نوع مقاله: **پژوهشی**

تاریخ دریافت: ۱۴۰۱/۰۵/۱۰
تاریخ پذیرش: ۱۴۰۱/۱۱/۱۰
صفحه: ۹۷ الی ۱۱۵

International Legal Research
تحقیقات حقوقی بین المللی

Volume 15, Issue 58, Winter 2022

Received: 2022/07/01
Accepted: 2023/01/30
Pages: 97 - 115

System: alr.ctb.iau.ir doi: 10.30495/alr.2023.1964598.2436 Article Type: **Research**

دوره ۱۵ / شماره ۵۸ / زمستان ۱۴۰۱

The supremacy of the jurisdiction of the International Criminal Court over the jurisdiction of the International Court of Justice in dealing with cyber-aggression

Alireza mohaghegh Harcheghan [1], Mohammad Ali Ardebily ✉[2], Ebrahim Beigzadeh [3], Mohammad Ali Mahdavi Sabet [4]

Abstract

Field and Aims: On July 17, 2018, two decades after the adoption of the Rome Statute of the International Criminal Court activated its jurisdiction over the crime of aggression. This crime was defined in 2010 by the Assembly of States Parties to the Rome Statute (ASP) as a material element of state conduct. "crime of aggression" in a position to effectively control or direct the political or military actions of a State and is in flagrant violation of the Charter of Nations It is considered united. The purpose of this research is to examine the jurisdiction of the International Criminal Court and the International Court of Justice in dealing with the crime of aggression, with an emphasis on cyber aggression.

Method: This research was analyzed in descriptive-analytical .

Findings and Conclusion: Cyber aggression means aggression that has been committed by computer-centered networks. In order to attribute cyber attacks to the government, it is necessary to consider the criterion of effective control. What is meant by effective control is that the government in question has exercised authority to form cyber aggression.The International Criminal Court has two jurisdictional regimes regarding the crime of cyber aggression. The first case is initiated by government referrals or due investigations by the prosecutor, and the second case is initiated by the Security Council referrals. another result of the research shows that the jurisdiction of the International Criminal Court in dealing with cyber aggression is superior to the jurisdiction of the International Court of Justice.

Keywords:supremacy, cyber-aggression, jurisdiction, International Criminal Court, International Court of Justice.

*Citation (APA): Mohaghegh harcheghan, A. R., Ardebili, M., Beigzadeh, E., & Mahdavi Sabet, M. A. (2023). The supremacy of the jurisdiction of the International Criminal Court over the jurisdiction of the International Court of Justice in dealing with cyber aggression. International Legal Research, 15(58), 97 - 115
https://alr.ctb.iau.ir/article_699181.html

1. PhD Student in Criminal Law and Criminology, Faculty of Law, Theology and Political Science, Science and Research Branch, Islamic Azad University, Tehran, Iran. (alireza.mohaghegh.1400@gmail.com)
2. Professor, Department of Criminal Law and Criminology, Faculty of Law, Shahid Beheshti University, Tehran, Iran. (Author) (m-Ardebili@sbu.ac.ir)
3. Professor, Department of International Law, Faculty of Law, Shahid Beheshti University, Tehran, Iran. (Ebrahim_Beigzadeh@sbu.ac.ir)
4. Associate Professor, Department of Criminal Law and Criminology, Faculty of Law, Theology and Political Science, Science and Research Branch, Islamic Azad University, Tehran, Iran.(ali@mahdavi.fr).

Volume 15, Issue 58, Winter 2022

Received: 2022/07/01
Accepted: 2023/01/30
Pages: 97 - 115

تحقیقات حقوقی بین المللی
International Legal Research

نوع مقاله: **پژوهشی**

تاریخ دریافت: ۱۴۰۱/۰۵/۱۰
تاریخ پذیرش: ۱۴۰۱/۱۱/۱۰
صفحه: ۹۷ الی ۱۱۵

Article Type: **Research**

سامانه: doi: 10.30495/alr.2023.1964598.2436alr.ctb.iau.ir

دوره ۱۵ / شماره ۵۸ / زمستان ۱۴۰۱

تفوق و برتری صلاحیت دیوان کیفری بین‌المللی بر صلاحیت دیوان دادگستری بین‌المللی در امر رسیدگی به تجاوز سایبری

علیرضا محقق هرچقان[۱]، محمدعلی اردبیلی✉[۲]، ابراهیم بیگ زاده[۳]، محمدعلی مهدوی ثابت [۴]

چکیده

زمینه و هدف: در ۱۷ جولای ۲۰۱۸، دو دهه پس از تصویب اساسنامه رم، دیوان کیفری بین‌المللی (ICC) صلاحیت خود را در مورد جنایت تجاوز فعال کرد. این جنایت در سال ۲۰۱۰ توسط مجمع کشورهای عضو اساسنامه رم (ASP) به‌عنوان یک عنصر مادی از رفتار دولت تعریف شد. «جنایت تجاوز» در وضعیتی است که به طور مؤثر کنترل یا هدایت اقدامات سیاسی یا نظامی یک دولت را به همراه دارد و اقدامش نقض آشکار منشور ملل متحد به حساب می‌آید. هدف از انجام این پژوهش بررسی حیطه صلاحیت‌های دیوان کیفری بین‌المللی و دیوان دادگستری بین‌المللی در رسیدگی به جنایت تجاوز با تأکید بر تجاوز سایبری است.

روش: این پژوهش، به شکل توصیفی – تحلیلی مورد تجزیه و تحلیل قرار گرفته است.

یافته‌ها و نتایج: منظور از تجاوز سایبری، تجاوزی است که از سوی شبکه‌های متمرکز بر رایانه صورت پذیرفته و به منظور انتساب حملات سایبری به دولت نیز ضرورت دارد تا معیار کنترل مؤثر مورد توجه قرار گیرد. در رسیدگی و احراز تجاوز سایبری، شورای امنیت دارای حقّ اولویت است و لیکن این تقدم به منزله‌ی صلاحیت انحصاری شورا نیست. دیوان کیفری بین‌المللی دارای دو رژیم صلاحیتی درباره‌ی تجاوز سایبری است. رژیم اول، طبق ارجاعات دولتی یا تحقیقات مقتضی، توسط دادستان آغاز شود و مورد دوم، با ارجاعات شورای امنیت شروع گردد. نتیجه دیگر تحقیق نشان می‌دهد که صلاحیت دیوان کیفری بین‌المللی در رسیدگی به تجاوز سایبری نسبت به صلاحیت دیوان دادگستری بین‌المللی دارای رجحان است. این برتری ناشی از شرایط ساختاری ICC و همچنین قضات این دیوان است.

واژگان کلیدی: تفوق و برتری، تجاوز سایبری، صلاحیت رسیدگی، دیوان کیفری بین‌المللی، دیوان دادگستری بین‌المللی.

*استناددهی (APA): محقق هرچقان، علیرضا، اردبیلی، محمدعلی، بیگ‌زاده، ابراهیم، مهدوی ثابت، محمد علی. (۱۴۰۱). تفوق و برتری صلاحیت دیوان کیفری بین‌المللی بر صلاحیت دیوان دادگستری بین‌المللی در امر رسیدگی به تجاوز سایبری. تحقیقات حقوقی بین‌المللی، ۱۵(۵۸)، ۱۱۵ - ۹۷

https://alr.ctb.iau.ir/article_699181.html

۱. دانشجوی دکتری رشته حقوق کیفری و جرم‌شناسی، دانشکده حقوق، الهیات و علوم سیاسی، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران. (alireza.mohaghegh.1400@gmail.com)

۲. استاد گروه حقوق کیفری و جرم‌شناسی، دانشکده حقوق، دانشگاه شهید بهشتی، تهران، ایران. (نویسنده مسئول) (m-Ardebili@sbu.ac.ir)

۳. استاد گروه حقوق بین‌الملل، دانشکده حقوق، دانشگاه شهید بهشتی، تهران، ایران. (Ebrahim_Beigzadeh@sbu.ac.ir)

۴. دانشیار گروه حقوق جزا و جرم‌شناسی، دانشکده حقوق، الهیات و علوم سیاسی، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران. (ali@mahdavi.fr)

مقدمه

نبودِ کیفر، حقیقت تلخی است که از یک منظر، به برخوردار نبودن جامعه‌ی جهانی از دادگاه بین‌المللی دارای صلاحیت اجباری برمی‌گردد و از منظر دیگر، به فقدان تمایل یا عدم توانایی دادگاه‌های ملی، در اِعمال صلاحیت کیفری نسبت به جنایت بین‌المللی ارتباط دارد. دادگاه‌های موردی[1] و دیوان‌های خاص بین‌المللی کیفری همیشه بعد از جنایات جنگی[2]، نسل‌زدایی[3] و تجاوز سرزمینی[4] تشکیل شده‌اند. محاکم نورنبرگ و توکیو و تشکیل دیوان‌های کیفری در دهه گذشته به منظور رسیدگی به اتهام «نقض گسترده و فاحش حقوق بشردوستانه»ی در کشور یوگسلاوی سابق و رواندا و همچنین سیرالئون، پس از رخ دادن یک فاجعه انسانی و به منزله‌ی واکنش افکار عمومی و نمایندگان مردم رخ دادند. همانطور که بعد از ارتکاب وقایعِ خونین زنجیره‌وار در سده‌ی گذشته و محاکمه نمودن و به تبع آن مجازات جنایتکاران، کماکان مسائل مرتبط با مسئولیت بین‌المللی دولت‌ها و تبیین مفهوم جرایم و جنایات بین‌المللی در چارچوب اسناد پیش‌نویس مهیا شده به وسیله‌ی حقوقدانان بین‌المللی و کیفری مطرح بوده و در موضوعات تئوری مراکز علمی - پژوهشی و دانشگاهی، مورد مداقّه قرار می‌گیرد. این در صورتی است که به تبع پیدایش نظم نوین و بروز ناشی از پدیده‌ی جهانی شدن، روزانه جنایات‌های متعدد به وقوع می‌پیوندند که از رسیدگی‌های کیفری مصون هستند.

یکی از زمینه‌های نوین فعالیت جنایتکاران، بحث تجاوز سایبری است. حملات و تجاوزهای سایبری که محصول پیشرفت‌های تکنولوژیک هستند، تمامی معادلات حقوقی پیش از به شکل‌گیری چنین فضایی را دگرگون نموده و موجب شده‌اند که نیازمند تغییرات گسترده قواعد و مقررات مرتبط در زمینه‌های داخلی و بین‌المللی، احساس شود. یکی از دشواری‌های موجود این است که یک حمله شبکه محور کامپیوتری را به سختی می‌توان جنایت تجاوز سایبری، به حساب آورد. این معضل سه علت دارد: اول) ماده‌ی ۸ مکرر اساسنامه، شامل اَعمال اشخاص خصوصی نمی‌شود و این در حالی است که همین اشخاص معمولاً طراحان چنین حملاتی هستند. دوم) یک حمله شبکه محور کامپیوتری فقط در شرایط بسیار خاصی به منزله‌ی «عمل تجاوز» در تحلیل بند ۲ ماده ۸ اساسنامه به حساب می‌آید و منظور حمله‌ایست که به واسطه‌ی نیروهای مسلح دولتی یک کشور انجام شده است. سوم) همانطورکه در بند اول ماده هشت مکرر اساسنامه دیوان آمده می‌توان چنین حملاتی را در حکمِ نقض روشن منشور ملل متحد دانست (آمبوس[5]، ۲۰۱۶: ۴۹۶). ماده هشتم مکرر اساسنامه پس از اولین کنفرانس بازنگری اساسنامه دیوان در سال ۲۰۱۰ و در

1. Ad hoc tribunals.
2. War crimes.
3. Genocide.
4. Territorial aggression.
5. Ambos.

کامپالا[1] که به تعریف جنایت تجاوز اختصاص دارد، از دو پاراگراف تشکیل شده است. بند اول آن درمورد تعریف جنایت تجاوز و بند دوم آن درمورد مصادیق جنایت تجاوز می‌باشد. از جمله مسائلی که در حوزه تجاوز سایبری در حقوق بین‌الملل مطرح است، انطباق یا عدم انطباق این دسته از حملات و جرائم سایبری با جنایت تجاوز و واکاوی امکان صلاحیت دیوان کیفری بین‌المللی در رسیدگی به آن‌هاست. اگرچه با شکل گرفتن دیوان کیفری بین‌المللی، ایده‌ی عینیت یافتن اصل صلاحیت جهانی[2] برای رسیدگی به مهمترین جنایات بین‌المللی با پیش‌بینی قاعده تکمیلی بودن[3] صلاحیت دیوان در اساسنامه آن –به این مفهوم که رسیدگی محاکم ملی دارای تقدم است و نه صلاحیت آن‌ها – محقَّق نگردید ولی با در نظر گرفتن رویه قضایی بین‌المللی، لازم است توجه شود که دایره‌ی صلاحیت جهانی دادگاه‌های داخلی به وسیله‌ی حقوق بین‌المللی مشخص می‌گردد. همان‌طور که نوع و چگونگی صلاحیت دادگاه‌های داخلی و فرآیند محاکمه متجاوزان، به موجب اساسنامه دیوان نیز با قید و بندهایی مشخص، محدود گردیده است. در این مقاله سعی بر آن است که ضمن بررسی اجمالی تجاوز سایبری، صلاحیت‌های دیوان کیفری بین‌المللی و دیوان دادگستری بین‌المللی در این زمینه بررسی و متعاقب آن رجحان و برتری صلاحیت دیوان کیفری بین المللی احراز شود.

۱. فضای سایبری

فضای سایبر در معنای عام کلمه به مجموعه‌ای از تعاملات انسان‌ها به وسیله‌ی کامپیوتر و دیگر تکنولوژی‌های جدید در حوزه ارتباطات اطلاق می‌شود. در سال ۱۹۸۴ این واژه بدون در نظر گرفتن عناصر زمان و مکان از سوی ویلیام گیبسون[4] مؤلف کتاب نورومونسر[5] استفاده شد. گیبسون، فضای سایبری را به صورت یک بازآفرینی دارای گرافیک از داده‌ها تلقی می‌کند. با مطالعه امروزی در نظریات گیبسون می‌توان چنین نتیجه گرفت که تئوری مورد نظر گیبسون، بیشتر به هوش مصنوعی و رباتیک نزدیک است (بریر[6]، ۲۰۱۰: ۱۴). گاه در اشاره به مفهوم تجاوز سایبری، از تعدی و تعرضی که لزوماً در بستر اینترنت شکل گرفته است. در واقع اینترنت دروازه فضای سایبر است اما فضای سایبر، با ویژگی‌هایی چون میزان و چگونگی دسترسی، راهبری، اطلاع‌یابی، بالندگی و اعتماد شناخته می‌شود (میلر[7]، ۲۰۱۴: ۲۲۱). برخی از صاحبنظران معتقدند که مفهوم سایبر در سطح بین‌المللی بسط پیدا کرده و رواج یافته و به همین دلیل، این واژه به یک لغت

1. Kampala.
2. Universal jurisdiction or global jurisdiction.
3. Complementarity.
4. William Gibson
5. Neuromoncer
6. Brier.
7. Miller.

بین‌المللی تبدیل شده است. با این وجود در زبان فارسی لغت «سایبر» را معادل واژه «مجاز» و لغت «اسپیس» را معادل واژه «فضا» ترجمه کرده‌اند و ترکیب «سایبر اسپیس» را معادل «فضای مجازی» دانسته‌اند. در همین معنا ترکیبات دیگری نظیر «جامعه مجازی» یا «شهروند مجازی» و «فروشگاه‌های مجازی» و امثال آن مطرح می‌شود. همه این ترکیبات در فضای مجازی مطرح می‌شوند (باستانی، ۱۳۸۳: ۵۴). از لحاظ لغوی، تجاوز سایبری به معنای تجاوز مجازی و دارای مفهومی غیرملموس[1] است. نخستین بار این اصطلاح «سایبرنتیک» توسط ریاضی‌دانی به نام نوربرت وینر در کتابی با عنوان «سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین» در سال ۱۹۴۸ به کار برده شده است. سایبرنتیک علم مطالعه و کنترل مکانیزم‌ها در سیستم‌های انسانی، ماشینی (کامپیوترها) است. فضای سایبر در معنا به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق کامپیوتر و مسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود. یک سیستم برخط، نمونه‌ای از فضای سایبر است که کاربران آن می‌توانند از طریق ایمیل با یکدیگر ارتباط برقرار کنند. برخلاف فضای واقعی، در فضای سایبر نیاز به جابجایی‌های فیزیکی نیست و کلیه اعمال فقط از طریق فشردن کلیدها یا حرکات ماوس صورت می‌گیرد (عاملی، ۱۳۹۰: ۲۳). با توجه به بررسی سنجه‌های گوناگون، از تعریف فضای سایبر به مفهوم خاص می‌توان بیان نمود که فضای سایبر، محیطی تشکیل‌یافته از سامانه‌ها و شبکه‌های ارتباطی متصل به هم است که قابلیت هر نوع رفتار متناسب با محیط مبادله داده، ذخیره و انتشار اطلاعات را دارد و برای نتیجه‌گیری از تعاریف بالا می‌توان گفت منظور از فضای سایبری، محیط و بستری است که در کامپیوتر و شبکه‌های گوناگون بر پایه نرم‌افزار وجود دارد.

۲. تجاوز سایبری

پیش از ارائه تعریف از مفهوم تجاوز سایبری، بهتر است مفهوم عام‌تر جنایت تجاوز، تبیین شود. در سال ۱۹۴۵ برای نخستین بار در تاریخ حقوق کیفری بین‌المللی، دادگاه نورنبرگ[2]، «جرم علیه صلح[3]» را در کنار «جنایت جنگی» و مفهوم «جنایت علیه بشریت[4]» را به عنوان جرمی مستقل، به رسمیت شناخت (دیهیم، ۱۳۸۴: ۴۵۱-۴۵۲). این جنایت به اَشکال برنامه‌ریزی[5]، آماده‌سازی[6]، شروع[7] و یا راه‌اندازی[8] جنگ تجاوزکارانه و یا جنگ در نقض آشکار معاهدات، توافقات یا تضمیناتِ بین المللی تعریف می‌گردد. در چنین تعریفی، مسئولیت کیفری فرد، بسیار وسیع تعریف

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

می‌شود (هونگجوکو [1] و بوچوالد [2]، ۲۰۱۷: ۲۵۹). در این اساسنامه، عنصر مادی جرم علیه صلح، «شرکت کردن و یا کمک کردن در برنامه‌ریزی یا راه‌اندازی جرم» و عنصر معنوی جرم نیز «آگاه بودن از این جنایت» مطرح شده بود (کلاوس [3]، ۲۰۱۹: ۴۹). با وجود ممنوع بودن تجاوز در منشور ملل متحد (بند اول، ماده یکم و بند چهارم ماده دوم) و طبیعتاً ضرورت اعاده به وضع سابق، همچنین در اساسنامه نورنبرگ، در هیچیک از این اسناد، تعریفی حقوقی از جرم تجاوز ارائه نشده و فقط منشور، صلاحیت احراز جرم تجاوز را برای شورای امنیت قائل شده است.[4] در نهایت کنفرانس کامپالا که در تاریخ یازدهم جون سال ۲۰۱۰ و در مورد بازنگری اساسنامه دیوان کیفری بین‌المللی تشکیل شده بود، تعریفی از جنایت تجاوز ارائه کرد. مطابق با بیانیه این کنفرانس، «جنایت تجاوز، با توجه به قطعنامه شماره ۳۳۱۴ مجمع عمومی، مجموعه اقدام‌هایی است که از سوی رهبری سیاسی و یا یک رهبری نظامی شکل گرفته و حاوی نقض فاحش و گسترده مقررات مرتبط در منشور ملل متحد است[5]». برای احراز «نقض بارز » باید سه عاملِ ویژگی، شدت و وسعت (بصورت تجمعی و نه به تنهایی و ناقص) برای رسیدن به کفایت وجود داشته باشند. (سلیمی،۱۳۹۹ : ۷۲) با توجه به تعاریف ارائه شده از جنایت تجاوز، در ادامه مفهوم تجاوز سایبری تبیین می‌گردد. تعریف دقیقی از تجاوز سایبری در منابع حقوقی بین‌المللی یافت نمی‌شود. با این وجود می‌توان این مفهوم را متناظر با مفهوم تجاوز در نظر گرفت، با این شرط که این تجاوز از سوی شبکه‌های متمرکز بر رایانه صورت گرفته باشد (مادوبیک-اکوی [6]، ۲۰۲۱: ۶۳۵). به منظور شناخت بیشتر از مفهوم تجاوز سایبری، لازم است تا مفهوم حمله سایبری نیز تبیین شود. با در نظر گرفتن طیف گسترده‌ای از اعمال منفی که می‌تواند در فضای سایبری رخ دهد، گریگ [7] «تهاجم سایبری» را اینگونه تعریف کرد: «...آسیب عمدی که با استفاده از وسایل الکترونیکی به یک فرد یا گروهی از افراد، صرفنظر از موقعیت واقعی و اجتماعیشان وارد می شود. این آسیب می‌تواند شامل اعمالِ مخرِّب، آسیب‌رسان، تهدیدآمیز و یا امری سیاسی باشد» (گریگ، ۲۰۱۰: ۱۴۳). بهترین راه برای تبیین مفهوم حمله سایبری [8] این است که آن را نه هدف حمله بلکه وسیله‌ای برای انجام یک حمله بدانیم. در اینگونه عملیات «شیوه ایجاد تاثیر» مهم نیست. بلکه «تأثیرگذاری» صِرف ملاک وقوع است. (Development, Concepts and Doctrine Center, 2022: 19) حملات موصوف فقط شکل جدیدی از سلاح هستندکه فقط به این دلیل که واژه‌ی

1. Hongju Koh.
2. Buchwald.
3. Claus.

۴. ماده ۳۹ منشور ملل متحد.

5. 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
6. Madubuike-Ekwe.
7. Grigg.
8. Cyber-Attack.

سایبری در نام چنین حملاتی به کار رفته است، طرز تفکر در مورد سلاح را تغییر نمی‌دهد. همانطور که حمله هوایی حمله از هواپیما است و نه حمله به هواپیما، حمله سایبری نیز سلاحی از رایانه است (نگوین[1]، ۲۰۱۳: ۱۰۸۲). کامپیوتر دقیقاً نحوه پرتاب سلاح است. این چارچوب به درک اینکه چگونه یک حمله سایبری می‌تواند به سیستم‌هایی که شبکه یا رایانه نیستند آسیب فیزیکی وارد کند، کمک می‌کند. با توسعهٔ فعالیت سایبری، صلح و امنیت سایبری، یک اصل ضروری است که با توسل به زور سایبری، نقض می‌شود. اصل منع توسل به زور، برای تعیین نقض یا عدم نقض مادهٔ ۲(۴) منشور ملل متحد و ممنوعیت آن در حقوق بین‌الملل عُرفی به کار می‌رود. در مقابل به‌کارگیری زور توسط فرد متخاصم، مداخلهٔ قانونی توسط شورای امنیت جامعه بین المللی به منظور ایجاد صلح و امنیت بین‌المللی، می‌تواند با ارجاع امر به دیوان کیفری بین‌المللی صورت گیرد. نقض صلح و امنیت سایبری بین‌المللی، با ارتکاب جرائم سایبری درصورت رسیدن به آستانهٔ مقتضی می‌تواند قابل احراز به عنوان «جنایت تجاوز» در قالب «فاعل معنوی» باشد. (اردبیلی،۱۴۰۰: ۵۴) وفقِ قاعدهٔ ۱۳ دستورالعمل تالین ۱ در سال ۲۰۱۳میلادی (Schmitt,2013:53) و نیز بند ۶ مادهٔ ۶۹ در دستورالعمل تالین ۲ در سال ۲۰۱۷ میلادی برحسب اثر، گستره و شدت در بروز جرائم و حملات سایبری، آستانهٔ جنایت تجاوز را باید «حملهٔ مسلحانه» دانست که دارای ماهیتِ نقضِ قواعد حقوق بین‌الملل و منع توسل به زور است و مسئولیت کیفری علاوه بر فرد متخاصم به فعالانِ غیردولتیِ مطلع نیز توسعه خواهد یافت. (Schmitt,2017:82-89) تعریف حملات سایبری که در این مقاله استفاده خواهد شد عبارت است از: «یک اقدام خصمانه با استفاده از رایانه یا شبکه‌ها یا سیستم‌های مرتبط برای ایجاد تخریب به منظور یک هدف سیاسی یا امنیت ملی» (هوروویتز[2]، ۲۰۲۰: ۲۴). ذکر این نکته حائز اهمیت است که این تعریف یکی از توسعه‌های علمی است و هیچ اثری در حقوق بین‌الملل ندارد. رایج‌ترین تهدیدات سایبری از طریق سرقت یا جنگ اطلاعاتی است. این ایده که یک کنش‌گر می‌تواند یک سیستم را «هک» کند و داده‌ها یا اطلاعات ارزشمند به سرقت ببرد (گلداسمیت[3]، ۲۰۱۳: ۱۳۴). از دیدگاه حقوق بین‌الملل این نوع حملات، اساساً جاسوسی است که توسط جامعه بین‌الملل نه تایید شده و نه محکوم می‌شود. رویه پیشین حقوق کیفری بین‌المللی نیز چنین بی‌تفاوتی را نشان می‌دهد. با توجه به تعریف تجاوز از منظر دیوان دادگستری بین‌المللی و همچنین دیوان کیفری بین‌المللی، حملات سایبری که دولت‌ها در یکی از ارکان آن (طراحی، تدارک، شروع و اجرا) حضور داشته باشند، تجاوز محسوب می‌شود.

1. Nguyen.
2. Horowitz
3. Goldsmith.

۳. انطباق حملات سایبری با مفهوم تجاوز از منظر ICJ و ICC

اولین مؤلفه‌ای که شرط مهم برای تجاوز بودن حملات سایبری است، دولتی بودن منشأ این حملات خواهد بود (هورورویتز، ۲۰۲۰: ۲۵). حملات سایبری در دنیا می‌تواند به اَشکال گوناگونی نظیر موارد ذیل صورت بگیرد (گراهام[1]، ۲۰۱۰: ۸۹):

۱- حمله سایبری، منشأ دولتی داشته و علیه دولت دیگری صورت می‌پذیرد. در این وضعیت سازماندهی، برنامه‌ریزی و اجرا توسط یک دولت شکل می گیرد.

۲- طراحی حمله‌ی سایبری توسط یک دولت است ولی اجرای آن از سوی اشخاص غیردولتی که مورد پشتیبانی دولت هستند تحقق می یابد.

۳- طراحی حمله‌ی سایبری از سوی افراد غیر دولتی است ولی اجرای آن با کمک دولت انجام می‌شود.

۴- در طراحی، سازماندهی و اجرای حمله‌ی سایبری، دولت مداخله‌ای ندارد.

بنابراین لازم است تا بررسی شود که هرکدام از موارد ذکر شده، تحت چه شرایطی قابل انتساب به دولت بوده و می‌توانند تجاوز محسوب شوند. مورد اول، پیشنیاز اولیه را دارد و سایر خصوصیات باید در آن سنجیده شود تا ذیل مفهوم تجاوز بایستد. موارد ۲ تا ۴ لازم است تا قابلیت انتساب به دولت را داشته باشند. دولت‌ها، تنها در قبال اعمال و رفتارهای برخلاف موازین حقوق بین‌الملل مأمورانشان مسئول هستند (کازوروسکا[2]، ۲۰۱۵: ۱۰۵). با این وجود، اگر هر شخص یا گروهی از اشخاص خصوصی، رسماً و قانوناً از سمت دولت یا به نمایندگی از دولت، اقدام کنند، همه‌ی اعمال آن‌ها قابلیت انتساب به دولت را دارد. این در حالی است که اصل عدم مسئولیت دولت نسبت به رفتارهای اشخاص خصوصی، در رویه‌ی قضایی بین‌المللی مورد تأکید بوده است (هنجنی و فرهادنیا، ۱۳۹۷: ۷۷). البته این امکان وجود دارد که این اعمال و رفتار زمینه‌ای برای مسئولیت بین‌المللی دولت باشد. چنین وضعیتی، در شرایطی محقق می‌شود که مقامات دولتی، در زمینه‌ی پیشگیری از این دسته از اعمال و یا مجازات نمودن مرتکبان آن، اهمال کنند. از این رو در اینکه کدام شخص یا اشخاص، از ارگان دولت به حساب می‌آیند، به قوانین داخلی هر کشور ارتباط دارد. بنابراین اگر این اشخاص، در فرآیند حمله سایبری، کوچک‌ترین مشارکتی داشته باشند و بتوان حملات مذکور را به این افراد منتسب نمود، عمل صورت گرفته از سوی دولت محسوب می‌گردد. با تحقق یافتن مجموعه‌ای از شرایط، اَعمال شرکت‌های خصوصی نیز از منظر حقوق بین‌الملل، موجب شکل‌گیری مسئولیت برای دولت خواهد بود و در اینجا باید ثابت شود که شرکت خصوصی مذکور، اقتدارات دولت خاصی را اِعمال نموده و یا اینکه شرکت، به دستور

1. Graham.
2. Kaczorowska.

دولت اقدام کرده است (کراوفورد[1]، ۲۰۰۵: ۴). کمیسیون حقوق بین‌الملل در ماده هشتم طرح مسئولیت دولت‌ها، امکان انتساب رفتارهای افراد و گروه‌ها به دولت را تأیید کرده است. مطابق این ماده رفتار یک شخص یا گروهی از اشخاص، اگر در حقیقت بر مبنای دستور یا تحت هدایت یا کنترل کشوری عمل کنند، از منظر حقوق بین‌الملل، اقدام آن کشور محسوب می‌شود. اینکه کدام خصیصه در عمل افراد یا گروه‌ها نشانگر تحت کنترل دولت بودن است، در پرونده‌های گوناگون دیوان دادگستری بین‌المللی مورد اشاره قرار گرفته است. دیوان دادگستری بین‌المللی در پاراگراف ۳۷۷ تا ۴۱۵، در رأی در خصوص شکایت دولت بوسنی از صربستان[2]، اعمال شبه نظامیان صرب را به دولت این کشور منتسب ندانست. دلیل دیوان این بوده است که دولت صربستان در قبال نیروهای شبه نظامی، کنترل مؤثر نداشته است. همچنین دیوان در قضیه شکایت نیکاراگوئه از آمریکا چنین معیاری را مورد توجه قرار داده است. برخلاف رویه دیوان دادگستری بین‌المللی، دیوان کیفری بین‌المللی برای یوگسلاوی سابق در پرونده تادیچ، معیار دیگری را در نظر گرفته است. دیوان در سال ۱۹۹۹، با در نظر گرفتن معیار «کنترل کلی» مسئولیت دولت را مورد توجه قرار داد. رأی دیوان به این شرح بود که: «از منظر حقوق بین‌الملل شرط انتساب اعمال و رفتارهای گروه‌های خصوصی به دولت‌ها این است که دولت مزبور بر گروه‌های خصوصی کنترل کلی اعمال نماید. در هر صورت، معیارهای این کنترل، در موارد مختلف و با توجه به شرایط گوناگون، می‌تواند متفاوت باشد[3]». پس از اینکه شرط قابلیت انتساب به دولت، محقق شود، لازم است معیارهای دیگری مورد واکاوی قرار بگیرد تا انطباق حمله‌ی سایبری با تجاوز احراز شود. به منظور شناسایی این معیارها، لازم است تعریف تجاوز از منظر قطعنامه مجمع عمومی مطرح گردد. مطابق این تعریف تجاوز استفاده از نیروهای مسلح توسط یک کشور بر علیه حاکمیت، تمامیت سرزمینی یا استقلال سیاسی، یا به هر شکل دیگر رفتار مخالف با منشور ملل متحد که در این تعریف مندرج است گفته می‌شود. آنچنان که در تعریف مجمع عمومی از تجاوز ارائه شده است، استفاده از نیروهای مسلح را به عنوان شرط اول، لازمه‌ی وقوع تجاوز است (شاو[4]، ۲۰۱۰: ۱۵۴). اگرچه در شکل سنتی تجاوز، منظور از نیروی مسلح، بخش عملیاتی نیروهای نظامی وابسته دولت است. لیکن «نیروهای مسلح» باید در معنای موَّسعش یعنی کلیه نیروهای نظامی (عملیاتی و ستادی) در نظر گرفت. بنابراین چنین به نظر می‌رسد که به هنگام عدم وجود جنگ مسلحانه، تمامی افراد نیروهای مسلح به جز کادر درمان، نیروی مسلح تلقی شده و حمله‌ی سایبری از سمت این افراد، یک حمله از سوی دولت به دولت دیگر خواهد بود. شرط دوم که در تعریف تجاوز، مورد توجه قرار گرفته، ناظر بر هدف حمله سایبری (علیه حکمیت، تمامیت سرزمینی، یا استقلال سیاسی کشور دیگر)

1. Crawford.
2. ICJ: Bosnia and Herzegovina V.Serbia and Montene gro, 2007.
3. International Criminal Tribunal for the Former Yugoslavia: Tadic case, Para.38.
4. Shaw.

است. از آنجا که حملات سایبری، به جای رخ دادن در فضای فیزیکی، در فضای مجازی حادث می‌شوند، می‌توان حملات سایبری را علیه اهداف فیزیکی تصور نمود. از این رو ویژگی حملات سایبری موجب می‌شود که از میان اهداف مذکور، اهداف حاکمیت و استقلال سیاسی بتوانند موضوع تهاجم قرار بگیرند. با این توضیح لازم است آسیب‌های ناشی از حملات سایبری به آستانه‌ای که همانا آستانه «حمله مسلحانه» می‌باشد (Schmitt,2013:47) برسد که بتوان آن را علیه حاکمیت و یا استقلال سیاسی دولت مورد هدف تلقی کرد (گیوکی و همکاران، ۱۴۰۰: ۲۲۹). بخش پایانی تعریف تجاوز، اعمال و رفتارهای نیروهای مسلح را به هر صورتی که مخالف با منشور ملل متحد باشد، مورد توجه قرار داده است. از این رو می‌توان هرگونه حملات سایبری مخالف قطعنامه‌های شورای امنیت و یا قطعنامه ۲۶۲۵[1] مجمع عمومی سازمان ملل را تجاوز در نظر گرفت که با توجه به آنچه گفته شد تعریف حملات سایبری با مفهوم تجاوز در دیوان کیفری بین‌المللی و دیوان دادگستری بین‌المللی دارای انطباق است. این هم پوشانی در مفاهیم «دولتی بودن»، «کنترل مؤثر» و «کنترل کلی» دیده می‌شود.

۴. مقایسه‌ی صلاحیت ICC و ICJ در رسیدگی به تجاوز سایبری

پس از ارائه‌ی تعاریف از تجاوز سایبری و بررسی شروط لازم برای اینکه حملات سایبری، به عنوان تجاوز محرز شوند، لازم است صلاحیت بررسی درباره‌ی جنایات سایبری مورد بررسی قرار بگیرد. توجه ویژه این مقاله به مقایسه صلاحیت دیوان کیفری بین‌المللی و صلاحیت دیوان دادگستری بین‌المللی معطوف گردیده است. اگرچه لازمه‌ی رسیدگی به تجاوز سایبری در یک محکمه‌ی بین‌المللی، احراز قبلی آن توسط کشور متبوع مرتکب است. لیکن سابقه نشان می‌دهد که احراز وقوع تجاوز امر ساده‌ای نمی‌باشد. این دشواری در احراز، موجب گردیده که منحصر بودن چنین مسئولیتی به شورای امنیت مورد تردید واقع شده و صلاحیت مراجع بین‌المللی دارای صلاحیت دیگری مانند مجمع عمومی سازمان ملل، دیوان دادگستری بین‌المللی و دیوان بین‌المللی کیفری مطرح گردد:

۴-۱ منحصر نبودن احراز تجاوز به شورای امنیت

براساس ماده ۲۴ منشور ملل متحد، حفظ صلح و امنیت بین‌المللی، یک مسئولیت اولیه و اصلی برای شورای امنیت به حساب می‌آید. لیکن چنین مسئولیتی انحصاری نبوده و قطعاً مجمع عمومی در این خصوص دارای صلاحیت است. شورای امنیت، پیش از آنکه مطابق با مواد ۴۱ و ۴۲

1. GA: Resolution 2625 (XXV). Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations,Doc. A/RES/25/2625 , 24 October 1970. At: http://www.un-documents.net/a25r2625.htm.

منشور، نسبت به حفظ صلح و امنیت بین‌المللی اقدام نماید، لازم است حضور تهدید صلح، عامل نقض صلح و یا عمل تجاوز را احراز کند.[1] لذا محرز نمودن تجاوز سایبری، پیش‌شرط هر اقدام شورای امنیت محسوب و چنین پیش‌شرطی به معنای انحصاری بودن آن برای شورای امنیت نیست (بلوکر[2]، ۲۰۰۷: ۸۷۲). لازم به تذکر است که مطابق با ماده ۲۴، شورای امنیت در بحث احراز تجاوز، دارای اولویت و تقدم است. این تقدم به این معنا نیست که شورا می‌تواند صلاحیت سایر نهادهای ذیصلاح ملل متحد را در این زمینه سلب نماید (آمبوس، ۲۰۱۶: ۴۹۷). بنابراین اگر در موقعیتی شورای امنیت، موضوعی نظیر حمله سایبری را تهدیدی برای صلح یا نقض صلح به حساب آورد و از احراز وقوع تجاوز خودداری کند دیگر نمی‌توان چنین نتیجه گرفت که تجاوز سایبری صورت نگرفته است. زیرا عدم احراز می‌تواند به خاطر وجود انگیزه‌های سیاسی در شورای امنیت رخ داده و نشانگر این مهم باشد که مواضع، نقطه نظرات، مصلحت‌ها و منفعت‌های سیاسی تمام اعضای دائم آن در تفسیر موضوع مورد مناقشه بین دو کشور تأثیرگذار است. در چنین وضعیتی، مجمع عمومی می‌تواند خود به اقدام موصوف دست بزند. البته باید توجه داشت که عدم احراز تجاوز از سوی شورای امنیت، نمی‌تواند یک نهاد قضایی را هم نسبت به عدم احراز ملزم نماید. بنابراین، در این شرایط احراز از سوی دیوان کیفری بین‌المللی در همان راستای اقدام شورای امنیت معتبر است (دارابی‌نیا و فروغی‌نیا، ۱۳۹۴: ۱۶۸) و نهادهای ذیصلاح دیگر ملل متحد می‌توانند موضوع را تجاوز محسوب نمایند.

۲-۴ مجمع عمومی و احراز تجاوز

با توجه به مسئولیت اولیه‌ی شورای امنیت در زمینه‌ی صلح و امنیت بین‌المللی، مجمع عمومی در این زمینه دارای مسئولیت ثانوی (مشترک) در چهارچوب اختیارات عام می‌باشد (شایگان‌فرد، ۱۳۸۷: ۲۷۲). هدف از چنین رویکردی این است که شورای امنیت به منزله‌ی نهادی که از منظر سیاسی حائز اهمیت است، ایجاد گردیده و اقدامات سریع و موثر برای حفظ صلح را انجام دهد. چنین نگاهی با بند اول ماده ۲۴ و «عبارت مسئولیت اولیه» دارای مطابقت است. زیرا واژه‌ی «اولیه» صرفاً به تقدم زمانی مرتبط نبوده بلکه بر تقدم ماهوی نیز دلالت دارد» (روسکینی[3]، ۲۰۱۰: ۹۰-۹۱). باید توجه داشت که این تفسیر از مسئولیت اولیه شورای امنیت، امکان فعالیت مجمع عمومی را در عرصه حفظ صلح براساس اختیارات خاص و عام اعطاء شده به آن سلب نمی‌کند. مجمع عمومی در زمان تصویب قطعنامه اتحاد برای صلح، مطابق چنین قاعده‌ای عمل می‌نماید (کلاوس، ۲۰۱۹: ۶۰). این نکته ضروری است که مجمع عمومی دارای حق تصمیم‌گیری در رابطه به

---

۱. ماده ۳۹ منشور سازمان ملل متحد.

2. Blokker.
3. Roscini.

بودجه‌ی ملل متحد است. به واسطه‌ی همین حق است که دیوان بین‌المللی دادگستری در باب هزینه‌های ویژه، به چنین ایده‌ای دست یافته که براساس ماده‌ی ۲۴ منشور، شورای امنیت در این موضوع، منحصراً دارای مسئولیت نبوده و منشور به درستی روشن کرده است که مسئولیت مجمع عمومی نیز مرتبط با صلح و امنیت بین‌المللی است.[1]

از این رو مجمع عمومی علاوه بر حق احرازِ تهدید، وجود شرایط نقض صلح و نیز وقوع تجاوز سایبری، حق توصیه به اقدامات عملی در زمینه‌ی واکنش نسبت به این موضوعات را نیز دارد. بعد از تصویب اساسنامه رم، در فرآیند برگزاری جلسات کمیسیون مقدماتی دیوان کیفری بین المللی، طرحی را در خصوص احراز تجاوز به وسیله‌ی آن دیوان به صورت مشترک از سوی کشورهای بوسنی و هرزگوین، نیوزلند و رومانی، ارائه گردید (دیهیم، ۱۳۸۴: ۱۱۴). بر اساس این طرح، اگر وضعیت مظنون به جنایت تجاوز به ICC ارائه شود و شورای امنیت نیز درباره بروز آن تصمیم‌گیری نکرده باشد، در نخستین مرحله از فرآیند شورای امنیت از طریق دیوان مطلع می‌گردد و در دومین مرحله در صورت محرز نشدن تجاوز از سوی شورا و یا اینکه شورا به ماده ۱۶ اساسنامه یعنی تعلیق تعقیب متوسل نشود، دیوان دارای این توانایی است که ظرف مدت ۱۲ ماه از تاریخ اعلام به شورا، وضعیت پیش آمده را به مجمع عمومی گزارش کرده و به تبع آن از مجمع بخواهد که بر اساس ماده‌ی ۹۶ منشور از دیوان بین‌المللی دادگستری نظر مشورتی تقاضا کند. در سومین مرحله، لازم است تا دیوان دادگستری بین المللی در نظر مشورتی خود، اقدام صورت گرفته را تجاوز محسوب نماید و در صورتی که مجمع عمومی هم با دیوان دادگستری هم‌نظر باشد، دیوان کیفری بین‌المللی می‌تواند فرآیند رسیدگی به جنایت تجاوز را شروع کند.

۳-۴ صلاحیت دیوان بین‌المللی دادگستری

دیوان بین‌المللی دادگستری، براساس ماده ۹۲ منشور سازمان ملل متحد، رکن قضایی اصلی سازمان ملل متحد بوده و اساسنامه‌اش جزء لاینفک منشور به حساب می‌آید.[2] بر اساس ماده‌ی ۳۶ اساسنامه، دیوان در همه‌ی اموراتی که از سوی اطراف دعوی به آن رجوع شده، دارای صلاحیت رسیدگی است. علاوه بر این بر اساس بند ۲ ماده مزبور، دیوان در مورد هرنوع دعوای حقوقی مابین دو طرفی که صلاحیتش را پذیرفته‌اند، در مورد هر مسئله مربوط به حقوق بین‌الملل با وجود هر نوع مسئله‌ای که در صورت اثبات شدن، نقض یک تعهد بین‌المللی را محقق سازد، دارای صلاحیت رسیدگی است (تراهان[3]، ۲۰۱۸: ۲۰۴). از آنجا که موضوع تجاوز سایبری در واقع نقض تعهدات بین‌المللی است که بر اساس بند چهارم ماده ۲ منشور ملل متحد کلیه کشورهای عضو ملل

1. Certain Expenses Of The united Nations (Article 17, Para 2, of The charter) ,20 July 1962 (Case Summaries).

۲. ماده ۹۳ منشور.

3. Trahan.

متحد، آن را پذیرفته و به آن متعهد هستند (میلر، ۲۰۱۴: ۲۲۵)، بنابراین صلاحیت دیوان بین‌المللی دادگستری در بحث احراز تجاوز سایبری و سایر مسائل قضایی مرتبط به آن، براساس نص صریح منشور ملل متحد، آشکار و غیرقابل تردید است. با مداقه در منشور ملل متحد، چنین برمی‌آید که شورای امنیت به هیچ عنوان نسبت به دیوان بین‌المللی دادگستری تقدم ندارد. اینگونه اولویت زمانی می‌توانست استنباط گردد که براساس خواست تهیه‌کنندگان منشور، سازمان ملل متحد به عنوان یک سازمان عمدتاً سیاسی در نظر گرفته می‌شد. لیکن به حساب آوردن تقدم و انحصار صلاحیت برای شورای امنیت نسبت به دیوان بین‌المللی دادگستری نه از مفهوم مسئولیت اولیه شورای امنیت برای حفظ صلح استنباط می‌شود و نه در هیچ یک از دیگر قوانین و مقررات منشور می‌توان دلیلی برای آن پیدا کرد (آیچنشهر[1]، ۲۰۲۰: ۵۲۲). اگرچه شورای امنیت قادر است تصمیماتی راکه دارای ماهیتی حقوقی و الزام‌آور هستند، در جریان رسیدگی به دعوی مطروحه در این شورا مانند قضاوت در مورد یک سرزمین مورد منازعه نسبت به یکی از طرفین مخاصمه، اتخاذ نماید ولیکن اساساً آیین تصمیم‌گیری در شورای امنیت با دیوان بین‌المللی دادگستری دارای تفاوت است. ضروری است که دیوان منحصراً براساس حقوق بین‌الملل تصمیم‌گیری کرده و این در صورتی که معیار تصمیم‌های شورای امنیت عمدتاً بر مبنای معیارهای سیاسی است (فروغی و عباسی، ۱۳۹۰: ۱۱۱). توجه به این تفاوت بنیادین در آیین‌های رسیدگی شورا و دیوان نمی‌توان به طرح دعوی با اعتبار قضاوت دیوان دادگستری در مورد اقدام همزمان در موضوع دعوایی که در شورای امنیت مطرح است، اعتراض کرد[2] (اسلون و هرناندز، ۱۳۹۶: ۹۴). از سوی دیگر براساس ماده ۹۶ منشور، نه فقط مجمع عمومی، حتی شورای امنیت هم این توانایی را دارد که در زمینه‌ی مسائل حقوقی دیوان بین‌المللی دادگستری را به ارائه‌ی رأی مشورتی دعوت کند. این نکته، نشان از تفاوت رویکردها و عملکردهای شورای امنیت و دیوان بین‌المللی دادگستری دارد (تراهان، ۲۰۱۸: ۲۲۸). به صورتی که شورای امنیت تاحدودی دارای رویکردهای سیاسی است ولی عملکرد دیوان، تماماً حقوقی بوده و انگیزه‌های سیاسی در آن دخیل نیست.

۴-۴ صلاحیت دیوان کیفری بین‌المللی و برتری آن

در موقعیتی که شورای امنیت وقوع تجاوز را احراز نکند، مطابق ماده ۱۶ اساسنامه رم می‌تواند[3]، درخواست تعلیق تحقیق یا تعقیب در مورد دعوی مطروحه نزد دیوان را بنماید که در چنین حالتی، دیوان نمی‌تواند هیچ تحقیق یا تعقیبی را در طی ۱۲ ماه شروع نماید و شورای امنیت، امکان تجدید این تصمیم را پس از ۱۲ ماه دارد و از این رو شورای امنیت قادر است که از

1. Eichensehr.
2. Tehran Judgment. International court of justice. (1980), pp. 3, 19, 22.
۳. با صدور قطعنامه‌ای به موجب فصل هفتم منشور.

رسیدگی دیوان جلوگیری به عمل آورد (اوکانل[1] و نیازماتو[2]، ۲۰۱۲: ۱۹۶). باید توجه داشت، لازمه‌ی درخواست تعلیق تحقیق و یا تعلیق تعقیب، کسب اتفاق آرای اعضای دایم شورای امنیت در صدور قطعنامه مربوط ضروری بوده (بلوکر، ۲۰۰۷: ۸۹۵) و تجربه نشان می‌دهد که به دست آوردن این اجماع در شورا، کار دشواری خواهد بود و عملاً موارد اینگونه تعلیق را به شکل قابل توجهی کاهش می‌دهد. لیکن در صورتی که شورای امنیت هیچ تصمیمی در مورد وقوع یا عدم وقوع تجاوز نگیرد و ضمناً نتواند اجماع لازم برای صدور قطعنامه‌ای مبنی بر تعلیق تحقیق یا تعقیب در دیوان، مطابق ماده ۱۶ اساسنامه رم را کسب کند، در خود دیوان می‌تواند به شکایت مطروحه مبنی بر ارتکاب جنایت تجاوز رسیدگی نماید.

دو رژیم صلاحیتی در مورد جرم تجاوز وجود دارد که بسته به شرایطی که در آن وضعیت به دادگاه ارجاع می‌شود، ممکن است «محرک» باشد. مورد اول، طبق ماده ۱۵، با ارجاعات دولتی یا تحقیقات مقتضی توسط دادستان آغاز می‌شود. دومی، مطابق ماده ۱۵، با ارجاعات شورای امنیت آغاز می‌گردد. اگرچه این مکانیسم‌های محرک، ماهیت «رویه‌ای» دارند اما دامنه صلاحیتی که دادگاه می‌تواند در مورد جرم تجاوزکارانه اعمال کند، بر اساس نحوه شروع رسیدگی است (هونگجوکو و بوچوالد ، ۲۰۱۷: ۲۸۸). از این رو، دو صلاحیت جداگانه در مورد جرم تجاوز وجود دارد، بسته به این که آیا صلاحیت قضایی با ارجاع دولتی یا تحقیقات مقتضی یا با ارجاع شورای امنیت آغاز شده است. یکی از تفاوت‌های اصلی این است که برای ارجاعات دولتی و تحقیقات مقتضی، ماده ۱۵ تصریح می‌کند: در رابطه با دولتی که عضو این اساسنامه نیست، دادگاه صلاحیت خود را در مورد جرم تجاوز هنگامی که توسط اتباع آن دولت یا در قلمرو آن کشور ارتکاب یافته باشد اعمال نخواهد کرد. بنابراین، در صورت عدم ارجاع شورای امنیت، دیوان بین‌المللی کیفری تنها در صورتی می‌تواند صلاحیت خود را در مورد جرم تجاوز اعمال کند که هم تابعیت و هم اصول مربوط به قلمرو صلاحیت را رعایت کرده باشد (میرمحمدصادقی، ۱۳۹۵: ۱۷۴). به عبارت دیگر، دیوان کیفری بین‌المللی کیفری تنها می‌تواند از فردی که تبعه یک دولت عضو است، صرفنظر از مصونیت‌های دارا بوده که در رسیدگی دیوان بدون تأثیر خواهد بود؛ به دلیل جنایت تجاوز ناشی از عمل تجاوزکارانه ارتکابی در قلمرو کشور عضو دیگر، تحقیق نماید. اتباع کشورهای غیرعضو و تجاوزاتی که در قلمرو آن‌ها مرتکب شده‌اند از صلاحیت دادگاه در مورد جرم تجاوز براساس ارجاعات دولتی و تحقیقات مقتضی خارج می‌شوند. از آنجایی که ارجاعات شورای امنیت براساس فصل هفتم منشور ملل متحد انجام می‌شود، رضایت کشورهای عضو را می‌توان در ماده ۲۵ منشور ملل متحد یافت که به موجب آن موافقت می‌کنند تصمیمات شورای امنیت را مطابق با این موضوع بپذیرند و اجرا کنند. از طریق این ماده همه کشورها، از

1. O’Connell.
2. Niyazmatov

جمله کشورهایی که عضو اساسنامه رم نیستند، موافقت می‌کنند که شورای امنیت اتباع خود یا جنایتی را که ادعا می‌شود در قلمرو آن مرتکب شده است به دیوان کیفری بین‌المللی ارجاع دهد. بر این اساس، طبق ماده ۱۵، دیوان کیفری بین‌المللی می‌تواند صلاحیت خود را در مورد جرم تجاوز ناشی از عمل تجاوزکارانه ارتکاب یافته توسط هر کشور، از جمله دولت‌های غیر عضو، اعمال کند و به بیان کاملتر باید گفت با ارجاع شورای امنیت، صلاحیت دیوان به «صلاحیت قهری» تبدیل می‌شود (سلیمی،۱۳۹۳ : ۱۸۰) و از این پس عنصر رضایت برای کشورها دیگر زایل گشته و راه برای فرار از رسیدگی دیوان برای متجاوز بسته خواهد شد.

در سال ۲۰۱۷، مجمع کشورهای عضو با اجماع، قطعنامه‌ای را برای فعال کردن صلاحیت دادگاه در مورد جنایت تجاوز (تصمیم فعال‌سازی[1]) را به تصویب رساند (کلاوس، ۲۰۱۹: ۶۰) که تأیید می‌کند در مورد ارجاع دولت یا تحقیقات مقتضی، دادگاه صلاحیت خود را در مورد جنایت تجاوز هنگامی که توسط یک تبعه یا در قلمرو کشور عضوی که این اصلاحات را تصویب یا نپذیرفته انجام شود، اعمال نخواهد کرد. این سوال مطرح می‌شود که آیا براساس ماده ۳۱ (۳) (الف) کنوانسیون وین در مورد حقوق معاهدات[2]، تصمیم فعال‌سازی یک توافق بعدی بین طرفین در مورد تفسیر اساسنامه رم است یا خیر؟ این وظیفه رسیدگی کننده است که هنگام تفسیر اساسنامه رم، به تصمیم فعالسازی اهمیت بدهد (همان: ۶۴). تصمیم فعال‌سازی به عنوان یک قاعده توسط مجمع کشورهای عضو اتخاذ می‌گردد و به این ترتیب بر کنوانسیون وین در مورد حقوق معاهدات غالب شده و از نظر قانونی برای ارکان ICC الزام‌آور می‌شود و بزرگترین کارکرد آن در عرصه بین المللی، اثر «پیشگیرانه» بودن آن (سلیمی، ۱۳۹۹ : ۸۰) و از همه مهمتر آنکه نقطه عطفی در پیشگیری از جنایت تجاوز و مقابله با عالیترین مجرمین بین المللی خواهد بود. (سلیمی، همان:۸۱) بنابراین، رژیم صلاحیتی جنایت تجاوز در صورت ارجاعات دولتی و تحقیقات مقتضی تنها پس از تصویب یا پذیرش توسط هر دو کشور متجاوز و قربانی ادعا شده عضو، قابل اعمال است. چنین به نظر می‌رسد که توانایی، شایستگی و برتری صلاحیت دیوان غیرقابل انکار است. علت این است که تمامی ۱۸ قاضی دیوان، به شکل عادلانه‌ای به نمایندگی از نظام‌های حقوقی اصلی در جهان گرد هم آمده‌اند. این افراد دارای مزیت‌های اخلاقی بوده و به عدالت و درستکاری شهره هستند. بنابراین قضات دیوان کیفری بین‌المللی با صلاحیت شخصی لازم برای احراز وقوع جنایت تجاوز (بدون در نظر گرفتن مصونیت های افراد مرتکب که می‌تواند مفَّری برای دور شدن از عدالت کیفری باشد) دارای صلاحیت‌های فردی بوده و هیچگونه انگیزه‌ای وجود ندارد که قضات دیوان را از احراز وقوع یا عدم وقوع تجاوز بر مبنای عناصر قانونی تجاوز موجود در حقوق بین‌الملل باز دارد.

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

از ۱۷ جولای ۲۰۱۸، وضعیتی که در آن به نظر می‌رسد یک عمل تجاوزکارانه رخ داده است، می‌تواند توسط شورای امنیت (صرفنظر از اینکه شامل کشورهای عضو یا عدم عضو باشد و یا نباشد) به دیوان ارجاع می‌شود. این ارجاع طبق فصل هفتم منشور سازمان ملل متحد عمل می‌کند. در صورت عدم ارجاع عمل تجاوزکارانه از شورای امنیت سازمان ملل، دادستان می‌تواند به ابتکار خود یا بنا به درخواست یک کشور عضو تحقیق را آغاز کند. دادستان ابتدا باید بررسی کند که آیا شورای امنیت در مورد یک عمل تجاوزکارانه توسط دولت مربوطه تصمیم گرفته است یا خیر. در صورتی که ظرف شش ماه پس از تاریخ اعلام وضعیت به شورای امنیت سازمان ملل از سوی دادستان، چنین تصمیمی گرفته نشده باشد، دادستان می‌تواند به تحقیقات ادامه دهد، مشروط بر اینکه بخش مقدماتی اجازه شروع تحقیقات را داده باشد (وانگ[1]، ۲۰۲۱: ۱۵). همچنین تحت این شرایط، دادگاه صلاحیت خود را در مورد جرم تجاوز هنگامی که توسط یک تبعه یا در قلمرو کشور عضوی که این اصلاحات را تصویب یا نپذیرفته است، صورت گرفته باشد، اعمال نخواهد کرد.

بحث و نتیجه‌گیری

با مداقه در نوشتار حاضر چنین به نظر می‌رسد که یکی از مباحثی که در حوزه حملات سایبری، در حقوق بین‌الملل مطرح است، منطبق بودن یا نبودن این دسته از حملات با جنایت تجاوز و واکاوی امکان صلاحیت دیوان کیفری بین‌المللی در رسیدگی به آن‌هاست. تعریف جنایت تجاوز در ماده ۸ مفاد اساسنامه رم دادگاه کیفری بین‌المللی (اساسنامه رم) تصریح می‌کند که عمل تجاوزکارانه دولتی عنصر مادی جنایت است که نشان‌دهنده ارتباط ذاتی بین مسئولیت کیفری فردی (بدور از هرگونه محدودیت و مصونیت قائل شدن برای فرد مرتکب) و مسئولیت دولت است. مفهوم تجاوز سایبری را می‌توان متناظر با مفهوم تجاوز در نظر گرفت، با این شرط که این تجاوز از سوی شبکه‌های متمرکز بر رایانه صورت گرفته باشد. به منظور انتساب جزایی رفتارها و اعمال اشخاص و گروه‌های غیردولتی و خصوصی در حملات سایبری به دولت، ضروری است تا معیار کنترل مؤثر مورد توجه باشد. اگرچه این معیار، با در نظر گرفتن یک آستانه‌ی بالا در عمل، دولت مجنیٌ علیه را برای اثبات، در وضعیت دشواری قرار می دهد. همچنین باید توجه داشت که در تجاوز سایبری از یک سو با اشغال سرزمین یک دولت مواجه نبوده تا بتوان معیار کنترل کلی را اعمال نمود و از سوی دیگر تجاوز دانستن چنین عملی نیز محل نزاع است. بنابراین برای مطابقت حملات سایبری با جنایت تجاوز، ضروری است تا تعریف موسع‌تری از تجاوز در حقوق بین‌الملل ارائه شود. از این رو، به نظر نمی‌رسد که اعمال معیار کنترل کلی از سوی جامعه

1. Wong.

بین‌المللی مورد پذیرش باشد. علاوه بر این، عنصر مادی جنایت در ماده ۸ اساسنامه رم مستلزم آن است که عمل تجاوزکارانه به دلیل ماهیت، شدت و مقیاس آن نقض آشکار منشور ملل متحد باشد و از طرف دیگر ضرورت اعاده وضع به حالت سابق، فارغ از هرگونه محدودیّت و مصونیّت، اجتناب‌ناپذیر باشد. محرز نمودن تجاوز سایبری، پیش‌شرط هر اقدام شورای امنیت به حساب می‌آید و چنین پیش‌شرطی به معنای انحصاری بودن احراز تجاوز سایبری توسط شورای امنیت نیست. در واقع تقدم و اولویت شورای امنیت در بحث احراز تجاوز به این معنا نیست که شورا صلاحیت انحصاری دارد و می‌تواند صلاحیت سایر نهادهای ذیصلاح ملل متحد را در این زمینه سلب نماید. بلکه این ارجاع ابزار بسیار مهم در تغییر صلاحیت تکمیلی به «صلاحیت قهری» برای دیوان است که در دیوان دادگستری بین المللی این امکان موجود نمی‌باشد و راه را برای ممانعت از بی‌کیفر مانی مرتکبین باز خواهد نمود و این همان نقطه عطف برای ایجاد صلح و امنیت بین‌المللی می‌باشد که در دیوان دادگستری بین المللی نمی‌توان یافت. در دیوان کیفری بین‌المللی دو رژیم صلاحیتی درباره‌ی احراز جنایت تجاوز وجود دارد که بسته به شرایطی که در آن وضعیت به دادگاه ارجاع می‌شود، ممکن است «مولد و یا محرک» باشد. مورد اول، مطابق با ارجاعات دولتی یا تحقیقات مقتضی توسط دادستان آغاز می‌شود و مورد دوم، با ارجاعات شورای امنیت. ترکیب دیوان از ۱۸ قاضی تشکیل شده که هرکدامشان نماینده نظام‌های اصلی حقوقی در جهان و دارای مزیت‌های اخلاقی هستند و از ویژگی‌های این قضات می‌توان به کمال، بی‌طرفی و استقلال آن‌ها اشاره نمود. از این رو انگیزه‌ای برای تشخیص ناصحیح در رسیدگی به وقوع تجاوز سایبری از سوی این قضات وجود ندارد و این خود عامل رجحان این نهاد در عرصه بین‌المللی خواهد بود.

منابع:

- اردبیلی، محمد علی (۱۴۰۰) حقوق جزای عمومی، جلد دوم، چاپ پنجاه و هشتم، تهران، انتشارات بنیاد حقوقی میزان
- اسلون، جیمز.جی و هرناندز، گلیدرآی (۱۳۹۶)، دیوان بین‌المللی دادگستری و توسعه حقوق سازمانی سازمان ملل متحد، چاپ اول، تهران: خرسندی.
- باستانی، برومند (۱۳۸۳). جرائم رایانه‌ای و اینترنتی، تهران: انتشارات بهنامی.
- دارابی‌نیا، مرتضی و فروغی‌نیا، حسین (۱۳۹۴)، رابطه شورای امنیت سازمان ملل متحد با دیوان کیفری بین‌المللی در زمینه‌ی جنایت تجاوز سرزمینی، پژوهشنامه حقوق کیفری، شماره ۱۱.
- دیهیم، علیرضا (۱۳۸۴). درآمدی بر حقوق کیفری بین‌المللی در پرتو اساسنامه دیوان کیفری بین‌المللی، تهران: وزارت امور خارجه، مرکز چاپ و انتشارات.
- سلیمی، صادق (۱۳۹۳)، ارتباط شورای امنیت و دیوان بین‌المللی کیفری در پرتو کنفرانس کامپالا، مجله پژوهش حقوق عمومی، شماره ۴۳
- سلیمی، صادق (۱۳۹۹)، محدودیت‌های دیوان بین المللی در اعمال صلاحیت نسبت به مرتکبین جنایت تجاوز، پژوهش حقوق عمومی، شماره ۶۹
- شایگان‌فرد، مجید (۱۳۸۷)، دیوان بین‌المللی کیفری و صلاحیت رسیدگی به جنایت تجاوز، مطالعات حقوق خصوصی، سال ۳۸، شماره ۴.
- عاملی، سعیدرضا (۱۳۹۰). رویکرد قضایی به آسیب‌ها، جرائم و قوانین و سیاست‌های فضای مجازی، چاپ اول، تهران: انتشارات امیرکبیر.
- فروغی، فضل‌الله و عباسی، آسیه (۱۳۹۰)، صلاحیت دیوان کیفری بین‌المللی نسبت به جنایت تجاوز، مطالعات حقوقی، دوره سوم، شماره ۲.
- گیوکی، آذر؛ کفایی‌فر، محمدعلی و رضایی، محمدتقی (۱۴۰۰). حملات سایبری و لزوم رعایت اصول اساسی حقوق بشردوستانه در آن‌ها، تحقیقات حقوقی بین‌المللی، دوره ۱۴، شماره ۵۱.
- میرمحمدصادقی، حسین (۱۳۹۵)، دادگاه کیفری بین‌المللی، چاپ نهم، تهران: دادگستر.
- هنجنی، علی و فرهادنیا، سعید (۱۳۹۷). بررسی مسئولیت بین‌المللی دولت‌ها در قبال اعمال گروه‌های تروریستی، تحقیقات حقوقی، شماره ۸۴.
- Ambos, Kai (2016). "Individual Criminal Responsibility for Cyber Aggression", Journal of Conflict & Security Law, Vol .21, No. 3, pp 495-504.

- Blokker, N. (2007). The Crime of Aggression and The United Nations Security Council. Leiden Journal of International Law, Vol 20, pp 867-894.
- Brier, Søren (2010). Cybersemiotics and The question of knowledge. In:nformation and Computation. Gordana Dodig-Crnkovic & Mark Burgin(eds). World Scientific Publishing Co.
- Claus Kreß (2019). On the Activation of icc Jurisdiction over the Crime of Aggression, Queen Mary Studies in International Law, Vol 33, pp. 43-64.
- Crawford, James (2005), Articles on Responsibility of States for Internationally Wrongful Acts 2001, Lauterpacht Research Centre for International Law, University of Cambridge.
- Development, Concepts and Doctrine Center (2022) Cyber Primer, Head Doctrne, 3rd Edition, Ministry of Defece, P 19
- Eichensehr, K. (2020). The law & politics of cyberattack attribution. UCLA Law Review, 67.
- Goldsmith, Jack (2013). How Cyber Changes the Laws of War, European Journal of International Law, Volume 24, pp 129-138.
- Graham, D. E. (2010). Cyber Threats and the Law of War. Journal of National Security Law and Policy, Vol 4.
- Grigg, D.W (2010). Cyber-Aggression: Definition and Concept of Cyberbullying. Aust. J. Guid. Counsell. Vol 20.
- Hongju Koh, Harold & Buchwald, Todd F (2017). The Crime of Aggression: The United States Perspective, American Journal of International Law, Volume 109, Issue 2, pp. 257 – 295.
- Horowitz, J. (2020). Cyber Operations under International Humanitarian Law: Perspectives from the ICRC. ASIL Insights.
- Kaczorowska, Alina (2015). Public International Law, fifth edition, London: Routledge.
- Madubuike-Ekwe, Joseph N (2021). Cyberattack and the Use of Force in International Law, Beijing Law Review, Vol 12, pp 631-649.
- Michael N Schmitt (2013) fivTallinn Manual on The International Law Applicable To Cyber Warfare1. Cambridge University Press, p.53
- Michael N Schmitt (2017). Tallinn Manual 2.0 on The International Law Applicable to Cyber Operations. Cambridge University Press, pp.82-89
- Miller.Kevin L (2014). The Kampala Compromise and Cyberattacks: Can There Be an International Crime of Cyber-Aggression? Southern California Interdisciplinary Law Journal, vol 23.
- Nguyen, Reese (2013). "Navigating 'Jus Ad Bellum' in the Age of Cyber Warfare." California Law Review 101(4), pp. 1079–1129.

- O'Connell, M. E. and Niyazmatov, M (2012). 'What is Aggression? Comparing the Jus ad Bellum and the ICC Statute', Journal of International Criminal Justice, vol 10, pp 189-207.
- Roscini, M. (2010). World Wide Warfare-Jus Ad Bellum and the Use of Cyber Force. Max Planck Yearbook of United Nations Law, vol 14, pp 85-130.
- Shaw, M. (2010). International Law (6th ed.). Cambridge: Cambridge University Press.
- Trahan, J (2018), From Kampala to New York—The Final Negotiations to Activate the Jurisdiction of the International Criminal Court over the Crime of Aggression, International Criminal Law Review, Vol 18, pp 197-243.
- Wong, Meagan S (2021), Aggression and State Responsibility at The International Criminal Court, International & Comparative Law Quarterly, vol 70, issue 4.