فصلنامهٔ مطالعات حقوق عمومی، دورهٔ ۴۹، شمارهٔ ۱، بهار ۱۳۹۸: ۱۳۹-۱۵۸
DOI: 10.22059/jplsq.2017.228162.1478

قابلیت اعمال قواعد حقوق بین‌الملل بشردوستانه در جنگ‌های سایبری

نازنین برادران[۱]*، همایون حبیبی[۲]

چکیده

در عصر اطلاعات با تغییر میدان‌های نبرد، جامعهٔ بین‌المللی در مواجهه با جنگ‌های سایبری است. حملات سایبری امروزه دستهٔ جداگانه از روش‌های جنگی را تشکیل می‌دهند و در عین حال می‌توانند نمایانگر نوع جدیدی از توسل به زور باشند، زیرا این توانایی را دارند که موجب ایجاد آثاری مانند صدمات عظیم و وسیع به زیرساخت‌های حیاتی یک دولت، تخریب اموال و از دست رفتن جان انسان‌ها شوند. به این ترتیب چه عملیات جنگی در یک مخاصمه تنها متشکل از حملات سایبری باشد و چه جنگ سایبری بخشی از یک مخاصمه با روش‌های متداول جنگی باشد، به‌هنگام کاربرد این روش نوین مخاصمه باید قواعد حقوق بین‌الملل بشردوستانه اعمال شود و دولت‌ها ملزم به رعایت این تعهدند که وسایل و شیوه‌های جدید مورد استفاده در جنگ ها، در تطابق با قواعد حاکم بر حقوق بین‌الملل بشردوستانهٔ موجود باشد. این مقاله درصدد است نشان دهد تا زمانی‌که قواعد خاص حقوق بشردوستانهٔ بین‌المللی در مخاصمات سایبری تدوین نشده باشد، همچنان می‌توان با توسل به اصول و قواعد موجود، روش‌های نبرد سایبری را در چارچوب حقوق بین‌الملل بشردوستانه به نظم درآورد.

کلیدواژگان

توسل به زور، حملات سایبری، حقوق بین‌الملل بشردوستانه، وسایل و شیوه‌های جنگ.

---

۱. استادیار، گروه حقوق، دانشکدهٔ حقوق و علوم انسانی، دانشگاه آزاد اسلامی، واحد شیراز، شیراز، ایران (نویسندهٔ مسئول). Email: na_baradaran@yahoo.com

۲. استادیار، گروه حقوق عمومی و بین‌الملل، دانشکدهٔ حقوق و علوم سیاسی، دانشگاه علامه طباطبایی، تهران، ایران. Email: homayounhabibi@gmail.com

تاریخ دریافت: ۱۳۹۵/۱۲/۰۲، تاریخ پذیرش: ۱۳۹۶/۰۷/۱۰

مقدمه: شناخت موضوع

اصل عدم توسل به زور، به‌عنوان یکی از اصول مهم سازمان ملل متحد، موضوع بند ۴ مادهٔ ۲ منشور است و در واقع سنگ بنای سازمان ملل متحد محسوب می‌شود، به‌نحوی که منع توسل به زور به جایگاه یک قاعدهٔ آمره در حقوق بین‌الملل رسیده و رعایت آن برای دول غیرعضو سازمان نیز الزامی است. در این ماده مقصود از زور، فقط زور نظامی است و سایر اقسام فشارها و اجبارهای سیاسی یا اقتصادی را در برنمی‌گیرد و ممنوعیت مطرح‌شده در آن نیز فقط شامل کاربرد زور نیست، بلکه تهدید به کاربرد آن را هم در برمی‌گیرد. بنابراین شاید تصور شود آنچه در بند ۴ مادهٔ ۲ منشور به‌عنوان منع استفاده از زور نظامی مطرح شده، استفاده از زور به‌وسیلهٔ سلاح‌های کلاسیک و شناخته شده است. اما منشور ملل متحد محصول گفتمان حقوقی بیش از شصت سال اخیر است و امروزه جنگ از مفهوم سنتی خود که در آن فقط از سلاح‌های کلاسیک استفاده می‌شد، فاصله گرفته و پیشرفت فناوری، ابزارهای جدیدی را در اختیار دولت‌ها قرار داده است که از جمله مهم‌ترین آنها استفاده از فضای سایبر جهت انجام حملات سایبری علیه دولت‌های مورد هدف است. در واقع امروزه فضای سایبر در حال تبدیل شدن به میدان جدید انجام عملیات نظامی است و به اذعان کارشناسان نظامی، فضای سایبر به‌عنوان یک عرصهٔ نوین جنگ، در حال ظهور است، این در حالی است که قدرت‌های بزرگ در حال تجهیز هرچه سریع‌تر و گسترده‌تر نیروهای خود برای جنگ‌های سایبری هستند. بنا به گزارش هیأت پانزده‌نفرهٔ متخصصان سازمان ملل متحد که در ژانویهٔ ۲۰۱۳ تهیه شده است[1]، امروزه چهل دولت در دنیا برای جنگ‌های سایبری تهاجمی خود را تجهیز کرده‌اند که نشانه‌های عملی این ادعا آن است که در سال‌های اخیر شاهد بروز موارد متعدد حملات سایبری میان دولت‌ها بوده‌ایم، برای مثال کشور آمریکا هدف حملات متعدد سایبری قرار گرفته که ادعا می‌شود از طرف کشور چین صورت گرفته است. مورد معروف دیگر، حملات سایبری سه‌هفته‌ای به کشور استونی در آوریل ۲۰۰۷ است که سبب ازکارافتادن وب‌سایت‌های رسمی دولتی، ایستگاه‌های تلویزیونی، بانک‌ها و... شد و ادعا می‌شود که از سوی فدراسیون روسیه صورت گرفته است. حملات سایبری علیه گرجستان در ژوئیه و اوت ۲۰۰۸ پیش از درگیری و نیز در جریان درگیری‌های مسلحانهٔ این کشور با فدراسیون روسیه اتفاق افتاد و سبب شد که وب‌سایت‌های دولتی از شبکه خارج شوند و تغییر شکل دهند و محتوای آنها با تبلیغات روسیه جایگزین شود (Shacketford, 2009: 204).

جمهوری اسلامی ایران نیز در سال ۲۰۱۰ میلادی از طریق کرم استاکس نت[2] هدف

1. On the Developments in the Field of Information and Telecommunications in the Context of International Securiy
2. Stuxnet

حملات سایبری با هدف ایجاد اختلال در فعالیت‌های هسته‌ای قرار گرفت و به تعدادی از سانتریفیوژهای فعال در مرکز هسته‌ای نطنز آسیب وارد شد و آمریکا و اسراییل مظنونان اصلی اجرای حملهٔ استاکس نت هستند.

حملات سایبری با پیچیدگی‌های فنی و تکنیکی خاصی همراهند که آنها را از حملات کلاسیک متمایز می‌سازد، مانند گمنامی و مشخص نبودن هویت اجراکنندگان حملات و نیز آثار مخرب مستقیم یا غیرمستقیم گسترده‌ای که این‌گونه سلاح‌ها می‌توانند ایجاد کنند. به همین دلیل برای درک بهتر ویژگی‌های مذکور توضیح برخی عبارات از جمله فضای سایبر و حملات سایبری ضروری است.

فضای سایبر فضایی غیرمادی و ناملموس است که توسط شبکه‌های رایانه‌ای به‌وجود آمده و دنیایی مجازی را در کنار دنیای واقعی ایجاد کرده است (فضلی، ۱۳۸۹: ۱۷). این فضا فراتر از اینترنت توسعه یافته است و تمامی فعالیت‌های دیجیتال شبکه‌ای را در برمی‌گیرد، فضای مذکور دارای گستره‌ای جهانی و بدون مرز، پوشیده و پنهان بوده و ماهیتاً برای آزادی گردش اطلاعات شکل گرفته است (پاکزاد، ۱۳۹۰: ۲۱۶).

اصطلاح «حملهٔ سایبری» می‌تواند پهنهٔ گسترده‌ای از اقدامات را شامل شود، ولی به لحاظ فنی می‌توان آن را تهاجم به امنیت داده‌ها دانست. هنگامی داده‌ها و اطلاعات موجود در شبکه‌ها را امن تلقی می‌کنیم که «محرمانه بودن»[1]، «یکپارچگی»[2] و «در دسترس بودن»[3] آن (که گاهی به‌اختصار CIA خوانده می‌شود) حفظ شده باشد. به این ترتیب هر گاه یکی از این اهداف امنیتی مورد تهدید واقع شده باشند، می‌توان از حملهٔ سایبری سخن گفت. حملاتی که در دسترس بودن را هدف قرار می‌دهند، سعی می‌کنند از دسترسی به شبکه (خواه از طریق اجرای حملات DoS[4]، خواه از طریق آفلاین کردن و خاموش کردن فیزیکی فرایندهای مجازی و...) جلوگیری کنند.

در حملاتی که محرمانه بودن را هدف قرار می‌دهند، مهاجمان تلاش می‌کنند به‌منظور نظارت بر فعالیت‌ها و استخراج اطلاعات سیستم‌ها و داده‌های کاربران، به شبکه‌های کامپیوتری نفوذ کنند. چالش واقعی این حملات هنگامی است که استخراج اطلاعات به روشی سازمان‌یافته و عظیم اتفاق بیفتد. در نهایت، حملاتی که یکپارچگی و صحت داده‌ها را هدف قرار می‌دهند، شامل ورود به سیستم برای تغییر و تخریب اطلاعات به‌جای استخراج آن می‌باشند.

اهداف و پیامدهای حملات بسیار متفاوت و گسترده است. اثر حمله می‌تواند صرفاً خرابکاری برای اهداف سیاسی باشد، مانند اینکه یک وب‌سایت دولتی توسط نفوذگران تغییر چهره دهد و در اصطلاح *Deface* شود.

---

1. Confidentiality
2. Integrity
3. Availability
4. Denial of Service Attacks

حمله ممکن است در پی آسیب رساندن عمده (و با ماهیت راهبردی) باشد. مانند صدمه زدن به توانایی‌های یک کشور برای پیاده‌سازی تصمیمات رسمی، دفاع از خود یا ارائهٔ خدمات به شهروندان (از طریق ارائهٔ سرویس خدمات شهری مانند برق، آب، مراقبت‌های بهداشتی و...).

به این ترتیب و با توجه به آثار متفاوتی که حملات سایبری ممکن است به‌بار آورند، این مسئله در حوزهٔ مباحث *حق بر جنگ* (توسل به زور) قابل طرح است که آیا این ابزارهای جدید، از جمله استفاده از فضای سایبر جهت انجام حملات سایبری، می‌توانند به‌مثابهٔ استفاده از زور نظامی موضوع بند ۴ مادهٔ ۲ منشور در نظر گرفته شوند و فراتر از آن آیا می‌توانند به آستانهٔ لازم برای ایجاد حملهٔ مسلحانه برسند، به‌گونه‌ای که براساس مادهٔ ۵۱ منشور ملل متحد امکان دفاع مشروع در مقابل آن حملهٔ مسلحانه وجود داشته باشد؟

هرچند هنوز در حوزهٔ حملات سایبری این مسئله نزد مراجع قضایی مطرح نشده، ولی می‌توان از آنچه دیوان بین‌المللی دادگستری در قضیهٔ فعالیت‌های نظامی و شبه‌نظامی آمریکا در نیکاراگوئه اعلام کرده است، نتیجه گرفت که آنچه تعیین‌کنندهٔ وقوع یک حملهٔ مسلحانه است، دامنه، مقیاس و آثار ایجادشده توسط آن حمله است (ICJ Rep, 1986: paras. 101,103,176).

از دیدگاه‌های دیوان در نظر مشورتی در مورد مشروعیت تهدید یا کاربرد سلاح‌های هسته‌ای نیز می‌توان استفاده کرد و گفت که چه در حمله و چه در دفاع نوع خاصی از سلاح موضوعیت ندارد و به این ترتیب ممنوعیت مادهٔ ۲ (۴) منشور در مورد هر گونه توسل به زوری صرف‌نظر از سلاح مورد استفاده قابل اعمال خواهد بود (ICJ Advisory Opinion, 1996: para.39).

به این ترتیب این حقیقت که در حملات سایبری از سلاح‌های کلاسیک استفاده نمی‌شود، به این معنا نیست که نمی‌توان آنها را به‌مثابهٔ حملهٔ مسلحانه در نظر گرفت (Roscini, 2010:114)، زیرا نحوهٔ طراحی یا استفادهٔ معمول از یک سلاح آن را به یک سلاح تبدیل نمی‌کند، بلکه مسئلهٔ مهم، قصدی است که متعاقب آن استفاده می‌شود و آثاری که به بار می آورد. بنابراین استفاده از هر نوع سلاح که به از دست رفتن جان انسان‌ها در سطحی وسیع یا تخریب اموال در سطحی گسترده منجر شود، می‌تواند به آستانهٔ لازم جهت ایجاد حملهٔ مسلحانه برسد (Zemanek, 2010: 21). برای مثال وقتی‌که حملهٔ سایبری به زیرساخت‌های حیاتی یک دولت صورت گیرد، به‌گونه‌ای که آسیب‌های انسانی و مالی وسیعی به‌بار آورد، به‌مثابهٔ یک حملهٔ مسلحانه محسوب می‌شود. البته شناسایی حملات سایبری به‌عنوان یک حملهٔ مسلحانه مسئلهٔ حقوقی پیچیده‌ای است و ثمرهٔ آن در مباحث حق بر جنگ[1] قابل ملاحظه است و خود می‌تواند به‌عنوان موضوع مستقلی مطالعه و ارزیابی شود. اما هر گاه حملهٔ

1. Jus ad Bellum

سایبری را بتوان یک حملهٔ مسلحانه تلقی کرد یا از این حملات به‌عنوان بخشی از عملیات مخاصمانهٔ یک طرف جنگ علیه طرف دیگر نام برد، سؤال دیگری نیز مطرح است و آن امکان و چگونگی اجرای قواعد حقوق بین‌الملل بشردوستانه در حین اجرای این حملات است. به این ترتیب باید به این پرسش پاسخ داده شود که آیا قواعد حقوق بین‌الملل بشردوستانه در حملات سایبری نیز باید رعایت شود؟ و با توجه به جدید و متفاوت بودن این روش‌ها و ابزارهای جنگی چطور می‌توان قواعد حقوقی از قبل موجود را بر آن بار کرد؟ در نوشتهٔ حاضر تلاش بر آن است که به این پرسش‌ها در قالب سه قسمت پاسخ داده شود.

اعمال قواعد حقوق بین‌الملل بشردوستانه در حملات شبکه‌ای کامپیوتری

پیش‌شرط قابلیت اجرای قواعد حقوق بین‌الملل بشردوستانه وجود یک مخاصمهٔ مسلحانه است. اصطلاح «مخاصمهٔ مسلحانه[1]» اولین بار در تدوین قواعد حقوق جنگ در کنوانسیون‌های ۱۹۴۹ ژنو به‌کار رفته است (Geneva Conventions I-IV,1949: art. 2.) و به وضعیت‌هایی گفته می‌شود که شامل درگیری و منازعه باشد. از مطالعهٔ مادهٔ دو مشترک کنوانسیون‌های ژنو این‌گونه استنباط می‌شود که نوع سلاح و روش جنگ اثری در قابلیت اجرای قواعد حقوق بین‌الملل بشردوستانه ندارد، بنابراین در مخاصمات سایبری یا عملیات سایبری در جریان سایر مخاصمات مسلحانه قابلیت اعمال دارد (Tallinn Manual on the International Law Applicable to Cyber Warfare , 2011:Rule.20) به‌عبارت دیگر، در این زمینه دو وضعیت ممکن است اتفاق بیفتد: حالت اول زمانی است که دو کشور در وضعیت صلح به‌سر می‌برند و توسل به زور از طریق حملهٔ سایبری توسط یک دولت علیه دولت دیگر سبب شروع مخاصمهٔ سایبری میان طرفین می‌شود. بدیهی است که در حالت مزبور حملهٔ سایبری مورد بحث باید به آستانهٔ لازم برای ایجاد حملهٔ مسلحانه رسیده باشد و به این ترتیب حملهٔ سایبری موردنظر واجد وصف حملهٔ مسلحانه به مفهوم کلاسیک آن می‌شود، برای مثال وقتی‌که حملهٔ سایبری علیه سیستم کنترل ترافیک هوایی یا تأسیسات اتمی صورت گیرد و آسیب‌های انسانی و مالی وسیعی به‌بار آورد، به‌مثابهٔ یک حملهٔ مسلحانه محسوب می‌شود و دولت حمله‌کننده موظف است، قواعد حقوق بین‌الملل بشردوستانه را در حملهٔ خود مدنظر قرار دهد.

حالت دوم زمانی است که در قالب و در اثنای یک مخاصمهٔ کلاسیک و سنتی از حملات سایبری در کنار ابزارهای سنتی به‌عنوان بخشی از ابزارها و روش‌های مخاصمه استفاده می‌شود،

1. Armed Conflict

مانند حملات سایبری علیه گرجستان در ژوئیه و اوت ۲۰۰۸ که در طول حملات مسلحانه با فدراسیون روسیه اتفاق افتاد. بنابراین با وجود جدید بودن عملیات سایبری نسبت به معاهدات حقوق بین‌الملل بشردوستانه و نبود قواعد معین و مشخص در حقوق جنگ که به‌طور واضح و مشخص در خصوص حملات سایبری وضع شده باشند، قواعد حقوق مخاصمات مسلحانه در چنین مواردی چه در مخاصمات بین‌المللی و چه داخلی قابل به‌کار بردن هستند.

طبقه‌بندی مخاصمات سایبری به لحاظ محدودهٔ جغرافیایی

به‌طور کلی، قلمرو اجرای قواعد حقوق بین‌الملل بشردوستانه به نوع مخاصمهٔ مسلحانه بستگی دارد. برای اینکه بدانیم چه قواعدی در هر مخاصمه به اجرا گذاشته می‌شود، ناگزیر از تعیین نوع مخاصمه با توجه به محدودهٔ جغرافیایی آن هستیم. مخاصمات بین‌المللی تابع مقررات مندرج در کنوانسیون‌های چهارگانهٔ ژنو و پروتکل اول الحاقی به این کنوانسیون‌ها هستند و مخاصمات غیربین‌المللی تابع مادهٔ سوم مشترک کنوانسیون‌های چهارگانه و پروتکل دوم الحاقی به این کنوانسیون‌ها می‌باشند و مشمول مجموعهٔ محدودتری از قواعد حمایتی‌اند. عملیات سایبری نیز با توجه به نوع مخاصمه ممکن است تابع قواعد متفاوتی باشند و از این نظر تفاوتی با سایر عملیات نظامی ندارند، ولی آنچه این عملیات را متفاوت می‌سازد، ویژگی بدون مرز فضای سایبر است. در عملیات سایبری ممکن است مکان انجام عملیات با مکان سیستم‌های سایبری مورد هدف لزوماً یکی نباشد و ممکن است این عملیات نه‌تنها از سوی یک دولت در کل سرزمین دولت دیگر که در فضاهای بین‌المللی مانند دریای آزاد یا از طریق فضای ماورای جو صورت پذیرد.

۱. طبقه‌بندی به‌عنوان مخاصمات مسلحانهٔ بین‌المللی

چنانچه درگیری مسلحانه‌ای میان دو یا چند کشور روی دهد، این درگیری را بین‌المللی می‌نامند. بر این نوع درگیری‌ها، حقوق بین‌الملل بشردوستانه و حقوق بین‌الملل بشر حاکم است. طبعاً اقدامات سایبری طرف‌های مخاصمه در این جنگ نیز تحت شمول مقررات ناظر بر مخاصمات بین‌المللی قرار می‌گیرد. اما در خصوص جنگ‌های صرفاً سایبری یک مخاصمهٔ مسلحانهٔ بین‌المللی زمانی وجود دارد که مخاصمات شامل یا محدود به عملیات سایبری باشد که بین دو یا چند دولت اتفاق می‌افتند. معیار پذیرفته‌شده برای وجود یک مخاصمهٔ مسلحانهٔ بین‌المللی از مادهٔ دو مشترک کنوانسیون‌های ۱۹۴۹ ژنو گرفته شده است. به این ترتیب شرایط لازم برای وجود یک مخاصمهٔ مسلحانهٔ بین‌المللی، وجود دو خصیصهٔ بین‌المللی بودن و درگیری‌های مسلحانه است (Geneva Conventions 1949, I-IV: art. 2).

همچنین یک مخاصمه زمانی‌که بازیگران غیردولتی درگیر در مخاصمات علیه دولت تحت

کنترل کلی یک دولت دیگر باشند نیز بین‌المللی تلقی می‌شود، البته در چنین مواردی تعیین اثبات اینکه آیا یک دولت فعالیت‌های سایبری یک بازیگر غیردولتی را کنترل می‌کند، امری مشکل خواهد بود (Tallinn Manual on the International Law Applicable to Cyber Warfare , 2011, Rule. 22: 2) این مسئله که چه زمانی اقدامات یک گروه مسلح سازمان‌یافته از بازیگران غیردولتی علیه یک دولت ممکن است به دولت دیگر منتسب شود، تا مخاصمهٔ بین‌المللی تلقی شود، موضوع مهمی است که باید به‌نحو مفصل‌تری تبیین شود که در این زمینه تحلیل رویهٔ قضایی بین‌المللی موجود مفید است. به‌طور مشخص در دادگاه کیفری بین‌المللی برای یوگسلاوی سابق در قضیهٔ تادیچ در رأی شعبهٔ تجدیدنظر این مسئله مطرح شده است .(ICTY, 1999: paras. 131-140, 145).

شعبهٔ تجدیدنظر معیار «کنترل کلی» را در تعیین اینکه آیا واحدهای صرب بوسنیایی به‌طور کافی تحت راهنمایی جمهوری فدرال یوگسلاوی بوده‌اند، به‌تفصیل بیان می‌کند. دادگاه می‌گوید کنترل توسط یک دولت بر روی نیروهای مسلح تابع یا شبه‌نظامیان یا واحدهای شبه‌نظامی ممکن است از ویژگی کلی برخوردار باشد (و باید شامل چیزی بیش از تهیهٔ کمک‌های مالی یا دادن تجهیزات نظامی یا آموزش باشد). به این ترتیب، نیازی نیست که اقدامات دولت شامل صدور دستورهای مشخص یا هدایت هر مورد از عملیات به‌طور جداگانه باشد. براساس حقوق بین‌الملل ضرورتی ندارد که مقامات کنترل‌کننده تمامی عملیات واحدهای وابسته به خود را کنترل کنند یا اهداف آنها را انتخاب کنند یا به آنها دستورهای مشخص مرتبط با اجرای عملیات نظامی را بدهند که به هر گونه نقض حقوق بشردوستانه منجر شود. کنترلی که به‌وسیلهٔ حقوق بین‌الملل ضروری است، زمانی وجود دارد که یک دولت (یا درزمینهٔ حقوق مخاصمات مسلحانه، طرف مخاصمه) در سازماندهی، هماهنگ‌سازی یا برنامه‌ریزی اقدامات نظامی گروه، علاوه‌بر کمک‌های مالی، آموزش، تجهیز کردن و فراهم آوردن کمک‌های عملیاتی به آن گروه دارای نقش باشد.

دیوان بین‌المللی دادگستری نیز اعلام کرده است تا جایی که به تعیین نوع مخاصمه مربوط است، معیار کنترل کلی «می‌تواند قابل اعمال و مناسب باشد» (ICJ Rep, 2007: para.404).

با استفاده از این معیار اگر دولت (الف) کنترلی کلی را بر روی یک گروه سازمان‌یافته از هکرهای کامپیوتری اعمال کند که در زیرساخت‌های سایبری دولت (ب) نفوذ کرده‌اند و موجب ایجاد صدمات فیزیکی جدی شده‌اند، جنگ مسلحانه، به لحاظ ماهیت، بین‌المللی تلقی می‌شود. لازم نیست که دولت (الف) گروه را به حمله به موارد خاصی از زیرساخت‌های دولت (ب) راهنمایی کند، بلکه فقط باید کنترل کافی بر روی گروه جهت اجرای حملات علیه زیرساخت‌های دولت هدف، اعمال کند.

به‌طور کلی استفاده از معیار *کنترل کلی* در زمینهٔ انتساب حملات سایبری به دولت، مورد

توافق گروه متخصصان بین‌المللی است که راهنمای تالین در مورد حقوق بین‌الملل قابل اعمال در جنگ‌های سایبری را تهیه کرده‌اند و هرچند در بین حقوقدانان بین‌المللی همچنان در خصوص قابلیت اعمال این قاعده برای تبیین مسئولیت بین‌المللی دولت اختلاف‌نظر وجود دارد، اما با توجه به رأی ذکرشده دیوان بین‌المللی دادگستری، می‌توان گفت این معیار در خصوص تعیین نوع مخاصمه حتماً قابل استفاده است.

علاوه‌بر بین‌المللی بودن، شرط ضروری دیگر برای وجود یک مخاصمهٔ مسلحانه بین‌المللی آن است که مخاصمه باید «مسلحانه»[1] باشد. قواعد حقوق جنگ به‌طور مستقیم مفهوم عبارت «مخاصمات مسلحانه» را توضیح نمی‌دهد، اما به‌طور واضح مفهوم آن دربرگیرندهٔ لزوم وجود «مخاصمات»[2] است. مخاصمات دربردارندهٔ کاربرد جمعی روش‌ها و ابزارهای جنگی است. مخاصمات می‌تواند شامل هر گونه ترکیبی از عملیات کلاسیک و سایبری باشد یا اینکه عملیات سایبری را به‌تنهایی در برگیرد. به هر حال، مخاصمات در هر زمانی‌که یک دولت درگیر حملهٔ سایبری علیه دولت دیگر باشد، وجود دارد.

هرچند وجود درگیری مسلحانه پیش‌شرط ضروری برای وجود مخاصمات بین‌المللی است، بحث بر سر آستانهٔ خشونت لازم همچنان ادامه دارد. براساس تفسیر کمیتهٔ بین‌المللی صلیب سرخ[3] از کنوانسیون‌های ۱۹۴۹ ژنو، «هر گونه تعارضی که بین دولت‌ها ایجاد شود و به مداخله‌ی نیروهای مسلح منجر شود، درگیری مسلحانه است. مهم نیست که مخاصمه چقدر به طول انجامد یا اینکه چقدر کشتار اتفاق بیفتد». (ICRC Geneva Convention 1 Commentary at 32; Geneva Convention II Commentary at 28; Geneva Convention III Commentary at 23, Geneva Convention IV Commentary at 20.)

برای مثال عملیات سایبری که به ایجاد آتش‌سوزی در یک تأسیسات نظامی کوچک منجر شود، کافی خواهد بود که یک مخاصمهٔ مسلحانهٔ بین‌المللی را آغاز کند و طرفی که چنین حملاتی را انجام داده است، از همان ابتدا ملزم به رعایت مقررات حقوق بین‌الملل بشردوستانه است.

۲. طبقه‌بندی به‌عنوان مخاصمات مسلحانهٔ غیر بین‌المللی

درگیری مسلحانهٔ غیر بین‌المللی، شامل جنگ داخلی به معنای اخص کلمه است. براساس مادهٔ ۳ مشترک عهدنامه‌های چهارگانهٔ ژنو، هر درگیری مسلحانه‌ای که بین‌المللی نباشد، غیربین‌المللی است. تعریف کلی و سلبی مذکور موجب شد تا پروتکل دوم الحاقی با تبیین و تجمیع معیارهای متعدد زیر درصدد توسعه و تکمیل تعریف درگیری مسلحانهٔ غیر بین‌المللی

1. "Armed"
2. "Hostilities"
3. International Committee of Red cross (ICRC)

در مادهٔ ۱ برآید: ۱. درگیری در قلمرو یکی از کشورهای متعاهد روی دهد؛ ۲. درگیری میان نیروهای مسلح یک کشور و نیروهای مسلح مخالف یا سایر گروه‌های مسلح سازمان‌یافته رخ دهد؛ ۳. نیروها یا گروه‌های مذکور تحت یک فرماندهی مسئول عمل کنند؛ ۴. نیروها یا گروه‌های مذکور بر بخشی از قلمرو یک کشور متعاهد کنترل داشته باشند، به‌گونه‌ای که بتوانند عملیات نظامی را به‌صورتی مداوم و متمرکز انجام دهند و به مقررات پروتکل عمل کنند.

در مقابلِ دیدگاه بلندنظرانهٔ مادهٔ ۳ مشترک، دیدگاه محدود پروتکل دوم موجب شد تا بسیاری از درگیری‌های مسلحانهٔ داخلی که حتی یکی از معیارهای مذکور در پروتکل را فاقد باشد، درگیری مسلحانهٔ غیربین‌المللی طبق پروتکل دوم محسوب نشود.

به‌منظور تعدیل دو دیدگاه مذکور، دادگاه بین‌المللی کیفری برای یوگسلاوی سابق، تعریف جدیدی از درگیری مسلحانهٔ داخلی ارائه داد. در این تعریف تجمیع سه معیار ملاک قرار گرفت: درگیری در قلمرو یک کشور، درگیری میان نیروهای دولتی و گروه‌های مسلح مخالف دولت یا گروه‌های مسلح مخالف با یکدیگر و بالاخره درگیری طولانی‌مدت (ضیایی بیگدلی، ۵۲:۱۳۹۲ و ۵۳).

در خصوص عملیات سایبری، یک مخاصمهٔ مسلحانه زمانی غیربین‌المللی است که خشونت مسلحانهٔ مستمری وجود داشته باشد که شامل عملیات کلاسیک و سایبری توأماً بوده یا اینکه فقط محدود به عملیات سایبری است و این درگیری بین نیروهای مسلح دولتی و گروه‌های مسلح یا بین خود این گروه‌ها رخ داده باشد. این درگیری باید به سطح حداقلی از خشونت رسیده باشد که معیار مسلحانه بودن حاصل شده باشد و نیز گروه‌های درگیر در منازعه باید تا حدی سازمان‌یافته باشند.

شاید در خصوص اینکه اقدامات ایذایی سایبری مخالفان دولت را بتوان مخاصمهٔ بین‌المللی تلقی کرد و مقررات حقوق جنگ را در مقابله با آن قابل اجرا دانست، تردید وجود داشته باشد. اما باید گفت که قابلیت اجرای قواعد حقوق مخاصمات به نوع عملیات نظامی یا وسایل معین یا شیوه‌های جنگی به‌کار گرفته شده، بستگی ندارد. به این ترتیب عملیات سایبری به‌تنهایی و در صورت نبود عملیات کلاسیک، اگر شرایط ضروری مطرح شده یعنی آستانهٔ شدت لازم و درجه‌ای از سازمان‌یافتگی را داشته باشند، در موارد استثنایی می‌توانند به ایجاد مخاصمهٔ مسلحانهٔ غیربین‌المللی منجر شوند. از سوی دیگر، اگر یک مخاصمه به‌عنوان مخاصمهٔ مسلحانهٔ غیربین‌المللی در نظر گرفته شود و در آن بیشتر حملات کلاسیک اجرا شود، قواعد حقوق مخاصمات مسلحانهٔ غیربین‌المللی بر هر گونه عملیات سایبری مرتبط صورت‌گرفته در چنین مخاصمه‌ای نیز حاکم خواهد بود، هرچند میزان استفاده از حملات سایبری نسبت به حملات کلاسیک بسیار کمتر باشد.

در پروتکل الحاقی دوم به کنوانسیون‌های ژنو، مواردی چون تنش‌ها و درگیری‌های داخلی مانند شورش‌ها، اقدامات خشونت‌آمیز پراکنده و سایر اقدامات دارای ماهیت مشابه به‌صراحت از

شمول مقررات حقوق بشردوستانه خارج شده‌اند، زیرا مخاصمهٔ مسلحانهٔ غیربین‌المللی محسوب نمی‌شوند، و این استثنا در مورد عملیات ایذایی سایبری پراکنده، هرچند مستقیماً بـه صـدمات فیزیکی یا آسیب منجر شوند نیز صادق است و صرف بروز اقدامات سایبری خشونت‌آمیز را نمی توان دلیلی بر شروع مخاصمهٔ غیربین‌المللی تلقی کرد؛ همچنـان‌کـه فعالیـت‌هـای ضـددولتی و ایجاد ناآرامی اجتماعی با استفاده از فضای سایبر خارج از مفهوم مخاصمهٔ مسلحانه است. بـرای مثال فراخوانی را که از طریق شبکه‌های اجتماعی در اینترنت برای شورش اقلیـت روس‌تبـار در استونی در سال ۲۰۰۷ میلادی اتفاق افتاد، نمی‌توان اقدام خصمانه در مفهوم مخاصمهٔ مسلحانه تلقی کرد. یا اقدامات مخالفان در مواردی چون نفوذ در شبکه‌های کامپیوتری، حذف یا نـابودی برخی اطلاعات (حتی در مقیاس بزرگ)، بهره‌برداری از شبکه‌های کامپیوتری و دزدی اطلاعات، به ایجاد مخاصمهٔ مسلحانهٔ غیربین‌المللی منجر نمی‌شوند. برای مثال بلوکه کردن برخی خدمات و عملکردهای اینترنت یا تغییر شکل دادن وب‌سایت‌های رسمی و دولتی به‌تنهایی بـرای ایجـاد مخاصمهٔ مسلحانه کافی نیستند، زیرا به شدت و آستانهٔ لازم برای ایجـاد یـک حملـهٔ مسـلحانه نرسیده‌اند و اغلب توسط افرادی انجام می‌گیرند که فاقد تشکیلات و سازماندهی لازم بـه‌عنـوان گروه نظامی مخالف دولت هستند.

همان‌طورکه در رأی شعبهٔ تجدیدنظر در قضیهٔ تادیچ ذکر شد، خشـونتی کـه سـبب ایجـاد مخاصمهٔ مسلحانهٔ داخلی می‌شود، باید مکرر[1] و در طول زمان ادامـه‌دار باشـد. بـه ایـن ترتیـب عملیات سایبری که در یک دورهٔ زمانی اتفاق می‌افتند، باید از ویژگـی مکـرر و ممتـد بـودن در طول زمان برخوردار باشند.

از دیگر معیارهای لازم برای ایجاد مخاصمهٔ مسلحانهٔ داخلی وجود حداقل یک گـروه مسـلح سـازمان‌یافتـهٔ غیردولتـی درگیـر مخاصـمات اسـت (AMW Manual, Commentary Accompanying ,2009: Rule 2 (a)). اگر گروهی توانایی اجـرای عملیـات نظـامی سـایبری را داشته باشد، «مسلح»[2] محسوب می‌شود و اگر تحت یک ساختار فرماندهی باشد که توان اجرای عملیات نظامی را دارد (ICTY, 2005: para. 129)، از ویژگی «سازمان‌یافته»[3] نیز برخوردار می شود. حدود سازماندهی لازم نیست که به آستانهٔ یک واحد نظامی منظم دولتی رسیده باشد. بـا این حال، اجرای عملیات خشونت‌بار سایبری و حملات شبکه‌های کامپیوتری به‌وسیلهٔ اشـخاص خصوصی یا گروه‌های کوچک از هکرها به‌تنهایی برای داشتن معیـار سـازماندهی کـافی نیسـت. اینکه آیا یک گروه سازمان‌یافته نظامی محسوب می‌شود یا خیر، امر کلی نیست و باید مورد بـه مورد بررسی شود.

---

1 "Protract"
2."Armed"
3. "Organized"

در مورد حملات سایبری مسئلهٔ سازماندهی مجازی قابل طرح است که در آن همهٔ فعالیت‌ها در حالت اتصال به اینترنت اتفاق می‌افتد. در یک طیف هکرهایی هستند که به‌طور کامل خودمختار عمل می‌کنند، در چنین مواردی با اینکه تعداد زیادی از هکرها در توافقی به یک دولت حمله می‌کنند، اما واجد معیار سازماندهی محسوب نمی‌شوند. در مقابل اگر یک گروه آنلاین از هکرها وجود دارند که دارای یک ساختار رهبری هستند که فعالیت‌های آنها را هماهنگ می‌کند، برای مثال از طریق محل‌یابی کردن اهداف سایبری برای اعضا، تقسیم ابزار حمله، اجرای ارزیابی‌های آسیب‌پذیری سایبری و تعیین این مسئله که آیا حملهٔ مجدد لازم است یا خیر و...، در واقع این گروه از هکرها در شکلی تشکیلاتی با یکدیگر همکاری می‌کنند و عنصر سازماندهی و فرماندهی در اینجا موجود است و عدم امکان ملاقات به‌صورت حضوری برای اعضای گروه، مانع داشتن معیار سازمان‌یافتگی در صورت وجود سایر شرایط نخواهد بود (Tallinn Manual on the International Law Applicable to Cyber Warfare , 2011, Rule. 23,para. 13.). شایان ذکر است که فضای سایبر محدود و منحصر به شبکهٔ جهانی اینترنت نیست، بلکه شبکهٔ جهانی اینترنت مهم‌ترین و گسترده‌ترین بخش فضای سایبر محسوب می شود، برای نمونه حملهٔ استاکس نت به ایران از طریق اینترنت صورت نگرفت، زیرا تأسیسات اتمی ایران به شبکهٔ جهانی اینترنت متصل نبوده است.

مثال دیگری که از مفهوم مخاصمه خارج است، اقدامات جمعی و همزمان تعداد زیادی از افراد و گروه‌های هکر است که در ظاهر شبیه به شکل‌گیری گروهی غیررسمی است. گاهی واقعه‌ای تحریک‌آمیز سبب می‌شود بدون اینکه هیچ‌گونه هماهنگی از قبل انجام گرفته باشد، عده‌ای به‌طور همزمان به اهداف مشترکی حمله کنند. برای مثال هنگامی‌که ویکی لیکس از سوی دولت آمریکا و مؤسسات آمریکایی مورد حمله قرار گرفت، حملات گسترده‌ای از سوی گروه‌های متعدد هکرها علیه مؤسسات آمریکایی سازماندهی شد. با این حال و به‌رغم شکل‌گیری یک گروه غیررسمی در دفاع از ویکی لیکس نمی‌توان گفت که آنها یک گروه سازمان‌یافتهٔ مسلح را تشکیل دهند، زیرا برای این منظور باید یک گروه متفاوت با سازماندهی و ساختار کافی که به‌صورت یک واحد عمل می‌کنند، وجود داشته باشد (Tallinn Manual on the International Law Applicable to Cyber Warfare , 2011,Rule. 23,para.13). این نکته را نیز نباید فراموش کرد که هرچند مادهٔ ۳ مشترک به‌طور خاص مقرر می‌کند که اجرای مقررات این ماده، وضعیت قانونی طرفین یک درگیری را عوض نمی‌کند، دولت‌ها اغلب تمایلی به پذیرش وجود یک مخاصمهٔ مسلحانهٔ غیربین‌المللی ندارند و به این ترتیب هرچند در عمل وجود یک گروه سایبری مسلح مخالف دولت و انجام جنگ سایبری به‌عنوان تنها روش مبارزهٔ مسلحانه علیه دولت در شرایط استثنایی قابل تصور است، پروتکل دوم الحاقی بر موارد خاصی از مخاصمات مسلحانهٔ غیربین‌المللی حاکم است. مخاصمات موردنظر پروتکل دوم الحاقی، مواردی است که درگیری بین

نیروهای مسلح یک دولت و نیروهای مسلح یا گروه‌های مسلح سازمان‌یافته‌ای وجود دارد که به‌حد کافی بر سرزمین کنترل دارند و آنها را قادر می‌کند که عملیات نظامی متمرکز و پیوسته‌ای را انجام دهند (Additional Protocol II. art.1.(1)) و هرچند کنترل بر فعالیت‌های سایبری می تواند یکی از نشانه‌های کنترل یک گروه بر سرزمین باشد، به‌تنهایی کافی نیست که کنترل سرزمینی موردنظر پروتکل دوم را تأمین کند (Tallinn Manual on the International Law Applicable to Cyber Warfare , 2011, Rule. 23,para.17) . ازاین‌رو در عمل، عملیات سایبری غیربین‌المللی هنگامی تحت شمول حقوق بین‌الملل بشردوستانه قرار می‌گیرد که در جریان یک مخاصمهٔ غیربین‌المللی کلاسیک رخ داده باشد.

اصول حقوق بین‌الملل بشردوستانهٔ قابل اعمال در جنگ‌های سایبری

پس از ملاحظهٔ قابلیت اعمال قواعد حقوق بین‌الملل بشردوستانه در مخاصمات سایبری یا عملیات سایبری در جریان سایر مخاصمات بین‌المللی و غیربین‌المللی اکنون باید به این پرسش پاسخ داد که در وضعیتی که هنوز هیچ مقررات صریحی در خصوص این نوع درگیری‌ها و عملیات نظامی وضع نشده است، چگونه طرف‌های درگیر باید حقوق بشردوستانه را به‌هنگام عملیات مدنظر قرار دهند. در پاسخ باید گفت هرچند بهتر است پدیده‌های مهم در مخاصمات مسلحانه مستقلاً و صراحتاً موضوع حکم قرار گیرند تا وظایف طرف‌های درگیر کاملاً مشخص شود و آنها نتوانند به مدد تفسیرهای حسب مورد مضیق یا موسع خود از اجرای حقوق طفره روند، اما در نبود چنین مقررات صریحی می‌توان همواره از مقررات عمومی و اصول کلی حقوق بشردوستانه بهره جست و حقوق و تکالیف طرف‌ها را تبیین کرد. در بخش آخر این مقاله قابلیت اعمال برخی از مهم‌ترین اصول حقوق بین‌الملل بشردوستانه در مخاصمات و عملیات سایبری بررسی می‌شود.

۱. اصل اساسی تفکیک

یکی از اصول مهمی که در این زمینه اعمال می‌شود، اصل تفکیک میان هدف‌های نظامی و غیرنظامی است که در هدایت درگیری‌های مسلحانهٔ بین‌المللی نقش بسیار اساسی دارد. دیوان بین‌المللی دادگستری در سال ۱۹۹۶ در نظریهٔ مشورتی خود در خصوص سلاح‌های هسته‌ای اعلام کرد که هدف از اعمال اصل اساسی تفکیک در حقوق بشردوستانه حمایت از جمعیت و اموال غیرنظامی است و این اصل تمایز میان رزمنده و غیررزمنده را مشخص می‌کند. دولت‌ها هرگز نباید جمعیت غیرنظامی را هدف قرار دهند و از سلاح‌هایی استفاده کنند که قادر به تمایز بین اهداف نظامی و غیرنظامی نیستند (ICJ Rep, 1996: paras.226- 257).

اما به‌طور کلی سلاح‌های اندکی وجود دارند که می‌توان آنها را ذاتاً غیر قادر به تفکیک بین

اهداف نظامی و غیرنظامی دانست. چنین سلاح‌هایی اغلب «کور»[1] نامیده می‌شوند و به این ترتیب غیرقانونی‌اند (ICJ Advisory Opinion ,1996, Dissenting Opinion of Judge Higgins paras.588-89). زمانی‌که سلاح‌ها توسط یک طرف متحارب برخلاف اصل تفکیک استفاده می‌شوند، به‌ندرت به‌دلیل کوری ذاتی سلاح‌هاست. بلکه ناشی از شلیک کورکورانه است که آن نیز اغلب به‌دلیل تصمیم قبلی آگاهانهٔ دستوردهندهٔ انسانی است. مثال روشن از بین سلاح‌هایی که ذاتاً قادر نیستند بین اهداف نظامی و غیرنظامی تفکیک کنند، سلاح‌های بیولوژیکی‌اند. یک ویروس می‌تواند یک بیماری مسری را به‌سرعت و در مقیاس وسیع منتشر کند، از طریق قیاس، این مثال می‌تواند در مورد ویروس‌های کامپیوتری هم مطرح شود، با این تفاوت که ویروس‌های کامپیوتری ساختهٔ دست انسان هستند و رفتار آنها علی‌القاعده تحت کنترل سازنده است، اما چنانچه ویروس‌های کامپیوتری نیز بتوانند به‌نحوی کنترل‌نشدنی از سیستم‌های نظامی به سیستم‌های غیرنظامی تسری یابند، آنها نیز در حکم سلاح‌های کور هستند و در نتیجه اجرای چنین حملاتی ناقض اصل تفکیک و قواعد حقوق بین‌الملل بشردوستانهٔ موجود در این زمینه است. اصل تفکیک را می‌توان از مهم‌ترین اصول محدودکننده در استفاده از بدافزارهای رایانه‌ای به‌عنوان ابزار حملهٔ نظامی تلقی کرد.

مقدمهٔ اجرای صحیح اصل تفکیک پاسخ به این پرسش است که چه کسانی غیرنظامی محسوب شده و از مزایای اصل تفکیک بهره‌مند می‌شوند و چه مواردی اهداف نظامی نیستند؟ پاسخ کوتاه آن است که غیرنظامیان جزء رزمندگان نیستند و هر آنچه تخریب، تصرف یا از کار انداختن آن مزیت نظامی مشخصی برای طرف مقابل ایجاد نکند، هدف نظامی محسوب نمی شود. این تعریف را می‌توان معنای مخالف اهداف نظامی دانست .

بند ۲ مادهٔ ۵۲ پروتکل الحاقی اول به کنوانسیون‌های ژنو، تعریفی از اهداف نظامی ارائه می کند، که انعکاس‌دهندهٔ حقوق بین‌الملل عرفی موجود در این زمینه است. حمله‌ها منحصراً باید به هدف‌های نظامی محدود شود، تا آنجا که به اموال مربوط می‌شود، هدف‌های نظامی به اموالی محدود می‌شوند که به لحاظ ماهیت محل، هدف یا کاربرد آنها سهم مؤثری در عملیات نظامی دارند و تخریب کلی یا جزئی، تصرف یا از کار انداختن آنها در شرایط زمانی موجود، مزیت نظامی معین محسوب می‌شود.

کلمات کلیدی در اینجا، ماهیت، محل، هدف یا کاربرد این اموال است. بعضی کامپیوترها از لحاظ ماهیت و هدف نظامی محسوب می‌شوند، برای مثال زمانی‌که به‌عنوان قسمتی از تسلیحات یا سیستم‌های تسلیحاتی یا وسایل ساخت آنها به‌کار گرفته شوند. در این موارد به‌طور خودکار، اهداف نظامی محسوب می‌شوند. اما حتی اگر کامپیوترها برای اهداف عمومی طراحی می‌شوند، با استفادهٔ عملی توسط رزمندگان، به اهداف نظامی تبدیل می‌شوند.

1."Blind"

استفادهٔ نظامی از یک کامپیوتر و در نتیجه تعیین آن به‌عنوان یک هدف نظامی باید در وسیع‌ترین مفهوم در نظر گرفته شود که شامل کلیهٔ مراحل اجرای نقشه، برنامه‌ریزی و طراحی برای حملات به‌وسیلهٔ تهیهٔ داده‌ها، ذخیره کردن اطلاعات نظامی، رمزگذاری، شکستن کدها و... می‌شود. در اساس، نرم‌افزار کامپیوتر بیش از سخت‌افزار کلید استفادهٔ نظامی از یک کامپیوتر معمولی است، اما هارد درایو کامپیوتر نیز ممکن است شامل اطلاعات نظامی باشد و حتی بعد از اینکه نرم‌افزار کامپیوتر جابه‌جا شود، سخت‌افزار ممکن است آلوده شود و در نتیجه ماهیت نظامی آن حتی بعد از جابه‌جایی نرم‌افزار باقی بماند.

از طرف دیگر حملات مستقیم عمدی علیه غیرنظامیان (که به‌طور مستقیم در مخاصمه مشارکت ندارند) یا اشیای غیرنظامی، ممنوع است و به‌عنوان جنایت جنگی تحت بند ۲ مادهٔ ۸ اساسنامهٔ دیوان کیفری بین‌المللی طبقه‌بندی شده‌اند.

این قاعدهٔ فراگیر حقوق مخاصمات مسلحانه که حملات مستقیم علیه اشخاص و اموال غیرنظامی را منع می‌کند، در مورد حملات شبکه‌ای کامپیوتری نیز مانند سایر حملات به‌شرط اینکه منتج به خشونت شود، به‌کار می‌رود. مثلاً حملهٔ سایبری که برای به‌دست گرفتن کنترل سیستم هدایت خطوط هواپیمایی کشوری انجام گیرد (یا برج کنترلی که پروازهای آن خط هوایی را تنظیم می‌کند) و هدف آن سقوط هواپیما و کشته شدن تمام مسافران آن پرواز باشد، حملهٔ عمدی مستقیم علیه اشخاص و اهداف غیرنظامی محسوب می‌شود و ناقض اصل تفکیک است (Dinstein, 2012: 266).

۲. اصل تناسب و ممنوعیت ایراد خسارات جانبی بیش‌ازحد

حمایت از اشخاص و اموال غیرنظامی، به موجب اصل تفکیک، تنها محدود به حملات غیرتبعیض‌آمیز یا کورکورانه و ممنوعیت حملات مستقیم علیه آنها نیست، بلکه موضوع اساسی دیگر کنترل و محدود کردن سطح صدمات جانبی به غیرنظامیان است. حقوق مخاصمات مسلحانهٔ بین‌المللی از این فرض آغاز می‌کند که در زمان اجرای عملیات نظامی ممکن است خساراتی هم به جمعیت غیرنظامی وارد شود و این قواعد تلاش می‌کند که این قبیل خسارات را تا حد ممکن محدود کند (Kalshoven, 2007: 109)؛ یعنی در عمل برخی صدمات جانبی به غیرنظامیان اجتناب‌ناپذیر بوده که به‌سبب عدم امکان دور نگه‌داشتن همهٔ اشخاص و اهداف غیرنظامی از میدان عملی جنگ در مخاصمات است. برخی غیرنظامیان نظامیان را همراهی می‌کنند، اعم از وابسته یا در استخدام (مانند تعلیم‌دهندگان، سرپرست‌ها، آشپزها، خدمه، نامه‌رسان‌ها و...) یا سایر غیرنظامیانی که در مجاورت یک هدف نظامی‌اند یا نزدیک به آن کار می‌کنند (برای مثال اشخاصی که مجاور فرودگاه‌های نظامی‌اند) یا اینکه ممکن است برخی غیرنظامیان موقتاً در زمان نامناسب در یک حوزهٔ نظامی حضور داشته باشند، مانند

فروشندگان، مهندسان تعمیرکنندهٔ کامپیوترها، متخصصان برق، لوله‌کش‌ها، کارگران ساختمانی و...، به‌علاوه اموال و اشیای غیرنظامی اغلب با اهداف نظامی آمیخته شده‌اند.

ممنوعیت خسارات جانبی بیش‌ازحد به اشخاص یا اهداف غیرنظامی به‌عنوان اصل تناسب شناخته می‌شود (Jensen, 2002: 1171).

اجرای اصل تناسب در حوزهٔ انتظار و پیش‌بینی صورت می‌پذیرد و کل دیدگاه بستگی به این دارد که چه چیزی به‌طور منطقی پیش از حمله قابل پیش‌بینی است. به‌عبارت دیگر، یک طرف مخاصمه به‌هنگام طراحی و اجرای حملهٔ نظامی باید پیش‌بینی کرده باشد که سطح صدمات جانبی به اشخاص و اشیای غیرنظامی در مقایسه با مزیت‌های نظامی که از حمله به دست می‌آید، آیا قابل تحمل بوده یا بیش از حد تلقی می‌شود.

مزیت‌های نظامی پیش‌بینی‌شده از یک حمله باید واقعی و مستقیم باشند، پس مواردی که فقط مبتنی بر فرض هستند، نباید در نظر گرفته شوند. به هر حال مزیت نظامی باید به‌صورت جامع در نظر گرفته شود. وقتی تعداد زیادی حملات در پیش است، لازم نیست که هر بخش به‌صورت جداگانه از کل مسئله در نظر گرفته شود (UK MOD, "Manual of the Law of Armed Conflict", (MOD 2004), para 5. 4. 4). بنابراین اگر حملهٔ شبکه‌ای کامپیوتری به‌طور سیستماتیک علیه یک سری از کامپیوترهای دشمن اجرا شود، مزیت نظامی حاصل از این تخریب یا تعدی و مداخلهٔ صورت‌گرفته بر هر کامپیوتر خاص مورد هدف، ممکن است به‌تنهایی اثر محدودی داشته باشد، بررسی کل وضعیت آشکار خواهد کرد که چه چیزی در خطر است، یعنی بررسی خسارات وارده به کل سیستم‌ها نشان می‌دهد که آیا مزیت‌های نظامی پیش‌بینی‌شده از یک حمله، واقعی و مستقیم است یا خیر.

به‌طور کلی در مورد حملات شبکه‌ای کامپیوتری اگر هنگام مختل کردن برخی سیستم‌های الکترونیکی نظامی از طریق حملات سایبری، این عمل به ورود صدمات جبران‌ناپذیر به زیرساخت‌های غیرنظامی (مدیریت آب‌ها، مراکز تحقیقاتی، سیستم‌های بانکداری، بازار بورس و...) منجر شود، باید خسارات جانبی بیش‌ازحد ارزیابی شود (Doyle Jr, 2002: 159).

۳. احتیاط‌های ممکن

مطابق با شق ۲ بند ۲ مادهٔ ۵۷ پروتکل الحاقی اول، کسانی که حملات را برنامه‌ریزی یا در مورد اجرای حملات تصمیم‌گیری می‌کنند، باید کلیهٔ احتیاط‌های ممکن را در انتخاب وسایل و شیوه‌های حمله به‌عمل آورند تا هنگام حمله از خسارات جانی اتفاقی به غیرنظامیان و نیز آسیب رساندن به اموال غیرنظامی اجتناب ورزند یا آن را به حداقل برسانند.

در این زمینه یک نکتهٔ مهم، تعیین مفهوم «احتیاط‌های ممکن»[1] است؟ یک تعریف در این زمینه در بند ۴ مادهٔ ۳ پروتکل دوم کنوانسیون «ممنوعیت یا محدودیت در استفاده از برخی سلاح‌های متعارف»، بیان شده است: احتیاط‌های ممکن مواردی هستند که عملی بوده یا به لحاظ عملی ممکن هستند و شامل در نظر گرفتن همهٔ شرایطی که در آن زمان (زمان حمله) حاکم بوده، از جمله ملاحظات نظامی و انسانی‌اند.[2]

احتیاط‌های ممکن می‌تواند بر مواردی چون زمان حمله، مهماتی که قرار است استفاده شود و نیز ترجیح برخی تاکتیک‌های خاص بر سایر موارد تأثیرگذار باشند (Rogers, 2004 : 98).

به‌منظور دستیابی به هدف دور کردن غیرنظامیان از آثار جنگ، در بند ۳ مادهٔ ۵۷ پروتکل الحاقی اول تصریح شده است که اگر امکان انتخاب بین چندین هدف نظامی برای دستیابی به یک مزیت نظامی، وجود دارد، هدفی باید انتخاب شود که انتظار می‌رود حداقل صدمه و آسیب را به غیرنظامیان وارد می‌کند. بنابراین در حملات سایبری نیز باید این اصل همواره مدنظر قرار گیرد. برای مثال طراحان یک بدافزار برای حمله به سامانه‌های کامپیوتری دشمن باید آثار جانبی حملهٔ سایبری را مدنظر قرار دهند. اما روی دیگر سکه در استفاده از عملیات سایبری فرصتی است که این نوع عملیات به‌دست می‌دهد تا طرف‌های مخاصمه بدون انجام اقدامات تخریبی وسیع به مزیت نظامی مطلوب دست یابند. این حملات شبکه‌ای کامپیوتری فرصت‌های جدیدی را برای انتخاب روش‌های نظامی مشابه که می‌توانند خسارات جانبی را به حداقل برسانند و زمینهٔ اجرای قاعدهٔ *احتیاط‌های ممکن* را به‌نحو مؤثرتری فراهم کنند، به‌وجود آورده است. برای مثال برای قطع کردن تردد در خطوط راه‌آهن به‌جای استفاده از حملات کلاسیک علیه خطوط راه‌آهن و قطارها (که طی آن احتمال ایراد خسارات جانبی بیش‌ازحد به غیرنظامیان وجود دارد)، چه‌بسا بتوان با اجرای حملهٔ شبکه‌ای کامپیوتری علیه مرکز کنترل راه‌آهن، جریان حمل‌ونقل را مختل کرد و مزیت نظامی موردنظر را به‌دست آورد و از آثار جانبی بیش‌ازحد اجتناب ورزید (Schmitt, 2005: 117).

به این ترتیب با انتخاب‌های جدیدی که طرفین مخاصمه در گزینش سلاح و شیوهٔ حمله به دست آورده‌اند و همگی حاصل پیشرفت فناوری به‌خصوص در عرصهٔ فضای سایبر هستند، شرایط برای به حداقل رساندن آسیب به غیرنظامیان مساعدتر شده است، به‌خصوص در بحث صدور هشدارهای مؤثر به غیرنظامیان، استفاده از فضای اینترنت جهت صدور این قبیل هشدارها میسر شده است.

---

1. Feasible Precautions.
2. Protocol on Prohibitions or Restrictions on the Use of Mins, Booby Traps and Other Devices (Protocol II) Annexed to the Convention on Prohibition or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to have Indiscriminate Effects (3 May 996).

نتیجه‌گیری

فضای سایبر امروزه بخشی انکارناپذیر از زندگی بشر را تشکیل می‌دهد و دولت‌ها کـه مـدت‌هـا خود را محصور در مرزهای ملی و حاکم بر فضای بین ایـن مرزهـا تلقـی مـی‌کردنـد، نـاگزیر از پذیرش واقعیت این فضای بدون مرز هستند و بی‌تردید روابط بین آنها در این فضا نیز براسـاس حقوق بین‌الملل قابل تنظیم بوده و حقوق بین‌الملل بر رفتار دولت‌ها در فضای سایبر نیـز قابـل اعمال است.

فضای سایبر در عین حال فضایی برای رقابت بین دولت‌ها و عرصه‌ای برای انجام فعالیت‌های خصمانهٔ دولت‌ها علیه یکدیگر نیز است و در اینجا نیز دولت‌ها موظف‌اند حقوق بین‌الملل حـاکم بر روابط خصمانه را در فضای سایبر محترم بشمارند. از یک طرف محدودیت‌های حق توسل بـه زور شامل استفاده از ابزارهای سایبری نیز می‌شود و از طرف دیگر، چنانچه از این فضا برای انجام فعالیت‌های نظامی استفاده شود، علی‌القاعده حقوق مخاصمات مسلحانه و به‌طور مشخص قواعد حقوق بین‌الملل بشردوستانه نباید نادیده گرفته شود.

اما از آنجا که به‌واسطهٔ جدید بودن پدیده، هنوز مقررات‌گذاری ویژه‌ای در خصوص اسـتفاده از فضای سایبر به‌عنوان محمل اقدامات خصمانه صورت نگرفته و تـلاش‌هـای ابتـدایی در رویـه سازی (مانند تدوین دستورالعمل تالین از سوی ناتو) واجد اثر حقوقی لازم نیستند، لاجرم بایـد از اصول و قواعد کلی حقوق بین‌الملل بشردوستانه برای تنظیم روابط خصمانه در فضای سـایبر استفاده کرد، زیرا همچنان‌که شرط مارتنس از ابتدای قرن بیستم بیان کرده است، نبـود قواعـد خاص مانع از اجرای قواعد و اصول کلی، عرف و حتی ندای وجدان نیست.

در این مقاله با انتخاب چند اصل از اصول حقوق بین‌الملل بشردوستانه نشان دادیم که بـا وجـود قواعد صریح چگونه می‌توان عملیات جنگی سایبری را تحت نظم حقوق بشردوسـتانه درآورد. بـا ایـن حال، با توجه به ویژگی‌های خاص و متفاوت فضای سایبر و از آنجا که عوامل متعددی کنترل فضـای سایبر را با مشکل مواجه می‌کنند و نیز نبود درک مشترک در خصوص قواعد حقوق بین‌الملـل قابـل اعمال بر رفتار دولت‌ها در این حوزه، بهتـر اسـت کـه اعضـای جامعـهٔ بـین‌المللـی هرچـه سـریع‌تـر معاهده‌ای جامع در خصوص قواعد حاکم بر جنگ‌های سایبری منعقد کنند.

منابع

۱. فارسی

الف) کتاب‌ها

۱. ضیایی بیگدلی، محمدرضا (۱۳۹۲). *حقوق بین‌الملل بشردوستانه*، چ اول، تهران: گنج دانش.

۲. فضلی، مهدی (۱۳۸۹). *مسئولیت کیفری در فضای سایبر*، چ اول، تهران: خرسندی.

ب) مقالات

۳. پاکزاد، بتول (۱۳۹۰)، «تروریسم سایبری»، *مجلهٔ تحقیقات حقوقی*، دانشگاه شهید بهشتی، ویژه‌نامهٔ شمارهٔ ۴.

۲. انگلیسی

A) BOOKS

4. Boothby, William H. , (2009). *Weapons and the Law of Armed Conflict*, Oxford University Press.
5. Bothe,Michael,Partsch,KARL Josef,Solf,Waldemar A.,(1982). *New Rules for Victims of Armed Conflicts*,Leiden , Martinus Nijhoff Publishers.
6. Dinstein , Yoram,(2010). *The Conduct of Hostilities Under the Law of International Armed Conflict*. 2nd edn , cup.
7. Greenwood , Christopher, (1998). " Law of Weaponary at the Start of the New Millennium." in MN Schmitt and LC Green, (eds).,*The Law of Armed Conflict :Into the Next Millennium*(Naval War College ,Newport,RI).
8. Hampson, F.J. (1993). "Means and Methods of Warefare in the Conflict in the Gulf**"**. *in* P. J. Rowe (ed), *The Gulf War of 1990-1991 in International and English Law* ,Routledge, London.
9. Harrison Dinniss, Heather, (2012). *Cyber Warfare and the Laws of War*,Cambridge Studies in International and Comparative Law.
10. Kalshoven, Frits, (2007). *Reflections on the Law of War: Collected Essays* ,Martinus Nijhof.
11. Roscini, Marco, (2010*)." World Wide Warfare- Jus ad Bellum and Use of Cyber Force***"**, Max Plank Yearbook of United Nations Law, Vol.14.

B) Articles

12. Dinstein ,Yoram, (2012)."The Principle of Distinction and Cyber War in International Armed Conflicts**"**, *Journal of Conflict and Security Law*,Vol.17,No.2.
13. Jensen, Eric Talbot (2002). "Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations?**"** , 18 *American University Intl L Rev* 1145.
14. Jensen, E.T.(2002). "Computer Attacks on Critical State Infrastructure: A Use of force Invoking the Right of self – Defence", 38 *Stanford J Intl L* 207.
15. JH Doyle Jr, (2002). *Computer Networks, Proportionality, and Military Operations*, *International Law Studies* 147,Vol.76, 200
16. Schmitt, Michael N. (1998)." Computer Network Attack and the Use of Force in International Law, Thoughts on a Normative

Framework**"**,Colum.J.*Transnat'IL*.,No.37,
17. Shacketford, Scott J. (2009). "From Nuclear war to Net war: Analogizing cyber Attacks in Interactional Law**"**, *Berkley Journal of International Law* , 192 et seq.
18. Shulman , M.R. (1999). "Discrimination in the Laws of Information Warefare**"**,Col.J.*Trans.L.*
19. Tsagourias , Nicholas,(2012) ." Cyber Attacks , Self Defence and the Problem of Attribution**",** *Journal of Conflict and Security Law* ,Oxford University Press, Vol.17, No.
20. Watts, Sean , (2010). "Combatant Status and Computer Network Attacks**"**, *Virginia Journal of International Law*, Vol.50-2, (2do).

C) Cases
21. Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. USA) (Merits)[1986] ICJ.
22. Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina V Serbia) [2007] ,ICJ.
23. International Court of Justice advisory opinion on the Legality of the Threat or Use of Nuclear Weapons,ICJ.1996.
24. Prosecutor V Galić (Judgment) ICTY-98-29 (5 December 2003).
25. Prosecutor V DuskoTadic 'a/k/a' DULE (Appeal) ICTY – 94-1- A(15 JULY 1999.

D) Documents
26. AMW Manual (Manual on International Law Applicable to Air and Missile Warefare, 15 May 2009.
27. Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949.
28. Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea. Geneva, 12 August 1949.
29. Convention (III) relative to the Treatment of Prisoners of War. Geneva, 12 August 1949.
30. Convention (IV) Relative to the Protection of Civilian Persons in Time of War (Opened for Signature 12 August 1949, Entered Into Force 21 October 1950).
31. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.
32. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977.
33. Tallinn Manual on the International Law Applicable to Cyber Warfare," Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Center of Excellence , General Editor: Michael

N.Schmitt, Cambridge University Press, New York , 2011.
34. UK MOD, "Manual of the Law of Armed Conflict", (MOD 2004).

E) Websites
35. https://ccdcoe.org/tallinn-manual.html.(last visited on 2017-06-22).
36. http://www.nato.int/cps/en/natohq/topics_78170.htm. (last visited on 2017-06-22).