حملات سایبری ازمنظر حقوق بین‌الملل (مطالعه موردی: استاکس‌نت)

حسین خلف رضایی*

تاریخ دریافت ۹۱/۸/۲۸	تاریخ پذیرش ۹۲/۲/۲۱

در سال ۲۰۱۰ استاکس‌نت با توجه به کارویژه‌ها و پیچیدگی‌هایش مورد توجه کارشناسان قرار گرفت. این بدافزار به‌گونه‌ای طراحی شد تا رایانه‌های خاصی را در ایران مورد هدف قرار دهد. اگرچه استاکس‌نت از طریق اینترنت در جهان منتشر شد، اما آثار مخرب آن محدود به سیستم‌های کنترلی خاصی بود که در ایران هدف قرار گرفته بودند. با رمزگشایی کدهای این بدافزار مشخص شد که همانند سلاحی علیه تأسیسات هسته‌ای کشورمان طراحی و به‌کار گرفته شده است تا عملیات گازرسانی سانتریفیوژها را در فرایند غنی‌سازی دچار اختلال کند. اهداف و آثار این بدافزار به‌گونه‌ای بود که بسیاری آن را با یک حمله مسلحانه مقایسه کردند.

کلیدواژه‌ها: حملات سایبری؛ استاکس‌نت؛ حمله مسلحانه؛ حقوق مخاصمات مسلحانه

---

* دانشجوی دکتری حقوق بین‌الملل، دانشکده حقوق و علوم سیاسی، دانشگاه تهران؛
Email: h.rezaei@mail.ut.ac.ir

مقدمه

حقوق عاملی برای سامان دادن به روابط اجتماعی است، بنابراین به اقتضای جریان‌های اجتماعی سیال و پویاست. حقوق مخاصمات مسلحانه نیز از این مجموعه خارج نیست و به فراخور تحولاتی که در نوع عوامل درگیر در مخاصمه، ابزارها و روش‌های جنگی رخ داده است، دستخوش تغییرات و دگرگونی‌هایی شده است. جنگ که در گذشته‌های نه‌چندان دور به‌مثابه یکی از ابزارهای سیاست ملی کشورها برای حل اختلافات بین‌المللی، تأمین یا بهبود منافع ملی انجام می‌شد، رفته‌رفته با خودنمایی بازیگران غیردولتی شکل دیگری به‌خود گرفت. نقش‌آفرینی این بازیگران که خود را در قلمرو جغرافیایی و حاکمیتی یک دولت محدود نمی‌دیدند، مستلزم بازنگری در قواعد بازی بود.

با تغییر و تحول طرف‌ها و عوامل درگیر در مخاصمات، شیوه‌ها و ابزارهای جنگی نیز تغییرات چشمگیری داشته‌اند. بهره‌گیری از روش‌های سایبری و خرابکاری توسط بدافزارهای رایانه‌ای از جمله روش‌ها و ابزارهای مخرب جدید به‌شمار می‌آید. شدت آثار حملات سایبری بسیاری از حقوق‌دانان و پژوهشگران را درباره امکان رسیدن به آستانه مخاصمه مسلحانه متقاعد کرده است. بدون شک خرابکاری و انهدام یک نیروگاه هسته‌ای توسط دولتی خارجی می‌تواند به‌عنوان حمله‌ای مسلحانه که در حوزه حقوق مخاصمات قرار می‌گیرد، ارزیابی شود.[۱]

اینترنت که ساخته ارتش ایالات متحده بود با سرعت غیرقابل باورنکردنی در همه زمینه‌ها تسری یافت و جهانی شد. در چنین فضایی طرح دولت الکترونیک در دستور کار بسیاری از کشورها قرار گرفت. در کنار فواید بی‌شمار این وسیله ارتباط جمعی نمی‌توان خطرهای فراوان آن را برای زندگی شخصی و اجتماعی افراد نادیده گرفت. درواقع، به

---

۱. حملات سایبری به کشورهای استونی (۲۰۰۷) و گرجستان (۲۰۰۸) که به باور بسیاری از جانب روسیه هدایت شده‌اند، از گسترده‌ترین موارد حملات سایبری دولتی بوده‌اند. در کنار حملات سایبری دولتی، از تروریسم سایبری و جرائم سایبری نیز می‌توان یاد کرد که دسته نخست مورد تأکید پژوهش حاضر است.

میزان گسترش و پیشرفت فضای الکترونیک و دربرگرفتن زیرساخت‌ها و امور حیاتی جامعه، به همان میزان نیز احتمال آسیب‌ها از آن افزایش می‌یابد.

بدافزار استاکس‌نت یکی از ابزارهای مخربی شناخته شده که به‌احتمال زیاد ازسوی طرفی دولتی تأسیسات کشورمان را هدف قرار داده است. اگرچه دولتی مسئولیت تهیه یا ارسال این بدافزار را به عهده نگرفته است، اما با توجه به قرائن، گمانه‌زنی‌ها بیشتر متوجه دولت آمریکاست؛ زیرا دولت و رئیس‌جمهور این کشور، حملات سایبری[1] علیه جمهوری اسلامی ایران را به‌طور رسمی در دستور کار خود قرار داده است. این موضوع، در حالی است که این کشور حملات سایبری علیه خود را جنگ عملی[2] تلقی می‌کند که در واکنش به آن درصورت نیاز از نیروی نظامی و ارتش کلاسیک نیز دریغ نخواهد کرد.

این پژوهش که مبتنی‌بر روش استنتاجی و تبیین مسائل و پرداختن به ابهامات است به واکاوی ماهیت حملات سایبری ازمنظر حقوق بین‌الملل می‌پردازد و حملات سایبری علیه تأسیسات زیربنایی ایران را مورد تحلیل قرار می‌دهد. بر این اساس، ابتدا مفاهیم مرتبط با فضای سایبر تبیین می‌شود، سپس حمله سایبری از نگاه حقوق بر جنگ[3] و حقوق در جنگ[4] مورد بررسی قرار می‌گیرد. همچنین به‌طور خاص، بدافزار استاکس‌نت ازمنظر حقوق مخاصمات مورد ارزیابی قرار می‌گیرد. پس از آن، موضوع مسئولیت ناشی از حملات سایبری دنبال خواهد شد و در نهایت، به نتیجه‌گیری و پیشنهادهای این پژوهش می‌پردازیم.

۱ تعریف و گونه‌شناسی حملات سایبری

در مدت زمان پانزده سال، شمار کاربران خصوصی اینترنت از حدود شانزده میلیون به عددی بالغ بر ۱/۷ میلیارد کاربر افزایش یافت (UK Government, 2010: 29). در کنار کاربران خانگی و اشخاص خصوصی، وابستگی مؤسسات عمومی و دولتی به اینترنت و

1. Cyberattacks
2. Act of War
3. *Jus ad Bellum*
4. *Jus in Bello*

شبکه‌های رایانه‌ای نیز افزایش چشمگیری داشته است که امور نظامی نیز از آن مستثنا نیست. بسیاری بر این باورند که فضای سایبر به‌مثابه قلمرو پنجم جنگی در کنار چهار قلمرو زمین، دریا، هوا و فضای ماورای جو به‌شمار می‌آید.[1] بنابراین این سؤال پیش می‌آید که قواعد از پیش تعیین شده حقوق بین‌الملل تا چه حد می‌توانند جواب‌گوی این فضای نوظهور باشند. بدیهی است که حقوق بین‌الملل برای سامان دادن به فعالیت دولت‌ها و روابط بین‌المللی به‌وجود آمده و فعالیت‌های خاصی را مدنظر قرار نمی‌دهد. بااین‌حال، واگذار کردن وضعیت‌ها و موضوعات جدید به قواعد از پیش موجود حقوق بین‌الملل می‌تواند در عمل با دشواری‌ها و در مواردی با کاستی‌هایی مواجه شود (Melzer, 2011: 3). تعیین حقوق و قواعد حاکم منوط به شناختن موضوعات و وضعیت‌های حقوقی یا تشخیص مصادیق و امور موضوعی است.

۱-۱ مفهوم فضای سایبر

در عصر ارتباطات و اطلاعات، فضای سایبر و اینترنت از اجزای جدایی‌ناپذیر زندگی جوامع بشری به‌شمار می‌آید. درباره معنای «فضای سایبر»[2] تعریف پذیرفته شده بین‌المللی وجود ندارد، اما برخی کشورها به تعریف این مفهوم پرداخته‌اند. «فضای سایبری» شبکه جهانی به هم پیوسته‌ای از اطلاعات دیجیتالی و زیرساخت‌های ارتباطی مانند اینترنت، شبکه‌های مخابراتی، شبکه‌های رایانه‌ای و انفورماتیک است.[3]

وزارت دفاع ایالات متحده فضای سایبری را این‌گونه تعریف کرده است: «دامنه‌ای جهانی در فضای اطلاعات که متشکل از شبکه‌ها و سامانه‌های مستقل فناوری اطلاعات از قبیل: اینترنت، شبکه‌های مخابراتی، سیستم‌های رایانه‌ای، و پردازنده‌ها و کنترلرهای تعبیه شده است» (Joint Chiefs of Staff, 2001: 141). در تعریف دیگری از این فضا آمده است: «فضایی

1. See for *e.g.*, US Department of Defense, *The National Military Strategy for Cyberspace Operations*, 2006, P. 3.
2. Cyberspace
3. See for The White House, *Cyberspace Policy Review*, 16 May 2011, P. 1.

که با استفاده از [رایانه‌ها و دیگر وسایل الکترونیکی] و توسط شبکه‌ها و تأسیسات فیزیکی به هم پیوسته به‌منظور ذخیره، تعدیل یا انتقال داده‌ها به‌کار گرفته می‌شود» (Lopez, 2007).

۱-۲ مفهوم حمله سایبری

در تعریف عمومی حمله سایبری گفته می‌شود: «یک عملیات سایبری که انتظار می‌رود باعث تلفات یا خسارات انسانی شده یا به صدمه و خسارت به اشیا بینجامد». اکثر حقوق‌دانان بر این باورند که حملات سایبری می‌تواند وضعیت مخاصمه مسلحانه به‌وجود آورد و از این نظر با حملات فیزیکی کلاسیک تفاوت ماهوی ندارد (Brown, 2011: 71). وزارت دفاع ایالات متحده با رویکردی موسع، حمله سایبری را اقدامی می‌داند که موجب «اختلال، انسداد،[1] تضعیف،[2] یا امحای اطلاعات موجود در رایانه‌ها یا شبکه‌های رایانه‌ای یا خود رایانه‌ها و شبکه‌های رایانه‌ای» می‌شود (US Department of Defense, 2006: GL-1).[3]

حملات سایبری انواع گوناگونی دارد که آنها را در سه دسته کلی می‌توان برشمرد: نرم‌افزارهای مخربی[4] که از طریق اینترنت منتشر می‌شوند،[5] حملات ممانعت از خدمات‌رسانی[6] و نفوذ از راه دور که افراد به سیستم هدف وارد می‌کنند (Sklerov, 2009: 13-14).

۱-۳ مفهوم جنگ سایبری

در جهان تعریف پذیرفته شده‌ای از «جنگ سایبری»[7] وجود ندارد، اما به‌طورکلی به جنگی

---

1. Deny
2. Degrade
3. See for, "Computer Network Attack", *HPCR Manual on International Law Applicable to Air and Missile Warfare* (May 15, 2009), at: http://www.ihlresearch.org/amw/manual/category/section-a-definitions,
4. Malware or Malicious Software
۵. این بدافزارها از دو دسته ویروس‌ها (Virus) و کرم‌ها (Worm) تشکیل شده‌اند. استاکس‌نت در دسته دوم ارزیابی می‌شود.
6. Danial- of - Service (DOS) The Most Severe form of DOS Attack is a Distributed Denial-of-service Attack (DDOS).
7. Cyber Warfare

اطلاق می‌شود که در فضای سایبر و با استفاده از روش‌ها و ابزارهای سایبری انجام می‌شود. مثلاً آلوده‌سازی یا تخریب شبکه رایانه‌ای طرف متخاصم با یک ویروس یا بدافزار می‌تواند یک جنگ سایبری باشد، درحالی‌که انهدام تأسیسات مخابراتی یا سایبری نظامی توسط بمباران هوایی نمی‌تواند چنین وصفی داشته باشد (Melzer, 2011: 4).[1]

وزارت دفاع ایالات متحده عملیات سایبری را این‌گونه تعریف می‌کند: «به‌کارگیری ظرفیت‌های سایبری در جایی که هدف اولیه آنها دستیابی به اهداف یا آثاری نظامی از/ در فضای سایبر باشد» (Joint Chiefs of Staff, 2001: 141). گزارش مرکز پژوهش‌های کنگره آمریکا نیز بیان داشته است: «جنگ سایبری را می‌توان برای توصیف ابعاد مختلفی از تهاجم به یا دفاع از اطلاعات و شبکه‌های رایانه‌ای در فضای سایبر مانند از بین بردن توانایی طرف مقابل در انجام این‌گونه امور به‌کار برد» (Hildreth, 2001: 1).

گفتنی است برخی دولت‌ها از جمله آمریکا[2] و روسیه حق دفاع مشروع در برابر حملات سایبری را در دکترین دفاعی خود محفوظ دانسته‌اند. مسئولان دولت روسیه به‌صراحت اعلام کرده‌اند در واکنش به حملات سایبری حتی می‌توانند از سلاح‌های اتمی استفاده کنند. دولت‌های کلینتون و بوش نیز تهدیدات ناشی از حملات سایبری را با عواقب استفاده از سلاح‌های سنتی دارای تخریب وسیع[3] مقایسه کرده‌اند (Kulesza, 2009: 142-144).[4]

---

1. The Same Approach is Taken by Marco Roscini, "World Wide Warfare-Jus ad Bellum and the Use of Cyber Force", In Armin Bogdany and Rüdiger Wolfrum (eds.), *Max Planck Year Book of United Nations Law*, Vol. 14, 2010, P. 96.

2. See Dep't of Def., Office of Gen. Counsel, An Assessment of International Legal Issues, May 1999, *Reprinted in* Thomas Wingfield, The Law of Information Conflict, National Security Law in Cyberspace (2000), at 431; Exec. Order No. 13,010, 61 Fed. Reg. 37,347 (July 15, 1996); Exec. Order 13,321, 66 Fed. Reg. 53,063 (Oct. 16, 2001).

3. Weapons of Mass Destruction

٤. جنگ الکترونیک یکی از عناصر مهم در جنگ خلیج فارس اول (۱۹۹۱) بود، اما پس از وقایع ۱۱ سپتامبر، حملات حملات سایبری معنای جدیدی پیدا کرد. به‌دلیل آسیب‌پذیری بالای ایالات متحده در برابر این‌گونه حملات، در تدابیر و دستورالعمل‌های نظامی و دفاعی این کشور توجه ویژه‌ای به این مسئله شده است. طبق برآوردها میانگین حملات سایبری علیه سیستم دفاعی ملی ایالات متحده از دویست مورد در سال ۱۹۹٤ به ٤۰۰۰۰ مورد در پایان سال ۲۰۰۲←

اکنون که مفاهیم پایه‌ای پژوهش حاضر به‌نحو اجمال روشن شد، به‌نظر می‌رسد برای پاسخ‌گویی به موضوعات تحقیق می‌بایست، ازنظر اصطلاحی و واژه‌شناسی (ترمینولوژی) نسبت اقدامات و عملیات‌هایی که در فضای سایبر روی می‌دهد را با مفاهیم کلاسیک حقوق بین‌الملل مانند زور،[1] حمله مسلحانه[2] و حمله[3] بازشناخت و همچنین این مسائل را ارزیابی کرد که آیا حملات یا عملیات‌های سایبری می‌توانند در چارچوب حقوق توسل به زور و حقوق مخاصمات مسلحانه به‌مثابه کاربرد «زور» و یا «حمله مسلحانه» تلقی شده و موجب اعمال مقررات هریک از این دو نظام حقوقی را فراهم آورند یا خیر.[4] ضمن آنکه مقررات منشور ملل متحد به‌ویژه فصل هفتم آن نیز می‌تواند مورد توجه قرار گیرد.

۲ حمله سایبری و حقوق بر جنگ

۲-۱ حمله سایبری به‌مثابه نقض حقوق توسل به زور

بند «٤» ماده (۲) منشور ملل متحد بیان می‌کند: «تمام اعضا در روابط بین‌المللی خود از تهدید به زور یا استفاده از آن علیه تمامیت ارضی یا استقلال سیاسی هر کشوری یا از هر

←رسید. البته مطابق اظهارات سازمان سامانه‌های اطلاعات دفاعی آمریکا (The U.S. Defence Information Systems Agency)، تنها یکی از ۱۵۰ مورد به‌طور واقعی شناسایی می‌شود. بنابراین، آمار واقعی بسیار بیشتر برآورد شده است. براساس برآورد وزارت دفاع آمریکا هزینه بازیابی و تعمیر زیان‌های وارده در اثر این حملات در نیمه سال ۲۰۰۹ بالغ بر صد میلیون دلار بوده است. برای آگاهی بیشتر، رک.:

D. Delibasis (2007). "The Right to National Self-defence: In Information Warfare Operations", *Bury St Edmunds*, PP. 31-38.

1. Force (Art. 2 (4)).
2. Armed Attack (UN Charter, art. 51)
3. Attack (Additional Protocol I to the Geneva Conventions, Art. 49 (1)).

٤. ممکن است معنا و مصداق «حمله مسلحانه» در هریک از این دو نظام حقوقی متفاوت باشد. چنان‌که تفسیر دیوان بین‌المللی دادگستری از این اصطلاح در ماده (۵۱) منشور ملل متحد، صدور آن از جانب یک دولت است و نه یک طرف غیردولتی. درصورتی‌که حمله مسلحانه در پرتو حقوق مخاصمات مسلحانه ازسوی گروه‌های مسلح غیردولتی نیز می‌تواند مصداق داشته باشد. بنابراین هر حمله مسلحانه‌ای نمی‌تواند موجب استناد دولت به حق دفاع مشروع وفق ماده (۵۱) منشور شود.

روش دیگری که با مقاصد ملل متحد مغایرت داشته باشد خودداری خواهند کرد». مسئله این است که آیا حملات سایبری می‌تواند در قلمرو موضوعی این مقرره قرار گیرد؟

اگرچه معنای متداول و متبادر از واژه «زور» آنچنان گسترده است که اجبار نظامی و غیرنظامی را نیز دربرمی‌گیرد، اما به‌نظر بیشتر حقوق‌دانان این مقرره ناظر به حالت نظامی و مسلحانه است (Randelzhofer, 2002: 117). البته نوع ابزارها و سلاح‌های به‌کار رفته در اعمال زور حصری نیست (I.C.J., 1996: para. 39). با این توصیف، عملیات‌های سایبری که دارای آثاری مشابه تسلیحات نظامی هستند نباید مورد مناقشه قرار گیرد (Schmitt, 1999: 916). بنابر نظر دیوان بین‌المللی دادگستری، بند «٤» ماده (۲) «به هرگونه کاربرد زوری صرف‌نظر از [نوع] سلاح به‌کار رفته» تسری می‌یابد (I.C.J, 1996: para. 39). بر این اساس، چون حملات سایبری دربردارنده سلاح‌های متعارف و کلاسیک نیستند، به‌خودی‌خود نمی‌تواند آن را از عنوان کاربرد زور مستثنا سازد.

در مقابل، عده‌ای با توجه به مقدمات[1] تدوین منشور ملل متحد که حاکی از تعمد دولت‌ها در عدم گسترش دامنه «زور» به فشارهای سیاسی یا اقتصادی بوده است،[2] استناد به بند «٤» ماده (۲) منشور را درباره عملیات‌های سایبری که به تخریب یا تلفات مستقیم جانی منجر نمی‌شود را مورد تردید قرار داده‌اند. طرف‌داران این رویکرد به ماده (٤١) منشور که در مورد تصمیمات و اقدامات غیرنظامی از قطع خطوط ارتباطی است، استناد می‌کنند که با اخذ ملاک از آن می‌توان، دست‌کم عملیات‌های سایبری که کارویژه آنها اختلال یا ممانعت در خدمات‌رسانی است، را در زمره اقدامات غیرنظامی طبقه‌بندی کرد و از شمول ماده (۲) بند «٤» منشور خارج دانست (Melzer, 2011: 7). اما به‌نظر می‌رسد با تفسیری غایی از منشور با توجه به مقدمه آن که «صیانت از نسل‌های آتی در برابر بلای جنگ» را

1. *Travaux Préparatoires*
2. A Brazilian Proposal to Extend the Prohibition to "the Threat or Use of Economic Measures in Any Manner Inconsistent with the Purposes of the United Nations"' Was Rejected at the San Francisco Conference; *Documents of the United Nations Conference on International Organization*, Vol. VI, 1945, PP. 559, 720–721.

هدف سازمان ملل متحد دانسته و در ماده (۱) به هدف حفظ صلح و امنیت بین‌المللی تصریح داشته است، می‌توان گفت که هرگاه ابزارها یا شیوه‌های غیرخشونت‌بار، صلح و امنیت بین‌المللی را به مخاطره اندازد با اهداف ملل متحد مغایرت خواهد داشت.[۱] گفتنی است که بند «٤» ماده (۲) آستانه‌ای از قبیل شدت یا مدت زمان برای ممنوعیت توسل به زور مشخص نکرده است.[۲] بنابراین، شمول این ممنوعیت گسترده‌تر از عنوان «تجاوز» (موضوع ماده (۳۹) منشور)[۳] یا «حمله مسلحانه» (موضوع ماده (۵۱) منشور و یا موضوع ماده (۲) مشترک کنوانسیون‌های ژنو) خواهد بود.[٤]

۲-۲ حمله سایبری به‌مثابه حمله مسلحانه

همان‌طور که دیوان بین‌المللی دادگستری در قضیه *نیکاراگوئه* بیان کرده است، باید میان شدیدترین صورت‌های کاربرد زور (که به آستانه حمله‌ای مسلحانه می‌رسند) و آنهایی که صرفاً اتفاقات مرزی هستند با توجه به «مقیاس و آثار»[۵] آن زور یا نیروی قهری تفکیک قائل شد. ازاین‌رو هر درگیری نظامی واجد عنوان حمله مسلحانه‌ای که مجوز دفاع مشروع است نخواهد بود (I.C.J, 1986: paras. 191 and 195). بنابراین، برای آنکه دولتی طبق ماده (۵۱)

---

۱. حملات سایبری از جانب دولت‌ها را مداخله در امور داخلی می‌توان تلقی کرد که از اصول سازمان ملل متحد است.

2. See for International Court of Justice, *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania) (Merits)*, Separate Opinion by Judge Alvarez, 1949, p. 47; International Law Commission, *Addendum-Eighth Report on State Responsibility by Mr. Roberto Ago, Special Rapporteur-the Internationally Wrongful act of the State, Source of International Responsibility (part 1)*, UN Document A/CN.4/318/Add.5-7, 1980, Paras. 58 and 86.

۳. تجاوز در قطعنامه چنین تعریف شده است: «به‌کارگیری نیروی نظامی توسط یک کشور علیه حاکمیت، تمامیت ارضی یا استقلال سیاسی کشوری دیگر یا به هر نحوی که با منشور ملل متحد سازگار نباشد». این قطعنامه هفت مورد از مصادیقی را که می‌تواند تجاوز تلقی شود را ذکر کرده است و البته بیان می‌کند که این موارد حصری نیستند. رک.:

G.A. Res. 3314 (XXIX), art. 1, U.N. Doc. A/3314, (Dec. 14, 1974), Arts. 1, 3 and 4.

4. See for International Court of Justice, *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua V. United States of America)*, Merits, 1986, paras. 191 and 195; International Law Commission, *Report of the International Law Commission on the Work of its Thirty-second Session, 5 May–25 July 1980, Official Records of the General Assembly, Thirty-fifth Session, Supplement No. 10*, UN Document A/35/10, 1980, P. 44.

5. Scale and Effects

منشور ملل متحد به حق دفاع مشروع استناد کند می‌بایست حمله سایبری را نه تنها توسل به زور بلکه به‌مثابه حمله‌ای مسلحانه[1] تلقی کند. البته منظور آن است که حملات سایبری خود موجد وضعیت مخاصمه مسلحانه شوند، نه آنکه یک مخاصمه کلاسیک و به‌عنوان یک روش جنگی به‌کار گرفته شوند. بنابراین باید گفت آیا ابزارهای سایبری می‌توانند در حکم سلاح به‌کار گرفته شوند.[2] دراین‌باره، گفته شده است: «این طراحی یا کاربرد متداول یک وسیله نیست که آن را سلاح می‌کند بلکه [ملاک] قصد و اثر به‌کارگیری آن است. استفاده از هر وسیله یا تعدادی از وسایل که باعث تلفات معتنابه جانی و/ یا تخریب گسترده مالی می‌شود می‌بایست حائز شرایط یک «حمله مسلحانه» انگاشته شود» (Quoted in: Melzer, 2011: 13). در بند «۱» ماده (٤۹) پروتکل اول الحاقی نیز آمده است: «حملات به معنای اعمال خشونت‌آمیز علیه طرف مقابل هستند اعم از آنکه تدافعی یا تهاجمی باشند».

معیاری که ژان پیکته در توصیف مخاصمه مسلحانه وفق ماده (۲) مشترک کنوانسیون‌های ژنو ارائه کرده نیز شایان توجه است. به‌نظر وی، کاربرد زور در جایی به‌عنوان «حمله مسلحانه» شناخته می‌شود که دارای دامنه، مدت و شدت کافی باشد (Graham, 2010: 87, 90). با توجه به معیار اثرمحور، درصورتی‌که کاربرد زور از طریق روش‌های سایبری به تلفات و خسارات معتنابه جانی و مالی منجر شود و یا آنکه تأسیسات زیربنایی و مهم[3] یک کشور را مورد هدف قرار دهد، می‌توان وقوع حمله‌ای مسلحانه را احراز کرد (Melzer, 2011: 14). این تأسیسات شامل مواردی است که برای تولید، انتقال یا توزیع انرژی به‌کار گرفته می‌شود یا مرتبط با حمل‌ونقل هوایی یا دریایی، خدمات بانکی و مالی، تجارت الکترونیک، آبرسانی، توزیع مواد غذایی، سلامت عمومی و سامانه‌ها و

---

1. In French: Aggression Armée.

۲. برای اطلاع از دیدگاه‌های برخی کشورها درخصوص حملات سایبری و انواع ابزارها و روش‌های سایبری، رک.:

Arie J. Schaap (2009). "Cyber Warfare Operations: Development and Use Under International Law", 2009 U.S. Air Force Academy, Department of Law, at:http://www.thefreelibrary.com/Cyber+warfare+operations%3a+development+and+use+under+international+law.-a0212035712.

3. Critical Infrastructures

شبکه‌های مهم اطلاعات هستند.[۱] بر این اساس، حمله سایبری به نهادهای مهم یک کشور مانند بازار بورس که پیامدهای سوئی بر رفاه اجتماعی یک کشور به‌جا می‌گذارد، حمله‌ای مسلحانه تلقی می‌شود.[۲]

در ابتدا، این‌گونه به ذهن متبادر می‌شود که حمله مسلحانه متضمن اعمال خشونت‌آمیزی است که به ایراد خسارات جانی یا تخریب اموال منجر می‌شود. در نتیجه حملات سایبری که چنین هدف یا پیامدی ندارند و برای ممانعت از خدمات‌رسانی و از کار انداختن یک برنامه طراحی شده‌اند را نمی‌توان حمله مسلحانه در نظر گرفت. دراین‌باره مباحثی انجام شده است،[۳] که به‌نظر می‌رسد بتوان حل آن را از فحوای بند «۲» ماده (۵۲) پروتکل اول الحاقی استنباط کرد. حال آنکه آنجا که تصرف، خنثی‌سازی یا بی‌اثر کردن[۴] برخی اموال (و بنا به تفاسیر بسیاری از دولت‌ها، یک موقعیت) که می‌تواند مزیتی نظامی دربرداشته باشد، هدفی نظامی تلقی شده است و می‌تواند موضوع حمله واقع شود (Ibid.: 26). بنابراین، از کار انداختن سیستم راداری یا موشکی یک کشور که مزیت نظامی غیرقابل انکاری دارد را به‌صرف اینکه موجب تلفات جانی یا تخریب نشده است را به‌سختی می‌توان حمله‌ای مسلحانه تلقی نکرد به‌گونه‌ای که حق دفاع مشروع را برای دولت زیان‌دیده پدید نیاورد.

در آوریل ۲۰۰۷ تعدادی از تارنماهای مهم کشور استونی مانند تارنمای ریاست جمهوری، پارلمان، وزارتخانه‌ها، احزاب سیاسی، رسانه‌های خبری و دو بانک مهم این کشور مورد حمله از نوع ممانعت از خدمات‌رسانی قرار گرفتند و در این میان، انگشت

---

1. See for, UN General Assembly Resolution 58/199 of 30 January 2004.

۲. برای دیدن رویکردهای متفاوت در ارزیابی مخاصمه مسلحانه، رک.:

Sklerov, Matthew J. (2009). "Solving the Dilemma of State Response to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect their Duty to Prevent", *Military Law Review,* Vol. 201, PP. 54-55.

3. See for Michael Schmitt (2011). "Cyber Operations and the Jus in Bello: Key Issues", *Naval War College International Law Studies*, PP. 5-8.

4. Capture and Neutralization

اتهام متوجه روسیه شد.[۱] این کشور موضوع را به شورای اتحادیه اروپا و ناتو گزارش کرد، اما ناتو این رخداد را به‌عنوان حمله‌ای مسلحانه که بتواند مجوز ورود این سازمان به‌عنوان دفاع مشروع دسته‌جمعی را فراهم آورد قبول نکرد. ناتو اعلام کرد در این برهه زمانی، حملات سایبری را یک کار نظامی مسلم نمی‌شناسد تا ماده (۵) پیمان ناتو درباره دفاع دسته‌جمعی مورد استناد قرار گیرد. این در حالی بود که وزیر دفاع استونی این وضعیت را با ماده (۳) (c) قطعنامه تعریف تجاوز قابل تحلیل می‌دانست که مطابق آن، «محاصره بنادر یا سواحل یک کشور توسط نیروهای نظامی کشوری دیگر» به‌منزله تجاوز قلمداد شده است.[۲] البته گفتنی است براساس ماده (٤١) منشور ملل متحد، «قطع کامل یا جزئی روابط اقتصادی، مواصلاتی و ریلی، دریایی، هوایی، پستی، تلگرافی، رادیویی، و دیگر وسایل ارتباطی» به‌عنوان اقداماتی که متضمن نیروی نظامی نیستند، به‌شمار آمده‌اند.

مایکل اشمیت، این برداشت که حملات سایبری چون متضمن اعمال خشونت نیستند، «حمله»[۳] محسوب نمی‌شوند را رد کرده و می‌گوید «حمله» اصطلاحی توصیفی و اثرمحور است و منظور از «خشونت»[٤] پیامدهای خشونت‌بار است و نه اعمال خشونت‌آمیز (Schmitt, 2002: 377). براساس ماده (۵۱) منشور ملل متحد و حقوق بین‌الملل عرفی، بروز مخاصمه مسلحانه به هر وسیله‌ای (I.C.J., 1996: para. 41)؛ پیش‌شرط استناد به حق دفاع مشروع است (I.C.J., 1986: para. 176)؛ هارولد کوه، مشاور حقوقی وزارت امور خارجه آمریکا، اظهار داشته است حملات سایبری مشمول حقوق مخاصمات مسلحانه بوده و ممکن است باعث وضعیتی شود که مبنای موجهی برای جنگ پدید آورد. به‌زعم وی

---

۱. گفتنی است در جریان حملات سایبری به استونی (۲۰۰۷) و گرجستان (۲۰۰۸)، مقامات روسی حاضر به پذیرش مسئولیت حملات سایبری نشدند و طرف‌های زیان‌دیده نیز نتوانستند مستنداتی حاکی از دخالت مستقیم کرملین یا مأموران یا مأذونین از جانب این کشور را پیدا کنند.

2. See for Johnny Ryan (2007). "Growing Dangers: Emerging and Developing Security Threats", *NATO REV*, Available at: http://www.nato.int/docu/review/2007/issue4/english/ analysis2.html.

3. Attack

4. Violence

قواعد فعلی حقوق بین‌الملل بر فضای سایبر حاکمیت دارند و به انعقاد معاهداتی نیازی نیست که قواعد خاصی بر این قلمرو اعمال کنند. این اولین تحول تکنولوژیک نیست که سؤالاتی را در برابر حقوق بین‌الملل قرار می‌دهد. بنابراین شبکه‌های رایانه‌ای نظامی، اهدافی نظامی هستند که باید در هدف قرار دادن آنها اصولی مانند تفکیک و تناسب مورد ملاحظه قرار گیرد. بر همین اساس، دولت‌ها در قبال اقدامات سایبری که تخلف از هنجارهای بین‌المللی است توسط اشخاصی که تحت کنترل آنها عمل می‌کنند مسئولیت دارند. به عقیده وی، توسل به زور و حمله که می‌تواند موجب دفاع شود، ممکن است با فعالیتی سایبری محقق شود. البته آستانه مشخصی برای میزان شدت یا خسارات پدید آمده برای احراز وضعیت مخاصمه در نظر گرفته نشده است (Perera, 2012).[1]

۳ حملات سایبری و حقوق مخاصمات مسلحانه (حقوق در جنگ)

۳-۱ حمله سایبری به‌عنوان شیوه‌ای جنگی

مبنای حقوق مخاصمات مسلحانه اصل محدودیت توسل به شیوه‌ها و ابزارهای جنگی است و اینکه طرف‌های مخاصمه نمی‌توانند سیاست‌های خود را با سبعیت و اقدامات غیرانسانی پیش برند. درواقع تنها هدف نظامی مشروع در جنگ تضعیف نیروها و قوای نظامی، طرف متخاصم است و نمی‌توان به تسلیحاتی متوسل شد که باعث خسارات یا تلفات بیش از حد انسانی می‌شود[2] و یا پیامدهایی دارد که با هدف یاد شده تناسبی ندارد.[3] هدف حقوق بشردوستانه حمایت از اشخاص، اموال و اماکنی است که با پدیده خانمان‌سوز جنگ دست‌به‌گریبان هستند. ازاین‌رو برای محافظت از مواردی که هدف قرار دادن آنها ضرورت نظامی ندارد، دارای مقرراتی است.

---

1. See for Read Koh's Remarks at: http://www.state.gov/s/l/releases/remarks/197924.htm.
2. See *Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight*, St Petersburg, 1868 ("St Petersburg Declaration").
۳. رک.: مواد (۳۵، ٤٨ و ٥١) پروتکل اول الحاقی.

با توجه به اینکه هدف مشروع در مخاصمه تضعیف و کاستن از توان رزمی طرف مقابل است و نه نابودی آن، حقوق مخاصمات مسلحانه محدودیت‌هایی درباره ابزارها و شیوه‌های جنگی مقرر کرده است و هرگونه اقدامی که از هدف مشروع فراتر رود را قبول نمی‌کند. برای مثال، استفاده از ابزارها و شیوه‌هایی که به درد و رنج نیروهای متخاصم بینجامد مورد منع این مجموعه حقوقی قرار گرفته است (بند «۲» ماده (۳۵) پروتکل اول الحاقی به کنوانسیون‌های ژنو). به‌عنوان یک اصل کلی و بنیادین حقوق بشردوستانه، افراد و اموال غیرنظامی از حملات و خطرهای ناشی از عملیات نظامی مصون هستند (مواد (۵۱ و ۵۲) پروتکل اول الحاقی به کنوانسیون ژنو). تأسیسات زیربنایی کشور اعم از آنکه دولتی باشند یا غیردولتی به‌دلیل کارویژه و دخالت مؤثر آنها در ملزومات زیست‌اجتماعی مشمول حمایت‌اند و از حمله مصون شناخته شده‌اند (مواد (٥٤) پروتکل اول و (١٤) پروتکل دوم الحاقی). نهادهای ملی و اجزای مهم کشور مانند نظام بانکی و اقتصادی، ارتباطات و مخابرات، پایانه‌ها و خطوط مواصلاتی، انرژی، سیستم آبرسانی و خدمات اورژانس نیز از این جمله‌اند. هدف قرار دادن این تأسیسات علاوه‌بر اینکه می‌تواند باعث تلفات و آسیب‌های جانی و مالی مستقیم یا غیرمستقیم شود، می‌تواند با هدف ارعاب مردم نیز انجام شود (Sklerov, 2009: 18-20). به‌هرحال، این مراکز عمدتاً با شبکه‌های رایانه‌ای هدایت می‌شوند که نسبت به حملات سایبری آسیب‌پذیرند.

۲-۳ حمله مسلحانه به‌عنوان ابزاری جنگی

از زمان تدوین مقررات لاهه و ژنو که اصلی‌ترین اسناد حقوق بشردوستانه را تشکیل می‌دهند، مدت‌هاست که می‌گذرد و دنیای فناوری به پیشرفت‌های شگرف و شگفت‌آوری دست پیدا کرده است. عرصه نظامی و تجهیزات دفاعی به‌عنوان یکی از حوزه‌هایی که ارتباط تنگاتنگی با پیشرفت‌های علمی و تکنولوژیک دارد نیز به‌تبع پیشرفت‌های علمی، تغییرات و تحولات بسیاری را تجربه کرده است. هانری دونان در سال ۱۸٦۳ با دوراندیشی این واقعیت

را دریافته بود که جنگ‌های آینده احتمالاً در عین کوتاه شدن بازه زمانی نزاع‌های خون‌بارتری خواهند داشت (Daoust and et al., 2002: 345). ماده (۳۶) پروتکل اول الحاقی به کنوانسیون‌های ژنو[1] به موضوع تسلیحات نوین پرداخته است: «طرف‌های معظم متعاهد در هنگام تحقیق، توسعه، تملک یا در اختیار گرفتن یک سلاح، وسیله یا شیوه جدید جنگی، موظفند تعیین کنند که آیا کاربرد آن در برخی یا در تمامی وضعیت‌ها، مطابق این پروتکل یا سایر قواعد حقوق بین‌الملل قابل اعمال بر آن طرف معظم متعاهد، ممنوع است یا خیر».

با توجه به این ماده دولت‌های متعاهد این سند می‌بایست از این امر که به‌کارگیری تسلیحات، ادوات یا روش‌های جنگی جدید با قواعد حقوقی بشردوستانه مغایرتی نداشته باشد، اطمینان حاصل کنند. البته منظور از واژه «جدید» نسبت به دولت مربوطه است، بدین‌معنا که در زرادخانه‌ها یا راهبردهای نظامی آن کشور جدید باشد که الزاماً با جدیدترین پیشرفت‌های علمی دنیا یکسان نیست (Sandoz and et al., 1987: 425). همچنان‌که از مضمون ماده (۳۶) در پرتو تعهد کلی‌تر ماده (۱) مشترک کنوانسیون‌های چهارگانه ژنو که از تعهد به «رعایت و اطمینان از رعایت» مقررات این کنوانسیون‌ها توسط دولت‌های متعاهد سخن گفته نیز می‌توان برداشت کرد دولت مزبور برای ایفای تعهد خود باید به مقررات لازم‌الاجرای معاهداتی و عرفی حقوق بین‌الملل توجه کند. شایان ذکر است که حتی پیش از تدوین ماده فوق، برخی کشورها تمهیدات و سازوکارهای داخلی برای چنین نظارتی را پیش‌بینی کرده بودند (Daoust and et al., 2002: 348). هرچند متأسفانه پس از تصویب پروتکل اول فقط عده‌ای از کشورها به پیش‌بینی سازوکارهایی برای نظارت یا بازبینی تسلیحات خود پرداختند (Ibid.: 361).

شیوه‌ها و ابزارهای سایبری[2] از مجموعه حقوق بشردوستانه مستثنا نیستند و هرگاه در

---

1. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, 8 June 1977 ("Additional Protocol I").

۲. در برخی نوشته‌ها و اسناد از تعبیر «سلاح اطلاعاتی» (Information Weapons) نیز استفاده شده است رک.:

Draft Information Security Convention (April 2012), Available on the Website of the Russian→

حملات سایبری اصول بنیادین حقوق مخصمات مانند اصل تفکیک، تناسب و ضرورت رعایت نشود، عمل خلافی انجام شده و مسئولیت بین‌المللی را به دنبال خواهد داشت.

۴ ارزیابی بدافزار استاکس‌نت ازمنظر حقوق مخاصمات مسلحانه

حملات سایبری دارای اهداف گوناگونی است که می‌تواند: تهاجمی یا تدافعی باشد. چنین اهدافی می‌تواند ماهیت حمله را تغییر دهد، به‌گونه‌ای که تا ممانعت از خدمات‌رسانی،[1] جاسوسی،[2] اقدامات خراب‌کارانه[3] و حتی وضعیت مخاصمه مسلحانه جلو رود. رویکردهای مختلفی درباره ماهیت حملات سایبری مطرح شده، اما تحت شرایطی حملات سایبری ممکن است به حمله‌ای مسلحانه برسند. بند «۱» ماده (۴۹) پروتکل اول حمله را به «اعمال خشونت علیه طرف مقابل اعم از دفاع یا تهاجم» دانسته است. ازاین‌رو، باید دید که آیا خراب‌کاری در تأسیسات هسته‌ای یک کشور از طریق رایانه‌ای که در حوزه مقررات حقوق مخاصمات مسلحانه قرار دارد، می‌تواند حمله‌ای مسلحانه تلقی شود یا خیر. درصورت مثبت بودن پاسخ، انطباق آن با حقوق بشردوستانه مسئله بعدی خواهد بود.

استاکس‌نت یکی از معروف‌ترین بدافزارهایی[4] است که برای در اختیار گرفتن سیستم کنترلی تأسیسات برنامه‌ریزی شد. در ابتدای سال ۲۰۱۰ یک شرکت امنیت رایانه‌ای در بلاروس این بدافزار را شناسایی و معلوم کرد که هزاران سیستم کنترل صنعتی را در گستره جهانی آلوده کرده است، البته آسیب چشمگیری گزارش نشده است. بنابر یافته‌های کارشناسان، استاکس‌نت به‌گونه‌ای برنامه‌ریزی شد که سیستم‌های کنترل صنعتی ساخت شرکت زیمنس آلمان را مورد هدف قرار دهد.[5] این بدافزار توسط یک حافظه جانبی وارد

←Embassy to the UK, at: http://rusemb.org.uk/policycontact/52.

1. Denial of Service (DOS) Attack and Distributed Denial of Service (DDOS) Attack
2. Espionage
3. Cyber Sabotage

استاکس‌نت نمونه‌ای بارز از این‌گونه حملات سایبری است.

4. Malware

۵. این بدافزار به‌گونه‌ای طراحی شد تا سیستم‌هایی را مورد هدف قرار دهد که دارای قابلیت‌های خاصی هستند. از←

سیستم شده و از خلأها و نقاط آسیب‌پذیر *مایکروسافت* برای اهداف خود بهره گرفته است. انتخاب حافظه جانبی به‌عنوان حامل این بدافزار به این دلیل بوده که بسیاری از سیستم‌های کنترلی به اینترنت متصل نیستند.

مهم‌ترین هدف این بدافزار، تأسیسات و تجهیزات غنی‌سازی اورانیوم ایران بوده است و به‌طور خاص برای هدف قرار دادن دستگاه‌های سانتریفیوژ تأسیسات نطنز برنامه‌ریزی شده بود. استاکس‌نت با در اختیار گرفتن سیستم کنترل سانتریفیوژها و به هم ریختن سطوح کاری این دستگاه‌ها (رساندن به سطح غیرقابل تحمل و کنترل دستگاه) درصدد تخریب و نابودی چرخه غنی‌سازی بود. آثار بدافزار استاکس‌نت به‌گونه‌ای بوده است که نگاه کارشناسان را به فراتر از یک حمله سایبری سوق داده و بسیاری از جمله کارشناسان امنیت ملی آمریکا را بر آن داشته تا استاکس‌نت را زمینه‌ساز جنگ‌های سایبری مورد ارزیابی قرار دهند و حتی عده‌ای از آن به‌عنوان سلاحی با آثار گسترده یاد کرده‌اند (Richardson, 2011: 13). به‌طوری‌که برخی با استناد به گفته مایکل هایدن، رئیس سابق سیا[1] و آژانس اطلاعات ملی،[2] اظهار داشته‌اند که استاکس‌نت، از جمله ابزارهای سایبری است که باعث آثاری فیزیکی می‌شود و همانند یک جنگ سایبری مرزها را طی کرده است (Ibid.: 12-13). ازاین‌رو می‌تواند به‌عنوان حمله‌ای مسلحانه ارزیابی شود (Ibid.: 15-16).[3] این اقدام ازمنظر

←گزارش‌ها و جزئیات فنی می‌توان دریافت که این هدف‌گذاری با توجه به سیستم‌های مورد استفاده در مراکز صنعتی ایرانی یعنی، شبکه‌هایی از رایانه‌های ساخت برخی شرکت‌های خاص و با سرعت پردازش خاص را مورد تهاجم قرار دهد. برای آگاهی بیشتر رک.:

John Richardson (2011). "Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield", PP. 9-11. Electronic Copy Available at: http://ssrn.com/abstract=1892888.

اطلاعات فنی بدافزار استاکس‌نت در پایگاه شرکت امنیتی رایانه‌ای *سیمانتک* در آدرس ذیل قابل دسترسی است:

http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.

1. Central Intelligence Agency (CIA)
2. National Security Agency (NSA)

۳. برای دیدن نظری که استاکس‌نت و به‌طورکلی هیچ‌یک از حملات سایبری که تاکنون رخ داده است را به‌منزله توسل به زور و در حد یک مخاصمه مسلحانه تلقی نمی‌کند، رک.:

Belk, Robert and Noyes (2012). Matthew, *On the Use of Offensive Cyber Capabilities: A Policy Analysis on Offensive US Cyber Policy*, USA: The Office of Naval Research, P. 116.

حقوق مخاصمات مسلحانه یا حقوق جنگ نیز قابل بررسی است. درصورتی‌که این اقدام به‌مثابه توسل به زور تلقی شود، می‌توان آن را ازمنظر اصول و قواعد حقوق بشردوستانه مورد ارزیابی قرار داد.

به‌طورکلی در هر مخاصمه‌ای اصول بنیادین حقوق بشردوستانه‌ای نظیر اصول تفکیک، تناسب، ضرورت نظامی و پرهیز از ایراد رنج غیرضرور باید مدنظر قرار گیرد. براساس اصل تفکیک فقط اهداف نظامی می‌توانند مورد حمله قرار گیرند. اهداف نظامی، اهدافی هستند که به‌دلیل ماهیت، موقعیت، هدف یا کاربری آنها ازنظر نظامی مؤثر بوده و تخریب کلی یا جزئی و توقیف یا بی‌اثر ساختن آنها در زمان حمله مزیتی نظامی به‌شمار می‌آید.[1] مواد (۵۱ و ۵۷) پروتکل اول الحاقی برای حمایت از غیرنظامیان، طرف‌های مخاصمه را به اتخاذ برخی تدابیر احتیاطی موظف دانسته و مقرر کرده که غیرنظامیان نباید مورد هدف مستقیم قرار گیرند و از حملاتی که خسارات جانبی آنها زیاد باشد نیز مصون بمانند.

اگرچه حملات سایبری به‌ندرت تلفات جانی مستقیم دارند، اما به‌طور غیرمستقیم می‌توانند اصول تفکیک و تناسب را خدشه‌دار و متضمن پیامدهای سوء جانی و مالی بسیاری باشند. برای مثال، یک حمله سایبری به شبکه ارتباطی مخابراتی و خطوط تلفنی می‌تواند تماس با مراکز اورژانس و پلیس را قطع کرده و باعث تلفات جانی و مالی شود. بدیهی است که هدف قرار دادن مراکز دارای انرژی‌های خطرناک مانند تأسیسات هسته‌ای یا سدها می‌تواند به‌مراتب آثار زیان‌بارتری داشته باشد. براساس ماده (٥٦) پروتکل اول الحاقی، تأسیسات دارای نیروهای خطرناک مانند سدها، آب‌بندها و نیروگاه‌های برق هسته‌ای درصورتی‌که حمله به آنها منجر به آزاد شدن نیروهای خطرناک و سرانجام ایجاد خسارت زیان‌بار شدید به جمعیت غیرنظامی شود، هرچند اهدافی نظامی باشند از حمله مصون هستند.

---

۱. بند «۲» ماده (۵۲) پروتکل اول الحاقی.

به‌هرحال میان حقوق توسل به زور و حقوق بشردوستانه باید تفکیک قائل شد. ازآنجاکه این دو نظام حقوقی ارتباطی باهم ندارند، ممکن است حمله سایبری ازمنظر حقوق توسل به زور (حقوق بر جنگ) همانند نظام حقوقی عام، عملی خلاف به‌شمار آید، اما الزاماً ناقض حقوق مخاصمات مسلحانه (حقوق در جنگ) به‌منزله نظام حقوقی خاص نباشد. برعکس پیش‌بینی حملات سایبری در چارچوب قواعد حقوق مخاصمات مجوزی برای تخطی از حقوق توسل به زور را فراهم نمی‌آورد. بنابراین حمله سایبری به تأسیسات تولید برق هسته‌ای درصورتی‌که به یک دولت قابل انتساب باشد، هم مغایر با حقوق توسل به زور و هم ناقض حقوق مخاصمات می‌تواند باشد و موجب مسئولیت بین‌المللی آن دولت خواهد بود.

۵ مسئولیت ناشی از حملات سایبری

براساس یک اصل حقوقی، هر عمل متخلفانه یا نقض‌کننده تعهدی متضمن مسئولیت جبران خسارت است. به‌طورکلی برای طرح قواعد مسئولیت بین‌المللی باید سه شرط مقدماتی فراهم باشد[1] اول، نقض یک تعهد بین‌المللی؛[2] دوم، انتساب عمل متخلفانه به یک دولت؛[3] و سوم، نبود عوامل رافع مسئولیت.[4] ماده (۳) طرح مواد درباره مسئولیت بین‌المللی دولت، عمل متخلفانه را شامل فعل یا ترک آن منتسب به دولتی می‌داند که ناقض تعهد بین‌المللی باشد. ازاین‌رو هرگاه این اقدام از جانب نهادها و ارگان‌های یک دولت[5] یا مأموران و یا اشخاصی به نمایندگی از دولت انجام شده باشد،[6] به‌منزله عمل دولت تلقی می‌شود. اما چالش اصلی مسئله انتساب در فضای سایبر است. درواقع هرچند تشخیص مبدأ یا محل انجام حملات سایبری برای متخصصان چندان دشوار نیست، اما این واقعیت نمی‌تواند

1. See for International Law Commission, *Draft Articles on the Responsibility of States for Internationally Wrongful Acts*, U.N. DOC. A/CN.4/L.602/ Rev. 1 (2001).
2. Ibid., Art. 3.
3. Ibid., Art. 5.
4. Ibid., Chapter V.
5. Art. 5 of the ILC Draft Articles.
6. Art. 7 and 8 of the ILC Draft Articles.

موجب انتساب حمله به دولت مبدأ حمله شود؛ زیرا اعمال اشخاص خصوصی به دولت متبوع آنها منتسب نخواهد شد مگر آنکه این موضوع به اثبات برسد.

همچنین به‌موجب اعلامیه اصول حقوق بین‌الملل درباره روابط دوستانه و همکاری میان دولت‌ها مطابق اعلامیه ۱۹۷۰[1] هرگونه مداخله مستقیم یا غیرمستقیم در امور داخلی یا خارجی دولت‌ها به هر دلیلی ممنوع است. بر این اساس، نه تنها تهاجم و مداخله نظامی بلکه «هرگونه مداخله یا تلاش برای متوجه کردن تهدیداتی علیه دولت یا مؤلفه‌های سیاسی، اقتصادی و فرهنگی آن» ازنظر بین‌المللی تخلف است.[2] به‌موجب این اعلامیه که یکی از اصول عرفی حقوق بین‌الملل شناخته می‌شود، «هیچ دولتی نباید از طریق اقتصادی، سیاسی، یا سایر اقدامات برای اجبار دولت دیگر استفاده کرده یا آن را تشویق کند. به این دلیل که اعمال حقوق حاکمیتی آن دولت را کنترل کند یا از مزایای آن به هر صورتی بهرمند شود».[3] ماده (۳۲) منشور حقوق و تکالیف اقتصادی دولت‌ها[4] نیز حاوی مقررات مشابهی است.

براساس آنچه گفته شد، یک حمله سایبری را می‌توان ناقض حقوق بین‌الملل تلقی کرد، هرچند نمی‌توان هر حمله سایبری را یک حمله نظامی تلقی کرد و به حق دفاع مشروع (ماده (۵۱) منشور ملل متحد) استناد کرد. شاید به همین دلیل بود که ناتو در جریان حملات سایبری گسترده‌ای که به استونی شد، به استناد دفاع مشروع دسته‌جمعی وارد عمل نشد. چنان‌که برخی، تصمیم به خودداری از به‌کارگیری ابزارها و حملات سایبری در جریان مخاصمه با لیبی را به سبب خطر رویه‌سازی آن تحلیل کرده‌اند و همین امر، اهمیت اتخاذ چنین راهبردی در دکترین دفاعی را آشکار می‌کند (Belk and Noyes, 2012: 33).

در قضیه استاکس‌نت پیچیدگی به‌اندازه‌ای بود که انگشت اتهام کارشناسان بر انجام

---

1. *Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations*, G.A. Res. 2625, U.N. GAOR, 25th Sess., U.N. Doc. A/Res/2625 (Oct. 24, 1970).
2. Ibid., Preamble, pt. 1.
3. Ibid.
4. General Assembly Resolution 3281 (XXIX) from December 12, 1974. ("The Charter of Economic Rights and Duties of States").

آن ازسوی تعدادی دولت‌ها نشانه رفت. بااین‌حال، هیچ‌کس مسئولیت تهیه یا ارسال این بدافزار را به عهده نگرفت. برخی گزارش‌ها از دخالت مستقیم و مسئولیت ایالات متحده و رژیم صهیونیستی در این اقدام خراب‌کارانه حکایت دارد.[1] گفته می‌شود، بدافزار استاکس‌نت قسمتی از برنامه سایبری آمریکا موسوم به «بازی‌های المپیک»[2] بوده که با موافقت مستقیم رئیس‌جمهور آمریکا انجام شده است (Dunn, 2012). بعد از استاکس‌نت، دو بدافزار دوکو[3] و شعله[4] منتشر شد که اولی بسیار شبیه استاکس‌نت بود. برخی بر این باورند که بدافزار شعله نیز به‌منظور نفوذ و کسب اطلاعات از شبکه‌های رایانه‌ای دولتی ایران و به‌خصوص برای هدف قرار دادن تأسیسات هسته‌ای و نفتی کشور برنامه‌ریزی شده است (Sanger, 2012).

گفتنی است با اعلام برخی اطلاعات درخصوص حملات سایبری دولت آمریکا علیه ایران، دولت اوباما به افشای اسرار دولتی در راستای اهداف انتخاباتی متهم شده و مورد انتقاد شدید برخی مقامات از جمله سناتور مک‌کین قرار گرفت (Dunn, 2012). این قرائن می‌تواند دولت آمریکا را به‌طور جدی در معرض اتهام و انتساب مسئولیت حملات سایبری به ایران قرار دهد.

مسئله اساسی این است که آیا دولتی که مسئول این اقدام بوده، ممنوعیت توسل به زور مطابق بند «۴» ماده (۲) منشور ملل متحد را نقض کرده است و آیا این اقدام به‌مثابه یک «حمله مسلحانه» است به‌طوری‌که موجب استناد به حق دفاع مشروع طبق ماده (۵۱) منشور شود؟

---

1. See for, *e.g.*, "Iran's Nuclear Program", *The New York Times* (Jan. 18, 2011), Available at: <http://topics.nytimes.com/top/news/international/countriesandterritories/iran/nuclear_program/index.html>; Broad, William J., John Markoff and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay", *The New York Times*, Published: January 15, 2011, Available at: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1and
2. Olympic Games
3. Duqu
4. Flame

اگر رویکرد متن‌گرای کلاسیک مبنای تفسیر قرار گیرد، ممکن است استاکس‌نت به‌دلیل عدم ماهیت فیزیکی و اجبار نظامی در این گستره نگنجد. این برداشت از «زور» می‌تواند با ماده (۴۱) منشور تأیید شود که فهرستی از «اقداماتی که متضمن کاربرد نیروی نظامی نیست» را بیان کرده است. اما با اتخاذ رویکردی اثرمحور و غایت‌گرا می‌توان این بدافزار را به‌دلیل هدف قرار دادن تأسیساتی که با امنیت ملی ارتباطی تنگاتنگ دارند و به‌علت مخاطرات قابل مقایسه با اقدامات نظامی مثالی از توسل به‌زور قلمداد کرد (Hollis, 2011). همچنین براساس اصل حقوق بین‌الملل، دولت‌ها مکلف‌اند احتیاطات لازم را در قلمرو خود برای جلوگیری از ارتکاب اعمال مجرمانه علیه دولت دیگر یا مردم آن دولت به‌کار گیرند.[1] در قضیه *کانال کورفو*، دیوان بین‌المللی دادگستری بیان می‌کند که «هر دولتی می‌تواند این را اجازه ندهد که قلمروش برای اعمالی مغایر با حقوق دیگر دولت‌ها به‌کار گرفته شود» (I.C.J., 1949: 22). البته نباید تصور شود که کوتاهی یک دولت از این مراقبت، هرچند عملی متخلفانه است، به معنای انتساب اعمال مورد اهمال به دولت است. چنان‌که دیوان بین‌المللی کیفری برای یوگسلاوی سابق در رأی *تادیچ* مسئولیت دولت میزبان در برابر عوامل و بازیگران غیردولتی را با در نظر گرفتن معیار *کنترل کلی*[2] مطرح کرد (I.C.T.Y. App. Ch., 1999: para. 49).

به‌طور خلاصه، در حقوق عرفی دولت‌ها در کشورشان مکلف‌اند جلو حملات مسلحانه غیردولتی‌ها را علیه دولت دیگر بگیرند. بنابراین دولتی که به پیشگیری از چنین حملاتی قادر باشد، درصورت کوتاهی از انجام تعهد، طبق حقوق بین‌الملل مسئولیت خواهد داشت.[3] البته به‌نظر می‌رسد مسئولیت بین‌المللی ناشی از قصور نسبت به جلوگیری از اعمال

---

1. See for, *S.S. Lotus* (*France v. Turkey*), 1927 P.C.I.J. (ser. A) No. 10, at 88 (Sept. 7, 1927) (Moore, J., Dissenting); *Case Concerning United States Diplomatic and Consular Staff in Tehran*, 1980 I.C.J. Rep. 3, 32–33, 44 (May 24). See also, G.A. Res. 2625, para. 1.

2. Overall Control

۳. در موارد فوق، برخی اقدام نظامی در برابر گروه غیردولتی و در مقام دفاع مشروع را ممکن دانسته‌اند. برای آگاهی بیشتر رک.: ←

متخلفانه عوامل غیردولتی متفاوت از انتساب آن عمل به دولت است. بنابراین دو نوع مسئولیت می‌تواند در آن کار متخلفانه باشد: مسئولیت در ارتکاب که از یک تعهد رفتاری منبعث می‌شود و مسئولیت در عدم جلوگیری که از تعهد رفتاری دیگری ناشی می‌شود. درهرحال، اقدام به دفاع مشروع منوط به احراز حمله‌ای مسلحانه است، در غیر این صورت بنابر یک اصل کلی در حقوق مسئولیت بین‌المللی، دولت‌ها در مواجهه با اعمال متخلفانه بین‌المللی می‌توانند با رعایت شرایطی خاص به اقدامات متقابل روی آورند و ازاین‌رو مانع تجری طرف متخلف و جلوگیری از تداوم عمل متخلفانه شوند.[1]

به‌نظر می‌رسد مشکل اصلی در حوزه حقوق سایبری، نبود قانون نیست، بلکه پیچیدگی‌هایی است که در احراز و تشخیص واقعیت‌ها و امور موضوعی وجود دارد که تعیین آنها پیش‌شرط اعمال قانون و صدور احکام قانونی است (Dunlap, 2011: 81). برای مثال برخی مقررات و اسناد مربوط به فعالیت‌های ماورای جو، هوانوردی و خلع سلاح را درباره جنگ سایبری قابل استناد دانسته‌اند. بااین‌حال مشکلات اجرای مقررات کلاسیک حقوق بین‌الملل برای این پدیده به‌نسبت نوظهور را نباید انکار کرد؛ زیرا انتساب حملات سایبری به یک دولت درصورت عدم پذیرش مسئولیت آن، امری دشوار است.

نظر بیشتر حقوق‌دانان این است که دولت‌ها باید با حملات سایبری همانند یک رفتار مجرمانه برخورد کنند و ارزیابی آنها به‌منزله حملات مسلحانه منوط به شرایطی خاص به‌ویژه انتساب آنها به یک دولت است. چنین رویکردی می‌تواند مشکلات اجرایی به دنبال داشته باشد: اولاً، واکنش صرفاً تدافعی و در پی وقوع یک حمله صورت می‌گیرد و ثانیاً، پیگرد کیفری با دشواری‌های خاصی مانند استرداد مجرمین مواجه است (Sklerov, 2009: 6). ازاین‌رو بسیاری معتقدند که نظام حقوقی موجود، دولت‌ها را نسبت به حملات سایبری در موضعی آسیب‌پذیر قرار می‌دهد. در این شرایط برخی از انعقاد کنوانسیون‌هایی خاص درباره

→Michael Schmitt (2003). "Preemptive Strategies in International Law", 24 *Mich. J. Int'l L.*, at 543. Quoted in: Sklerov, *op.cit*, P. 48.

1. See for I.C.J., *Gabcikovo-Nagymaros Project* (Hung. V. Slovk.), Merits, 1997 I. C. J. Rep., paras. 55–56.

حملات سایبری صحبت می‌کنند. چنانکه در «نشست بین‌المللی مقامات عالی‌رتبه مسئول در حوزه موضوعات امنیتی» که در روسیه برگزار شد، «پیش‌نویس کنوانسیون درباره امنیت بین‌المللی اطلاعات»[۱] منتشر شد.

در مقدمه این سند، امنیت سایبری به‌منزله یکی از مؤلفه‌های اساسی در نظام امنیت بین‌المللی و عاملی مهم در تضمین حقوق و آزادی‌های بنیادین دانسته شده است. بنابراین به‌دلیل ضرورت هماهنگی اقدامات دولت‌ها در فضای سایبر با اصول و هنجارهای پذیرفته شده بین‌المللی و در پیش گرفتن راهبردهای هماهنگ اجرایی و تقنینی در مقابله با اعمال مجرمانه، انعقاد کنوانسیون بین‌المللی پیشنهاد شده است.[۲] درحالی‌که برخی دیگر از تغییر حقوق جنگ دفاع کرده‌اند، به‌گونه‌ای که امکان دفاع پیشگیرانه علیه این حملات حتی بدون احراز انتساب آن به یک دولت را فراهم آورد. از دیدگاه عده‌ای حقوق عرفی واکنش نظامی در برابر حملات گروه‌های غیردولتی را پذیرفته است (Sklerov, 2009: 11-12).[۳]

۶ جمع‌بندی و نتیجه‌گیری

فضای سایبر به‌عنوان بارزترین جلوه عصر ارتباطات و اطلاعات همانند همه دستاوردهای بشری، تهدیدها و فرصت‌های بسیاری را فراروی جوامع بشری قرار داده است. این حوزه هم با اقبال جهانی مردم و کاربران خصوصی روبه‌رو شده و هم مورد توجه فزاینده دولت‌ها

---

1. *Draft Information Security Convention* (April 2012), http://rusemb.org.uk/policycontact/52.

۲. برای مطالعه اسناد مربوط به امنیت سایبری رک.:

UN General Assembly Resolution A/RES/65/41, "Developments in the Field of Information and Telecommunications in the Context of International Security"(8 December 2010); UN General Assembly Resolution A/RES/55/29, "Role of Science and Technology in the Context of International Security and Disarmament"(20 November 2000); UN General Assembly Resolution A/RES/64/211, "Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructures" (21 December 2009).

۳. البته دیوان بین‌المللی دادگستری چنین نظری را نپذیرفته است. برای مثال رک.:

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, 2004, 43 I.L.M. 1009, 1050 (2004).

در جهت خدمات عمومی مانند دولت الکترونیک و حتی نظامی قرار گرفته است. بدیهی است هدف نظام حقوقی سامان دادن به روابط و تمشیت امور جامعه است و هر موضوعی که با حقوق تابعان جامعه مرتبط باشد، مشمول مقررات حقوقی خواهد بود. ازاین‌رو، در نظام حقوقی پویا و کارآمد، قواعد و هنجارهای حقوقی متناسب با موضوعات مورد ابتلای جامعه تفسیر یا اصلاح می‌شوند.

آثار شگرف فضای سایبر و تفاوت ماهوی آن با فضای عینی و مادی که پیش‌تر و بیشتر مورد توجه واضعان مقررات داخلی و بین‌المللی قرار گرفته، ابهامات و تردیدهایی را درخصوص کارآمدی نظام حقوقی کنونی در برابر این پدیده مطرح کرده است که با توجه به رهیافت‌ها و معیارهای ذهنی و عینی حقوق توسل به‌زور و حقوق مخاصمات مسلحانه قابل توصیف است. به‌طوری‌که حمله سایبری به تأسیسات تولید برق هسته‌ای، درصورتی‌که به دولتی قابل انتساب باشد، با حقوق توسل به‌زور مغایرت دارد و همچنین ناقض حقوق مخاصمات است. بااین‌حال، مقررات موجود ممکن است زمینه را برای تفاسیر گوناگون و حتی تفسیر به رأی دولت‌ها فراهم آورد. توصیف حمله مسلحانه و شدت و دامنه آن، توصیف حملات سایبری به‌عنوان حمله‌ای مسلحانه، قلمرو درگیری و نبرد، مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری انجام شده از قلمرو آنها، راه‌های مقابله یا دفاع در برابر حملات سایبری و راه‌های جبران زیان‌دیدگان از مهم‌ترین چالش‌های حملات سایبری است. همچنین در فضای سایبر مسئله انتساب از مشکلات اصلی طرح مسئولیت دولت‌هایی است که حملات سایبری انجام می‌دهند، یا از آن حمایت می‌کنند.

ازاین‌رو تدوین چارچوب کارآمد و مؤثر حقوقی مانند جرم‌انگاری و پیش‌بینی مقررات خاص در حوزه سایبر، هماهنگی مقررات ملی کشورها و همکاری بین‌المللی از طریق انعقاد موافقت‌نامه‌های منطقه‌ای برای مقابله با جرائم یا حملات سایبری، سازوکارهای پیشگیری و پیگیری تخلفات یا حملات سایبری، زیرساخت‌های فناوری برای تشخیص و مقابله با تخلفات یا حملات سایبری (پدافند غیرعامل) از بایسته‌های نظام حقوقی ملی و بین‌المللی کنونی است.

منابع و مآخذ

1. "Computer Network Attack", *HPCR Manual on International Law Applicable to Air and Missile Warfare* (May 15, 2009), http://www.ihlresearch.org/amw/manual/category/section-a-definitions.
2. "Iran's Nuclear Program", *The New York Times* (Jan. 18, 2011), http://topics.nytimes.com/top/news/international/countriesandterritories/iran/nuclear_program/index.html.
3. "Symantec's W32.Stuxnet Report", http://www.symantec.com/security_response/writeup.jsp? docid=2010-071400-3123-99.
4. Belk, Robert and Noyes, Matthew (2012). *On the Use of Offensive Cyber Capabilities: A Policy Analysis on Offensive US Cyber Policy*, USA: The Office of Naval Research.
5. Broad, William J., John Markoff and David E. Sanger (2011). "Israeli Test on Worm Called Crucial in Iran Nuclear Delay", *The New York Times*, Published: January 15, Available at: http://www.nytimes.com/2011/01/16/ world/middleeast/16stuxnet.html?_r=1and.
6. Brown, Gary D. (2011). "Why Iran Didn't Admit Stuxnet Was an Attack", *JFQ*, Issue 63.
7. Daoust, Isabelle, Coupland Robin and Ishoey Rikke (2002). "New Wars, New Weapons? The Obligation of States to Assess the Legality of Means and Methods of Warfare", *International Review of the Red Cross*, No. 846, 30-06-, http://www.icrc.org/eng/assets/files/other/345_364_daoust.pdf.
8. *Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight*, St Petersburg, 1868 ("St Petersburg Declaration").
9. Delibasis, D. (2007). "The Right to National Self-defence: In Information Warfare Operations", *Bury St Edmunds*.
10. Dep't of Def., Office of Gen. Counsel, An Assessment of International Legal Issues, May 1999, *Reprinted in* Thomas Wingfield, The Law of Information Conflict, National Security Law in Cyberspace (2000).
11. *Documents of the United Nations Conference on International Organization*, Vol. VI, 1945.
12. *Draft Information Security Convention* (April 2012), available on the website of the Russian Embassy to the UK, http://rusemb.org.uk/policycontact/52.
13. Dunlap, Charles J. (2011). "Perspectives for Cyber Strategists on Law for Cyberwar"*, Strategic Studies Quarterly*.
14. Dunn, John E. (2012). "Stuxnet Details Leaked to Boost Obama, Alleges McCain", at: http://news.techworld.com/security/3362243/stuxnet-details-leaked-to- boost-obama-alleges-mccain.

15. Exec. Order 13,321, 66 Fed. Reg. 53,063 (Oct. 16, 2001).

16. Exec. Order No. 13,010, 61 Fed. Reg. 37,347 (July 15, 1996).

17. Graham, David E. (2010). "Cyber Threats and the Law of War", 4 *Journal of National Security Law and Policy*.

18. Hildreth, Steven A. (2001). Congressional Research Service Report for Congress No. RL30735, Cyberwarfare 11, http://www.fas.org/irp/crs/RL30735.pdf.

19. Hollis, Duncan, "Could Deploying Stuxnet be a War Crime?", Available at: http://opiniojuris.org/2011/01/25/could-deploying-stuxnet-be-a-war-crime.

20. http://www.state.gov/s/l/releases/remarks/197924.htm.

21. I.C.J., *Case Concerning United States Diplomatic and Consular Staff in Tehran*, 24 May 1980, I.C.J. Rep. 1980.

22. I.C.J., *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania)*, Merits, separate opinion by Judge Alvarez, 1949.

23. I.C.J., *Corfu Channel case* (Merits), 9 Apr. 1949, I.C.J. Rep, 1949.

24. I.C.J., *Gabcikovo-Nagymaros Project* (Hung. V. Slovk.), Merits, 1997 I.C.J. 7.

25. I.C.J., *Gabcikovo-Nagymaros Project* (Hung. V. Slovk.), Merits, I. C. J. Rep. 1997.

26. I.C.J., *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, 2004, 43 I.L.M. 1009, 1050 (2004).

27. I.C.J., *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, ICJ Rep.1996.

28. I.C.J., *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, merits, ICJ Rep.1986.

29. I.C.T.Y., *Prosecutor v. Tadic*, Case No. IT-94-1-A, I.C.T.Y. App. Ch., 1999.

30. ICRC (2008). "How is the Term 'Armed Conflict' Defined in International Humanitarian Law?".

31. International Law Commission, *Addendum-Eighth report on State Responsibility by Mr. Roberto Ago, Special Rapporteur-the Internationally Wrongful act of the State, Source of International responsibility (part 1)*, UN document A/CN.4/318/Add.5–7, 1980.

32. International Law Commission, *Draft Articles on the Responsibility of States for Internationally Wrongful Acts*, U.N. Doc. A/CN.4/L.602/ Rev. 1 (2001).

33. International Law Commission, *Report of the International Law Commission on the Work of its Thirty-second Session, 5 May–25 July 1980, Official Records of the General Assembly, Thirty-fifth Session, Supplement No. 10*, UN document A/35/10, 1980.

34. Johnny Ryan (2007). "Growing Dangers: Emerging and Developing Security Threats", *NATO REV*, http://www.nato.int/docu/review/2007/issue4/ english/analysis2.html.

35. Joint Chiefs of Staff, Joint Publication 1-02, Dep't of Def. Dict. of Military and Assoc'd Terms (12 Apr. 2001). available at: http://www.dtic.mil/doctrine/jel/newoubs/jp102.pdf.

36. Kulesza, Joanna (2009). "State Responsibility for Cyber-attacks on International Peace and Security", *Polish Yearbook of International Law*, Vol. XXIX, Electronic Copy Available at: http://ssrn.com/abstract=1668020.

37. Lopez, C. Todd (2007). Fighting in Cyberspace Means Cyber Dominance, A. F. Print News, http://www.af.mil/news/story.asp?id=123042670.

38. Melzer, Nils (2011). "Cyberwarfare and International Law", *UNIDIR RESOURCES*.

39. P.C.I.J., *S.S. Lotus* (*France v. Turkey*), 1927 P.C.I.J. (ser. A) No. 10. (Sept. 7, 1927) (Moore, J., Dissenting).

40. Perera, David (2012). "Cyber Attacks Subject to International Law, Says State Dept", http://www.fiercegovernmentit.com/story/cyber-attacks-subject-international-law-says-state-dept/2012-09-19?utm_source=rssandutm_medium=rss.

41. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, 8 June 1977 ("Additional Protocol I").

42. Randelzhofer, Albrecht (2002). "Article 2(4)", in Bruno Simma (ed.), *The Charter of the United Nations: A Commentary*, Vol. I.

43. Richardson, John, "Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield", 2011. Electronic copy Available at: http://ssrn.com/abstract=1892888.

44. Roscini, Marco (2010). "World Wide Warfare-Jus ad bellum and the Use of Cyber Force", in Armin Bogdany and Rüdiger Wolfrum (eds.), *Max Planck Yearbook of United Nations Law*, Vol. 14.

45. Sandoz, Y., C. Swinarski and B. Zimmermann (eds) (1987). *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, Martinus Nijhoff, Geneva.

46. Sanger, David E. (2012). "Obama Order Sped Up Wave of Cyberattacks Against Iran", Published: June 1, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=1and_r=3andseid=autoandsmid=tw-nytimestechand.

47. Schaap, Arie J. (2009). "Cyber Warfare Operations: Development and Use Under International Law", U.S. Air Force Academy, Department of Law, at: http://www.thefreelibrary.com/Cyber+warfare+operations%3a+development+and+use+under+international+law.-a0212035712.

48. Schmitt, Michael N. (2002). "Wired Warfare: Computer Network Attack and Jus in Bello", *International Review of the Red Cross*, Vol. 84, No. 846.

49. Schmitt, Michael (1999). "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", *Columbia Journal of Transnational Law*, Vol. 37.

50. Schmitt, Michael (2011). "Cyber Operations and the Jus in Bello: Key Issues", *Naval War College International Law Studies*.

51. Sklerov, Matthew J. (2009). "Solving the Dilemma of State Response to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect their Duty to Prevent", *Military Law Review,* Vol. 201.

52. The United Nations, G. A. (1970). *Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among states in Accordance with the Charter of the United Nations*, G.A. Res. 2625, U.N. GAOR, 25th Sess., Annex, Agenda Item 85, U.N. Doc. A/Res/2625.

53. The White House, *Cyberspace Policy Review*, 16 May 2011.

54. UK government (2010). *"A Strong Britain in an Age of Uncertainty: The National Security Strategy*".

55. UN General Assembly Resolution 2625 (XXV), October 24, 1970.

56. UN General Assembly Resolution 3281 (XXIX), December 12, 1974.

57. UN General Assembly Resolution 3314 (XXIX), U.N. Doc. A/3314, 1974.

58. UN General Assembly Resolution 58/199, 30 January 2004.

59. UN General Assembly Resolution A/RES/55/29, "Role of Science and Technology in the Context of International Security and Disarmament", 20 November 2000.

60. UN General Assembly Resolution A/RES/64/211, "Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructures", 21 December 2009.

61. UN General Assembly Resolution A/RES/65/41, "Developments in the Field of Information and Telecommunications in the Context of International Security", 8 December 2010.

62. US Department of Defense, *The National Military Strategy for Cyberspace Operations*, 2006.

63. Williams, Christopher (2011). "Israeli Security Chief Celebrates Stuxnet Cyber Attack," *The Telegraph*, http://www.telegraph.co.uk/technology/ news/8326274/ Israeli-security-chief-celebrates-Stuxnet-cyber-attack.html.