مطالعات حقوق انرژی، دورهٔ ۸، شمارهٔ ۱، بهار و تابستان ۱۴۰۱، صفحات ۱۹۳-۱۷۳ (مقاله علمی پژوهشی)

ضرورت تقویت امنیت سایبری بخش انرژی توسط دولت‌ها*

پرویز فرشاسعید

دانشجوی دکترای حقوق بین‌الملل عمومی، دانشگاه آزاد اسلامی، واحد اصفهان (خوراسگان)، اصفهان،ایران

محمود جلالی**

دانشیار گروه حقوق، دانشکده علوم اداری و اقتصاد دانشگاه اصفهان،اصفهان، ایران

مهناز گودرزی

دانشیار گروه روابط بین‌الملل، دانشگاه آزاد اسلامی، واحد اصفهان (خوراسگان)،اصفهان، ایران

چکیده

نقش با اهمیت رایانه و اینترنت و خدماتی که این فناوری‌ها به بشریت ارائه می‌دهند، باعث شده است بخش انرژی هم به این فناوری‌های نوین وابسته گردد. به دنبال چنین وابستگی‌ای، خطراتی هم برای حوزهٔ انرژی ایجاد گردیده که مهم‌ترین آن‌ها، هدایت حملات سایبری علیه این بخش است. در پژوهش پیش رو، این پرسش مطرح شده است که ضرورت تقویت امنیت سایبری بخش انرژی توسط دولت‌ها چیست و باید چه اقداماتی را در سطح داخلی و بین‌المللی در پیش بگیرند؟ با استفاده از روش توصیفی- تحلیلی به این پرسش پاسخ داده شده است که به دلیل افزایش وابستگی بخش انرژی به فناوری‌های حوزهٔ سایبری و افزایش تعداد بازیگران و مرتکبان حملات سایبری در جهان، نیاز است تا دولت‌ها به تقویت امنیت سایبری بخش انرژی خود بپردازند. اقداماتی که دولت‌ها می‌توانند در سطح داخلی انجام دهند شامل افزایش ایمنی سامانه‌های داخلی، استخدام نیروهای قابل اعتماد و متخصص و تدوین قوانین شفاف و سختگیرانه برای حوزهٔ سایبر است. در سطح بین‌المللی نیز همکاری آن‌ها برای تدوین یک معاهدهٔ بین‌المللی الزام‌آور دربارهٔ ممنوعیت حملات سایبری به بخش انرژی، می‌تواند مهم‌ترین اقدام باشد.

واژگان کلیدی: *امنیت سایبری، بخش انرژی، حملات سایبری، فناوری‌های نوین.*

---

* مقاله حاضر مستخرج از رساله با عنوان «قلمرو انطباق اصول حاکم بر دفاع مشروع سنتی با دفاع مشروع در فضای سایبر از دیدگاه حقوق بین‌الملل» می‌باشد.

** نویسندهٔ مسئول Email: m.jalali@ase.ui.ac.ir

تاریخ دریافت: ۱۸ بهمن ۱۳۹۹، تاریخ تصویب: ۳۰ خرداد ۱۴۰۱

DOI: 10.22059/JRELS.2022.316656.413

مقدمه

امنیت سایبری عملی برای دفاع از رایانه‌ها، سِرورها، دستگاه‌های تلفن همراه، سامانه‌های الکترونیکی، شبکه‌ها و داده‌ها در برابر حملات مخرب است. همچنین به عنوان امنیت فناوری اطلاعات یا امنیت اطلاعات الکترونیکی شناخته می‌شود. این اصطلاح در زمینه‌های مختلفی از تجارت تا رایانه‌های سیار اعمال می‌شود و می‌تواند به چند دستهٔ رایج تقسیم گردد (Kaspersky.com). بخش انرژی در حال ورود به انقلابی دیجیتالی – اگرچه با تأخیر خاصی نسبت به سایر بخش‌ها– است. فناوری‌های اطلاعات و ارتباطات رفته‌رفته در حال به‌کار گرفته شدن در زیرساخت‌های انرژی و نیز تغییر فرایندهای تولید، تبدیل، ذخیره و مصرف انرژی هستند (Desaranaud, 2017: 13).

دیجیتالی شدن موجب تغییر جامعهٔ جهانی شده و به‌رغم فرصت‌های مثبتی که به همراه داشته، تغییری در فهم ما نسبت به امنیت شخصی و عمومی ایجاد نکرده است. این دیجیتالی شدن بخش انرژی، با وجود این‌که باعث راحتی انجام کارها و ارتقای این بخش شده، به دلیل این‌که بخشی از فضای سایبری گردیده، خطرات و مضراتی را هم برای این بخش به همراه داشته است. به دنبال پیشرفت سریع فناوری‌های دیجیتالی از سال ۱۹۷۰ به این سو، از ارتباط درونی بین خدمات فیزیکی و مجازی، خطر دیجیتالی جدیدی پدید آمده و به‌تازگی استفاده از حجم زیادی از داده‌ها به تهدیدهای امنیتی فیزیکی مانند جنگ‌ها و بلایای طبیعی افزوده شده است (Mikko & Kisa, 2020: 353). انرژی همواره قسمتی از منافع ملی بوده و بنابراین تا حد زیادی در برابر خطرات آسیب‌پذیر بوده است (Vasileiou, 2019: 6).

رقابت بین‌المللی دولت‌ها و قطب‌بندی‌های بین‌المللی که در سطح جهان شکل گرفته، رقابتی بین‌المللی را در جهان پدید آورده است که این رقابت هم‌اکنون به دلیل کارکردها و ویژگی‌های فضای سایبر به این عرصه کشیده شده است. کشورهایی که در دنیا رقیب هم هستند، دریافته‌اند که اگر بخش انرژی را هدف حملات سایبری قرار دهند می‌توانند با کمترین هزینه بیشترین خسارت‌ها را به رقبای خود وارد سازند. از آغاز سال ۱۹۸۲ تا کنون که اولین حملهٔ سایبری به خطوط گاز سیبری روسیه انجام و موجب انفجار در این خطوط شد، حملات سایبری متعددی به بخش انرژی انجام شده است که برای نمونه می‌توان به حملهٔ سایبری استاکس‌نت[1] به سایت هسته‌ای نطنز در ایران اشاره کرد. استاکس‌نت یکی از معروف‌ترین بدافزارهایی است که برای در اختیار گرفتن سامانهٔ کنترلی تأسیسات برنامه‌ریزی شد. در ابتدای سال ۲۰۱۰، یک شرکت امنیت رایانه‌ای در بلاروس این بدافزار را شناسایی و معلوم کرد که هزاران سامانهٔ کنترل صنعتی را در گسترهٔ جهانی آلوده کرده است (خلف‌رضایی، ۱۳۹۲: ۱۴۰).

1. Stuxnet

استاکس‌نت به گونه‌ای طراحی شده بود که سامانه‌های کنترل صنعتی ساخت شرکت زیمنس آلمان را مورد حمله قرار دهد. مهم‌ترین هدف این بدافزار، تأسیسات و تجهیزات غنی‌سازی اورانیوم ایران بوده است و به‌طور خاص برای هدف قرار دادن دستگاه‌های سانتریفیوژ تأسیسات نطنز برنامه‌ریزی شده بود (خلف‌رضایی، ۱۳۹۲: ۱۴۱). اگرچه به‌طور رسمی اثبات نشد، اما کشورهای ایالات‌متحده‌آمریکا و اسرائیل در پشت این حملات بودند و قصد آن‌ها ایجاد اختلال و مانع در برنامهٔ هسته‌ای جمهوری اسلامی ایران بود؛ زیرا ایران هسته‌ای، منافع آن‌ها را در خاورمیانه به خطر می‌انداخت و این رقابتی سیاسی بین این دولت‌ها و دولت جمهوری اسلامی ایران بود.

حملهٔ سایبری معروف دیگری که به بخش انرژی انجام شد، حملهٔ سایبری آگوست ۲۰۱۲ معروف به شامون[1] بود که نزدیک به سی هزار رایانهٔ مربوط به شرکت نفتی آرامکو عربستان سعودی را نابود کرد. هدف اصلی از انجام این حمله، خرابکاری و ایجاد اختلال در فعالیت‌های صنعتی این شرکت بود. در سال ۲۰۱۴ نیز دویست‌وپنجاه شرکت انرژی در ایالات‌متحده و اروپای غربی با ویروسی شبیه استاکس‌نت آلوده شدند که انرجتیک بر[2] نامیده می‌شد. این بدافزار از سال ۲۰۱۱ در حال فعالیت بوده و بیشتر تولیدکنندگان برق، اپراتورهای توزیع نفت و برق و تولیدکنندگان تجهیزات را آلوده کرده بود. در سال ۲۰۱۵ نیز یک حملهٔ سایبری به شبکهٔ برق اوکراین باعث قطع برق دویست هزار نفر از شهروندان این کشور گردید (Desaranaud, 2017: 16). در ژوئن سال ۲۰۱۷ حملات سایبری در ابعاد جهانی به برخی از بزرگترین شرکت‌های جهان در آمریکا، اروپا و بخشی از آسیا انجام شد که نیروگاه هسته‌ای «چرنوبیل» و شرکت بزرگ نفت و گاز «روس‌نفت» روسیه، هدف این حملات قرار گرفتند. موارد یادشده از حملات سایبری به تأسیسات انرژی در سراسر دنیا، نشان می‌دهد بخش انرژی که مهم‌ترین قسمت تمدن بشری است، با چالش حملات سایبری روبه‌روست.

دربارهٔ موضوع مورد بحث ما –یعنی ضرورت تقویت امنیت سایبری بخش انرژی– تاکنون پژوهش‌های فراوانی انجام نشده است. در سال ۲۰۱۷ مقاله‌ای با عنوان «حملات سایبری و زیرساخت‌های انرژی: پیش‌بینی خطرات»[3] توسط گابریل دزرنود[4] نوشته شده است. نویسنده در این مقاله بیان می‌کند که با توجه به این‌که سامانه‌های بخش انرژی به تجهیزات دیجیتالی جدید متصل شده‌اند، این باعث کارایی بهتر این بخش گردیده اما این تأسیسات را در معرض

1. Shamoon
2. Energetic bear
3. Gabrielle, Desarnaud (2017). "Cyber Attacks and Energy Infrastructures: Anticipating Risks". Études de l'Ifri, Ifri,1-60. https://www.ifri. org /en/publications/etudes –de –lifri/ cyber –attacks -and-energy –infrastructures –anticipating –risks
4. Gabrielle Desarnaud

حملات سایبری قرار داده است. اگرچه بعد از حملهٔ سایبری استاکس‌نت علیه تأسیسات هسته‌ای ایران در سال ۲۰۱۰، تعداد و پیچیدگی این حملات افزایش یافته است. امروزه با وجود آگاهی واقعی از تهدیدات حملات سایبری به بخش انرژی، هنوز تهدیدات وجود دارند. مقامات کشور فرانسه از نزدیک با شرکت‌های انرژی کار می‌کنند تا چهارچوب قانونی الزام‌آوری ایجاد و اپراتورهای مهم را محافظت نمایند. این رویکرد برای کشورهای دیگر اروپایی نیز الهام‌بخش است، اما نیاز است اقدامات مشترکی به‌سرعت در سراسر اتحادیهٔ اروپا انجام شود تا امنیت بخش انرژی تضمین گردد.

در پایان‌نامهٔ کارشناسی‌ارشد آقای کنستانتینا جی واسیلف[1] با عنوان «امنیت سایبری در بخش انرژی: یک نگرش جامع»[2]، نویسنده بیان می‌کند که دولت‌ها باید به تعریف مشترکی از مفهوم امنیت سایبری و حملهٔ سایبری برسند؛ زیرا چنین اقدامی می‌تواند مسئلهٔ انتساب یک حمله و مجازات فاعل آن را آسان‌تر نماید. بحث دیگر، هماهنگ ساختن قوانین ملی و قوانین بین‌المللی برای حل مسئلهٔ صلاحیت است و دولت‌ها باید توافق‌نامه‌های دوجانبه و چند جانبه‌ای امضا کنند؛ چنین اقداماتی می‌تواند توسط سازمان‌های چندجانبه مانند ناتو و سازمان ملل‌متحد مورد حمایت قرار گیرد. اقدام دیگر، ایجاد ابزاری اطلاعاتی است که شرکت‌ها بتوانند اطلاعات خود را دربارهٔ تجربهٔ حمله به‌اشتراک بگذارند و دولت‌ها داده‌ها و مدارک الکترونیکی را به‌منظور تعیین عاملان حملات سایبری و اقدام به‌موقع جمع‌آوری کنند.

تحقیق پیش رو نیز به دلیل فقر منابع در موضوع مورد بحث، یعنی ضرورت تقویت امنیت سایبری بخش انرژی که موضوعی بسیار مهم برای دولت‌هاست، نوشته شده است. با توجه به افزایش حملات سایبری که هر روزه در سطح جهان علیه این بخش مهم و پُراهمیت انجام می‌گیرد و در آینده نیز خطرات بیشتری از طریق فضای سایبری متوجه این بخش خواهد شد و با توجه به این‌که تا کنون به بحث امنیت سایبری به عنوان موضوعی کلی پرداخته شده و مقالات متعددی هم دربارهٔ آن نگاشته شده است، نگارندگان کوشیده‌اند توجه همگان را به این موضوع مهم و باارزش -یعنی امنیت سایبری بخش انرژی- جلب کنند تا دولت‌ها ترغیب گردند توجه بیشتری برای حفاظت از این بخش انجام دهند.

در این تحقیق، افزون بر کنکاش در بحث ضرورت تقویت امنیت سایبری، به دنبال پاسخ به این پرسش هستیم که چه اقداماتی می‌تواند در سطح داخلی یا بین‌المللی توسط دولت‌ها برای تقویت امنیت سایبری اتخاذ گردد؟ با روش توصیفی-تحلیلی به این پرسش پاسخ داده شده که به دلیل وابستگی شدید بخش انرژی به فضای سایبری و فناوری‌های مرتبط با این

1. Konstantina G.Vasileiou
2. Cybersecurity in the Energy Sector A Holistic Approach

حوزه و افزایش تعداد بازیگران و مرتکبان حملات سایبری در جهان، نیاز است تا دولت‌ها به‌منظور جلوگیری از وارد آمدن خسارت‌های احتمالی در آینده، به تقویت امنیت سایبری این حوزه بپردازند؛ وگرنه دچار خسارت‌ها و زیان‌هایی خواهند شد که ممکن است در نتیجهٔ حملات سایبری رقبایشان به آن‌ها وارد گردد. در این نوشتار، نخست دلایل آسیب‌پذیری این بخش بیان شده و سپس اقداماتی که دولت‌ها می‌توانند، چه در سطح داخلی و چه در سطح بین‌المللی، انجام دهند، مطرح گردیده است. آنچه تفاوت تحقیق حاضر با تحقیقات انجام‌شده قبلی را نشان می‌دهد، ارائهٔ راهکارهایی در سطح داخلی و بین‌المللی است که می‌تواند مورد توجه دولت‌ها قرار گیرد.

۱. دلایل آسیب‌پذیری بخش انرژی

یکی از مهم‌ترین ویژگی‌های عصر حاضر، تحولات سریع فناوری اطلاعات و ارتباطات است. این تحولات، فرصت‌های بسیاری را در حوزه‌های مختلف برای انسان‌ها ایجاد کرده، باعث بهبود و تغییر در زندگی آن‌ها شده است. اینترنت به عنوان شبکهٔ جهانی اطلاعات و ارتباطات، بزرگترین پدیدهٔ این تحولات است (رضایی و بابازاده مقدم، ۱۳۹۳: ۴۴). با توجه به تأثیر چشمگیر اینترنت به عنوان یک ابزار ارتباطی و رسانهٔ نوین در تأمین آزادی بیان و بهبود زندگی مردم، استفاده از آن امری ضروری است. کنارگذاشتن این فناوری از بیم آسیب‌ها و مضرات آن، اقدامی نسنجیده بوده و دولت‌هایی موفق هستند که بتوانند با تدابیر و اقدامات مناسب، ضمن استفادهٔ کامل از تمام فواید و امکانات اینترنت، آسیب‌های آن را از بین برده یا به حداقل برسانند (رضایی و بابازاده مقدم، ۱۳۹۳:۷۹). چنانکه اینترنت به عنوان پدیده‌ای مهم تمام سطوح زندگی و تمدن بشری را دربرگرفته و سیطرهٔ آن، بخش انرژی را نیز رها نکرده و این بخش به این فناوری بسیار وابسته شده است. چنین وابستگی‌ای باعث شده تا دولت‌های رقیب و گاه خرابکاران بخش خصوصی به طمع بیفتند تا حملات سایبری را علیه این بخش تدارک ببینند. آنچه باعث آسیب‌پذیری این بخش گردیده، وابستگی روزافزون و شدید بخش انرژی به فناوری‌های حوزهٔ سایبری و افزایش تعداد بازیگران و مرتکبان حملات سایبری در جهان است که در ادامه به آن‌ها پرداخته خواهد شد.

۱. ۱. افزایش وابستگی بخش انرژی به فناوری‌های حوزهٔ سایبری

بخش عمده‌ای از فعالیت‌ها و تعاملات اقتصادی، تجاری، فرهنگی، اجتماعی و حاکمیتی کشورها در همهٔ سطوح، اعم از افراد، مؤسسات غیردولتی و نهادهای دولتی و حاکمیتی، در فضای سایبری انجام می‌گیرد. امروزه تمامی زیرساخت‌های حیاتی واحدهای صنعتی و

تجهیزات مدرن شهری و کشوری از سامانه‌های کنترل و اتوماسیون مبتنی بر شبکه برای پایش و کنترل فرایندهای خود بهره می‌برند. استفاده از فناوری ارتباطات و رایانه که به‌منظور افزایش کیفیت کارایی و ضریب اطمینان در سامانه‌های اتوماسیون و کنترل به‌کار می‌روند، تهدیدات ناخواسته‌ای را متوجه این سامانه‌ها کرده‌اند؛ ازجمله مهم‌ترین این تهدیدات، حمله‌های سایبری است (افشار و همکاران، ۱۳۹۳: ۳۱). این وابستگی شدید تأسیسات بخش انرژی باعث گردیده دولت‌ها در سطح بین‌المللی به فکر اقدامات خرابکارانه علیه رقبای خود بیفتند؛ زیرا زیرساخت‌های بخش انرژی، مهم‌ترین و ارزشمندترین زیرساخت‌های کشورها هستند و هرگونه حملهٔ سایبری موفق علیه این زیرساخت‌ها، خسارت‌های جبران‌ناپذیری را به کشورهای قربانی وارد می‌سازد. هرچه سرعت و شتاب اینترنت بیشتر گردد، یعنی دولت‌ها از اینترنت پرسرعت‌تر استفاده کنند، خطر حملات سایبری نیز گسترده‌تر می‌شود. تأثیر گستردهٔ فضای سایبری باعث شده است وجوه مختلف زندگی مردم دنیا با آن درآمیخته و هرگونه بی‌ثباتی، ناامنی و چالش در این حوزه، زندگی شهروندان را به خطر بیندازد. تجربه‌ای که از حملات نظامی علیه کشورهای دیگر وجود دارد این است که ابتدا حملات سایبری به زیرساخت‌های حیاتی این کشورها هدایت شده و پس از فلج کردن این قسمت‌ها، حملات نظامی انجام گرفته‌اند؛ برای مثال، در جنگ اوستیای جنوبی در سال ۲۰۰۸، پیش از این‌که روس‌ها به خاک گرجستان حمله کنند، حمله‌ای سایبری به منابع اینترنتی دولت گرجستان انجام گرفت و در نتیجهٔ آن، سایت‌های دولتی گرجستان از دسترس خارج شد. تهدیدی که ویروس استاکس‌نت برای زیرساخت‌های حیاتی کشورهای صنعتی ایجاد کرد، دو وجهه دارد؛ از یک‌سو، ویروس استاکس‌نت نشان‌دهندهٔ فرصت برای تروریست‌ها، هکرها، مجرمان و دولت‌ها برای نفوذ و تخریب سامانه‌های الکتریکی، مالی، گاز، نفت، آب و فاضلاب است و از سوی دیگر، سطح پیچیدگی ویروس استاکس‌نت به بسیاری از سران دولت‌های صنعتی گوشزد نمود که احتمال حملات سایبری به زیرساخت‌های صنعتی حیاتی آن‌ها وجود دارد (Trautman & Ormerod, 2018: 798). براساس گزارش ماه نوامبر مؤسسهٔ مکافی[1] دربارهٔ تهدیدات سایبری، حجم تهدیدات بدافزاری مشاهده‌شده توسط آزمایشگاه مکافی به‌طور متوسط ۴۱۹ تهدید در دقیقه و در نیمهٔ دوم سال ۲۰۲۰ با افزایش ۴۴ تهدید در دقیقه (۱۲ درصد) بوده است (McAffee Report, 2020: 5). براساس این مطالعه در نیمهٔ دوم این سال، حملات سایبری علیه بخش علم و فناوری نسبت به نیمهٔ نخست این سال، ۹۱ درصد افزایش داشته است (McAffee Report, 2020: 7). چنین پایگاه‌های علم و فناوری، گاهی مرتبط با مطالعات حوزهٔ انرژی هستند

1. McAffee

که به دلیل ارزشمندی بالا، مورد توجه دولت‌ها و بخش خصوصی بوده و هدف ارزشمند و پُراهمیتی برای دولت‌های رقیب است تا حملات سایبری را علیه آن‌ها هدایت کنند.

۲. ۱. افزایش تعداد بازیگران و مرتکبان حملات سایبری در جهان

امروزه به دلیل ظرفیت‌های ویژه‌ای که فضای سایبری و فناوری‌های این حوزه برای بشر فراهم آورده، تمام امور زندگی بشری به این فضا و فناوری‌های مرتبط با آن وابسته گردیده است. گستردگی شبکهٔ اینترنت در سطح جهانی و وابستگی همهٔ امور بشری به این فناوری نوین، حجم و تعداد حملات سایبری را بسیار افزایش داده است. به دنبال همه‌گیری ویروس کرونا، فعالیت‌های دورکاری کارکنان دولتی و شرکت‌های خصوصی و سکونت در منزل تعداد زیادی از مردم باعث شده است افراد بیشتری از اعضای جامعه به ارتکاب حملات سایبری بپردازند. متأسفانه اکنون در حال مشاهدهٔ حملات سایبری علیه بیمارستان‌ها، گروه‌های تولیدکننده و زیرساخت‌های حیاتی مرتبط با توسعه و توزیع واکسن کووید ۱۹ هستیم. این حملات سایبری احتمالاً در سال ۲۰۲۱ کاهش نخواهد یافت. بنابراین سازمان‌ها و دفاع‌کننده‌ها باید هشیار باشند. هم‌اکنون ما شاهد افزایش تعداد عوامل دولتی هستیم که تحقیقات ویروس کرونا را هدف قرار داده‌اند. این هدف قرار دادن مستقیم دولت، مراکز بهداشتی، دارویی و سازمان‌های غیردولتی، احتمالاً به خاطر داشتن اطلاعات ارزشمند ادامه خواهد یافت (Fire eye, 2020: 5). به‌تازگی ایالات‌متحده‌آمریکا به‌طور آشکار چین، روسیه و ایران را به تلاش برای هک کردن یکی از شرکت‌های تحقیقات جهانی متهم کرده است (Fire eye, 2020: 5). اگرچه گزارش مؤسسهٔ فایر آی بیشتر دربارهٔ حملات سایبری برای دسترسی به تحقیقات واکسن کروناست، اما روشن است که حوزه‌های دیگر مرتبط با فضای سایبری نباید مورد غفلت قرار گیرد. زیرساخت‌های بخش انرژی به خاطر داشتن ارزش اقتصادی بالا همواره مورد توجه دولت‌ها و عوامل خصوصی بوده است. چنین افزایشی در تعداد بازیگران و مرتکبان حملات سایبری باعث می‌گردد حجم حملات سایبری به زیرساخت‌های بخش انرژی افزایش یابد و اگر دولت‌ها نتوانند اقدامات احتیاطی و حفاظتی را برای حفاظت از زیرساخت‌ها و تأسیسات این حوزه مانند آب، برق، نفت، گاز و سایر حوزه‌های مرتبط انجام دهند، در آینده به دلیل گسترش در تعداد حملات سایبری و مرتکبان این حملات، شاهد ناامنی و برهم خوردن امنیت زیرساخت‌های این حوزه خواهند بود. پیدایش قدرت‌های نوظهور در حوزهٔ فناوری سایبر مانند کره شمالی، چین، ایران و عربستان، باعث گردیده حجم و تعداد حملات سایبری افزایش یابد؛ به‌ویژه در حال حاضر با قطب‌بندی‌هایی که در سطح جهانی شکل گرفته است و دولت‌هایی مانند ایران و عربستان که دارای ذخایر و تأسیسات نفت و گاز هستند و

حکومت‌هایی ایدئولوژیک دارند، به دلیل رقابت سیاسی در منطقه، ممکن است علیه تأسیسات نفت و گازی خودشان حملات سایبری انجام دهند و خسارت‌های بسیار شدید و گسترده‌ای را وارد کنند. از سوی دیگر، دولت اسرائیل دشمن دیرینهٔ کشور جمهوری اسلامی ایران، ممکن است برای افزایش نارضایتی مردم ایران اقداماتی را علیه تأسیسات نفت و گاز و سایر زیرساخت‌های مهم بخش انرژی انجام دهد و خساراتی را به آن‌ها وارد سازد. دولت کره شمالی و چین هم ممکن است در مقابل اقدامات آمریکا دست به حملات سایبری علیه تأسیسات و زیرساخت‌های مهم بخش انرژی این کشور بزنند و از آن‌سو، ایالات‌متحده‌آمریکا نیز به تلافی این اقدامات، حملات سایبری متعددی را علیه این دولت‌ها هدایت کند. چنین وضعیتی در جهان باعث گردیده کشورها متوجه حملات سایبری به بخش انرژی خود باشند و اقدامات احتیاطی را برای حفاظت از این بخش انجام دهند. عملیات فضای سایبری برای حمله‌کننده مزایای زیادی، مانند هدایت پنهان عملیات با منافع زیاد و خطر پایین کشف آن را دربر دارد (Bailey, 2020: 240) و این دلیلی است که هدایت‌کنندگان این حملات به انجام آن‌ها تمایل دارند و هر روز شاهد افزایش این حملات در سطح جهان هستیم.

۲. اهداف دولت‌ها از انجام حملات سایبری به بخش انرژی

۱. ۲. اهداف سیاسی

فضای سایبری نماد برجسته‌ای از حیات مدرن جامعهٔ بشری است. افراد و جوامع در سراسر جهان به‌وسیلهٔ فضای سایبری به یکدیگر متصل شده و ارتباط برقرار می‌کنند (Taskanian, 2017: 339). این پیوند جامعهٔ بشری به‌وسیلهٔ اینترنت، اگرچه باعث سرعت گردش اطلاعات و انجام شدن سریع کارها گردیده، از جهتی دیگر دریچه‌های متعددی را برای سوءاستفادهٔ افراد و دولت‌ها گشوده است. رقابت و مسابقه‌ای که پیش از این در ساخت سلاح‌های کلاسیک وجود داشت، هم‌اکنون به این فضا کشیده شده و عرصهٔ نوینی را برای رقابت دولت‌ها ایجاد کرده است؛ برای مثال، دولت‌هایی مانند آمریکا و اسرائیل که در جبههٔ مخالف کشور ایران قرار دارند همواره در تلاش هستند تا از طریق فضای سایبری خساراتی را به کشورمان وارد آورند. چنانکه پیش‌تر گفته شد، در سال ۲۰۱۰ تأسیسات هسته‌ای نطنز مورد حملات سایبری قرار گرفتند. همچنین در جریان انتخابات سال ۲۰۲۰ آمریکا، دولت‌مردان این کشور اتهاماتی را علیه دولت جمهوری اسلام ایران و دولت روسیه مطرح کردند مبنی بر این‌که این دولت‌ها قصد دخالت در انتخابات ایالات‌متحده‌آمریکا را داشته‌اند. ادعای دولت آمریکا بر این اساس بود که ایران و روسیه با دستبرد سایبری به داده‌های انتخاباتی رأی‌دهندگان آمریکایی و انتشار اخبار جعلی به‌منظور ایجاد سردرگمی، کوشیده‌اند در انتخابات این کشور دخالت کنند. جان

راتکلیف[1]، هماهنگ‌کنندهٔ نهادهای امنیتی آمریکا و کریستوفر ری[2]، مدیر پلیس امنیت داخلی آمریکا، ادعا کردند ایران در تلاش بوده با ارسال ایمیل‌های حاوی پیام‌های مرعوب‌کننده به رأی‌دهندگان حامی حزب دموکرات در چندین ایالت آمریکا، به‌ویژه دو ایالت فلوریدا و پنسیلوانیا – ایالاتی که در آن‌ها رقابت سختی میان دو نامزد انتخابات ریاست جمهوری در جریان بود– اخلال ایجاد کند. این رقابت سیاسی دولت‌ها باعث گردیده که بخش انرژی هم از این تهدیدها در امان نماند و رقابت‌های سیاسی دولت‌ها به این حوزهٔ مهم و باارزش نیز کشیده شود؛ زیرا مهم‌ترین هدفی که کشورهای رقیب دارند، وارد کردن خسارت به رقبای خود است که به دلیل اهمیت زیاد و فوق‌العادهٔ تأسیسات و زیرساخت‌های مرتبط با بخش انرژی، می‌توان انتظار داشت که در حال و آینده حملات به این بخش با شدت بیشتری ادامه یابد و دامنه و گسترهٔ خسارت‌های وارده به این بخش نیز افزایش بسیار و چشمگیری یابد.

۲،۲. اهداف اقتصادی

به دلیل این‌که بخش انرژی دارای اهمیت اقتصادی زیادی است، مهم‌ترین هدف حملات سایبری است. این بخش، ستون فقرات جامعهٔ بشری بوده و باعث چرخیدن چرخ زندگی روزمرهٔ مردم دنیاست و سایر قسمت‌های تمدن و حیات بشری نیز به این بخش وابسته هستند. جرایم سایبری و حملات سایبری علیه بخش انرژی در نوع خودش چالش‌های فراوانی را ایجاد می‌کند. این تهدیدها نمی‌تواند حذف گردد، بلکه می‌تواند کاهش داده شود (Kumar et al, 2017: 250). انگیزهٔ مرتکبان حملات سایبری به زیرساخت‌های بخش انرژی، دستیابی به منافع اقتصادی است که به دو روش سرقت اطلاعات و جاسوسی انجام می‌گیرد. تعداد مشخصی از حملات سایبری به شرکت‌های انرژی نشان‌دهندهٔ این واقعیت است که دلایل حملات به این بخش، مالی و نیز ژئوپلیتیکی است (Desaranaud, 2017: 25).

حملات سایبری به بخش انرژی، افزون بر هدف به‌دست آوردن منافع اقتصادی، با هدف وارد کردن خسارت‌ها و تضعیف اقتصادی دولت‌های رقیب نیز انجام می‌شوند. چالش‌های اقتصادی، بیشترین تهدیدهای امنیتی وجودی را در بُعد سیاسی امنیت ملی به بار می‌آورد. بی‌گمان ناتوانی دولت در تأمین نیازها و رفاه اقتصادی مردم موجب نارضایتی ملت و به تبع آن کاهش مشروعیت و مقبولیت آن می‌شود (جعفری، ۱۳۹۸: ۱۲۱). کاهش توان اقتصادی دولت‌ها در سطح داخلی زندگی مردم، چنین کشورهایی را تحت تأثیر قرار می‌دهد و باعث نارضایتی مردم از حکومت‌ها می‌گردد؛ چنانکه در بحث تحریم‌های اقتصادی نیز چنین اهدافی دنبال می‌شود.

1. John Lee Ratcliffe
2. Christopher Asher Wray

اگر دولت‌ها بتوانند بخش انرژی رقبای خود را از کار بیندازند یا در کارکرد آن اختلال ایجاد کنند، می‌توانند نارضایتی‌های گسترده‌ای را در کشورهایی که هدف این حملات قرار می‌گیرند، ایجاد نمایند؛ برای مثال، اگر حملات سایبری بتواند برای مدتی در سامانه‌های پالایشگاهی صنعت نفت و گاز دولت‌هایی مانند عربستان یا ایران اختلال ایجاد کند و در نتیجهٔ چنین اختلالی، سامانهٔ حمل‌ونقل این کشورها از کار بیفتد، چنین کاری باعث نارضایتی در حجم گسترده‌ای، به‌ویژه در کشوری مانند ایران، خواهد گردید؛ زیرا به دلیل فشارهای گستردهٔ اقتصادی صبر و طاقت مردم در حد پایینی است.

۳. اقدامات دولت‌ها در تقویت امنیت سایبری بخش انرژی

ازآنجاکه حملات سایبری به بخش انرژی جزء خطرناک‌ترین آسیب‌های ساخت دست بشر هستند، جهان امروز نیاز به توجه ویژه‌ای به این آسیب‌ها دارد. اگر جامعهٔ جهانی برای رویارویی با تهدیدات سایبری بخش انرژی اقدامات ضروری و مناسبی را انجام ندهد و راه‌حل درست و منطقی برای برخورد با این پدیده پیدا نکند، در آینده مصایب و مشکلاتی برای صلح و امنیت جهانی پدید خواهد آمد. آنچه مشخص و روشن است، این است که برای رویارویی با این تهدیدها، ابتدا باید در سطح داخلی اقداماتی توسط دولت‌ها انجام گیرد؛ زیرا بدون توجه داخلی به این‌گونه حملات، امنیت بین‌المللی نیز تأمین نخواهد شد. اقداماتی که دولت‌ها می‌توانند در سطح داخلی انجام دهند شامل افزایش ایمنی سامانه‌های داخلی، استخدام نیروهای قابل اعتماد و متخصص و تدوین قوانین شفاف و سختگیرانه برای حوزهٔ سایبر است. به‌منظور افزایش امنیت سایبری بخش انرژی در سطح بین‌المللی نیز اقداماتی مانند تدوین معاهدهٔ بین‌المللی دربارهٔ ممنوعیت حملات سایبری به بخش انرژی، می‌تواند مهم‌ترین راهکار و راه‌حل باشد.

۱. ۳. سطح داخلی

تأمین امنیت سایبری بخش انرژی در سطح داخلی دارای ارزش و اهمیت فراوانی است؛ زیرا بدون تأمین امنیت سایبری داخلی نمی‌توان امنیت سایبری بین‌المللی را تأمین کرد. ازجمله ابعاد منفی و ویرانگر فضای سایبری، تهدیدها و آسیب‌هایی است که افراد و دولت‌ها علیه یکدیگر در این فضا به وجود می‌آورند، اما نکتهٔ جالب‌تر آن‌که بسته به شرایط سیاسی و بین‌المللی و فنی، برخی از دولت‌ها، دستاوردها، سیاست‌ها و اقدامات سایبری برخی از کشورها را دست‌مایهٔ ایجاد تهدیدهایی جدی علیه آن‌ها در فضای واقعی می‌کنند. یکی از کشورهایی که از این حیث در آستانهٔ تهدیدهایی راهبردی است، جمهوری اسلامی ایران،

به‌واسطهٔ تنش سایبری با عربستان سعودی است (داوند و سلطانی‌نژاد، ۱۳۹۷: ۷۲). چنین دولت‌هایی مانند ایران که در تیررس حملات سایبری گسترده‌ای از طرف بازیگران بین‌المللی متعددی هستند، لازم است برای ارتقای امنیت سایبری تمام بخش‌ها، به‌ویژه بخش بسیار مهم انرژی، اقدامات پیشگیرانه‌ای را انجام دهند. در حوزهٔ سایبری نیز مانند حوزهٔ بهداشت و درمان، پیشگیری بهتر از درمان است؛ زیرا هزینه‌هایی که دولت‌ها برای پیشگیری از حملات سایبری انجام می‌دهند، بسیار کمتر از هزینه‌هایی است که پس از انجام حملات سایبری لازم است؛ برای مثال، می‌توان با کمترین هزینه در ایمن‌سازی سامانه‌های داخلی، با نصب ابزارهای به‌روز و فناوری‌های نوین این حوزه در مقابل حملات سایبری مخرب، حوزهٔ انرژی و سایر حوزه‌های مرتبط با آن را ایمن ساخت؛ درحالی‌که پس از ارتکاب حملات سایبری علیه سامانه‌های بخش انرژی، آلودگی‌های گسترده و خسارات جبران‌ناپذیری به سامانه‌های رایانه‌ای این بخش وارد خواهد آمد که جبران چنین خساراتی بسیار سخت و پُرهزینه خواهد بود.

در سطح داخلی برای این‌که امنیت سایبری بخش انرژی افزایش یابد، نیاز است تا در سطح ملی همکاری‌های گسترده‌ای بین بخش انرژی و دولت شکل گیرد. نه دولت و نه بخش خصوصی، به‌تنهایی نمی‌توانند از کشور دفاع کنند. این مأموریتی مشترک است. دولت و صنعت باید به عنوان شریک برای این کار دست در دست هم بدهند (Obama, 2015). بنابراین نیاز است تا همهٔ بخش‌های مرتبط با بخش انرژی به صورت نزدیک و تنگاتنگ برای حفاظت بخش انرژی در قبال حملات سایبری همکاری و همراهی کنند. اما آنچه شایستهٔ اعتناست، اقدامات دولت‌هاست؛ زیرا دولت‌ها هم در سطح داخلی و هم در سطح بین‌المللی دارای اختیار و اقتدار هستند و نحوهٔ عملکرد و برنامه‌های آن‌ها هم در سطح داخلی و هم در سطح بین‌المللی می‌تواند بسیار مؤثر و کارا باشد. در این قسمت به اقداماتی می‌پردازیم که لازم است دولت‌ها برای مقابله با حملات سایبری در سطح داخلی انجام دهند.

۱. ۱. ۳. افزایش ایمنی سامانه‌های داخلی

در بحث افزایش ایمنی سامانه‌های داخلی بخش انرژی، آنچه باید مورد توجه قرار گیرد، ارتقای ایمنی این سامانه‌هاست. به‌منظور ارتقای ایمنی سامانه‌های داخلی این بخش، نخست باید بودجه‌ای برای به‌روزرسانی این سامانه‌ها توسط کشورها در سطح داخلی لحاظ گردد. با استفاده از این بودجه می‌توان اقدام به خرید سامانه‌های به‌روز و جدید نمود و کلاً تجهیزات و سامانه‌ها را نوسازی کرد. همچنین آنچه می‌تواند در حال حاضر به ایمن‌سازی بخش انرژی کمک کند، جداسازی این بخش از سایر قسمت‌های فضای مجازی در داخل کشورهاست. با توجه به خطر حملات سایبری، دولت‌هایی مانند دولت ایران باید بخش سایبری حوزهٔ انرژی

را از دیگر بخش‌ها کاملاً جدا کنند؛ زیرا با وضعیت آشفتهٔ فضای سایبری کنونی و سوءاستفادهٔ دولت‌ها از این وضعیت، بخش انرژی با خطر حملات سایبری از طرف بازیگران متعددی روبه‌رو شده است. استفاده از فناوری‌های فضای سایبر با توجه به رویکردهای جدید در دنیای کنونی امری گریزناپذیر است. با نگرش به این‌که قواعد و ابزار فضای سایبر در اختیار دیگران است، بازیگر یا کشوری که می‌خواهد وارد این عرصه شود باید تلاش کند از همهٔ ظرفیت‌ها، نقاط مثبت و فرصت‌های آن استفاده و با تهدیدات موجود در این فضا مبارزه کند و بیشترین بهره‌برداری لازم را از آن داشته باشد و این مهم بدون داشتن ساختار مناسب برای مقابله با تهدیدات این حوزه امکان‌پذیر نیست (حسینی و ظریف‌منش، ۱۳۹۲: ۴۲). افزون بر این، آنچه در بحث افزایش ایمنی سامانه‌های داخلی می‌توان گفت این است که چنین سامانه‌هایی باید از آخرین و به‌روزترین ابزارها استفاده کنند. همچنین نصب آخرین و به‌روزترین آنتی‌ویروس‌ها می‌تواند در کنترل حملات سایبری مخرب تااندازه‌ای تأثیرگذار باشد.

۲. ۱. ۳. استخدام نیروهای قابل اعتماد و متخصص

امروزه اقدامات و حملات تروریستی فراوانی در فضای سایبر متوجه دولت‌هاست که از ویژگی‌های این حملات می‌توان به ناشناخته بودن و سرعت حملات یادشده اشاره کرد و معمولاً این‌گونه حملات پس از وقوع شناسایی می‌شوند. بنابراین با ایجاد یک راهبرد ملی در استقرار حداکثر امنیت در فضای سایبر می‌توان به کاهش آسیب‌پذیری کشور در مقابل حملات پرداخته، از بروز خسارت به زیرساخت‌های اطلاعاتی پایه و حیاتی و نیز دارایی‌های ملی جلوگیری کرد (حسینی و ظریف‌منش، ۱۳۹۲: ۴۲). در بحث تأمین امنیت سایبری بخش انرژی یکی از مهم‌ترین اقدامات می‌تواند استخدام نیروی انسانی قابل اعتماد و متخصص باشد. آموزش کارمندان نیز بسیار مهم است. بیشتر اوقات هکرها برای رخنه در امنیت شبکه روی خطاهای انسانی برنامه‌ریزی می‌کنند. فردی که در بخش امنیت صنعتی کار می‌کند طی مصاحبه‌ای اظهار داشت که ساده‌ترین راه برای ورود بدافزار به یک کارخانهٔ صنعتی، ریختن فلش درایوها در پارکینگ خودرو یک شرکت است. بی‌شک کارمند بی‌احتیاط آن را برداشته و اندکی بعد در سایت از آن استفاده می‌کند (Desarnaud, 2017: 37). چنین اقدامات ناخواسته و پیش پا افتادهٔ کارکنان شرکت‌ها، گاهی به‌سادگی می‌تواند اطلاعات ارزشمندی از شرکت‌ها را در اختیار هکرها قرار دهد. یکی دیگر از روش‌هایی که دولت‌های متخاصم در سطح جهان برای ضربه زدن به رقبای خود انجام می‌دهند، استفاده از اطلاعاتی است که کارکنان بخش انرژی در اختیار آن‌ها قرار می‌دهند. این کارکنان گاهی با وسوسه‌های مالی در دام سرویس‌های جاسوسی قرار می‌گیرند و اطلاعات مهم محل کارشان را در اختیار آن‌ها قرار می‌دهند. در پاره‌ای موارد نیز

نداشتن تخصص کافی این نیروها باعث می‌گردد ناخواسته اطلاعاتی در اختیار هکرها و حمله‌کنندگان سایبری قرار گیرد. در بحث استخدام کارکنان آنچه شایستهٔ اعتناست، این است که باید قبل از استخدام، گذشتهٔ افراد بررسی گردد و همچنین از نظر شخصیتی افرادی باثبات شخصیت و وفادار به کشور استخدام گردند. پس از استخدام نیز چنین افرادی باید از نظر درآمد و دستمزد تا جایی تأمین باشند که هیچ پیشنهاد مالی نتواند آن‌ها را به همکاری و معاضدت با دولت‌های بیگانه وادارد.

۳. ۱. ۳. تدوین قوانین شفاف و سختگیرانه برای حوزهٔ سایبر

اقدام مهم دیگری که لازم است دولت‌ها برای تقویت امنیت سایبری خود انجام دهند، تدوین قوانین شفاف و سختگیرانه در حوزهٔ داخلی است. تدوین چنین قوانینی می‌تواند مانع اقدامات مجرمانه علیه بخش انرژی در داخل کشورها گردد. اگر افراد ساکن این کشورها متوجه باشند در صورت ارتکاب هرگونه جرمی که به امنیت سایبری این بخش خسارت وارد کند، تحت پیگرد قرار خواهند گرفت و طبق قوانین و مقررات با آن‌ها برخورد خواهد شد، به فکر انجام حملات سایبری علیه این بخش نخواهند افتاد. چنین تدابیری موجب خواهد شد امنیت سایبری بخش انرژی تقویت گردد و افراد کمتری در سطح داخلی، به انجام اقدامات خرابکارانه علیه این بخش روی آورند.

۲. ۳. سطح بین‌المللی

گسترش علم و دانش مدرن، فضایی را فراهم کرده تا جوامع نه‌تنها به ادعای مک لوهان[1] در دهکده‌ای جهانی و در مجاورت هم زندگی کنند، بلکه در بهره‌برداری از این فضای مشترک نیز با یکدیگر همکاری کنند. اینترنت در فضایی به گسترهٔ جهانی برای برقراری ارتباطات بین‌المللی گسترده شده است. توسعه و کاربرد اینترنت در روابط بین‌المللی رو به گسترش است و البته این امر تنها مختص به دولت‌های توسعه‌یافته‌ای نیست که به آخرین فناوری‌های روز دسترسی دارند، بلکه توسعهٔ دولت‌های کمتر توسعه‌یافته را نیز دربر می‌گیرد (شهبازی، ۱۳۹۶: ۲۳۴). استفاده از فناوری دیجیتال و مسابقهٔ 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 اگر با مقررات و ابزارهای قانونی و سایبری قوی حمایت نشود، هم‌زمان آسیب‌پذیری ناشی از جرایم سایبری و حملات سایبر را افزایش می‌دهد؛ زیرا راهکارهای سنتی سایبری مؤثر نخواهد بود.

1. McLuhan

افزون بر اقداماتی که دولت‌ها می‌توانند در سطح ملی برای تقویت امنیت سایبری بخش انرژی خود انجام دهند، در سطح جهانی نیز می‌توانند به اقداماتی متوسل گردند که چنین اقداماتی می‌تواند تأمین‌کنندهٔ امنیت سایبری بخش انرژی باشد. فضای سایبری همچون شبکه‌ای درهم‌تنیده تمام کشورهای جهان را به هم متصل کرده و چنین وابستگی‌ای باعث ایجاد تهدیدات مشترک برای جامعهٔ بین‌المللی گردیده است. ازاین‌رو امنیت تمام دولت‌ها، به‌ویژه بخش انرژی که مهم‌ترین و باارزش‌ترین بخش حیات مدرن بشر است، در گرو همکاری جامعهٔ بین‌المللی است. همکاری‌های جامعهٔ بین‌المللی تنها زمانی می‌تواند مؤثر باشد که در چهارچوب موافقت‌نامه‌ها و معاهده‌های بین‌المللی الزام‌آور نمود یابد. تجاربی که از حوزه‌های دیگر دانش بشری مانند حوزه‌های شیمیایی و هسته‌ای به‌دست آمده است، این بوده که تنها همکاری‌های بین‌المللی تا حدی توانسته جلوی خطرات این فناوری‌ها را بگیرد و تدوین معاهده‌های بین‌المللی توانسته به حل معضلات و مشکلات این حوزه‌ها کمک شایانی نماید. این تجربه می‌تواند برای حوزهٔ مورد بحث ما، یعنی تقویت امنیت سایبری بخش انرژی، هم مؤثر باشد و دولت‌ها با همکاری یکدیگر به تدوین یک معاهدهٔ بین‌المللی الزام‌آور دربارهٔ ممنوعیت حملات سایبری به بخش انرژی همت گمارند و به تقویت امنیت سایبری این بخش بپردازند. بی‌میلی دولت‌ها برای مشارکت در قانون‌گذاری بین‌المللی، این ذهنیت را ایجاد کرده است که حقوق بین‌الملل در رویارویی با چالش‌هایی که به‌وسیلهٔ پیشرفت‌های سریع فناوری ایجاد می‌گردد، ناتوان است. در پاسخ، چندین طرح هنجارسازی غیردولتی با هدف پُر کردن این خلأ، مانند هنجارهای سایبری مایکروسافت[1] و راهنمای تالین[2] ارائه گردیده است. هنجارهای سایبری مایکروسافت شامل هدف قرار ندادن شرکت‌های فناوری اطلاعات و ارتباطات با هدف آسیب‌پذیر نمودن آن‌ها یا اتخاذ اقداماتی با انگیزهٔ کاهش اعتماد عمومی به خدمات و محصولات آن‌ها توسط دولت‌ها، اتخاذ یک سیاست روشن اصول‌محور برای برخورد با آسیب‌پذیری‌های محصولات و خدمات، ایجاد محدودیت در بحث گسترش سلاح‌های سایبری، متعهد ماندن به فعالیت‌های عدم اشاعه دربارهٔ سلاح‌های سایبری، محدودیت مشارکت دولت‌ها در عملیات سایبری تهاجمی، کمک دولت‌ها به بخش خصوصی برای کشف حملات سایبری، واکنش به آن‌ها و جبران خسارات است (www.Microsoft.com). دربارهٔ راهنمای تالین هم باید گفت که این راهنما در سال ۲۰۱۳ توسط گروه ویژه‌ای از کارشناسان مستقل که توسط مرکز عالی دفاع سایبری[3] در سازمان ناتو گرد آمده بودند تا دستورالعملی دربارهٔ قانون حاکم بر جنگ سایبری تنظیم کنند، تهیه گردید. هدف این

1. Microsoft
2. Tallin Manual
3. Cyber Defense Center of Excellence

دستورالعمل تسری هنجارهای حقوقی و قانونی به این‌گونه جنگ‌های نوین است و به‌طور کلی دربرگیرندهٔ حقوق بر جنگ حقوق بین‌الملل حاکم بر توسل به زور از سوی کشورها به عنوان ابزار سیاست ملی و حقوق در جنگ حقوق بین‌الملل تنظیم‌کنندهٔ رفتار درگیری‌های مسلحانه است. عناصر مرتبط حقوق بین‌الملل مانند مسئولیت دولت‌ها و حقوق دریاها نیز در این دستورالعمل گنجانده شده است (صلاحی و کشفی، ۱۳۹۵: ۳۶). به‌طور خلاصه این دستورالعمل، برخلاف آنچه در کاربرد رایج از آن استنباط می‌شود، دربارهٔ امنیت سایبری نگارش نشده است (صلاحی و کشفی، ۱۳۹۵: ۳۷). ظهور این هنجارهای غیرالزام‌آور برای دولت‌ها فرصتی ایجاد می‌کند تا دیگربار ادعایی را دربارهٔ ایجاد یک موقعیت قانون‌گذاری مشابه سوابق تاریخی، ازجمله شکل‌گیری نظام‌های حقوقی برای قطب جنوب و ایمنی هسته‌ای مطرح کنند. اگر دولت‌ها می‌خواهند اطمینان داشته باشند که خلأ قدرت کنونی به روشی به‌کار گرفته نمی‌شود که توانایی آن‌ها را برای رسیدن به اهداف راهبردی و سیاسی‌شان بکاهد، باید نقش محوری داشته باشند (Macak, 2017: 817).

بنابراین در بحث امنیت سایبری نیز نیاز است تا دولت‌ها پیشگام شوند و با همکاری‌های بین‌المللی و تدوین معاهده‌ای در بحث امنیت سایبری بخش انرژی، به وضعیت کنونی جهان پایان دهند؛ زیرا امنیت سایبری این حوزه صلح و امنیت بین‌المللی را به دنبال خواهد داشت.

۱. ۲. ۳. تدوین معاهدهٔ بین‌المللی الزام‌آور دربارهٔ ممنوعیت حملات سایبری به بخش انرژی

امروزه با توجه به اهمیت موضوع‌های مرتبط با فضای سایبری، ازجمله جرایم ارتکابی، خلأها و چالش‌های ناشی از نبود یا نقص یا کمبود قوانین و مقررات، دولت‌ها و سازمان‌های بین‌المللی به فعالیت‌های گسترده و جدی به‌منظور پاسخگویی به نیازها اقدام کرده تا این حوزهٔ نوظهور را درک و قاعده‌مند سازند. توسعه و تکامل فضای سایبری سبب ایجاد اشکال مختلفی از جرایم سایبری شده است. ازاین‌رو در دهه‌های اخیر کشورها برای مبارزه با جرایم سایبری در جهت تدوین معاهدات بین‌المللی گام برداشته‌اند (کتانچی و پورقهرمانی، ۱۳۹۸: ۳۱). هم‌زمان که اینترنت در قالبی گسترده و همه‌گیر در حال ورود به تمامی جنبه‌های زندگی بشر است، رفته‌رفته هنجارها و قواعد مرتبط با آن نیز شکل می‌گیرند. بااین‌حال، پیش از هر چیز باید دانست که مرکز ثقل توجه، تجلی عملی اصول و قواعد اینترنت نیست، بلکه مهم تمرکز بر یک نظام فراملی مشتمل بر اصول و قواعدی است که به‌منظور ضابطه‌مند کردن استفاده از اینترنت توسط افراد و میان آن‌ها به‌کار می‌آید (Wu, 1997: 663).

اینترنت مانند هر امر اجتماعی دیگر، نیازمند نظام‌دهی است و بخشی از این نظام‌دهی در قالب تدوین قوانین و مقررات انجام می‌شود. تدوین مقررات برای اینترنت زمانی می‌تواند تأمین‌کنندهٔ آزادی‌های مشروع بوده و به مردم اطمینان دهد که دسترسی و استفادهٔ آن‌ها از خدمات اینترنتی، امن، ارزان و پایدار است که ضمن درک صحیح از ویژگی‌های اینترنت و شرایط جامعه، براساس اصول حقوقی تدوین شده باشد (رضایی و بابازاده مقدم، ۱۳۹۳: ۸۰). بنابراین آنچه در حال حاضر عیان و مشخص است، نبود قوانین و هنجارهای دقیق و مشخص برای رویارویی با حملات سایبری به بخش انرژی در سطح جهانی است. برای چیره شدن بر این مشکل و قاعده‌مند کردن فضای سایبری بخش انرژی، تدوین معاهدهٔ بین‌المللی الزام‌آور دربارهٔ ممنوعیت حملات سایبری به زیرساخت‌های این بخش می‌تواند راهکار خوب و مناسبی برای حل مشکلات این حوزه باشد. چنین معاهده‌ای از یک‌سو، دولت‌ها را ملزم به همکاری در تقویت امنیت سایبری در سطح جهانی خواهد نمود و از سوی دیگر، مانع فعالیت‌های مخرب دولت‌ها علیه این بخش مهم و پراهمیت، یعنی بخش انرژی، خواهد شد.

امروزه درخواست‌ها برای هنجارهای سایبری به‌منظور امن کردن و ادارهٔ فضای سایبری، امری همه‌گیر شده است. حقوق بین‌الملل کامل‌ترین نظام حقوقی نیست و بی‌شک حتی در فضای سایبری ناقص‌ترین نظام حقوقی است (Xiao, 2020: 349). هنجارهای مربوط به فضای سایبری در سطح بین‌المللی در میان دولت‌ها بسیار مورد مناقشه و در سطح داخلی بین دولت‌ها چندپاره است. با وجود فعالیت‌های دیپلماتیک در طول دو دههٔ گذشته، توافق ذهنی بین هنجارهای حاکم بر قدرت سایبری اجباری هنوز در مرحلهٔ ابتدایی قرار دارد (Maurer, 2020: 283).

نتیجه

نقش مهمی که فناوری‌های حوزهٔ اطلاعات و ارتباطات در تمدن کنونی بشری دارند باعث گردیده که روزبه‌روز استفاده از این فناوری‌ها در سطح جهان افزایش یابد. تمام امور بشر وابسته به فناوری‌های این حوزه گردیده است؛ به‌گونه‌ای که به جرأت می‌توان گفت هیچ حوزه‌ای از حیات و تمدن بشری را نمی‌توان یافت که نیازمند اینترنت و فضای سایبری نباشد. از امور شخصی مانند دوست‌یابی و همسریابی گرفته تا پیچیدگی‌های اتصالات اینترنتی شرکت‌های نفت و گاز، همه‌وهمه به این فضا وابسته گردیده است. این وابستگی شدید تمدن بشری، به‌ویژه صنایع و تأسیسات پُراهمیت بخش انرژی، به فضای سایبری باعث گردیده خطراتی نیز برای آن‌ها وجود داشته باشد. خطراتی مانند حملات سایبری که به‌تازگی همه‌روزه خبرهایی در سطح جهانی دربارهٔ این پدیدهٔ نوظهور شنیده می‌شود. رقابت و دشمنی دولت‌ها

در سطح جهانی و منطقه‌ای باعث گردیده از این حوزه، یعنی فضای سایبری، بهره برده و خسارت‌های سنگینی را به رقبای خود وارد کنند؛ به‌ویژه کشور جمهوری اسلامی ایران که سیاست‌های جهانی و منطقه‌ای آن براساس مقابله با زورگویان و قدرت‌های جهانی و حمایت از مظلومان و مستضعفان دنیا مانند ملت مظلوم فلسطین، عراق، سوریه و یمن شکل گرفته است، همواره در معرض خطر حملات سایبری قرار دارد. نه‌تنها ایران، بلکه دولت‌هایی مانند عربستان سعودی که به عنوان یکی از کشورهای مهم در حوزهٔ انرژی است، همواره با خطر حملات سایبری روبه‌روست. این خطرات به دلیل افزایش وابستگی بخش انرژی به فناوری‌های حوزهٔ سایبری و افزایش تعداد بازیگران حملات سایبری در سطح جهانی ایجاد گردیده و دولت‌ها از ارتکاب چنین حملاتی، اهداف سیاسی و اقتصادی خود را دنبال می‌کنند. برای رویارویی با چنین وضعیتی، نیاز است دولت‌ها برای تقویت امنیت سایبری بخش انرژی خود اقداماتی در سطح داخلی و بین‌المللی انجام دهند. آنچه دولت‌ها می‌توانند در سطح داخلی انجام دهند اقداماتی مانند افزایش ایمنی سامانه‌های داخلی، استخدام نیروهای قابل اعتماد و متخصص و تدوین قوانین شفاف و سختگیرانه برای حوزهٔ سایبر است. در سطح بین‌المللی نیز باید اقداماتی توسط دولت‌ها انجام گیرد تا از ظرفیت بین‌المللی کشورها نیز بتوان برای رویارویی با حملات سایبری استفاده کرد که مهم‌ترین اقدام در سطح بین‌المللی می‌تواند تهیهٔ معاهده‌ای برای ممنوعیت حملات سایبری به بخش انرژی باشد. اگر دولت‌ها بتوانند چنین اقداماتی را در سطح داخلی و بین‌المللی انجام دهند، تااندازهٔ زیادی می‌توانند امنیت سایبری بخش انرژی کشورهای خود را ارتقا دهند؛ وگرنه با وضعیتی که هم‌اکنون بر جهان حاکم است و روزبه‌روز شاهد افزایش حملات سایبری در سطح جهانی هستیم، تنها آینده‌ای که می‌توانیم پیش روی دنیا ببینیم، جهانی پُر از ناامنی، هرج‌ومرج و بی‌نظمی خواهد بود که بالطبع چنین وضعیتی حیات و تمدن بشری را با خطرات جدی روبه‌رو خواهد کرد.

بیانیه نبود تعارض منافع

نویسندگان اعلام می‌کنند که تعارض منافع وجود ندارد و تمام مسائل اخلاق در پژوهش را شامل پرهیز از دزدی ادبی، انتشار و یا ارسال بیش از یک بار مقاله، تکرار پژوهش دیگران، داده‌سازی یا جعل داده‌ها، منبع‌سازی و جعل منابع، رضایت ناآگاهانه سوژه یا پژوهش‌شونده، سوءرفتار و غیره، به‌طور کامل رعایت کرده‌اند.

منابع

الف) فارسی

۱. افشار، احمد؛ عاطفه ترمه‌چی؛ عارفه گلشن؛ آزاده آقائیان؛ حمیدرضا شهریاری (۱۳۹۳). «مروری بر امنیت سایبری سیستم‌های کنترل صنعتی». *مجلهٔ کنترل*، جلد هشتم، شمارهٔ اول، ص۴۵-۳۱.
DOI: 20.1001.1.20088345.1393.8.1.4.0

۲. جعفری، افشین (۱۳۹۸). «حاکمیت بر فضای سایبر از منظر حقوق بین‌الملل و نظام حقوقی جمهوری اسلامی ایران». *فصلنامهٔ رهیافت انقلاب اسلامی*، شمارهٔ ۴۹، ص۱۳۲-۱۰۹. در:
http://www.rahyaftjournal.ir/article_105596.html (۱۲ مهر ۱۳۹۹)

۳. حسینی، پرویز؛ حسین ظریف‌منش (۱۳۹۲). «مطالعهٔ تطبیقی ساختار دفاع سایبری کشورها». *فصلنامهٔ پژوهش‌های حفاظتی ـ امنیتی دانشگاه جامع امام حسین (ع)*، شمارهٔ ۵، ص۶۸-۴۱. در: https://jpas.ihu.ac.ir/article_200978.html (۲۰ آبان ۱۳۹۹)

۴. خلف‌رضایی، حسین (۱۳۹۲). «حملات سایبری از منظر حقوق بین‌الملل؛ مطالعهٔ موردی: استاکس‌نت». *فصلنامهٔ مجلس و راهبرد*، سال بیستم، شمارهٔ ۷۳، ص۱۵۳-۱۲۵. در: https://nashr.majles.ir/article_80.html (۱۲ آذر ۱۳۹۹)

۵. داوند، محمد؛ احمد سلطانی‌نژاد (۱۳۹۷). «امنیتی‌سازی تنش سایبری جمهوری اسلامی ایران و عربستان سعودی: تهدیدها و الزامات راهبردی». *فصلنامهٔ راهبرد*، سال بیست‌وهفتم، شمارهٔ ۸۶، ص۹۸-۷۱.
DOI: 20.1001.1.10283102.1397.27.1.4.8

۶. رضایی، مهدی؛ حامد بابازاده مقدم (۱۳۹۳). «اصول تدوین قوانین و مقررات برای اینترنت با تأکید بر مصوبات یونسکو و شورای اروپا». *فصلنامهٔ پژوهش حقوق عمومی*، سال پانزدهم، شمارهٔ ۴۲، ص۸۲-۴۳. در:
https://qjpl.atu.ac.ir/article_254.html (۱۲ دی ۱۳۹۹)

۷. شهبازی، آرامش (۱۳۹۶). «در تکاپوی توسعهٔ حقوق بین‌الملل اینترنت». *فصلنامهٔ پژوهش حقوق عمومی*، شمارهٔ ۵۴، ص۲۴۵-۲۱۹. DOI: 10.22054/ Q JPL.2017.7432

۸. صلاحی، سهراب؛ سید مهدی کشفی (۱۳۹۵). «جنگ سایبری از منظر حقوق بین‌الملل با نگاه به دستورالعمل تالین». *فصلنامهٔ مطالعات قدرت نرم*، شمارهٔ ۱۴، ص۴۷-۲۸. در: http://www.spba.ir/article_40920.html(۲۰ فروردین ۱۴۰۰)

۹. کتانچی، الناز؛ بابک پورقهرمانی (۱۳۹۸). «سیاست‌های نمادین معاهدهٔ جرایم سایبری شورای اروپا». *فصلنامهٔ مطالعات بین‌المللی*، شمارهٔ ۲، ص۴۷-۳۱, DOI: 10.22034/ISJ.2019.99238

ب) خارجی

-Articles

10. Bailey, Christopher E (2020). "Offensive Cyberspace Operations :A Gray Area in Congressional Oversight". *Boston University International Law Journal*,Vol 38,Issue 2, p240-285. https://www.bu.edu/ilj/archives/38-2/- (Accessed 20 February 2021).

11. Desarnaud, Gabrielle (2017). "Cyber Attacks and Energy Infrastructures: Anticipating Risks". *Études de l'Ifri*, Ifri, p1-60. https ://www .ifri. org /en/publications/etudes –de –lifri / cyber –attacks -and-energy –infrastructures –anticipating –risks (Accessed 12 September 2020).

12. Macak, Kubo (2017). "From cyber Norms to Cyber Rules:Re engaging States as Law - Makers". Leiden *Journal of International Law*, Volume 30, Issue 4, p877-899 DOI: 10.1017/S0922156517000358.

13. Maurer, Tim (2020). "A Dose of Realism: The Contestation and Politics of Cyber Norms". *Hague Journal on the Rule of Law*, Volume 12, Issue 2, p283-305. https://link.springer.com/article/10.1007/s40803-019-00129-8- (Accessed 10 July 2021).

14. Mikko, Rajavuori; Huhta, Kaisa (2020). "Digitalization of Security in the Energy Sector: Evolution of Eu Law and Policy". *Journal of World Energy Law and and Business*,Vol 13, Issu 4, p353-367 DOI: 10.1093/jwelb/jwaa030.

15. Trautman, Lawrence J; Ormerod, Peter (2018). "Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things". *University of Miami Law Review*,Vol 72, 761, p761-826. https://repository.law.miami.edu/umlr/vol72/iss3/5/- (Accessed 10 August 2020).

16. Tsakanyan, V.T (2017). "The role of Cybersecurity in world politics". *Vestnik RUDN. International Relations*, Vol 17, No 2, p339-348 DOI: 10.22363/2313-0660-2017-17-2-339-348.

17. Vasileiou, Konstantina G (2019). "Cyber Security in the Energy Sector". a Holistic Approach, *University of Piraeus, Department of International &European Studies*.

https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/12412/Vasileiou_18012.pdf?sequence=2&isAllowed=y – (Accessed 25 July 2020).
18. Venkatachary, Sampath Kumar; Prasad Jagdish; Samikannu Ravi (2017). "Economic Impacts of Cyber Security in Energy Sector: A Review". *International Journal of Energy Economics and Policy*, Vol 7, Issue 5, p250-262. https://econjournals.com/index.php/ijeep/article/view/5283- (Accessed 5 october 2020).
19. Wu, Timothy S (1997). "Cyberspace Sovereignty?- The Internet and the International System". *Harvard Journal of Law & Technology*, Vol.10, no 3, p648-666. https://jolt.law.harvard.edu/volumes/volume-10-1- (Accessed 10 July 2020).
20. Xiao, Alex (2020). "Responding to Election Meddling in the Cyberspace: An International Law Case Study on the Russian Interference in the 2016 Presidential Election". *Duke Journal of Comparative & International Law*, Vol 30, Number 2, p349-378. https://scholarship.law.duke.edu/djcil/vol30/iss2/6/- (Accessed 8 September 2020).

- Documents

21. Cyber Security Predictions (2020). https://www.fireeye. com/ current –threats / annual – threat -report. html
22. MCAffee Labs Threats Report, November (2020). https://www.mcafee.com /enterprise /en –us /assets /reports /rp- quarterly -threats-nov-2020.pdf23. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security
24. President Barack Obama, Remarks by the President at the National Cybersecurity Communications Integration Center ,delivered 13 January (2015). Arlington, Virginia. https://www.americanrhetoric.com/speeches/barackobama/barackobamanccic.htm
25. International Cybersecurity Norms: Part 2. https://www.Microsoft.com

Energy Law Studies, 2022,
8(1): 173-193, DOI: 10.22059/JRELS.2022.316656.413

The Necessity of Strengthening Cyber Security of Energy Sector by State

Parviz Farshasaid
PhD Student in Public International Law ,Department of International law, Isfahan (Khorasgan (Branch ,Islamic Azad University , Isfahan ,Iran
Mahmoud Jalali*
Associate Professor, Department of Law, University of Isfahan, Isfahan ,Iran
Mahnaz Goodarzi
Associate professor, Department of International relations, Isfahan (Khorasgan) Branch ,Islamic Azad University , Isfahan ,Iran

Abstract
The important role of computer and the Internet and the services that these technologies provide to humanity have made the energy sector dependent on these new technologies. This dependence has led to risks for the energy sector, the most important of which is directing cyber-attacks . In the present study, a question has been raised, *i.e.*, what is the need for states to strengthen the cyber security of their energy sector and what measures should be taken domestically and internationally? Using the descriptive-analytical method, the question has been answered that due to the increasing dependence of the energy sector on cyber technologies and the increasing number of actors and perpetrators of cyber attacks in the world, States need to strengthen their cyber security in their energy sector. What states can do at the domestic level includes increasing the security of domestic systems, recruiting reliable and specialized personnel, and developing clear and strict rules for cyberspace. At the international level, drafting a binding international treaty banning cyber-attacks on the energy sector is the most important measure that they can adopt.

Keywords: Cyber Security, Energy Sector, Cyber Attacks, New Technologies.

* Corresponding Author Email: m.jalali@ase.ui.ac.ir
Received: 6 February 2021, Accepted: 20 June 2022

Declaration of conflicting interests
The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The authors received no financial support for the research, authorship, and/or publication of this article.