بررسی تطبیقی و تحلیل تعریف حمله سایبری از منظر دکترین، رویه- کشورها و سازمان‌های بین‌المللی در حقوق بین‌الملل

جبار اصلانی*
امیرحسین رنجبریان**

تاریخ دریافت:۱۳۹۴/۰۵/۲۹ تاریخ پذیرش:۱۳۹۴/۰۷/۱۴

چکیده

رشد فزاینده تکنولوژی در حوزه اطلاعات و ارتباطات، تهدیدهایی نیز به دنبال داشته است که حمله سایبری نمونه بارز چنین تهدیدی محسوب می‌گردد. تبعات چنین حملاتی به حدی جدی است که بازیگران بین‌المللی به ویژه دولت‌ها را جهت اتخاذ رویه‌های مناسب و مواضع سیاسی-حقوقی به تکاپو واداشته است. مهم ترین چالش فراروی این موضوع مسئله مفهوم‌شناسی و تعریف حمله سایبری و لزوم تبیین و تعیین دایره مفهومی این پدیده است که در میان رویه رسمی کشورها و سازمان‌های بین‌المللی به شدت اختلافی است، به طوری که تاکنون هیچ‌گونه اجماعی در خصوص تعریف حمله سایبری حاصل نشده است. پژوهش حاضر با رویکردی تطبیقی به بررسی و تحلیل تعاریف ارائه شده از حمله سایبری از دیدگاه برخی کشورها و سازمان‌های بین‌المللی پرداخته و در نهایت فقدان چنین اجماع حقوقی را در حقوق بین‌الملل به عنوان یک چالش جدی قلمداد کرده است.

کلید واژگان

حمله سایبری، امنیت سایبری، رویه کشورها، سازمان‌های بین‌المللی، عملیات اطلاعاتی.

* دانشجوی دوره دکتری حقوق بین‌الملل دانشگاه تهران.
jabbar968@yahoo.com

**استادیار دانشکده حقوق و علوم سیاسی دانشگاه تهران.
aranjbar@ut.ac.ir

مقدمه

اصطلاح حمله سایبری یا حملات سایبری اخیرا در رسانه‌های جمعی مورد توجه قرار گرفته و به آن پرداخته شده و همگان تا حد زیادی با ادبیات آن آشنایی پیدا کرده‌اند. تقریبا طی یک دهه گذشته تحلیلگران در خصوص تبعات و پیامدهای احتمالی حملات سایبری تأمل کرده و اندیشیده‌اند. سناریوهای مختلفی در رابطه با خسارات فیزیکی یا اقتصادی شدید و بعضا گسترده این حملات وجود دارد که از آن جمله می‌توان به کارکرد ویروسی اشاره کرد که به اسناد مالی یک سیستم اقتصادی حمله کرده یا بازار بورس و اوراق بهادار یک کشور را از کار می‌اندازد[1] و یا با ارسال یک پیام نادرست باعث توقف و از کار افتادن یک راکتور هسته‌ای[2] و یا یک سد آبی[3] می‌گردد و یا حتی با ایجاد اختلال در سیستم کنترل ترافیک هوایی موجب بروز سوانح هوایی و برخورد هواپیماها با یکدیگر می‌شود. با این تفاسیر، تا زمانی که دولت‌ها به تعریف مشخص و روشنی از حمله سایبری که مورد قبول و اقبال جامعه بین‌المللی باشد، نرسند یقینا پرداختن به ابعاد و جوانب پیچیده و متنوع موضوع و ارائه توصیه و پیشنهادات حقوقی و تحلیل آنها برای کارشناسان و حقوق دانان بسیار دشوار خواهد بود. لذا سؤالی که مطرح می‌گردد این است که حمله سایبری چیست، چه ویژگی‌هایی دارد و آیا اساسا هر حمله‌ای را که در فضای سایبر صورت می‌گیرد می‌توان یک نوع حمله به مفهوم سنتی و کلاسیک آن در حقوق بین‌الملل موضوعه[4] قلمداد کرد یا خیر؟ به هر تقدیر تدقیق در ابعاد فنی این مهم پیش‌شرط نیل به تعریفی جامع از

1. Duncan, B.Hollis, Why States Need an International Law for Information Operations, ***11 LEWIS &CLARK L.REV***. 1023 (2007), p 123.
2. Antolin-Jenkins, Vida, (2008), Defining the Parameters of Cyber war Operations: Looking for Law in All the Wrong Places, ***51 NAVAL L. REV. 132***, 140, p 132.
3. Gellman, Barton, (2002), Cyber Attacks by Al Qaeda Feared; Terrorists at Threshold of Using Internet as Tool of Bloodshed: Experts Say, ***WASH. POST***, June 27, at A01.
۴. منظور از حمله در حقوق بین‌الملل موضوعه حدود و آستانه‌ای است که برای تحقق مفهوم حمله در منشور ملل متحد (بند ۴ ماده منشور ملل متحد) و رویه قضایی محاکم بین‌المللی (همانند نظر دیوان بین‌المللی دادگستری در قضیه نیکاراگوئه ۱۹۸۶) در نظر گرفته شده است به طوری که بتوان به مفاد مندرج در ماده ۵۱ منشور ملل متحد جهت اعمال دفاع مشروع و یا فصل ششم و هفتم منشور و نهایتا تحقق مسئولیت بین‌المللی دولت یا سازمان بین‌المللی (طرح مسئولیت بین‌المللی دولت ها ۲۰۰۱ و سازمان‌های بین‌المللی ۲۰۱۱) استناد کرد.

آن خواهد بود. وجود تعریفی جامع و مانع از حمله سایبری که از اقبال عمومی برخوردار باشد، بدون شک برای ادامه راه و تعیین و تشخیص تبعات این نوع از حملات در فضای حقوقی تأثیر مستقیم خواهد داشت. تردیدی نیست که فقدان تعریفی مشخص و جامع‌الاطراف نه تنها مسیر حقوقی پیش‌رو را مبهم می‌نماید، بلکه منجر به نوعی تشتت آراء و تنوع و چندگانگی در تفسیر و رویه عملی و سرانجام نیل به نتایج حقوقی بعضا متناقض خواهد گردید. بنابراین، اهمیت و لزوم وجود یک تعریف معین و قابل قبول دست کم برای شروع موضوع و تبیین، تطبیق و تحلیل آن بسی شایان توجه بوده و پرداختن تفصیلی به آن را ضروری می‌نماید. لازم به ذکر است کهدر پژوهش حاضر ابتدا ماهیت حمله سایبری تبیین شده و سپس تفکیک و دسته‌بندی حملات سایبری مورد بررسی قرار خواهند گرفت و سپس در ادامه تعاریف موجود از نقطه‌نظر صاحب-نظران و سازمان‌های بین‌المللی و منطقه‌ای مورد بررسی و تحلیل قرار می‌گیرند و در پایان مطالب جمع‌بندی خواهند شد.

۱.۲. تعیین ماهیت حمله سایبری

لازم به ذکر است که حملات سایبری در چارچوب گسترده‌تری از آنچه به گونه سنتی عملیات اطلاعاتی نامیده می‌شود، قرار می‌گیرند. عملیات اطلاعاتی(Information Operations)ــ که جنگ اطلاعاتی نیز زیر مجموعه‌ای از آن محسوب شده و به هنگام مخاصمه مسلحانه موضوعیت پیدا می‌کند[1] بکارگیری یکپارچه توانمندی‌های اصلی جنگ الکترونیک، عملیات شبکه‌ای کامپیوتری، عملیات روانی، نیرنگ نظامی و امنیت عملیات هماهنگ با توانمندی–های پشتیبان و مرتبط ویژه و به منظور اثر گذاری، متوقف کردن، تخریب یا ربودن تصمیمات انسانی و ماشینی و نیز پشتیبانی از فرایند های تصمیم گیری نهادهای ملی است[2]. طبق استراتژی نظامی ملی ایالات متحده آمریکا در خصوص عملیات فضای سایبر (۲۰۰۶)، «عملیات شبکه‌ای کامپیوتری»(Computer Network Operations)، شامل «حملات شبکه‌ای کامپیوتری»(Computer Network Attacks)، «دفاع شبکه‌ای کامپیوتری»(Computer Network Defense) و « عملیات امکان پذیر ساختن بهره‌برداری از

1. Schmitt, M.N, (1998-1999), Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, ***Colum. J. Transnat'l L.37***,P 89.
2. United States Department of Defense (DoD), (2006) The National Military Strategy for Cyberspace Operations, p 3; Available at: <www.dod.gov/pubs/foi/ojcs/07-F- 2105doc1.pdf.

شبکه‌های کامپیوتری» (ComputerNetwork Exploitation Enabling Operations) می‌شود. گرچه ازاین کارها در مطبوعات بیشتر تحت عنوان حملات سایبری یاد می‌شود، ولی «عملیات امکان پذیر ساختن بهره برداری از شبکه‌های کامپیوتری» متفاوت از حملات شبکه‌ای و دفاع شبکه‌ای می‌باشد، چون که این نوع از عملیات بیشتر بر گردآوری و تحلیل اطلاعات تمرکز دارد تا قطع شبکه‌ها و چه بسا خود مقدمه یک حمله باشد[1]. این عملیات‌ها می‌تواند با هدف انتشار اطلاعات و با مقاصد تبلیغاتی انجام گیرد؛ برای مثال، با محو وبسایت‌ها و جایگزین کردن محتویات آنها با مطالب دیگر. در حمله‌های سال ۲۰۰۸ به گرجستان، وبسایت‌های ریاست جمهوری، وزارت امور خارجه و بانک ملی گرجستان از میان رفت و مجموعه‌ای از تصویرهای «میخاییل ساکاشویلی» رئیس جمهوری گرجستان در کنار «آدولف هیتلر» در آنها منتشر شد[2]. عملیات امکان‌پذیر ساختن بهره‌برداری، همچنین می‌تواند با هدف سرقت اطلاعات مهم از کامپیوترها انجام گیرد. در این زمینه « دریچه‌های تله‌ای » (Trap Doors) و «ردیاب‌ها » (Sniffers) ابزارهایی سودمند برای جاسوسی سایبری به شمار می‌آید. دریچه تله‌ای به یک کاربر بیرونی امکان می‌دهد در هر زمان به یک نرم افزار دسترسی داشته باشد، بدون آنکه مالک کامپیوتر یا کاربر آن از آن آگاه باشد. ردیاب‌ها، ابزاری برای دزدیدن نام کاربر و کلمه عبور هستند. گرچه در حقوق بین الملل بشر دوستانه (مخاصمات مسلحانه)، جاسوسی به عنوان یک تکنیک نظامی ممنوع نشده است، ولی در سطوح ملی جرم انگاشته می‌شود[3]. با این تفاسیر، «عملیات امکان پذیر ساختن بهره برداری از شبکه‌های کامپیوتری» از چارچوب بررسی و کاوش مفهومی حملات سایبری خارج شده[4] و فقط دو مفهوم مذکور (حملات شبکه‌ای کامپیوتری و

1. Watts, S., (2010), Combatant Status and Computer Network Attack, ***Va.J.Int'l L.50***, P 400.

2. Cooperative Cyber Defense Centre of Excellence (CCDCOE), (2008), Cyber Attacks against Georgia: Legal Lessons Identified, PP.7-8. Available at: < www. carlisle. army. mil /DIME/ documents/ Georgia %201%200. pdf.>

3. Dinstein, Yoram, War, Aggression and Self-Defence, Third Edition, Cambridge University Press, 2001, p 101.

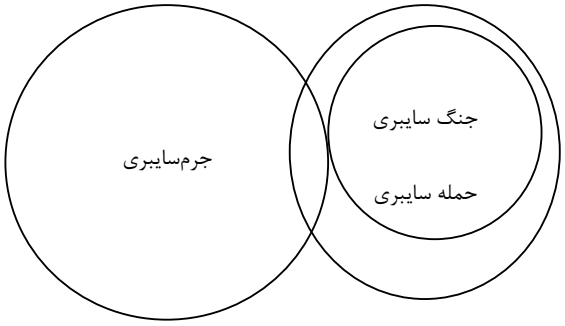
۴. عملیات امکان پذیر ساختن بهره برداری از شبکه‌های کامپیوتری در واقع نوعی شروع به انجام حمله می‌تواند باشد و از این رو، خارج ساختن از دایره مفهومی حمله سایبری منطقی به نظر می‌رسد زیرا، در حمله سایبری یک فعل یا اقدام ایجابی به مرحله عمل رسیده و از حالت بالقوه بودن درآمده است.

دفاع شبکه‌ای کامپیوتری) مدنظر قرار خواهند گرفت و تعاریف ارائـه شـده در ادامـه بـر دایـره و چارچوب مفاهیم دوگانه فوق متمرکز خواهد شد.

۱. لزوم تفکیک میان جرائم سایبری، حملات سایبری و جنگ سایبری

پیش از ورود به بحث تعریف حملات سایبری، ضروری است که تمـایز مفهـومی میـان عنـاوین مجزا و سه‌گانه جرائم سایبری، حملات سایبری و جنگ سایبری تعیین گردند، زیـرا، در پـژوهش حاضر فقط مفهوم حملات سایبری ملاک و معیار عمل است و لـذا پـرداختن بـه مفهـوم جـرائم سایبری در حوزه نظام‌های حقوقی ملی از بعد کیفری و یا پرداختن به مفهوم جنگ‌های سـایبری و امکان اعمال قواعد حقوق بین‌الملل بشر دوستانه بر آن، از ساختار این تحقیق خـارج اسـت. بـا این حال، اشاره مختصر و اجمالی به این مفاهیم و تعیین حدود و ثغور آنها بـرای ادامـه پـژوهش امری ضروری و اجتناب‌ناپذیر بوده و اعمال تفکیک مزبور قطعا از خلط مباحث و انحراف مفهومی جلوگیری می‌کند.

ذکر این نکته ضروری است که حملات سایبری در کلیت خود همگی به قلمرو حقوق بین‌الملل ورود پیدا نکرده و فقط برخی از این نوع حملات در قلمرو و فضای مباحث حقوق بین‌الملل قابلیت طرح و مباحثه دارند؛ از این رو، باید متذکر شد که میان مفاهیم حمله سایبری، جرم سایبری و جنگ سایبری تفاوت وجود دارد. جهت تبیین هر چه بهتر این مسئله می‌توان تفکیک مزبور را در قالب شکل و جدول زیر ترسیم نمود تا به این طریق گستره پژوهش به نحو احسن مشخص گردد:



جدول: تفکیک ماهوی میان حمله سایبری، جنگ سایبری و جرم سایبری

ردیف	ماهیت و ویژگی اقدام سایبری	توصیف نوع اقدام سایبری
۱	اقدامات سایبری که صرفا توسط بازیگران غیردولتی صورت می‌گیرد.	جرم سایبری
۲	اقدام سایبری توسط سیستم کامپیوتری صورت گرفته و صرفا ناقض قوانین کیفری است.	جرم سایبری
۳	هدف حمله سایبری تخریب و ایجاد اختلال در عملکرد شبکه کامپیوتری باشد.	حمله سایبری و جنگ سایبری
۴	حمله باید دارای اهداف سیاسی و یا امنیتی باشد.	حمله سایبری و جنگ سایبری
۵	آثار حمله سایبری همانند یک حمله مسلحانه بوده و یا عمل سایبری در چارچوب یک حمله مسلحانه رخ داده باشد.	جنگ سایبری

همان‌گونه که در جدول و شکل فوق مشخص گردید، تحقیق حاضر درصدد بررسی تطبیقی تعاریف ارائه شده از حملاتی است که مشخصا قلمرو حقوق بین‌الملل را درگیر کرده است و از این رو، به بررسی مصادیقی که داخل در دسته‌بندی جرائم سایبری (حقوق کیفری داخلی) قرار می‌گیرند، نخواهد پرداخت. به این‌ترتیب، حملات سایبری مورد نظر که به حوزه حقوق بین‌الملل ربط پیدا می‌کنند باید از ویژگی‌های مندرج در بندهای ۳ و ۴ جدول فوق برخوردار باشند تا بتوان به بررسی مفهومی آنها از نظرگاه حقوق بین‌الملل معاصر پرداخت. به عبارت دیگر، هدف حمله سایبری باید تخریب و ایجاد اختلال در عملکرد شبکه‌های کامپیوتری هدف باشد و دارای اغراض سیاسی و امنیتی بوده و اینکه آثار حمله به سان یک حمله مسلحانه باشد[1] و یا اینکه

۱. تاکنون و در عرصه عمل هیچ حمله سایبری مشمول تعریف و مفهوم حمله مسلحانه به مفهوم کلاسیک آن نشده است و حداقل هیچ کشور و یا سازمانی چنین ادعایی را مطرح نکرده است. اما در این رابطه مطالعه موسوم به راهنمای تالین، حمله استاکس‌نت به تأسیسات هسته‌ای ایران را مصداق بارز یک حمله و نقض بند ۴ ماده منشور ملل متحد تلقی کرده است. آنچه که واضح است تاکنون هیچ معیار کمی یا کیفی مشخصی برای تلقی کردن حملات سایبری به عنوان حمله مسلحانه تعیین و وضع نشده است و مسئله به‌صورت موردی و در قالب رویه‌ای پیگیری می‌گردد.

حمله سایبری در قالب و چارچوب یک حمله مسلحانه کلاسیک رخ داده باشد[۱]. با این وصف، جستار در شناخت و تبیین تعریف حمله سایبری امری اجتناب‌ناپذیر به نظر می‌رسد که تعیین چارچوب‌های فنی- حقوقی آن لاجرم راهگشای امکان اعمال قواعد و مقررات موجود حقوق بین‌الملل بر این پدیده خواهد بود. به این دلیل پرداختن به تعاریف ارائه شده از سوی صاحب‌نظران (حقوق دانان بین‌المللی و کارشناسان حوزه تکنولوژی اطلاعات) و همچنین مواضع رسمی اعلام شده از سوی دولت‌ها و سازمان‌های بین‌المللی مختلف در قبال تعریف حمله سایبری بسیار مهم می‌باشد. تطبیق و قیاس این تعاریف با یکدیگر بدون شک می‌تواند نشانگر وفاق و یا عدم وفاق در این خصوص باشد.

۲. تعاریف موجود از حمله سایبری

در این قسمت ابتدا نظریه علما، متخصصین و اساتید حقوق بین‌الملل در باب تعریف حملات سایبری مطرح و مورد تجزیه و تحلیل قرار خواهد گرفت و در مرحله بعد، موضع‌گیری و رویه رسمی دولت‌ها در خصوص تعریفی که از حملات سایبری ارائه کرده‌اند مورد بررسی و تحلیل قرار گرفته و پس از آن تعاریفی که برخی سازمان‌های بین‌المللی دولتی و نهادهای مستقل از حمله سایبری ارائه کرده‌اند، مورد کنکاش قرار می‌گیرد. در نهایت سعی بر آن است تا با بررسی جمیع جهات و بهره‌گیری از تعاریف ارائه شده و با توجه به اتفاقات عینی که در ورطه عمل رخ داده است، تعریفی کاربردی و درخور و- حتی‌المقدور- ملموس و بسیار نزدیک به واقعیت این نوع از حملات در دنیای واقعی ارائه گردد. ذکر این نکته پیش از ورود به تعریف ضروری است که حملات سایبری به طور کلی در چارچوب طیف گسترده‌تری از آنچه که موسوم به «عملیات اطلاعاتی» (Information Operations) است قرار می‌گیرد.

۱. نمونه بارز چنین وضعیتی در مخاصمه مسلحانه ۲۰۰۸ بین گرجستان و روسیه اتفاق افتاد که به موجب آن یک شرکت خصوصی طرف دار دولت روسیه اقدام به حمله سایبری علیه کلیه سایت‌های رسمی دولت گرجستان نمود و طی این حمله تمامی سایت‌های رسمی دولت خارج از سرویس شدند. حمله سایبری مزبور در اثنای حمله نظامی کلاسیک به گرجستان و به عنوان یکی از تکنیک های جنگی صورت گرفت، هر چند که دولت روسیه انتساب چنین حملاتی را به خود رسما انکار نمود.

۲.۱. از منظر صاحب‌نظران و متخصصین

تعاریف مختلفی از حمله سایبری از سوی صاحب‌نظران در هر دو بخش حقوقی و فنی صورت گرفته است که اهم آنها به شرح ذیل می‌باشند:

الف) نخست می‌توان به تعریفی که «ریچارد کلارک»ـ کارشناس امنیت ملی دولت ایالات متحده آمریکا– ارائه کرده است، اشاره کرد. وی حمله سایبری را این گونه تعریف می‌کند:

«اقداماتی است که توسط کشورها برای نفوذ در کامپیوترها یا شبکه‌های کامپیوتری کشور یا کشورهای دیگر به منظور ورود (ایراد) خسارت یا ایجاد اختلال انجام می‌شود»[1].

در تحلیل و به عبارتی نقد این تعریف می‌توان گفت که سه عنصر یعنی عامل حمله، هدف و قصد از انجام حمله ملاک قرار داده شده است، بدون اینکه انحاء و اشکال ایجاد اختلال مورد توجه قرار گرفته باشد. علاوه بر این، در خصوص عامل حمله، فقط از کشورها به طور عام نام برده شده است، که با این وصف اگر حمله‌ای در چارچوب و قلمرو جغرافیایی تحت کنترل و صلاحیت یک کشور (فضای سایبرو شبکه‌های تحت کنترل کشورها) توسط افراد و گروه‌های غیردولتی و خصوصی علیه کشور ثالثی انجام بپذیرد، اصولاً: از دایره تعریف یاد شده خارج خواهد شد و آنها را در بر نخواهد گرفت و به این صورت باید شاهد نوعی خلأ در پوشش حقوقی این دست از حملات بود. با این وضعیت می‌توان گفت تعریف مذکور تا حد زیادی ناقص بوده و بخش مهمی از حملات را توسط گروه‌های خصوصی و غیردولتی انجام می‌گیرند، در بر نمی‌گیرد و منجر به ایجاد خلاء خواهد شد.

ب) تعریف دوم از حمله سایبری توسط «مایکل هایدن»ـ رئیس سابق سازمان امنیت ملی آمریکاـ ارائه شده است. نامبرده حمله سایبری را این گونه تعریف کرده است:

«هرگونه تلاش عامدانه برای ایجاد اختلال یا از بین بردن شبکه‌های کامپیوتری کشور دیگر»[2].

1. Clarke, Richard A. & Knake, Robert K, (2010), Cyber War: The Next Threat to National Security and What to Do about It, p 6.
2. Gjelten, Tom, (2010), Extending the Law of War to Cyberspace, NAT'L PUB. RADIO. Available at: http://www.npr.org/templates/story/story.php?storyId=130023318 (last visited Apr. 18, 2012).

همان‌گونه که پیدا است تعریف یاد شده نیز بسیار کلی بوده و هیچ تفکیکی میان جرم سایبری، حمله سایبری و جنگ سایبری قائل نشده است و مرز میان تشخیص آنها را در هاله‌ای از ابهام قرار داده است که فقدان چنین تفکیکی قطعا دست مفسرین و سیاستگذاران را در اعمال گسترده چارچوب قواعد جنگ در فضای سایبر باز می‌گذارد که مسلما می‌تواند تبعات خطرناک و سوئی در گسترش جنگ و جنگ‌طلبی کشورها به همراه داشته باشد. از این رو، کلیت تعریف فوق در واقع پاشنه آشیل و نقطه ضعف اصلی آن است که منجر به عدم اقبال از آن می‌گردد. در قیاس با تعریف نخست، که عاملین حمله را مضیق و منحصر به بازیگران دولتی نموده بود، این تعریف آنچنان کلی و موسع است که به سادگی قابل تفسیر می‌باشد و همان‌گونه که ذکر شد، می‌تواند خطرناک باشد و تبعات منفی به دنبال داشته باشد و موجب تشتت در روابط میان کشورها و در نهایت تهدیدی برای صلح موجود در سطح جامعه بین‌المللی باشد.

ج) سومین تعریفی که از حمله سایبری ارائه گردیده است، تعریفی است که « مارتین لیبیکی»ـ به عنوان کارشناس فنی و متخصص فناوری اطلاعات – عنوان کرده است. وی حمله سایبری را این گونه تعریف کرده است:

«حملات دیجیتالی به سیستم‌های کامپیوتری که منجر به آن می‌شود که سیستم‌های کامپیوتری مورد حمله در ظاهر امر به‌صورت نرمال و طبیعی عمل کنند، اما در واقع پاسخ هایی مغایر با واقعیت تولید و صادر می‌کنند»[1].

این رویکرد نسبت به تعریف حملات سایبری در حقیقت طیف گسترده‌ای از تهدیدات بالقوه علیه امنیت ملی کشوری که زیرساخت‌های سایبری وی هدف قرار داده شده‌اند اما به سطح و آستانه «حملات معنایی»[2] نرسیده‌اند را مستثنا می‌کند. واقعیت امر این است که این تهدیدات می‌تواند موجبات ورود ضرر و زیان به سیستم‌ها و شبکه‌های کامپیوتری کشور مورد هدف و قربانی را فراهم آورد؛ بنابراین هر تعریفی از حمله سایبری که موارد پیش‌گفته را مستثنا نماید، ضرورتا تعریف ناقصی خواهد بود که جامعیت لازم را ندارد.

1. Libicki, Martin, (1996), what is Information Warfare? Center for Advanced Concepts and Technology Institute for National Strategic Studies, Third Edition, p 77.

۲. ترجمه فارسی صورت گرفته از Semantic Attack توسط مؤلفین و مترجمین متخصص در حوزه علوم کامپیوتری ارائه شده است و این ترجمه هم اکنون در متون فنی و تخصصی کامپیوتری رایج و متداول است.

د) چهارمین تعریفی که مورد بررسی و تحلیل قرار می‌گیرد، تعریفی است که توسط گروه متخصصین و حقوق دانان پروژه تحقیقاتی راهنمای تالین (Tallinn Manual) در خصوص حقوق بین‌الملل قابل اعمال بر جنگ‌های سایبری به شرح ذیل ارائه گردیده است:

«حمله سایبری یک عملیات سایبری تهاجمی یا تدافعی است که می‌تواند منجر به ایراد صدمه (جراحت) یا مرگ به اشخاص یا باعث ایجاد خسارت یا تخریب اموال گردد»[1].

نکته اصلی در باب تحلیل تعریف یاد شده مسئله نتیجه و تبعات حمله انجام شده است. نباید این–گونه برداشت کرد که اعمال و افعال خشونت‌بار الزاما باید منتج به نتایجی بشوند که از کاربرد زور به‌صورت کلاسیک و سنتی آن بر می‌آید. در این رابطه باید متذکر شد که حملات بیولوژیک، شیمیایی یا رادیولوژیک معمولا همان آثار کلاسیک و سنتی مخاصمات را بر اهداف مورد حمله ندارند، ولی با این حال اتفاق‌نظر جهانی بر این است که این نوع از توسل به زور به عنوان یک امر و موضوع حکمی در عالم حقوق حمله تلقی می‌شوند[2]. نکته غامض این تعریف در حقیقت در نتایج و اثراتی است که از خود به جای می‌گذارد. از نقطه‌نظر ارائه‌کنندگان این تعریف، حمله سایبری در صورتی عنوان و وصف حمله را خواهد داشت که منجر به نتایج مندرج در تعریف -یعنی ورود صدمات جانی و مالی- گردد در غیر این صورت از پوشش چارچوب گفته شده خارج خواهد شد و بالطبع آثار حقوقی مورد نظر بر آن بار نخواهد شد. مجدد باید تأکید نمود که تبعات یک عملیات، تبعات و آثاری است که عموما قلمرو و دایره مفهوم و اصطلاح حمله را مشخص و معین می‌نماید؛ به عبارتی خشونت بایستی در مفهوم تبعات و آثار خشونت‌بار آن مورد توجه و مداقه قرار بگیرد و از این جهت به صرف اعمال خشونت‌بار محدود نمی‌گردد. برای نمونه، عملیات سایبری که کارکرد سیستم کنترل و نظارت بر داده‌ها و اطلاعات– موسوم به SCADA – یک نیروگاه برق را تغییر داده و منجر به ایجاد حریق در آن گردد، مشمول تعریف حمله شده و داخل در چارچوب مذکور خواهد بود. لذا از آنجایی که تبعات ناشی از عملیات سایبری مزبور مخرب بوده است، در نتیجه دارای وصف حمله می‌باشد. بنابراین همان گونه که ملاحظه شد

1. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, (2013), Prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, p 92.
2. Tadić, (1995), Decision on the Defense Motion for Interlocutory Appeal, 2 October, Paras. 120 & 124 (regarding chemical weapons).

مبنای اصلی تعریف راهنمای تالین نتیجه محور بودن حملات سایبری است نه خود حملات؛ به این صورت که اگر این نوع از حملات اثرات و تبعات خشونت‌بار، عینی و محسوس از خود بر جای بگذارند، وصف حمله را پیدا کرده و در این مرحله است که قواعد حقوق بین‌الملل در حوزه‌ها و زمینه‌های مرتبط (حقوق توسل به زور، حقوق در جنگ و حقوق مسئولیت بین‌المللی) قابلیت اعمال و اجرا پیدا خواهند کرد.

۲.۲. از منظر کشورها

در این قسمت به تعاریف ارائه شده و موضع متفاوت دو کشور آمریکا و روسیه در قبال حمله سایبری پرداخته می‌شود. نحوه برداشت و استنباط این دو کشور قاعدتا از این نظر مهم و قابل توجه است که طرز تلقی آنها از حمله سایبری در واقع ترجمان سیاست عملی و رویه عملی آنان می‌باشد. حتی می‌توان این گونه تفسیر کرد که تعاریف و مواضع رسمی دولت‌ها و بعضا سازمان‌های بین‌المللی می‌تواند مقدمه و پایه‌ای برای اقدامات عملی بعدی آنان در فضای سایبر و همچنین نشانگر جهت‌گیری سیاست حقوقی آنها باشد. لازم به ذکر است که رویه و موضع اکثر کشورهای غربی به رویکرد آمریکا نزدیک بوده و می‌توان گفت که آمریکا نماینده تفکر و رویکرد غربی در این زمینه بوده و موضع کشورهای سوسیالیستی و در حال توسعه نظیر چین و کشورهای عضو سازمان همکاری شانگ‌های به رویکرد روسیه نزدیک‌تر است و از این رو روسیه نماینده تفکر بلوک شرق می‌باشد.

الف) ایالات متحده آمریکا

در ساختار سیاسی و حقوقی ایالات متحده آمریکا، وزارت دفاع این کشور در پرداختن به موضوعات مربوط به ابعاد نظامی فضای سایبر و حملات سایبری پیش قراول بوده و نقش راهبری را به عهده داشته است. معروف‌ترین تعریف از «حملات شبکه‌ای کامپیوتری» (Computer Network Attack) توسط وزارت دفاع آمریکا ارائه شده است که آن را «عملیاتی برای از هم گسیختن، کاهش دادن یا نابودی اطلاعات موجود در کامپیوترها و شبکه‌های کامپیوتری یا خود کامپیوترها و شبکه‌ها می‌داند»[1]. در این تعریف، دوگونه حمله شبکه‌ای

1. United States Department of Defense (DoD), (2006) The National Military Strategy for Cyberspace Operations. Available at: <www.dod.gov/pubs/foi/ojcs/07-F- 2105doc1.pdf.

کامپیوتری، یکی حمله‌هایی که هدف آنها کامپیوترها یا شبکه‌های کامپیوتری است و دیگر، حمله‌هایی که هدفشان ربودن اطلاعات موجود در کامپیوترها یا شبکه‌های کامپیوتری است، از هم جدا شده است. مسئله‌ای که در این تعریف وجود دارد این است که آیا تعریف وزارت دفاع ایالات متحده شامل دست کاری یک شبکه کامپیوتری برای دستیابی به یک نتیجه و هدف بیرون از شبکه هم می‌شود یا نه؟ این هدف، با از کار انداختن خود شبکه تفاوت دارد[1]. تازه‌ترین مقررات حقوق بین‌الملل حاکم بر جنگ دریایی و موشکی که در سال ۲۰۰۹ در دانشگاه «هاروارد» و در چارچوب برنامه سیاست بشر دوستانه و پژوهش در زمینه درگیری‌ها تنظیم و تدوین شده است، تعریف وزارت دفاع آمریکا از حملات شبکه‌ای کامپیوتری را به گونه‌ای بازنگری کرده است که عملیات دست- کاری اطلاعات کامپیوتری برای به دست گرفتن کنترل کامپیوتر یا شبکه کامپیوتر را نیز در بر بگیرد. به عبارت دیگر، حمله می‌تواند مستقیما بر ضد یک کامپیوتر، کامپیوترهای موجود در یک شبکه یا کل شبکه کامپیوتری صورت گیرد[2]. بنابراین، با توجه به تعاریف ارائه شده از سوی وزارت دفاع آمریکا و دانشگاه «هاروارد » می‌توان گفت که هر دو بر سیستم کامپیوتری به عنوان یک هدف تمرکز دارند و همچنین حمله‌های متعارف به تأسیسات شبکه کامپیوتری را در بر می‌گیرد[3]. در این راستا، آموزه مشترک عملیات اطلاعاتی ایالات متحده در سال ۲۰۰۶ دیدگاه مضیق و محدودتری را در خصوص حملات شبکه‌ای کامپیوتری اتخاذ نمود به این صورت که عملیات را اقدامات انجام شده با بهره گیری از شبکه‌های کامپیوتری برای از هم گسیختن، جلوگیری از دسترسی، کاهش یا نابودی اطلاعات موجود در کامپیوترها و شبکه‌های کامپیوتری یا خود کامپیوترها و شبکه‌های کامپیوتری، تعریف می‌کند و از حمله‌هایی که بیرون از کامپیوتر یا شبکه کامپیوتری صدمات و خساراتی به بار می‌آورد بحث نمی‌کند[4]. مضاف بر این، فرماندهی سایبری ایالات متحده آمریکا در سال ۲۰۱۱ حمله سایبری را این‌گونه تعریف کرده است: «یک اقدام (فعل) خصمانه که با بهره‌گیری از

1. Silver, D.B, (2001), **Computer Network Attack as a use of Force Under Article 2(4) of the United Nations Charter**, in: Schmitt/O'Donnell (eds), Computer Network Attack and International Law, P 76.
2. http://ihlresearch.org.
3. Kuehl, D.T, (2001), **Information Operations, Information Warfare, and Computer Network Attack-Their Relationship to National Security in the Information Age**, in: Schmitt/O'Donnell (eds), Computer Network Attack and International Law, 2001, pp 44-45.
4. Joint Doctrine for Information operations, at: www. dtic. mil.

کامپیوتر یا سیستم‌ها و یا شبکه‌های مرتبط به قصد ایجاد اختلال و یا تخریب سیستم ها، زیرساخت‌ها و تجهیزات حساس سایبری دشمن صورت می‌گیرد[1]». فرماندهی مزبور در ادامه اشعار می‌دارد که تبعات و اثرات حملات سایبری ضرورتا به سیستم‌ها یا داده‌ها و اطلاعات کامپیوترهای هدف محدود نمی‌شود. علاوه بر این، در انجام حمله سایبری می‌توان از ابزارهای واسطه‌ای مختلفی نظیر وسایل ثانویه و خارجی، انتقال دهنده‌های الکترونیکی، کدهای تعبیه شده و یا اپراتورهای انسانی استفاده کرد. در رابطه با تحلیل تعریف اخیر باید متذکر شد که ویژگی اصلی و کلیدی این رویکرد این است که حملات سایبری را فقط به اقدامات و افعال خصمانه‌ای محدود کرده است که قصد آنها ورود صدمه به سیستم‌ها و زیرساخت‌های سایبری حساس است و از این جهت دایره و قلمرو تعریف را به هدف حمله محدود کرده است.

در تحلیل تعاریف مذکور باید خاطر نشان نمود که غالب تعاریف ارائه شده از سوی نهادهای مختلف دولتی و امنیتی آمریکا بین جرائم سایبری، حملات سایبری و جنگ سایبری قائل به تفکیک نشده‌اند که عدم دسته‌بندی میان این مفاهیم منجر به نوعی لجام گسیختگی در تفسیر و طبعا اعمال قواعد حقوق بین‌الملل بنا به مصلحت و مصالح ملی و نظامی خواهد شد که در نوع خود- خواسته و یا ناخواسته- می‌تواند معادلات موجود در روابط بین‌المللی را به مخاطره بیندازد. البته تحلیل دیگر در رابطه با عدم تفکیک فوق می‌تواند این باشد که شاید مقامات آمریکایی درصدد هستند تا با اتخاذ عامدانه چنین رویکردی، خود و جامعه بین‌المللی را کماکان در انتظار هنجارمند ساختن مفهوم دقیق حملات سایبری و جنگ سایبری بگذارند و با پیروی از این استراتژی منتظر اتفاقات و رویه‌های بعدی در حوزه سایبری باشند تا بتوانند از رهگذر رویه‌هایی که در عمل اتفاق می‌افتند، زمینه را برای رسیدن به قواعد حقوقی مطلوب و مورد نظر خود در حوزه حقوق بین‌الملل فراهم کنند.

ب) روسیه

تاکنون به غیر از ایالات متحده آمریکا و روسیه تقریبا هیچ کشوری به‌صورت رسمی و در قالب موضع‌گیری واحد و به عنوان یک سیاست کلی و استراتژی واحد اقدام به تعریف حمله سایبری

1. Cartwright, Gen. James E., (2011), Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories on Joint Terminology for Cyberspace Operations, p 5.

ننموده است. سایر کشورهای مدعی در این خصوص نظیر چین هم تـاکنون رسـما و بـه‌صـورت انفرادی اقدام به ارائه تعریف مستقل خود از حملات سایبری ننموده‌اند. لازم به ذکر است روسـیه اقدام به تعریف جنگ اطلاعاتی و نه حمله سایبری به شرح ذیل نموده است:

«هرگونه ایجاد اختلال در عملکرد و به هم ریختن سازماندهی امکانات، تجهیزات و سیستم‌های کلیدی نظامی، صنعتی و اداری دشـمن و همچنـین وارد آوردن فشـارهای روانـی اطلاعـاتی بـر رهبران سیاسی یا نظامی، نیروهای مسـلح و تـوده مـردم از طریـق بکـارگیری تکنولـوژی‌هـای اطلاعاتی[1]».

اقدام به تعریف جنگ اطلاعاتی به جای پرداختن به ابعاد و جوانب فنی و حقوقی حمله سایبری از سوی روسیه کاملا مبتنی بر سیاست‌ها و رویکردهای متفاوت و مبتنی بر مصالح امنیتی ملی این کشور می‌باشد. گستره و قلمرو تعریف جنگ اطلاعاتی مذکور به حدی موسع و تفسیر بردار است که عملا دست یازیدن به یک چارچوب مشترک و معـین جهـت اعمـال قواعـد حقـوقی حقـوق بین‌الملل را بسیار سخت و شاید غیرممکن سازد. البته کشورهای روسیه و چین در قالب سـازمان همکاری‌های شانگهای-که کشورهایی همچون ایران، هند و پاکستان در آن به‌صورت اعضا ناظر حضور دارند- اقدام به ارائه تعریف مشترک و موسعی از حمله سـایبری کـرده‌انـد کـه در قسـمت مربوط به سازمان‌های بین‌المللی به آن پرداخته می‌شود.

لازم به ذکر است که وزارت امور خارجه روسیه نیز در راستای اهمیت مسئله امنیت فضای سـایبر و پدیده حملات سایبری و با ابتنا و تأکید بر قطعنامه‌های مجمـع عمـومی در خصـوص مباحـث مربوط به امنیت فضای سایبر[2] و تکنولوژی‌های اطلاعاتی[3]. بـه ویـژه قطعنامـه ۸ دسـامبر ۲۰۱۰ مجمع عمومی سازمان ملل متحد در خصوص «تغییر و تحولات در زمینه اطلاعـات و ارتباطـات در چارچوب امنیت بین‌المللی»[4]، در ۹ سپتامبر ۲۰۱۱ در نشست بین‌المللـی مقامـات عـالی رتبـه

1. Jeffrey Carr, (2011), Inside Cyber Warfare, 2nd Edition, O'Reilly Media, Inc, Sebastopol, CA, 2011.
2. A/RES/65/41 of the General Assembly of the United Nations, 8 December 2010, **"Developments in the field of information and telecommunications in the context of international security".**
3. Resolution 20 November 2000, A/RES/55/29 of the General Assembly of the United Nations, **"Role of science and technology in the context of international security and disarmament".**
4.A/RES/65/41, Op.cit.

مسئول در خصوص موضوعات امنیتی در شهر «یکاترینبورگ» (Yekaterinburg) اقدام به تهیه و تدوین پیش‌نویس کنوانسیونی در باب امنیت اطلاعات بین‌المللی[1] نمود. در راستای تحلیل محتوای کنوانسیون پیشنهادی روسیه، مؤسسه مطالعات امنیت اطلاعات دانشگاه دولتی مسکوو مرکز تحقیقات و مطالعات مخاصمات مسلحانه-به عنوان یک گروه تحقیقاتی مستقل مستقر در بریتانیا- اقدام به تجزیه و تحلیل مفاد سند مزبور و ارائه نظریات تفسیری نموده‌اند[2]. آنچه که در این کنوانسیون به عنوان نقطه ثقل مورد تأکید قرار گرفته است، تمرکز بر دو مفهوم « امنیت سایبری» و « امنیت اطلاعاتی» و همچنین بهره‌گیری از معیار کنترل محتوا می‌باشد. ماده ۲ این سند به تعاریف و اصطلاحات اختصاص یافته است که در بخشی از آن اصطلاح « جنگ اطلاعاتی» و نه حمله سایبری تعریف شده است. ماده مزبور جنگ اطلاعاتی را این گونه تعریف کرده است که یک تعریف موسع و کلی تلقی می‌گردد:

«درگیری و مخاصمه میان دو یا چند کشور در فضای اطلاعاتی به منظور وارد نمودن خسارت بر سیستم ها، پروسه‌ها و منابع اطلاعاتی و همچنین ورود خسارت به ساختارها و زیرساخت‌های مهم و حیاتی، تخریب سیستم-های سیاسی، اقتصادی و اجتماعی؛ همچنین بکارگیری کمپین‌های گسترده روانی علیه جمعیت یک کشور به منظور بی‌ثبات نمودن دولت و جامعه آن کشور و همچنین وادار کردن یک کشور به اتخاذ تصمیماتی در راستای منافع دشمن و مخالفان»[3].

در سند مذکور روسیه تلاش دارد تا مفاهیم یاد شده را در یک چارچوب و به سان یک مفهوم واحد مورد بررسی قرار بدهد و این امر دقیقا نقطه اختلاف و تلاقی دیدگاه روسیه با کشورهای غربی در باب امنیت اطلاعات در فضای سایبر و به تبع آن حملات سایبری است. رویکرد کشورهای غربی در حقیقت این است که این دو (امنیت سایبری و امنیت اطلاعاتی) را مفاهیمی

1. Russia's Draft Convention on International Information Security – A Commentary, (2012), Published by Conflict Studies Research Centre and Institute of Information Security Issues Moscow State University.
2. Available at : http://www.conflictstudies.org.uk/publications.php.
3. Russia's Draft Convention on International Information Security – A Commentary, (2012), Published by Conflict Studies Research Centre and Institute of Information Security Issues Moscow State University, Article 2.

جدا و مستقل از یکدیگر دانسته و آثار حقوقی متفاوتی را بر آنها بار می‌کنند و بر این باور هستند که نباید به عنوان یک مفهوم واحد و یکسان مورد استنباط قرار بگیرند[1].

۲.۳ . از منظر سازمان‌های بین‌المللی

در میان سازمان‌های بین‌المللی که مباحث مربوط به تهدیدها و حملات سایبری و به طور کلی امنیت اطلاعات و شبکه‌های کامپیوتری را در دستور کار خود دارند، فقط سازمان همکاری شانگهای مستقیما و به صراحت حمله سایبری را تعریف کرده است. سایر سازمان‌های بین‌المللی نظیر ناتو، اتحادیه اروپا و اتحادیه آفریقا بیشتر استراتژی‌های عملی و سیاست‌های کلی خود را در قبال بحث امنیت سایبری در فضای سایبر در قبال حملات سایبری اعلام نموده‌اند. بنابراین در این قسمت تعریف ارائه شده از سوی سازمان همکاری شانگهای و موضع کلی ناتو در خصوص امنیت و استراتژی سایبری مورد بررسی و تحلیل قرار می‌گیرد.

الف) سازمان همکاری شانگهای

سازمان همکاری شانگهای متشکل از کشورهایی همچون روسیه و چین به عنوان اعضا اصلی و کشورهایی همچون هند، پاکستان و ایران به عنوان اعضا ناظر است (بیگ‌زاده، ۱۳۹۱، ص ص ۷۷۰-۷۶۹). موضع‌گیری استراتژیک این سازمان در قبال مقوله امنیت سایبری و به تبع آن تعریف حمله سایبری منعکس کننده و گویای مواضع مورد توافق این کشورها در باب اسناد منتشره از سوی سازمان است. بنابراین، تعریف سازمان همکاری شانگهای از حمله سایبری به نوعی مبین و مؤید دیدگاه رسمی و حاصل وفاق دول عضو آن- به ویژه روسیه و چین- است. برخلاف رویکرد مضیق و نتیجه‌محور کشورهای غربی، رویکرد سازمان مزبور در قبال حملات سایبری کاملا موسع و ابزار محور می‌باشد. سازمان ضمن اعلام نگرانی خود از تهدیدهای احتمالی ناشی از بکارگیری تکنولوژی‌ها و ابزار اطلاعاتی و ارتباطاتی نوین به منظور ایجاد اختلال در ثبات و امنیت بین‌المللی در سطوح نظامی و غیرنظامی، «جنگ اطلاعاتی» را این گونه تعریف می‌کند:

1 .Russia's Draft Convention on International Information Security – A Commentary, (2012), Published by Conflict Studies Research Centre and Institute of Information Security Issues Moscow State University, pp 26-27.

«شستشوی مغزی–روانی جمعی به منظور بی‌ثبات کردن جامعه و کشور و همچنین وادار ساختن کشور به اتخاذ تصمیماتی در راستای تأمین منافع گروه و طرف مخالف»[1].

علاوه بر این، سازمان همکاری شانگهای نشر و انتشار اطلاعات را به عنوان یکی از تهدیدهای اصلی فراروی امنیت اطلاعات برای سیستم‌های اجتماعی، سیاسی و اقتصادی- سیاسی و همچنین حوزه‌های روانی و فرهنگی سایر کشورها مضر و مخرب تلقی می‌کند[2]. بنابراین، به نظر می‌رسد که سازمان مذکور یک دیدگاه و برداشت کاملا موسعی را از حملات سایبری مطمح نظر قرار داده است به طوری که پذیرش این دیدگاه منجر به این نتیجه می‌شود که استفاده از تکنولوژی سایبری موجب تضعیف ثبات سیاسی کشورها می‌گردد. صاحب‌نظران بر این باور هستند که تعریف یاد شده گویا و توجیه‌گر تلاش و اقدام برای محدود ساختن و اعمال سانسور بر آزادی بیان در شبکه جهانی اینترنت است[3]. نمونه بارز و برجسته نگرانی فوق در تلاش کشورهایی نظیر مصر[4] و لیبی[5] برای سرکوب سیاسی مخالفان از طریق استفاده از رسانه‌ای نوین بوده است به طوری که آنها هرگونه فعالیت سیاسی سایبری مخالف خود را بر نتابیده و با ابزارهای کنترلی و نظارتی خود اقدام به سرکوب آنها می‌نمودند. از آنجایی شبکه جهانی اینترنت به طور فزاینده‌ای مبدل به سکویی جهانی برای تبادل آراء و تجربیات تبدیل شده است، لذا چنین تعریف هایی می‌تواند زمینه‌ساز سرکوب و در نهایت تهدید برای حقوق بشر[6] تلقی شود.

ب) سازمان پیمان آتلانتیک شمالی (ناتو)

از نقطه نظر تحول سازمانی، روند توجه جدی ناتو به مسئله تهدیدها و حملات سایبری به حمله سال ۲۰۰۷ علیه استونی برمی‌گردد که پس از وقوع حمله سایبری مذکور این سازمان به وجود

1. Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, (2008), 61ST Plenary Meeting, Annex I.
2. Shanghai Cooperation Agreement, Annex I, at 209.
3. Gjelten, Tom, (2010), Extending the Law of War to Cyberspace, ***NAT'L PUB. RADIO***. Available at: http://www.npr.org/templates/story/story.php?storyId=130023318.
4. Richtel, Matt, (2011), Egypt Halts Most Internet and Cell Service, and Scale of Shutdown Surprises Experts, ***N.Y. TIME***, at A11.
5. Gentile, Sal, (2011), Gadhafi Regime "Turns Off the Tap" on Libya's Internet, Live Blog: Libya Revolts, PBS, Available at: http://www.pbs.org/wnet/need-to-know/the-daily-need/libya-revolts-a-live-blog/7679/.
۶. چنین تفسیر موسعی می‌تواند زمینه‌ساز تهدید علیه حقوقی همچون آزادی ارسال و دریافت اطلاعات در فضای مجازی، آزادی عقیده و آزادی بیان باشد.

دو خلاء دکترین منسجم و یکپارچه سایبری و همچنین استراتژی جامع سایبری اذعان نمود[1]. بلافاصله و به تبع وقوع این حمله، ناتو به منظور بررسی رسمی حملات سایبری نخستین جلسه خود را در سال ۲۰۰۸ـ با عنوان اجلاس بخارست در رومانی ـ تشکیل داد. ماحصل اجلاس بخارست تشکیل دو رکن جدید با تمرکز بر بحث حملات سایبری با عناوین "مقام مدیریت دفاع سایبری"[2] و «مرکز عالی همکاری دفاع سایبری» بود. اگرچه تشکیل دو رکن یاد شده پیشرفت‌ها و دستاوردهای خوبی را در قبال تعیین استراتژی سایبری سازمان به دنبال داشته است ولی به هر تقدیر سازمان توانایی کافی و لازم جهت مقابله با تهدیدهای موجود سایبری علیه اموال و تأسیسات دیجیتال خود را ندارد. دلیل چنین وضعیتی پیچیدگی و نهانی بودن حملات سایبری است که اساسا غیرقابل پیش‌بینی بوده و در کمترین زمان ممکن رخ می‌دهند.

به اینترتیب، باید اذعان داشت که برنامه‌ها و توانمندی‌های سایبری ناتو نیز کماکان در مراحل اولیه تکامل خود قرار دارد و هنوز به پختگی لازم در این حوزه نرسیده است به طوری که سازمان هنوز تعریف رسمی و مورد اجماعی را از حمله سایبری ارائه نداده است. البته لازم به ذکر است که تهیه و تدوین اصول راهنمای تالین بنا به دعوت و حمایت مرکز عالی همکاری دفاع سایبری ناتو انجام شده است که متخصصین و محققین این پروژه در قاعده شماره ۳۰ اقدام به تعریف حمله سایبری کرده‌اند[3]. اگر بتوان از حمایت و دعوت ناتو به تهیه و تدوین این پروژه این گونه برداشت کرد که نظرات محققین این پروژه مورد تأیید و در واقع بیانگر رویکرد ناتو نسبت به حملات سایبری است، لذا تعریف مذکور (پیشتر مورد اشاره و تحلیل قرار گرفته است) را می‌توان به ناتو نسبت داد و بر این باور بود که تعریف ناتو از حمله سایبری همین مفهومی است که در راهنمای تالین آمده است. نباید این نکته را از نظر دور داشت که ناتو تاکنون موضع و رویکرد رسمی خود را در خصوص تعریف حمله سایبری اعلام نکرده است و از این رو، نمی‌توان به قطع یقین تعریف راهنمای تالین را به رویکرد رسمی ناتو نسبت داد.

1. Hughes, Rex B., (2011), NATO and Cyber Defense: Mission Accomplished?, ATLANTISCH PERSPECTIEF. Available at: http://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf.

2. Cyber Defense Management Authority.

۳. حمله سایبری یک عملیات سایبری تهاجمی یا تدافعی است که می‌تواند منجر به ایراد صدمه (جراحت) یا مرگ به اشخاص یا باعث ایجاد خسارت یا تخریب اموال بگردد.

نتیجه‌گیری

با نگاهی توصیفی-تحلیلی به مطالب و عناوین مذکور در رابطه با مفهوم و تعریف حمله سایبری از منظر کشورها و سازمان‌های بین‌المللی، باید اذعان داشت که در وهله اول باید میان مفاهیم سه‌گانه جرم سایبری، حمله سایبری و جنگ سایبری قائل به تفکیک شد زیرا، خلط نمودن مفاهیم سه‌گانه مذکور موجب تزلزل و تشتت در رسیدن به نتایج حقوقی مورد نظر خواهد شد. با تفکیکی که انجام شد، مفهوم حمله سایبری مشخصا اگر با قصد و نیت صدمه زدن به تأسیسات و شبکه‌های کامپیوتری سایر کشورها رخ دهد، آن وقت است که می‌توان مدعی امکان اعمال حقوق بین‌الملل بر آن شد. با پذیرش تفکیک یاد شده، مشکل اصلی در تعریف حمله سایبری و عدم وجود اجماع بین‌المللی در این خصوص کماکان باقی است. با ابتنا بر رویکرد موسع روسیه و رویکرد مضیق ایالات متحده آمریکا نسبت به تعریف حمله سایبری، باید گفت که متأسفانه تعریف مفهوم مذکور از نظر هنجاری عقیم مانده و تاکنون محل اختلاف و مناقشه میان دولت‌ها و سازمان‌های بین‌المللی است. فقدان اتفاق‌نظر در رابطه با تعریف حمله سایبری، بدون شک پرداختن به جوانب و ابعاد حقوقی آن را از منظر حقوق بین‌الملل بسیار سخت و مشکل خواهد نمود و حتی به جرأت می‌توان گفت که تا حدی بررسی‌ها و تحلیل‌ها را نیز به بن‌بست می‌کشاند. پر واضح است که اختلاف‌نظر کشورهای روسیه و آمریکا و همچنین اختلاف دیدگاه سازمانی سازمان هایی نظیر ناتو و سازمان همکاری‌های شانگهای در زمینه ارائه یک تعریف واحد، مشترک و مورد توافق چالش حقوقی پدیده حملات سایبری را دو چندان کرده و به رویه سازی انفرادی کشورها در این زمینه دامن می‌زند که چنین جریانی مسلما بر خلاف نفع مشترک و نظم حقوقی جامعه بین‌المللی خواهد بود.

فهرست منابع

الف) فارسی

۱. بیگ‌زاده، ابراهیم؛ **حقوق سازمان‌های بین‌المللی**، چاپ دوم، انتشارات مجد، ۱۳۹۱.

ب) لاتین

2. A/RES/65/41 of the General Assembly of the United Nations, 8 December 2010, "**Developments in the field of information and telecommunications in the context of international security**".
3. Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, (2008), 61ST Plenary Meeting.
4. Antolin-Jenkins, Vida, (2008), **Defining the Parameters of Cyber war Operations: Looking for Law in All the Wrong Places**, 51 NAVAL L. REV. 132, 140.
5. Cartwright, Gen. James E., (2011), **Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands**, Dirs. of the Joint Staff Directories on Joint Terminology for Cyberspace Operations 5.
6. Chairman of the Joint Chiefs of Staff, **Joint Doctrine for Information operations**, Available at: www. dtic. mil/ doctrine/ new-pubs/jp3-13.pdf.
7. Clarke, Richard A. & Knake, Robert K, (2010), **Cyber War: The Next Threat TO National Security and What to Do about It**, 6.
8. Commentary on the HPCR, (2009), p 1. Available at: http://ihlresearch.org/amw/Commentary%20on%20the%20HPCR%20Manual.pdf.
9. Cooperative Cyber Defense Centre of Excellence (CCDCOE), (2008), **Cyber Attacks against Georgia: Legal Lessons Identified**, PP.7-8. Available at: < www. carlisle. army. mil /DIME/ documents/ Georgia %201%200. pdf.>
10. Duncan B. Hollis, (2007), **Why States Need an International Law for Information Operations**, 11 LEWIS & CLARK L. REV. 1023, 1042.
11. Gellman, Barton, (2002),**Cyber Attacks by Al Qaeda Feared; Terrorists at Threshold of Using Internet as Tool of Bloodshed: Experts Say**, WASH. POST, June 27, at A01.
12. Gentile, Sal, (2011), **Gadhafi Regime "Turns Off the Tap" on Libya's Internet**, Live Blog: Libya Revolts, PBS, Available at: http://www.pbs.org/wnet/need-to-know/the-daily-need/libya-revolts-a-live-blog/7679/.

13. Gjelten, Tom, (2010), **Extending the Law of War to Cyberspace**, NAT'L PUB. RADIO. Available at: http://www.npr.org/templates/story/story.php?storyId=130023318 (last visited Apr. 18, 2012).
14. Gjelten, Tom**, Seeing the Internet as an 'Information Weapon**,' NAT'L PUB. RADIO. Available at: http://www.npr.org/templates/story/story.php?storyId=130052701.
15. Hughes, Rex B., (2011), **NATO and Cyber Defense: Mission Accomplished?,** ATLANTISCH PERSPECTIEF. Available at: http://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf.
16. Jeffrey Carr, (2011), **Inside Cyber Warfare**, 2nd Edition, O'Reilly Media, Inc, Sebastopol, CA, 2011.
17. Kuehl, D.T, (2001), **Information Operations, Information Warfare, and Computer Network Attack-Their Relationship to National Security in the Information Age**, in: Schmitt/O'Donnell (eds), Computer Network Attack and International Law, 2001, pp 44-45.
18. Libicki, Martin, (1996), **What is Information Warfare?,**Center for Advanced Concepts and Technology Institute for National Strategic Studies, Third Edition, p 77.
19. Resolution 20 November 2000, A/RES/55/29 of the General Assembly of the United Nations, **"Role of science and technology in the context of international security and disarmament".**
20. Resolution 21 December 2009, A/RES/64/211 of the General Assembly of the United Nations, "**Creation of a global culture of cyber security and taking stock of national efforts to protect critical information infrastructures**".
21. Richtel, Matt, (2011), **Egypt Halts Most Internet and Cell Service, and Scale of Shutdown Surprises Experts**, N.Y. TIME, at A13.
22. Russia's Draft Convention on International Information Security – A Commentary, (2012), Published by Conflict Studies Research Centre and Institute of Information Security Issues Moscow State University.
23. Schmitt, M.N, (1998-1999), **Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework**, Colum. J. Transnat'l L.37 PP 890-891.
24. Silver, D.B, (2001), **Computer Network Attack as a use of Force Under Article 2(4) of the United Nations Charter**, in: Schmitt/O'Donnell (eds), Computer Network Attack and International Law, P 76.
25. Tadić, (1995), Decision on the Defense Motion for Interlocutory Appeal, 2 October, Paras. 120 & 124 (regarding chemical weapons).

26. **TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE**, (2013), Prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press.
27. United States Department of Defense (DoD), (2006)**The National Military Strategy for Cyberspace Operations.** Available at: <www.dod.gov/pubs/foi/ojcs/07-F- 2105doc1.pdf. last accessed 17 July 2009.
28. Watts, S., (2010), **Combatant Status and Computer Network Attack**, Va.J.Int'l L.50 P 400.