Modern Technologies Law, 2025, 6(12) https://www.mtlj.usc.ac.ir

Modern Technologies Law

University of Science and Culture

http://doi.org/10.22133/mtlj.2025.458309.1329

Cyberwar Crimes in the Criterion of Threshold of Severity Before the International Criminal Court

Hossein Mirmohammadsadeghi[1], **Mahdi Hosseini**[2*]

[1] Prof. of Criminal Law and Criminology, Faculty of Law, Shahid Beheshti University, Tehran, Iran.

[2] PhD in Criminal Law and Criminology, Faculty of Law, Shahid Beheshti University, Tehran, Iran.

Article Info

Original Article

Received:
18-05-2024
Accepted:
02-08-2024

Keywords:
Cyber War Crime
Severity Threshold
International Criminal Court
Legal Severity
Relative Severity

Abstract

Various countries have focused on cyber-attacks as part of the modern threat environment. For this reason, it is necessary to impose restrictions on the laws of war on cyber-attacks manifested in the form of cyber wars. The limitations related to the laws of war, the violation of which is considered to be a war crime and can be dealt with by the International Criminal Court, have been established for traditional physical wars and their application in the field of cyber wars is faced with ambiguities, and one of the mentioned ambiguities is the threshold of the severity of cyber war crimes for the proceedings before the ICC. Based on this, this research deals with the fundamental question of what level of severity threshold is necessary to deal with war crimes caused by cyber wars before the International Criminal Court. For this purpose, despite the ambiguity of the severity threshold, it is possible to clarify the level of jurisdiction of the court to deal with some behaviors committed in cyber wars as war crimes. In this regard, using the descriptive-analytical method and inferred from the decisions issued by the Court in previous cases and cases, two types of "threshold of the severity of proceedings before the International Criminal Court", i.e. "threshold of legal severity" and "threshold of relative severity", recognized and by analyzing how they are used in cyber war crimes, quantitative and qualitative indicators, such as the scale, nature, manner of committing crimes and their effects, are considered as effective factors in reaching the threshold of the severity in proceedings.

***Corresponding author**
e-mail: hosseini.mhdi@gmail.com

How to Cite:
Mirmohammadsadeghi, H., & Hosseini, M. (2025). Cyber War Crimes in the Criterion of Threshold of Severity before the International Criminal Court. *Modern Technologies Law*, *6*(12), 1-19.

Published by University of Science and Culture https://www.usc.ac.ir
Online ISSN: 2783-3836

1. Introduction

Although no cyber warfare situation had been analyzed by the International Criminal Prosecutor until 2023, in a significant written submission, the Prosecutor of the International Criminal Court made it clear that while no article of the Rome Statute specifically addresses cyberattacks, such conduct could potentially meet the elements of international crimes, such as war crimes, as previously defined, and the Office of the Prosecutor of the Court confirmed this as the current official position of the International Criminal Court. In light of this strategy, it is necessary to apply the general and specific elements of "war crimes" to "cyberwarfare." In this regard, one of the necessary contextual elements is the fulfillment of the "threshold of severity" for war crimes committed in the context of cyberwarfare before the International Criminal Court.

As stated in the preamble to the Rome Statute, the ICC was established only to investigate and prosecute the most serious crimes of concern to the international community as a whole, with other crimes remaining within the domestic jurisdiction of national legal systems. One mechanism devised to ensure this division of labour is the inclusion in the Rome Statute of a threshold of gravity that a situation must meet in order to be admissible to the Court. In Article 17 of the Statute of the International Criminal Court, "gravity" is considered a common element for all crimes, and there are numerous references to gravity in the definitions of crimes set out in Articles 6, 7, 8 and 8 bis of the Rome Statute. Article 5 also states that the jurisdiction of the Court is limited to the most serious crimes of concern to the international community as a whole.

On the other hand, with regard to war crimes, Article 8, paragraph 1, of the Rome Statute stipulates that the Court shall prosecute war crimes " in particular when committed as part of a plan or policy or as part of a large-scale commission of such crimes" and thus it appears that the Rome Statute has set a "special threshold" for the prosecution of war crimes before the International Criminal Court. The Office of the Prosecutor of the International Criminal Court has also acknowledged this article as a legal guideline indicating that the Court should focus on war crimes that meet these requirements. However, the Pre-Trial Chamber of the Court is of the opinion that the term "in particular" mentioned in Article 8, paragraph 1, implies that the existence of a plan, policy, or large-scale commission, contrary to what is stated, is not a condition for the jurisdiction of the Court and is not necessary to establish the existence of severity.

In any case, the criterion of "severity" is still considered an acceptable and necessary threshold for determining the Court's jurisdiction to investigate war crimes; moreover, an important question that this study attempts to answer is: assuming the possibility of war crimes occurring in the context of cyberwars, which has also been clarified by the Prosecutor of the International Criminal Court, what level of severity is required for the International Criminal Court to investigate war crimes committed in the context of cyberwars?

The criterion of "severity" is, first, the threshold for non-discretionary proceedings in the International Criminal Court and is referred to as "legal severity" and, second, based on Article 53, paragraph 1, subparagraph (c) and Article 53, paragraph 2, subparagraph (c) of the Rome Statute, it also serves another function within the framework of the Court's proceedings and guides the Prosecutor's decision in selecting and prioritizing situations and cases that are admissible for investigation and prosecution, which is referred to as "relative severity." The aforementioned severity is intended to focus the Court's resources on the most serious incidents.

2. Methodology

Because the present study has a documentary approach to the jurisprudence of international courts, international documents, and research studies, it uses a descriptive-analytical method and, by utilizing library resources, in the first part of this study, the "legal severity" necessary to address war crimes resulting from cyberwars before the International Criminal Court is addressed, and in the second part, the "relative severity" necessary to address war crimes resulting from cyberwars before the International Criminal Court is addressed.

3. Results and Discussion

The increasing use of cyberattacks in the world has led to the expansion of their effects and has created cyberwars, which, like all other types of war, all countries in the world are forced to regulate and impose restrictions on them. Among the aforementioned restrictions is the possibility of war crimes in cyberwars. Some actions committed in cyber operations can be considered as cyberwar crimes based on existing regulations if there are general background elements for the occurrence of war crimes in cyberwar. One of the necessary background elements is reaching the threshold of severity for jurisdiction before the International Criminal Court. As can be deduced from Articles 17 and 53 of the Rome Statute, there are two types of severity thresholds for proceedings before the International Criminal Court, namely the threshold of legal severity and the threshold of relative severity.

Regarding the threshold of legal severity, the jurisprudence of the International Criminal Court, such as the decision of the Prosecutor not to open an investigation into the Mavi Marmara incident, indicates that the assessment of legal severity should be based on quantitative and qualitative factors, such as the scale, nature, manner of commission of the crimes, as well as their effects. The "scale" factor, which can be considered to some extent in line with the opinion of the Tallinn Manual, emphasizes the scope of general physical effects and, from this perspective, is the subject of criticism in cyber warfare, which, despite the conventional perception of their severity, has not created a range of physical effects. The "nature" factor cannot be considered as an appropriate criterion for assessing the threshold of legal severity due to its lack of inclusion in liability arising from omissions in cyberwar crimes. The "manner of commission" factor cannot be mentioned as an effective factor in assessing the threshold of legal severity of cyberwarfare; Because the examples of the aforementioned factor cannot be considered to be very evident in cyberwarfare and only some acts committed in the cyberwarfare domain, such as causing serious disruption to data related to the general health of patients, can be assessed by this index as crimes reaching the threshold of legal severity. Finally, the factor of "impact" can be considered a widely used factor in assessing reaching the threshold of legal severity of the investigation; because its scope has also been extended to cyberwarfare causing non-physical disruptions. The sum of these factors does not have a fixed importance and must be assessed on a case-by-case basis and if the overall assessment indicates sufficient severity, it is not necessary that all conditions be met collectively.

Regarding the threshold of relative gravity, the Office of the Prosecutor's Policy Document on Case Selection and Prioritization states that the threshold of relative gravity is higher than the threshold of legal gravity and that it is assessed using the quantitative and qualitative factors assessed for the threshold of legal gravity. Cyberwarfare, like crimes committed by traditional means, can potentially meet all the factors identified by the Court to reach the threshold of relative gravity. For this purpose, the quantitative and qualitative factors of gravity, together with the mental element of the alleged perpetrator and the circumstances and circumstances of the crime, can be considered equally.

حقوق فناوری‌های نوین

http://doi.org/10.22133/mtlj.2025.458309.1329

جنایت‌های جنگی ناشی از رایاجنگ در سنجهٔ آستانهٔ شدت رسیدگی نزد دیوان کیفری بین‌المللی

حسین میرمحمدصادقی[۱]، مهدی حسینی[۲*]

[۱] استاد حقوق کیفری و جرم‌شناسی، دانشکدهٔ حقوق دانشگاه شهید بهشتی، تهران، ایران.

[۲] دانش‌آموختهٔ دکتری حقوق کیفری و جرم‌شناسی، دانشکدهٔ حقوق دانشگاه شهید بهشتی، تهران، ایران.

اطلاعات مقاله

مقالهٔ پژوهشی

تاریخ دریافت:
۱۴۰۳/۰۲/۲۹

تاریخ پذیرش:
۱۴۰۳/۰۵/۱۲

واژگان کلیدی:
جنایت جنگی سایبری
آستانهٔ شدت
دیوان کیفری بین‌المللی
شدت قانونی
شدت نسبی

چکیده

کشورهای مختلف بر حملات سایبری، به‌منزلهٔ بخشی از محیط تهدید مدرن، تمرکز کرده‌اند. بدین‌سبب، وضع محدودیت‌های حقوق جنگ بر حملات سایبری تجلی‌یافته در قامتِ رایاجنگ‌ها ضرورت یافته است. محدودیت‌های مربوط به حقوق جنگ، که نقض آن‌ها ایجادگرِ جنایات جنگی و قابل رسیدگی نزد دیوان کیفری بین‌المللی دانسته می‌شود، برای جنگ‌های فیزیکیِ سنتی وضع شده‌اند و کاربستشان در پهنهٔ رایاجنگ‌ها، با ابهام‌هایی مواجه است و یکی از ابهام‌های مذکور، آستانهٔ شدت جنایات جنگیِ سایبری برای رسیدگی نزد دیوان است. براین‌اساس، این پژوهش به این پرسش بنیادین می‌پردازد که برای رسیدگی به جنایات جنگی ناشی از رایاجنگ‌ها نزد دیوان کیفری بین‌المللی، وصول به چه سطحی از آستانهٔ شدت ضروری است. برای این منظور، تلاش می‌شود تا علی‌رغم ابهام آستانهٔ شدت رسیدگی، بتوان نسبت به تبیین سطح صلاحیت دیوان برای رسیدگی به برخی رفتارهای ارتکاب‌یافته در رایاجنگ‌ها، به‌عنوان جنایت جنگی، اقدام کرد. در این راستا، با استفاده از روش توصیفی-تحلیلی و مستنبط از تصمیمات صادرشده از سوی دیوان در پرونده‌ها و قضایای سابق، دو گونهٔ «آستانهٔ شدت رسیدگی نزد دیوان کیفری بین‌المللی»، یعنی «آستانهٔ شدت قانونی» و «آستانهٔ شدت نسبی»، بازشناسی شده و با تحلیل چگونگی کاربست آن‌ها در جنایات جنگیِ سایبری، شاخص‌های کمّی و کیفی، همچون مقیاس، ماهیت، شیوهٔ ارتکاب جنایات و همچنین تأثیرات آن‌ها، به‌عنوان عوامل مؤثر در وصول به آستانهٔ شدت رسیدگی دانسته می‌شوند.

***نویسندهٔ مسئول**

رایانامه: hosseini.mhdi@gmail.com

نحوهٔ استناددهی:

میرمحمدصادقی، حسین، و حسینی، مهدی (۱۴۰۴). جنایت‌های جنگی ناشی از رایاجنگ در سنجهٔ آستانهٔ شدت رسیدگی نزد دیوان کیفری بین‌المللی. حقوق فناوری‌های نوین، ۶(۱۲)، ۱-۱۹.

ناشر: دانشگاه علم و فرهنگ https://www.usc.ac.ir

شاپای الکترونیکی: ۳۸۳۶-۲۷۸۳

مقدمه

افزایش روزافزون حملات سایبری و کاربرد فزاینده آن‌ها به عنوان ابزاری نظامی در سطح جهانی، که منجر به ظهور رایاجنگ‌ها[1] شده، نگرانی دولت‌ها و سازمان‌های بین‌المللی را برای تنظیم این حملات تشدید کرده است. با توجه به دشواری ایجاد سازوکارهای بین‌المللی جدید برای مقابله با این حملات، تلاش‌ها بر سازوکارهای حقوقی موجود، به‌ویژه حقوق کیفری و ساختارهای موجود در دیوان کیفری بین‌المللی، مانند جنایت جنگی، متمرکز شده است.

هرچند تا سال ۲۰۲۳ دادستان کیفری بین‌المللی هیچ موقعیت مربوط به یک رایاجنگ را تجزیه‌وتحلیل نکرده بود، در سال ۲۰۲۳ در یک اظهارنظر مهم مکتوب، به‌صراحت اعلام کرد درحالی‌که هیچ ماده‌ای از اساسنامهٔ رم به‌صورت مشخص به حملات سایبری اختصاص ندارد، چنین رفتاری ممکن است به‌طور بالقوه عناصر بسیاری از جنایات بین‌المللی همچون جنایات جنگی را، که پیش‌تر تعریف شده است، برآورده کند (Khan, 2023) و دفتر دادستانی دیوان نیز آن را درحکم موضع رسمی و کنونی دیوان کیفری بین‌المللی تأیید کرد (Greenberg, 2023). دادستان دیوان این مهم را با برگزاری «همایش رسیدگی به جرایم سایبری در چهارچوب اساسنامهٔ رم» که با مشارکت فعال شرکت مایکروسافت برگزار می‌شد، در ابتدای سال ۲۰۲۴ آغاز کرد و در آن دادستان دوباره بر نکتهٔ خود درخصوص قابلیت تعقیب جرایم سایبری به‌عنوان جنایت جنگی در چهارچوب اساسنامهٔ رم سخن گفت[2]. در پرتو این راهبرد، تطبیق عناصر عمومی و اختصاصی «جنایات جنگی» بر «رایاجنگ‌ها» ضرورت می‌یابد. در این راستا یکی از عناصر زمینه‌ای لازم، تحقق «آستانهٔ شدت رسیدگی» برای جنایات جنگیِ ارتکاب‌یافته در چهارچوبِ رایاجنگ‌ها نزد دیوان کیفری بین‌المللی است.

آن‌گونه که در مقدمهٔ اساسنامهٔ رم ذکر شده است، دیوان کیفری بین‌المللی فقط برای تحقیق و تعقیب قانونی «شدیدترین جنایات مربوط به جامعهٔ بین‌المللی به‌عنوان یک کل» تأسیس شده است و سایر جنایات همچنان در حوزهٔ صلاحیت‌های داخلی نظام‌های حقوقی ملی باقی مانده است. یکی از سازوکارهایی که برای اطمینان از این تقسیم کار ابداع شده، گنجاندن آستانهٔ شدتِ رسیدگی در اساسنامهٔ رم است که یک وضعیت باید از آن عبور کند تا نزد دیوان پذیرفته شود. در مادهٔ ۱۷ اساسنامهٔ دیوان کیفری بین‌المللی، «شدت» گونه‌ای عنصر زمینه‌ای مشترک برای همهٔ جنایات محسوب می‌شود و در تعریف جنایات که در مواد ۶، ۷، ۸ و ۸ مکرر اساسنامهٔ رم ذکر شده است، ارجاعات متعددی به «شدت» وجود دارد. همچنین مادهٔ ۵ بیان می‌کند که صلاحیت دیوان محدود به «شدیدترین جنایات مربوط به کل جامعهٔ بین‌المللی» است.

درخصوص جنایات جنگی، بند ۱ مادهٔ ۸ اساسنامهٔ رم مقرر می‌دارد که دیوان جنایات جنگی را «به‌ویژه هنگامی که به‌عنوان بخشی از یک طرح یا سیاست یا به‌عنوان بخشی از ارتکاب بزرگ‌مقیاس چنین جنایاتی ارتکاب یافته باشد»، تحت تعقیب قرار می‌دهد و این‌گونه به‌نظر می‌رسد که اساسنامهٔ رم برای تعیین یک «آستانهٔ ویژه» برای رسیدگی به جنایات جنگی نزد دیوان کیفری بین‌المللی اقدام کرده است. درخصوص بند مذکور، دیوان کیفری بین‌المللی در احکام قبلی خود مانند قضیهٔ جمهوری دموکراتیک کنگو (ICC, 2006, p. 70)، تصریح کرده است که دو شرط مذکور در این بند، قابلیت جایگزین‌شدن به‌جای یکدیگر را دارند و به‌منظور تحقق «آستانهٔ ویژه» در جنایات جنگی، ضرورتی برای ارائهٔ شواهدی مبنی‌بر تحقق هر دوی آن‌ها وجود ندارد و عبارت «به‌ویژه»[3] مذکور در بند ۱ مادهٔ ۸، بیان‌کنندهٔ شرط «آستانه» برای تحقق جنایات جنگی تحت اساسنامهٔ رم است (Schabas, 2016, p. 226) و باید براساس آن، رسیدگی شود.

دفتر دادستانی دیوان کیفری بین‌المللی نیز این ماده را «به‌عنوان دستورالعمل قانونی که نشان می‌دهد دیوان باید بر جنایات جنگی که این الزامات را برآورده می‌کنند، تمرکز کند» تصدیق کرده است (ICC, 2014, para. 137). بااین‌حال، شعبهٔ مقدماتی دیوان بر آن نظر است که اصطلاح «به‌ویژه» مذکور در بند ۱ مادهٔ ۸ دلالت بر این دارد که وجود یک طرح، سیاست یا ارتکاب در مقیاس بزرگ، برخلاف آنچه گفته

---

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

2. https://www.icc-cpi.int/news/statement-icc-prosecutor-karim-aa-khan-kc-conference-addressing-cyber-enabled-crimes-through.

3. «In particular».

می‌شود، شرط صلاحیت دادگاه نیست و برای احراز وجود «شدت» لازم نیست (ICC, 2019, p. 65) و برای این‌که دیوان کیفری بین‌المللی جهت رسیدگی به یک جنایت جنگی واجد صلاحیت دانسته شود، ضرورتی برای وجود یک طرح یا سیاست یا ارتکابِ مقیاس‌بزرگ وجود ندارد و حتی یک عمل واحد نیز ممکن است به‌عنوان جنایت جنگی موضوع رسیدگی دیوان واقع شود.

درهرحال، معیار «شدت» همچنان یک آستانهٔ مقبول و لازم برای تعیین صلاحیت دیوان به‌منظور رسیدگی به جنایات جنگی دانسته می‌شود. وانگهی پرسشی مهم که در این پژوهش برای پاسخ به آن تلاش می‌شود، بدین شرح است که با فرضِ پذیرش امکان وقوع جنایات جنگی در چهارچوبِ رایاجنگ‌ها، که دادستان دیوان کیفری بین‌المللی نیز به آن تصریح کرده است، برای رسیدگی به جنایات جنگیِ ارتکاب‌یافته در بسترِ رایاجنگ‌ها نزد دیوان کیفری بین‌المللی، چه میزان از شدت لازم است؟

معیار «شدت» اول این‌که آستانهٔ رسیدگیِ غیراختیاری در دیوان کیفری بین‌المللی است و از آن با عنوان «شدت قانونی» یاد می‌شود و دوم این‌که مستند به بند «ج» از پاراگراف نخست مادهٔ ۵۳ و بند «ج» از پاراگراف دوم مادهٔ ۵۳ اساسنامهٔ رم، کارکردی دیگر را نیز در چهارچوب فرایند رسیدگی دیوان ایفا می‌کند (Stegmiller, 2009, p. 562; Sa´ Couto & Cleary, 2008, pp. 850-854) و موجب هدایت تصمیم دادستان در انتخاب و اولویت‌بندی موقعیت‌ها و پرونده‌های قابل قبول برای تحقیق و تعقیب قضایی می‌شود[1] که از آن با عنوان «شدت نسبی» نام برده می‌شود (Roscini, 2019, pp. 253-255). شدت مذکور برای تمرکز منابع دیوان بر شدیدترین وقایع موجود است (Stegmiller, 2009, p. 356). براین‌اساس، به‌سبب آن‌که پژوهش حاضر رویکردی اسنادی به رویهٔ قضایی دیوان‌های بین‌المللی، اسناد بین‌المللی و مطالعات پژوهشی دارد، از روش توصیفی - تحلیلی استفاده کرده و با بهره‌مندی از منابع کتابخانه‌ای، در بخش نخست از این پژوهش به «شدت قانونی» لازم برای رسیدگی به جنایات جنگی ناشی از رایاجنگ‌ها نزد دیوان کیفری بین‌المللی و در بخش دوم، به «شدت نسبی» لازم برای رسیدگی به جنایات جنگی ناشی از رایاجنگ‌ها نزد دیوان کیفری بین‌المللی پرداخته می‌شود.

۱. شدت قانونی

بند «د» از پاراگراف اول مادهٔ ۱۷ اساسنامهٔ رم مقرر می‌دارد که یک پرونده اگر «از اهمیت کافی برای توجیه اقدام بیشتری از سوی دیوان برخوردار نباشد»، پذیرفته نیست و نباید به آن رسیدگی شود. همچنین مادهٔ ۵۳ اساسنامهٔ مذکور مقرر می‌دارد که دادستان دیوان درصورتی‌که پرونده را طبق مادهٔ ۱۷ غیرقابل قبول بداند، نمی‌تواند تحقیقات را آغاز کرده یا پس از تحقیقات، اقدام به تعقیب کند. براساس این مقررات، این سؤال مطرح می‌شود که کدام حملات سایبری شدیدتر و کدام یک از آستانهٔ لازم برای رسیدگی در دیوان کیفری بین‌المللی شدت کمتری دارند؟ باوجود اهمیت عنصر «شدت» برای رسیدگی نزد دیوان کیفری بین‌المللی، قرینه‌ای در اساسنامهٔ دیوان کیفری بین‌المللی یا تاریخچهٔ تدوین آن وجود ندارد تا عواملی را روشن کند که باید برای ارزیابی شدت و اهمیت جنایات، طبق مواد ۱۷ و ۵۳ اساسنامه، در نظر گرفته شود.

برای تحلیل موضوع، گاهی به نظر سند مقررات تالین[2] استناد می‌شود؛ هرچند که دیدگاه‌هایی متفاوت درخصوص آستانهٔ شدت رسیدگی مورد نیاز از نظر سند مقررات تالین مطرح شده است (Efrony et al., 2018, p. 583). از منظر سند مقررات تالین، برای وصول به آستانهٔ شدت لازم برای وقوع توسل به زور و مخاصمهٔ مسلحانه، «ایجاد آثار فیزیکی» از اهمیت ویژه‌ای برخوردار است و در این راستا، تصریح می‌کند که «عملیات سایبری که به‌طور جدی تعدادی از افراد را مجروح کرده یا می‌کشد یا باعث آسیب قابل توجه یا تخریب اموال می‌شود، شرط مقیاس

---

۱. مستند به مادهٔ ۷۸ اساسنامهٔ رم، معیار «شدت» دارای کارکردی دیگر نیز هست و آن کمک به دیوان برای تعیین کیفر است.

۲. سند مقررات تالین به بررسی حقوق حاکم بر جنگ‌های سایبری پرداخته و به‌طورکلی، دربرگیرندهٔ حقوق بر جنگ (حقوق بین‌الملل حاکم بر توسل به زور از سوی کشورها به‌عنوان ابزار سیاست ملی) و حقوق در جنگ (حقوق بین‌الملل تنظیم‌کنندهٔ رفتار در مخاصمات مسلحانه که به‌عنوان حقوق مخاصمات مسلحانه یا حقوق بشردوستانهٔ بین‌المللی نیز شناخته می‌شود) است. این سند که توسط متخصصین و محققان حقوق بین‌الملل طرح‌ریزی شد، در دو نسخه و در سال‌های ۲۰۱۳ و ۲۰۱۷ تدوین شد و به‌دنبال تسری هنجارهای حقوقی و قانونی موجود به جنگ‌های نوین است. سند نخست به حقوق بین‌الملل مربوط به رایاجنگ می‌پردازد۲. نسخهٔ دوم سند در سال ۲۰۱۷ که توسط گروهی متنوع‌تر از کارشناسان تشکیل شد۲، به عملیات سایبری به‌طور گسترده‌تر، هم در حین و هم در خارج از مخاصمات مسلحانه می‌پردازد۲ و برای گنجاندن حقوق بین‌الملل حاکم بر فعالیت‌های سایبری در زمان صلح به‌روزرسانی شده است.

و اثرات را برآورده می‌کند» و یک «مخاصمهٔ مسلحانه» را تشکیل می‌دهد (Schmitt, 2017, p. 341). از منظر سند مقررات تالین، این شاخصی است برای ارزیابی آستانهٔ شدت وقوع مخاصمات مسلحانهٔ سایبری؛ وانگهی برخی از پژوهشگران (Trahan, 2022, pp. 138-139; Trahan, 2021, p. 1142) برای تعیین آستانهٔ شدت لازم برای رسیدگی به جنایات جنگی ناشی از رایاجنگ‌ها نزد دیوان کیفری بین‌المللی، همسو با اظهار نظر مذکور، برای «ایجاد آثار فیزیکی» اهمیت ویژه‌ای قائل شده و آن را معیار وصول به آستانهٔ شدت رسیدگی نزد دیوان نیز می‌دانند. این درحالی است که چنانچه شرح آن خواهد گذشت، شاخص‌های سند مقررات تالین برای ارزیابی وقوع «توسل به زور» سایبری ممکن است با رویکرد بالقوهٔ دیوان برای تعریف «آستانهٔ شدت رسیدگی» به عملیات‌های سایبری نزد دیوان، مطابقت نداشته و متفاوت باشد. در همین راستا، برخی دیگر از پژوهشگران (Keihanlou & Rezadoust, 2015, p. 201) نسبت به پذیرش معیارهای مقیاس و تأثیرات، مخالف جدی و برآن‌اند که «تسری نظر دیوان بین‌المللی دادگستری در قضیهٔ نیکاراگوئه به حملات سایبری به این معنا که این حملات نیز درصورت داشتن آثار زیاد، به استناد رأی مذکور، حملهٔ مسلحانه تلقی شوند، قابل انتقاد به‌نظر می‌رسد و توجه به اثر تا زمانی می‌تواند موجه باشد که با اصول اولیهٔ مورد پذیرش تداخل نکند؛ در غیر این صورت، توالیِ این غایت‌انگاری افراطی، به نتایجی غیرمعقول و ناخواسته منتهی می‌شود که به‌صورت قطعی، مدنظر طراحان نظامِ منشوری توسل به زور نبوده است.»

درصورتی‌که معیار ارائه‌شده از سوی سند مقررات تالین، برای ارزیابی شدت لازم برای رسیدگی نزد دیوان کیفری بین‌المللی نیز معیار تلقی شود، بسیاری از عملیات‌های سایبری که موجب آثار فیزیکی و خسارات جدی در دنیای بیرونی نمی‌شوند، صلاحیت رسیدگی در دیوان را به‌سبب عدم وصول به آستانهٔ شدت برای پذیرش رسیدگی دیوان نخواهند یافت و دراین‌صورت، باید به این سؤالات مهم پاسخ داد که آیا ایجاد آثار فیزیکی همیشه دارای شدت بیشتر و آسیب بزرگ‌تر تلقی می‌شود؟ آیا سقوط بازار سهام، که ممکن است به تعداد زیادی از بازنشستگان مسن آسیب برساند و کیفیت زندگی آن‌ها را به‌طور چشمگیری کاهش دهد، به‌صورت قطعی دارای شدت کمتر است؟ این‌که یک شرکت کشتی‌رانی جهانی و تعدادی از شرکت‌های دیگر در سراسر جهان به‌سبب نیاز به خاموش‌کردن تمام عملکردهای وابسته به فناوری اطلاعاتِ خود در یک حملهٔ بدافزاری، کارکردی از خود را از دست بدهند که باعث ضرر اقتصادی گسترده به بسیاری از کشورهای جهان می‌شود، آیا دارای شدت پایین‌تر به‌شمار می‌رود؟ اگر این اتفاق همراه با نابودی ترابایتیِ داده‌های سازمان‌ها و شرکت‌های دولتی، از رسانه‌ها گرفته تا شرکت‌های راه‌آهن و به‌دنبال آن قطعی برق گسترده رخ می‌داد، سطح شدت آن چگونه قابل تحلیل بود؟[1] آیا ارتکاب عملیات‌های سایبری علیه داده‌های رایانه‌ای که هیچ اثر فیزیکی ایجاد نمی‌کند و فقط به حذف کل داده‌ها منجر می‌شود، می‌تواند واجد گونه‌ای از «شدت رسیدگی» نزد دیوان باشد؟ اگر داده‌های مورد حملهٔ سایبری مشتمل بر داده‌های پزشکی در دوران شیوع ویروس کووید-۱۹ باشند و آثار بی‌هنجاری بر نظام سلامت یک کشور باقی بگذارند، چطور؟ درحالی‌که به‌نظر نمی‌رسد بتوان همهٔ مثال‌های مذکور در سؤالات اخیر را فاقد شدت لازم برای پذیرش رسیدگی دیوان تلقی کرد، می‌توان از ردِ ملاکِ «لزوم ایجاد آثار فیزیکی برای وجود آستانهٔ شدت پذیرش رسیدگی دیوان» سخن گفت. در همین راستاست که از سند مقررات تالین به‌سبب حذف حملات DDoS[2] و تخریب داده‌ها از شمول «توسل به زور»، به‌شدت انتقاد شده است.

بسیاری از اندیشمندان و حقوق‌دانان مؤثر در جوامع حقوقی بین‌المللی تا پیش از همه‌گیری ویروس کووید-۱۹، درخصوص شمول داده‌های رایانه‌ای، به‌عنوان موضوعات غیرملموس، تحت مقررات حمایت حقوق بشردوستانهٔ بین‌المللی از اموال به بحث‌های تفصیلی پرداخته بودند[3] و تا آن زمان هیچ‌گونه حمله به داده‌های رایانه‌ای را به‌سبب عدم ایجاد آثار فیزیکی، موجب ایجاد آستانهٔ شدت لازم برای رسیدگی در

---

۱ . مانند آنچه به‌سبب حملهٔ NotPetya، همراه با عملیات نظامی تهاجمی نیروهای روسیه علیه اوکراین، انجام شد (Greenberg, 2018).

۲. حملهٔ DDoS یا حملهٔ بندآوری خدمات گونه‌ای حملهٔ سایبری است که هدفش دسترسناپذیرکردنِ یک ماشین یا منبع شبکه با پرکردن حجم تقاضاها از سوی سیستم‌های هماهنگ است. حملات مذکور معمولاً به سیستم هدف نفوذ نمی‌کنند، بلکه آن را با پیام‌ها یا درخواست‌های بیش از حد درگیر می‌کنند تا آن را بیش از حد مشغول کنند و مجبور به خاموش‌شدن آن شوند. حملات DoS دائمی حملات جدی هستند که به سیستم آسیب می‌رسانند و باعث جایگزینی یا نصب مجدد سخت‌افزار می‌شوند. هنگامی که حملهٔ DoS توسط تعداد زیادی رایانهٔ سازماندهی‌شده در بات‌نت‌ها انجام می‌شود، به آن حملهٔ DDoS گفته می‌شود.

۳ . برای مطالعهٔ اختلاف‌نظرهای موجود درخصوص این‌که آیا داده‌ها باید تحت حمایت حقوق بشردوستانهٔ بین‌المللی و به‌عنوان «شیء» در نظر گرفته شوند یا خیر، قابل ملاحظه است:

دیوان کیفری بین‌المللی نمی‌دانستند، با شیوع ویروس مذکور و پی‌بردن به اهمیت داده‌های رایانه‌ایِ حوزهٔ سلامت عمومی و پزشکی، قائل به استثنا شده[۱] و حمله به داده‌های مذکور را برآورندهٔ آستانهٔ شدت لازم برای پذیرش رسیدگی دیوان تلقی می‌کنند (Trahan, 2021, 1145) و این درحالی است که بدیهی است صرفِ داده‌های پزشکی نیستند که واجد اهمیت تلقی می‌شوند و می‌توان از برخی گونه‌های دیگر از داده‌های رایانه‌ای، همچون داده‌های مربوط به زیرساخت‌های اطلاعاتی ملی، داده‌های مربوط به زیرساخت‌های حیاتی مانند نیروگاه‌های برق و شبکه‌های توزیع آب، داده‌های مربوط به زندگی خصوصی شهروندان و داده‌های هویتی غیرنظامیان، نام برد که ارتکاب حملهٔ سایبری علیه آن‌ها را، بدون ایجاد آثار فیزیکی و با ایجاد خسارات غیرفیزیکی شدید، می‌توان واجد وصف شدت لازم برای پذیرش رسیدگی دیوان تلقی کرد.

بنابراین، باوجود نظر سند مقررات تالین و برخی نظرات، که ذکر شد، به‌نظر می‌رسد که نباید به‌طور کلی سایر رایاجنگ‌ها را که در مقیاس بزرگ و به‌صورت تهاجمی واقع می‌شوند و تأثیرات فیزیکی ایجاد نمی‌کنند، غیرشدید دانست و از آستانهٔ شدت رسیدگی دیوان کیفری بین‌المللی استثنا کرد. همان‌گونه که شعبهٔ دیوان کیفری بین‌المللی در رسیدگی به اعتراض ثبت‌شده به رسیدگی شعبهٔ مقدماتی در پروندهٔ «الحسن» توضیح می‌دهد، شرط «شدت» دادگاه را موظف نمی‌کند که فقط جدی‌ترین پرونده‌ها را انتخاب کند، بلکه فقط آن را متعهد می‌کند که پرونده‌های با شدت ناچیز و بسیار اندک را تعقیب نکند (Le Procureur c. Al Hassan, 2020, p. 59).

درهرحال، دستیابی به تعریفی متقن از «آستانهٔ شدت قانونی در عملیات‌های سایبری» مستلزم بررسی رویهٔ دیوان کیفری بین‌المللی در موارد مشابه است. هرچند هر وضعیتی که در آن دادگاه کیفری بین‌المللی پرونده‌ای را در رابطه با عملیات سایبری با شدت کافی تلقی کرده و مورد تعقیب قرار دهد، به‌خودی‌خود مهم خواهد بود و روشن می‌کند که اساسنامهٔ رم شامل برخی از عملیات‌های سایبری می‌شود. تا به امروز پرونده‌های دیوان کیفری بین‌المللی بیشتر بر حوزه‌های «سنتی» غیرسایبری متمرکز بوده است. دادستان دیوان کیفری بین‌المللی در «همایش رسیدگی به جرایم سایبری در چهارچوب اساسنامهٔ رم»، که با مشارکت فعال شرکت مایکروسافت در سال ۲۰۲۴ برگزار شد، دوباره بر نکتهٔ خود درخصوص قابلیت تعقیب جرایم سایبری به‌عنوان جنایت جنگی در چهارچوب اساسنامهٔ رم سخن گفت[۲] و در این راستا، تبیین آستانهٔ شدت رسیدگی به جنایات جنگی ناشی از رایاجنگ برای دیوان، موضوعی مقتضی و درحال شکل‌گیری است.

پرونده‌های موضوع رسیدگی دیوان کیفری بین‌المللی تا به امروز بر جنایات نسبتاً بزرگ و برخی جنایات با شدت کمتر همچون کشتن دوازده صلح‌بان مورد بحث در پروندهٔ ابوگردا[۳] (Whiting, 2015) و تخریب نُه مقبره و یک مسجد مورد بحث در پروندهٔ المهدی[۴] (ICC,

---

J.T. Biller and M.N. Schmitt, 'Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare', International Law Studies, 95, 2019, p. ۱۸۱.

۱ . شایان ذکر است که قسمت دوم از بند دوم پاراگراف دوم مادهٔ ۸ اساسنامهٔ رم «حمله به اشیای غیرنظامی در جریان مخاصمات مسلحانهٔ بین‌المللی» را جنایت جنگی محسوب کرده و بند سوم از پاراگراف دوم مادهٔ مذکور نیز همین حکم را در جریان مخاصمات مسلحانهٔ غیربین‌المللی نیز جاری دانسته است. درخصوص مواردی که حمله به داده‌ها به‌عنوان حمله به اشیای مورد حمایت تلقی شده است، برای مثال، چنین گفته شده است که داده‌ها شامل «داده‌های پزشکی، داده‌های بیومتریک، داده‌های تأمین اجتماعی، سوابق مالیاتی، حساب‌های بانکی، پرونده‌های مشتریان شرکت‌ها یا فهرست‌ها و سوابق الکترونیکی» است. همچنین گفته شده است که «حذف، محدودکردن یا دستکاری در داده‌های ضروری غیرنظامی می‌تواند به‌سرعت خدمات دولتی و کسب‌وکارهای خصوصی را به بن‌بست کامل برساند» و این موجب شده است که کمیتهٔ بین‌المللی صلیب سرخ «داده‌های غیرنظامی» را به‌عنوان «اشیای غیرنظامی» برای اهداف حقوق بشردوستانهٔ بین‌المللی تلقی کند (Mac˘a´k, 2015, p. 55; Horowitz, 2020).

2. https://www.icc-cpi.int/news/statement-icc-prosecutor-karim-aa-khan-kc-conference-addressing-cyber-enabled-crimes-through.

۳. بحر ادریس ابوگردا (متولد سال ۱۹۶۳) از فرماندهان ضد دولت سودان بود که در دارفور می‌جنگید. در سال ۲۰۰۸، دادستان دیوان کیفری بین‌المللی شواهدی را ارائه کرد مبنی‌بر این‌که ابوگردا و دو فرماندهٔ دیگر مرتکب جنایات جنگی در رابطه با عملیاتی در سال ۲۰۰۷ شده‌اند که در آن، به اردوگاه صلح‌بانان اتحادیهٔ آفریقا در دارفور حمله کرده و دوازده نفر را کشته‌اند. در سال ۲۰۰۹، شعبهٔ مقدماتی اظهار داشت که دلایلی مبنی‌بر مسئولیت ابوگردا نسبت به سه مورد جنایت جنگی وجود دارد: قتل، غارت و هدایت عمدی حملات علیه کارکنان و تأسیسات به‌کارگرفته‌شده در مأموریت حافظ صلح. ابوگردا اولین فردی بود که بدون بازداشت و داوطلبانه در دادگاه کیفری بین‌المللی کیفری حاضر شد. محاکمهٔ وی با رد اتهامات و رد درخواست تجدیدنظر دادستان در سال ۲۰۱۰ به پایان رسید.

٤. در سال ۲۰۱۲، خشونت مسلحانه‌ای در مالی رخ داد و گروه‌های مسلح مختلفی همچون انصارالدین و القاعده، کنترل شهر تیمبوکتو را به دست گرفتند. احمد المهدی در آوریل سال ۲۰۱۲، برای حمایت از این جنبش‌های مسلحانه به مالی آمده و در ارتباط مستقیم با رهبران انصارالدین و القاعده بود. در سال ۲۰۱۲ المهدی و افراد تحت فرماندهی وی به ده مورد از مهم‌ترین و مشهورترین مکان‌ها در شهر تیمبوکتو حمله کرد و نابود شد. پیرو همین حملات، مالی وضعیت موجود در قلمرو سرزمینی خود را به دیوان کیفری بین‌المللی ارجاع داد و شعبهٔ اول مقدماتی دیوان در سال ۲۰۱۵، حکم جلب المهدی را به‌سبب جنایات جنگی با رفتار حملهٔ عمدی علیه بناها و آرامگاه‌های تاریخی و مذهبی صادر کرد. شعبهٔ بدوی در سال ۲۰۱٦، المهدی را به‌عنوان

2022) متمرکز بوده است که در هر دو مورد اخیر، کشتن افراد یا تخریب اشیای فیزیکی وجود داشت. وانگهی به‌صورت کلی، رویهٔ قضایی دیوان کیفری بین‌المللی نشان داده است که ارزیابی شدت یک رفتار باید براساس عوامل کمّی و کیفی مانند مقیاس، ماهیت، شیوهٔ ارتکاب جنایات و همچنین تأثیرات آن‌ها صورت گیرد (Roscini, 2022). این عوامل را دفتر دادستان و شعبهٔ مقدماتی برای ارزیابی شدت رسیدگی نزد دیوان در نظر گرفته می‌گیرد. برای مثال، دادستان در تصمیم خود مبنی‌بر عدم شروع تحقیقات درخصوص حادثهٔ کشتی ماوی مرمره به‌دلیل شدت ناکافی، از آن‌ها استفاده کرد (Buchan, 2015, pp. 497-498; ICC, 2014, para. 138). شعبهٔ مقدماتی چنین مقرر کرد که شاخص‌هایی که دادستان استفاده کرده مناسب است، اما نتیجه گرفت که آن‌ها به‌اشتباه استفاده شده‌اند (ICC, 2015, paras. 20-21). در ذیل به‌صورت تفصیلی به هریک از عوامل مذکور، که مستنبط از سوابق رسیدگی نزد دیوان کیفری بین‌المللی هستند، رسیدگی می‌شود. شایان ذکر است که این عوامل اهمیت ثابتی ندارند و باید به‌صورت موردی ارزیابی شوند (Schabas, 2008, p. 740). همچنین، درصورتی‌که ارزیابی کلی حاکی از شدت کافی باشد، ضروری نیست که همهٔ شرایط ذیل برآورده شوند (O'Brien, 2012, p. 543). به‌عبارت بهتر، برای وصول به آستانهٔ شدت لازم به‌منظور رسیدگی دیوان کیفری بین‌المللی، معیارهای ذیل به‌صورت تجمیعی ارائه نمی‌شود، بلکه حتی درصورتی‌که براساس یکی از عوامل زیر، نوعی شدت کلی محقق شده باشد، می‌توان از وصول به آستانهٔ شدت لازم سخن گفت.

۱-۱. مقیاس

حملات سایبری به‌طور بالقوه آسیب فیزیکی درخور توجهی به افراد و اشیا وارد می‌کند؛ برای مثال ممکن است یک نیروگاه برق را در میانهٔ زمستانی سخت خاموش کند و درنتیجه، به‌دلیل دمای پایین، موجب مرگ‌ومیر غیرنظامیان شود. یک حملهٔ سایبری ممکن است رایانه‌های کنترل آب سدها را از کار بیندازد و درنتیجه، باعث ایجاد سیل شود. همچنین می‌تواند سیستم کنترل ترافیک هوایی را مختل کند و موجب سرنگونی هواپیمای غیرنظامی در منطقه‌ای مسکونی شود. هریک از حملات مذکور، ممکن است در مقیاس کوچک یا وسیع انجام شود و ارزیابی از شدت هر حملهٔ سایبری در ارزیابی آن، به‌عنوان حمله‌ای دارای شدت لازم برای رسیدگی ازطریق دیوان، تأثیرگذار است. شاخص «مقیاس» را می‌توان شامل موارد زیر دانست: «تعداد قربانیان مستقیم و غیرمستقیم ناشی از حملهٔ سایبری، میزان خسارات ناشی از حملهٔ سایبری و به‌ویژه آسیب‌های جسمی یا روانی وارده به قربانیان و خانواده‌های آن‌ها یا گستردگی جغرافیایی یا زمانی آن‌ها (شدت بالای جنایات در مدتی کوتاه یا شدت کم جنایات در زمانی طولانی)» (The Office of the Prosecutor, 2013, para. 62). براین‌اساس، برای مثال دفتر دادستانی دیوان تصمیم گرفت تحقیقات را درخصوص پروندهٔ کشتی ماوی مرمره آغاز نکند؛ زیرا تعداد قربانیان در مقایسه با سایر موارد بررسی‌شده به‌دست دادستان «نسبتاً محدود» بود (ICC, 2014, para. 138). شعبهٔ مقدماتی دیوان نیز تعداد قربانیان را مهم دانسته و برای مثال، در تصمیماتش برای مجوزدادن به انجام تحقیقات درخصوص موقعیت‌های کنیا و گرجستان، به آن ترتیب اثر داده است (ICC, Situation in Kenya, 2010, paras. 190-191; ICC, 2016, para. 5). همچنین در قضیهٔ کومور[1] که براثر تیراندازی نیروهای رژیم اسرائیل به کشتی حامل کمک‌های بشردوستانهٔ عازم نوار غزه، ده نفر کشته شده بودند، دفتر دادستانی دیوان چنین موضع گرفت که تلفات موجود به آستانهٔ شدت لازم برای رسیدگی در دیوان کیفری بین‌المللی نرسیده است (The Office of the Prosecutor, 2017, para. 336). این درحالی است که دفتر دادستانی دیوان در پروندهٔ ابوگردا دربارهٔ کشتن دوازده حافظ صلح «به‌دلیل اهمیت هدف و تأثیر در عملیات حفظ صلح» اقدام کرد[2]؛ بنابراین الزاماً تعداد تلفات لازم برای رسیدن به آستانهٔ شدت، معیار تعیین‌کننده نیست؛ زیرا به‌وضوح عوامل دیگری برای تجزیه‌وتحلیل وجود دارد که در ادامه به آن‌ها پرداخته خواهد شد. برای مثال، زمانی که دادستان دیوان کیفری بین‌المللی تأثیر در عملیات‌های حافظ صلح را بخشی از تجزیه‌وتحلیل شدت

شریک در ارتکاب جنایت جنگی با رفتار حمله به اهداف مورد حمایت، یعنی تعداد نُه مقبره و یک مسجد، در شهر تیمبوکتو به نه سال زندان محکوم کرد. در سال ۲۰۲۱، دادگاه تجدیدنظر مجازات قطعی وی را به‌مدت دو سال کاهش داد.

1. Comoros situation

۲ . همچنین تحقیقات مقدماتی درخصوص جنایات انگلستان در عراق، به دلیل کافی‌نبودن شدت آغاز نشد (Whiting, 2015).

در پروندهٔ ابوگردا در نظر گرفت، بر سنجش سایر عوامل صحه گذاشت. همچنین ایجاد مقدار متوسط از آسیب فیزیکی یا تخریب اشیا، ممکن است آستانهٔ شدت را از منظر دفتر دادستانی دیوان برآورده نکند، اگرچه ممکن است در صورت هدف قرارگرفتن یک شیء خاص محافظت‌شده، استثنا ایجاد شود[1] و از این منظر، شاخص‌های سند مقررات تالین برای ارزیابی وقوع «توسل به زور» سایبری، ممکن است با رویکرد بالقوهٔ دیوان برای تعریف آستانهٔ شدت رسیدگی به عملیات‌های سایبری نزد دیوان، مطابقت نداشته و متفاوت باشد.

همچنین عملیات سایبری ممکن است گستردگی جغرافیایی شایان توجهی داشته باشد، اما همچنان به خسارات فیزیکی محدود منجر شود. برای مثال، ویروس مخرب استاکس‌نت به رایانه‌های چندین کشور ازجمله ایران، اندونزی، هند، آذربایجان، ایالات متحده و پاکستان سرایت کرد، اما فقط به تأسیسات غنی‌سازی اورانیوم ایران در نطنز آسیب فیزیکی وارد کرد و درعین‌حال آسیب کمی به رایانه‌هایی وارد کرد که ویژگی‌های خاصی نداشتند. همچنین حملات DDoS اغلب شامل میلیون‌ها روبوشبکه[2] در چندین کشور می‌شود که ازطریق یک یا چند ربات مهاجم[3] کنترل می‌شوند، اما این حملات فقط با خاموش‌کردن سرورها و سیستم‌هایی که بسیار به آن‌ها رجوع می‌شود به آسیب موقتِ برگشت‌پذیر به آن‌ها منجر می‌شود و این آسیب ممکن است به قطع موقت خدمات منجر شود، اما آسیب فیزیکی به افراد یا اموال را موجب نمی‌شود؛ بنابراین حتی با فرض این‌که این جرایم در صلاحیت عمومی دیوان کیفری بین‌المللی قرار بگیرند، عملیاتی مانند حملات DDoS علیه استونی در سال ۲۰۰۷ که زیرساخت‌های بانکی و ارتباطی در منطقهٔ بالتیک را مختل کرد، باوجود گستردگی دامنهٔ جغرافیایی وقوع آن، بعید است که از نظر شاخص «مقیاس» به‌اندازهٔ کافی شدید باشند؛ مگر این‌که به تلفات فیزیکی جانی یا تخریب اموال منجر شوند (Roscini, 2022) یا براساس نظریهٔ تجمیع رویدادها، بتوان به شناسایی صلاحیت برای رسیدگی به آن‌ها اقدام کرد. عملیات‌های سایبری تأثیرات متعددی در دنیای فیزیکی ایجاد می‌کند (Owens et al., 2009, p. 80; Palojarvi, 2009, p. 32; Boothby, 2013, p. 390). تأثیرات اولیه بر سیستم یا شبکهٔ رایانه‌ای است که به آن حمله شده؛ یعنی حذف، خراب‌شدن یا تغییرداده یا نرم‌افزار یا اختلال در سیستم ازطریق حملهٔ DDoS یا سایر حملات سایبری. تأثیرات ثانویه روی زیرساختی است که سیستم یا شبکه‌ای که به آن حمله شده روی آن اداره می‌شود؛ یعنی تخریب یا ناتوانی جزئی یا کلی آن. تأثیرات ثالث بر صاحبان سیستم‌هایی هستند که عملیات سایبری را مرحله‌بندی می‌کنند یا از خدمات سیستم‌های رایانه‌ای بهره‌مند می‌شوند؛ مانند افرادی که دیگر از برق تولیدشده توسط یک نیروگاه غیرفعال‌شده توسط یک عملیات سایبری بهره‌مند نمی‌شوند. تأثیرات ثالث ممکن است دائمی، موقت یا زودگذر باشند (Fanelli & Conti, 2012, pp. 323-324). بنابراین، آسیب فیزیکی به اموال یا ازدست‌دادن جان و جراحت افراد، تأثیرات سطح دوم یا سوم یک عملیات سایبری است؛ نه تأثیرات سطح اول آن.

وانگهی، فارغ از سطح تأثیرات ایجادشده در اثر یک عملیات سایبری، موضوعیت قائل‌شدن برای آثار فیزیکی همان نگاه مبتنی‌بر آثار است که تلقی خود از شاخص «مقیاس» را نیز در لزوم ایجاد آثار فیزیکی، محدود می‌کند و این درحالی است که چنانچه پیش‌تر نیز توضیح داده شده است، به نظر می‌رسد نمی‌توان تجلی هریک از معیارهای مذکور را الزاماً در آثار فیزیکی محدود کرد و بسیاری از خسارات غیرفیزیکی ممکن است حتی در داوری عرفی نیز زیان بیشتری به‌نسبت آثار فیزیکی تلقی شوند. براین‌اساس، به نظر می‌رسد که فارغ از فیزیکی یا غیرفیزیکی‌بودنِ آثار و زیان‌های ایجادشده، توجه به مقیاس آثار ناشی از رایاجنگ‌ها، به‌صورت موردبه‌مورد، ضروری است.

شعبهٔ تجدیدنظر دیوان کیفری بین‌المللی دریافت که برای عبور از آستانهٔ شدت لازم برای رسیدگی نزد دیوان، لازم نیست که رفتار مذکور «سیستماتیک یا در مقیاس بزرگ» باشد (Roscini, 2019, 263)؛ زیرا این شروط مربوط به مرحلهٔ تحقق شرط کلی آستانهٔ شدت برای رسیدگی

---

۱. برای مثال، دراین‌خصوص، ذیل رأی صادرشده در قضیهٔ المهدی، چنین گفته شده است که «جرایم علیه اموال ممکن است در مقایسه با جرایم علیه شخص از شدت کمتری برخوردار باشد، اما این درصورت درنظرگرفتن ویژگی اشیا و وضعیت قانونی آن‌هاست» (ICC, 2022, paras. 77 and 79-82). همچنین دراین‌خصوص، گاهی از بیمارستان‌های مورد هدف در کشور روسیه سخن گفته می‌شود (Bezhan, 2016).

2. Botnet.
3. Botmaster.

نزد دیوان کیفری بین‌المللی نیست؛ بلکه در مرحلهٔ پذیرش دادرسی متمایز میان الزامات صلاحیتی برای جنایات جنگی و جنایات علیه بشریت، پدید می‌آید و نباید در ارزیابی «مقیاس» مورد توجه واقع شود.

۱-۲. ماهیت

برای توجیه تحقیقات و تعقیب یک رفتار از سوی دیوان کیفری بین‌المللی، ضروری نیست موقعیت یا پرونده‌ای موجدِ تعداد زیادی تلفات باشد (ICC, 2017, p. 184). درواقع عوامل کیفی نیز باید در نظر گرفته شوند. در این راستا، شاخص «ماهیت» به‌طور ویژه «اشاره به عناصر خاص جرایمی مانند قتل، تجاوز جنسی و سایر جرایم دارد که در آن‌ها نوعی خشونت جنسی یا جنسیتی، جنایات علیه کودکان، آزار و اذیت یا تحمیل شرایط نابودکنندهٔ زندگی بر یک گروه وجود دارد» (The Office of the Prosecutor, 2013, para. 63). این بدان‌معناست که برخی از جرایم به‌گونه‌ای از نظر ماهیتی، شدیدتر از سایرین دانسته می‌شوند. برای مثال، نظام‌های حقوقی ملی و بین‌المللی پیشنهاد می‌کنند که قتل از نظر مجازات، از جدی‌ترین جرایم محسوب شود. جرایم خشونت جنسی و آن‌هایی که شامل شکنجه و رنج جسمی یا روانی بر بزه‌دیده است نیز جدی تلقی می‌شوند. این درحالی است که همان‌طور که هیئت دیوان متذکر می‌شود، جرایم علیه اموال به‌طور نسبی کمتر جدی تلقی می‌شوند (ICC, 2022, p. 77). این شاخص که براساس آن، میان جنایاتِ در صلاحیت دیوان کیفری بین‌المللی و به‌ویژه جنایات جنگی در سلسله‌مراتب به‌وجود می‌آید، یارای ایجاد اختلافات نظری بسیار را دارد؛ زیرا مبنای آن در اساسنامهٔ رم تصریح نشده است. بااین‌حال، اگر این شاخص درخصوص عملیات‌های سایبری نیز پذیرفته و اِعمال شود، موارد مربوط به حملات سایبری، که فقط باعث آسیب به اموال فیزیکی می‌شوند، مانند قضیهٔ استاکس‌نت، ممکن است از منظر ماهیت جنایت، با مفهوم پیش‌گفته، به‌اندازهٔ کافی شدید تلقی نشوند؛ به‌خصوص اگر در مقایسه با سایر موارد مربوط به قتل یا آسیب به گروه‌های آسیب‌پذیر همچون اطفال سنجیده شوند.

درهرحال، به‌نظر می‌رسد که این معیار برای ارزیابی شدت، در انتخاب و اولویت‌بندی پرونده‌های قابل پذیرش توسط دفتر دادستانی دیوان مناسب‌تر به‌نظر می‌رسد تا برای ارزیابی وصول به آستانهٔ شدت قابل پذیرش. اشخاص ممکن است نه‌تنها در قبال افعال، بلکه در قبال ترک‌فعل‌ها در فضای سایبر نیز مسئول باشند؛ به‌ویژه درخصوص مسئولیت مافوق یا فرمانده‌ای که به‌دلیل عدم پیشگیری از وقوع یک عملیات سایبری منتج به یک جنایت بین‌المللی که توسط شخص تحت کنترل مؤثر آن فرمانده واقع شده است، این موضوع مصداق می‌یابد (موضوع مادهٔ ۲۸ اساسنامهٔ رم). برای مثال، در تصمیم پروندهٔ علی، شعبهٔ مقدماتی این استدلال دفاعی را که مبنی‌بر این بود که یک پرونده با ترک فعل هرگز نمی‌تواند از شدت کافی برخوردار باشد، رد کرد؛ زیرا معتقد بود که چنین نتیجه‌گیری با متن، موضوع و هدف اساسنامه مغایر است (ICC, 2012, para. 46)[۱]. براین‌اساس، مشاهده می‌شود که موضوعیت‌بخشی به معیارِ ماهیت رفتار برای ارزیابی شدت جنایت واردشده می‌تواند موجب خروج ترک‌فعل‌ها از آستانهٔ شدت لازم شود و این درحالی است که نمی‌توان با این حکم کلی نسبت به خروج ترک‌فعل‌ها از آستانهٔ شدت لازم برای رسیدگی در دیوان کیفری بین‌المللی اقدام کرد.

۱-۳. روش ارتکاب

برخی از معیارهایی که ازطریق آن‌ها می‌توان به ارزیابی وجود این شاخص اقدام کرد، شامل موارد زیر است: «ابزاری که برای ارتکاب جرم به‌کار می‌رود، میزان مشارکت مرتکب در ارتکاب جرم و قصد مرتکب (اگر در این مرحله قابل تشخیص باشد)، میزان سازمان‌یافتگی یا وجود برنامهٔ پیشینی در ارتکاب جنایت، ارتکاب جنایت در نتیجهٔ سوءاستفاده از قدرت یا ظرفیت رسمی، وجود عناصر ویژه از ارتکاب ظلم مانند

---

۱. در سند خط‌مشی درخصوص انتخاب پرونده و اولویت‌بندی که دفتر دادستانی دیوان در سال ۲۰۱۶ منتشر کرد، دفتر دادستانی چنین مقرر می‌دارد: «مسئولیت فرماندهان و سایر مافوق‌ها براساس مادهٔ ۲۸ اساسنامه، یک شکل کلیدی مسئولیت است؛ زیرا ابزاری حیاتی برای تضمین اصل فرماندهی مسئولانه و درنتیجه پایان‌دادن به معافیت از مجازات جنایات‌کاران و کمک به پیشگیری از ارتکاب آن جنایات ارائه می‌دهد» (The Office of the Prosecutor, 2016, para. 36). در همین راستا، هنگامی که واحدهای نظامی کشورها از رایاجنگ‌ها استفاده می‌کنند، به احتمال زیاد موجب ایجاد مسئولیت حقوقی فرماندهان نیز می‌شود (Sliedregt, 2016, p. 521).

آسیب‌پذیربودنِ بزه‌دیدگان، هرگونه انگیزهٔ تبعیض یا استفاده از تجاوز جنسی و خشونت جنسی به‌عنوان ابزاری برای ازبین‌بردن گروه‌ها» (The Office of the Prosecutor, 2013, para. 64).

در حالتی که در ارتکاب جنایات علیه تمامیت جسمانی، استفاده از قدرت برق، قمه و سلاح‌های ممنوعه را در زمرهٔ روش‌های مشددهٔ ارتکاب جنایت به‌شمار می‌آورند، ابزارهای استفاده‌شده برای اجرای جنایات ناشی از رایاجنگ‌ها، یعنی بدافزارها و زیرساخت‌های سایبری مانند رایانه‌ها و سرورها، بعید است عامل تشدیدکننده‌ای در روش ارتکاب جنایت محسوب شوند. تشخیص هدف مرتکب از ارتکاب جنایت در زمینهٔ عملیات‌های سایبری ممکن است دشوار باشد؛ زیرا بدافزار به‌دلیل خطاهای فنی یا دانش ناکافی از سامانه‌های مورد هدف، ممکن است به‌طور پیش‌بینی‌ناپذیری عمل کند. بااین‌حال، برخی از عملیات‌های سایبری را می‌توان به‌طور مشخص ظالمانه توصیف کرد. برای مثال، یک عملیات سایبری که داده‌های پزشکی بیماران را تغییر می‌دهد؛ به‌طوری که آن‌ها درمان اشتباه، دردناک یا غیرضروری دریافت کنند، به‌یقین ظالمانه بوده و از منظر روش ارتکاب جرم، جنایت را از منظر شدت به آستانهٔ لازم می‌رساند.

گفته شده است که پیش‌زمینهٔ تجاوزکارانهٔ یک جنگ نیز عاملی تشدیدکننده در ارزیابی شدت است (Schabas & El Zeidy, 2016, p. 815)[1] و برای این وضعیت، گروه جاسوسی سایبری «Fancy Bear» مثال زده می‌شود و ادعا می‌شود که با دستور روسیه، نرم‌افزاری را آلوده کرده است که به نیروهای روسی اجازه می‌دهد به ارتباطات تلفنی و داده‌های موقعیت محلی نظامیان اوکراینی دسترسی داشته باشند و درنتیجه، به آن‌ها حمله کنند (Roscini, 2019, p. 267). در مثال دیگر، که گونه‌ای جنایت جنگی علیه غیرنظامیان محسوب می‌شود، جریان حملات رژیم اسرائیل علیه غزه در سال ۲۰۲۳ است که رژیم اسرائیل مکان‌یابیِ تجمعات انسانی را به‌جای ترور فرماندهان نظامی در دستور کار قرار داده و براساس پردازش داده‌های خامی که با ثبت‌نام همهٔ جمعیت نوار غزه در نرم‌افزار همراهِ «Lavender»، جمع‌آوری شده است، کشتار یا خودداری از آن را تجویز می‌کند (Frankel, 2024). بااین‌حال، به‌نظر می‌رسد که دیدگاه احتسابِ پیش‌زمینهٔ تجاوزکارانهٔ یک جنگ به‌منزلهٔ عاملی مشدد در ارزیابی آستانهٔ شدت رسیدگی، به دو دلیل پذیرفته نیست: اول این‌که مشخص نیست چگونه دادستان در مرحلهٔ بررسی مقدماتی ثابت می‌کند که پیش‌زمینهٔ یک جنگ، تجاوزکارانه و ناقض حق بر جنگ بوده است؛ به‌ویژه اگر دیوان نتواند صلاحیت خود را درخصوص جرم تجاوز در آن پرونده اعمال کند، در عمل امکان اثبات این موضوع منتفی خواهد بود. دوم این‌که درنظرگرفتن پیش‌زمینهٔ تجاوزکارانهٔ جنگ به‌عنوان عامل مشددهٔ ارزیابی شدت، خطر خلطِ میان حق بر جنگ و حقوق در جنگ و درنتیجه، تضعیف اصل برابری متخاصمان را در پی خواهد داشت. در همین راستا، دیوان کیفری بین‌المللی تاکنون از این دیدگاه حمایت نکرده است که پیش‌زمینهٔ یک جنگ تجاوزکارانه عاملی مشدده در ارزیابی شدت محسوب شود.

۱-۴. تأثیرگذاری

تأثیرات واقع‌شده درنتیجهٔ ارتکاب عملیات‌های سایبری، می‌تواند در موارد زیر ارزیابی شود: «رنج‌های متحمل‌شده توسط بزه‌دیدگان و افزایش آسیب‌پذیری آن‌ها، سپس وحشت ایجادشده برای آن‌ها درنتیجهٔ رنج‌ها و آسیب‌ها و آسیب‌های اجتماعی، اقتصادی و زیست‌محیطی که بر جوامع آسیب‌دیده وارد می‌شود» (The Office of the Prosecutor, 2013, para. 65). براین‌اساس، معیار «تأثیرات» دو جنبه دارد: تأثیر مستقیم بر بزه‌دیدگان و تأثیر گسترده‌تر بر جامعه. با توجه به نظر شعبهٔ مقدماتی دیوان کیفری بین‌المللی، تاثیرگذاری غیرمستقیم بر اشخاصی غیر از بزه‌دیده می‌تواند در ارزیابی شدت کافی برای رسیدگی دیوان کیفری بین‌المللی مؤثر باشد، اما نبود آن الزاماً وجود آستانهٔ شدت را نفی نمی‌کند (ICC, 2014, p. 47).

گنجاندن این عامل در ارزیابی آستانهٔ شدت لازم برای رسیدگی نزد دیوان کیفری بین‌المللی مستلزم این است که حتی در مواردی که عملیات سایبری براساس شاخص‌های کمّی به تعداد اندک قربانیان منجر می‌شود، اگر از منظر شاخص‌های کیفی موجب آثار قابل توجهی شده

1. The Comoros' letter of referral in relation to the Mavi Marmara, 14 May 2013, para. 25, available in: https://www.icc-cpi.int/iccdocs/otp/Referral-from-Comoros.pdf.

باشند، ممکن است دارای شدت لازم محسوب شوند. برای مثال، حملات سایبری که به مرگ صلح‌بانان و کارکنان بشردوستانه منجر می‌شود، به‌دلیل اهمیت مأموریت‌های حافظ صلح و تأثیر بازدارنده‌ای که ممکن است بر آن‌ها داشته باشد، دارای آثار درخور توجه دانسته می‌شود (ICC, The Prosecutor v. Bahr Idriss Abu Garda, 2010, p. 33; ICC, 2016, p. 55). همچنین برخی از حملات سایبری، که برای تأثیرگذاری در انتخابات سیاسی برخی کشورها انجام می‌شود، ممکن است تأثیر درخور توجهی در جامعهٔ مورد هدف داشته باشد. برای مثال، در آگوست ۲۰۱۷، مخالفان دولت کنیا ادعا کردند که هکرها با نفوذ به پایگاه دادهٔ کمیسیون انتخابات کنیا، نتایج انتخابات اخیر را دست‌کاری کرده‌اند تا اطلاعات رأی‌دهندگان را به‌دست آورند و راهبرد تبلیغاتی هدفمند را تهیه کنند (De Souza Dias , 2018). متعاقب انتخاب مجدد رئیس‌جمهور کنیا، آقای کنیاتا، دست‌کم ۲۴ نفر در خشونت‌هایی که پس از انتخاب مجدد وی واقع شد، کشته شدند. برخی از حملات سایبری نیز ممکن است بر اقتصاد یک کشور تأثیر بگذارد؛ مانند حملات DDoS در سال ۲۰۰۷ علیه استونی. به‌طورکلی، حملات سایبری، که زیرساخت‌های حیاتی ملی را هدف قرار می‌دهند و درنتیجه، ارائهٔ خدمات ضروری به جامعهٔ آن کشور را مختل می‌کنند، دارای تأثیرات شایان توجه بر جامعه محسوب می‌شوند؛ به‌ویژه اگر تأثیرات آن‌ها بلندمدت باشد. در چهارچوب این شاخص، نه‌تنها آسیب‌های اجتماعی و اقتصادی را باید در این زمینه در نظر گرفت، بلکه آسیب به محیط‌زیست را نیز باید در نظر گرفت؛ برای مثال، حملهٔ سایبری به یک کارخانهٔ شیمیایی که با هدف انتشار مواد خطرناک در اقیانوس در طول مخاصمه‌ای مسلحانه انجام می‌شود، ممکن است از منظر آثار سوئی که بر محیط زیست وارد می‌آورد، برآورندهٔ شاخص تأثیرات محسوب شود.

۲. شدت نسبی

چنانچه گفته شد، شدت نسبی با هدف تمرکز منابع دیوان بر جدی‌ترین و شدیدترین موضوعات است و برخلاف شدت قانونی، در انتخاب یا اولویت‌بندی پرونده‌های موضوع رسیدگی براساس شدت نسبی، دادستان دیوان از اختیار گسترده‌ای برخوردار است.

تاکنون، دادستان دیوان کیفری بین‌المللی در اعمال تفکیک میان شدت به‌منزلهٔ آستانهٔ پذیرش رسیدگی در دیوان کیفری بین‌المللی و شدت به‌منزلهٔ یک عامل اختیاری در انتخاب و اولویت‌بندی پرونده‌ها، به‌وضوح تمایز قائل نشده است (Stegmiller, 2011, p. 331). بااین‌حال، به‌نظر می‌رسد که آستانهٔ لازم برای آنچه که از آن به‌عنوان شدت قانونی یاد می‌شود، نباید خیلی بالا باشد (Stegmiller, 2011, 351). درواقع، «به نظر می‌رسد که آستانهٔ شدت قانونی پشتوانه‌ای را فراهم می‌کند تا اطمینان حاصل شود که دادگاه موارد جرایمی را که از نظر فنی با تعاریف در اساسنامه مطابقت دارند، اما جزئی هستند رد می‌کند» (DeGuzman, 2008, p. 1440). همان‌طور که گفته شده که «شدت تعریف‌شده» برای جنایات دیوان کیفری بین‌المللی مستلزم فرض به‌نفع شدت قانونی است و [...] آستانهٔ شدت اضافی در عمل فقط به جنایات جنگی مرتبط است» (Ambos, 2016, p. 294). نتیجه این است که در عمل، شدت قانونی باید فقط از تحقیقات و تعقیب قانونی جنایات جنگی در مقیاس کوچک و منفرد جلوگیری کند و نباید از تعقیب و تحقیق درخصوص جنایات نسل‌کشی یا جنایت علیه بشریت، یعنی جنایاتی که فی‌نفسه شدیدند، جلوگیری کند (DeGuzman, 2008, pp. 1457-1458; Stegmiller, 2011, pp. 351-355). براین‌اساس، یک حملهٔ سایبری صِرف علیه افراد یا اشیای محافظت‌شده در یک مخاصمهٔ مسلحانه که منجر به تأثیرات کم و خفیف می‌شود، از آستانهٔ شدت قانونی عبور نمی‌کند (Stegmiller, 2011, p. 352). از سوی دیگر، رفتار سایبری که باعث ایجاد، تحریک یا تسهیل جنایت نسل‌کشی می‌شود، نیازی به تلفات زیادی ندارد تا قابل قبول برای رسیدگی نزد دیوان کیفری بین‌المللی تلقی شود. همین آستانهٔ پایین باید برای ارزیابی شدت قانونی مورد استفاده قرار گیرد.

در ارزیابی شدت نسبی برای انتخاب و اولویت‌بندی وضعیت‌ها و پرونده‌ها است که دادستان اختیار بیشتری دارد. در واقع، «آستانهٔ شدت نسبی نسبتاً بالا است و در هر صورت بالاتر از آستانه شدت قانونی است» (Ambos, 2016, p. 294). این موضوع در یک سند خط‌مشی در

خصوص انتخاب پرونده و اولویت‌بندی که توسط دفتر دادستانی دیوان در سال ۲۰۱۶ منتشر شد[۱]، تأیید شده است و بیان می‌کند: «دفتر ممکن است آزمون سخت‌گیرانه‌تری را هنگام ارزیابی شدت برای اهداف انتخاب پرونده نسبت به آزمونی که از نظر قانونی طبق مادهٔ ۱۷ اساسنامه برای ارزیابی پذیرش مورد نیاز است، اعمال کند» (The Office of the Prosecutor, 2016, para. 36). معیارهای ارائه‌شده توسط سند سیاستی مذکور مشابه با معیارهای مختلفی است که کارشناسان سند مقررات تالین در خصوص زمانی که یک عملیات سایبری «توسل به زور» است، پیشنهاد کرده‌اند؛ از جمله: شدت، فوریت، مستقیم بودن، تهاجمی بودن (مداخله‌آمیز بودن)، قابل اندازه‌گیری بودن اثرات، ماهیت نظامی داشتن، سطح مشارکت دولت و مشروعیت احتمالی (Op. Cit., p. 13). اگرچه به‌طور قطعی، معیارهای پیش‌بینی‌شده توسط سند مقررات تالین برای هدفی متفاوت پیش‌بینی شده است، وانگهی برای در نظر گرفتن این‌که کدام عملیات سایبری ممکن است به آستانهٔ شدت لازم برای رسیدگی در دیوان کیفری بین‌المللی برسد نیز مفید است و به نظر می‌رسد که این معیارها می‌توانند برای دادستان دیوان کیفری بین‌المللی، در ارزیابی مؤثر باشند.

همچنین همان‌گونه که گفته شده است، شرایط فردی مرتکب ادعاشده، از جمله نقش وی به‌عنوان «مسئول‌ترین» در ارتکاب جنایت، می‌تواند در ارزیابی اهمیت نسبی، نه قانونی، مورد توجه قرار گیرد (Ambos, 2016, pp. 293). علاوه‌براین، معیارهای کمّی و کیفی پیش‌گفته، مشتمل بر مقیاس، ماهیت، روش و آثار، را می‌توان در ارزیابی شدت نسبی نیز در نظر گرفت (Stegmiller, 2011, p. 352). درنهایت، شدت نسبی اجازه می‌دهد تصمیمات برای مقایسهٔ بین پرونده‌های درحال بررسی و بالقوه در دیوان اتخاذ شود (Stegmiller, 2011, p. 355). بنابراین، حتی پرونده‌های مربوط به رفتار سایبری، که طبق مادهٔ ۱۷ اساسنامهٔ دیوان قابل قبول تلقی می‌شوند، ممکن است توسط دفتر دادستانی دیوان، به‌سبب عدم وصول به آستانهٔ شدت نسبی، مورد تحقیق یا تعقیب قانونی قرار نگیرند؛ اگر تعداد قربانیان به‌طور قابل توجهی کمتر از سایر موارد مشابه باشد. ازسوی‌دیگر، نمی‌توان این موضوع را رد کرد که ممکن است دادستان دیوان تصمیم به انتخاب وضعیت‌ها و پرونده‌های خاص مربوط به مشارکت یا معاونت در جنایات بین‌المللی ازطریق رایاجنگ‌ها، به‌دلیل تأثیرات آن‌ها یا به‌منظور بازدارندگی از بازارتکاب آن‌ها در آینده، بگیرد (The Office of the Prosecutor, 2016, para. 46)؛ حتی اگر عملیات‌های سایبری مذکور به‌نسبت سایر موارد، قربانیان کمتری داشته باشد[۲] و این رویکرد «بیان‌کننده»، یعنی پیگیری تعقیب‌هایی که بیشتر از ارزش‌ها محافظت می‌کنند و درنتیجه، ارسال پیامی برای دستیابی به یک نتیجهٔ معین، در واقع جنبه‌ای مهم و قانونی از راهبردهای دادستانی دیوان است (Cross, 2020, pp. 67-68).

بی‌شک ممکن است که وضعیت‌ها و پرونده‌های خاص مربوط به عملیات‌های سایبری که موجب مشارکت یا معاونت در ارتکاب جنایات بین‌المللی تحت صلاحیت دیوان کیفری بین‌المللی می‌شوند، از منظر شدت، قابل قبول تلقی شوند. رایاجنگ‌ها، مانند جنایات مرتکب‌شده با ابزارهای سنتی، به‌طور بالقوه می‌توانند تمام عوامل شناسایی‌شده توسط دیوان برای وصول به آستانهٔ شدت را برآورده کنند. این‌که آیا دادستان واقعاً تصمیم خواهد گرفت که وضعیت‌ها و پرونده‌های قابل پذیرش از رفتارهای سایبری را بر سایر موقعیت‌ها و پرونده‌ها ارجحیت ببخشد، موضوعی است که در صلاحیت دادستانی او قرار می‌گیرد (Cross, 2020, pp. 16-17) و در آن، عوامل کمی و کیفیِ شدت همراه با رکن روانی مرتکب ادعایی و شرایط و اوضاع و احوال وقوع جنایت، می‌توانند به‌طور مساوی در نظر گرفته شوند. بنابراین، دادستان ممکن است تصمیم بگیرد که یک

---

۱. در پاراگرف ۳۲ از سند خط‌مشی درخصوص انتخاب پرونده و اولویت‌بندی دفتر دادستانی دیوان درخصوص شدت قانونی و در پاراگراف‌های ۳۵ تا ٤١ آن درخصوص شدت نسبی، بحث شده است (The Office of the Prosecutor, 2016, paras. 32, 35-41).

۲. برای مثال، چنانچه پیشتر نیز مورد اشاره قرار گرفت، می‌توان از مقایسهٔ رویکرد متفاوت دیوان نسبت به دو پروندهٔ کومور و پروندهٔ ابوگردا، بهره برد. توضیح آنکه در قضیهٔ کومور، دفتر دادستانی دیوان کیفری بین‌المللی این موضع را اتخاذ کرد که تعداد ده مورد قربانی جانی نمی‌تواند شرط وصول به آستانهٔ شدت را برآورده سازد؛ هرچند برخی ملاحظات دیگر نیز غیر از تعداد قربانیان، در این خصوص وجود داشت. از سوی دیگر، چنانچه ذکر شد، در قضیهٔ ابوگردا، دفتر دادستانی دیوان درخصوص کشته‌شدن دوازده حافظ صلح، «به‌سبب اهمیت هدف و تأثیر بر عملیات‌های حافظ صلح»، اقدام کرد.

پرونده مربوط به رفتار سایبری را بررسی یا تعقیب کند؛ اما به‌سبب ملاحظات مقایسه‌ای، احتمال شناسایی و دستگیری مظنون یا در دسترس بودن شواهد، در خصوص مورد دیگر به نتیجهٔ متفاوتی برسد.

نتیجه‌گیری

استفادهٔ فزاینده از حملات سایبری در جهان، موجب گسترش تأثیرات آن‌ها شده و برخی رایاجنگ‌ها را پدید آورده است که مانند همهٔ دیگر گونه‌های جنگ، همهٔ کشورهای جهان ناگزیر از تنظیمگری و وضع محدودیت بر آن‌ها هستند. ازجملهٔ محدودیت‌های مذکور، امکان‌سنجیِ وقوع جنایات جنگی در رایاجنگ‌هاست. درصورتی می‌توان برخی اقدامات ارتکاب‌یافته در عملیات‌های سایبری را به‌عنوان جنایت جنگیِ سایبری براساس مقررات موجود تلقی کرد که عناصر زمینه‌ایِ عمومی برای وقوع جنایات جنگی در رایاجنگ نیز وجود داشته باشد. یکی از عناصر زمینه‌ایِ لازم، وصول به آستانهٔ شدت صلاحیتی برای رسیدگی نزد دیوان کیفری بین‌المللی است. آن‌گونه که از مواد ۱۷ و ۵۳ اساسنامهٔ رم مستنبط است، دو گونهٔ آستانهٔ شدت رسیدگی، یعنی آستانهٔ شدت قانونی و آستانهٔ شدت نسبی، نزد دیوان کیفری بین‌المللی موجود است.

درخصوص آستانهٔ شدت قانونی، رویهٔ قضایی دیوان کیفری بین‌المللی، همچون تصمیم دادستان در آغازنکردن تحقیقات درخصوص حادثهٔ کشتی ماوی مرمره، بیانگر آن است که ارزیابی شدت قانونی باید بر اساس عوامل کمی و کیفی، همچون مقیاس، ماهیت، شیوهٔ ارتکاب جنایات و همچنین تأثیرات آن‌ها، انجام شود. عامل «مقیاس» که تا حدی با نظر سند مقررات تالین همسوست، بر گسترهٔ آثارِ عموماً فیزیکی تأکید دارد و از این منظر، موضوع انتقاد در رایاجنگ‌هایی است که باوجود تلقیِ عرفی از شدیدبودنِ آن‌ها، ایجادگرِ گستره‌ای از آثار فیزیکی نبوده‌اند. عامل «ماهیت» به‌سبب عدم شمول نسبت به مسئولیت ناشی از ترک فعل در جنایات جنگیِ سایبری، نمی‌تواند معیاری مناسب برای ارزیابی آستانهٔ شدت قانونی دانسته شود. از عامل «شیوهٔ ارتکاب» نیز به‌عنوان عامل مؤثر در ارزیابی آستانهٔ شدت قانونی رایاجنگ‌ها نمی‌توان نام برد؛ زیرا مصادیق عامل مذکور را نمی‌توان چندان در رایاجنگ‌ها متجلی دانست و فقط برخی اعمال ارتکاب‌یافته در پهنهٔ رایاجنگ‌ها، همچون ایجاد اختلال جدی در داده‌های مربوط به سلامت عمومی بیماران، یارای ارزیابی توسط این شاخص، به‌عنوان جنایات واصل به آستانهٔ شدت قانونی، هستند. درنهایت، عامل «تأثیرگذاری» را می‌توان عاملی پرکاربرد در ارزیابی وصول به آستانهٔ شدت قانونیِ رسیدگی تلقی کرد؛ زیرا دایرهٔ شمول آن بر رایاجنگ‌های ایجادگرِ اختلال‌های غیرفیزیکی نیز گسترده شده است. مجموع این عوامل دارای اهمیتی ثابت نیستند و باید به‌صورت موردی ارزیابی شوند و درصورتی‌که ارزیابی کلی حاکی از شدت کافی باشد، ضروری نیست که همهٔ شرایط به‌صورت تجمیعی برآورده شوند.

درخصوص آستانهٔ شدت نسبی، سند خط‌مشی دفتر دادستانی دیوان درخصوص انتخاب پرونده و اولویت‌بندی تصریح می‌کند که آستانهٔ شدت نسبی به‌نسبت شدت قانونی بالاتر است و برای ارزیابی آن، از عوامل کمّی و کیفی ارزیابی‌شده برای آستانهٔ شدت قانونی بهره گرفته می‌شود. رایاجنگ‌ها مانند جنایات مرتکب‌شده با ابزارهای سنتی، به‌طور بالقوه می‌توانند تمام عوامل شناسایی‌شده توسط دیوان برای وصول به آستانهٔ شدت نسبی را برآورده کنند. برای این منظور، عوامل کمّی و کیفیِ شدت همراه با رکن روانی مرتکب ادعایی و شرایط و اوضاع‌واحوال وقوع جنایت، مساوی در نظر گرفته می‌شوند.

منابع

کیهانلو، فاطمه و رضادوست، وحید (۱۳۹۴). حملات سایبری به‌مثابهٔ توسل به زور در سیاق منشور سازمان ملل متحد. تحقیقات حقوقی، ۱۸(۶۹)، ۱۹۳-۲۰۸. https://doi.org/10.22133/mtlj.2023.367442.1137

Ambos, K. (2016). *Treatise on international criminal law: volume III: international criminal procedure*. Oxford University Press.

Biller, J., & Schmitt, M. (2019). Classification of cyber capabilities and operations as weapons, means, or methods of warfare. *International Law Studies*, *95*, 179-225. Link

Boothby, W. H. (2013). Methods and Means of Cyber Warfare. *International Law Studies*, *89*(1), 8. Link

Buchan, R. (2014, December). The Mavi Marmara Incident and the International Criminal Court. In *Criminal Law Forum* (Vol. 25, No. 3, pp. 465-503). Dordrecht: Springer Netherlands.

Cross, M. E. (2020). Strategising International Prosecutions: How Might the Work of the Kosovo Specialist Prosecutor's Office Come to Be Judged? *international criminal law review*, *20*(1), 43-76.
https://doi.org/10.1163/15718123-02001011

DeGuzman, M. M. (2008). Gravity and the legitimacy of the International Criminal Court. *Fordham International Law Journal*, *32*, 1400. Link

Efrony, D., & Shany, Y. (2018). A rule book on the shelf? Tallinn manual 2.0 on cyberoperations and subsequent state practice. *American Journal of International Law*, *112*(4), 583-657. https://doi.org/10.1017/ajil.2018.86

Fanelli, R., & Conti, G. (2012). A methodology for cyber operations targeting and control of collateral damage in the context of lawful armed conflict. In C. Czosseck, R. Ottis, & K. Ziolkowski (Eds.), *4th International Conference on Cyber Conflict (CCDCOE, 2012)*. Link

Frankel, S. (2024). When AI Decides Who Lives and Dies, The Israeli military's algorithmic targeting has created dangerous new precedents. *Foreign Policy*. Link

Greenberg A. (2023). The International Criminal Court Will Now Prosecute Cyberwar Crimes. *Wired.* Link

Greenberg, A. (2018). The untold story of NotPetya, the most devastating cyberattack in history. *Wired, August*, *22*. Link

Horowitz, J. (2020). Cyber operations under international humanitarian law: Perspectives from the ICRC. *ASIL Insights*, *24*(11). Link

International Criminal Court, Office of the Prosecutor. (2013). *Referral from Comoros*. Link

Le Procureur c. Ahmad Al Faqi Al Mahdi (2022). Case Information Sheet. ICC-01/12-01/15

Le Procureur c. Al Hassan. (2020). Affaire n° ICC-01/12-01/18-601-Red OA, Arrêt relatif à l'appel de M. Al Hassan contre la décision de la Chambre préliminaire I intitulée «Décision relative à l'exception d'irrecevabilité pour insuffisance de gravité de l'affaire soulevée par la défense». Link

Mačák, K. (2015). Military objectives 2.0: The case for interpreting computer data as objects under international humanitarian law. *Israel Law Review*, *48*(1), 55-80. https://doi.org/10.1017/S0021223714000260

O'Brien, M. (2012). Prosecutorial discretion as an obstacle to prosecution of United Nations peacekeepers by the International Criminal Court: The big fish/small fish debate and the gravity threshold. *Journal of International Criminal Justice*, *10*(3), 525-545. Link

Owens, W. A., Dam, K. W., & Lin, H. S. (2009). *Technology, policy, law, and ethics regarding U.S. acquisition and use of cyberattack capabilities*. The National Academies Press.

Palojärvi, P. (2009). *Battle in bits and bytes-computer network attacks and the law of armed conflict*. Finland:
Erik Castrén Institute of International Law and Human Rights. Link

Roscini, M. (2019). Gravity in the Statute of the International Criminal Court and Conduct that Constitutes, Instigates or Facilitates International Crimes. *Criminal Law Forum*, *30*(3), 247–272. http://dx.doi.org/10.2139/ssrn.3435439

Roscini, M. (2022). Cyber Operations Can Constitute War Crimes Under the ICC Jurisdiction Without Need to Amend the Rome Statute. Link

Sa´ Couto, S., & Cleary, K. (2008). The gravity threshold of the International Criminal Court. *American University International Law Review*, *23*(3), 667-717. Link

Schabas, W. A. (2008). Prosecutorial discretion v. judicial activism at the International Criminal Court. *Journal of International Criminal Justice*, *6*(4), 731–761. https://doi.org/10.1093/jicj/mqn045

Schabas, W. A. (2016). *The International Criminal Court: A Commentary on the Rome Statute* (2nd ed.). Oxford University Press.

Schabas, W. A., & El Zeidy, M. M. (2016). Article 17. In O. Triffterer & K. Ambos (Eds.), *The Statute of the International Criminal Court, A Commentary* (3rd ed.). Oxford.

Schabas, W. A., & El Zeidy, M. M. (2016). Article 17. In O. Triffterer & K. Ambos (Eds.), *The Statute of the International Criminal Court, A Commentary* (3rd ed.). Oxford.

Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed.). Cambridge University Press.

Situation in Georgia (27 January 2016). Decision on the Prosecutor's request for authorization of an investigation, Pre-Trial Chamber I, ICC-01/15-12

Situation in Kenya (2010, March 31). ICC-01/09-19-Corr, Decision Pursuant to Article 15 of the Rome Statute on the Authorization of an Investigation into the Situation in the Republic of Kenya, Pre-Trial Chamber II.

Pre-Trial Chamber, I. I. (2012). *Prosecutor v. William Samoei Ruto, Henry Kiprono Kosgey and Joshua Arap Sang. Decision on the Confirmation of Charges Pursuant to Article 61 (7)(a) and (b) of the Rome Statute*. ICC-01/09-01/11. 23 de enero de 2012. Dissenting Opinion Judge Hans-Peter Kaul. Link

Chamber, A. (2006). *Judgment on the Prosecutor's appeal against the decision of Pre-Trial Chamber I entitled" Decision on the Prosecutor's Application for Warrants of Arrest, Article 58*. ICC-01/04-169. The Hague: International Criminal Court.

Situation in the Islamic Republic of Afghanistan (2019, April 12). Decision Pursuant to Article 15 of the Rome Statute on the Authorisation of an Investigation into the Situation in the Islamic Republic of Afghanistan, Pre-Trial Chamber II, ICC-02/17. Link

Situation in the Republic of Burundi (2017, October 25). ICC-01/17-9-RED, Decision Pursuant to Article 15 of the Rome Statute on the Authorization of an Investigation into the Situation in the Republic of Burundi, PTC III. Link

Situation on Registered Vessels of Comoros, Greece and Cambodia (2014, November 6). Report (ICC-01/13-6-AnxA). Link

Situation on Registered Vessels of the Union of the Comoros, The Hellenic Republic and the Kingdom of Cambodia (2015, July 16). Decision on the request of the Union of the Comoros to review the Prosecutor’s decision not to initiate an investigation (ICC-01/13-34-Anx). Pre-Trial Chamber I. Partly Dissenting Opinion of Judge Peter Kova´cs. Link

Stegmiller, I. (2011). *The Pre-Investigation Stage of the ICC, Criteria for Situation Selection*. Berlin: Duncker & Humblot.

Stegmiller, I. (2011). *The Pre-Investigation Stage of the ICC, Criteria for Situation Selection*. Berlin: Duncker & Humblot.

Stegmiller, I. (2009). The gravity threshold under the ICC statute: Gravity back and forth in Lubanga and Ntaganda. *International Criminal Law Review*, *9*(3), 547-565. https://doi.org/10.1163/157181209X457983

The Office of the Prosecutor (2013). Policy Paper on Preliminary Examinations. International Criminal Court. Link

The Office of the Prosecutor (2016). Policy Paper on Case Selection and Prioritisation, International Criminal Court. Link

The Office of the Prosecutor (2017). Report on Preliminary Examination Activities. *International Criminal Court.* Link

The Prosecutor v. Abu Garda (2010, February 8). Decision on the Confirmation of Charges (ICC-02/05-02/09-243-RED). Pre-Trial Chamber I.

Trahan J. (2021). The Criminalization of Cyber-operations Under the Rome Statute. *Journal of International Criminal Justice*, *19*(5), 1133–1164. https://doi.org/10.1093/jicj/mqab066

Trahan, J. (2021). The criminalization of cyber-operations under the Rome statute. *Journal of International Criminal Justice*, *19*(5), 1133-1164. https://doi.org/10.1093/jicj/mqab066

Trahan, J. (2022). Contributing to Cyber Peace by Maximizing the Potential for Deterrence: Criminalization of Cyberattacks under the International Criminal Court's Rome Statute. In S. J. Shackelford, F. Douzet, & C. Ankersen (Eds.), *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace* (pp. 131–153). Cambridge University Press. https://doi.org/10.1017/9781108954341.007

Van Sliedregt, E. (2016). Command responsibility and cyberattacks. *Journal of Conflict and Security Law*, *21*(3), 505-521. https://doi.org/10.1093/jcsl/krw012

Whiting, A. (2015). The ICC Prosecutor Should Reject Judges' Decision in Mavi Marmara. *Just Security*. Link

[In persian]

Keihanlou, Fatemeh and Rezadoust, Vahid (2015). *Cyberattacks as a Use of Force in the Context of the United Nations Charter*. Legal Researchs, *18*(69), 193-208. https://doi.org/10.22133/mtlj.2023.367442.1137