مقاله

مجلهٔ
پژوهشهای حقوق جزا و جرم‌شناسی

علمی ـ پژوهشی

شماره ۱۰

هزار و سیصد و نود و شش ـ نیمسال دوم (دوفصلنامه)

شهر دانش

پژوهشکدهٔ حقوق

http://jclc.sdil.ac.ir/article_58376.html

حمله سایبری به مثابه جنایت تجاوز و بررسی صلاحیت دیوان کیفری بین‌المللی در رسیدگی به آن

دکتر پرستو اسمعیل‌زاده ملاباشی*

چکیده:

از جمله صلاحیت‌های دیوان کیفری بین‌المللی رسیدگی به جنایت تجاوز می‌باشد. در ابتدای تصویب اساسنامه دیوان کیفری بین‌المللی تعریفی از جنایت تجاوز ارائه نشده بود و تعریف این جرم به آینده و بازنگری‌های اساسنامه موکول شد تا اینکه در نهایت تعریف این جرم در سال ۲۰۱۰ در قالب ماده ۸ مکرر اساسنامه دیوان کیفری بین‌المللی مورد تصویب قرار گرفت. با وجود اینکه در تعریف جرم مذکور اشاره‌ای به حملات سایبری نشده است ولی به نظر می‌رسد که می‌توان آن حملات را با توجه به متن اساسنامه دیوان و قطعنامه ۳۳۱۴ مجمع عمومی سال ۱۹۷۴ به عنوان جنایت تجاوز در نظر گرفت. برای اینکه بتوانیم حملات سایبری را در چارچوب جنایت تجاوز مورد بررسی قرار دهیم اینگونه حملات می‌بایستی به آستانه شدت مورد نیاز در مورد تحقق جنایت تجاوز رسیده باشند. در حقیقت آستانه جنایت تجاوز را می‌توان نقض جدی‌ترین قواعد حقوق بین‌الملل دانست. برای تحقق جنایت تجاوز، افرادی که مرتکب حملات سایبری می‌شوند نیز عمدتاً می‌بایستی از اوضاع و احوال واقعی که منجر به نقض آشکار حقوق بین‌الملل می‌شوند، مطلع باشند که البته اثبات این امر در مورد حملات سایبری معمولاً دشوار است. با وجود اینکه می‌توان حملات سایبری را در قالب صلاحیت دیوان کیفری بین‌المللی مورد توجه و بررسی قرار داد ولی به نظر می‌رسد بهترین حالت، توافق دولت‌ها در مورد روشن کردن ابعاد مربوط به حملات سایبری در خصوص جنایت تجاوز و تخصیص قضاتی آگاه به مسائل مربوط به حملات سایبری و تکنولوژی‌های مرتبط با آن در دیوان کیفری بین‌المللی باشد.

مجلهٔ پژوهش‌های حقوق جزا و جرم‌شناسی، شمارهٔ ۱۰، نیمسال دوم ۱۳۹۶
صفحهٔ ۴۳-۶۵، تاریخ وصول: ۱۳۹۶/۰۱/۲۳، تاریخ پذیرش: ۱۳۹۶/۰۷/۱۹

* دکترای حقوق بین‌الملل، دانشگاه آزاد اسلامی واحد نجف‌آباد و مدرس دانشگاه
Email: parastou.esmailzadeh@yahoo.com

کلیدواژه‌ها:
حملات سایبری، تجاوز، دیوان کیفری بین‌المللی، مسؤولیت کیفری.

مقدمه

با پیشرفت تکنولوژی، مباحث حقوقی مربوط به آن نیز وارد مرحلهٔ جدیدی از حیات خود می‌شوند. تحول تکنولوژی و ابزارهای مربوط به آن باعث دگرگونی و تحول در کاربرد متناسب علم حقوق نیز در حوزه‌های مربوطه شده است به نحوی که بعضاً قواعد و مقررات گذشته قادر به پاسخگویی و نظم‌دهی در جرایم ارتکابی و جلوگیری از سوءاستفاده‌های این پیشرفت‌ها نیستند. از جمله پیشرفت‌هایی که در سال‌های اخیر با آن مواجه شده‌ایم به وجود آمدن فضای سایبر و به تبع آن شکل‌گیری حملات سایبری بوده است. حملات سایبری که زاییده پیشرفت تکنولوژی می‌باشند تمام معادلات قانونی قبل از به وجود آوردن این فضا را دگرگون کرده و باعث نیاز به تغییر قواعد و مقررات مربوطه در حوزه‌های داخلی و بین‌المللی شده‌اند. در حوزه حقوق بین‌الملل، حملات سایبری و استفاده از ابزارهای سایبری به عنوان سلاح، باعث نیاز به بررسی ماهیت اینگونه حملات در قالب قواعد موجود حقوق بین‌الملل شده‌اند. با توجه به اینکه معمولاً روند انعقاد معاهده‌ای بین‌المللی برای به نظم درآوردن این موضوع نوپا با مقاومت دولت‌ها و عدم تمایل آنها برای انعقاد چنین معاهداتی در حقوق بین‌الملل مواجه می‌باشد و همچنین با عنایت به فقدان هرگونه رویه و عرف در این خصوص و زمان‌بر بودن به وجود آمدن راهکارهای جدید، چاره‌ای جز انطباق مسائل حادث با مقررات موجود باقی نمی‌ماند. یکی از موضوعاتی که راجع به حملات سایبری در حقوق بین‌الملل مطرح می‌شود انطباق اینگونه حملات در چارچوب جنایت تجاوز و بررسی امکان صلاحیت دیوان کیفری بین‌المللی در رسیدگی به آنهاست. در مقاله حاضر به بررسی این موضوع خواهیم پرداخت که آیا حملات سایبری می‌توانند به عنوان جنایت تجاوز با تعریف فعلی در دیوان کیفری بین‌المللی مورد رسیدگی قرار گیرند یا خیر. در قسمت اول مقاله حاضر به تعریف جنایت تجاوز و صلاحیت دیوان کیفری بین‌المللی در رسیدگی به جنایت تجاوز می‌پردازیم و در قسمت دوم، حملات سایبری را تعریف نموده و خصوصیات آن حملات را مورد تجزیه و تحلیل قرار می‌دهیم. در قسمت سوم مقاله نیز حملات سایبری و امکان وقوع جنایت تجاوز در این حملات و صلاحیت دیوان کیفری بین‌المللی را درباره آن مورد بررسی قرار می‌دهیم.

۱- تعریف جنایت تجاوز و صلاحیت دیوان کیفری بین‌المللی در رسیدگی به آن

۱-۱- تعریف جنایت تجاوز

جنایت تجاوز برای اولین بار تحت عنوان «جرم علیه صلح» توسط دادگاه‌های نورنبرگ و توکیو مورد پیگرد قانونی قرار گرفت. این جرم به عنوان برنامه‌ریزی، آماده‌سازی، شروع و یا به راه انداختن جنگ متجاوزانه و یا جنگ در نقض معاهدات بین‌المللی، توافقات یا تضمینات تعریف می‌شود. در تعریف مذکور مسؤولیت کیفری فردی نیز بسیار موسّع تعریف شده بود به نحوی که تعریف این جرم شامل شرکت در طرح یا توطئه مشترک برای انجام هر عمل متجاوزانه می‌گردید.[۱]

مطابق با بند ۴ ماده ۲ منشور نیز توسل به زور ممنوع اعلام شده است و استثنائات قابل اعمال این ماده مطابق با مواد ۳۹ و ۵۱ منشور یا با تجویز شورای امنیت و یا به عنوان دفاع مشروع است که متعاقباً قطعنامه ۱۴ دسامبر ۱۹۷۴ مجمع عمومی محدودیت‌های مذکور را با شفافیت بیشتری توضیح داده است. مطابق با قطعنامه مذکور تجاوز محدود به توسل به نیروهای مسلح سنتی می‌باشد. زیرا با مطالعه دقیق این قطعنامه مشخص می‌شود که محوریت آن بر دولت‌هاست و مضافاً اینکه در متن این قطعنامه از نمونه‌هایی به عنوان تجاوز ذکر نموده که همگی حکایت از به وقوع پیوستن جنگ‌های سنتی دارد. از جمله این نمونه‌ها تهاجم نیروهای مسلح یک دولت به دولتی دیگر، بمباران کردن سرزمین یک دولت از طریق نیروهای مسلح دولت دیگر و مسدود کردن بنادر و سواحل دولت‌های دیگر از طریق نیروهای مسلح می‌باشند.[۲] در بند ۴ ماده ۳ قطعنامه مذکور نیز در تعریف تجاوز، حمله مسلحانه را محدود به میدان جنگ‌های سنتی شامل زمین، دریا و هوا یا با حمله به نیروهای هوایی یا دریایی و ناوگان‌های هوایی یک دولت می‌کند. البته در مورد شناخت تجاوز در این قطعنامه تقریباً اتفاق نظر وجود دارد چون در قطعنامه مذکور رهنمودهای قابل توجهی در خصوص تعریف تجاوز برشمرده است.[۳] اگرچه در قطعنامه مذکور همان‌طور که اشاره گردید به

1. Kai Ambos, "The Crime of Aggression after *Kampala*," *German Year Book of International Law* 53 (2010): 463-510.
2. Article 3 of the General Assembly's Resolution, 3314 (XXIX), 1974.
3. Carsten Stahn and Goran Sluiter, *The Emerging Practice of the International Criminal Court, Legal Aspects of International Organization* (Leiden: Martinus NIJFOFF Publisher, 2009), Vol. 48, 713.
   Stephen Dycus, "Congress's Role in Cyber *Warfare*," *Journal of National Security Law & Policy* 4:155 (2010): 713.

جنگ‌های سنتی اشاره شده است ولی ماده ۴ قطعنامه مذکور به جامع نبودن مصادیق تجاوز مندرج در ماده قبلی خود اشاره می‌کند. از مواد مندرج در منشور و قطعنامه مذکور نیز این موضوع استنباط می‌گردد که در حقیقت، جنایت تجاوز نقطه اصلی وقوع جنگ است همانند آنچه که مطابق با توافقنامه سال ۱۹۳۳ لندن، تجاوز عمل قهرآمیزی تعریف شده است که یک دولت علیه دولت دیگر انجام می‌دهد.[۴]

در حقیقت می‌توان گفت پیشینه تعریف جنایت تجاوز برای اولین بار به توافقنامه چندجانبه تعریف تجاوز که بین هشت کشور جهان[۵] از جمله ایران در سال ۱۹۳۳ در لندن[۶] منعقد شد برمی‌گردد.[۷] (واحدی، ۱۳۸۹: ۱۱۲، ۱۱۱) این نکته لازم به ذکر است که می‌بایستی میان جنگ تجاوزکارانه که موجب مسؤولیت بین‌المللی دولت می‌گردد و جنایت تجاوز که مسؤولیت کیفری افراد را می‌تواند به دنبال داشته باشد و از جمله موارد اعمال صلاحیت دیوان کیفری بین‌المللی است، تفاوت قائل شد.

۱-۲- صلاحیت دیوان کیفری بین‌المللی در رسیدگی به جنایت تجاوز و تعریف این جرم

شروع تأسیس دیوان کیفری بین‌المللی هم به تصمیم مجمع عمومی سازمان ملل متحد به سال ۱۹۹۴ برمی‌گردد که در آن مجمع تصمیم گرفت تا با الهام از طرح اساسنامه‌ای که کمیسیون حقوق بین‌الملل ارائه داده بود به تأسیس یک دیوان کیفری بین‌المللی مبادرت

۴. اسحاق آل حبیب، *دیوان کیفری بین‌المللی و جمهوری اسلامی ایران* (تهران: مرکز چاپ و انتشارات وزارت امور خارجه، ۱۳۷۸)، چاپ اول، ۵۰۷.

۵. این هشت کشور عبارت بودند از: ایران، افغانستان، استونی، لتونی، لهستان، رومانی، ترکیه و اتحاد جماهیر شوروی.

۶. مطابق با ماده ۲ این معاهده دولتی که ابتدا به یکی از اقدامات ذیل مبادرت کرده باشد، متجاوز شناخته می‌شود: ۱. اعلان جنگ به مملکت دیگر؛ ۲. مورد تهاجم قرار دادن خاک مملکت دیگر به وسیلهٔ قوای مسلح ولو اینکه اعلان جنگ نکرده باشد؛ ۳. حمله به خاک و یا طیارات مملکت دیگر به وسیلهٔ قوای بری یا بحری و یا هوایی ولو اینکه اعلان جنگ نکرده باشد؛ ۴. به محاصره بحری در آوردن سواحل یا بنادر در مملکت دیگر؛ ۵. مساعدت به دسته‌های مسلحی که در خاک او تشکیل گردیده و خاک مملکت دیگر را مورد تهاجم قرار داده‌اند یا امتناع از اتخاذ اقدامات مملکت در خاک خود با وجود تقاضای دولتی که مورد تهاجم واقع شده برای محروم نمودن دسته‌های مسلح مزبور از هرگونه معاضدت یا حمایت.

۷. قدرت‌اله واحدی، *حقوق بین‌الملل کیفری* (تهران: انتشارات جنگل، ۱۳۸۹)، چاپ اول، ۱۱۱ و ۱۱۲.

ورزد. با وجود تمام مخالفت‌ها و دیدگاه‌های موجود در این قضیه[۸]، نهایتاً در ۱۷ جولای سال ۱۹۹۸ اساسنامه‌ای برای ایجاد دیوان کیفری بین‌المللی دائمی در شهر رم تصویب و در تاریخ ۱ جولای سال ۲۰۰۲ اجرایی شد.

دیوان کیفری بین‌المللی اولین و در حال حاضر تنها دیوان بین‌المللی است که صلاحیت رسیدگی به جرایم بین‌المللی را دارد. مطابق با اساسنامه این دیوان، صلاحیت دیوان کیفری بین‌المللی محدود به شدیدترین جرایمی که قابل انتساب به اشخاص هستند، می‌باشد. جرایمی که تحت صلاحت دیوان قرار دارد جرایم نسل‌کشی[۹]، جرایم علیه بشریت[۱۰]، جرایم جنگی[۱۱] و جنایت تجاوز[۱۲] می‌باشند. سه جرم اول به تفصیل در اساسنامه تبیین و تعریف شده است. با وجود این، اعضای شورای امنیت سازمان ملل متحد به قرار دادن جنایت تجاوز در صلاحیت دیوان کیفری بین‌المللی تمایلی نداشتند زیرا مطابق با فصل هفتم منشور ملل متحد، وظیفهٔ حفظ و برقراری صلح و امنیت بین‌المللی و جلوگیری از تجاوز و احراز آن با شورای امنیت بود و شورای امنیت به ویژه اعضای دائم این شورا تمایلی به واگذاری اختیارات خود به دیوان کیفری بین‌المللی نداشتند.[۱۳] در برابر عدم تمایلی که کشورهای عضو شورای امنیت از خود نشان می‌دادند، کشورهایی که خصوصاً به تازگی از استعمار آزاد شده بودند به دلیل وضعیت‌هایی که در سابق تجربه کرده بودند بر تحت شمول قرار گرفتن این جرم در صلاحیت دیوان پافشاری و تأکید می‌کردند.[۱۴] به منظور ایجاد تعادل بین دیدگاه‌های مختلف کشورها در مورد صلاحیت دیوان در رسیدگی به جرایم مربوط به تجاوز، نهایتاً مطابق با ماده ۵ اساسنامه رم صلاحیت رسیدگی به این جرم به دیوان واگذار گردید ولی تعریف جنایت تجاوز به آینده موکول شد.[۱۵] در حقیقت اعمال صلاحیت عملی دیوان در مورد جنایت تجاوز با توجه به اینکه منوط به تعریف جنایت تجاوز و تعیین شرایط آن در زمان تجدیدنظر و

---

۸. ویلیام ا. شبث، *دیوان کیفری بین‌المللی*، ترجمه سید باقر میرعباسی و حمید الوئی نظری (تهران: انتشارات جنگل، ۱۳۸۴)، چاپ اول، ۳۱-۲۴.

9. Genocide.
10. Crimes against Humanity.
11. War Crimes.
12. Aggression.

۱۳. محمدجواد شریعت‌باقری، *حقوق کیفری بین‌المللی* (تهران: انتشارات جاودانه، جنگل، ۱۳۸۸)، چاپ اول، ۲۷ و ۲۸.

14. Benjamin N. Schiff, *Building the International Criminal Court* (New York: Cambridge University Press, 2008), 74.
15. Leila Nadya Sadat, "The International Criminal Court: Past, Present and *Future*," *Washington University Global Studies Law Review* 12 (3) (2013): 410.

بازنگری اساسنامه بعد از هفت سال شد، دیوان در رسیدگی به این نوع از جرایم دارای صلاحیت خفته[۱۶] می‌باشد.[۱۷] در واقع می‌توان گفت جنایت تجاوز به عنوان مبنای درگیری اساسی بین دولت‌ها محسوب شده زیرا اولاً تعریف پذیرفته‌شده‌ای بین دولت‌ها در حقوق بین‌الملل در این خصوص وجود ندارد؛ ثانیاً هیچ توافقی مبنی بر اینکه آیا شورای امنیت می‌بایستی نقشی در تعیین وقوع جنایت تجاوز داشته باشد یا نه حاصل نشده بود.[۱۸] علی‌رغم این موضوع بعضی بر این عقیده بودند[۱۹] در صورتی که شورای امنیت سازمان ملل متحد در موضوعی خاص وقوع جنایت تجاوز را احراز نماید رسیدگی به آن را می‌تواند به دیوان ارجاع دهد. این دیدگاه در راستای ماده ۳۹ منشور ملل متحد[۲۰] شکل گرفت که در گزارش کمیسیون حقوق بین‌الملل نیز در خصوص پیش‌نویس اساسنامه دیوان کیفری بین‌المللی مورد تأکید قرار گرفته است.[۲۱]

با توجه به موضع‌گیری دولت‌ها طی سال‌های اخیر در مورد تعریف جنایت تجاوز و صلاحیت دیوان کیفری بین‌المللی در مورد رسیدگی به آن می‌توان به دو دیدگاه مختلف در این خصوص دست یافت. دیدگاه اول همان‌طور که پیشتر هم بدان اشاره شد متعلق به دولت‌های عضو شورای امنیت است که با تکیه بر منشور ملل متحد، صلاحیت شورا را صلاحیتی انحصاری در احراز جنایت تجاوز می‌دانند. در دیدگاه دوم در مورد احراز جنایت تجاوز برای شورای امنیت، صلاحیت اولیه و نه انحصاری در نظر گرفته می‌شود که در صورت سکوت و یا شکست شورای امنیت، برای دیوان حق مسلم رسیدگی به اینگونه جرایم جایز شمرده می‌شود.[۲۲] در حقیقت عدم موفقیت ارائه تعریفی در خصوص تجاوز ماهیتاً ناشی از

16. Dormant Jurisdiction.
17. Malcolm D. Evans, *International Law* (New York: Oxford University Press, 2010), 3rd Ed, 774
18. Marlies Glasius, *The International Criminal Court A global Civil Society Achievement* (New York: Routledge Taylor & Francis Group, 2006), 62.

۱۹. برای مطالعه بیشتر نک:

Matthias Schuster, "The Rome Statute and the Crim of Aggression: A Gordian Knot in Search of a *Sword*," *Criminal Law Forum* 14 (2003): 35-39.

۲۰. این ماده مقرر می‌دارد: «شورای امنیت وجود هرگونه تهدید علیه صلح، نقض صلح، یا عمل تجاوز را احراز و توصیه‌هایی خواهد نمود یا تصمیم خواهد گرفت که برای حفظ یا اعاده صلح و امنیت بین‌المللی به چه اقداماتی بر طبق مواد ۴۱ و ۴۲ باید مبادرت شود.»

21. Draft Statute for an International Criminal Court with Commentaries, Report of the International Law Commission on the Work of its Forty-sixth Session, 1994, 44, Accessed October 15, 2016, http://legal.un.org/ilc/texts/instruments/english/commentaries/7_4_1994.pdf.

۲۲. علیرضا دیهیم، *درآمدی بر حقوق کیفری بین‌المللی (در پرتو اساسنامه دیوان کیفری بین‌الملل)* (تهران:

چالش‌های سیاسی اساسی بود که دولت‌ها در ارتباط با نقش‌ها و وظایف شورای امنیت و دیگر ارگان‌های سازمان ملل در ارتباط با حفظ و برقراری صلح و امنیت بین‌المللی در منشور سازمان ملل متحد با یکدیگر داشتند.[۲۳] به نظر می‌رسد با توجه به اینکه شورای امنیت رکن سیاسی سازمان ملل متحد است و تاریخ نشان داده است این رکن از اعمال نفوذ قدرت‌های بزرگ جهان که اغلب در شورای امنیت به عنوان اعضای دائم هستند، مصون نبوده است، بهترین وضعیت برای احراز جنایت تجاوز رسیدگی از طریق قضات بی‌طرف دیوان کیفری بین‌المللی باشد.[۲۴]

مطابق با ماده ۵ اساسنامه دیوان کیفری بین‌المللی مقرر گردیده که «دیوان زمانی صلاحیت خود را در مورد جنایت تجاوز اعمال می‌کند که مقرره‌ای مطابق با مواد ۱۲۱ و ۱۲۳ اساسنامه دیوان در خصوص تعریف جنایت تجاوز تصویب گردد و شرایطی که وفق آن دیوان در خصوص این جرم اعمال صلاحیت می‌کند مشخص شود ضمن اینکه مطابق با ماده مذکور چنین مقرره‌ای می‌بایستی با مقررات مربوطه در منشور ملل سازگار باشد. به طور یقین محسوب نمودن جنایت تجاوز به عنوان یکی از جرایمی که در صلاحیت دیوان است می‌تواند حداقل نشان‌دهنده اهمیت این جرم در نگاه جامعه بین‌المللی محسوب شود چه در غیر این صورت یعنی در صورت نبودن این جرم در صلاحیت دیوان، این دیدگاه غالب می‌شد که این جرم در سطح بین‌المللی از اهمیت کافی برخوردار نیست.[۲۵]

بدین‌منظور کنفرانس رم به موجب قطعنامه‌ای کمیسیون مقدماتی را تشکیل داد که یکی از وظایفش بررسی تعریف تجاوز، تعیین عناصر تشکیل‌دهنده آن جرم و شرایط اعمال صلاحیت دیوان بود. کمیسیون مذکور طی سال‌های ۱۹۹۹ تا ۲۰۰۱ اجلاس اول تا هشتم خود را تشکیل داد ولی به دلیل اختلاف‌نظرات گسترده‌ای که بین دولت‌ها وجود داشت

مرکز چاپ و انتشارات وزارت امور خارجه، ۱۳۷۸)، ۵۴۰ و ۵۴۱.

23. Roger S. Clark, "The Crime of Aggression and the International Criminal Court", Edited by José Doria Hans-Peter Gasser M. Cherif Bassiouni, The Legal Regime of the International Criminal Court, Essays in Honor of Professor Igor Blishchenko, Martinus NIJHOFF Publisher Claus Kreb, Leonie von Holtzendorff, "The Kampala Compromise on the Crime of Aggression" (Leiden: Journal of International Criminal Justice, 2010), 663.

۲۴. برای دیدن نظریهٔ موافق نک:

Larry May, *Aggression and Crimes Against Peace* (New York: Cambridge University Press, 2008), 227.

۲۵. برای مطالعه بیشتر نک: جواد طهماسبی، *صلاحیت دیوان کیفری بین‌المللی* (تهران: انتشارات جاودانه، جنگل، ۱۳۸۸)، چاپ اول، ۲۶۸.

نتیجه‌ای از این نشست‌ها حاصل نشد[۲۶] تا اینکه گروه کاری ویژه در این خصوص بعد از تشکیل جلسات متعدد از سال ۲۰۰۳ تا ۲۰۰۹ مجموعه‌ای از اصلاحیه‌ها را ارائه داد. اصلاحیه‌های مذکور مبتنی بر تعریف تجاوز در قطعنامه ۳۳۱۴ سال ۱۹۷۴ مجمع عمومی بود ولی اصلاحیه‌های پیشنهادی محدوده وقوع جنایت تجاوز را تا حد قابل توجهی کاهش می‌داد. این اصلاحیه در کنفرانس بازنگری کامپالا در سال ۲۰۱۰ مورد تصویب دولت‌های عضو اساسنامه دیوان کیفری بین‌المللی قرار گرفت. پیشنهاد مذکور در قالب بند ۱ ماده ۸ مکرر اساسنامه دیوان کیفری بین‌المللی، جنایت تجاوز را برنامه‌ریزی، آماده‌سازی، آغاز یا اجرای عملی تجاوزکارانه توسط شخصی که در موقعیت اعمال کنترل یا هدایت عملی اقدام سیاسی یا نظامی یک دولت قرار دارد و آن عمل به واسطه ماهیت، شدت و گستره‌اش نقض آشکار منشور ملل متحد محسوب می‌شود، تعریف می‌کند. در ادامه بند ۲ ماده ۸ مکرر عمل تجاوزکارانه مذکور در بند ۱ را استفاده یک دولت از نیروهای مسلح علیه حاکمیت، تمامیت سرزمینی یا استقلال سیاسی دولت دیگر یا به هر شیوه دیگری که با منشور ملل متحد ناسازگار باشد در نظر می‌گیرد. در ادامه ماده مذکور مصادیق مندرج در قطعنامه ۳۳۱۴ سال ۱۹۷۴ مجمع عمومی به عنوان اعمال متجاوزانه آورده شده است. هیئت‌های نمایندگی در کامپالا علی‌رغم ارتباط بین ممنوعیت تجاوز که نقض جدی ممنوعیت استفاده از زور محسوب می‌شود و جنایت یا جنایت تجاوزی را که افراد مرتکب آن می‌شوند، بین آنها تفکیک قائل شد.[۲۷]

تعریف تجاوز در ماده ۸ مکرر اساسنامه رم را می‌توان به دو بخش تقسیم نمود. بخش اول عمل متجاوزانه[۲۸] و بخش دوم نیز جنایت تجاوز. در حالی که یک عمل متجاوزانه شکلی از رفتار دولت است، جنایت تجاوز بر مسؤولیت کیفری افراد تمرکز می‌کند. برای اینکه فردی برای ارتکاب جنایت تجاوز مورد تعقیب قرار گیرد ابتدا در قضیه مذکور می‌بایستی تجاوزی از جانب دولت به وقوع پیوسته باشد.[۲۹] با توجه به متن بند ۲ ماده ۸ مکرر اساسنامه رم، عمل تجاوزکارانه محدود به مواردی که احصاء شده نمی‌باشد. از یک طرف هر اقدامی را که با

---

۲۶. طهماسبی، پیشین، ۲۶۹.

۲۷. عبدالمجید سودمندی، مترجم، *رسیدگی به جنایت تجاوز در دیوان کیفری بین‌المللی* (تهران: مؤسسه فرهنگی هنری انتشاراتی نگاه بینه، ۱۳۹۴)، ۳۰.

28. The Act of Aggression.

29. Matthew Gillett, "The Anatomy of an International Crime: Aggression at the International Criminal *Court*," *International Criminal Law Review* 13: 4 (2013): 836.

منشور ملل متحد مباینت داشته باشد را مورد توجه قرار می‌دهد و از طرف دیگر مصادیق ذکرشده به عنوان اعمال متجاوزانه را جامع و حصری تلقی نمی‌کند.

در کنفرانسی که در سال ۲۰۱۰ در کامپالا به منظور بازنگری اساسنامه دیوان کیفری بین‌المللی تشکیل گردید، اعضای شرکت‌کننده در کنفرانس مذکور تصمیماتی را در خصوص تعریف عمل متجاوزانه و جنایت تجاوز اتخاذ نمودند و صلاحیت رسیدگی دیوان کیفری بین‌المللی به جرم مذکور را به طور بالقوه حتی در صورتی که شورای امنیت موضوعی را به دیوان ارجاع ننماید، در نظر گرفتند. دولت‌های شرکت‌کننده تصمیم گرفتند که صلاحیت دیوان در رسیدگی به این جرم تا مدتی پس از ۱ ژانویه ۲۰۱۷ برمبنای تصمیم لاحق اجرا نگردد. حتی بعد از تاریخ مذکور نیز صلاحیت دیوان در رسیدگی به این جرم محدود می‌باشد زیرا به منظور اعمال نشدن صلاحیت دیوان نسبت به دولت‌ها چندین استثناء برای دولت‌ها وجود دارد که مطابق آن صلاحیت دیوان نسبت به کشورهایی که عضو دیوان نیستند قابل گسترش نمی‌باشد. در خصوص مباحث مربوط به برنامه فعال‌سازی دقیق صلاحیت دیوان نیز ابهامات زیادی وجود دارد.[۳۰] مطابق با مصوبه کنفرانس بازنگری کامپالا در مورد اساسنامه دیوان کیفری بین‌المللی، صرفاً جرایم تجاوزی که توسط تصمیم متعاقب دولت‌های عضو در سال ۲۰۱۷ اتخاذ می‌شود در محدوده صلاحیت دیوان قرار خواهند گرفت. به بیان دیگر، جرایم تجاوزی که تا قبل از سال ۲۰۱۷ به وقوع پیوسته باشند جزء صلاحیت دیوان نیستند حتی اگر ۳۰ کشور مورد نظر اصلاحات مربوطه را قبل از سال ۲۰۱۷ تصویب و یا قبول کنند. از طرف دیگر در صورتی که شورای امنیت اقدامی انجام ندهد، موضوعی که می‌بایستی مورد توجه قرار گیرد این است که اگر یکی از کشورهای عضو، الحاقیه‌ها را تصویب و یا قبول نکند صلاحیت دیوان در مورد جنایت تجاوز در مقابل آن دولت اعمال می‌شود یا خیر. به بیان دیگر موضوع مورد بحث این است که آیا قصور دولت در تصویب الحاقیه‌ها به این معناست که صلاحیت دیوان در مقابلش قابل اعمال نیست و یا اینکه آن دولت می‌بایستی به طور ایجابی عدم تمایل خود را در اعمال صلاحیت دیوان اعلام نماید.[۳۱] مطابق با بند ۵ ماده ۱۲۱ اساسنامه دیوان کیفری بین‌المللی، در صورتی که دولت عضو، الحاقیه را تصویب و یا قبول نکرده باشد دیوان نمی‌بایستی صلاحیت خود را در مورد جرمی که در الحاقیه آمده است

30. Sean D. Murphy, *The Crime of Aggression at the ICC, Oxford Handbook of the Use of Force in International Law* (New York, Marc Weller, ed., Oxford University Press, 2015), 533, 534.
31. Ibid, 17, 18.

نسبت به اتباع دولت مذکور یا سرزمین دولت مذکور که جرم در آن به وقوع پیوسته اعمال نماید. به این ترتیب ملاحظه می‌گردد با توجه به ترتیباتی که در مورد صلاحیت دیوان در رسیدگی به جنایت تجاوز مورد توافق قرار گرفته است مرتکبین این جرایم همگی نمی‌توانند مورد تعقیب و محاکمه قرار گیرند.

۲- تعریف و خصوصیات حملات سایبری

۲-۱- تعریف حملات سایبری

با وارد شدن تکنولوژی‌های نوین به زندگی روزمره جوامع در سطح بین‌المللی، حوزهٔ حقوق جنگ نیز از اینگونه پیشرفت‌ها بی‌تأثیر نمانده است. همان‌طور که فضای سایبر در داخل کشورها باعث به وجود آمدن انواع جدیدی از جرایم که با عنوان جرایم سایبری از آنها یاد می‌شود شده است، در سطح بین‌المللی هم به وجود آمدن فضای سایبر و به دنبال آن سوءاستفاده‌ها از این فضا که از جملهٔ آنها توسل به حملات سایبری است، باعث شده است که عناوین مجرمانه متفاوتی در انطباق با این فضای جدید شکل گرفته و یا اینکه عناوین موجود به شکلی متفاوت و با بهره‌گیری از فضای سایبر مورد بررسی و تجزیه و تحلیل قرار گیرند. تعریف واحدی از حملات سایبری وجود ندارد ولی اینگونه حملات را می‌توان عملیاتی تعریف نمود که باعث اختلال[۳۲]، نفی[۳۳]، تنزل[۳۴] و تخریب[۳۵] اطلاعات موجود در کامپیوترها و شبکه‌های کامپیوتری یا خود کامپیوترها و شبکه‌های کامپیوتری می‌شوند.[۳۶] حملات سایبری می‌توانند از شدت و ضعف متفاوتی برخوردار باشند. این حملات می‌توانند از ایجاد اخلال در دسترسی به اطلاعات موجود در کامپیوترها و سیستم‌ها تا حملات سایبری به سیستم‌های بیمارستان‌ها، سیستم‌های تدافعی یک دولت، سیستم‌های مالی، سیستم‌های مربوط به حمل و نقل و غیره دولت‌ها متغیر باشد. حمله سایبری مؤثر به هرکدام از سیستم‌های مذکور می‌تواند اثرات بسیار مخرب و فاجعه‌باری را در پی داشته باشد. به عنوان مثال حمله سایبری به

32. Disrupt.
33. Deny.
34. Degrade.
35. Destroy.
36. Sophie Charlotte Pank, *What is the Scope of Legal Self-Defense in International Law?*, Aarhus Denmark, Juridik Institut, Jus Ad Bellum with a Special View to New Frontier for Self-Defense, RETTID, Specialeafhandling 19, http://law.au.dk/fileadmin/Jura/dokumenter/forskning/rettid/Afh_2014/afh19-2014.pdf, Visited on 15 March 2016, 2014, 7, 8.

شبکه‌ها و سیستم‌های مربوط به حمل و نقل می‌تواند باعث برخورد هواپیماها و یا تصادم بین قطارها شود و یا در مورد حمله سایبری به خدمات آب‌رسانی نیز می‌توان گفت این حملات ممکن است باعث باز شدن سدها و جاری شدن آب آنها شوند.[۳۷]

وقوع حملات سایبری که دولت‌ها در سال‌های اخیر با آنها مواجه شده‌اند در واقع زنگ خطری برای مواجهه روزافزون دولت‌ها با اینگونه حملات بود. حملات سایبری به استونی در سال ۲۰۰۷، حملات سایبری به گرجستان در سال ۲۰۰۸، انتشار ویروس استاکس‌نت در سال ۲۰۱۰، حملات سایبری به شرکت سونی و بسیاری دیگر از اینگونه حملات که دولت‌ها با آنها مواجه شده‌اند موضوع رویارویی روزافزون دولت‌ها را با اینگونه حملات و یا حتی حملات سایبری شدیدتر، پررنگ‌تر می‌کند.

۲-۲- خصوصیات حملات سایبری

خصوصیاتی که معمولاً حملات سایبری که در فوق به آنها اشاره گردید دارند، این است که آنها اخلال در سیستم‌های غیرنظامی را نیز ایجاد می‌کنند. اگرچه ایراد خسارات جانی و یا مرگ نیز می‌تواند از جمله آثار حملات سایبری در نوع شدیدترین آنها باشد، ولی حملات سایبری که دولت‌ها معمولاً با آنها مواجه می‌شوند از جمله حملاتی هستند که منتهی به اخلال در استفاده شهروندان از سیستم‌های بانکی و منابع رسانه‌ای و دیگر خدمات ارائه‌شده توسط دولت به شهروندانشان می‌شوند. از جمله خصوصیات دیگر حملات سایبری این است که حملات سایبری اغلب توسط بازیگران غیردولتی به وقوع می‌پیوندند در حالی که تحت تعقیب قرار گرفتن مطابق با حقوق بین‌الملل مستلزم آن است که اقدامات توسط بخش دولتی صورت گرفته باشد و در حملات سایبری معمولاً انتساب حملات سایبری که توسط اشخاص صورت می‌پذیرد به دولت دشوار است.[۳۸]

اثرات حملات سایبری معمولاً یا مستقیم هستند یا غیرمستقیم[۳۹].[۴۰] در حملات سایبری اثرات مستقیم بر روی سیستم کامپیوتری یا شبکه مورد هدف قرار می‌گیرد در حالی که اثرات غیرمستقیم بر سیستم‌هایی که با سیستم مورد هدف قرارگرفته تعامل دارند و مردمی که بر

37. Jay P. Kesan and Carol M. Hayes, "Mitigative Counterstriking: Self-Defense and Deterrence in *Cyberspace*," *Harvard Journal of Law and Technology* 25(2) (2012), 445.
38. Keven L. Miller, "The Kampala Compromise and Cyberattacks: Can There be an International Crime of *Cyber-Aggression?*," *Southern California Interdisciplinary Law Journal* 23 (2014): 227-229.
39. Direct and Indirect Effects.
40. Dycus, op.cit., 163.

آن سیستم تکیه کرده‌اند، ظاهر می‌شود. اثرات مستقیم می‌توانند شامل به خطر انداختن انسجام، اعتماد و در دسترس بودن سیستم‌ها شوند ولی چنین اثرات مستقیمی معمولاً برگشت‌پذیر می‌باشند.[۴۱] اثرات غیرمستقیم حملات سایبری معمولاً بیشتر و گسترده‌تر از اثرات مستقیم هستند زیرا بیشتر تمرکز حمله‌کنندگان بر تخریب بعد از حمله است تا آسیب‌رسانی به سیستم‌هایی که مستقیماً مورد حملات سایبری قرار می‌گیرند. در بعضی موارد حتی اثرات غیرمستقیم حملات سایبری بسیار وخیم‌تر و سنگین‌تر از اثرات مستقیم اینگونه حملات هستند و برخلاف اثرات مستقیم حملات سایبری که قابلیت برگشت‌پذیری دارند، اثرات غیرمستقیم این حملات معمولاً به راحتی به حالت اولیه قبل از حمله درنمی‌آیند. اثرات غیرمستقیم حملات سایبری می‌توانند شامل پیامدهای اقتصادی قابل توجه و مهمی باشند که نه‌تنها دولتی را که مورد حملات سایبری قرار گرفته است تحت تأثیر قرار می‌دهد بلکه آثار این حملات می‌توانند به کشورهای دیگری که با کشور قربانی حملات سایبری به نوعی در ارتباط هستند نیز تأثیر گذارد. مضافاً اینکه در صورتی که یک کمپانی و یا شرکت با حملات سایبری مواجه شود تعمیر سیستم آن کمپانی خصوصی کاری پرهزینه است و هم‌زمان حملات انجام‌شده قابلیت تخریب شهرت آن کمپانی را هم دارد. ترس از حملات سایبری بر رفتار کاربران اینترنت نیز که می‌بایستی اقدامات مهمی را در زمانی خاص انجام دهند، همانند پرداخت مالیات و یا قسط‌های بانکی تأثیر می‌گذارد و این موضوع باعث ناامنی در فضای سایبر و عدم اعتماد کافی کاربران به این فضا می‌شود. نتایج و اثرات حملات سایبری در مقایسه با سلاح‌های سنتی ذاتاً معلوم نیستند به نحوی که برخی از مفسرین بر این عقیده هستند که حتی یک حمله کوچک سایبری می‌تواند آثار بسیار مخربی را با خود به همراه داشته باشد.[۴۲] این آثار مخرب تا حدی می‌توانند ویرانگر باشند که بعضاً حمله‌ای سایبری می‌تواند به عنوان حمله‌ای مسلحانه با توجه به شدت و وخامتش تلقی شود یعنی اینگونه حملات سایبری منتهی به ایراد خسارات جانی و مالی به افراد می‌شوند.[۴۳] در بین اثرات حملات سایبری که در فوق به آنها اشاره کردیم اثراتی که دولت‌ها در حملات سایبری با آنها سر و کار دارند اغلب از نوع اثرات غیرمستقیم است زیرا هدف از حملات سایبری به دولت‌ها

41. Kesan & Hayes, op.cit., 431.
42. Ibid, 431, 432.
43. Knut Dormann, "Applicability of the Additional Protocols to Computer Network Attacks", Stockholm, International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Published online by International Committee of the Red Cross, Accessed September 11, 2016, https://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf, (2004): 2, 3.

بجا گذاشتن آثار مخربی است که به راحتی قابلیت بازگشت به وضعیت قبل از حمله را نداشته باشند.

از طرف دیگر، با توجه به ماهیت حملات سایبری و در دسترس بودن این فضا، همه افراد در سراسر جهان می‌توانند با در اختیار داشتن امکاناتی کم و با هزینه‌ای ناچیز مبادرت به حملات سایبری علیه دولت‌ها نمایند. حملات سایبری هم که در سال‌های اخیر به وقوع پیوسته است از جمله حملاتی که به کشور گرجستان صورت پذیرفت همگی حاکی از این بود که این حملات توسط اشخاصی از خارج از خاک این کشور صورت پذیرفته بودند که هیچ ارتباط مستقیمی با سازمان و نهادی خاص نداشتند. در حقیقت می‌توان گفت از بین رفتن مرزها در فضای سایبر خصوصیتی است که این فضا با خود به همراه داشته است که شاید بتوان به یقین ادعا نمود که تا قبل از به وجود آمدن این فضا، حقوق بین‌الملل با چالش‌های مشابهی در این زمینه مواجه نشده بود. حتی استفاده از تکنولوژی‌های جدید در صنعت هواپیما و دوربردها هم با وجود اینکه پیشرفت قابل توجهی را در طی کردن مرزهای یک کشور به وجود آوردند ولی ماهیتاً با فضای سایبر متفاوت هستند. از آنجایی که این فضا به طور ملموس قابل مشاهده نیست حملاتی هم که در این فضا صورت می‌پذیرند به راحتی قابل تشخیص و شناسایی نیستند. در حقیقت این فضا نه‌تنها مرزهای سنتی بین کشورها را با چالش مواجه کرده بلکه مفاهیم متفاوتی را از مرز در حوزه حقوق بین‌الملل مطرح نموده است.[۴۴] در واقع از جمله خصوصیات بارز دیگری که حملات سایبری دارند این است که اینگونه حملات اغلب توسط بازیگران غیردولتی صورت می‌پذیرند زیرا با توجه به اینکه برعکس سلاح‌های سنتی، ابزار و وسایل مورد استفاده در مورد حملات سایبری به آسانی و با هزینه‌ای کم در اختیار افراد عادی قرار می‌گیرند. نتیجتاً اینکه امروزه خصوصیت مذکور در فضای سایبر باعث دگرگونی مفاهیم سنتی مربوط به حقوق جنگ و دیگر رشته‌های حقوق بین‌الملل شده است.

از جمله خصوصیات حملات سایبری که با شدت زیادی در جهان به وقوع پیوسته‌اند را

---

۴۴. برای مطالعه بیشتر نک:

Wolff Heintschel von Heinegg, Legal Implications of Territorial Sovereignty in Cyberspace, (4th International Conference on Cyber Conlfict, NATO CCD COE Publications, Tallinn, Accessed October, 2016, 2012, https://ccdcoe.org/sites/default/files/multimedia/pdf/1_1_von_Heinegg_LegalImplications OfTerritorialSovereigntyInCyberspace.pdf.

می‌توان به همراه داشتن مرگ و یا تخریب فیزیکی اموال بیان نمود.[۴۵] به عبارت دیگر حملات سایبری که با شدت و وخامت زیادی علیه دولت‌ها به وقوع می‌پیوندند اغلب زیرساخت‌های حیاتی کشورها را مورد هدف قرار می‌دهند. هرچند آنچه که دولت‌ها بیشتر با آن مواجه می‌شوند حملات سایبری هستند که از شدت کمی برخوردار هستند و تعداد اینگونه حملات به مراتب بسیار قابل توجه‌تر از حملات سایبری است که به عنوان جنگ سایبری تلقی می‌شوند با این وجود حملات سایبری با شدت بالا نیز نباید از توجهات پنهان ماند.

از طرفی دیگر، هرگونه تعقیب مطابق با حقوق بین‌الملل عموماً در قبال یک دولت صورت می‌پذیرد ولی با این وجود جنگ‌های سایبری اخیر از جمله حملات سایبری به استونی و گرجستان و همین‌طور ویروس استاکس‌نت نشان دادند که دولت‌ها می‌توانند حملات سایبری را طراحی کرده و با در اختیار قرار دادن تجهیزات لازم برای انجام حملات، عده‌ای افراد عادی را نیز اجیر نموده و به وسیلهٔ آنان حملات سایبری را علیه دولت‌های دیگر انجام دهند. به بیان دیگر دولت‌ها با توجه به خصوصیات فضای سایبر که از جمله آنها ناشناس ماندن حمله‌کنندگان است، از این فضا استفاده نموده و حملاتی را که می‌خواهند علیه دولت‌های خاص انجام دهند به واسطهٔ افراد عادی و به صورت غیرمستقیم به انجام رسانیده و هدایت می‌کنند. مباحث مربوط به انتساب و برقراری ارتباط بین فردی که حملات سایبری را انجام داده است به دولتی خاص کار ساده‌ای نیست خصوصاً اینکه در فضای مجازی از بین بردن آثار ارتکاب جرم می‌تواند راحت‌تر و قابل دسترس‌تر از دنیای واقعی باشد.

۳- حملات سایبری و جنایت تجاوز

همان‌طور که پیشتر نیز اشاره گردید با گسترش تکنولوژی‌های مرتبط با فضای مجازی، مفاهیم نوینی نیز الزاماً می‌بایستی وارد ادبیات حقوق بین‌الملل شوند و به تبع آن نیز راه‌حل‌های حقوقی مناسب با توجه به شرایط و وضعیت‌های کنونی ایجاد و در نظر گرفته شود. با وجود اینکه حملات سایبری سال‌های طولانی است که سیستم‌ها و کامپیوترهای کاربران، اعم از دولتی و خصوصی را تحت تأثیر خود قرار می‌دهد اخیراً توجهات قابل ملاحظه‌ای را به سمت خود جلب نموده است به طوری که حقوقدانان نظریه‌ها و تفاسیر و تعابیر متفاوتی را از ورود این تکنولوژی به عرصه بین‌المللی و انطباق آن با قواعد موجود حقوق بین‌الملل ارائه کرده‌اند. دلیل توجه و اهمیت روزافزون به حملات سایبری بیشتر به

45. Miller, op. cit., 227.

دلیل این است که با پیشرفت تکنولوژی اینگونه حملات قابلیت تخریب بیشتری را نیز ایجاد نموده‌اند و هم‌زمان افزایش قابل توجه اینگونه حملات هم تأثیر بسزایی در اهمیت آنها داشته است. یکی از موضوعاتی که در مورد حملات سایبری مورد توجه و بررسی قرار گرفته است امکان وقوع جنگ سایبری و توسل به زور با این حملات است. تکنولوژی‌های امروزی به طور یقین با مفاهیم و قواعد موجود در حقوق بین‌الملل هماهنگی کامل ندارند زیرا شکل‌گیری قواعد مذکور در حقوق بین‌الملل به قبل از ایجاد فضای سایبر برمی‌گردد و از طرف دیگر به دلیل اینکه به نظم درآوردن این فضا در سطح بین‌الملل به زمان زیادی نیاز دارد و با توجه به استفاده دوگانه‌ای که از این فضا می‌شود معمولاً دولت‌ها تمایل زیادی برای انعقاد معاهده‌ای بین‌المللی به منظور نظم دادن به این حوزه جدیدالورود به حقوق بین‌الملل و تبیین مفاهیم آن نشان نمی‌دهند. بنابراین در نبود قواعدی مستقیم برای به نظم درآوردن این بخش از تکنولوژی در حقوق بین‌الملل چاره‌ای جز بررسی قابلیت تطبیق قواعد فعلی حقوق بین‌الملل در این حوزه نیست. از زاویه‌ای دیگر تکنولوژی حاضر تغییر قابل توجهی در افرادی که مبادرت به جنگ و توسل به زور از طریق حملات سنتی انجام می‌دادند، به وجود آورده است به این معنی که با توجه به ماهیت فضای سایبر که قابل دسترس برای همگان می‌باشد سلاح‌های سایبری به راحتی در اختیار افراد عادی قرار می‌گیرند. البته این نکته را نیز می‌بایستی مورد توجه قرار داد که موضوع بررسی به وقوع پیوستن جنایت تجاوز در خصوص حملات سایبری زمانی امکان‌پذیر است که دولت خود این حملات را انجام دهد و یا حملات سایبری که از طریق افراد صورت پذیرفته‌اند، قابلیت انتساب به دولت را داشته باشند.

همان‌طور که قبلاً نیز اشاره گردید قطعنامه۳۳۱۴ سال ۱۹۷۴ مجمع عمومی سرآغاز و پیش‌درآمدی بر تعریف تجاوز در حقوق کیفری بین‌المللی است. در حقیقت قطعنامه مذکور مبنای مذاکرات در خصوص اینکه چه اعمالی از فرمانده و هدایت‌کنندگان جنگی به عنوان تجاوز تلقی می‌شود، بود. بنابراین تعریف جنایت تجاوز نیز تا حدود زیادی برگرفته از قطعنامه مجمع عمومی است.[۴۶] با وجود اینکه بازنگری اساسنامه در کامپالا و توافقات حاصله از آن بدون نقص نمی‌باشد ولی بالاخره بعد از سال‌ها کشمکش، دولت‌های عضو توانستند تصمیم بر آماده‌سازی زمینه‌های مربوط به صلاحیت دیوان در رسیدگی به این جرم را فراهم کنند.[۴۷]

46. Jonathan A. Ophardt, "Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's *Battlefield*," *Duke Law and Technology Review* 3 (2010): 13.

47. Claus Kreb, Leonie von Holtzendorff, "The Kampala Compromise on the Crime of ←

با توجه به متن بند ۲ ماده ۸ مکرر اساسنامه رم که عبارت‌پردازی قطعنامه ۳۳۱۴ مجمع عمومی سال ۱۹۷۴ را در مورد تعریف تجاوز تکرار می‌کند، روش‌های نوین جنگی از جمله توسل به زور سایبری را که در آن سال غیر قابل پیش‌بینی بود و در حال حاضر از جمله موضوعات مدرن و مهم حقوق بین‌الملل می‌دانند، مورد توجه قرار نداده است. البته این نکته نیز لازم به ذکر است که مصادیق بیان‌شده مطابق با متن بند ۲ ماده ۸ مکرر اساسنامه رم تمثیلی است و به صورت حصری بیان نگردیده است ولی اینگونه اقدامات برای اینکه بتوانند جنایت تجاوز محسوب شوند می‌بایستی به طور مضیق تفسیر شوند تا با اهداف مندرج در ماده مذکور هماهنگی داشته باشند.[۴۸]

از سوی دیگر این نکته نیز باید مورد توجه قرار گیرد که با در نظر گرفتن مفهوم حملات مسلحانه در قالب ماده ۵۱ منشور ملل متحد، دیوان بین‌المللی دادگستری در نظریه مشورتی خود در مورد مشروعیت تهدید به استفاده از سلاح‌های هسته‌ای در سال ۱۹۹۶[۴۹] بیان نمود که اعمال حق دفاع مشروع بستگی به نوع سلاحی که برای حمله مورد استفاده قرار می‌گیرد ندارد. البته در مورد اقدامات سایبری تلقی آن اقدامات به عنوان سلاح به نظر موضوعی دشوار می‌باشد. با این وجود به نظر می‌رسد حملات سایبری مخربی که آثار آنها با حملاتی که با سلاح‌های سنتی صورت می‌پذیرند، یکسان باشد و زیرساخت‌های حیاتی دولت‌ها را تخریب کند و تلفات جانی و مالی در پی داشته باشد را بتوان در قالب بند ۲ ماده ۸ مکرر اساسنامه رم به عنوان جنایت تجاوز محسوب نمود.[۵۰] بدین معنی که ایراد خسارات فیزیکی به اشخاص و یا تخریب اشیاء که فراتر از حملات ساده به برنامه‌ها و یا اطلاعات کامپیوتری هستند می‌توانند به عنوان اعمال خشونت‌آمیز تلقی شوند همانند حملات سایبری که سیستم کنترل‌کننده سد را در اختیار می‌گیرد که نتیجتاً منتهی به باز شدن سد و کشته شدن افرادی که در آن منطقه قرار دارند، می‌شود.[۵۱]

بنابراین در صورتی که بخواهیم جرایم سایبری را در چارچوب جنایت تجاوز مورد بررسی قرار دهیم، اینگونه حملات می‌بایستی به آستانه مورد نیاز رسیده باشند. تشخیص این موضوع

Aggression," *Journal of International Criminal Justice* (2010): 1217.

48. Otto Triffterer and Kai Ambos, T*he Rome Statute of the International Criminal Court: A Commentary* (C. H. BECK. Hart. Nomos Publications, 2016), 617.
49. Legality of the Threat of Use of Nuclear Weapons, Advisory Opinion of International Court of Justice, 1996, para. 39.
50. Triffterer & Ambos, op.cit., 617.
51. Ibid, 355, 356.

بستگی به معیار وقوع تجاوز یعنی نقضی آشکار دارد که می‌بایستی با خصوصیت شدت و مقیاس کافی نیز همراه باشد. به عبارت دیگر آستانه تحقق جنایت تجاوز را می‌توان نقض جدی‌ترین قواعد حقوق بین‌الملل تلقی نمود.[۵۲] البته در صورتی جنایت تجاوز به وقوع می‌پیوندد که فرد مجرم از اوضاع و احوال واقعی که منجر به نقض آشکار می‌شود، مطلع باشد. این معیار در حقیقت بیان‌کنندهٔ الزامات عنصر معنوی مندرج در ماده ۳۰ اساسنامه رم است که هم قصد و هم اطلاع را با هم دربر می‌گیرد. بنابراین می‌توان گفت که مقرره‌های مذکور مجرمیت را محدود می‌کنند.[۵۳]

در مورد حملات سایبری مسؤولیت فردی همانند دیگر حملات، محدود به اشخاصی است که سطحی از فرماندهی با کنترل مؤثر بر سیاست تهاجمی دولت خود دارند و دولتی بودن این افراد برای وقوع جنایت تجاوز در حملات سایبری از اهمیت زیادی برخوردار است. اگرچه مسؤولین دولتی در رده‌های بالا در مورد حملات سایبری اطلاعات فنی و تکنیکی نداشته باشند و هدایت و رهبری آنها ممکن است صرفاً شامل صدور فرمان برای راه انداختن و آغاز یک حمله سایبری باشد، و آنها به دلیل فقدان قابلیت‌های فنی در اینگونه حملات قادر به نظارت صحیح و درست نباشند، با این وجود با توجه به ماده ۸ مکرر اساسنامه رم، به نظر می‌رسد شخصی که در موقعیت صدور دستور برای انجام اقدامی تجاوزکارانه می‌باشد و به طور مؤثر بر آن اقدام کنترل دارد، لازم نیست که اطلاعات جزئی از حمله و ابزاری که توسط آن حمله صورت می‌گیرد، داشته باشد. همین حد کفایت می‌کند که مقام دستوردهنده آگاهی داشته باشد که دستورش اعمال می‌شود و آن دستور عواقب زیان‌باری نسبت به اشخاص و اشیای مورد هدف دارد.[۵۴]

از طرف دیگر ارزیابی و در نظر گرفتن عنصر معنوی در حملات سایبری معمولاً دشوار و به راحتی امکان‌پذیر نمی‌باشد خصوصاً این موضوع بیشتر در مواردی صدق می‌کند که بعضی عواقب خاص قصد می‌شود ولی عواقب دیگری که طی آن جریانات نیز به طور عادی دور از انتظار نیست، رخ می‌دهد. سؤال و مسئله‌ای که در اینجا مورد توجه قرار می‌گیرد این است که آیا افراد برای عواقب قصدنشده‌ای که از حملات ناشی می‌شوند، مسؤول هستند. به عبارت دیگر عواقب مذکور مورد قصد حمله‌کنندگان نبوده‌اند ولی اینگونه عواقب در آن حملات

52. Miller, op. cit., 236.
53. Ibid, 239, 240.
54. Kai Ambos, "Individual Criminal Responsibility for Cyber *Aggression*," *Journal of Conflict and Security Law, Oxford University Press* 21 (2016): 503, 504.

قابلیت پیش‌بینی را داشته‌اند. آیا شدت در این عواقب باعث آشکار بودن عمل تجاوز می‌شود.[۵۵] به نظر می‌رسد در اینگونه موارد اگرچه ماهیت آن اقدام با خود عواقب وخیمی به همراه دارد ولی عنصر معنوی به طور خاص می‌بایستی وجود داشته باشد.

در نهایت، اگرچه انعقاد معاهدات و توافقاتی راجع به رژیم حقوقی بین‌المللی فضای سایبری محتمل است ولی به نظر می‌رسد در آینده‌ای نزدیک این اتفاق نیفتد. حتی کشورهایی که موافق رسیدن به توافقی در خصوص فضای سایبر هستند توافقشان به این علت می‌باشد که از منظر و منفعت خود به این موضوع نگاه می‌کنند و حتی اینگونه حملات را با توجه به برداشت‌های خود تفسیر و مفاهیم آن را گسترش می‌دهند[۵۶] پس راه‌حل موجود در بررسی حملات سایبری در هر زمینه‌ای، انطباق آن با مقررات موجود در حقوق بین‌الملل می‌باشد که در مورد جنایت تجاوز و وقوع آن در قالب صلاحیت دیوان کیفری بین‌المللی، به نظر می‌رسد که با توجه به تعاریف ارائه‌شده از این جرم، از جمله اساسنامه رم و همین‌طور قطعنامه ۳۳۱۴ مجمع عمومی سازمان ملل به سال ۱۹۷۴، بتوان با تفسیری از مقررات ذکرشده برخی از حملات سایبری را که از شدت زیادی برخوردار هستند و عمل فرد حمله‌کننده قابل انتساب به دولت باشد را جنایت تجاوز تلقی نمود. اگرچه در مورد حملات سایبری تلاش می‌شود تا اینگونه حملات در قالب تفسیر مقررات موجود از جمله مقررات مربوط به حقوق بین‌الملل و حقوق کیفری بین‌المللی به نظم درآید ولی راه‌حل عملی‌تر زمانی خواهد بود که در مورد حملات سایبری چه در مباحث مربوط به امکان وقوع حمله مسلحانه و یا توسل به زور و امکان وقوع جنایت تجاوز در مورد اینگونه حملات، دولت‌ها توافقاتی مجزا با در نظر گرفتن خصوصیات این فضا داشته باشند. مضافاً اینکه در مورد رسیدگی به جنایت تجاوز در قالب حملات سایبری، با توجه به خصوصیات منحصر به فرد این فضا و اینگونه حملات، می‌بایستی تدابیری در خصوص نحوه تعقیب و رسیدگی به آنها مورد توجه قرار گیرد. به عنوان مثال در صورت مطرح شدن اینگونه حملات در قالب جنایت تجاوز در دیوان کیفری بین‌المللی، قضاتی که در مسند قضاوت قرار می‌گیرند می‌بایستی آشنایی کافی با حملات سایبری و خصوصیات فضای سایبر داشته باشند تا بتوانند تمام ابعاد اینگونه حملات را در احراز وقوع جنایت تجاوز مورد تجزیه و تحلیل قرار داده و در نهایت مبادرت به تصمیم در این

55. Miller, op. cit., 240.
56. Charles J. Dunlap Jr, "Perspectives for Cyber Strategists on Law for *Cyberwar*," *Strategic Studies Quarterly* 5(1) Spring (2011): 83.

خصوص نمایند.

نتیجه

بند ۱ ماده ۸ مکرر اساسنامه دیوان کیفری بین‌المللی به تعریف جنایت تجاوز می‌پردازد و آن را برنامه‌ریزی، آماده‌سازی، آغاز یا اجرای عملی تجاوزکارانه توسط شخصی که در موقعیت اعمال کنترل یا هدایت عملی اقدام سیاسی یا نظامی یک دولت قرار دارد و آن عمل به واسطه ماهیت، شدت و گستره‌اش نقض آشکار منشور ملل متحد محسوب می‌شود، تعریف می‌کند. در ادامه بند ۲ ماده ۸ مکرر عمل تجاوزکارانه مذکور در بند ۱ را نیز استفاده یک دولت از نیروهای مسلح علیه حاکمیت، تمامیت سرزمینی یا استقلال سیاسی دولت دیگر یا به هر شیوه دیگری که با منشور ملل متحد ناسازگار باشد، مورد توجه قرار می‌دهد.

از یک طرف با روشن شدن تعریف جنایت تجاوز و صلاحیت دیوان کیفری بین‌المللی در رسیدگی به آن و از طرف دیگر با تعریف حملات سایبری و خصوصیات آن در مقاله حاضر و همین‌طور با در نظر گرفتن این موضوع که فضای سایبر به عنوان پنجمین میدان نبرد نیازمند همکاری‌ها و اقدامات حقوقی هماهنگی میان دولت‌هاست، تا زمانی که دولت‌ها در این زمینه به توافق نرسند مقابله دولت‌ها هم به طور خاص در برابر اینگونه حملات و تجاوزات ناکارآمد خواهد بود. همچنین نمی‌توان در عالم واقع با این دیدگاه به صلح و امنیت بین‌المللی که آرزوی دیرینه بشر بوده است، دست یافت. در سطح بین‌الملل، دولت‌ها به دلایل گوناگون از جمله منافع سیاسی خود تمایلی به انعقاد معاهده در مورد نظم‌دهی به حملات سایبری در ابعاد مختلف آن از جمله مسؤولیت کیفری افراد در قالب جنایت تجاوز ندارند و از طرف دیگر با توجه به جدید بودن موضوعات مربوطه هنوز عرف بین‌المللی در مورد اینگونه حملات شکل نگرفته است. بنابراین بهترین راه‌حل در نظم دادن به موضوعات جدید انطباق آنها با مقررات موجود است. در مورد حملات سایبری و وقوع جنایت تجاوز با توجه به متن بازنگری‌شده اساسنامه رم و قطعنامه ۳۳۱۴ مجمع عمومی سازمان ملل می‌توان چنین نتیجه‌گیری نمود که بعضی از حملات سایبری که از شدت و وخامت زیادی برخوردار هستند را می‌توان به عنوان جنایت تجاوز در نظر گرفت و در نهایت با شرایط پیش‌بینی‌شده در اساسنامه رم، دیوان کیفری بین‌المللی صلاحیت رسیدگی به آنها را داشته باشد. البته این موضوع نیز واضح است که دولت‌ها در مقام عمل حتی در مورد تفسیر قواعد حقوقی هم منافع و شرایط موجود خود را در نظر گرفته و مطابق با آن رویه‌ای را در پیش می‌گیرند. به عبارت

دیگر اگرچه به لحاظ حقوقی می‌توان مقررات موجود حقوقی را به نحوی تفسیر نمود که جنایت تجاوز شامل برخی از انواع حملات سایبری نیز بشود ولی آنچه که دولت‌ها به آن عمل می‌کنند، می‌تواند کاملاً متفاوت باشد. شاید این پیش‌بینی در مورد رویکرد دولت‌ها دور از انتظار نباشد که دولت‌ها حداقل تا زمانی که حملات سایبری را تهدیدی جدی برای بقای حیات خود در نظر نگیرند تمایل چندانی به تعمیم و گسترش مفهوم تجاوز برای دربر گرفتن حملات سایبری نیز نداشته باشند. ولی با توجه به پیشرفت روزافزون تکنولوژی و امکان شدید شدن آثار حملات سایبری، دولت‌ها در آینده‌ای نه‌چندان دور می‌بایستی وضعیت حملات سایبری را از تعریف اینگونه حملات تا وضعیت‌های حقوقی حاکم بر آنها روشن نمایند. در مورد جنایت تجاوز و حملات سایبری نیز به نظر می‌رسد حتی در صورت احراز وقوع این جرم، دیوان کیفری بین‌المللی می‌بایستی از قضاتی استفاده نماید که آگاهی لازم و کافی با حملات سایبری و تکنولوژی‌های مرتبط با این فضا را داشته باشند. به عبارت دیگر شرایط مساعد و مناسب با رسیدگی به اینگونه جرایم نیز می‌بایستی فراهم گردد.

فهرست منابع

الف. منابع فارسی

آل حبیب، اسحاق. *دیوان کیفری بین‌المللی و جمهوری اسلامی ایران*. چاپ اول. تهران: مرکز چاپ و انتشارات وزارت امور خارجه، ۱۳۷۸.

دیهیم، علیرضا. *درآمدی بر حقوق کیفری بین‌المللی (در پرتو اساسنامه دیوان کیفری بین‌الملل)*. چاپ دوم. تهران: مرکز چاپ و انتشارات وزارت امور خارجه، پاییز ۱۳۸۴.

سودمندی، عبدالمجید، مترجم. *رسیدگی به جنایت تجاوز در دیوان کیفری بین‌المللی*. تهران: مؤسسه فرهنگی هنری انتشاراتی نگاه بینه، ۱۳۹۴.

شبث، ویلیام ا. *دیوان کیفری بین‌المللی*. چاپ اول. ترجمه سید باقر میرعباسی و حمید الوئی نظری. تهران: انتشارات جنگل، ۱۳۸۴.

شریعت‌باقری، محمدجواد. *حقوق کیفری بین‌المللی*. چاپ هشتم. تهران: انتشارات جنگل، جاودانه، ۱۳۸۸.

طهماسبی، جواد. *صلاحیت دیوان کیفری بین‌المللی*. چاپ اول. تهران: انتشارات جاودانه، جنگل، ۱۳۸۸.

واحدی، قدرت‌اله. *حقوق بین‌الملل کیفری*. چاپ اول. تهران: انتشارات جنگل، ۱۳۸۹.

ب. منابع انگلیسی

Ambos, Kai. "Individual Criminal Responsibility for Cyber *Aggression.*" *Journal of Conflict and Security Law, Oxford University Press* 21 (2016): 495–504.

Brenner, Susan, and W., Leo L. Clarke. "Civilians in Cyberwarfare: *Conscripts.*" *Vanderbilt Journal of Transnational Law* 43: 1011 (2010): 1011-1076.

Clark, Roger S. The Crime of Aggression and the International Criminal Court, Edited by José Doria Hans-Peter Gasser M. Cherif Bassiouni, The Legal Regime of the International Criminal Court, Essays in Honor of Professor Igor Blishchenko, Martinus NIJHOFF Publisher, 2009.

Coleman, Keven. "Russia's Cyber Forces". (Doctrine), Last Modified May 27, 2008. Last Accessed October 10, 2016. http://defensetech.org/2008/05/27/russias-cyber-forces.

Cornish, Paul, and David Livingstone and Dave Clemente and Claire Yorke. "on Cyber Warfare". A Chatham House Report. p. 10. November 2010. Accessed May 12, 2016. https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/r1110_cyberwarfare.pdf.

Dunlap Jr, Charles J. "Major General, USAF Retired, Perspectives for Cyber Strategists on Law for *Cyberwar.*" *Strategic Studies Quarterly* 5(1) Spring (2011): 81-99.

Dycus, Stephen. "Congress's Role in Cyber *Warfare.*" *Journal of National Security Law & Policy* 4: 155 (2010): 155-171.

Evans, Malcolm D. *International Law*. 3rd Ed. New York: Oxford University Press, 2010.

General Assembly's Resolution, 3314 (XXIX), 1974.

Gillett, Matthew. "The Anatomy of an International Crime: Aggression at the International Criminal *Court.*" *International Criminal Law Review* 13: 4 (2013): 829-864.

Glasius, Marlies. *The International Criminal Court a global Civil Society Achievement.* New York: Routledge Taylor & Francis Group, 2006.

Hathaway, Oona A., and Rebecca Crootof and Philip Levitz and Haley Nix and Aileen Nowlan and William Perdue and Julia Spiegel. "The Law of *Cyber-Attack.*" *California Law Review* 100: 817 (2012): 817-886.

Heaton, Major J. Ricou. "Civilians at War: Reexamining the Status of Civilians Accompanying the Armed *Forces.*" *The Air Force Law Review* 57 (2005): 157-195.

Heinegg, Wolff Heintschel Von. "Legal Implications of Territorial Sovereignty in Cyberspace." Paper Presented at the 4th International Conference on Cyber Conlfict, NATO CCD COE Publications, Tallinn, June 5, 8, 2012, https://ccdcoe.org/sites/default/files/multimedia/pdf/1_1_von_Heinegg_LegalImplicationsOfTerritorialSovereigntyInCyberspace.pdf, Accessed October, 2016.

Kai Ambos, "The Crime of Aggression after *Kampala.*" *German Year Book of International Law* 53 (2010): 463-510.

Kesan, Jay P., and Carol M. Hayes. "Mitigative Counterstriking: Self-Defense and Deterrence in *Cyberspace.*" *Harvard Journal of Law and Technology* 25: 2 Spring (2012): 415-529.

Knut Dormann. "Applicability of the Additional Protocols to Computer Network Attacks". Stockholm, International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Published online by International Committee of the Red Cross, Accessed September 11, 2016. https://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf, (2004), 1-12.

Kreb, Claus, and Leonie Von Holtzendorff. "The Kampala Compromise on the Crime of *Aggression.*" *Journal of International Criminal Justice* 8 (2010): 1179-1217.

Legality of the Threat of Use of Nuclear Weapons, Advisory Opinion of International Court of Justice, 1996.

Lipson, Howard F. "Trading and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues." Special Report CMU/sei-2002-sr-009, Pittsburgh: Carnegie Mellon Software Engineering Institute, November 2002.

May, Larry. *Aggression and Crimes against Peace*. New York: Cambridge University Press, 2008.

Miller, Kevin L. "The Kampala Compromised and Cyberattacks: Can There be an International Crime of *Cyber-Aggression?.*" *Southern California Interdisciplinary Law Journal* 23: 2 (2014): 217-260.

Ophardt, Jonathan A. "Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's *Battlefield.*" *Duke Law and Technology Review* 3 (2010): 1-27.

Pank, Sophie Charlotte. "What is the Scope of Legal Self-Defense in International Law?", Jus Ad Bellum with a Special View to New Frontier for Self-Defense, Aarhus Denmark, Juridik Institut, RETTID, Specialeafhandling 19, (2014). Accessed March 15, 2016. http://law.au.dk/fileadmin/Jura/dokumenter/forskning/rettid/Afh_2014/afh19-2014.pdf. Rome: 1-43.

Rome Statute of the International Criminal Court, 1998, Accessed October, 2016. https://www.icc-cpi.int/nr/rdonlyres/ea9aeff7-5752-4f84-be94-0a655eb30e16/0/rome_statute_english.pdf.

Sadat, Leila Nadya. "The International Criminal Court: Past, Present and *Future.*" *Washington University Global Studies Law Review* 12(3) (2013): 403-410.

Schiff, Benjamin N. *Building the International Criminal Court*. New York: Cambridge University Press, 2008.

Schmitt, Michael N. *Cyber Operations in International Law: The Use of Force,*

Collective Security, Self Defence, and Armed Conflicts, Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy. Washington: National Academic Press, 2010.

Schuster, Matthias. "The Rome Statute and the Crime of Aggression: A Gordian Knot in Search of a *Sword.*" *Criminal Law Forum* 14: 1–57 (2003): 1–57.

Sean D. Murphy, *The Crime of Aggression at the ICC, Oxford Handbook of the Use of Force in International Law*. Marc Weller, Ed. New York: Oxford University Press, 2015.

Stahn, Carsten, and Göran Sluiter. *The Emerging Practice of the International Criminal Court, Legal Aspects of International Organization*. Vol. 48. Leiden: Martinus Nijhoff Publisher, 2009.

Swanson, Lesley. "The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber *Conflict.*" *Loyola of Los Angeles International and Comparative Law Review* 32: 303 (2010): 303-333.

Triffterer, Otto, and Kai Ambos. *The Rome Statute of the International Criminal Court: A Commentary, C. H. BECK*. Hart. Nomos Publications, 2016.

Cyber-Attacks as the Crime of Aggression and examining the Jurisdiction of International Criminal Court in its Investigations

Dr. Parastou Esmailzadeh Molabashi
Ph.D. in International Law, Islamic Azad University of Najafabad and University Lecturer,
Email: parastou.esmailzadeh@yahoo.com

The crime of aggression is one of the crimes that international criminal court can deal with. There is not a decisive definition about the meaning of the crime of aggression at the time of the ratification of the Rome Statute. There was an agreement between the state parties to define the crime of aggression at the time of reviewing the statute in the future. Consequently, the Crime of Aggression was being defined in 2010 under Article 8bis of the International Criminal Court Statute. Although the definition of the crime of aggression does not refer to cyber-attacks, but it seems that some kinds of these attacks according to the Rome Statute and the General Assembly Resolution 3314 of 1974, can be considered as the crime of aggression. In order to assess the cyber-attacks in the context of crime of aggression, these attacks must reach the threshold of the crime of aggression, that is to say, the most serious breach of international law regulations. For committing the crime of aggression, the perpetrators of cyber-attacks need to be aware of the circumstances that lead to the clear violation of International Law which is usually something difficult to be proven. Although some cyber-attacks can be counted as the crime of aggression, it seems that since that cyber space has its own characteristics, the best way to deal with these kinds of attacks is an agreement between states and also allocating the judges in ICC who are specialized in the field of cyberspace.

Keywords: Cyber-Attacks, Cybercrime, The Crime of Aggression, International Criminal Court, Responsibility.

ISSN 2345-2986

Journal of CRIMINAL LAW AND CRIMINOLOGY

VOL. V, No. 2 2017-2

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