مجله حقوقی بین‌المللی/ شماره ۶۳/ پاییز ـ زمستان ۱۳۹۹/ صفحات ۲۶۴ ـ ۲۳۷

موانع بنیادین فراروی تدوین حقوق بین‌الملل حاکم بر حملات سایبری*

علیرضا رنجبر **
علی گرشاسبی ***

شناسه دیجیتال اسناد (DOI) : 10.22066/CILAMAG.2020.111943.1823
تاریخ دریافت: ۱۳۹۸/۰۸/۱۹ تاریخ پذیرش: ۱۳۹۸/۱۰/۲۹

برای آنکه دنیایی را در یک دانه شن ببینی،
و بهشتی را در یک گُل وحشی،
بی‌نهایت را در دست خود نگه دار،
و ابدیت را در یک ساعت قرار ده ...
ویلیام بلیک

چکیده

عملیات سایبری به علت ماهیت انتزاعی فضای سایبر و مفاهیم ناملموس مطرح در آن، نسبت به فضای عینی، قلمرویی نا شناخته برای حقوق بین‌الملل به حساب می‌آید. قدم‌گذا شتن حقوق بین‌الملل در قلمرو سایبر، همچون قدم‌گذاشتن *آلیس* در سرزمین عجایب، مملو از شگفتی‌ها و ناشناخته‌ها است که در مقایسه و مطابقت با قوانین دنیای عینی، هنوز نمی‌توان برای اتفاقات درون آن، پاسخ در ستی پیدا کرد. این فرایند، منجر به ظهور موانعی در مسیر تدوین حقوق بین‌الملل حاکم بر حملات سایبری شده است. بنیادی‌ترین این موانع را می‌توان در دو مورد «کاستی در ادبیات حقوقی بین‌المللی مرتبط با مفاهیم تکنیکی حملات سایبری» و «ضعف در برقراری ارتباط بین مفاهیم حقوقی دنیای عینی و دنیای سایبری» خلاصه کرد. گرچه اصول و قواعد حقوق بین‌الملل پاسخگوی قسمتی از جنبه‌های حقوقی

* نویسندگان از دکتر پوریا عسکری، عضو هیئت علمی دانشگاه علامه طباطبایی(ره) که با نظرات ارزشمند خود موجب تقویت این نگاره شدند تشکر می‌کنند.

** نویسنده مسئول، کارشناسی ارشد حقوق بین‌الملل، دانشکده حقوق دانشگاه آزاد اسلامی واحد تهران مرکزی
alirezaranjbar@ymail.com
*** دانش‌آموخته دکتری حقوق بین‌الملل دانشکده حقوق‌وعلوم‌سیاسی دانشگاه تهران aligarshasbi@alumni.ut.ir

بین‌المللی حملات سایبری است، اختلاف‌نظر دولت‌ها حکایت از آن دارد که پاسخ‌های فعلی کافی نبوده و ناسازگاری‌ها بر سازگاری‌ها غلبه دارد. عجالتاً دو راهکار کلی «تدوین معاهدات منطقه‌ای و بین‌المللی» و «توسل به اقدامات موجد اعتماد» را می‌توان به منظور ازمیان‌برداشتن موانع بنیادین پیش روی تدوین حقوق بین‌الملل حاکم بر حملات سایبری معرفی کرد تا از طریق این دو اقدام، ادبیات حقوقی بین‌المللی مربوط به حملات سایبری قوام یابد و مدون شود.

واژگان کلیدی

حمله سایبری، فضای سایبر، دفاع مشروع، توسل به زور، بازیگران غیردولت

مقدمه

ظهور و گسترش فضای سایبر موجب شکل‌گیری دنیایی انتزاعی درون دنیای عینی شده است؛[1] دنیایی که مأمنی برای ماجراجویی بعضی از اشخاص–دولت‌ها و بازیگرانِ غیردولتی و اشخاص حقیقی و حقوقی شده که با بهره‌گیری از ویژگی‌های این فضای جدید، در صدد دستیابی به اهدافِ غالباً غیرقانونی خود از طریق فضای سایبر هستند. گرچه قانونگذاران و دولتمردان سعی دارند با تعمیم دامنه قوانین موجود و تفسیر موسع این قوانین که بر اساس خصوصیات دنیای عینی تدوین شده‌اند، محیط دنیای سایبر را همچون محیط دنیای عینی، نظام‌مند و مبتنی بر قانون کنند (مجازی‌سازی قوانین موجود)، ویژگی‌های منحصر به فرد این فضا و تمایز دنیای سایبر با دنیای عینی در بعضی از مفاهیم و اَشکال، تا کنون مانع از تحقق کامل این هدف شده است.

اقدامات خصمانه سایبری[2] ازجملهٔ این ماجراجویی‌هاست که از طریق دنیای سایبر محقق شده و گاه آثار مخرب و جبران‌ناپذیری هم در بُعد عینی و هم در بُعد سایبری دارد که در بعضی موارد قابل مقایسه با حملات مسلحانه است و از آن به‌عنوان حملات سایبری یاد می‌شود. اما برخلاف دنیای عینی که «حقوق توسل به زور» و «حقوق بشردوستانه»، در و برای آن تدوین و تکامل

۱. بعضی نویسندگان اعتقاد دارند فضای سایبر، دنیایی موازی و متفاوت با فضای عینی است و به همین علت، ویژگی‌های آن کاملاً ناشناخته و ناملموس است. در اینجا باید این نکته توضیح داده شود که گرچه موازی‌بودن و متفاوت‌بودن فضای سایبر با فضای عینی انکارناپذیر است، این به معنی جدابودن و مستقل‌بودن فضای سایبر از فضای عینی نیست. ارتباط این دو قلمرو با یکدیگر مانع از آن می‌شود که این دو فضا مجزا از یکدیگر قلمداد شوند. بدون تردید، حیات و ثبات فضای سایبر به فضای عینی وابسته است. در حقیقت، گرچه فضای سایبر به‌صورت موازی با فضای عینی وجود دارد، مستقل از آن نیست بلکه جزئی از فضای عینی به حساب می‌آید. برای درک این موضوع می‌توان سخت‌افزارهایی (مانند سرورها) را مثال زد که در دنیای عینی واقع شده‌اند و بدون وجود آن‌ها، تصور فضای سایبر محال است. به عبارت دیگر، گرچه تصور دنیای عینی بدون وجود دنیای سایبر ممکن است، خلاف آن، یعنی وجود دنیای سایبر بدون وجود دنیای عینی ممکن نیست.

۲. این اقدامات شامل طیف گسترده‌ای از فعالیت‌ها ازجمله هک‌کردن تلفن همراه و دزدی اطلاعات شخصی بخصوص دزدی از اشخاص معروف، سرقت اطلاعات محرمانه، جاسوسی و گردآوری اطلاعات، ازکارانداختن تارنماهای دولتی و سایر اقدامات می‌شوند.

یافته و جایگاه قابل قبولی را به دست آورده، در حال حاضر، سرفصلی به نام حقوق بین‌الملل حاکم بر مخاصمات سایبری (یا حقوق حملات سایبری) که مورد قبول اکثریت دولت‌ها بوده و در خصوص آن اجماع حاصل شده و الزام‌آور باشد وجود ندارد. گرچه اقدام ناتو در راستای تدوین حقوق بین‌الملل حاکم بر حملات سایبری در قالب دو نسخه «راهنمای تالین برای حقوق بین‌الملل قابل اعمال بر نبردهای سایبری»[۳] که در سال‌های ۲۰۱۳ و ۲۰۱۷ و تحت نظارت *مایکل اِن. اشمیت* انجام شد،[۴] گامی رو به جلو به حساب می‌آید،[۵] همان‌طور که از نام آن‌ها پیداست، این دو مجموعه چیزی بیش از راهنما نیستند و به نظر می‌رسد تا رسیدن به نقطه‌ای که قوانین و مقررات لازم‌الاجرایی در این زمینه وضع شود، فاصله وجود دارد.[۶] رسیدن به چنین نقطه‌ای نیازمند بررسی دقیق و واکاوی جنبه‌های مختلف حملات سایبری و خلأهایی است که حقوق بین‌الملل تا کنون نتوانسته پاسخی قاطع را پیش روی دولت‌ها جهت پُرکردن این خلأها قرار دهد. برطرف‌کردن خلأهای موجود در حقوق بین‌الملل در خصوص حملات سایبری محقق نخواهد شد مگر زمانی‌که به‌عنوان اولین قدم، موانع پیش روی حقوق بین‌الملل مربوط به حملات سایبری شناسایی و از میان برداشته شود. بدون

3. *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, 2013; *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, 2017.

۴. نسخه اول راهنمای *تالین* بر عملیات‌های سایبری جدی متمرکز است که منجر به نقض اصل منع توسل به زور (بند ۴ ماده ۲ منشور ملل متحد) در روابط بین‌الملل شده و توسل به حق دفاع مشروع را برای دولت‌ها امکان‌پذیر می‌کند یا حمله سایبری که در طول مخاصمه مسلحانه صورت می‌پذیرند. اما نسخه دوم به تحلیل حقوقی اقدامات سایبری می‌پردازد که ذیل عنوان توسل به زور یا مخاصمات مسلحانه قرار نمی‌گیرند. ن.ک:

- www.ccdcoe.org/tallinn-manual.html (last visited: 25 July, 2019)

۵. لازم به ذکر است این اقدام ناتو به دلیل سفارشی‌بودن آن که باعث شده فقط دیدگاه‌های ناتو در قبال حملات سایبری به این راهنما تزریق شود، مورد انتقاد قرار گرفته است. ن.ک:

- Kristen Eichensehr, "Review of the Tallinn Manual on the International Law Applicable to Cyber Warfare", (Michael N. Schmitt ed. 2013), *American Journal of International Law*, Vol. 108, pp. 2014; See also: Terence Check, Book Review: "Analyzing the Effectiveness of the Tallinn Manual's Jus Ad Bellum Doctrine on Cyberconflict: A NATO-Centric Approach", *Cleveland State Law Review*, 2013.

اما این اقدام، اولین گام جدی جهت تدوین مقررات قراردادی و عرفی در حوزه حقوق مخاصمات سایبری به حساب می‌آید که اولاً نتیجه چندین سال تحقیق بیش از بیست محقق و متخصص برجسته در این حوزه تحت هدایت پروفسور *مایکل اشمیت* است. وی استاد کالج جنگ نیروی دریایی ایالات متحد امریکا (War College United States Naval) و استاد مدعو در تعدادی از دانشگاه‌های معتبر امریکا و اروپا است و حدود بیست سال در ارتش امریکا به‌عنوان قاضی در بخش‌های مربوط به حقوق بین‌الملل فعالیت داشت. باید او را ازجمله معدود افرادی دانست که در دو بُعد حقوقی و فنی دارای دانش قابل‌توجهی در این زمینه است؛ دوم اینکه حداقل دولت‌های عضو ناتو در روابط میان خود می‌توانند به آن استناد کنند؛ و سوم اینکه می‌تواند سنگ بنای اقدامات حقوقی بعدی باشد که در این خصوص انجام خواهد شد.

۶. گرچه اصول و قواعد کلی حقوق بین‌الملل حاکم بر مخاصمات مسلحانه می‌توانند پاسخگوی چالش‌های مطرح‌شده در جنگ سایبری باشند، به دلیل ماهیت متفاوت فضای سایبر، این پاسخ‌ها نمی‌توانند پاسخ‌های کامل و بدون نقصی باشند و در نتیجه عموماً منتهی به طرح پرسش‌های بیشتر یا پیچیده‌ترشدن مسائل خواهند شد.

تردید، اصلی‌ترین مانع پیش روی حقوق بین‌الملل، چالش‌های مرتبط با مفاهیم انتزاعی و ناملموس موجود در فضای سایبر (در مقایسه با فضای عینی) در رابطه با مکان و زمان حملات سایبری است. بنابراین برای بررسی این موانع باید لنز فنی را بر دیدگان حقوق بین‌الملل قرار داد و مسائل حقوقی را در تطبیق با مسائل فنی مربوط به فضای سایبر نظاره کرد. با توجه به نقش معیارهای «مکان» و «زمان» در حملات سایبری، می‌توان چالش‌های فراروی حقوق بین‌الملل در قبال این گونه حملات را در دو بخش چالش ادبی ـ فنی (مکان) و چالش حقوقی ـ تطبیقی (زمان) بحث کرد.

۱. چالش ادبی ـ فنی: کاستی در ادبیات حقوقی بین‌المللی مرتبط با مفاهیم تکنیکی حملات سایبری

«حملات سایبری» در بستر و از طریق «فضای سایبر» محقق می‌شوند. با وجود این و علی‌رغم مباحث بسیار درباره حملات سایبری، به علت ماهیت انتزاعی فضای سایبر، در ارتباط با مفاهیم مطرح‌شده در این محیط، اختلاف‌نظرها فراوان و ادبیات موجود کم‌رنگ است. بنابراین، مقدمه تعریف حملات سایبری، تعریف فضای سایبر و تفکیک تعاریف میان این فضا و فضای عینی و استخراج تفاوت‌ها و شباهت‌ها میان این دو فضا به منظور تطبیق راهکارهای حقوقی موجود بر فضای سایبر است.

۱-۱. تعریف فضای (قلمرو) سایبر در چارچوب ادبیات حقوق بین‌الملل

اصلی‌ترین چالش حقوق‌دان در ارتباط با حملات سایبری، تعریف فضای سایبر و ترسیم مرزهای این فضا در پرتو حقوق بین‌الملل است. «مرز»، رکن جدایی‌ناپذیر و تعیین‌کننده قلمرو کشور است و زمانی که صحبت از حملات سایبری در میان است باید حدود این مرز و همچنین قلمرو مجازی دولت‌ها در فضای سایبر نیز مشخص شود زیرا در فضای عینی، حمله یا تجاوز، زمانی معنا می‌یابد که قلمرو و مرزهای یک دولت، مورد حمله نیروهای نظامی دولتی دیگر قرار بگیرد.[۷] در حقیقت، تعریف فضای سایبری و مشخص‌کردن چارچوب‌های این فضا مطابق با معیارهای حقوق بین‌الملل، اقدام اول در مسیر تدوین حقوق بین‌الملل حاکم بر حملات سایبری است. بدیهی است اگر این گام به‌درستی برداشته نشود، ادامه مسیر نیز ناهموار و رسیدن به مقصد و مقصود، مشکل خواهد شد.[۸]

7. "How is the Term "Armed Conflict" Defined in International Humanitarian Law?", *International Committee of the Red Cross (ICRC) Opinion Paper*, March 2008, pp. 1-3.

۸. غالب نویسندگان مستقیماً وارد بررسی مقوله حمله سایبری شده و به بررسی ابعاد و آثار این حملات از منظر حقوق بین‌الملل عمومی، حقوق بین‌الملل بشردوستانه، حقوق بین‌الملل بشر و دیگر شاخه‌های مرتبط حقوق بین‌الملل پرداخته‌اند، بدون آنکه مشخصات حقوقی فضای سایبر را که حملات سایبری از طریق آن به وقوع می‌پیوندد مشخص کنند. بدون شک، تا زمانی‌که ابعاد و ویژگی‌های فضای سایبر از منظر حقوق بین‌الملل ترسیم نشود، بررسی آن از منظر این علم، به‌درستی ممکن نیست و چه‌بسا موضوع را پیچیده‌تر کند.

کنوانسیون حقوق و تکالیف دولت‌ها (مونته ویدئو)، چهار شرط اصلی (جمعیت دائمی/ قلمرو مشخص/ حکومت/ اهلیت برقراری ارتباط با دیگر دولت‌ها) را به‌عنوان شرایط حقوقی دولت برشمرده است.[۹] قلمرو مشخص یا بُعد مکانی، تعیین‌کننده محدوده اِعمال حاکمیت دولت است که حدود آن با مرز مشخص می‌شود. مفهوم قلمرو از این جهت حائز اهمیت است که تعیین‌کننده حوزه اِعمال قدرت دولت و در حقیقت، موجودیت حکومت است. روشن است که بدون وجود قلمرو، حکومتی وجود نخواهد داشت تا اعمال حاکمیت کند.[۱۰]

مرز در دنیای عینی و فیزیکی، خطی است که قلمرو سرزمینی یا فضای دریایی بین دو کشور را ترسیم می‌کند.[۱۱] ویژگی کلیدی مرز از منظر حقوق بین‌الملل این است که «باید به‌آسانی قابل شناسایی و به‌سختی قابل عبور باشد»،[۱۲] که این دو ویژگی در راستای اعمال حاکمیت دولت است.

اما در سوی مقابل به نظر می‌رسد که مرز در فضای سایبری مفهومی ندارد. فضای سایبر به‌عنوان «فضای جهانی در محیط اطلاعاتی متشکل از شبکه وابسته زیرساخت‌های فناوری اطلاعات، ازجمله اینترنت، شبکه‌های ارتباطات راه دور، سامانه‌های رایانه‌ای، پردازنده و کنترل تعبیه شده برای آن‌ها»[۱۳] تعریف شده است. بر اساس این تعریف، مهم‌ترین ویژگی فضای سایبر، وابستگی زیرساخت‌ها در فضای یکپارچه و جهانی (بدون مرز) است که یکی از خصوصیات دهکده جهانی[۱۴] و درست در نقطه مقابل فضای عینی است. به عبارت ساده‌تر، مرز در دنیای عینی، ملموس و قابل تشخیص ولی در فضای مجازی غیرملموس و غیرقابل تشخیص است و نمی‌توان همچون مرز سیاسی یا جغرافیایی برای آن حدود و ثغوری ترسیم کرد.

نظر به مراتب فوق، این پرسش مطرح می‌شود که آیا می‌توان قواعد حقوق بین‌الملل را در خصوص اعمال حاکمیت، به فضای سایبر نیز تعمیم داد؟ به نظر می‌رسد برای پاسخ به این پرسش باید به‌جای تمرکز بر شکل مرز در فضای سایبر، به میزان ارتباط آن با حوزه اقتدار و اعمال صلاحیت دولت توجه کرد. تعیین مرز در دنیای عینی به منظور تعیین قلمرو و حوزه اقتدار و اعمال صلاحیت دولت است. بنابراین در ارتباط با اقدامات خصمانه سایبری می‌توان این‌گونه تفسیر کرد

9. Convention on Rights and Duties of States (Montevideo Convention), 1933, art.1.

10. John P. Grant and J. Craig Barker, *Parry & Grant Encyclopædic Dictionary of International Law*, Third Edition, Oxford University Press, 2009, p. 599.

11. Martin Pratt, *Booklet of Applied Issues in International Land Boundary Delimitation / Demarcation Practices*, (A Seminar organized by the OSCE Borders Team in co-operation with the Lithuanian OSCE Chairmanship, 31 May to 1 June 2011 Vilnius, Lithuania), 2011, p. 8.

12. *British Guiana Boundary Case* (1899) 188 C.T.S. 76; *Alaska Boundary Arbitration* (1903) 15 R.I.A.A. 481 cited in: John P. Grant and J. Craig Barker, *Parry & Grant Encyclopædic Dictionary of International Law*, Third Edition, Oxford University Press, 2009, p. 69.

13. *Department of Defense Dictionary of Military and Associated* Terms (Joint Publication 1-02), 8 November 2010 (As Amended through 15 December, 2012), p. 74.

14. Marcel Danesi, *Dictionary of Media and Communications*, M.E. Sharpe, 2009, p. 135.

که هرگونه اقدام خصمانه سایبری که حوزه اقتدار و حاکمیت دولت را هدف قرار دهد،[۱۵] ممکن است در حکم تجاوز سایبری به مرز دولت تلقی شود. برای درک این تفسیر باید به این نکته توجه داشت که دولت‌ها در دنیای عینی حاکمیت خود را در سراسر قلمرو خود اعمال می‌کنند، اما در دنیای سایبر به دلیل نبود مرز مشخص و ملموس، اعمال حاکمیت از طریق سخت‌افزارهایی که در دنیای عینی واقع شده‌اند و دروازه‌های ورود و خروج داده‌ها بین دنیای سایبر و دنیای عینی به حساب می‌آیند می‌توانند با توجه به حساسیت آن‌ها برای نظم عمومی و منافع ملی کشور، مرز مجازی قلمداد شوند. برای مثال، در شدیدترین شکل اقدام خصمانه سایبری (یعنی حمله سایبری)، ازکارانداختن سرورهای نیروگاه هسته‌ای مستقر در قلمرو دولتی دیگر که می‌تواند منجر به ازکارافتادن خنک‌کننده‌های آن نیروگاه شود و در نهایت، انفجاری هسته‌ای را به دنبال داشته باشد، گونه‌ای تجاوز به مرز و قلمرو آن دولت به حساب می‌آید.[۱۶]

بنابراین می‌توان قلمرو سایبر را از منظر حقوق بین‌الملل این‌گونه تعریف کرد: فضای سایبر، ناملموس و بدون مرز است که قلمرو دولت‌ها در آن قابل ترسیم نیست. از آنجا که حضور دولت‌ها در فضای سایبر از طریق سخت‌افزارهای مستقر در قلمرو آن‌ها امکان‌پذیر می‌شود، می‌توان این سخت‌افزارها را مرز میان دنیای سایبر و دنیای عینی به حساب آورد که هرگونه تلاشی برای ورود غیرمجاز به شبکه ملی دیگر دولت‌ها از طریق این دروازه‌های ورودی، نقض اصل احترام به مرز و حاکمیت دولت‌ها به حساب می‌آید. چنین ورودی لزوماً به معنی حمله سایبری در حکم حمله مسلحانه نخواهد بود، همان‌گونه که نمی‌توان عبور شخص از مرز کشور به‌صورت غیرقانونی یا فعالیت‌های جاسوسی اتباع یک کشور در کشوری دیگر را حمله نظامی قلمداد کرد.[۱۷]

با عنایت به ترسیم قلمرو فضای سایبر از منظر حقوق بین‌الملل، گام بعدی تعریف حملات

---

۱۵. قلمرو مشخص (جغرافیا) و حکومت (اقتدار) دو شرط اصلی تشکیل دولت است که بالاتر مورد اشاره قرار گرفت. اقتدار یک دولت در تمام جغرافیای آن مستولی است به‌طوری‌که حاکمیت دولت شامل زیر زمین و آسمان نیز می‌شود و این موضوع در کنوانسیون‌های مختلف ازجمله کنوانسیون حقوق دریاها مصوب ۱۹۸۲ (بند ۲ ماده ۲) مورد توجه قرار گرفته است.

۱۶. برای تقویت این فرضیه می‌توان به قطعنامه تعریف تجاوز اشاره کرد. به‌موجب ماده ۱ قطعنامه پیش‌گفته، «تجاوز» به «به‌کارگیری نیروی نظامی توسط یک دولت علیه حاکمیت، تمامیت ارضی یا استقلال سیاسی دولتی دیگر یا هر رفتار دیگری که در تضاد با منشور ملل متحد باشد که در دامنه این تعریف می‌گنجد» گفته می‌شود. بنابراین در صورتی‌که حملات سایبری معادل حمله مسلحانه باشد و علیه حاکمیت، تمامیت ارضی یا استقلال سیاسی کشور دیگر، یا هر عمل دیگری که در تعارض با منشور ملل متحد باشد ازجمله تهدید به زور یا استفاده از آن علیه تمامیت ارضی یا استقلال سیاسی کشوری دیگر (بند ۴ ماده ۲ منشور)، می‌توان آن را تجاوز تلقی کرد.

۱۷. با استناد به رأی دیوان بین‌المللی دادگستری در قضیه فعالیت‌های نظامی و شبه‌نظامی در و علیه نیکاراگوئه (نیکاراگوئه علیه امریکا)، می‌توان «حملات سایبری شدید» را که معادل حمله نظامی است، «توسل به زور» و اقدامات با آثار تخریبی کمتر از حملات سایبری شدید را «مداخله در امور داخلی» دولت هدفِ مداخله توصیف کرد. ن.ک:
ICJ, *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America*), Judgment of 27 June, 1986, (Merits), p. 101, para. 191.

سایبری از منظر حقوق بین‌الملل حاکم بر مخاصمات مسلحانه در چارچوب تعریف ارائه‌شده از قلمرو فضای سایبر است.

۱-۲. تعریف حملات سایبری در چارچوب حقوق بین‌الملل

اولین و اصلی‌ترین چالش مفهومی پیش روی حقوق بین‌الملل در قبال حملات سایبری، نبود اجماع در خصوص ارائه تعریف مشخص از «حملات سایبری» و ترسیم چارچوب آن است. مشکل اصلی این است که هر دولتی بر اساس زیرساخت‌ها، توانایی‌ها و منافع خود، حملات سایبری را تعریف می‌کند. به عبارت دقیق‌تر، اصولاً (و نه لزوماً) دولت‌هایی که زیرساخت‌های‌شان وابستگی بیشتری به فضای سایبر دارد و بیشتر در معرض این‌گونه حملات قرار می‌گیرند،[۱۸] طبیعتاً تمایل دارند هرگونه حمله سایبری را تهدید و توسل به زور در چارچوب بند ۴ ماده ۲ منشور ملل متحد به حساب آورند تا بتوانند به حق دفاع مشروع متوسل شوند.[۱۹] برعکس، دولت‌هایی که زیرساخت‌های‌شان وابستگی کمتری به فضای سایبر دارد، تمایل به محدودکردن محدوده حملات سایبری دارند. بدیهی است «هر میزان یک کشور در فناوری پیشرفته‌تر باشد، آسیب‌پذیری بیشتری نسبت به حملات سایبری دارد. اگر شبکه‌های رایانه‌ای به «سامانه غالب»[۲۰] زیرساخت‌های شهروندی و نظامی تبدیل شوند، ناتوانی‌شان به معنای فلج‌شدن کشور خواهد بود».[۲۱] ایالات متحد امریکا که وابستگی اقتصادی و نظامی عظیمی به فناوری شبکه‌های اطلاعاتی دارد، مثال برجسته‌ای از یک کشور آسیب‌پذیر در قبال حملات سایبری است.[۲۲] قطعاً به علت همین حساسیت و دغدغه بوده که گستره وسیعی از تألیفات اندکی که حملات سایبری را از منظر حقوق بین‌الملل بررسی کرده‌اند، توسط اندیشمندان و متخصصان امریکایی و در نشریات این کشور و با استفاده از اسناد ایالات متحد امریکا منتشر شده تا از این طریق پاسخ نظامی امریکا به چنین حملات را قانونی و موجه جلوه دهند.[۲۳] ازاین‌رو به نظر می‌رسد تعاریف ارائه‌شده تا کنون بی‌طرفانه نبوده و اجماعی جهانی که تعادل میان منافع دولت‌ها و آثار و الزامات حقوقی را تأمین کند، هنوز حاصل نشده است.

این توضیح ضروری است که اقدامات صورت‌گرفته در فضای سایبر، می‌تواند در گروه‌بندی‌های

۱۸. آهنی امینه، محمد و فاطمه زهرا فتح‌اللهی؛ «حقوق بین‌الملل مدرن در مواجهه با جنگی پست‌مدرن (نبرد سایبری)»، *راهبرد*، سال بیست‌وسوم، شماره ۷۲، پاییز ۱۳۹۳، ص ۱۳۰.

۱۹. کیهانلو، فاطمه و وحید رضادوست؛ «حملات سایبر به مثابه توسل به زور در سیاق منشور سازمان ملل متحد»، *فصلنامه تحقیقات حقوقی*، شماره ۶۹، ۱۳۹۴، ص ۲۰۴.

20. Dominant system

21. Marco Roscini, "World Wide Warfare -Jus ad bellum and the Use of Cyber Force", *Max Planck Yearbook of United Nations Law*, Vol. 14, 2010, p. 87.

22. Matthew C. Waxman, "Cyber Attacks as "Force" under UN Charter Article 2(4)", *International Law Studies*, Vol. 87, 2011, p. 45.

23. Marco Roscini, *op.cit.*, p. 90.

مختلقی قرار گیرند که لزوماً تمامی‌شان حملات سایبری به حساب نمی‌آیند. به عبارت دیگر، گرچه واژگان مختلفی چون «جنگ سایبری»[۲۴] و «حمله سایبری»[۲۵] برای تعریف اقدامات خصمانه‌ای که در فضای سایبر به وقوع می‌پیوندند از سوی سیاست‌مداران، نظامیان و اصحاب رسانه به‌کار می‌رود، بسیاری از آن‌ها خارج از گستره مفهوم حملات مسلحانه در مفهوم اخص قرار می‌گیرند.[۲۶] بسیاری از حملات سایبری که در رسانه‌ها و در میان جدال لفظی سیاست‌مداران از آن‌ها به‌عنوان حملات سایبری یاد می‌شود (مانند حمله سایبری برای دزدی اطلاعات نظامی)، در اصل، حمله سایبری معادل با حمله مسلحانه نیست. تا کنون نیز چنین حملاتی در رویه دولت‌ها و قوانین موجود، حمله سایبری تلقی نشده‌اند.[۲۷] در راهنمای تالین ۲۰۱۳ اقداماتی از قبیل عملیات سایبری روانی و جاسوسی سایبری، حمله در مفهوم نظامی شناخته نشده است.[۲۸]

اولین چالش در ارائه تعریف از حملات سایبری این است که این حملات به گونه‌ای تعریف شوند که معادل با حملات مسلحانه در نظر گرفته شوند. تا به حال برای تعریف حملات سایبری از سه نظریه استفاده شده است: نظریه مبتنی بر اثر/ نتیجه، نظریه مبتنی بر هدف، و نظریه مبتنی بر وسیله.[۲۹] در میان آن‌ها نظریه مبتنی بر اثر/ نتیجه، بیشترین تطبیق را با حملات مسلحانه دارد و به نظر می‌رسد در میان علمای حقوق بین‌الملل نیز از مقبولیت بیشتری برخوردار است[۳۰] و با رویکرد حقوق بین‌الملل بشردوستانه، مطابقت بیشتری دارد. این موضوع از این جهت مهم است که رویکرد حقوق بین‌الملل بشردوستانه، نتیجه‌محور است؛ بدین معنا که اگر حملات سایبری آثار مخاصمه مسلحانه را داشته باشد، حمله مسلحانه شناخته خواهد شد زیرا مجموعه حقوق بین‌الملل بشردوستانه به دنبال حمایت از نظامیان و غیرنظامیان در زمان ظهور و بروز مخاصمات مسلحانه

24. Cyber war - Cyber warfare

25. Cyber attack

26. Laurie K. Blank, "International Law and Cyber Threats from Non-State Actors", *International Law Studies* (U.S. Naval War College), Vol. 89, 2013, p. 435.

27. Terry D. Gill and Paul A. L. Ducheine, "Anticipatory Self-Defense in the Cyber Context", *International Law Studies* (U.S. Naval War College), Vol. 89, 2013, p. 459.

28. *Tallinn Manual on the International Law Applicable to Cyber Warfare*, prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Center of Excellence, Cambridge University Press, 2013, Rule 30, second commentary.

29. *See*: Laurie K. Blank, *op. cit.*, 2013, p. 415; Nils Melzer, "Cyberwarfare and International Law", *UNIDIR Resources*, 2011, p. 5; Ian Brownlie, *International Law and the Use of Force by States*, Clarendon Press, 1963, p. 362; Karl Zemanek, "Armed Attack", in RüdigerWolfrum (ed.), *Max Planck Encyclopedia of Public International Law*, 2010, para. 21, cited in: Nils Melzer, *op.cit.*, 2011, p. 13.

برای ملاحظه چکیده این سه نظریه، ن.ک: علیرضا رنجبر؛ «ظرفیت‌سنجی بند ۴ ماده ۲ منشور ملل متحد در قبال حملات سایبری از نظرگاه حقوق بین‌الملل»، مجموعه مقالات همایش هفتادمین سالگرد تأسیس سازمان ملل متحد (۱۳۹۴: انجمن ایرانی مطالعات سازمان ملل متحد و دانشکده روابط بین‌الملل وزارت امور خارجه)، اداره نشر وزارت امور خارجه، ۱۳۹۶، صص ۴۲۹ – ۴۲۵.

۳۰. رنجبر؛ *همان*، صص ۴۲۶ – ۴۲۵.

است و به چگونگی رخداد مخاصمه کاری ندارد. در تقویت این نظر می‌توان به شرط *مارتنز* نیز استناد کرد که به‌موجب آن، در جایی که موافقت‌نامه بین‌المللی وجود ندارد، نظامیان و غیرنظامیان همچنان زیر چتر حمایتی اصول حقوق بین‌الملل که ریشه در عرف مقرر، اصل انسانیت و آنچه از خرد جمعی نشأت می‌گیرد قرار خواهند گرفت.[۳۱] بنابراین گرچه حملات سایبری در کنوانسیون‌های چهارگانه ژنو و پروتکل‌های الحاقی آن به‌عنوان مخاصمات مسلحانه شناسایی نشده‌اند، اگر حملات سایبری از حیث آثار با حملات فیزیکی برابری و همانندی کنند می‌توانند از منظر حقوق بین‌الملل بشردوستانه، بخشی از مخاصمات مسلحانه تلقی شوند.[۳۲] در فرایند رسیدگی در دیوان بین‌المللی یوگسلاوی سابق در پرونده *تادیچ* نیز دادستان دیوان استدلال کرد «آنچه در مخاصمه مسلحانه بین‌المللی غیرانسانی است نمی‌تواند در مخاصمه مسلحانه داخلی، انسانی باشد».[۳۳] این دیدگاه می‌تواند تقویت‌کننده نظریه مبتنی بر اثر/ نتیجه در خصوص حملات سایبری باشد.

در ارائه تعریف حقوقی از حملات سایبری به نظر می‌رسد تعریف ارائه‌شده از حملات سایبری در راهنمای *تالین* که رویکرد اثر/ نتیجه محور را دنبال می‌کند، ازجمله بهترین تعاریفی است که با هدف حقوق بین‌الملل بشردوستانه سنخیت دارد[۳۴] و می‌تواند مرجع محسوب شود. به‌موجب راهنمای پیش‌گفته، حمله سایبری عبارت است از «عملیات در محیط سایبری، خواه تهاجمی یا دفاعی که معقولانه این انتظار از آن می‌رود که منتهی به جرح یا مرگ افراد یا ورود خسارت به اشیاء یا تخریب آن‌ها شود».[۳۵] همچنین در تعریف حقوقی باید به این نکته نیز توجه داشت که حملات سایبری در «ماهیت» و «اثر» باید با حملات مسلحانه مقایسه شود. به عبارت دیگر، برای تلقی حملات سایبری به‌عنوان حملات مسلحانه، همراهی دو شرط لازم است: اول، حملات سایبری باید در «ماهیت» به شکلی باشند که به‌موجب فصل هفتم منشور ملل متحد، تهدیدی علیه صلح و امنیت بین‌المللی تلقی شود یا در چارچوب دفاع مشروع، البته با رعایت شرایط مندرج

31. Additional Protocol I to the Geneva Convention of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, Art. 1(2), 12 December, 1977, 1125 U.N.T.S. 3

32. Djamchid Momtaz, L'évolution du droit international humanitaire applicable à la conduite des hostilities, in: Conduct of Hostilities: the Practice, the Law and the Future (37th Round Table on Current Issues of International Humanitarian Law), International Institute of Humanitarian Law, 2015, p. 50.

33. ICTY, *Prosecutor v. Dusko Tadic*, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 1995, para. 119.

۳۴. از این جهت می‌توان به این تعریف استناد کرد که هم افراد و هم اموال را تحت پوشش قرار داده و به آثار حمله سایبری توجه کرده است، در حالی که سایر تعاریف ارائه‌شده چنین جامعیتی ندارند. برای مثال، یکی از تعاریف ارائه‌شده به شرحی که در ادامه خواهد آمد، افراد را خارج از حملات سایبری قرار داده است: «منظور از «حملات سایبری»، تلاش برای عوض‌کردن، مختل‌کردن، کم‌کردن یا نابودکردن سامانه‌ها یا شبکه‌ها یا اطلاعات یا برنامه‌های موجود بر روی آن‌هاست». ن.ک:
- Matthew C. Waxman (1), *op.cit.*, p. 43.

35. *Tallinn Manual on the International Law Applicable to Cyber Warfare*, prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Center of Excellence, Cambridge University Press, 2013, Rule 30.

در ماده ۵۱ منشور ملل متحد و همچنین رعایت شروط عُرفی ضرورت و تناسب، منافع اساسی دولت را تهدید کند[۳۶] و دوم باید اثر مخرب فیزیکی یا اثری مشابه آن داشته باشد تا بتوان آن را جلوه‌ای از جنگ‌های مدرن و یکی از اشکال نقض بند ۴ ماده ۲ منشور قلمداد کرد[۳۷] که این شرط در تعریف راهنمای *تالین* از حملات سایبری مورد توجه قرار گرفته است.

برای ارائه تعریفی که ابعاد فنی حملات سایبری را در کنار ابعاد حقوقی پوشش دهد می‌توان نیم‌نگاهی به طبقه‌بندی وزارت دفاع امریکا داشت. نهاد مذکور، اقدامات سایبری را در چهار دسته «عملیات شبکه رایانه‌ای»،[۳۸] «دفاع شبکه رایانه‌ای»،[۳۹] «عملیات رایانه‌ای تهاجمی»[۴۰] و «توسل به شبکه رایانه‌ای»[۴۱] طبقه‌بندی کرده است:[۴۲]

عملیات شبکه رایانه‌ای: اقداماتی است که امکان جابه‌جایی داده‌ها از یک مکان به مکان دیگر را میسر می‌کند. این عملیات شامل پیکربندی، عملکرد، نظارت و ارزیابی تمامی سخت‌افزارها ـ سرورها و تلفن‌ها ـ نرم‌افزارها ـ سامانه‌های عامل و برنامه‌ها ـ و شبکه‌ها ـ متصل به سیم یا بی‌سیم ـ است.

دفاع شبکه رایانه‌ای: اقداماتی که برای دفاع از شبکه و مهم‌تر از همه، دارایی‌های اطلاعاتی و اطلاعات طبقه‌بندی‌شده در شبکه صورت می‌گیرد. این اقدامات نه‌تنها شامل استفاده از فناوری‌هایی مانند فایروال‌ها (دیوارهای آتشین) و سامانه‌های تشخیص نفوذ، بلکه شامل سازماندهی مفاهیمی مانند تقسیم یا بخش‌کردن شبکه‌ها نیز می‌شود. تمرکز مدافعان سایبری بر این است که از محرمانگی، یکپارچگی و در دسترس‌بودن اطلاعات موجود در یک سازمان اطمینان حاصل کنند.

عملیات رایانه‌ای تهاجمی: استفاده از نرم‌افزار، سخت‌افزار و شبکه‌ها برای رهاکردن نرم‌افزاری (مخرب) با اثرگذاری مشخص در برابر دشمن ـ معمولاً به منظور اختلال، تخریب یا ازبین‌بردن توانایی دشمن. از آنجا که ممکن است داده‌ها قبل از رسیدن به هدف مورد نظر، نیاز به حرکت در «مسیرهای بین مبدأ و مقصد بسته اطلاعاتی» چندگانه داشته باشند، هدف‌گیری [در این عملیات] فرایند بسیار دشواری است. در طول مسیر، دشمنان فرصت رصد، رهگیری یا تغییر مسیر را دارند.

---

۳۶. حق دفاع مشروع به‌عنوان استثنای پذیرفته‌شده در منشور، زمانی محقق می‌شود که برای دولت شرایطی ایجاد شود که دفاع از آسیب جبران‌ناپذیر به حقوق اساسی آن، جز از راه توسل به زور امکان‌پذیر نباشد. ن.ک:
- Sindhu Vijaya Kumar, "The Essence of Self Defense under Article 51 of UN Charter - a Privilege or Priority", *Acta Universitatis Danubius*, Vol.VII, no.1/2011, p. 38.

۳۷. رنجبر؛ *همان*، ص ۴۴۶.

38. Computer network operations (CNO)

39. Computer network defense (CND)

40. Offensive computer operations (OCO)

41. Computer network exploitation (CNE)

42. Robert J. Butler, "Cyber War: Definitions, Deterrence, and Foreign Policy (Testimony before the House Foreign Affairs Committee)", *Center for a New American Security*, 2015, p. 2.

توسل به شبکه رایانه‌ای: استفاده از سخت‌افزارها، نرم‌افزارها و شبکه‌ها برای درک بهتر دشمن از طریق جمع‌آوری و تجزیه و تحلیل داده‌ها.

طبقه‌بندی وزارت دفاع امریکا از این جهت حائز اهمیت است که از لحاظ فنی بین اقسام مختلف اقدامات خصمانه سایبری قائل به تفکیک شده است. همان‌طور که مشخص است، از میان تعاریف ارائه‌شده، تنها «عملیات رایانه‌ای تهاجمی» به دلیل ماهیت مخرب خود و قدرت اثرگذاری منفی بر فعالیت‌های طرف دیگر، ظرفیت تحقق حملات سایبری در مفهوم حقوق توسل به زور را دارد و سایر تعاریف به دلیل ماهیت غیرمرتبط خود با حملات سایبری نمی‌توانند در حوزه این حملات قرار بگیرند.

با ترکیب دو معیار فنی و حقوقی و استخراج معیار مشترک می‌توان آن دسته از اقداماتی را که از لحاظ فنی در مرحله عملیات رایانه‌ای تهاجمی قرار می‌گیرند و از لحاظ حقوقی آثاری همانند حمله نظامی مسلحانه در دنیای عینی به جا می‌گذارند (رویکرد نتیجه‌محور)[۴۳] حمله مسلحانه سایبری به حساب آورد. اقدامات انجام‌شده خارج از این چارچوب، حمله مسلحانه به حساب نمی‌آید بلکه بسته به میزان و شدت آن می‌توان حملات ضعیف‌تر را مداخله سایبری، جاسوسی، جمع‌آوری اطلاعات، اختلال در ارتباطات، اختلال در تبلیغات سیاسی و سایر اقدامات مداخله‌جویانه که به حد حمله مسلحانه نمی‌رسند تلقی کرد.[۴۴]

۲. چالش حقوقی ـ تطبیقی: ضعف در برقراری ارتباط بین مفاهیم حقوقی دنیای عینی و دنیای سایبری

به علت مسائل فنی مربوط به حملات سایبری، تطبیق دنیای سایبری با دنیای عینی، امری پیچیده است. از این منظر، دو چالش اصلی «تعامل و تقابل حملات سایبری با حملات عینی» و «شناسایی منشأ حقیقی حمله در حملات سایبری و تعارض آن با فوریت» پیش روی حقوق بین‌الملل قرار دارند.

۲-۱. تعامل و تقابل حملات سایبری با حملات عینی

ظهور فضای سایبر و وقوع حملات سایبری، چالش مفهومی مهمی را در رابطه بین حملات سایبری و حملات عینی در عالم حقوق بین‌الملل مطرح کرده است.

شکل غالب واکنش به حمله عینی، توسل به دفاع مشروع مندرج در ماده ۵۱ منشور ملل متحد است. از سوی دیگر، اولین و محتمل‌ترین گزینه برای پاسخ به حملات سایبری، واکنش به آن در

۴۳. برای مثال، هر دولتی در فضای سایبر، زیرساخت‌هایی دارد که از طریق آن اعمال حاکمیت می‌کند یا این زیرساخت‌ها پیوند ناگسستنی با وظایف حاکمیتی دولت‌ها دارند که تداخل در کارکرد آن‌ها منتهی به تداخل کارکرد دولت‌ها می‌شود. ازکارانداختن این زیرساخت‌ها می‌تواند اسباب توسل به حق دفاع مشروع را فراهم کند.

44. Laurie K. Blank, *op.cit.*, p. 415.

قالب اقدام سایبری است که این دو باید در چارچوب مفاد منشور ملل متحد و اصول حاکم بر حقوق توسل به زور صورت پذیرد. اما دو فرض دیگر نیز در اینجا قابل طرح است: فرض اول، توسل به دفاع و واکنش سایبری در برابر حملات عینی است و فرض دوم، توسل به دفاع مشروع عینی در قبال حملات سایبری است.

در خصوص فرض اول، این پرسش مطرح است که آیا می‌توان در قالب دفاع سایبری به حمله عینی پاسخ داد؟ پاسخ به این پرسش از این جهت قابل تأمل است که در حال حاضر، بخش‌های نظامی بسیاری از کشورها (ازجمله استرالیا، اسرائیل، امریکا، ایتالیا، آلمان، برزیل، بریتانیا و چین) به‌صورت رسمی و غیررسمی، واحدهای جنگ / دفاع سایبری راه‌انداخته‌اند تا در برابر تهدیدات و حملات سایبری و حتی حملات عینی سایر دولت‌ها با استفاده از فضای سایبر واکنش نشان دهند.[۴۵] حتی ارتش آلمان در کنار نیروی زمینی، نیروی هوایی و نیروی دریایی، واحد «فرماندهی سایبر و اطلاعات فضایی»[۴۶] راه‌انداخته است[۴۷] و می‌توان گفت در آینده نزدیک، دیگر دولت‌ها نیز اقدامات کم‌وبیش مشابهی انجام خواهند داد.[۴۸] حال این پرسش مطرح می‌شود که آیا می‌توان در قبال حملات عینی به دفاع سایبری متوسل شد؟

برای پاسخ به پرسش بالا ابتدا باید شرایط تحقق دفاع مشروع را در مواجهه با حمله سایبری بررسی کرد. شرایط تحقق دفاع مشروع به دو دسته شرایط عرفی و شرایط معاهده‌ای یا مدون تقسیم می‌شوند. از منظر حقوق بین‌الملل عرفی، رعایت شروط «ضرورت»، «تناسب» و «فوریت» برای تحقق دفاع مشروع ضروری است.[۴۹] شرایط استناد به حق دفاع مشروع از منظر منشور ملل متحد (شرایط مدون) نیز شامل «وقوع حمله مسلحانه»، «وجود تهدید فوری و گسترده»، «رعایت تناسب میان دفاع و حمله» و «گزارش به شورای امنیت و سازمان‌های منطقه‌ای مرتبط» می‌شود.[۵۰]

---

45. Marco Roscini, *op.cit*., pp. 97-98.

46. Cyber and Information Space Command (CIR)

47. www.dw.com/en/german-army-launches-new-cyber-command/a-38246517 (last visited on: 25 July 2019).

۴۸. ایران نیز در زمره کشورهایی است که به اهمیت فضای سایبر بخصوص در ابعاد نظامی آن پی برده است. «قرارگاه پدافند سایبری ایران» به‌عنوان زیرمجموعه‌ای از «سازمان پدافند غیرعامل کشور»، وظیفه «مصون‌سازی و پایدارسازی سرمایه‌های سایبری کشور از طریق پایش و تشخیص تهدیدات، کشف، مدیریت و کنترل آسیب‌پذیری‌ها، اعلام هشدارهای لازم، امن‌سازی، تدوین و انتشار نظامات (ملاحظات، مقررات، الزامات و اصول) پدافندی، آموزش و نهادینه‌سازی پدافند سایبری، مدیریت صحنه عملیات پدافند سایبری و دفاع حقوقی در برابر تهدیدات و حمله دشمن» را عهده‌دار است. (بیانیه رسالت پدافند سایبری کشور). برای اطلاعات بیشتر در خصوص این سازمان، ن.ک: https://www.papsa.ir (last visited: 25 July, 2019)

49. *Nicaragua v. United States*, 1986, p. 94, para.176.

۵۰. ماده ۵۱ منشور ملل متحد بیان می‌دارد: «در صورت وقوع حمله مسلحانه علیه یک عضو ملل متحد، تا زمانی که شورای امنیت، اقدام لازم برای حفظ صلح و امنیت بین‌المللی را به عمل آورد، هیچ‌یک از مقررات این منشور به حق ذاتی دفاع از خود، خواه فردی یا دسته‌جمعی لطمه‌ای وارد نخواهد کرد. اعضا باید اقداماتی را که در اعمال این حق دفاع از خود به عمل می‌آورند

در صورت جمع‌شدن این شرایط، کشوری که مورد حمله مسلحانه واقع شده می‌تواند به دفاع مشروع متوسل شود. لذا اگر دفاع سایبری منطبق با شرایطی باشد که برای دفاع مشروع برشمرده شد، قاعدتاً منعی در خصوص تلقی این اقدامات به‌عنوان دفاع مشروع در برابر حملات مسلحانه عینی وجود ندارد.

حال به‌فرض، دولتی در فضای سایبری یا فیزیکی مورد تجاوز گسترده قرار گرفته و تنها وسیله دفاعی‌اش مقابله در فضای سایبری علیه کشور متجاوز است ولی نیروی تخریب‌کننده مورد استفاده در فضای سایبر، بسیار بیشتر از تجاوز فیزیکی است که به آن تحمیل شده است مانند حمله سایبری در قالب دفاع مشروع به نیروگاه اتمی که به انفجار هسته‌ای یا ازکارانداختن زیرساخت‌های کشور متجاوز و فلج‌شدن آن کشور منتهی شود (مثل اتفاقی که برای استونی افتاد). در اینجا آیا دولتی که مورد تجاوز قرار گرفته و اقداماتی فراتر از حمله متناسب علیه دولت متجاوز انجام داده می‌تواند دفاع خود را بر مبنای شروط عرفی پیش‌گفته، متناسب ارزیابی کند؟

قطعاً به‌سادگی نمی‌توان به این پرسش پاسخ داد زیرا از یک سو بقای کشور و استمرار حاکمیت آن در میان است و از سوی دیگر چنین واکنشی برخلاف اصل تناسب در توسل به دفاع مشروع است. دیوان بین‌المللی دادگستری در نظر مشورتی «قانونی‌بودن تهدید یا استفاده از سلاح‌های هسته‌ای»، در خصوص متوسل‌شدن به حمله هسته‌ای در مقام توسل به دفاع مشروع، پا را از شرایط عرفی و معاهده‌ای مربوط به دفاع مشروع فراتر گذاشت و بیان داشت: «دیوان نمی‌تواند به‌طور قطعی تصدیق کند که تهدید یا استفاده از سلاح‌های هسته‌ای در موارد شدید دفاع مشروع که در آن بقای کشور در معرض خطر خواهد بود، قانونی یا غیرقانونی است».[۵۱] البته این موضع دیوان با نسبت ۷ رأی موافق به ۷ رأی مخالف قضات دیوان با رأی تعیین‌کننده رئیس دیوان، به‌شدت مورد انتقاد حقوق‌دانان قرار گرفت.[۵۲]

فوراً به شورای امنیت گزارش دهند. این اقدامات به‌هیچ‌وجه در اختیار و مسئولیتی که شورای امنیت بر طبق این منشور دارد و به‌موجب آن برای حفظ و اعاده صلح و امنیت بین‌المللی و در هر موقع که ضروری تشخیص دهد اقدام لازم به عمل خواهد آورد، تأثیری نخواهد داشت».

51. ICJ, *Advisory Opinion of 8 July 1996, Legality of the Use by a State of Nuclear Weapons in Armed Conflict*, 1996, p. 263, para. 97.

52. Christopher Hubbard, "A Critique of the Advisory Opinion of the International Court of Justice on the Legality of the Threat or Use of Nuclear Weapons", 8 July, 1996: The Nuclear Weapons Case, B.A. Thesis, Edith Cowan University, 1997.

به تعبیر یکی از نویسندگان، دیوان در رأی مذکور، دو رویکرد متعارض و مبهم را در پیش گرفته است؛ ابتدا تهدید یا به‌کارگیری سلاح‌های هسته‌ای را به‌طور کلی مخالف با حقوق بین‌الملل حاکم بر مخاصمات مسلحانه، و به‌طور خاص، مخالف با اصول و قواعد حقوق بین‌الملل بشردوستانه تلقی می‌کند و در جای دیگر در خصوص ممنوعیت به‌کارگیری این سلاح‌ها در مقام دفاع مشروع، زمانی که بقای یک کشور در خطر است ابراز تردید می‌نماید. ن.ک:

Devesh Awmee, "Nuclear Weapons before the International Court of Justice: A Critique of the Marshall Islands v United Kingdom Decision", *Victoria University of Wellington Law Review*, Vol. 49, 2008, p. 67.

طبیعتاً این نوع رویکرد دیوان بین‌المللی دادگستری مورد استقبال کشورهایی ازجمله امریکا است که سلاح‌های هسته‌ای دارند. ن.ک:

در روایتی دیگر از فرض اخیر، اگر کشوری مورد حمله مسلحانه سایبری یا فیزیکی قرار گیرد و شدت حمله آن‌چنان نباشد که بقا و حیات کشور را به خطر اندازد اما کشور مدافع، امکانات و توانایی‌های لازم را برای رویارویی فیزیکی با آن حمله نداشته باشد و اگر با حمله سایبری به تجاوز پاسخ دهد، آثار مخرب‌تر و نامتناسب‌تری در قیاس با حمله تجاوزکارانه به بار می‌آورد، آیا کشور مورد تجاوز می‌تواند به دفاع مشروع در فضای سایبر متوسل شود؟ برخلاف فرض قبلی، پاسخ به این پرسش روشن‌تر است زیرا همان‌طور که در فرض قبلی بیان شد، درباره توسل به دفاع مشروع در فضای سایبر که نامتناسب با آثار تجاوز فیزیکی باشد، حتی در صورت وجود خطر برای بقای کشور و استمرار حاکمیت آن، حقوق‌دانان اتفاق‌نظر ندارند. بنابراین بدیهی است اگر از یک سو بقا و حیات کشور به خطر نیفتد (عدم رعایت شرط ضرورت) و از سوی دیگر، پاسخ به حمله، بزرگ‌تر از خود حمله باشد (عدم رعایت شرط تناسب)، چنین پاسخی در چارچوب حقوق بین‌الملل غیرقابل توجیه است.

در فرض دوم، توسل به دفاع غیرسایبری در قبال حمله سایبری مطرح است. روشن است که این روش بیشتر می‌تواند از سوی دولت‌هایی مورد استفاده قرار بگیرد که به علت محدودیت امکانات و فناوری‌های لازم نمی‌توانند به حملات سایبری در محیط سایبر پاسخ بدهند. بنابراین، زمانی که دولتی قربانی حملات سایبری می‌شود، تنها محدود و مقیّد به دفاع مشروع سایبری نیست بلکه می‌تواند به‌عنوان پاسخ به حملات سایبری، به حملات نظامی دست یازد.[۵۳] البته برای توسل به دفاع مشروع عینی در قبال حملات سایبری، کسب اطمینان از منشأ حقیقی حملات سایبری ضروری است.[۵۴]

گرچه این فرضیه برای اولین بار از سوی سران روسیه و امریکا مطرح شد،[۵۵] به نظر می‌رسد برای اولین بار و به‌صورت جدی و در قالب یک سند، از سوی ناتو در نشست ۲۰۱۴ *ولز* و در اعلامیه نهایی این نشست که به «اعلامیه ولز»[۵۶] معروف شد، مورد توجه قرار گرفت. در بخشی از این اعلامیه، ناتو با توجه به گسترش تهدیدات و حملات سایبری، سیاست دفاعی خود را در این زمینه یا آنچه به‌عنوان «دفاع سایبری» از آن یاد می‌کند، هسته وظیفه دفاع جمعی این سازمان تلقی می‌کند و امکان اتخاذ تصمیم توسط شورای آتلانتیک شمالی در قالب ماده ۵ ناتو[۵۷] را در

Robert F. Turner, "Nuclear Weapons and the World Court: The ICJ's Advisory Opinion and Its Significance for U.S. Strategic Doctrine", *International Law Studies*, in: *The Law of Military Operations: Liber Amicorum, Professor Jack Grunawalt*, Michael N., Schmitt (ed.), 1998.

53. Laurie K. Blank, *op.cit.*, p. 418.

۵۴. در بخش بعدی در این خصوص توضیحات بیشتری ارائه شده است.

55. Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", *Berkeley Journal of International Law*, Vol. 27:1, 2009, pp. 216-217.

56. Wales Declaration, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, 2014.

۵۷. این ماده مقرر می‌دارد: «دولت‌ها توافق دارند که حمله‌ای مسلحانه علیه یک یا تعدادی از آن‌ها در اروپا و امریکای شمالی، به معنای حمله علیه تمام آن‌ها تلقی خواهد شد و در نتیجه موافقت می‌نمایند در صورتی که چنین حمله‌ای به وقوع پیوست، هر یک از آن‌ها، در راستای عمل به حق دفاع مشروع انفرادی یا جمعی خود بر اساس ماده ۵۱ منشور ملل متحد، دولت یا دولت‌های

قبال حمله سایبری محتمل به حساب می‌آورد.[۵۸]

از تجمیع بند ۷۲ اعلامیه *ولز* و ماده ۵ ناتو این نتیجه حاصل می‌شود که در صورت وقوع حمله سایبری از جنس حملات مسلحانه علیه دولت‌های عضو ناتو، سایر دولت‌های عضو می‌توانند مطابق ماده ۵۱ منشور ملل متحد و در قالب دفاع مشروع به اقدامات مقتضی ازجمله اقدام نظامی تحت عنوان دفاع مشروع جمعی متوسل شوند. البته در بخش پایانی ماده ۵ ناتو مقرر شده است که «هرگونه حمله مسلحانه و اقدامات اتخاذشدهٔ ناشی از آن، فوراً به شورای امنیت گزارش خواهد شد. این اقدامات، زمانی که شورای امنیت، اقدامات لازم را جهت بازگرداندن و برقراری صلح و امنیت بین‌المللی اتخاذ نماید، متوقف می‌شود».[۵۹]

استدلال ناتو از این جهت حائز اهمیت است که در حال حاضر سازمان‌ها و پیمان‌های منطقه‌ای دیگری ازجمله اتحادیه آفریقا، اتحادیه ملل امریکای جنوبی[۶۰] و سازمان همکاری‌های شانگهای وجود دارند که در اسناد مؤسس آن‌ها، به‌صورت مستقیم یا غیرمستقیم، حق دفاع مشروعِ اعضا به‌صورت انفرادی یا جمعی مورد اشاره قرار گرفته است.

۲-۲. «شناسایی منشأ حقیقی حمله» در حملات سایبری و تعارض آن با «فوریت»

با توجه به اینکه یکی از ویژگی‌های اساسی جنگ‌های سایبری، گمنام‌بودن و گمنام‌ماندن است، شناسایی منبع حملات سایبری به دلیل مقابله با آن‌ها اهمیت دوچندانی دارد. در حملات سایبری باید به این مهم توجه داشت که اقدام به حمله از رایانه‌ای مستقر در یک کشور، حاکی از آن نیست که حمله به‌طور قطع از جانب همان کشور صورت گرفته است،[۶۱] بلکه ممکن است منشأ حمله از کشورهای دیگر، حتی بیش از صد کشور عبور کرده و قابل ردگیری باشد.[۶۲] برای نمونه، ادعا شده است که مسیر حمله سایبری ۲۰۰۷ به استونی از کشورهایی چون ایالات متحد امریکا، مصر، پرو و روسیه عبور کرده بود.[۶۳] ازاین‌رو نباید به‌طور قطع پنداشت که کشور محل استقرار سخت‌افزار رایانه‌ای که از آن حمله صورت گرفته است، یقیناً آغازکننده حمله یا مطلع از این اقدام بوده است. بنابراین،

مورد حمله را از طریق اقدامات آنی، هرآنچه ضروری می‌نماید، به‌صورت انفرادی یا با همراهی دیگر دولت‌ها یاری رساند تا امنیت را در منطقه آتلانتیک شمالی بازگردانده و برقرار نماید (نمایند) که می‌تواند شامل استفاده از نیروهای مسلح نیز باشد ...».

58. Wales Summit Declaration, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, September 5, 2014, para.72.

59. North Atlantic Treaty Organization, 1949, Art. 5.

۶۰. برای کسب اطلاعات بیشتر در خصوص اتحادیه ملل امریکای جنوبی، ن.ک: علیرضا رنجبر؛ «نقش اتحادیه ملل امریکای جنوبی در حفظ صلح و امنیت بین‌المللی و منطقه‌ای»، *مجله پژوهش‌های حقوقی*، شماره ۲۸، نیمسال دوم، ۱۳۹۴.

61. Marco Roscini, *op.cit.*, p. 96.

62. Laurie K. Blank, *op.cit.*, pp. 416-417.

63. Marco Roscini, *op.cit.*, pp. 96-97.

پیش از متوسل‌شدن به هرگونه اقدام خصمانه، کشور قربانی باید از منشأ بروز حملات اطمینان یابد.[۶۴] البته تعیین منشأ حمله سایبری الزاماً همیشه دشوار نیست. بخصوص با پیشرفت فناوری یا همراه‌شدن حملات سایبری با حملات عینی، امکان شناسایی منبع حمله سایبری در بیشتر موارد امکان‌پذیر است.[۶۵] برای نمونه (همراهی حملات سایبری با حملات عینی) می‌توان به حمله هوایی اسرائیل به تأسیسات هسته‌ای الکبیر (الخبیر) در شمال سوریه اشاره کرد که با نام «عملیات باغستان»[۶۶] در سپتامبر ۲۰۰۷ به وقوع پیوست. در این حمله هوایی، پیش از آنکه هواپیماهای اسرائیلی اقدام به بمباران تأسیسات هسته‌ای سوریه کنند، ارتش اسرائیل سامانه دفاع هوایی سوریه را از طریق جنگ الکترونیک مختل و زمینه حمله هوایی موفقِ بمب‌افکن‌هایِ اسرائیلی را فراهم کرد.[۶۷]

شناسایی و ردگیری عاملان حملات سایبری در دنیای سایبر و به عبارت دیگر، تعیین منشأ حملات سایبری که ارتباط مستقیم با بحث مسئولیت بین‌المللی دولت‌ها دارد، فرایندی بسیار سخت، پیچیده و کاملاً متفاوت با حملات عینی است.[۶۸] این چالش از آنجا نشأت می‌گیرد که به دلیل ماهیت زیرساخت‌های اطلاعاتی، اغلب نمی‌توان به‌طور دقیق مشخص کرد که حملات سایبری از کجا آغاز و هدایت شده است. این امر از لحاظ حقوقی ارتباط بین حمله و مسئول اصلی را مشکل می‌کند.[۶۹] به‌علاوه، زمانی که پای بازیگران غیر دولت و اشخاص (هکرها که در ظرفیت شخصی خود اقدام می‌کنند) نیز به حملات سایبری کشیده شود، تشخیص منشأ حملات سایبری و انتساب حملات به آن‌ها بیش از پیش سخت خواهد شد.

بنابراین، بحث مسئولیت بین‌المللی مجریان حملات سایبری (دولت‌ها، بازیگران غیر دولت و اشخاص) را نیز باید مورد توجه قرار داد:

در خصوص *دولت‌ها* باید به این موضوع اشاره کرد که در حال حاضر کشورهای مختلفی به‌صورت رسمی و غیررسمی واحدهای جنگ سایبری خود را تشکیل داده‌اند. به هر حال باید توجه داشت این واحدها چه رسمی و چه غیررسمی، «ارگان قانونی دولت»[۷۰] به حساب می‌آیند و مطابق با اصل «وحدت دولت»،[۷۱] مسئولیت اقدامات آن‌ها با دولت‌ها است.[۷۲] همچنین «گرچه هکرها

64. Laurie K. Blank, *op.cit*., pp. 416-417.
65. Marco Roscini, *op.cit*., p. 97.
66. Operation Orchard
67. Terry D. Gill and Paul A. L. Ducheine, *op.cit*., pp. 461-462.
68. *Ibid*., pp. 467-468.
69. Richard A. Clarke, Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It*, Harper Collins, New York, 2010, (proposing a doctrine of *cyber equivalency)* as cited in: Matthew C. Waxman, *op.cit*., 2011, p. 50.
70. De jure organs of a state
71. Unity of State
۷۲. ماده ۴ طرح مسئولیت دولت بیان داشته است: «۱) رفتار هر ارگان دولتی به‌موجب حقوق بین‌الملل، فعل آن دولت تلقی می‌شود فارغ از اینکه آن ارگان کارکرد تقنینی، قضایی، اجرایی یا کارکردی دیگر داشته باشد و اعم از اینکه ارگان مذکور در

ارگان قانونی دولت نیستند، افراد و شرکت‌هایی که از سوی دولت‌ها برای انجام حمله سایبری به خدمت گرفته می‌شوند قابل انتساب به دولت‌ها هستند».[۷۳] ماده ۸ طرح مسئولیت بین‌المللی دولت در این خصوص به‌روشنی راه‌گشا است: «رفتار شخص یا گروهی از اشخاص در صورتی‌که در واقع به دستور، تحت هدایت یا کنترل دولت عمل کنند به‌موجب حقوق بین‌الملل، فعل دولت تلقی می‌شود». حتی تحریک گروهی از اشخاص به انجام حملات سایبری از سوی دولت، در صورتی‌که اقدامات این گروه به‌طور کلی مورد حمایت دولت قرار بگیرد، فعل دولت تلقی خواهد شد.[۷۴]

در پرونده کارکنان دیپلماتیک و کنسولی امریکا در تهران، دیوان بین‌المللی دادگستری به‌صراحت بیان می‌دارد، گرچه حمله اولیه به سفارت امریکا در تهران به دولت ایران قابل انتساب نبود، پشتیبانی بعدی مقامات ایرانی و تصمیم به استمرار اشغال سفارت، عمل اشغال و بازداشت را به دولت ایران منتقل کرد.[۷۵] مفاد رأی دیوان در ماده ۱۱ طرح مسئولیت بین‌المللی دولت بدین شکل از نو تأیید شده است: «رفتاری که به‌موجب مواد پیشین به دولت منتسب نشود، با وجود این در صورتی که و تا حدی که آن دولت آن رفتار را تأیید و همچون رفتار خویش تلقی کند، به‌موجب حقوق بین‌الملل، فعل آن دولت تلقی می‌شود».

در سوی مقابل، زمانی که منشأ حمله، *بازیگران غیردولتی* مستقر در قلمرو کشوری دیگر باشند، چه وضعیتی شکل خواهد گرفت؟ در این مرحله آیا دولت قربانی می‌تواند علیه بازیگران غیردولتی مستقر در قلمرو دولتی دیگر که حمله از جانب آن نبوده و مسئولیت مستقیم برای حمله نداشته، متوسل به زور شود؟ پاسخ به این پرسش‌ها از این جهت مهم است که ماهیت دنیای جهانی‌شده و مرتبط امروز که با اتکای گسترده به فناوری، سامانه‌های رایانه‌ای و ارتباط اینترنتی ترکیب شده بدین معنی است که بازیگران غیردولت، چه در ظرفیت انفرادی و چه در قامت گروهی، با توجه به راحت‌بودن انجام حملات سایبری و گمنامی منشأ این حملات،[۷۶] می‌توانند اثر مهمی از طریق فضای سایبری داشته باشند.[۷۷]

این مسئله در خصوص بازیگران غیردولتی مستقر در قلمرو یک دولت، مشخص است که در مرحله اول، دولت سرزمینی، مسئول حمله مسلحانه علیه دولت هدف است و در صورتی که دولت سرزمینی مایل یا قادر نباشد که حملات مسلحانه از داخل سرزمین آن، علیه دولت دیگر را متوقف

سازمان دولتی چه موقعیتی دارد و اعم از اینکه ارگان مذکور، عضوی از دولت مرکزی باشد یا عضوی از واحد دولت محلی. ۲) ارگان شامل هر شخص یا نهادی می‌شود که به‌موجب حقوق داخلی دولت، وضعیت مزبور را داشته باشد».

73. Marco Roscini, *op.cit*., p. 99.

74. *Ibid*., pp. 99-101.

75. ICJ, *United States Diplomatic and Consular Staff in Teheran (United States v. Iran*), 1980, para. 74.

۷۶. حبیبی، همایون و وحید بذّار؛ «حملات سایبری و ممنوعیت توسل به زور»، *فصلنامه تعالی حقوق*، دوره ۳، شماره ۱۹، ۱۳۹۶، صص ۱۵۷-۱۵۶.

77. Laurie K. Blank, *op.cit*., p. 407.

کند، حقوق بین‌الملل به‌کارگیری نیروی نظامی را در مقام دفاع مشروع در پاسخ به حمله مسلحانه، تا زمانی که چنین رویه‌ای لازم و متناسب باشد اجازه می‌دهد.[۷۸] باید توجه داشت از آنجا که دولت محل استقرار گروه‌های غیردولتی، نقشی در حمله ندارد، و هرگونه اقدام کشور قربانی مستلزم نقض حاکمیت دولت محل استقرار گروه‌های غیردولتی است، دولت قربانی ابتدا باید رضایت دولت سرزمینی را کسب کند یا دلایلی ارائه دهد که دولت سرزمینی نمی‌خواهد یا نمی‌تواند اقداماتی انجام دهد که مانع تهدیدات بازیگران غیردولتی در آینده شود یا آن‌ها را از بین ببرد.[۷۹]

البته بعضی دیگر از حقوق‌دانان معتقد به اعمال یک پیش‌شرط هستند و آن این است که «دولت قربانی ابتدا باید از دولت محل مخفی‌شدن تروریست‌ها بخواهد در راستای پاسخگویی به وظیفه قانونی خود، اطمینان حاصل کند که از قلمرو او برای آسیب‌رساندن به کشورهای دیگر استفاده نمی‌شود. اگر این دولت موافقت کند و عملیات مؤثری را به منظور ازمیان‌برداشتن تهدیدات آغاز کند، نفوذ به داخل خاک آن کشور توسط نیروهای دولت قربانی غیرمجاز است».[۸۰] البته این پیش‌شرط، زمانی عقلانی است که تهدید فوری نباشد. این امر از اصل ضرورت پیروی می‌کند که همراه با اصل تناسب، دیوان بین‌المللی دادگستری آن را به‌عنوان شرایط تحقق دفاع مشروع به رسمیت شناخته است.[۸۱]

در حقیقت، در راستای احترام به حق حاکمیت دولت‌ها بر قلمرو خود که قاعده آمره حقوق بین‌الملل شناخته می‌شود و در منشور نیز بازتاب یافته است، نخست باید از دولت مقر تروریست‌ها خواست تا با آنان مبارزه کند.. « اگر چنین فرصتی برای انجام این کار فراهم آید اما دولت سرزمینی نتواند عملیات متقابل انجام دهد یا چنین روشی را در حالی‌که قادر به انجام باشد انتخاب نکند یا نتواند اقدام مناسب انجام دهد، دولت قربانی می‌تواند در مقام دفاع مشروع از خود، اقدام نظامی انجام دهد»[۸۲] و بدین وسیله به فعالیت‌های خرابکارانه و غیرقانونی این گروه‌ها خاتمه بخشد. به عبارت دقیق‌تر، ورود دولت ثالث به قلمرو دولت دیگر برای مقابله با معضلی که دولت سرزمینی نمی‌تواند یا نمی‌خواهد آن را حل کند، در حالی که نتایج منفی آن بر دولت ثالث اثرگذار است، اجتناب‌ناپذیر و ضروری است و مثال‌های متعددی نیز در این زمینه وجود دارد.[۸۳]

78. Louise Arimatsu and Mohbuba Choudhury, "Year in Review", *Yearbook of International Humanitarian Law*, Vol. 13, 2010, p. 291.

79. Laurie K. Blank, *op.cit*, p. 416.

80. Michael N. Schmitt, "Drone Attacks under the Jus Ad Bellum and Jus in Bello: Clearing the 'Fog of Law'", *Yearbook of International Humanitarian Law*, Vol.13, 2010, p. 316.

81. ICJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America*), Judgment of 27 June, 1986, p. 103, para.194; ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion of 8 July, 1996, p. 245, para. 41; ICJ, *Oil Platforms (Iran v United States of America)*, Judgment of 6 November, 2003, p. 183, para. 43 and pp. 196–199, paras.73-77; etc.

82. Michael N. Schmitt, *op.cit*., pp. 316-317.

83. Ashley Deeks, "Unwilling or Unable: Toward a Normative Framework for Extraterrotial Self-Defense", *Virginia Journal of International Law*, Vol. 52, 2012, pp. 547-550.

آنچه مسلم است با توجه به نظم بین‌المللی کنونی و معیارهای حقوق بین‌الملل، هر دولتی مسئول کنترل و حاکمیت قلمرو تحت حکومت‌اش است و در خصوص اقدامات غیرقانونی اتباع خود چه در بُعد داخلی و چه در بُعد بین‌المللی مسئول است و نه‌تنها باید راهکارهای مناسبی را به منظور جلوگیری از این اقدامات غیرقانونی اتخاذ کند، بلکه باید اجازه ندهد بخش‌هایی از خاک خود، پناهگاه امن و مطمئن برای بازیگران غیرقانونیِ فراملی شود. همان‌طور که دیوان در رأی کانال *کورفو* بیان می‌دارد، هیچ دولتی نباید اجازه دهد که قلمرواش برای اقدامات مخالف حقوق سایر دولت‌ها به کار رود.[۸۴] بنابراین گرچه دولت، مسئول حملات سایبری نیست، تعهد خود نسبت به این بخش از رأی دیوان را نقض کرده و در این چارچوب مرتکب قصور شده و مسئول است.[۸۵]

زمانی که دولتی نخواهد یا نتواند از اقدامات خصمانه بازیگران غیردولتی که از خاک آن علیه دولت دیگر صورت می‌گیرد جلوگیری کند، برخی معیار «نخواستن»[۸۶] یا «نتوانستن»[۸۷] را مطرح کرده‌اند.[۸۸] به‌موجب این معیار، زمانی که دولتی نمی‌تواند از اقدامات خصمانه بازیگران غیردولتی که از خاک آن علیه دولتی دیگر صورت می‌گیرد جلوگیری کند، دولتی که مورد حمله قرار گرفته است می‌تواند رأساً به منظور مبارزه با این اقدامات وارد قلمرو دولت دیگر شود.

پیشنهاد شده است در زمان حمله گروه‌های غیردولتی از قلمرو دولت دیگر، دولت قربانی پنج معیار را مدنظر قرار دهد:[۸۹]

۱. همکاری اولیه یا کسب رضایت از دولت سرزمینی به جای استفاده یک‌جانبه از زور؛

۲. درخواست از دولت سرزمینی برای رسیدگی به تهدید و تعیین زمان مناسب برای ارائه پاسخ؛

۳. ارزیابی منطقی از ظرفیت دولت سرزمینی و کنترل آن بر مناطق تحت نفوذ؛

۴. ارزیابی منطقی ابزار پیشنهادی دولت سرزمینی برای سرکوب تهدید؛

۵. ارزیابی روابط قبلی دولت قربانی با دولت سرزمینی که حمله از آن صورت می‌پذیرد.[۹۰]

مجدداً تأکید می‌شود که رعایت شرایط فوق، زمانی منطقی خواهد بود که مسئله فوریت، موضوعیت نداشته باشد، یعنی در جایی که حملات، مستمر و ادامه‌دار باشد.

در خصوص حملات سایبری بازیگران غیردولتی و انتساب اَعمال آن‌ها به دولت‌ها، معیارهای

---

84. *Corfu Channel (United Kingdom v. Albania*), ICJ Reports 1949, 4 et seq. (22). A/RES/55/63 of 4 December 2000 recommends that States ensure "that their laws and practice eliminate safe havens for those who criminally misuse information technologies", (para. 1).

85. Marco Roscini, *op.cit*., p. 102.

86. Unwilling

87. Unable

88. Ashley Deeks, *op.cit*., pp. 501-502.

89. Ashly Deeks, "The Geography of Cyber Conflict: Through a Glass Darkly", *International Law Studies* (U.S. Naval War College), Vol. 89, 2013, pp. 9-10.

90. *Ibid*., pp. 10-16.

کنترل مؤثر[۹۱] (دیوان بین‌المللی دادگستری در قضیه نیکاراگوئه علیه امریکا)[۹۲] و کنترل کلی[۹۳] (دیوان بین‌المللی کیفری برای یوگسلاوی سابق در قضیه *تادیچ*)[۹۴] مطرح شده‌اند. گرچه برخی معتقد به اعمال کنترل مؤثر در دنیای سایبر[۹۵] و برخی دیگر معتقد به اعمال کنترل کلی هستند،[۹۶] عده‌ای نیز این مسئله را مطرح کرده‌اند که با توجه به چالش شناسایی منبع حملات سایبری بهتر است که معیار کنترل مؤثر پذیرفته شود.[۹۷]

در نهایت، در خصوص حملات سایبریِ افراد (هکرها) نیز باید به این نکته توجه داشت که در موارد معدود نیز حملات سایبری گرچه از قلمرو یک کشور به وقوع می‌پیوند، نه دولت‌ها در آن نقش دارند و نه بازیگران غیردولت، بلکه حمله را هکرها انجام می‌دهند. در این گونه موارد نمی‌توان رفتار آن‌ها را به دولت منتسب کرد، گرچه ممکن است به دلیل عدم اتخاذ اقدامات ضروری و معقول نسبت به جلوگیری یا متوقف‌کردن حمله مسئول شناخته شود (برای مثال با قطع دسترسی اینترنت مرتکبین حمله در صورتی که امکان شناسایی آن‌ها وجود داشته باشد).

اهمیت مشخص‌کردن منشأ حملات سایبری از این جهت است که برای استناد به حق دفاع مشروع، رعایت شرط «فوریت»[۹۸] الزامی است، در حالی که ممکن است تعیین منشأ حمله، فرایندی طولانی و پیچیده باشد که در تعارض با شرط فوریت در دفاع مشروع قرار گیرد. شایان ذکر است به‌موجب شرط فوریت، توسل به دفاع مشروع در برابر حمله مسلحانه نباید بدون دلیل به تأخیر بیفتد و در صورت تأخیر، حق دفاع مشروع برای کشور مورد حمله از بین می‌رود زیرا چنین اقدامی دیگر دفاع محسوب نشده و اقدام تلافی‌جویانه قلمداد می‌شود؛[۹۹] اگرچه این به این معنی نیست که چنین پاسخی برای اینکه قانونی تلقی شود باید آنی باشد.[۱۰۰] این شرط برای تمایز میان دفاع مشروع به‌عنوان استثنای قاعده منع توسل به زور و حملات مسلحانه به‌عنوان نقض قاعده منع توسل به زور پیش‌بینی شده است.[۱۰۱]

با توجه به مطالب مذکور، در این خصوص این پرسش مطرح می‌شود که با توجه به شرط فوریتِ توسل به حق دفاع مشروع، آیا امکان دارد «فوریت» و «تشخیص منشأ حقیقی حمله» را

91. Effective control

92. ICJ, *Judgment on Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States*) - (Merits), 1986, pp. 64-65, para. 115.

93. Overall control

94. ICTY, *Prosecutor v. Tadić*, Case No. IT-94-1-A, Appeals Chamber, Judgment, 15 July 1999, p. 49, para. 120.

95. Marco Roscini, *op.cit*., p. 100.

96. Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", *Berkeley Journal of International Law*, Vol. 27, 2009, 192 et seq. p. 235.

97. Marco Roscini, *op.cit*. p. 100.

98. Immediacy

99. Laurie K. Blank, *op.cit*., p. 419.

100. Terry D. Gill and Paul A. L. Ducheine, *op.cit*., p. 451.

101. *Ibid*.

با یکدیگر جمع نمود یا خیر. به عبارت بهتر، چه مدت زمانی را باید به‌عنوان ملاک توسل به حق دفاع مشروع در برابر حملات سایبری در فرض تشخیص منشأ اصلی و حقیقی حمله مدنظر قرار داد: زمانی که حمله صورت می پذیرد، یا زمانی که منشأ حقیقی حمله و انتساب آن به یک دولت روشن می‌شود که ممکن است چندین ساعت، روز، هفته و ماه یا بیشتر به طول بینجامد. در پاسخ به این پرسش، تا کنون چند دیدگاه مطرح شده است:

به‌موجب دیدگاه اول، تنها زمانی می‌توان شرط فوریت را در دفاع مشروع رعایت کرد که منشأ حمله مشخص و قابل انتساب باشد. دیدگاه دوم بیانگر این است که شرط فوریت، بازتاب‌دهنده این حقیقت است که هدف نهایی از توسل به دفاع مشروع، مجازات حمله‌کننده نیست، بلکه پاسخ به او (در مفهوم دفع خطر) است. ازاین‌رو این الزام، بخصوص در مورد فضای سایبر باید منعطف اِعمال شود. اگر شبکه رایانه‌ای نظامی یک دولت، ظرفیت خود را به علت حمله سایبری از دست بدهد، راه‌اندازی مجدد چنین شبکه‌ای برای پاسخ به حملهٔ صورت‌گرفته، زمان‌بَر خواهد بود. در فرضی دیگر، اگر متجاوز، از بمب‌های سایبریِ منطقی[۱۰۲] یا زمانی استفاده کند، خسارت واقعی زمانی اتفاق می‌افتد که حمله سایبری واقع می‌شود؛ که ممکن است در احراز شرط فوریت، تأخیر ایجاد کند[۱۰۳] و ملاک این شرط را به زمان فعال‌شدن و اثرگذاری این بمب‌ها تغییر دهد.

به نظر می‌رسد برای استناد به حق دفاع مشروع در قبال حملات سایبری باید بین حملات سایبری مقطعی و حملات سایبری مستمر، قائل به تفکیک شد. در فرضی که حمله سایبری صورت می‌گیرد و به اتمام می‌رسد، در صورت عدم پاسخ در زمان مناسب و در چارچوب شرایط حقوقی تعیین‌شده، دیگر پایه‌ای برای استناد به دفاع مشروع وجود ندارد. به عبارت دیگر، با توجه به اهمیت عنصر فوریت در تحقق دفاع مشروع، زمانی می‌توان به این حق متوسل شد که بلافاصله پس از حملات سایبری و با رعایت شروط عرفی و مدون دفاع مشروع انجام شود. در غیر این صورت، استناد به دفاع مشروع پس از مدت زمانی معقول، غیرقابل قبول است. اما اگر حملات سایبری استمرار داشته باشد و در طول حملات مستمر و به‌هم‌پیوسته، هویت حمله‌کننده مشخص شود، امکان توسل به دفاع مشروع وجود دارد. فرض دیگری که در این راستا باید مورد توجه قرار گیرد، تجمیع حملات سایبری و عینی است که امکان شناسایی عامل حملات سایبری را تسهیل می‌کند. همچنین تهدیدات و حملات سایبری می‌تواند نشانه‌ای نسبت به امکان حمله عینی به‌وسیله دولت تهدیدکننده باشد.[۱۰۴]

102. Logic bomb

نحوه عملکرد بمب‌های منطقی به این شکل است که بخشی از کد، عمداً داخل یک سامانه نرم‌افزاری قرار می‌گیرد که در شرایط خاص و از پیش تعیین‌شده‌ای منتهی به آثار مخرب و خرابکارانه می‌شود. ن.ک:

Laurie K. Blank, *op.cit.*

103. Marco Roscini, *op.cit.*, pp. 119-120.

104. Terry D. Gill and Paul A. L. Ducheine, *op.cit.*, p. 462. Also see: Marco Roscini, *op.cit.*, p. 104.

نتیجه

گرچه بحث حقوق بین‌الملل حاکم بر فضای سایبر و حملات سایبری از دهه‌های گذشته مطرح و در این سال‌ها پیشرفت و تکامل یافته است، همچنان با دو چالش بنیادین، یکی ناظر بر «ضعف ادبیات حقوقی بین‌المللی در قبال مفاهیم تکنیکی حملات سایبری» و دیگری ناظر بر «ضعف در برقراری ارتباط بین مفاهیم حقوقی دنیای عینی و دنیای سایبری» که اولی بُعد مکان و دومی بُعد زمان را پوشش می‌دهند روبه‌روست. روشن است تا زمانی‌که این چالش‌های بنیادین مرتفع نشود، دیگر مسائل و چالش‌های مربوط به حملات سایبر نیز همچنان موضوع اختلاف و منازعه قرار خواهند داشت. عوامل اصلی تداوم این چالش‌های بنیادین به شرح ذیل است:

۱. اجماعی در خصوص مفاهیم مطروحه در فضای سایبر حاصل نشده و هر دولتی سعی در ارائه تعریف مطابق با امکانات و زیرساخت‌های خود دارد. به عبارت دیگر، چارچوب فضای سایبر و اجزا و عناصر آن با توجه به سلایق دولت‌ها و تفسیرهای شخصی آن‌ها قبض و بسط پیدا می‌کند که این امر موجب بی‌ثباتی و مانعی بر سر قوام‌یافتن حقوق بین‌الملل حاکم بر حملات سایبری شده است.

۲. افرادی که در هر دو زمینه حقوق بین‌الملل و فضای سایبر صاحب‌نظر و متخصص باشند و رویکردی جامع به هر دو حوزه داشته باشند و مواضع مختلفی را بیان کنند، انگشت‌شمارند. بدون شک، تدوین و شکل‌گیری حقوق بین‌الملل حاکم بر فضای سایبر به تعامل حقوق‌دانان بین‌المللی به منظور انعکاس نظرات نظام‌های حقوقی مختلف و متخصصان فضای سایبر یا افرادی که در هر دو حوزه فعالیت داشته باشند نیاز دارد. مثال برجسته‌ای که می‌توان از این افراد برشُمرد، *مایکل ان.اشمیت* است. او یکی از معدود افرادی است که در هر دو زمینه مطالعاتی داشته و چهره‌ای شناخته‌شده در این حوزه است.[۱۰۵]

۳. درحالی‌که «دولت‌های قدرتمند همچون امریکا و روسیه این حق را برای خود قائل شده‌اند که حملات سایبری را جنگ قلمداد کنند و حق دفاع مشروع را برای خود محفوظ به حساب می‌آورند»،[۱۰۶] در عمل چنین اتفاقی تا کنون رُخ نداده است. این طرز تفکر در میان سران دیگر دولت‌ها نیز وجود دارد، به‌صورتی که در اغلب موارد، هر گونه حمله سایبری را توسل به زور تلقی می‌کنند که می‌تواند پاسخ کوبنده آن‌ها را در بر داشته باشد. اما به نظر می‌رسد که خود نیز آگاه‌اند که هرگونه حمله سایبری، معادل حمله مسلحانه به کشور آن‌ها نیست. برای مثال، پیش از انتخابات ریاست جمهوری امریکا در سال ۲۰۱۶، بعضی از مقامات این کشور، هرگونه حمله سایبری را تهدید علیه امنیت ملی و در حکم حمله نظامی به حساب می‌آوردند و حق دفاع مشروع و توسل به نیروی نظامی را در قبال هرگونه حمله

---

۱۰۵. برای ملاحظه کارنامه علمی و اجرایی *مایکل ان .اشمیت*، ن.ک:
<www.pilac.law.harvard.edu/michael-n-schmitt> and
<www.usnwc.edu/Faculty-and-Departments/Directory/Michael-N-Schmitt>

106. Marco Roscini *op.cit*., pp. 108-109.

سایبری برای خود قائل می‌شدند[۱۰۷] اما در زمان برگزاری انتخابات ریاست جمهوری و پس از آن که ادعا شد سامانه‌های رأی‌گیری، مورد حملات سایبری روسیه قرار گرفته‌اند، حتی دولت جدید امریکا جز محکوم‌کردن فعالیت‌های مذکور و در بعضی موارد، اعمال تحریم علیه روسیه[۱۰۸] و اعلام جرم علیه دوازده نفر از افسران سرویس اطلاعاتی روسیه،[۱۰۹] کار دیگری نکرد. باید توجه داشت، به هر میزان که این تهدیدها نسبت به امنیت ملی و اقتصادی یک کشور جدی باشند، باز هم حمله مسلحانه‌ای نیستند که بیانگر استفاده از زور باشند و بتوان در قبال آن‌ها به حق دفاع مشروع استناد کرد.[۱۱۰]

۴. تحقق مسئولیت بین‌المللی دولت‌ها در حملات سایبری، در گرو انتساب حمله (فعل) به یک دولت به‌موجب حقوق بین‌الملل و نقض تعهد بین‌المللی توسط همان دولت است.[۱۱۱] مشخص‌نکردن چارچوب معین برای فضای سایبری باعث خواهد شد به دلیل نبود تعریف مورد قبول در جامعه جهانی، هریک از دولت‌ها مطابق با امکانات، زیرساخت‌ها، توانایی‌ها و معیارهای شخصی دیگر، فضای سایبر و حملات سایبری را تعریف کند. به همین دلیل درحالی‌که در جهان عینی، جنگ‌ها به سمت جنگ‌های نیابتی پیش می‌روند، در جهان مجازی نیز جنگ‌ها به سمت جنگ‌های سایبری[۱۱۲] در حرکت‌اند که در هر دوی آن‌ها بحث اثبات و انتساب مسئولیت با مشکل روبه‌روست. بنابراین، ماهیت مخفیانه حملات سایبری چه در قالب حمله و چه در قالب دفاع، یکی از موانعی است که مانع شکل‌گیری و مشخص‌شدن رویه دولت‌ها می‌شود.[۱۱۳]

بنابر آنچه گفته شد، برای ازمیان‌برداشتن موانع فراروی تدوین حقوق بین‌الملل حاکم بر حملات سایبری، اجماع دولت‌ها بر حداقل استانداردهایی در زمینه حقوق بین‌الملل حاکم بر حملات سایبری و تدوین کنوانسیون بین‌المللی در این زمینه ضروری است؛ گرچه رسیدن به توافق میان دولت‌ها در مراحل اولیه، به‌ویژه در خصوص تعریف و تعیین ویژگی‌های حملات سایبری و مشخص‌کردن آستانه حملات سایبری که موجب فعال‌شدن حق توسل به زور می‌شود دشوار خواهد بود. بدیهی است کشورهای غربی و در رأس آن‌ها امریکا که زیرساخت‌های‌شان وابستگی شدیدی به فضای مجازی دارد و به همین دلیل در برابر حملات سایبری شکننده‌ترند، به دنبال پایین‌آوردن این آستانه

107. "Russian Cyber Attacks 'Act of War': US Senator McCain", *Gulf News*, January 5, 2017, https://gulfnews.com/world/americas/russian-cyber-attacks-act-of-war-us-senator-mccain-1.1956554.

108. Peter Baker, "White House Penalizes Russians Over Election Meddling and Cyberattacks", *The New York Times*, March 15, 2018, www.nytimes.com/2018/03/15/us/politics/trump-russia-sanctions.html.

109. The Associated Press, "12 Russians Indicted for Meddling in 2016 US Election", The New York Times, 13 July, 2018, https://www.nytimes.com/aponline/2018/07/13/us/politics/ap-us-trump-russia-probe.html

110. Terry D. Gill and Paul A. L. Ducheine, *op.cit*., p. 460.

۱۱۱. ماده ۲ طرح مسئولیت بین‌المللی دولت به نقل از: کمیسیون حقوق بین‌الملل سازمان ملل متحد، *مسئولیت بین‌المللی دولت؛ متن و شرح مواد کمیسیون حقوق بین‌الملل*، ترجمه: علیرضا ابراهیم‌گل، چاپ سوم، شهر دانش، ۱۳۹۰.

112. Matthew C. Waxman (1), *op.cit*., pp. 50-51.

113. Matthew C. Waxman (2), "Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions", *International Law Studies* (U.S. Naval War College), Vol. 89, 2013, p. 121.

هستند تا هرگونه اقدام خصمانه سایبری را در دایره حملات سایبری قرار دهند و توسل به دفاع مشروع را برای خود محفوظ دارند. در سوی مقابل، کشورهای درحال‌توسعه که وابستگی کمتری به زیرساخت‌های سایبری دارند، به دنبال بالابردن آستانه حملات سایبری خواهند بود.

نظر به مراتب فوق، می‌توان دو راهکار ذیل را به‌عنوان قدم‌های اولیه در راه تدوین حقوق بین‌الملل حاکم بر حملات سایبری برشُمرد:

قدم اول، «تدوین معاهدات منطقه‌ای و بین‌المللی» است. تدوین معاهدات منطقه‌ای به منظور شاخ و برگ‌بخشیدن به ادبیات حقوقی مربوط به حملات سایبری و رسیدن به اجماع در سطح منطقه مفید خواهد بود تا از این رهگذر وفاق بین‌المللی حاصل شود. بدیهی است که تدوین معاهدات منطقه‌ای، گذر از سیاست‌های ملی به اجماع بین‌المللی را از طریق سازمان‌های منطقه‌ای امکان‌پذیر می‌کند که این امر در نهایت می‌تواند زمینه‌ساز معاهده‌های بین‌المللی شود.

آنچه در تدوین معاهده بین‌المللی در حوزه حقوق حاکم بر حملات سایبری باید مورد توجه قرار گیرد، در مرحله اول، ایجاد تعادل بین ملاحظات و منافع دولت‌های دارای فناوری در سطوح مختلف است، همانند کنوانسیون حقوق دریاها که توانست بین منافع کشورهای دارای فناوری و فاقد فناوری توازن برقرار کند.

قدم دوم، «توسل به اقدامات موجد اعتماد»[۱۱۴] از سوی دولت‌ها و شفاف‌سازی فعالیت‌های سایبری آن‌هاست. ایجاد سامانه‌ای بین‌المللی که فعالیت‌های سایبری کشورها را در سراسر جهان پایش کند، همانند «سیستم نظارت بین‌المللی»[۱۱۵] که در «معاهده جامع منع آزمایش‌های هسته‌ای»[۱۱۶] استفاده شده است می‌تواند گامی مؤثر در پایش و رهگیری حملات سایبری باشد. شاید ظهور و تثبیت فناوری بلاکچین[۱۱۷] بتواند گامی رو به جلو در این عرصه به حساب بیاید.

114. Confidence Building Measures (CBM)
115. International Monitoring System (IMS)
116. Comprehensive Nuclear-Test-Ban Treaty (CTBT)
117. Blockchain

منابع:

الف. فارسی

ـ کتاب

- کمیسیون حقوق بین‌الملل سازمان ملل متحد، مسئولیت بین‌المللی دولت؛ *متن و شرح مواد کمیسیون حقوق بین‌الملل*، ترجمه: علیرضا ابراهیم‌گل، چاپ سوم، شهر دانش، ۱۳۹۰.

ـ مقاله

- آهنی امینه، محمد و فاطمه زهرا فتح‌اللهی؛ «حقوق بین‌الملل مدرن در مواجهه با جنگی پست‌مدرن (نبرد سایبری)»، *راهبرد*، سال بیست‌وسوم، پاییز ۱۳۹۳، شماره ۷۲.
- حبیبی، همایون و وحید بذّار؛ «حملات سایبری و ممنوعیت توسل به زور»، *فصلنامه تعالی حقوق*، دوره سوم، شماره ۱۹، ۱۳۹۶.
- _____؛ «ظرفیت‌سنجی بند ۴ ماده ۲ منشور ملل متحد در قبال حملات سایبری از نظرگاه حقوق بین‌الملل»، مجموعه مقالات همایش هفتادمین سالگرد تأسیس سازمان ملل متحد (۱۳۹۴: انجمن ایرانی مطالعات سازمان ملل متحد و دانشکده روابط بین‌الملل وزارت امور خارجه)، اداره نشر وزارت امور خارجه، ۱۳۹۶.
- کیهانلو، فاطمه و وحید رضادوست؛ «حملات سایبر به مثابه توسل به زور در سیاق منشور سازمان ملل متحد»، فصلنامه تحقیقات حقوقی، شماره ۶۹، ۱۳۹۴.

ب. انگلیسی

- Books

- P. Grant and J. Craig Barker, *Parry & Grant Encyclopædic Dictionary of International Law*, Third Edition, Oxford University Press, 2009
- James Crawford, *Brownlie's Principles of Public International Law*, 8th Edition, Oxford University Press, 2012.
- *Department of Defense Dictionary of Military and Associated Terms* (Joint Publication 1-02), 8 November 2010 (As Amended through15 December 2012).
- Marcel Danesi, *Dictionary of Media and Communications*, M.E. Sharpe, 2009.
- *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, 2013.

- Bruno Simma, *The Charter of the United Nations: A Commentary*, Third Edition, Vol. I, Oxford University Press, 2012.

- Articles

- Ashley Deeks, "Unwilling or Unable: Toward a Normative Framework for Extraterrotial Self-Defense", *Virginia Journal of International Law*, Vol. 52, 2012.
- Ashly Deeks, "The Geography of Cyber Conflict: Through a Glass Darkly", *International Law Studies* (Naval War College), Vol. 89, 2013.
- Laurie K. Blank, "International Law and Cyber Threats from Non-State Actors", *International Law Studies* (Naval War College), Vol. 89, 2013.
- Louise Arimatsu and Mohbuba Choudhury, "Year in Review", *Yearbook of International Humanitarian Law*, Vol. 13, 2010.
- Marco Roscini, "World Wide Warfare -Jus ad bellum and the Use of Cyber Force", *Max Planck Yearbook of United Nations Law*, Vol. 14, 2010.
- Matthew C. Waxman, "Cyber Attacks as "Force" under UN Charter Article 2(4)", *International Law Studies*, Vol. 87, 2011.
- Matthew C. Waxman, "Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions", *International Law Studies* (Naval War College), Vol. 89, 2013.
- Michael N. Schmitt, "'Attack' as a Term of Art in International Law: The Cyber Operations Context", in: C. Czosseck, R. Ottis, K. Ziolkowski (Eds.), 4th International Conference on Cyber Conflict, NATO CCD COE Publications, 2012.
- Michael N. Schmitt, "Drone Attacks under the Jus Ad Bellum and Jus in Bello: Clearing the 'Fog of Law'", *Yearbook of International Humanitarian Law*, Vol.13, 2010.
- Robert F. Turner, "Nuclear Weapons and the World Court: The ICJ's Advisory Opinion and Its Significance for U.S. Strategic Doctrine", *International Law Studies*, in: *The Law of Military Operations: Liber Amicorum, Professor Jack Grunawalt*, Michael N., Schmitt (ed.), 1998.
- Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", *Berkeley Journal of International Law*, Vol. 27:1, 2009.
- Terry D. Gill and Paul A. L. Ducheine, "Anticipatory Self-Defense in the Cyber Context", *International Law Studies* (Naval War College), Vol. 89, 2013.

- Case Law

- ICTY, *Prosecutor v. Dusko Tadic*, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 1995.

- ICJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America*), Judgment of 27 June 1986 (Merits).
- ICJ, *Advisory Opinion of 8 July 1996, Legality of the Use by a State of Nuclear Weapons in Armed Conflict*, 1996.
- ICJ, *United States Diplomatic and Consular Staff in Teheran (United States of America v. Iran*), ICJ Reports 1980.
- ICJ, *Corfu Channel (United Kingdom v. Albania*), ICJ Reports 1949.
- ICTY, *Prosecutor v. Tadić*, Case No. IT-94-1-A, Appeals Chamber, Judgment, 15 July 1999.
- ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion of 8 July 1996.
- ICJ, *Oil Platforms (Iran v United States of America*), Judgment of 6 November 2003.

- Instruments

- Convention on Rights and Duties of States (Montevideo Convention), 1933.
- Additional Protocol I to the Geneva Convention of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, Art. 1(2), 12 December, 1977, 1125 U.N.T.S.3.
- Wales Declaration, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, 2014.
- North Atlantic Treaty Organization, 1949.

- Reports

- "How is the Term 'Armed Conflict' Defined in International Humanitarian Law?", *International Committee of the Red Cross (ICRC) Opinion Paper*, March 2008.
- Martin Pratt, Booklet of Applied Issues in International Land Boundary Delimitation / Demarcation Practices, (A Seminar organized by the OSCE Borders Team in co-operation with the Lithuanian OSCE Chairmanship, 31 May to 1 June 2011 Vilnius, Lithuania), 2011.
- Robert J. Butler, "Cyber War: Definitions, Deterrence, and Foreign Policy (Testimony before the House Foreign Affairs Committee)", *Center for a New American Security*, 2015.
- Nils Melzer, "Cyberwarfare and International Law", *UNIDIR Resources*, 2011.

- Thesis

- ÖykülIrmakkesen, "The Notion of Armed Attack under the UN Charter and the Notion of International Armed Conflict – Interrelated or Distinct?",

LL.M. Paper written under the supervision of Professor Marco Sassòli, Geneva Academy, August 2014.

- Websites

- www.ccdcoe.org/tallinn-manual.html
- www.dw.com/en/german-army-launches-new-cyber-command/a-38246517
- www.pilac.law.harvard.edu/michael-n-schmitt
- www.usnwc.edu/Faculty-and-Departments/Directory/Michael-N-Schmitt
- "Russian Cyber Attacks 'Act of War': US Senator McCain", *Gulf News*, January 5, 2017, available at: www.gulfnews.com/news/americas/usa/russian-cyber-attacks-act-of-war-us-senator-mccain-1.1956554
- Peter Baker, "White House Penalizes Russians Over Election Meddling and Cyberattacks", *The New York Times*, March 15, 2018, available at: www.nytimes.com/2018/03/15/us/politics/trump-russia-sanctions.html
- The Associated Press, *12 Russians Indicted for Meddling in 2016 US Election*, *The New York Times*, 13 July 2018, available at: https://www.nytimes.com/aponline/2018/07/13/us/politics/ap-us-trump-russia-probe.html.

ج. فرانسوی

- Chapitre dans le livre

- Djamchid Momtaz, L'Évolution du Droit International Humanitaire Applicable à la Conduite des Hostilitiés, in: Conduct of Hostilities: the Practice, the Law and the Future (37th Round Table on Current Issues of International Humanitarian Law), International Institute of Humanitarian Law, 2015.