نشریه‌ی علمی شهر ایمن
JOURNAL OF RESILIENT CITY
(JRC)

الگوهای تدافعی و پیشگیرانه جمهوری اسلامی ایران در مقابله با حملات سایبری با تأکید بر حمله استاکس نت

آرامش شهبازی[1*]؛ غلامرضا جلالی[2]؛ مهران جابری[3]؛

۱- استادیار دانشگاه علامه طباطبایی، تهران، ایران (نویسنده مسئول)
۲- دانشیار دانشگاه عالی دفاع ملی، تهران، ایران
۳- دانشجوی دکترای مدیریت فناوری اطلاعات دانشگاه علامه طباطبایی، تهران، ایران

دریافت دست‌نوشته: ۱۴۰۰/۰۱/۲۰؛ پذیرش دست‌نوشته: ۱۴۰۰/۰۳/۰۱

واژگان کلیدی
استاکس نت
ایران
ایالات متحده آمریکا
جنگ سایبری
تأسیسات هسته ای

چکیده

سالها چنین تصور می شد که استفاده از سلاح‌های هسته ای، عمده ترین تهدید علیه جهان معاصر محسوب می‌شود. با توسل دولت ها به فضای سایبری برای پیشبرد اهداف کوتاه مدت و بلند مدت خویش، برخی، جدی ترین تهدید حال حاضر را سوء استفاده دولتها از گستره عظیم و منعطف فضای سایبری در تحقق اهدافشان تلقی میکنند. با این حال، به نظر می رسد، جدی ترین تهدید دنیای معاصر، در عمل، زمانی محقق می شود که هر دوعامل در یکدیگر قرار گیرد. در این وضعیت، از این طریق می توان جنگی سایبری علیه تأسیسات و پایگاههای هسته ای دولتهای قربانی ترتیب داد و این سناریو ترکیبی، موجب تشدید عوامل خطرآفرین پیشین و شدت مخاطره را چندین برابر می سازد. البته با توجه به فقدان تحقق آستانه جنگ در عمده این موارد، نمی توان به حکومت حقوق بشردوستانه بین المللی امیدوار بود، لکن این نوشته در صدد است تا با تبیین یکی از جدی ترین و بارزترین مثالها در این زمینه، پرونده ویروس استاکس نت، به تحلیل این امر بپردازد که منافع و حقوق دولت قربانی در چنین مواردی به چه نحو قابل احقاق خواهد بود. به این منظور ضمن مفهوم شناسی چنین اقداماتی به حقوق بین الملل حاکم بر وضعیت موصوف پرداخته و امکان دفاع مشروع و عمل متقابل قربانی، به ویژه با ملاحظه مرور زمان را مورد بررسی قرار می دهیم.

۱- مقدمه

از اواخر نیمه دوم قرن بیستم که دسترسی به اینترنت و فضای مجازی رو به فزونی نهاد و از همان زمان که تکنولوژی کاربرد شبکه‌های اطلاعاتی در میان توده مردم رواج یافت، انتظار میرفت در آینده عصر فناوری اطلاعات، سطح دسترسی مخاطبان به اینترنت و کاربرد آن در زندگی روزمره به حدی شایع شود که بدون آن عملا بسیاری از فعالیتهای روزمره مردم قرن بیست و یکم به مخاطره افتاد.

با این حال به جرأت میتوان اذعان داشت که رشد استفاده از شبکه‌های اطلاعاتی منحصر به ضروریات زندگی روزمره نیست؛ بسیاری از اقدامات، اکتشافات و اختراعاتی که توسط سیاستمداران، وکال، پزشکان، منجمین و امثالهم صورت میپذیرد، به اتکاء و استناد به پایگاه ها و داده‌های اطلاعاتی و با کمک نرمافزارهای پیچیده‌ای صورت میگیرد که متخصصین دانش رایانه طراحی و در اختیار کاربران قرار میدهند.

هر چقدر این تحوالت، افق‌های روشنی را در زندگی بشر امروزی فراهم‌آورده، و به همان میزان که دانش حقوق بین‌الملل بواسطه

* نویسنده مسؤل: دانشگاه علامه طباطبایی، تهران، ایران؛ رایانامه: arameshshahbazi@gmail.com

چنین تحوالتی غنی‌تر گردیده است، به همین نحو، چالشهای جدی نیز برخی حوزههای حقوق بینالملل را مورد تهدید قرار دادهاست. لذا اگر در حقوق بین الملل کالسیک تجاوز به قلمرو سرزمینی یک دولت تنها از طریق ادوات و مهمات جنگی و با استفاده از نیروی انسانی مسلح امکانپذیر می‌نمود، امروزه چنین امری با استفاده از هواپیماهای دوربرد بدون سرنشینی که قادرند از رادارهای امنیتی بگذرند یا از طریق زیردریایی‌های پیشرفته‌ای که براحتی گیرندههای امنیتی را در می نوردند، به راحتی امکانپذیر است. اگر پیش از این جرایم سازمان یافته فرامرزی در گردهماییهای باندهای مافیایی هدایت و رهبری، و در محل اجرا میشد، امروزه به راحتی از طریق تکنولوژیهای پیشرفته رایانهای و تنها از طریق چند دستور نرمافزاری، امکان دستکاری در مطالعات کاربران، دسترسی به اطالعات محرمانه و سری، و سوء استفاده از اطالعات بدون نیاز به حضور فیزیکی در محل میسر شدهاست. با اینحال، از آنجا که هر پیشرفتی تنها در پرتو درک الزامات و قلمرو حقوق و تعهدات ذی ربط نتایج قابل قبولی به همراه خواهد داشت، گسترش شبکه اینترنت و دسترسی به اطالعات موجود در این شبکه توسط کاربران در قالب های مختلف، با شناسایی عوامل و مؤلفه هایی که به امنیت استفاده کاربران منتهی میشوند و مانع از ربایش اطالعات یا دستکاری در شبکه با اهدافی غیرقانونی می شوند، خواهد توانست به بهترین نحو پیشرفتهای موجود در این عرصه را با شکوفایی دانش بشری و تسهیل در تبادل ایمن اطالعات قرین سازد.

از این حیث می توان مدعی شد که تحول در برخی مفاهیم حقوق بین الملل کالسیک که بواسطه پیشرفت در زمینه های تکنولوژی و در فضای مجازی صورت میگیرد، زمینهای را جهت طرح برخی پرسشهای کلیدی در حقوق بینالملل معاصر فراهم ساخته است که عمده این پرسشها با محوریت مفهوم »امنیت دولتها در فضای مجازی« مطرح می شوند و به عنوان مباحثی قابل توجه در چشمانداز آتی مسائل اساسی و امنیتی حقوق بینالملل قابل مالحظه و مداقه اند. قرن بیست و یکم سرآغاز تحولی جدی در یکی از چالش برانگیزترین حوزه های حقوق بین الملل یعنی حقوق مخاصمات مسلحانه نیز بوده است. بنابراین دسترسی بشر به اسلحه های جدید، پیشرفت تکنولوژی و توسل به ترفندهای امروزی، باعث شده است تا نه تنها پدیده شوم مخاصمه به کلی از چارچوب حقوق بین الملل رخت برنبندد، که به مدد برخی تحوالت اخیر بر پیچیدگی های آن نیز افزوده گردد. مخاصمه و اشکال مختلف آن که بدواً در حقوق بین الملل سنتی به عنوان یک اصل در روابط بین الدول مورد قبول قرار گرفته بود و در پرتو تحوالت متعاقب توسط اسناد حقوقی مختلف) مانند پیمان بریان کلوگ، میثاق جامعه ملل و منشور ملل متحد(بعنوان یک استثناء در روابط فیمابین دولتها مورد قبول قرار گرفت، با توسعه چشمگیر تکنولوژی بسیار سریعتر از تحول مفهومی در حوزه حقوق و تعهدات حاکم در این بخش متحول گردید. اما عالوه بر این ضرورت توجه به تحول مفهومی مخاصمه در حقوق بینالملل معاصر که عملا از آنجا ناشی میشود که این بحث پیوند وثیقی با مفهوم حاکمیت سرزمینی دولتها پیدا میکند و اتکا بر حاکمیت و اقتدار سرزمینی هر دولت به منزله استواری رکن رکین حکومت است، تحول مفهومی در ماهیت مخاصمه که از توسل به زور با ادوات جنگی به جنگ مجازی با دستکاری و تخریب اطالعات رایانه ای همراه شده، نه تنها مفاهیم و اصول اساسی و بنیادین مخاصمه را دستخوش تغییراتی جدی کرده، که با به چالش کشاندن عناصر و شاکله های مخاصمه در شکل سنتی طرح مباحثی مثل ضرورت تفکیک، مشروعیت و قانونمندی این اقدامات از یکسو و امکان طبقه بندی چنین اقداماتی در قالبهای سنتی تجاوز، دفاع مشروع و توسل به زور را مطرح نمودهاست.

یکی از جدی ترین تهدیدات در فضای سایبری، توسل به بدافزارها، ویروس ها و کرم ها در فضای سایبری به منظور وارد آوردن آسیب به هدف یا قربانی است. سابقه استفاده ازاین بدافزارها به سالها پیش باز می گردد و به مدد توسعه فناوری این روند رو به توسعه است. عدم امکان شناسایی دقیق عامل حمله، باز بودن فضای سایبری و دسترسی راحت بسیاری از بازیگران از جمله دولتها، افراد، شرکتها، فراهم آورندگان سرویسهای اینترنتی بر مخاطرات توسل به حمالت سایبری در این حوزه دامن زده و از طرفی طبقه بندی این قسم از اقدامات در قالب جنگ یا حمله یا عمل تجاوزکارانه و از طرفی راهکارهای حقوقی قربانی از دفاع مشروع، اقدام متقابل و امثالهم را در هاله ای ابهام قرار داده است. دراین مقاله به یکی از جدی ترین کرمهای رایانه ای که صنعت هسته ای ایران را مورد هدف قرار داد، یعنی استاکس نت، به تحلیل راهکارهای حقوقی ایران در حفاظت از منافعش در چنین وضعیتهایی خواهیم پرداخت. به این منظور، نخست به تحلیل مفهومی فضای سایبری، جنگ سایبری و حمله سایبری می پردازیم. آنگاه با تفکیک میان جنگ

سایبری و حمله سایبری، به تحلیل ماهیت اقدام ایاالت متحده و اسرائیل در کاربرد این کرم و واکنشها و راهکارهای حقوقی ایران در مقابل آن خواهیم پرداخت.

۲- بند اول: حدود و ثقور مفاهیم کلیدی

۲-۱- مبحث اول: قلمرو فضای سایبری

برخی فضای سایبری را محیطی که مراودات رایانه ای و در مفهومی ارتباطات دیجیتالی میان کاربران در آن جریان می یابد، می دانند.[۱] به این ترتیب، فضای سایبری به تمامی شبکه های کامپیوتری در سرتاسر جهان و به هر چیزی که مرتبط می شوند یا تحت کنترل دارند، اطالق می شود. با این حال، فضای سایبری به اینترنت محدود نمی شود، بلکه هر آنچه را که ممکن است از طرقی دیگر غیر از شبکه های کامپیوتری ارتباطاتی را برای مخاطبانش به همراه داشته باشد، در بر می گیرد.[۲] در هر حال، روشن است آنچه در قالب فضای سایبری قرار می گیرد، خارج از شبکه ای از ماشینها و دستگاههای کامپیوتری نیست. اما بهره برداری از داده های موجود در این دستگاهها، الزاماً نیازمند استفاده از اینترنت نیست. [۳]

فضای سایبری، قلمروی ماورای مرزهای دولتهاست و این در حالی است که چالشها و اختالفات جامعه بین المللی در زمینه بهره برداری از این فضا، در هر حال در قلمرو مرزهای ملی دولتها صورت می گیرد. معضل زمانی به صورت ویژه خودنمایی می می کند که بدانیم عموماً ارتباطاتی که منجر به تحقق جرایمی در فضای سایبری می شود، توسط شبکه یا شبکه هایی طراحی و هدایت می شود، که گاه برای همیشه مبهم باقی می ماند و یا به نحوی ترکیبی است که امکان رهگیری و رصد کردن آن ناممکن است.[۴]

۲-۲- مبحث دوم: حمله سایرری، جنگ سایرری و معیارهای شناسایی

عموماً دولت های قرن بیست و یکم بر این باورند جنگهای سنتی جای خود را به حملات سایبری داده است که علاوه بر هزینه کمتر از جنگهای متداول، از این طریق قادرند آسیب لازم را به صورت غیر مستقیم به اهداف مورد نظر خود وارد سازند، هرچند در چنین فرضی، خسارات و تبعات ناشی از جنگهای سنتی را متحمل نمی شوند.[۵] هزینه های شروع یک جنگ سایبری معمولاً مشتمل بر هزینه های آموزش و بکارگیری رزمندگان سایبری و خرید نرم افزارها و سخت افزارهای مورد نیاز برای انجام حملات سایبری است، در حالی که در جنگهای سنتی این هزینه به مراتب سنگین تر است. [۶]

با این حال، باید در نظر داشت که یک حملۀ سایبری موفق می تواند سیستم های مهم و حساسی از جمله سیستم های تدافعی یک دولت، سیستم های بیمارستان ها، سیستم های مالی، سیستم های مربوط به حمل و نقل و غیره را مورد هدف خود قرار دهد. حمله سایبری موفق به هر کدام از این سیستم ها می تواند اثرات بسیار مخرب و فاجعه باری را در پی داشته باشد. به عنوان مثال حمله سایبری به شبکه ها و سیستم های مربوط به حمل و نقل می تواند باعث برخورد هواپیماها و یا تصادم بین قطارها شود و یا در مورد حمله سایبری به خدمات آبرسانی نیز می توان گفت این حملات ممکن است باعث باز شدن سدها و جاری شدن آب آنها شوند.[۷] با این حال، بسیاری معتقدند حمله

Brandon Valeriano and Ryan C. Maness. "Cyber War versus Cyber Realities: Cyber Conflict in the International System." (Oxford University Press Scholarship Online, ۲۰۱۵): ۲. Accessed August ۳۰, ۲۰۱۵

[۲] Clarke and Knake (۲۰۱۰: ۷۰) cited in Valeriano, ibid

[۳] در دستگاههایی که به دلائل امنیتی یا غیر از آن، کاربران در فضای غیر از اینترنت فعالیت می کنند، سیستمهای دارای شکاف هوایی گفته می شود. برای مطالعه بیشتر رک: Koppel, ibid, pp. ۴۲-۴۳

[۴] Joel Brenner. Glass Houses: Privacy, Secrecy, and Cyber Insecurity in a Transparent World (Penguin, ۲۰۱۳), p.۲۸.

[۵] Jay P. Kesan, Carol M. Hayes, Mitigative Counterstriking, ibid.

[۶] Susan W. Brenner, Leo L. Clarke, Civilians in Cyberwarfare: Conscripts, Vanderbilt Journal of Transnational Law, Vol. 43: 1011, 2010, p. 1013

[۷] Jay P. Kesan, Carol M. Hayes, Mitigative Counterstriking: Self-Defense and Detterence in Cyberspace, Harvard Journal of Law and Technology, Vol. ۲۵, Number ۲, Spring ۲۰۱۲, p. ۴۴۵

زمانی با مخاطرات جدی و غیرقابل جبران روبروست که علیه زیرساختهای حیاتی کشور به ویژه تأسیسات هسته ای و الکتریکی همراه باشد. [۸]

بهرحال، بطور معمول، از منازعات میان دولتها در فضای سایبری در یک مفهوم وسیع و گسترده تحت عنوان درگیری[۹] یاد می شود. این اصطلاح عام، که با عملیات[۱۰] سنخیت زیادی دارد، به حدی منعطف است که می تواند وضعیتهای مختلفی را در بر گیرد، بی آنکه لزوماً مستلزم توسل به جنگ را به ذهن متبادر سازد. برخی معتقدند این مناسب ترین کاربرد از دیگری در فضا سایبری است، چراکه اساساً معنای مصطلحی که از جنگ به ذهن متبادر می شود، به مخاطره افتادن جان افراد به واسطه حمله ای فیزیکی است، در حالی که ممکن است متعاقب درگیری در فضای سایبری، جان افراد یک مملکت نیز به مخاطره افتد، لکن این امر نتیجه مستقیم و بی واسطه آن نخواهد بود.[۱۱] اقداماتی از این دست که حمله های مبتنی بر محروم سازی از سرویس (*DDOD*) است، معمولاً برای از کار انداختن سرویس *http* به کار میرود که باعث میشود سایتهای روی سرور از دسترس خارج شوند.[۱۲] نمونه دیگری از این قسم، عملیات سرباز برنز در سال ۲۰۰۷ بود که به اختلاف میان استونی و روسیه باز می گشت.[۱۳] با این حال، در عمل همه عملیات های سایبری چندان هم خوش خیم نیستند و برخی مشتمل برتجاوز و حمله ای جدی و سهمگین می باشند. در چنین وضعیت هایی ترپدورها یا تروجانها، نرم افزارهای غیرسایبری هستند که به یک برنامه اضافه می شوند و زمینه ای را برای ورود به شبکه یا برنامه نرم افزاری قربانی فراهم می کنند. البته ممکن است این نرم افزارها تا سالها غیرفعال بمانند یا مخاطره ای به همراه نداشته باشند ولی به محض عملیاتی شدن، می توانند ضربات جدی به ویژه به قربانی به منظور سرقت اطلاعات حساس و محرمانه از پایگاهای اطلاعاتی امن وارد کنند.[۱۴]

حملات سایبری که به آنها حملات شبکه کامپیوتری[۱۵] هم گفته می شود عملیاتی هستند که باعث اختلال[۱۶]، نفی[۱۷]، تنزل[۱۸] و تخریب[۱۹] اطلاعات موجود در کامپیوترها و شبکه های کامپیوتری می شوند. تعریف اراده شدهٔ اخیر مبتنی بر دکترین نظامی امریکا است که این تعریف خود زیر مجموعهٔ عملیات شبکه کامپیوتری است. به عبارت دیگر از نظر دکترین نظامی امریکا عملیات شبکه کامپیوتری سه دسته هستند. دسته اول حملاتی که به شبکه کامپیوتری صورت می گیرد، دسته دوم دفاعیات شبکه های کامپیوتری[۲۰] و دسته سوم سوء استفاده از

[۸] Susan W. Brenner, Leo L. Clarke, Civilians in Cyberwarfare: Conscripts, Vanderbilt Journal of Transnational Law, Vol. ۴۳: ۱۰۱۱, ۲۰۱۰, p. ۱۰۲۸

[۹] conflict

[۱۰] Operation

[۱۱] Valeriano, ibid, p.۱۰

[۱۲] Valeriano, ibid, p.۱-۱۰

[۱۳] در ماه آوریل سال ۲۰۰۷ زیرساخت های الکترونیکی استونی هدف حمله هماهنگ تعدادی از هکرها قرار گرفت، بنا به گزارشات موجود اولین حمله از داخل خاک کشور روسیه صورت گرفته است. مقامات استونی روسیه را به خاطر آغاز این حملات و حمایت از آن مقصر اصلی این حملات میدانستند. به گزارش مقامات روسی این حملات با همکاری سازمان جوانان " نازسی " و با حمایت کرملین صورت گرفته و هیچ حمایتی از جانب مقامات دولتی و ملی دریافت نکرده است. بنا به آخرین بیانیه انتشار یافته از سوی یکی از نزدیک ترین همکاران پوتین، نخست وزیر روسیه میتوان این حملات را به مقامات روسی نسبت داد.

[۱۴] Valeriano, ibid, ۱۰

[۱۵] Computer Network Attacks (CNA)

[۱۶] Disrupt

[۱۷] Deny

[۱۸] Degrade

[۱۹] Destroy

[۲۰] Computer Network Defenses (CND)

داده های شبکه های کامپیوتری[۲۱]که معمولاً شامل جاسوسی است که با ابزاری صورت می گیرد که به سیستم ها نفوذ می کنند و اطلاعات مربوطه را کپی و به طرف متخاصم امکان استفاده غیر مجاز از آن اطلاعات را می دهد.[۲۲]

در خصوص مفهوم و قلمرو جنگ سایبری، دو برداشت مضیق و موسع، قابل تصور است. در مفهوم مضیق، برخی جنگ سایبری را اقدامات انجام شده توسط یک دولت که به منظور نفوذ و یا ایجاد اختلال در کامپیوتر و یا شبکه های رایانه ای دیگر دولت ها صورت میگیرد تعریف کرده اند.[۲۳]برخی نیز جنگ سایبری را حملات و آسیب های دیجیتالی دانسته است که موجب میشود به نظر برسد که سیستم رایانه ای طبیعی عمل میکند در حالی که جواب های مغایر با واقعیت ارائه می دهد.[۲۴]در مفهومی وسیع تر نیز حملات سایبری را عبارت از یک جریان روانشناختی برای بی ثبات کردن جامعه و دولت می دانند که موجب انتشار اطلاعات مضر در سیستم های اجتماعی، سیاسی، معنوی، فرهنگی و اخلاقی به منظور آسیب به امنیت اطلاعاتی میشود.[۲۵] حمله سایبری از نقطه نظر فنی اقداماتی است که برای ایجاد اختلال و در معرض خطر قرار دادن عملکرد شبکه های رایانه ای کشورهای دیگر با اهداف سیاسی و امنیت ملی صورت می پذیرد. حملات سایبری صورت گرفته در دهه اخیر مانند حمله به استونی در سال ۲۰۰۷ و افزایش تعداد نفوذ به زیر ساخت های الکترونیکی ایالات متحده آمریکا حاکی از جاذبه بالا و شدت خطرات احتمالی این دسته جدید از جنگ اطلاعاتی یا حملات سایبری است. در « اقداماتی که از سوی یک دولت برای هدف قرار دادن مجموع می توان این تعریف را از حملات سایبری ارائه نمود زیرساختهای اساسی دولت دیگری از جمله سیستم بانکی، انرژی و حمل و نقل عمومی که به شبکه رایانهای متصل هستند صورت میپذیرد»

در خصوص ارتباط میان جنگ سایبری و حمله سایبری می توان مدعی شد که هر حمله سایبری جنگ سایبری محسوب نمی شود ولی هر جنگ سایبری حمله ای سایبری را دربر دارد. به گفتاری دیگر، حملات سایبری حملاتی هستند که هدفشان تضعیف عملکرد شبکه کامپیوتری هدف مقابل برای اهداف سیاسی یا امنیت ملی است.[۲۶]ولی جنگ سایبری حمله ای سایبری است که اثرات آن می بایستی مشابه با حملهٔ مسلحانه باشد یا حمله می بایستی در چهارچوب یک درگیری مسلحانه به وقوع پیوسته باشد.[۲۷]

در قاعده ۳۰ حمله سایبری عملیات تهاجمی «: راهنمای تالین نیز تعریف دیگری از حملهٔ سایبری آمده است که یا تدافعی است که از آن به طور معقول انتظار ایراد صدمه، یا مرگ اشخاص و یا وارد کردن خسارات به اشیا میرود.[۲۸]حملات سایبری عمدتاً به دو شکل صورت می پذیرند: اول: حملاتی که اطلاعات را هدف

[۲۱]Computer Network Exploitations (CNE)

[۲۲]Sophie Charlotte Pank, What is the Scope of Legal Self-Defense in International Law? Jus Ad Bellum with a Special View to New Frontier for Self-Defense, RETTID ۲۰۱۴, Specialeafhandling ۱۹, pp. ۷, ۸, Available at: http://law.au.dk/fileadmin/Jura/dokumenter/forskning/rettid/Afh_۲۰۱۴/afh۲۰۱۴-۱۹.pdf Visited on March ۲۰۱۶

[۲۳]See More Than Firewalls: Three Challenges to American Cyber Security, Asymmetric Threat (Aug. ۲۰۱۱), available at http://asymmetricthreat.net/docs/ snapshot۲۰۱۱_۰۸.pdf (citing Clarke's definition); Understanding Cyber Warfare

[۲۴]Libicki, Martin C., What is Information Warfare? (Washington, D.C.: National Defense University Press, ۱۹۹۵),p. ۷۷

[۲۵] سید یاسر ضیایی، مونا خلیل زاده، مسئولیت بین المللی دولتها ناشی از حملات سایبری، مجله پژوهشهای حقوقی، شماره ۲۳ ، بهار ۱۳۹۲ ، صفحه -۸۷۱۲۲

[۲۶]Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel, "the law of cyber-attack", California Law Review, Vol. ۱۰۰:۸۱۷, ۲۰۱۲,p.۸۲۶

[۲۷]Ibid, p.۸۳۳

[۲۸]Tallinn Manual on the International Law Applicable to Cyber warfare", Prepared by the International Group of Experts at the Initiative of the NATO Cooperative Cyber Defence Centre of Excellence, General Editor: Michael N. Schmitt, Cambridge University Press, ۲۰۱۳, p. .۱۰۶

قرار می دهند دوم: حملاتی که سیستم های کنترلی را مورد حمله و هدف قرار می دهند. سرقت و تخریب اطلاعات از جمله رایج ترین اشکال حملات در فضای سایبری هستند که به قصد تخریب سرویس های اطلاعاتی صورت می گیرند. از طرف دیگر حملاتی هستند که تمرکزشان بر سیستم های کنترلی است و با قصد از کار انداختن یا دستکاری زیرساخت های فیزیکی طراحی می شوند. برای مثال می توان به حمله علیه شبکه های تأمین کننده برق، خطوط راه آهن یا تأمین کنندگان آب اشاره کرد. این حملات می توانند با استفاده از اینترنت در ارسال برنامه های مخرب یا نفوذ به سیستم های امنیتی مرتبط صورت پذیرد.[۲۹] غلیرغم اینکه حملات سایبری همانند حملات سنتی نیستند ولی می توانند منجر به تخریب های فیزیکی جدی شوند. به عبارت دیگر با توجه به اینکه در حملات سایبری احتمال چنین نتایج مخربی وجود دارد، یک حملهٔ سایبری ممکن است منتهی به یک درگیری مسلحانه شود[۳۰]

همچنین، قاعده ۲۰ راهنمای تالین این موضوع پذیرفته شده را مورد تأکید قرار می دهد که عملیات سایبری که در قالب درگیری های مسلحانه بوقوع می پیوندند موضوع حقوق مربوط به مخاصمات مسلحانه قرار می گیرند فارغ از اینکه آن عملیات توسل به زور محسوب شوند یا خیر. اگر حملات سایبری جنگ محسوب شوند نتیجتاً قواعد حقوق بشردوستانه بین المللی بر آنها اعمال می شود ولی طیف وسیعی از حملات سایبری در چهارچوب جنگ سایبری قرار نمی گیرند و معمولاً بیشتر اینگونه حملات در قالب حملات سایبری معمولی صورت می گیرند.[۳۱]

با وجود اینکه راهنمای تالین آن دسته از حملات سایبری را مورد خطاب قرار می دهد که بیشترین شدت و وخامت را دارند ولی باید به این نکته نیز اذعان نمود که اغلب حملات سایبری که دولت ها با آن روبه رو می شوند به سطح درگیری مسلحانه نمی رسد.[۳۲] جنگ سایبری اقدامی تلقی می گردد که اثرش همانند اثرات حملهٔ مسلحانه باشد. در نتیجه صرفاً تعداد محدودی از حملات سایبری ممکن است منتهی به درگیری های مسلحانه شوند. بیشتر حملات سایبری در چهارچوب بهره برداری های سایبری[۳۳] هستند که طی آن اطلاعات به منظور جاسوسی جمع آوری میشوند[۳۴] و صرفاً می توان گفت اینگونه حملات حداقل می توانند دخالت در امور داخلی دولتها تلقی شوند. اعلامیهٔ اصول حقوق بین الملل در خصوص روابط دوستانه و همکاری میان دولت ها مطابق با منشور ملل متحد مصوب ۲۴ اکتبر ۱۹۷۰ مجمع عمومی که منعکس کنندهٔ حقوق بین الملل عرفی است نیز تأکید بر عدم مداخله دولت ها در امور داخلی دیگر دولت ها دارد.[۳۵]

[۲۹] Murat Dogrul, Adil Aslan, Eyyup Celik, Developing an International Cooperation on Cyber Defense and Deterrence Against Cyber Terrorism, ۳ ۲۰۱۱rd International Conference on Cyber Conflict C. Czosseck, E. Tyugu, T. Wingfield (Eds.) Tallinn, Estonia, ۲۰۱۱, CCD COE Publications, p. ۳۴, Available at: https://ccdcoe.org/ICCC/materials/proceedings/dogrul_aslan_celik.pdf(last visited at ۲۰۱۷/۶/۳۰).

[۳۰] Lesley Swanson, "The Era of Cyber Warfare: Applying International Humanitarian Law to the ۲۰۰۸ Russian-Georgian Cyber Conflict", Loyola of Los Angeles International and Comparative Law Review, Vol. ۳۲:۳۰۳, ۲۰۱۰, p.۳۱۲

[۳۱] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel (n ۱۶) p. ۸۴۰

[۳۲] Wolff Heintschel von Heinegg, The Tallinn Manual and International Cyber Security Law, Yearbook of International Humanitarian Law, Volume ۱۵, ۲۰۱۲, Springer Publications, p. ۴

[۳۳] Cyber Exploitation

[۳۴] Robin Geib, "The legal regulation of cyber-attacks in times of armed conflict", proceedings of the Bruges Colloquium, Technological Challenges for the Humanitarian Legal Framework, ۱۱th Bruges Colloquium, ۲۲-۲۱October ۲۰۱۰, p. ۵۱, available at: https://www.coleurope.eu/sites/default/files/uploads/page/collegium_۴۱_۰.pdf

[۳۵] Declaration on Principles of International Law concerning Friendly Relations and Co-operation among

البته باید توجه داشت که تفکیک انواع مصادیق درگیری در فضای سایبری به حمله و جنگ محدود نمی شود و برخی جرایم سایبری جدی عبارتند از : جاسوسی سایبری، سرقت اموال فکری و سایر اقدامات کیفری دیگری که تهدیداتی جدی و واقعی به تمامی دولتها، شرکتهای خصوصی و افراد وارد می کند.[۳۶] به این ترتیب، باید توجه داشت که به نظر برخی، به ویژه در ارتکاب جنایات در فضای سایبری، ضرورتی به تحقق فعلی در قالب جنگ نیست، بلکه از جمله آثار جدی و سهمگین درگیری های سایبری می توان به سرقت اطلاعات که در بسیاری موارد به جاسوسی منتج می شوند، اشاره کرد.[۳۷]

۳- بند دوم: ممنوعیتها و محدودیتهای جنگ سایبری

در اصل تاکنون هیچ معاهده ای که مستقیماً در زمینه محدودیت یا ممنوعیتهای وارده بر جنگهای سایبری میان دولتها منعقد شده باشد، تدوین نشده است. علاوه بر مقاومت دولتها زمینه ورود ممنوعیتهایی از این دست، چنین ادعا می شود که با توجه به حکومت اصول و قوانین حقوق بشردوستانه بین المللی، نیازی به سند یا اسناد متفاوت و جدیدی در مورد جنگهای سایبری نیست. به علاوه با توجه به فحوای بند ۴ ماده ۲ منشور ملل متحد و امکان تسری مفاد ماده ۳۹ و ۵۱ منشور در زمینه تصمیمات شورای امنیت ملل متحد در زمینه تهدید علیه صلح، نقض صلح و تجازو، اقدام به وضع تعهداتی اضافی برای دولتها در این زمینه ضروری به نظر نمی رسد.[۳۸] البته در فرض احراز آستانه تحقق جنگ سایبری، می توان از تسری مفاده ماده ۵۱ منشور در دفاع مشروع و اتخاذ موضع مناسب از سوی شورای امنیت در مورد وقوع تجاوز، یا تهدید یا نقض صلح سخن میان آورد. در این وضعیت، لازم است تا کلیه اصول و قواعد حاکم بر جنگ به چنین مواردی نیز تسری یابد.[۳۹] در این گونه موارد منطقی تر آن است که به این قضیه بیاندیشیم که دولت قربانی یک جنگ سایبری در مقابل عمل متجاوزکارانه چه پاسخی می تواند داشته باشد و به عبات دیگر، شاید لازم باشد در نهایت به لزوم آمادگی نظامی دولتها در مقابل چنین اقداماتی به جای توجه به اقدامات تدافعی پس از تجاوز متمرکز شویم. [۴۰] بااین حال، مسأله چندان ساده نیست. چرا که اساساً ماهیت یک مخاصمه مسلحانه با حمله سایبری به لحاظ استفاده از تجهیزات و ادوات جنگی، متجاوز و همچنین قربانی و سایر عوامل دخیل در قضیه متفاوت است. از این حیث، به زعم برخی، حتی در صورت تحقق آستانه شدت و حدت خسارت، در عمل نمی توان از حکومت حقوق بشردوستانه بین المللی در چنین وضعیتهایی سخن گفت، این درحالی است که برخی با احراز آستانه جنگ، نظری مغایر دارند.[۴۱]

به هر طریق، مسأله ای که همچنان قابل توجه و تأمل است دشواری و ضرورت تفکیک میان نقش نظامیان وغیر نظامیان در فضای سایبری و در زمان حمله است. در حقوق بشردوستانه بین المللی، تفکیک میان نظامیان و غیرنظامیان از اصول پذیرفت شده و اساسی است و با توجه به عدم امکان اعمال این تفکیک در فضا سایبری، شاید این موضوع قدری مشکل ساز باشد زیرا تفاوت بین نظامیان و غیر نظامیان که مطابق با حقوق بین الملل مورد حمایت قرار می گیرند در فضای سایبری دشوار است.[۴۲] این بحث، خود زمینه طرح ارتش سایبری در فضای سایبری را مطرح می سازد در انطباق با وضعیت جنگهای سنتی می توانند در قالب رزمندگان طبقه بندی شوند.

States in accordance with the Charter of the United Nations, ۲۴ October ۱۹۷۰, A/RES/۲۶۲۵/۲۵

[۳۶] Schmitt, ibid, ۴

[۳۷] Valeriano, ibid, .۷

[۳۸] Dorothy E. Denning, Obstacles and Options for Cyber Arms Control, Georgetown University, Presented at Arms Control in Cyberspace, Heinrich Boll Foundation, Berlin, Germany, June ۲۹, ۳۰, ۲۰۰۱, p. ۷

[۳۹] Dorothy E. Denning, Obstacles and Options for Cyber Arms Control, ibid

[۴۰] Jay P. Kesan, Carol M. Hayes, Mitigative Counterstriking: Self-Defense and Detterence in Cyberspace, Harvard Journal of Law and Technology, Vol. ۲۵, Number ۲, Spring ۲۰۱۲, p. ۴۴۱

[۴۱] Jay P. Kesan, Carol M. Hayes, Mitigative Counterstriking, ibid

[۴۲] Ibid., p. ۴۴۴

۴- بند سوم: ماهیت اقدام به استفاده از کرمهای رایانه ای علیه سایر دولت

بند ۴ ماده ۲ منشور توسل به زور را علیه تمامیت ارضی یا استقلال سیاسی دولت های دیگر ممنوع اعلام نموده این ممنوعیت را با دو استثنا همراه نموده است. زمانیکه شورای امنیت توسل به زور را مجاز بداند و دیگری ماده۵۱ در قالب دفاع مشروع در صورتیکه حملهٔ مسلحانه ای رخ دهد. به عبارت دیگر ماده ۲ توسل به زور را ممنوع اعلام می کند در حالی که ماده ۵۱ توسل به زور را زمانی مجاز قلمداد می کند که در قالب حملهٔ مسلحانه باشد.زیرا همه حملات مسلحانه توسل به زور هستند ولی همه توسل به زورها حمله مسلحانه نیستند.[۴۳]

به عبارت دیگر یک دولت می تواند قربانی نوعی از زور سایبری شود که در فضای سایبری با کاربرد نیروی نظامی همراه نیست. در چنین وضعیتی، عملاً حق دفاع مشروع ماده ۵۱ منشور ملل متحد منتفی می شود ولی دولت قربانی همچنان می تواند از راهکارهای دیگری به منظور خودیاری همچون قطع روابط دیپلماتیک و امثالهم بهره برد.[۴۴]در هر حال، بر اساس معیارهای حقوقی بین المللی در فضای سایبری، یک حمله می تواند در فضای سایبری نیز محقق شود. بند ۱ ماده ۴۹ پروتکل اول الحاقی به کنوانسیون های ژنو، حمله را به معنای اقداماتی خشونت آمیز علیه دشمن[۴۵]یاد می کند. بدین معنا که وقوع حمله بستگی به میزان عواقب خشونت آمیزی دارد که لزوماً ناشی از سلاح های سنتی نمی شود. این معیار که اصطلاحاً معیار مبتنی بر اثر[۴۶]خوانده می شود در مورد فضای سایبری به نحو دیگری در گزارش تالین مورد توجه قرار گرفته است.[۴۷]

در گزارش تالین هفت معیار برای تشخیص آستانه توسل به زور با حملهٔ سایبری پیشنهاد شده است که عبارتند از:

۱- شدت عمل[۴۸]که شامل ایراد صدمهٔ فیزیکی به اشخاص یا اموال است که به تنهایی منجر به استفاده از زور می شود. حملاتی که شدت و وخامت بیشتری دارند و به میزان بیشتری منافع ملی حیاتی دولت های قربانی را تحت تأثیر قرار می دهند مفهوم بیشتر و ملموس تری را از توسل به زور در حملات سایبری ترسیم می کنند.

۲- فوریت عمل[۴۹]بدین معنا که هر چه عواقب حمله زودتر نشان داده شود دولت ها فرصت کمتری برای پیدا کردن روشی مسالمت آمیز برای حل اختلاف دارند.

۳- مستقیم بودن عمل[۵۰]؛ هرچه عواقب ناشی از حملهٔ اولیه ضعیف تر باشد به همان اندازه احتمال اینکه دولت مسؤول در نقض منع توسل به زور شناخته شود کاهش می یابد. در فاکتور فوریت تمرکز بر معیار زمانی عواقب ناشی از حملات است در صورتیکه در معیار مستقیم بودن زنجیره ای از علت و معلول ها مورد بررسی قرار می گیرد.

۴- معیار تهاجم[۵۱]؛ هرچه سیستم های مورد حمله قرار گرفته از امنیت بیشتری برخوردار باشند به همان اندازه نیز اهمیت حملاتشان بیشتر می شود. به عنوان مثال فشار اقتصادی باعث هیچگونه تجاوزی نمی شود درحالیکه در جنگ یک دولت تمامیت سرزمینی دولت دیگر را نقض می کند که فقط در مثال اخیر می توان به این نتیجه رسید که توسل به زور به وقوع پیوسته است. در حملات سایبری این معیار به دقت می بایستی بکار برده شود. اقداماتی از قبیل غیر فعال کردن مکانیزم های

[۴۳] Charles J. Dunlap Jr., Major General, USAF Retired, Perspectives for Cyber Strategists on Law for Cyberwar, Strategic Studies Quartery, Spring ۲۰۱۱, p. ۸۵

[۴۴] Charles J. Dunlap, ibid.

[۴۵] Acts of Violence against an Adversary

[۴۶] Effects-Based Analysis

[۴۷] Charles J. Dunlap Jr., Major General, USAF Retired, Perspectives for Cyber Strategists on Law for Cyberwar, Strategic Studies Quarterly, Spring ۲۰۱۱, p. ۸۵

[۴۸] Severity

[۴۹] Immediacy

[۵۰] Directness

[۵۱] Invasiveness

امنیت سایبری علیرغم خصوصیت تهاجمی اشان توسل به زور محسوب نمی شوند.

۵- قابلیت اندازه گیری[۵۲]: هرچه پیامدهای حمله قابلیت اندازه گیری بیشتری داشته باشند منافع بیشتری از دولت ها تحت تأثیر آن حمله قرار می گیرند. حقوق بین الملل، اجبار اقتصادی را با وجود اینکه باعث ضرر و رنج بسیاری می گردد به عنوان توسل به زور محسوب نمی کند.

۶ . مشروعیت فرضی[۵۳]: در حقوق بین الملل اعمالی که ممنوع اعلام نشده اند مجاز هستند. به عنوان مثال در حقوق بین الملل پذیرفته شده است که توسل به زور جنگ روانی یا جاسوسی را شامل نمی شود. در صورتی که چنین اقداماتی با عملیات سایبری صورت گیرند آنها قانونی تلقی می شوند

۷- مسؤولیت[۵۴]: حقوق مسؤولیت دولت زمانی که دولت مسئول حملات سایبری است قابل اعمال است ولی باید به این نکته نیز توجه کرد که هرچه ارتباط بین دولت و حملات سایبری بیشتر باشد احتمال اینکه دولت های دیگر آن حملات را در قالب توسل به زور تعریف نمایند بیشتر خواهد شد. [۵۵]

دیوان بین المللی دادگستری به صراحت در قضیه نیکاراگوئه اظهار می دارد هرگونه توسل به زوری به حمله مسلحانه تقلیل نمی یابد. مقیاس و آثار حمله ای که به عنوان حمله مسلحانه شناخته می شود، طبعتاً بالاترین مقیاس توسل به زور است. با این حال، صرفاً در وضعیتی که توسل به زور ماهیتاً عملی نظامی باشد، یک دولت می تواند در مقابل به دفاع مشروع متوسل شود. [۵۶]

به این ترتیب به نظر می رسد با اقدامات ذی ربط، به طریق روشنی، خرابکاری صنعتی بین المللی صورت گرفته که این امر نقض حقوق حاکمیتی ایران بر اساس منشور ملل متحد تلقی می شود.

۵- بند چهارم: استفاده از کرم استاکس نت علیه تأسیسات هسته ای ایران

متخصصین امنیت شبکه معتقدند استاکس نت پیچیده ترین تکنولوژی در کاربرد برنامه های مخربی است[۵۷] که تاکنون برای حمله های هدفمند تهیه شده است و هرچند برخی از آن به عنوان ویروس یا بدافزار یاد می کنند، بسیاری آنرا موشک دقیق نظامی سایبری[۵۸] خوانده اند و از آن به عنوان یک بمب سایبری یا قابلیت تخریبی چشمگیر یاد می کنند.[۵۹] که اعتقاد برخی این برنامه با همکاری چندین کشور طراحی شده و نمی توان به طور دقیق مهاجم را شناسایی کرد،[۶۰] شواهدی جدی حاکی از این است که این ویروس اقدامی مشترک از طرف امریکا و اسرائیل است و اساساً به منظور آسیب رساندن به زیرساختهای هسته ای ایران طراحی شده و به همین دلیل هم به عنوان یک سلاح

[۵۲] Measurability

[۵۳] Presumptive Legitimacy

[۵۴] Responsibility

[۵۵] Michael N. Schmitt, Cyber Operations in International Law: The Use of Force, Collective Security, Self Defence, and Armed Conflicts, Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy, ۲۰۱۰, pp. ۱۵۵, .۱۵۶

[۵۶] CASE CONCERNING MILITARY AND PARAMILITARY ACTIVITIES IN AND AGAINST NICARAGUA (Nicaragua v. United States of America) International Court of Justice June ۲۷, ۱۹۸۶ ICJ reports, Para. ۵۳-۵۲

[۵۷] John Richardson, Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield, Journal of Computer and Information Law, Vol. ۲۹, Issue ۱, Fall ۲۰۱۱, P. ۶

[۵۸] precision, Military-grade Cyber Missile

[۵۹] J .Davis, cyber warfare, stuxnet, scada in MoCANA security, ۱۰/۲۱/۹Blog, available at https://www.mocana.com/blog/۲۱/۰۹/۲۰۱۰/malware-turns-out-to-be-serious-cyber-weapon((۲۰۱۷/۶/۲۶

[۶۰] John Richardson, Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield, Journal of Computer and Information Law, Vol. ۲۹, Issue ۱, Fall ۲۰۱۱, P. ۳

آزار جمعی[۶۱]شناخته می شود.[۶۲]بنابر برخی گزارشها، این ویروس توانسته است بالغ بریک هزار سانتریفیوژ موجود در تجهیزات غنی سازی اورانیوم در نطنز را آلوده و مورد حمله قرار دهد.[۶۳]

از آنجاکه استاکس نت یک برنامه کامپیوتری بسیار پیچیده از راه دور است، در قالب یک الگوی نیمه مستقل طراحی شده و این قابلیت را داراست که اهداف تعیین شده را بدون نیاز به اتصال به شبکه اینترنت مورد حمله و هدف خود قرار دهد.[۶۴]به این ترتیب، به محض اینکه ویروس بر روی سیستم قربانی شروع به کار کرد، به سرعت با کامپیوتر سرور از راه دور ارتباط برقرار می کند و می تواند اطلاعات اختصاصی مورد نظر را به سرقت برده و یا اینکه کنترل سیستم را در دست بگیرد.[۶۵]

کرم استاکس نت برای نخستین بار در بلاروس کشف شد، هنگامی که ضمن تحقیقات فنی و کارشناسی در گروه تحقیق و توسعه ای در مینسک، به این کرم برخوردند. شواهد حاکی از این بود که سرورهای حاوی این کرم در مالزی و دانمارک از طریق کارت اعتبار جعلی و با نام تجاری تقلبی به ثبت رسیده اند.[۶۶]گر زمان کشف استاکس نت این کرم توانسته بود ۱۰۰۰۰۰ رایانه در سرتاسر دنیا را به ویروس آلوده کند که ۶۰۰۰۰ دستگاه در ایران، ۱۰۰۰۰ در اندونزی و ۵۰۰۰ دستگاه در هند مستقر بودند.[۶۷]بسیاری معتقدند ویروس اساساً تحولی مدرن در زرادخانه جنگهای مدرن است[۶۸]

نسل بعدی استاکس نت یعنی شعله[۶۹]نیز هرچند مشابهت هایی به برنامه اولیه داشت، با هدفی وسیع تر و دامنه ای حجیم تر طراحی شد که البته به ادعای مقامات دولتی به اندازه استاکس نت آثار تخریبی به همراه نداشته است. در اصل هدف این ویروس راه یابی و جمع آوری اطلاعات از شبکه های کامپیوتری دولت ایران برای هدف قرار دادن تأسیسات هسته ای و نفتی کشور بود.[۷۰]

یکی از مسئولین سازمان انرژی اتمی ایران، همزمان با روند تخریب ویروس اعلام کرد که این ویروس از طریق سی دی ها و سیستمهای حافظه جانبی از طریق متخصصین خارجی[۷۱]به تأسیسات مرکزی وارد شده و در صدد وارد کردن آسیبهای جدی به این تأسیسات بوده است.[۷۲]البته مطابق گزارشهای تکمیلی، راکتور بوشهر تنها هدف نهایی ویروس نبوده است. بلکه[۷۳]این ویروس در صدد بوده تا تأسیسات هسته ای دیگر به

[۶۱] Weapons of Mass Annoyance

[۶۲] John Richardson, Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield, Journal of Computer and Information Law, Vol. ۲۹, Issue ۱, Fall ۲۰۱۱, P. ۸

[۶۳] Jon R. Lindsay, Stuxnet and the Limits of Cyber Warfare, Security Studies, Version: ۱۵January ۲۰۱۳, p. ۱

[۶۴] James P. Farwell, Rafal Rohozinski, Stuxnet and the Future of Cyber War, Survival, ۵۳:۱, p. ۲۴

[۶۵] John Richardson, Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield, Journal of Computer and Information Law, Vol. ۲۹, Issue ۱, Fall ۲۰۱۱, P. ۵

[۶۶] Stark, ibid.

[۶۷] Ibid.

[۶۸] Ibid.

[۶۹] Flame

[۷۰] حسین خلف رضایی، حملات سایبری از منظر حقوق بین الملل)مطالعه موردی: استاکس نت(، فصلنامه مجلس و راهبرد، سال بیستم، شماره ۷۳ ، بهار۱۳۹۲ ، ص. ۱۴

[۷۱] Stuxnet Virus Spread Individuals Said Identified by Iran Official,'' Islamic Republic of Iran Broadcasting, October ۲۰, ۲۰۱۰.

[۷۲] Islamic Republic News Agency, October ۱۶, ۲۰۱۰; ''Bushehr Reactor to Get Main Fuel in Second Week of October,'' Islamic Republic News Agency, October ۵, ۲۰۱۰

[۷۳] Iran Official Points to West's Hand in Computer Worm at Nuclear Plant,'' Islamic Republic of Iran News Network,

جز بوشهر را نیز تخریب و نابود سازد.[۳۴]کارشناسان فنی ایرانی، استدلال کرده اند از آنجاکه استاکس نت به منظور دستکاری و تخریب تجهیزات مورد استفاده در تاسیسات هسته ای و سانتریفیوژها طراحی شده است، هدف دراز مدت این ویروس، تخریب و نابودسازی کلیه فعالیتهای هسته ای ایران است.[۷۵]

ادعاهای مبتنی بر تلاشهای آمریکا و اسرائیل در زمینه خرابکاری در برنامه های سانتریفیوژ ایران[۷۶]نیویورک تایمز در ژانویه ۲۰۰۹ اعلام کرد اینگونه تلاشهای تخریبی شامل تضعیف سیستم های الکتریکی، سیستم های کامپیوتری و دیگر شبکه های مرتبط در ایران و نابودسازی صنعت هسته ای ایران است.[۷۷]

در این قضیه براساس رأی دیوان بین المللی دادگستری در قضیه نیکاراگوئه، روشن است که اسرائیل و امریکا نمی توانند به دفاع مشروع جمعی علیه ایران برای استفاده از استاکس نت استناد کنند. هیچ خطر قریب الوقوعی از سوی ایران به این منظور وجود نداشته است. بنابراین ادعای دفاع مشروع پذیرفته نیست. حتی به سختی می توان این عملیات مستمر و مقطعی را در قالب دفاع مشروع پیشدستانه توجیه کرد.

اقدامات ایران در چرخه سوخت هسته ای، با کاربرد بمب هسته ای متفاوت است و مجموعه اقداماتی که منجر به غنی سازی می شود، به منزله تهدید کاربرد سلاح هسته ای علیه امریکا محسوب نمی شود. مقررات حقوق بین الملل عرفی نیز متضمن هیچگونه قاعده ای نیست که بر اساس آن دولتی بتواند با ارزیابی خود، حقی مبتنی بر دفاع مشروع جمعی را اعمال نماید.[۷۸]حق دفاع مشروع جمعی تنها در صورت وقوع حمله مسلحانه قابل اعمال است. اصطلاح حمله مسلحانه نیز عموماً در وضعیتهایی به کار می رود که یک نتیجه روشن و بارز برای این امر وجود داشته باشد که جان افراد انسانی در معرض مخاطره قرار گرفته است.[۷۹]عملیات استاکس نت بمنظور آسیب رساندن به تولیدات سانتریفیوژهایی است که ایران در تأسیسات هسته ای خود به کار می برد صورت گرفته است. آیا به این ترتیب، می توان اقدام ایالات متحده و اسرائیل را حمله مسلحانه علیه ایران تلقی کرد؟ به این ترتیب، با توجه به فقدان حمله مسلحانه قبلی یا تهدید قریب الوقوع چنین امری از سوی ایران به نظر می رسد که اقدام ایالات متحده و اسرائیل، توسل به دفاع مشروع تلقی نشده، بلکه نقض حقوق بین الملل محسوب می شود

بااین حال، عملیات استاکس نت، بیش از آنچه به عنوان یک حمله مسلحانه تلقی شود، می تواند در قالب یک خرابکاری صنعتی مورد بررسی قرار گیرد. لذا سوالی که مطرح می شود این است که آیا یک عملیات سایبری در اصل می تواند دارای آثار مشابهی چون بروز خسارات فیزیکی در نتیجه کاربرد بمب فیزیکی در جنگهای سنتی داشته باشد؟

پاسخ به ماهیت عملیات سایبری باز می گردد. برخی از این عملیاتها می توانند آثاری مشابه استاکس نت داشته یا شدت و قوت بیشتر یا کمتری داشته باشند، هرچند خسارات فیزیکی ناشی از این اقدامات دقیقاً همانند زمانی نخواهد بود که غیرنظامیان در مخاصمات مسلحانه مورد آسیب قرار می گیرند.

بند پنجم: چگونگی توسل به استاکس نت علیه تأسیسات هسته ای ایران عملیات استاکس نت با استفاده از دو کرم اینترنتی آغاز شد، هر چند این دو کرم به لحاظ تکنیکی با یکدیگر تفاوت داشتند، هدف هر دو تخریب سانتریفیوژهای تأسیسات هسته ای نظنز بود. سانتریفیوژهای این پایگاهها در حال غنی سازی

۲۰۱۰, ۵October

[۳۴] Transmitting Virus to Iran Systems, In Vain- AEOI Chief," Islamic Republic News Agency, September ۲۹, ۲۰۱۰

[۷۵] David Albright and Andrea Stricker, "Stuxnet Worm Targets Automated Systems for Frequency Converters: Are Iranian Centrifuges the Target?" Institute for Science and International Security, November ۱۷, ۲۰۱۰

[۷۶] Islamic Republic of Iran News Network, October ۵, .۲۰۱۰

[۷۷] David E. Sanger, "U.S. Rejected Aid for Israeli Raid on Nuclear Site," New York Times, January ۱۱, ۲۰۰۹

[۷۸] Jeffrey L. Dunoff, Steven D. Ratner, and David Wippman. International Law: Norms, Actors, Process: A Problem-Oriented Approach (New York, NY: Aspen, ۲۰۱۰) p.۸۷۱

[۷۹] Ibid.

اورانیوم بودند. و برخی ادعاها از ارسال این کرم اینترنتی، کنترل دستیابی ایران به ساخت بمب هسته ای بیان شده است.[۸۰]

در اصل شالوده تأسیسات هسته ای نطنز به سانتریفیوژهای نسل آی.آر ۱ باز می گردد که طراحی اروپایی از اواخر دهه ۶۰ و اوائل دهه ۷۰ میلادی است و از سوی عبدالقدیر خان، قاچاقچی تأسیسات هسته ای به سرقت رفته بود. نقاط جدی ضعف و عدم استحکام این تأسیسات که در شرایط تحریمی توسط ایران از طریق پاکستان به دست آمده بود، به ویژه در گزارشهای آژانس بین المللی انرژی اتمی مشهود است. در این گزارش آمده بود این تأسیسات در بهترین شرایط تنها تا نصف میزانی که روی کاغذ کارآیی دارند، در حال بازدهی هستند. به همین دلیل، ایران مجبور بود تا فشار سانتریفیوژ ها را تا میزان قابل ملاحظه ای کم کند و این به معنای ضعف عملکرد و در نتیجه آن بازدهی کمتر سانتریفیوژهاست.[۸۱]

در زمانی که برای نخستین بار از استاکس نت علیه ایران استفاده شد، ایران در حال بهره برداری از نوعی سیستم حفاظتی آبشاری در تأسیسات نطنز بود. سانتریفیوژها از حساسیت فوق العاده ای برخوردار بودند و از آنجا که توازن سانتریفیوژها امری اساسی و تعیین کننده است، در صورتی که یک سانتریفیوژ آسیب ببیند، به سختی بقیه سیستم قادر است به جبران عملکرد سانتریفیوژ دیگر بپردازد یا جایگزین آن شود. اگر این موضوع، به کرات تکرار شود، گاز هگزافلوراید اورانیوم[۸۲]آزاد می شود و این جدی ترین آسیب وارده به تأسیسات غنی سازی اورانیوم محسوب می شود.[۸۳]

هر دو کرمی که به تأسیسات نطنز وارد شدند، اهداف یکسانی داشتند، و البته مستقل از یکدیگر عمل می کردند. هر چند، آسیبهای وارده از استاکس نت در یک مقطع زمانی کشنده و مهلک نبود، استمرار عملکرد باعث از دست رفتن کارآیی و راندمان تأسیسات می شد. بنابراین حمله به تأسیسات هسته ای نطنز از طریق استاکس نت حمله ای از طریق شکاف هوایی بود که با فلش مموری حاوی کرم انتقال یافت و یا زمانی که به عنوان یک بمب عمل کند، خاموش باقی ماند. با این حال، پس از اینکه شروع به کار کرد، تمامی شبکه سخت افزاری نطنز را آلوده کرد.[۸۴]

[۸۰] Zetter, Kim. "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History." Wired Magazine, July ۱۱, ۲۰۱۱. http://www.wired.com/۲۰۱۵/۰۷/۲۰۱۱-how-digital-detectives-deciphered-stuxnet/ (last visited at ۲۰۱۷/۶/۲۷).

[۸۱] Langner, "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve." The Langner Group (۲۰۱۳): ۵-۶.

[۸۲] به کنسانتره جامد اورانیوم که حاصل تغییراتی در سنگ معدن استخراج شده است که کیک زرد گفته می شود. کیک زرد جامد است، به منظور غنی سازی اورانیوم از تکنولوژی بخصوصی بهره برده می شود که نیازمند حالت گازی است. بنابراین کنسانتره اکسید اورانیوم جامد طی فرآیندی شیمیایی به هگزافلوراید اورانیوم (UF۶) تبدیل می شود. هزافلوراید اورانیوم در دمای اتاق جامد است، ولی در دمایی نه چندان بالا به گاز تبدیل می شود.برای آن که UF۶ به دست آمده در مرحله تبدیل، به عنوان سوخت هسته ای مورد استفاده قرار گیرد، باید ایزوتوپ قابل شکافت آن را غنی کرد. البته سطح غنی سازی بسته به کاربرد سوخت هسته ای متفاوت است. برای یک رآکتور آب سبک، سوختی با ۵ درصد اورانیوم ۲۳۵ مورد نیاز است، درحالی که در یک بمب اتمی، سوخت هسته ای باید حداقل ۹۰ درصد غنی شده باشد. غنی سازی با استفاده از یک یا چند روش جداسازی ایزوتوپ های سنگین و سبک صورت می گیرد. در حال حاضر، دو روش رایج برای غنی سازی اورانیوم وجود دارد که عبارتند از انتشار گاز و سانتریفوژ گاز. در روش انتشار گازی)دیفیوژن(، گاز طبیعی UF۶ با فشار بالا از یک سری سدهای انتشاری عبور می کند. این سد ها که غشاهای نیمه تراوا هستند، اتم های سبک تر را با سرعت بیشتری عبور می دهند. در نتیجه UF۶۲۳۵ سریع تر از UF۶۲۳۸ عبور می کند. با تکرار این فرآیند در مراحل مختلف، گازی نهایی به دست می آید که غلظت U۲۳۵ بیشتری دارد. در روش سانتریفوژ گاز، گاز UF۶ را به مخزن هایی استوانه ای تزریق می کنند و گاز را با سرعت بسیار زیادی می چرخانند. نیروی گریز از مرکز موجب می شود Uf۶۲۳۵ که اندکی از UF۶۲۳۸ سبک تر است، از مولکول سنگین تر جدا شود و غنی سازی صورت گیرد. اختلال در این مراحل باعث می شود چرخه غنی سازی به خوبی عمل نکند و کارآیی خود را از دست بدهد..Langner, ibid, p ۹

[۸۳] Langner, ibid, p. ۷.

[۸۴] Langner, Ralph. "Cracking Stuxnet: a ۲۱st-century cyber weapon." TED Talk, ۲۰۱۱

۶- بند ششم: راهکارهای حقوقی ایران در مقابله با استاکس نت

تسلط بر فضای سایبری به عنوان ابزاری جدید در ارزیابی اقتدار دولتها محسوب می شود. استفاده از تکنیکهای سایبری بعنوان ابزار هوشمند علیه سایر دولتها به سال ۱۹۸۰ برمی گردد و استفاده نظامی از این نوع ابزارها به سال ۱۹۹۰ مربوط است. [۸۵] دولت جمهوری اسلامی ایران به عنوان نمونه ای از دولتهایی محسوب می شود که سردمدار فعالیتهای سایبری در بین دولتهای منطقه خلیج فارس و حتی فراتر از آن طبقه بندی می شود.[۸۶]مداخلات خارجی مکرر سایبری به ویژه پس از استفاده از استاکس نت علیه ایران، باعث شد تا در سال ۲۰۱۱ حضرت آیت الله خامنه ای مقام معظم رهبری دستور تاسیس شورای عالی فضای سایبری را به منظور طراحی اقدامات و برنامه های مؤثر در این زمینه صادر کند.[۸۷]بسیاری از مقامات عالیرتبه سپاه نیز ضمن بیان موضع مقتدرانه ایران در مقابل این قسم از حملات اظهار داشته اند ما کشور خودمان را با ابزارهای جدید مجهز ساخته ایم زیرا جنگ سایبری در فضای سایبری خطرناک تر از جنگ فیزیکی بوده و مسئولین ایران بویژه رهبر انقلاب اسلامی همگی به این نکته اشاره داشته اند بنابراین ما آماده جنگهای نرم و فیزیکی هستیم.[۸۸]بااین حال، از آنجاکه سیاست کلی و استراتژی کلان دولت جمهوری اسلامی ایران هرگز بر مبنای تهاجم و تجاوز استوار نبوده، و بر اصل همزیستی مسالمت آمیز و صلح دوستی مبتنی بوده، و البته آبشخوری در اصول مصلحت، حکمت و منفعت دارد،[۸۹]از یک سو مشتمل بر اعمال مغایر با حقوق بین الملل نیست و از سوی دیگر بر موضعی منفعلانه بنا نشده است، از این حیث، اقدام متقابل با رعایت قیودی همچون تناسب، و اقداماتی به منظور پیشگیری از ظهور شکافهای امنیتی در فضای سایبری یا تقویت سازوکارهای دفاعی در مقابل حملاتی به شکافهای هوایی امنیتی را در دستور کار خود قرار می دهد.

عملیات استاکس نت در فاصله زمانی سال ۲۰۰۶ تا ۲۰۱۰ میلادی توسط ایالات متحده و اسرائیل علیه ایران شکل گرفت. در پاسخ، لازم است به مقطع زمانی پس از ۲۰۱۰ مراجعه کنیم. مسأله این است که آیا ایران در حال حاضر، پس از گذشت قریب به یک دهه از توسل آمریکا به این اقدام می تواند در مقام دفاع مشروع برآید یا خیر؟

در عمل مفهوم حاکمیت در قلمرو مرزهای ملی دولتها با فضای سایبری بسیار متفاوت است.[۹۰]به همان اندازه که قلمرو ملی محل تجلی حاکمیت دولت است، فضای سایبری به واسطه ویژگی مرز ناپذیری اش، به موجودیتهایی به غیر از دولت، به ویژه دولتها و سازمانهای غیر دولتی این اجازه را می دهد تا بتوانند از قدرت بیشتری نسبت به دولت برخوردار باشند و بدون

[۸۴] Clifford Stoll's The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage (New York: Doubleday, ۱۹۸۹) details Soviet cyber espionage in the ۱۹۸۰s. U.S. officials have described the use of primitive cyber-attacks against Serbia in the ۱۹۹۰s

[۸۵] IB Times UK, October ۳, ۲۰۱۳, http://iranian.com/posts/view/post/۲۱۹۲۲(last visited at ۲۰۱۷/۳/۰۹).

[۸۷] در متن دستور مورخ ۱۷ / ۱۲ / ۱۳۹۰ آمده است: این شورا وظیفه دارد مرکزی به نام مرکز ملی فضای سایبری کشور ایجاد نماید تا اشراف کامل و به روز نسبت به فضای سایبری در سطح داخلی و جهانی و تصمیمگیری نسبت به نحوه مواجهه فعال و خردمندانه کشور با این موضوع از حیث سختافزاری، نرمافزاری و محتوایی در چارچوب مصوّبات شورای عالی و نظارت بر اجرای دقیق تصمیمات در همه سطوح تحقق یابد. نکات اساسی در مورد وظایف شورای عالی و مرکز ملی فضای سایبری با تأکید بر توجه جدّی به آن، در پیوست این حکم ابلاغ میگردد . برای آگاهی از شرح وظایف و روند امور اجرایی شورا رک: http://majazi.ir/general_content/ visited at ۲۰۱۷/۶/۲۸).

[۸۸] Ahmad Rezaie, "General Araghi: Iran is Ready For Any Hard and Soft Wars," Kabir News, September ۲۵, ۲۰۱۲, http://kabirnews.com/general-araghi-irgc-is-readyfor- any-hard-and-soft-wars/.۳۲۸۷

[۸۹] http://www.yjc.ir/fa/news (last visited at 28/6/2018).

[۹۰] Johan Eriksson and Giampiero Giacomello. "The Information Revolution, Security, and International Relations: (IR) Relevant Theory?" (International Political Science Review ۳, ۲۰۰۶): ۲۲۴. http://www.jstor.org/stable/۲۰۴۴۵۰۵۳. Accessed July ۳۰, .۲۰۱۵

هراس از اعمال حاکمیت دولت، اطلاعات را در فضا سایبری مبادله و در راستای اهداف خود از آن بهره برداری کنند. [۹۱]
در قضیه اقدامات ایالات متحده در استاکس نت، می توان اقدام این اقدام را به عنوان یک عمل تجاوزکارانه با توجه به مفاد قطعنامه تعریف تجاوز مجمع عمومی ملل متحد در سال) ۱۹۷۴ (در نظر گرفت. در بند اول این قطعنامه تجاوز عبارت است از بکار بردن نیروی مسلح توسط یک کشور علیه حاکمیت تمامیت سرزمینی یا « : آمده است استقلال سیاسی کشور دیگر و یا به هر طریق دیگر که با منشور ملل متحد آنچنانکه در این تعریف آمده است تباین داشته باشد. در این تعریف کلمه کشور الف – بدون توجه به مسایل مربوط به شناسایی و یا اینکه کشوری عضو سازمان ملل هست یا نه بکار برده شده است. ب – در صورت اقتضا شامل مفهوم گروهی از کشورها است .
از سوی دیگر در جزء اول بند دوم ماده ۸ مکرر توافق دولتها در اجلاس کامپالا در خصوص مصادیق عمل تجاوزکارانه آمده است: عمل تجاوزکارانه، به معنای استفاده از نیروی مسلح به وسیله یک دولت در مقابل حاکمیت، تمامیت سرزمینی یا استقلال سیاسی دولت دیگر است، یا به هر روش دیگری که ناسازگار با منشور ملل متحد باشد که هر یک از اعمال ذیل، صرف نظر از اعلام جنگ باید مطابق بند ۲۹ قطعنامه ۳۳۱۴ مجمع عمومی ملل متحد به عنوان یک عمل تجاوزکارانه تعیین شود.
هرچند وفاق دولتها در زمینه تعیین مصادیق عمل تجاوزکارانه با توجه به قطعنامه ۳۳۱۴ ازا ین حیث که برخی ملاحظات حقوق بین الملل مدرن از جمله مداخله بازیگران غیردولتی در تجاوز یا عدم توجه به ارتکاب جنایت در فضای سایبری محل انتقاد است، چنین به نظر می رسد که از دستاورد کامپالا نیز می توان به منظور احراز وقوع تجاوز در فضای سایبری بهره برداری کرد.
با توجه به اینکه ایران، ایالات متحده و اسرائیل عضو اساسنامه دیوان کیفری بین المللی نیستند، عملاً گزینه بررسی این قضیه در این مرجع محلی از اعراب ندارد. با این حال، لازم است به اقداماتی که دولت ایران می تواند یا می توانست در مقابل انجام دهد، اشاره کنیم.

۷- مبحث اول: اعمال پیشگیرانه

اعمال پیشگیرانه عبارت است از شناسایی راه های نفوذ وحمله و مقابله با آنها جهت افزایش ضریب امنیت، ایمنی و پایداری ارتباطات در فضای سایبری. از جمله روشهای جلوگیری می توان به موارد ذیل اشاره نمود:
۱ . طراحی ایمن و پایدار سیستم ها: در صورتیکه امنیت جزو معیارها و اصول اولیه و اساسی طراحی سیستم ها، قرار بگیرد، سیستم ها بسیار ایمن تر و پایدارتر از قبل خواهند بود و با حذف یا کاهش حفره های امنیتی، در عمل، ارتباطات سایبری با ایمنی بیشتری در مقابل هکرها و بدافزارها به فعالیت می پردازند.
۲ . متوقف نمودن حملات: از دیگر راه های جلوگیری از حملات می توان به متوقف نمودن آنها اشاره کرد. این روش، تنها با استفاده از تجهیزات پیشرفته امنیتی و وضع قوانین لازم ملی، بدون نقض قوانین و هنجارهای بین المللی، میسر است.

۸- مبحث دوم: اعمال واکنشی

اقدام متقابل از جمله ضمانت اجراهای بین المللی است که به عنوان عملی قانونی اما غیردوستانه دولتی علیه دولت دیگر، به منظور وادار کردن آن دولت به تغییر رفتار یا به عنوان واکنشی در مقابل انجام عمل متخلفانه، مورد قبول و شناسایی قرار گرفته است. [۹۲] با این حال، اقدام متقابل یک اقدام تنبیهی نیست[۹۳]چرا که اساساً دولتها در حقوق بین الملل مجوزی برای تنبیه دولت دیگر در اختیار ندارند. [۹۴]بر اساس ماده ۴۹ طرح مسئولیت بین المللی دولت ناشی از اعمال متخلفانه بین المللی حدود و ثغور اقدام متقابل محدود شده است. بر این اساس اقدام متقابل محدود به رعایت محدوده زمانی معین، اصل تناسب و اتمام اقدام متقابل در صورت عدم تکرار عمل از سوی دولت خاطی است.
حمله سایبری امری غیر قانونی است و حتی در فرضی که با اصل ممنوعیت توسل به زور مغایرتی نداشته باشد، می تواند مصداقی از مداخله در امور داخلی سایر دولتها محسوب شود. به این ترتیب، در خصوص مبادرت به اقدام متقابل در برابر حملات سایبری چنین به

[۹۱] Eriksson and Giacomello, ibid, ۲۲۴

[۹۲] رابرت بلدسو و بوسلاو بوسچک، فرهنگ حقوق بین الملل، ترجمله علیرضا پارسا، ص. ۴۱۷ .

[۹۳] لازم به توضیح است که بر اساس ماده ۳۰ پیش نویس کمیسیون حقوق بین الملل در خصوص مسئولیت) ۱۹۹۶ (، اقدام متقابل نوعی مجازات تلقی میشود، در حالی که بر اساس طرح اخیر ماهیتاً چنین نیست.

[۹۴] James Crawford, The International Law Commission Article on State Responsibility, p. ۳۲۴

نظر می رسد که دولت قربانی بر اساس بند ۱ ماده ۴۹ طرح، می تواند علیه دولتی که به حمله مبادرت ورزیده، به منظور وادار ساختن دولت مذکور به ایفای تعهدات خویش، اقدام به عمل متقابل نماید. با این حال، سوال اینجاست که چه نوع عمل متقابلی در این خصوص قابل تصور است؟

در این قالب، تنها با توسل به اقدامات متقابل با رعایت قید تناسب و قید زمان امکان پذیر است. در ماده ۴۹ طرح مسئولیت بین المللی دولت) ۲۰۰۱ (آمده است: اقدام متقابل منحصراً در راستای حصول هدف مورد نظر صورت می گیرد. یعنی اقدام باید متضمن قابلیت تحقق هدف مشروع باشد. به علاوه هیچ هدف متعارف دیگری برای به دست آوردن هدف مورد نظر قابل پیگیری نباشد، به عبارت دیگر، هیچ اقدام جایگزین دیگری که مشتمل بر محدودیتهای کمتری باشد، موجود نباشد، و نهایتاً برای آنکه اقدام مورد نظر توجیه پذیر باشد، منفعتی که از اقدام حاصل می شود، از آسیب وارده درنتیجه عمل بیشتر باشد، به این ترتیب، خسارتی بیش از هدف مورد نظر به همراه نداشته باشد. همچنین ماده ۵۰ طرح مسئولیت صراحت دارد که عمل اقدام متقابل متضمن رعایت تعهداتی برای دولتهاست: از جمله:

الف- تعهد اجتناب از تهدید یا استفاده از زور، بدان گونه که در منشور ملل متحد مندرج گشته است؛

ب- تعهداتی مبنی بر حفظ حقوق بنیادین بشر؛

ج- در نظر گرفتن تعهدات دارای ویژگی بشردوستانه که اقدامات تلافی جویانه را منع می کند؛

د- ملاحظه سایر تعهدات،به موجب قواعد آمرهٔ حقوق بین الملل عام

همچنین بر همین اساس، کشوری که به اقدام متقابل مبادرت می ورزد،از ایفای تعهداتش در موارد ذیل معاف نمی شود:

الف- تعهداتی که به موجب هر آیین حل و فصل منازعه، میان آن کشور و کشور مسؤول، موجود است.

ب- لزوم به رسمیت شناختن غیرقابل نقض بودن مصونیت نمایندگان ، عرصه و اعیان، بایگانیها و اسناد در روابط دیپلماتیک و کنسولی.

در چنین وضعیتی روشن است که رعایت چنین قیودی با توجه به پیچیدگی و انعطاف قابل ملاحظه فضای سایبری و توسعه روزافزون فناوری که به خلق شکافهای اینترنتی می انجامد این خود زمینه ای را برای فرار از قیود عمل متقابل فراهم می کند، می افزاید، بسیار دشوار خواهد بود. این موضوع زمانی پیچیده تر خواهد شد که دولت قربانی حمله، به واسطه تخریب اطلاعات و داده ها از دسترسی به منابع اطلاعاتی دست اول خود نیز محروم شه باشد و عمل متقابل در این قبیل موارد برای قربانی بسیار دشوار می شود. این امر در جایی حتی ممکن است چنان به درازا بیانجامد که فوریت مندرج در بند ۲ ماده ۵۲ طرح مسئولیت در خصوص لزوم اقدام متقابل فوری مشمول مرور زمان شده و زمان مقتضی برای اقدام متقابل از سوی قربانی از دست برود.[۹۵]به علاوه بر اساس بند ۳ همین ماده در صورتی که عمل متخلفانهٔ بین المللی، متوقف شده باشد، قربانی قادر به اقدام متقابل علیه دولت خاطی نیست ودر صورتی که موضوع مورد اختلاف یا مورد نقض نزد مرجع قضایی یا دیوان داراری صلاحیتی مطرح شده و در حال رسیدگی باشد، توسل به اقدام متقابل، میسر نخواهد بود.

۹- نتیجه گیری

در این مقاله به تحلیل این امر پرداختیم که تجاوز در قالب حقوق جنگ قابل بررسی است. استاکس نت در خلال یک دوره تقریباً ۵ ساله اتفاق افتاد. شاید ایران می توانست در یک مقطع زمانی کوتاه مدت پس از این اقدام مبادرت به پاسخ نماید، با این حال، حتی در فرض دفاع مشروع در قالب ماده ۵۱ ، که به زعم دیوان بین المللی دادگستری و مولف، نیازمند احراز آستانه ای خاص است، امکان دفاع مشروع، با گذشتن بیش از یک دهه از آن در عمل منتفی است.

با این حال، از طرف دیگر، نباید از نظر دور داشت که حملات سایبری در موارد عدیده ای، با توجه به نوع و میزان بدافزار یا ویروسی که مورد استفاده قرار می گیرد، می تواند آثار بسیار مخربی به همراه داشته باشد ولذا شاید تا زمانی که مجموعه ای اصول و قواعد حاکم بر این حوزه، طراحی و مدون نشود، لازم است حملات سایبری به صورت موردی مورد توجه قرار گیرند. بسیاری از حقوقدانان معتقدند توسل به استاکس نت، یک هشدار جدی است. با توسل به استاکس نت، گونه ای جدید از جنگ به ادبیات حقوقی بین المللی افزوده شده است که در فقدان اصول و قواعدی برای حکومت بر این عرصه، لازم است تا با راهکارهایی حقوقی ابواب غلبه مطلق فناوری بر حقوق بسته و به مدد گفتمان متخصصان فنی و حقوقدانان، راهکارهایی برای ضابطه مند کردن آن تعبیه و طراحی شود. لذا در این دورانِ گذار به سمت تنظیم و تدوین قوانین، استناد به قواعد حقوق بین الملل عام، می تواند روابط میان دولتها در فضای سایبری را تحت حدود و ضوابطی ضابطه مند گرداند. البته امر به واسطه ماهیت خاص فضای سایبری در عمل با دشواری هایی جدی روبروست. موضوع این مقاله بطور خاص بر موضوع حملات و جنگهای سایبری منحصر بود. در این زمینه، تسری اصول و قواعد حاکم بر حقوق بشردوستانه بین المللی یا حقوق بین المللی کیفری، بدون توجه به به ماهیت خاص حملات سایبری از جمله بدون مرز بودن این فضا جهت شناسایی مرتکب اصلی و منحصر به فرد حمله، چگونگی اعمال اقدام واکنشی یا تدافعی از عمل متقابل و دفاع مشروع گرفته تا طراحی ایمن و پایدار سیستمها و توقف حمله با رعایت

[۹۵] مونا خلیل زاده، امید شعبانی، میثم اقبالی، جایگاه اقدام متقابل در برابر حملات سایبری از منظر حقوق بین الملل، فصلنامه مطالعات بین المللی پلیس، شماره ۱۷ دوره پنجم، بهار ۱۳۹۳ .ص. ۲۲

استانداردهای فنی لازم، برای اعمال اقدامات تدافعی یا واکنشی کار دشواری است.[۹۶]همین امر در خصوص اقدامات مؤخر دولت ایران درمقابل حمله به تأسیسات هسته ای نظنز قابل توجه است. هرچند، نتوان توسل به کرم استاکس نت را در قالب حمله نظامی در حقوق بین الملل طبقه بندی کرد، به نظر می رسد با معیار قطعنامه تعریف تجاوز می تواند مصداقی از تجاوز غیر نظامی علیه ایارن محسوب شود که البته در این فرض باب دفاع مشروع موضوع ماده ۵۱ منشور بسته خواهد شد. با این حال، در چنین فرضی همچنان امکان توسل به اقدام متقابل با رعایت شروط مندرج در طرح مسئولیت(۲۰۰۱) میسر است. لکن در فرض اخیر نیز، رعایت قیودی مانند تناسب و فوریت محل توجه و تأمل است. به نظر می رسد با گذشت بیش از یک دهه از توسل به استاکس نت علیه ایران، اقدام متقابل با رعایت قید تناسب دراین موضوع منتفی است. از سوی دیگر، البته با توجه به اینکه تبعات برخی از حملات سایبری به ویژه به تأسیسات و ساختارهای حیاتی کشورها می تواند به تهدید علیه صلح و امنیت بین المللی بیانجامد و حتی زمینه ای را برای تأمل در ظرفیتهای مراجع کیفری بین المللی از جمله دیوان کیفری بین المللی برای بررسی وضعیت موجود فراهم سازد، لکن از آنجا که ایران، ایالات متحده و اسرائیل، هیچکدام عضو اساسنامه نیستند، دراین مجال از ورود به جنبه های کیفری بین المللی قضیه اجتناب کردیم.

بی تردید، در آینده ای که رشد و توسعه فناوری به کشف ویروسها و بدافزارهای جدیدتر می انجامد، تسلیح دولتها به اقدامات دفاعی و امنیتی بیشتر، به منظور پرکردن شکافها و حفره های امنیتی در فضای سایبری، از اولویتی حیاتی برخوردار است و البته اقدام متقابل در زمان مقتضی و رعایت تناسب، می تواند راهکاری برای پیشگیری از بروز دیگر اقداماتی از این دست خواهد بود.

[۹۶] ضیایی، ۱۳۹۲ ، ص. ۵۳

۱۰- مراجع

[۱] پاکزاد، بتول، تروریسم مجازی،رساله دکتری حقوق کیفری و جرم شناسی، دانشکده حقوق دانشگاه شهید بهشتی، ۷۹۸۸

[۲] حسن بیگی، حقوق و امنیت درفضای مجازی، موسسه مطالعات و تحقیقات بین المللی ابرار معاصر تهران، چاپ اول، ۷۹۸۴.

[۳] حلمی، نصرت الله، تدوین و توسعه حقوق بین اللمل : مسئولیت بین المللی دولت و حمایت سیاسی، تهران : میزان، چاپ اول، ۷۹۸۱

[۴] فضلی، مهدی، مسئولیت کیفری در فضای مجازی، تهران : خرسندی، چاپ اول، ۷

[5] Benatar Marco, The Use of Cyber Force: Need for Legal Justification?, Goettingen Journal of International Law 1 (2009)

[6] Berkman, S., Boswell, N.Z., Brüner, F.H., Gough, M., McCormick, J.T., Pedersen, P.E., Ugaz, J. and Zimmermann, S. (2008), "The fight against corruption: international organizations at a cross-roads", Journal of Financial Crime, Vol. 15 No. 2

[7] Bradbury Steven G., The Developing Legal Framework for Defensive and Offensive Cyber Operations, 2 Harv. Nat'l Sec. J. 629, 2011

[8] Cilluffo FrankJ, Paul Byron Pattak , George Charles Salmoiraghi Bad Guys and Good Stuff: When and Where Will the Cyber Threats Converge?, 12 DePaul Bus. L.J. 131 1999-2000

[9] Cilluffo FrankJ. & Paul Byron Pattak, Cyber Threats: Ten Issues for Consideration, 1 Geo. J. Int'l Aff. ۴۱ ۲۰۰۰

[10] Elvins,M. (2003), "Europe's response to transnational organised crime", in Edwards,A. and Gill, P. (Eds), Crime: Perspectives on Global Security, Routledge, London.

[11] Ferrer, M. (2009), "Prosecuting extortion victims: how counter-terrorist finance measure executive order 13224 is going to far", Journal of Financial Crime, Vol. 16 No. 3.

[12] Filho, L.A. (2008), "The dynamics of drug-related organized crime and corruption in Brazil from a development perspective", Journal of Financial Crime, Vol. 15 No. 1.

[13] Fisher, J. (2008), "The UK's faster payment project: avoiding a bonanza for cybercrime fraudsters", Journal of Financial Crime, Vol. 15 No. 2.

نشریه‌ی علمی شهر ایمن
JOURNAL OF RESILIENT CITY
(JRC)

Defensive and preventive patterns of the Islamic Republic of Iran against cyber-attacks emphasizing on the Stuxnet attack

Gholamreza Jalali[1]; Aramesh Shahbazi*[2]; Mehran Jaberi[3];

۱- Associate Professor, National Defense University, Tehran, Iran (Corresponding Author)
۲- Assistant Professor, Allameh Tabatabai University, Tehran, Iran
۳- PhD student in Information Technology Management, Allameh Tabatabai University, Tehran, Iran

Abstract:

It was thought for many years that the use of nuclear weapons was the biggest threat against the contemporary world. Concerning governments' resorting to cyberspace to advance their short-term and long-term goals, some consider the most serious current threat to be the governments' abuse of the widespread and flexible concept of cyberspace in order to achieve their goals. However, it seems that the most serious threat of the contemporary world, in practice, is realized when both factors are combined. In this situation, it is possible to organize a cyber war against the nuclear facilities and bases of the victim states, and this combined scenario causes the aggravation of the previous risk factors and multiplies the severity of the risk. Although, due to the lack of realization of the threshold of war in most of the cases, there is no hope for the rule of international humanitarian law, this article intends to analyze how the interests and rights of the victim government can be achieved in such cases by explaining one of the most serious and obvious examples in this field, the Stuxnet virus case. For this, along with the conceptology of such measures, we will address the international laws governing the situation described above and examine the possibility of legitimate defense and reciprocity of the victim, especially considering the passage of time.

Key Words: Stuxnet, Iran, The U.S.A, cyber war, nuclear facilities

* Corresponding author: Tehran, Iran; arameshshahbazi@gmail.com