مطالعات حقوقی
دوره سیزدهم، شماره اول، بهار ۱۴۰۰

ضرورت تدوین کنوانسیون بین‌المللی حملات سایبری

پرویز فرشاسعید* **محمود جلالی**** **مهناز گودرزی*****

چکیده

توانایی دولت‌ها در استفاده از فناوری‌های سایبری باعث شده است که بتوانند با استفاده از این فناوری‌ها خساراتی را به رقبایشان وارد کنند. روزانه میلیون‌ها حمله سایبری در سراسر دنیا اتفاق می‌افتد که چنین حملاتی علیه تأسیسات نظامی، سیستم‌های بانکی، تأسیسات هسته‌ای و سایر زیرساخت‌های حیاتی کشورها انجام می‌گیرد. در حال حاضر قوانین شفاف و مدونی برای حوزه سایبری وجود ندارد و کشورهایی که دارای توان بالایی در این حوزه هستند از فرصت استفاده کرده حملاتی را علیه رقبایشان انجام می‌دهند. این پژوهش، به این سؤال پاسخ می‌دهد که چه ضرورتی دارد که کشورها به تدوین کنوانسیونی بین‌المللی در مبارزه با حملات سایبری بپردازند و فعالیت‌های سایبری خودشان را در چارچوب چنین کنوانسیونی محدود کنند؟ با استفاده از روش توصیفی- تحلیلی بحث خواهد شد که چون تدوین یک کنوانسیون بین‌المللی می‌تواند نقش مهمی در بازدارندگی از انجام حملات سایبری، مدیریت مؤثر بحران، حل مشکل انتساب و مسئولیت بین‌المللی دولت‌ها، تعیین اندازه و ماهیت اقدام‌های متقابل در برابر حملات سایبری داشته باشد، ضرورت دارد دولت‌ها به تدوین یک کنوانسیون بین‌المللی درباره حملات سایبری بپردازند و با گنجاندن قوانین و مقررات الزام‌آور در چنین کنوانسیونی به این وضعیت نابسامان پایان دهند.

واژگان کلیدی: حملات سایبری، حوزه سایبری، فناوری‌های سایبری، کنوانسیون بین‌المللی.

---

* دانشجوی دکتری حقوق بین الملل، دانشگاه آزاد اسلامی، واحد اصفهان، (خوراسگان)، اصفهان، ایران
parvizfarshasaid@yahoo.com

** دانشیار گروه حقوق دانشگاه اصفهان، اصفهان، ایران.(نویسنده مسئول)
m.jalali@ase.ui.ac.ir

***استادیار گروه روابط بین الملل دانشگاه آزاد اسلامی،واحد اصفهان (خوراسگان)، اصفهان، ایران.
goodarzi_mahnaz@yahoo.com

تاریخ دریافت: ۱۳۹۸/۱/۱۶ تاریخ پذیرش:۱۳۹۹/۷/۲۳

سرآغاز

به دلیل ظرفیت‌های فضای سایبری، می‌توان گفت که تقریباً تمامی جنبه‌های زندگی مردم دنیا از بانکداری گرفته تا ادارات دولتی، سازمان‌ها و نهادهای نظامی و حتی زندگی خصوصی مانند همسریابی، همه به این فضا وابسته شده است. هر روز صدها میلیون انسان جهت برقراری ارتباطات، جستجوی اطلاعات و انجام معاملات تجاری عادی از فضای سایبری استفاده می‌کنند و با توجه به تهدیداتی که از طرف فناوری‌های سایبری وجود دارد امنیت در فضای سایبری به دغدغه اصلی جامعه بین‌المللی تبدیل شده است. فضای سایبری یک حوزه گسترده‌ای از تهدیدها علیه دولت‌ها و افراد را از سرقت اطلاعات و جاسوسی سایبری گرفته تا اشکال متعدد دیگری از حملات سایبری از جمله «حملات محرومیت از سرویس»[1] یا از کار انداختن سایت‌های اینترنتی در بر می‌گیرد. به‌عنوان نمونه می‌توان در حال حاضر، به فعالیت‌های جاسوس‌های سایبری برای به دست آوردن اطلاعات محرمانه در مورد واکسن کرونا علیه دولت ایالات‌متحده امریکا اشاره کرد. این می‌تواند در سایر حوزه‌های علمی که دارای منافع اقتصادی زیاد باشد نیز اتفاق افتد. در چنین وضعیتی که قانون و قاعده مشخصی برای فعالیت‌های سایبری دولت‌ها وجود ندارد، مشخص است که نظم و امنیت بین‌المللی با چالش جدیدی روبرو شده که قبلاً بی‌سابقه بوده است. آنچه می‌تواند به حل این معضل کمک کند همکاری دولت‌ها در سطح بین‌المللی برای حل این مشکل است و این نمی‌تواند اتفاق بیفتد مگر اینکه دولت‌ها به تدوین یک کنوانسیون بین‌المللی درباره حملات سایبری بپردازند.

در بحث ضرورت تدوین کنوانسیون بین‌المللی درباره حملات سایبری تاکنون تحقیقات زیادی انجام نگرفته است. در «کنفرانس امنیت سایبری»[2] چهاردهم فوریه سال ۲۰۱۷ *براد اسمیث*[3] پیشنهاد تدوین کنوانسیونی بین‌المللی با نام «کنوانسیون دیجیتال ژنو»[4] شبیه «کنوانسیون ۱۹۴۹ ژنو»[5] را مطرح کرد. «کنوانسیون ۱۹۴۹ ژنو» مفادی را برای زمان جنگ وضع کرده است که از افرادی که دیگر در جنگ نیستند حفاظت و حمایت می‌کند. در ۲۱ جولای

---

1. denial of service attack
2. Cyber Security Conference
3. Brad,Smith
4. Geneva Digital Convention
5. The Geneva Conventions of 1949

سال ۲۰۱۷ مقاله ارزشمندی توسط *مت استراپ سانجیاونی*[1] در *مجله فلسفه و فناوری*[2] با عنوان «چرا جهان نیاز به یک کنوانسیون بین‌المللی درباره جنگ سایبری دارد»[3] منتشر شده که در آن به ضرورت تدوین کنوانسیونی بین‌المللی درباره جنگ سایبری اشاره شده است. در این مقاله ایشان از دیدگاه حقوق جنگ به قضیه حملات سایبری پرداخته و تأکید کرده‌اند که در حال حاضر جهان برای کنترل حملات سایبری مخرب نیازمند کنوانسیونی مانند کنوانسیون ژنو است. البته باید بیان کرد که همه حملات سایبری به عنوان جنگ سایبری به شمار نمی‌آیند. در بحث حوزه سایبری بین حملات سایبری، جرم سایبری و جنگ سایبری تفاوت وجود دارد. جنگ سایبری همیشه تأمین‌کننده شرایط یک حمله سایبری است اما تمام حملات سایبری جنگ سایبری نیستند. تنها حملات سایبری که دارای تأثیرهایی برابر با حملات مسلحانه متعارف یا حملاتی که در چارچوب مخاصمات مسلحانه بوده و به سطح جنگ سایبری ارتقا یابند جنگ سایبری تلقی می‌شوند. پژوهش پیش رو با بررسی جامع و تفصیلی این دو مورد یعنی پیشنهاد تدوین «کنوانسیون دیجیتال ژنو» براد اسمیث و مقاله سانجیاونی، ضرورت تدوین کنوانسیون بین‌المللی جامع و کامل درباره حملات سایبری را پیشنهاد می‌دهد که تمام جوانب حوزه سایبری یعنی حملات سایبری، جرم سایبری و جنگ سایبری را در برگیرد. همچنین در این پژوهش برای کارایی بهتر کنوانسیون در مواجهه با تغییرات سریع فناوری سایبری پیشنهاد پیش‌بینی کنفرانس‌های دوره‌ای ۹۰ روزه یا کمتر از این زمان داده شده است. جهت ضمانت اجرای کنوانسیون پیشنهاد تأسیس سازمانی با عنوان «سازمان بین‌المللی نظارت بر فعالیت‌های سایبری دولت‌ها» جهت نظارت بر فعالیت‌های سایبری دولت‌های عضو و بررسی گزارش‌های دولت‌های قربانی حملات سایبری داده شده و پیشنهاد دادگاهی ویژه جهت بررسی شکایات دولت‌های عضو کنوانسیون از نوآوری‌های این پژوهش است.

آنچه پژوهش حاضر به دنبال آن است یافتن این پاسخ است که برای دولت‌ها چه ضرورتی وجود دارد تا به تدوین یک کنوانسیون بین‌المللی درباره حملات سایبری بپردازند؟ این مقاله به کنکاش و بررسی پیرامون این موضوع می‌پردازد و در ابتدا به بررسی موانع موجود بر سر راه یک کنوانسیون بین‌المللی درباره حملات سایبری می‌پردازد و سپس فواید وجود چنین کنوانسیونی را

---

1. Mette Eilstrup-Sangiovanni
2. Philosophy and Technology
3. Why the World Needs an International Cyber War Convention

مطرح می‌کند و در نهایت انگیزه دولت‌ها برای عضویت در چنین کنوانسیونی را بیان می‌کند.

۱. دلایل و ضرورت‌های تدوین کنوانسیون بین‌المللی حملات سایبری

حملات سایبری یک پدیده نوظهور است که هنوز قاعده حقوقی معتبری در قالب معاهدات یا عرف بین‌المللی در خصوص آن شکل نگرفته است (قاسمی و نامدار، ۱۳۹۷: ۲۲۸). در تاریخ ۱۴ فوریه ۲۰۱۷، پیشنهاد «کنوانسیون دیجیتال ژنو»[1] برای اولین بار توسط *براد اسمیت*[2] در «کنفرانس امنیت سایبری»[3] که یکی از معتبرترین کنفرانس‌های رمزگذاری و امنیت فن‌آوری اطلاعات در امریکا است، مطرح شد. کنفرانس سال ۲۰۱۷ در امریکا با حضور ۱۵ سخنران اصلی، ۷۰۰ سخنران و ۵۰۰ نشست و ۵۵۰ شرکت حاضر در نمایشگاه آن برگزار شد. این طرح بر ضرورت هنجارسازی برای مقابله با تهدیدات سایبری دولت‌ها و کشورها علیه شهروندان و شرکت‌های خصوصی در دیگر کشورها و در کشور خود و ضرورت حفاظت و توانمندسازی شهروندان در برابر حملات سایبری تحت حمایت دولت‌ها از قبیل هک و سرقت اطلاعات و ضرورت ضابطه‌مند کردن رفتار دولت‌ها در فضای سایبری بر اساس هنجارهای جهانی تأکید می‌کند. در این کنفرانس، *براد اسمیت* بیان کرد که آنچه ما اکنون نیاز داریم یک کنوانسیون دیجیتالی است. ما به کنوانسیونی نیاز داریم تا از دولت‌های دنیا بخواهد متعهد شوند تا دیگر در حملات سایبری علیه عوامل خصوصی شرکت نکنند و زیرساخت‌های غیرنظامی را هدف قرار ندهند (Smith, 2017:10) و شاید بیشتر از همه‌چیز، ما نیاز داریم تا دولت‌ها کاری مانند کنوانسیون ۱۹۴۹ ژنو و کنوانسیون‌های بعدی که تدوین کرده‌اند انجام دهند. آنچه دنیا نیاز دارد یک سازمان مستقل جدید تا حدی شبیه آژانس بین‌المللی انرژی هسته‌ای است که برای چندین دهه به کار عدم اشاعه اشتغال داشته است (Smith, 2017:10).اگر شما به گذشته نگاه کنید که آنچه در سال ۱۹۴۹ اتفاق افتاد، دولت‌های جهان تشخیص دادند که نمی‌توانند از غیرنظامیان در هنگام جنگ بدون وجود سازمان خصوصی یعنی یک کمیته بین‌المللی صلیب سرخ حفاظت کنند (Smith, 2017:10). *براد اسمیت* این ایده را مطرح کرد که کشورها نیازمند تدوین و تبعیت از قواعد جهانی در زمینه حملات سایبری هستند تا دولت‌ها را نسبت به اجرای هنجارهای لازم

1. Geneva Digital Convention
2. Brad,Smith
3. Cyber Security Conference

برای حفاظت از شهروندان در اینترنت، در زمان صلح متعهد سازد. وی از سوی دیگر التزام شرکت‌های فن‌آوری به بی‌طرفی در منازعات سایبری، با هدف جلب اعتماد و ثبات آنلاین را مورد تأکید قرار داد.

استفاده از فناوری دیجیتال و مسابقه بین دولت‌ها، در عصر تحول دیجیتال باعث رشد سریع این فناوری شده است. چنین تحولی طیف گسترده‌ای از فرصت‌های توسعه را برای دولت‌ها فراهم می‌کند اما هم‌زمان آسیب‌پذیری برای جرائم سایبری و حملات سایبر را افزایش می‌دهد؛ اگر با مقررات و ابزارهای قانونی و سایبری قوی حمایت نشود، زیرا راهکارهای سنتی سایبری مؤثر نخواهد بود (Al Aridi, 2018:6).

ظهور حملات سایبری قسمت جدیدی از سیر تکاملی جنگ و ادامه تغییرات آن است که به‌وسیله تغییرات تکنولوژیک ایجاد شده است (Asif Khan & et al,2017:20). علی‌رغم تهدیدات بسیار زیاد فناوری‌های حوزه سایبری تعداد کمی از معاهدات در مورد مسائل امنیت سایبری وجود دارد. در حال حاضر اصلی‌ترین معاهدات بین‌المللی در حوزه سایبری «کنوانسیون ۲۰۰۱ جرائم سایبری»[1] و پروتکل الحاقی ۲۰۰۶ آن و «توافقنامه امنیت اطلاعاتی بین‌المللی سازمان همکاری شانگهای ۲۰۰۹»[2] هستند. هر دو موافقت‌نامه در تعداد اعضا و قلمرو محدودیت دارند. مذاکره بر سر یک معاهده بین‌المللی جامع درباره حملات سایبری تاکنون با عدم پذیرش به‌ویژه از طرف دولت‌های غربی همراه بوده است. از نظر تاریخی، بحث‌های مهمی که تاکنون در حوزه سایبری مطرح‌شده این بوده است که حقوق بین‌الملل موجود را در حوزه فضای سایبری بکار گیرند. دستورالعمل تالین[3] قابل‌اعمال در جنگ‌های سایبری که دارای مجموعه‌ای از قوانین است که چطور حقوق بین‌الملل موجود مانند حق بر جنگ، حقوق بین‌الملل بشردوستانه و حقوق مسئولیت دولت در فضای سایبری بکار می‌رود مهم‌ترین نتیجه ذکرشده

---

1. Convention on Cyber Crime
2. The agreement between the governments of state members of the Shanghai Cooperation Organization on cooperation in the field of ensuring the international information security

۳. مرکز عالی دفاع سایبری جمعی ناتو (NATO CCD COE) در سال ۲۰۰۹، از گروهی متشکل از ۲۰ متخصص مستقل حقوق بین‌الملل دعوت کرد تا راهنمایی را در زمینه قوانین نافذ در جنگ سایبری تدوین کنند. ماحصل تلاش این گروه بعد از ۳ سال فعالیت، راهنمایی معروف به راهنمای تالین است که از آن به‌عنوان سندی غیررسمی و غیر الزام‌آور نام برده شده است. هدف اصلی این پروژه پاسخ به این سؤال بود که چگونه می‌توان معیارهای حقوقی موجود را به شکل جدید جنگ یعنی جنگ سایبری تعمیم داد؟

چنین بحث‌هایی بوده است.

با این حال، راهنمای تالین نتوانست خارج از گروه محدود اعضای ناتو که از آن حمایت می‌کردند موردتوجه قرار گیرد (Lucas, 2017:40). همچنین دستورالعمل تالین قوانین جدید بین‌المللی برای حوزه سایبری ارائه نمی‌دهد بلکه قوانین حقوق بین‌الملل موجود را تفسیر می‌کند. تاکنون این تفسیر نتوانسته دولت‌ها را تشویق کند تا فعالیت‌هایشان را در فضای سایبری محدود کنند (Lucas, 2017:17). با توجه به مواردی که مطرح شد، نیاز است تا دولت‌ها به فکر یک معاهده جامع و کامل درباره حملات سایبری در سطح جهان باشند و برای اینکه تدوین چنین معاهده‌ای بتواند باعث عضویت اکثر کشورهای جهان و همچنین باعث ترغیب دولت‌ها جهت عضویت در آن باشد باید به شناسایی موانع موجود بر سر راه آن پرداخت و همچنین فواید عضویت دولت‌ها را در چنین معاهده مشخص و معین کرد تا دولت‌های بیشتری ازجمله دولت‌هایی که دارای فناوری پیشرفته‌ای هستند به عضویت در چنین معاهده‌ای ترغیب شوند.

۲. موانع موجود بر سر راه تدوین کنوانسیون بین‌المللی حملات سایبری

هنگام تدوین هر کنوانسیون بین‌المللی موضوع مشکلات و موانعی که بر سر آن وجود دارد باید به‌طور کامل و احسن مورد شناسایی و توجه قرار گیرد، در غیر این صورت اجرای معاهده با مشکل مواجه خواهد شد. در مورد تدوین یک کنوانسیون بین‌المللی درباره حملات سایبری نیز موانع و مشکلاتی وجود دارد که در این قسمت به تجزیه‌وتحلیل آن‌ها پرداخته می‌شود.

۲-۱. فقدان تعریف مشخص از حمله سایبری

یکی از شیوه‌های نوین تخاصم درصحنه بین‌المللی، حملاتی است که در بستر فضای سایبری صورت می‌گیرد (قاسمی و نامدار،۱۳۹۷: ۱۹۹). درباره اصطلاح حمله سایبری، تعاریف متعددی ارائه شده است به‌نحوی‌که می‌توان گفت برای آن تعریف مشترکی وجود ندارد. در این قسمت به‌عنوان مثال به چند تعریف اشاره می‌شود. *ریچارد کلارک* و *رابرت کناک* کارشناس امنیت ملی دولت ایالات‌متحده امریکا، حمله سایبری را این‌طور تعریف کرده است: «اقداماتی است که توسط کشورها برای نفوذ در کامپیوترها یا شبکه‌های کامپیوتری کشور یا کشورهای دیگر به‌منظور ورود خسارت یا ایجاد اختلال انجام می‌شود» (Clarke & Knake, 2010: 6).

مارتین لیبیکی کارشناس فنی و متخصص فناوری اطلاعات نیز تعریف دیگری از حمله سایبری به این شرح ارائه کرده است: «حملات دیجیتالی به سیستم‌های کامپیوتری که منجر به آن می‌شود تا سیستم‌های کامپیوتری موردحمله، در ظاهر امر به صورت معمولی و طبیعی عمل کنند، اما در واقع پاسخ‌هایی مغایر با واقعیت تولید و صادر می‌کنند (Libicki, 1996:77).

همچنین متخصصین و حقوقدانان «راهنمای تالین»[1] نیز حمله سایبری را این‌گونه تعریف کرده‌اند: «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 شود» (Tallin Manual, 2013: 92).تعریف راهنمای تالین از حمله سایبری به دلیل ماهیت حقوقی آن به نظر می‌رسد مرتبط‌ترین تعریف در حقوق بین‌الملل باشد. حتی اگر تعیین اینکه چه هنگام حمله سایبری اتفاق می‌افتد و چه موقع آن به حد یک حمله مسلحانه می‌رسد مشکل باشد، تعریف ارائه‌شده در راهنمای تالین با تمرکز آن بر نتایج نسبت به تعاریف دیگر استاندارد دقیق‌تری را ارائه می‌دهد.

با توجه به تعاریفی که ارائه شد این حقیقت آشکاراست که هنوز اجماعی در سطح بین‌المللی برای ارائه یک تعریف مشخص و یکسان از حمله سایبری وجود ندارد. فقدان اتفاق‌نظر در رابطه با تعریف حمله سایبری، بدون شک پرداختن به جوانب حقوقی آن را از منظر حقوق بین‌الملل بسیار سخت و مشکل خواهد کرد و حتی به جرأت می‌توان گفت که تا حدی بررسی‌ها و تحلیل‌ها را نیز به بن‌بست می‌کشاند (اصلانی و رنجبریان، ۱۳۹۴: ۲۷۵). نخستین گام در حل معضل حملات سایبری، ارائه یک تعریف جامع و کامل توسط کارشناسان حوزه سایبری است که مورد پذیرش و اجماع همه آنان باشد. در رابطه با حملات سایبری، ناگفته پیداست که یک توافق جامع در تعریف حمله سایبری از اهمیت بالایی برخوردار است. یک تعریف مشخص و دقیقی از حمله سایبری که در جامعه بین‌المللی روی آن توافق شود موجب کارایی حقوق بین‌الملل می‌شود؛ بنابراین اگر قرار است یک ممنوعیت جامع بین‌المللی برای حملات سایبری وجود داشته باشد چنین تعریفی نیاز است و این تعریف باید به‌طور دقیق و مشخص در یک کنوانسیون بین‌المللی گنجانده شود.

---

1. Tallin Manual

۲-۲. زمان‌بر بودن مذاکره بر سر یک کنوانسیون بین‌المللی حملات سایبری

یکی از مشکلات دیگری که برای تدوین یک معاهده درباره حملات سایبری وجود دارد این است که مذاکره بر سر آن زمان‌بر خواهد بود. به دلیل اینکه قدرت‌های بزرگ سایبری تاکنون از این وضع موجود به نحو احسن استفاده کرده‌اند بعید است بتوان به‌راحتی آن‌ها را وارد مذاکره برای تدوین چنین کنوانسیونی کرد، زیرا فناوری سایبری و فضای سایبری به دلیل گستردگی و پیچیدگی آن و منافعی که برای دولت‌های دارای فناوری برتر سایبری دارد قابل‌مقایسه با هیچ حوزه دیگری نیست. مذاکره بر سر معاهدات یک فرایند آهسته و طاقت‌فرسا است که برای مسائل حوزه سایبر و اینترنت نامناسب است (Finnemore, 2011:93). کنوانسیون حقوق دریاها محصول ۹ سال مذاکره طاقت‌فرسای کشورهای عضو سازمان ملل متحد از سال ۱۹۷۳ تا سال ۱۹۸۲ بود. درحالی‌که مذاکره بر سر کنوانسیون منع گسترش، تولید، انباشت و به‌کارگیری سلاح‌های شیمیایی و انهدام آن‌ها چندین سال در جریان بوده است. تجربه از مذاکرات این معاهدات و مذاکرات سایر معاهده‌های بین‌المللی مانند مذاکرات معاهده بین‌المللی منع مین‌های زمینی نشان می‌دهد که هنجارسازی بین‌المللی و پذیرش آن‌ها یک فرایند آهسته است و این فرایند اغلب به‌وسیله مذاکرات رسمی که وزن سیاسی آن بالا است سرعت می‌یابد. اگرچه مسیر یک توافق بین‌المللی الزام‌آور درباره حملات سایبری راه دور و درازی است اما توسل به مذاکرات ممکن است تأثیر مثبتی در این رابطه داشته باشد (Sangiovanni, 2017:29)؛ بنابراین جامعه جهانی باید با صبر و حوصله وافر و همکاری‌های گسترده و تنگاتنگ، اقدام به مذاکره بر سر چنین کنوانسیونی کند. در غیر این صورت و با توجه به پیچیدگی و اهمیت موضوع فناوری سایبری بعید است تصور کرد که در کوتاه‌مدت دولت‌ها بتوانند به تدوین کنوانسیونی بین‌المللی درباره حملات سایبری دست یابند.

۲-۳. تغییر سریع فناوری در حوزه سایبری

تغییر سریع فناوری در حوزه سایبری نیز مشکلی است که بر سر راه یک کنوانسیون بین‌المللی درباره حملات سایبری وجود دارد. این تنها مختص حوزه سایبری نیست، زیرا در حقیقت تمام حوزه‌های کنترل تسلیحات بین‌المللی با مشکلات پیشرفت‌های فناوری مواجه می‌شوند. از ابتدای تدوین کنوانسیون سلاح‌های شیمیایی در سال ۱۹۹۳ پیشرفت‌های جدید در

صنایع شیمیایی باعث شده ضمائم این کنوانسیون و فهرست مواد ممنوعه آن به‌روزرسانی شود. همچنین بیشتر موافقت‌نامه‌های کنترل تسلیحات بین‌المللی کنفرانس‌های دوره‌ای را برای به‌روزرسانی این کنوانسیون‌ها پیش‌بینی کرده‌اند. به‌عنوان مثال، دولت‌های طرف کنوانسیون بین‌المللی منع جنگ‌افزارهای شیمیایی هفت کنفرانس دوره‌ای از زمانی که کنفرانس در سال ۱۹۷۵ اجرایی شد، برگزار کرده‌اند که این کنوانسیون را مطابق با پیشرفت‌های جدید علمی و تکنولوژیک به‌روزرسانی کنند. بدون شک هیچ توافق بین‌المللی کامل نخواهد بود و هرگونه توافقی که در حوزه سایبری به دست آید با توجه به ماهیت این حوزه و تغییرات سریع تکنولوژیک آن نیازمند تغییر و به‌روزرسانی خواهد بود (Sangiovanni, 2017:29)؛ بنابراین هنگام تدوین یک کنوانسیون بین‌المللی درباره حملات سایبری باید این ویژگی فناوری سایبری یعنی تغییرات سریع در این حوزه مورد لحاظ قرار گیرد تا به دلیل تغییرات سریع فناوری چنین کنوانسیونی کارایی خود را از دست ندهد. بهترین راه‌حل پیش‌بینی کنفرانس‌های دوره‌ای برای بررسی پیشرفت‌های جدید علمی و تکنولوژیک این حوزه است که بهتر است هر ۹۰ روز یا کمتر از این زمان برگزار شود و کنوانسیون بر اساس آخرین تغییرات و پیشرفت‌های فناوری بروز رسانی شود و مشکلات و معضلات موجود حل شود.

۲-۴. کارکرد دوگانه فناوری سایبری

مشکل کارکرد دوگانه فناوری‌های سایبری به هیچ‌وجه مختص این حوزه نیست. سلاح‌های شیمیایی نمونه خوبی جهت مقایسه با فناوری‌های سایبری است. بیشتر سلاح‌های شیمیایی، گستره‌ای از کاربردهای صنعتی و خانگی دارند. برای مدت‌های طولانی مشکل کارکرد دوگانه مشکل کنوانسیون سلاح‌های شیمیایی بوده است. علی‌رغم این مشکلات به‌وسیله قوانین الزام‌آور موجود در این کنوانسیون ازجمله تسلیم اظهارنامه‌ها درباره تملک، محل دقیق، کنترل، دریافت و طرح انهدام این سلاح‌ها (Chemical Weapons Convention,1997, Art 3) اقدام‌های اجرایی ملی مانند اقدام‌های ضروری برای اجرای معاهده مانند وضع مجازات قانونی، راه‌اندازی مرجع ملی برای ارتباط مؤثر با سازمان و سایر دولت‌های عضو و همکاری با سازمان این مشکلات تا حدودی برطرف شده‌اند (Chemical Weapons Convention,1997, Art 7) و تاکنون مانع قانون‌شکنی از طرف دولت‌ها شده است. مشابه این در حوزه سایبر نیز می‌تواند اتفاق بیفتد.

در مورد فناوری‌های سایبری نیز می‌توان از تجربه کنوانسیون سلاح‌های شیمیایی استفاده کرد؛ به این نحو که در کنوانسیون بین‌المللی درباره حملات سایبری، قوانین الزام‌آوری گنجانده شود که دولت‌ها نتوانند به‌آسانی آن‌ها را نقض کنند. همچنین می‌توان به‌عنوان ضمانت اجرای این کنوانسیون یک سازمان جهانی با عنوان «سازمان بین‌المللی نظارت بر فعالیت‌های سایبری دولت‌ها» برای نظارت بر فعالیت‌های سایبری دولت‌های عضو با سازوکار قانونی خاصی ایجاد کرد که دول عضو هرکدام یک نماینده در این سازمان داشته باشند و در زمینه جلوگیری از انجام حملات سایبری با همدیگر همکاری کنند و همچنین گزارش‌های دولت‌هایی که مورد حملات سایبری قرارگرفته‌اند در این نهاد به‌صورت تخصصی بررسی شود. همچنین لازم است در کنار چنین سازمانی یک دیوان بین‌المللی ویژه برای حوزه سایبر تأسیس شود تا شکایات دولت‌هایی که مورد حمله سایبری قرارگرفته‌اند در چنین نهادی مورد بررسی قرار گیرد تا دولت‌ها اطمینان خاطر داشته باشند که در صورتی که مورد حمله سایبری قرار گرفتند، دادگاهی بین‌المللی برای شکایات آن‌ها وجود خواهد داشت.

۲-۵. عدم تمایل قدرت‌های بزرگ سایبری

به دلیل اینکه هنوز مسئله استفاده از فناوری سایبری موضوعی تازه است و مضرات و فواید آن به‌طور کامل مشخص نشده است، یکی از مهم‌ترین مشکلات موجود بر سر راه یک معاهده بین‌المللی درباره سلاح‌های سایبری این است که هنوز برای مذاکره درباره آن زود است. از نظر تاریخی معاهدات حاکم بر فناوری‌های سلاح‌های جدید تنها پس از اینکه این فناوری‌ها برای مدتی مورد استفاده قرار گرفته‌اند تدوین شده‌اند (Schmit and Vihul, 2016:44). نمونه‌های قابل‌ذکر، معاهداتی است که حاکم بر مین‌های زمینی ضدنفر و بمب‌های خوشه‌ای است. دلیل این امر این است که دولت‌ها تردید دارند تا کاربرد سلاح‌هایی را که ممکن است به آن‌ها در میدان نبرد برتری بدهد محدود کنند مگر اینکه که آن‌ها تجربه کافی به دست آورند تا هزینه‌های دقیق و فواید انجام دادن آن را بسنجند؛ بنابراین یک کنوانسیون سایبری الزام‌آور زمانی می‌تواند مورد حمایت دولت‌ها قرار گیرد که آن‌ها با فناوری‌ها و کارکردهای فناوری سایبر به‌طور کامل آشنا شوند (Schmit and Vihul, 2016:44)؛ بنابراین با توجه به اینکه قدرت‌های بزرگ سایبری به دلیل اینکه از مزایای این فناوری استفاده می‌کنند بعید است به‌راحتی بتوان

آن‌ها را قانع کرد که عضو کنوانسیونی شوند کـه مـانع فعالیـت آن‌هـا در فضـای سـایبر شـود و محدودیت‌هایی را برای آن‌ها ایجاد کند. به‌عنوان مثـال، چطـور مـی‌تـوان از دولـت‌هـایی ماننـد ایالات‌متحده امریکا و اسرائیل انتظار داشت تن به امضای معاهـده‌ای دهنـد کـه باعـث محـدود کردن فعالیت‌های سایبری چنین دولت‌هایی شود. این دو کشور از ظرفیت فضای مجازی استفاده می‌کنند و بر علیه دولت‌های مخالف خود مانند جمهوری اسلامی ایران دست به حملات سایبری می‌زنند که چنین حملاتی خسارات بسیار گسترده‌ای را بر کشورهای مورد حملـه واقـع‌شـده وارد می‌کند. در حال حاضر به دلیل اینکه دولت‌های معدودی دارای توانایی سایبری بالا هستند بعیـد است که بتوان چنین دولت‌هایی را ترغیب کرد که تن به پـذیرش معاهـده‌ای بدهنـد کـه باعـث محدود شدن فعالیت‌های سایبری آن‌ها شود. تنها زمـانی مـی‌تـوان امیـد بـه تـدوین و امضـای کنوانسیون بین‌المللی درباره حملات سایبری داشت که دولت‌هایی جدید و متعدد بـه حـد قـدرت سایبری ایالات‌متحده امریکا و سایر کشورها با فناوری سایبری بالا مانند اسرائیل، روسیه و چـین برسند و این دولت‌ها منافع قدرت‌های سایبری حال حاضر در دنیـا را بـه خطـر اندازنـد. در ایـن صورت دولت‌هایی مانند امریکا و روسیه از ترس به خطر افتادن منافعشان جهـت تـدوین چنـین معاهده‌ای پیش‌قدم خواهند شد.

۲-۶. تعیین ماهیت و چارچوب معاهده سایبری

تعیین ماهیت معاهده بین‌المللی درباره سلاح‌های سایبری مشکلی است که حـل آن بسـیار دشوار است. معاهدات بین‌المللی کنترل تسلیحات می‌توانند شـکل‌هـای متعـددی داشـته باشـند. بعضی از معاهدات بین‌المللی کنترل تسلیحات موجود بسیار خاص و الزام‌آور هسـتند درحـالی‌کـه بعضی دیگر از این معاهدات بسیار ساده هستند که دارای هیچ‌گونه ابزار کنترل‌کننده و شناسـایی کننده و حتی ابزاری که نشان‌دهنده عمل دولت‌ها طبق معاهـده باشـد نیسـتند. در حـال حاضـر بیشتر طرفداران همکاری بین‌المللی درباره امنیت سایبری تمایل به معاهداتی دارند کـه در آن‌هـا قوانین داوطلبانه و غیر الزام‌آوری نسبت به معاهدات الزام‌آور وجود داشته باشد. ایـن موضـوع بـر این حقیقت استوار است که مخاصمه سایبری خیلی جدید است و فناوری‌هـای سـایبری بـه‌طـور پیوسته در حال تغییر است و بنابراین امکان یک توافق بین‌المللـی مشـکل اسـت (Finnemore, 2011:91)؛ بنابراین با قوانین داوطلبانه و غیرالزام‌آور، متقاعد کردن دولـت‌هـای بـی‌میـل جهـت

پذیرش یک معاهده ساده‌تر خواهد بود.

البته برای حملات سایبری باید یک معاهده الزام‌آور حقوقی دقیقی طراحی شود، زیرا ویژگی‌های فضای سایبری نیاز به یک معاهده رسمی الزام‌آور را مطرح می‌کند. نخستین ویژگی تعداد زیاد فعالان در حوزه سایبر است. سلاح‌های سایبری نسبتاً در دسترس آسان کنشگران مختلف از دولت‌ها گرفته تا عوامل غیردولتی است و حملات سایبری می‌تواند از خاک هر کشوری انجام گیرد و از قلمرو هر کشوری عبور کند. جهت جلوگیری از حملات سایبری در قلمرو کشورها یک کنوانسیون سایبری بین‌المللی باید دارای قواعدی باشد که کشورها ملزم به تبعیت از آن‌ها باشند. تجربه‌ای که از سازمان‌های بین‌المللی به دست آمده است نشان می‌دهد که هرگاه حل یک مشکل نیازمند همکاری بین گروه‌های کوچک با منافع نسبتاً یکسان باشد معاهدات بین‌المللی غیررسمی انعطاف‌پذیر کفایت می‌کند. درحالی‌که هر چه یک گروه بزرگ‌تر و نامتجانس‌تر باشد نیاز به قوانین الزام‌آور بیشتر خواهد بود (Sangiovanni, 2017: 29).

ویژگی دوم فضای سایبری مسئله تشخیص رفتار دولت‌ها در این فضا است؛ بنابراین به دلیل ویژگی‌های خاص فضای سایبری دولت‌ها نمی‌توانند در این فضا فعالیت‌های مضر را از فعالیت‌های غیرمضر تشخیص دهند؛ بنابراین تدوین معاهدات الزام‌آور با جزئیات بالا که دارای قوانین شفاف درباره ممنوعیت حملات سایبری باشد و مجازات شدید را علیه دولت‌های متخلف اعمال کند می‌تواند دولت‌ها را ترغیب به عضویت در این‌گونه معاهدات کند.

سومین ویژگی فضای سایبری این است که سلاح‌های سایبری هم به‌طور گسترده در دسترس هستند و هم پنهان کردن آن‌ها ساده است. تجربه از حوزه‌های دیگر کنترل تسلیحات با خصوصیات مشابه مثل سلاح‌های شیمیایی و بیولوژیک دلالت بر ارزش بالای ایجاد قواعد الزام‌آور شفاف علیه حملات سایبری می‌کند. به دلیل اینکه سلاح‌های شیمیایی و بیولوژیک به‌طور گسترده و با قیمت بسیار پایین در دسترس هستند کاربرد این دسته از سلاح‌ها در حال حاضر نتوانسته است آن‌طور که باید، محدود شود. چنین اتفاقی در مورد سلاح‌های سایبری نیز می‌تواند درست باشد. در دنیای معاصر با وجود دولت‌های قدرتمند در عرصه سایبری و وجود منافع گوناگون این دولت‌ها احتمال توسل آن‌ها به سلاح‌های سایبری زیاد است و بنابراین دولت‌ها باید اعتماد داشته باشند که هرگونه حمله سایبری با محکومیت شدید بین‌المللی همراه خواهد بود و باعث واکنش دولت‌ها ازجمله اعمال تحریم‌هایی علیه دولت متجاوزگر خواهد شد

وگرنه آن‌ها به این نتیجه خواهند رسید که بهترین استراتژی ساختن سلاح‌های سایبری خودشان است؛ بنابراین باید یک معاهده رسمی وجود داشته باشد تا عاری از قوانین مبهم باشد و شامل قوانین شفاف مسئولیت بین‌المللی برای دولت‌هایی باشد که معاهده را نقض می‌کنند (Abbott and Snidal, 2000).

مهم‌ترین نیاز برای تدوین یک معاهده درباره حملات سایبری تضمین الزام دولت‌ها در عمل به آن در سطح داخلی است. نمایندگان دولت‌ها که در سطح بین‌المللی درباره هنجارها و قوانین بین‌المللی حوزه سایبری مذاکره می‌کنند ممکن است در داخل کشور در ترغیب قانون‌گذاران جهت تدوین قوانین لازم داخلی طبق معاهده سایبری که درباره آن مذاکره می‌کنند مشکل داشته باشند. بسیاری از حقوقدانان عقیده دارند که اعطای نمایندگی به سازمان‌های بین‌المللی می‌تواند ابزار قدرتمندی در دست سیاستمداران جهت تقویت قدرت آن‌ها در رقابت‌های سیاسی داخلی باشد. با پذیرفتن تعهدات الزام‌آور معاهده‌ای دولت‌ها می‌توانند روی قانون‌گذاران فشار بیاورند تا قوانین کافی و مورد نیاز را برای اجرای معاهده تصویب کنند (Sangiovanni,2017:33)؛ بنابراین می‌توان نتیجه گرفت که در بحث تدوین یک کنوانسیون بین‌المللی باید قوانینی گنجانده شود که دارای ماهیت الزام‌آور باشند که دولت‌ها نتوانند از آن‌ها تخطی کنند در غیر این صورت نمی‌توان امید به ادامه و اجرای چنین معاهده‌ای داشت. به دلیل ویژگی خاص فضای سایبر دولت‌هایی که به عضویت کنوانسیون بین‌المللی درباره حملات سایبری درآمده‌اند ممکن است به دلیل منافعی که برایشان وجود دارد اقدام به نقض چنین معاهده‌ای کنند ولی اگر بدانند در صورت نقض معاهده اقدام‌های تنبیهی برای آن‌ها وجود دارد ممکن است از ترس چنین اقدام‌های تنبیهی تن به اجرای دقیق معاهده بدهند و از نقض آن بپرهیزند؛ بنابراین ضمانت اجرای یک معاهده بین‌المللی درباره حملات سایبری می‌تواند اقدام‌های تنبیهی باشد که در معاهده گنجانده‌شده‌اند. همچنین در درون چنین معاهده‌ای قوانینی در حمایت از دولت‌هایی گنجانده شود که مورد حمله سایبری قرار گرفته‌اند یعنی دولت‌های عضو در اسرع وقت با همکاری یکدیگر اقدام به شناسایی عامل حمله کنند و کمک‌های فنی و علمی را به دولت زیان‌دیده جهت رفع آسیب ایجادشده از حملات سایبری و جبران خسارات ایجادشده از حمله بکنند.

۲-۷. مشکل اجرای کنوانسیون سایبری توسط دولت‌های عضو

برای اینکه یک کنوانسیون سایبری در سطح جهانی مؤثر و مفید باشد باید اجرای آن از طرف دولت‌های عضو به نحو احسن و درست صورت گیرد، در غیر این صورت چنین معاهده‌ای مؤثر و کارساز نخواهد بود. به دلیل ویژگی‌های خاص فضای سایبری و فناوری‌های حوزه سایبری، مهم‌ترین مشکل یک کنوانسیون بین‌المللی سایبری، اجرای چنین معاهده‌ای است و همچنین طبق تجربه‌ای که از معاهدات دیگر وجود دارد دولت‌های عضو یک معاهده، زمانی طبق آن عمل می‌کنند که مطمئن شوند دیگر دولت‌ها نیز مطابق آن عمل می‌کنند. بسیاری را عقیده بر این است که هر معاهده بین‌المللی که هدفش محدود کردن فعالیت‌های سایبری دولت‌ها باشد به آسانی نمی‌تواند به موفقیتی دست یابد، زیرا دولت‌ها به‌ویژه دولت‌هایی که دارای فناوری پیشرفته‌ای در حوزه سایبر هستند تمایلی به محدود کردن فعالیت‌های سایبری خود نخواهند داشت؛ بنابراین جهت اجرای بهتر یک معاهده بین‌المللی نیاز است تا قبل از تدوین آن کارشناسان حقوق بین‌الملل و کارشناسان حوزه سایبر به‌گونه‌ای به تدوین چنین معاهده‌ای بپردازند که در هنگام اجرا با مشکلی مواجه نشود. با وجود این، نقض‌های حقوق بین‌الملل آن‌قدر متعدد و آشکار بوده‌اند که منجر شده بسیاری از مردم فکر کنند که حقوق بین‌الملل دارای ارزش اندکی است و اکنون ممکن است به‌عنوان چیزی که متعلق به گذشته است نگریسته شود (Elliot,2018:268). در بحث فناوری‌های عرصه سایبری می‌توان گفت اگرچه به دلیل ویژگی خاص سلاح‌های سایبری مانند ماهیت کاربرد دوگانه آن‌ها و این واقعیت که آن‌ها به‌طور ساده قابل پنهان شدن هستند کنترل این سلاح‌ها مشکل است (Singer and Friedman, 2014:127)؛ بنابراین اگر کنوانسیونی در حوزه سایبری تدوین شود و دولت‌ها نخواهند به‌درستی همکاری کنند به دلیل ویژگی‌های خاص فناوری‌های سایبری اجرای درست چنین معاهده بسیار دشوار و مشکل خواهد بود.

۳. فواید وجود کنوانسیون بین‌المللی حملات سایبری

برای اینکه یک کنوانسیون بین‌المللی درباره حملات سایبری مورد توجه و پذیرش دولت‌ها در سطح جهانی شود باید به‌گونه‌ای تنظیم شود که جذابیت‌ها و منافعی برای آن‌ها داشته باشد. چنین معاهده‌ای در سطح اول برای اینکه باعث مشارکت گسترده جهانی شود،

نخست باید دولت‌های دارای فناوری پیشرفته در حوزه سایبری را تشویق به عضویت در چنین معاهده‌ای کند، زیرا در صورت عدم عضویت چنین دولت‌هایی عضویت دولت‌های دیگر که از فناوری بالایی در حوزه سایبری برخوردار نیستند نه فایده‌ای خواهد داشت و نه چندان مؤثر خواهد بود؛ دوم اینکه، نیاز است تا یک گروه برجسته از کارشناسان حقوق بین‌الملل و کارشناسان حوزه سایبری با بررسی‌ها و مطالعات گسترده و تخصصی قوانینی تنظیم کنند که تمام قلمروهای حوزه سایبری را تحت پوشش قرار دهد و همچنین شایسته است این قوانین به‌گونه‌ای تنظیم شود که راه هرگونه سوءاستفاده از این قوانین بسته شود و به‌راحتی توسط دولت‌ها نقض نشود و باعث محدودیت رفتارهای خلاف قوانین و مضر دولت‌ها در فضای سایبری شود؛ سوم، در چنین کنوانسیونی اقدام‌های تنبیهی پیش‌بینی شود تا اگر دولت‌هایی برخلاف این کنوانسیون عمل کردند علیه آن‌ها بکار گرفته شود و بتوان ضمانت اجرایی چنین معاهده‌ای را تضمین کرد. اگرچه یک کنوانسیون بین‌المللی درباره حملات سایبری می‌تواند فواید متعددی داشته باشد اما در این قسمت مهم‌ترین فواید چنین معاهده‌ای مورد بررسی و تجزیه و تحلیل قرار می‌گیرد.

۳-۱. بازدارندگی از انجام حملات سایبری

به دلیل اینکه چارچوب حقوقی دقیق و شفافی برای حوزه سایبری وجود ندارد دولت‌هایی که دارای فناوری سایبری بالایی هستند، با سوءاستفاده از این وضعیت حملاتی را علیه رقبایشان انجام می‌دهند و چنان‌که شاهد هستیم تعداد حملات سایبری مخرب در جهان در حال افزایش است. تنها چیزی که می‌تواند جلوی این افزایش حملات سایبری را بگیرد تنظیم قواعد روشن و شفاف برای این حوزه است. به دلیل نبود قوانین روشن و شفاف و افزایش حملات سایبری و افزایش آسیب‌پذیری دولت‌ها در برابر آن‌ها، بازدارندگی سایبری در سال‌های اخیر مورد توجه فراوانی قرار گرفته است. وضعیت آنارشیک‌گونه فضای سایبر، آثار عمیقی روی منافع و امنیت ملی کشورها می‌گذارد. کنشگران ناشناس متعددی روزانه منافع و زیرساخت‌های حیاتی دیگر کنشگران را تهدید می‌کنند. دولت‌ها باید راهی برای کاستن از آسیب‌های این فضا بیابند و استراتژی بازدارندگی می‌تواند در این زمینه بکار آید (زابلی‌زاده و وهاب‌پور، ۱۳۹۷: ۴۷). هدف بازدارندگی سایبری کاهش توسل دولت‌ها به حملات سایبری علیه رقبایشان است. اگر دولت‌ها بدانند که هزینه انجام حملات سایبری علیه رقبایشان از نتیجه مورد انتظار حمله بیشتر است

هرگز اقدام به چنین کاری نخواهند کرد. برای بازدارندگی سایبری ابتدا باید ظرفیت‌های دفاعی کشورها تقویت شود. اگر ظرفیت‌های دفاعی کشورها به‌اندازه کافی قوی و قدرتمند باشد به دلیل احتمال موفقیت کمتر دولت‌ها اقدام به حملات سایبری علیه آن‌ها نخواهند کرد، زیرا می‌دانند چنین حمله‌ای نتیجه دلخواه آن‌ها را نخواهد داشت و هزینه بی‌فایده‌ای است. دوم، تقویت توان دولت‌ها جهت تنبیه حمله‌کنندگان و دادن پاسخ متقابل به آن‌ها نیز می‌تواند به هدف بازدارندگی سایبری کمک کند. چنانچه دولت‌ها بدانند اگر علیه دولت‌های دیگر اقدام به حمله سایبری کنند آن‌ها نیز در عوض دارای توانایی اقدام تلافی‌جویانه سایبری هستند، به‌هیچ‌وجه چنین حملاتی را انجام نخواهند داد. متخصصان حقوقی راهنمای تالین اعتقاد دارند که حقوق جنگ و اصول حقوق بین‌الملل بشردوستانه به‌طور مستقیم قابل کاربرد در حوزه فضای سایبر هستند و بنابراین نیاز به معاهدات بیشتر نیست ولی با توجه به ویژگی‌های فناوری‌های سایبری به نظر می‌رسد که چنین نیست.

مهم‌ترین هدف همه کنوانسیون‌های بین‌المللی کنترل تسلیحات فراهم کردن اطلاعات است. یکی از روش‌های فراهم کردن اطلاعات توسط کنوانسیون‌های بین‌المللی کنترل تسلیحات از طریق ایجاد سازوکارهایی برای مبادله منظم اطلاعات است. چنین مبادله اطلاعاتی ممکن است به‌صورت تضمین دوجانبه از طرف دولت‌ها باشد که درنتیجه آن، دولت‌ها درباره فعالیت‌ها، انگیزه‌ها و اهدافشان برای تضمین دادن به دولت‌های دیگر اطلاعات فراهم می‌کنند و یا ممکن است یک معاهده دارای سیستم کنترل باشد که فعالیت‌های دولت‌ها را از خارج کنترل کند (Abbott, 1993:4). روش دوم، فراهم کردن اطلاعات توسط کنوانسیون‌های بین‌المللی کنترل تسلیحات به‌وسیله ایجاد قوانین رسمی است که به‌طور شفاف موارد مجاز و غیرمجاز را مشخص کند. کنوانسیون‌های بین‌المللی کنترل تسلیحات به‌وسیله غیرقانونی اعلام کردن بعضی از رفتارهای دولت‌ها مقاصد آن‌ها را شفاف می‌کنند، چون اگر دولتی یک تعهد آشکار و الزام‌آوری را که در معاهده به آن اشاره شده نقض کند اهداف و مقاصد آن دولت کاملاً آشکار است. این کارکرد در حوزه سایبر نیز بسیار مهم است، زیرا به دلیل ویژگی خاص این حوزه توانایی‌ها و انگیزه‌های دولت‌ها اغلب مشخص نیست. با ایجاد قوانین شفاف و الزام‌آور یک کنوانسیون بین‌المللی مانع فعالیت‌های غیرمجاز دولت‌ها خواهد شد (Sangiovanni, 2017:19)؛ بنابراین با پیش‌بینی یک سیستم کنترل برای نظارت بر فعالیت‌های سایبری دول عضو کنوانسیون می‌توان

فعالیت‌های سایبری آن‌ها را زیر نظر داشت و بر آن‌ها نظارت کرد. همچنین با وضع قوانین مشخص درباره موارد استفاده مجاز و غیرمجاز از فناوری سایبری می‌توان به سهولت دولت‌های خاطی را شناسایی کرد و اقدام‌های تنبیهی را علیه آن‌ها به کار گرفت که این می‌تواند موجب بازدارندگی از انجام حملات سایبری شود.

۳-۲. مدیریت مؤثر بحران

فناوری سایبری بیش از دیگر سلاح‌های موجود در دنیا صلح و امنیت بین‌المللی را تهدید می‌کند، زیرا به دلیل ماهیت این فناوری، تشخیص اقدام‌های عمدی از غیرعمدی بسیار مشکل است. مدیریت مؤثر بحران فایده مهم دیگر یک کنوانسیون بین‌المللی سایبری جهت کاهش دادن خطر مخاصمه اتفاقی به‌وسیله افزایش شفافیت و معرفی سازوکارهایی برای مدیریت بحران است. یک هدف مهم معاهدات کنترل سلاح‌های هسته‌ای مذاکره شده در طول جنگ سرد، ایجاد کانال‌های ارتباطی بین ابرقدرت‌ها و بنابراین کاهش دادن خطر حوادث یا سوءتفاهم‌هایی بود که موجب جنگ می‌شد. بسیاری از کارشناسان سایبری عقیده دارند که خطرات ایجاد جنگ اتفاقی در فضای سایبر بیشتر از حوزه هسته‌ای است. یک دلیل مشکل تشخیص فعالیت‌های سایبری غیرمضر از حملات سایبری خصمانه آشکار است (Libicki, 2009). یک حمله سایبری علیه شبکه دفاع هوایی یک کشور حتی اگر اشتباهی باشد ممکن است باعث شود آن دولت نتیجه بگیرد که حملات عمدی هستند و نادانسته موجب یک جنگ نظامی شود. دلیل دیگر مشکل حملات عوامل غیردولتی است. یک حمله سایبری که توسط عوامل غیردولتی از قلمرو یک دولت دیگر شکل می‌گیرد ممکن است باعث شود که دولتی که مورد حمله قرار گرفته به‌طور اشتباه نتیجه‌گیری کند که آن دولتی که این حملات توسط عوامل غیردولتی از خاک آن انجام می‌گیرد، در انجام و شکل‌گیری این حملات دست دارد و این امکان دارد باعث شود تا علیه آن دولت دست به اقدام تلافی‌جویانه بزنند. با توجه به این مشکلات یک کنوانسیون سایبری باید تمرکزش بر کاهش دادن خطرات مخاصمات اتفاقی به‌وسیله ایجاد کانال‌های قوی ارتباط بین دولت‌ها و ایجاد سازوکارهای هشداردهنده ابتدایی اجباری باشد که به‌موجب آن دولت‌ها توافق کنند که اگر در قلمرو خود متوجه هرگونه حمله‌ای به کشورهای دیگر شدند فوراً به یکدیگر اطلاع‌رسانی کنند (Sangiovanni,2017:21)؛ بنابراین با توجه به وضعیت کنونی جهان،

شایسته است تا دولت‌ها جهت مدیریت و کنترل بحران‌هایی که ممکن است درنتیجه استفاده از این فناوری ایجاد شود هر چه سریع‌تر به تدوین معاهده‌ای بین‌المللی همت گمارند وگرنه با توجه به وضعیت کنونی جهان و افزایش رو به رشد استفاده از فناوری‌های سایبری و همچنین افزایش حملات سایبری بدون وجود کنوانسیون سایبری مدیریت بحران‌های ایجاد شده بسیار سخت و مشکل خواهد بود.

۳-۳. حل مشکل انتساب حملات سایبری

امروزه جنگ سایبری به یک واقعیت تبدیل شده است. این در حالی است که فقدان مرز در فضای سایبری، این امکان را برای مرتکبان حملات سایبری فراهم آورده است تا خود را در پس آدرس‌های اشتباهی و حیله‌های اینترنتی پنهان کنند؛ امری که شناسایی منشأ حمله سایبری را با دشواری‌هایی مواجه ساخته است (چهاربخش و قاسمی، ۱۳۹۱:۱۴۰). اگر هزینه‌های نقض یک کنوانسیون سایبری بین‌المللی درباره حملات سایبری تضمین نشود تأثیر در صحنه بین‌المللی زیاد نخواهد بود و اینجا مسئله انتساب و مسئولیت بین‌المللی دولت‌ها مطرح می‌شود. همچنین اگر در معاهده مشکل نحوه شناسایی متجاوزان حل نشود، هیچ ساز وکار معناداری برای اجرا و تنبیه نمی‌تواند طراحی شود. اگرچه تاکنون به مسئله انتساب در فضای سایبر با بدبینی نگریسته شده است بسیاری از کارشناسان بر این عقیده هستند که با اختصاص وقت و منابع کافی مسئله انتساب موثق حملات سایبری قابل حل است حداقل هنگامی که حملات با مقیاس بالا علیه زیرساخت‌های حیاتی صورت گیرد. با وجود این، انتساب موثق هم زمان‌بر و هم پرهزینه است. انتساب موثق نیاز به پاسخ اضطراری سریع و جمع‌آوری اطلاعات و مدارک مرتبط با حملات دارد. این نیازمند آن است تا دولت‌ها متخصصینی را جهت بررسی تجهیزات الکترونیک و وسایل ذخیره داده‌ها آموزش دهند. اگر داده‌ها و اطلاعات جمع‌آوری شود آن‌ها باید برای انتساب مورد تجزیه و تحلیل قرار گیرد. این ممکن است به ابزار ماهرانه‌ای جهت تجزیه و تحلیل و تفسیر نیاز داشته باشد و ممکن است به دسترسی به تعدادی از منابع مختلف اطلاعاتی وابسته باشد. چنین توانایی‌های فنی در حال حاضر فراتر از توان بسیاری از دولت‌ها است.طراحی یک سازوکار انتساب مشترک دولت‌ها را قادر خواهد کرد تا در منابع فنی و مالی سهیم شوند و این باعث خواهد شد انتساب موثق برای بیشتر دولت‌ها با هزینه کمتر فراهم شود

.(Sangiovanni,2017:22)

هنگام ملاحظه اینکه چطور یک سیستم را برای انتساب سایبری مشترک طراحی کرد، مدل «پیمان منع جامع آزمایش‌های هسته‌ای»[1] بهترین نمونه است. «پیمان منع جامع آزمایش هسته‌ای» توسط مجمع عمومی سازمان ملل در سپتامبر ۱۹۹۶ پذیرفته شده اما هنوز اجرایی نشده است. این پیمان، کشورهای عضو را از هرگونه انفجار هسته‌ای در هر مکانی تحت قلمرو یا کنترل کشورهای عضو منع می‌کند. یکی از مهم‌ترین ملزومات اجرای این پیمان، استقرار سامانه‌های نظارت بین‌المللی از جمله ایستگاه‌های لرزه‌نگاری فراصوت است. تاکنون بیش از ۱۶۰ کشور این معاهده را امضا کرده و به تصویب مجالس خود رسانده‌اند؛ اما برای اجرایی شدن آن لازم است که ۴۴ کشور نام برده در پیوست ۲ این پیمان، آن را تصویب کنند که از این تعداد، هنوز ۸ کشور (ایران، امریکا، هند، مصر، چین، پاکستان، کره شمالی و اسرائیل) این اقدام را عملی نکرده‌اند. معاهده ۱۸۰ روز پس از امضا و تصویب آن از سوی این ۸ کشور وارد مرحله اجرایی خواهد شد.

با در نظر گرفتن سیستم کنترل بین‌المللی «پیمان منع جامع آزمایش هسته‌ای» به عنوان نمونه نیاز است تا یک سازوکار انتساب مشترک طراحی شود تا به دولت‌ها در ایجاد تأسیسات سایبری جمع‌آوری داده‌ها و تحلیل فنی با هزینه کم کمک کند. چنین سازوکاری به کشورهایی که اکنون توانایی‌های فنی بومی جهت جمع‌آوری و تحلیل داده‌ها برای انتساب ندارند کمک می‌کند و ممکن است انگیزه مهمی برای آن‌ها جهت عضویت در یک معاهده سایبری باشد. اگرچه یک سازوکار انتساب مشترک به کشورهایی که هم‌اکنون فناوری سایبری پیشرفته‌ای دارند کمک خواهد کرد. انتساب یک‌جانبه توسط یک دولت به اندازه انتساب جمعی دارای اعتبار نیست. نتیجه‌ای که از کشور عراق درنتیجه پیدا نکردن سلاح‌های کشتارجمعی به دست آمد نشان داد که نتیجه‌گیری‌های به دست آمده توسط سازمان‌های بین‌المللی مرتبط از آن‌هایی که توسط هر کشور به‌طور جداگانه به دست می‌آیند دارای اعتبار بیشتری هستند (Ifft, 2005:3). در حوزه سایبری اگر دولتی بخواهد بر اساس برداشت خودش نسبت به مسئله انتساب علیه منبع مظنونی، حمله سایبری کند این ممکن است موجب اتهام از طرف کشورهای دیگر در ملاحظه با منابع و روش‌های انتساب شود و می‌تواند به عنوان یک عمل تجاوز بین‌المللی تفسیر شود. به

1. Comprehensive Test Ban Treaty

خاطر این دلایل انتساب بهتراست به یک عامل بی‌طرف بین‌المللی محول شود که وظیفه‌اش فراهم کردن داده‌های موثق و تحلیل آن‌ها برای دولت‌هایی است که به آن‌ها نیاز دارند (Sangiovanni, 2017: 23).

۳-۴. تجویز اقدام‌های متقابل

اینکه دولت‌ها چطور به حملات سایبری پاسخ دهند به‌طور عام نادیده گرفته شده است. به جای اندیشیدن درباره اقدام‌های متقابل تمرکز روی دفاع مشروع قرار گرفته که در ماده ۵۱ منشور سازمان ملل بیان شده است و به دولت‌ها اجازه می‌دهد تا به حملات مسلحانه از جمله حملات سایبری که در چارچوب حملات مسلحانه قرار می‌گیرند اقدام به دفاع مشروع کنند. تمرکز بر حملات سایبری با این ذهنیت که به حد حمله مسلحانه برسند تا بتوان در برابر آن‌ها به دفاع مشروع متوسل شد مشکلاتی را برای دولت‌ها ایجاد می‌کند، زیرا تعداد کمی از حملات سایبری از آستانه حمله مسلحانه عبور کرده‌اند و عملیات سایبری مخرب زیر آن سطح نیز انجام می‌گیرند. زمانی که مسئله انتساب حملات سایبری حل شد اقدام‌هایی باید برای تنبیه متخلفان سایبری اتخاذ شود و این نیازمند یک کنوانسیون بین‌المللی سایبری است تا این کار را انجام دهد. بر اساس ماده ۴۹ (۱) طرح مسئولیت بین‌المللی دولت، دولت صدمه‌دیده می‌تواند علیه دولت مسئول تخلف بین‌المللی، برای وادار کردن دولت مسئول به ایفای تعهدات خود، به اقدام‌های متقابل مبادرت ورزد (حلمی، ۱۳۸۷: ۳۹۳). اقدام‌های متقابل باید با زیان وارده متناسب باشند و با توجه به شدت فعل متخلفانه بین‌المللی و حقوق مورد بحث انجام شوند (The Draft Articles on Responsibility of Sates for Internationally Wrongful Acts,2001,Art 51). اگرچه در حال حاضر هنوز هیچ معاهده بین‌المللی درباره اینکه چه چیزی یک پاسخ متناسب به یک حمله سایبری را شکل می‌دهد وجود ندارد و نه هیچ سازوکار معاهده‌ای برای تجویز چنین پاسخی موجود نیست؛ بنابراین این یک وضعیت بسیار خطرناک است. یک کنوانسیون سایبری با وضع قوانین شفاف و با تعیین اندازه و ماهیت اقدام‌های تلافی‌جویانه در برابر حملات سایبری احتمال جنگ و درگیری بین دولت‌ها را کاهش می‌دهد.

۳-۵. تعیین حدود و قلمرو مسئولیت دولت در فضای سایبر

فضای سایبری به‌طور گسترده‌ای در حال تبدیل شدن به یک قلمرو مورد علاقه برای مجرمان است. این به دلیل ماهیت فضای سایبری است که در شکل ناشناس بودن، فوری بودن تأثیرات، عدم انتساب عمل و نبود هیچ‌گونه مرز بین‌المللی نمود پیدا می‌کند (Sandeep & Sharma,2017:1347). برای اینکه یک کنوانسیون سایبری مؤثر باشد، باید این مسئله را در نظر بگیرد درباره اینکه چطور حقوق مسئولیت دولت در فضای سایبر بکار می‌رود. بدون شباهت به حوزه هسته‌ای که به‌طور منظم تحت حاکمیت دولت‌ها است حوزه سایبری حد حملات متناوب را به‌وسیله گروه‌های غیردولتی بالا می‌برد. این ویژگی فضای سایبری این سؤال را ایجاد می‌کند که چه موقع دولت‌ها می‌توانند و باید مسئول فعالیت‌های سایبری به‌وسیله عوامل غیردولتی باشند. بر اساس اصل حاکمیت، دولت‌ها ملزم هستند تا بر زیرساخت‌ها و فعالیت‌های سایبری در قلمرو خودشان کنترل داشته باشند (Tallin Manual 2013,rule 1). همچنین بر اساس حقوق بین‌الملل، یک دولت ممکن نیست آگاهانه اجازه دهد که قلمروش برای اعمالی که مخالف حقوق دولت‌های دیگر است مورد استفاده قرار گیرد (Corfu Channel Case, 1949). مطابق این اصول حقوق بین‌الملل، دولتی که عملیات سایبری یک بازیگر غیردولتی به‌طور مستقیم قابل انتساب به آن است تا جایی که عامل غیردولتی تحت کنترل مستقیم یا تحت دستورات حکومت آن دولت دست به اقدام می‌زند می‌تواند از نظر حقوقی مسئولیت داشته باشد و اینکه دولت زیان‌دیده می‌تواند در برابر آن متوسل به اقدام‌های متقابل شود. اصل مسئولیت مستقیم باید به‌طور رسمی در یک کنوانسیون بین‌المللی سایبری تأیید شود.

۴. تشویق به عضویت دولت‌ها در کنوانسیون بین‌المللی حملات سایبری

برای اینکه دولت‌ها به عضویت معاهده‌ای درآیند باید انگیزه‌ای برای آن‌ها جهت عضویت در چنین معاهده‌ای وجود داشته باشد در غیر این صورت لزومی ندارد آن‌ها تن به پذیرش معاهده بدهند. درباره عضویت دولت‌ها در یک کنوانسیون بین‌المللی درباره حملات سایبری نیز وضعیت می‌تواند این‌گونه باشد. در بحث پیوستن دولت‌ها به یک کنوانسیون بین‌المللی درباره حملات سایبری اگر در چنین کنوانسیونی کمک‌های فنی و مالی جهت کمک به افزایش توان دفاع سایبری دولت‌ها گنجانده شود می‌تواند انگیزه بسیار مهمی برای دولت‌ها جهت عضویت در چنین

معاهده‌ای باشد. یک کنوانسیون سایبری اگر بتواند دولت‌ها را ملزم کند تا به کشورهای عضو آن معاهده که مورد حملات سایبری مخرب قرار می‌گیرند کمک کند، باعث می‌شود دولت‌ها تشویق به عضویت در چنین معاهده‌ای شوند. کمک مالی دولت‌های عضو کنوانسیون جهت تعمیر و بازسازی تأسیسات حیاتی دولت صدمه‌دیده نیز محرکی است که باعث عضویت دولت‌های بیشتر در چنین معاهده‌ای خواهد شد. به عنوان نمونه کنوانسیون سلاح‌های شیمیایی انواعی از کمک‌های اضطراری را برای دولت‌های عضو فراهم می‌کند و یک کمک مالی داوطلبانه برای کمک و حفاظت از سلاح‌های شیمیایی ایجاد کرده است Chemical Weapons (Convention,1997:art 8). همچنین دبیرخانه فنی به‌وسیله تجهیزات کشف و سیستم‌های هشداردهنده تجهیزات حفاظتی و کمک فنی به دولت‌های عضو کمک می‌کند تا در برابر حملات شیمیایی از آن‌ها محافظت بیشتری شود (Weapons Convention,1997:art 8). این می‌تواند در مورد سلاح‌های سایبری نیز مورد استفاده قرار گیرد و در کنوانسیون بین‌المللی درباره حملات سایبری نیز انواعی از کمک‌ها برای دولت‌های عضو در موارد اضطراری پیش‌بینی شود و همچنین کمک‌هایی به دولت‌هایی که از توان سایبری ضعیفی برخوردارند و نسبت به دیگر اعضا از آسیب‌پذیری بیشتری برخوردارند لحاظ شود تا این موارد بتواند باعث تشویق دولت‌ها به عضویت در چنین معاهده‌ای شود.

فرجام سخن

در حال حاضر فضای سایبری به عرصه کشمکش دولت‌ها در سطح بین‌المللی تبدیل شده است؛ به نحوی که هرروزه حملات سایبری متعددی در این فضا انجام می‌گیرد. چنین وضعیتی چالشی جدی و مهم برای صلح و امنیت بین‌المللی است. با وجود تهدیدات بسیار زیاد فناوری‌های حوزه سایبری تعداد کمی از معاهدات در مورد مسائل امنیت سایبری وجود دارد. مهم‌ترین معاهدات بین‌المللی در حوزه سایبری «کنوانسیون ۲۰۰۱ جرائم سایبری» و پروتکل الحاقی ۲۰۰۶ آن و «توافقنامه امنیت اطلاعاتی بین‌المللی سازمان همکاری شانگهای ۲۰۰۹» هستند. درباره این دو معاهده باید گفت که هم تعداد اعضا و هم قلمرو آن‌ها دارای محدودیت است. مذاکره بر سر یک معاهده بین‌المللی جامع درباره حملات سایبری تاکنون با عدم پذیرش به‌ویژه از طرف دولت‌های غربی همراه بوده است. از نظر تاریخی بحث‌های مهمی که تاکنون در

حوزه سایبر مطرح شده این بوده است که حقوق بین‌الملل موجود را در حوزه فضای سایبر بکار گیرند. دستورالعمل تالین قابل اعمال در جنگ‌های سایبری که دارای مجموعه‌ای از قوانین است که حقوق بین‌الملل موجود مانند حق بر جنگ، حقوق بین‌الملل بشردوستانه و حقوق مسئولیت دولت در فضای سایبر چگونه بکار می‌رود مهم‌ترین نتیجه ذکرشده بحث‌هایی بوده است. با این حال، راهنمای تالین نتوانست خارج از گروه محدود اعضای ناتو مورد توجه قرار گیرد. همچنین دستورالعمل تالین قوانین جدید بین‌المللی برای حوزه سایبر ارائه نمی‌دهد بلکه قوانین حقوق بین‌الملل موجود را تفسیر می‌کند. تاکنون این تفسیر نتوانسته دولت‌ها را تشویق کند تا فعالیت‌هایشان را در فضای سایبر محدود کنند.

برای مواجهه با چنین وضعیتی نیاز است تا دولت‌ها با همکاری هم اقدام به تدوین یک کنوانسیون بین‌المللی درباره حملات سایبری کنند. اگرچه تدوین یک کنوانسیون بین‌المللی عملی سخت و طاقت‌فرسا است ولی به هر نحو ممکن چنین کاری هر چه سریع‌تر باید انجام گیرد. بر سر راه تدوین چنین کنوانسیونی موانع متعددی وجود دارد که در این مقاله به تشریح بررسی شده است مانند فقدان تعریف مشخص از حمله سایبری، زمان‌بر بودن مذاکره بر سر چنین کنوانسیونی، تغییر سریع فناوری، کارکرد دوگانه فناوری‌های سایبری، تعیین ماهیت و چارچوب کنوانسیون، مشکل اجرای کنوانسیون توسط دولت‌های عضو و عدم تمایل قدرت‌های بزرگ سایبری؛ اما از بین این موانع مهم‌ترین آن‌ها عدم تمایل قدرت‌های بزرگ سایبری به تشکیل چنین کنوانسیونی است، زیرا در حال حاضر فضای سایبری مزایا و فواید زیادی را نصیب چنین دولت‌هایی می‌کند. با بهره‌گیری از توان سایبری بالا کشورهایی که توانایی سایبری بالایی دارند بدون اینکه به‌راحتی شناسایی شوند حملات سایبری را با هزینه بسیار کم علیه رقبایشان انجام می‌دهند درحالی‌که خسارات منتج شده از این حملات بسیار زیاد است. تنها زمانی می‌توان دولت‌ها را در سطح بین‌المللی تشویق به عضویت در چنین معاهده‌ای کرد که فوایدی برای آن‌ها داشته باشد یا از این وضعیت موجود احساس خطر کنند. با توجه به اینکه قدرت‌های سایبری در سطح دنیا در حال افزایش هستند انحصار سایبری قدرت‌هایی مانند ایالات‌متحده امریکا، اسرائیل، روسیه و چین در حال کاهش است و این موجب می‌شود که با حس خطر حملات سایبری چنین کشورهایی خودشان جهت تدوین یک کنوانسیون بین‌المللی درباره حملات سایبری پیش‌قدم شوند، زیرا در صورت عدم همکاری قدرت‌های بزرگ سایبری تدوین و

شکل‌گیری چنین معاهده‌ای عملاً غیرممکن خواهد بود؛ بنابراین با توجه به سرمایه‌گذاری‌هایی که دولت‌ها در سطح جهانی در حوزه فناوری سایبری انجام می‌دهند و افزایش تعداد قدرت‌های سایبری در سطح جهانی امید به تدوین چنین کنوانسیونی بیش از پیش افزایش یافته است، زیرا خطر و مضرات حملات سایبری بیشتر از هر زمانی برای دولت‌ها در سطح جهانی آشکار شده و این عاملی است که به تدوین یک کنوانسیون بین‌المللی درباره حملات سایبری بیشتر از هر چیز دیگری کمک خواهد کرد.

منابع

الف. فارسی

اصلانی، جابر، رنجبریان، امیرحسین (۱۳۹۴) «بررسی تطبیقی و تحلیل تعریف حمله سایبری از منظر دکترین، رویه کشورها و سازمان‌های بین‌المللی در حقوق بین‌الملل»، **فصلنامه تحقیقات حقوقی**، شماره ۷۱، صص ۲۵۷-۲۸۷.

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

زابلی‌زاده، اردشیر، وهاب پور، پیمان (۱۳۹۷) «قدرت بازدارندگی در فضای سایبر»، **فصلنامه مطالعات بین‌رشته‌ای رسانه و فرهنگ**، دوره ۸، شماره ۱۵، صص ۷۴-۴۷.

قاسمی، علی و چهاربخش ویکتور بارین (۱۳۹۱) «حملات سایبری و حقوق بین‌الملل»، **مجله حقوقی دادگستری**، دوره ۷۶، شماره ۷۸، صص ۱۱۵-۱۴۶.

قاسمی غلامعلی و نامدار، سعید (۱۳۹۷) «بررسی مفهوم دفاع مشروع در پرتو حملات سایبری (با تأکید بر حمله استاکس‌نت به تأسیسات هسته‌ای ایران)»، **نشریه مطالعات حقوقی دانشگاه شیراز**، دوره ۱۰، شماره ۱، صص ۲۳۵-۱۹۹

ب. انگلیسی

Abbott, Kenneth W. (1993) "Trust but Verify:' the Production of Information in Arms Control Treaties and other International Agreements" **Cornell International Law Journal**.Vol 26, Issue 1, pp. 1-58

Abbott, Kenneth W. & Snidal, Duncal (2000) "Hard and Soft Law in International Governance", **International Organization**,Vol 54,

Issue 3, pp. 421–456.

Clarke, Richard A. & Knake, Robert K. (2010) **Cyber War: The Next Threat to National Security and What to Do about It**, New York: Harper Collins Publisher.

Elliot, Edward (2018. "Future of International Law", **California Law Review**, Voiume 6, Issue 4, pp. 268-278.

Eilstrup-Sangiovanni, M. (2017) "Why the World Needs an International Cyberwar Convention", **Philosophy and Technology**,Vol 31, Issue 3, pp. 379-407.

Khan, Asif and Ullah, Maseeh and Rehman, Fazal and Ghani, Abdul (2017) "Cyber Attacks in International Law: From Atomic War to Computer War",**Available at SSRN**: https://ssrn.com/abstract =3064787 or http://dx.doi.org/10.2139/ssrn.3064787

Libicki, Martin (1996) **What is Information Warfare?** Center for Advanced Concepts and Technology Institute for National Strategic Studies, Third Edition.Washington,DC:Institute for National Strategic Studies

Lucas, George (2017) **Ethics of Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare**, Oxford: Oxford University Press.

Sandeep, Mittal and Priyanka Sharma (2017) "Enough Law of Horses and Elephants Debated… Let's Discuss the Cyber Law Seriously", **International Journal of Advanced Research in Computer Science**, Vol. 8, pp. 1343-1348.

Schmitt, Michael N. and Liis Vihul (2016) **The Emergence of International Legal Norms for Cyberconflict**, In FritzAllhoff, Adam Henschkeand BradleyJ. Strawser (eds.) Binary Bullets. The Ethics of Cyberwarfare (pp. 34–55), Oxford University Press.

Singer, Peter W and Allan Friedman (2014) **Cybersecurity and Cyberwar:What Everyone Needs to Know?** Oxford,UK: Oxford University Press.

Documents

Al Aridi, Alaa (2018) Disparity between Current Legal Frameworks and Digital Transformation Development in GCC States, 6th

International Conference of PhD Students and Young Researchers, ISBN 978-609-459-986-6, Vilnius University.

Chemical Weapons Convention, 1997

Draft Articles on Responsibility of states for Internationally wrongful Acts, Adopted by International law Commission of United Nations Organization at 2001.

Finnemore, Martha (2011) Cultivating International Cyber Norms,In Americas Cyber Future: Security and Prosperity in the Information Age,eds. Kristin Lord and Travis Sharp,vol.II,pp 89-100

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).

Ifft, Edward (2005) Witness for the prosecution: international organizations and arms control verification. Arms Control Association, Nov.1. https://www.arms control.org/act/2005_11 /NOV-Ifft.

Libicki, Martin (2009) Cyberdeterrence and Cyberwar, Santa Monica: RAND.

Sanger, David E, John Markoff and Thom Shanker (2009) BU.S. Steps up Effort on Digital Defenses. NY Times, April 27.(Last visited November 2019)

Smith, Brad (2017) Transcript of Keynote Address at the RSA Conference 2017 "The Need for a Digital Geneva Convention" President Microsoft Corporation San Francisco, California February 14

Tallin 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 Defense Centre of Excellence, Cambridge University Press

The Corfu Channel Case (United Kingdom v Albania) (Merits), Judgement of 9 April 1949, ICJ Reports 1949.