فصلنامهٔ مطالعات حقوق عمومی، دورهٔ ۴۷، شمارهٔ ۲، تابستان ۱۳۹۶: ۵۳۷-۵۵۹

حملات سایبری و اصول حقوق بین‌الملل بشردوستانه (مطالعهٔ موردی: حملات سایبری به گرجستان)

پرستو اسمعیل‌زادهٔ ملاباشی[۱]، محسن عبداللهی[۲*]، سیدقاسم زمانی[۳]

چکیده

قرن ۲۱ آغاز تحول در یکی از حوزه‌های حقوق بین‌الملل یعنی حقوق مخاصمات مسلحانه است. دسترسی به سلاح‌های جدید، پیشرفت تکنولوژی و توسل به ترفندهای امروزی سبب شده است نه تنها پدیدهٔ شوم مخاصمه به کلی از چارچوب حقوق بین‌الملل رخت برنبندد، بلکه با بروز تحولات اخیر بر پیچیدگی‌های آن افزوده شد. در حقوق بین‌الملل سنتی، اصل بر وجود مخاصمه در روابط بین دولت‌ها بود که پس از روبه‌روشدن با تحولات به‌وجودآمده و با متأثرشدن از اسناد حقوقی مختلف بعدی به صورت یک استثنا درآمد و با توسعهٔ چشمگیر تکنولوژی، مخاصمات و اشکال آن سریع تر از تحول مفاهیم حقوقی در این حوزه تغییر شکل داد. تحول مفهومی در توسل به زور نه تنها مفاهیم و اصول بنیادین مخاصمه را دستخوش تغییراتی کرده، که با به چالش‌کشاندن شاکله‌های مخاصمهٔ سنتی، طرح مباحثی مثل ضرورت تفکیک، مشروعیت و قانونمندی این اقدامات را مطرح کرده است. در این مقاله درصددیم با تحلیل مفهومی جنگ سایبری به امکان تسری قواعد حاکم بر مخاصمات مسلحانهٔ سنتی بر فضای مجازی و خلأهای حقوقی آن بپردازیم. چون این امر بدون تأمل در رویهٔ بین‌المللی میسر نیست، به مطالعهٔ حملات گرجستان (۲۰۰۸) به‌منزلهٔ مطالعهٔ موردی می‌پردازیم.

کلیدواژگان

اصل تفکیک، اصل تناسب، اصل بی‌طرفی، اصل ضرورت نظامی، جنگ سایبری، گرجستان، مخاصمهٔ مسلحانه.

---

۱. گروه حقوق، دانشگاه آزاد اسلامی، واحد نجف‌آباد، نجف‌آباد، ایران.
۲. گروه حقوق، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، دانشیار دانشکدهٔ حقوق دانشگاه شهید بهشتی، تهران، ایران (نویسندهٔ مسئول). تلفن: ۰۹۱۲۳۷۷۴۲۳۷
Email: abdollahi75@hotmail.com
۳. دانشیار دانشکدهٔ حقوق و علوم سیاسی، دانشگاه علامه طباطبایی، تهران، ایران.
تاریخ دریافت: ۱۳۹۵/۰۸/۲۹، تاریخ پذیرش: ۱۳۹۵/۱۰/۱۳

مقدمه

ایجاد و رشد شگفت‌انگیز اینترنت سبب به‌وجودآمدن جامعهٔ اطلاعاتی جهانی شده است. دولت‌ها از اینترنت برای ارائهٔ اطلاعات به شهروندانشان استفاده می‌کنند (Lipson, 2002: 3). اینترنت همزمان با ایجاد میلیون‌ها شغل جدید خطرها و تهدیدهای جدی را نیز با خود همراه آورده است. روابط تجاری و جوامع در کل به طور فزاینده‌ای به کامپیوتر و شبکه‌های اینترنتی متکی شده‌اند که این موضوع سبب به‌وجودآمدن حملات و جرایم سایبری در دنیا شده است. پیشرفت روزافزون تکنولوژی در تمامی ابعاد زندگی بشریت موجبات دگرگونی و تغییر روش‌های توسل به جنگ را نیز برای دولت‌ها فراهم کرده است، به طوری که می‌توان ادعا کرد که ماهیت جنگ امروزه با توجه به پیشرفت‌های تکنولوژی تغییر کرده و دگرگون شده است به طوری که فضای سایبر بعد از زمین، دریا، هوا و جو به‌منزلهٔ پنجمین میدان نبرد شناخته می‌شود (Cornish & others, 2010: viii). با پیشرفت روزافزون تکنولوژی و وابستگی کشورها به این تکنولوژی، می‌توان به این حقیقت رسید که جنگ‌های دهه‌های آینده جنگ‌های سایبری خواهند بود.

امروزه علاوه بر اینکه به‌کارگیری فضای سایبر به‌منزلهٔ یک روش جنگی محسوب می‌شود، این فضا و سلاح‌های کاربردی در آن به‌منزلهٔ ابزار جنگ نیز در اختیار دولت‌ها علیه اهدافشان قرار گرفته است. دولت‌ها دریافته‌اند که توسل به فضای سایبر به‌منزلهٔ میدان جنگ و استفاده از سلاح‌های سایبری در آن مزایای زیادی به همراه دارد. حملات و جنگ در فضای سایبر به دلیل گمنام‌ماندن هویت حمله‌کنندگان، ارزان‌بودن حملات، سرعت، مشکلات موجود در بحث انتساب و مبهم‌بودن قواعد قابل اعمال در فضای سایبر از استقبال بیشتری در مقایسه با جنگ‌های سنتی برخوردارند. از طرف دیگر، وابستگی روزافزون دولت‌ها به فضای سایبر، اطلاعاتی که این فضا در اختیارشان قرار می‌دهد و آسیب‌پذیری سبب حساس‌بودن و اهمیت این حملات می‌شود به‌گونه‌ای که با پیشرفت تکنولوژی، به‌کارگیری حملات سایبری به جای جنگ سنتی دور از انتظار نخواهد بود. حقوق بین‌الملل بشردوستانه نیز از جمله شاخه‌هایی از حقوق بین‌الملل است که به‌ویژه به‌واسطهٔ پیشرفت تجهیزات و ابزارهای توسل به زور متحول شده است. این تحول به‌ویژه با ورود فضای مجازی شکلی جدید یافته است و این پرسش را به ذهن متبادر می‌کند که آیا حقوق بشردوستانهٔ بین‌المللی موجود می‌تواند به ابهامات موجود در توسل به جنگ‌های مجازی پاسخ دهد و آیا این نظام حقوقی سنتی می‌تواند به نظمی هنجاری در فضای سایبری بیانجامد؟ با توجه به تعریف مخاصمهٔ مسلحانه و لزوم توسل به حملات فیزیکی از سوی متخاصمان، شدت و آستانهٔ تخریب، برخی بر این نظرند که این نظام حقوقی پاسخگوی معضلات موجود در توسل به جنگ مجازی نیست و در عین حال برخی به‌واسطهٔ آثار

و تبعات این جنگ‌ها، قواعد و مقررات حاکم بر مخاصمهٔ مسلحانهٔ سنتی را قابل تسری بـه ایـن حوزه می‌دانند. به همین لحاظ ضرورت قطعی دارد که جوامع بشری علاوه بـر دسـتیابی هرچـه دقیق‌تر علمی و کاربردی به این پدیدهٔ جدید در زمینه‌های مختلف به تجزیه و تحلیـل مباحـث مختلف حقوقی آن در سطح بین‌الملل از جمله جایگاه حقوق بین‌الملل بشردوسـتانه در آن نیـز مبادرت ورزند. براساس نظریهٔ دوم ذکرشده لازم است تا به اصول حاکم بر حقـوق بشردوسـتانهٔ بین‌المللی از جمله اصل تفکیک، تناسب، بی‌طرفی و لزوم رعایت ضرورت نظامی توجه شـود. بـا توجه به وضعیت، خصوصیات و شرایط خاصی که هر کدام از حمـلات سـایبری -کـه بـه وقـوع پیوسته است- به خود اختصاص می‌دهند به نظر می‌رسد برای تحلیل و تبیـین قابلیـت اعمـال قواعد موجود در حقوق بین‌الملل در این‌گونه حملات بهترین راه‌حل مطالعهٔ مـوردی ایـن‌گونـه حملات باشد تا ضمن بررسی خصوصیات حملات مذکور، جایگـاه آن حمـلات نیـز در مقـررات حقوق بین‌الملل فعلی ارزیابی شود. از جمله حملات سایبری که در چند سـال اخیـر بـه وقـوع پیوسته حملات سایبری به گرجستان است که با توجه به خصوصـیات ایـن حمـلات و شـرایط خاصی که طی آن این حملات به وقوع پیوسته نیازمند بررسی و ارزیابی جداگانه‌ای است. لذا از این حیث در مقالهٔ حاضر، نخست به مفهوم‌شناسی جنگ سایبری، سپس قلمرو و حدود شـمول آن و اصول حاکم بر آن در قالب حقوق بشردوستانهٔ بین‌المللی می‌پردازیم و با توجه بـه مطالعـهٔ موردی حملات گرجستان به ارزیابی قضیه خواهیم پرداخت.

مفهوم‌شناسی جنگ سایبری

همان‌طورکه پیشرفت تکنولوژی در تمام ابعاد زندگی بشر تأثیر می‌گذارد تأثیر آن در روش‌هـای جنگ نیز اجتناب‌ناپذیر است. فضای سایبری علاوه بر اینکه اکنون به‌منزلهٔ یک نوع ابزار جنـگ به کار گرفته می‌شود، از جهت تحلیلی نیز جنگ در این فضا به‌منزلهٔ یکی از روش‌های جنـگ و فضای مذکور به‌منزلهٔ یک میدان جنگ مورد توجه قـرار گرفتـه اسـت. فضـای سـایبر در حـال تبدیل شدن به یک میدان جنگ جدید جهانی اسـت کـه ممکـن اسـت بـرای روابـط خصـمانه به‌تنهایی یا در کنار دیگر میدان‌های عملیاتی اسـتفاده شـود (Yde, 2013: 3). همـان‌طـور کـه پیش‌تر اشاره شد پس از زمین، دریا، هوا و فضا از فضای سایبر به‌منزلهٔ پنجمـین میـدان نبـرد[1] نام برده می‌شود (Tsagourias & Buchan, 2015: 436). به طور کلی فضای سایبر منبعی بـرای تبادل اطلاعات تلقی می‌شود. از نظر فیزیکی تعریفی که می‌توان از این فضا ارائـه کـرد عبـارت است از فضای ارتباط بین تعداد بیشماری از کامپیوترهـا و سیسـتم‌هـا (اصـلانی، ۱۳۹۳: ۳-۴). درخصوص تعریف فضای سایبر هیچ اتفاق نظری وجود ندارد به همین ترتیب تعریف مشـخص و

1. Fifth Battlespace or Battlefield.

دقیقی از جنگ سایبری موجود نیست (همان: ۳). تعاریف متعددی درخصوص جنگ سایبری بیان شده است از جمله اینکه عده‌ای آن را شامل اقداماتی می‌دانند که به‌منظور تخریب، انسداد، تنزل یا مختل‌کردن اطلاعات یک کامپیوتر یا یک شبکه شکل می‌گیرد یا بعضاً به تهاجمی‌بودن این اقدامات تأکید می‌شود (Sandvik, 2012: 31) و عده‌ای دیگر نیز به آثار به‌جامانده از این‌گونه حملات بیشتر توجه دارند (Waxman, 2011: 432).

پیشرفت تکنولوژی سبب شده است که دولت‌ها به این نتیجه برسند که استفاده از سلاح‌های سایبری به جای استفاده از سلاح‌های سنتی می‌تواند مزایای زیادی را برایشان همراه داشته باشد. از آنجا که فضای سایبر فضایی مبتنی بر گمنامی است و حملات در این فضا بسیار ارزان‌تر و سریع‌تر از روش‌های سنتی و انتساب در حملات سایبری امری دشوار است، از این حملات استقبال زیادی شده است. همچنین، مرتکبان این حملات به دلیل فقدان هرگونه معاهده یا عرف بین‌المللی، که این‌گونه حملات را به طور مستقیم مورد خطاب قرار دهد، از این کمبود با توسل به این‌گونه حملات استفاده می‌کنند. از طرف دیگر، با رشد روزافزون تکنولوژی و وابستگی شدید دولت‌ها به اینترنت و تکنولوژی‌های وابسته به آن، این فضا در صورت فقدان یا نقص امکانات امنیتی (حسن‌بیکی، ۱۳۹۴: ۸۱-۸۳) به‌منزلهٔ ضعف دولت‌ها تلقی می‌شود و می‌تواند هدف دشمن برای حمله قرار گیرد. جنگ سایبری معمولاً درگیری بین دولت‌ها در فضای سایبر است، اما ممکن است به طرق گوناگون بازیگران غیردولتی را نیز درگیر کند. خصوصیت دیگری که جنگ در فضای سایبر دارد این است که هدایت دقیق و مناسب حمله در جنگ سایبری بسیار مشکل است. عملیاتی که در فضای سایبری یا میدان نبرد مجازی به وقوع می‌پیوندد به‌سادگی قابل شناسایی نیست، بنابراین انتساب آن عمل نیز به همین شکل کار ساده‌ای نیست. این‌گونه عملیات و حملات می‌توانند در نهایت آثار فیزیکی نیز در پی داشته باشند، اما حملات ذاتاً و معمولاً به صورت پنهانی اتفاق می‌افتند.

بعضی بر این نظرند که جنگ جهانی دوم آغاز جنگ سایبری است که طی آن ارتش طرف مقابل به صورت عمدی از طریق هک رادیوی هواپیماهای نظامی اغفال می‌شد (Research Report, XVII. Model United Nations of Lübeck (MUNOL), 2014: 3). بعد از مواجهه با حملاتی از قبیل آنچه در سال ۲۰۰۷ در استونی اتفاق افتاد، رودررو شدن با جنگ سایبری از اهمیت ویژه‌ای برخوردار شد (Kelsey, 2008: 1429). از جمله دیگر حملات سایبری مهم ویروس استاکس نت بود که در سال ۲۰۱۰ با هدف تحت تأثیر قراردادن تأسیسات و تجهیزات غنی‌سازی اورانیوم ایران به وقوع پیوست. اهمیت این ویروس به‌گونه‌ای بود که برخی از آن به‌منزلهٔ سلاح سایبری که می‌تواند آثاری فیزیکی داشته باشد نام می‌برند (خلف‌رضایی، ۱۳۹۲: ۱۴۱).

به طور یقین جنگ سایبری بیشتر از یک حملهٔ ساده به یک وب‌سایت یا یک ایمیل است.

آنچه ما در جنگ سایبری با آن مواجه‌ایم مقیاسی بزرگ‌تر در سطح جهان دارد که حملات سایبری با هدف تعطیلی یک پایگاه دفاع هوایی، نفوذ به شبکهٔ دفاعی متمرکز دشمن یا حملات سایبری بر نیروگاه‌های دولت یا ایستگاه‌های رسانه از آن جمله‌اند (Ibid: 1427-1435). حملات سایبری درجات مختلفی دارند که حداقل آن استفاده از کامپیوتر در حمله به سیستم کامپیوتری دیگر تا حملاتی که آثار مخرب فراوانی در زیرساخت‌های دولت مورد حمله می‌گذارند متغیرند (Berner & others, 2010: 1028). نکتهٔ درخور توجه درخصوص جنگ سایبری این است که اگرچه برخی حملات در فضای سایبر تهاجمی‌اند، اما از شدت کمتری برخوردارند، لذا بهتر است آن‌ها را در درجه‌ای پایین‌تر از جنگ قلمداد کرد. این موضوع به‌منزلهٔ کم‌اهمیت قلمدادکردن حملات سایبری نیست، بلکه بیشتر به دلیل اقداماتی است که در پاسخ به این حملات اتخاذ می‌شود (Cornish & others, 2010: 10). به نظر می‌رسد در صورتی که حملات سایبری با تفسیر موسع تری در چارچوب جنگ سایبری قرار گیرند امکان توسل دولت‌ها حتی به سلاح‌های سنتی برای پاسخگویی به این حملات بالاتر می‌رود و در نهایت ممکن است یک حملهٔ سایبری ساده به وقوع جنگی در عالم واقع منجر شود و به خطرافتادن صلح و امنیت بین‌المللی را با خود همراه داشته باشد.

نکتهٔ درخور توجه دیگر درخصوص ارتباط بین حملات و جنگ سایبری این است که هر حملهٔ سایبری جنگ سایبری شناخته نمی‌شود، اما هر جنگ سایبری حمله‌ای سایبری را دربر دارد. درخصوص حملات سایبری نیز تعریف واحدی وجود ندارد. فرهنگ لغات مدرن تمامی انواع مداخلات آنلاین را به‌منزلهٔ حملات سایبری تلقی می‌کند، اما بسیاری از مفسران چنین استفادهٔ گسترده‌ای را از اصطلاح حملهٔ سایبری صحیح نمی‌دانند. شورای تحقیقات ملی امریکا[1] در گزارش سال ۲۰۰۹ درخصوص قابلیت‌های حملهٔ سایبری[2]، حملات سایبری را به‌منزلهٔ «استفاده از اقداماتی عمدی برای تغییر، مختل، فریب یا کاهش و یا از بین بردن سیستم‌های کامپیوتری دشمن یا شبکه‌ها یا اطلاعات و یا برنامه‌های موجود در این سیستم‌ها و یا شبکه‌ها» تعریف می‌کند (Heaton, 2005: 159). تعریف دیگری نیز از حملهٔ سایبری در قاعدهٔ ۳۰ راهنمای تالین[3] آمده است که مقرر می‌دارد: «حملهٔ سایبری عملیات سایبری تهاجمی یا

1. National Research Council.
شورای تحقیقات ملی از سوی آکادمی ملی علوم در سال ۱۹۱۶ به‌منظور همکاری با جامعهٔ علمی و تکنولوژی با اهداف آکادمیک در ارتقای سطح علمی و ارائهٔ پیشنهاد به دولت در امریکا تأسیس شد.

2. Cyberattack Capabilities.

۳. راهنمای تالین که با عنوان کامل «راهنمای تالین درخصوص حقوق بین‌الملل قابل اعمال در جنگ‌های سایبری» شناخته می‌شود درحقیقت پژوهشی غیرالزام‌آور درخصوص چگونگی اعمال حقوق بین‌الملل و به‌خصوص حقوق جنگ و بشردوستانه درخصوص حملات سایبری است. این راهنما به‌واسطهٔ دعوت مرکز همکاری عالی دفاع سایبری ناتو در تالین از گروهی از کارشناسان و متخصصان برای تهیهٔ این راهنما آغاز شد

تدافعی است که از آن به طور معقول انتظار ایراد صدمه، یا مرگ به اشخاص و یا واردکردن خسارات به اشیا می‌رود» (Tallinn Manual, 2013: 106). از جمله تعاریف دیگری که از حملهٔ سایبری ارائه می‌شود می‌توان به حملات سایبری به‌منزلهٔ هر اقدامی که به‌منظور تضعیف عملکرد یک شبکهٔ کامپیوتری برای اهداف سیاسی یا امنیت ملی صورت می‌گیرد اشاره کرد (Hathaway & Others, 2012: 826). این در حالی است که جنگ سایبری حمله‌ای سایبری است که آثار آن می‌بایستی مشابه با حملهٔ مسلحانه (عبداللهی، ۱۳۸۸: ۲۶۷) یا حمله می‌بایستی در چارچوب یک درگیری مسلحانه به وقوع پیوسته باشد (Ibid: 833). در هر حال به نظر می‌رسد اگر یک حملهٔ سایبری که حتی آثاری مشابه حملاتی که با سلاح‌های معمولی انجام می‌شوند نداشته باشد، اما در شرایط جنگ اتفاق افتاده و انتساب آن حمله به دولتی خاص امکان‌پذیر باشد در قالب حقوق جنگ ارزیابی خواهد شد. در غیر این صورت حداقل می‌توان گفت مطابق با بند ۱ مادهٔ ۲ منشور ملل متحد که بیان می‌دارد «سازمان بر مبنای اصل تساوی حاکمیت کلیهٔ اعضا قرار دارد»، به طور ضمنی دولت‌ها از هرگونه اقدامی علیه دولت دیگر که سبب ناتوانی دولت موردنظر در ادارهٔ امور دولتی‌اش شود منع می‌شوند.

از طرف دیگر، جنگ سایبری و سنتی نیز با یکدیگر تفاوت دارند. جنگ سایبری با اهدافی نظیر آنچه گفته شد در فضای مجازی به وقوع می‌پیوندد، در صورتی که جنگ‌های سنتی در زمین، هوا، دریا یا فضا اتفاق می‌افتند و آن‌ها درگیری مسلحانه‌ای هستند که علیه حاکمیت، تمامیت ارضی یا استقلال سیاسی دولت‌های دیگر در یک میدان جنگ مشخص صورت می‌گیرند (United Nations General Assembly, A/RES3314, 1974).

مشکل درخصوص استقرار چارچوب حقوقی جنگ سایبری تنهانبودن هیچ قاعده و نظم برای اعمال آن نیست، بلکه چگونگی اعمال قواعد موجود در فضایی جدید و کاملاً متفاوت است. به دلیل خصوصیات منحصربه‌فرد فضای سایبر، به‌ناچار مفاهیم کلیدی حقوق بین‌الملل می‌بایستی تفسیر تا متناسب با جنگ سایبری تبیین شوند (Yde, 2013: 5). بنابراین، هرچه تکنولوژی جدیدتر و منحصربه‌فردتر باشد چالش‌های پیش‌رو در تفاسیر حقوقی بیشتر می‌شود، اما این موضوع این حقیقت را که قواعد موجود قابل اعمال‌اند تحت تأثیر قرار نمی‌دهد، بلکه فقط تفسیر قواعد را برای اعمال چالش‌برانگیزتر (Ibid) و خطرناک‌تر می‌کند.

قلمرو حملهٔ سایبری در چارچوب حقوق بشردوستانهٔ بین‌المللی

اعمال قواعد حقوق بشردوستانه در حملات سایبری موضوع بحث‌برانگیزی میان محققان است.

و متعاقباً در سال ۲۰۱۳ راهنمای مذکور از سوی انتشارات کمبریج به چاپ رسید. برای مطالعهٔ بیشتر ر.ک. (Tallinn Manual, 2013: 16-23).

سؤال اصلی این است که آیا حقوق بشردوستانه در جنگ‌های سایبری قابل اعمال است یا با توجه به تحولات اخیر در توسل به جنگ های سایبری لازم است تا این حوزه مورد بازنگری قرار گیرد و قواعد و مقررات جدیدی در این خصوص تدوین شود؟

بعضی محققان بر این نظرند که وقتی قصد از حملات سایبری ایجاد صدمات فیزیکی یا خسارات باشد یا اینکه آن حملات منتهی به آن آثار شوند، این‌گونه حملات به درگیری مسلحانه منجر خواهند شد (Dorman, 2004: 2-3). بنابراین، در اینجا مقررات و قواعد بین‌المللی دیگری به کار گرفته می‌شود که رفتار و عملکرد دولت‌ها را هنگام درگیری‌های مسلحانه به نظم درمی‌آورد. این مقررات که حقوق بشردوستانهٔ بین‌المللی[1] یا حقوق حاکم در جنگ[2] نامیده می‌شوند شاخه‌ای از حقوق بین‌الملل‌اند که رفتار دولت‌های متخاصم و بازیگران غیردولتی طی جنگ‌های بین‌المللی و غیربین‌المللی فارغ از اینکه جنگ به شکل قانونی یا غیرقانونی آغاز شده باشد را به نظم درمی‌آورند و برای محدودکردن آثار درگیری‌های مسلحانه تلاش می‌کنند (Summary of the Geneva Conventions of 1949 & their Additional Protocols, 2011: 1-2).

حقوق حاکم در جنگ به طور سنتی از حقوق ژنو و لاهه تشکیل شده است. حقوق ژنو شامل دسته‌ای از معاهدات است که برای حمایت از وضعیت اسرا، زندانیان، مجروحان و بیمارانی است که قادر به ادامهٔ مبارزه نیستند.[3] با توجه به الحاق کلیهٔ کشورها به این معاهدات، مقررات مندرج در آن‌ها حالت عام‌الشمول و آمره گرفته‌اند (ضیایی‌بیگدلی، ۱۳۹۲: ۳۲). حقوق لاهه نیز متشکل از کنوانسیون‌های ۱۸۹۹ و ۱۹۰۷ است که روش‌ها و ابزار جنگ را شامل می‌شود (Rules of International Humanitarian Law & Other Rules Relating to the Conduct of Hostilities, Collection of Treaties & Other Instruments, 1989: 13-161). متخصصان حقوق بشردوستانه می‌بایست درخصوص حملات سایبری نیز به موضوع مهم قابلیت اعمال حقوق حاکم بر درگیری‌های مسلحانه در این نوع حملات توجه کنند (Kelsey, 2008: 1429). در حال حاضر، هیچ اجماعی درخصوص اعمال حقوق بشردوستانه نسبت به جنگ سایبری وجود ندارد. این موضوع از قطعی‌نبودن تعریف واحدی از جنگ سایبری سرچشمه می‌گیرد. همچنین هیچ‌گونه عرف و رویه‌ای نیز در این زمینه موجود نیست (Hughes, 2009: 5). حقوق بین‌الملل فعلی به طور صریح مقرراتی درخصوص جنگ سایبری ندارد، اما عمدتاً اعتقاد بر این است که محدودیت‌های ناشی از حقوق فعلی می‌بایستی درخصوص حملات

1. International Humanitarian Law.
2. Jus in Bellum.
۳. حقوق ژنو شامل چهار کنوانسیون سال ۱۹۴۹ و دو پروتکل الحاقی آن در سال ۱۹۷۷ و از جمله کنوانسیون‌های مربوط به بهبود وضعیت مجروحان و بیماران نیروهای مسلح خشکی و دریایی می‌شود.

سایبری نیز اعمال شوند، اما همچنان اعمال قواعد حقوق بشردوستانه دربارهٔ این‌گونه حملات در هاله‌ای از ابهام است (Kelsey, 2008: 1427). به عبارت دیگر، در حال حاضر هیچ مقرره‌ای در حقوق بشردوستانه یا حقوق بین‌الملل عرفی وجود ندارد که به‌صراحت در زمان جنگ یا صلح، جنگ سایبری یا حملات سایبری را ممنوع اعلام کند. البته فقدان چنین مقرره‌ای کاملاً واضح و قابل توجیه است، زیرا به‌وجودآمدن قواعد حقوق بشردوستانه به قرن ۱۹ میلادی برمی‌گردد که اصولاً فضای سایبری در آن زمان هنوز به وجود نیامده بود (Swanson, 2010: 305).

مباحث زیادی درخصوص ناکافی‌بودن حقوق بین‌الملل فعلی درخصوص فضای سایبری و اینکه به چه میزان نیاز است که معاهده‌ای فضای سایبر را به نظم درآورد وجود دارد (Valo, 2014: 8). بعضی از حقوق‌دانان بین‌المللی بر این باورند که حقوق بشردوستانهٔ بین‌المللی نمی‌تواند درخصوص جنگ سایبری اعمال شود، زیرا بر خلاف جنگ‌های سنتی در جنگ‌های سایبری هیچ‌گونه عملیات فیزیکی وجود ندارد. به عبارت دیگر، حملات سایبری به درگیری مسلحانه منجر نمی‌شوند، بنابراین خارج از محدودهٔ حقوق بشردوستانهٔ بین‌المللی باقی می‌مانند (Swanson, 2010: 313). مطابق با مادهٔ ۲ مشترک کنوانسیون‌های چهارگانهٔ ژنو و بند ۳ مادهٔ ۱ پروتکل الحاقی اول به کنوانسیون‌های مذکور، حمله می‌بایستی حملهٔ مسلحانه تلقی شود تا حقوق بین‌الملل بشردوستانه در آن قابل اعمال باشد. در نتیجه در صورتی که حملهٔ سایبری به آستانهٔ یک درگیری مسلحانه برسد، حقوق بین‌الملل بشردوستانه به اندازهٔ کافی انعطاف دارد تا حملات سایبری نیز تحت پوشش آن قرار گیرند (Ibid: 314). حتی برخی محققان از جمله مایکل اشمیت بر این نظرند که بعضی از حملات سایبری به آستانهٔ حملهٔ مسلحانه می‌رسند و در نتیجه مطابق با مادهٔ ۵۱ منشور ملل متحد، دولت قربانی می‌تواند به دفاع مشروع متوسل شود (Schmitt, 2013: 176). موضع‌گیری صلیب سرخ نیز اعمال حقوق بشردوستانه درخصوص حملات سایبری است که حملهٔ مسلحانه تلقی می‌شوند؛ بدین‌شرح که ابزارها و روش‌های جنگ طی زمان تغییر می‌کنند و این ابزارها و روش‌ها همان ابزارها و روش‌های زمان تهیهٔ پیش‌نویس کنوانسیون‌های چهارگانه ژنو نیستند، اما حقوق بین‌الملل بشردوستانه درخصوص تمامی اقداماتی که از سوی طرفین در جریان مخاصمهٔ مسلحانه به وقوع می‌پیوندد اعمال می‌شود و می‌بایستی به آن احترام گذاشته شود (Cyber Warfare & International Humanitarian Law: the ICRC Position, 2013: 2). مطابق مادهٔ ۲ مشترک در کنوانسیون‌های چهارگانهٔ ژنو «علاوه بر مقرراتی که باید در زمان صلح اجرا شود، این کنوانسیون در صورت وقوع جنگ رسمی یا هرگونه مخاصمهٔ مسلحانه که بین دو یا چند دولت از دولت‌های معظمهٔ متعاهد صورت پذیرد به موقع اجرا گذاشته خواهد شد حتی در صورتی که یکی از دولت‌ها وجود حالت جنگ را تصدیق نکرده باشند». در نتیجه به نظر می‌رسد قواعد حاکم بر جنگ‌های سنتی در

درگیری‌های سایبری قابل اعمال است، اما می‌بایستی به این نکته نیز توجه کرد که تمامی حملات سایبری نمی‌بایستی تحت پوشش این قواعد قرار گیرند (Jastram & Quintin, 2011: 3). چارچوب حقوقی قابل اعمال در حقوق بشردوستانه صرفاً درخصوص حملاتی است که به سطح حملهٔ مسلحانه رسیده یا اینکه حملات سایبری هنگام درگیری‌های مسلحانه اتفاق افتاده باشند (Hathaway & Others, 2012: 817). البته درخصوص اینکه چه میزان شدت و وخامت در توسل به زور سبب درگیری مسلحانهٔ بین‌المللی می‌شود بین حقوق‌دانان اتفاق‌نظر وجود ندارد (Roscini, 2014: 132)، اما عملکرد دولت‌ها، اعتقاد حقوقی آن‌ها، نظریات قضایی و دیدگاه اکثر مفسران حقوق بین‌الملل نیز حاکی از این است که برای رسیدن به سطح درگیری مسلحانه، حمله می‌بایستی به سطح معینی از شدت و وخامت رسیده باشد. درخصوص ارزیابی شدت و وخامت می‌توان به تعداد جنگجویان، نوع و تعداد سلاح‌های استفاده‌شده و مدت زمان و گستردگی حمله توجه کرد (Final Report on the Meaning of Armed Conflict in International Law, 2010: 29-30).

درخصوص حملات سایبری نظریهٔ غالب در سطح بین‌المللی بر این است که حقوق بین‌الملل برای دربر گرفتن حملات سایبری کافی است. این دیدگاه در بعضی مقالات و اسناد بین‌المللی همانند راهنمای تالین نیز منعکس شده و حاکی از این است که اصول عمومی بین‌الملل می‌بایستی درخصوص حملات سایبری اعمال شوند (Valo, 2014: 7). برخی نویسندگان نیز بر این باورند که یک‌سری قواعد مربوط به حقوق درگیری‌های مسلحانه می‌بایست تغییر کنند تا بتوانند حملات سایبری را دربر گیرند.[1] با اینکه تعریف درگیری مسلحانه در کنوانسیون‌های ژنو حملات سایبری را دربر نمی‌گیرد، اما با تفسیری از کنوانسیون‌های مذکور، حملات سایبری می‌توانند در آن تعریف قرار گیرند. به بیان دیگر، حقوق بشردوستانه به طور مستقیم برای جنگ‌های سایبری به وجود نیامده است، اما این قواعد به اندازهٔ کافی قابلیت انعطاف دارند تا شامل تکنولوژی های جدید نیز بشوند. این موضوع در شرط مارتنز نیز انعکاس یافته که ابتدا در مقدمهٔ کنوانسیون دوم ۱۸۹۹، سپس در بند ۲ مادهٔ ۱ پروتکل الحاقی اول به کنوانسیون‌های ژنو بیان شده است. وقتی هیچ موافقت‌نامهٔ بین‌المللی در قضیهٔ مورد بحث وجود ندارد یا در وضعیت‌هایی که پروتکل ذکرشده شامل آن نمی‌شود، عرف تثبیت‌شده، اصول انسانیت و وجدان عمومی در موارد موردنظر قابل اعمال‌اند (Ibid: 7-8). این موضوع در قضیهٔ مشروعیت استفاده از سلاح‌های هسته‌ای نیز از سوی دیوان بین‌المللی دادگستری تأیید شده است (Legality of the Threat or Use of Nuclear Weapons, 1996: 78). درخصوص محدودیت‌هایی بر این‌گونه قواعد همانند اصل تفکیک، صلیب سرخ نیز موضع

---

۱. برای مطالعهٔ بیشتر ر.ک. (Hollis, 2007: 1023).

مشابهی را اتخاذ کرده است که بر مبنای آن این‌گونه قواعد صرفاً به روش یا سلاح خاصی محدود نیستند (Geib, 2010: 51).

اگر حملهٔ سایبری به‌منزلهٔ حمله‌ای مسلحانه تلقی شود به‌تبع دیدگاه مذکور مقررات حقوق بشردوستانه از جمله ممنوعیت حمله به غیرنظامیان، اموال غیرنظامی، افراد و اموال تحت حمایت، همچنین محدودشدن خسارات مادی قابل اعمال دانسته خواهد شد. همین طور در این‌گونه حملات، متخاصم در استفاده از زیرساخت‌های سایبری در سرزمین‌های بی‌طرف محدودیت خواهد داشت (Schmitt, 2013: 178). ملاحظه می‌شود با اینکه حقوق در جنگ برای اعمال در حملات سایبری تکوین نیافته و ممنوعیتی برای آن‌ها تصریح نکرده است، اما قواعد حاصل از حقوق جنگ رفتار متخاصمان را نظم می‌دهد (Geib, 2010: 53). نتیجه اینکه قواعد حقوق بین‌الملل بشردوستانهٔ کنونی عموماً نسبت به جنگ‌های سایبری قابلیت اعمال دارند هرچند اعمال برخی از این قواعد نیازمند دقت و توجه بیشتری است. در هر حال در انطباق حملات سایبری با تعاریف بایستی دقت لازم اعمال شود، زیرا هرگونه طرز تلقی یا موضع‌گیری می‌تواند زمینهٔ ایجاد عرف بین‌المللی را در حوزهٔ موردنظر فراهم کند.

در ادامه به بررسی چهار اصل از حقوق بشردوستانه در بحث حملات سایبری می‌پردازیم که مناقشات زیادی را نیز بین حقوق‌دانان بین‌المللی ایجاد کرده‌اند (خلیل‌زاده، ۱۳۹۳: ۶۰).

اصول حاکم بر جنگ سایبری در چارچوب حقوق بشردوستانهٔ بین‌المللی

۱. اصل تفکیک و قابلیت اعمال آن در جنگ‌های سایبری

اصل تفکیک[1] یکی از اصول بنیادین و ضروری حاکم بر حقوق درگیری‌های مسلحانه (Bothe, 2011: 51) و از جمله حقوق بین‌الملل عرفی قابل اعمال در درگیری‌های مسلحانهٔ بین‌المللی و غیربین‌المللی است (Henckaerts & Doswald-Beck, 2009: 3) و حتی برخی این اصل را به‌منزلهٔ قاعده‌ای آمره تلقی می‌کنند (زمانی و رفیعی، ۱۳۹۲: ۴۴). این اصل افراد نظامی را که می‌توانند در درگیری‌های مسلحانه و غیرنظامیانی که نباید در چنین حملاتی هدف قرار گیرند تعیین می‌کند. اصل مذکور همچنین بین اهداف نظامی مجاز و اشیا و اموال غیرنظامی که نمی‌توانند مورد حمله قرار گیرند تفکیک قائل شده است. این اصل در مواد ۴۷ و (ii) (a) (۲) ۵۷ و بند ۴ مادهٔ ۵۱ پروتکل الحاقی اول به کنوانسیون ژنو و مادهٔ ۲۷ کنوانسیون چهارم لاهه

1. The Principle of Distinction.

قید شده است. حملات کورکورانه[1] نیز مطابق بند ۴ و ۵ مادهٔ ۵۱ پروتکل الحاقی اول به کنوانسیون‌های چهارگانه ژنو ممنوع‌اند. حملات کورکورانه به حملاتی گفته می‌شوند که نمی‌توانند به سمت یک هدف نظامی خاص روانه یا اینکه آن حملات عواقبی دارند که نمی‌توانند به اندازهٔ کافی محدود شوند که در نتیجه آن حملات اهداف نظامی، غیرنظامیان و اموال غیرنظامی را بدون تمایز دربر می‌گیرند (Ishøy, 2008: 109). درخصوص فضای سایبر با توجه به ارتباط بین شبکه‌های غیرنظامی و نظامی، بعضی از حقوق‌دانان بین‌المللی بر این نظرند که این اصل برای تنظیم قواعد مربوط به جنگ سایبری نامناسب‌اند، زیرا امکان مداخلهٔ سیگنال‌های استفاده‌شده در حملات سایبری با شبکه‌های غیرنظامی را نمی‌توان نادیده گرفت. همچنین، اعمال اصل تفکیک در فضای سایبر بسیار مشکل است، زیرا فضای سایبر مبتنی بر گمنامی است و مشکلات مربوط به انتساب، تشخیص اهداف قانونی را از غیرقانونی مشکل می‌کند (Lobel, 2012: 629-631). با وجود مشکلاتی که درخصوص اعمال این اصل در حملات سایبری وجود دارد، طراحی این‌گونه حملات می‌تواند به‌گونه‌ای شکل گیرد که قابلیت اعمال این اصل را داشته باشد. مطابق قاعدهٔ ۳۱ راهنمای تالین نیز اصل تفکیک قابلیت اعمال درخصوص حملات سایبری را دارد. در صورت هرگونه تردید یا ابهام نسبت به اینکه آیا یک فرد نظامی است یا غیرنظامی یا اینکه یک شیء مربوط به غیرنظامیان است یا خیر؟ نیز مطابق مادهٔ ۵۰ و بند ۳ مادهٔ ۵۲ پروتکل الحاقی اول به کنوانسیون‌های چهارگانهٔ ژنو، آن موارد غیرنظامی تشخیص داده می‌شوند. این موضوع در دفترچهٔ راهنمای نظامی تعدادی از کشورها نیز قید شده است (Henckaerts & Doswald-Beck, 2009: 24). قاعدهٔ ۳۳ راهنمای تالین نیز مقررات مشابهی را در این زمینه مقرر کرده است؛ بدین‌شرح که در صورت تردید نسبت به اینکه یک شخص غیرنظامی است، آن فرد می‌بایستی غیرنظامی محسوب شود. از آنجا که هیچ لباس متحدالشکل قابل استفاده در فضای سایبر نیز وجود ندارد و با توجه به خصوصیات و ماهیت فضای سایبر، تشخیص اینکه یک هدف نظامی یا غیرنظامی است بسیار مشکل است (Lobel, 2012: 629-631). مطابق پروتکل الحاقی اول، قراردادن زندگی غیرنظامیان در مواجهه با هرگونه خطر یا تهدید و حتی گرسنه نگه‌داشتن مردم ممنوع اعلام شده است. در اصل مذکور این ممنوعیت به شکل مشابه در تخریب اموال و اشیایی که برای زنده‌ماندن اشخاص ضرورت دارند نیز پیش‌بینی شده است. همچنین، مادهٔ ۳۶ پروتکل الحاقی اول به کنوانسیون‌های چهارگانهٔ ژنو دربارهٔ سلاح‌های جدید نیز بیان می‌دارد در صورتی که طرفین معاهده روش‌ها و سلاح‌های نوین جنگی را به کار گیرند متعهدند ممنوعیت یا عدم ممنوعیت استفاده از آن‌ها را مطابق پروتکل مذکور یا دیگر قواعد حقوق بین‌الملل تعیین کنند. مطابق مادهٔ ۵۵ پروتکل الحاقی اول، استفاده از روش‌ها و ابزار جنگی که به

1. Indiscriminate Attacks.

تهدید سلامت یا زنده‌ماندن جمعیت منجر شود ممنوع اعلام شده است (Bothe, 2011: 53-54).

از مقررات مذکور این نتیجه حاصل می‌شود که نه‌تنها واردکردن خسارات فیزیکی به جمعیت غیرنظامی ممنوع است، بلکه ابزاری که به تغییر هرگونه شرایط زندگی منجر و سبب رنج غیرنظامیان شود نیز ممنوع است. در حملات سایبری عواقب بعدی می‌توانند به‌منزلهٔ آلام تلقی شوند. اگر حمله‌ای سایبری سبب بی‌نظمی و هرج و مرج در یک کشور شود به طور قطع تمام جنبه‌های زندگی غیرنظامیان را تحت تأثیر قرار می‌دهد، اگرچه آن حمله نمی‌توانسته است به طور فیزیکی به غیرنظامیان آسیبی بزند. البته این موضوع نیز نباید مغفول واقع شود که یک حملهٔ سایبری به‌تنهایی نیز می‌تواند به طور مستقیم یا غیرمستقیم به مرگ یا خسارات فیزیکی منجر شود. در نتیجه دولت‌ها می‌بایست در استفاده از سلاح‌هایی که قادر نیستند بین نظامیان و غیرنظامیان تفکیک قائل شوند خودداری کنند (Kelsey, 2008: 1436) که این موضوع در نظریهٔ مشورتی سال ۱۹۹۶ دیوان بین‌المللی دادگستری در قضیهٔ مشورتی مشروعیت تهدید به استفاده از سلاح‌های هسته‌ای نیز تأیید شده است (Legality of the Threat or Use of Nuclear Weapons, 1996: 78).

در صورتی که بخواهیم جنگ سایبری را در چارچوب اصل تفکیک بررسی کنیم تجزیه و تحلیل آن مشابه همان تجزیه و تحلیل جنگ‌های با سلاح سنتی خواهد بود. بعضی بر این باورند که اهداف قانونی و مشروع در جنگ‌های سنتی دربارهٔ جنگ‌های سایبری نیز قانونی‌اند. بنابراین، هرگونه ممنوعیت یا محدودیتی مطابق حقوق بشردوستانه در جنگ‌های سایبری نیز قابل اعمال است. به عبارت دیگر، استفاده از سلاح‌های سایبری بر اهداف نظامی مجاز است و در وضعیت‌هایی که جمعیت و اموال غیرنظامی به خطر می‌افتند اهمیت این اصل آشکار می‌شود که طی آن هر حمله‌ای که سبب مرگ یا واردشدن خسارت به جمعیت غیرنظامی شود ممنوع است (Kelsey, 2008: 1437-1438). به بیان دیگر، استفاده از سلاح سایبری در جنگ ممنوع نیست و صرفاً شیوهٔ کاربرد سلاح‌های سایبری است که می‌تواند به نقض اصل تفکیک منتهی شود (ممتاز و شایگان، ۱۳۹۳: ۱۰۳). علاوه بر این، اعمال اصل تفکیک نیز از سوی راهنمای تالین تأیید شده است (Tallinn Manual, 2013: Rule 31: 110). نکتهٔ دیگری که در این زمینه باقی می‌ماند اهدافی است که استفادهٔ دوگانه[1] دارند یعنی هم از سوی نظامیان استفاده می‌شوند و هم غیرنظامیان. اعمال این اصل درخصوص این اهداف بسیار دشوار است. از جملهٔ این اهداف می‌توان به نیروگاه‌های برق، پل‌ها و زیرساخت‌های غیرنظامی، که از سوی ارتش در جنگ استفاده می‌شوند، اشاره کرد (Kelsey, 2008: 1437). بیشتر استفاده‌هایی نیز که از فضای سایبر و وسایل و ابزار مربوط به آن می‌شود ذاتاً دوگانه است و عملاً موضوع اعمال

1. Dual-use Targets.

اصل تفکیک را با دشواری‌های زیادی مواجه می‌کنـد (Department of Defense Cyberspace Policy Report, 2011: 3).

۲. اصل تناسب و قابلیت اعمال آن در جنگ‌های سایبری

اصل تناسب[1] یکی از اصول مهم حقوق بشردوستانه است که به موجب آن باید نسبت معقـول و قابل توجیهی در نتایج نظـامی حاصـل از حملـه بـا زیـان‌هـای اتفـاقی وارده بـه افـراد و امـوال غیرنظامی وجود داشته باشد.

این اصل در قسمت ب از بند ۵ مادۀ ۵۱ پروتکل الحاقی اول به کنوانسیون‌های چهارگانـۀ ژنـو آمده است که مقرر می‌دارد: «در کنار سایر موارد، انواع حملات زیر به‌عنوان حمـلات غیرهدفمنـد محسوب می‌گردند: ..... ب. حملـه‌ای کـه انتظـار مـی‌رود سـبب ازدسـت‌دادن جـان غیرنظامیـان، واردشدن خسارت به غیرنظامیان، باعث ورود خسارت به اموال غیرنظامیان و تلفیقی از آن‌ها شـود که در ارتباط با دستاوردهای پیش‌بینی‌شدۀ عینی و مستقیم بیش از اندازه شود».

این اصل به طور کلی به‌منزلۀ یک اصل در حقوق بین‌الملل عرفی در درگیری‌های مسـلحانۀ بین‌المللی و غیربین‌المللی پذیرفته شده (Talbot, 2013: 204) و مستلزم برقـراری تعـادل بـین مزیت‌های نظامی و حمایت از غیرنظامیان است. البته حقوق بشردوستانه مشخص نکـرده اسـت که چگونه ارزش‌های مختلف می‌بایستی در مقابل همدیگر برای اعمال این اصل سنجیده شـوند (Dill, 2010: 3).

برای کارآمدبودن اصل تناسب به اقدامات دیگری نیز نیاز اسـت. مطـابق مـادۀ ۵۷ پروتکـل الحاقی اول به کنوانسیون‌های چهارگانۀ ژنو، متخاصمان می‌بایستی تمام احتیاط‌هـای ممکـن و مراقبت‌های ثابت را به‌منظور اجرای اصل تناسب و تفکیک در نظر گیرند. همچنین مطابق ایـن ماده، تعهداتی برای متخاصمان وجود دارد کـه شـامل خـودداری از حملـه‌ای اسـت کـه بـالقوه نامتناسب است، لغوکردن یا به تعویق‌انداختن حمله‌ای که بالقوه نامتناسب اسـت و همـین‌طـور انتخاب هدفی که بیشترین سازگاری را با اصل تناسب دارد. این اصل غالباً به شـکل غیرعمـد و صرفاً به دلیل سهل‌انگاری و بی‌دقتی در هدف‌گیری ناشی از سه دلیل عمده نقـض شـده اسـت. اول ناآگاهی، دوم ناتوانی در تخمین میزان نیروی نظامی استفاده‌شـده در برابـر اهـداف و سـوم ناتوانی در هدف قراردادن دقیق و کامل. در حملات سایبری همۀ ایـن مـوارد از عوامـل مـذکور می‌توانند به وقوع بپیوندند (Schmitt, 1998: 1080-81) (به نقل از: اصـلانی، ۱۳۹۱: ۱۶). بعضـاً این رویکرد نیز وجود دارد که اصل تناسب درخصوص جنگ‌های سایبری قابلیت اعمـال نـدارد، بلکه مرکزیت این مباحث بیشتر در به‌کـارگیری ایـن اصـل در مـوارد بـه‌خصوصـی از عملیـات

1. The Principle of Proportionality.

سایبری است. مطابق راهنمای تالین، در حملات سایبری آسیب به غیرنظامیان یا اشیا غیرنظامی فی‌نفسه سبب غیرقانونی‌شدن آن حمله نمی‌شود، بلکه این موضوع به ارتباط بین صدمه‌ای که حمله‌کننده به طور معقول انتظار دارد که ناخواسته به غیرنظامیان و نظامیان وارد شود و مزیت نظامی که او در نتیجهٔ حمله پیش‌بینی می‌کند بستگی دارد (Tallinn Manual, 2013: 132).

به عبارت دیگر، در بسیاری از حملات سایبری اصل تناسب به‌راحتی قابلیت اعمال و اجرا ندارد. برای مثال، طی جنگ خلیج‌فارس حمله‌ای سایبری با هدف حمله به شبکهٔ توزیع برق عراق صورت گرفت، اگرچه این حمله به اختلال در فرماندهی و کنترل مؤثر نیروهای عراقی منجر شد، اما آثار مخربی ناشی از قطع‌شدن برق در بیمارستان‌ها، سیستم‌های حمل و نقل و سیستم‌های ارتباطی به‌منزلهٔ آثار غیرمستقیم این حملات گذاشته شد (Ibid: 17). با اینکه قابلیت اعمال این اصل در اکثر حملات سایبری به دلیل ماهیت فضای سایبر دشوار است نمی‌توان امکان اعمال این اصل را کلاً منتفی برشمرد.

۳. اصل بی‌طرفی و قابلیت اعمال آن در جنگ‌های سایبری

منابع اصل بی‌طرفی[1] در حقوق بین‌الملل شامل حقوق بین‌الملل عرفی و در بخش‌هایی نیز حقوق معاهدات به خصوص بیانیهٔ ۱۸۵۶ پاریس، کنوانسیون لاهه ۱۹۰۷ درخصوص حقوق و وظایف قدرت‌ها و اشخاص بی‌طرف در صورت وقوع جنگ زمینی، کنوانسیون ۱۹۰۷ لاهه درخصوص حقوق و وظایف قدرت‌ها و اشخاص بی‌طرف در جنگ‌های دریایی، کنوانسیون‌های چهارگانهٔ ژنو و پروتکل الحاقی اول به کنوانسیون‌های چهارگانهٔ ژنو سال ۱۹۷۷ می‌شوند (The Law of Armed Conflict, Neutrality, 2002: 2).

سرزمین کشورهای بی‌طرف مطابق حقوق بشردوستانهٔ بین‌المللی از تعرض مصون‌اند (باث، ۱۳۹۱: ۶۳۷). انجام هرگونه اقدام خصمانه در چنین سرزمین‌هایی ممنوع است. بی‌طرفی درواقع موضع رسمی است که دولتی که در درگیری مسلحانه حضور ندارد یا نمی‌خواهد در آن درگیر شود اتخاذ می‌کند. این وضعیت مستلزم حقوق و وظایفی خاص است. اشخاص بی‌طرف در صورتی که به اقدامات خصمانه علیه متخاصمان مبادرت کنند از وضعیت بی‌طرفی خارج می‌شوند (Ibid: 3).

دولت‌های متخاصم نیز وظایفی در این خصوص دارند؛ از جمله اینکه آن‌ها می‌بایست به مکان‌های بی‌طرف احترام گذارند و از واردکردن خسارت به آن‌ها اجتناب کنند. متخاصمان می‌بایست به نیروهای مسلحشان دستورالعمل‌هایی مبنی بر خودداری از هرگونه اقدام

1. The Principle of Neutrality.

خشونت‌بار در محدودهٔ مکان‌های بی‌طرف صادر کنند (Ibid). ممنوعیت‌های موجود در حقوق مربوط به بی‌طرفی سرچشمه‌گرفته از اصل برابری حاکمیت دولت‌ها در حقوق بین‌الملل است که اعمال صلاحیت در سرزمین دولتی دیگر را منع می‌کند (شایگان، ۱۳۹۵: ۳۴۲). حقوق مربوط به اصل بی‌طرفی می‌تواند مانعی در انجام بخشی از حملات سایبری تلقی شود، اما متأسفانه اینترنت به‌گونه‌ای طراحی نشده است که رعایت اصل بی‌طرفی در آن پیش‌بینی شده باشد. بدین‌توضیح که اینترنت فی‌نفسه شامل مجموعه‌ای از شبکه‌هاست که بخش‌های خصوصی و دولتی را دربر دارد، اما شبکه‌های کامپیوتری نظامی ساختاری جدا از طراحی عمومی اینترنت دارند و هنگام بهره‌برداری‌شدن باید به اینترنت متصل شوند. نیروهای نظامی اغلب هنگام وقوع درگیری مسلحانه از سیستم ارتباطی اینترنت به‌منزلهٔ منبع پشتیبانی‌کنندهٔ ساختار شبکهٔ کامپیوتری خود استفاده می‌کنند (Kodar, 2012: 113-114).

در نهایت با توجه به نکاتی که دربارهٔ بی‌طرفی ذکر شد و ماهیت حملات سایبری، می‌توان به این نتیجه رسید که حملات سایبری معمولاً با حقوق مربوط به بی‌طرفی در تعارض‌اند. ماهیت حملات سایبری این موضوع را مطرح می‌کند که آیا حملات سایبری می‌توانند با دقت و ظرافتی انجام شوند که دولت‌های بی‌طرف را تحت تأثیر خود قرار ندهند. از طرف دیگر، برای دولت‌های بی‌طرف نیز این خطر وجود دارد که ناخواسته از طریق شبکه‌هایشان جنگ بین متخاصمان را هموار و تسهیل کنند.

۴. اصل ضرورت نظامی در جنگ‌های سایبری

اصل ضرورت نظامی استفاده از زور موردنیاز در انجام عملیات را مجاز شمرده است، در عین حال مبادرت به اعمالی که حقوق جنگ آن را منع کرده است مجاز نمی‌داند. اصل ضرورت نظامی می‌بایستی همراه با دیگر اصول حقوق جنگ و همین‌طور محدودیت‌های قانونی خاصی که در موافقت‌نامه‌های بین‌المللی مربوط به حقوق جنگ بیان شده است به کار گرفته شود (Graham, 2010: 98). اصل مذکور با اهداف جنگ رابطه‌ای تنگاتنگ دارد (ساعد، ۱۳۹۳: ۲۶۳). در حقیقت اصل ضرورت بیان‌کنندهٔ این موضوع است که در عملیات نظامی می‌بایست با توسل به کمترین اقدام تخریبی به امتیازی نظامی دست یافت (نوده‌توپچی، ۱۳۹۳: ۷۸) و میزان صدمات و خساراتی که حملات وارد می‌کنند می‌بایست با منفعت نظامی آن تناسب داشته باشند (تدینی و کازرونی، ۱۳۹۵: ۲۷). درخصوص فضای سایبر این اصل بیشتر در پاسخ به حملات سایبری کاربرد می‌یابد. در حملات سایبری که به حد درگیری مسلحانه رسیده باشند، با توجه به مادهٔ ۵۱ منشور، دولت‌های قربانی می‌توانند در دفاع مشروع به زور متوسل شوند، اما با توجه به اصل ضرورت نظامی در جنگ‌های سایبری و ماهیت حملات سایبری، اقدامات متقابل الکترونیکی می‌تواند

به‌منزلهٔ دفاع مشروع در پاسخ به حملات سایبری صورت گیرد. آنچه در قبال حملات سایبری ضرورت اقدام نظامی را ایجاب می‌کند صرفاً برای جلوگیری از حملات سایبری است (Ibid: 99) و توسل به سلاح‌های جنبشی برای مقابله با حملات سایبری با این اصل انطباق ندارد و می‌تواند آثار مخربی را با خود همراه داشته باشد و در نهایت به جنگ در فضای واقعی میان دولت‌ها منتهی شود.

حملات سایبری به گرجستان

۱. واقعیات قضیه

در ۲۰ جولای ۲۰۰۸ به وب‌سایت رئیس‌جمهور گرجستان حملهٔ سایبری از نوع حملات محروم‌سازی از سرویس توزیع‌شده صورت گرفت. حملات انجام‌شده وب‌سایت مذکور را برای مدت ۲۴ ساعت بست و مقدمه‌ای شد برای حملات وسیع‌تری که ظرف کمتر از یک ماه به وقوع پیوستند. در آگوست ۲۰۰۸ حملات هماهنگی از نوع محروم‌سازی از سرویس توزیع‌شده به وب‌سایت‌های دولتی گرجستان همزمان با درگیری نیروهای نظامی روسیه با گرجستان شکل گرفت. با پیشرفت حملات زمینی حملات سایبری نیز افزایش می‌یافتند. حملات سایبری به گرجستان اولین حمله ای بود که حملات سایبری با حملات زمینی نیروهای مسلح هم زمان با یکدیگر ترکیب شده بودند (Ashmore, 2009: 10).

حملات سایبری به گرجستان از قلمرو سرزمین روسیه صورت پذیرفته بود، اما همانند حملات انجام‌شده به استونی، کارشناسان نتوانستند بین مقامات روسی با حملات مذکور ارتباطی بیابند. در عین حال سازمانی که با حدود صد کارشناس به طور داوطلبانه در این زمینه فعالیت دارد طی بررسی خود اعلام کرد که سطح آماده‌سازی بستر حمله و شناسایی‌های صورت‌گرفتهٔ قبلی در حملهٔ گرجستان به‌وضوح نشان می‌دهد که هکرهای روس برای حملات از سوی مقامات دولت روسیه آماده شده بودند (Kozlowski, 2014: 240). زیرساخت‌های فناوری اطلاعات گرجستان به میزان کافی پیشرفته نبود به همین دلیل حملات سایبری به گرجستان پیچیدگی حملات استونی را نداشتند. وب‌سایت‌های بانکی، رسانه‌ای و دولتی مسدود شدند و انتقال و ارسال اطلاعات به گرجستان و از گرجستان به دیگر نقاط دنیا با مشکل مواجه شد. حملات سایبری که در گرجستان اتفاق افتاد با حملات سایبری استونی متفاوت بود، زیرا آن ها علاوه بر حملات نفی سرویس توزیع‌شده، از حملات دیگری[1] نیز استفاده کرده بودند که خصوصیت این حملات مشکل‌تربودن شناسایی حمله بود. گرجستان برای مقابله با حملات سایبری مذکور و برقراری ارتباط‌های داخلی و بین‌المللی‌اش کمک‌های زیادی دریافت کرد. شرکت گوگل فضایی

1. SQL Injection Attacks.

اینترنتی را برای حمایت از وب‌سایت‌های وزیر امور خارجه و سرویس اخبار روزانهٔ آنلاین گرجستان در نظر گرفت. یک شرکت خصوصی امریکایی فراهم‌کنندهٔ خدمات اینترنتی[1] نیز به گرجستان کمک کرد (Ashmore, 2009: 10-11).

۲. تحلیل حقوقی قضیه

اینکه آیا حملات سایبری به گرجستان حملهٔ مسلحانه تلقی می‌شده و آیا این کشور متعاقباً حق توسل به دفاع مشروع را داشته یا نه؟ موضوعی نسبتاً پیچیده است. همان‌طور که گفته شد، میان حملهٔ سایبری و جنگ سایبری در چارچوب حقوق بشردوستانهٔ بین‌المللی وجه فارقی وجود دارد. وقتی حملات سایبری به ایجاد صدمات فیزیکی یا خسارات منجر و زمانی که آن حملات به آثار موردنظر منتهی شوند، این‌گونه حملات به درگیری مسلحانه یا جنگ سایبری منجر خواهند شد (Dorman, 2004: 3). از طرف دیگر نیز مطابق قاعدهٔ ۲۰ راهنمای تالین، هرگونه عملیات سایبری که در چارچوب حملهٔ مسلحانه به وقوع بپیوندد موضوع حقوق مربوط به مخاصمات مسلحانه خواهد بود. به عبارت دیگر، در صورتی که مخاصمات مسلحانهٔ بین‌المللی به وقوع بپیوندد حقوق درگیری‌های مسلحانه بر تمامی عملیات سایبری که در قالب آن مخاصمه به وقوع می‌پیوندد نیز اعمال می‌شود (Tallinn Manual, 2013: 75). در نتیجه اینکه در چنین وضعیت‌هایی مقررات و قواعد بین‌المللی حاکم در زمان مخاصمات مسلحانه به کار گرفته می‌شوند تا رفتار و عملکرد دولت‌ها را هنگام درگیری‌های مسلحانه به نظم درآورند. این در حالی است که به نظر برخی دیگر، حقوق بشردوستانهٔ بین‌المللی نمی‌تواند درخصوص جنگ سایبری اعمال شود، زیرا بر خلاف جنگ‌های سنتی در جنگ‌های سایبری هیچ‌گونه عملیات فیزیکی وجود ندارد. به عبارت دیگر، حملات سایبری به درگیری مسلحانه منجر نمی‌شوند، بنابراین حملات سایبری خارج از محدودهٔ حقوق بشردوستانهٔ بین‌المللی باقی می‌مانند (اصلانی، ۱۳۹۳: ۵).

با وجود این، حقوق جنگ چارچوب مفیدی را صرفاً برای حملات سایبری در سطح یک حملهٔ مسلحانه یا حملات سایبری که در چارچوب یک مخاصمهٔ مسلحانهٔ در جریان می‌یابد، فراهم می‌آورد (Hathaway & others, 2012: 817). هر چند در این خصوص اتفاق‌نظری موجود نیست، عملکرد دولت‌ها، اعتقاد حقوقی آن‌ها، نظریات قضایی و دیدگاه اکثر مفسران حقوق بین‌الملل حاکی از این است که برای رسیدن به سطح درگیری مسلحانه، حملهٔ سایبری می‌بایست به سطح معینی از شدت و وخامت رسیده باشد. درخصوص ارزیابی شدت و وخامت نیز می‌توان به تعداد جنگجویان، نوع و تعداد سلاح‌های استفاده‌شده و مدت زمان و گستردگی

1. Internet Service Provider.

حملـه توجـه داشـت (Final Report on the Meaning of Armed Conflict in International Law, 2010: 29-30).

دو جنبهٔ درخور توجه در حملات سایبری به گرجستان وجود دارد؛ نخست اینکه بین حملات بـا سلاح‌های سنتی و حملات سایبری هماهنگی کامل وجود دارد که این امـر در نـوع خـود بـی‌سـابقه است. جنبـهٔ دوم، آمـاده‌سـازی ابزارهـای سـایبری، آمـوزش و وب‌سـایت‌هـای مخصـوص بـرای بـر عهده گرفتن حملات است که همگی حاکی از این موضوع است که روسیه خیلـی پـیش‌تـر در حـال آماده‌شدن برای این جنگ بوده است. دسترسـی بـه ابزارهـا و نـرم‌افزارهـای مربوطـه بـرای حملـه و آموزش استفاده از این ابزارها به طور یقین زمـان زیـادی را مـی‌طلبیـده اسـت (Kozlowski, 2014: 240).

در تحلیل حقوقی این قضیه می‌توان گفت با توجه به اینکه حمـلات سـایبری بـه گرجسـتان بـا حملات فیزیکی روسیه همراه شده است، در نتیجه حمله‌ای مسلحانه به وقوع پیوسته است، اما فـارغ از اقدامات جنبشی شکل گرفته حملات به آستانه‌ای نرسیده بودند که بتوان آن‌ها را به‌تنهایی حملـهٔ مسلحانه قلمداد کرد (Watts, 2011: 71). حملات سایبری مذکور به وب‌سایت‌های دولتی گرجسـتان صورت گرفته بود و سبب ازکارافتادن رسانه‌های این کشور و اخلال در ارتباطات داخل و خارج کشـور شد (Lomidze, 2011: 6)، اما شدت حملات در سطحی نبود که خسارات و صدمات شـدید بـه ایـن کشور وارد کند. با در نظر گرفتن تقارن حملات زمینی و سایبری و لاجرم تحقق جنـگ سـایبری در قالب حقوق بشردوستانهٔ بین‌المللی، لازم است تا به تحلیل این امر بپردازیم که آیـا اصـول حـاکم بـر مخاصمات مسلحانهٔ سنتی به این حملات نیز تسری می‌یابند یا خیر؟

معمولاً با توجه به اینکـه در فضـای سـایبر عمـلاً هـدف قـراردادن سیسـتم خاصـی بـدون آسیب‌رسانی به سیستم‌های دیگر به‌ندرت اتفاق می‌افتـد، در عمـدهٔ حمـلات سـایبری امکـان و قابلیت تفکیک و شناسایی شبکه‌های نظامی از غیرنظامی وجود ندارد یا در صورت وجودداشـتن نیز حملات سایبری محدودی با قابلیت تشخیص و تفکیک هـدف طراحـی مـی‌شـوند. حمـلات سایبری انجام‌شده به گرجستان با توجه به اینکه سیستم‌هایی را هدف قـرار داد کـه نظامیـان و غیرنظامیان از آن‌ها استفاده می‌کردند و اخلال ایجادشده صرفاً به سیستم‌هایی کـه نظامیـان از آن‌ها استفاده می‌کردند منتهی نشد، این حملات اصل تفکیک در حقوق بین‌الملل بشردوسـتانه را نقض کردند. حملات سایبری مذکور سبب اخلال در تبادل صحیح اطلاعات شـد و مـی‌تـوان گفت مردم این کشور نیز قربانی حملات سایبری به گرجستان بودند. درخصوص اصـل تناسـب نیز با عنایت به اینکه ارتباط معقولی بین صدمات وارده به غیرنظامیان و مزیت نظامی حاصله از حملات سایبری وجود نداشت این اصل نیز در حملات سایبری بـه گرجسـتان در نظـر گرفتـه نشده است، زیرا اصولاً هدف در این‌گونه حملات سیستم‌هایی بوده اسـت کـه کـاربردی دوگانـه داشته اند. بنابراین، این اصل از اصول حقوق بشردوستانه نیز در حملات سایبری بـه گرجسـتان

نقض شده است. دربارهٔ رعایت‌کردن یا نکردن اصل بی‌طرفی در حمله به گرجستان، چون حملات به گرجستان فقط از فضای سرزمین روسیه انجام شده بود و فضای هیچ کشور دیگری نیز مستقیماً استفاده نشد یا هدف قرار نگرفت، انتساب رعایت‌نکردن اصل بی‌طرفی فاقد توجیه به نظر می‌رسد. دربارهٔ اصل ضرورت نظامی همان‌طور که پیش‌تر نیز ذکر شد با توجه به اینکه این اصل بیشتر در پاسخ به حملات سایبری موضوعیت می‌یابد از بحث و تحلیل حاضر خارج است.

نتیجه‌گیری

بی‌تردید وابستگی پایداری میان جامعه و حقوق برقرار است، لذا هرگونه تحولی در جامعه نیازمند بازنگری جدی در حقوق و تعهدات حاکم بر آن تحول است. رشد دانش بشری در عرصه‌های گوناگون، حقوق بین‌الملل معاصر را نیز به طور چشمگیری متحول کرده و به پیوند میان علوم مختلف انجامیده است. روشن است هرگاه این تحول زمینه‌ساز پویایی حقوق بین‌الملل شود، چشم‌اندازی از حرکت و کارآمدی حقوق بین‌الملل را به تصویر می‌کشد، اما زمانی که قواعد و مقررات حقوقی قادر به ساماندهی آن تحولات نباشند، شکافی حادث می‌شود که بی‌تردید نیازمند تأملی جدی در اقتضائات موجود و چالش‌های مفروض است و در صورتی که درخصوص موضوعی جدید با کمبود منابع مواجه شویم به‌ناچار باب تفاسیر متعدد در قالب قواعد موجود بازمی‌گردد که قطعاً همهٔ این تفاسیر به نتایج مشابهی که در نهایت می‌بایستی به برقراری صلح و امنیت بین‌المللی در سطح جهان ختم شوند منتهی نخواهند شد. مسلماً بهترین راه‌حل برای به نظم‌درآوردن وضعیت حقوقی تکنولوژی‌های جدید در سطح بین‌المللی انعقاد معاهداتی برای مشخص‌کردن چارچوب آن‌هاست که جنگ سایبری از آن مستثنا نیست، اما با توجه به عملی‌نبودن این موضوع در شرایط کنونی، حداقل تفاسیری می‌بایستی مطرح و از سوی دولت‌ها پذیرش شوند که با اهداف منشور ملل متحد در حفظ صلح و امنیت بین‌المللی همسو باشند.

یکی از چالش‌هایی که دولت‌ها با تحول تکنولوژی با آن مواجه شده‌اند قابلیت استفاده از فضای سایبر در قالب ابزاری جنگی و یا میدان نبرد است. هرچند هنوز رویهٔ حقوقی منسجمی در این‌گونه موارد شکل نگرفته است، اما در صورت احراز رسیدن حملات سایبری به درگیری مسلحانه یا وقوع حملات سایبری با هر درجه‌ای از شدت و ضعف در خلال درگیری‌های مسلحانهٔ سنتی، می‌توان اصول و مقررات فعلی حقوق بشردوستانهٔ سنتی را به فضای مجازی نیز تعمیم داد و تا ایجاد رویهٔ منسجم و هنجارسازی در این باره به نظمی نسبی در این زمینه دل بست و با توجه به مقررات موجود در حقوق بشردوستانه حملات سایبری را به نظم درآورد. مطالعهٔ موردی حملات سایبری به گرجستان نیز مؤید این موضوع است که با توجه به شرایط خاصی که مطابق با آن حملات سایبری به وقوع پیوستند یعنی متقارن‌شدن حملات سنتی و

سایبری، حملات سایبری در چارچوب حقوق بشردوستانه قابل بررسی‌اند. با بررسی حملات سایبری این نتیجه حاصل شد که هرچند حقوق بشردوستانه قابلیت اعمال در حملات سایبری مذکور را دارند، اما به‌واسطهٔ خصوصیات و ماهیت حملات سایبری که درخصوص گرجستان به وقوع پیوسته اصول حقوق بشردوستانه نقض شده است.

منابع

الف) فارسی

۱. اصلانی، جبار (۱۳۹۳). «حملات سایبری از منظر حقوق بشردوستانه با نگاهی به قضیهٔ استاکس نت و ایران»، فصل‌نامهٔ *مطالعات بین‌المللی*، سال دهم، شمارهٔ ۴، ۱-۲۸.

۲. باث، میشل (۱۳۹۱). *حقوق بشردوستانه در مخاصمات مسلحانه*، حقوق بی‌طرفی، ترجمهٔ سیدقاسم زمانی، تهران: مؤسسهٔ مطالعات و پژوهش‌های حقوقی شهر دانش.

۳. تدینی، عباس و کازرونی، سیدمصطفی (۱۳۹۵). «کاربردهای نظامی فناوری نانو از منظر حقوق بین‌الملل بشردوستانه»، مجلهٔ *حقوقی بین‌المللی*، شمارهٔ ۵۴، ۲۵۷-۳۰۶.

۴. حسن‌بیکی، ابراهیم (۱۳۸۴). *حقوق و امنیت در فضای سایبر*، تهران: مؤسسهٔ فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر.

۵. خلف‌رضایی، حسین (۱۳۹۲). «حملات سایبری از منظر حقوق بین‌الملل» (مطالعهٔ موردی: استاکس نت)، فصل‌نامهٔ *مجلس و راهبرد*، سال بیستم، شمارهٔ ۷۳، ۱۲۵-۱۵۳.

۶. خلیل‌زاده، مونا (۱۳۹۳). *مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری*، تهران: مجمع علمی و فرهنگی مجد.

۷. زمانی، سیدقاسم و رفیعی، سیدرضا (۱۳۹۲). «کاربرد سلاح‌های حاوی اورانیوم ضعیف‌شده از منظر حقوق بشردوستانهٔ بین‌المللی»، مجلهٔ *حقوقی بین‌المللی*، شمارهٔ ۴۹، ۳۵-۶۰.

۸. ساعد، نادر (۱۳۹۳). *حقوق بشردوستانه و مسائل نوظهور (جنگ های پسانوین)*، چاپ دوم، تهران: انتشارات خرسندی.

۹. شایگان، فریده (۱۳۹۵). «اعمال حقوق بی‌طرفی در فضای سایبر»، فصل‌نامهٔ *مطالعات حقوق عمومی*، دورهٔ ۴۶، ۳۳۷-۳۵۷.

۱۰. ضیایی‌بیگدلی، محمدرضا (۱۳۹۲). *حقوق بین‌الملل بشردوستانه*، چاپ اول، تهران: گنج دانش.

۱۱. عبداللهی، محسن (۱۳۸۸). *تروریسم، حقوق بشر و حقوق بشردوستانه*، چاپ اول، مؤسسهٔ مطالعات و پژوهش‌های حقوقی شهر دانش.

۱۲. ممتاز، جمشید و شایگان، فریده (۱۳۹۳). *حقوق بین‌الملل بشردوستانه در برابر چالش‌های*

مخاصمات مسلحانهٔ عصر حاضر، مؤسسهٔ مطالعات و پژوهش‌های حقوقی شهر دانش.
۱۳. نواده‌توپچی، حسین (۱۳۹۳). *حقوق جنگ و مخاصمات مسلحانه*، چاپ اول، تهران: انتشارات خرسندی.

ب) انگلیسی

14. Ashmore, William C (2009). "Impact of Alleged Russian Cyber Attacks", Baltic Security & Defence Review, Vol. 11, 4-40.
15. Bothe, Michael (2011). "Setting the scene: New Challenges for IHL, International Humanitarian Law and New Weapon Technologies", 34th Round Table on Current Issues of International Humanitarian Law (Sanremo, 8th-10th September 2011), International Institute of Humanitarian Law,Available at: http://www.iihl.org/iihl/Documents/IHL%20and%20new%20weapon%20technologies_Sanremo%20%282%29.pdf, Visited on 10 September 2016.
16. Brenner, Susan W. & Clarke, Leo L (2010). "Civilians in Cyberwarfare: conscripts", *Vanderbilt Journal of Transnational Law*, Vol. 43: 1011-1076.
17. Cornish, Paul & Others (2010). *On Cyber Warfare*, A Chatham House Report, Available at: https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/r1110_cyberwarfare.pdf, Visited on 9 May 2016.
18. Dill, Janina (2010). *Applying the Principle of Proportionality in Combat Operations*, Policy Briefing, Oxford Institute for Ethics, Law and Armed Conflict.
19. Dormann, Knut (2004). *Applicability of the Additional Protocols to Computer Network Attacks*, International Committee of the Red Cross, Available at: https://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf, Visited on 11 September 2016.
20. Geib, Robin (2010). *The Legal Regulation of Cyber Attacks in times of Armed Conflict*, Proceedings of the Bruges Colloquium, Technological Challenges for the Humanitarian Legal Framework, 11th Bruges Colloquium, 21-22 October 2010, Available at: https://www.coleurope.eu/sites/default/files/uploads/page/collegium_41_0.pdf, Visited on 20 September 2016.
21. Graham, David E (2010). "Cyber Threats and the Law of War", *Journal of National Security Law and Policy*, Vol, 4, 87-102.
22. Hathaway, Oona A. & others (2012). "The Law of Cyber-Attack", California Law Review, Vol. 100:817-876.
23. Henckaerts, Jean-Mari & Doswald-Beck, Louise (2009). "Customary International Humanitarian Law", Vol 1: Rules, International Committee of the Red Cross, Cambridge University Press.
24. Hollis, Duncan B (2007). "Why States Need an International Law for Information Operations", Lewis & Clark L. Review, Vol. 11:4, 1023-1061.
25. Hughes, Rex (2009). *Towards a Global Regime for Cyber Warfare*, Cyber Security Project, Chatham House, London, Available at: http://www.ccdcoe.org/publications/virtualbattlefield/07_HUGHES%20Cyber%20Regime.pdf, Visited on 14 October 2016.

26. Ishøy, Rikke (2008). Handbook on the Practical Use of International Humanitarian Law, Danish Red Cross, Second Edition, Revised Edition.
27. Jastram, Kate & Quintin, Anne (2011). "The Internet in Bello: Cyber War Law, Ethics and Policy", Seminar held 18 November 2011, Berkeley Law, 2011, Available at: http://www.law.berkeley.edu/files/cyberwarfare_seminar--summary_032612.pdf, Visited on 19 September 2016.
28. Kelsey, Jeffrey T. G (2009). Note, "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare", Michigan Law Review, Vol. 106:1427-1451.
29. Kodar, Erki (2012). "Applying the Law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocol 1", ENDC Proceedings, Vol 15, 107-132.
30. Kozlowski, Andrzej (2014). "Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan", *European Scientific Journal*, February 2014 /SPECIAL/ edition vol.3, 237-245.
31. Lipson, Howard F (2002). Tracking *and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*, Carnegie Mellon Software Engineering Institute, Special Report CMU/sei-2002-sr-009.
32. Lobel, Hannah (2012). "Cyber War Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict", *Texas International Law Journal*, Vol 47, Issue 3, 617-640.
33. Lomidze, Irakli (2011). *Cyber Attacks against Georgia*, Ministry of Justice of Georgia, Data Exchange Agency, Available at: http://dea.gov.ge/uploads/GITI%202011/GITI2011_3.pdf, Visited on 6 October 2016.
34. Roscini, Marco (2014). *Cyber Operations and the Use of Force*, Oxford University Press.
35. Sandvik, Kristin Bergtora (2012). *Towards a Militarization of Cyberspace?*, Cyberwar as an Issue of International Law, Peace Research Institute Oslo, Available at: http://file.prio.no/publication_files/Prio/Sandvik-Cyberwar-and-International-Law-PRIO-Paper-2012.pdf, Visited on 26 December 2016.
36. Schmitt, Michael N (2013). "Reaction, Cyberspace and International Law: The Penumbral Mist of Uncertainty", Harvard Law Review Forum, Vol. 126:176.
37. Swanson, Lesley (2010). "The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict", Loyola of Los Angeles International and Comparative Law Review, Vol. 32:303-333.
38. Talbot, Eric Jensen (2013). "Cyber Attacks: Proportionality and Precautions in Attack", International Law Studies, Vol 89, 198-217.
39. Tsagourias, Nicholas & Buchan, Russell (2015). *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing.
40. *The Law of Armed Conflict, Neutrality, International Committee of the Red Cross* (2002). Available at: https://www.icrc.org/eng/assets/files/other/law8_final.pdf, Visited on 7 June 2016.
41. Valo, Janne (2014). "Cyber Attacks and the Use of Force in International Law", University of Helsinki, Master's Thesis, Available at: https://helda.helsinki.fi/bitstream/handle/10138/42701/Cyber%20Attacks%20and%20the%20Use%20of%20Force%20in%20International%20Law.pdf?sequence

=2, Visited on 7 October 2016.
42. Watts, Sean (2011). "Low-Intensity Computer Network Attack and Self-Defense, International Law and the Changing Character of War", International Law Studies, Vol. 87, 59-87.
43. Waxman, Matthew C (2011). *Cyber-Attacks and the Use of Force: Back to the Future of Article* 2 (4), The Yale Journal of International Law, Vol. 36: 421-459.
44. Yde, Iben (2013). *The Law of Cyber Armed Conflicts: Translating Existing Norms of International Humanitarian Law into Cyber Language*, Royal Danish Defense College, Available at: http://www.fak.dk/en/publications/Documents/The%20Law%20of%20Cyber%20Armed%20Conflicts.pdf, Visited on 2 September 2016.

ج) آرا و اسناد

45. Cyber Warfare and International Humanitarian Law: The ICRC Position (2013). Available at: https://www.icrc.org/eng/assets/files/2013/130621-cyber-warfare-q-and-a-eng.pdf, Visited on 28 December 2016.
46. Final Report on the Meaning of Armed Conflict in International Law (Summary). International Law Association, The Hague Conference, Use of Force, 2010
47. Legality of the Treat or Use of Nuclear Weapons (1996). Advisory Opinion, International Court of Justice.
48. Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I) 1977.
49. Research Report, XVII. Model United Nations of Lübeck (MUNOL). 2014, Available at: http://www.munol.org/uploads/ResearchReports/2014/GA%201%20-%20Establishing%20international%20regulations%20for%20cyber%20warfare%20to%20prevent%20harm%20on%20civilians.pdf, Visited on 16 September 2016.
50. Rules of International Humanitarian Law and Other Rules Relating to the Conduct of Hostilities, Collection of Treaties and Other Instruments, International Committee of the Red Cross, Geneva 1989, Revised and updated Edition, 2005.
51. Tallinn Manual on the International Law Applicable to Cyber Warfare (2013). Prepared by International Group of Experts at the Invitation of NATO Cooperative Cyber Defence Centre of Excellence (edited by M. N. Schmitt), Cambridge University Press.
52. Summary of the Geneva Convention s of 1949 and their Additional Protocol", International Humanitarian Law, American Red Cross, April 2011, Available at: http://www.redcross.org/images/MEDIA_CustomProductCatalog/m3640104_IHL_SummaryGenevaConv.pdf, Visited on 12 September 2016.
53. United Nations General Assembly, A/RES/3314 (XXIX) 14 December 1974, Available at: http://unispal.un.org/UNISPAL.NSF/0/023B908017CFB94385256EF4006EBB2A, Visited on 11 September 2016.