Center for Strategic Research
Quarterly Journal of Diplomatic Strategies in International Organizations
https://sazmanbeynolmelal.csr.ir E-ISSN: 2588-6665
Vol. 3, No. 2, Issue. 10, Summer 2025 Received: 2023/08/14 Accepted: 2024/05/07
Research paper

State Responsibility in International Law and the Attribution of Cyberattacks

Reza Rahmati
PhD in International Relations, Faculty of Law and Political Science, University of Tehran, Tehran, Iran.
Email: rahmatii@gmail.com

Abstract

International law and its related domains, including the law of armed conflict and international humanitarian law, have undergone significant transformations, one of which concerns the environment in which wrongful acts are committed. In today's world, cyberspace has replaced physical spaces as a principal arena. Cyber operations—including espionage, cybercrimes, and, more broadly, cyberattacks—constitute violations of states' obligations under international law. Given their capacity to inflict physical damage and human harm, such acts not only undermine states' obligations but also give rise to state responsibility. Key questions arise as to whether cyberattacks fall within the notion of an "attack" as envisaged under the Geneva Conventions, how the responsible state or entity may be identified, and, once identified, how the conduct can be attributed to a state and what the ensuing consequences of responsibility would be. Accordingly, the central research question of this study is framed as follows: *To what extent can cyberattacks be attributed to state conduct?* Addressing this question requires, first, determining whether cyberattacks qualify as "attacks" under international law, which in turn necessitates a functional interpretation of Article 2(4) of the UN Charter, followed by a detailed inquiry into the processes of identification and attribution of cyberattacks.

Keywords: Cyberattacks, State Responsibility, Attribution, Identification

سال سوم، شماره دوم (پیاپی ۱۰)، تابستان ۱۴۰۴، صص. ۳۱-۶۰
تاریخ دریافت: ۱۴۰۲/۰۵/۲۳ ـ تاریخ پذیرش: ۱۴۰۳/۰۲/۱۸

مقاله پژوهشی

مسئولیت بین‌المللی دولت‌ها و مسئله انتساب حملات سایبری

رضا رحمتی
دانش‌آموخته دکتری تخصصی روابط بین‌الملل، دانشکده حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران
Email: rahmatii@gmail.com

چکیده

حقوق بین‌الملل و حوزه‌های وابسته به آن، از جمله حقوق جنگ و حقوق بشردوستانه بین‌المللی دستخوش تغییرات فراوانی شده است که یکی از آن‌ها تغییر در محیط ارتکاب جرم است. اعمال و عملیات سایبری اعم از جاسوسی، اعمال جرم و در حد گسترده‌تر آن یعنی حملات سایبری، خلاف تعهدات دولت‌ها در حقوق بین‌الملل هستند. این اعمال از آنجایی که قابلیت وارد کردن خسارات فیزیکی و صدمات انسانی را دارند؛ رافع تعهدات دولت‌ها و نقض مسئولیت دولت‌ها محسوب می‌شوند. بررسی اینکه این حملات جزو دسته «حمله» مد نظر کنوانسیون‌های ژنو قرار می‌گیرند یا خیر و در صورت اطلاق این عنوان به حملات سایبری چگونه دولت یا ارگان حمله‌کننده قابل شناسایی است و در صورت شناسایی چگونه رفتار او قابل انتساب به یک دولت است و متعاقباً مسئولیت دولت وفق این انتساب چیست؛ مسائلی هستند که حقوق بین‌الملل باید به آن‌ها پاسخ دهد؛ بنابراین پرسش پژوهش حاضر بدین ترتیب صورت‌بندی شده است که «آیا و تا چه اندازه‌ای حملات سایبری قابل انتساب به رفتار دولت‌ها هستند؟» برای پاسخ به این سؤال ابتدا باید به این موضوع توجه کرد که آیا حملات سایبری، ذیل عنوان «حمله» قرار می‌گیرند یا خیر، لازم است ابتدا در این خصوص تفسیر کارآمدی از ماده ۲ (بند ۴) منشور ارائه داد و سپس به مسئله شناسایی و سپس انتساب حمله سایبری پرداخت.

کلیدواژه‌ها: حملات سایبری، مسئولیت دولت، شناسایی، انتساب

مقدمه

با ظهور گروه «دولت اسلامی عراق و شام» با نام اختصاری «داعش»، حقوق بین‌الملل دستخوش تغییرات فراوانی شده است. بعضی از این تغییرات به علت نبود کارایی در برخی از شاخه‌های این بستر مطالعاتی و گروهی دیگر به دلیل تحولات جدیدی است که سبب می‌شود به مفاد و موازین جدید روی آورده شود. برای مثال از مباحث حقوقی دستخوش تغییر، می‌توان به مفهوم مصونیت (اعم از شخصی و رسمی)، مسئولیت، صلاحیت (اعم از سرزمینی، فعال، منفعل و جهانی) و شناسایی اشاره کرد. پیشرفت حقوق بین‌الملل وام‌دار بسیاری از معماها و حوادث و تلاش‌های حقوقدانان این بستر برای یافتن راه‌حل این معماها است. حقوق بین‌الملل فضا، حقوق تجارت بین‌الملل، حقوق بشردوستانه بین‌المللی، حقوق جنگ، حقوق بین‌الملل دریاها و برخی دیگر از شاخه‌های آن نیز متناسب با نیازها و معماهای جدید تغییراتی داشته‌اند.

حقوق جنگ[1] و حقوق بشردوستانه بین‌المللی[2] از موارد مهم دچار تغییر هستند. این دو را «حقوق بین‌الملل زمان مخاصمه» می‌نامند (Schmitt, 2012). حقوق جنگ مجموعه قواعد و هنجارهایی است که وقتی یک دولت «توسل به زور» را به‌عنوان یکی از ابزارهای سیاست خود برگزیند؛ بر رفتار دولت‌ها حاکم می‌شود و حقوق بشردوستانه بین‌المللی نیز با این موضوع ارتباط پیدا می‌کند که چطور نظامیان و سایر افراد مسلح می‌توانند از زور استفاده کنند؛ از جمله اینکه چطور و چه چیزی می‌تواند مورد حمله قرار گیرد و برعکس.

اما جدا از منظومه فکری، موضوع و محیط مطالعاتی نیز دستخوش تغییراتی شده است. پیش‌تر موضوع مورد مطالعه حقوق بین‌الملل، افراد، سازمان‌ها و دولت‌ها در یک محیط طبیعی و با یک مسئله فیزیکی مورد توجه بود؛ اینک فضا، جای مکان را گرفته و موضوع مورد مطالعه از جغرافیا به فضا تبدیل شده است؛ بنابراین در جهان فعلی، نت جای مکان‌ها را گرفته است. این دنیای شبکه‌ای نمونه مجازی دنیای واقعی با حضور افراد، سازمان‌ها و حتی دولت‌ها است که در دنیای امروز، شبکه و شبکه‌های فضایی را به وجود آورده‌اند و می‌توان از آن به‌عنوان «فضای دیجیتال شده» دنیای واقعی یاد کرد. در این فضای جدید هم جرم و هم مجرم حضور دارد؛ بنابراین در این فضا جرائم (هرچند به‌گونه‌ای متفاوت با دنیای واقعی) صورت می‌گیرند.

1. Jus ad Bellum
2. Jus In Bello

«حملات سایبری» از مهم‌ترین عرصه‌های فضای سایبر هستند؛ بررسی اینکه اساساً این حملات جزو دسته «حمله» مطمح نظر کنوانسیون‌های ژنو قرار می‌گیرند یا خیر و در صورت اطلاق این عنوان به حملات سایبری چگونه دولت یا کنشگر حمله‌کننده قابل شناسایی است و در صورت شناسایی چگونه رفتار او قابل انتساب به آن دولت است و متعاقباً مسئولیت دولت وفق این انتساب چیست؛ مسائلی هستند که حقوق بین‌الملل باید به آن‌ها پاسخ دهد؛ بنابراین پرسش پژوهش حاضر بدین ترتیب صورت‌بندی شده است که «آیا و تا چه اندازه‌ای حملات سایبری قابل انتساب به رفتار دولت‌ها هستند؟» برای پاسخ دادن به این سؤال ابتدا باید به این موضوع توجه داشت که آیا حملات سایبری، ذیل عنوان «حمله» قرار می‌گیرند یا خیر و سپس به مسئله شناسایی و متعاقباً انتساب حمله سایبری پرداخت.

حقوق مسئولیت بین‌المللی دولت‌ها قابلیت انتساب فعل یا ترک فعل متخلفانه بین‌المللی را احراز می‌کند. اعمال و عملیات سایبری اعم از جاسوسی، خرابکاری، اعمال جرم و در حد گسترده‌تر آن یعنی حملات سایبری که خلاف حقوق بین‌الملل هستند و به دست افراد، گروه‌ها و دولت‌ها صورت می‌گیرند؛ احتمالاً قابل انتساب به دولت‌ها هستند. همچنین حتی اگر اعمال و حملات سایبری قابل انتساب به دولت‌ها نباشند؛ دولت‌ها را از مسئولیت بین‌المللی بری نمی‌کند. پژوهش حاضر به لحاظ هدف «کاربردی»، از نظر روش، «توصیفی- تحلیلی» و به لحاظ نحوه گردآوری اطلاعات «کتابخانه‌ای» به انجام رسیده است. منابع موجود کتابخانه‌ای برای بررسی این مهم عبارت‌اند از: ۱. کتاب‌ها، مقالات و آثار مکتوب علمی؛ ۲. معاهدات اعم از دوجانبه، چندجانبه و بین‌المللی و ۳. آرا، اعم از آرای دیوان بین‌المللی دادگستری، دیوان بین‌المللی کیفری سابق و دادگاه یوگوسلاوی.

۱. حملات سایبری به‌مثابه حمله

برای اطلاق عنوان «حمله» به عملیات سایبری، ابتدا باید تفسیر صحیح از حمله و زور را مشخص شود. «ماده ۲» (بند ۴) منشور ملل متحد چکیده تلاش‌های بشری برای نیل به سازوکاری صحیح برای «ممنوعیت توسل به زور» قلمداد می‌شود. این ماده نتیجه تجربه بشری هزاره‌ها برای تحدید زور به‌عنوان ابزار سیاست ملی و محلی بوده است. تلاش‌هایی که پیش از میلاد و با تمدن‌های هلنیستی، ایران و مصر ترتیب داده شد و نمونه آن را می‌توان در پکس رومانا، منشور کورش و غیره مشاهده کرد تا تلاش‌های بشر بعد از میلاد که در دکترین جنگ عادلانه، دکترین نظام فکری «سنت

آگوستین»[1]، دکترین وستفالیایی، تلاش‌های «جان لاک»[2] و «هوگو گروسیوس»[3]، معاهدات صلح لاهه، جامعه ملل، پیمان‌های لوکارنو و غیره، خود را نشان داده است و ماده ۲ (بند ۴) خلاصه‌ای از همه آن تلاش‌ها برای محدودیت و ممنوعیت توسل به زور بوده است.

۱-۱. تفسیر ماده ۲ (بند ۴) منشور

برای فهم اینکه عملیات سایبری می‌تواند ذیل عنوان «توسل به زور» که در قاعده «ممنوعیت توسل به زور» ماده ۲ منشور ملل متحد ترسیم شده است؛ گنجانده شود یا خیر، ابتدا باید مشخص شود که «زور نظامی» چیست و چه تفسیری از زور توسل به همه انواع آن را در بر می‌گیرد؟ حقوق بین‌الملل نشان می‌دهد؛ درحالی‌که تعریف زور باید به نوع نظامی آن محدود شود؛ باید تفسیر موسعی از تعریف زور نظامی صورت گیرد. «ایان براونلی»[4] از یک تعریف دوبخشی که نیاز به «سلاح» دارد استفاده کرده و «از بین بردن زندگی و اموال مردم» به‌عنوان معرف سلاح به‌کار رفته است. «باوت»[5] به توسل احتمالی به تسلیحات خشونت‌آمیز اشاره می‌کند که «صدمات انسانی» به بار می‌آورد. یکی از دلایلی که برای تعریف سلاح به این ابعاد «پیامدمحور» توجه شده است؛ ورود تسلیحات شیمیایی و میکروبی، به‌عنوان ابزارهای نظامی در قرن بیستم بوده است؛ بنابراین و به‌طورکلی برای توضیح «زور» دو رویکرد «پیامدمحور» و «چهارچوب-ابزارمحور» وجود دارد (Heather harrison, 2012, p. 46). منظور از رویکرد پیامدمحور، دیدگاه غایت‌محورانه است که ناظر به تأثیر نهایی زور است و منظور از دیدگاه چهارچوب-ابزارمحور این است که مستقل از پیامد و نتیجه نهایی، ممنوعیت شامل هرگونه ابزار و چهارچوبی می‌شود که در آن از زور استفاده شده است. در اینجا دو دیدگاه در «تفسیر موسع از زور» و «تفسیر مضیق از زور» بررسی می‌شود؛ یکی از مواد مترقی که محصول تلاش‌های بسیار حقوق‌دانان و یک رویه قوی بین‌المللی برای ممنوعیت توسل به زور است؛ ماده ۲ (۴) منشور سازمان ملل متحد است. از این ماده تفاسیر مختلفی صورت گرفته است.

1. Saint Augustinus
2. John locke
3. Hugo Grotius
4. Ian Brownlie
5. Bowett

۱-۱-۱. تفسیر موسع از زور

در این تفسیر زور به‌مثابه کلیه اشکال فشار ممنوع است؛ از جمله آن‌هایی که به‌صورت سیاسی و اقتصادی ترتیب داده می‌شود و تأثیر تهدیدآمیزی برای تمامیت ارضی یا استقلال سیاسی هر کشور دارد (Farer, 1985, p. 405- 408.) .این تفسیر موسعی از ماده ۲ (بند ۴) است که کشورهای غیر غربی نظیر کشورهای بلوک شرق و دیگر کشورها، درست از زمان کنفرانس سان‌فرانسیسکو مطرح کرده‌اند. نویسندگان پیرو این مکتب، شامل ایان براونلی، «یورام دینستاین[1]»، «کریستین گری»[2] و در خصوص حمله شبکه رایانه‌ای، «جیمز باند» در این گروه قرار می‌گیرند (Harrison Dinniss, 2012, p. 47). این یک تفسیر غایت‌مند از ماده ۲(بند ۴) است که با رویکرد ابزارمحور تفسیر آن کاملاً متفاوت است. این رویکرد نه‌تنها زور و برخورد نظامی، بلکه به‌طورکلی کاربرد زور و انواع دیگر برخوردها، نظیر برخوردهای سیاسی، اقتصادی و غیره را ممنوع می‌کند. این رویکرد همچنین کشورهای جهان سوم را به هدفشان می‌رساند؛ هدفی که کشورهای توسعه‌یافته را به وارد آوردن فشار و همان برخورد نظامی نظیر تحریم‌ها یا محدودیت‌ها علیه آن‌ها متهم می‌کنند (Yorman 1994, p. 18), (Kelsen, 1956), (Rifaat, 1980).

۱-۱-۲. تفسیر مضیق از «حمله»

برخلاف تفسیر موسع غایت‌محور از ماده ۲ (۴) منشور ملل متحد، کشورهای توسعه یافته یا بلوک غرب نظیر آمریکا و متحدان آن، تفسیر مضیقی مطرح کرده‌اند که می گوید ماده ۲ (درباره اصل عدم توسل به زور) و ماده ۵۱ متعاقب آن (درباره دفاع) بازگشتی است به استفاده از زور «مسلح»، «نظامی» و «فیزیکی». حامیان این رویکرد بر این باورند که موضوع و هدف منشور سازمان ملل و مواد آن، یعنی مواد ۴۱، ۴۲ و ۵۱ که تدابیر شورای امنیت را به رسمیت می‌شناسند؛ برای برخوردهای سیاسی و اقتصادی نیست؛ بلکه فقط نیروهای نظامی را در بر می‌گیرند. از دیدگاه قائلان به این تفسیر، بحث‌های متضاد موجود راجع به محدودیت خاص در ماده ۵۱ درباره «حملات مسلحانه» نشان می‌دهند؛ تدوین‌کنندگان، ممنوعیت «زور» را به‌عنوان مقوله‌ای وسیع تر که به روش‌های عام غیرنظامی تسری می‌یابد در نظر نداشته‌اند و برعکس آن، روح منشور را لحاظ کرده‌اند که به‌طورکلی درباره تمهیدات در سرتاسر منشور و حاکی از توجه دقیق‌تر به زور نظامی است نه ابزارهای دیگر توسل به قدرت یا فشار. اینان

1. Yoram Dinstein
2. Christine Gray

همچنین بر آن هستند که باید علاوه بر موضوع، به هدف شارحان منشور و جامعه شناسی حقوقی منشور توجه داشت (Waxman, 2011, p. 46). قائلان به تفسیر مضیق از زور بر آن‌اند که شارحان و مفسران منشور همگام با «تعریف محدود از زور»، «تعریف محدود از تجاوز» را نیز پیش برده‌اند. در سال‌های اولیه تدوین و در پی تفسیر منشور، بحث‌های مشابه با آن بر سر تعریف ماده ۲ (۴) از «زور» نیز در مجمع عمومی مطرح شده و این بحث‌ها به سوءبرداشت از ممنوعیت «تجاوز» نیز سرایت کرده است. آمریکا و متحدان غربی آن تعریف مضیقی از «تجاوز» را مطرح کرده‌اند که بر حملات نظامی تأکید می‌کرد؛ درحالی‌که کشورهای درحال‌توسعه از تعریف موسعی حمایت می‌کردند که اشکال دیگر برخورد یا فشار اقتصادی را در بر می‌گرفت (Waxman, 2011, p. 46).

۱-۲. استفاده نظامی و غیرنظامی از زور فیزیکی

آیا ماده ۲ (۴) می‌تواند انواع دیگر زور و حملات را در برگیرد؟ عامل «نظامی» در این سطح بسیار مهم است؛ چون آن را از دیگر اشکال فشارها و نیروها نظیر فشار اقتصادی و سیاسی متمایز می‌کند و از طرف دیگر این همان نیروی نظامی فیزیکی است که می‌تواند طبق ماده ۲ (۴) همان تفسیر مضیق از ممنوعیت توسل به زور تلقی شود. هنگامی‌که یک دولت از مواد بیولوژیکی یا شیمیایی نه به‌عنوان سلاح نظامی بلکه به‌مثابه ابزاری علیه کشور دیگر استفاده کند که می‌تواند پیامدهای زیان‌باری در برداشته باشد؛ احتمالاً به سبب به بار آوردن صدمات و تلفات متوسل به زور شده است. هرچند این کار در ظاهر استفاده فیزیکی از ادوات و سلاح‌ها یا حتی زور نظامی تلقی نمی‌شود؛ ولی می‌تواند مشمول ماده ۲ (۴) شود. بنابراین، «در برخی شرایط، استفاده خصمانه از اشکال غیرنظامی زور فیزیکی می‌تواند مشمول ماده ۲ (۴) شود؛ به‌ویژه اگر نتایجی عظیم مثلاً معادل یک حمله اتمی به بار آورد که طبق ماده ۵۱ حق دفاع از خود را خواهد داشت» (Silver, 2002, p.82). دیوان بین‌المللی دادگستری در قضیه نیکاراگوئه خبر داد: «تصمیم بر این بوده و ایالات متحده آمریکا به‌وسیله آموزش، تسلیح، تجهیز، تأمین مالی و حمایت از نیروهای کنترا یا به‌صورت دیگر با تحریک، پشتیبانی و کمک به فعالیت‌های نظامی و شبه‌نظامی در نیکاراگوئه، علیه آن کشور اقدام کرده است؛ البته طبق حقوق بین‌الملل عرفی این اقدام آمریکا نقض تعهد مبنی بر عدم مداخله در امور داخلی کشور دیگر به شمار می‌رود»[1]. بنابراین «با اینکه حمله مسلحانه رخ نداده است؛ طبق حقوق بین‌الملل عرفی مداخله در امور داخلی کشور

1. http://www.icj-cij.org/docket/?sum=367&p1=3&p2=3&case=70&p3=5

دیگر نقض تعهد بین‌المللی» است. در این شرایط «توسل به زور فیزیکی غیرنظامی در مخاصمات بین‌المللی توسط یک کشور وقتی از نظر تأثیر مخرب فیزیکی آن‌ها (خواه به‌موجب ضوابط یک حمله مسلحانه باشد یا خیر)، به‌اندازه کافی با زور نظامی شباهت داشته باشد؛ می‌تواند مشمول ماده ۲ (بند ۴) شود» (Silver, 2002, p. 82). نمونه تسلیحات بیولوژیکی و شیمیایی بیانگر این است که «سطح و عمق آسیب‌رسانی و میزان خسارت وارده، رویکرد مناسبی برای تفسیر است.»

۱-۳. سلاح

هر آنچه را که «باعث خسارت فیزیکی و صدمات انسانی شود» سلاح می‌نامند. این تعریف در میان تعاریف مختلف، نزدیک‌ترین تعریف به برداشت پژوهش از سلاح است (Silver, 2002, p. 82). در خصوص تعریف سلاح نیز دو رویکرد وجود دارد؛ نخست رویکرد مضیق و دوم رویکرد موسع. رویکرد مضیق بر آن است که تنها سلاح‌های نظامی جزو سلاح محسوب می‌شوند؛ درحالی‌که رویکرد دوم مستقل از ابزار و ادوات، آثاری را که هر ابزار به بار می‌آورد؛ عنصر تعیین‌کننده‌ای برای تعریف سلاح در نظر می‌گیرد. در همین خصوص می‌توان به مثال متعارف چاقو اشاره کرد. چاقو تا زمانی که در دست آشپز است؛ ابزاری برای کار و آشپزی است؛ اما هنگامی‌که یک تبهکار از آن استفاده می‌کند به‌عنوان ابزار صدمه استفاده می‌شود؛ بنابراین آنچه در اینجا به‌عنوان سلاح اهمیت دارد؛ نتیجه‌ای است که از آن به دست می‌آید.

۲. حملات سایبری، به‌مثابه سلاح

نخستین سند بین‌المللی که به قانونمند کردن سلاح‌های حاصل از پیشرفت‌های فناوری پرداخت؛ بیانیه ۱۸۶۸ سن‌پترزبورگ بود. طبق این بیانیه «هیچ ضرورتی ندارد که اقدامات یک طرف درگیری سبب تشدید رنج یا ناتوانی نیروی نظامی طرف مقابل شود؛ پس هر سلاحی که به این امر منتهی شود؛ مغایر حق انسانی است». ۸۰ سال بعد، اعضای متعاهد پروتکل اول الحاقی ۱۹۷۷ به کنوانسیون‌های چهارگانه ژنو ۱۹۴۹، ماده‌ای تحت عنوان «سلاح‌های جدید» (ماده ۳۶) در پروتکل گنجاندند. این ماده دولت‌ها را موظف می‌کند قبل از به‌کارگیری هر سلاح، ابزار یا روش نوین جنگی، از قانونی بودن آن اطمینان حاصل کنند. به‌علاوه از دولت‌ها می‌خواهد در هر مرحله‌ای از مطالعه، توسعه، کسب و پذیرش سلاح، ابزار یا روش‌های جدید جنگی، آن‌ها را با قواعد موجود در پروتکل یکم الحاقی و قواعد حقوق بین‌الملل قابل اعمال مطابقت

دهند تا بتوانند قانونی بودن یا غیرقانونی بودن آن را تعیین کنند (شریفی، ۱۳۹۹: ۱۲۵). در این تعریف، نه نگاه ابزارگرایانه به سلاح، بلکه شرایط به‌کارگیری آن سلاح است که آن را مشمول قانونی بودن یا غیرقانونی بودن می‌کند. ماده ۳۶ به این موضوع اشعار دارد که به‌کارگیری یک سلاح، ابزار یا روش جدید جنگی ناقض حقوق بین‌الملل ممنوع است (Boulanin, 2015). تحولات تکنولوژیک سبب شده تا نیاز به قانون‌گذاری و شکل‌گیری رویه جدید در حقوق بین‌الملل احساس شود.

در اینجا این پرسش مطرح است که چه عاملی به سلاح جنبه «نظامی» می‌دهد؟ در پاسخی کوتاه به این پرسش باید گفت که «وقتی سلاح، ابزار یا حتی یک فناوری (بدون آنکه ذاتاً آسیب‌زا باشد) می‌تواند سبب وارد آمدن صدمه جانی یا خسارت مادی شود؛ به شکلی زور نظامی یا مسلح را تشکیل می‌دهد» و در نتیجه می‌تواند مشمول ماده ۲ (۴) قرار گیرد و توسل به زور تلقی شود (Silver, 2002, p. 8). دستورالعمل تالین که توسط گروه بین‌المللی حقوق‌دانان درباره حقوق بین‌الملل فضای سایبر ارائه شده؛ در مواد مختلف از جمله قاعده ۴۲ به مسئله حملات سایبری و عملیات سایبری بر اساس تعریف اشاره کرده است (Tallin, 2013, p. 118).

پرسش بعدی این است که چگونه می‌توان گفت که یک فناوری جدید، نوعی زور نظامی یا زور مسلح یا حمله مسلحانه جدید است؟ پاسخ مناسب مربوط به نکته‌ای است که پیش‌تر به آن اشاره شد؛ یعنی رویکرد نتیجه‌محور. به این معنا رفتار بعدی کشور در چهارچوب و نتیجه شرایطی است که حمله اتفاق بیفتد و مسئله این است که آیا این فناوری با انواع دیگر اهداف نظامی یا تخاصمی کشور مرتبط است یا خیر!

برای اطلاق عنوان «حمله» به حملات سایبری ناگزیر باید رویکردی را اتخاذ کرد که ویژگی‌های حمله را به‌طور دقیق برشمرد و بررسی کند. مقررات حقوق بین‌الملل عرفی و معاهده‌ای شبیه به پروتکل یکم الحاقی، معاهدات خلع سلاح، قواعد مربوط به عدم مداخله و غیره قابل اعمال به فضای سایبری نیز هستند. فعل یا ترک فعل متخلفانه یک دولت، زمانی «حمله» محسوب می‌شود که متفاوت با اقدامات عادی و با «شدت» همراه باشد. «خسارت»، «شدت»، «فوریت» و «مصدومیت» از جمله مسائلی هستند که این موضوع را تأیید می‌کنند. برخی از این ویژگی‌ها که در آرای محققان حقوق بین‌الملل دسته‌بندی شده است، به قرار زیر است:

۲-۱. شدت خسارات و صدمات

طبق این شرایط اگر عمل یا ترک فعلی سبب کشته شدن افراد یا ورود خسارات مادی فراوان یا اندکی شود؛ آن عمل احتمالاً نظامی است؛ هراندازه آسیب کمتر باشد؛ احتمال اقدام نظامی ضعیف‌تر است. شدت خسارت می‌تواند تمام شرایط حمله را توضیح دهد. شدت حمله می‌تواند تأیید کند که مثلاً یک اقدام سایبری ذیل حمله سلاح‌های سایبری قرار گیرد و حمله شبکه‌ای کامپیوتری تا چه اندازه تأثیرات خسارت‌بار و پیامدهای بعدی فوری دارد. شدت حمله است که می‌تواند مستقل از نگاه ابزارگرایانه، یک حمله شبکه‌ای کامپیوتری را در ذیل حمله مسلحانه قرار دهد و میزان تخریب و آثار حمله را تهدیدی برای امنیت ملی، تمامیت ارضی و استقلال سیاسی قلمداد کند.

۲-۲. فوریت پیامدهای حمله

فعل یا ترک فعلی که تأثیراتش، ظرف چند ثانیه یا چند دقیقه مشاهده می‌شود (هنگام انفجار بمب یا تشعشعات هسته‌ای ناشی از حمله سایبری به یک نیروگاه هسته‌ای)، عملیات احتمالاً نظامی است؛ اگر آثار حمله طی هفته‌ها و ماه‌ها ظاهر شوند؛ آن عمل به‌احتمال بسیار اقتصادی یا سیاسی است؛ بنابراین سرعت آثار مخرب در ویژگی «سلاح» بسیار اهمیت دارد (Schmitt, 2013).

۲-۳. هدف مستقیم

فعل یا ترک فعلی را که تنها علت نتیجه حاصل باشد؛ می‌توان ذیل توسل به زور یا حمله مسلحانه قرار داد. به عبارتی وقتی پیوند بین علت و تأثیر آن محکم باشد؛ نشانه ماهیت نظامی آن اقدام است. یکی از مهم‌ترین تلاش‌ها برای مقررات‌زایی عملیات سایبری، دستورالعمل تالین ۲۰۱۰ است که سلاح‌های سایبری را بر اساس «صدمه، خسارت، تخریب یا انهدام» تعریف کرده است (Tallin, 2013, p. 118).

۲-۴. تهاجمی بودن عمل نسبت به کشور هدف

عبور از مرز نیز نشانه عملیات نظامی است؛ اقداماتی که از خارج از مرز کشور هدف انجام می‌شود؛ بیشتر جنبه دیپلماتیک یا اقتصادی دارند.

۲-۵. قابلیت اندازه‌گیری خسارت

اگر بتوان تأثیر عمل را به‌سرعت ارزیابی کرد؛ نظیر عکس‌برداری از «یک حفره آلوده به دود» که به‌عنوان هدف مورد استفاده قرار گرفته؛ عملیات خصلت نظامی قوی خواهد داشت و هر چه فرایند ارزیابی خسارت ذهنی‌تر باشد؛ جنبه دیپلماتیک یا اقتصادی عملیات بیشتر است و هرچه جنبه جنبشی[1] و فیزیکی عملیات بیشتر باشد؛ جنبه نظامی آن بیشتر است. قطعنامه‌های ۱۳۶۸ و ۱۳۷۳ شورای امنیت ملل متحد بلافاصله بعد از حوادث یازده سپتامبر ۲۰۰۱، با ارائه مفهوم «سلاح نامحسوس»، به مسئله سوءاستفاده از سلاح‌هایی به‌عنوان عناصر تعریف‌کننده سلاح اشاره کرده است که می‌تواند به تلفات انسانی و تخریب تجهیزات منجر شود.

۲-۶. مسئولیت

هرچند درباره حملات سایبری مسئله مسئولیت بین‌المللی کمتر پذیرفته می‌شود؛ با این حال اگر کشوری مسئولیت مشهودی در قبال اقدام تخریبی بر عهده بگیرد؛ به احتمال زیاد می‌توان آن را یک اقدام سنتی با برچسب غیرنظامی دانست (Schmitt, 2013), (Strwltov, 2015, pp191-192), (Boulanin, 2015).

بنابراین در قطعنامه‌های ۱۳۶۸ و ۱۳۷۳ شورای امنیت در خصوص سلاح به پیامدهای خشونت‌آمیزی شبیه به آسیب، انهدام، مرگ، جراحت و غیره اشاره شده است. اگر وقوع آثاری همچون جراحت، مرگ، ضرر و زیان، آسیب و غیره که در فضای فیزیکی دولت را به جبران خسارت وامی‌دارد؛ در فضای سایبر نیز اتفاق بیفتد؛ همان مقررات ناظر به فضای فیزیکی بر آن نیز ساری و جاری خواهد بود. درباره حقوق بشردوستانه بین‌المللی اگر سلاح‌هایی با ویژگی‌های پیش‌گفته توسط دولتی استفاده شود، مسئله ممنوعیت یا قانونی نبودن آن‌ها پیش می‌آید (ضیائی بیگدلی، ۱۳۹۲: ۲۶۶). از یک منظر نیز برای ارائه تعریفی مناسب از سلاح سایبری می‌توان بر سه عنصر مهم تأکید کرد: ۱. بستر: به این معنی که سلاح سایبری باید در چهارچوب فعلی از جنگ سایبری به کار گرفته شود. می‌توان این مفهوم را درگیری میان بازیگران ملی یا غیرملی توصیف کرد که مشخصه آن استفاده از سامانه‌های اطلاعاتی فناورانه با هدف به دسته آوردن، حفظ یا دفاع از شرایط راهبردی، عملیاتی یا مزیت تاکتیکی است؛ ۲. قصد: ورود خسارت فیزیکی (حتی غیرمستقیم) به تجهیزات یا افراد یا خرابکاری یا ورود خسارت مستقیم به سامانه‌های اطلاعاتی هدف با استفاده از سلاح سایبری است و

1. Kenetic

۳. وسیله یا ابزار: حمله از طریق کاربرد سامانه‌های اطلاعاتی فناورانه از جمله اینترنت انجام می‌شود. به نظر می‌رسد این‌ها تنها عناصر مورد استفاده برای تعیین مجموعه‌ای از ابزارهای رایانه‌ای با عنوان سلاح است (شریفی، ۱۳۹۹: ۱۳۴).

۳. مسئولیت دولت وفق حمله سایبری

برای تشریح مسئله مسئولیت دولت ابتدا باید عنصر شناسایی حمله‌کننده سایبری بررسی شود و سپس به انتساب حمله و سرانجام به مسئولیت دولت وفق این انتساب برای جبران خسارت یا آسیب ناشی از فعل سایبری یا ترک فعل سایبری متخلفانه استناد شود.

۳-۱. معمای شناسایی حمله‌کننده سایبری

دو معمای مهم درباره حملات سایبری، نخست معمای شناسایی حمله‌کننده سایبری و دوم معمای انتساب حمله به حمله‌کننده است. اگر حمله‌ای به‌عنوان حمله سایبری شناسایی و سپس طبق ماده (۲)، منشور سازمان ملل مشمول توسل به زور شود؛ می‌تواند برای دولت مسئولیت ایجاد کند؛ بنابراین، اولین اقدام مسئله شناسایی و عامل آن است. پیچیدگی شناسایی حملات سایبری، آنجایی قابل فهم‌تر است که توجه شود مسئله عاملیت در حملات هنوز با اجماع حدی همراه نیست. انتساب حمله سایبری به یک بازیگر خاص (یک کشور، یک گروه، سازمان یا شخص) یکی از مهم‌ترین مسائل در این زمینه است. واژه «ناشناس»[1] در بیشتر فعالیت‌ها در زمینه اقدامات شبکه کامپیوتری به‌کار می‌رود؛ تا آنجا که میزان فعالیت‌های آشکار از فعالیت پنهانی کمتر است؛ اما چند فعالیت مانند حمله و تهدید به حمله را می‌توان در فضای سایبری به‌عنوان اقدام یک بازیگر خاص شناسایی کرد.[2] هرچند بین ابعاد حمله و شناسایی آن یک رابطه علت و معلولی وجود دارد؛ با وجود این، اکثر اعمال قابل انتساب ممکن است آشکار نباشند. هرچه ابعاد و تأثیر یک حمله بزرگ‌تر باشد؛ مسئله شناسایی مهاجم مشکل‌تر خواهد بود.

1. Ananymous

۲. نظیر حمله متعارف، فرض بر این است که حمله سایبری و حمله شبکه‌ای کامپیوتری به‌عنوان اقدامات خرابکارانه یک دولت خاص در سطح بین‌المللی به دولت‌ها منتسب هستند.

با توجه به استفاده رایج از «بات نت‌ها»[۱] و تغییرات فراوان IP و سامانه‌های متعدد غیر قابل شناسایی که در حملات شبکه کامپیوتری اتفاق می‌افتد[۲]؛ دشوار است که بتوان با قطعیت گفت؛ موجودی که به نظر می‌رسد هویت مهاجم داشته باشد؛ در واقع حمله‌کننده نهایی است. از تغییر IP می‌توان یا برای پنهان کردن منشأ حمله استفاده کرد یا به‌عمد کوشش نمود که به علت حمله، طرف دیگر سرزنش شود. یک نمونه اولیه از مورد اخیر در سال ۱۹۹۹ اتفاق افتاد؛ وقتی انجام حمله علیه وزارت ترابری آمریکا[۳] انکار شد. به‌ظاهر این حمله از یک سرور در مریلند[۴] توسط پیروان جنبش «فالون گونگ»[۵] صورت گرفت و در واقع، برای از کار انداختن سرورهای مریلند و شبکه وزارت حمل‌ونقل طراحی شده بود و موجب شد «فالون گونگ» مقصر شناخته شود. با این حال، مهاجمان مرتکب اشتباهاتی شدند و ردپای حمله تا یک کامپیوتری آدرس وزارت امنیت عمومی چین زده شد (Healther, 2012, p. 99). بنابراین، شناسایی منشأ حمله سایبری دشوار است و صِرف انجام عملیات سایبری از یک سرزمین خاص برای شناخت منشأ آن به‌عنوان مهاجم کافی نیست و حتی بعد از آن نمی‌تواند در نظام حقوق بین‌الملل برای دولت مسئولیت ایجاد کند.

علی‌رغم این موضوع که در حمله متعارف دولت‌ها نمی‌توانند یا کمتر می‌توانند دخالت در آن حمله را انکار کنند؛ در فضای سایبری انکار دخالت آسان‌تر است؛ برای مثال در جریان حمله DOS استونی، اگرچه رد آدرس IP که در حملات علیه کشور استونی دخالت داشتند تا آدرس IP رسمی مقامات کشور روسیه دنبال شد؛ روسیه هرگونه دخالتی را انکار کرد و مدعی شد که این کامپیوترها به دنبال بدنام کردن روسیه هستند و از خارج کرملین مورد دست‌کاری قرار گرفتند. گزارش‌های بعدی توسط تحلیلگران امنیت سایبری این ادعا را تأیید نمود و به نبود شواهد و امکان تغییر

---

۱. بات‌نت‌ها شبکه‌هایی هستند که با در اختیار گرفتن مجموعه‌ای از کامپیوترها که بات (bot) نامیده می‌شوند؛ تشکیل می‌شوند. این شبکه‌ها را یک یا چند مهاجم که Botmasters نامیده می‌شوند؛ با هدف انجام فعالیت‌های مخرب کنترل می‌کنند. به عبارت بهتر هکرها/ اتکرها (attacker) با انتشار ویروس‌ها و برنامه‌های مخرب به‌صورت غیرقانونی و بدون اطلاع صاحب کامپیوتر کنترل آن را به دست می‌گیرند و با استفاده از مجموعه‌ای از این کامپیوترها درخواست‌های جعلی زیادی را به سمت سرور یا سایت قربانی ارسال می‌کنند که به انجام یک حمله DDoS منجر می‌شود.

۲. از این لحاظ، حمله می.تواند از زیرساخت کشور (الف) انجام شود، مهاجم در کشور (ب) باشد و کنترل سیستم کامپیوتری سلاح سایبری در کشور (ج) باشد.

3. US department of Transport

4. Maryland

۵. فالون گونگ روش تزکیه ذهن و بدن بر اساس سه اصل حقیقت، نیک‌خواهی و بردباری است. این روش از دوران باستان نسل به نسل به‌صورت تزکیه پنهانی و سینه‌به‌سینه از استاد به شاگرد منتقل شد و در سال ۱۹۹۲ به دست «لی هنگ‌جی» در کشور چین عمومی شد. در ۲۰ ژوئیه ۱۹۹۹، با توجه به تعداد زیاد تمرین کنندگان این روش، حزب کمونیست چین آن را ممنوع اعلام کرد و شروع به آزار و شکنجه اعضای آن کرد.

آدرس IP مهاجم اشاره داشتند (Healther, 2012, p. 100)؛ بنابراین اولین مسئله در حملات سایبری حل کردن معمای شناسایی منشأ این حملات است.

۳-۲. مسئله انتساب حملات سایبری به رفتار دولت‌ها

حتی اگر حمله‌ای از کشوری انجام و منشأ آن شناسایی شود؛ نمی‌توان آن را مانند حمله متعارف نسبت داد. وقتی حمله از کار انداختن خدمات (DOS) در سال ۲۰۰۷ علیه استونی اثبات شد؛ تمایز بین حملاتی که منشأ آن از یک نشانی خاص است و حملاتی که صرفاً از یک کامپیوتر آسیب‌دیده نشئت می‌گیرد، بسیار دشوار بود. (Healther, 2012, p. 99). همان‌طور که توسل به سلاح‌های سایبری و حملات سایبری، در حقوق عرفی و معاهده‌ای ممنوع نشده است؛ برای انتساب حملات سایبری به رفتار دولت‌ها باید به سراغ اصول بنیادین موجود در حقوق عرفی و معاهده‌ای رفت و با استفاده از اصول کلی و بنیادین حقوق عرفی و معاهده‌ای بین‌المللی، به تعریف سلاح، شناسایی و غیره در خصوص حملات سایبری پرداخت. همچنین می‌توان و باید با استفاده از اصول بنیادین حقوق بشردوستانه (عرفی و معاهده‌ای) به وضع قواعد و مقرراتی مبادرت کرد که با استفاده از آن‌ها حملات و سلاح‌های سایبری در ذیل مقررات عرفی و قراردادی بین‌المللی قرار گیرد و در همین زمینه بتوان به حقوق سلاح‌های سایبری، مسئله شناسایی حملات سایبری و مسئولیت بین‌المللی دولت‌ها پیرامون آن پرداخت. حقوق مسئولیت بین‌المللی دولت‌ها که مجموعه‌ای از قواعد و مقررات حقوق معاهده‌ای و عرفی بین‌المللی محسوب می‌شود؛ ناظر به مسئولیت بین‌المللی دولت‌ها و سازمان‌های بین‌المللی، در صورت ارتکاب فعل یا وقوع ترک فعل متخلفانه است؛ بنابراین مسئله انتساب حمله، از مسئله شناسایی مهم‌تر است و اهمیت آن نیز به پیچیدگی‌های فنی آن بازمی‌گردد.

مسئولیت در قضیه «کارخانه کروزوف»[1] در رأی دیوان دائمی دادگستری ریشه دارد که دیوان در آن، با تکیه بر موضوع جبران خسارت، به رفتار خلاف دولت اشاره داشت؛ موضوعی که بعدها در قضیه «کانال کورفو[2]» تأیید شد. همچنین در قضیه «کشتی جنگی رنگین‌کمان» در رابطه با اختلاف دولت فرانسه و نیوزلند[3] بیان شد که هر نوع نقض تعهد توسط دولت ناشی از هر تعهد و منهای منشأ آن، مسئولیت دولت

1. The Factory At Chorozow, Germany v. Poland(the merits), 1928 P.C.I.J. (ser.A) No. 17 (sept. 13), available at http://www.worldcourts.com/pcij/ eng/ decisions/1928.09.13=chorzow1.html.
2. Corfo Channel Case, (UK V. Albania), merits,I.C.J Reports,1949,p. 37
3. Gabcikovo-Nagymaros Project(Hungary v. Slovakia),I.C.J. Reports 1997,p. 251, para. 75.

را به دنبال دارد (شریفی، ۱۳۹۹). برای انتساب حملات سایبری به رفتار دولت‌ها باید به سراغ اصول کلی و بنیادین حقوق بین‌الملل رفت و تعین آن را می‌توان در «طرح پیش نویس مواد کمیسیون حقوق بین‌الملل راجع به مسئولیت دولت‌ها نسبت به اعمال متخلفانه بین‌المللی» مشاهده کرد. برای انتساب حمله یا عمل متخلفانه به یک کشور، قوانین کمیسیون حقوق بین‌الملل درباره عمل متخلفانه در فضای سایبری نیز وجود دارد. علاوه بر متخلفانه بودن، یک عمل باید به دولت قابل انتساب باشد تا مقررات ناظر به مسئولیت دولت بر آن اعمال شود. این بخش بر مبنای حقوق بین‌الملل عرفیِ مسئولیت دولت است که در مواد کمیسیون حقوق بین‌الملل درباره مسئولیت دولت مقرر شده است.[۱]

در قلمروِ فضای سایبری، یک عمل متخلفانه بین‌المللی می‌تواند شامل دامنه بسیار وسیعی از قلمروهای حقوق بین‌الملل منشور، حقوق مخاصمات مسلحانه بین‌المللی، حقوق دریاها، حقوق هوا، حقوق بشر و ... را در بر گیرد. از جمله اینکه این حملات می تواند شامل نقض منشور سازمان ملل (توسل به زور از طریق تمهیدات سایبری) یا نقض تعهد حقوق مخاصمات مسلحانه (حمله سایبری علیه اهداف یا اشخاص غیرنظامی و به‌طورکلی کنوانسیون‌های چهارگانه ژنو و پروتکل‌های الحاقی ۱۹۷۷ به آن‌ها) یا نقض قوانین صلح که مخاصمه را در بر نمی‌گیرد (نقض حقوق دریایی[۲] یا اصل عدم مداخله)؛ تلقی شود. [۳]

منحصربه‌فرد بودن اقدامات سایبری به این دلیل است که حملات سایبری می توانند پنهانی باشند و دولت‌ها ممکن است دیگر بازیگران یا سایر بازیگران غیردولتی را به انجام حمله تحریک کنند. ایجاد یک رژیم حقوقی بین‌المللی دائمی برای تعریف مسئولیت دولت در حقوق بین‌الملل که قابل دسترس باشد؛ ضروری است.

حقوق مسئولیت بین‌المللی دولت تنها به عمل یا ترک عملی تسری می‌یابد که حقوق بین‌الملل را نقض می‌کند؛ به عبارت دیگر، یک عمل ارتکابی یک نهاد دولتی یا عمل قابل انتساب به آن را می‌توان به‌حساب «یک عمل متخلفانه بین‌المللی» گذاشت؛ البته اگر آن عمل مغایر با حقوق بین‌الملل باشد. برای نمونه، حقوق بین‌الملل فی‌نفسه

---

۱. باید اشاره شود که حقوق مخاصمات مسلحانه حاوی چندین مقررات خاص راجع به مسئولیت دولت به خاطر نقض آن است؛ به‌خصوص، ماده ۳ کنوانسیون چهارم لاهه و ماده ۹۱ پروتکل ۱ الحاقی موضوع غرامت در مورد نقض مقررات خاص حقوق جنگ مسلحانه را مطرح می‌کنند (مواد راجع به مسئولیت دولت).

۲. کنوانسیون حقوق دریایی، ماده ۱۹.

۳. به‌عنوان مثال، کشتی جنگی یک کشور هنگام عبور بی‌ضرر از آب‌های کشوری دیگر حق انجام عملیات سایبریِ مغایر با منافع ملی دولت ساحلی را ندارد (Schmitt, 2013, p. 30).

به عمل جاسوسی نمی‌پردازد. از این‌رو، مسئولیت دولت به خاطر یک عمل جاسوسی سایبری که توسط یک نهاد دولتی در فضای سایبری انجام می‌شود؛ با موضوع حقوق بین‌الملل سروکار ندارد؛ مگر اینکه جنبه‌های خاص جاسوسی، ممنوعیت حقوقی بین‌المللی ویژه‌ای را نقض کند (مثلاً در مورد جاسوسی سایبری که مستلزم ارتباط دیپلماتیک باشد)(Schmitt, 2013, p. 30). حقوق مسئولیت بین‌المللی دولت را باید بر اساس منشأ حمله، اینکه یک حمله با همکاری شرکت‌های ارائه‌دهنده خدمات سایبری صورت گرفته و میزان کنترل دولت بر روی آن شرکت تا چه حد است؛ تفسیرپذیر و به لحاظ منشأ و کاربرد متفاوت است.

۳-۲-۱. انتساب اعمال ارتش‌های سایبری

«ماده ۴» «پیش‌نویس مواد راجع به مسئولیت دولت‌ها بابت اعمال متخلفانه بین‌المللی»، با عنوان «رفتار نهادهای یک دولت» تأکید می‌کند «عمل یک نهادِ دولتی باید عمل آن دولت طبق حقوق بین‌الملل به شمار رود؛ آن نهاد وظایف قانون‌گذاری، اجرایی، قضایی یا سایر وظایف را انجام دهد و در هر موقعیتی باشد؛ در تشکیلات دولت است و ماهیت آن هرچه باشد، به‌عنوان نهاد دولت مرکزی یا یک واحد سرزمینی آن دولت است». یک «نهاد دولتی شامل شخص یا سازمانی است که طبق قانون داخلی کشور آن جایگاه را دارد». در داوری دهم دسامبر ۲۰۰۵ درباره «فعالیت‌های مسلحانه در سرزمین کنگو (شکایت جمهوری دموکراتیک کنگو علیه اوگاندا[1])»، این مسئله مطرح شد که آیا اقدامات «جنبش آزادی‌بخش کنگو[2]» که یک گروه شورشی محسوب می‌شد در سرزمین جمهوری دموکراتیک کنگو، قابل انتساب به اوگاندا هست یا خیر. سرانجام دیوان به این نتیجه رسید که هیچ شواهد معتبری وجود ندارد که نشان دهد اوگاندا جنبش آزادی‌بخش کنگو را ایجاد کرده است. اوگاندا تأیید کرده که آموزش و پشتیبانی نظامی داده است و شواهدی دال بر آن وجود دارد؛ ولی دیوان صحت شواهد را تأیید نکرده است که اوگاندا بتواند استفاده آقای «ژان پیر بمبا[3]» از این کمک‌ها یا خود او را در کنترل خویش درآورد. از نظر دیوان، رفتار جنبش آزادی‌بخش کنگو «آلتِ دست» بودن اوگاندا را تأیید نمی‌کند (ماده ۴ پیش‌نویس مواد کمیسیون حقوق بین‌الملل راجع به مسئولیت دولت‌ها وفق اعمال متخلفانه بین‌المللی ۲۰۰۱) (Armed

1. ICJ Reports 2005.The Armed Activities on the Territory of the Congo Case (Democratic Republic of Congo v. Uganda).
2. Congo Liberation Movement
۳. معاون رئیس جمهور سابق جمهوری دموکراتیک کنگو.

Activities "Judgment", P. 226, Para 160)؛ بنابراین دیوان با استناد به ماده ۴ پیش‌نویس مسئولیت، استناد کرد که رفتار جنبش آزادی‌بخش کنگو قابل انتساب به رفتار دولت اوگاندا نیست و به همین دلیل در شکل‌گیری این نیرو و کنترل آن به دست اوگاندا تأیید نمی‌کند که عمل متخلفانه‌ای صورت گرفته باشد و دیوان این انتساب را تأیید نمی‌کند.

مفهوم «نهادِ یک دولت» به حقوق مسئولیت دولت تسری یافته است. هر شخص یا سازمانی که آن جایگاه را طبق قوانین داخلی کشور در اختیار دارد؛ صرف‌نظر از کارکرد یا جایگاه آن در سلسله‌مراتب حکومتی، نهادی از آن کشور خواهد بود[1]. هر فعالیت سایبری که توسط نهادهای اطلاعاتی، نظامی، امنیت داخلی، گمرکات یا دیگر نهادهای دولتی صورت می‌گیرد؛ اگر آن نهاد تعهد حقوقی بین‌المللی قابل اجرا برای آن کشور را نقض کند؛ طبق حقوق بین‌الملل دارای مسئولیت دولتی خواهد بود. آرای دیوان بین‌المللی دادگستری در خصوص اقامه دعوی گروگان‌گیری آمریکا علیه ایران، مفهوم نهاد را بسط داده است.

مهم نیست که نهاد مورد نظر منطبق با دستور، فراتر از دستور یا بدون آن عمل کرده است یا نه؛ وقتی نهادی دولتی عملی را مرتکب شده باشد؛ مشروط بر اینکه آن نهاد با جایگاه رسمی خود آشکارا عمل کند؛ حتی اگر به‌اصطلاح خارج از اختیارات قانونی اقدام کند؛ اگر نقض تعهدات بین‌المللی باشد؛ برای آن دولت مسئولیت حقوقی بین‌المللی ایجاد می‌کند (Schmitt, 2013, p. 31). بررسی‌های تاریخی نشان می‌دهد که تعریف نهاد و کاربرد آن گسترده و نگاهی به آرای دادگاه‌ها مؤید مفهوم‌سازی است. دیوان بین‌المللی دادگستری در قضیه «فعالیت‌های مسلحانه در سرزمین کنگو (شکایت جمهوری دموکراتیک کنگو علیه اوگاندا)» در سال ۲۰۰۵ و اجرای کنوانسیون جلوگیری و مجازات نسل‌کشی (در دعوای بوسنی و هرزگوین علیه صربستان و مونته‌نگرو) [2] در سال ۲۰۰۷، نهاد را بار دیگر مفهوم‌سازی کرده است.

امروزه بعد از زمین، دریا، هوا و فضا، «فضای سایبری» حوزه دیگر مداخله و جنگ قلمداد می‌شود و به دلیل اهمیت آن در قرن ۲۱، قدرت‌ها سعی می‌کنند به پنجمین بُعد از جنگ در میدان نبرد البته به‌وسیله کامپیوترها دست یابند. به این ترتیب، هر دولتی سعی می‌کند امنیت، برنامه، ارتش، پدافند، استراتژی‌های سایبری و ... را طراحی

1. Draft Articles on State Responsibility, Art. 4 (2).
2. Judgment, Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), International Court of Justice, 26 February 2007, available online at: http://www.icj-cij.org/docket/files/91/13685. pdf (hereinafter 'Judgment')

کند. انتساب فعل یا ترک فعل متخلفانه بین‌المللی ارتش‌های سایبری به دولت آسان‌ترین مسیر مسئولیت بین‌المللی دولت وفق یک عمل متخلفانه سایبری است. در این خصوص می‌توان به هکرهای «خودسر» اشاره کرد که این واحدهای سایبری جزء نهادها و کارگزاران دولت‌ها به شمار می‌روند. کلیه اعمال یا ترک افعال نهادهای یک دولت خودبه‌خود و ضرورتاً قابل انتساب به آن دولت هستند. [1]

۳-۲-۲. عناصر اقتدار سایبری دولت

«ماده ۵» پیش‌نویس با عنوان «رفتار افراد یا نهادهایی که عناصری از اقتدار دولتی را اعمال می‌کنند»؛ توضیح می‌دهد: «رفتار شخصی یا نهادی که بر اساس ماده ۴ نهاد دولتی نیست؛ اما از سوی قانونِ آن دولت، مجاز به اعمال عناصر اقتدار دولتی است؛ باید طبق حقوق بین‌الملل به‌عنوان عمل دولتی محسوب شود؛ مشروط بر آنکه شخص یا نهاد در موارد خاص به آن عمل کند.»

دیوان پس از رد استدلال جمهوری دموکراتیک کنگو مبنی بر اینکه جنبش آزادی بخش کنگو را می‌توان مطابق با ماده ۴ مقررات به‌عنوان یک «نهاد» اوگاندا در نظر گرفت؛ به نتیجه رسید رفتار اعضای جنبش آزادی‌بخش کنگو را نمی‌توان به اوگاندا منتسب کرد؛ زیرا بر اساس مقرراتی که بیان می‌دارد؛ از [نظر] دیوان، رفتار جنبش آزادی‌بخش کنگو رفتار «یک نهاد» اوگاندا (ماده ۴) و همچنین نهادی که از جانب آن عناصر اقتدار حکومتی را اعمال نماید (ماده ۵)، نیست. دیوان اشعار می‌دارد «اقدامات ایجادکننده نسل‌کشی توسط اشخاص یا نهادهای جمهوری فدرال یوگسلاوی سابق ارتکاب نیافته، بلکه از طریق اعمال عناصر اقتدار حکومتی که صاحب قدرت بودند ارتکاب یافته بود (ماده ۵)» (Armed Activities, 2005 "Judgment").

هکرها می‌توانند نهادهای دولت و در عین حال عضو شرکت‌ها و بخش خصوصی کشور باشند که از طریق قانونِ آن دولت، صاحب‌اختیار و قدرت شده‌اند و عناصری از اقتدار دولتی خود را اعمال می‌کنند. آن‌ها الزاماً نهادهای دولتی نیستند؛ اما به‌موجب قانونِ آن دولت، به‌منظور اعمال عناصر اقتدار دولتی مجاز شده‌اند. برای انتساب حمله سایبری به حمله‌کننده، هکرها می‌توانند نیمه‌دولتی، نیمه عمومی، اعضای نهادهای عمومی، اعضای نهادهای دولتی و به‌عنوان نهادهای شبه‌دولتی باشند که می‌توانند از طریق قانون دولت مبدأِ خود، برای اعمال عناصر اقتدار آن دولت، مجاز شده باشند.

1. Draft Article on State Responsibility, Art. 4 (1)

رفتار هکر در این مورد به دولت قابل انتساب است؛ چراکه دولت «شخص یا سازمان را مهیای اقدام در چنین جایگاهی در موارد خاص می‌کند».

تیم‌های پاسخ‌گویی به حوادث کامپیوتری[1] که «کمک‌های اولیه واکنش اضطراری و خدمات تریاژ را به قربانیان یا قربانیان احتمالی عملیات سایبری یا جرائم سایبری ارائه می‌دهند و معمولاً به شیوه‌ای عمل می‌کنند که شامل هماهنگی میان بخش ارائه‌دهنده و نهادهای دولتی است»؛ یک نمونه از نهادهای مجاز به استفاده از اقتدار دولتی در زمینه سایبری هستند (Roscini, 2014, p. 35). دولت‌ها می‌توانند بخش خصوصی یا برخی از داوطلبان را برای حمله سایبری به یک دولت دیگر تحریک کنند؛ بنابراین، رفتار آن‌ها تحت اعمال عنصر اقتدار دولتی قرار می‌گیرد و به عبارتی، برخلاف نماینده دولت تحت ماده ۸ مفاد طرح کمیسیون حقوق بین‌الملل، انتساب طبق ماده ۵ تا زمانی که قانون داخلی برخی از توابع دولتی را به فرد یا نهاد مورد نظر سپرده است؛ مستلزم آن نیست که اقدامات تحت کنترلِ «مؤثر» مقامات دولتی یا در راستای آن محدودیت‌ها صورت پذیرند. در این زمینه می‌توان به شرکت‌های خصوصی اشاره کرد که از سوی دولت مسئول عملیات سایبری علیه دولت‌های دیگر هستند.

با این حال، این موضوع تحت کنترل و محدودیت مؤثر دولت نیست؛ اما برای ایجاد مسئولیت دولت، عناصر عملیاتی اقتدار دولتی ضروری است. به‌عنوان مثال، دولت ممکن است قوانینی برای مجاز نمودن تیم‌های پاسخ‌گویی به حوادث کامپیوتری برای انجام دفاع سایبری از شبکه‌های دولتی داشته باشد. حال اگر آن شرکت در این قالب فعالیت کند؛ فعالیت‌هایش به‌طور خودکار مسئولیت دولت حمایت‌کننده خود را درگیر می‌کند. در عین حال اگر یک تیم پاسخ‌گویی به حوادث کامپیوتری بخش خصوصی، خدمات امنیت اطلاعات را برای شرکت‌های خصوصی انجام می‌دهد؛ هیچ‌گونه مسئولیت دولتی وجود ندارد (Schmitt, 2013, p. 31).

واحد سایبری نیروهای دفاع ملی استونی[2] نمونه خوبی در این زمینه است. این واحد، یک سازمان متشکل از برنامه‌نویسان، دانشمندان کامپیوتر و مهندسان نرم‌افزاری و غیره یک سازمان داوطلب است که در زمان جنگ تحت فرماندهی متحد نظامی عمل می‌کند (Gjelten, 2011). وزیر دفاع وقت استونی، «جاک آویکسو» در این زمینه گفته است: «انجمن [ما] متخصصان در دفاع سایبری را که در بخش خصوصی و

1. National Computer Emergency Response Teams (CERTs)

۲. سازمانی شبه‌نظامی است که بخشی از ارتش استونی محسوب می‌شود. این سازمان ۲۱،۵۵۱ نفر پرسنل دارد که در ۱۵ بخش در کشور استونی به انجام وظیفه می‌پردازند.

همچنین در سازمان‌های مختلف دولتی کار می‌کنند؛ گرد هم می‌آورد» (Gjelten, 2011). واحد سایبری که از زیرساخت‌های اطلاعاتی استونی حمایت و از اهداف گسترده دفاع ملی پشتیبانی می‌کند؛ در شرایط اضطراری با تیم واکنش پاسخ‌گویی به حوادث کامپیوتری استونی برای پاسخ به حملات سایبری همکاری می‌کند؛ اما هیچ‌گونه تعهدات قراردادی یا پرداخت از سوی دولت ندارد (Roscini, 2014, p. 35).

۳-۲-۳. کنترل کلی و مؤثر دولت بر عمل متخلفانه سایبری

«ماده ۸» طرح پیش‌نویس مواد با عنوان «رفتار هدایت‌شده یا تحت کنترل یک دولت»، بیان می‌دارد: «رفتار شخص یا گروهی از اشخاص، در صورتی باید طبق حقوق بین‌الملل، رفتار دولت در نظر گرفته شود که آن شخص یا گروه افراد بر اساس دستورالعمل‌ها، یا تحت هدایت یا کنترل آن دولت عمل نمایند». ممکن است هکرها جزء نهادهای دولتی و نمایندگان دولتی نباشند؛ اما مقامات دولتی می‌توانند رفتار آن‌ها را تحریک کنند. در سال ۲۰۰۱، به‌عنوان مثال، پس از آنکه یک هواپیمای جاسوسی نیروی دریایی ایالات متحده با جت جنگنده چینی در جنوب دریای چین برخورد کرد؛ وب‌سایت‌هایی ظاهر شدند که دستورالعمل‌هایی در مورد چگونگی از کار انداختن رایانه‌های دولتی ایالات متحده به هکرها ارائه دادند. همچنین به نظر می‌رسد که دولت روسیه «هکرهای میهن‌پرست» را برای انجام حملات سایبری علیه استونی در سال ۲۰۰۷ تشویق کرده باشد. وبلاگ‌ها، انجمن‌ها و وب‌سایت‌های زبان روسی نیز دستورالعمل‌هایی درباره چگونگی غلبه بر وب‌سایت‌های دولتی گرجستان و فهرست وب‌سایت‌های آسیب‌پذیر گرجستان را منتشر کرده‌اند (Roscini, 2014, p. 39).

هنگامی‌که یک حمله سایبری در کنترل دولت باشد؛ مسئولیت دولت در دو رژیم برای حملات سایبری اعمال می‌شود؛ «معیار کنترلِ مؤثر عملیاتی» و «معیار کنترلِ کلی». این استانداردها به حل مسئله انتساب کمک می‌کنند و دو نوع استانداردهای کنترل و توابع آن‌ها در زمینه حملات سایبری را توضیح می‌دهند. منشأ این معیار دو رأی دیوان بین‌المللی دادگستری و یک رأی دیوان بین‌المللی کیفری یوگسلاوی سابق است؛ در ابتدا دیوان بین‌المللی دادگستری در قضیه فعالیت‌های نظامی و شبه‌نظامی با «معیار کنترلِ موثّر عملیاتی» و در وهله دوم، دیوان بین‌المللی دادگستری در قضیه «فعالیت‌های مسلحانه» و سپس دیوان بین‌المللی کیفری برای یوگسلاوی سابق[1] در

1. Prosecutor v. Tadic. “Judgement in Sentencing Appeals, IT-94-1-A and IT-94-1- Abis.” 26 January 2000

قضیه «تادیچ»[1] با «معیار کنترلِ کلی». انتخاب آگاهانه کمیسیون حقوق بین‌الملل در مرجح دانستن فرمول مورد پذیرش دیوان بین‌المللی دادگستری در قضیه «فعالیت‌های نظامی و شبه‌نظامی» بر معیار «کنترل کلی» از سوی شعبه تجدیدنظر دیوان بین‌المللی کیفری یوگسلاوی سابق در قضیه دادستان علیه تادیچ ارائه شده بود.

در قضیه «فعالیت‌های مسلحانه در جمهوری کنگو» (جمهوری دموکراتیک کنگو و اوگاندا)، دیوان بین‌المللی دادگستری به ماده ۸ از مواد کمیسیون حقوق بین‌الملل اشاره کرد و بدون اینکه ضروری بداند درباره معیار جایگزین مطرح‌شده از سوی شعبه تجدیدنظر دیوان بین‌المللی کیفری یوگسلاوی سابق در قضیه تادیچ اظهار نظر نماید؛ به قابلیت انتساب عملیات گروه‌های شبه‌نظامی (جنبش آزادی‌بخش کنگو) در قلمرو جمهوری دموکراتیک کنگو توجه داشت.

بوسنی و هرزگوین در حمایت از استدلال خود مبنی بر اینکه اعمال گروه‌های ارتش جمهوری صرب بوسنی[2] و گروه‌های شبه‌نظامی قابل انتساب به جمهوری فدرال یوگسلاوی هستند؛ بر فرمول جایگزین برای انتساب بر مبنای هدایت و کنترل تصریح‌شده از سوی شعبه تجدیدنظر دیوان بین‌المللی کیفری یوگسلاوی سابق در قضیه تادیچ تأکید کرد. دیوان بین‌المللی دادگستری فرمول شعبه تجدیدنظر دیوان بین‌المللی کیفری یوگسلاوی سابق به‌عنوان معرف حقوق بین‌الملل عرفی در مورد موضوع مطرح در آن را رد و اظهار کرد: «بر اساس رویه قضایی، ثابت‌شده و محقق است که دیوان تعیین خواهد کرد که آیا مدعیٌ‌علیه طبق قاعده حقوق بین‌الملل عرفی مقرر در ماده ۸ مواد پیش‌نویس طرح کمیسیون حقوق بین‌الملل در رابطه با مسئولیت دولت مسئول بوده است یا خیر.» بنابراین دیوان بین‌المللی دادگستری در اینجا مسئولیت دولت را مطرح می‌کند که دولت «کنترلِ مؤثری» بر روی چنین بازیگرانی دارد.

علاوه بر این، دیوان بین‌المللی دادگستری در رأی ۲۷ ژوئن ۱۹۸۶ درباره قضیه فعالیت‌های نظامی و شبه نظامی اشعار می‌دارد: «برای اینکه این رفتار به مسئولیت قانونی ایالات متحده منجر گردد؛ در اصل باید ثابت شود این دولت در طی دوره‌ای که نقض‌های ادعایی ارتکاب یافته؛ کنترل مؤثری بر روی عملیات نظامی یا شبه نظامی داشته است». به‌طور خلاصه، دکترین کنترل مؤثر که منشأ آن در رأی دیوان بین‌المللی

---

۱. در این قضیه تادیچ و وکلایش تلاش کردند در همان اولین پرونده، صلاحیت و مشروعیت دادگاه و نهاد مؤسس (شورای امنیت) را با چالش‌های اساسی مواجه کنند و به نظر می‌رسد رأی صلاحیتی دادگاه در این پرونده، به‌خوبی نمایانگر غایت‌گرایی دادگاه و خروج از رضایت باطنی قدرت‌های مؤسس است.

2. VRS

دادگستری در قضیه نیکاراگوئه است؛ کنترل یک کشور بر روی گروه‌های شبه‌نظامی یا سایر بازیگران غیردولتی را تنها در صورتی می‌پذیرد که بازیگران مورد نظر در «وابستگی کامل» به دولت عمل نمایند (Shackelford, 2010, p. 197). در قضیه تادیچ، دیوان بین‌المللی کیفری یوگسلاوی سابق معیار کنترل کلی را در زمینه مسئولیت کیفری شخصی و با هدف تعیین ماهیت مخاصمه مسلحانه به تصویب رساند. دیوان در پاراگراف ۱۳۱، صفحه ۵۶ توضیح می‌دهد: «به‌منظور انتساب اعمال یک گروه نظامی یا شبه نظامی به یک کشور، باید ثابت شود که دولت کنترل کلی بر گروه را نه‌تنها از طریق تجهیز و تأمین مالی گروه، بلکه از طریق هماهنگ کردن یا کمک به برنامه‌ریزی عمومی فعالیت نظامی آن در دست دارد.» بر اساس معیار کنترل کلی که در قضیه تادیچ در دیوان بین‌المللی کیفری یوگسلاوی سابق نشان داده شده است؛ در جایی که یک دولت در سازمان‌دهی و هماهنگی، علاوه بر حمایت از یک گروه، نقش داشته باشد؛ کنترل کامل آن را نیز دارد؛ به این ترتیب که اعمال آن گروه به دولت قابل انتساب است.

در مورد بازیگران غیردولتی، دیوان بین‌المللی دادگستری در قضیه نیکاراگوئه اظهار داشت که کنترلِ مؤثر، استاندارد مناسبی حداقل در زمینه شبه‌نظامی برای اعمال در این پرونده است. اگر این تصمیم را به شبه‌نظامیان سایبری تعمیم دهیم؛ دولت تنها در مواردی برای مشارکت آن‌ها مسئول خواهد بود که از این حملات سایبری حمایت می‌کند (اگر بتوان کنترل مؤثر آن‌ها را فراتر از هر شکلی ثابت کرد) (Shackelford, 2010, p. 202). با توجه خاص به چندین عملیات اینترنتی، اختلاف‌نظر قابل‌توجهی میان دیوان بین‌المللی دادگستری و رویکرد دیوان بین‌المللی کیفری یوگسلاوی سابق وجود ندارد؛ هر دو احتمالاً در اغلب موارد به استفاده از معیار کنترل مؤثر سوق داده می‌شوند؛ چراکه به نظر نمی‌رسد گروه‌های سایبری سازمان‌یافته و سلسله مراتبی هنوز وجود داشته باشند. پشتیبانی واضح برای اجرای معیار کنترل مؤثر در عملیات سایبری را همچنین می‌توان در سخنرانی مشاور حقوقی وزارت امور خارجه ایالات متحده، «هارولد کوه»[1]، در تارنمای سایبر دولت آمریکا یافت؛ آنجا که ادعا می‌کند: «دولت‌ها در سطح بین‌المللی زمانی مسئول اقدامات سایبری انجام‌شده از طریق «بازیگران نیابتی» هستند که آن‌ها بر اساس دستورالعمل دولت یا تحت هدایت یا کنترل آن عمل می‌کنند». برای نمونه آذربایجان حمله سایبریِ گروهی از هکرها با عنوان «ارتش

1. Harold Koh

سایبری ارمنی»، تحت «هدایت و کنترل» دولت ارمنستان را تقبیح کرد (Roscini, 2014, p. 40).

این شرایط را باید از مواردی که در آن‌ها شهروندان خصوصی ابتکار عمل را در انجام عملیات سایبری (به‌اصطلاح رخنه‌گران[1] یا هکرهای میهن‌پرست) در دست می‌گیرند؛ متمایز نمود. حوزه اصلی قابل اجرا بودن ماده ۸ نسبتاً محدود است؛ زیرا آن حوزه به دستورالعمل‌ها یا هدایت یا کنترل یک عملیات خاص برای دخالت دادن مسئولیت دولت محدود می‌شود.

به علت ماهیت مخفیانه فعالیت‌های سایبری و مشکلات فنی شناسایی مسببان، قضیه تادیچ باید در مورد عملیات سایبری بر معیار مورد بحث در قضیه نیکاراگوئه ترجیح داده شود. در واقع، دقیقاً به دلیل مشکلات شناسایی است که معیار «کنترل مؤثر» مرجح است؛ زیرا این امر موجب جلوگیری از این می‌شود که دولت‌ها به‌طور ناخواسته یا مخرب به عملیات سایبری متهم شوند (Schmitt, 2013, p. 38). موضوع دیگر فراهم ساختن زمینه حمله سایبری به دست دولت است که بسته به عمق و میزان کاربرد این زمینه قابل تغییر است.

۳-۲-۴. تأیید بعدی عملیات سایبری توسط دولت

ماده ۱۱ با عنوان: «رفتار تصدیق شده و مورد پذیرش یک دولت به‌عنوان رفتار آن دولت»، اظهار می‌دارد: «رفتاری که مطابق با مواد قبلی به دولت قابل انتساب نیست؛ باید در صورتی و تا حدی که دولت رفتار مورد نظر را تصدیق می‌نماید؛ به‌عنوان رفتار خود در نظر گیرد». ماده ۱۱ در مورد انتساب رفتاری به دولت است که در زمان ارتکاب، قابل انتساب به آن نبوده، اما پس از آن از سوی دولت به رسمیت شناخته شده و مورد پذیرش قرار گرفته است. همچنین ماده ۱۱ مبتنی بر اصلی است که رفتار شخصی را به‌صرف اینکه شخصی آن را مرتکب شده است نمی‌توان به یک دولت منتسب کرد؛ با وجود این، تصدیق می‌کند که آن رفتار را باید در صورتی و تا حدی که دولت رفتار مورد نظر را تصدیق می‌کند و به‌عنوان رفتار خود در نظر می‌گیرد، عمل آن دولت در نظر گرفت.

علاوه بر این در تفسیر اشاره شده که: میان مفاهیمی از جمله «تصدیق» و «پذیرش» با مفاهیمی مانند «حمایت» یا «موافقت» تمایز وجود دارد. همچنین

---

۱. رخنه‌گری به استفاده از رایانه و شبکه‌های رایانه‌ای در جهت اعتراض و مقاصد سیاسی گفته می‌شود. این واژه را در سال ۱۹۹۶ برای اولین بار یکی از اعضای گروه هکر مکتب گاو مرده، به نام اُمگا ابداع کرد (hacktivists).

کمیسیون حقوق بین‌الملل در تفسیر خود ملاحظه می‌کند: «به‌عنوان موضوع کلی، طبق ماده ۱۱، یک رفتار در صورتی که دولت صرفاً به وجود واقعی رفتار اذعان نماید یا تأیید کلامی آن را اظهار کند؛ قابل انتساب به دولت نخواهد بود. در مناقشات بین‌المللی، دولت‌ها اغلب مواضعی را اتخاذ می‌کنند که به «موافقت» یا «تأیید» رفتار در معنای عام نزدیک می‌شود؛ اما هیچ‌گونه فرض مسئولیتی را شامل نمی‌شود. از سوی دیگر زبان «پذیرش»، با خود ایده‌ای را مطرح می‌کند که آن رفتار از سوی دولت در واقع به‌عنوان رفتار خود دولت تصدیق می‌شود» (Crawford, 2002, p. 123). دیوان بین‌المللی دادگستری در قضیه «کارکنان دیپلماتیک و کنسولی ایالات متحده آمریکا در تهران، ایالات متحده علیه ایران»، ۲۹ مه ۱۹۸۰، به این استاندارد اشاره کرد. دیوان اظهار داشت که چنانچه شهروندان یک دولت را یک نهاد ذی‌صلاح دولت ایران برای انجام عملیاتی خاص گماشته باشد؛ اقدامات آن شهروندان می‌تواند به دولت قابل انتساب باشد. در آنجا، درحالی‌که دیوان شواهد کافی برای انتساب اقدامات شهروندان به دولت نیافت؛ دادگاه نتیجه گرفت که حکومت ایران در عین حال مسئول است؛ زیرا از تعهداتش تحت کنوانسیون ۱۹۶۱ وین در مورد روابط دیپلماتیک و کنوانسیون ۱۹۶۳ روابط کنسولی برای محافظت از سفارت آمریکا و کارکنان آن آگاه بوده و در انجام تعهداتش قصور ورزیده است.

تأیید و تصدیق حمله سایبری از سوی یک دولت دور از ذهن به نظر می‌آید. برخلاف حمله فیزیکی، حمله سایبری روشن و مشخص نیست و این مزیت آن برای مهاجم است و پذیرش و تصدیق آن منطقی نیست. با این حال اگر دولت دیگری بعد از حمله، حمایت خود را از مهاجم و قابلیت‌های سایبری آن برای محافظت از بازیگران غیردولتی در برابر عملیات ضد سایبری تصدیق کند؛ مسئولیت دولت برای این عملیات و هرگونه اقدامات بعدی مربوط به این گروه مطرح می‌شود.

به‌عنوان نمونه هیچ بازیگر غیردولتی و در واقع هیچ قدرت کم‌توانی، امکانات آزمایش استاکس‌نت[1] را ندارد؛ چه برسد به ساخت و استفاده از آن. این قابلیت‌ها محدود به کشوری است که ظرفیتی قوی در زیرساخت‌ها و سازه‌های حوزه سایبری و درنتیجه توان استفاده از این ظرفیت را داشته باشد. ایالات متحده و اسرائیل، کرم کامپیوتری استاکس‌نت را برای حمله به برنامه غنی‌سازی اورانیوم ایران طراحی کرده بودند. عملیات، با کدگذاری به نام «بازی‌های المپیک»، تحت فرماندهی «جورج واکر بوش» با مشارکت اسرائیل آغاز شد و باراک اوباما رئیس‌جمهور آن را ادامه داد. مقامات

1. Stuxnet

فعلی و گذشته ایالات متحده بیان می‌دارند که یک حمله سایبری مخرب علیه برنامه هسته‌ای ایران را کارشناسان آمریکایی و اسرائیلی ترتیب دادند که تحت دستورات مخفی رئیس‌جمهور اوباما قرار داشت. طرحی که درصدد کُند کردن پیشرفت آشکار ایران برای ساخت بمب اتمی، بدون شروع یک حمله نظامی متعارف بود. پس از گذشت چند سال، برخی از مقامات ایالات متحده اذعان کردند که «ایالات متحده پنج سال پیش تلاش کرده است یک نسخه از ویروس کامپیوتری استاکس‌نت را برای حمله به برنامه تسلیحات هسته‌ای کره شمالی به کار ببرد؛ اما به گفته افرادی که با کمپین مخفی آشنا هستند، شکست خورده است». بر اساس یک منبع اطلاعاتی ایالات متحده، توسعه‌دهندگان استاکس‌نت ویروسی را تولید کرده بودند که هنگام برخورد با تنظیمات به زبان کره‌ای در یک دستگاه آلوده فعال می‌شد. این اظهارات می‌تواند پذیرش ضمنی ایجاد و راه‌اندازی این سلاح‌ها علیه تأسیسات هسته‌ای ایران باشد.

نتیجه‌گیری

«پیچیدگی» مهم‌ترین اصل جامعه‌شناختی حاکم بر فضای سایبر است. پیش از مسئله انتساب و حل معمای شناسایی در حملات سایبری، مسئله مهم این است که آیا دولت مسئول در این اقدام، ممنوعیت توسل به زور را مطابق «بند ۴، ماده ۲» منشور ملل متحد نقض کرده است و آیا اساساً حمله‌ای ترتیب داده شده است؛ به‌گونه‌ای که هم حائز قید مسلحانه باشد و هم موجب استناد دولت حمله شونده به پاسخ‌های متعارف و معاهده‌ای شبیه به دفاع مشروع ذیل ماده ۵۱ منشور ملل متحد باشد. با رویکرد ابزارمحور به زور و حمله که همان رویکرد کلاسیک به‌عنوان مبنای تفسیر ماده ۲ (بند ۴) منشور است؛ کمتر می‌توان حمله‌ای سایبری را شناسایی کرد که واجد قید مسلحانه باشد؛ چراکه از یک‌سو این حملات ماهیت فیزیکی ندارند و از دیگر سو زور نظامی را در بر نمی‌گیرند. با وجود این، اتخاذ یک رهیافت نتیجه/پیامدمحور می‌تواند کمک کند تا حملات و عملیات سایبری ذیل توسل به زور و به‌عنوان یک حمله مسلحانه به رسمیت شناخته شوند. نوعی حملات سایبری که بتوانند آسیب یا خسارتی به‌اندازه تخریب تأسیسات هسته‌ای به بار آورند که با امنیت ملی یک کشور در ارتباط است؛ از حیث مخاطرات، قابل مقایسه با اقدامات نظامی هستند و مصداقی از توسل به زور نظامی نیز محسوب می‌شوند.

در گام بعد مسئله شناسایی عامل و انتساب این حملات به دولت ملی خاص مطرح می‌شود. در حملات سایبری پیچیدگی به‌اندازه‌ای است که به‌ندرت بتوان منشأ آن را

شناسایی کرد. طبیعی است که دولت‌ها به سبب مسئولیت جبران خسارت مترتب بر آن، مسئولیت تهیه یا ارسال بدافزار را بر عهده نگیرند. برای نمونه در جریان حمله استاکس‌نت به ایران با وجود دخالت مستقیم و مسئولیت ایالات متحده و اسرائیل در این اقدام خرابکارانه که قسمتی از برنامه سایبری آمریکا موسوم به «بازی‌های المپیک» بود و بر اساس گزارش‌های مختلف با موافقت مستقیم رئیس‌جمهور آمریکا انجام شده است و حتی در جریان دو حمله دیگر توسط «دوکو» و «شعله» (که به‌منظور نفوذ و کسب اطلاعات از شبکه‌های رایانه‌ای دولتی ایران و به‌خصوص برای هدف قرار دادن تأسیسات هسته‌ای و نفتی کشور برنامه‌ریزی شده بود)، دولت ایالات متحده حاضر به پذیرش مسئولیت آن نشد. با این حال، حقوق بین‌الملل در چنین شرایطی نیز مسکوت نیست. اگر این حمله با عدم مشارکت یا معاونت دولت ایالات متحده ترتیب داده می‌شد. همچنین بر اساس اصل حقوق بین‌الملل، دولت‌ها مکلف‌اند احتیاطات لازم را در قلمرو خود برای جلوگیری از ارتکاب اعمال مجرمانه علیه دولت دیگر یا مردم آن دولت به کار گیرند. با این حال پیچیدگی‌های بسیاری در خصوص شناسایی و انتساب حملات سایبری وجود دارد و این حوزه مطالعاتی نیازمند رشد و توسعه و وضع قواعد و مقررات تنظیم‌کننده برای کنترل رفتار متخلفانه است.

فهرست منابع

- ضیایی بیگدلی، محمدرضا (۱۳۹۴). ***حقوق بین‌الملل بشردوستانه. چاپ سوم***، تهران: گنج دانش.
- شریفی طرازکوهی، حسین؛ برمکی، جعفر (۱۳۹۹). ***چالش‌های فضای سایبری در پرتو ماده ۳۶ پروتکل یکم الحاقی ۱۹۷۷***. مجله حقوقی بین‌المللی، شماره ۶۲، صص ۱۱۹-۱۴۴.

References

- Brenner, S.W., (2006).At Light speed: Attribution and Response to Cyber Crime/ Terrorism/ warfare. Journal of Criminal Law and Criminology, No, 97, 2006 - 2007.
- Crawford, James (2002). The International Law Commission's Articles on State Responsibility. Cambridge University press.
- Delibasis, D. (2007). the right to National Self-Defence in Information Warfare Operations, 2007.
- Dinstein, Y. (2001).Computer Network Attacks and self-Defence. in: Schmitt/O'Donnell (Eds), Computer Network Attack and International Law.
- Farer J (1985).political and economic coercion in contemporary international law. American journal of international law, 79.
- Harrison Dinniss, Heather (2012). Cyber warfare and the Law of War. Cambridge University press.
- Kelsen, Hans (1956). General international law and the law of the united nations. in the United Nations: ten years' legal progress 1, 5.
- Randelzhofer, Albrecht (2003). the charter of the United Nations: a commentary. supra note 9, at 118.
- Rifaat, Ahmed M. (1980). International aggression: a study of the legal concept. 120, 234.
- Roscini, Marco (2010). World Wide Warfare-jus ad bellum and use of force. Max Planck Yearbook of United Nations Law, Volume 14.
- Schmitt, N. Michael (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press.
- Schmitt, Michael (2012).Attack as a Term of Art in International Law: The Cyber Operations Context. 2012 4th International Conference on Cyber Conflict.
- Shackelford, J. Scott (2010). State Responsibility for Cyber Attacks: Competing Standards for A Growing Problem. Conference on Cyber Conflict, CCD COE Publications, 2010, Tallinn, Estonia.
- Silver, b. Daniel (2002). computer network attack as use of force under article 2 (4) of the United Nations charter. international law studies, vol 76, p 82.
- Waxman C. Matthew (2011). cyber-attacks as "force". under un charter article 2(4)" international law studies, vol 87 p 46.
- Yorman Dinstein (1994). war, aggression and self defense. 2d Ed.
- Boulanin, Vincent (2015). Implementing Article 36 Weapon Reviews in the Light of Increasing Autonomy in Weapons Systems. SIPRI Insight on Peace and Security, No.201/1.
- Tallin Manual (2013). On the International Law Applicable to Cyber Warfare, NATO Cooperative Defense Centre of Excellence, Cambridge University Press, Cambridge.
- Turns, David (2013). Cyber War and the Concept of Attack in International Humanitarian Law. in Saxon, Dan (ed.) International Humanitarian Law and the Changing Technology of War, Boston, Martinus Nijhoff Publishers.
- Streltsov, Anatoly (2015). Key Trends of International Law Relating to the Conflicts in Cyber Space. in Greppi, Edoardo (ed.) Conduct of Hostilities: The Practice, The Law and The Future, International Institute of Humanitarian Law.
- ICJ Reports(2005). The Armed Activities on the Territory of the Congo Case. (Democratic Republic of Congo v. Uganda).

- Gjelten, Tom (2011). Volunteer Cyber Army Emerges in Estonia. January 4, 2011, viewed at 3. 8. 2020, available in: http://www.npr.org/2011/01/04/ 132634099/ in-estonia-volunteer-cyber-army-defends-nation.
- D. Eshel, (2010). Israel Adds Cyber-Attack to IDF. 11 February 2010, viewed at 5. 12. 2020 available in: http://defensetech.org/2010/02/11/israel-adds-cyber-attack-to-idf/
- Goetz, John (2009). national defence in cyberspace. 11 February. Viewed at 12. 10. 2020 Available in: http://www.spiegel.de/international/germany/ war-of-the-future-national-defense-in-cyberspace-a-606987.html
- Singer, E David (2013). U.S. Blames China's Military Directly for Cyberattacks. May 6, 2013 viewed at 20. 4. 2020 available in: http://www.nytimes.com/2013/05/07/ world/ asia/ us-accuses-chinas-military-in-cyberattacks.html