آموزه‌های حقوق کیفری، دانشگاه علوم اسلامی رضوی، دورهٔ نوزدهم، شمارهٔ ۲۳، بهار ـ تابستان ۱۴۰۱
نوع مقاله: علمی ـ پژوهشی (۲۶۹ـ۲۹۶)

اثربخشی دستورالعمل تالین ۲۰۱۷ میلادی بر صلاحیت دیوان کیفری بین‌المللی

در ایجاد صلح و امنیت سایبری بین‌المللی*

□ علیرضا محقق هرچقان[۱]
□ محمدعلی اردبیلی[۲]
□ ابراهیم بیگ‌زاده[۳]
□ محمدعلی مهدوی ثابت[۴]

چکیده

توجه به روابط دوستانه و ضرورت حل‌وفصل اختلاف به شیوهٔ التزام به منع مداخلهٔ دولت‌ها در امور دیگر کشورها، امری اجتناب‌ناپذیر است. با توسعهٔ فعالیت سایبری، صلح و امنیت سایبری، یک اصل ضروری است که با توسل به

* تاریخ دریافت: ۱۴۰۰/۵/۱۰ ـ تاریخ پذیرش: ۱۴۰۱/۲/۲۸.

۱. دانشجوی دکتری 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).

زور سایبری نقض می‌شود. اصل منع توسل به زور، برای تعیین نقض یا عدم نقض مادۀ (۴)۲ منشور ملل متحد و ممنوعیت آن در حقوق بین‌الملل عرفی به کار می‌رود. در مقابل به کارگیری زور توسط فرد متخاصم، مداخلۀ قانونی توسط شورای امنیت جامعه بین‌المللی 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، در صورت رسیدن به آستانۀ مقتضی می‌تواند قابل احراز به عنوان «جنایت تجاوز» در قالب «فاعل معنوی» باشد. وفقِ قاعدۀ ۱۳ دستورالعمل تالین ۱ در سال ۲۰۱۳ میلادی و نیز بند ۶ مادۀ ۶۹ در دستورالعمل تالین ۲ در سال ۲۰۱۷ میلادی بر مبنای اثر، گستره و شدت در بروز جرائم سایبری، آستانۀ جنایت تجاوز را باید «حملۀ مسلحانه» دانست که دارای ماهیت نقضِ قواعد حقوق بین‌الملل و منع توسل به زور است و مسئولیت کیفری علاوه بر فرد متخاصم به فعالان غیر دولتیِ مطلع نیز توسعه خواهد یافت.

واژگان کلیدی: منع مداخله، صلح و امنیت سایبری، دیوان کیفری بین‌المللی، دکترین اثربخشی، مسئولیت کیفری فردی.

مقدمه

صلح و امنیت سایبری در سطح بین‌الملل، همراه با پیشرفت فناوری و ایجاد ابزارهای مجهز به فناوری‌های روز دنیا، نظام حق و تکلیف را در عرصۀ بین‌الملل با تحولات چشمگیری از حیث مقررات بین‌المللی روبه‌رو خواهد ساخت. ظهور جرائم سایبری نظیر هکتیویسم یا هک سیاسیِ سایبری با استفاده از سلاح‌های سایبری، در قالب مسائل مطروحۀ قواعد حقوق بین‌الملل عرفی، امری اجتناب‌ناپذیر است. پروتکل اول الحاقیِ سال ۱۹۷۷ و پروتکل دوم الحاقیِ سال ۱۹۴۹ به کنوانسیون‌های چهارگانۀ ژنو ۱۹۴۹ در مسئله تعیین ضابطۀ سلاح برای کشوری که قصد استفاده از آن را دارد، ملاک این است که به تازگی سلاح موصوف توسط دولت مورد تجاوز و تخاصم، به عنوان وسیله ارتکاب جنایت تبیین و توصیف شده باشد (ICRC, 2006: 935). سلاح سایبری به ویروس‌های رایانه‌ای گفته می‌شود که در چندین مرحله رمزگذاری شده و ساختار آن به گونه‌ای است که آنتی‌ویروس‌های معمولی به دلیل وجود پیچیدگی‌های ساختاری، قادر به شناسایی و از بین بردن آن نیستند و همچنین برنامه‌ریزی آن‌ها به گونه‌ای است

که یک هدف خاص را مورد حمله قرار می‌دهند. اهمیت ارائهٔ تعریفی دقیق از سلاح بدین‌علت است که در صورت عدم تعریف عبارت و اصطلاحات «تسلیحات جدید»، این تسلیحات تبدیل به ابزاری برای فرار از مسئولیت بین‌المللی دولت‌ها در تحمیل «توسل به زور» می‌شود که دولت‌ها به دلیل اغراض سیاسی از آن استقبال می‌نمایند (Blake & Imburgia, 2010: 160). ضرورت تعیین ضابطه‌ای خاص برای ورود یک اتهام به فرد مرتکب فاقد مصونیت، تحت عناوینِ نقض آشکار صلح و امنیت و نیز جنایت بین‌المللی، مطابق با فصل هفتم منشور سازمان ملل متحد مشخص می‌شود. این واقعهٔ مهم و ضروری بین‌المللی غیر قابل انکار، برای اولین بار در نشست تالین به منصّهٔ ظهور رسید و «حملهٔ مسلحانه» به عنوان آستانهٔ نقضِ صلح و امنیت سایبری تعیین شد. البته انجام این ابتکار و نوآوری باید با رعایت اصول حاکم در حقوق کیفری بین‌المللی و ایراد انتساب جزایی با اعطای صلاحیت به دیوان کیفری بین‌المللی صورت گیرد.

در این مقاله به بررسی این موضوع خواهیم پرداخت که آیا توافقات صورت‌گرفته توسط اعضای مذاکره‌کننده در شهر تالین[۱] به قصد ایجاد صلح و امنیت سایبری بین‌المللی که به ایجاد دستورالعمل منتهی شد، با توسعهٔ صلاحیت دیوان کیفری بین‌المللی تحقق خواهد یافت یا خیر؟

در قسمت اول مقالهٔ حاضر به عدم مداخله و منع توسل به زور، در قسمت دوم به اثربخشی و تأثیرگذاری به مفهوم توسعه صلاحیت دیوان در امر رسیدگی به نقض صلح و امنیت سایبری، و در قسمت سوم نیز به دفاع مشروع به عنوان تنها مورد استثنای قانونی و قابل قبولِ توسل به زور و شدت آستانه در اقدامات سایبری خواهیم پرداخت.

۱. اصل عدم مداخله و منع توسل به زور

لزوم حل‌وفصل اختلافات بین‌المللی به شیوه‌های مسالمت‌آمیز در حقوق بین‌الملل در

۱. دستورالعمل تالین در حقوق بین‌الملل، قابل اعمال در نبردهای سایبری «متعلق به بازهٔ زمانی سال‌های ۲۰۱۳ تا ۲۰۱۷ میلادی در شهر تالین در کشور استونی است که توسط «مایکل اشمیت» استاد حقوق بین‌الملل، پیرامون مقررات حاکم بر اقدامات و عملیات سایبری با همکاری یک گروه پژوهشگر و به سفارش مرکز عالی دفاع مشترک سایبری و با راهبری ناتو (پیمان آتلانتیک شمالی) در ولزِ بریتانیا، در قالب اصل ۴ پیمان ناتو تهیه شده است.

معاهدات چند و دوجانبه مورد پشتیبانی قرار گرفته و در تصمیمات دیوان بین‌المللی دادگستری اِعمال گردیده است (Imburgia, 1998: 53).[1] در این مورد، توجه به مادۀ ۲ از اعلامیۀ روابط دوستانۀ مجمع عمومی ورسای مورد نظر است (Nicaragua judgment, 2015: 26). اصل حل‌وفصل اختلافات به شیوه‌های مسالمت‌آمیز با ماهیت عرفی توسط دولت‌ها، به‌گونه‌ای که صلح و امنیت بین‌المللی و عدالت به مخاطره نیفتد نیز مؤید همین اصل می‌باشد. در این خصوص، رجوع به بند الف قاعدۀ ۶۵ دستورالعمل تالین بر مواد ۲(۳) و ۳۳(۱) منشور نیز قابل استناد خواهد بود. بند ب قاعدۀ مذکور نیز از مادۀ ۲(۳) منشور ملل متحد اقتباس شده است. ادعای یک دولت دایر بر نفوذ دولت دیگر در زیرساخت‌های سایبری آن به گونه‌ای که وفق قاعدۀ ۴ دستورالعمل تالین، اصل حاکمیت را نقض کند، اختلاف میان دو دولت به شمار می‌آید. کارشناسان کارگروه بین‌المللی در مذاکرات تالین معتقدند که بر خلاف مادۀ ۲(۳) منشور ملل متحد که به‌طور خاص اعمال خود را به «اختلاف بین‌المللی» محدود می‌سازد، مادۀ ۳۳ منشور به هر گونه اختلاف مربوط با صلح و امنیت بین‌المللی دلالت دارد. با وجود این، کارشناسان موافقت کرده‌اند که بند الف، تنها با اختلافات بین‌المللی سروکار دارد؛ زیرا مادۀ ۳۳ مشتمل بر اختلافاتی است که صلح و امنیت بین‌المللی را به مخاطره می‌افکند. بنابراین ماده ۲(۳) را به آن تخصیص دادند. در حل‌وفصل اختلافات بین‌المللیِ مشمول فعالیت‌های سایبری، دولت‌ها تنها اجازه دارند که به «شیوه‌های مسالمت‌آمیز» متوسل شوند و طبعاً باید این کار را به شیوه‌ای انجام دهند که صلح و امنیت بین‌المللی به خطر نیفتد (Schmitt, 2017: 305). وفق شقّ الفِ قاعدۀ یادشده، دولت‌های طرف اختلاف بین‌المللی که به صورت احتمالی صلح و امنیت بین‌المللی را به مخاطره افکنده‌اند، ملزم به جستجو برای حل‌وفصل قضیه به شیوه‌های مسالمت‌آمیز هستند.

۱ـ۱. اصل منع مداخله توسط دولت‌ها

با امعان‌نظر به قاعدۀ ۶۶ دستورالعمل تالین، یک دولت نباید از طریق ابزارهای سایبری در امور داخلی و یا خارجی دولت دیگر مداخله نماید. این قاعده، مداخلۀ

1. Nicaragua judgment, para. 290; UN GGE 2015 Report, paras. 26, 28(b).

اجباری یک دولت به وسیلهٔ ابزارهای سایبری را منع نموده است و بر اصل برابری حاکمیت دولت‌ها در حقوق بین‌الملل تأکید دارد. کارگروه کارشناسان بین‌المللی موافقت کرده‌اند که منع مداخله در امور داخلی و یا خارجی دولت دیگر، از جملهٔ حقوق بین‌الملل عرفی است. در واقع دولت‌ها مرتباً اصل برابری حاکمیت دولت‌ها را ابراز کرده و به آن متوسل می‌شوند.[1] علاوه بر دیوان بین‌المللی دادگستری، دیوان کیفری بین‌المللی و کمیسیون حقوق بین‌الملل، جایگاه عرفیِ ممنوعیت ذی‌ربط را به‌رسمیت می‌شناسند. لیکن در پرداختن به اصل منع مداخله، از بیان‌های[2] متناقضی استفاده شده است. به طور خاص، دولت‌ها در پاره‌ای از مواقع به جای «مداخله»[3] از اصطلاح «دخالت»[4] استفاده می‌نمایند (Ibid.: 313). اصطلاح مداخله یعنی اقدامات دخالت‌آمیز در امتیازات حاکمیتی دولت دیگر که واجد اثر قهرآمیز محدود بوده و این قاعده صرفاً در مناسبات دولت‌ها اجرا می‌شود. این موضوع تلویحاً بدان‌معناست که ابزارهای سایبریِ واجد ماهیت جبرگونه را نباید برای تغییر یا اصلاح مخفیانهٔ ساختار حکومتی یا اجتماعی کشوری دیگر به کار گرفت. در این مورد، اعلامیهٔ روابط دوستانهٔ مجمع عمومی ورسای (روبو، ۱۳۹۹: ۶۳۱) غالباً با این عنوان که مصادیق مداخلهٔ ممنوعه را مقرر می‌دارد، مرجع ارجاع واقع می‌شود. سازماندهی، تحریک، مساعدت، تأمین مالی یا مشارکت در آشوب داخلی یا اعمال تروریستی در دولت دیگر، یا پذیرش بی‌چون و چرای[5] جرائم سازمان‌یافته در قلمرو داخلی کشور که به منظور ارتکاب چنین اقداماتی ترتیب داده شده‌اند، در شمار این مصادیق هستند. دیوان بین‌الملل دادگستری، بازتاب حقوق بین‌الملل عرفی بودنِ مقررات ماهوی اعلامیه را به رسمیت شناخته و در ضمن اصطلاح «زور» در حقوق بین‌الملل تعریف نشده است. «زور» در این قاعده علاوه بر

1. See: e.g., UN GGE 2015 Report, paras. 26, 28(b); Ministry of Foreign Affairs of China, the Cnetra1 Conference on Work Relating to Foreign Affairs, Beijing (29 November 2014).
2. Declaration on Friendly Relations, 1949: 375.
3. Intervention.
4. Interference.
5. Acquiescing.

زور فیزیکی، عمل ایجابی طراحی‌شده به منظور محروم ساختن دولتی دیگر از آزادی انتخاب خویش و تلویحاً یا به صراحت وادار ساختن آن دولت به عمل به شیوه‌ای غیرارادی را در بر می‌گیرد و خودداری غیر داوطلبانه از عمل به شیوه‌ای معین نیز به همین معنا دلالت دارد. این اصل بیان می‌دارد:

«هیچ دولتی نباید دولت دیگر را برای به اجرا درآوردن اِعمال حقوق حاکمیتی خویش و نیز گرفتن هر نوع امتیازی از او تحت اجبار قرار دهد» (Schmitt, 2017: 317).

تمامی کارشناسان کارگروه مذاکرات تالین موافقت نموده‌اند که توسل به زور سایبری وفق قاعدهٔ ۶۸ دستورالعمل تالین توسط یک دولت دیگر همواره جبرآمیز بوده و موجب شکل‌گیری نوعی از مداخله می‌گردد و اجبار کافی برای پشتیبانی از احراز مداخلهٔ غیرقانونی شکل مستقیم به خود می‌گیرد (Ibid.: 319; Declaration on Friendly Relations, prins. 3). اصل منع مداخله، شامل پرداختن به موارد مربوط به مداخلهٔ مستقیم یا غیر مستقیم در امور داخلی یا خارجی، در عرصه سایبری نیز پدیدار می‌شود. کارگروه بین‌المللی مذاکرات تالین موافقت کردند که عدم قطعیت در خصوص احراز هویت از جانب دولت، مادامی که عملیات‌های مربوطه توسط یک دولت انجام گیرند، وفق قواعد ۱۸ـ۱۵ قابل انتساب به دولت‌ها و نهادهای مربوطه هستند و بنابراین ماهیت اِعمال زور داشته، به هدف دخالت در امور داخلی یا خارجی دولت صورت می‌گیرند؛ پس این اعمال مانع توصیف آن‌ها به عنوان مداخله نمی‌شوند. کارشناسان در این زمینه متفق‌القول بودند که قصد، عنصر معنوی تشکیل‌دهندهٔ نقض ممنوعیت مداخله است. وضعیت‌هایی که در آن‌ها فعالیت‌های سایبری واجد اثر اجبارِ عملی به مفهوم غیر قانونی هستند، باید از وضعیت‌هایی که در آن‌ها دولت قصد اجبار رسمی به مفهوم قانونی دارد، تفکیک شوند. همچنین ایشان موافقت نمودند که عدم موفقیت عملیات سایبریِ جبرآمیز در ایجاد برایند مورد نظر، تأثیری بر نقض یا عدم نقض این قاعده ندارد (Schmitt, 2017: 322).

۱ـ۲. مداخله توسط سازمان ملل متحد

با امعان‌نظر به صراحت قاعدهٔ ۶۷ دستورالعمل تالین که برگرفته از مادهٔ ۲(۷) منشور ملل متحد بوده و اصل آن بر عدم مداخلهٔ ملل متحد به وسیلهٔ ابزارهای سایبری در اموری

است که اساساً تحت صلاحیت داخلی یک دولت می‌باشد، این اصل صرفاً اعمال نظر شورای امنیت برخاسته از فصل هفتم منشور ملل متحد است. تمایز این اصل با قاعده صریح ۶۶ که مبین فعالیت‌های صورت‌گرفته توسط دول یا قابل انتساب به آن‌هاست، اجتناب‌ناپذیر است (League of Nations Covenant, 1993, 1819 UNTS 3113). کارگروه کارشناسی بین‌المللی در مذاکرات تالین، اتفاق‌نظر داشتند که منظور از «اموری که اساساً تحت صلاحیت داخلی دولت است»، شامل اهداف مصرّح در ماده اول منشور ملل متحد نشده و به طور خاص، مسائل متضمن «صلح و امنیت بین‌المللی» را تحت پوشش خود قرار نمی‌دهد.

«مایکل اشمیت» این وضعیت را در خصوص فعالیت‌های سایبری بسیار حائز اهمیت می‌داند و علت آن را این گونه بیان می‌نماید:

> «ماهیت مرتبط زیرساخت سایبری و فعالیت‌ها بدین‌معناست که فعالیت‌های مربوط به اقدامات صورت‌گرفته در یک کشور، اغلب بر همان فعالیت‌ها در کشور دیگر تأثیر می‌گذارد».

البته به طور مشخص، این اقدامات دارای زمینهٔ «اخلال در صلح و امنیت بین‌المللی» می‌باشد و همچنین بستر را برای نظارت بر «تعهدات حقوق بین‌الملل بشرِ دولت‌ها» فراهم می‌سازد (Schmitt, 2017: 326).[1] این قاعده بر خلاف قاعده ۶۶ دستورالعمل یادشده، واجد عنصر اجبار نیست و کارگروه مزبور در مذاکرات تالین موافقت کرده‌اند که توصیف مناسب‌تر واژهٔ «مداخله» این است که سازمان ملل متحد نباید از طریق ابزارهای سایبری داخلی در صلاحیت امور داخلی کشورها مداخله نماید. قاعده مزبور، هیچ گونه خدشه‌ای را به حقِ شورای امنیت مبنی بر صدور مجوز یا دستور اقدامات سایبری به موجب فصل هفتم منشور ملل متحد در راستای حفظ یا اعادهٔ «صلح و امنیت سایبری» وارد نمی‌سازد (UN Charter, ART 39) و با همین رویکرد، ظهورِ سازمان‌های بین‌المللی نظیر دیوان کیفری بین‌المللی معنا و مفهوم حقوقی پیدا کرده و زمانی که شورای امنیت مبادرت به تصمیم و اقدامی نماید، کلیهٔ کشورها موظف‌اند از آن مقرره اطاعت نموده و

1. See: e.g., GA Res. 65/222, UN Doc. A/RES/65/222 (11 April 2011), GA RES. 65/203, UN Doc. A/RES/65/203-16 March 2011 (Schmitt, 2017: 326).

آن را اجرا نمایند (UN Charter, ART 25). بر همین اساس، تأسیس دیوان کیفری بین‌المللی صورت گرفت و نسبت به تنظیم و تصویب سندی که در آن جنایات بین‌المللی تبیین و صلاحیت رسیدگی به آن‌ها تعیین شود، مبادرت گردید (میرمحمدصادقی، ۱۳۸۸: ۱۴).

۱ـ۳. تبیین و تعریف توسل به زور

دیوان بین‌المللی دادگستری اعلام نمود که مواد (۴)۲ و ۵۱ منشور ملل متحد که با قواعد ۷۰ـ۹۸ و قواعد ۷۰ـ۷۵ دستورالعمل تالین به ترتیب در رابطه با منع توسل به زور و دفاع مشروع بدون در نظر گرفتن سلاح‌های به کار رفته، از عبارت «هر گونه اِعمال زور» استفاده می‌شود. در محیط سایبری، این نه ابزار به کار رفته، بلکه همان گونه که در قاعدهٔ ۶۹ دستورالعمل توصیف شده است، پیامدهای عملیات ذی‌ربط و شرایط پیرامونی است که عبور یا عدم عبور از آستانهٔ به کارگیری زور را تعیین می‌کند. شیوه یا ابزار جنگی سایبری را می‌توان برای ایجاد پیامدهایی مانند اختلال جزئی در فعالیت‌هایی سایبری به کار گرفت که آشکارا به کارگیری زور به شمار نمی‌آیند. رویهٔ دولتی تنها تبیین اجرای عملیات‌های سایبری در حقوق، توسل به زور را آغاز کرده است؛ وجهی از حقوق بین‌الملل که بر توسل دولت به زور به مثابه ابزاری از سیاست ملی حکومت دارد. کارگروه بین‌المللی کارشناسان تصدیق کرده‌اند که چون تهدیدها و فرصت‌های سایبری در حال ظهور و تکامل هستند، رویهٔ دولتی می‌تواند تفاسیر کنونی از توسل به زور را در فضای سایبر تغییر دهد. قاعدهٔ ۶۹ دستورالعمل تالین در مقام تعریف به کارگیری زور اشعار می‌دارد که زمانی مقیاس و آثار یک عملیات سایبری به اندازهٔ عملیات‌های غیر سایبری نائل خواهد آمد که در سطح به کارگیری زور برابر باشند. این موضوع خود موجب شکل‌گیری به کار بستن و اعمال زور می‌شود. هیچ تعریف یا معیار معتبری برای «تهدید» یا «توسل به زور» وجود ندارد. با وجود این، انواعی از عملیات جبرآمیز وجود دارند که مشمول ویژگی‌های به کارگیری زور نیستند (Schmitt, 2017: 328). بررسی مفهوم «توسل به زور» مطابق با قاعدهٔ ۷۱ دستورالعمل تالین، در رابطه با «حملهٔ مسلحانه» که آستانه‌ای است که یک دولت در آن می‌تواند به صورت قانونی در قالب دفاع مشروع، از زور استفاده کند، سودمند است.

۱ـ۴. ممنوعیت تهدید و توسل به زور

با صراحت مادهٔ ۶۸ دستورالعمل، عملیاتی که موجب شکل‌گیری تهدید یا توسل به زور علیه یکپارچگی یک سرزمین یا استقلال سیاسی یک دولت شود یا به هر طریق دیگر با اهداف منشور ملل متحد ناسازگار باشد، غیر قانونی است. ممنوعیت موجود در مادهٔ ۲(۴) منشور ملل متحد، مؤید همین امر و منبعث از حقوق بین‌الملل عرفی و مبیّن آن است که تهدید یا به کارگیری زور، ناسازگار با «اهداف ملل متحد» به منظور ایجاد فرض غیر قانونی بودن هر گونه تهدید همراه با به کارگیری زور قرار داده شده بود. اقداماتی که علیه یکپارچگی سرزمین یا استقلال سیاسی کشورها هدایت نشده‌اند نیز می‌توانند در زمانی که با اهداف ملل متحد ناسازگار باشند، ممنوعیت ذی‌ربط را نقض کنند. دو استثنای کاملاً پذیرفته‌شده بر ممنوعیت توسل به زور وجود دارد: ۱ـ به کارگیری زور با مجوز شورای امنیت ملل متحد، ذیل فصل هفتم منشور؛ ۲ـ دفاع مشروع وفق مادهٔ ۵۱ و حقوق بین‌الملل عرفی. کارگروه بین‌المللی تالین موافقت نمود که هر عملیات سایبری که وفق قاعدهٔ ۷۱، از نظر مقیاس و آثار به سطح یک «حملهٔ مسلحانه» برسد و توسط یک دولت انجام گرفته یا به او قابل انتساب باشد، «توسل به زور» محسوب گشته و بروز آن می‌تواند در قالب «تجاوز سایبری» متصور و دارای قابلیت استماع باشد.

۱ـ۵. ضابطهٔ توسل به زور

به منظور تعیین نقض یا عدم نقض، مادهٔ ۲(۴) منشور ملل متحد و ممنوعیت مربوط به آن در حقوق بین‌الملل عرفی به کار می‌رود. در مقابل این مفهوم، مفهوم «حملهٔ مسلحانه» با امکان یا عدم امکان واکنش دولت هدف به یک اقدام با توسل به زور وجود دارد که بدون نقض ممنوعیت توسل به زور بیان می‌شود. از دیدگاه گروه بین‌المللی کارشناسان، دولت‌های مواجه با به کارگیری زور در جایگاهی که «حملهٔ مسلحانه» محسوب نمی‌شود، چنانچه خواستار پاسخی قانونی هستند، باید به اقدامات دیگری همچون اقدامات متقابل یا اعمال سازگار با مستمسک ضرورت متوسل شوند. «عملیات سایبری یا تهدید به عملیات سایبری» از منظر توسل به زور، در دو وضعیت اعمال می‌شود: وضعیت نخست، عملیاتی سایبری محسوب می‌شود که برای مخابرهٔ تهدید به همراه به کارگیری

زور (اعم از فیزیکی یا سایبری) استفاده می‌شود. وضعیت دوم، تهدید مخابره‌شده به هر شیوه‌ای دایر بر انجام عملیات‌های سایبری بوده که خود توسل به زور به شمار می‌آیند.

تهدید توسط دولت‌ها و مقامات صاحب منصب دایر بر عملی کردن آن تهدیدها، چنانچه عمل تهدیدآمیز قانونی باشد، مشروع است. البته دو استثنای به رسمیت شناخته‌شده بر ممنوعیت بین‌المللی به کارگیری زور وجود دارد: ۱ـ اعمال حق دفاع مشروع؛ ۲ـ اقدامات صورت‌گرفته در راستای اجرای قطعنامهٔ شورای امنیت ذیل فصل هفتم منشور ملل متحد.

۲. اثربخشی و رسیدگی به نقض صلح و امنیت سایبری

دکترین اثرگذاری[1] با دو شرط اساسی بودن و مستقیم بودن (Akehurst, 2008: 197)، یکی از مبانی نوین صلاحیت قانونی است که به صلاحیت فراسرزمینی[2] نیز مشهور شده است و تنها اشاره‌کننده به صلاحیت قانونی دولت‌ها و تضمین‌کنندهٔ «توسعهٔ صلاحیت» قوانین ملی دولت‌ها به قوانین فراسرزمینی است. اگرچه این دکترین، تعمیم صلاحیت سرزمینی عینی از حقوق کیفری به حقوق سایبری است، لیکن می‌تواند در ایجاد صلاحیت جهانی فرضی نیز مؤثر باشد (Ryngaert, 2008: 194). بند ج قاعدهٔ ۹ دستورالعمل تالین، بیان‌کنندهٔ دکترین فعالیت سایبری مؤثر در قلمرو خود است و بر اساس این دکترین، اعمال صلاحیت بر یک جنایت مستلزم وقوع عنصر سازندهٔ آن جنایت در قلمرو دولت یا برخی دیگر از پیوندهای سرزمینی است (Schmitt, 2017: 57; Libman v. 1985: para. 74). کارگروه بین‌المللی بر اهمیت این دکترین در عرصهٔ سایبری و نیز بازتاب حقوق بین‌الملل عرفی سایبری متفق‌القول بودند. شرایطِ به رسمیت شناخته‌شده در این زمینه، از این قرارند: دولتی که مبادرت به تصویب قوانین مبتنی بر آثار می‌نماید، باید منفعت و علقه‌ای واضح و از نظر بین‌المللی پذیرفته‌شده در این عمل داشته باشد. آثاری که دولت مترصد تنظیم آن‌هاست، باید به اندازهٔ کافی، مستقیم و قصدشده[3] یا پیش‌بینی‌پذیر[4] باشند. آن

1. Effects doctrine.
2. Extraterritorial jurisdiction.
3. Intended.
4. Predictable.

آثار باید به اندازهٔ کافی برای تعمیم قانون دولت به اتباع خارجیِ خارج از قلمرو آن اساسی باشند و این بدان‌معناست که منصرف از صلاحیت سرزمینی و با اِعمال صلاحیت مبتنی بر آثار، اقداماتی که موجب تعدیِ غیر قانونی و ناروا شود، در حقوق بین‌الملل از آن به «جنایت» یاد می‌شود (Akehurst, 2008: 221). در نتیجه، تصویب قانون بر مبنای دکترین اثرگذاری، در راستای حمایت از یک دولت در برابر آثار اساسی عملیات‌های سایبریِ انجام‌شده در خارج از قلمرو آن، مادامی که منافع مشروع سایر دولت‌ها در آن حیطه به گونه‌ای ناروا مورد تخطئه قرار نگیرد، مجاز خواهد بود (Schmitt, 2017: 64). اِعمال هر نوع از صلاحیت بر مبنای اصل صلاحیت سرزمینی، مشروط به محدودیت‌های معینی است که در حقوق بین‌الملل در حیطهٔ اختیارات صلاحیتی مقرر شده‌اند. البته باید توجه نمود که مصونیت و تعرض‌ناپذیری حاکمیتی موضوع قاعدهٔ شمارهٔ ۵ دستورالعمل تالین و همچنین مصونیت دولت‌ها از اِعمال صلاحیت[1] موضوعِ قاعدهٔ شمارهٔ ۱۲، از جمله محدودیت‌هایی است که به صورت عام‌الشمول مورد شناسایی قرار گرفته است.[2]

۲ـ۱. صلاحیت دیوان کیفری بین‌المللی

متعاقب انعقاد قرارداد صلح ۱۹۳۳ میلادی در اَروشای اوگاندا برای تشکیل دولت، به وسیلهٔ اعلام رادیویی، نسل‌کشی توتسی‌های بینوا را از هوتوهای رواندایی درخواست نمودند. این مورد را شاید بتوان اولین جنایت علیه صلح و امنیت دانست (دایموند، ۱۴۰۰: ۳۹۱). رسیدگی به جنایت علیه صلح و امنیت در قالب جنایت تجاوز، پس از آن بارها دستخوش دوری از عدالت کیفری و گریبانگیر ماهیت سیاسی آن قوانین گردید (Clark, 2010: 663). لیکن مطلوب‌ترین وضعیت در سطح جامعهٔ بین‌المللی و برگرفته از منشور سازمان ملل متحد، آن قوانینی است که در ایجاد نظم و صلح و امنیت بین‌المللی، دوری از سیاست‌زدگی و احراز امور به وسیلهٔ قضاوت عادل و بی‌طرف باشد (May, 2008: 227). دورکهایم «جرم» به مفهوم حقوق ملی و «جنایت» به مفهوم فراملی

1. Immunity of states from the exercise of jurisdiction.

2. Oppenheim's International Law, at 458 – Shaw's International Law, at 478.

و بین‌المللی جنایت را به وضعیت معین و شدیدی که ناقض «وجدان عمومی» باشد، معرفی می‌نماید (بریث‌ناچ، ۱۳۸۷: ۴۳). در خصوص رسیدگی به جنایت علیه صلح و امنیت بین‌المللی، با توسعه مفهوم مسئولیت کیفری فردی که به میزان غیر قابل تردید «آستانه جنایت تجاوز» از ممنوعیت مندرج در مادهٔ ۲(۴) منشور ملل متحد، تخطی نموده است (Draft Code of Crimes against the Peace and Security of Mankind, at 43). در دادگاه‌های کیفری بین‌المللیِ موردی Ad hoc، با تبیین انجام عمل تجاوزکارانه در قالب طرح یا توطئهٔ مشترک، مجرم قلمداد می‌شود (Ambos, 2010: 51). مطابق بند ۴ مادهٔ ۲ منشور سازمان ملل، جنایت تجاوز توأم با قهر و غلبه که بدون اطلاع و رضایت کشور قربانی باشد، مشمول ممنوعیت توسل به زورِ غیر قانونی می‌شود که به وسیلهٔ قطعنامهٔ ۱۴ دسامبر ۱۹۷۴ مجمع عمومی تبیین شده است و موارد اعلامی وفق بند ۴ مادهٔ ۳ قطعنامهٔ مذکور می‌تواند در قالب تعریف جنایت تجاوز گنجانده شود و در این باره، قول و بیان مخالفی وجود نداشته و همگی متفق‌القول هستند (Stahn & Sluiter, 2010: 713). البته باید توجه داشت که مطابق با مواد ۳۹ و ۵۱ منشور ملل متحد، اقدام مزبور اگر با تجویز شورای امنیت بوده و یا به عنوان دفاع مشروع انفرادی یا جمعی (سودمندی، ۱۳۹۴: ۳۵) باشد، شامل استثنائات قانونی می‌شود. ارتکاب جنایت تجاوز توسط افراد که با مسئولیت کیفری فردی همراه است و متمایز از عمل تجاوزکارانهٔ دولتی همراه با مسئولیت بین‌المللی دولتی است، شأن نزول ایجاد دیوان کیفری بین‌المللی را آشکار می‌سازد. مرجع موصوف در سال ۱۹۹۴ میلادی، منبعث از تصمیمات مجمع عمومی سازمان ملل متحد، مستخرج از مادهٔ ۲۰ پیش‌نویس کمیسیون حقوق بین‌الملل (شبث، ۱۳۸۴: ۳۲) پا به عرصه وجود نهاد و صلاحیت آن تحت عنوان جنایات «معاهده‌محور و قراردادی» تعیین شد. پس از این واقعه، اساسنامهٔ رم تصویب‌شده در سال ۱۹۹۸ میلادی، در سال ۲۰۰۲ میلادی با صلاحیت انحصاریِ رسیدگی به جنایت تجاوز با قابلیت انتساب به افراد ظاهر شد. علی‌رغم تصریح فصل هفتم منشور سازمان ملل که شورای امنیت وظیفهٔ حفظ و برقراری صلح و امنیت بین‌المللی و جلوگیری از جنایت تجاوز و احراز آن را دارد، اعضای دائم آن تمایلی به اعطای صلاحیت به دیوان کیفری بین‌المللی ندارند (شریعت‌باقری، ۱۳۹۷: ۲۷ـ۲۸). در مقابل، کشورهای مستعمره و تازه استقلال‌یافته همواره

اصرار و تأکیدی بر این واقعهٔ حقوقی بین‌المللی دارند (Schiff, 2008: 74). البته به منظور تثبیت ارادهٔ جامعهٔ بین‌المللی وفق مادهٔ ۵ اساسنامهٔ رم، صلاحیت رسیدگی موصوف به تعویق افتاد (Sada, 2013: 410) و با این فرایند، دیوان در خصوص این جنایت دارای صلاحیت خفته[1] شد (Evans, 2010: 774) و عدم قطعیت احراز صلاحیت موصوف، خود مبین عدم توافق بین‌المللی در این باره گشت (Glasius, 2006: 62). این در حالی است که به محض احراز جنایت تجاوز توسط شورای امنیت، تکلیف ارجاع امر به دیوان قطعی خواهد بود (Schuster, 2003: 35). فعال‌سازی این صلاحیت همواره برای کشورهای غیرعضو محل تأمل و تردید است (Murphy, 2015: 533, 534). لیکن از حیث ارجاع موضوع از سوی شورای امنیت به واسطهٔ «نقض صلح و امنیت»، امری انکارناپذیر است. با این رویکرد، کنفرانس رم به وسیلهٔ قطعنامهٔ ۳۳۱۴ سال ۱۹۷۴ میلادی توسط مجمع عمومی سازمان ملل به بررسی تعریف و تبیین عناصر تشکیل‌دهندهٔ جنایت تجاوز با معیار اصلی نقض منشور ملل متحد (روبو، ۱۳۹۹: ۷۵۰) که عبارت از جدی‌ترین نوع استفادهٔ غیر قانونی از زور است، پرداخت (سودمندی، ۱۳۹۴: ۵۵).[2] در سال ۲۰۱۰ در کنفرانس کامپالا در این زمینه در قالب بند ۱ مادهٔ ۸ مکرر اساسنامهٔ رم به صدور اصلاحیه مبادرت ورزید و جنایت تجاوز را به واسطهٔ ماهیت، شدت و گسترهٔ عمل آن تعریف نمود و در بند ۲ مادهٔ ۸ مکرر، عمل تجاوزکارانه را با تکمیل عبارت «به هر روش دیگری با منشور ملل متحد در تعارض باشد» تبیین نمود. طبق قواعد حقوق بین‌الملل مربوط به حقوق جنگ، هر گونه نقضِ جدیِ ممنوعیت توسل به زور مندرج در منشور ملل متحد، جنایت تجاوز محسوب می‌شود. این امر مورد تأیید کارگروه ویژهٔ کامپالا[3] نیز قرار گرفت (همان: ۳۰). این مسئله هنگامی قابلیت تحت تعقیب قرار گرفتن را دارد که قائم به ارادهٔ افراد مرتکب نبوده و از جانب دولت به وقوع پیوسته باشد(Gillet, 2013: 836). با امعان‌نظر به نقطهٔ عطف بودن کنفرانس بازنگری کامپالا در سال ۲۰۱۷، که مبنی بر

1. Dormant jurisdiction.
2. See: e.g., Informal Inter-Sessional Meeting of the Special Working Group on the Crime of Aggression, ICC–ASP/5/SWGCA/INF, 5 September 2006, 18-20.
3. Special Working Group on the Crime of Aggression.

توسعهٔ صلاحیت دیوان کیفری بین‌المللی در رسیدگی به جنایت تجاوز برای کشورهای عضو، و عدم توسعهٔ صلاحیت مرجع اخیرالذکر برای کشورهای غیر عضو در امر موصوف در بازهٔ زمانی ماقبل سال ۲۰۱۷ ضروری خواهد بود (Murphy, 2015: 17).

نتایج حاصل از این کنفرانس را می‌توان چنین برشمرد: الف- توسعه مفهوم توسل به زور به لحاظ شدت؛ ب- محدود ساختن و تصریح نمودن مصادیق مرتکبان جنایت تجاوز تحت عنوان «جنایت عالی‌رتبه»؛[1] ج- صلاحیت انحصاری شورای امنیت در فعال‌سازی صلاحیت دیوان نسبت به اقدامات تجاوزکارانه مربوط به روابط میان کشورها و دولت‌های عضو و غیر عضو (روبو، ۱۳۹۹: ۷۵۰)؛ د- مطابق ماده (۱)۱۱۹ اساسنامه دیوان «صلاحیت در تعیین صلاحیت» به دیوان داده می‌شود. با توجه به تعیین صلاحیتِ تکمیلی برای دیوان کیفری بین‌المللی، امکان رسیدگی و تعقیب جمیع مرتکبان جنایت تجاوز میسر نیست (اسمعیل‌زاده ملاباشی، ۱۳۹۶: ۵۲). از این حیث با آمرانه بودن نظم عمومی در سطح بین‌المللی با تعارض و یا حتی تضاد مواجه خواهیم بود.

۲ـ۲. جرائم سایبری و ظهور تجاوز سایبری

بر اساس نوشته‌های پروفسور الریش در کتاب ***پیدایش بین‌المللی حقوق کیفری اطلاعات***، اولین موردی که جرم سایبری نامیده شد، ابتدا در مطبوعات عمومی تحت عنوان «سوءاستفاده‌های غیر قانونی از سیستم و فضای سایبری» در سال ۱۹۶۰ بود (خلیلی‌پور رکن‌آبادی و نورعلی‌وند، ۱۳۹۱: ۱۷۴). جرائم سایبری به اقداماتی اطلاق می‌شوند که در سامانه‌ها و شبکه‌های رایانه‌ای با ایجاد مخاطرات، فرایندهای حاکم را مختل، تضعیف و یا تخریب می‌نمایند و از انواع خاصی نظیر بحران‌سازهای سایبری شامل ویروس‌ها، پالس‌های الکترومغناطیسی و بمب‌های منطقی (همان: ۲۵۰)، جاسوسی سایبری، هک سیاسی در قالب ظهور هکتیویسم (جلالی، ۱۳۹۵: ۱)، سابوتاژها یا خرابکاری سایبری و یا جرائم بیولوژیکی سایبری، فیشینگ و جاسوسی سایبری با قصدهای کاملاً متمایز همچون منافع نظامی، صنعتی، سیاسی و فنی برخوردارند (Dashora, 2011: 251). جرائم سایبری می‌توانند از شدت و ضعف متفاوتی برخوردار

1. Leadership crime.

باشند و دامنهٔ آن‌ها با درگیری‌های کم‌شدت[1] همراه است (هیبلزگری، ۱۳۸۹: ۶۹). ویژگی اختلال، تخریب فاجعه‌آمیز و ممانعت‌کنندهٔ کارکردهای سیستم عمومی، از شاخصه‌های بارز این جرائم است (Kesan & Hayes, 2012: 445). اقداماتی همچون انتشار ویروس استاکس‌نت در سال ۲۰۱۰، حکومت‌ها را با مشکلاتی عظیم همچون اخلال در سیستم‌های غیر نظامی کشور روبه‌رو ساخت که مصداق بارز اخلال در نظم، صلح و امنیت سایبری بین‌المللی به شمار می‌رفت. دوران ما عصری است که در آن سرمایهٔ بانکی در کمتر از یک‌میلیاردم ثانیه از قاره‌ای مورد ربایش و سرقت سایبری قرار می‌گیرد (Hanagan, 2000: 83). در رابطهٔ حقوقی ایجادشده، این ارتباط تنها میان دولت مرتکب و دولت مجنی‌علیه شکل می‌گیرد و می‌توان آن را در قالب «اقدام متقابل» با رعایت اصل تناسب از سوی دولت مجنیّ‌علیه در قالب حق تحمیل مسئولیت بین‌المللی به دولت متجاوز دانست (خلیل‌زاده، ۱۳۹۳: ۳۴). این همان بروز مقابله با قتلگاه سنتی دولت‌های ضعیف، مقابل دولت‌های قوی در «جنگ پست‌مدرن» است (هیبلزگری، ۱۳۸۹: ۵۴). جرائم سایبری را به لحاظ تشخیص دشوارِ مرتکب، «جرائم کور» می‌نامند و اگرچه این جرائم توسط بازیگران غیر دولتی ارتکاب می‌یابند، لیکن دارای قابلیت انتساب به دولت متبوع خواهند بود (Miller, 2014: 227-229). قطعنامهٔ ۳۳۱۴ سال ۱۹۷۴ مجمع عمومی، پایه و اساس اقدامات فرماندهان و هدایت‌کنندگان و مبنای تعریف جنایت تجاوز است (Ophardt, 2010: 13). با امعان‌نظر به بند ۲ مادهٔ ۸ مکرر اساسنامهٔ رم، تجاوزات سایبری در دیوان کیفری بین‌المللی قابلیت پذیرش داشته و باید توجه داشت که مستنبط از مادهٔ ۵۱ منشور ملل متحد، نوع سلاح در تجاوزات مسلحانه بی‌تأثیر و غیر مؤثر خواهد بود.

۳. دفاع مشروع و شدت آستانه در عملیات سایبری

دفاع مشروع در اکثر نظام‌های حقوقی، به عنوان سبب سلب مسئولیت از زیان‌دیده شناخته می‌شود و مطابق رویهٔ بین‌المللی باید آن را به عنوان یک اصل جهانی برشمرد (کاتوزیان، ۱۳۹۵: ۳۱۷). البته منظور از دفاع مشروع، اقدام به حمله به صورت «فعل مثبت»

1. Low-intensity.

است و «ترک فعل» به هیچ عنوان «حمله» محسوب نمی‌شود. این قاعده برای ترک فعلی که جرم هم باشد، صادق است و مستلزم فعل بودنِ حمله و عدم شمول آن نسبت به ترک فعل است.

۳ـ۱. دفاع مشروع از منظر دستورالعمل تالین

در رابطه با عملیات‌های سایبری سازمان‌یافته، انجام‌پذیرفته و هدایت‌شده توسط بازیگران غیر دولتی و انحصاراً در چارچوب قلمرو خود یک دولت، دولت‌ها می‌توانند وفق قوانین داخلی خود (با لحاظ کردن ضوابط حقوق بین‌الملل، مثلاً حقوق بین‌الملل بشر، و در وضعیت‌های معطوف به مخاصمات مسلحانهٔ غیر بین‌المللی وفق حقوق مخاصمات مسلحانه) با زور به آن‌ها پاسخ دهند. حق به کارگیری زور در قالب دفاع مشروع با مجوز صریح قاعدهٔ ۱۳ در دستورالعمل تالین ۱ با توجه به میزان و اثرات عملیات سایبری (Schmitt, 2013: 53) به فراتر از حملات مسلحانهٔ فیزیکی و حملاتی که انحصاراً از رهگذر عملیات‌های سایبری ارتکاب یافته‌اند، تسری می‌یابد. گروه بین‌المللی کارشناسانِ تعیین‌شده در مذاکرات تالین به اتفاق آرا نتیجه گرفت که پاره‌ای از عملیات‌های سایبری می‌توانند به اندازهٔ کافی برای قرار گرفتن ذیل مفهوم «مخاصمهٔ مسلحانه» در معنای مندرج در منشور شدید باشند (NATO Wales Summit Declaration, 2011: paras. 4, 72, 16.3.3). چنانچه توسل به زور، به آستانهٔ یک حملهٔ مسلحانه[1] برسد، دولت حق دارد با به کارگیری زور در قالب دفاع مشروع، دست به پاسخ زند. دیوان، مقیاس و آثاری را به عنوان معیارهای معتبرِ اقدامات واجد وصف یک حملهٔ مسلحانه و تفکیک آن از اقداماتی که فاقد آن وصف هستند، مورد شناسایی قرار داد. اکثریت کارشناسان موافقت کردند که رویهٔ دولتی، حق دفاع مشروع در برابر عملیات‌های سایبری در سطح حملهٔ مسلحانه را که توسط بازیگران غیر دولتی مثل گروه‌های تروریستی یا شورشی و بدون مشارکت مطلق یا اطلاع یک دولت از اقدامات آن‌ها صورت می‌گیرد، دارد. اهداف عملیات سایبری که خواسته‌های فرامرزی بودن، اندازه و آثار حمله را محقق می‌سازد، می‌تواند مبنای حملهٔ مسلحانه را تعیین نماید. اگر هدف ذی‌ربط مربوط به اموال اشخاص دولتی

1. Armed attack.

یا خصوصی موجود و حاضر در قلمرو دولت باشد، اقدام مربوطه حمله‌ای مسلحانه علیه آن کشور قلمداد می‌شود. اِعمال حق دفاع مشروع، مشمول بایسته‌های ضرورت، تناسب، قریب‌الوقوع بودن و فوریت است (قواعد ۷۲ـ۷۳). بی‌گمان، حق دست یافتن به دفاع مشروع نیز مشروط به تعیین منطقیِ در شرف وقوع بودن یا وقوع یافتن حملهٔ مسلحانه و نیز هویت مهاجم است. تعیین این امور نه به صورت پسینی بلکه باید به صورت پیشینی باشد. قاعدهٔ ۷۱ دستورالعمل تالین اذعان می‌دارد دولتی که هدف عملیات سایبریِ در سطح حمله مسلحانه قرار دارد، می‌تواند حق ذاتی خویش مبنی بر دفاع مشروع را اِعمال نماید. شکل‌گیری یا عدم شکل‌گیری حملهٔ مسلحانه توسط عملیات سایبری به مقیاس و آثار آن وابسته است. طبق مادهٔ ۵۱ منشور ملل متحد، در صورت وقوع حمله‌ای مسلحانه علیه یک عضو ملل متحد، و تا زمانی که شورای امنیت اقدامات ضروری را برای حفظ صلح و امنیت بین‌المللی اتخاذ کند، هیچ چیز در منشور حاضر، حق ذاتی دفاع مشروع فردی یا جمعی را مخدوش نمی‌سازد. این قاعده حق دفاع مشروع مبتنی بر حقوق بین‌الملل عرفی را به رسمیت می‌شناسد. گروه بین‌المللی کارشناسان ابراز داشت که اصطلاحات حملهٔ مسلحانه و تجاوز را باید از هم تفکیک کرد. این قاعده به دفاع مشروع می‌پردازد که شرط مسبوق آن «حملهٔ مسلحانه» است. در مقابل، تجاوز یکی از وضعیت‌هایی است که در آن شورای امنیت ملل متحد می‌تواند اختیارات خود را به موجب فصل هفتم منشور ملل متحد در آن مورد به کار گیرد. هرچند عمل تجاوز می‌تواند موجب شکل‌گیری حملهٔ مسلحانه شود، ولی ضرورتاً همیشه این گونه نیست.[1] اجرای دفاع مشروع با قصد پیش‌بینی‌شده[2] صورت می‌گیرد و اقدام با قصد عطف به ماسبق شده،[3] پذیرفته نیست (Schmitt, 2013: 58). مادهٔ ۵۱ منشور ملل متحد به وضعیتی اشاره دارد که در آن، «حمله‌ای مسلحانه رخ داده است». بدیهی است که این ماده، وقایعی که در آن آثار حملهٔ مسلحانه پیشتر پدیدار شده‌اند،

1. Reference to Article 3 (g) of the Definition of Aggression by the International Court of Justice in the Nicaragua Judgment, para. 195.
2. Ex ante.
3. Ex post facto.

یعنی زمانی را که حملهٔ مسلحانهٔ سایبری موجب ایراد خسارت یـا جراحـت شـده یـا در فرایند ایراد آن‌هاست، در بر می‌گیرد. همچنین مادهٔ مزبور، وضعیت‌هـایی را نیـز کـه در آن‌ها عملیات سایبری گام آغازین انجام یک حملهٔ مسلحانهٔ فیزیکی است، شامل می‌شود. مصداق چنین وضعیتی، عملیات‌های سایبری هـدایت‌شـده علیـه پدافنـد هـوایی دولـت دیگر به منظور «آماده‌سازی میدان جنگ» برای نبـردی هـوایی اسـت. دولـت ذی‌ربـط می‌تواند به مجرد «قریب‌الوقوع» بودن حمله از خود دفاع کند. چنین اقدامی در حقوق بین‌الملل، دفاع مشروع پیشگیرانه یا پیش‌دستانه[1] نام دارد کـه بایـد بـه صـورت فـوری و شدید باشد (Ibid.: 61).

۳ـ۲. مفهوم و معیارهای شدت آستانه در اقدامات سایبری

کارگروه بـین‌المللـی کارشناسـان در مـذاکرات تـالین، بـه رویکـردی کـه در صـدد ارزیابی احتمال توصـیف یـک عملیـات سـایبری بـه عنـوان بـه کـارگیری زور از سـوی دولت‌هاست، اشاره کرد. شیوهٔ تبیین‌شده بر این فـرض مبتنـی اسـت کـه در نبـود یـک آستانهٔ تعریف قطعی، دولت‌هـایی کـه در فکـر عملیـات‌هـای سـایبری یـا هـدف آن‌هـا هستند، باید در قبال ارزیابی احتمالی جامعهٔ بین‌المللی از نقض یا عدم نقض ممنوعیـت به کارگیری زور از جانب عملیات‌های ذی‌ربط، حساسیت بالایی داشـته باشـند. آسـتانهٔ صلاحیتی[2] به مفهوم احراز صلاحیتِ یـک مرجـع قـضایی بـین‌المللـی در رسـیدگی بـه جنایت رخ‌داده در سطح جامعه بین‌الملل، نسبت به جنایات بین‌المللـی متعـدد متفـاوت است. این آستانه در جرائم جنگی با فقدان، و در جرائم علیه بشریت به میزان بسیاری با گستردگی یا سازماندهی روبه‌روسـت (ذاکرحسین، ۱۳۹۵: ۴۲). ایـن تفـاوت در خـصوص جنایات سنتی و جنایات سایبری اهمیتـی ویـژه دارد و بـه شـرح زیـر نیازمنـد بررسـی از حیث نظری و قضایی است:

۳ـ۳. ضوابط و معیارهای تعیینیِ نظری، در شدت آستانه

رویکرد فوق بیانگر آن است که احتمال دارد دولت‌ها در حین اتخاذ تـصمیم راجـع

1. Anticipatory self-defence.
2. Jurisdictional threshold.

به توصیف یا عدم توصیف عملیاتی چون عملیات سایبری به عنوان به کارگیری زور، عوامل زیر را مورد نظر قرار دهند و اهمیت قابل توجهی برای آن‌ها قائل شوند. این عوامل صرفاً اسبابی هستند که انجام ارزیابی از سوی دولت‌ها در مورد به کارگیری زور را تحت تأثیر قرار می‌دهند:

الف) شدت: به عنوان حائز اهمیت‌ترین عامل، پیامدهای آسیب فیزیکی به افراد یا اموال در عملیات سایبری که واجد توصیف توسل به زور است؛ به هر میزان که پیامدهای مربوطه از منافع ملی حیاتی بیشتر تخطی کنند، در توصیف عملیات سایبری به عنوان به کارگیری زور، نقش بیشتری خواهند داشت. در این رابطه، دامنه، مدت زمان و تراکم پیامدها، تأثیر چشمگیری بر سنجش شدت آن‌ها خواهد داشت.

ب) فوریت: هر مقدار که پیامدها زودتر بروز پیدا کنند، دولت‌ها فرصت کمتری برای توسل به حل‌وفصل مسالمت‌آمیز یک اختلاف یا پیش‌بینی آثار آسیب‌زای آن‌ها خواهند داشت. دولت‌ها نسبت به پیامدهایی که با تأخیر پدیدار می‌شوند و به آرامی در گذر زمان بروز می‌کنند، نگرانی کمتری از پیامدهای فوری دارند و احتمال توصیف یک عملیات سایبری با نتایج فوری به عنوان به کارگیری زور نسبت به عملیاتی سایبری که حصول آثار مورد نظر آن، هفته‌ها یا ماه‌ها طول می‌کشد، از جانب آن‌ها بالاتر است.

پ) بی‌واسطگی: هر میزان که فاصلهٔ علت و معلولی مابین عمل ابتدایی و پیامدهای آن بیشتر باشد، احتمال کمتری وجود دارد که دولت‌ها عامل مربوطه را ناقض ممنوعیتِ به کارگیری زور قلمداد کنند. احتمال توصیف عملیات سایبری که در آن‌ها علت و معلول به وضوح با یکدیگر پیوند دارند، به عنوان به کارگیری زور، نسبت به عملیات‌هایی که فاصلهٔ این دو از هم بسیار زیاد است، بیشتر است.

ت) میزان رخنه‌گری:[1] میزان رخنه‌گری به مقدار نفوذ اقدامات سایبری در دولت هدف و سامانه‌های سایبری آن بر خلاف منافع دولت دلالت دارد. به عنوان یک قاعده، هر قدر که یک سامانهٔ سایبری هدفی ایمن‌تر باشد، نگرانی راجع به نفوذ در آن بیشتر است. امکان نفوذ در سامانه‌ای نظامی که دارای گواهینامهٔ بیمهٔ ارزیابی سطح ۷[2]

1. Invasiveness.
2. Evaluation Assurance Level 7-EAL7.

مطابق با استاندارد امنیتی معیارهای مشترک [ارزیابی امنیتی فناوری اطلاعات] است، نسبت به بهره‌برداری صرف از آسیب‌پذیری‌های یک سامانهٔ فاقد گواهینامه و همگانی در دانشگاهی غیر نظامی یا کسب و کارهای کوچک، بیشتر بوده و امکان شدت رخنه‌گری بالاتری را دارد. به علاوه، هر قدر که آثار قصدشده از یک عملیات سایبری، محدود به کشوری خاص باشد، شدت رخنه‌گری قابل تصور از آن عملیات بالاتر است.

ث) سنجش‌پذیری آثار: این عامل از تمایل بالای کشورها به توصیف اقدامات به عنوان به کارگیری زور در زمانی که پیامدها آشکار هستند، ناشی می‌شود. نیروهای مسلح همواره دست به عملیاتی زده‌اند که به کارگیری زور به شمار آمده و آثار عملیات‌ها عموماً قابل ارزیابی بوده‌اند. در عرصهٔ سایبر، ممکن است پیامدها کمتر آشکار و مشخص باشند. هر قدر که مجموعهٔ پیامدها قابل سنجش‌تر و مشخص‌تر باشد، ارزیابی وضعیت برای دولت در رسیدن یا نرسیدن عملیات سایبری مورد نظر از لحاظ سطح به کارگیری زور آسان‌تر خواهد بود.

ج) ماهیت نظامی: وجود پیوند میان عملیات سایبری مورد نظر و عملیات‌های نظامی، احتمال توصیف به عنوان به کارگیری زور را بالا می‌برد. مقدمهٔ منشور مقرر می‌دارد: «جز در راستای منفعت مشترک، از نیروهای مسلح استفاده نخواهد شد». مادهٔ ۴۴ در وضعیتی که آشکارا بر به کارگیری زور نظامی دلالت دارد، از اصطلاح «زور» بدون واژهٔ توصیفی «مسلح» استفاده می‌کند. به کارگیری زور از دیرباز به عنوان نشانگر استفاده از عامل زور توسط نیروهای نظامی یا دیگر نیروهای مسلح فهم شده و البته ماهیت نظامی زیرساخت سایبریِ هدف عملیات سایبری نیز قابل ملاحظه است که دولت‌ها آن را مدّنظر قرار خواهند داد.

چ) مشارکت دولت: میزان مشارکت دولت در عملیات سایبری را در گستره‌ای از عملیات‌هایی که توسط خود دولت انجام می‌شوند (نظیر فعالیت‌های نیروهای مسلح با عوامل اطلاعاتی آن) تا مواردی که دخالت دولت در آن ثانوی و جزئی است، دربرمی‌گیرد. به هر میزان که پیوند میان یک دولت و عملیات‌های سایبری آشکارتر و نزدیک‌تر باشد، احتمال توصیف آن عملیات‌ها به عنوان به کارگیری زور توسط آن دولت از سوی دیگر دول بیشتر خواهد بود.

ح) مشروعیت فرضی: حقوق بین‌الملل به طور کلی واجد ماهیتی منع‌کننده است. اعمالی که ممنوع نیستند، مجازند. در نبود ممنوعیت صریح معاهداتی یا ممنوعیت عرفی پذیرفته‌شده، یک عمل قانونی فرض می‌شود؛ برای نمونه، حقوق بین‌الملل، تبلیغات، عملیات‌های روانی، جاسوسی یا صِرف فشار اقتصادی را به‌خودی‌خود منع نمی‌کند. بنابراین، اَعمالی که ذیل این موارد و دیگر مقولات از این دست قرار می‌گیرند، به صورت مفروض قانونی هستند و به همین سبب احتمال تلقی آن‌ها به عنوان به کارگیری زور از سوی دولت‌ها پایین است (Schmitt, 2017: 333-337).

۳ـ۴. ضوابط و معیارهای تعیینی قضایی، در شدت آستانه

اولین آستانهٔ اثباتی در ارزیابی مقدماتی، «مبنای معقول»[1] است که مبنای تصمیم‌گیری دادستان قرار می‌گیرد. دومین آستانه برای اصدار قرار جلب یا احضاریه علیه متهم، «موجبات معقول»[2] خواهد بود، و سومین آستانه که در مرحلهٔ پیش دادرسی و به منظور تأیید اتهامات متهم به کار می‌رود، «موجبات متقن و محکم»[3] است. چهارمین آستانه برای محکومیت و اِتمام دادرسی قاطع و مستند، آستانهٔ «ورای شک معقول»[4] است. پنجمین آستانهٔ مطرح، وفق مادهٔ ۵۳ اساسنامهٔ رم همانا «دلایل متقن و محکم»[5] در راستای احراز تحقق منفعت عدالت و انطباق با مقتضیات آن است (ذاکرحسین، ۱۳۹۹: ۱۹۱ـ۱۹۲). دیوان کیفری بین‌المللی برای قابلیت پذیرش دعوی از شدت آستانهٔ شدت[6] در بند ۱د ماده ۱۷ اساسنامهٔ دیوان یاد می‌کند (Pre-Trial Chamber 1, 2006: 2) و طرح مفهوم آستانهٔ شدت به طور خاص به سال ۱۹۹۲ برمی‌گردد. در تعریف و جایگاه مفهوم آستانهٔ شدت باید گفت که هر زمانی وضعیت خاصی از سوی دولت‌ها، شورای امنیت یا به ابتکار دادستان دیوان بین‌المللی شناسایی شود، دادستان مزبور باید مبنای معقولی را در امر

1. Reasonable basis.
2. Reasonable grounds.
3. Substantial grounds.
4. Beyond reasonable doubt.
5. Substantial reasons.
6. Gravity threshold.

تصمیم‌گیری نسبت به تعقیب نمودن یا عدم تعقیب اتخاذ نماید. مرحلهٔ اول بر اساس صلاحیت موضوعی، زمانی و شخصی می‌پردازد. در این مرحله، اقدام تحت عنوان قابلیت پذیرش از حیث صلاحیت تکمیلی[1] صورت می‌گیرد (کیتی چایساری، ۱۳۸۷: ۵۴). مرحلهٔ دوم از حیث داشتن شدت کافی و یا آستانهٔ شدت بر اساس بند ۱د از مادهٔ ۱۷ اساسنامه، باید قابلیت پذیرش داشته باشد. معیارهای قابل پذیرش در آستانهٔ شدت عبارت‌اند از:

الف) درجه و میزان جرم که در حال حاضر در خصوص جرائم سایبری و ارتکاب کمّی آن انکار ناپذیر است.

ب) ماهیت جرم که در خصوص موضوع مزبور دارای وضعیت غیر سنتی و غیر عادی بوده و دارای ماهیت گستردگی در اضرار به غیر است و در حالت بین‌المللی آن می‌تواند در قالب ورود خسارات جبران‌ناپذیر متصور باشد.

ج) شیوهٔ ارتکاب جرم که در خصوص مانحن‌فیه بدون حضور در جغرافیای جرم و در محیط امنیت عدم دستگیریِ مرتکب می‌تواند فرایند جرم ارتکابی را به طور کامل طی نماید.

د) تأثیر ارتکاب جرم که علی‌رغم مضیق بودن رکن مادی جرائم موصوف به واسطهٔ گستردگی رکن معنوی و سوءنیت خاص قصد مجرمانه بسیار موسع خواهد بود.

تحقق و تعیین آستانهٔ تجاوز در مذاکرات تالین ۱ مستخرج از قاعدهٔ ۱۳ به معنای ارتکاب جرائم سایبری است که به آستانهٔ «حملهٔ مسلحانه» رسیده باشد. همچنین با توجه به تصویب کارگروه کارشناسی مطابق بند ۶ از مادهٔ ۶۹ دستورالعمل تالین ۱، می‌توان رسیدن به آستانهٔ «حملهٔ مسلحانه» را از مفهوم سنتی آن به فعالیت‌های مبتنی بر توسل به زور در فعالیت فعالان غیر دولتی، که تعرضاتشان می‌تواند تجاوز به حاکمیت کشور مجنیّ‌علیه تلقی شود، تسری و توسعه داد (Schmitt, 2013: 49-52). با عنایت و استنباط از وجود قاعدهٔ ۱۷ در دستورالعمل تالین ۲ در سال ۲۰۱۷، حقوق مسئولیت بین‌المللی به صورت عینی بر وجود وقایع اعمال می‌شود. عملیات‌های سایبری یک بازیگر

1. Complimentary.

غیر دولتی، چنانچه یک دولت به صورت واقعی بر آن رفتار خاص بازیگر غیر دولتیِ ذی‌ربط، «کنترل مؤثر» داشته باشد، به آن دولت قابل انتساب است. شدت عملیات‌های سایبریِ هدایت‌شده علیه دولت مجنیّ‌علیه، به میزان قابل ملاحظه‌ای حائز اهمیت است و عملیات‌های سایبری با سطح و آستانهٔ پایین که صرفاً موجب اختلال گردد، نیاز به اثبات و مستندسازی دارد (Id., 2017: 82-89). البته در صورتی جنایت تجاوز به وقوع می‌پیوندد که فرد مجرم از اوضاع و احوال واقعی که منجر به نقض آشکار حقوق و قوانین می‌شود، مطلع باشد. این معیار در حقیقت بیان‌کنندهٔ الزامات عنصر معنوی مندرج در مادهٔ ۹۱ اساسنامهٔ رم است که هم قصد و هم اطلاع را با هم در بر می‌گیرد.

۳ـ۵. مسئولیت کیفری فردی

در قلمرو صلح و امنیت بین‌المللی و در وضعیت فعلی عرصهٔ بین‌المللی، ارتباط با چالش‌های معاصر در حقوق بین‌الملل کیفری از نظر تمامی دولت‌های عضو و حتی غیر عضو دیوان کیفری بین‌المللی مغفول واقع شده است (Anderson, 2010: 421). در مواد ۶ تا ۸، دستورالعمل تالین دولت‌ها را در نقض تعهدات بین‌المللی در حوزهٔ اقدامات سایبری مسئول دانسته و همچنین این اقدامات را تعریف نموده است. با وجود این، اقدامات سایبری داخلی یک کشور بدون کنترل مؤثر، آن دولت را از مقولهٔ مسئولیت مستثنا دانسته است (Schmitt, 2013: 40). قابلیت پذیرش دعوی در دیوان کیفری بین‌المللی را می‌توان اِعمال صلاحیت تکمیلی با حفظ حق تقدم رسیدگی به جنایاتی نظیر «تجاوز سایبری» برای دادگاه‌های ملی، در اساسنامهٔ رم به صورت بالقوه دانست (Delmas-Marty, 2006: 3). قابلیت پذیرش به لحاظ جلوگیری از تعارض حاکمیت ملی در جرائم ارتکابی سرزمینی با حاکمیت بین‌المللی در جنایات بین‌المللی و نیز مهار شکل‌گیری اقتدار قضایی فوق‌العاده دیوان به سبب نگرانی دولت‌های بزرگ مؤثر است (عنایت، ۱۳۸۲: ۱۳۴ـ۱۳۵). توجه به «مکانیزم ماشه» در راستای بیان توانمندی دادستان و دادرسی یک موضوع، به منظور اعمال صلاحیتش در جایگاه «فعال‌سازی صلاحیت خفتهٔ دیوان کیفری بین‌المللی»[1] ضروری است (ذاکرحسین، ۱۳۹۹: ۸۲). در مورد

1. Activation of Dormant Jurisdiction in the International Criminal Court.

نقض صلح و امنیت سایبری که بروز آن به وسیلهٔ ارتکاب حملات یا جرائم سایبری رخ می‌دهد، مسئولیت کیفری فردی منحصر به فرماندهان، یا کنترل مؤثر تحت سیاست حاکمه و متخذه از سوی دولت متخاصم، منعکس‌کنندهٔ حقوق بین‌المللی عرفی خواهد بود (Schmitt, 2013: 81, 83). مستند به مادهٔ **۹** مکرر اساسنامهٔ رم، استقرار مسئولیت با صدور دستور حمله یا ارتکاب جرائم سایبری محقق می‌شود و اطلاعات و اِشراف فنی و تخصصی حاکم بر فناوری‌های سایبری ضرورت ندارد (Ambos, 2016: 503-504). با توجه به سختی احراز سوءنیت و عنصر معنوی در تجاوز سایبری، بروز این جرائم در قالب «فاعل معنوی»[1] و یا «فاعل غیر مباشر»[2] برای مرتکبان متصور و قابل «انتساب جزایی» خواهد بود. تعریف فاعل معنوی آن است که فردی جهت داشتن اقتدار، جرم [جنایتی] عمدی را از طریق فردی که دارای مسئولیت کیفری است، مرتکب می‌شود (اردبیلی، ۱۴۰۰: ۲/ ۵۱ـ۵۲). فاعل معنوی در مفهوم مغز متفکر و عامل اساسی بروز جنایت، مورد قبول تمام نظام‌های حقوقی است (Giliker, 2010: 138). فاعل غیر مباشر، مغز متفکر جنایت به صورت غیر قابل ارجحیت و فاقد اولویت، در سیاست جنایی و کیفری خواهد بود (Elliott & Quinn, 2005: 469). فاعل معنوی برگرفته از حقوق کیفری عرفی است که تفاوت اساسی با مرتکب جرم و معاون جرم دارد. معاون جرم ضمن داشتن سوءنیت، شخصی را وادار، تحریک یا ترغیب می‌نماید و به تبع، مباشر و فاعل اصلی[3] هستند که مسئولیت کیفری پیدا می‌کنند؛ حال آنکه فاعل معنوی، مسئولیت مستقل دارد و فاعل غیر مباشر فاقد مسئولیت کیفری است (Ashworth, 2006: 453). با توجه به گسترش فضای سایبری در حوزهٔ عملیات و اقدامات بین‌المللی، دولت‌ها و حکومت‌ها در مقام ورود اتهام به کشور متخاصم و یا در مقام دفاع مشروع، استنباط‌های خود را تفسیر و گسترش می‌دهند (Dunlap, 2011: 83). نقش مؤثر و انکارناپذیر بازیگران غیر دولتی نیز در این خصوص، در مذاکرات تالین خاصه در سال **۲۰۱۷** میلادی شناسایی و تصریح شد.

1. Perpetration-by-means.
2. Auteurmediat.
3. Principal offender.

نتیجه‌گیری

اصطلاح «صلح و امنیت بین‌المللی» برگرفته از میثاق جامعهٔ ملل، در عصر فناوری‌های نوین، خاصه دوران ظهور و بروز فعالیت‌های سایبری، در قالب «صلح و امنیت بین‌المللی سایبری» رخ می‌نماید. تصور پا به عرصه گذاشتن هژمونی‌های قدرت‌های بزرگ با ارتکاب حملات سایبری و بروز جنایت تجاوز سایبری، نقض فصل هفتم منشور ملل متحد و مستند به مادهٔ ۲ اعلامیهٔ روابط دوستانهٔ مجمع عمومی ورسای که بیان‌کننده حل‌وفصل اختلافات به شیوه‌های مسالمت‌آمیز توسط دولت‌هاست، به صورت یک خطر برای صلح جهانی، نقض صلح و ایجاد تجاوزی انتزاعی و مجازی را[1] ممکن می‌سازد. دستورالعمل تالین در سال‌های ۲۰۱۳ و ۲۰۱۷ مطابق با بند الف قاعدهٔ ۶۵ دستورالعمل تالین، امکان توسعهٔ مسئولیت کیفری فردی را به شرط احراز جرائم سایبری به واسطهٔ ماهیت، شدت و گستردگی و آستانهٔ مقتضی ممکن ساخته است. مفهوم شدت آستانه در مذاکرات تالین زمانی است که حمله به آستانهٔ «حملهٔ مسلحانه» برسد. موجبات ضرورتِ احراز مسئولیت کیفری فردی در جنایت تجاوز سایبری در قالب «فاعل معنوی» و به عنوان مغز متفکر جنایت قابل پیگرد خواهد بود. فعالیت‌های سایبری با توسل به زور توسط فعالان غیر دولتی می‌تواند به مفهوم تجاوز سنتی به تمامیت ارضی و حاکمیت کشور مجنیّ‌علیه تلقی شده و توسعه یابد. توجه به بند ج قاعدهٔ ۹ دستورالعمل تالین، بیان‌کنندهٔ دکترین فعالیت سایبری دارای اثرگذاری اساسی در قلمرو خود است. بر این اساس، اِعمال صلاحیت بر یک جنایت، مستلزم وقوع عنصر سازندهٔ آن جنایت در قلمرو دولت است. دولت‌ها در مقام عمل حتی در مورد تفسیر قواعد حقوقی، هم منافع و هم شرایط موجود خود را در نظر گرفته و مطابق با آن، رویه‌ای را در پیش می‌گیرند. به عبارت دیگر، شرایط مناسب با رسیدگی به این گونه جنایات باید فراهم گردد و حتی می‌توان با اشراف کامل بر تأثیرگذاری آن‌ها بر دولت مجنیّ‌علیه در اعطای صلاحیت به دیوان کیفری بین‌المللی و یا تأسیس «پلیس سایبری بین‌المللی» با رویکرد پیشگیرانه و یا تأسیس «دیوان کیفری سایبری بین‌المللی» با رویکرد پیگیرانه در قالب واکنش جامعهٔ بین‌المللی در مقابل این نقض آشکار مبادرت نمود.

---

1. In abstracto.

کتاب‌شناسی

۱. اردبیلی، محمدعلی، ***حقوق جزای عمومی***، چاپ پنجاه و هشتم، تهران، میزان، ۱۴۰۰ ش.

۲. اسمعیل‌زاده ملاباشی، پرستو، «حمله سایبری به مثابه جنایت تجاوز و بررسی صلاحیت دیوان کیفری بین‌المللی در رسیدگی به آن»، ***مجله پژوهش‌های حقوق جزا و جرم‌شناسی***، سال پنجم، شماره ۱۰، پاییز و زمستان ۱۳۹۶ ش.

۳. بریث‌ناچ، سیموس، ***جرم و مجازات از نظرگاه امیل دورکیم***، ترجمه محمدجعفر ساعد، تهران، خرسندی، ۱۳۸۷ ش.

۴. خلیل‌زاده، مونا، «اقدامات متقابل علیه حملات سایبری در حقوق بین‌الملل»، ***مجله حقوقی استیناف***، سال اول، شماره ۲، بهار ۱۳۹۳ ش.

۵. خلیلی‌پور رکن‌آبادی، علی، و یاسر نورعلی‌وند، «تهدیدات سایبری و تأثیر آن بر امنیت ملی»، ***فصلنامه مطالعات راهبردی***، سال پانزدهم، شماره ۲ (پیاپی ۵۶)، تابستان ۱۳۹۱ ش.

۶. دایموند، جَرِد، ***فروپاشی؛ چگونه جوامع راه فنا یا بقا را برمی‌گزینند***، ترجمه فریدون مجلسی، چاپ ششم، تهران، نشر نو، ۱۴۰۰ ش.

۷. ذاکرحسین، محمدهادی، ***آیین پیش‌دادرسی دیوان کیفری بین‌المللی ـ دفتر نخست: فرایند گزینشگری قضایا***، تهران، شهر دانش، ۱۳۹۹ ش.

۸. همو، ***راهنمای دیوان کیفری بین‌المللی***، تهران، شهر دانش، ۱۳۹۵ ش.

۹. روبو، دیدیه، ***حقوق کیفری بین‌المللی***، ترجمه بهزاد رضوی‌فرد و محمد فرجی، تهران، میزان، ۱۳۹۹ ش.

۱۰. سودمندی، عبدالمجید، ***رسیدگی به جنایت تجاوز در دیوان کیفری بین‌المللی***، مقدمه محمدجواد شریعت‌باقری، تهران، نگاه بینه، ۱۳۹۴ ش.

۱۱. شبث، ویلیام ا.، ***مقدمه‌ای بر دیوان کیفری بین‌المللی***، ترجمه سیدباقر میرعباسی و حمید الوئی نظری، تهران، جنگل، ۱۳۸۴ ش.

۱۲. شریعت‌باقری، محمدجواد، ***حقوق کیفری بین‌المللی***، چاپ پانزدهم، تهران، جنگل، جاودانه، ۱۳۹۷ ش.

۱۳. عنایت، سیدحسین، «قابلیت پذیرش دعوی در دیوان کیفری بین‌المللی»، مقاله در: ***دیوان کیفری بین‌المللی و جمهوری اسلامی ایران***، به اهتمام اسحاق آل حبیب، چاپ هشتم، تهران، وزارت امور خارجه، ۱۳۸۲ ش.

۱۴. کاتوزیان، ناصر، ***الزام‌های خارج از قرارداد (مسئولیت مدنی)***، چاپ چهاردهم، تهران، دانشگاه تهران، ۱۳۹۵ ش.

۱۵. کیتی چایساری، کریانگ ساک، ***حقوق کیفری بین‌المللی***، ترجمه حسین آقایی جنت‌مکان، چاپ سوم، تهران، جنگل، ۱۳۸۹ ش.

۱۶. میرمحمدصادقی، حسین، ***دادگاه کیفری بین‌المللی***، تهران، دادگستر، ۱۳۸۸ ش.

۱۷. هیبلزگری، کریس، ***جنگ پست‌مدرن، سیاست نوین درگیری***، ترجمه احمدرضا تقاء، چاپ سوم، تهران، دانشگاه امام حسین علیه‌السلام، ۱۳۸۹ ش.

18. Akehurst, Michael, ***Jurisdiction in International Law***, Oxford University Press, 2008.

19. Ambos, Kai, "Individual Criminal Responsibility for Cyber Aggression", ***Journal of Conflict and Security Law***, Vol. 21(3), Oxford University Press, 2016.

20. Id., "The Crime of Aggression after Kampala", ***German Yearbook of International Law***, Vol. 53, 2010.

21. Anderson, Michael, "Reconceptualizing Aggression", ***Duke Law Journal***, Vol. 60(2), 2010.
22. Ashworth, Andrew, ***Principles of Criminal Law***, 5th Ed., London, Oxford University Press, 2006.
23. Blake, Duncan & Joseph S. Imburgia, "Bloodless Weapons? The need to conduct legal reviews of certain weapons and the implications of defining them as 'Weapons'", ***Air Force Law Review***, Vol. 66(1), 2010.
24. Clark, Roger S., "The Crime of Aggression and the International Criminal Court", in: José Doria & Hans-Peter Gasser & M. Cherif Bassiouni (Eds.), ***The Legal Regime of the International Criminal Court; Essays in Honour of Professor Igor Blishchenko***, Martinus Nijhoff Publishers, 2009.
25. Dashora, Kamini, "Cyber Crime in the Society: Problems and Preventions", ***Journal of Alternative Perspective in the Social Science***, Vol. 3(1), 2011.
26. Declaration on Friendly Relations, prins 3; International Law Commission, Declaration on Rights and Duties of States, Annexed to GTRes. 375(IV) (6 December 1949) Art. 3.
27. Delmas-Marty, Mireille. "Interactions between National and International Criminal Law in the Preliminary Phase of Trial at the I.C.C", ***Journal of International Criminal justice***, Vol. 4(1), 2006.
28. Dunlap, Charles J., Jr., "Perspectives for Cyber Strategists on Law for Cyberwar", ***Strategic Studies Quarterly***, Vol. 5(1), 2011.
29. Elliott, Catherine & Frances Quinn, ***Criminal Law***, 3rd Ed., London, Cambridge University Press, 2005.
30. Evans, Malcolm D., ***International Law***, 3rd Ed., New York, Oxford University Press, 2010.
31. Giliker, Paula, ***Vicarious Liability in Tort: A Comparative Perspective***, 2nd Ed., London, Cambridge University Press, 2010.
32. Glasius, Marlies, ***The International Criminal Court: A Global Civil Society Achievement***, New York, Routledge Taylor & Francis Group, 2006.
33. Hanagan, Michael, "State and Capital: Globalizations Past and Present", in: Don Kalb & Marco van der Land & Richard Staring & Bart van Steenbergen & Nico Wilterdink (Eds.), ***The Ends of Globalization: Bringing Society Back In***, Oxford University Press, 2000.
34. ICRC, A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Addition Protocol 1 of 1977 - International Committee of the Red Cross - Genrva, 2006.

35. Informal Inter-Sessional Meeting of the Special Working Group on the Crime of Aggression, ICC–ASP/5/SWGCA/INF.1, 5 September 2006, 18-20, <https://asp.icc-cpi.int/sites/asp/files/asp_docs/SWGCA/ICC-ASP-5-SWGCA-INF1_English.pdf>.
36. Kesan, Jay P. & Carol M. Hayes, "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace", ***Harvard Journal of Law & Technology***, Vol. 25(2), 2012.
37. May, Larry, ***Aggression and Crimes against Peace***, New York, Cambridge University Press, 2008.
38. Miller, Kevin L., "The Kampala Compromised and Cyberattacks: Can There be an International Crime of Cyber-Aggression?", ***Southern California Interdisciplinary Law Journal***, Vol. 23(2), 2014.
39. NATO Wales Summit Declaration, para. 72; Government Response to the AIV/CAVV Report, para. 4; The White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World at 10, 13; DoD Manual, para. 16.3.3, 2011.
40. Ophardt, Jonathan A., "Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield", ***Duke Law & Technology Review***, Vol. 9(1), 2010.
41. Reference to Article 3 (g) of the Definition of Aggression by the International Court of Justice in the Nicaragua Judgment.
42. Ryngaert, Cedric, ***Jurisdiction in International Law***, Oxford University Press, 2008.
43. Schiff, Benjamin N., ***Building the International Criminal Court***, New York, Cambridge University Press, 2008.
44. Schmitt, Michael N., "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defence, and Armed Conflicts", in: ***Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy***, Washington, National Academic Press, 2010.
45. Id., ***Tallinn Manual on the International Law Applicable To Cyber Warfare***, Cambridge University Press, 2013.
46. Id., ***Tallinn Manual 2.0 on the International Law Applicable To Cyber Operations***, Cambridge University Press, 2017.
47. Schuster, Matthias, "The Rome Statute and the Crime of Aggression: A Gordian Knot in Search of a Sword", ***Criminal Law Forum***, Vol. 14(1), 2003.
48. Stahn, Carsten & Göran Sluiter (Eds.), ***The Emerging Practice of the International Criminal Court***, Series: ***Legal Aspects of International Organizations***, Vol. 48, Leiden, Martinus Nijhoff Publishers, 2009.