (2020), 84-128.

- Miller, K. “The Kampala Compromise and Cyberattacks - Can There Be an International Crime of Cyber-Aggression?”. *Southern California Interdisciplinary Law Journal*, 23, (2014), 217-260.

- Morozov, E. “An Army of Ones and Zeroes”. Slate. August 14, 2008. Accessed May 2, 2024. http://www.slate.com/articles/technology/technology/2008/08/an_army_of_ones_and_zeroes.html.

- Nye, JS. *The Future of Power*. New York: Public Affairs, 2011.

- O’Connell, Mary Ellen & Judith Gardam. *Initial Report on the Meaning of Armed Conflict in International Law*. London: International Law Association, 2008.

- Ophardt, J. “Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow’s Battlefield”. *Duke Law & Tech Review*, 9, 3(2010), 1-28.

- Permanent Mission of Liechtenstein to the United Nations. “The Council of Advisers’ Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare”. August 2021. Accessed May 2, 2024. Available at: https://www.regierung.li/files/medienarchiv/The-Council-of-Advisers-Report-on-the-Application-of-the-Rome-Statute-of-the-International-Criminal-Court-to-Cyberwarfare.pdf

- Preparatory Commission for the International Criminal Court. “Report of the Preparatory Commission for the International Criminal Court, Addendum, add. Part II Finalized draft text of the Elements of Crimes”, 2000, U.N. Doc. PCNIC/2000/1/Add.2.

- Prosecutor v Akayesu, ICTR-96-4-T, 2 September 1998.

- Prosecutor v Ljube Bosˇkoski and Johan Tarcˇulovski (Judgment), IT-04-82-T, 10 July 2008.

- Prosecutor v Zejnil Delalic´, et al, IT-96-21-T, 16 November 1998.

- Prosecutor v. Bemba, ICC-01/05-01/08-424, Decision Pursuant to Article 61(7)(a) and (b) of the Rome Statute on the Charges of the Prosecutor Against Jean-Pierre Bemba Gombo, 15 June 2009.

- Prosecutor v. Furundžija (Judgment), ICTY, Trial Chamber IT-95-17/1-T, 1998.

- Prosecutor v. Haradinaj, Case No. IT-04-84bis-T, Retrial Judgment, Int’l Crim. Trib. for the former Yugoslavia, 29 Nov. 2012.

- Prosecutor v. Limaj, Case No. IT-03-66-T, Trial Chamber Judgment, Int’l Crim. Trib. for the Former Yugoslavia, 30 Nov. 2005.

- Prosecutor v. Milošević, Case No. IT-02-54-T, Decision on Motion for Judgment of Acquittal, Int’l Crim. Trib. for the Former Yugoslavia, 16 June 2004.

- Prosecutor v. Mrkšić, Case No. IT-95-13/1-T, Trial Chamber Judgment, Int’l Crim. Trib. for the Former Yugoslavia, 27 Sep. 2007.

- Prosecutor v. Ntaganda, ICC-01/04-02/06-2359, Judgment, 08 July 2019.

- Prosecutor v. Ongwen, ICC-02/04-01/15-1762-Red, Trial Judgment, 4 Feb. 2021.

- Prosecutor v. Tadić, Case No. IT-94- 1-A, Appeals Chamber Judgment, Int'l Crim. Trib. for the Former Yugoslavia, 15 July 1999.

- Prosecutor v. Tadić, Case No. IT-94-1-l, Decision on the Defense Motion for Interlocutory Appeal on Jurisdiction, Int'l. Crim. Trib. for the Former Yugoslavia, 2 Octoer 1995.

- Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 1125 U.N.T.S. 609. 8 June 1977. Accessed May 2, 2024. Available at: www.icrc.org/applic/ihl/ihl.nsf/Article.xsp?actionopenDocument&documentId93F022B3010AA404C12563CD0051E7384

- Remy, Steven B. *War Crimes, Law, Politics, & Armed Conflict in the Modern World*. New York: Routledge, 2023.

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

- Saxon, Dan. "Violations of International Humanitarian Law by Non-State Actors during Cyberwarfare: Challenges for Investigations and Prosecutions". *Journal of Conflict and Security Law*, 21, 8(2016), 555-574. https://doi.org/10.1093/jcsl/krw018

- Saxon, Dan. *International Humanitarian Law and the Changing Technology of War*. Leiden: Martinus Nijhoff, 2013.

- Schmitt, Michael N. and Vihul Liis. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.

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

- Waxman, Matthew C. "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)". *Yale Journal of International Law*, 36, (2011), 421-459. http://dx.doi.org/10.2139/ssrn.1674565

- Zuckerman, E. "Misunderstanding Cyberwar in Georgia". Reuters. August 16, 2008. Accessed May 2, 2024. https://www.reuters.com/article/us-georgia-comments/misunderstanding-cyber-war-in-georgia%20idUSGOR66065320080816/

This Page Intentionally Left Blank