DOI: http://dx.doi.org/10.22106/jlj.2012.11057

حملات سایبری و حقوق بین‌الملل[1]

علی قاسمی[2]

ویکتور بارین چهاربخش[3]

چکیده

حمله‌ی سایبری، مصداق سلاح جدیدی است که می‌تواند روش هدایت جنگ مدرن توسط بازیگران دولتی و غیردولتی را دگرگون سازد. سرشت بی‌مانند این تهدید و توانمندی مرتکبان جنگ‌های سایبری در آسیب رساندن، کشتار و تخریب فیزیکی از طریق فضای سایبر، تعاریف سنتی توسل به زور را متحول ساخته است.

در این نوشتار، حملات سایبری بازیگران غیردولتی صرفاً به منظور احراز انتساب آن‌ها به یک دولت بررسی می‌شود. پرسش اصلی این است که آیا یک حمله‌ی سایبری، اقدامی مادون آستانه‌ی توسل به زور، در حد توسل به زور و یا توسل به زوری معادل یک حمله‌ی مسلحانه است؟ پژوهش حاضر نتیجه می‌گیرد که حمله‌ی سایبری را می‌توان وفق ماده‌ی ۲ (۴) منشور ملل متحد، توسل به زور مسلحانه توصیف نمود. از سوی دیگر، حمله‌ی سایبری گسترده به زیرساخت‌های اساسی که خسارات مادی یا تلفات انسانی قابل قیاس با حمله‌ی مسلحانه با سلاح‌های متعارف را در پی داشته باشد، حق توسل به دفاع مشروع را به دولت قربانی اعطاء می‌نماید. هم‌چنین، در واکنش به حمله‌ی سایبری که در حد حمله‌ی مسلحانه نباشد، اما حمله‌ی مسلحانه‌ی قریب‌الوقوعی را با تسلیحات متعارف تدارک ببیند، می‌توان به دفاع مشروع متوسل گردید.

واژگان کلیدی: فضای سایبر، توسل به زور، حمله‌ی سایبری، حمله‌ی مسلحانه، دفاع مشروع، تناسب.

---

۱. تاریخ دریافت مقاله ۱۳۹۰/۳/۲۴؛ تاریخ پذیرش نهایی مقاله ۱۳۹۱/۴/۱۲.

۲. دکتری حقوق بین‌الملل، عضو هیأت علمی دانشگاه علوم قضایی و خدمات اداری؛ نویسنده مسؤول:
a.ghasemi1959@yahoo.com

۳. دکتری حقوق بین‌الملل.

درآمد

گسترش فزاینده‌ی فن‌آوری اطلاعات و ارتباطات به تحول و دگرگونی جوامع در ابعاد مختلف سیاسی، امنیتی، اقتصادی و اجتماعی منجر شده است. جوامع، به نحو فزاینده‌ای به رایانه و شـــبکه‌های رایانه‌ای و خدمات حیاتی متکی به اینترنت وابسته شده‌اند. اهمیت جهانی فضای مجازی، آسیب‌پذیری‌هایی را نیز برای آن در پی داشته اســـت؛ این بدین دلیل اســـت که فن‌آوری و تخصص در زمینه‌ی سایبر، ساده و ارزان به دســـت می‌آید؛ این امر به کشـــورهای ضعیف‌تر و حتی کنشگران غیردولتی امکان می‌دهد که به کشـــورهای دارای قدرت نظامی متعارف برتر، آسیب‌های قابل توجهی ماننـــد از کار انداختن ژنراتورهای برق، قطع سیســـتم کنترل و ارتباطات فرماندهی، ســـرنگون کردن هواپیماها، ذوب راکتورهای هســـته‌ای، انفجار خطوط لوله و تخریب تســـلیحات را وارد نمایند. هر کس در هر نقطه از جهـــان، به صرف دارا بودن توان و در اختیار داشـــتن ابزارهای لازم، می‌تواند به فضای مجازی کشور هدف آسیب رساند. لذا، مهاجمان رایانه‌ای قادرند بدون هشـــدار قبلی، به شـــبکه‌های ملی یورش آورده و با آن‌چنان سرعتی گســـترش یابند که بسیاری از مواضع هدف حتی فرصت شنیدن صـــدای آژیر خطر را نیز نیابند و یا در صورت هشـــدار قبلی، برای محافظت از خود، فرصتی نداشته باشند (حسن‌بیگی، ۱۳۸۴: ۱۴).

در نتیجه‌ی بروز چنین تهدیداتی است که امنیت در فضای سایبر به دغدغه‌ی عمومی جامعه‌ی بین‌المللی بدل شده است. در این چارچوب، مجمع عمومی سازمان ملل متحد، مجموعه‌ای از قطعنامه‌ها را در خصوص پیشـــرفت‌های حاصل شـــده در خصوص اطلاعات و ارتباطات از راه دور و تأثیر آن بر امنیت بین‌المللی تصویب نموده و تأکید کرده اســـت: «سوءاستفاده‌ی جنایت‌کارانه از فن‌آوری‌های اطلاعاتی می‌تواند تأثیر شـــدیدی بر تمامی کشورها داشته باشد» (A/RES/56/121 of 19 Decem-ber 2001)؛ «این فن‌آوری‌هـــا می‌توانند به صورت بالقوه برای مقاصد مغایر با هدف حفظ ثبات و امنیت بین‌المللی، استفاده شوند» (A/RES/63/37 of 2 December 2008) و «انتشار اطلاعات و استفاده از فن‌آوری‌ها و روش‌های اطلاعاتی، بر منافع کل جامعه‌ی بین‌المللی تأثیر می‌گذارد» (A/RES/64/25 of 2 December 2009).

یکی از جنبه‌هایی که حقوق‌دانان بین‌المللی می‌توانند موضوع امنیت سایبری

را از آن منظر بررســی نمایند، جنبه‌ی حقوق توســل به زور است؛ یعنی قواعدی که توســل به زور توســط دولت‌ها را در روابط بین‌المللی تنظیم می‌نماید. نوشتار حاضر بر موضوع توســل به زور یک دولت در فضای ســایبر و علیه دولت دیگر تمرکز دارد. حملات سایبری ارتکابی توسط کنشگران غیردولتی، صرفاً به منظور تبیین قابلیت یا عدم قابلیت انتساب به یک دولت بررســی می‌شود. بنابراین، پژوهش حاضر منصرف از «جرایم ســایبری»[1] ارتکابی توسط اشــخاص حقیقی یا حقوقی خصوصی است که به لحاظ منافع شــخصی مانند سرقت پول از حساب‌های بانکی و علیه محرمانه بودن داده‌ها و سیســتم‌های رایانه‌ای صورت می‌گیرند. در ضمن، «تروریسم سایبری»[2] که عبارت است از تخریب یا اخلال گســترده‌ی داده‌ها، اطلاعات یا سامانه‌های رایانه‌ای یا ارتباطی از طریق فضای ســایبر با انگیزه‌های سیاسی، مذهبی، ایدئولوژیک و نژادی (پاکزاد، ۱۳۸۸: ۸۷) با این تحقیق ارتباط نمی‌یابد.

این نوشتار در مقام پاســخ به این پرسش است که یک حمله‌ی سایبری چه ماهیتی دارد؟ آیا اقدامی مادون آســتانه‌ی توسل به زور یا در حد توسل به زور است و یا آن‌که توســل به زور، معادل یک حمله‌ی مســلحانه تلقی می‌شــود و این‌که چه واکنش‌هایی را می‌توان در پاسخ به چنین حمله‌ای نشان داد.

۱. مفاهیم

«حملات ســایبری»[3] در چارچــوب طیف گســترده‌تری از آن‌چه «عملیات اطلاعاتی»[4] نامیده می‌شود، قرار می‌گیرند. عملیات اطلاعاتی که «جنگ اطلاعاتی»[5] نیز زیرمجموعه‌ای از آن اســت و هنگام مخاصمه‌ی مســلحانه به آن توسل می‌شود (Schmitt, 1998: 890-891)، بــه کارگیــری منســجم توانمندی‌هــای جنــگ الکترونیکی، عملیات شــبکه‌ای رایانه‌ای، عملیات روانی، حیله‌های نظامی و عملیات هماهنگ با قابلیت‌های پشــتیبانی اســت که به منظور تأثیرگذاری، متوقف نمودن، تخریب یا سرقت اطلاعات دشمن و در عین حال پشتیبانی از فرایندهای تصمیم‌گیری

1. Cyber Crimes
2. Cyber Terrorism
3. Cyber Attacks
4. Information Operations
5. Information Warfare

نهادهای ملی صورت می‌گیرد (www.dod.gov).

«فضای سایبر»،[1] فضایی غیرمادی و ناملموس است که توسط رایانه‌ها و شبکه‌های رایانه‌ای به وجود آمده و دنیایی مجازی را در کنار دنیای واقعی ایجاد نموده است (فضلی، ۱۳۸۹: ۱۷). این فضا، فراتر از اینترنت توسعه یافته است و تمامی فعالیت‌های دیجیتال شبکه‌ای را در بر می‌گیرد؛ فضای مذکور «دارای گستره‌ای جهانی و بدون مرز، پوشیده و پنهان، ناهنجارمند و کنترل‌ناپذیر است. فضای سایبر ماهیتاً برای آزادی گردش اطلاعات شکل گرفته و محدودیت در این فضا معنا ندارد» (پاکزاد، ۱۳۹۰: ۲۱۶).

از دیدگاه استراتژی نظامی، «عملیات شبکه‌ای رایانه‌ای»[2] مشتمل بر «حملات شبکه‌ای رایانه‌ای»،[3] «دفاع شبکه‌ای رایانه‌ای»[4] و «عملیات بهره‌برداری از شبکه‌های رایانه‌ای مرتبط»[5] می‌باشد. به رغم آن‌که، اغلب در مطبوعات از چنین عملیاتی به عنوان حملات سایبری یاد می‌شود، با عملیات بهره‌برداری از شبکه‌های رایانه‌ای مرتبط، متفاوت نبوده و بر گردآوری و تحلیل اطلاعات تمرکز دارد تا قطع شبکه‌ها؛ لذا، می‌تواند مقدمه‌ای بر یک حمله باشد (Watts, 2010: 400)؛ عملیات بهره‌برداری از شبکه‌های رایانه‌ای مرتبط، هم‌چنین می‌تواند با هدف جاسوسی و سرقت اطلاعات مهم از رایانه‌ها انجام گیرد. با وجود عدم ممنوعیت جاسوسی در حقوق بین‌الملل، این امر به طور معمول در بسیاری از نظام‌های حقوقی جهان جرم‌انگاری شده است (Dinstein, 2001: 101).

نوشتار حاضر فارغ از عملیات بهره‌برداری از شبکه‌های رایانه‌ای مرتبط که برای سرقت اطلاعات و جاسوسی است، صرفاً حملات شبکه‌ای رایانه‌ای و دفاع شبکه‌ای رایانه‌ای، یعنی عملیات شبکه‌ای رایانه‌ای که گسترده‌تر از جاسوسی و سرقت اطلاعات بوده و با قصد خصمانه صورت می‌گیرد، را بررسی می‌نماید. چنین عملیاتی با هدف تغییر یا نابودی اطلاعات موجود در رایانه‌های هدف یا شبکه‌ی رایانه‌ای و به منظور از کار انداختن سیستم کنترل و ارتباطات فرماندهی دشمن و وارد کردن خسارات خارج

1. Cyberspace
2. Computer Network Operations (CNO)
3. Computer Network Attacks (CNA)
4. Computer Network Defense (CND)
5. Related Computer Network Exploitation Enabling Operations (CNE)

از شبکه‌ی رایانه‌ای هدف انجام می‌گیرد.

در این نوشـــتار از عبارات توســـل به زور در فضای سایبر و حملات سایبری استفاده می‌شـــود تا با اصطلاحات حقوق توسل به زور ســـازگار باشد. مراد از واژه‌ی «ســـایبر»[1] هر آن چیزی اســـت که با فن‌آوری اطلاعات، اینترنـــت و فضای مجازی مرتبط باشد. بنابراین، در سیاق پژوهش حاضر، حملات سایبری، استفاده‌ی خصمانه از زور در فضای ســـایبر اســـت که می‌تواند یک حمله‌ی منفرد، نخستین ضربه از یک مخاصمه‌ی مســـلحانه، یا حمله‌ای در چارچوب مخاصمه‌ی مسلحانه‌ای باشد که قبلاً شـــروع شده اســـت. بر این اساس، «حملات جنبشـــی»[2] که با سلاح‌های متعارف در فضای واقعی و علیه تأسیسات رایانه‌ای صورت می‌گیرد، از شمول نوشتار حاضر خارج می‌باشد.

۲. شناسایی و انتساب

پیش از پرداختن به بحث «انتساب»،[3] موضوع شناسایی حمله‌کننده در فضای ســـایبر اولویت دارد. مرتکب حملات ســـایبری می‌تواند با ارائه‌ی آدرســـی اشتباه در سیستم آدرس‌دهی[4] یا اســـتفاده از شبکه‌های دستگاه خودکار، خود را مخفی نماید. در حقیقت، هرچند یکی از مزیت‌های مهم جنگ ســـایبری، ناشـــناخته ماندن است، امکان شناســـایی کشـــور منبع حمله وجود دارد؛ اما این الزاماً بدین معنی نیست که آن کشـــور یا حتی صاحبان رایانه‌های مربوطه، در پس چنین حملاتی قرار داشته‌اند (Brenner, 2006: 424). به عنوان مثال، حملات ســـایبری صورت گرفته در ســـال ۲۰۰۷ میلادی به کشور استونی، از کشورهایی مانند ایالات متحده آمریکا، مصر، پرو و فدراسیون روسیه صورت گرفت؛ اما حمله‌ی سال ۱۹۹۸ به سیستم رایانه‌ای وزارت دفاع ایالات متحده آمریکا، توسط یک نوجوان اسرائیلی و چند دانشجوی کالیفرنیایی و از طریق یک رایانه در امارات متحده عربی صورت پذیرفت (Shackelford, 2009: 231-204).

1. Cyber
2. Kinetic Attacks
3. Attribution
4. Internet Protocol (IP)

به هر حال، شناسایی کشور مسؤول حمله‌ی سایبری، در نهایت امکان‌پذیر است. به عنوان مثال، حمله‌ی سایبری ممکن است در پی یک حمله‌ی متعارف صورت گیرد؛ حمله‌ای که امکان شناسایی مرتکب آن فراهم است (Dinstein, 2001: 112)؛ پیشرفت‌های صورت گرفته در فن‌آوری رایانه و ساز و کارهای اینترنت، می‌تواند شناسایی منبع حمله‌ی سایبری را آسان‌تر نماید. در فرض شناسایی مرتکبان حمله‌ی سایبری، این پرسش مطرح می‌شود که آیا می‌توان حمله را بر اساس قواعد و اصول حقوقی مسؤولیت دولت‌ها به یک دولت منتسب نمود و در نتیجه اعمال قواعد حقوق توسل به زور را آغاز نمود؟ این پرسش از آن جهت است که بر خلاف جنگ متعارف، حملات سایبری علاوه بر کشورها، به سادگی می‌توانند توسط گروه‌ها و حتی افراد ارتکاب یابند.

در مقام پاسخ به این پرسش، پنج فرض را می‌توان در نظر گرفت. نخستین و ساده‌ترین، فرض «نفوذگران سایبری نظامی»[1] است. هرچند جزییات توانمندی سایبری نظامی کشورها، امری طبقه‌بندی شده و محرمانه است، در چندین ارتش ملی، یگان سایبری تشکیل شده است. به عنوان مثال، چین اعلام نموده که گردان‌ها و هنگ‌های فضای سایبر تشکیل داده است (Condron, 2006: 405)؛ ارتش رژیم صهیونیستی نیز دارای کارکنانی است که در گروه جنگ اینترنتی خدمت می‌نمایند (Eshel, 2010: 76)؛ ایالات متحده آمریکا، نیز اخیراً فرماندهی نظامی سایبری را به منظور مقابله با حملات سایبری تشکیل داده است (Beaumont, 2010: 10). برخی کارشناسان معتقدند جمهوری اسلامی ایران یکی از پنج کشور دارای قوی‌ترین ارتش‌های سایبری است (www.bangdad.com).

در این فرض، اقدام نفوذگران سایبری نظامی باید به دولتی که ارگان‌های قانونی آن می‌باشند، نسبت داده شود؛ زیرا به موجب ماده‌ی ۴ (۱) طرح مسؤولیت بین‌المللی دولت، تنظیم شده توسط کمیسیون حقوق بین‌الملل سازمان ملل متحد:[2] «اقدام هر نهاد دولتی اعم از این که عهده‌دار وظایف تقنینی، اجرایی، قضایی یا غیر

1. Uniformed Hackers

۲. طرح مذکور در پنجاه و سومین اجلاس کمیسیون حقوق بین‌الملل در نهم آگوست ۲۰۰۱ میلادی به تصویب رسید و سپس به مجمع عمومی سازمان ملل متحد تقدیم شد. مجمع عمومی نیز این طرح را طی قطعنامه‌ی A/ RES/56/83 of 28 January 2002 تصویب نمود.

آن باشـــد، صرف‌نظر از موقعیت آن در تشـــکیلات دولت و بدون توجه به وصف آن به عنوان نهاد حکومت مرکزی یا نهاد مربوط به واحد محلی دولت، طبق حقوق بین‌الملل اقدام دولت محسوب می‌گردد» (حلمی، ۱۳۸۷: ۵۵)؛ حتی در فرض غیرنظامی بودن نفوذگران سایبری، نتیجه‌ی مذکور تغییر نمی‌یابد.

در فرض دوم، نفوذگران ســـایبری ممکن اســـت عضو تشکیلات حکومتی یا اشخاص شبه‌دولتی باشند؛ مانند شرکت‌های خصوصی شده یا پیمانکاران مستقل که قانوناً حدودی از اقتدار دولت را اعمال می‌نمایند. در تمامی موارد مذکور، بر اســـاس ماده‌ی ۵ طرح مسؤولیت بین‌المللی دولت، رفتار نفوذگران سایبری به دولت منتسب می‌گردد؛ مشروط بر آن که شخص یا واحد مزبور در آن مورد خاص در صلاحیت خود اقدام کرده باشد (حلمی، ۱۳۸۷: ۶۶).

بر اســـاس فرض ســـوم، این امکان وجود دارد که نفوذگران سایبری، عضو یا مستخدم یک دولت نباشند، بلکه اشـــخاص یا شرکت‌هایی باشند که توسط دولت‌ها و بـــه منظور اقدام به حملات ســـایبری اجیر شـــده‌اند (Ophardt, 2010: 12-18). پرســـش این اســـت که در چه صورتی می‌توان اقدام چنین افراد و شرکت‌هایی را به دولت منتســـب نمود؟ ماده‌ی ۸ طرح مسؤولیت بین‌المللی دولت مقرر می‌نماید: «اگر شخص یا گروهی از اشخاص مطابق دستورها، یا به راهنمایی یا به فرمان دولت عمل کرده باشند، وفق حقوق بین‌الملل اقدام آن‌ها، عمل دولت محسوب می‌شود» (حلمی، ۱۳۸۷: ۸۲). در قضیـــه‌ی نیکاراگوئه، دیوان بین‌المللی دادگســـتری اســـتدلال کرد: «مشارکت ایالات متحده آمریکا به صورت آشکار در تأمین مالی، سازماندهی، آموزش و تجهیـــز، گزینش اهداف نظامی یا شـــبه‌نظامی و طراحی کل عملیات ضد انقلابیون نیکاراگوئه، فی‌نفسه برای انتســـاب اعمال ارتکابی آنان به ایالات متحده آمریکا کافی نمی‌باشـــد. چرا که ایالات متحده آمریکا بایـــد در دوره‌ی مذکور بر عملیات نظامی یا شبه‌نظامی ضدانقلابیون نیکاراگوئه، «کنترلی مؤثر»[1] می‌داشت» (Nicaragua case, 1986, Para: 115)؛ هم‌چنین در قضیه‌ی نســـل‌زدایی، دیوان مدعی شـــد که معیار کنتـــرل مؤثر برای انتســـاب اقدامات خلاف حقوق بین‌الملل به یـــک دولت، با تغییر ماهیت اعمال خلاف مذکور و در فقدان یک «قانون خاص»،[2] تغییر نمی‌یابد (Geno-

1. Effective Control
2. Lex Specialis

cide case, 2007, Para: 401)؛ اما دادگاه بین‌المللی کیفری یوگسلاوی سابق اعلام نمود که درجه‌ی کنترل می‌تواند مطابق شرایط واقعی هر قضیه، متفاوت باشد (Prosecutor v.Tadic, 1999, Para: 117). دادگاه مذکور برای انتساب اقدامات گروه‌های مسلح سازمان‌یافته به یک دولت خارجی، معیاری موسع را برگزید. از منظر این دادگاه برای چنین انتسابی معیار «کنترل کلی»[1] کافی است. به موجب این معیار، دولتی که در سازماندهی، هماهنگ نمودن یا طراحی عملیات نظامی گروه نظامی و هم‌چنین تأمین مالی، آموزش و تجهیز یا فراهم نمودن پشتیبانی عملیاتی برای آن گروه نقش دارد، صرف‌نظر از هرگونه دستور خاص دولت کنترل‌کننده در خصوص ارتکاب هر یک از اعمال مذکور، مسؤول تلقی می‌شود (Prosecutor v.Tadic, 1999, Para: 137).

«شاکلفورد»[2] معتقد است که به دلیل ماهیت پنهان فعالیت‌ها در فضای سایبر و مشکلات فنی شناسایی مرتکبان حملات سایبری، معیار «کنترل کلی» را باید برای شناسایی و انتساب حملات سایبری بر معیار کنترل مؤثر ترجیح داد (Shackelford, 2009: 235)؛ این دیدگاه چندان قابل پذیرش نمی‌باشد. در واقع، به دلیل معضلات مربوط به شناسایی مرتکبان حملات سایبری، معیار کنترل مؤثر ارجحیت می‌یابد؛ زیرا این معیار مانع از آن می‌شود که دولتی به سادگی به حملات سایبری متهم گردد؛ به ویژه در فرضی که دولت قربانی، مدعی حق دفاع مشروع باشد.

فرض چهارم هنگامی است که نفوذگران سایبری، ارگان قانونی یا عملی دولت نباشند، اما اقدامات آن‌ها با تحریک عوامل دولت در وب‌سایت‌ها، «اتاق‌های گفت‌وگو»[3] ایمیل‌ها صورت پذیرد. به عنوان مثال در سال ۲۰۰۱ میلادی پس از برخورد یک هواپیمای جاسوسی نیروی دریایی ایالات متحده آمریکا با یک جت جنگنده‌ی چینی در جنوب دریای چین، وب‌سایت‌هایی پیدا شدند که در خصوص چگونگی از کار انداختن رایانه‌های دولتی ایالات متحده آمریکا آموزش می‌دادند (Weisbord, 2009: 20)؛ هرچند در خصوص اقدام به «تحریک»،[4] در طرح مواد

1. Overall Control
2. Shackelford
3. Chat Rooms
4. Incitement

کمیســـیون حقوق بین‌الملل در مورد مسؤولیت دولت، مقرره‌ی صریحی وجود ندارد، بر اســـاس ماده‌ی ۸ طرح مذکور می‌توان نتیجه گرفت که اقدامات تحریک‌آمیز دولت در حد هدایت و کنترل اقدامات شـــخص یا گروهی از اشخاص، مسؤولیت دولت را در پی خواهد داشت (حلمی، ۱۳۸۷: ۸۲).

گاهـــی این امکان وجود دارد که پس از اقـــدام به تحریک، مقامات دولتی به نحو علنـــی از اقدامات صورت گرفته حمایت نماینـــد. در قضیه‌ی کادر دیپلماتیک و کنسولی، دیوان بین‌المللی دادگستری حکم نمود که هرچند حمله‌ی اولیه به سفارت ایالات متحده آمریکا در تهران قابل انتســـاب به دولت ایران نبوده است، اما پشتیبانی بعدی مقامات ایران و تصمیم به دایمی کردن اشـــغال سفارت، این اقدام را به اعمال دولت بدل نموده است (Tehran Diplomatic & Consular Staff Case, 1980, Para: 74).

هم‌چنین، ماده‌ی ۱۱ طرح مسؤولیت دولت مقرر داشته است «چنانچه اقدامی که طبق مواد پیش‌گفته قابل انتساب به یک دولت نیست، از سوی آن دولت به عنوان اقدام خود شناسایی و پذیرفته شود، در همان حدودی که شناسایی و پذیرش صورت گرفته است، وفق حقوق بین‌الملل عمل آن دولت محسوب می‌شود» (حلمی، ۱۳۸۷: ۱۰۲). باید توجه داشـــت که اعتراف علنی به ارتکاب حملات ســـایبری توسط عوامل دولت، امری بعید است؛ همان‌گونه که گفته شد، فن‌آوری‌های سایبری ابزاری مناسب برای مخفی نگه داشـــتن هویت حمله‌کنندگان اســـت. در صورت اعتراف عامل دولت به ارتکاب حمله‌ی سایبری، امکان انتساب این اقدام به دولت بیشتر فراهم می‌شود.

در فـــرض پنجم، حملات ســـایبری از رایانه‌های موجود در کشـــوری خاص و بدون دخالت هیچ دولتی، سرچشـــمه گرفته‌اند. هر چنـــد در چنین موردی، اقدام نفوذگران ســـایبری را نمی‌توان به کشوری نســـبت داد، اما این امکان وجود دارد که کشور محل استقرار رایانه‌های نفوذگران سایبری را مسؤول دانست؛ چنین مسؤولیتی به دلیل عدم اتخاذ اقدامات ضروری و عقلایی جهت جلوگیری یا متوقف کردن حمله مانند غیرممکن کردن دسترســـی اینترنتی مرتکبان، ایجاد می‌شود. در چنین حالتی عمل خلاف دولت، حمله‌ی ســـایبری نیست، بلکه نقض تعهد اجازه ندادن به استفاده از قلمرو دولت برای اعمال خلاف حقوق دیگران اســـت (A/RES/55/63 of 4 De-

cember 2000). فروض چهارم و پنجم از جمله مصادیق تروریسم سایبری محسوب می‌شوند.

۳. حملات سایبری و ممنوعیت تهدید و توسل به زور در حقوق بین‌الملل

حمله‌ی سایبری منتسب به یک دولت، نقض قاعده‌ی عرفی عدم مداخله در اموری است که هر دولت حق دارد بر اساس اصل حاکمیت دولت، در خصوص آن‌ها آزادانه اتخاذ تصمیم نموده و نظام سیاسی، اقتصادی، اجتماعی و فرهنگی خود را انتخاب و سیاست خارجی خود را تنظیم نماید (Nicaragua case, 1986, Para: 205). وضعیت‌های توصیف شده در اعلامیه‌ی سال ۱۹۸۱ میلادی[1] مجمع عمومی سازمان ملل متحد در خصوص عدم مداخله، حمله‌ی سایبری را تحت پوشش قرار می‌دهد (A/RES/36/103 of 9 December 1981)؛ اما احراز این‌که آیا حملات سایبری برابر با توسل به زور در روابط بین‌المللی است، ساده نیست. ماده‌ی ۲ (۴) منشور ملل متحد مقرر می‌نماید: «تمامی اعضاء در روابط بین‌المللی خود از تهدید به زور یا استفاده از آن علیه تمامیت ارضی یا استقلال سیاسی هر کشوری یا از هر روش دیگری که با مقاصد ملل متحد مباینت داشته باشد، خودداری خواهند نمود». دیوان بین‌المللی دادگستری، مقرره‌ی مذکور را بازتاب حقوق بین‌الملل عرفی دانسته و بر ماهیت عرفی آن تأکید می‌نماید (Nicaragua case, 1986, Paras: 187-190). کمیسیون حقوق بین‌الملل نیز، حداقل هسته‌ی اصلی مقرره‌ی مذکور یعنی منع توسل به زور را «قاعده‌ی آمره»[2] می‌داند (Ago, ۱۹۸۰: ۴۴). این مقرره شامل دو ممنوعیت است؛ نخست، منع تهدید و دوم، منع توسل به زور.

با استفاده از ماده‌ی ۲ (۴) منشور ملل متحد، تهدید به زور این‌گونه تعریف شده است: «تهدید صریح یا ضمنی، شفاهی یا عملی به استفاده‌ی غیرقانونی از قوای مسلح در آینده و علیه یک یا چند کشور، که تحقق آن به اراده‌ی تهدیدکننده بستگی دارد» (Roscini, 2007: 235). بنابراین، پاسخ به این پرسش که آیا به موجب ماده‌ی ۲ (۴) منشور ملل متحد، تهدید به حمله‌ی سایبری تهدیدی غیرقانونی

۱. در اعلامیه‌ی مذکور مداخله در امور داخلی و خارجی دیگر کشورها ممنوع شده است.

2. Jus cogens

محســـوب می‌شود، به غیرقانونی دانستن و یا ندانستن حمله‌ی سایبری بستگی دارد. در واقع دیوان بین‌المللی دادگســـتری، قانونی بودن تهدید را با قانونی بودن توســـل به زور در شرایط یکســـان مرتبط دانسته است (Nuclear weapons case, 1996, Para: 47). بنابراین، پرســـش اصلی این است که آیا توسل به زور در فضای سایبر را می‌توان گونه‌ای توسل به زور به معنی ماده‌ی ۲ (۴) منشور ملل متحد تلقی نمود؟

در مقام پاسخ باید گفت رویکردی «غایت‌مدار»[1] به ماده‌ی ۲ (۴) منشور ملل متحد، با حمایت از تفســـیر مضیق مقرره‌ی مذکور، آن را صرفاً به حمله‌ی مســـلحانه محدود می‌داند. در واقع، هدف اساســـی منشور آن‌گونه که در مقدمه‌ی آن ذکر شده، محفوظ داشـــتن نسل‌های آینده از مصایب جنگ بوده و نه منع نمودن تمامی اشکال قهـــر و اجبار. عبارت «کارهـــای مقدماتی»[2] مذکور در این ماده بیانگر آن اســـت که که طراحان منشـــور بر این قصد نبوده‌اند که ممنوعیت توســـل به زور را به فشارهای اقتصادی و سیاسی تسری دهند. اصلاحیه‌ی ارائه شده توسط برزیل که تمامی اشکال تهدید یا توســـل به اقدامات اقتصادی مغایر با اهداف ملل متحد را ممنوع می‌دانست، در کنفرانس سال ۱۹۴۵ سانفرانسیسکو رد شد (Documents, 1945: 720-721). اسناد بعدی ســـازمان ملل متحد مانند اعلامیه‌ی ســـال ۱۹۷۰ میلادی در خصوص روابط دوســـتانه (A/RES/2625 (xxv) of 24 October 1970) و اعلامیه‌ی سال ۱۹۸۷ میـــلادی در مورد عدم توســـل بـــه زور (A/RES/42/22of18November 1987) از این نظریه حمایت می‌نمایند که ماده‌ی ۲ (۴) منشـــور ملل متحد به توسل به زور مسلحانه اشـــاره می‌نماید؛ در حالی‌که اصل عدم مداخله به اشکال دیگر اجبار تسری می‌یابد (Randelzhofer, 2002: 118).

در فرض پذیرش این‌که ماده‌ی ۲ (۴) منشـــور ملل متحد صرفاً توسل به زور مســـلحانه را منع می‌نماید، این پرسش مطرح می‌شود که لفظ مسلحانه به چه معنی است؟ آیا حملات ســـایبری را می‌توان توسل به زور مسلحانه دانست؟ در مقام پاسخ می‌توان گفت لفظ مســـلحانه یا مســـلح به معنی تجهیز به یک ســـلاح یا درگیری با اســـتفاده از یک سلاح است (Garner, 2009: 123). سلاح نیز ابزار مورد استفاده یا طراحی‌شده برای اســـتفاده جهت صدمه زدن به دیگری یا قتل وی است (Garner,

1. Teleological
2. Travaux Preparatoires

2009: 1730)؛ تقریباً تمامی اشیاء می‌توانند به عنوان سلاح به کار روند؛ در صورتی که قصد دارنده‌ی آن خصمانه باشد. دیوان بین‌المللی دادگستری در نظریه‌ی مشورتی خود در خصوص مشروعیت توسل به سلاح‌های هسته‌ای تصریح نمود که مواد ۲ (۴)، ۴۲ و ۵۱ منشـــور ملل متحد، به تسلیحات خاصی اشاره ندارد. این مواد، صرف‌نظر از تســـلیحات مورد استفاده، تمامی مصادیق توســـل به زور را در برمی‌گیرد (Nuclear Weapons case, 1996, Para: 39)؛ بنابراین، ضرورتی نیســـت تســـلیحات مذکور دارای آثار انفجاری بوده و یا برای اهداف تهاجمی ســـاخته شـــده باشـــند. بی‌تردید، اســـتفاده از برخی «سلاح‌های غیرجنبشی با کاربرد دوگانه»،[1] از قبیل مواد بیولوژیک یا شـــیمیایی علیه یک کشور، باید از سوی کشـــور قربانی به عنوان توسل به زور در معنی ماده‌ی ۲ (۴) منشور ملل متحد تلقی گردد. دیوان بین‌المللی دادگستری به نحو ضمنی پذیرفته است که استفاده از تسلیحات غیرجنبشی می‌تواند موجب نقض ماده‌ی ۲ (۴) منشـــور ملل متحد گردد؛ زیرا دیوان در قضیه‌ی نیکاراگوئه، تســـلیح و آموزش کنتراها توسط ایالات متحده آمریکا را به عنوان تهدید یا توسل به زور علیه نیکاراگوئه توصیف نمود (Nicaragua case, 1986, Para: 228)؛ «براونلی» از جنگ شیمیایی و بیولوژیـــک نام می‌برد؛ زیرا از عناصر بیولوژیک (میکروبی) و شـــیمیایی می‌توان در جهت نابود کردن حیات و اموال بهره برد (Brownlie, 1963: 362). هر دو استدلال مذکور به خوبی با حملات ســـایبری انطباق می‌یابند. این حقیقت که چندین کشور، فن‌آوری ســـایبری را در دکتریـــن نظامی خود لحاظ نمـــوده و از آن با عنوان جنگ ســـایبری نام می‌برند و یگان‌های نظامی با تخصص ســـایبری ایجاد نموده‌اند، از این دیدگاه حمایت می‌کند که «اســـب‌های تروا»،[2] «کرم‌ها»،[3] «ویروس‌ها» و مانند آن‌ها، سیســـتم‌های تسلیحاتی دیگری می‌باشند که اگرچه ارزان‌تر و سریع‌تر از یک موشک هستند، اما تخریب بیشتری به بار می‌آورند (Lewis, 2010: 310). واقعیت آن است که آثار غیرمستقیم حملات سایبری اغلب مهم‌تر از آثار مستقیم آن است. این امر در خصوص بســـیاری از حملات با تسلیحات متعارف نیز صدق می‌نماید. به عنوان مثال، اقدام به بمباران بازار سهام یا دیگر مؤسسات مالی، توسل به زور مسلحانه و نه اعمال

1. Dual use non kinetic weapons
2. Trojan Horses
3. Worms

فشار اقتصادی تلقی می‌شود؛ هرچند پیامدهای اقتصادی این اقدام بسیار سنگین‌تر از خسارات وارده به ساختمان بازار بورس و مؤسسات مالی باشد.

به استناد ذیل بند «ب» از شق (۳) ماده‌ی ۳۱ مقاوله‌نامه‌ی وین در خصوص حقـــوق معاهدات، می‌توان پذیرفت که مقرره‌ی مذکور در مقام تبیین قواعد تفســـیر معاهدات، به هر رویه‌ی مؤخر بر اجرای معاهده تصریح می‌نماید «که دلالت بر توافق طرف‌های معاهده در رابطه با تفســـیر معاهده داشته باشد» (ضیایی بیگدلی، ۱۳۸۳: ۳۲۹)؛ تاکنون برخی کشورها مانند ایالات متحده آمریکا، روسیه و استونی به صراحت دیـــدگاه خود را مبنی بر تلقی حمله‌ی ســـایبری به عنوان گونه‌ای از توســـل به زور مســـلحانه ابراز نموده‌اند. سند استراتژی نظامی ملی سال ۲۰۰۴ میلادی وزارت دفاع ایالات متحده آمریکا به ســـلاح‌هایی با آثار گســـترده اشـــاره می‌نماید که بیشتر آثار مختل‌کننده دارند تا نابودکننده؛ این ســـند چارچوب حملات سایبری صورت گرفته نسبت به سیستم‌های اطلاعاتی بازرگانی یا علیه شبکه‌های حمل و نقل را از مصادیقی دانســـته است که ممکن است به مراتب پیامدهای اقتصادی و روانی بیشتری از پرتاب یک سلاح‌کشـــنده داشته باشـــند (www.defense.gov). فدراسیون روسیه، نیز بر این باور اســـت که «تســـلیحات اطلاعاتی می‌توانند آثار مخرب قابل مقایسه‌ای با آثار تسلیحات نابودی جمعی داشته باشند» (Johnson, 2001: 443)؛ وزیر دفاع استونی، «محاصره‌ی سایبری»[1] را معادل محاصره‌ی دریایی بنادر می‌داند که از دسترسی یک کشور به جهان ممانعت می‌کند (www.nato-pa.int).

۴. واکنش علیه حملات سایبری

با این فرض که کشـــور قربانی بتواند مبدأ حمله‌ی سایبری را شناسایی کند و آن را به کشـــوری انتســـاب نماید، چندین گزینه را بدین شرح در دسترس خواهد داشت:

1. Cyber Blockade

۴-۱. توسل به شورای امنیت سازمان ملل متحد

کشـــور قربانی بر اساس ماده‌ی ۳۵ (۱) منشـــور ملل متحد می‌تواند وضعیت را به شـــورای امنیت ارجاع نماید؛ ممکن است شورای مذکور روش‌های مناسب را بر اســـاس ماده‌ی ۳۶ (۱) منشـــور جهت حل و فصل اختلاف توصیه نماید؛ در صورتی که شـــورا وضعیت را تهدیدی علیه صلح، نقض صلـــح یا اقدام تجاوزکارانه تلقی کند، می‌تواند اختیارات خود را بر مبنای فصل هفتم منشور اعمال کند.

هر چند در نظر طراحان منشـــور ملل متحد تهدید علیه صلح به اســـتفاده از قوای مسلح متعارف محدود بود (Osterdahl, 1998: 85)، اما دامنه‌ی آن به تدریج توســـعه یافت؛ به نحوی‌که، شـــورا می‌تواند با ارزیابی شرایط خاص هر قضیه، هرگونه اقدامی را، تهدیدی علیه صلح تلقی نماید.

چنانچه شـــورای امنیت سازمان ملل متحد، یک حمله‌ی سایبری را تهدیدی علیـــه صلح تلقی کند، می‌تواند به موجب ماده‌ی ۳۹ منشـــور ملل متحد توصیه‌هایی را ارائـــه نموده و برای جلوگیری از وخیم‌تر شـــدن بحران و به موجب ماده‌ی ۴۰ این منشـــور اقداماتی را پیشنهاد نماید و سرانجام به اســـتناد مواد ۴۱ و ۴۲ منشور ملل متحد در خصوص اقدامات مبتنی بر عدم توسل به زور و یا توسل به زور اتخاذ تصمیم کند. شـــورای امنیت ســـازمان ملل متحد هم‌چنین می‌تواند محاصره‌ی سایبری را بر کشور مسؤول حمله‌ی سایبری و به منظور ممانعت از استمرار یا تکرار حمله، تحمیل نماید.

۴-۲. رجوع به دادگاه بین‌المللی

کشـــور مســـؤول حمله‌ی ســـایبری را می‌توان جهت جبران غرامت ناشی از نقض ماده‌ی ۲ (۴) منشـــور ملل متحد و اصل عدم مداخله، به یک دادگاه بین‌المللی از جمله دیوان بین‌المللی دادگســـتری، احضار نمود. با این وجود باید توجه داشـــت که تعیین میزان خســـارات ناشـــی از یک حمله‌ی ســـایبری، امری دشوار است؛ زیرا، مؤسســـات مالی ممکن است در تهیه‌ی اطلاعات دقیق و تعیین میزان خسارات مردد باشند (www.carlisle.army)؛ هم‌چنین، دیوان بین‌المللی دادگستری مانند سایر دادگاه‌های بین‌المللی، فاقد صلاحیت اجباری است؛ بنابراین، هر دو طرف اختلاف باید

در خصوص ارجاع قضیه به دیوان، توافق نمایند.

وفـــق ماده‌ی ۹۶ منشـــور ملل متحد، گزینـــه‌ی دیگر می‌تواند درخواســـت نظریه‌ی مشـــورتی از دیوان بین‌المللی دادگســـتری در خصوص مشـــروعیت یا عدم مشروعیت حملات سایبری باشد. چنین نظریاتی اختیاری و غیرالزام‌آورند؛ هرچند در شکل‌گیری یک قاعده‌ی عرفی بین‌المللی مؤثر می‌باشند (Conforti, 2005: 276)؛ برخی مفســـران بر این عقیده‌اند که حملات سایبری که تجاوز محسوب شوند، افزون بر مسؤولیت دولت، مســـؤولیت کیفری بین‌المللی افراد مرتکب را نیز در پی خواهند داشت (Weisbord, 2009: 39).

۳-۴. مقابله به مثل و اقدام متقابل

کشور قربانی یک حمله‌ی سایبری می‌تواند به مقابله به مثل و اقدامات متقابل غیرنظامی علیه حمله‌کننده متوسل شـــود. بر اساس ماده‌ی ۴۹ (۱) طرح مسؤولیت بین‌المللـــی دولت، دولت صدمه‌دیده می‌تواند علیه دولت مســـؤول تخلف بین‌المللی، برای وادار ســـاختن دولت مذکور به ایفـــای تعهدات خود، به اقدامات متقابل مبادرت ورزد (حلمـــی، ۱۳۸۷: ۳۹۳). حملات ســـایبری و تبلیغات ســـایبری با هدف ایجاد شورش و منازعه‌ی داخلی در کشور هدف، امری غیرقانونی بوده و با اصول ممنوعیت توســـل به زور و ممنوعیت مداخله در امور داخلی سایر کشورها مغایر است؛ این‌گونه مداخلات کشور صدمه‌دیده را قادر می‌ســـازد اقدامات متقابل متناسب و سازگاری با حدود و شرایط مذکور در مواد ۵۰ تا ۵۲ طرح مسؤولیت بین‌المللی دولت اتخاذ نماید.

پرسشـــی که در این راستا مطرح می‌شود، این است که آیا کشور قربانی یک حمله‌ی ســـایبری می‌تواند به اقدام متقابل مبتنی بر توســـل به زور علیه حمله‌کننده مبادرت ورزد؟ از آن‌جا که در حقوق بین‌الملل معاصر چنین اقدام متقابلی بر اســـاس مـــاده‌ی ۵۰ (۱) طرح مســـؤولیت بین‌المللی دولت، امری غیرقانونی اســـت (حلمی، ۱۳۸۷: ۳۹۹)، پاســـخ مثبت به این پرسش در صورتی است که در ماده‌ی ۵۱ منشور یا حقوق بین‌الملل عرفی، توســـل به دفاع مشـــروع در مقابل حمله‌ی سایبری امری مجاز باشـــد. باید توجه داشت که چنانچه توسل به زور در فضای سایبر تحت شمول ماده‌ی ۲ (۴) منشـــور ملل متحد قرار گیرد و اقدام به آن بر اســـاس مقرره‌ی مذکور

و در نتیجه‌ی ماده‌ی ۵۰ (۱) طرح مسؤولیت بین‌المللی دولت ممنوع باشد، کشور قربانی حمله‌ی سایبری نمی‌تواند واکنش نشان دهد؛ مگر آن‌که حمله‌ی سایبری شدید بوده و آثار گسترده‌ای داشته باشد؛ در این صورت به استناد ماده‌ی ۵۱ منشور ملل متحد، کشور مذکور محق به واکنش می‌باشد. وضعیتی که مدنظر کمیسیون حقوق بین‌الملل از تصویب ماده‌ی ۵۰ طرح مسؤولیت بین‌المللی دولت بوده، ناظر بر کشوری است که در برابر نقض پیشین مثلاً یک معاهده‌ی بازرگانی توسط کشور دیگر، به زور مسلحانه متوسل گردد، بر اساس ماده‌ی ۵۰ (۱) طرح مذکور، چنین اقدام متقابلی که تناسبی با اقدام اولیه ندارد، منع شده است. در واقع این ادعا که کشور قربانی حمله‌ی سایبری نمی‌تواند با ارسال کدهای انحرافی اقدام به تلافی کند؛ مگر آن‌که حمله‌ی سایبری به آستانه‌ی یک حمله‌ی مسلحانه رسیده باشد، ادعایی غیرمنطقی است؛ موضوع دیگر آن‌که، پیامدهای قابل انتظار حمله‌ی سایبری متقابل، باید با پیامدهای حمله‌ی اولیه متناسب شد. چنین محاسبه‌ای دشوار است؛ زیرا مانند تسلیحات بیولوژیک، ویروس ارسال شده در فضای سایبر، ممکن است به نحو غیرقابل کنترلی منتشر گردد (Delibasis, 2007: 364).

۱-۳-۴. توسل به زور مسلحانه به استناد دفاع مشروع

پرسش این است که حمله‌ی سایبری از کدام ویژگی‌ها، گستردگی و پیامدها باید برخوردار باشد تا بتوان علیه آن به زور مسلحانه متوسل شد؟ پاسخ این پرسش در ادامه خواهد آمد.

۲-۳-۴. شرایط تلقی حمله‌ی سایبری معادل حمله‌ی مسلحانه

ماده‌ی ۵۱ منشور ملل متحد مقرر می‌کند: «در صورت وقوع حمله‌ی مسلحانه علیه یک عضو ملل متحد تا زمانی که شورای امنیت اقدامات لازم برای حفظ صلح و امنیت بین‌المللی را به عمل آورد، هیچ یک از مقررات این منشور به حق ذاتی دفاع از خود اعم از فردی یا دسته‌جمعی لطمه‌ای نخواهد رسانید». کشور قربانی توسل به زور سایبری در صورت تلقی چنین حمله‌ای به عنوان یک حمله‌ی مسلحانه، می‌تواند به دفاع مشروع متوسل شود.

در قضیـــه‌ی نیکاراگوئه، دیوان بین‌المللی دادگســـتری به این موضوع اذعان نمود که در منشـــور ملل متحد و حقوق قراردادی تعریفی از حمله‌ی مسلحانه وجود ندارد (Nicaragua case, 1986, Para: 176)؛ ضمن آن‌که ماده‌ی ۵۱ منشور ملل متحد بدون اشـــاره به سلاح خاصی بر هرگونه توســـل به زور صرف‌نظر از سلاح‌های اســـتفاده شده حاکم اســـت (Nuclear weapons case, 1996, Para: 39)؛ امری که از ســـیاق ماده‌ی ۲ (۴) منشـــور ملل متحد بر می‌آید. این حقیقت که در حمله‌ی ســـایبری، تســـلیحات متعارف به کار گرفته نمی‌شـــوند، لزوماً بدین معنی نیست که مســـلحانه بودن آن را منتفی نماید. هم‌چنان‌که آمده است «اسم و کاربرد عادی یک وســـیله نیست که آن را به یک ســـلاح مبدل می‌کند، بلکه قصد از استفاده و آثار آن است که چنین وسیله‌ای را به سلاح تبدیل می‌نماید. بنابراین، استفاده از هر وسیله یا تعدادی از وســـایل که تلفات قابل ملاحظه‌ی انسانی یا تخریب گسترده‌ی اموال را در پی داشـــته باشد، حمله‌ی مسلحانه محسوب می‌شود» (Zemanek, 2010: 21)، به نظر می‌رســـد این نتیجه‌گیری، از حمایت شورای امنیت سازمان ملل متحد برخوردار است. شورای مذکور در واکنش به حملات یازدهم سپتامبر ۲۰۰۱ میلادی حق دفاع مشروع را برای ایالات متحده آمریکا در حالی به رسمیت شناخت که تسلیحات مورد استفاده، هواپیماهای ربوده شده بودند (S/RES/1368 of 12 September 2001).

پرســـش این اســـت که آیا هر گونه توســـل به زور در فضای سایبر، حمله‌ی مسلحانه محسوب می‌شود؟ دیوان بین‌المللی دادگستری شدیدترین اشکال توسل به زور یعنی حملات مســـلحانه را از اشکال توســـل به زور با شدت کم‌تر، تفکیک نموده است (Nicaragua case, 1986, Para: 195). معیار این تفکیک «مقیاس و نتایج»[1] حملات بوده اســـت. یکی از نویســـندگان مثال‌هایی از حملات ســـایبری که معادل حملات مســـلحانه می‌باشند را بدین شرح برمی‌شمرد: «مرگ و میر ناشی از از دست دادن کنترل بر سیستم‌های رایانه‌ای پشتیبان حیات، قطع گسترده‌ی جریان برق که آثار زیان‌بار قابل ملاحظه‌ای داشـــته باشد، از کار انداختن رایانه‌های کنترل تأسیسات آب‌رسانی و ســـدها که نتیجه‌ی آن بروز سیل در مناطق مسکونی باشد، تصادف‌های عمدی مرگ‌بار طراحی شده مانند دادن اطلاعات غلط به رایانه‌های هواپیما و گداخت

1. Scale and Effects

هســـته‌ای یک رآکتور در نیروگاه هســـته‌ای که موجب انتشار مواد رادیو اکتیو شده و تلفات بی‌شماری را در مناطق اطراف دارای جمعیت متراکم به بار آورد. از سوی دیگر، قطع ارتباطات بر اثر یک حمله‌ی شبکه‌ای موقت که تلفات مهم انسانی یا مادی به بار نیاورد را نمی‌توان یک حمله‌ی مسلحانه دانست، هرچند می‌تواند مصداق توسل به زور باشـــد» (Dinstein, 2001: 105). این نویسنده دیدگاه کسانی که سرقت اطلاعات حســـاس نظامی را هر چند به تلفات انســـانی یا نتایج تخریبی منجر نشود را حمله‌ی مسلحانه دانسته‌اند (Joyner & Lotrionte, 2001: 855) نپذیرفته است.

این امر مشخص نیست که برای تلقی یک حمله‌ی سایبری به عنوان حمله‌ای مســـلحانه، چنین حمله‌ای باید علیه کدام رایانه‌ها و شبکه‌های رایانه‌ای، هدایت شده و صـــورت گیرد. در یک حمله‌ی متعارف مســـلحانه در این‌که هدف حمله، نظامی یا غیرنظامی باشد، تفاوتی نیست؛ در هر دو فرض، حمله می‌تواند جنبه‌ی مسلحانه داشته باشد. کشوری که هدف حمله در آن استقرار داشته، حق دفاع مشروع خواهد داشت؛ زیرا تمامیت ارضی آن نقض شده است. به همین دلیل دینشتاین به درستی استدلال می‌نماید: «یک حمله‌ی مسلحانه‌ی متعارف علیه یک هدف غیرنظامی در قلمرو کشور هدف، می‌تواند یک حمله‌ی مســـلحانه باشد؛ هرچند هیچ یک از نظامیان کشته نشده باشـــند یا صدمه‌ای به اموال نظامی وارد نشده باشد؛ بر این اساس، دلیلی ندارد که در خصوص حملات سایبری علیه سیســـتم‌های غیرنظامی، نتیجه‌گیری متفاوتی داشته باشیم؛ حتی اگر حمله، شبکه‌ی رایانه‌ای یک بیمارستان غیرنظامی را هدف قرار داده باشـــد و با تأسیسات نظامی ارتباطی نداشته باشـــد، تأثیر مخرب این اقدام، آن را به یک حمله‌ی مسلحانه بدل می‌نماید. این حقیقت که شبکه‌ی رایانه‌ای توسط شرکتی اداره می‌شود که تابعیت کشور ثالثی را دارد یا سیستم رایانه‌ای مورد استفاده‌ی کشور قربانی، در خارج از مرزهای آن مثلاً در یک پایگاه نظامی خارج از کشور قرار دارد، در حقیقت امر تغییری ایجاد نمی‌کند» (Dinstein, 2001: 106-107). در شرایطی که وارد کردن خســـارت به کشوری خاص یا شهروندانش، هدف نبوده و حمله‌ی سایبری به نحو تصادفی رخ داده یا هدف واقعی آن کشـــور دیگری بوده است، توسل کشوری که هدف حمله‌ی سایبری واقع شده به دفاع مشروع، محل تردید است. طبق یافته‌ی دیوان بین‌المللی دادگستری در قضیه‌ی سکوهای نفتی، یک حمله‌ی مسلحانه باید با

قصد خاص آســـیب رساندن انجام شده باشد (Oil Platforms case, 2003, Para: 64). مشخص نیست که در این قضیه دیوان بر یک خصیصه‌ی عام حمله‌ی مسلحانه تأکید نموده اســـت و یا آن‌که خصیصه‌ی مذکور را به این پرونده محدود دانسته است (Gray, 2008: 146).

پرسش مهم این اســـت که آیا یک حمله‌ی سایبری به شبکه‌ی رایانه‌ای یک زیرســـاخت غیرنظامـــی می‌تواند در صورت دارا بودن معیـــار مقیاس و تحقق نتیجه، به نحو بالقوه یک حمله‌ی مســـلحانه تلقی شـــود؟ در صورتی که به زیر ســـاخت‌های مهم حمله شـــود و چنین حمله‌ای با تلفات و خسارات گســـترده همراه باشد، پاسخ مثبت اســـت؛ اما در خصوص این‌که زیرساخت‌های مهم کدام‌اند، توافقی وجود ندارد. مجمع عمومی سازمان ملل متحد اعلام نموده است که هر کشور باید زیر ساخت‌های مهم اطلاعاتی را خود تعیین نماید (A/RES/58/199 of 23 December 2003)؛ سند «استراتژی ملی تأمین امنیت فضای سایبر»[1] سال ۲۰۰۳ ایالات متحده آمریکا، زیرســـاخت‌های مهم را مشـــتمل بر «دارایی‌های مادی و ســـایبری نهادهای عمومی و خصوصی در بخش کشـــاورزی، غذا، آب، بهداشـــت عمومی، خدمـــات اضطراری، حکومت، صنایع دفاعی، اطلاعـــات و مخابرات، انرژی، حمل و نقل، بانکداری و مالی، مواد شـــیمیایی و خطرناک و پست و کشـــتیرانی»، می‌داند (www.us-cert.gov). «کمیســـیون اتحادیه‌ی اروپا»،[2] نیز زیرساخت‌های مهم را «تأسیسات منابع فیزیکی، خدمات و فن‌آوری اطلاعات، شبکه‌ها و ســـرمایه‌های زیربنایی می‌داند که اختلال یا نابودی آن‌ها بر ســـلامتی، ایمنی، امنیت یا حیات اقتصادی شهروندان یا کارکرد مؤثر حکومت تأثیری جدی و شدید خواهند داشت» (http://eur-lex.europa).

موضوع شناســـایی زیرســـاخت‌های مهم ملی با توجه به ایـــن واقعیت که در بیشتر کشورها چنین زیرساخت‌هایی در مالکیت بخش خصوصی می‌باشند، پیچیده‌تر می‌گردد. در پایان باید گفت نظریه‌ی زیرســـاخت‌های مهـــم، با نظریه‌ی امنیت ملی مرتبط اســـت که به همان میـــزان، تعریف آن در حقوق داخلـــی و همچنین حقوق بین‌الملل دشـــوار اســـت. در نتیجه، کشـــورها در تعیین تهدیدات علیه امنیت ملی و زیرساخت‌های مهم خود، اختیارات گسترده‌ای دارند.

1. National Strategy to Secure Cyberspace
2. Commission of the European Union

۳-۳-۴. الزامات حقوقی دفاع مشروع علیه حمله‌ی سایبری

به هنگام توسل به دفاع مشروع علیه یک حمله‌ی سایبری که در حد حمله‌ی مسلحانه باشد، باید الزامات «ضرورت»،[1] «تناسب»[2] و «فوریت»[3] رعایت شود (Dinstein, 2005: 208-211). ضرورت بدین معنی است که توسل به زور آخرین گزینه و راه‌کار است؛ لذا باید سایر راه‌کارها ناکارآمد بوده یا احتمالاً ناکارا و بی‌فایده باشند. به عنوان یک الزام و شرط حداقلی، ضرورت بر این دلالت دارد که کشوری که درصدد دفاع مشروع است، باید دریابد که حمله‌ی سایبری یک تصادف نبوده و موضوع را نمی‌توان با توسل به روش‌های کم‌تر قهرآمیز حل و فصل نمود؛ روش‌هایی چون جلوگیری از دسترسی نفوذگران سایبری به شبکه‌ها و وب‌سایت‌های هدف حمله از طریق توسل به دفاع سایبری.

در خصوص الزام تناسب باید گفت که در عمل، واکنش یکسانی به حمله‌ی سایبری امکان‌پذیر نمی‌باشد. چرا که گاهی کشور قربانی فاقد فن‌آوری توسل به حمله‌ی سایبری بوده و یا متجاوز فاقد یک شبکه‌ی به حد کافی توسعه‌یافته برای حمله به آن است (Greenberg, 1998: 32). پرسش این است که آیا می‌توان مجموعه‌ای از حملات سایبری با مقیاس کوچک را به عنوان یک حمله‌ی مسلحانه تلقی نمود؟ پاسخ به این پرسش را نمی‌توان به قطع و یقین داد؛ چرا که در واقع، دکترین «انباشت رویدادها»[4] که اغلب توسط اسراییل و ایالات متحده آمریکا و به منظور واکنش علیه حملات تروریستی بدان استناد می‌شود، محل مناقشه و اختلاف است. به موجب این دکترین، چندین حمله‌ی مرزی کوچک و با شدت اندک را می‌توان در مجموع یک حمله‌ی مسلحانه تلقی نمود و در مقابل آن به دفاع مشروع متوسل شد (Zemanek, 2010: 7). در قضیه‌ی سکوهای نفتی، دیوان بین‌المللی دادگستری دکترین مذکور را به صراحت رد نکرد، اما آن را در پرونده‌ی مطروحه قابل اعمال ندانست (Oil Platforms case, 2003, Para: 64).

سرانجام این‌که، الزام فوریت بیانگر آن است که هدف غایی دفاع مشروع،

1. Necessity
2. Proportionality
3. Immediacy
4. Accumulation of Events

تنبیه مهاجم نمی‌باشد، بلکه هدف، دفع حمله‌ی مسلحانه است. چنین الزامی به‌ویژه در خصوص حملات سایبری باید به نحو انعطاف‌پذیری به کار رود؛ چرا که برای مثال، در فرض استفاده‌ی متجاوز از «بمب‌های هوشمند یا زمانی»[1] خسارات واقعی مدت‌ها پس از حمله‌ی سایبری ایجاد خواهد شد؛ امری که واکنش در قالب دفاع مشروع را با تأخیر مواجه می‌سازد.

۴-۳-۴. دفاع مشروع بازدارنده علیه حمله‌ی سایبری

باید توجه داشت حتی هنگامی که توسل به زور در فضای سایبر، به آستانه‌ی حمله‌ی مسلحانه نرسیده باشد، کشور قربانی هم‌چنان می‌تواند در وضعیتی به «دفاع مشروع بازدارنده»[2] علیه حمله‌ی سایبری مذکور متوسل شود؛ حمله‌ای که هدف آن تدارک یک حمله‌ی مسلحانه‌ی متعارف فوری است (Robertson, 2001:139).

در قضیه‌ی نیکاراگوئه، دیوان بین‌المللی دادگستری در خصوص موضوع دفاع مشروع بازدارنده، اتخاذ موضع نکرد؛ «زیرا موضوع قانونی بودن واکنش نسبت به یک تهدید فوری به حمله‌ی مسلحانه، توسط طرفین اختلاف مطرح نشده بود» (Nicaragua case, 1986, Para: 194)؛ هم‌چنین در پرونده‌ی مربوط به فعالیت‌های مسلحانه در سرزمین کنگو، دیوان در این خصوص اظهارنظر نکرد؛ زیرا اوگاندا در نهایت مدعی شد که اقداماتش در پاسخ به حملات مسلحانه‌ای بوده که پیشتر وقوع یافته بودند. در ادامه دیوان چنین حکم نمود که: «ماده‌ی ۵۱ منشور ملل متحد، فقط دفاع مشروع را در چارچوب دقیقی که مقرر نموده موجه دانسته و اجازه نمی‌دهد کشوری به منظور دفاع از منافع امنیتی فرضی خود، فراتر از این معیارها به زور متوسل شود» (Armed Activities case, 2005, Paras: 143,148).

پرسش این است که حمله‌ی مسلحانه قریب‌الوقوع، از حیث ماهیت چگونه حمله‌ای است که واکنش بازدارنده از نوع «پیش‌دستانه»[3] را ایجاب می‌نماید؟ به اعتقاد برخی حق دفاع مشروع پیش‌دستانه در برابر یک حمله‌ی مسلحانه‌ی قریب‌الوقوع، با حقوق بین‌الملل عرفی (High Level Panel, ۲۰۰۴: ۶۳) و هم‌چنین ماده‌ی

1. Logic or time bombs
2. Anticipatory self-defense
3. Preemptive

۵۱ منشـــور ملل متحد مطابقت دارد (Secretary-General, 2005; 33)؛ هرچند به موجب تفســـیر تحت‌اللفظی از مقرره‌ی مذکور، دفاع مشروع پس از وقوع حمله‌ی مســـلحانه مجاز می‌باشد، اما بر اســـاس ماده‌ی ۳۲ مقاوله‌نامه‌ی وین در مورد حقوق معاهدات، اعمال معیارهای مقرر در ماده‌ی ۳۱ مقاوله‌نامه‌ی مذکور، نباید به تفسیری منجر شـــود که به وضوح باطل و غیرمنطقی باشـــد. این انتظار که ابتدا باید کشورها هدف یک حمله‌ی مســـلحانه‌ی ســـنگین قرار گیرند تا بتوانند واکنش نشـــان دهند، انتظاری مبتنی بر واقعیت نمی‌باشد. منطق دفاع مشروع، دفع حمله‌ی مسلحانه است. در فرضی که خطر فوری و قطعی باشـــد و گزینه‌ای دیگر در دسترس نباشد و زمانی برای مذاکره باقی نمانده باشـــد (محمدعلی‌پور، ۱۳۷۹: ۲۴)، واکنش در همان لحظه، امری ضروری است؛ زیرا امکان توســـل به راهکاری دیگر، فراهم نمی‌باشد؛ لذا کشور قربانی باید بتواند به دفاع مشروع متوسل شود.

«اشمیت» معتقد است برای احراز حق دفاع مشروع پیش‌دستانه علیه حمله‌ی ســـایبری که فی‌نفسه معادل یک حمله‌ی مسلحانه نباشـــد، سه عامل را باید در نظر گرفت: نخســـت آن‌که حمله‌ی ســـایبری، جزیی از یک عملیات کلی است که به حد حمله‌ی مسلحانه می‌رسد؛ دیگر آن‌که حمله‌ی سایبری، مرحله‌ای ضروری از حمله‌ای قریب‌الوقوع و اجتناب‌ناپذیر اســـت؛ و ســـوم آن‌که طرف مدافـــع، در آخرین فرصت باقی‌مانـــده جهت مقابله‌ی مؤثر با حمله، واکنش نشـــان می‌دهد (Schmitt, 1998: 932-933)؛ این واکنش دفاعی نه با خود حمله‌ی ســـایبری، بلکه با کل حمله‌ای که حمله‌ی ســـایبری مرحله‌ی ابتدایی آن است، باید متناسب باشد (Schmitt, 1998: 933).

۴-۴. دفاع مشـــروع علیه حمله‌ی سایبری از منظر حقوق بین‌الملل عرفی

همان‌گونه که آورده شد، به موجب ماده‌ی ۵۱ منشور ملل متحد، می‌توان به دفاع مشروع علیه حمله‌ی سایبری متوسل شد. پرسش این است که آیا قاعده‌ی عرفی در این خصوص وجـــود دارد؟ در قضیه‌ی نیکاراگوئه، دیوان بین‌المللی دادگســـتری دریافت که هویت کاملاً مجزایی میان قواعد عرفی بین‌المللی توسل به زور و مقررات

ناظر بر آن در منشـــور ملل متحد وجود نـــدارد و حقوق بین‌الملل عرفی صرف‌نظر از حقوق بین‌الملل معاهدات به وجود و کارکرد خود ادامه می‌دهد؛ حتی اگر هر دو نظام حقوقی محتوای یکســـانی داشته باشـــند (Nicaragua case, 1986, Para: 179). حـــدود یک دهه‌ی پیش، «داماتو» پیش‌بینی نمود که حمله‌ی شـــبکه‌ای رایانه‌ای به زودی به موجب حقوق بین‌الملل عرفی کاملاً ممنوع خواهد شد (D'Amato, 2001: 69)؛ در این میان برخی مفســـران بر این باور بودنـــد که تاکنون هیچ قاعده‌ی عرفی بین‌المللی در این خصوص شـــکل نگرفته اســـت؛ زیرا این پدیده هنوز جدید است و رویه و عملکردی از کشـــورها در خصوص آن وجود ندارد (Schmitt, 1998: 921)؛ اما این اســـتدلال پذیرفتنی نمی‌باشـــد؛ هرچند حملات ســـایبری همزاد شبکه‌های رایانه‌ای می‌باشـــند و به همان اندازه قدمت دارند و چندان پدیده‌ی جدیدی نیستند، اما صرف ســـپری شدن دوره‌ی زمانی کوتاهی مانع از شکل‌گیری یک قاعده‌ی جدید حقوق بین‌الملل عرفی نمی‌باشد (Continental shelf case, 1969, Para: 74). در نتیجه، برخی قواعد عرفی به ســـرعت ظاهر می‌شوند. به عنوان مثال، موضوعاتی چون حاکمیت بر فضای ماوراء جو و رژیم فلات قاره، به دلیل رویه‌ی گســـترده‌ی کشورها در واکنش به یک وضعیت جدید، به ســـرعت شکل گرفتند (انجمن حقوق بین‌الملل، ۱۳۸۴: ۳۸).

موضوع دیگر آن‌که، «رویه»[1] به عنوان یکی از عناصر تشکیل‌دهنده‌ی عرف، نه فقط اعمال فیزیکی بلکه «اعمال کلامی»[2] را نیز در برمی‌گیرد. اعمال کلامی به معنی اظهاراتی اســـت که در مقابل اعمال فیزیکی قرار می‌گیرند و در واقع شـــکل رایج‌تری از رویه‌ی کشور در مقایســـه با رفتار فیزیکی می‌باشند. بیانیه‌های دیپلماتیک (شامل اعتراضیه‌ها)، بیانیه‌های مرتبط با سیاســـت دولت، اظهـــارات مطبوعاتی، نظام‌نامه‌ی رســـمی (برای مثال در خصوص قوانین نظامی)، دســـتورالعمل‌های صادره خطاب به نیروهای مسلح، دیدگاه‌های حکومت‌ها در خصوص پیش‌نویس معاهدات، قانونگذاری، آراء و تصمیمـــات دادگاه‌هـــای ملی و مقامـــات اجرایی، دفاعیات صـــورت گرفته در محضر دادگاه‌های بین‌المللی، بیانیه‌های مطرح شـــده در ســـازمان‌های بین‌المللی و قطعنامه‌های تصویب شـــده از ســـوی این مراجع، که به عنوان نمونه‌هایی از رویه‌ی

1. Usus
2. Verbal Acts

کشور بدان‌ها اســـتناد می‌شـــود، همگی نمونه‌هایی از اعمال کلامی هستند (انجمن حقوق بین‌الملل، ۱۳۸۴: ۲۹-۲۸). در واقع، چند کشـــور نظریات خود را در خصوص موضوع دفاع مشروع در واکنش به حمله‌ی سایبری بیان نموده‌اند. این رویه که مبین «نظر حقوقی»[1] اســـت، باید گسترده و واقعاً یک شـــکل باشد (Continental shelf case, 1969, Para: 74). بـــه رغم آن‌که بیانیه‌ها و اعلامیه‌های موجود در خصوص موضوع مورد بررســـی، توسط تعداد محدودی از کشـــورها صادر شده‌اند، اما این امر مانع شکل‌گیری عرف در این خصوص نمی‌باشد. انجمن حقوق بین‌الملل خاطر نشان می‌کند که معیار گسترده بودن رویه‌ی کشورها بیشتر جنبه‌ی کیفی دارد تا کمی. به عبارت دیگر، بحث بر سر تعداد کشورهای مشارکت‌کننده در رویه نیست، بلکه موضوع آن اســـت که کدام کشورها در ایجاد رویه نقش داشـــته‌اند (انجمن حقوق بین‌الملل، ۱۳۸۴: ۴۶). «کاســـسه»، مثال فضای ماوراء جـــو را مطرح می‌کند که با وجود آن‌که دو کشـــور فن‌آوری بهره‌برداری از آن را دارا بوده‌اند، همگرایی آنان ایجاد ســـریع یک قاعده‌ی حقوق بین‌الملل عرفی را موجب شـــد (Cassese, 2005: 158). مشابه این وضعیت بر حملات سایبری حاکم است جهت احراز یک رویه‌ی کلی در این خصوص، باید رویه‌ی کشورهای دارای فن‌آوری‌های پیشرفته‌ی سایبری را لحاظ نمود.

ایـــالات متحده آمریـــکا، در خصوص حق دفاع مشـــروع در تقابل با حملات سایبری، مواضعی را اتخاذ نموده است. بر اساس ارزیابی وزارت دفاع این کشور، کشور حامی حملات سایبری، حق توسل به دفاع مشروع را برای طرف مقابل ایجاد می‌کند. از منظر این وزارت‌خانه، هرگاه یک حمله‌ی شـــبکه‌ای رایانه‌ای هماهنگ، سیســـتم کنترل ترافیک هوایی یک کشور و یا سیستم‌های بانک‌داری و مالی آن را مختل کند، دریچه‌ی چندین سد را باز کند و در نتیجه سیل جاری شود و هر یک از این اقدامات تلفات گســـترده غیرنظامیان و یا خســـارات مادی را در پی داشته باشد، کشور اخیر، قربانی و هدف یک حمله‌ی مسلحانه یا عملی برابر با یک حمله‌ی مسلحانه واقع شده است (www.au.af.mil).

ســـند ســـال ۲۰۰۹ میلادی حکومت انگلســـتان با عنوان «استراتژی امنیت سایبری انگلستان»[2] نیز توسل به هر گزینه‌ای را امکان‌پذیر دانسته و بر لزوم توسعه‌ی

1. Opinio Juris
2. Cyber Security Strategy of the United Kingdom

توانمندی‌های نظامی و غیرنظامی برای اقدام به دفاع علیه حمله‌ی ســـایبری، تأکید می‌نماید (www.cabinetoffice.gov.uk). یک مقام ارشـــد نظامی روســـیه نیز بر اساس امکان استفاده‌ی فاجعه‌آمیز از ابزار جنگ اطلاعاتی استراتژیک توسط دشمن، علیه سیســـتم‌های فرماندهی و کنترل این کشور یا توان رزمی نیروهای مسلح، برای روســـیه حق استفاده‌ی از تســـلیحات هســـته‌ای علیه ابزار و قوای جنگ اطلاعاتی و ســـپس علیه خود کشـــور متجاوز را محفوظ می‌داند (Antolin-Jenkins, 2005: 166). هم‌چنان که معاون ســـتاد کل نیروهای مســـلح جمهوری اسلامی ایران نیز از حملات بازدارنده‌ی ســـایبری علیه کســـانی خبر می‌دهد که به مراکز مختلف کشور حمله می‌کنند (www.mardomsalari.com).

رویه‌ی سازمان‌های بین‌المللی مربوطه، شکل دیگری از رویه‌ی کشورها است کـــه در ارزیابی وجود یک قاعده‌ی حقـــوق بین‌الملل عرفی باید مورد توجه قرار گیرد (انجمن حقوق بین‌الملل، ۱۳۸۴: ۳۶)؛ هم‌چنان‌که ســـران کشـــورها و حکومت‌های عضو پیمان ناتو[1] در اجلاس بیســـتم نوامبر سال ۲۰۱۰ میلادی در لیسبن نیز ضمن تبیین موضع خود در خصوص حملات ســـایبری و با اذعان به روند رو به رشـــد این تهدیدها، چنین اظهار داشـــته‌اند: «به منظور تأمین دسترسی دائم و نامحدود پیمان ناتو به فضای ســـایبر و سیستم‌های مهم آن، جنبه‌ی سایبری مخاصمات جدید را در دکتریـــن ناتو لحاظ نموده و قابلیت‌های ردیابـــی، ارزیابی، بازدارندگی، دفاع و جبران را در مواجهه با یک حمله‌ی ســـایبری علیه سیســـتم‌های حساس و با اهمیت پیمان، بهبود می‌بخشیم. به ویژه تلاش خواهیم کرد تا سال ۲۰۱۲ قابلیت واکنش به حملات ســـایبری را ارتقاء داده و تمامی ارکان پیمان را تحت حفاظت ســـایبری قرار دهیم» (www.nato.int).

1. Heads of State and Government Meeting of the North Atlantic Council

برآمد

امروزه جنگ سایبری به یک واقعیت بدل شده است؛ این در حالی است که فقدان مرز در فضای سایبر، این امکان را برای مرتکبان حملات سایبری فراهم آورده است که خود را در پس آدرس‌های اشتباهی و حیله‌های اینترنتی پنهان نمایند؛ امری که شناسایی منشاء حمله‌ی سایبری را با دشواری‌هایی مواجه ساخته است.

پرسش اساسی این است که آیا یک حمله‌ی سایبری، اقدامی مادون آستانه‌ی توسل به زور است یا گونه‌ای توسل به زور یا حتی توسل به زور در حد یک حمله‌ی مسلحانه تلقی می‌شود؟

در مقام پاسخ، آن قسم از حملات سایبری صورت گرفته در مقیاس گسترده و علیه زیرساخت‌های مهم را باید حمله‌ی مسلحانه دانست؛ حملاتی که نتیجه‌ی آن بروز خسارات مادی عمده یا تلفات انسانی قابل قیاس با یک حمله‌ی مسلحانه با تسلیحات متعارف باشد؛ چنین حملاتی وفق ماده‌ی ۵۱ منشور ملل متحد، کشور قربانی را به دفاع مشروع مجاز می‌سازد. افزون بر این، دفاع مشروع علیه حمله‌ی سایبری که به آستانه‌ی یک حمله‌ی مسلحانه نائل نشده، اما مهیاکننده‌ی حمله‌ی مسلحانه‌ی قریب‌الوقوع با تسلیحات متعارف باشد، امکان‌پذیر است.

حقوق بین‌الملل عرفی نیز با توجه به وجود نسبی رویه‌ی کشورها و اعتقاد حقوقی، به‌ویژه در خصوص حق دفاع مشروع علیه حملات سایبری، می‌تواند نقشی را در این زمینه ایفاء نماید. این فرایند ادامه دارد و می‌تواند به شکل‌گیری یک قاعده‌ی عرفی در سال‌های پیش رو منجر گردد. ضمن آن‌که همکاری‌های بین‌المللی در سطوح منطقه‌ای و جهانی می‌تواند در مقابله با حملات سایبری که پدیده‌ای بدون مرز است، نقش مؤثری ایفاء نماید. در این راستا ضرورت انعقاد معاهده‌ای خاص در مورد ممنوعیت حملات سایبری بیش از پیش احساس می‌شود.

فهرست منابع

انجمن حقوق بین‌الملل، ***اصول حاکم بر شکل‌گیری حقوق بین‌الملل عرفی عام***، مترجم: محمدجعفر قنبری جهرمی، تهران: دراک، چاپ اول، ۱۳۸۴.

پاکزاد، بتول، ***تروریسم سایبری***، رساله‌ی دکتری حقوق کیفری و جرم‌شناسی، دانشکده‌ی حقوق دانشگاه شهید بهشتی، ۱۳۸۸.

پاکزاد، بتول، ***«ماهیت تروریسم سایبری»***، مجله‌ی تحقیقات حقوقی دانشگاه شهید بهشتی، ویژه‌نامه‌ی شماره‌ی ۴، بهار ۱۳۹۰.

حسن‌بیگی، ابراهیم، ***حقوق و امنیت در فضای سایبر***، تهران: مؤسسه‌ی فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران، چاپ اول، ۱۳۸۴.

حلمی، نصرت‌الله، ***تدوین و توسعه حقوق بین‌الملل: مسؤولیت بین‌المللی دولت و حمایت سیاسی***، تهران: میزان، چاپ اول، ۱۳۸۷.

ضیایی بیگدلی، محمدرضا، ***حقوق معاهدات بین‌المللی***، تهران: گنج دانش، چاپ اول، ۱۳۸۳.

فضلی، مهدی، ***مسؤولیت کیفری در فضای سایبر***، تهران: خرسندی، چاپ اول، ۱۳۸۹.

محمدعلی پور، فریده، ***دفاع مشروع در حقوق بین‌الملل***، تهران: دفتر مطالعات سیاسی و بین‌المللی، چاپ اول، ۱۳۷۹.

نورمحمدی، مرتضی، ***«سایبر تروریسم: تروریسم در عصر اطلاعات»***، مجموعه‌ی مقالات تروریسم و مقابله با آن، به اهتمام عباسعلی کدخدایی؛ نادر ساعد، تهران: مجمع جهانی صلح اسلامی، چاپ اول، ۱۳۹۰.

Advisory Opinion on the Legality of the Threat or use of Nuclear weapons ICJ Reports 1996.

Ago, R., ***"Eight Report on State Responsibility"***, in: ILC (ed.), Yearbook of the International Law Commission, vol. 2, 1980.

A More Secure World: ***Our shared Responsibility***, Report of the High Level Panel on Threats, Challenges and Change, Doc. A/59/565.

Antolin-Jenkins, V.M., ***"Defining the Parameters of Cyberwar***

Operations: Looking for Law in All the wrong Places?" Naval Law Review, No. 51, 2005.

Armed Activities on the Territory of the Congo (DRC V.Uganda), ICJ Reports 2005.

Beaumont, P., ***"US Appoints First Cyber warfare General"***, the Observer, 10. 23 May 2010.

Brenner, S.W., ***"At Light speed: Attribution and Response to Cyber Crime/ Terrorism/ warfare"***, Journal of Criminal Law and Criminology, No, 97, 2006 - 2007.

Brownlie, I., ***International Law and the use of Force by States***, Oxford: Clarendon Press, 1963.

Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina V. Serbia and Montenegro), Merit, Judgment of 26 February 2007.

Case Concerning North Sea Continental shelf, ICJ Reports 1969.

Case Concerning Oil Platforms (Iran V. United states), ICJ Reports 2003.

Cassese, A., ***International Law***, Oxford: Oxford University Press, second Edition. 2005.

Condron, S.M., ***"Getting It Right: Protecting American Critical Infrastructure in Cyberspace"***, Harvard Journal of Law and Technology, No. 20, 2006-2007.

Conforti, B., ***The Law and Practice of the United Nations***, Leiden: Martinus Nijhoff, 2005.

D'Amato, A., ***"International Law, Cybernetics, and Cyberspace"***, in: Schmitt/O'Donnell (eds), Computer Network Attack and International Law, 2001.

Delibasis, D., ***The Right to National Self-Defence in Information warfare Operations***, London: Arena Books, 2007.

Dinstein, Y., ***"Computer Network Attacks and self-Defense"***, in: Schmitt/O'Donnel (eds), Computer Network Attack and Interna-

tional Law, 2001.
Dinstein, Y., ***war, Aggression and Self-Defence***, Cambridge: Cambridge University Press, 3rd ed, 2005.
Documents of the United Nations Conference on International Organization, vol. 6, 1945.
Eshel, D., ***"Israel Adds Cyber-Attack to IDF"***, Available at: www.military.com/features/o,15240,210486,00.html, 2010.
Garner, B.A. (ed), ***Black's Law Dictionary***, Eagan: West Group, 9th ed, 2009.
Gray, C., ***International Law and the Use of Force***, Oxford: Oxford University Press, 2008.
Greenberg, L.T., ***Information Warfare and International law***, Mishawaka: National Defense University Press, 1998.
ICTY, Prosecutor V. Tadic, Case No. IT-94-1-A, Appeals Chamber, Judgment, 15 July 1999. Available at: www.icty.org
In Larger Freedom: ***Towards Development***, Security and Human Rights for All", Report of the Secretary-General, Doc. A/59/2005.
Johnson, P.A., ***"Is it Time for a Treaty on Information warfare?"***, in: Schmitt/O'Donnell (eds), Computer Network Attack and International Law, 2001.
Joyner, C.C.; Lotrionte, C., ***"Information Warfare as International Coercion: Elements of a Legal Framework"***, European Journal of International Law, No. 12, 2001.
Lewis, J., ***"To Protect the U.S. Against Cyberwar, Best Defense is a Good Offense"***, U.S. News and World Report, 29 April 2010.
Military and Paramilitary Activities in and Against Nicaragua (Nicaragua V. United states), ICJ Reports 1986.
Ophardt, J.A., ***"Cyber warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield"***, Duke Law and Technology Review, No. 3, 2010.
Osterdahl, I., ***Threat to Peace***, Uppsala: Lustus Forlag, 1998.

Randelzhofer, A., ***"Article 2 (4)"***, in: Simma, B. (ed.), The charter of the United Nations: A Commentary, vol. 1, 2002.
Robertson Jr., H.B., ***"Self-Defense Against Computer Network Attack Under International Law"***, in: Schmitt/O'Donnell (eds), Computer Network Attack and International Law, 2001.
Roscini, M., ***"Threats of Armed Force and Contemporary International Law"***, Netherlands International Law Review, No. 54, 2007.
Schmitt, M.N., ***"Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework"***, Colum. J. Transnat'l L., No. 37, 1998-1999.
Shackelford, S.J., ***"From Nuclear war to Net war: Analogizing Cyber Attacks in International Law"***, Barkeley Journal of International Law, No. 27, 2009.
UN Doc. A/RES/2625 (XXV) of 24 October 1970.
UN Doc. A/RES/36/103 of 9 December 1981.
N Doc. A/RES/42/22 of 18 November 1987.
UN Doc. A/RES/55/63 of 4 December 2000.
UN Doc. A/RES/56/121 of 19 December 2001.
UN Doc. A/RES/58/199 of 23 December 2003.
UN Doc. A/RES/63/37 of 2 December 2008.
UN Doc. A/RES/64/25 of 2 December 2009.
UN Doc. S/RES/1368 of 12 December 2001.
United States Diplomatic and Consular Staff in Tehran (United states V. Iran), ICJ Reports 1980.
Watts, S., ***"Combatant status and Computer Network Attack"***, va. J.Int'l L., No. 50, 2010.
Weisbord, N., ***"Conceptualizing Aggression"***, Duke J.Comp. & Int'l L., No. 20. 2009.
Zemanek, k., ***"Armed Attack"***, Max Planck Encyclopedia of Public International Law, Oxford: Oxford University Press, 2010.

www.cabinetoffice.gov.uk/media/216620/csso906.pdf
www.us-cert.gov/reading-room/cyberspace-strategy.pdf
www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf
www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf
www.nato-pa.int/default.asp?SHORTCUT=1782
www.au.af.mil/au/awcgate/dod-io-legal/dod-io-legal.pdf
www.mardomsalari.com/template1/NewsPrintableversion.aspx?NID=99623
www.nato.int/nato-static/assets/pdf
www.defense.gov/news/mar2005/d20050318nms.pdf
www.bangdad.com/bangdad/pages/details.asp?id=263
www.eur-lex.europa.eu/LexUriserv/LexUriserv.do?uri=com:2005:0576