فصلنامهٔ امنیت پژوهی (علمی-پژوهشی)
سال پانزدهم: شماره ۵۳ - بهار ۱۳۹۵

Amniat Pajouhi: A Security Studies Quarterly Research Journal
Vol 15, No 53, 2016 Spring

تاریخ دریافت: ۹۴/۵/۰۵ **تاریخ تأیید: ۹۴/۷/۱۵**

بررسی تهدیدهای پیش‌نویس موافقت‌نامه امنیت سایبری از منظر منافع ملی جمهوری اسلامی ایران

سید احمد میرزایی[۱]
علی صالحی[۲]
سعید سعیدی[۳]

چکیده

با رشد روزافزون استفاده از فضای مجازی در زندگی بشری، این پدیده نوین فرصت‌ها و تهدیدهای جدید و ناشناخته‌ای را به همراه خود آورده است. جدای از فرصت‌های آن، مهم‌ترین راه حل برای تأمین امنیت دولت‌ها، تدوین موافقت‌نامه‌ای برای امنیت فضای سایبری است که پیش‌نویس ارائه‌شده توسط روسیه، مطالعه موردی[۴] این مقاله است، اما نباید از یاد ببریم که مطمئناً هر موافقت‌نامه‌ی، ازآن‌رو که دولت‌ها را متعهد می‌سازد تا حوزه حاکمیتی خود را محدود سازند، تبعات سیاسی بر منافع، قدرت و امنیت ملی دولت‌های تعهد دهنده دارد و شاید بتوان گفت که خود این موافقت‌نامه نیز برای منافع دولت‌ها تهدیدهای به همراه خواهد داشت. ازاین‌رو سؤال پژوهش پیش‌رو این است که تهدیدهای پیش‌نویس ارائه‌شده توسط دولت روسیه برای منافع ملی جمهوری اسلامی ایران چه هستند؟ در این راه فرضیه ما آن است که این موافقت‌نامه نه‌تنها حاکمیت ملی جمهوری اسلامی ایران را محدود می‌سازد بلکه برای امنیت ملی و منافع ما تهدیدزا خواهد بود. در این راه پژوهشگران با استفاده از رویکرد روش‌شناختی هرمنوتیک و شیوه توصیفی- تحلیلی سعی به بازشناسی و تشریح مسئله طرح شده داشته‌اند.

واژگان کلیدی: *منافع ملی، امنیت ملی، امنیت سایبر، تهدید صلح بین‌المللی، پیش‌نویس موافقت‌نامه امنیت سایبری*

---

۱. استادیار رشته دیپلماسی کنترل تسلیحات دانشگاه صنعتی مالک اشتر (ahmadm@yahoo.com)
۲. کارشناس ارشد دیپلماسی کنترل تسلیحات دانشگاه صنعتی مالک اشتر (salehi.ali2008@yahoo.com)
۳. کارشناسی ارشد اطلاعات دانشکده علوم وفنون فارابی (shamsshams202@gmail.com)

4. Case Study

مقدمه

تقریباً در اواخر سال ۱۳۸۸ بود که منابع اطلاعاتی غرب، خبر از حملـه سـایبری بـه تأسیسـات هسته‌ای کشورمان دادند. با آن‌که این حمله از سوی سازمان انرژی اتمی مورد تأیید قرار گرفت اما گفته شد که این حمله دفع شده است. بعدها گفته شد که گویا این حمله سایبری پـروژه‌ای مشترک بین نیروهای ارتش سایبری اسرائیل و امریکا بوده است (Diplomacyirani, 2014).

این حمله که توسط بدافزاری، از نوع ویروس، تحت عنـوان «اسـتاکس‌نـت[1]» صـورت پـذیرفت، دارای پیچیدگی در برنامه‌نویسی و نحوه عملیات سایبری بوده است؛ اما تهدیدها فضـای سـایبر به استاکس‌نت محدود نمی‌شود بلکه حدودا در دهه ۱۹۹۰ نسل سوم جرائم رایانه‌ای که مختص فضای سایبر است، رشد چشمگیری یافت به‌نحوی‌که محیط مذکور را به فضایی مخوف تبـدیل نمود که دارای انواع تهدیدها و ناامنی‌هاست. به عبارت بهتر به عقیده خانم اکانل از ابتدا، محیط مجازی برای امن بودن خلق نشده است (O'Connell, 2012:25).

ناامنی سایبری انواع و اقسامی دارد. از تبلیغات و به راه انداختن تبلیغات سیاسی[2] علیـه دولتـی خاص گرفته تا سرقت و کلاه‌برداری‌های چندملیتی؛ یعنی اینکه تهدیدها سایبری فقط به حوزه سیاسی محدود نمی‌شود بلکه شامل تهدیدهای علیه بنیان‌هـای خـانواده، اقتصـاد، صـنعت و ... است. به عبارتی بهتر برای هر چیزی که درجایی، برای کسی باارزش باشد و آن چیز بتوانـد بـا اینترنت و یا وسایل الکترونیکی که دارای بخش‌های نرم‌افزاری هسـتند و فضـایی بـرای ذخیـره اطلاعات دارند[3]، مرتبط شود، فضای سایبر می‌تواند خطرساز باشـد. ازایـن‌رو بـه‌شـدت نیـاز بـه اقدامی در جهت امنیت‌زایی در فضای مجازی، احساس می‌شود.

اما ازآن‌رو که محیط مجازی، محیطی است بین‌المللی که دارای خصوصیات فضـای مکـانیکی و فیزیکی عادی نیست، نمی‌توان برای آن بین دولت‌ها مرز و محدوده‌ای مشخص ترسیم نمود تـا

1. Stuxnet
2 .Propaganda
3. Hard

در حیطه آن به اعمال حاکمیت بپردازند (Balayan, 2013:63). باآنکه بسیاری از دولت‌ها در حیطه حاکمیتی خود[۱] قوانینی را برای امنیت فضای سایبر تدوین نموده‌اند، اما به دلیل آن‌که محیط سایبر محیطی فراملی است، نمی‌توان آن قوانین را در تمامی جوانب مفید دانست؛ به‌عبارت‌دیگر در محیط سایبر ما با بحران خلأ حاکمیت، خلأ داشتن مرزهایی مشخص و به‌صورت کلی‌تر با خلأ مفاهیم حقوقی روبرو هستیم. ازاین‌رو درگام اول نیاز است این خلأها پرگردند؛ و در گام بعدی به فکر تشکیل موافقت‌نامه‌ی همه‌جانبه برای امنیت فضای مجازی باشیم.

در این مقاله پژوهشگران با علم به این نکته که پیش‌نویس موافقت‌نامه امنیت فضای مجازی ارائه‌شده از سوی روسیه (FMRU,2011)، همانند هر پدیده دیگر به همراه خود تهدیدها و فرصت‌هایی را به آورده است، از بررسی فرصت‌های آن پیش‌نویس صرف‌نظر نموده و با ذکر دلایلی به تشریح خطرات و تهدیدها آن برای امنیت و منافع ملی جمهوری اسلامی ایران پرداخته‌اند. لازم به ذکر است، بررسی این موضوع که «آیا اساساً داشتن یک معاهده بین‌المللی برای فضای سایبر موافق منافع ملی ما است؟» نیازمند پژوهشی جداگانه است که از آن صرف‌نظر نموده‌ایم و این سؤال را به‌عنوان سؤال اصلی این پژوهش انتخاب نمودیم که «تهدیدها و مضرات پیش‌نویس کنونی موافقت‌نامه امنیت فضای سایبر کدامند؟» در این راه ما با بررسی بند به بند موافقت‌نامه مذکور، با دیده شک به آن نگریسته و سعی داریم با مورد مقایسه قرار دادن آن با دیگر موافقت‌نامه‌های خلع سلاح، تهدیدها آن را برشماریم

طرح مسئله

امروزه با توجه به گسترش فناوری‌های دیجیتال و کاربردهای گسترده آن، بسیاری از دولت‌ها طرح‌های توسعه و زیرساخت‌های خود را با محوریت فضای سایبر بنا نهاده‌اند. در این راستا بسیاری از دولت‌ها زیرساخت‌های کلیدی و حیاتی خود را با استفاده از فضای مجازی کنترل

۱. منظور حوزه حاکمیتی با تعریف سنتی است.

می‌کنند که امکان آسیب‌پذیری هرچه بیشتر آنان را فراهم می‌نماید. دولت ایران نیز از این قاعده مستثنا نیست و بسیاری از ارتباطات، اطلاعات و بنیان‌های پیشرفت خود را بر فضای مجازی و قابلیت‌های آن بنا نهاده است؛ که با توجه به گسترش روزافزون تهدیدها سایبری، بستری مناسب برای ضربه زدن به نظام مقدس جمهوری اسلامی از سوی دشمنان ایران فراهم آمده است.

از طرف دیگر با توجه به تهدیدهای که فضای سایبر برای دولت‌ها و امنیت نظام بین‌المللی به همراه آورده است؛ هرکدام از اعضای جامعه بین‌المللی در راه دستیابی به امنیت و ایجاد فضای مجازی امن‌تر تلاش‌هایی صورت داده‌اند؛ که مهم‌ترین این اقدامات، ممارستی بوده است که دولت روسیه برای ارائه پیش‌نویسی به‌منظور ایجاد امنیت در فضای سایبر، از خود نشان داده است. هدف روسیه از این اقدام، به‌ظاهر این بوده است که با تدوین قوانینی جامع بر فضای سایبر، می‌توان امنیت این حوزه را تأمین نمود. البته باید به یاد داشت که هر عهدنامه بین‌المللی به‌خودی‌خود امنیت‌زا نیست بلکه نحوه اجرا و پایبندی به آن است که برای جامعه بین‌المللی امنیت به ارمغان می‌آورد. ازاین‌رو طبیعی است که هر عهدنامه، توافق، برنامه اقدام مشترک و موافقت‌نامه بین‌المللی محدودیت‌هایی را به همراه داشته باشد. پس منطقی است که دولت‌ها باید در هنگام الحاق و پذیرش به آن‌ها، محدودیت‌های آن توافق‌نامه را در نظر داشته و بر اساس آن‌ها برای الحاق یا عدم الحاق به آن معاهده برنامه‌ریزی نمایند.

مطمئنا اگر پیش‌نویس مذکور به موافقت‌نامه‌ی جهان‌شمول تبدیل گردد، همانند دیگر عهدنامه‌های بین‌المللی، الزامات و محدودیت‌هایی را برای جمهوری اسلامی ایران به همراه خواهد آورد؛ که با توجه به قابلیت‌های تهدیدهای فضای مجازی، باید دولت‌مردان، تصمیم‌سازان و جامعه علمی ایران به این نکته بیاندیشند که کدام ماده و تبصره موافقت‌نامه و کدام تهدید فضای سایبر برای منافع ملی و امنیت جمهوری اسلامی ایران خطرهای بیشتری دارد؛ و باید مذاکره‌کنندگان ایرانی در فرایند تدوین پیش‌نویس موافقت‌نامه امنیت سایبری روسیه، نسبت

به آن‌ها حساس‌تر بوده و بر حذف یا ترمیم آن‌ها پافشاری بیشتری نمایند. سعی پژوهشگران در این مقاله بر آن بود که بر پیش‌نویس مذکور تمرکز نمایند؛ ازاین‌رو سؤال اصلی این پژوهش این است که تهدیدها پیش‌نویس ارائه‌شده توسط دولت روسیه برای منافع ملی جمهوری اسلامی ایران چه هستند؟

اهمیت و ضرورت

نظر به وابستگی منافع ملی به فضای سایبر و قابلیت‌های دنیای مجازی برای تولید و تبادل فناوری، علاوه بر فرصت‌ها، دنیای مجازی تهدیدها فراوانی نیز برای امنیت ملی دولت‌ها ایجاد کرده است. ازاین‌رو نیاز است که راهکاری مطمئن برای ایجاد فضای سایبری امن تدارک دیده شود. پیش‌نویس موافقت‌نامه مورد بحث در صورت تصویب و لازم‌الاجرا شدن، تأثیر مستقیمی بر فضای مجازی، اقدامات دولت‌ها در آن[1]، شیوه‌های تجارت و تبادل اطلاعات و ... دارد. این موارد و تغییرات اعمالی بر آن‌ها می‌توانند زندگی روزمره بسیاری از انسان‌ها را دست‌خوش تغییر نماید. چراکه فضای مجازی همان‌طور که قابلیت‌های بسیاری برای توسعه در اختیار دولت‌ها قرار می‌دهد می‌تواند خطرساز بوده و ارکان دولت‌ها را هدف قرار دهد. ازاین‌رو دور از ذهن نیست که دولت‌ها اتباع، شرکت‌ها و ... تحت صلاحیت حاکمیتی خود را ملزم به پیروی از قوانینی برای به نظم کشیدن فضای مجازی بنمایند؛ اما نکته‌ای که در محافل علمی و بخصوص حقوقی در این مورد مطرح شده این است که ازآن‌رو که محیط سایبر دارای قابلیت‌های فیزیکی نیست، چگونه می‌توان مرزی مشخص برای اقدامات حقوقی دولت‌ها ترسیم نماییم تا از این رهگذر تداخلی در منافع و قوانین دولت‌ها با یکدیگر پیش نیاید؟ جواب سؤال در برخورد اول بسیار ساده است و آن تدوین موافقت‌نامه‌ی بین‌المللی برای امنیت در فضای مجازی است؛ اما همان‌گونه که سیاست‌پژوهان و متفکرین حوزه امنیت کشورمان معتقدند تدوین موافقت‌نامه‌ی

۱.اعم از امور نظامی و غیر نظامی (حوزه‌ای که در ایران تحت عنوان فاوا شناخته می‌شود)، تعریف مصادیق مجرمانه و غیرمجرمانه (که در ایران تحت عنوان فتا موردبررسی قرارمی گیرد)، تعریف مصادیق حاکمیتی و غیرحاکمیتی و ...

همه‌جانبه که کاملاً مطابق با منافع ملی ایران باشد کاری بس دشوار و پیچیده است. این مهم از دو بعد قابل‌بررسی است اول جوهره غیرثابت و در حال تغییر سیاست است و دوم از تجارب تلخ گذشته نشئت می‌گیرد.

جوهره در حال تغییر مدام سیاست را درمانی نیست اما تجارب دیگر موافقت‌نامه‌های کنترل تسلیحاتی و خلع سلاح (به‌خصوص درزمینهٔ عدم اشاعه تسلیحات هسته‌ای) که کشورمان را وارد جرگه‌ای از تعهدهای سنگین و منافی منافع ملی نموده است، بسیاری از اندیشمندان، دولت‌مردان و سیاست‌گذاران ایرانی را بر آن داشته که بیش‌ازپیش در باب مسئله موافقت‌نامه امنیت سایبری غور نمایند. این مهم ازآن‌رو شکل می‌گیرد که در حقیقت هر موافقت‌نامه بین‌المللی به رفتار دولت‌ها چه در سطح بین‌المللی و چه در سطح ملی شکل داده و از آن‌ها کرداری متعارف و «مسئولیت‌مدار[1]» را انتظار دارد. در حقوق معاهدات بین‌المللی و ادبیات حاکم بر موافقت‌نامه‌های بین‌المللی عبارت «مسئولیت[2]» و مشتقات آن به طرفی از معاهده گفته می‌شود که نخست اینکه مراحل پذیرش و الحاق را به صورت کامل طی کرده باشد و دوم اینکه نسبت به اقدام و به اجرا درآوردن معاهده مذکور توانمند باشد (میرزایی سید احمد، ۱۳۸۳:۶). ازاین‌رو انتظار می‌رود که در تمامی سطوح و زمینه‌هایی که آن معاهده جاری است، تعهد دهندگان و دولت‌های مسئول طبق ضوابط آن توافق عمل نمایند؛ و عملی غیرمسئولانه از خود نشان ندهند چراکه در غیر این صورت نسبت به جامعه بین‌المللی و متضررین باید جوابگو باشند (ضیائی بیگدلی،۱۳۹۱:۲۳۸). پس می‌توان اهمیت این موضوع را درک نمود که اگر به موافقت‌نامه امنیت سایبری و فرایند تشکیل آن بی‌تفاوت باشیم و سعی نکنیم که منافع ملی خود را در آن بیابیم و برای جلوگیری از تصویب موارد تهدیدزا در آن معاهده تلاش ننماییم؛ دیری نخواهد پایید که در عملی انجام‌شده قرار می‌گیریم که مجبور به پذیرش آن خواهیم بود.

1. Responsibility
2. Response

ازاین‌رو معقول است که ما در این پژوهش تهدیدها پیش‌نویس موافقت‌نامه امنیت سایبری که توسط دولت روسیه تدوین‌شده است را یافته و در پی راه‌حلی برای آن بگردیم.

لازم به ذکر است که پیش‌نویس‌های دیگری نیز از سوی اتحادیه اروپا، کانادا، امریکا و ... برای موافقت‌نامه امنیت سایبری به جامعه جهانی ارائه‌شده‌اند که بنا به تأخر زمانی و کامل بودن مباحثی که وزارت امور خارجه روسیه حتی در موارد بسیار جزئی لحاظ کرده است، محققان بنا به نظر کارشناسان حوزه سایبر لازم دانستند که فقط به نقد و تجزیه و تحلیل پیش‌نویس روسی موافقت‌نامه امنیت سایبری بپردازند.

اهداف، سؤال‌ها و فرضیه تحقیق

هدف این مقاله، پی بردن به تهدیدهای پیش‌نویس موافقت‌نامه امنیت سایبری بر منافع ملی ایران و راه‌های مقابله با آن‌ها است؛ بنابراین نیاز است که پیش‌نویس مذکور را تهدیدمحور، فرض کنیم و از این فرض که حاکمیت ملی جمهوری اسلامی ایران تحت تأثیر آن قرار می‌گیرد، به تشریح مسائل بپردازیم.

سؤال اصلی: پیش‌نویس موافقت‌نامه امنیت سایبری که توسط دولت روسیه تهیه‌شده است، چه تهدیدهایی برای امنیت، منافع و حاکمیت ملی جمهوری اسلامی ایران دارد؟

فرضیه:

پیش‌نویس موافقت‌نامه امنیت سایبری روسیه، درزمینهٔ «جاسوسی اینترنتی»، «تروریسم»، «حقوق بشر»، «امنیت ملی»، «حاکمیت ملی»، «دفاع از خود» و «سوء استفاده از فضای مجازی» تهدیدهایی علیه جمهوری اسلامی ایران به همراه خواهد آورد.

پیشینه تحقیق

محققان بسیاری در باب امنیت فضای سایبر قلم زده‌اند که می‌توان به کتب «امنیت سایبری بدون جنگ سایبری[1]» و «سایبر امن و امنیت سایبری: چیزی که شما نیازدارید بدانید[1]» اشاره

1. Security Cyber without Cyber war

نمود. از طرف دیگر باید به این نکته نیز توجه داشت که محققان متعددی درزمینهٔ تهدیدهای موافقت‌نامه‌های بین‌المللی نسبت به منافع ملی ایران دست به پژوهش زده‌اند که می‌توان از کتاب‌هایی همچون «حقوق خلع سلاح و حاکمیت دولت‌ها» و «موافقت‌نامه تسلیحات زیستی» یاد کنیم. این پژوهش نتیجه تحقیقی است که به‌صورت غیرمستقیم از مجموعه کتاب‌های بالا استدلال نموده و به‌صورت مستقیم از دو ایستگاه اینترنتی کنترل تسلیحاتی و خلع سلاح «سی اس آر سی[۲]» و «آی‌ای اس آی[۳]» نتیجه گرفته است. ایستگاه‌های مذکور اهتمام فراوانی نسبت به امر تهدیدها و نقاط ضعف موافقت‌نامه امنیت سایبری که توسط دولت روسیه به جامعه جهانی ارائه گشته، از خود نشان داده‌اند.

البته پیش‌نویس‌های دیگری از سوی اتحادیه اروپا، کانادا، امریکا و... ارائه گشته که بنا به تأخر زمانی و کامل بودن مباحثی که وزارت امور خارجه روسیه حتی در موارد بسیار جزئی لحاظ کرده است[۴]؛ محققان لازم دانستند که فقط به‌نقد و تجزیه و تحلیل این پیش‌نویس همت بگمارند.

مفاهیم و مبانی نظری

همان‌گونه که گفته شد سؤال اصلی این مقاله نحوه تأثیر پیش‌نویس موافقت‌نامه امنیت سایبری ارائه‌شده از سوی روسیه، بر منافع و امنیت ملی جمهوری اسلامی ایران است و یا به عبارت بهتر بررسی تهدیدها آن موافقت‌نامه بر امنیت ایران است. محققان بر این باورند که این پژوهش، دارای بار ارزشی است، درنتیجه رویکرد روش‌شناختی اثبات‌گرایانه که روش تولید علم، در عصر مدرن است، دارای شرایط لازمه برای حل مسئله موردبحث نبوده و باید از الگوی دیگری برای این منظور استفاده کنیم. دلیل این امر آن است که به نظر اندیشمندان رویکرد

1. Cyber Security And Security Cyber: That You Need Know
2. CSRC
3. IISI

۴. منتقدان غربی پیش‌نویس مذکور مکرراً در مورد روگرفت برداری و جرح و ترمیم بسیاری از مباحثی که در دیگر پیش‌نویس‌ها آورده شده است و عدم نوآوری در آن، توسط روس‌ها تذکر داده‌اند.

روش‌شناختی انتقادی، آن‌گونه که پوزیتیویسم‌ها معتقد بودند، علم خالی از ارزش و جهت‌گیری هنجاری نیست (سید امامی،۱۳۹۰:۶۰) و این دقیقاً نکته‌ای است که ما در این پژوهش از آن پیروی می‌کنیم، زیرا ما نیز می‌خواهیم بر مبنای منافع و امنیت ملی جمهوری اسلامی ایران (هنجارها و ارزش‌های ملی) به تحلیل پیش‌نویس موافقت‌نامه مذکور بپردازیم؛ بنابراین حتماً رویکرد اثبات‌گرایی نخواهد توانست، فضا و بستر مناسبی را برای تحلیل ما فراهم آورد.

از طرف دیگر پژوهشگران بر این باورند که مقاله پیش رو پژوهشی است کاربردی که فقط رویکرد روش‌شناختی هرمنوتیک[1] (سید امامی، ۱۳۹۰:۵۷)، می‌تواند شرایط و امکانات لازم را برای تجزیه و تحلیل آن فراهم آورد. بنابراین باید مطالعه‌ای بین پیش‌نویس موافقت‌نامه امنیت سایبری، دیگر موافقت‌نامه‌های کنترل تسلیحاتی و خلع سلاحی و همچنین امنیت و منافع ملی ایران، با استفاده از روش حل مسئله هرمنوتیک و تفسیرگرایی صورت گیرد. در حقیقت تلاش این پژوهش بر آن است که با ارائه تفسیری جامع از منافع و امنیت ملی ایران و پیش‌نویس موافقت‌نامه مذکور، فضای مناسبی برای مقایسه این دو پارامتر مهیا سازیم. مطمئناً این بستر نمی‌تواند بدون توجه به تجارب موافقت‌نامه‌های کنترل تسلیحاتی و خلع سلاحی گذشته امکان‌پذیر شود. ازاین‌رو محققان بعد از غور و جست‌وجو در رفتارشناسی دولت جمهوری اسلامی ایران در عرصه بین‌المللی و همچنین کنکاش درزمینهٔ منافع ملی ایران، بر اساس روش استقرایی[2]، به این برداشت دست‌یافته‌اند که مواردی همچون تروریسم، حقوق بشر و ... (که در ضمن این مقاله به تحلیل آن‌ها خواهیم پرداخت) مواردی هستند که در موافقت‌نامه‌های متفاوت به‌عنوان اهرم فشاری علیه ملت ایران استفاده‌شده‌اند. به‌طور مثال می‌توان به تحریم‌های یک‌جانبه اتحادیه اروپا و امریکا بعد از حوادث سال ۱۳۸۸ و به بهانه حمایت از

1. Hermeneutic

۲. چرا که همان گونه که دکتر رمضانی (۱۳۸۳) ابراز می دارند سیاست خارجی ایران الگوی رفتاری منسجم و مشخصی ندارد.

حقوق بشر در ایران اشاره کرد. ازاین‌رو می‌توان آن‌ها را خط قرمز و جزو موارد تهدیدزا برای امنیت ملی ایران، قلمداد کرد.

از طرف دیگر باید به یاد داشت که وقتی بحث از استقراگرایی و تفسیرگرایی به میان می‌آید، بی‌تردید نقش برداشت‌ها، درک و تفسیر انسانی (طبق رویکرد هرمنوتیک) پررنگ می‌شود. ازاین‌رو سعی محققان این پژوهش بر آن است که در قالب نظریه گفتمانی[1]، مفاهیم بین ذهن‌های ناشی از استقرا و تأویل را شفاف‌سازی کنند (نش،۱۳۹۳:۵۵) و تا جای ممکن از خلط مبحث جلوگیری نمایند. در این راستا تلاش کردیم که قالب فکری قدرت محور روسیه و غرب را در قالب نظریه گفتمانی به نظم درآوریم. این مهم بدان دلیل است که آقای پاپر ابراز می‌دارند: «تفسیرگرایان هیچ ملاک عامی برای قیاس ندارند و طبق این رویکرد هرکس می‌تواند تفسیر نوینی از یک متن ارائه دهد» (سید امامی،۱۳۹۰:۷۷). مطمئناً اگر قرار باشد همان‌گونه که پاپر می‌گوید دور باطل تفسیرگرایی ادامه یابد تا بی‌نهایت نمی‌توان به یک نتیجه عام در مورد یک پدیده مشخص، دست یافت. به همین دلیل لازم دانستیم که برای دوری گزیدن از تفسیرگرایی لجام‌گسیخته‌ای که پاپر مدنظر داشت، مبنا و میزانی قرار دهیم تا با قیاس قرار دادن آن سنگ بنا[2] از هجو دوری گزینیم. ما نیز چاره را در آن یافتیم که تفسیر پیش‌نویس موافقت‌نامه امنیت سایبری را در چارچوب حاصله از گفتمان قدرت محور روسیه و غرب و نیز منافع و امنیت ملی ایران قرار دهیم. تا در این چارچوب بتوانیم به علم و دانشی قابل استناد و روشمند دست یابیم.

درمجموع هدف ما بر آن است که از منطق نظریه گفتاری و روش حل مسئله رویکرد هرمنوتیک که نمونه بارز آن دو را دکتر میرزایی در کتاب «دیپلماسی جنگ‌افزارهای زیستی» (۱۳۹۱) استفاده نموده‌اند، به‌عنوان روش حل مسئله بهره بجوییم. در این راستا بر اساس منطق بین ذهن‌های کتاب مذکور و چارچوب حل مسئله تفسیرگرایی که اصل و اساس یک گزاره را

1. Reading
2. Millstone

در موارد متشابه و یا قصد و نیت نویسندگان، جست‌وجو می‌کنند. ما نیز در مطالعه‌ای توصیفی-تحلیلی به بررسی تهدیدها ناشی از موافقت‌نامه امنیت سایبری خواهیم پرداخت.

در پایان این چارچوب نظری، برای درک هر چه بهتر از مقوله امنیت در پژوهش به‌عمل‌آمده، باید خاطرنشان کنیم که اعتقاد محققان این پژوهش به دکترین امنیت‌محور «دفاع فعال» است. این دکترین ازآن‌رو اتخاذشده است که طبق رویکرد نظام بین‌المللی و رویه حاکم بر روند کنترل تسلیحات و خلع سلاح، معاهدات و توافق‌نامه‌های امنیتی، حوزه حاکمیتی دولت‌ها را تهدید و محدود می‌نماید (ساعد، ۹۳:۱۳۸۸). ازاین‌رو باید در تحلیل معاهدات امنیت بین‌المللی به‌گونه‌ای رفتار نمود که تمهیدات لازم را برای دفاع از منافع و امنیت ملی بیش‌ازپیش اندیشید. البته همان‌گونه که متخصصان حوزه دفاع سایبری به‌خوبی از این امر مطلع هستند، در دنیای مجازی، نزاع و درگیری به‌صورت مستمر با صلح و ثبات آمیخته است و نمی‌توان به‌صورت شفاف و دقیق بین اقدامات خصمانه و غیرخصمانه تفکیکی روشن ایجاد نمود (ابراهیم نژاد و اسکندری، ۲۵:۱۳۹۲). نظر به این خصوصیت فضای سایبر، فعالین حوزه امنیت که در جست‌وجوی بیشترین امنیت برای دولت خویش‌اند راهکاری به‌جز راهکار جنگ‌محور که تمامی اقدامات بازیگران بین‌المللی را خصمانه انگاشته و در پی چاره‌جویی در برابر خصومت‌ورزی‌های دشمنان است انتخاب می‌شود؛ اما باید توجه داشت که درواقع حتی در بدترین حالت و وضعیت نیز نمی‌توان فضای سایبر را به‌کل سیاه فرض کرد و خود را از مزایای آن بی‌بهره نمود (حسن بیگی، ۱۰:۱۳۸۸). چراکه به‌طور مثال دولت هند توانسته است، در کنار تمامی مخاطرات فضای سایبر، با محور توسعه قرار دادن دنیای مجازی، در سال ۲۰۱۴، به سومین اقتصاد بزرگ جهان تبدیل شود (پیش‌بینی می‌شود که در سال ۲۰۱۵ هند، با کنار زدن چین، به دومین اقتصاد بزرگ جهان ارتقا درجه یابد) (WTO, 2013). با توجه به نکات فوق به نظر می‌رسد، بهترین الگوی حل مسئله ما دکترین «دفاع فعال» باشد، زیرا دکترین دفاع فعال، شدیدترین حالت راهکار امنیت‌محور است که هم خصوصیت مقابله با تهدید دکترین جنگ‌محور را دارد و هم به ما

اجازه می‌دهد دنیا را خاکستری بنگریم و از جوانب مثبت فضای سایبر بهره‌مند شویم؛ یعنی در عمل با آن‌که مقصود دولت دفاعی است، اما برخی اهداف، سیاست‌ها و استراتژی‌های امنیتی تهاجمی را نیز دنبال می‌کند. ازاین‌رو تفکیک مرزهای دفاع فعال از راهکار جنگ‌محور کاری بس دشوار است. در دکترین دفاع فعال، ساختارها، نیروها و توانمندی‌های دولت در ترکیبی پیچیده، برای ایجاد امنیت بکار گرفته می‌شوند (عبدالله‌خانی،۱۳۸۹:۶۵). باید به یاد داشت که در طی این مقاله مضمون‌هایی همچون شفاف‌سازی، اعتمادسازی و ارائه اطلاعات و سوابق تاریخی که از اصول دکترین امنیت‌محور «دفاع فعال» می‌باشند، به‌صورت صریح یا ضمنی استفاده خواهد شد.

بررسی پیش‌نویس موافقت‌نامه امنیت سایبری

باید در باب کلیت این کنوانسیون ابراز داشت که وزارت امور خارجه روسیه سعی نموده است تمامی زوایه‌ها و نهفته‌های فضای سایبر را از منظر امنیت بین‌الملل و حقوق بین‌الملل پوشش دهد. ازاین‌رو پیش‌نویس مذکور که در سال ۲۰۱۱ به جامعه جهانی ارائه شد، دارای ۲۳ ماده است، که در نوع خود بسیار جامع می‌نماید. چون در مورد مبحث بسیار غیرثابت سایبر سخن می‌گوید، سعی شده است ادبیات جدیدی را به حوزه معاهدات کنترل تسلیحاتی و خلع سلاحی وارد سازد که بسیاری از منتقدین آن بر این نکته تأکید می‌کنند. در این راستا در بعضی موارد از تعاریف بسیار کلی و در بعضی موارد از تعاریف بسیار دشوار استفاده‌شده است.

دربندهای مقدماتی[1] این کنوانسیون همان‌طور که پیش‌بینی می‌شود و طبیعی نیز است مواردی چون حقوق بشر و آزادی‌های اساسی همچون آزادی بیان، جریان آزاد اطلاعات و ... وجود دارد. روس‌ها باآنکه خود از دولت‌هایی هستند که مدام از سمت غرب به نقض آزادی بیان و اختناق متهم می‌شوند اما به‌وفور در این کنوانسیون از عبارات حقوق بشری استفاده کرده‌اند. محققان بعد از بررسی‌های جامع، با دیگر منتقدین این کنوانسیون هم‌عقیده شدند که ریشه

1. Preparative paragraphs (p.p.)

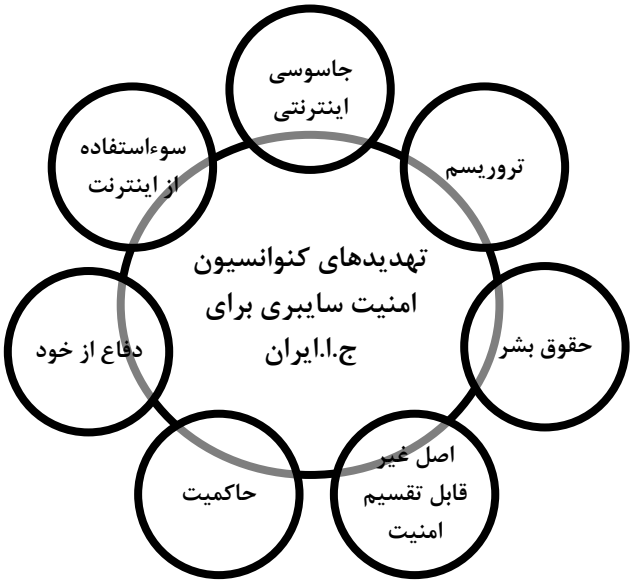
این حقوق بشر در رفتارها و بینش غربی به موضوع آزادی‌های بشری است و درنتیجه به آن معاهده رنگ و بوی غربی داده است (Cybersecurity Act of 2012)؛ اما همان‌طور که خواهیم دید، روس‌ها در این موافقت‌نامه سعی داشته‌اند که این مفاهیم حقوق بشری را با بینش غیر غربی تعدیل کنند. ازاین‌رو به‌شدت مورد نقد منتقدین غربی خود قرارگرفته است.

البته باید یادآور شد که غرب در چندساله اخیر از حقوق بشر و مفاهیم وابسته به آن برای مقابله، تهدید و تحریم کشورمان استفاده کرده و در حقیقت از هر متن بین‌المللی که در آن ذکری از حقوق بشر شده است استفاده می‌کند تا ایران را محکوم نماید. بنابراین ممکن است که غرب از موافقت‌نامه سایبری نیز به بهانه‌ی آزادی بیان، تفسیر وسیع به نفع خود نماید؛ اما همان‌گونه که مایکل مکروف می‌گوید: «همه حکومت‌ها به آزادی بیان و تبادل‌نظر اعتقاددارند اما تفاوت حکومت ها در درک این نکته است که ازنقطه نظر سیاسی و فرهنگی انتشار کدام نظرات ممکن است موجبات تهدید ملی را فراهم آورد»(Kuehl, 2010:59). ازاین‌رو پیشنهاد محققان آن است که در بررسی چنین متن‌هایی، در مراحل تدوین، مفاهیمی که ممکن است مورد سوء استفاده‌های احتمالی غرب قرار گیرند را شفاف‌سازی نمایند به‌گونه‌ای که به اصول اعتقادی یا سیاسی جمهوری اسلامی ایران لطمه وارد نسازد.

ازنظر تحلیلگران اروپایی در حقیقت انگیزه اصلی روس ها برای نگاشتن این پیش‌نویس در آن است که روس‌ها می‌خواهند، از این طریق، وزنه تعادلی با موافقت‌نامه امنیت سایبری اتحادیه اروپا معروف به موافقت نامه بوداپست (۱۹۹۴) ایجاد نمایند. از طرف دیگر در کنکاش برای انگیزه روس‌ها از تهیه این پیش‌نویس، پژوهشگر در آمار ارائه‌شده توسط سازمان‌های خصوصی امنیت شبکه به نکته جالبی برخورد کرده است که آن را به‌صورت خلاصه می‌توان در قالب این جمله ابراز نمود که در یک دهه اخیر روسیه اصلی‌ترین قربانی تمامی انواع عملیات سایبری می‌باشد (Athena, 2014).

حال به بررسی بندهای اصلی[1] پیش‌نویس مذکور و تهدیدات ناشی از آن می‌پردازیم.

تهدیدهای موافقت‌نامه امنیت سایبری برای امنیت و منافع ملی جمهوری اسلامی ایران



منبع (یافته‌های تحقیق)

جاسوسی اینترنتی

در تفسیر ماده ۴ موافقت نامه تحت عنوان «تهدیدات اساسی علیه صلح و امنیت بین‌المللی در فضای تبادل اطلاعات» می‌توان گفت:

بسیاری از دولت‌ها برای جاسوسی اینترنتی، دزدی اینترنتی و دزدی فنی- مهندسی و ... به‌صورت مشخص سرمایه‌گذاری‌های کلانی انجام می‌دهند و بخش ویژه‌ای از فعالیت‌های خود در فضای سایبر را به این حوزه اختصاص می‌دهند و این اقدامات را جزء جرائم سایبری نمی‌دانند و در قوانین داخلی آن دولت‌ها نیز اقدامات مذکور جرم محسوب نمی‌شوند.[2] اما این مفاهیم و مفاهیمی ازاین‌دست در این ماده ذکر نشده‌اند (theatlantic,2013- mashable,2014- wikipedia,2013).

1. Operative paragraphs (o.p.)

۲.همانند آنچه که در افشاگری‌های آقای اسنودن شاهد بودیم دولت امریکا از تمامی جهان، به‌صورت گسترده و همه جانبه جاسوسی می نماید.

از طرف دیگر به‌طور اساسی این معاهده نیز همانند همه توافق‌نامه‌ها و قراردادهای بین‌المللی که مرجع رسیدگی‌کننده به آن‌ها، دولت‌ها هستند، دولت‌ها را مسئول اجرای این توافق دانسته است؛ به‌عبارت‌دیگر این معاهده با سکوت خود در باب دزدی و جاسوسی سایبری دولتی، دست دولت‌ها را برای ادامه کارهای تخلف آمیزشان باز گذاشته است. امروزه وقتی سخن از جاسوسی به میان می‌آید اولین چیزی که به ذهن خطور می‌کند جاسوسی اینترنتی است؛ اما در تمامی متن این موافقت‌نامه حتی یک مورد هم از کلمات مترادف با جاسوسی در زبان انگلیسی[1] استفاده‌نشده است. به نظر پژوهشگران ازآن‌رو که ما از قربانیان حملات سایبری هستیم، اگر دولت جمهوری اسلامی بخواهد معاهده‌ای جامع را تهیه کند، باید تعریف انواع و اقسام مختلف عملیات سایبری را به‌صورت مشخص در طی ماده‌ای مستقل و تعهدات مربوط به آن را ضمن ماده جداگانه دیگری بگنجاند.

تروریسم

خطر دیگری که دولت‌ها در قرن ۲۱ با آن همواره دست به گریبان‌اند و امروزه تقریباً در تمامی موافقت‌نامه‌ها رد پایی از آن به چشم می‌خورد، مسئله تروریسم و افراط‌گرایی است. امروزه فضای سایبر به تروریسم اجازه می‌دهد اقداماتی چون ارتباطات، جمع‌آوری اطلاعات، عضوگیری، تبلیغات، جنگ روانی، سازمان‌دهی، جمع‌آوری پول و کمک‌های مالی و ... را به‌سرعت انجام دهند.[2]

ازیک‌طرف باید به یاد داشت که در الگوی رفتاری جمهوری اسلامی ایران در باب مواجهه با موضوع تروریسم همواره به همراه بیم از سوءاستفاده غربی‌ها از این واژگان علیه گروه‌های مقاومت اسلامی، امیدی نیز در بهره‌برداری علیه تروریست‌های واقعی وجود دارد. از طرف دیگر ریشه این ترس و امید در اقدامات و تفاسیری است که غربیان بر اساس منطق فایده‌گرایی‌شان

1. Spy ،Espionage،Intelligence

۲. به وضوح می‌توان نمونه این اقدامات را در مورد «داعش» دید. این گروه که اکثریت اعضای آن افرادی تحصیل کرده، متخصص و آشنا با فضای سایبر هستند، نشان داده اند از فضای سایبر به نحو احسن برای اقدامات مذکور استفاده می‌کنند.

نسبت به مقوله تروریسم، از رویدادها دارند. در منطق غربی و به‌خصوص آمریکایی، تروریست‌ها، برحسب موقعیت‌های زمانی و مکانی مختلف، به دودسته خوب و بد تقسیم می‌شوند. ازاین‌رو در موارد مشابه نمایندگان جمهوری اسلامی با نگاهی بدبینانه به لفظ تروریست در متن یک موافقت‌نامه، در مورد آن متن با مقایسه بین دیگر مزایا و معایب تصمیم‌گیری می‌کنند و به‌صرف وجود یک عبارت تروریست اکتفا نمی‌کنند[1] (میرزایی، ۱۶۳:۱۳۹۱).

در متن کنوانسیون امنیت سایبری برای اقدامات تروریستی از ادبیاتی چون حمله سایبری، تخریب ساختارهای اجتماعی و اخلال در فضای مجازی استفاده شده. که این موارد قسمت بسیار اندکی از فعالیت‌های گروه‌های تروریستی در فضای مجازی را شامل می‌شود (IISI,2014). با هدف تکمیل موافقت‌نامه مذکور باید علاوه بر اضافه نمودن و توسعه دادن به مفهوم اقدامات تروریستی در کلیت متن، دربندهای مقدماتی نیز به موافقت‌نامه‌های دوازده‌گانه مبارزه با تروریسم ویژه کنوانسیون «جلوگیری از منابع مالی تروریسم (۲۰۰۱)» اشاره کرد. تا از این طریق در نحوه جمع‌آوری کمک‌های مالی به تروریست‌ها (به‌خصوص گروهک‌هایی همچون منافقین، داعش و ...) اخلال ایجاد شود.

البته همان‌گونه که گفته شد در منطق آمریکایی همواره تروریست‌های خوب و تروریست‌های بد وجود دارد که از نظر آن‌ها همواره گروه‌های مقاومتی همچون حزب‌الله لبنان و گروه حماس از تروریست‌های بد محسوب می‌شوند (Conway,2003:24). در همین چارچوب و در جریان جنگ ۵۰ روزه اسرائیل و غزه، گروهی از صهیونیست‌ها که خود را از سازمان‌های مردم‌نهاد می‌خواندند، با ارائه دادخواستی به یکی از دادگاه‌های ایالت کالیفرنیا خواستار مسدودسازی

۱. ازجمله موارد مشابه، مبحث بیوتروریسم در کنوانسیون تسلیحات زیستی بود که جمهوری اسلامی ایران تلاش داشت در مذاکرات پروتکل الحاقی کنوانسیون تسلیحات زیستی، این مفهوم روشن شود و نیز با اصرار بر گنجانیدن «Covert Operative» به نوعی اقدامات مخفی دولت‌ها را نیز در برگیرد.

تمامی دامنه‌های[1] ثبت‌شده ایرانی (با پسوندIR.) شدند. استدلال آن‌ها در آن دادخواست، کمک دولت ایران به تروریست‌ها (مردم غزه و حماس) بود.

به نظر محققان پژوهش پیش‌رو، بر اساس منافع جمهوری اسلامی و با توجه به تجارب موافقت‌نامه‌های گذشته یا باید مفهوم «اقدامات تروریستی در فضای مجازی» در متن موافقت‌نامه امنیت سایبری و در پروتکل‌های الحاقی‌اش (مثلاً تبلیغات و جنگ روانی، جلوگیری از ارسال پیام و اطلاع‌رسانی تروریستی و ...) به شدت محدود شود و یا به‌طورکلی عبارت «تروریسم» از آن متن حذف گردد. تا از این طریق جلوی سوء استفاده‌های احتمالی غرب، گرفته شود.

حقوق بشر

مفاهیم و جزئیات حقوق بشری ارائه‌شده دربندهای ۷،۴ و ۸ ماده ۴ معاهده مذکور، عیناً در میثاق بین‌المللی حقوق سیاسی- مدنی[2]، کنوانسیون اروپایی حقوق بشر[3] و همچنین کنوانسیون جرائم سایبری اتحادیه اروپا موسوم به کنوانسیون بوداپست نیز تکرار شده است. با این تفاوت که در آنجا این مبحث با کلیت کنوانسیون هم‌خوانی و ارتباط معنایی بیشتری دارد. در آن متون به‌صورت تخصصی در مورد حقوق بشر صحبت می‌شود و دولت‌ها خود را به رعایت آن اصول، در تمامی زمینه‌ها ملزم می‌دارند. کارشناسان عقیده دارند که از مقایسه دقیق‌تر موافقت‌نامه‌های مذکور می‌توان به این نتیجه رسید که گویا رونوشت‌برداری صورت پذیرفته است (CSRC,2010). ازاین‌رو گنجاندن این مفاهیم در این معاهده امکان به وجود آمدن این شائبه را دارد که دیگر دولت‌هایی که عضو کنوانسیون اروپایی حقوق بشر و کنوانسیون بوداپست نیستند، از این طریق خود را به آن‌ها متعهد می‌کنند. چرا که در روند رسیدگی قضایی در دیوان یکی از روش‌های بررسی پرونده‌ها، رجوع به سوابق مورد مناقشه است (ضیائی

1. Domain
2. International Covenant on Civil & Political Rights
3. European Convention on Human Rights

بیگدلی محمدرضا، ۵۰۲:۱۳۸۸). ازاین‌رو این نکته برای منافع جمهوری اسلامی ایران ممکن است تهدیدزا باشد. چراکه رویکرد قانون‌گذاران آن موافقت‌نامه‌ها غربی و غیراسلامی بوده است[1] که با فرهنگ و دیدگاه ملت ایران نسبت به مقوله آزادی متفاوت است.

در همین راستا در بند ۹ ماده ۴ موافقت‌نامه، دولت‌ها را وادار به رعایت حقوق و آزادی‌های بشری در فضای تبادل اطلاعات و ارتباطات نموده است؛ اما این عملکرد با رویکرد غربی به حقوق بشر متفاوت است. چراکه آنان معتقدند «هیچ کس، در هیچ جایی و در هیچ زمانی حق اخلال در حقوق دیگران را ندارد و تنها محدودیت آن، تحقیقات قوای انتظامی است» برای نمونه می‌توان به ماده ۱۹ میثاق بین‌المللی حقوق سیاسی- مدنی اشاره داشت. طبق آن معاهده فقط حقوق بشر می‌تواند به دلایل زیر نقض شود: الف) محترم شماردن حقوق و آبروی انسآن‌ها ب) برای محافظت از امنیت ملی یا نظم عمومی یا مسائل اخلاقی (جلالی فراهانی، ۱۳۳:۱۳۸۴).

به نظر پژوهشگران، این نوع حقوق بشر بر طبق استانداردهای لیبرال- پروتستانیسم اروپایی بنا نهاده شده است، به‌طور مثال این الگوی فکری هیچ سنت، بنیان و اصل غیر قابل تغییری را نمی‌پذیرد. ریشه این طرز فکر در این جمله هیراکلیت است که می‌گوید: «هیچ‌چیزی به‌جز اصل تغییر، ثابت نیست.» این در حالی است که در قانون اساسی ایران از وظایف رئیس‌جمهوری حفظ سنت‌ها، ارزش‌ها و ... برشمرده شده است. در ورای این بحث، هم‌چنان‌که کیت نش در کتاب «جامعه‌شناسی سیاسی معاصر» به تحقیق اثبات نموده است آزادی سایبری که مدنظر نویسندگان غربی موافقت‌نامه‌های حقوق بشری است، قابل گسترش به دیگر نقاط جهان نیست. این بحث جای بسیاری برای کنکاش و پژوهش دارد که خارج از بحث ما در این مقاله است. از طرف دیگر باید به یاد داشت که حتی بین خود اروپاییان نیز بر سر شکل به اجرا

۱. مثال بارز آن تبلیغات سایبری مسائل ضد اخلاقی است که مغایر قوانین، هنجارها و فرهنگ ایرانی- اسلامی ما است و در صورت فیلترینگ آن‌ها توسط جمهوری اسلامی ایران نقض این معاهده تلقی خواهد شد.

درآوردن آن اتفاق‌نظر وجود ندارد (مثلاً بین روس‌ها و انگلیسی‌ها). به نظر پژوهشگر ریشه اصلی این تفاوت دیدگاه‌ها در پایبندی دولت‌ها و جوامع به سنت‌ها است.

اصول غیرقابل تقسیم امنیت

در تفسیر ماده ۵ تحت عنوان «مبانی و اصول تضمین امنیت بین‌المللی اطلاعات» می‌توان گفت:

در این ماده مهم‌ترین، پیچیده‌ترین و خطرناک‌ترین چیزی که ذکرشده است و می‌تواند امنیت جمهوری اسلامی ایران را به خطر بیاندازد عبارتی است که دربند ۲ تحت عنوان «اصول غیرقابل تقسیم امنیت» ذکرشده است. باید پذیرفت این کنوانسیون در تمامی جوانب رنگ و بوی اروپایی دارد. چراکه مبانی حقوق مفهوم «اصول غیرقابل تقسیم امنیت» برای اولین بار در طی نشست سران سازمان امنیت و همکاری اروپا[1] (OSCE,2014) در بوداپست (۱۹۹۴) تدوین شده است. بااین وجود هنوز در خود اروپا نیز مسائلی مانند «اصول غیرقابل تقسیم امنیت» حل‌وفصل نشده است (Bumiller and Shanker, 2012:55-79).

کاربرد مفهوم «اصول غیرقابل تقسیم امنیت» بدین شیوه چالش‌برانگیز است. تاریخچه استفاده از این عبارت را باید در بحث استقرار موشک‌های چتر دفاع ضدموشکی غرب در اروپای دوران تنش‌زدایی جنگ سرد، جستجو کرد. رهبران شوروی در آن زمان استدلال می‌کردند که مفهوم امنیت برای آن‌ها غیرقابل تجزیه و تفکیک است. استدلال غرب بر این اصل استوار بود که موشک‌های مذکور ربطی به شوروی ندارد و فقط برای ایجاد هر چه بیشتر امنیت است؛ اما روس‌ها آن را نمی‌پذیرفتند و ابراز می‌داشتند که روس‌ها انتظار ندارند، درحالی‌که امنیت آمریکایی‌ها افزایش می‌یابد، امنیت ایشان کم شود. ازاین‌رو آن‌ها امنیت را چیزی می‌انگاشتند که نمی‌تواند برای یکی از بازیگران بیشتر از دیگر بازیگران وجود داشته باشد.

۱. این سازمان (OSCE) بزرگترین سازمان بین دولتی امنیتی است که فعالیت‌هایی در زمینه کنترل تسلیحات، حقوق بشر، آزادی مطبوعات و انتخابات آزاد دارد. با آنکه این سازمان اروپایی است اما بسیاری از کشورهای غیر اروپایی نیز در آن شرکت دارند.

اگر بخواهیم اساسی و بنیادین به بررسی این قضیه بپردازیم، باید گفت که ریشه این بحث در معمای امنیت نهفته است. ازآن‌رو که بشریت هنوز نتوانسته است برای معمای امنیت راه‌حلی نهایی بیابد، نه‌تنها ما در این مقاله بلکه هیچ پژوهشگری نیز نمی‌تواند به‌یقین بگوید عبارت «اصول غیرقابل تقسیم امنیت» و یا عبارت «دولت‌های عضو امنیتشان را در قبال افزایش هزینه‌های امنیتی دیگر دولت‌ها تقویت نخواهند کرد» در یک معاهده باعث صلح‌زایی می‌شود و به نظر می‌رسد، تحلیل صحیح از این عبارت فقط و فقط در ذهن تصمیم‌سازان سیاسی و در لحظه تصمیم‌گیری رخ می‌دهد. بدین معنا که در حالی که یک‌طرف بازی، امنیت خود را افزایش می‌دهد، تصمیم‌گیران طرف مقابل فکر کنند امنیت آن‌ها روبه‌زوال است.

از جانب دیگر هدف از عبارت «اصول غیرقابل تقسیم امنیت» بدین معنا نیست که شامل همه دولت‌ها شود (کولیور و دیگران، ۶۹:۱۳۷۹). به‌عنوان مثال ممکن است که اروپا و امریکا بتوانند بر سر این مفهوم با یکدیگر توافق نمایند تا امنیت آن‌ها و بقیه گروه غرب (ژاپن، استرالیا و ...) یکپارچه باشد؛ اما حتی حاضر نیستند این مفهوم را با روس‌ها به اشتراک بگذارند، چه رسد به قدرت‌های نوظهوری مانند جمهوری اسلامی ایران، یعنی حاضر نیستند که منافع و امنیت جمهوری اسلامی ایران را با منافع و امنیت خود غیرقابل تقسیم بدانند. بنابراین ذکر این عبارت در متن، بدون شفاف‌سازی، قابل تفسیر وسیع به نفع دولت‌های مدعی «جامعه جهانی» خواهد بود. مثال واضح آن در رفتار دوگانه غرب نسبت به «معاهده عدم اشاعه تسلیحات هسته‌ای»[1] است.

اما بسیاری از متفکران بر این عقیده‌اند که فضای مجازی از اصول غیرقابل تقسیم متفاوتی پیروی می‌کند. چراکه در آن همانند دنیای مکانیکی نمی‌توان به‌صورت یک‌جانبه عمل نمود. بنابراین به رغم اینکه در مواجه با اقدامات مجرمانه فراملی نیازمند اقدامات و هماهنگی‌های

1. NPT

مشترک دولت‌ها هستیم (IISI,2011). باید از عبارات موجود در ماده ۵ و بخصوص بند ۲ حتماً تفسیر و تشریحی واضح و شفاف ارائه گردد.

حاکمیت

موضوع مورد مناقشه دیگری که دربندهای ۱،۴،۵،۸ ماده ۵ بدان پرداخته‌شده است، حاکمیت است. موضوع حاکمیت ازآن رو حائز اهمیت است که اگر وضعیت آن مشخص شود، دولت‌ها می‌توانند با استفاده از مکانیسم‌های قانونی خود و اتخاذ اقدامات لازم از بسیاری از فعالیت‌های غیرقانونی و مجرمانه در فضای سایبر جلوگیری نماین(Creemers,2012:81) . به عبارت بهتر، ازآن‌رو که در حال حاضر بر فضای سایبر به‌صورت رسمی هیچ قانونی قابل اجرا نیست؛ دولت‌ها در عمل حق هیچ‌گونه برخوردی با منابع حملات سایبری ندارند؛ هیچ نظام حاکمیتی مشخصی در فضای سایبر وجود ندارد؛ نمی‌توان انتظار ایجاد امنیت و ثبات در محیط مجازی را از سوی دولت‌ها داشت؛ یعنی فضایی که قانون آن را پاستوریزه نکرده باشد، مطمئناً میکروب جرم مجال رشد و نمو می‌یابد.

در این کنوانسیون همانند بسیاری از موافقت‌نامه‌های خلع سلاح و کنترل تسلیحاتی «نظام حاکمیت ملی»[1] پیشنهادشده است که بر طبق آن دولت‌ها می‌توانند بر اساس حاکمیت ملی و با استفاده از قوانین داخلی خود بر شرکت های فعال در فضای سایبر، فعالین فضای مجازی و بر گوشه‌ای از اینترنت که در سطح حاکمیت داخلی خود قرار می‌گیرد، نظارت کنند. روس‌ها ماهیت و هدف اصلی این اقدام را دوری گزیدن از دخالت در شبکه اینترنت دیگر دولت‌ها دانسته‌اند. به نظر می‌رسد این طرز فکر به‌کلی، غیرمفید و ناکارآمد است؛ زیرا بسیاری از تهدیدها، عملیات و حملات سایبری علیه کشورمان، خارج از حوزه حاکمیتی دولت ایران صورت می‌پذیرد (مانند استاکس نت، کرم فلون و ...) و این امر در حالی است که نه‌تنها این اقدامات از سوی دولت‌های غربی تحت پیگرد قرار نمی‌گیرد بلکه این‌گونه حملات درعمل از

1. National Sovereignty

سوی آن‌ها حمایت نیز می‌شود. این اتفاق برای بسیاری از دیگر دولت‌ها مخصوصاً در عملیاتی مانند پول‌شویی، کلاه‌برداری و دزدی اینترنتی که در دولت سوم برنامه‌ریزی‌شده است، تکرار می‌شود.

در ضمن در این طرح، هیچ اشاره‌ای به حاکمیت بر منابع و زیرساخت‌های اینترنت که در حقیقت وظیفه داده‌پردازی اینترنت بین‌المللی را بر عهده دارند، نشده است. بیشتر این مراکز در امریکا قرار دارند و دولت مذکور بر آن‌ها نفوذ دارد (Deibert,2010:66). در جریان افشاگری‌های اسنودن، این سوءاستفاده به اثبات رسید (Theguardian,2014). ازاین‌رو ما (بدون استفاده از اینترنت ملی) هر کاری در فضای مجازی انجام دهیم زیر نظر و تحت سیطره امریکا خواهد بود؛ و از اساس در چنین محیطی حفاظت اطلاعات معنا ندارد.

با توجه به گفته‌های بند بالا و نیز دقت نظر به متن پیش‌نویس و همچنین بررسی بر تاریخچه تشکیل رژیم کنترل صادرات می‌توان دست به این پیش‌بینی زد که حتی اگر پیش‌نویس فوق نیز به تصویب و تایید تمامی دولت‌ها برسد، باز هم نمی‌توان از گسترش برنامه کنترل صادرات بر زیرساخت‌های فضای سایبر جلوگیری نمود. به‌طور مثال می‌توان به تحریم‌های یک‌جانبه امریکا علیه کشورمان اشاره بنماییم که در طی آن تحریم‌ها، قطعات، تراشه‌ها و ریزپردازنده‌ها توسط امریکا به ایران فروخته نمی‌شود.[1] ازاین‌رو محققان بر این باورند که قبل از تشکیل هرگونه مجمع جهانی در مورد فضای سایبر و تهدیدها آن باید تکلیف موضوع حاکمیت بر فضای سایبر و همچنین حاکمیت بر تجهیزات و زیرساخت‌های آن مشخص شود.

دفاع از خود

بنا به آنچه روس‌ها در بند ۱۱ ماده ۵ پیش‌نویس موافقت‌نامه امنیت سایبری در باره «دفاع از خود» نگاشته‌اند، می‌توان گفت که این ماده در اصل واکنشی است به ماده چهارم سند دفاع سایبری ناتو (تالین) که ناظر بر دفاع از هم‌پیمانان است (CSRC, 2010). بی‌گمان هر دولتی در

۱. قانون داماتو

چارچوب موازین قانونی منشور، عرف و حقوق بین‌الملل از حق دفاع مشروع برخوردار است؛ اما به نظر می‌رسد روس‌ها می‌خواهند از این طریق و با موازی‌سازی تأثیر و تبعات ماده ۴ سند تالین را کمرنگ نمایند.

به‌رغم اینکه به ظاهر شاید این‌گونه تصور شود که عبارت «دفاع از خود» می‌تواند منافع و امنیت ملی جمهوری اسلامی ایران را تأمین نماید امّا ازآن‌رو که این کنوانسیون برای تمایز بین انواع عملیات سایبری شاخصی بیان نکرده است؛ مفهوم امنیت را در قالب عبارت «دفاع از خود» منوط به اقدامات خصمانه نموده است؛ اما نمی‌توان هر عملیات سایبری را در دسته اقدامات خصمانه جای داد و در این حالت این سؤال در ذهن ناظرین بی‌طرف شکل می‌گیرد که با توجه به متن پیش‌نویس و ساختار فضای سایبر، دولت‌های تعهد دهنده (جدای از مباحث فنی و در قالب الگوهای سیاسی) بنا به چه شاخصی می‌توانند مهاجم را شناسایی و او را کیفر نمایند؟ یعنی آنکه چگونه می‌توانند نیت مهاجم را تشخیص دهند (قاسمی و بارین، ۱۶:۱۳۹۲)؟

به‌عبارت‌دیگر ازآن‌رو که در سال‌های اخیر، بعد از فروپاشی اتحادیه جماهیر شوروی و به‌خصوص بعد از رویدادهای ۱۱ سپتامبر رفتارهای یک‌جانبه‌گرایانه امریکا به‌صورت افسارگسیخته‌ای به‌ویژه درزمینهٔ دشمن‌تراشی با مسلمانان و محور شرارت خواندن جمهوری اسلامی ایران افزایش یافته است. چه تضمین و ضمانتی وجود دارد که آمریکاییان با عدم سوءاستفاده از این بند و در قالب دفاع از خود کوچک‌ترین عملیات سایبری را حمله و جنگ سایبری نخواند و تحت عنوان «دفاع از خود» دست به اقدام متقابل نزند. خلأ مفهومی و حقوقی مرتبط با فضای سایبر و جزئیات فنی، سیاسی و حقوقی نیز به آن‌ها در این زمینه کمک می‌نماید. ازاین‌رو با توجه به ماده ۲ و بند ۹ مقدمه این کنوانسیون، باید دربند ۱۱ ماده ۵ بین جنگ اطلاعات[1] و رفتارهای تهاجمی[2] و عملیات[3] تفکیک قائل شد؛ یعنی این موافقت‌نامه باید

1. Information warfare
2. Aggressive
3. Operation

به‌طور شفاف در بخش تعاریف، این مفاهیم را روشن سازد. به‌خصوص اینکه در کشورهای مختلف تعاریف مختلفی از این مفاهیم و اقدامات ارائه‌شده است. مثلاً کانادا در قوانین فضای سایبر خود این مفاهیم و اقدامات را به گونه متفاوتی از دیگر دولت‌ها (مانند استرالیا، امریکا و ...) تعریف نموده است(Asis, 2013) .

سوءاستفاده از اینترنت

در ماده ۶، بند ۲، موافقت‌نامه از دولت‌ها خواسته است که با توجه به حقوق دیگر دولت‌ها، اجازه هیچ‌گونه سوءاستفاده از فضای سایبر، زیرساخت‌های دنیای مجازی و حوزه صلاحیت قضایی‌شان برای به‌کارگیری علیه دیگر دولت‌ها را ندهند؛ اما این ماده و مفاد آن چقدر می‌تواند با واقعیت هم‌خوانی و همراهی داشته باشد. اوباما در تاریخ ۲۲ ژوئن ۲۰۱۱ به پنتاگون دستور می‌دهد که از انجام حمله سایبری در قلمرو سرزمینی دیگر دولت‌ها بدون اطلاع اولیه آن‌ها خودداری نماید. از طرف دیگر و به‌صورت هم‌زمان، حکم مشابه ای به نیروهای آمریکایی اجازه می‌دهد که حمله سایبری و جاسوسی علیه دیگر کشورها انجام دهند (streltsov,2013:56). یعنی بر اساس این ماده امریکا نمی‌تواند در فضای سایبر دست به اقدامات نظامی بزند ولی می‌تواند با استفاده از یک سری کدهای برنامه‌نویسی رایانه‌ای و شناسایی حفره‌های امنیتی سامانه دفاع سایبری کشور هدف، خود را برای درگیری‌های احتمالی در هنگام جنگ سایبری آماده سازد. پژوهش‌ها نشان داده است که این امکان ازلحاظ فنی وجود دارد که در مورد استاکس‌نت نیز چنین اتفاقی افتاده است. طبق اسناد منتشره آمریکایی‌ها اطلاعاتی در مورد حفره‌های امنیتی رایانه‌های ایرانی را در اختیار اسرائیل قرار داده اند(New York Times, 2010).

اما این‌همه‌ی بحث نیست، بلکه آمریکایی‌ها با سرمایه‌گذاری‌های کلانی که درزمینهٔ جاسوسی و جمع‌آوری اطلاعات نموده‌اند، به‌هیچ‌وجه نمی‌توانند این ماده را عملیاتی نمایند. هم‌اکنون چندصد شبکه، سایت، سازمان و ... علیه ایران مشغول فعالیت‌اند که همگی از طرف دولت امریکا حمایت مالی و اطلاعاتی می‌شوند؛ که هرگز آن‌ها را تعطیل نخواهند کرد. همانند این

وضعیت را در مورد موافقت‌نامه تسلیحات شیمیایی و موافقت‌نامه تسلیحات بیولوژیک و نیز در مورداجرای مفاد «معاهده عدم اشاعه تسلیحات هسته‌ای[1]» شاهد هستیم. با آن‌که دولت امریکا خود را متعهد به از بین بردن تسلیحات مذکور نموده است اما کوچک‌ترین تلاشی برای از بین بردن تمامی ذخائر تسلیحاتی خود نمی‌کند و به کاهش کمی آن‌ها و گاهی افزایش کیفی آن‌ها همت می‌گمارد.

در اینجا لازم است یادآور شویم که بنا به این ماده، اگر دولت ایران اجازه استفاده از زیرساخت‌ها و فضای سایبر خود را به افرادی بدهد که از منظر دیگر دولت‌ها افراد سرکشی هستند، اولاً ایران متهم به نقض این موافقت‌نامه می‌شود؛ ثانیاً آن دولت‌ها می‌توانند بر اساس این ماده زیرساخت‌های خاصی مانند ماهواره‌های بین‌المللی را از دسترسی ایران خارج سازند. نمونه بارز این قضیه درباره قطع پخش برنامه‌های شبکه ایرانی «پرس تی وی[2]» است. ازاین‌رو نیاز است که به پروژه ساخت ماهواره ملی و همچنین تولید دیگر ادوات و تجهیزات زیرساختی بیش از پیش همت گمارد.

نتیجه‌گیری

با توجه به اینکه، نزدیک به یک قرن است از تولد اولین سازمان بین‌المللی می‌گذرد (جامعه ملل) و فضای حاکم بر روابط بین‌الملل کوچک‌ترین تغییری نکرده است. هرچند سازمان‌های بین‌المللی در بسیاری از زمینه‌ها توانسته‌اند به موفقیت‌هایی دست یابند اما هنوز مهم‌ترین نگرانی دولت‌ها همانند قرون‌وسطا در مورد بقایشان است و هنوز فضای آنارشیک نظام بین‌المللی در بسیاری از موارد دولت‌ها را مجبور به خوداتکایی می‌نماید. ازاین‌رو دولت‌ها باوجود تعدد موافقت‌نامه‌ها، نهادها و رژیم‌های خلع سلاحی و کنترل تسلیحاتی نمی‌توانند به‌صورت کامل به‌نظام بین‌المللی اتکا کنند و امنیت خود را به آن‌ها بسپارند. فضای سایبر نیز همانند دیگر پدیده‌های جامعه بشری از این الگو خارج نیست و با توجه به آنچه در ضمن این مقاله

1. NPT
2. Press TV

ارائه شد، می‌توان به این نتیجه رسید که پیش‌نویس موافقت‌نامه امنیت فضای سایبر نیز، مانند دیگر موافقت‌نامه‌ها می‌تواند در بعضی زمینه‌ها برای بازتولید امنیت، موفقیت نسبی بیابد اما حتماً نمی‌تواند به‌صورت جامع بدان دست یابد. در این مقاله ما با استفاده از روش تحقیق تفسیرگرایی به غور در ادبیات دیپلماتیک جمهوری اسلامی ایران درزمینهٔ موافقت‌نامه‌های کنترل تسلیحاتی و خلع سلاحی پرداخته و با استفاده از آن تجارب به بررسی و کنکاش درزمینهٔ پیش‌نویس موافقت‌نامه امنیت سایبری که توسط روسیه تهیه شده است، پرداختیم. در روش تفسیرگرایی با استفاده از رویکرد گفتمانی به تجزیه و تحلیل موضوعات بر اساس تجارب گذشته و تفکرات و تصمیمات سیاستمداران پرداختیم. از این رهگذر در این پژوهش پیش‌رو به‌صورت مکرر از تصمیمات و گفته‌های دولت‌مردان غربی نقل قول کردیم؛ و از لحاظ حقوقی به دفعات بسیار بین مواد پیش‌نویس مذکور و دیگر معاهدات بین‌المللی همانندسازی[1] نمودیم.

نتیجه این سعی و ممارست آن بود که در این مقاله ما هفت بوته آزمایش برای پیش‌نویس موافقت‌نامه امنیت سایبری تحت عناوینی همچون: جاسوسی اینترنتی، تروریسم، حقوق بشر، اصول غیرقابل تقسیم امنیت، حاکمیت، دفاع از خود، سوءاستفاده از اینترنت، تهیه دیدیم و مواردی را که از دید پژوهشگران برای امنیت و منافع ملی جمهوری اسلامی، مهم و خطیر به نظر می‌رسید مورد کنکاش قراردادیم که شرح نتایج آن‌ها به‌صورت خلاصه در جدول زیر گنجانده‌شده است:

عنوان تهدیدها	نحوه تهدیدها
جاسوسی اینترنتی	عدم ممنوعیت برای جاسوسی، عدم تطابق با واقعیت
تروریسم	استفاده ابزاری غرب از تروریسم، عدم شفافیت، عدم گستردگی‌های لازم برای موضوع تروریسم
حقوق بشر	عدم فهم مشترک از موضوع حقوق بشر، ریشه داشتن موضوع

1. Homogenize

	در حقوق اروپا
اصول غیرقابل تقسیم امنیت	عدم شفافیت و عدم تطابق با واقعیت در باب اصول مذکور
حاکمیت	عدم کارایی نظام حاکمیت ملی، عدم وجود حاکمیت بر زیرساخت‌ها و احتمال تشکیل رژیم کنترل صادرات
دفاع از خود	عدم شفافیت، وابستگی دفاع از خود به عبارت جنگ سایبری
سوءاستفاده از اینترنت	انحصارگری زیرساخت‌ها، عدم تطابق با واقعیت

(یافته‌های تحقیق)

همان‌گونه که در متن به تفسیر بیان شد، پیش‌نویس موافقت‌نامه امنیت سایبری که توسط دولت روسیه تهیه شده است، تلویحا هیچ اشاره‌ای به موضوع بسیار حساس جاسوسی اینترنتی ننموده است. این موضوع ازآن‌رو مهم است که در سال‌های اخیر شاهد رشد روزافزون جاسوسی سایبری هستیم. از این منظر جامعه بین‌المللی انتظار دارد که موافقت‌نامه امنیت سایبری نه‌تنها به این موضوع بپردازد بلکه چارچوب محکم و استواری را برای پیشگیری از جاسوسی سایبری بنا نهد.

در بند بعدی محققان در ضمن بررسی موافقت‌نامه، نظر به موضوع تروریسم، پی به این نکته بردند که در موافقت‌نامه امنیت سایبری، مفهوم «تروریسم» به‌خوبی پرورانیده نشده و دارای نقاط ضعف و ابهام بسیاری است. در اینجا لازم است یادآور شویم، بنا به تجارب موافقت‌نامه‌های دیگر (که در متن در موردشان به تفسیر توضیح داده‌شده است) یا باید تعریف بسیار دقیق و مضیقی از تروریسم در معاهده گنجانده شود و یا مفهوم آن به‌کلی از متن معاهده حذف گردد.

در ادامه ما با ریشه یابی مفهوم «حقوق بشر» در حقوق اروپا و یادآوری این نکته که در تمامی ۳۰ سال گذشته، حقوق بشر همواره ابزاری در دست غرب بوده که به‌وسیله آن حیثیت جمهوری اسلامی را هدف قرار داده است؛ این نکته را متذکر شدیم که درک جامعه بشری از این مفهوم یکسان نیست و نیاز به کنکاش بیشتری در این وادی وجود دارد. در همین راستا ما

باید به یاد داشته باشیم که هیچ‌گاه دولت‌های ابرقدرت، امنیت خویش را با دیگر دولت‌ها همسان و یکسان نمی‌انگارند و حتماً در این راستا به دست‌اندازی و زیاده‌خواهی همت خواهند گمارد. به‌خصوص اینکه این پیش‌نویس در خصوص این دو مفهوم هیچ‌گونه شفافیتی ندارد و زمینه مناسبی را برای سوءاستفاده‌های احتمالی دولت‌های بزرگ فراهم خواهد نمود.

درباره موضوع «حاکمیت»، همان‌گونه که بسیاری از اندیشمندان معتقدند، نظام مفهومی حاکمیت در برابر پدیده «فضای مجازی» رنگ‌باخته و نیازمند بازتعریف است. ازاین‌رو اساساً تشکیل موافقت‌نامه‌ی بر این مفهوم قدیمی و ناکارآمد نه‌تنها کاری بس عبث است بلکه زمینه اختلاف و سردرگمی دولت‌های تعهد دهنده را نیز فراهم می‌آورد.

همان‌گونه که در متن پژوهش و در زیر موضوع «دفاع از خود» گفته شد، این مفهوم در موافقت‌نامه امنیت سایبری به‌خوبی گنجانیده و پرورانیده نشده است. چراکه این مفهوم حقوقی در ارتباط با «جنگ» معنا می‌یابد، این در حالی است که جنگ سایبری و نحوه تسریع یافتن انواع دیگر جنگ‌ها به محیط سایبر، هنوز از مفاهیم گنگ حقوق بین‌الملل است.

یکی دیگر از موضوعاتی که ذهن دولت‌های جنوب را مدام درگیر خود می‌نماید، این نکته است که اگر دکترین حاکمیت ملی در فضای سایبر رسمیت بیابد، چگونه بر مراکز داده‌پردازی بین‌المللی که در حوزه سرزمینی دولت‌های شمال قرار دارند، می‌توان اعمال‌نفوذ کرد؟ و یا چگونه می‌توان از اعمال‌نفوذ آن دولت‌ها جلوگیری به عمل آورد؟ و دیگر سؤالاتی ازاین‌دست که پیش‌نویس موافقت‌نامه امنیت سایبری، تهیه‌شده توسط دولت روسیه، نمی‌تواند به آن‌ها پاسخ مناسب دهد. این پژوهش به تحقیق این امر را به اثبات رسانید که حداقل درزمینه‌هایی همچون آزادی تبادل اطلاعات و حقوق بشر، مبارزه با تروریسم، جلوگیری از جاسوسی اینترنتی و ... این پیش‌نویس می‌تواند تهدیدزا باشد.

منابع

۱. میرزایی، سید احمد .(۱۳۹۱). «***کنوانسیون تسلیحات زیستی***»، تهران: انتشارات دانشگاه صنعتی مالک اشتر، چاپ اول. صص ۱۶۳

۲. میرزایی، سید احمد .(۱۳۸۳). «***کنوانسیون منع توسعه، تولید، انباشت و به‌کارگیری سلاح‌های شیمیایی***»، تهران: انتشارات دانشگاه مالک اشتر، چاپ ۳.

۳. ضیائی بیگدلی، محمدرضا .(۱۳۸۸). «***حقوق بین‌الملل عمومی*** »، تهران: انتشارات کتابخانه گنج دانش، چاپ ۶، صص ۵۰۲.

۴. ضیائی بیگدلی، محمدرضا .(۱۳۹۱). «***حقوق معاهدات بین‌المللی***»، تهران: انتشارات کتابخانه گنج دانش، چاپ ۵، ۲۳۸.

۵. نش، کیت .(۱۳۹۳). «***جامعه‌شناسی سیاسی معاصر***»، دل‌افروز محمدتقی، تهران: انتشارات کویر، چاپ ۱۲، صص ۵۵.

۶. سید امامی، کاووس .(۱۳۹۰). «***پژوهش در علوم سیاسی***»، تهران: انتشارات پژوهشکده مطالعات فرهنگی و اجتماعی، چاپ ۳،صص ۷۷-۵۷.

۷. رمضانی، روح‌الله .(۱۳۸۳). «***چارچوبی تحلیلی برای بررسی سیاست خارجی جمهوری اسلامی ایران***»، ترجمه طیب علیرضا، تهران: انتشارات نشرنی، چاپ ۳

۸. ساعد، نادر .(۱۳۸۸). «***حقوق خلع سلاح و حاکمیت دولت‌ها***»، تهران: انتشارات خرسندی، چاپ ۱، ص ۹۳.

۹. عبدالله خانی، علی .(۱۳۸۹). «***نظریه‌های امنیت***»، تهران: انتشارات ابرار معاصر، چاپ ۱، صص۶۵.

۱۰.جلالی فراهانی، امیرحسین .(۱۳۸۴). «***پیشگیری وضعی از جرائم سایبر در پرتو موازین حقوق بشر***»، تهران: انتشارات فقه و حقوق، چاپ ۲، صص ۱۳۳

۱۱.حسن‌بیگی، ابراهیم .(۱۳۸۸). «***حقوق و امنیت در فضای سایبر***»، تهران: انتشارات دانشگاه عالی دفاع ملی، چاپ ۲، صص۱۰.

۱۲.ابراهیم‌نژاد، محمد، اسکندری، حمید .(۱۳۹۲). «***جنگ سایبری***»، تهران: انتشارات بوستان حمید، چاپ ۱، صص ۳۵.

۱۳.کولیور، ساندرا و دیگران .(۱۳۷۹). «آزادی، حق و امنیت»، ترجمه آقایی، علی‌اکبر، ***فصلنامه مطالعات راهبردی***، شماره ۴۹، صص ۶۹.

۱۴.قاسمی، علی، بارین، چهار بخش ویکتور .(۱۳۹۲). «مبانی حقوقی کاربرد زور در فضای سایبر بر پایه حقوق بین‌الملل»، ***مجله سیاسی- اقتصادی***، تهران، شماره ۲۹۲، صص ۱۶

15. Diplomacy Irani, www.***diplomacyirani.org***/Iran/Stux_net/US,2/1/2014,2/2/2014

16. Mary Ellen O'Connell .(2012). ***Cyber Security without Cyber War***, Journal of Conflict & Security Law, Oxford University Press, pp 25.

17. Foreign ministry of Russia, ***Cyber security convention***, www.FMRU.ru/cyber_security_convention, 4/9/2010, 2/5/2011

18. WTO, ***Indian increase rate***,www.WTO.org,18/6/2012,2/5/2013

19. Dan Kuehl, quoted by Grace Chng .(2010). "***Cyber War: One Strike, and You're Out***, «*Sunday Times,* July 18, (Singapore)», pp 59.

20. ***Cybersecrity Act*** of 2012, 112th Congress, 2 Decisions, Feb2012

21. Caspersky, ***Caspersky secutity list***,www.athena.ir/Securelist / January, 18/1/2014, 25/3/2014

22. Alexander Balayan .(2012). ***The Role of Conflicts of the New Type in the Formation of the Information,*** New York Times, October 11, pp 63.

23. Maura Conway .(2003). ***Cyber cortical Warfare: The Case of Hizbollah***.org, Department of Political Science, 28, pp 24.

24. Ronald J. Deibert, ***The geopolitics of internet control: Censorship***, sovereignty, and cyberspace, Oxford University Press, 2,2010

25. Elisabeth Bumiller and Thom Shanker .(2012). "***PanettaWarns of Dire Threat of Cyberattack***, *New York Times*, October 11, pp 55-59.

26. CSRC, ***Cyber security convention***, www.CSRC.org/draftconvention/cybersecrity/russai.pdf,30/4/2010 4/5/2010

27. IISI, ***Cyber security convention***, www.IISI.org/Cybersecrity/Russia/convention.pdf, 5/6/2010, 6/9/2011

28. Rogier Creemers .(2012). "***The Internet, Soft War, Sovereignty, and China***,» MILTON WOLF SEMINAR COMPENDIUM, pp 81.

29. Streltsov A .(2013). ***International information security: description and legal aspects***, Disarmament Forum, pp 56.

30. Mashable, snowden,***www.mashable.com***/2014/06/05/edward-snowden-revelations, 5/6/2014, 8/10/2014

31. Theatlantic, snowden, ***www.theatlantic.com***/politics/archive/2014/07/a-devastating-leak-for-edward-snowdens-critics/373991, 1/7/2014, 8/8/2014

32. Theguardian, NSA, http://***www.theguardian.com***/us-news/the-nsa-files, 6/2/2014, 5/3/2014

33. Wikipedia, Global surveillance disclosures, http://***en.wikipedia.org***/wiki/Global_surveillance_disclosures_2013, 2/5/2013, 5/7/2014

34. Asis, Cybersecurity and Cyberwar, http://***news.asis.io***/sites/default/files/Cybersecurity_and_Cyberwar.pdf, 2/10/2013, 19/11/2013

35. OSCE, all thing about OSCE, ***www.OSCE.org***, 1/3/2014, 2/5/2014

36. New York Times, stuxnet&iran, ***www.NYTIMS.com***/stuxnet&iran, 20/1/2010, 16/4/2011