**Criminal Law and Criminology Studies** Online ISSN: 2588-5901

Journal of the Faculty of Law and Political Science Volume: 52, Issue:2

Homepage: https://clcs.ut.ac.ir Autumn & Winter 2023

# The Function and Influence of the UN Security Council on the Development of the ICC Jurisdiction (with Emphasis on the Resolutions Issued against the Crime of Cyber-Aggression)

**Alireza Mohaghegh Harcheghan**[1] | **Mohammad Ali Ardebili** [2]✉ |

**Ebrahim Beigzadeh** [3] **Mohammad Ali Mahdavi Sabet** [4] |

1. Criminal Law and Criminology, Department of Criminal Law and Criminology, Faculty of Law, Theology and Political Science, Science and Research Branch, Islamic Azad University, Tehran, Iran. E-mail: alireza.mohaghegh.1400@gmail.com
2. Corresponding Author: Department of Criminal Law and Criminology, Faculty of Law, Shahid Beheshti University, Tehran, Iran. E-mail: m-ardebili@sbu.ac.ir
3. Department of International Law, Faculty of Law, Shahid Beheshti University, Tehran, Iran. E-mail: ebrahim_beigzadeh@sbu.ac.ir
4. Department of Criminal Law and Criminology, Faculty of Law, Theology and Political Science, Islamic Azad University, Tehran, Iran. E-mail: ali@mahdavi.fr

## Article Info

**Article type:**
Research Article

**Article history:**
Manuscript Received:
26 November 2022
Final revision received:
13 January 2023
Accepted:
10 February 2023
Published online:
15 March 2023

**Keywords**:
*Cyber aggression, United Nations Security Council, development of the jurisdictional, International Criminal Court, Security Council resolutions.*

## ABSTRACT

Cyber aggression is one of the crimes that has been discussed in the international legal regime due to the late progress of technology. This qualitative research was conducted in terms of purpose, practical and in terms of gathering information in a documentary way and through laws, international documents, the obtained information was analyzed in a descriptive-analytical form in order to answer this question: if the Jurisdiction of confirmation the cyber aggression by the Security Council is not exclusive, what is the function and influence of the United Nations Security Council on the development of jurisdiction of other authorities such as the International Criminal Court? The findings of the research show that Article 8 of the Statute of the International Criminal Court does not include the actions of private individuals, only if a cyber attack can be considered as an aggression if it is an "armed attack". Law 12 of the Tallinn guidelines is also clear in this regard. The competence of the Security Council in the matter of verifying cyber aggression has precedence and priority, this precedence does not constitute exclusive jurisdiction. The jurisdictional regime of the court in recognizing the crime of aggression in the case of government referrals and appropriate investigations can be applied only after approval or acceptance by each of two aggressor and the alleged victim member state. The Security Council can refer a situation to the International Criminal Court or suspend the prosecution and investigation of the Court temporarily, extendable and obliged for one years.

**Cite this article:** Mohaghegh Harcheghan, Alireza; Ardebili, Mohammad Ali; Beigzadeh, Ebrahim & Mahdavi Sabet, Mohammad Ali, (2023). "The Function and Influence of the UN Security Council on the development of the ICC jurisdiction (with Emphasis on the Resolutions Issued against the Crime of Cyber-Aggression)", *Criminal Law and Criminology Studies*, 52 (2): 149-168, DOI: https://doi.org/10.22059/JQCLCS.2023.351373.1799

 Publisher: University of Tehran Press.
https://doi.org/10.22059/JQCLCS.2023.351373.1799

**مطالعات حقوق کیفری و جرم شناسی**
**مجله دانشکده حقوق و علوم سیاسی**
https://clcs.ut.ac.ir
شاپا الکترونیکی: ۵۹۰۱-۲۵۸۸
دوره ۵۲، شماره ۲
پاییز و زمستان ۱۴۰۱

# کارکرد و تأثیرگذاری شورای امنیت سازمان ملل متحد بر توسعه صلاحیت دیوان کیفری بین‌المللی

## (با تأکید برقطعنامه‌های صادره علیه جنایت تجاوز سایبری)

**علیرضا محقق هرچقان [۱] | محمدعلی اردبیلی✉[۲] | ابراهیم بیگ‌زاده[۳] | محمدعلی مهدوی ثابت[۳]**

۱. گروه حقوق کیفری و جرم شناسی، دانشکده حقوق، علوم سیاسی و الهیات، دانشگاه آزاد اسلامی، واحد علوم تحقیقات تهران، تهران، ایران. رایانامه: alireza.mohaghegh.1400@gmail.com

۲. نویسنده مسئول: گروه حقوق کیفری و جرم شناسی، دانشکده حقوق، دانشگاه شهید بهشتی، تهران، ایران.
رایانامه: m-ardebili@sbu.ac.ir

۳. گروه حقوق بین‌الملل، دانشکده حقوق، دانشگاه شهید بهشتی، تهران، ایران. رایانامه: ebrahim_beigzadeh@sbu.ac.ir

۴. گروه حقوق کیفری و جرم شناسی، دانشکده حقوق، الهیات و علوم سیاسی، دانشگاه آزاد اسلامی، تهران، ایران.
رایانامه: ali@mahdavi.fr

**اطلاعات مقاله**

**نوع مقاله:**
مقالهٔ پژوهشی
تاریخ دریافت:
۱۴۰۱/۹/۵
تاریخ بازنگری:
۱۴۰۱/۱۰/۲۳
تاریخ پذیرش:
۱۴۰۱/۱۱/۲۱
تاریخ انتشار:
۱۴۰۱/۱۲/۲۴

**کلیدواژه‌ها:**
*تجاوز سایبری، توسعهٔ صلاحیت، دیوان کیفری بین‌المللی، شورای امنیت سازمان ملل متحد، قطعنامه‌های شورای امنیت.*

**چکیده**

تجاوز سایبری، از جمله جنایت‌هایی است که به‌واسطهٔ پیشرفت فناوری در رژیم حقوقی بین المللی و به‌ویژه ظرفیت رسیدگی آن به‌عنوان یک جنایت در دیوان کیفری بین‌المللی به کمک شورای امنیت و قطعنامه‌های صادره مورد بحث قرار گرفته است.

این پژوهش، به شکل توصیفی – تحلیلی تجزیه‌وتحلیل شده است و به لحاظ هدف، کاربردی و به لحاظ گردآوریِ اطلاعات، به روش اسنادی و با مراجعه به قوانین، اسناد بین‌المللی و منابع معتبر انجام شده و اطلاعات به‌دست‌آمده به شکل توصیفی_تحلیلی تجزیه‌وتحلیل شده‌اند تا به این پرسش پاسخ داده شود که «در صورت منحصر نبودنِ احرازِ تجاوز سایبری به شورای امنیت، کارکرد و تأثیرگذاری شورای امنیت سازمان ملل متحد بر توسعهٔ صلاحیت مراجع دیگری، نظیر دیوان کیفریِ بین‌المللی، چیست؟».

یافته‌های پژوهش نشان می‌دهد که مادهٔ ۸ مکرر اساسنامهٔ دیوان کیفری بین‌المللی، شامل اعمال اشخاص خصوصی نمی‌شود و تنها در صورتی یک عملیات سایبری را می‌توان تجاوز دانست که به آستانه و میزان «حملهٔ مسلحانه» رسیده باشد. قانون ۱۲ دستورالعمل تالین نیز در این زمینه صراحت دارد.

صلاحیت شورای امنیت در بحث احراز تجاوز سایبری دارای تقدم و اولویت است و این تقدم به‌منزلهٔ صلاحیت انحصاری نیست. رژیم صلاحیتیِ دیوان در شناسایی جنایت تجاوز، در صورت ارجاعات دولتی و تحقیقات مقتضی، تنها پس از تصویب یا پذیرش دست‌کم یکی از دو کشور متجاوز و مجنی‌علیه یا قربانی (عضو مدعی قربانی)، قابل اعمال است. شورای امنیت می‌تواند وضعیت را به دیوان کیفری بین‌المللی ارجاع دهد یا تعقیب و تحقیق دیوان را به‌صورت موقت، به مدت یک سال تمدید کند.

**استناد:** محقق هرچقان، علیرضا؛ اردبیلی، محمدعلی؛ بیگ‌زاده، ابراهیم و مهدوی ثابت، محمدعلی (۱۴۰۱). کارکرد و تأثیرگذاری شورای امنیت سازمان ملل متحد بر توسعه صلاحیت دیوان کیفری بین‌المللی (با تأکید برقطعنامه‌های صادره علیه جنایت تجاوز سایبری)، *مطالعات حقوق کیفری و جرم شناسی*، ۲ (۵۲)، ۱۶۸-۱۴۹،
https://doi.org/10.22059/JQCLCS.2023.351373.1799 DOI:

ناشر: مؤسسه انتشارات دانشگاه تهران.



DOI: https://doi.org/10.22059/JQCLCS.2023.351373.1799

## ۱. مقدمه:

پس از گذشت بیش از نیم‌قرن از ظهور فناوری رایانه و تحولات جدیِ منتج از آن در زیست انسانی، فضای سایبری ایجادشدهٔ ناشی از اتصال رایانه‌ها به یکدیگر، به ظرفیتی برای فعالیت بزهکاران بدل شده است. یکی از مهم‌ترین این جرائم، تجاوزی است که به‌دلیل بروز در فضای سایبر، به‌عنوان «تجاوز سایبری» شناخته می‌شود.[۱] این حملات و تجاوزات هر روز با پیشرفت های تکنیکی، شکل جدیدی به خود گرفته و ازاین‌رو معادلات حقوقی زمان پیش از ظهور فضای سایبری را متحول کرده‌اند؛ بنابراین حقوق بین‌الملل سایبری با در نظر گرفتن قواعد ناظر بر «حاکمیت» و «صلاحیت»، صرف‌نظر از وجود عنصر قلمرو سرزمینی و خاکی، تعریف جدیدی را از روابط بین دول ارائه کرده و فعالیت‌ها در فضای سایبری را در این زمینه مدنظر قرار داده است.[۲] توجه به موضوع «تجاوز سایبری»، به‌عنوان یک جنایت بین‌المللی، در تحولات سیاست جنایی بین‌المللی امری ضروری و دشوار خواهد بود. این دشواری علاوه‌بر سرعت تحولات تکنولوژیکی و تغییر شکل تجاوز، علل دیگری نیز دارد؛ یک علت آن این است که به‌سختی می توان یک حملهٔ شبکه‌ای کامپیوتری را ذیل تعریف جنایت تجاوز سایبری قرار داد (Ambos, 2016: 497). مطابق مادهٔ ۸ مکرر اساسنامهٔ دیوان کیفری بین‌المللی «برنامه‌ریزی، تدارک، آغاز یا اجرای اقدام تجاوزکارانه توسط صاحب‌منصبی که به‌نحو مؤثری اقدام سیاسی یا نظامیِ یک دولت را کنترل یا هدایت می‌کند، که با توجه به ماهیت، شدت و گسترهٔ آن، موجب نقض آشکار منشور ملل متحد می‌شود»، تجاوز سایبری نامیده می‌شود. دومین علت این است که در تحلیل بند ۲ مادهٔ ۸ اساسنامه، یک حملهٔ شبکه‌محور کامپیوتری فقط در شرایط بسیار خاصی به‌منزلهٔ «عمل تجاوز» به‌حساب می‌آید؛ یعنی حمله‌ای که به‌واسطهٔ نیروهای مسلح دولتی یک کشور انجام شده باشد. سومین علت این است که آنچنان که در بند ۱ مادهٔ ۸ مکرر اساسنامهٔ دیوان درج شده، می‌توان چنین حملاتی را به‌منزلهٔ نقض آشکار منشور ملل متحد به‌شمار آورد. نخستین مؤلفه‌ای که شرط مهمی برای «تجاوز» محسوب شدنِ حملات سایبری است، دولتی بودن منشأ آن است (Horowitz, 2020: 25). انتساب حملات سایبری به یک دولت، پایان فرایند شناسایی تجاوز سایبری نیست. در مرحلهٔ بعد لازم است استفاده از نیروهای مسلح محرز شود. علت این امر آن است که در تعریف تجاوز از سوی مجمع عمومی، استفاده از نیروهای مسلح، لازمهٔ وقوع

---

۱. نوع سنتی و سرزمینی آن با عنوان «جنایت تجاوز» به‌طور گسترده وجود دارد که ممنوعیت آن به‌صورتِ یک قاعدهٔ آمره (JusCogens) در سطح بین‌الملل پذیرفته شده است.

۲. ر.ک: مقالهٔ مشترک علیرضا محقق هرچقان و آقایان دکتر محمدعلی اردبیلی، دکتر ابراهیم بیگ‌زاده، با عنوان «حقوق بین الملل سایبری و توسعهٔ صلاحیت دیوان کیفری بین‌المللی؛ با تأکید بر مذاکرات ۲۰۱۷ تالین» در *فصلنامهٔ مطالعات حقوق عمومی*، انتشاریافته به‌صورت الکترونیکی، شمارهٔ ۳، دورهٔ ۵۳، پاییز ۱۴۰۲.

تجاوز است (Shaw, 2010: 154). شایان ذکر است که «نیروهای مسلح» باید در معنای وسیع آن، یعنی همهٔ نیروهای نظامی (عملیاتی و ستادی) در نظر گرفته شوند. با اینکه منشور ملل متحد صلاحیت احراز جنایت تجاوز را برای شورای امنیت قائل شده است[۱]؛ این دشواری در احراز موجب شده که انحصارِ چنین مسئولیتی برای شورای امنیت مورد تردید واقع شود و صلاحیت مراجع بین‌المللی دیگر، نظیرِ مجمع عمومی سازمان ملل، دیوان دادگستری بین‌المللی و دیوان کیفری بین‌المللی نیز مطرح شود. مطابق مادهٔ ۲۴ منشور ملل متحد، شورای امنیت در بحث احراز تجاوز، دارای اولویت و تقدم است.

روش تحقیق این مقاله از نوع توصیفی–تحلیلی است تا به این پرسش پاسخ دهد: «در صورت منحصر نبودن احراز تجاوز سایبری به شورای امنیت، کارکرد و تأثیرگذاری شورای امنیت بر توسعهٔ صلاحیتِ دیوان کیفری بین‌المللی چیست؟». پاسخ به این پرسش، با حمل بر صحت، ابتدا مستلزم شناسایی ماهیت تجاوز سایبری و واکاوی صلاحیت رسیدگی‌کننده به آن است. در این زمینه لازم است تا اثربخشی دستورالعمل تالین بر صلاحیت دیوان کیفری بین‌المللی در ایجاد صلح و امنیت بین‌المللی سایبری در سیر مطالعات و پژوهش قرار بگیرد.[۲]

## ۲. تجاوز سایبری

تعریف دقیقی از تجاوز سایبری در منابع حقوقی بین‌المللی دیده نمی‌شود. با این حال، می‌توان این مفهوم را متناظر با تجاوز سنتی دانست، مشروط بر اینکه تجاوز از سوی شبکه‌های متمرکز بر رایانه انجام شده باشد (Madubuike-Ekwe, 2021: 635)؛ بنابراین پیش از ارائهٔ تعریف تجاوز سایبری، بهتر است به مفهوم عام‌تر آن، یعنی تجاوز، پرداخته شود. با وجود ممنوعیت تجاوز در منشور ملل متحد (بند ۱ مادهٔ ۱ و بند ۴ مادهٔ ۲) و همچنین در اساسنامهٔ نورنبرگ و اصول مطروحهٔ آن در قطعنامهٔ (۱)۹۵ در سال ۱۹۴۵، در هیچ‌یک از این اسناد، تعریفی حقوقی از جرم تجاوز ارائه نشده و منشور تنها به بیان این نکته اکتفا کرده که صلاحیت احراز تجاوز با شورای امنیت است. تجاوز در روابط بین‌الملل، اقدام یا سیاست توسعه‌ای است که توسط یک دولت به ضرر دولت دیگر و از طریق یک حملهٔ نظامی بدون دلیل[۳] و به‌منظور جبران یا مجازات پس از خصومت انجام می‌شود. تجاوز در حقوق بین‌الملل به‌عنوان هرگونه استفاده از نیروی مسلح در

---

۱. مادهٔ ۳۹ منشور ملل متحد.

۲. رک: مقالهٔ مشترک علیرضا محقق هرچقان و آقایان دکتر محمدعلی اردبیلی و دکتر ابراهیم بیگ‌زاده، با عنوان «اثربخشی دستورالعمل تالین ۲۰۱۷ میلادی بر صلاحیت دیوان کیفری بین‌المللی در ایجاد صلح و امنیت سایبری بین‌المللی»، *دوفصلنامهٔ علمی–پژوهشی آموزه‌های حقوق کیفری دانشگاه علوم اسلامی رضوی*، انتشاریافته به‌صورت الکترونیکی، شمارهٔ ۲۳، دورهٔ ۱۹، بهار و تابستان ۱۴۰۱.

3. Unprovoked military attack

روابط بین‌الملل تعریف شده است که با ضرورت دفاعی، اقتدار بین‌المللی یا رضایت کشوری که در آن از زور استفاده می‌شود، توجیه نشده باشد (Darcy, 2021: 106). دادگاه نورنبرگ[۱]، برای اولین‌بار در تاریخ حقوق کیفری بین‌المللی در سال ۱۹۴۵، «جرم علیه صلح»[۲] را در کنار «جنایت جنگی» و مفهومِ «جنایت علیه بشریت»[۳] را به‌عنوان جنایت‌های مستقل، به رسمیت شناخت (دیهیم، ۱۳۸۴: ۴۵۱-۴۵۲). این جنایت شامل برنامه‌ریزی[۴]، آماده‌سازی[۵]، آغاز[۶] و یا راه‌اندازی[۷] جنگ تجاوزگونه و یا جنگ در نقض آشکار معاهدات بین‌المللی، توافقات یا تضمینات تبیین شده است. مسئولیت کیفریِ فردیِ اشخاص[۸]، در چنین مفهومی بسیار وسیع مشخص شده بود (Hongju Koh & Buchwald, 2017: 259)؛ البته باید گفت در خصوص شروع جنگ تجاوزکارانه، این عمل نه‌تنها مشمول «جنایات بین‌المللی» می‌شود، بلکه از آن به‌عنوان بزرگ‌ترین جنایت بین المللی[۹] نیز یاد می‌شود[۱۰] (سودمندی، ۱۳۹۴: ۱۸۹). در اساسنامهٔ دادگاه‌های نورنبرگ و توکیو، عنصر مادی جرم علیه صلح، «شرکت و یا کمک در برنامه‌ریزی یا راه‌اندازی جرم» و عنصر معنوی جرم نیز «آگاهی از این جنایت» مطرح شده بود (Ambos, 2010: 509). معاهدات و اعلامیه‌های رسمی متعددی از زمان جنگ جهانی اول، ازجمله میثاق جامعهٔ ملل (مادهٔ ۱۰) و منشور سازمان ملل متحد (مادهٔ ۳۹)، به‌دنبال منع اَعمال تجاوزکارانه برای تضمین امنیت جمعی بین کشورها، به وجود آمده‌اند. در چنین مواردی جامعهٔ ملل و سازمان ملل متحد معمولاً از رویهٔ دستور آتش‌بس پیروی می‌کنند و دولت را تنها در صورتی متجاوز می‌دانند که آن دستور را رعایت نکند (McDougall, 2021: 81, 82).[۱۱] سرانجام پیشرفت زیادی که در کارگروه ویژهٔ جرم تجاوز[۱]

1. Nuremberg trials, Nov 20, 1945 – Oct 1, 1946
2. Crimes against peace
3. Crimes against humanity
4. Planning
5. Preparation
6. Beginning
7. To launch

۸. شورای امنیت در قضیهٔ تهاجم [تجاوز] عراق به کویت در قطعنامهٔ ۶۷۴ (۱۹۹۰)، بر این مسئولیت اشخاص که مرتکب نقض فاحش کنوانسیون‌های ژنو شده‌اند، تأکید کرده است.

۹. The supreme international crime

۱۰. In “Judicial Decicial, Decisions, International Military Tribunal (Nuremberg), Judgment and Sentences “41 American Journal of International Law (1947), at 186.

۱۱. چنین دستورهای آتش‌بسی، پایان خصومت میان ترکیه و عراق در سال ۱۹۲۵، یونان و بلغارستان در همین سال، پرو و کلمبیا در سال ۱۹۳۳، یونان و همسایگانش در سال ۱۹۴۷، هلند و اندونزی در سال ۱۹۴۷، هند و پاکستان در سال ۱۹۴۸، اسرائیل و همسایگانش در سال ۱۹۴۹، اسرائیل، بریتانیا، فرانسه و مصر در سال ۱۹۵۶ و اسرائیل، اردن و مصر در سال ۱۹۷۰ را نشان می‌دهند. هیچ‌یک از این کشورها در آن زمان متجاوز اعلام نشدند (Ibid: 106)؛ از سوی دیگر، ژاپن در سال ۱۹۳۳ در منچوری، پاراگوئه در منطقهٔ چاکو در سال ۱۹۳۵، کرهٔ شمالی و سرزمین اصلی چین در کره، در سال‌های ۱۹۵۰ و

صورت گرفت و در پیشنهادهای ۲۰۰۹ منعکس شد، دریچه‌ای را برای اولین کنفرانس بازنگری اساسنامهٔ دیوان موسوم به کنفرانس کامپالا، به‌منظور تعریف جنایت تجاوز، گشود. طبق بیانیهٔ این کنفرانس، «جنایت تجاوز، با توجه به قطعنامهٔ شمارهٔ ۳۳۱۴ مجمع عمومی، مجموعه اقداماتی است که از سوی رهبری سیاسی و یا نظامی شکل گرفته و حاوی نقض فاحش و گستردهٔ مقرراتِ منشور ملل متحد است[۲]». در تعریف مذکور، چهار نوع از انواع مشارکت، یعنی طراحی، تدارک، شروع و اجرای عمل تجاوزگونه تبیین شده است (ذاکرحسین، ۱۴۰۱: ۶۰). با توجه به تبیین مفهوم تجاوز، تجاوز سایبری را می‌توان تجاوزی قلمداد کرد که با استفاده از شبکه‌های رایانه‌ای و به‌صورت ایجاد اختلال، نفی، تنزل و یا تخریب اطلاعات موجود در فضای سایبری، در بستر یک حملهٔ سایبری[۳] رخ می‌دهد (اسماعیل‌زاده، ۱۳۹۶: ۵۲). منظور از حملهٔ سایبری، «آسیبی عمدی است که با استفاده از وسایل الکترونیکی و ایجاد اختلال در دسترسی به اطلاعات موجود در کامپیوتر، به یک فرد یا گروهی از افراد بدون در نظر گرفتن سن آنها وارد شود. این آسیب می تواند شامل اَعمال توهین‌آمیز، تحقیرآمیز، زیانبار، تهدیدآمیز، سیاسی و ناخواسته باشد» (Grigg, 2010: 143).

## ۳. دستورالعمل تالین و شناسایی جنایت تجاوز سایبری

دستورالعمل راهنمای تالین[۴] (با عنوان اصلیِ «کتابچهٔ راهنمای تالین دربارهٔ حقوق بین‌المللِ قابل اجرا در جنگ سایبری»[۵]) یک مطالعهٔ آکادمیک و غیرالزام‌آور در خصوص نحوهٔ اعمال قوانین بین الملل (به‌ویژه قانون بین‌المللی حقوق بشردوستانه و حقوق بین‌الملل بشردوستانه) در منازعات سایبری است. بین سال‌های ۲۰۰۹ و ۲۰۱۲، کتاب راهنمای تالین به دعوت مرکز تعالی دفاع سایبری همکاری ناتو، مستقر در تالین، توسط یک گروه بین‌المللی متشکل از حدود بیست متخصص نوشته شد (Efrony & Shany, 2018: 586) و در آوریل ۲۰۱۳، انتشارات دانشگاه کمبریج این راهنما را منتشر کرد. مسئولیت گروه بین‌المللی متشکل از متخصصان در مذاکرات تالین در سال ۲۰۱۷، تبیین چگونگی اِعمال قواعد حقوقی در فضای سایبری و شناسایی ابعاد

---

۱۹۵۱ و اتحاد جماهیر شوروی در مجارستان در سال ۱۹۵۶ متجاوز بودند، زیرا این کشورها دستورهای آتش‌بس را رعایت نکردند (Heller, 2020: 2019).

1. Special Working Group on the Crime of Aggression. (**SWGCA**)
2. ICC-Reviw conference of the Rome Staute cocludes in kampala, Available at https://asp.icc-cpi.int/reviewconference/pressreleaserc/review-conference-of-the-rome-statute-concludes-in-kampala
3. Cyber-Attack
4. The Tallinn Manual
5. Tallinn Manual on the International Law Applicable to Cyber Warfare

منحصر به این فضا بود. قواعدی که در این زمینه استخراج شده‌اند، دارای منشأ حقوق بین‌الملل عرفی و الزام‌آور برای همهٔ دولت‌ها هستند. در سال ۲۰۰۷، کشور استونی هدف یک‌سری از حملات سایبری در بسیاری از وب‌سایت‌های دولتی، مالی و خبری قرار گرفت که به جابه‌جایی مکان برگزاری اجلاس تالین منتهی شد[1] و پس از انجام تحقیقات و رسیدگی، فقط یک دانش آموز ساکن استونی _بنابر شواهد کافی که علیه او جمع‌آوری شده بود_ محکوم شد و در خصوص سایر افراد مهاجم، خاصه کسانی که در حوزهٔ قضایی فدراسیون روسیه سکونت داشتند، محاکمه بسیار دشوار بود (Czosseck, 2011: 183). اکنون که مبنای اصلی حملات تعیین شده است، آیا این حملات به آستانهٔ جنایت رسیده است؟ «جنایت تجاوز الزاماً مستلزم آن است که از منظر چند شاخصهٔ ماهیت[2]، شدت[3] و مقیاس[4]، نقض آشکار منشور ملل متحد باشد» (McDougall, op cit: 96)؛ همچنین آیا تسلط همراه با سوءنیت[5]در فضای سایبر موجود، «تهاجم، الحاق، اشغال نظامی» یا هریک از اقدامات تجاوزکارانهٔ تعریف‌شده در حال حاضر را شامل می‌شوند؟ به‌نظر می‌رسد اجماع فعلی این‌گونه نیست و آسیب‌های وارده به استونی در مقایسه با سایر کشورها، مانند ایالات متحده، که به شبکه‌های سایبری متصل نیستند، نسبتاً محدود بوده است (Shackelford, 2010: 238). اگرچه دولت روسیه هرگونه دخالت مستقیم در حملات سایبری استونی را رد کرد، قابلیت انتساب جزاییِ اقدامات تهاجمی در زمینهٔ جرائم سایبری صورت گرفته و احراز صلاحیت، از سوی دیوان کیفری بین‌المللی کماکان دشوار بود. متعاقب آن ناتو یک مرکز دفاع سایبری را در تالین ایجاد کرد تا بررسی کند واکنش نظامی تئوریک به یک حملهٔ سایبری چه می‌تواند باشد. شدت عملیات سایبری در شناسایی این‌دست عملیات به‌عنوان «جنایت تجاوز» اثرگذار است. مطابق اساسنامهٔ رم، در صورت بروزِ جرائم و حملات سایبری، از آنجا که توسل به زور سایبری محقق شده است، صلاحیت تحقیق، تعقیب و رسیدگی به جنایت تجاوز با مجوز دستورالعمل تالین ممکن است. میزان مسئولیت هر دولت، بر اساس ضوابط مندرج در قاعده‌های ۱۵ و ۱۷ دستورالعمل تالین (مبنی بر اینکه به‌دلیل نقض اصل حاکمیت سایبری، تجاوز سایبری محرز خواهد بود) و نیز نقض فصل هفتم منشور سازمان ملل غیرقابل اغماض است. مطابق با بند ۲ مادهٔ ۸ مکرر اساسنامهٔ رم، اصلاحی ۲۰۱۰، و همچنین مطابق با قطعنامهٔ ۳۳۱۴و نیز قانون ۱۲ دستورالعمل تالین، تنها در صورتی یک عملیات سایبری

1. Rain Ottis, Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective, CCDCOE (Mar. 2, 2008), available on: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf
2. Character
3. Gravity
4 Scale
5. Bad intention

را می‌توان تجاوز محسوب کرد که به آستانهٔ «حملهٔ مسلحانه» رسیده باشد (اشمیت، ۱۳۹۴: ۲۱۳). اگرچه با شکل گرفتن دیوان کیفری بین‌المللی، ایدهٔ عینیت یافتن اصل صلاحیت جهانی[1] برای رسیدگی به مهم‌ترین جنایات بین‌المللی با پیش‌بینی قاعدهٔ تکمیلی بودن[2] صلاحیت دیوان در اساسنامهٔ آن (به این مفهوم که رسیدگی محاکم ملی دارای تقدم است و نه صلاحیت آنها) محقق نشد، لیکن با در نظر گرفتن رویهٔ قضایی بین‌المللی لازم است توجه شود که دایرهٔ صلاحیت جهانی دادگاه‌های داخلی به‌وسیلهٔ حقوق بین‌المللی مشخص می‌شود. البته با توجه به نوع و چگونگی صلاحیت محاکم داخلی به مفهوم قلمرو محفوظ[3]، که همانا قلمرو فعالیت‌های غیر تعهدآور دولت به‌موجب حقوق بین‌الملل است (شایگان، ۱۳۸۰: ۱۲۰)، فرایند محاکمهٔ متجاوزان، به موجب اساسنامهٔ دیوان و تحت شرایط محدود موجود در اساسنامهٔ دیوان، صورت می‌پذیرد.

## ۴. شورای امنیت و تجاوز سایبری

بر اساس منشور ملل متحد، شورای امنیت سازمان ملل متحد مسئولیت حفظ صلح و امنیت بین‌المللی را بر عهده دارد. باید توجه داشت که این مسئولیت در انحصار شورا نیست و بدون شک مجمع عمومی سازمان ملل در این امر صلاحیت دارد. شورای امنیت بر اساس نمایندگی از سوی ملل، مهم‌ترین رکن نظام بین‌المللی برای مدیریت درگیری‌ها و رفع آن، به‌منظور اعادهٔ صلح عمل می‌کند (آقایی و قاسمی، ۱۳۹۲: ۱۱۲) و می‌تواند در زمینهٔ حفظ صلح و امنیت بین‌المللی تصمیماتی اتخاذ کند که برای همهٔ کشورهای عضو سازمان ملل الزام‌آور باشد. این منشور به شورای امنیت این اختیار را می‌دهد که در خصوص گسترهٔ وسیعی از اقدامات، ازجمله تحریم و توسل به زور که ممکن است برای حفظ یا بازگرداندن صلح و امنیت بین‌المللی ضروری باشد، تصمیم‌گیری کند (لنتنر، ۱۳۹۸: ۲۳۹). شورا می‌تواند چنین تصمیماتی را در مواردی اتخاذ کند که مطابق با مادهٔ ۳۹، «وجود هرگونه تهدید علیه صلح، نقض صلح یا اقدام تجاوزکارانه» را تشخیص دهد. اِحراز تجاوز سایبری، پیش‌شرط هر اقدام شورای امنیت است؛ زیرا اساساً شورا به منظور حفظ صلح و امنیت بین‌المللی مطابق با مواد ۴۱ و ۴۲ منشور، باید در ابتدا وجود یک عامل را که منجر به تهدید صلح یا عامل نقض صلح است، شناسایی کرده، یا تجاوز را احراز کند.[4] البته چنین پیش‌شرطی به معنای انحصاری بودن صلاحیتِ شورا نیست (Blokker, 2007: 872) و مطابق با مادهٔ ۲۴ منشور، شورای امنیت در چنین صلاحیتی دارای تقدم است، لیکن نمی تواند از دیگر مراجع ذی‌صلاح ملل متحد در این حوزه را سلب صلاحیت کند (Escarameia,

1. Universal jurisdiction or global jurisdiction
2. Complementarity
3. Domaine reserve

۴. مادهٔ ۳۹ منشور سازمان ملل متحد.

2017: 93). با درنظرگرفتن چنین وضعیتی، اگر شورای امنیت یک عملیات سایبری را عامل نقض صلح تلقی کند، ولی اقدام تجاوزکارانه را احراز نکند، لزوماً نمی‌توان نتیجه گرفت که تجاوز رخ نداده است، زیرا «بعضاً شورای امنیت به‌واسطهٔ برخی انگیزه‌های سیاسی، تفسیری متفاوت را ارائه می‌کند» (Akande, 2008: 311)؛ در این صورت، مجمع عمومی با دارا بودن مسئولیت ثانویه (مشترک) در چارچوب اختیارات عام، می‌تواند ورود کند (شایگان‌فرد، ۱۳۸۷: ۲۷۲). چنین نگاهی با بند ۱ مادهٔ ۲۴ و «عبارت مسئولیت اولیه» مطابقت دارد، زیرا واژهٔ «اولیه» صرفاً به تقدم زمانی مرتبط نیست، بلکه بر تقدم ماهوی نیز دلالت دارد» (Dinstein, 2017: 253)؛ به‌عنوان مصداق، اخیراً قطعنامهٔ مجمع عمومی سازمان ملل متحد ES-11/1 با عنوان «تجاوز به اوکراین»[1]، در ۲ مارس ۲۰۲۲، به تصویب رسید.[2] این مکانیسم در سال ۱۹۵۰ با قطعنامهٔ «اتحاد برای صلح»[3] معرفی شد که اعلام کرد: «اگر شورای امنیت به‌دلیل عدم اتفاق آرای اعضای دائمی، در هر موردی که به‌نظر می‌رسد تهدیدی برای صلح، نقض صلح یا اقدامی دربارهٔ تجاوز باشد، مسئولیت اصلی خود را برای حفظ صلح و امنیت بین‌المللی انجام ندهد، مجمع عمومی فوراً موضوع را با هدف ارائهٔ توصیه‌های مناسب به اعضا برای اقدامات دسته‌جمعی، ازجمله در باب نقض صلح یا اقدام تجاوزکارانه، استفاده از نیروی مسلح، در صورت لزوم، برای حفظ یا بازگردانی صلح و امنیت بین‌المللی بررسی می‌کند».

از سوی دیگر، دیوان دادگستری بین‌المللی، به این دلیل که مجمع عمومی در ارتباط با بودجهٔ ملل متحد حق تصمیم‌گیری دارد، به این نتیجه رسیده است که مطابق با مادهٔ ۲۴ منشور، مسئولیت شورای امنیت در بحث احراز تجاوز سایبری یک مسئولیت انحصاری نیست و مجمع عمومی نیز در بحث حفظ صلح و امنیت بین‌المللی مسئول است. همچنین مجمع عمومی در بحث تجاوزهای سایبری، علاوه‌بر داشتن حق احراز تجاوز، می‌تواند اقدامات عملی خاصی را توصیه کند. در سال ۱۹۶۲، نظر مشورتی دیوان بین‌المللی دادگستری بیان کرد: «درحالی‌که اقدامات اجرایی[4] در حوزهٔ انحصاری شورای امنیت است، مجمع عمومی صلاحیت اتخاذ طیف وسیعی از تصمیمات، ازجمله ایجاد یک نیروی حافظ صلح، را دارد» (Binder, 2017: 106). نکتهٔ دیگر این است که محرز نشدن تجاوز از سمت شورای امنیت، به‌منزلهٔ الزام یک نهاد قضایی دیگر نسبت به عدم احراز نخواهد بود (دارابی‌نیا و فروغی‌نیا، ۱۳۹۴: ۱۶۸) و از همین رو دادستان دیوان بر

1. Aggression against Ukraine: resolution / adopted by the General Assembly

۲. این قطعنامه در نشست ویژهٔ اضطراری مجمع عمومی به تصویب رسیده است. نشست ویژهٔ اضطراری یک نشست برنامه ریزی‌نشدهٔ مجمع عمومی سازمان ملل متحد برای ارائهٔ توصیه‌های فوری در خصوص یک وضعیت خاص مربوط به حفظ صلح و امنیت بین‌المللی در هر موردی است که شورای امنیت به‌دلیل وتوی یک عضو دائمی اقدام نکند.

3. The Uniting for Peace resolution: United Nations General Assembly Resolution 377

4. Enforcement measures

اساس احراز وقوع تجاوز سایبری توسط مجمع عمومی نیز می‌تواند شروع به تحقیق در خصوص جنایت موصوف کند (میرمحمد صادقی، ۱۴۰۰: ۲۷۸) که این عمل هم در راستای اقدام شورای امنیت معتبر است.

## ۵. ارتباط شورای امنیت و دیوان در تجاوز سایبری

در یک نگاه کلی رابطهٔ شورای امنیت و دیوان در مواد ۵ و۱۳ و ۱۶ تصریح شده است؛ دو دیدگاه در خصوص رسیدگی به جنایت تجاوز توسط دیوان وجود دارد؛ یکم: باور به «صلاحیت انحصاری» شورای امنیت و دوم: باور به «صلاحیت اولیه» و نه انحصاری آن و بنابراین، این باورِ دوم است که مبنای کار دیوان در امر رسیدگی به جنایت مزبور قرار می‌گیرد (Petty, 2008: 13). شورای امنیت به استناد بند ۲ از مادهٔ ۱۳ اساسنامهٔ رم و به موجب فصل هفتم منشور ملل متحد، باید وضعیتی را که در آن جنایت رخ داده (صرف‌نظر از مخدوش کردن اصل رضایت دولت‌ها)، به دادستان ارجاع دهد (Pellrt, 2002: 1080)؛ البته درصورتی‌که شورای امنیت بخواهد می‌تواند دیوان کیفری بین‌المللی را از رسیدگی به جنایت تجاوز منع کند و در صورت احراز تجاوز، با توجه به صلاحیت خود، به تصمیمات شِبه‌قضایی نظیر تعیین مجازات متجاوز اقدام کند (شایگان، ۱۳۸۰: ۱۹۷). شورای امنیت درصورتی‌که جنایت را تجاوز به‌شمار نیاورد، می‌تواند دعوی مرتبط با آن را به حالت تعلیقِ تعقیب یا تعلیقِ تحقیق درآورد. در این صورت دیوان به مدت دوازده ماه قادر به رسیدگی در این زمینه نخواهد بود که البته این مدت از سوی شورای امنیت قابل تمدید است (O'Connell and Niyazmatov, 2012: 196). با وجود این باید توجه داشت که در عمل، چنین منعی از سوی شورای امنیت بسیار بعید است، زیرا برای صدور چنین قطعنامه‌ای لازم است که اتفاق اعضای دائم شورا موافق باشند. نگاهی به رویهٔ شورا در سالیان گذشته نشان می‌دهد که دسترسی به چنین اجماعی بسیار دشوار است. از ژانویهٔ ۲۰۱۷ به بعد، پس از فعال شدن صلاحیت دیوان در خصوص جنایت تجاوز، شورای امنیت و دیوان به روش‌های مختلفی تعامل دارند (Ruys, 2018: 890):

- شورای امنیت بر اساس فصل هفتم منشور و طبق مادهٔ ۳۹ آن، در مواردی که تهدیدی علیه صلح و امنیت بین‌المللی وجود دارد، دست به اقدامات مسالمت‌آمیز و در نهایت قهرآمیز می زند. در این اثنا، مطابق مادهٔ ۱۶ اساسنامهٔ دیوان، به شورا «حق وتوی موقت» در خصوص اِعمال صلاحیت دیوان اعطا شد (حجازی و صلح‌چی، ۱۳۹۹: ۱۵).

- شورای امنیت می‌تواند وضعیتی را به دیوان کیفری بین‌المللی ارجاع دهد که این اختیار را داشته باشد تا دربارهٔ هر چهار جنایت تحت اساسنامهٔ رم، از جمله جنایت تجاوز، بدون هیچ

شرط دیگری تحقیق کند.[1] اختیارات شورای امنیت بر اساس منشور ملل متحد، مبنای قانونی دارد که بر اساس آن دیوان کیفری بین‌المللی می‌تواند چنین جنایاتی را بدون نیاز به رضایت دولت‌های درگیر بررسی کند.

- در مواردی که دادستان رأساً[2] تحقیقات را آغاز می‌کند، یا زمانی‌که وضعیتی از سوی یک دولت عضو ارجاع می‌شود، دادستان باید به شورای امنیت در خصوص تحقیقات اطلاع دهد و به شورای امنیت مهلت شش‌ماهه بدهد تا بروز یک عمل تجاوزکارانه را احراز کند. اگر شورای امنیت ظرف شش ماه عمل تجاوزکارانه را احراز نکند، دادستان تنها در صورتی می‌تواند اقدام کند که قضات بخش مقدماتی دادگاه[3] اجازه دهند. اوکامپو ادعا می‌کند که جدید بودن رژیم حقوقی دیوان کیفری بین‌المللی، آن را از محدودهٔ شورای امنیت یا از هوس‌های ایالات متحده خارج کرده است (Ocampo, 2009: 13).

- شورای امنیت همچنین می‌تواند تحقیقات در خصوص جنایت تجاوزکاری را طبق مادهٔ ۱۶ اساسنامهٔ رم، به مدت یک سال تعلیق کند. این ماده به‌طور یکسان دربارهٔ هر چهار جنایت اصلی تحت اساسنامهٔ رم اعمال می‌شود.

- تصمیم شورای امنیت در خصوص عمل تجاوزکارانه، طبق مادهٔ ۳۹، برای دیوان کیفری بین‌المللی الزام‌آور نیست. این نکته از اصول دادرسی اساسنامهٔ رم برمی‌آید و به‌صراحت در مواد ۱۵ bis و ۱۵ ter تأیید شده است؛ بنابراین، دیوان به‌طور کامل استقلال قضایی خود را در برابر شورا حفظ می‌کند، زیرا باید ارزیابی خود را در باب وقوع تجاوز انجام دهد.

بر خلاف دادستان‌های بین‌المللی دادگاه‌های «توافقی» که موقعیت‌های انتخاب‌شده از سوی سیاستمداران به آنها ارجاع می‌شد، دیوان کیفری بین‌المللی از استقلال برای انتخاب موقعیت‌ها جهت تحقیق برخوردار است. اوکامپو توضیح می‌دهد که نقش شعبهٔ مقدماتی PTE برای تأیید قضایی انتخاب یک موقعیت برای تحقیق و به‌منظور ترویج بی‌طرفی انجام گرفته است (Ocampo, 2009: 14). وقتی صحبت از ارجاعات توسط شورای امنیت به میان می‌آید، دادستان وظیفه دارد تحقیقات را آغاز کند، اما اختیار دارد که پس از بررسی اولیه نتیجه‌گیری کند که مبنای منطقی برای ادامه وجود ندارد (Scafferling, 2012: supra note 62 at 152). در مقابل، استدلال می‌شود که اختیار دادستانی تحت اساسنامهٔ رم با وظایف و اختیارات شورای امنیت سازگار نیست (Ohlin, 2009: 83). ادعا می‌شود که دادستان حق ندارد از انجام یک بررسی مقدماتی، با تشخیص اینکه هیچ مبنای معقولی برای ادامه وجود ندارد، امتناع کند؛ این استدلال پذیرفتنی نیست، زیرا دیوان خارج از قلمرو سازمان ملل تشکیل شده است.

1. Article 15 ter Rome Statute; Article 13 (b) Rome Statute
2. proprio motu
3. Court's Pre-Trial Division

عملیات سایبری باید در قلمرو یا توسط تبعهٔ یکی از کشورهای عضو دیوان انجام شود. این الزام توسط مادهٔ ۱۲ (۲) اساسنامهٔ رم مقرر شده است. پیوند صلاحیت سرزمینی[1]، مشکلات غیرقابل‌حلی را در زمینهٔ سایبری ایجاد نمی‌کند. برخلاف آنچه در نگاه اول به‌نظر می‌رسد، فضای سایبری حوزه‌ای نیست که حاکمیت سرزمینی و صلاحیت قضایی دولت در آن اعمال نشود؛ در واقع، یک حملهٔ سایبری از دو لایهٔ فیزیکی و ترکیبی (یا منطقی) تشکیل شده است: لایهٔ اول شامل زیرساخت فیزیکی است که داده‌ها از طریق آن، به‌صورت سیمی یا بی‌سیم حرکت می کنند. سرورها، روترها، ماهواره‌ها، کابل‌ها، سیم‌ها و رایانه‌ها در این لایه قرار دارند؛ لایهٔ دوم شامل پروتکل‌هایی است که به داده‌ها اجازه می‌دهند تا مسیریابی و درک شوند، همچنین نرم افزار مورد استفاده و خود داده‌ها نیز در این لایه قرار دارند؛ بنابراین دیوان بین‌المللی کیفری زمانی می‌تواند صلاحیت قلمرو خود را اعمال کند که جزء فیزیکی مورد حمله، در قلمرو یک دولت عضو واقع شده باشد. با این حال، هنوز بحث این است که آیا همهٔ انواع آثار زیانبار مربوط به ایجاد صلاحیت قضایی هستند یا فقط آسیب فیزیکی؟

## ۶. قطعنامه‌های شورای امنیت و دیوان علیه جنایت تجاوز

قطعنامه‌های شورای امنیت اگرچه در برخی موارد دارای ماهیتی تشویقی و پند و اندرزی[2] هستند (Gruenberg, 2009: 469)، فی‌الواقع تصمیمات و اقداماتی قهری[3] هستند که علیه یک دولت اتخاذ می‌شوند که این تکلیف در متن قطعنامه‌های صادره، با واژهٔ Urges به معنای «فرامی خواند» [مکلف می‌کند] بیان می‌شوند، ولیکن رعایت قواعد بنیادین حقوق بین‌الملل، نظیر احترام به حاکمیت دولت‌ها، مدنظر شورا قرار دارد (Frowein, 2004: 167) و این مهم در متن قطعنامه های صادره با واژهٔ Recognizing به معنای «با درک اینکه» مشخص و معین می‌شود. گرچه مسئولیت اولیهٔ احراز وقوع عمل تجاوزکارانه به شورای امنیت اعطا شده است، ولی این واقعه یک مسئولیت انحصاری نیست. صدور قطعنامه‌های شورای امنیت به‌صورت بی‌طرفانه و بر پایهٔ مادهٔ ۴۱ منشور و فصل هفتم آن صورت می‌گیرد و حداقل در یک مورد شورای امنیت نشان داده که امتیازات اعطاشده به آن را می‌توان به یک نهاد بی‌طرف واگذار کرد، هرچند این امر بر اساس ارادهٔ شورای امنیت است. صدور قطعنامهٔ ۶۸۷ شورای امنیت (Scott, 2010: 111) و یا قطعنامهٔ ۵۹۸ شورای امنیت سازمان ملل متحد در خصوص ایران و عراق، صدور قطعنامهٔ ۸۲۷ ذیل فصل هفتم و مادهٔ ۲۹ منشور ملل متحد، به تأسیس دادگاه کیفری بین‌المللی برای یوگسلاوی[4] در سال

1. The territorial jurisdictional link
2. Exhortatory
3. Enforcement Measures

۱. به‌عنوان رکن فرعی شورای امنیت و با صلاحیت اجباری Juridiction Obligatoir

۱۹۹۳ (شایگان، ۱۳۸۰: ۲۰۳) تصمیم گرفت تا نسبت به تعقیب افرادی که مرتکب نقض‌های شدید حقوق بشردوستانه در قلمروی سرزمینی یوگسلاوی سابق از ابتدای سال ۱۹۹۱ میلادی شده بودند، اقدام کند (Bassiouni, 1994: 786). این نخستین محکمهٔ بین‌المللی برای رسیدگی به مرتکبان جرائم بین‌المللی بعد از تشکیل محاکم نظامی بین‌المللی نورنبرگ و توکیو بود. در زمینهٔ تجاوز سایبری نیز، اعضای شورا توافق دارند که اجرای هنجارهای موجود، به رفتار مسئولانهٔ دولت در فضای سایبری و اقدامات اعتمادسازی و ظرفیت‌سازی، به حداقل رساندن بی‌اعتمادی بین کشورهای عضو و ثبات در حوزهٔ سایبری کمک می‌کند. یکی از مهم‌ترین قطعنامه‌های شورای امنیت در زمینهٔ تجاوز سایبری، قطعنامهٔ ۲۳۴۱ (۲۰۱۷) است. در یک بحث اختصاصی، شورای امنیت در ۱۳ فوریهٔ ۲۰۱۷ از کشورهای عضو خواست تا به خطر حملات تروریستی علیه زیرساخت‌های حیاتی رسیدگی کنند. شورا از طریق قطعنامهٔ ۲۳۴۱ خود که در همان تاریخ به تصویب رسید، کمیتهٔ مبارزه با تروریسم خود را با حمایت ادارهٔ اجرایی کمیتهٔ مبارزه با تروریسم[1] هدایت می‌کند تا تلاش‌های کشورهای عضو برای محافظت از زیرساخت‌های حیاتی در برابر حملات تروریستی را بررسی کند. در مقدمهٔ قطعنامه چنین آمده است: «کشورهای عضو می توانند تصمیم بگیرند که چه چیزی را زیرساخت حیاتی در نظر بگیرند. امنیت سایبری یکی از «جریان تلاش‌ها» برای حفاظت است. ارتقای آگاهی نسبت به تهدیدات و آسیب‌پذیری‌های تروریست سایبری از طریق گفت‌وگوی منظم محلی، آموزش و اطلاع‌رسانی، نقش حیاتی دارد[2]». در ۲۶ اوت ۲۰۲۰، اندونزی یک جلسه را در خصوص «تجاوز سایبری علیه زیرساخت‌های حیاتی» ترتیب داد تا آگاهی را دربارهٔ آسیب‌پذیری و نیاز به حفاظت از زیرساخت‌های حیاتی در برابر چنین حملاتی افزایش دهد (Roshanaei, 2021: 86).[3]

در خصوص نقش شورای امنیت سازمان ملل متحد و پذیرش صلاحیت دیوان کیفری بین‌المللی در خصوص جنایت تجاوز سایبری، چهار ترکیب می‌تواند وجود داشته باشد (Barriga & Blokker, 2017: 623): ۱. پذیرش صلاحیت دیوان کیفری بین‌المللی به‌علاوهٔ فیلتر شورای امنیت؛ ۲. عدم لزوم پذیرش صلاحیت دیوان کیفری بین‌المللی توسط دولت متجاوز، به‌علاوهٔ

1. Counter-Terrorism Committee Executive Directorate (CTED)
2. The UN Security Council Resolution 2341 (2017)

۴. در این جلسه، چگونگی اثرگذاری هنجارهای رفتار مسئولانهٔ دولت در فضای سایبری در محافظت از زیرساخت‌های حیاتی و اثر آن بر حفظ صلح و امنیت بین‌المللی بررسی شد، درحالی‌که اکثر اعضای شورا کاربرد حقوق بین‌الملل در فضای سایبری را در زمان صلح به رسمیت می‌شناختند، اختلاف‌هایی بر سر کاربرد آن در زمان درگیری‌های مسلحانه وجود داشت. اگرچه چنین اهمیت افزایش آگاهی شورا را در خصوص تهدیدات سایبری علیه صلح و امنیت بین‌المللی، از جمله فناوری‌های نوظهور، تشخیص داده است، اما نشان داد که شورا باید بااحتیاط با این موضوع برخورد کند و استدلال می‌کند که چندین سؤال مربوط به «تعریف و دامنه» بی‌پاسخ مانده است.

فیلتر شورای امنیت؛ ۳. پذیرش صلاحیت دیوان کیفری بین‌المللی توسط دولت متجاوز، به‌علاوهٔ فیلتر شورای امنیت و ۴. عدم لزوم پذیرش صلاحیت دیوان کیفری بین‌المللی توسط دولت متجاوز و عدم فیلتر شورای امنیت[1].

به‌منظور همکاری بهتر دیوان کیفری بین‌المللی در زمینهٔ تجاوز سایبری، افزودن اقدامات سایبری به فهرست اعمال تجاوزکارانه، با عملیاتی شدن جرم تجاوزکارانه مناسب خواهد بود. ازاین‌رو اقدامات سایبری باید به اقدامات تجاوزکارانهٔ مندرج در مادهٔ ۸ bis (۲) اساسنامه افزوده شود؛ بنابراین بند (h) جدید مادهٔ ۸ مفاد بند ۲ به شرح زیر خواهد بود:

*استفاده از اقدامات سایبری برای اهداف توهین‌آمیز که به‌طور چشمگیری سبب اختلال یا تخریب نهادهای دولتی، نظامی، تجاری، فرهنگی یا رسانه‌ای یا سایر فعالیت های اجتماعی در کشور دیگر شود.*

در این صورت، دادستان و قضات دیوان بین‌المللی کیفری باید تعیین کنند که آیا الزامات زمینه‌ای «ماهیت، شدت و مقیاس» برای یک عمل تجاوزکارانه و درنتیجه جنایت تجاوزکارانه برآورده شده است یا خیر؟ چنین فیلتر محکمی، تنها فاحش‌ترین حملات سایبری در سراسر مرزها را زیر نظر دیوان باقی می‌گذارد.

## ۷. ماهیت کارکرد قطعنامه‌های شورای امنیت علیه جنایت تجاوز

بعد از شکست جامعهٔ ملل، روابط حاکم میان کشورها با رعایت اصل احترام به حاکمیت دول (صرف‌نظر از وجود معاهدهٔ منع تجاوز[2] که اصل اجتناب‌ناپذیرِ حفظ تعامل حاکمیت دولت‌هاست) به سازمان ملل متحد این امکان را داد که با ایجاد ضمانت اجرای کافی و مؤثر جلوی تجربهٔ مجدد ناتوانی جامعهٔ ملل را بگیرد. این مهم ابتدا با صدور قطعنامه‌های مجمع عمومی به‌صورت غیر لازم‌الاجرا و سپس با صدور قطعنامه‌هایی با رویکرد حفظ صلح و امنیت بین‌المللی و از همه مهم‌تر مطابق فصل هفتم منشور «اعادهٔ وضعیت[3] به حالت سابق»[4] در صورت بروز نقض، توسط شورای امنیت با جایگاه حافظ حقوق اساسی جامعهٔ بین‌المللی (شایگان، ۱۳۸۰: ۴۱)، ماهیت لازم الاجرا بودن را به‌دست آورد. بر همین پایه، قطعنامهٔ ۱۸ژانویهٔ ۱۹۹۸ با عنوان «اعلامیهٔ دربارهٔ پیشگیری و رفع اختلافات که می‌تواند صلح و امنیت بین‌المللی را تهدید کند و نقش سازمان ملل متحد در این زمینه» صادر شد.[5] نظریهٔ مسئولیت حمایت، مبنا و اساس عملکرد شورای امنیت

1. Illustrative Chart on Conditions for the Exercise of Jurisdiction, Icc-Asp/8/20/Add.1
2. Pact of non - aggression
3. SC.Res.678(1990),29Nov
4. Restitution integrum = re-establishment
5. GA.Res.43/51

است که در قطعنامهٔ ۱۶۷۴ مصوب سال ۲۰۰۶ تصریح شد. این نظریه مبتنی بر سه نوع مسئولیت برای شورا خواهد بود: الف) از فصل ششم منشور، مسئولیت پیشگیری[۱]؛ ب) از فصل هفتم منشور، مسئولیت واکنش[۲] و ج) از فصل هشتم منشور، مسئولیت بازسازی[۳]، با وجود تعدد حوزه‌های قطعنامه‌های صادرهٔ شورای امنیت[۴]، تخصیص امر در حوزهٔ جنایت تجاوز، با یک رویکرد امکانِ مصداق‌یابی[۵] و اتخاذ سیاست جنایی بین‌المللی انبساطی[۶] روبه‌روست. نخستین قطعنامه با شمارهٔ ۲۵ در سپتامبر ۱۹۹۱، در قالب وضعیت «تهدید امنیت به صلح و امنیت بین المللی» مطرح شد. همین وضعیت در قطعنامهٔ ۶ اکتبر ۱۹۹۲ تأکید شد. بر این واقعه قطعنامهٔ ۲۲ فوریه ۱۹۹۳، به وضعیت «نقض فاحش و همه‌جانبهٔ حقوق بشردوستانهٔ بین‌المللی که تهدید علیه صلح و امنیت» تسری پیدا کرد. هدف اصلی صدور قطعنامه به مفهوم واکنش بین‌المللی به امر جنایت تجاوز، خاصه جنایت تجاوز سایبری، تضمین تعرض‌ناپذیری مرزها و حاکمیت دولت‌ها بود. با توجه به قطعنامهٔ مجمع عمومی سازمان ملل متحد در سال ۱۹۲۷، که با عنوان «کنفرانس پان‌امریکن ۱۹۲۸» مفهوم‌یابی شد، عرف بین‌الملل به‌اندازهٔ کافی گسترش یافت تا جرم تجاوز را «جنایت بین‌المللی» محسوب کند.[۷] شورای امنیت با توجه به بروز جنایت بین‌المللی، در خصوص تجاوز به‌طور اعم، و نیز در خصوص جنایت تجاوز سایبری به‌طور اخص، با تأکید بر راه‌حل به کارگیری «تفسیر پویا و هدف‌گرایانه»[۸] (Orakhelashvili, 2005: 25)، باید نسبت به ایجاد دادگاه و یا اعطای صلاحیت به دیوان کیفری بین‌المللی، به‌موجب فصل هفتم منشور، عمل کند (شایگان، ۱۳۸۰: ۲۱۰).[۹] بدیهی است اصل تفسیر قانون که در حکم قانون است، می‌تواند مؤید این ادعا باشد.[۱۰] شورای امنیت در چارچوب وظیفهٔ پیشگیرانهٔ خود، مبتنی بر جرم‌شناسی امنیت‌مدار (ابرندآبادی، ۱۳۹۱: ۱۱۰)، و نیز مطابق UN DOC. S/25266,10 Feb. 1993, Para34 وظیفهٔ حفظ

1. Responsibility to prevent
2. Responsibility to react
3. Responsibility to rebuild

۴. صرف‌نظر از سیاسی بودن این نهاد و نیز وجود شُبهات در خصوص عدم صلاحیت تقنینی در عرصهٔ بین‌المللی (شایگان، ۴۲:۱۳۸۰) آن، مطابق مادهٔ ۲۵ منشور ملل متحد، قطعنامهٔ صادرهٔ شورای امنیت برای همگان الزام‌آور است. Resolotion RC/RES.6,Article15 bis para3

۵. با توجه به تمثیلی بودن موارد مصرح در قطعنامهٔ ۳۳۱۴ و نیز مطابق بند ۲ مادهٔ ۸ مکرر اساسنامهٔ رم اصلاحی سال ۲۰۱۰.

6. International expaniobary criminal policy

۷. شورای امنیت دو قطعنامهٔ ممانعت‌کننده در خصوص اِعمال صلاحیت دیوان، مستنبط از مادهٔ ۱۶ اساسنامه صادر کرده است (Burchill, 1996: 86): اولی) قطعنامهٔ S/RES/1422(2002) با موضوع منع اِعمال صلاحیتِ یک‌ساله برای دولت‌های غیر عضو که در عملیات حفظ صلح در بوسنی‌وهرزگوین شرکت کرده بودند؛ دومی) قطعنامهٔ S/RES/1487(2003) با موضوع تمدید یک سال دیگر قطعنامهٔ ۱۴۲۲.

8. Dynamic and objective description

۹. ر.ک: UN DOC.S/25266,10Feb.1993,PARA.34

10. Legis interpretatio legis vim obtinet

صلح و امنیت بین‌المللی سایبری را بر عهده دارد. از طرف دیگر تعهد دولت‌های عضو کنوانسیون های چهارگانهٔ ژنو، مطابق مادهٔ ۱ مشترک آن کنوانسیون‌ها و پروتکل ۱ منضم به آنها، مبنی بر اطاعت‌پذیری از شورای امنیت را موجب می‌شود. بر این اساس ایجاد دادگاه اختصاصی یا ارجاع امر به دیوان کیفری بین‌المللی، در قالب اقدامی متقابل از نوع Actio popularis در مقابل متجاوز جنایت تجاوز (به‌طور اخص متجاوز جنایت سایبری)، برای مقابله با نقض قواعد آمره Erga Omnes میسر می‌شود (شایگان، ۱۳۸۰: ۲۱۲).

## ۸. تصمیم فعال‌سازی

در سال ۲۰۱۷، مجمع کشورهای عضو با اجماع، قطعنامه‌ای را برای فعال کردن صلاحیت دیوان در خصوص جنایت تجاوز (تصمیم فعال‌سازی[1]) به تصویب رساند (Claus, 2019: 60) که تأیید می‌کند دربارهٔ ارجاع دولت یا تحقیقات مقتضی دادگاه صلاحیت خود را در خصوص جنایت تجاوز، هنگامی‌که توسط یک تبعه یا در قلمرو کشور عضوی که این اصلاحات را تصویب یا نپذیرفته است انجام گیرد، اعمال نخواهد کرد. تأثیر حقوقی تصمیم فعال‌سازی به‌عنوان ابزاری معتبر برای تفسیر اساسنامهٔ رم کاملاً روشن نیست. البته با استخراج اصول عمومی حقوق بین‌الملل مستند به بند ۳ مادهٔ ۲۱ اساسنامهٔ رم که نباید متناقض با حقوق بشرِ شناخته‌شدهٔ بین‌المللی باشد، باید قصد اصلی و صریح آن در تفسیر قلمرو صلاحیت، همواره با تحدید اختیارات دیوان همراه باشد، لیکن در مقام عمل به استناد فصل هفتم منشور ملل متحد و حسب نقض صلح و امنیت (سایبری) باید حیطهٔ صلاحیت رسیدگی دیوان کیفری بین‌المللی را توسعه داد (آل‌حبیب و ارسنجانی، ۱۳۸۳: ۳۹۷). این سؤال مطرح می‌شود که آیا بر اساس مادهٔ ۳۱ (۳) (الف) کنوانسیون وین در خصوص حقوق معاهدات[2]، تصمیم فعال‌سازی یک توافق بعدی بین طرفین دربارهٔ تفسیر اساسنامهٔ رم است یا خیر. این وظیفهٔ مترجم، یعنی دادگاه است که هنگام تفسیر اساسنامهٔ رم، به تصمیم فعال‌سازی اهمیت بدهد (Claus, 2019: 64). با این حال، شاید دیدگاه بهتر این باشد که تصمیم فعال‌سازی یک قانون سازمانی است که توسط مجمع کشورهای عضو صادر می‌شود و به این ترتیب، بر کنوانسیون وین در باب حقوق معاهدات غالب بوده، از نظر قانونی برای ارگان‌های دیوان الزام‌آور است؛ بنابراین، رژیم صلاحیتی جرم تجاوز در صورت ارجاعات دولتی و تحقیقات مقتضی، تنها پس از تصویب یا پذیرش توسط هر دو کشور متجاوز و قربانی ادعاشدهٔ عضو، قابل اعمال است.

1. Activation Decision
2. Vienna Convention on the Law of Treaties

## ۹. نتیجه

با امعان نظر به صراحت مادهٔ ۲۵ منشور ملل متحد، مبنی بر الزام‌آور بودن قطعنامه‌های صادره از سوی شورای امنیت برای جامعهٔ بین‌المللی، کلیهٔ کشورهای عضو و حتی غیر عضو اساسنامهٔ رم، با ارجاع دادن وضعیتی مبنی بر بروز جنایت به دیوان توسط شورای امنیت توافق دارند. بر این اساس، طبق مادهٔ ۱۵، دیوان کیفری بین‌المللی می‌تواند صلاحیت خود را در خصوص جرم تجاوز ناشی از عمل تجاوزکارانهٔ ارتکاب‌یافته توسط هر کشور، ازجمله دولت‌های غیر عضو، اِعمال کند. اساسنامهٔ رم با عرصهٔ سایبری به لحاظِ امکان نقض صلح و امنیت بین‌المللی سایبری دارای ارتباط است و این ارتباط وفق دستورالعمل تالین، در صورت رسیدن اقدامات قهرآمیز سایبری به آستانه‌های مطروحه، نظیر آستانهٔ «حملهٔ مسلحانه» در تجاوز سایبری، و همچنین وجود مسئولیت کیفری فردی در هر دو سند اساسنامهٔ دیوان و تکالیف موجود در دستورالعمل تالین ۲۰۱۷، تصریح شده است و صدور قطعنامه‌های تعهدآور و الزامی شورای امنیت نیز آن را عملیاتی می سازد، لیکن مانند بسیاری از (یا همهٔ) قوانین بین‌المللی، گفتن اینکه دربارهٔ عملیات سایبری اعمال می‌شود، صرفاً قدم اول است. جزئیات این اعمال و تعیین دقیق نحوهٔ اعمال آن، کلید پیشرفت به‌سوی یک نظام بین‌المللی باثبات‌تر و قابل پیش‌بینی‌تر خواهد بود. دو راه برای گسترش صلاحیت جنایات تجاوزکارانه سایبری وجود دارد: اولاً) کشورهای دیگرِ عضو اساسنامهٔ رم می‌توانند اصلاحیهٔ جنایت تجاوز را تصویب کنند؛ ثانیاً) صلاحیت جرم تجاوز در سال ۲۰۲۵ توسط دولت‌های عضو بررسی می‌شود. دولت‌ها در سطح ملی، می‌توانند بازنگری رژیم قضایی را با رویکرد مطابقت آن با سایر جنایات اساسنامهٔ رم و مباحث مرتبط با جرائم سایبری در نظر بگیرند.

جامعهٔ بین‌الملل در سطح فراملی و بین‌المللی با تمسک به ماهیت و مأموریت شورای امنیت و نظر به بند ۳ مادهٔ ۲۱ اساسنامهٔ رم، که نباید متناقض با حقوق بشر بین‌المللی باشد، با حفظ صلاحیت دیوان، مطابق تصریح اساسنامهٔ آن مبتنی بر تحدید اختیارات آن مرجع، در مقام عمل و به استناد فصل هفتم منشور ملل متحد و حسب ضرورتِ ممانعت از بروز نقض صلح و امنیت (سایبری) و در صورت وقوع، فوریت در اعادهٔ وضع به حال سابق، که همان صلح و امنیت سایبری در سطح بین‌المللی است، امکان توسعهٔ صلاحیت دیوان کیفری بین‌المللی در امر رسیدگی مبتنی بر قطعنامه‌های صادره از سوی شورای امنیت وجود خواهد داشت. همچنین اصلاح اساسنامهٔ دیوان برای اجازه دادن به ارجاعات مجمع عمومی ارزشمند است و در عین حال چارچوبی را برای پرونده‌های آینده تضمین می‌کند. باید توجه داشت که اصلاح اساسنامه اگرچه لازم است، لیکن کافی نیست؛ زیرا چالش‌های اصلی مربوط به تعریف جنایات یا قوانین مربوط به حقوق بین‌الملل بشردوستانه نیست، بلکه به موانع فنی شناخته‌شده برای شناسایی عاملان و جمع

آوری شواهد مربوط می‌شود. افزودن اقدامات سایبری به فهرست اعمال تجاوزکارانه با عملیاتی شدن جنایت تجاوزکارانه مناسب خواهد بود.

## منابع

### الف) فارسی


۱. آقایی، سید داود و قاسمی، فائزه (۱۳۹۲). راهکار پیشنهادی برای اصلاح شورای امنیت سازمان ملل. *فصلنامهٔ سیاست*، دانشکدهٔ حقوق و علوم سیاسی، تهران، ۴۳(۳)، ۱۲۲-۱۰۷.

۲. آل‌حبیب، اسحاق و ارسنجانی، ماه‌نوش (۱۳۸۲). *دیوان کیفری بین‌المللی و جمهوری اسلامی ایران، «اساسنامهٔ دیوان کیفری بین‌المللی رم»*. چ هشتم، تهران: مرکز چاپ و انتشارات وزارت امور خارجه.

۳. اسماعیل‌زادهٔ ملاباشی، پرستو (۱۳۹۶). حملهٔ سایبری به‌مثابهٔ جنایت تجاوز و بررسی صلاحیت دیوان کیفری بین‌المللی در رسیدگی به آن. *مجلهٔ پژوهش‌های حقوق جزا و جرم‌شناسی*، ص ۵۲.

۴. اشمیت، مایکل ان (۱۳۹۴). *راهنمای تالین در خصوص «حقوق بین‌الملل قابل اعمال در جنگ‌های سایبری»*. ترجمهٔ گروه مترجمان، تهران: جهان جام جم.

۵. حجازی، امرالدین و صلح‌چی، محمدعلی (۱۳۹۹). «تأثیر شورای امنیت سازمان ملل متحد و عدالت کیفری بین‌المللی. *پژوهش حقوق کیفری*، ۹(۳۳).

۶. دارابی‌نیا، مرتضی و فروغی‌نیا، حسین (۱۳۹۴). رابطهٔ شورای امنیت سازمان ملل متحد با دیوان کیفری بین‌المللی در زمینهٔ جنایت تجاوز سرزمینی. *پژوهشنامهٔ حقوق کیفری*، ۱۱، ۱۴۱-۱۷۰.

۷. دیهیم، علیرضا (۱۳۸۴). *درآمدی بر حقوق کیفری بین‌المللی در پرتو اساسنامهٔ دیوان کیفری بین المللی*. تهران: وزارت امور خارجه، مرکز چاپ و انتشارات.

۸. ذاکرحسین، محمدهادی (۱۴۰۱). اختیارات دادستان دیوان کیفری بین‌المللی در آغاز فرایند ارزیابی مقدماتی. *حقوق دادگستری*، ۱۱۷، ۵۹-۸۱.

۹. سودمندی، عبدالمجید (۱۳۹۴). *رسیدگی به جنایت تجاوز در دیوان کیفری بین‌المللی*. چ اول، تهران: نگاه بینه.

۱۰. شایگان، فریده (۱۳۸۰). *شورای امنیت سازمان ملل متحد و مفهوم صلح و امنیت بین‌المللی*. چ اول، زیر نظر دکتر جمشید ممتاز، تهران: دانشکدهٔ حقوق و علوم سیاسی دانشگاه تهران.

۱۱. شایگان‌فرد، مجید (۱۳۸۷). دیوان بین‌المللی کیفری و صلاحیت رسیدگی به جنایت تجاوز. *مطالعات حقوق خصوصی*، ۳۸(۴)، ۲۷۹-۲۵۵.

۱۲. لنتنر، گابریل‌ام (۱۳۹۸). *شورای امنیت سازمان ملل متحد و دیوان کیفری بین‌المللی: سازوکار ارجاع در نظریه و عمل*. چ اول، تهران: خرسندی.

۱۳. میرمحمدصادقی، حسین (۱۴۰۰). *دادگاه کیفری بین‌المللی*. چ دهم، تهران: دادگستر.

۱۴.نجفی ابرندآبادی، علی‌حسین (۱۳۹۱). تقریرات درس جرم‌شناسی؛ از جرم‌شناسی انتقادی تا جرم شناسی امنیتی. *دورهٔ دکتری حقوق کیفری و جرم‌شناسی*، تهران: دانشکدهٔ حقوق دانشگاه شهید بهشتی.

## ب) انگلیسی

15. Akande, D. (2008). The International Court of Justice and the Security Council: Is there Room for Judicial Control of Decisions of the Political Organs of the United Nations?. *International & Comparative Law Quarterly*, 46(2), 309-343.
16. Ambos, K. (2016). Individual Criminal Responsibility for Cyber Aggression. *Journal of Conflict & Security Law*, 21(3), 495-504.
17. Kai, A.(2010). The Crime of Aggression after Kampala. *German Year Book of International Law*, 53, p.509.
18. Barriga S, Blokker N (2017). *Entry into Force and Conditions for the Exercise of Jurisdiction: Cross-Cutting Issues*. In: Kreß C, Barriga S (eds) The Crime of Aggression: A Commentary. Cambridge University Press, Cambridge و 621–645.
19. Bassiouni, MC (1994). The United Nations Commission of Experts Established Pursuant to Security Council Resolution 780 (1992). *American Journal of International Law*, 88(4), 784 – 805.
20. Binder, C. (2017). *Uniting for Peace Resolution (1950). Max Planck Encyclopedia of International Law*. Oxford University.
21. Blokker, N. (2007). The Crime Of Aggression And The United Nations Security Council. *Leiden Journal Of International Law*, 20, 867-894.
22. Burchill, S. (1996). *Theories of International*.University Press.
23. Claus Kreß (2019). On the Activation of icc Jurisdiction over the Crime of Aggression. *Queen Mary Studies in International Law*, 33, 43-64.
24. Czosseck, C. (2011). Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security. *International Journal of Cyber Warfare and Terrorism*, 1, 183-194.
25. Darcy, S. (2021). Accident And Design: Recognising Victims Of Aggression In International Law. *International & Comparative Law Quarterly*, 70(1), pp 103-132.
26. Dinstein, Y. (2017). *War, aggression and self-defence*. sixth edition, Cambridge University Press.
27. 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.*
28. Escarameia, P. (2017). *The International Criminal Court and the Crime of Aggression*, Ashgate.
29. Frowein, J. A.(1998). Unilateral Interpretation of Security Council Resolutions-A Threat to Collective Security?.. In Liber Amicorum Günther Jaenicke-Zum 85 Geburtstag, edited by Volkmar Götz, Peter Selmer and Rüdiger Wolfrum, 89-134. Berlin: Springer.
30. Gruenberg, J. (2009). An Analysis of United Nations Security Council Resolutions: Are All Countries Treated Equall?. *Case Western Reserve Journal of International Law* 41.
31. Grigg, D.W (2010). "Cyber-Aggression: Definition and Concept of Cyberbullying" Aust. J. Guid. Counsell. Vol 20.
32. Heller, kj. (2020). Who Is Afraid of the Crime of Aggression?. *Journal of International Criminal Justice*,. 18(1), 2019-2031.
33. Hongju, Koh, Harold & Buchwald, Todd F (2017). The Crime of Aggression: The United States Perspective. *American Journal of International Law* , 109 (2), 257 – 295.

34. Horowitz, J. (2020). *Cyber Operations under International Humanitarian Law: Perspectives from the ICRC*. ASIL Insights.
35. ICC-Reviw conference of the Rome Staute cocludes in kampala, Available at https://asp.icc-cpi.int/reviewconference/pressreleaserc/review-conference-of-the-rome-statute-concludes-in-kampala
36. Madubuike-Ekwe, J. N. (2021). Cyberattack and the Use of Force in International Law. *Beijing Law Review*, 12, 631-649.
37. McDougall, C. (2021). *The Crime of Aggression under the Rome Statute of the International Criminal Court*. 2nd edition, Cambridge University Press.
38. Ocampo L.M. (2009.) *The International Criminal Court in motion, in Stahn C. and Sluiter G.*, eds, The Emerging practice of the International Criminal Court. MartinusNijhoff, Leiden-Boston.
39. O'Connell, M. E. & Niyazmatov, M (2012). What is Aggression? Comparing the Jus ad Bellum and the ICC Statute. *Journal of International Criminal Justice*, 10, 189-207.
40. Ohlin J. (2009). *Peace, Security and Prosecutorial Discretion*, in C. Stahn and G. Sluiter (eds), in Stahn C. and Sluiter G., eds, The Emerging practice of the International Criminal Court, MartinusNijhoff, Leiden-Boston
41. Orakhelashvili, A. (2005). The Impact of Peremptory Norms on the Interpretation and Application of United Nations Security Council Resolutions. *The European Journal of International Law*, 16(1), 59-88
42. Pellet, A. (2002). Applicable Law." In The Rome Statute of the International Criminal Court: A Commentary, Vol.II., edited by Antonio Cassese. Paola Gaeta and John R.W D .Jones, 1051-1084. Oxford: Oxford Univevsity Press
43. Petty, K. (2008). *A.Sixty Year in the Making: the Definition of Aggression for the International Criminal Court*. University Law Center.
44. Politi, M. (2012). The ICC and the Crime of Aggression: A Dream that Came Through and the Reality Ahead. *Journal of International Criminal Justice*, 10(1), 267–288.
45. Roshanaei, M (2021). Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies. *Journal of Computer and Communications*, 9 (8), 80-102
46. Ruys, T. (2018). Criminalizing Aggression: How the Future of the Law on the Use of Force Rests in the Hands of the ICC. *European Journal of International Law*, 29(3), , 887–917.
47. Scafferling C (2012). International Criminal Procedure, Oxford.
48. Shackelford, S. J. (2010). Estonia Two-and-A-Half Years Later: A Progress Report on Combating Cyber Attacks. *Journal of Internet Lawl* 21, 230-242.
49. Shirley V. Scott (2010). *International Law in World Politics*. Second Edition, Lynne Rienner Publishers.