Original Article

Applicability of International Humanitarian Law Rules in Cyber Attacks by Looking at Tallinn Manual 2

Azar Givkey[1], Mohammad Ali Kafaei Far*[2], Mohammad Taghi Rezaei[3]

1. PhD Student, Department of International Law, Faculty of Humanities, Qom Branch, Islamic Azad University, Qom, Iran.
2. Assistant Professor, Department of International Law, Faculty of Humanities, Qom Branch, Islamic Azad University, Qom, Iran. (Corresponding author) Email: ma.kafaeifar@gmail.com
3. Assistant Professor of Law, Faculty of Social Sciences, Payame Noor University, Tehran, Iran.

Received: 14 Feb 2019 Accepted: 26 Dec 2020

Abstract

Background and Objective: The Phenomenon of Cyber Warfare, Which as a Result of Increasing Advances in Science and Technology, Has Today Become a New Method of Warfare in the Field of International Relations, Is Slowly Moving Towards Legalization, As With the Development of Cyber Weapons, We Are Witnessing The Emergence of Legal Issues in the Field of International Humanitarian Law, To Evolve the Legal Concept of War and the Use of Force and Efforts to Regulate and Extend the Rules of Armed Conflict to Such Confrontations by Governments.

In This Regard, Despite the Fact That We Have not Witnessed a Binding Treaty, But With the Development of the Tallinn Manuals 1 and 2, an Attempt Was Made to Reveal the Shadow of the General Rules of International Law on Cyber Activities.

This Study Tries to Examine the Concept of War and Armed Conflict, in Accordance With the Progress of Science and the Use of Cyberspace as a Battlefield of Governments, The Ability to Observe the Principles and Rules of Armed Conflict in Cyber Warfare by Looking at Tallinn 2 Instructions on Cyber Attacks.

Materials and Methods: This Research has Been Done by Using Descriptive-Analytical Method, by Collecting Materials and Organizing Them to Achieve the Final Goal of the Research, ie, Proving the Applicability of the Rules of the Law of Armed Conflict on Cyber Operations.

Findings: As the Use of Any Type of Weapon, in Certain Circumstances, May be Interpreted as the Use of Force or War, Cyber Operations, If They Have the Characteristics Described in the Tallinn 2 and in Relation to the Tallinn 1 And the Previous Theories Have Been Developed and Interpreted, it is Considered a War and the Special Effects of the War Will be Borne On it.

Conclusion: The Rules of International Law of Armed Conflict Can be Applied in Situations Where the Use of Cyber Operations has Characteristics That, According to Tallinn 2, Recognize Cyber Weapons Operations as a Cyber War.

Keywords: Cyber Warfare; Armed Conflict Law; Humanitarian Law; Cyber Attacks; Tallinn Manual

Please cite this article as: Givkey A, Kafaei Far M A, Dr. Rezaei M T. Applicability of International Humanitarian Law Rules in Cyber attacks by Looking at Tallinn Manual 2. *Iran J Med Law*, Special Issue on Human Rights and Citizenship Rights 2018; 173-186.

مقاله پژوهشی

قابلیت اعمال قواعد حقوق بشردوستانه بین‌المللی در حملات سایبری با نگاهی به دستورالعمل تالین ۲

آذر گیوکی[۱]، محمدعلی کفایی‌فر[۲*]، دکتر محمدتقی رضایی[۳]

۱. دانشجوی دکتری گروه حقوق بین‌الملل، دانشکده علوم انسانی، واحد قم، دانشگاه آزاد اسلامی، قم، ایران.

۲. استادیار گروه حقوق بین‌الملل، دانشکده علوم انسانی، واحد قم، دانشگاه آزاد اسلامی، قم، ایران. (نویسنده مسؤول)

Email: ma.kafaeifar@gmail.com

۳. استادیار گروه حقوق، دانشکده علوم اجتماعی، دانشگاه پیام نور، تهران، ایران.

دریافت: ۱۳۹۷/۱۱/۲۵ پذیرش: ۱۳۹۹/۱۰/۰۶

چکیده

زمینه و هدف: پدیده جنگ‌های سایبری، که درنتیجه پیشرفت‌های روزافزون علوم و فناوری، امروزه به شیوه جدید جنگ در عرصه روابط بین‌المللی بدل گشته است، آرام آرام به سوی قانونمند شدن به پیش می‌رود، کما اینکه با پیشرفت سلاح‌های سایبری، شاهد مطرح شدن مباحث حقوقی در زمینه حقوق بین‌الملل بشر دوستانه، جهت تحول مفهوم حقوقی جنگ و توسل به زور و تلاش برای قاعده‌مند کردن و تسری قواعد حاکم بر مخاصمات مسلحانه بر این‌گونه رودررویی‌ها از سوی دولت‌ها هستیم. در این راستا، علی‌رغم اینکه شاهد معاهده الزام‌آوری نبوده‌ایم، اما با تدوین دستورالعمل‌های تالین ۱ و ۲ کوشش شد که سایه قواعد عام حقوق بین‌الملل به صورت ملموس بر فعالیت‌های سایبری آشکار شود. این پژوهش، تلاش دارد با بررسی مفهوم جنگ و مخاصمه مسلحانه، به تناسب پیشرفت علوم و استفاده از فضای مجازی به‌عنوان صحنه نبرد دولت‌ها، قابلیت رعایت اصول و قواعد حقوق مخاصمات مسلحانه در جنگ‌های سایبری را با نگاهی به دستورالعمل تالین ۲ درباره حملات سایبری بررسی نماید.

مواد و روش‌ها: این پژوهش، با استفاده از روش توصیفی - تحلیلی، با گردآوری مطالب و سازماندهی آنها برای رسیدن به هدف نهایی پژوهش، یعنی، اثبات قابلیت استفاده از قواعد حقوق مخاصمات مسلحانه بر عملیات سایبری، صورت گرفته است.

یافته‌ها: همان‌طورکه استفاده از هر نوع سلاح، در شرایط خاصی، ممکن است توسل به زور یا جنگ تعبیر شود، عملیات سایبری، نیز در صورتی که دارای ویژگی‌هایی باشد که توسط دستورالعمل تالین ۲، توصیف شده و به نسبت دستورالعمل تالین ۱ و نظریه‌های پیشین، بسط‌یافته و تفسیر شده است، جنگ محسوب شده و آثار خاص جنگ بر آن بار خواهد شد.

نتیجه‌گیری: قواعد حقوق بین‌الملل مخاصمات مسلحانه، در شرایطی که استفاده از عملیات سایبری، دارای ویژگی‌هایی باشد که مطابق دستورالعمل تالین ۲، عملیات ارتکاب‌یافته با سلاح سایبری را به‌عنوان یک جنگ سایبری شناسایی می‌کنند قابلیت اعمال دارد.

واژگان کلیدی: جنگ سایبری؛ حقوق مخاصمات مسلحانه؛ حقوق بشردوستانه؛ حملات سایبری؛ دستورالعمل تالین

مقدمه

با پیشرفت علوم و فناوری، شاهد تحول ابزارها و مفاهیم بسیاری در زمینه‌های مختلف و مرتبط با روابط انسانی و اجتماعی هستیم؛ جنگ نیز، به‌عنوان گونه‌ای از روابط میان دولت‌ها، از تحول و پیشرفت، بی‌بهره نمانده و از اشکال سنتی خود و جنگ‌های تن به تن با ابزارهای سخت، به جنگ افزارهایی غیرملموس و کم‌هزینه‌تر و البته با قدرت تخریبی بیشتر جهش یافته است. گسترش و توسعه فناوری اطلاعات و استفاده روزافزون دولت‌ها از فضای دیجیتال و در پی آن، گسترش تبادل اطلاعات از طریق شبکه‌های کامپیوتری، فضایی را در اختیار دولت‌ها قرار داده است که در آن، علاوه بر آسان‌تر کردن دستیابی به اطلاعات، از فضای سایبر، در جهت نیل به اهداف خصمانه خود از جمله، ایجاد وقفه در فعالیت‌های اقتصادی و تجاری دولت هدف، و توقف یا تخریب زیرساخت‌های حیاتی آن دولت است.

اولین حمله سایبری در جهان، در سال ۱۹۸۸، از طریق کرم موریس (Morris Worm) که توسط رابرت تاپان موریس، استاد مؤسسه فناوری ماساچوست (Massachusetts Institute of Technology)، جهت ایجاد اختلال در زیرساخت‌های سایبری در ایالات متحده، صورت گرفت. پس از آن در سال ۲۰۰۶، برنامه‌های پرتاب فضایی ناسا، مورد حمله قرار گرفت. در سال ۲۰۰۷، اختلال موقتی در سرویس‌های دولتی و بانکداری دولت استونی، توسط دولت روسیه به وقوع پیوست. در ماه آوریل همان سال، سرویس ایمیل‌های وزارت دفاع ایالات متحده مورد هجمه سایبری قرار گرفت. در سال ۲۰۰۸، شبکه‌های کامپوتری گرجستان، از سوی دولت روسیه، مورد تهاجم قرار گرفت. در سال ۲۰۰۹، زیرساخت‌های رژیم صهیونیستی، از سوی افراد ناشناس، مورد حمله قرار گرفت. همچنین، در اکتبر سال ۲۰۱۰، بدافزار استاکس نت (Stuxnet)، به چند کشور از جمله ایران حمله کرد؛ تصور بر آن است که این بدافزار برای وارد کردن ضربه به زیرساخت‌های هسته‌ای ایران مورد استفاده قرار گرفت. پس از این حملات، در سال ۲۰۱۳، شرکت روسی کاسپراسکای، کشورهای اروپای شرقی، شوروی سابق، آسیای مرکزی را مورد حمله قرار داد.

چنان‌که دیدیم، تا به حال حملات سایبری فراوانی، در عرصه روابط بین دولت‌ها حادث شده است و این حملات به صورت روزافزون در حال افزایش است که، علی‌رغم وارد آوردن آسیب‌های جدی به بخش‌های مورد هدف، ممکن است به سایر بخش‌ها یا افراد غیرمرتبط، لطماتی وارد نماید. حقوق بین‌الملل با عنایت به قواعد حقوق توسل به زور و مخاصمات مسلحانه، کوشیده است پدیده حملات سایبری را در جهت کاهش یا جبران خسارت به قربانیان، قاعده‌مند نموده و با تهیه و تدوین قواعدی از جمله دستورالعمل تالین ۱ و ۲ (Tallinn Manual)، حملات سایبری را جرم‌انگاری نموده و تحت قواعد حقوق توسل به زور و مخاصمات مسلحانه، به تبیین قوانینی در جهت مواجهه با این‌گونه حملات برآید.

این تحقیق، بر آن است که با تعریف مفاهیم حمله و جنگ سایبری، مخاصمه مسلحانه و توسل به زور، در ابتدا به اثبات پدیده حملات سایبری به‌عنوان جنگ، پرداخته و سپس، به بررسی لزوم رعایت قواعد حقوق توسل به زور و مخاصمات مسلحانه در این پدیده بپردازد.

فضای سایبری

در اصطلاح، فضای سایبر، «به مجموعه محیط‌هایی، همچون اینترنت گفته می‌شود که اشخاص در آنها از طریق رایانه‌هایی متصل، با یکدیگر ارتباط برقرار می‌کنند» (۱). فضای سایبر در کنار زمین، دریا، هوا و فضا به‌عنوان قلمرو پنجم درگیری و جنگ قلمداد می‌شود؛ چنان‌که، به تعبیر وزارت دفاع ایالات متحده، فضای سایبر «قلمرو جهانی در محیط اطلاعاتی، شامل شبکه‌های به هم پیوسته از زیرساخت‌های فناوری اطلاعات، شامل اینترنت، شبکه ارتباطات از راه دور، سیستم‌های کامپیوتری و پردازشگرها و کنترل‌گرهای تعبیه شده» است و از آن به‌عنوان «قلمرو جدید جنگ» نام برده است؛ همچنین، مرکز عالی همکاری دفاع سایبری ناتو، واقع در استونی، فضای سایبر را چنین تعریف کرده است «فضای سایبر، دسته‌ای از سیستم‌های اطلاعات در هم تنیده وابسته به زمان و کاربران انسانی است که در حال کنش و واکنش متقابل هستند» (۲).

این فضا از آن جهت که داده‌ها و اطلاعات فراوانی در آن وجود دارد، فضای اطلاعات نیز نامیده می‌شود و بر همین اساس در تعریف دیگری، فضای سایبر، به محیطی گفته شده که ناظر بر کلیه منابع اطلاعاتی قابل دسترس در شبکه‌های رایانه‌ای است (۳)؛ می‌توان گفت، فضای سایبر عبارت است از «یک محیط الکترونیکی که اطلاعات از طریق آن تولید، انتقال، دریافت، ذخیره‌سازی، پردازش و پاک می‌گردد» (۴).

سند راهبردی پدافند غیرعامل سایبری جمهوری اسلامی ایران، مصوب ۱۳۹۴، فضای سایبری را شبکه‌های وابسته به یکدیگر، از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای، پردازنده‌های تعبیه‌شده، کنترل‌گرهای صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط و انسان، به منظور تولید، پردازش، ذخیره‌سازی، مبادله، بازیابی و بهره‌برداری از اطلاعات می‌داند که ممکن است در ارتباط مستقیم و مداوم با سامانه‌های فناوری اطلاعات و شبکه‌های ارتباطی اعم از شبکه اینترنت باشد و یا تنها قابلیت اتصال به محیط پیرامونی در آن تعبیه شده باشد (۵).

حمله سایبری

حملات سایبری، که در چهارچوب طیف گسترده‌ای از آنچه عملیات سایبری نامیده می‌شود، قرار می‌گیرند، عبارتند از «به‌کارگیری منسجم توانمندی‌های جنگ الکترونیکی، عملیات شبکه‌ای کامپیوتری، عملیات روانی، حیله‌های نظامی و عملیات هماهنگ با قابلیت‌های پشتیبانی که به منظور تأثیرگذاری، متوقف نمودن، تخریب یا سرقت اطلاعات دشمن و در عین حال پشتیبانی از فرآیندهای تصمیم‌گیری نهادهای ملی صورت می‌گیرد» (۶). عملیات سایبری، شامل سه دسته عملیات حمله سایبری، استثمار سایبری و دفاع سایبری است؛ استثمار سایبری، عملیات جمع‌آوری اطلاعات است برای به دست آوردن داده‌ها از هدف یا سیستم‌های اطلاعاتی خودکار دشمن یا شبکه‌ها؛ در مقابل، دفاع سایبری، عبارت است از فعالیت‌هایی برای حمایت، کنترل، تحلیل، کشف و پاسخ به فعالیت غیرمجاز داخل سیستم‌های اطلاعاتی و شبکه‌های کامپیوتری (۷).

شورای تحقیقات ملی ایالات متحده، در گزارش سال ۲۰۰۹ درخصوص قابلیت حمله سایبری، حملات سایبری را به منزله استفاده از اقداماتی عمدی برای تغییر، مختل کردن، فریب دادن، کاهش دادن، یا از بین بردن سیستم‌های کامپیوتری دشمن یا شبکه‌ها یا اطلاعات و برنامه‌های موجود در این سیستم‌ها می‌داند (۸).

در سال ۲۰۱۰، ستاد مشترک ارتش ایالات متحده حمله سایبری را به‌عنوان عملی خصمانه با استفاده از کامپیوتر یا شبکه‌های مرتبط یا سیستم‌ها، تعریف کرد که برای اختلال و یا نابود کردن زیرساخت‌های حساس و بحرانی سایبری، دارایی‌ها یا فعالیت‌های دشمن در نظر گرفته شده است. این آثار حمله سایبری لزوماً به سیستم‌های کامپیوتری هدفمند یا خوددادده‌ها محدود نیست به‌عنوان مثال، حملات به سیستم‌های کامپیوتری، به جهت تنزل و یا نابود کردن زیرساخت‌ها در نظر گرفته شده است. حمله سایبری ممکن است از وسایل حمل و نقل متوسط، از جمله دستگاه‌های جانبی، فرستنده‌های الکترونیکی، کد تعبیه‌شده و یا اپراتور انسانی استفاده کند (۹).

سند راهبردی پدافند غیرعامل، هر رویداد یا واقعه با قابلیت وارد نمودن ضربه به مأموریت‌ها، وظایف، تصویر یا اشتهار دستگاه متولی، سرمایه ملی سایبری یا پرسنل دستگاه، به واسطه یک سامانه اطلاعاتی، از طریق دسترسی غیرمجاز، انهدام، افشاء، تغییر اطلاعات و یا ممانعت از (ایجاد اختلال در) ارائه خدمت را یک تهدید سایبری دانسته و اشاره می‌کند که تهدیدات سایبری، قادر به تأثیرگذاری بر سرمایه‌های ملی سایبری در سطوح فراملی، ملی، دستگاهی، استانی، منطقه حیاتی و حساس و زیرساختی خواهند بود (۵)؛ از سوی دیگر، با تفکیک تعریف میان تهدید سایبری و تهاجم سایبری، تهاجم سایبری را هرگونه اقدام غیرمجاز سایبری تلقی می‌کند که با هدف نقض سیاست امنیتی یک سرمایه سایبری و ایجاد خرابی یا خسارت، ایجاد اختلال در عملکرد یا از کاراندازی خدمات و یا دستیابی به اطلاعات سرمایه ملی سایبری مذکور انجام گیرد. همچنین، استفاده عمدی از یک سلاح سایبری علیه یک سامانه اطلاعاتی، به شکلی که موجب بروز یک حادثه سایبری شود نیز،

تهاجم سایبری دانسته و تهاجم‌های سایبری شاخص را شامل جرایم سایبری سازمان‌یافته، عملیات شناسایی برای تهاجم سایبری، مبارزه سایبری و جنگ سایبری، می‌داند. سند مذکور، همچنین، جنگ سایبری را بالاترین سطح و پیچیده‌ترین نوع از تهاجم یا عملیات سایبری می‌داند که علیه منافع ملی سایبری کشورها انجام شده و شدیدترین پیامدها را خواهد داشت، این‌گونه تهاجم‌های سایبری، که دولت‌ها آنها را جنگ علیه منافع ملی خود تلقی می‌کنند، توسط نیروهای سایبری کشور مهاجم یا گروه‌های سازماندهی‌شده تحت فرمان دولت‌های متخاصم و از طریق سلاح‌های سایبری تحت کنترل یا رهاشده توسط این نیروها و با هدف جاسوسی سایبری با حمایت دولت‌ها جهت جمع‌آوری اطلاعات برای برنامه‌ریزی تهاجم‌های سایبری بعدی، یورش سایبری جهت بسترسازی برای هرج و مرج و شورش مردمی، از کاراندازی تجهیزات و تسهیل و تکمیل تهاجم فیزیکی و تخریب یا اختلال گسترده به‌عنوان هدف نهایی یا همان جنگ سایبری صورت می‌گیرد (۵).

قاعده ۳۰ دستورالعمل تالین ۱ (۱۰)، همچنین، قاعده ۹۲ دستورالعمل تالین ۲ (۲)، حمله سایبری را این‌گونه تعریف می‌کند «حمله سایبری، عملیات سایبری تهاجمی یا تدافعی است که از آن به‌طور معقول، انتظار ایراد صدمه یا مرگ به اشخاص، یا وارد کردن خسارات به اشیاء می‌رود»؛ این قواعد، تعریفی از «حمله» را مقرر می‌کند که از تعریف مندرج در ماده ۴۹(۱) پروتکل اول الحاقی بهره می‌گیرد، به این مفهوم که «حمله، اقدامات خشونت‌بار علیه دشمن چه به صورت تهاجمی و چه به شکل دفاعی» است. از رهگذر این تعریف که مورد پذیرش گسترده‌ای قرار گرفته است، این توسل به خشونت علیه یک هدف است که حملات را از دیگر عملیات‌های نظامی متمایز می‌کند؛ عملیات‌های غیرخشونت‌باری، مانند عملیات‌های سایبری روانی یا جاسوسی سایبری، حمله به شمار نمی‌آیند (۱۱).

در یک تعریف جامع و مختصر، «حمله سایبری عبارت است از «هر اقدامی که به منظور تخریب کارکرد شبکه‌های کامپیوتری انجام شده و یک هدف امنیت ملی یا سیاسی ورای آن وجود داشته باشد».

منظور از «هر اقدام انجام‌شده»، این است که، یک حمله سایبری می‌تواند شامل هک، بمباران، قطع، آلوده ساختن، و اقداماتی این‌چنینی شود، اما برای آنکه این عمل، یک حمله سایبری تلقی شود، بایستی هدف آن تخریب یا اختلال در عملکرد شبکه‌های کامپیوتری باشد (۱۲).

«برای تخریب عملکرد»، یعنی، حملات عملی در عملکرد سیستم کامپیوتر اختلال ایجاد نموده و این امر منجر به عملکرد بد شبکه شود، مثل ویروس، کرم‌های کامپیوتری، و تروجان؛ و این مفهوم، در مقابل حملات معنایی (Semantic Attack)، سیستم عامل را حفظ می‌کند، اما صحت اطلاعاتی را که فرآوری کرده و اطلاعاتی که به آن واکنش نشان می‌دهد، هدف می‌گیرد (۱۳).

عبارت «از یک شبکه کامپیوتری» نشان می‌دهد که هدف یک حمله سایبری باید یک شبکه کامپیوتری، یعنی، سیستمی از کامپیوترها و وسائلی که از طریق کانال‌های ارتباطی با یکدیگر مرتبطند، باشد (۱۴).

عبارت «وجود یک هدف امنیت ملی یا سیاسی ورای حمله»؛ وجود یک هدف امنیت ملی یا سیاسی است که موجب تمایز میان حمله سایبری و جرم سایبری ساده می‌شود. هرگونه اقدام تهاجمی که توسط بازیگر دولتی در عرصه سایبری انجام می‌شود، لزوماً دلالت بر امنیت ملی داشته، در صورت تأمین سایر عناصر، حمله سایبری محسوب می‌شود (۱۳).

جنگ سایبری

جنگ سایبری، عبارت است از استفاده از کامپیوتر و اینترنت برای جنگیدن در فضای سایبر (۱۵)؛ به تعبیر دیگر، نفوذ غیرمجاز به وسیله، از طرف، یا در حمایت از یک دولت، به شبکه‌ها یا کامپیوترهای ملی دیگر، یا هر فعالیت متأثرکننده سیستم‌های کامپیوتری، که هدف آن جمع کردن، تغییر دادن یا دستکاری اطلاعات باشد یا باعث مختل شدن یا صدمه زدن به کامپیوتر، طرح شبکه، یا اهداف کنترل سیستم کامپیوتر شود، جنگ سایبری خواهد بود (۷).

مرکز عملیات سایبری ایالات متحده، جنگ سایبری را «استفاده عمدی از فعالیت‌های مختل‌کننده، یا تهدید مربوط

به آن، علیه کامپیوترها و شبکه‌ها، با هدف ایراد ضرر و زیان یا اکثراً با هدف اجتماعی، ایدئولوژیکی، مذهبی، سیاسی یا اهداف مشابه، یا به جهت وادار کردن شخصی برای انجام چنین اهدافی» می‌داند.

در نهایت، سازمان همکاری‌های شانگهای، جنگ سایبری را در تعریفی جامع، چنین معرفی می‌کند «مقابله میان دولت‌ها در عرصه اطلاعاتی با هدف صدمه زدن به سیستم‌های اطلاعاتی، فرآیندها و منابع، زیرساخت‌های حیاتی و مهم، تضعیف سیستم‌های سیاسی، اقتصادی و اجتماعی، عملیات روانی گسترده برای عدم ثبات دولت و جامعه، همچنین مجبور کردن دولت برای اتخاذ تصمیماتی در راستای منافع مخالفین» (۱۳).

مبنای رعایت حقوق مخاصمات مسلحانه در حملات سایبری

عملیات‌های سایبری اجراشده در سیاق یک مخاصمه مسلحانه، مشمول حقوق مخاصمات مسلحانه هستند (۱۱)، لذا لازم‌الاجرا بودن حقوق مخاصمات مسلحانه، بستگی به وجود مخاصمه مسلحانه دارد (۱۱)؛ چنان‌که در ماده ۲ مشترک کنوانسیون‌های چهارگانه ژنو، مورد اشاره قرار گرفته است، لازم‌الرعایه شدن حقوق مخاصمات مسلحانه با سه مفهوم ارتباط دارد که عبارتند از: وقوع جنگی که رسماً اعلان شده باشد؛ هرگونه مخاصمه مسلحانه‌ای که میان دو یا چند دولت معظم متعاهد بروز کند، ولو آنکه یکی از دول مزبور وجود وضعیت جنگی را شناسایی ننموده باشد؛ اشغال یک سرزمین بدون مقاومت. از میان سه معیار پیش‌گفته، مهم‌ترین و متداول‌ترین معیار اعمال حقوق مخاصمات مسلحانه، معیار اول است که همان درگیری‌های مسلحانه فعال می‌باشد و دو معیار دیگر، جنبه تکمیلی دارند (۱۶).

اعمال حقوق مخاصمات مسلحانه بر عملیات‌های سایبری می‌تواند دردسرساز باشد. غالباً تشخیص وجود حمله‌ای سایبری، منشا آن، هدف قصد شده از حمله یا اثرات دقیق حمله ذیربط دشوار است. با این حال، این مسائل موضوعی به اعمال حقوق مخاصمات مسلحانه خدشه‌ای وارد نمی‌سازند (۱۱).

معیارهای شناسایی توسل به زور به‌عنوان مخاصمه مسلحانه در حملات سایبری

ژان پیکته (Jean Pictet)، در تفسیر ماده ۲ مشترک، معیاری را مطرح نموده است که مطابق آن، توسل به زور زمانی به حد مخاصمه مسلحانه می‌رسد که توسل زور اعمال شده حائز «شدت»، «استمرار» و «محدوده کافی» باشد (۱۷).

در طول سال‌ها، یک سری ابزارهای بین‌المللی پدید آمده‌اند که باعث تسهیل استفاده از معیارهای پیکته شده‌اند؛ از جمله، قطعنامه «تعریف تجاوز» مجمع عمومی سازمان ملل متحد؛ در حالی که این قطعنامه، تعریفی قطعی از حمله مسلحانه ارائه نمی‌دهد، نمونه‌هایی از اقدامات دولتی که به نظر می‌رسد واجد شرایط این واژه هستند ارائه می‌دهد که با پذیرش گسترده بین‌المللی نیز مواجه شدند (۱۸).

در خصوص توسل به زورهای مدرن از جمله حملات سایبری نیز سه دیدگاه با برداشت از معیار ژان پیکته مطرح شده است.

نخستین دیدگاه، دیدگاه ابزار محور است که با اعمال آن باید ارزیابی کرد که آیا خسارت‌های حاصله از یک حمله سایبری که قبلاً از طریق حملات سنتی حاصل می‌شد؛ به‌عنوان مثال با اعمال این مدل، حمله سایبری که منجر به قطع شبکه برق می‌شود، می‌تواند حمله مسلحانه قلمداد شود، زیرا قبل از پیشرفت و توسعه ابزارها و قابلیت‌های سایبری، تخریب و انقطاع شبکه برق، نوعاً مستلزم بمباران ایستگاهها و نیروگاههای برق یا استفاده از سایر ابزارهای انفجاری سنتی بوده است.

دیدگاه دوم دیدگاه نتیجه محور یا اثرگراست. این دیدگاه به اثر و نتیجه کلی حمله سایبری نسبت به دولت قربانی نظر دارد، به‌عنوان مثال، با توجه به این دیدگاه، دستکاری در اطلاعات مؤسسات مالی و بانکی یک کشور از طریق فضای سایبر که موجب برهم خوردن سیستم اقتصادی آن می‌شود، می‌تواند حمله مسلحانه تلقی گردد، زیرا چنین اعمالی هرچند شبیه حملات سنتی نیست، اما از آنجا که در اثر دستکاری و نفوذ در سیستم‌های اقتصادی صدماتی به آن‌ها وارد آمده و موجب از کار افتادن آن‌ها می‌شود؛ این نتیجه با اثر یک حمله مسلحانه برابری می‌کند.

سومین دیدگاه، جنبه مطلق داشته و هر نوع حمله علیه زیرساخت‌های حیاتی ملی (National Critical Infrastructure) یک دولت را بر مبنای نتایج سنگینی که از حمله به چنین سیستم‌های زیرساختی حاصل می‌شود، حمله مسلحانه می‌داند (۱۷).

هرچند محتوای هر سه دیدگاه، مورد مجادلات و مباحثات فراوانی واقع شده، اما اهمیت اساسی آنها در این حقیقت نهفته است که هر سه دیدگاه به این نکته مهم تأکید دارند که عملیات سایبری می‌تواند تنها در برخی حالات، حمله مسلحانه محسوب شود.

پروفسور «مایکل اشمیت» تلاش می‌کند بین دیدگاه‌های مذکور پیوند برقرار کند (۱۹) او که طرفدار رویکرد نتیجه‌گرا است وجود هفت خصوصیت را برای تطابق اثرات حمله سایبری با حمله مسلحانه لازم می‌داند و معتقد است وجود هفت خصوصیت ذیل، حمله سایبری را به حمله مسلحانه بدل می‌نماید (۱۹).

۱. شدت آسیب
۲. فوریت نتایج حمله
۳. مستقیم بودن
۴. تهاجم به دولت مدنظر
۵. قابلیت اندازه‌گیری خسارت
۶. مشروعیت مفروض
۷. مسئولیت (۱۹).

مارک شولمان، معتقد است که نبرد اطلاعاتی، همانند دیگر مخاصمات مسلحانه، تحت شمول محدودیت‌های بشردوستانه است، هرچند که اطلاق عنوان مسلحانه در معنای سنتی آن نسبت به حملات سایبری صادق نباشد (۲۰).

دیوان بین‌المللی دادگستری برای تمایز بین شدیدترین اَشکال توسل به زور ازجمله حمله مسلحانه و اَشکال با شدت کمتر (Short of war)، ضابطه میزان و اثر را به کار برده است (۲۱)، همچنین با توجه به اینکه، پروتکل الحاقی اول به کنوانسیون ۱۹۴۹ ژنو، حمله را عمل خشوت‌آمیز علیه دشمن تعریف کرده و اذعان داشته است که حمله مسلحانه یک عمل یا یک سلسله از عملیات نظامی مسلحانه است که هم شدت قابل توجهی داشته و هم نتایج آن تخریب زیرساخت‌های حیاتی دولت قربانی، قربانی کردن مردم و محروم ساختن دولت از دارایی‌های فیزیکی همچون قلمروش است، نتیجه می‌گیریم که در خصوص اینکه آیا حمله سایبری به حد حمله مسلحانه می‌رسد یا خیر، باید بر نتایج حوادث تکیه نمود و در نتیجه باید تحلیلی تأثیرگرایانه از یک حمله سایبری را در شناخت یک وضعیت به‌عنوان مخاصمه مسلحانه، - که دستورالعمل تالین ۲ آن را وضعیتی معرفی می‌کند که مشتمل بر عملیات‌های خصمانه بوده و به عملیات‌های انجام شده با به‌کارگیری ابزارهای سایبری اشاره دارد - مد نظر قرار داد.

دستورالعمل تالین ۲، نیز، دیدگاه مخالفی را مطرح ساخته است که تصدیق می‌نماید براساس قضیه نیکاراگوئه هرگونه استفاده غیرقانونی از زور که حمله مسلحانه به شمار می‌آید، موجب بروز حق دفاع از خود می‌گردد؛ هیچ آستانه شدتی وجود ندارد که توسل به زور را از حمله مسلحانه تفکیک کند و به این ترتیب، هیچ فاصله‌ای میان توسل به زور غیرقانونی و حمله مسلحانه وجود ندارد، هرچند ممکن است اصول ضرورت و تناسبِ قابل اِعمال بر اقدامات معطوف به دفاع از خود پاسخ‌های قابل اعمال برای دولت مورد حمله را محدود سازند. رویکرد اخیر، بیانگر آن است که احتمال دارد دولت‌ها از جمله در حین اتخاذ تصمیم راجع به توصیف یک عملیات همچون عملیاتی سایبری به‌عنوان توسل به زور، عواملی را که ذیلا بیان می‌شود مطمح نظر قرار دهند و اهمیت قابل توجهی برای آن‌ها قائل شوند. لازم به تأکید است که این عوامل صرفاً اسبابی هستند که انجام ارزیابی از سوی دولت‌ها راجع به توسل به زور را تحت تأثیر قرار می‌دهند؛ این عوامل معیارهایِ حقوقی رسمی نمی‌باشند.

۱- شدت

پیامدهای متضمن آسیب فیزیکی به افراد یا اموال فی‌النفسه ولنفسه عملیات سایبری را واجد وصف توسل به زور می‌نمایند. پیامدهایی که صرفاً موجب مزاحمت یا رنجش می‌گردند، هرگز توسل به زور قلمداد نمی‌شوند. در حالت بینابین، هر چقدر که پیامدهای مربوطه از منافع ملی حیاتی بیشتر تخطی کنند، در توصیف عملیات سایبری به‌عنوان

توسل زور نقش بیشتری خواهند داشت. در این رابطه، دامنه، مدت زمان و تراکم پیامدها تأثیر چشمگیری بر سنجش شدت آن‌ها خواهد داشت. شدت، مهم‌ترین عامل در این تحلیل است.

۲- فوریت

هر مقدار که پیامدها زودتر بروز پیدا کنند، دولت‌ها فرصت کمتری را برای توسل به حل و فصل مسالمت‌آمیز یک اختلاف یا به طریقی دیگر پیش‌بینی آثار آسیب‌زای آن‌ها خواهند داشت.

۳- بی‌واسطگی

هر چقدر فاصله علت و معلولی، میان عمل ابتدایی و پیامدهای آن بیشتر باشد، احتمال کمتری وجود دارد که دولت‌ها عامل مربوطه را ناقض ممنوعیت به‌کارگیری زور قلمداد کنند. در حالی که عامل فوریت بر جنبه موقتی پیامدهای مورد نظر تمرکز دارد، بی‌واسطگی زنجیره عِلّی را بررسی می‌نماید.

۴- میزان نفوذپذیری (Invasiveness)

میزان نفوذپذیری به مقدار نفوذ اقدامات سایبری در دولت هدف و سامانه‌های سایبری آن برخلاف منافع آن دولت دلالت دارد. به‌عنوان یک قاعده، هر قدر یک سامانه سایبری هدف ایمن‌تر باشد، نگرانی راجع به نفوذ در آن بیشتر است، برای مثال، نفوذ در سامانه‌ای نظامی که دارای گواهینامه بیمه ارزیابی سطح ۷ ((Evaluation Assurance Level 7 (EAL7)) مطابق با استاندارد امنیتی معیارهای مشترک [ارزیابی امنیتی فناوری اطلاعات] (۲۲) است، نسبت به بهره‌برداری صرف از آسیب‌پذیری‌های یک سامانه فاقد گواهی‌نامه و همگانی در دانشگاهی غیرنظامی یا کسب و کارهای کوچک، شدت رخنه‌گری بالاتری دارد (۲۳). به‌علاوه، هر قدر آثار قصد شده از عملیاتی سایبری محدود به کشوری خاص باشد، شدت رخنه‌گری متصوره از آن عملیات بالاتر است.

نام دامنه، شاخصی بسیار نمایان در فضای سایبر است و می‌تواند در ارزیابی شدت رخنه‌گری متصور از یک عملیات واجد اهمیت باشد. عملیات‌های سایبری که به طور خاص نام دامنه یک دولت معین (همچون «mil.ee») یا ارگان یک دولت مشخص را هدف قرار می‌دهند را می‌توان به این سبب نسبت به عملیات‌هایی که علیه پسوندهایِ نام دامنه خاص غیردولتی مانند «com.» هدایت می‌گردند، دارای شدت نفوذپذیری بیشتری دانست.

۵- سنجش‌پذیری آثار

این عامل از تمایل بالای کشورها به توصیف اقدامات به‌عنوان به‌کارگیری زور زمانی که پیامدها آشکار هستند ناشی می‌شود. از دیرباز، نیروهای مسلح، مبادرت به عملیات‌هایی نموده‌اند که به‌کارگیری زور به شمار آمده است و آثار عملیات‌ها (همچون مورد ارزیابی‌های مربوط به خسارت نبرد) عموماً قابل ارزیابی بوده‌اند. در عرصه سایبر، ممکن است پیامدها کمتر آشکار و مشخص باشند. بنابراین، هر قدر که مجموعه پیامدها قابل سنجش‌تر باشد، ارزیابی وضعیت برای دولت در حین تعیین رسیدن یا نرسیدنِ عملیات سایبریِ مورد نظر به سطح به‌کارگیری زور آسان‌تر خواهد بود.

۶- ماهیت نظامی

وجود پیوند میان عملیات سایبری مورد نظر و عملیات‌های نظامی، احتمال توصیف به‌عنوان به‌کارگیری زور را بالا می‌برد. این گزاره با این واقعیت که منشور ملل متحد به‌طور خاص به اقدامات نظامی می‌پردازد تقویت می‌شود. مقدمه منشور مقرر می‌دارد که «جز در راستای منفعت مشترک، از نیروی مسلح استفاده نخواهد شد»، در حالی که ماده ۴۴ منشور، در وضعیتی که آشکارا بر به‌کارگیری زور نظامی دلالت دارد از اصطلاح «زور» بدون واژه توصیفی «مسلح» استفاده می‌کند. به‌علاوه، به‌کارگیری زور از دیرباز به‌عنوان حکایت کردن از استفاده از زور توسط نیروهای نظامی یا دیگر نیروهای مسلح فهم شده است. ماهیت نظامی زیرساخت سایبریِ هدف عملیات سایبری نیز ملاحظه‌ای است که دولت‌ها مطمح نظر قرار خواهند داد (۲۴).

۷- مشارکت دولت

میزان مشارکت دولت در عملیات سایبری در گستره‌ای از عملیات‌هایی که توسط خود دولت انجام می‌شوند (مثل فعالیت‌های نیروهای مسلح یا عوامل اطلاعاتی آن) تا مواردی که دخالت دولت در آن ثانوی و جزئی است را دربر می‌گیرد. به هر میزان که پیوند میان یک دولت و عملیات‌های سایبری آشکارتر و نزدیک‌تر باشد، احتمال توصیف آن عملیات‌ها به‌عنوان توسل به زور توسط آن دولت از سوی دیگر دول بیشتر خواهد بود.

۸- مشروعیت فرضی

حقوق بین‌الملل به‌طورکلی، واجد ماهیتی منع‌کننده است. اعمالی که ممنوع نیستند مجازند؛ به این ترتیب، در غیاب ممنوعیت صریح معاهداتی یا ممنوعیت عرفیِ پذیرفته‌شده، یک عمل، قانونی فرض می‌شود، برای نمونه، حقوق بین‌الملل، تبلیغات، عملیات‌های روانی، جاسوسی یا صرف فشار اقتصادی را به خودی خود منع نمی‌کند.

عوامل پیش‌گفته حصری نیستند، بلکه، بسته به شرایط پیرامونی، ممکن است دولت‌ها به دیگر عوامل همچون فضای غالب سیاسی، حکایتِ عملیات سایبری از توسل به زور نظامی در آینده، هویت مهاجم، سابقه عملیات‌های سایبری مهاجم و ماهیت هدف (مانند زیرساخت حساس) توجه کنند (۱۱).

حملات سایبری، برای برخی دولت‌ها، بسیار مؤثرتر از حملات معمول است، به دلیل اینکه کشورهای بسیار صنعتی دارای بیشترین وابستگی به کامپیوتر هستند پس بیشتر در برابر حملات سایبری آسیب‌پذیر هستند، حملات سایبری ممکن است یک سلاح قدرتمندتر برای آنها محسوب شود. این تغییر در ساختار قابلیت‌های تهاجمی، احتمال حملات سایبری را افزایش می‌دهد. به این ترتیب، دولت‌های قوی‌تر ممکن است به خاطر خوانش‌های گسترده‌تر از بند ۴ ماده ۲ منشور ملل متحد، فعالیت‌های اجباری مانند حملات سایبری را ممنوع کنند (۱۳).

حمله سایبری به‌عنوان مخاصمه مسلحانه

در مواردی که حملات سایبری، توسط نیروهای مسلح منظم به موازات حملات مسلحانه زمینی، هوایی و دریایی به قلمرو یک کشور صورت گیرد، شبیه آنچه در حملات سایبری علیه گرجستان واقع شد؛ تردیدی در مخاصمه مسلحانه بودن آن وجود ندارد.

در غیاب اثرات تخریب مستقیم، براساس قطعنامه ۵۸/۱۹۹ مجمع عمومی سازمان ملل متحد در سال ۲۰۰۴، تفسیر مناسب از ضابطه میزان و اثر باید با مراجعه به مفهوم «زیرساخت‌های حیاتی» که حفاظت از آنها در امنیت سایبری دولت نقش اساسی دارد، صورت گیرد. نقش مفهوم زیرساخت‌های حیاتی در حملات سایبری، بسیار پررنگ است، زیرا حمله سایبری علیه شبکه رایانه‌ای هر ساختار غیرنظامی را نمی‌توان حمله مسلحانه دانست؛ بلکه این ساختارها باید زیرساخت‌های حیاتی محسوب شوند. در سطح بین‌المللی، اجماعی درباره زیر ساخت‌های حیاتی وجود ندارد.

مجمع عمومی سازمان ملل بیان داشته که هر کشوری، خود زیرساخت‌های حیاتی اطلاعاتی‌اش را مشخص می‌سازد؛ همچنین، قطعنامه مذکور اعلام نمود که زیرساخت‌های حیاتی شامل زیرساخت‌هایی می‌شود که برای تولید، انتقال و توزیع انرژی، حمل و نقل دریایی و هوایی، سرویس‌های مالی و بانکداری، تجارت الکترونیک، ذخایر آبی، توزیع غذا و بهداشت عمومی مورد استفاد قرار می‌گیرد و از همه مهم‌تر زیرساخت‌های حیاتی اطلاعاتی که به شکل روزافزونی به هم پیوستگی آنها بیشتر شده و عملکرد سایر زیرساخت‌ها را تحت تأثیر قرار می‌دهد.

سازمان همکاری‌های شانگهای هم در مقدمه توافقنامه همکاری‌های کشورهای عضو، زیرساخت‌های حیاتی را شامل امکانات، تسهیلات، سیستم‌ها و نهادهای عمومی که حمله علیه آنها نتایج مستقیمی بر امنیت ملی از جمله اشخاص، جامعه و دولت خواهد داشت، می‌داند.

مرکز استراتژی ایالات متحده نیز زیرساخت‌های حیاتی را چنین برشمرده است:

«دارایی‌های مادی و سایبری، تأسیسات عمومی و خصوصی در زمینه کشاورزی، غذا، آب، سلامت عمومی، سرویس‌های اورژانس دولت، انرژی، اطلاعات، ارتباطات، حمل و نقل، بانکداری و امور مالی، مواد سمی و شیمیایی، امور پستی و کشتیرانی» (۲۵).

به این ترتیب، به نظر می‌رسد جامعه بین‌المللی می‌بایست فهرستی از زیرساخت‌های بنیادین هر دولت را اعلام و منتشر نماید تا چنانچه این زیرساخت‌ها در معرض حملات سایبری قرار گیرند، دولت بتواند با تحقق شروط ابتدایی انتساب و توصیف این حملات به آن درجه‌ای که در قواعد سنتی مقرر شده - که از شروط دفاع مشروع است - از روی حسن نیت اقدام به پاسخگویی نماید؛ می‌توان گفت که زیرساخت‌های

حیاتی همان سرمایه‌های فیزیکی هستند که پایداری کشورها بدان‌ها وابسته است. چنین استثنایی باعث تغییر اساسی در چارچوب حقوق حاکم بر توسل به زور نخواهد شد و به یک دولت اجازه خواهد داد تا به اعمال حق ذاتی دفاع از خود در پاسخ به یک تهدید نوین بپردازد.

به علاوه، نظر دیوان بین‌المللی دادگستری (۲۱) بر این بوده که حمله مسلحانه می‌بایست با قصد معین وارد آوردن صدمه‌هایی از قبیل مرگ و میر ناشی از صدمه به رایانه‌های کنترل‌کننده دستگاههای احیاء بیماران، قطع گسترده شبکه‌های برق که اثرات زیانبار قابل توجهی دارد، خاموش کردن و قطع برق رایانه‌های کنترل‌کننده سدها و دستگاههای آبرسان و در نتیجه جاری شدن سیل به مناطق مسکونی، طراحی تصادفات عمدی مثلاً در نتیجه دادن اطلاعات غلط به رایانه‌های هواپیما باشد.

از سوی دیگر، با توجه به نظر مشورتی دیوان بین‌المللی دادگستری (۲۶) «ممانعت از هر نوع توسل به زور، بدون توجه به تسلیحات به کار گرفته شده» است؛ تردیدی نیست که، عملیات سایبری، از این جهت که اثرات آنها قابل مقایسه با سلاح‌های شیمیایی، بیولوژیکی یا هسته‌ای است، تحت حکومت بند ۴ ماده ۲ منشور ملل متحد قرار می‌گیرند. این قطعاً شامل استفاده از عملیات سایبری به‌عنوان ابزار تهاجمی یا دفاعی که برای کشتن یا وارد کردن آسیب به افراد یا تخریب زیرساخت‌ها، هم می‌شود، بدون توجه به اینکه این چنین تخریبی، شامل خسارات فیزیکی، صدمات کارکردی یا هردوی آنها باشد (۲۷).

دیوان بین‌المللی دادگستری در سال ۱۹۸۶ در قضیه نیکاراگوئه (۲۸) تأکید کرد تعریفی از حمله مسلحانه نه در منشور و نه در حقوق قراردادی نشده است. با این وجود، دیوان در رأی مشورتی خود درباره سلاح‌های هسته‌ای ۱۹۹۶، متذکر شد که ماده ۵۱ منشور اشاره به سلاح خاصی نداشته و درخصوص هرگونه توسل به زور صرف نظر از نوع سلاح کاربردی اعمال می‌شود. درواقع نه نقش یک ابزار، نه استفاده معمول از یک اسلحه، آن را سلاح نمی‌سازد؛ بلکه قصدی که پشت توسل به آن سلاح نهفته است و اثرات آن است که آن را سلاح می‌سازد. به عبارت دیگر کاربرد هرگونه ابزار یا تعدادی از ابزارها که با قصد وارد آوردن ضرر و زیان قابل توجه به زندگی افراد و تخریب گسترده اموال، همراه می‌شود، از شروط حمله مسلحانه می‌باشد (۲۹). این نتیجه‌گیری، با تأیید حق دفاع مشروع ایالات متحده در پاسخ به حملات ۱۱ سپتامبر ۲۰۰۱ توسط شورای امنیت تقویت می‌شود. زیرا سلاح‌های به کار گرفته شده در آن قضیه، هواپیماهای ربوده شده بودند (۲۱).

اعمال حقوق مخاصمات مسلحانه بر حملات سایبری

منشور ملل متحد، ضمن بند ۴ ماده ۲، که از اصول منشور ملل متحد و جزئی از حقوق بین‌الملل عرفی است تمام دولت‌های جهان را ورای طبیعت قراردادی منشور ملل متحد، ملزم و متعهد می‌نماید، از توسل به زور در حد گسترده، خودداری نمایند، در این بند آمده است «دول عضو در روابط بین‌المللی خود، مکلفند از تهدید و یا توسل به زور علیه تمامیت ارضی و استقلال سیاسی دولت‌ها و یا از هر شیوه‌ای که مغایر با اهداف منشور ملل متحد باشد، خودداری نمایند».

درواقع برای تحقق وضعیت جنگی و شمول حقوق مخاصمات مسلحانه، ضرورتی ندارد که یک دولت، عملاً درگیر جنگ باشد، ازاین‌رو، در جایی که درگیری واقعی رخ نداده است، ممکن است جنگ در حال وقوع باشد. همچنین، بند ۴ ماده ۲ منشور ملل متحد، نه فقط توسل رسمی به زور، از طریق اعلان جنگ را ممنوع می‌داند، بلکه توسل به زور به صورت غیررسمی را هم ممنوع می‌کند (۱۶). درواقع، زمانی که یک مخاصمه مسلحانه رخ می‌دهد، حقوق بین‌الملل بشردوستانه است که بر این وضعیت حاکم می‌باشد فارغ از اینکه آیا مخاصمه مسلحانه موجود مطابق با حق برجنگ باشد یا نباشد؛ به این ترتیب، قابلیت اِعمال حقوق مخاصمات مسلحانه به قرار گرفتن وضعیت ذیل حقوق توسل به زور بستگی ندارد. وفق اصل اِعمال برابر، حتی نوعی از توسل به نیروی مسلح که از چشم‌انداز حقوق توسل به زور غیرقانونی است نیز مشمول حقوق مخاصمات مسلحانه است (۱۱ و ۳۰).

توسل به زور و حمله مسلحانه، ضوابطی هستند که اهداف هنجاری متفاوتی دارند. ضابطه «توسل به زور» به منظور

تعیین نقض یا عدم نقض ماده ۲(۴) منشور ملل متحد و ممنوعیت مربوط به آن در حقوق بین‌الملل عرفی به کار می‌رود. در مقابل، مفهوم حمله مسلحانه با امکان یا عدم امکان واکنش دولت هدف به یک اقدام همراه با توسل به زور و بدون اینکه خود ممنوعیت توسل به زور را نقض نماید سروکار دارد. این تفکیک، مهم است، زیرا صرف وقوع توسل به زور به تنهایی به‌کارگیری زور در پاسخ به آن را توجیه نمی‌کند؛ به این ترتیب، دولت‌های مواجه با به‌کارگیری زوری که حمله مسلحانه به شمار نمی‌آید، در صورتی که خواستار پاسخ قانونی هستند باید به دیگر اقدامات نظیر اقدامات متقابل یا اعمال سازگار با اصل ضرورت متوسل شوند (۱۱).

قاعده ۸۰ دستورالعمل تالین ۲، در مورد اینکه حقوق مخاصمات مسلحانه در خلال مخاصمات مسلحانه بین‌المللی و غیربین‌المللی، بر چنین فعالیت‌هایی اِعمال می‌گردد تأکید دارد (۳۲-۳۱). مخاصمه مسلحانه، در دستورالعمل مذکور، به وضعیتی مشتمل بر عملیات‌های خصمانه شامل عملیات‌های انجام شده با به‌کارگیری ابزارهای سایبری اشاره دارد؛ اصطلاح «عملیات‌های سایبری»، «حملات سایبری» را دربر می‌گیرد، ولی محدود به آن‌ها نیست. حملات سایبری، اصطلاحی فنی[1] است که به دسته‌ای خاص از عملیات‌های سایبری اشاره دارد، به‌علاوه پاره‌ای از عملیات‌های سایبری مانند عملیات‌هایی که ارائه یاری‌رسانی بشردوستانه را تحت تأثیر قرار می‌دهند، حتی اگر به سطح یک «حمله» نرسند، تابع حقوق مخاصمات مسلحانه هستند. ابعاد دقیق حقوق مخاصمات مسلحانه که اِعمال می‌گردند، به ماهیت بین‌المللی یا غیربین‌المللی مخاصمه بستگی دارند.

اعمال حقوق مخاصمات مسلحانه بر حملات سایبری در شرایط سه‌گانه متمایزی مطرح می‌شود:

۱- در طول یک مخاصمه مسلحانه سنتی

درگیری میان روسیه و گرجستان در سال ۲۰۰۸ به‌عنوان اولین نمونه از یک مخاصمه مسلحانه که همراه با حملات سایبری صورت گرفته، پذیرفته شده است. حملات سایبری متصل به عملیات نظامی ارتش که امکان انتساب آنها به یکی از طرفین اختلاف وجود داشته باشد، به محض شروع، تحت شمول حقوق بشردوستانه قرار می‌گیرند (۳۳). قاعده ۲۰ دستورالعمل تالین ۱، همچنین، قاعده ۸۰ دستورالعمل تالین ۲، به وضوح اعلام می‌کنند که در صورت وقوع حمله سایبری در طول یک مخاصمه مسلحانه بین‌المللی، قواعد حقوق مخاصمات مسلحانه، بر همه حملات سایبری در طول آن مخاصمه، مجری خواهد بود.

۲- حملات سایبری مستقل

ویروس استاکس نت در سال ۲۰۱۰-۲۰۰۹ که به تأسیسات هسته‌ای ایران حمله کرد نمونه حملات مستقل سایبری است که باعث شد بسیاری از سانتریفیوژها برداشته شوند و باعث خرابی‌های بیش از حد انتظار بود. با توجه به تفسیر پیکته از ماده ۲ مشترک کنوانسیون‌های چهارگانه ژنو و رویه عملی دولت‌ها حاکی از آن است که حمله سایبری یک گروه وابسته به دولت به قصد ایراد صدمه و خسارت فیزیکی به اموال یا جان اشخاص، شروع یک مخاصمه مسلحانه تلقی می‌شود.

۳- حملات سایبری در راستای حمایت از حملات سنتی

هنگامی که حمله سنتی با سلاح متعارف، آغاز شده است و به خودی خود، واجد شرایط یک مخاصمه مسلحانه نیست و ممکن است به وسیله حمایت یک حمله سایبری به چنین سطحی از شدت و آسیب برسد. در چنین شرایطی، همراهی و توأمان شدن حملات سایبری، به‌عنوان شاخصه‌ای از قصد طرف مقابل به کار گرفته می‌شود (۳۴).

باید در نظر داشت که اعمال حقوق مخاصمات مسلحانه بر عملیات‌های سایبری می‌تواند دردسرساز باشد. غالباً تشخیص وجود حمله‌ای سایبری، منشأ آن، هدف قصد شده از حمله یا اثرات دقیق حمله ذیربط دشوار است. با این حال، این مسائل موضوعی، به اعمال حقوق مخاصمات مسلحانه خدشه‌ای وارد نمی‌سازند.

به نظر می‌رسد، تا زمانی که قاعده صریحی از حقوق مخاصمات مسلحانه، فعالیت‌های سایبری را انتظام نبخشد، باید به شرط مارتنز (The Martens Clause) که در کنوانسیون چهارم لاهه، کنوانسیون‌های ۱۹۴۹ ژنو (۳۶-۳۵) و پروتکل اول الحاقی (۳۷). یافت می‌شود توجه کرد. متن کنوانسیون چهارم لاهه مقرر می‌دارد:

1. Term of art

«تا زمان صدور مجموعه‌ای کامل‌تر از قواعد جنگ، طرفین معظم متعاهدین اعلام این نکته را مقتضی می‌پندارند که در موارد گنجانده نشده در مقررات اتخاذی توسط آن‌ها، ساکنین و متخاصمین تحت حمایت و حکومتِ اصول حقوق ملل، به گونه‌ای که از استعمال مسلم در میان مردمان متمدن ناشی شده‌اند، قواعد انسانیت و تعالیم وجدان عمومی باقی می‌مانند»؛ به این ترتیب، تا هر زمان که فعالیت‌های سایبری در جریان مخاصمه‌ای مسلحانه انجام شوند، شرط مارتنز که بازتاب حقوق بین‌الملل عرفی است، به منظور تضمین اینکه چنین فعالیت‌هایی در خلأ حقوقی صورت نمی‌گیرند عمل می‌کند و این نکته به مسئله متنازع‌فیه قابلیت اعمال حقوق بین‌الملل بشر در خلال مخاصمه مسلحانه خدشه‌ای وارد نمی‌سازد (۱۱).

نتیجه‌گیری

رعایت حقوق مخاصمات مسلحانه، به‌عنوان مجموعه قواعدی برای قانونمند نمودن و محدود ساختن اعمال ارتکابی در زمان وقوع مخاصمه، مستلزم شناسایی یک وضعیت به‌عنوان مخاصمه مسلحانه است. آن‌گونه که از ماده ۲ مشترک کنوانسیون‌های چهارگانه ژنو ۱۹۴۹، برمی‌آید، مخاصمه مسلحانه بین‌المللی، وضعیتی است که یک یا چند دولت، در مقابل دولتی دیگر، متوسل به نیروی مسلح شوند؛ علاوه بر این، عدم اعلام حالت جنگ یا عدم شناسایی آن از سوی طرفین مخاصمه، ملاک و ضابطه‌ای برای تشخیص مخاصمات مسلحانه بین‌المللی نیست و هر اختلافی که میان دولت‌ها باعث درگیری مسلحانه میان دولت‌ها شود، مطابق این ماده، مخاصمه مسلحانه بین‌المللی محسوب است؛ حملات سایبری، با توجه به دستورالعمل‌های تالین ۱ و ۲، عملیات سایبری تهاجمی یا تدافعی است که از آن به‌طور معقول، انتظار ایراد صدمه یا مرگ به اشخاص یا وارد کردن خسارت به اشیا می‌رود، اما در تعریفی که حقوقدانان ارائه داده‌اند، حملات سایبری عبارتند از هر اقدامی که به منظور تخریب کارکرد شبکه‌های کامپیوتری انجام شده و یک هدف امنیت ملی یا سیاسی ورای آن وجود دارد. در راستای رعایت حقوق مخاصمات مسلحانه در مورد حملات سایبری، لازم است اثبات کنیم که حملات سایبری، عنوان مخاصمه را دارا هستند. لذا، با مرور ماده ۲ مشترک، به سه معیار در رابطه با رعایت حقوق مخاصمات مسلحانه مواجه می‌شویم که عبارتند از مخاصمه مسلحانه، جنگ اعلان شده و اشغال یک سرزمین؛ به‌علاوه، اجماع بین‌المللی بر این عقیده است که مخاصمه برای اینکه شرایط مخاصمه مسلحانه را دارا شود باید از شرایط خاصی که دستورالعمل تالین ۲ به خوبی تشریح نموده است، شامل شدت، فوریت، بی‌واسطگی، میزان نفوذپذیری، سنجش‌پذیری آثار، ماهیت نظامی، مشارکت دولت و مشروعیت فرضی برخوردار باشد.

در بررسی مخاصمات مسلحانه غیرمتعارف، با سه رویکرد مواجه هستیم که عبارتند از رویکرد مبتنی بر ابزار، رویکرد مبتنی بر آثار و رویکرد مبتنی بر مسئولیت مطلق؛ رویکرد مبتنی بر آثار، پذیرفته‌تر بوده و این به آن معنی است که حمله سایبری، در صورتی که آثاری چون حملات سنتی داشته باشند و به زعم دستورالعمل تالین ۲ با قصد تخریب زیرساخت‌های حیاتی صورت گرفته باشد، مشمول قواعد حقوق مخاصمات مسلحانه خواهند بود. به این ترتیب، بر مبنای آنچه به‌عنوان فرضیه پژوهش، مورد نظر بوده است، اعمال قواعد حقوق بشردوستانه، زمانی نسبت به حملات سایبری امکان‌پذیر است که این حملات به یک دولت خاص منتسب شده و همچنین، حملات مذکور، منجر به ایراد صدمه، مرگ، خسارت یا تخریب مشابه با حملات متعارف‌شده و چنین نتایجی نسبت به حملات مزبور قابل پیش‌بینی باشد؛ این حملات، می‌بایست براساس معیارهای مورد اشاره در دستورالعمل تالین ۲، تحت عنوان مخاصمه مسلحانه قابل شناسایی باشد؛ حتی اگر این حمله در طول حمله سنتی صورت نگرفته باشد. علاوه بر رعایت قواعد حقوق مخاصمات مسلحانه، در غیاب مجموعه‌ای کامل‌تر از قواعد جنگ، طرفین با توجه به شرط مارتنز، پایبند به قواعد انسانیت و تعالیم وجدان عمومی باقی می‌مانند.

References

1. Ottis R, Peeter L. Cyberspace: Definition and Implications Cooperative Cyber Defence of Excellence. Tallin Estonia; 2010. p. 2.

2. Board of Authors and Editors of Microsoft Publication. Microsoft Computer Dictionary. Translate by Gholizadeh Nouri Farhad. 1th. Tehran: Azar Publication; 2002. p. 195.

3. www.library.arizona.edu

4. EastWest Institute. The Russia-US Bilateral on Cybersecurity Critical Terminology Foundations; 2011. p. 20.

5. Passive Defense Strategic Document; 2015. p. 4, 3.

6. Chaharbakhsh VB, Ghasemi A. Cyber Attacks and international Law. The Judiciary's Law Journal 2012; 78: 117.

7. Abbasi M, Moradi H. Cyber War From The International Humanitarian Law Perspective. Scientifi Quarterly Journal Of Majlis and Rahbord 2015; 81: 50, 47.

8. Esmailzadeh Mollabashi P, Abdollahi M, Zamani GH. Cyber-ttacks and The Princoples of International Humanitarian Law (Case Study: Cyber-attacks on Georgia). Quarterly Journal of Public Law Studies 2017; 47-2: 542.

9. Chayes A. Rethinking Warfare: The Ambiguity of Cyber Attacks. Harvard National Security Journal 2008; Vol 6. p. 480.

10. Tallinn Manual On The International Law Applicable To Cyber Warfare, Perpared by International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Center of Excellence. Cambridg university press; 2013. p. 47, No. 9.

11. Tallinn Manual 2.0 On The International Law Applicable To Cyber Operation, Perpared by International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Center of Excellence; 2017. p. 415. Rul 80, Para 2, 12. Para 4. Para 3. Rule 69, Para 9.

12. Jenkins AV. Defining the Parameters of Cyber war Operations: Looking for Law in All the wrong places. 51 Naval l. REV.132; 2005. p. 138.

13. Hathaway 0, Crootof R, Levitz PH, Nix H, Nowlan A, Perdue, Spiegel J. The Law of Cyber-Attack. California Law Review; 2012. Vol. 100. p. 825, 823, 828, 821, 842.

14. Clarke RA, Knake RK. Cyber War: The Next Threat to National Security and What to do about it; 2010. p. 70, 74.

15. Abdollahkhani A'. Soft War Information Warfare. 1th. Tehran: Abrar International Institute for Contemporary Cultural Studies and Research; 2007. p. 135.

16. Kolb R, Hyde R. An Introduction to the International Law of Armed Conflicts. Translate by Lesani Hesam Al-din. 1th. Tehran: Majd Publication; 2014. p. 123, 127, 25, 26.

17. Sharp WG. Cyber Space and the Use of Force. Aegin research corporation; 1999. p. 60, 61, 117.

18. Graham DE. Cyber Threats and the Law of War. Journal of National Security Law & Policy 2010; Vol 4: 87, 91.

19. Schmitt M. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. Columbia: Journal of Transnational Law; 1999. Vol. 37. p. 892, 914, 915.

20. Shulman MR. Discrimination in the Laws of Information Warfare. Col J Trans L; 1999. p. 7.

21. ICJ Report 1980. Case Concerning United States Diplomatic and Consular Staff in Tehran. S.C/Res/1308 (2001) of 12 Sept. and S.C/Res/1373 (2001) of 28 Sept. Parase 93, 95. 2003: para 64.

22. The Common Criteria for Information Technology Security Evaluation.

23. Common Criteria for Information Technology Security Evaluation, International Standard ISO/IEC 15408. ver. 3.1; July 2009.

24. DoD Manual; para. 16.3.1.

25. United States National Strategy Secure Cyberspace; 1999. www.dhs.gov/x. library/ assets/ national- cyberspace-strategy.pdf/

26. International Court of Justice, Legality of the Threat or Use of Nuclear Weapons. Advisory opinion; 1996. p. 39.

27. Melzer N. Cyber Warfare and International Law. The United nationa Institute for Disarmament Research (UNIDIR); 2011. p. 7.

28. Nicaragua v. United States of America - Military and Paramilitary Activities in and against Nicaragua. Judgment of 27 June 1986. Merits Judgments; 1986 ICJ 1; 27 June 1986. Para.176, 188.

29. Zemanek K. Armed attack Max Plank Encyclopedia of Public International Law; 2010. p. 21.

30. UK Manual, paras. 3.12, 3.12.1; ICRC Geneva Convention I 2016 Commentary, paras. 186, 215-216.

31. UN GGE 2015 Report; Para 28 (d).

32. Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Secretary General. at 2, UN Doc. A/69/112; 30 June 2014. Australia: Developments in the Field of Information and Telecommunications in the Context of International Security. Report of the Secretary General. Japan: at 15, UN Doc. A/68/156 Add. 1; 9 September 2013. European Union, Conclusions, General Affairs Council Meeting, Doc. 11357/13; 25 June 2013.

33. Harrison Dinniss H. Cyber Warfare and the Laws of War. Translate by Hakimiha Sa'id, Shahrokh Hooman. 1th. Tehran: Mizan Publication; 2016. p. 139.

34. Dinniss HH. Cyber Warfare and the Laws of War. Cambridge University Press; 2014. p. 126, 128.

35. Geneva Convention I; 1949. Art. 63

36. Geneva Convention II, Art. 62; Geneva Convention III, Art. 142; Geneva Convention IV, Art. 158.

37. Protocol I to the Geneva Conventions; Art. 1(2).