تأثیر عملکرد بازیگران دولتی بر تغییرات استراتژی سایبری آمریکا (۲۰۲۰-۲۰۰۰)

سیده زهره مخملباف [۱]، شیرزاد آزاد [۲]

چکیده

از زمان ظهور فناوری سایبری تا به امروز، این عرصه دارای پیشرفت‌های زیادی بوده و حوزه‌های مختلفی را تحت تأثیر قرار داده است، بطوریکه نبود آن در روند زندگی بشر مشکل‌ساز بوده و از طرفی هم می‌تواند بعنوان ابزاری تهدیدآمیز عمل کند. امروزه گسترش فناوری سایبری مسبب نگرانی‌های جدیدی درخصوص امنیت ملی کشورها شده است. بازیگران متعددی از این فناوری برای اهداف گوناگون بویژه حملات سایبری استفاده می‌کنند. در مقاله حاضر تلاش می‌شود تا ضمن معرفی بازیگران دولتی مهم عرصه سایبری، به تأثیر آنها بر روند تغییر استراتژی‌های ایالات متحده آمریکا و واکنش این کشور برای حفظ امنیت خود در قبال اینگونه تهدیدات و تحولات پرداخته شود. هدف این مقاله، بررسی اقدامات کشورهای چین، روسیه، ایران و کره شمالی بعنوان رقبای آمریکا و کشورهای فعال در فضای سایبری بوده است تا بتوان به روند تغییرات در استراتژی ایالات متحده آمریکا و نحوه واکنش آن بعنوان پیشرفته‌ترین بازیگر سایبری پی‌برد. لذا به دنبال پاسخ به این پرسش هستیم که این بازیگران دولتی فعال در فضای سایبری، چه تأثیری بر روند تغییر استراتژی این کشور در برابر تهدیدات فضای سایبری داشته‌اند. از این‌رو، یافته‌ها حاکی از آن است که افزایش اثرگذاری فناوری‌های سایبری بر امنیت ملی، ظهور بازیگران دولتی و رشد تحرکات سایبری آنها بر کنار گذاشتن رویکرد تدافعی و اتخاذ رویکردی تهاجمی در برابر تهدیدات سایبر تأثیرگذار بوده‌اند. مقاله پیش‌رو، براساس چارچوب امنیت ملی و به روش تبیینی و با استفاده از منابع کتابخانه‌ای نگارش شده است.

واژگان کلیدی: امنیت، فضای سایبری، تهدید، آمریکا، استراتژی

---

[۱] کارشناسی‌ارشد روابط بین‌الملل دانشگاه فردوسی مشهد z.nastaran57@gmail.com

[۲] دانشیار، دکتری علوم سیاسی، دانشگاه فردوسی مشهد

مقدمه

از سال ۱۹۲۶ که واژه سایبر برای اولین بار بکار گرفته شد و شکل ساده و ابتدایی آن در آلمان نازی استفاده می‌شد تا به امروز شاهد پیچیدگی‌های فراوان در این حوزه هستیم زیرا که با بخش‌های مختلف صنعتی، نظامی، امنیتی و ...کشورها در ارتباط است. اهمیت این موضوع زمانی بیشتر مشخص گردید که با پیشرفت فناوری در فضای سایبر، این امر وسیله‌ای مهم برای کشورهای قدرتمند به حساب می‌آید، چراکه از این طریق می‌توانند در عرصه بین‌المللی بسیار تأثیرگذار بوده و یا از جانب سایر قدرت‌ها تحت تأثیر قرار گیرند، تا جائیکه برخی کارشناسان شکل جنگ‌های آینده میان کشورها را در حوزه جنگ‌های سایبری می‌دانند. کشورهایی که توانایی بالاتری در فضای سایبر دارند، گاه رویکردی دفاعی را پیش می‌گیرند و به دنبال حفظ زیرساخت‌ها و شبکه‌های حیاتی خود هستند و یا در رویکردی تهاجمی، زیرساخت‌ها و مراکز مهم دشمنان خود را هدف قرار می‌دهند.

در این بین ایالات متحده آمریکا دارای جایگاهی ویژه‌ای می‌باشد. باتوجه به استقرار مرکز اصلی اینترنت جهان در این کشور، در واقع زمین بازی در تقابل کشورها در فضای سایبر از آن آمریکا است. استراتژی سایبری آمریکا دستخوش تغییر و تکامل زیادی بوده است؛ یعنی از آغاز تدوین استراتژی اینترنت در زمان لیندون جانسون در ۱۹۶۴، تا دوران ریاست جمهوری بیل کلینتون (۲۰۰۱-۱۹۹۷) که فضای سایبر در معنای واقعی خود ظهور می‌کند. بیل کلینتون در فرمان ریاست جمهوری ۶۸ دستور حفظ کشور را در برابر حملات سایبری داد. دولت بوش این کار را با استراتژی ملی برای امنیت فضای سایبر گسترش داد. در دوران اوباما و ترامپ نیز به اشکال مختلف، شاهد تغییراتی در رویکرد این کشور هستیم. بطورکلی این کشور در عرصه سایبری دشمنان و رقبای مختلفی دارد که به اشکال مختلف به دنبال دفع تهدید آنها می‌باشد که در ادامه این اثر به آنها اشاره می‌کنیم.

این تحقیق براساس اهمیت روزافزون فناوری‌های سایبری در همه ابعاد زندگی بویژه بحث امنیت ملی کشورها نگاشته شده است. دلیل انتخاب این موضوع جدال محتمل سایبری میان کشورهای پیشرو در این عرصه و شناخت اقدامات و تقابلات آنها می‌باشد. در این پژوهش تلاش می‌شود تا ضمن معرفی بازیگران دولتی مهم عرصه سایبر، به تأثیر آنها بر روند تغییر استراتژی‌های ایالات متحده آمریکا و واکنش این کشور برای حفظ امنیت خود در قبال اینگونه تهدیدات و تحولات پرداخته شود. لذا به دنبال پاسخ به این پرسش هستیم که بازیگران دولتی فعال در فضای سایبر، چه تأثیری بر روند تغییر استراتژی این کشور در برابر تهدیدات فضای سایبر داشته‌اند. از این‌رو، نشان می‌دهیم که افزایش اثرگذاری فناوری‌های سایبری بر امنیت ملی، ظهور بازیگران دولتی و رشد تحرکات سایبری آنها بر تحول استراتژی آمریکا و اتخاذ رویکردی تهاجمی در برابر

تهدیدات سایبر تأثیرگذار بوده‌اند. روش تبیینی برای انجام این پژوهش در نظر گرفته شده است، زیرا به بررسی یک رابطه علت و معلولی میان ظهور بازیگران دولتی و تحرکات آنها با تغییرات استراتژی سایبری آمریکا می‌پردازیم. این پژوهش از طریق گردآوری اطلاعات اسناد بالادستی آمریکا، منابع کتابخانه‌ای و مقالات اینترنتی انجام گرفته است.

۱- پیشینه پژوهش

درخصوص رابطه بین امنیت و فضای سایبر، تاکنون پژوهش‌های انجام گرفته است و عمده تحقیقات پیرامون این موضوع، بر مباحث مرتبط با فضای فناوری سایبر تمرکز دارند. در این بین به آثاری که به موضوع ما نزدیک است اشاره می‌شود.

- در مقاله فضای سایبر و سیاست خارجی آمریکا، Maker, Simran R (۲۰۱۷) در کمیته ملی سیاست خارجی آمریکا به بررسی کشورهای مختلف و تهدیدات آنها توجه کرده است. وی این عرصه را از زاویه تدافعی می‌نگرد و نقش آن را در سیاست خارجی آمریکا نشان می‌دهد.

- مقاله‌ای با عنوان اعلام توانمندی‌های حمله سایبری از Libicki (۲۰۱۳) در مرکز مطالعات استراتژیک رند[1]در همکاری با وزارت دفاع آمریکا، به قدرت سایبری نظامی آمریکا در اسناد این کشور برای بازدارندگی در برابر سایر رقبای خود می‌پردازد. وی اشاره می‌کند که بازدارندگی سایبری می‌تواند ابزاری مناسب برای دفع خطرات سایبری ناشی از سوءاستفاده دیگران باشد.

- در کتاب تهدید سایبری ایران، Anderson و Sadjadpour (۲۰۱۸)، به توانایی‌ها و خطرات این کشور نسبت به آمریکا اشاره دارند. این اثر که توسط اندیشکده کارنگی منتشر شده است، به سه مقوله جاسوسی، خرابکاری و انتقام ایران توجه دارد.

- در اثری دیگر Connell و Volger (۲۰۱۷)، در مقاله رویکرد روسیه به جنگ سایبری، به قدرت این کشور در رابطه با آمریکا پرداخته‌اند. ضمن اینکه نهادها، سازمان‌ها و توانایی‌های سایبری این کشور را مطرح می‌کنند.

- Sabotka (۲۰۱۵)، روند تحول قدرت سایبری کشورهای مهم این عرصه را در پژوهشی با نام ارزیابی تاریخی و ظهور تهدیدات سایبری دولت-ملت‌ها، بررسی می‌کند. در این اثر، روند تحول و قدرت سایبری چهار کشور چین، روسیه، ایران و کره شمالی، همچنین حملات سایبری آنها را تا سال ۲۰۱۵، نشان می‌دهد.

[1] Rand Institute

- Medvedef (۲۰۱۵)، رابطه روسیه و آمریکا در عرصه سایبری را در پژوهشی با نام تحلیل نظری تهاجمی-دفاعی توانایی سایبری روسیه مورد بررسی قرار داده است. وی در این پژوهش به تدافعی و تهاجمی بودن دکترین‌های سایبری روسیه اشاره می‌کند و این دکترین‌ها را با رویکردی تهاجمی، هماهنگ‌تر می‌بیند. لذا این مسئله برای آمریکا یک تهدید محسوب می‌شود.

- Scalise (۲۰۱۵)، در مقاله جاسوسی سایبری، به نقش ارتش چین و هدف قرار دادن آمریکا اشاره دارد. این مقاله واحدهای سایبری چین را معرفی کرده و توصیه‌هایی را برای تقویت زیرساخت‌های آمریکا ارائه می‌کند.

- در مقاله‌ای را با عنوان جنگ جهانی سی، Geers et al (۲۰۱۴)، در موسسه فایر آی[1] قدرت سایبری کشورهای مختلف سراسر جهان را مورد مطالعه قرار دادند. البته این اثر توضیح چندانی در مورد خطرات این کشورها برای آمریکا ندارد.

- Spade (۲۰۱۲)، در پژوهشی مقایسه‌ای و کاربردی با نام قدرت سایبری چین بر امنیت ملی آمریکا، خطرات این کشور را برای امنیت آمریکا برمی‌شمرد. وی این موضوع را مورد توجه قرار داده است که قدرت چین تا چه حد امنیت ملی آمریکا را تهدید می‌کند و راهکارهایی را برای تقویت سیاست سایبری آمریکا پیشنهاد می‌دهد. چین حملات سایبری مختلفی را به کشورهایی مثل ژاپن و آمریکا داشته است، لذا آمریکا از این گسترش چین در فضای سایبر احساس خطر می‌کند.

- Lieberthal and Singer (۲۰۱۲)، در موسسه‌ی بروکینگز[2] پژوهشی را با نام امنیت سایبر و روابط چین و آمریکا انجام داده و به استراتژی بازدارندگی و دفاعی آمریکا اشاره دارند. همچنین آنها به ویژگی‌های روابط دو کشور، مسئله نسبت دادن، مواجه تهاجمی و مباحثات بین دو کشور می‌پردازند.

- Hjortdal (۲۰۱۱)، نیز در مقاله استفاده چین از جنگ سایبری، به تهدیدات چین برای غرب بویژه آمریکا پرداخته است. نویسنده سعی دارد ضمن نشان دادن اغراق آمریکا در مورد خطر سایبری چین، به ویژگی‌ها و اهداف سایبری این کشور، مخصوصا جاسوسی‌های سایبری آن اشاره کند.

بطورکلی برخلاف آثار مذکور، آنچه که در این پژوهش مورد توجه قرار گرفته است، نقش بازیگران دولتی بر تحول استراتژی‌های سایبری آمریکا، تغییرات در سیاستگذاری‌ها و واکنش نهادهای مربوطه با این تهدیدات می‌باشد. در واقع نشان دادیم که عملکرد بازیگران مختلف نسبت به آمریکا مسبب اتخاذ رویکردی تهاجمی از جانب این کشور شده و نهادهای مرتبط را به تغییر رویه واداشته است. در این نگارش، براساس استراتژی

[1] Fire Eye
[2] Brookings Institute

سایبری آمریکا به چهار کشور روسیه، چین، ایران و کره شمالی اشاره می‌شود. هدف ما بررسی اقدامات کشورهای رقیب آمریکا و نحوه واکنش آمریکا به این اقدامات می‌باشد، چراکه با شناخت این رویه‌ها بهتر می‌توان رویدادهای این عرصه را تحلیل نمود.

۲- چارچوب نظری

چارچوب نظری بکار رفته در این پژوهش، نظریه امنیت ملی می‌باشد. امنیت ملی به الزاماتی اشاره می‌کند که بقای کشور و دولت ملی را از طریق بکارگیری قدرت اقتصادی، ارتش و توان سیاسی و استفاده از ابزار دیپلماسی حفظ می‌کند. مفهوم امنیت ملی در گذر زمان دستخوش دگرگونی‌های عمده‌ای گردید و از نظر افقی و عمودی نیز توسعه یافت. از نظر افقی، برداشتی از امنیت ملی که فقط مسائل امنیتی غرب را در مظان توجه قرار می‌داد و یا الگوهایی از مباحث و نظریات امنیت را به بحث می‌گرفت که بر محیط امنیتی کشورهای درحال توسعه منطبق نبوده و قابلیت کاربرد نداشت، مورد انتقاد جدی امنیت‌پژوهان واقع گردید. از نظر عمودی نیز تحت تأثیر تحولات ساختاری جهان، ظهور و افزایش تعداد کشورهای مستقل و مواجه آنان با مشکلات و پیچیدگی‌های ویژه امنیتی بود و ضرورت توسعه مفهومی امنیت، که فراتر از امنیت سنتی و رهایی از تقلیل‌گرایی نظامی‌گرایانه باشد را مورد توجه قرار داد و بدین ترتیب، دیدگاه‌هایی طرح و بسط یافتند که رویکردی متمایز از رویکرد سنتی را به نمایش می‌گذارند (کریمی مله، ۱۳۹۱: ۶۲-۶۳).

همانگونه که گفته شد تعداد مسائل و مفاهیم مرتبط با امنیت ملی افزایش یافته است. از پایان جنگ سرد، امنیت ملی به طرز فزاینده‌ای جنبه‌های اقتصادی، زیست محیط و حتی اطلاعاتی به جای مفاهیم صرفا مربوط به مرزهای فیزیکی یک کشور را داشته است. گسترش این مفاهیم جدید باعث شده که تعارف امنیت ملی نیز تغییر کند. امروزه نیز با دستیابی به اینترنت و رشد اطلاعات در جهان و کاربرد آن در حوزه‌های مختلف و زندگی روزمره، نگرانی‌ها در مورد نفوذ و استفاده از آن توسط هکرها و بازیگران خارجی وجود دارد (Watson, 2008: 5-7). ماندل نیز در دسته‌بندی خود از عناصر مفهومی امنیت ملی این موضوع را به خوبی نشان می‌دهد و باتوجه به ماهیت چندوجهی مفهوم امنیت ملی، شناخت و ترکیب عناصر تشکیل دهنده آن شامل حوزه‌های نظامی، اقتصادی، منابع-محیطی و سیاسی-فرهنگی می‌باشد (ماندل،۱۳۷۷: ۵۹ -۷۷).

توسعه فناوری‌های رایانه‌ای، نیاز به رویکردی جدید را به وجود آورد و به دنبال آن، زمینه‌ای برای مفهوم بروز شده امنیت ملی را که در برگیرنده فضای سایبری بود، فراهم آورد. رشد این فناوری در رایانه‌ها و شبکه‌های ارتباطی و ادغام آن با حوزه‌های مختلف، فضایی جدید را خلق کرد (Ben-Israel and Tabansky, 2014:

55, 56). امروزه باتوجه به رشد فناوری سایبر، مفهوم امنیت سایبر وارد حوزه امنیت ملی شده است. بخش‌های مهم زیرساخت‌های حیاتی کشورها با فضای سایبر گره خورده و حفظ امنیت سایبری، به حفظ امنیت ملی کمک می‌کند (National Strategy to secure Cyberspace, 2003: vii). از این‌رو سیاست امنیت ملی چارچوبی را برای توضیح چگونگی تأمین امنیت یک کشور برای حفظ دولت و شهروندانش نشان می‌دهد و بصورت یک سند یکپارچه منتشر می‌شود. این سند می‌تواند یک طرح، استراتژی یا دکترین نامیده شود. سیاست امنیت ملی منافع اصلی یک کشور را ترسیم می‌کند و خطوط راهنمایی را برای تهدیدات و فرصت‌های جاری و پیش‌رو فراهم می‌آورد. بصورت سلسله مراتبی، سیاست امنیت ملی نسبت به سایر سیاست‌های امنیتی فرعی مثل دکترین نظامی دارای برتری است (DCAF, 2005: 1). با این تعاریف می‌توان تهدیدات سایبری را در دسته‌بندی‌های مختلفی قرار داد. اما بطورکلی چهار نوع تهدید سایبری در مقابل امنیت ملی وجود دارد که عبارتند از: جنگ سایبری، جرایم سایبری، تروریسم سایبری و جاسوسی اقتصادی (لرد و شارپ،۱۳۹۲: ۹۶).

۳- معرفی بازیگران دولتی و واکنش آمریکا

در ابتدا باید خاطرنشان کرد که آمریکا در استراتژی‌های خود به کشورهای رقیب، دشمنان و رویکردهای متضاد آنها نسبت به این کشور اشاره می‌کند. از نگاه آمریکا، این کشورها پشت مفاهیم حاکمیتی پنهان شده و قوانین و حقوق سایر کشورها را توسط جاسوسی‌های اقتصادی و فعالیت‌های سایبری خطرناک زیرپا می‌گذارند و باعث آسیب به حوزه‌های فردی، تجاری و دولتی در سراسر جهان می‌شوند. براساس دیدگاه آمریکا، کشورهای مهمی چون روسیه، چین، کره شمالی و ایران همگی از فضای سایبر بعنوان وسیله‌ای استفاده می‌کنند که آمریکا، متحدین و شرکایش را به چالش بکشند (National Cyber Strategy, 2018: 1-3). آمریکا نیز براساس اسناد استراتژیک خود به این تهدیدات واکنش نشان می‌دهد. تغییر در استراتژی سایبری آمریکا، فرایندی است که نزدیک به نیم قرن، از دولت جانسون تا به امروز را در برمی‌گیرد (Yang, 2016: 210).

در دوران ریاست جمهوری ریگان، کنگره این کشور روسای جمهور را موظف کرد که بعد از انتخابات ریاست جمهوری استراتژی امنیت ملی خود را ارائه دهند. بعد از این تصمیم، روسای جمهور آمریکا بعد از انتخاب شدن، سندی را تحت عنوان استراتژی امنیت ملی منتشر می‌نمایند (عبداله‌خانی،۱۳۸۳: ۳۴). آمریکا نیز بعنوان یک کشور مهم هنوز به پیشرفت‌های حوزه سایبری نیاز دارد، لذا امنیت سایبری از دوران بیل کلینتون

بعنوان یکی از تهدیدات برجسته وجود داشته است (Maker, 2017: 36). اسناد مختلفی در رابطه با امنیت ملی منتشر می‌شوند که همه آنها بخشی را به بحث چالش‌ها و سیاست‌های مرتبط با فضای سایبر اختصاص داده‌اند. این اسناد اصلی شامل استراتژی امنیت ملی (ان.اس.اس)[1] استراتژی دفاع ملی (ان.دی.اس)[2] استراتژی نظامی ملی (ان.ام.اس)[3] و سند بازنگری دفاعی چهار ساله (کیو.دی.آر) [4] می‌باشند (Dale, 2013: 3-9). در ادامه به معرفی چین، روسیه، ایران و کره شمالی، فعالیت‌های آنها و واکنش ایالات متحده در قبال این حملات اشاره خواهد شد.

۳-۱- چین

معرفی قدرت سایبری چین: از سال ۱۹۹۱، ارتش چین بطور فزاینده‌ای در حوزه‌های مختلف سایبری پیشرفته، در بخش‌های دولتی، نظامی و شهری آن سرمایه‌گذاری کرده است. این کار، تلاش همه‌جانبه‌ای برای ساخت قدرت اقتصادی و سیاسی چین می‌باشد. همچنین قدمی بزرگ برای توسعه قابلیت‌های جنگ سایبری بعنوان ابزار جنگ نامتقارن و شکست برتری قدرت نظامی ایالات متحده آمریکا است. چینی‌ها این نکته را به خوبی دریافتند که فضای سایبر می‌تواند عرصه‌ای برای جنگ باشد و قدرت سایبری اکنون در جایگاه بالایی و همطراز با قدرت زمینی، دریایی و هوایی رده‌بندی می‌شود (Spade, 2012: 2). دلایل چرایی بهره‌برداری گسترده چینی‌ها از فضای سایبر، اینطور خلاصه می‌شود: پرکردن شکاف بین برنامه‌های تحقیقاتی خود با آمریکا به منظور ترسیم اهداف آینده؛ جمع‌آوری اطلاعات طرح‌ها و استراتژی‌های آمریکا؛ توانمندسازی عملیات‌های نظامی آینده؛ کم کردن زمان تحقیق و توسعه برای فناوری‌های نظامی؛ شناخت آسیب‌پذیری‌های سیستم‌ها و اقدامات متقابل توسعه‌ای آمریکا (Wortzel, 2013: 4).

بین ارتش چین و هکرها هماهنگی و سازگاری وجود دارد. ارتش چین رقابت‌های هک را برای تشویق هکرها به توسعه تکنیک‌های کد های سی.ان.ای[5] زمینه‌سازی می‌کند. برخی از نفوذی‌ها، از برنامه‌ها و نرم‌افزارهای برنامه‌نویسان کلاه سیاه چینی استفاده می‌کنند. شرکت‌های آی.تی[6] چینی هم که حامی ارتش این کشور هستند، این هکرها را برای حملات سایبری استخدام می‌کنند (Spade, 2012: 17). از این رو حملات مشکوک چین به آمریکا در حوزه‌های عمومی و خصوصی، به رویدادی هر روزه در رسانه ها تبدیل شده و

[1] National Security Strategy (NSS)
[2] National Defense Strategy (NDS)
[3] National Military Strategy (NMS)
[4] Quadrennial Defense Review (QDR)
[5] CNE Techniques
[6] IT Companies

بحثی همیشگی در جامعه ی سیاسی آمریکا است (Lieberthal and Singer, 2012: 2). اقدامات چین علیه آمریکا عمدتا بعنوان اقداماتی شناخته می‌شوند که با جرایم سایبری معمولی متفاوتند و به نظر می‌رسد اهداف استراتژیک خاصی را مدنظر دارند. دسترسی چین به شبکه‌های سایبری آمریکا بطور همزمان زمینه‌های پنهانی را برای استفاده از آنها و حملات سایبری در آینده را فراهم می‌کند (Lieberthal and Singer, 2012: 3). از همین‌رو معاون وقت رئیس فرماندهان ستاد مشترک نیروهای مسلح آمریکا، جیمز کارت رایت[1] گفته بود که یک حمله سایبری تمام عیار از جانب چین توانایی تأثیری مشابه سلاح‌های کشتارجمعی را دارد (Hjortdal, 2011: 8). گزارش کمیسیون آ.پی[2]در سال ۲۰۱۳ نشان داد که ۹۶ درصد جاسوسی‌های سایبری توسط چین انجام می‌گیرد و هر سال میلیاردها دلار دارایی‌های اطلاعاتی به سرقت می رود (Brown and Singh, 2018: 17).

یکی از شناخته شده‌ترین حملات چین به آمریکا، به باران تایتان[3]معروف است که از سایر حملات خطرناک‌تر بود، زیرا یکی از این حملات، در عرض بیست دقیقه و در یک روز قادر به نفوذ در اهداف مهمی مثل فرماندهی مهندسی سیستم‌های اطلاعاتی ارتش، سیستم‌های اطلاعاتی دفاعی و یا تأسیسات دفاع استراتژیک و فضایی ارتش بود. البته پکن این ادعاها را انکار می‌کند و بیان می‌دارد که فناوری سایبری این کشور فقط اهداف تدافعی داشته و آمریکا را به جاسوسی از چین متهم می‌کند (Rubenstein, 2014 :5). یکی از اقدمات دیگر چین دسترسی به ابزارهای هک آژانس امنیت ملی آمریکا در سال ۲۰۱۶ بود که از این ابزار برای حمله به متحدین آمریکا و شرکت‌های خصوصی در اروپا و آسیا استفاده می‌کرده است که نشان می‌دهد آمریکا، کنترل بخش‌های کلیدی امنیت سایبری خود را از دست داده است. چین برخی از این ابزارهای هک ان.اس.ای را فروخت که مورد استفاده هکرهای روسیه و کره شمالی قرار گرفت و توانستند حملاتی را به سایر کشورها داشته باشند. گروه هکرهای چینی که مسبب این کار بود، مسئول حملات سایبری متعددی به برخی از حساس‌ترین اهداف دفاعی آمریکا مثل صنایع هوایی، ماهواره‌ای و هسته‌ای هم بوده است (Perlroth, Sanger and Shane, 2019).

واکنش آمریکا به چین: در این میان، آمریکا نیز دست به اقدامات مختلفی زد. در سال ۲۰۱۴ وزارت دادگستری تایید کرد که پنج هکر چینی را بخاطر اقدام علیه امنیت ملی آمریکا از طریق فضای سایبر، متهم کرده است. اداره‌ی اف.بی.آی که مأمور انجام و پیگیری این تحقیقات بود، این پنج نفر را وابسته به واحد ۶۱۳۹۸ از

[1] James Cartwright
[2] IP commission report
[3] Titan Rain

سومین دپارتمان ارتش چین معرفی کرد. این پرونده، اولین اتهامی بود که آمریکا علیه یک بازیگر دولتی برای این نوع هک سایبری وارد می‌کرد که به گفته دادستان کل آمریکا نیازمند پاسخی محکم به چین است و آمریکا با کشورهایی که به دنبال اخلال در شرکت‌های آمریکایی هستند مدارا نخواهدکرد. این گروه در یک بازه زمانی هشت ساله، یعنی از سال ۲۰۰۶ تا ۲۰۱۴ چندین شرکت و نهاد مهم آمریکایی مثل شرکت برق وستینگ هوس[1] شرکت فولاد آمریکا[2] و برخی صنایع انرژی، کشاورزی و ... را مورد هدف قرار داد. عمده فعالیت‌های آنها توطئه برای کلاهبرداری و سوء استفاده‌های رایانه‌ای، دستیابی به اطلاعات حفاظت شده با مقاصد تجاری و مالی خصوصی، انتقال برنامه و کدهای خاص به منظور صدمه به سیستم‌های حفاظت شده، سرقت هویت، جاسوسی اقتصادی و سرقت اسرار تجاری بوده است (Department of Justice, 2014).

در آگوست ۲۰۱۷ دونالد ترامپ نیز، فرمان اجرایی جدیدی را برای تحقیق و بررسی اقدامات، سیاست‌ها و روش‌های چین در ارتباط با حوزه‌های تکنولوژیک و اطلاعات صادر می‌کند. نتیجه این تحقیق در قالب سندی در مارس ۲۰۱۸ منتشر شد که نشان داد فعالیت‌های سایبری چین تهدید جدی برای موقعیت رقابتی و اقتصاد آمریکا است و آمادگی برای واکنش به چین یکی از ملاحظات جدی آمریکا به شمار می‌آید (Limmergard, 2018: 13).

۳-۲- روسیه

معرفی قدرت سایبری روسیه: نخبگان آکادمیک و نظامی روسیه در طی دهه گذشته اسناد زیادی را منتشر کرده‌اند که نشان از تلاش کرملین برای مدرن‌سازی جنگ اطلاعاتی است و همچنین استراتژی استفاده از ابزارهای سایبری برای ایجاد اختلال در سلاح‌های دشمن، تصمیم‌گیرندگان و ذهن شهروندان رقبایش را مدنظر قرار می‌دهد (Sonftness, 2017: 100). یکی از روش‌های مورد استفاده روسیه، نیابت سایبری[3] می‌باشد که دارای دو ویژگی است. اول اینکه موثر بوده و مقرون به صرفه است، زیرا این نیابت‌ها به پشتیبانی فنی کمی نیاز دارند. در بسیاری از موارد فقط کافی است تا لیست اهداف حمله را برای آنها مشخص نمود و زمانی که دیگر نیازی به آنها نیست، می‌توان منحل‌شان کرد. دوم اینکه، هکرها برای عملیات نبرد اطلاعاتی مناسب هستند، چون مقیاس عدم شناسایی زیادی را برای کرملین فراهم می‌آورند و مسئله نسبت دادن را پیچیده می‌کنند. حتی در تحقیقات گسترده هم به ندرت ردی از آنها در ارتباط با سیستم‌های دولتی پیدا

[1] Westinghouse Electric Co.
[2] United States Steel Corp
[3] Cyber Proxy

می‌شود. از این‌رو رقبای مسکو معمولا مدرک قطعی برای اینکه کرملین مسئول این کارها بوده یا خیر، نمی‌یابند (Connell and Vogler, 2017: 11, 12). دومین توانایی سایبری روسیه، گروه‌های تهدید پایدار پیشرفته (ای.پی.تی)[1] می‌باشند که بخش اصلی عملیات‌های اطلاعاتی سایبری روسیه هستند. این گروه‌ها ارتباطات مستقیمی با دولت روسیه دارند که البته دولت حمایت از این گروه‌ها را انکار می‌کند. ولی روی هم رفته فعالیت این گروه‌ها با اهداف و جهان‌بینی کرملین همسو می‌باشد (Connell and Vogler, 2017: 10). سومین نیروی سایبری روسیه، آر.بی.ان[2] است که وظیفه این سازمان حمایت‌های لجیستیکی از حملات سایبری می‌باشد. حملات پشتیبانی شده توسط این سازمان جزء شناخته شده‌ترین ارتش‌های بات نتی جهان است. این سازمان، یک سازمان جنایی محسوب می‌شود که با دولت روسیه هم در ارتباط است. ارتباط چنین گروه‌هایی با کرملین در حملات سایبری به استونی در ۲۰۰۷ و گرجستان در ۲۰۰۸ خود را نشان می‌دهد (Regester, 2015: 29, 30).

یکی از چالش‌های پیش‌روی دولت آمریکا در مورد روسیه این است که دقیقا نمی‌داند چه واحدی پشت این حملات قرار دارد و ریشه‌یابی آن کار دشواری می‌باشد، به این معنا که واقعا این حملات بطور مستقل و توسط یک فرد یا گروه انجام شده و یا اینکه کرملین مسئول هدایت آنها است (Sabotka, 2015: 2) و کاملا مشخص نیست که عامل حملات، دولتی یا غیردولتی‌اند، زیرا اغلب فعالیتی مشترک دارند. یکی دیگر از حملات مهم روسیه به آمریکا، حمله سایبری مونلایت میز[3] بود که در سال‌های ۱۹۹۸ تا۲۰۰۰ اتفاق افتاد و اطلاعات محرمانه‌ای از وزارت دفاع آمریکا، وزارت انرژی، ناسا و موسسات خصوصی را به سرقت برد (Klimberg, 2011: 49). با گذشت زمان و پیشرفت در این حوزه، روسیه بدافزار اکتبر سرخ[4] را در سال ۲۰۱۲ برای نفوذ به سیستم‌های رایانه‌ای آمریکا فرستاد. این بدافزار به شرکت‌های مایکروسافت حمله کرد و اطلاعات حفاظت شده آن را به سرقت برد (Rubenstein, 2014: 4). نمونه دیگر رویکرد تهاجمی روسیه در تلاش‌های این کشور برای نفوذ در انتخابات سال ۲۰۱۶ آمریکا خودش را نشان داد، که در این فعالیت، مقامات کرملین اجازه نفوذ و سرقت اطلاعات مربوط به انتخابات و اهداف حساس را صادر نمودند (Coats, 2017: 1)، زیرا امروزه نفوذ امنیتی بخاطر استفاده کشورها از ماشین‌های رأی‌گیری آسان شده است (Lee and Rotoloni, 2017: 5).

[1] Advanced Persistent Threat (ATP)
[2] Russian Business Network (RBN)
[3] Moonlight Maze
[4] Red October

واکنش آمریکا به روسیه: سال‌ها قبل، مقامات آمریکایی ارتباطی را بین نفوذ در سیستم‌های رایانه‌ای متعلق به پنتاگون، ناسا، وزرات انرژی، دانشگاه‌های خصوصی و آزمایشگاه‌ها یافتند که ریشه تمام این حملات از یک شبکه رایانه‌ای در روسیه بود (Bussing, 2013: 6). لذا در سال ۲۰۱۳ آمریکا طرح حفظ زیرساخت‌های ملی را که براساس استراتژی دفاعی برای دفاع از بخش زیرساخت‌های حیاتی بود، منتشر کرد. این طرح آسیب‌پذیری‌ها و خطرات خاص هر بخش، اهداف احتمالی و روش‌های پرداختن به این زیرساخت‌ها را ارزیابی کرد. از این‌رو دولت باید نظارت دائمی بر تمام سیستم‌های سایبری را داشته باشد و اشتراک‌گذاری اطلاعاتی فوری را در طول تمام وقایع سایبری هدایت کرده و همه بخش‌ها باید اطلاعات مهم خود را پشتیبانی کند (Softness, 2017: 103).

بعد از هک شدن کمیته ملی دموکراتیک[1] در سال ۲۰۱۶ آمریکا اعلام کرد که ممکن است با حملات سایبری بیشتری مواجه شود. در این بین، بخاطر روابط رو به وخامت آمریکا و روسیه و تأکید پوتین بر جنگ اطلاعاتی، توجه عمومی بر روسیه متمرکز شد. بعد از گزارشات شرکت‌های امنیت سایبری مثل کرود استایک[2] و مندینت،[3] ادعا شد که روسیه این حملات را هدایت کرده است (Softness, 2017: 99). در عملیات سایبری علیه انتخابات، هکرهای روسی تلاش کردند تا به سیستم‌های انتخاباتی حداقل ۲۱ ایالات نفوذ کنند. مثلا در ایالات ایلینوی، هکرهای روسی توانستند به داده‌های ثبت شده‌ی رأی دهندگان دسترسی یابند (Fryer-biggs, 2018). از سال ۲۰۱۵، اف.بی.آی به وزارت فناوری اطلاعات در مورد خطر هکرهای روسیه هشدار داده بود، اما بررسی‌های فنی سیستمی هیچ چیز مشکوکی را نشان نداد. مدتی بعد هکرها ایمیل‌های آلوده‌ای را برای کارمندان هیلاری کلینتون[4] (نامزد انتخابات) ارسال کردند. با مشخص شدن این نفوذ سایبری و مدت‌ها تحقیق و بررسی، در دسامبر ۲۰۱۶، اوباما در فرمانی اجرایی، دستور تحریم شش نفر از هکرهای روسیه را داد که در این عملیات شرکت داشتند و ۳۵ نفر از دیپلمات‌های روسیه هم مجبور به ترک آمریکا شدند. در ادامه همین موضوع در سال ۲۰۱۸ وزارت دادگستری اتهام ۱۲ نفر از اعضای آژانس اطلاعاتی روسیه را اعلام کرد (CNN news, 2019).

در زمان ریاست جمهوری ترامپ، هکرهای آمریکایی اجازه دسترسی به سیستم‌های روسیه را بعنوان بخشی از راهبرد تلافی‌جویانه برای مداخله روسیه در انتخابات آمریکا دریافت کردند. جامعه اطلاعاتی و پنتاگون

[1] Democratic National Committee
[2] CrowdStrike
[3] Mandiant
[4] Hillary Clinton

بطور کامل با طرح کلی حمله سایبری تهاجمی که دست آمریکا را برای حمله به روسیه باز می‌گذارد، موافقت کردند. این کار یکی از مهم‌ترین طرح‌های نبرد سایبری است که تحت مجوز سیاست دولتی، عملیات تهاجمی را برای پیشبرد سریع امکانپذیر می‌کند. مقامات امنیت ملی آمریکا از تلاش‌های متناوب روسیه علیه سازمان‌ها و مبارزات سیاسی آمریکا خبر می‌دادند. این کشور بعد از انتخابات ۲۰۱۶ احتمال می‌دهد که حتی مسکو ممکن است نفوذهای تهاجمی را باز هم از سرگیرد. در زمان ریاست اوباما حملات سایبری مهم باید مستقیما توسط رئیس جمهور امضا می‌شد و عملیات‌های جزئی‌تر نیازمند تایید سه کمیته هماهنگی سیاسی، کمیته نمایندگان شورای امنیت ملی و کمیته مدیران بود. اما از آنجائیکه سازمان‌های جاسوسی می‌توانند از طریق عواملی به سرویس‌های دشمن خود نفوذ کنند و کدرمزها را یاد بگیرند و اطلاعات، نقشه‌ها و رمزها را کپی کرده و یا بمب‌های منطقی را در سیستم‌های دشمن پنهان کنند، به همین دلیل نیروهای سایبری ارتش می‌بایست سریعا وارد عمل شوند و واکنش نشان دهند. از همین‌رو جان بولتون، مشاور وقت امنیت ملی اظهار داشت که هرکشوری بخواهد فعالیتی سایبری علیه آمریکا انجام دهد، باید انتظار داشته باشد که این یکی از بخش‌های ایجاد ساختار بازدارندگی است و ما همانطور که ازخود دفاع می‌کنیم، بصورت تهاجمی نیز پاسخ خواهیم داد (Fryer-biggs, 2018).

به همین خاطر یکی از تصمیمات ایالات متحده نسبت به روسیه، حمله به شبکه برق این کشور بعنوان یک هشدار و نفوذ بدافزاری مختل کننده در سیستم‌های این کشور بود. این حمله طبق صلاحیت‌های قانونی کنگره در مورد مجوز نظامی سایبری ذیل دستور ترامپ در سال ۲۰۱۸، مبنی بر اجرای عملیات‌های تهاجمی سایبری انجام گرفت. در واقع، فرماندهی سایبری می‌تواند بدون نیاز به تأیید ریاست جمهوری این کار را انجام دهد. در واقع آمریکا عملیات شناسایی شبکه‌های روسیه را از سال ۲۰۱۲ آغاز کرده بود (Sullivan, 2019) و موفق شد تا این عملیات تهاجمی را علیه زیرساخت‌های حیاتی این کشور انجام دهد. جزئیات این عملیات، سری باقی ماند و مسکو نیز سعی کرد زیاد به آن نپردازد. البته در اصل، مجوز حمله به روسیه در دوران ریاست جمهوری اوباما صادر شده بود، اما باید تا مدتی سری باقی می‌ماند، همانطور که مسبب حمله سایبری به تأسیسات هسته‌ای ایران، برای مدتی آشکار نشد (Carrol, 2019). بعد از این رخداد روسیه اعلام کرد که مانع از حمله سایبری آمریکا به زیرساخت‌های حیاتی خود شده و ادعا نمود که آمریکا نیز در سال‌های اخیر حملاتی را به سیستم‌های حمل‌ونقل، بانکی و انرژی داشته است. از دید کرملین، این حمله همه نشانه‌های جنگ سایبری و عملیات نظامی علیه روسیه را داشته است (Moscowtimes, 2019).

۳-۳- ایران

معرفی قدرت سایبری ایران: ایران کشوری است که از توانمندی‌های تهاجمی و تدافعی عرصه سایبری آگاه است و از سال ۲۰۰۲ به بعد، عمیقا با مسائل و فناوری‌های مربوط به این حوزه سروکار دارد. بعد از آن سال یک شورای عالی برای این حوزه و توسعه آن تأسیس شد و در مدت زمان کوتاهی ارتش سایبری ایران گسترش یافت و توانمندی‌های خود را در آموزش افسران مربوط به ابعاد رویکرد تهاجمی و تدافعی آغاز کرد. بطورکلی دو زنجیره سایبری تحت فرماندهی ایران در حوزه سایبر فعالیت دارند: یکی زیرنظر مستقیم سپاه پاسداران انقلاب فعالیت دارد که شامل نیروهای نخبه سایبری است و دیگری زیرنظر دولت ایران قرار ندارد، ولی بطور غیرمستقیم توسط ایران پشتیبانی و حمایت می‌شوند، مثل گروه‌هایی همچون حزب‌اله (Maker, 2017: 25). از طرفی هم این کشور تاکنون هدف اقدامات خرابکارانه و جاسوسی از جانب کشورهایی مثل خود آمریکا، اسرائیل، فرانسه و بریتانیا بوده است و این حملات انگیزه مضاعفی برای توسعه بومی توانایی‌های دفاعی و تهاجمی ایران و اقدامات تلافی‌جویانه شده است (Anderson and Sadjadpour, 2018).

ایلان برمن[1] معاون شورای سیاست خارجی آمریکا در سال ۲۰۱۳، در سخنرانی خود در کمیته مجلس نمایندگان آمریکا درخصوص لزوم توجه به قدرت سایبری ایران و تدوین استراتژی‌های مناسب با آن و تقویت آمریکا در برابر این کشور، اشاره نمود. وی این نکته را یادآور شد که قابلیت‌های تهاجمی سایبری ایران در مسیر تکامل و رشد حرکت دارد. در طی سال‌های گذشته حملات سایبری متعددی به این کشور انجام گرفته که در پاسخ آن، مقامات ایرانی از فضای سایبر برای مقابله با غرب استفاده کرده‌اند. وی اینطور اظهار داشت که ایران سرمایه‌گذاری‌های زیادی را در ارتقای توانایی‌های تهاجمی خود کرده است. از اواخر سال ۲۰۱۱ بیش از یک میلیارد دلار برای توسعه توانایی‌های سایبری خودش اختصاص داده و خود را چهارمین قدرت سایبری جهان می‌داند. عمده هکرهای ارتش این کشور با واحد سایبری سپاه همکاری می‌کنند. از طرفی هم، ایران توانایی‌های سایبری خود را برای توسعه با شرکای استراتژیک مثل سوریه پیش می‌برد (Berman, 2013: 3).

درخصوص اقدامات سایبری ایران باید گفت که این کشور بطور عمده بر رقبای خاورمیانه‌ای، یعنی عربستان و اسرائیل تمرکز دارد، اما نسبت به آمریکا نیز فعالیت‌هایی داشته است مانند گروه هکری راکت کیتن[2] که شرکت‌های دفاعی آمریکا را هک کرد، گروه هکری اویل ریگ[3] که برخی از شرکت‌های آمریکایی را مورد

[1] Ilan Berman
[2] Rocker Kitten
[3] OilRig

حمله قرار داد و دیگری، گروه هکری ای.پی.تی۳۳ به شرکت‌های بخش انرژی و موسسات آکادمیک آمریکا نفوذ کرد (NCSC, 2018: 9). یکی دیگر از حملات سایبری ایران، به نهادهای مالی آمریکا بود که به منظور واکنش به وضع تحریم‌های اقتصادی جدید علیه این کشور اتفاق افتاد. سه بانک جی.پی.مورگان[1] بانک آمریکا کورپ[2] و سیتی گروپ[3] از سال ۲۰۱۱ مورد حمله ایران بوده‌اند. در این موارد آمریکا نتوانست مشخص کند که آیا این حملات توسط دولت انجام شده یا توسط گروه‌های مرتبط با آن و یا اینکه هکرهای وطن‌پرست مسبب آن بوده‌اند. هیچکدام از مقامات پنتاگون یا وزارت امنیت داخلی در مورد جزئیات این حملات صحبتی نکردند. گرچه این حملات از نوع حملات داس بوده و پیچیدگی خاصی ندارد، اما می‌توانست بسیار مخرب باشد. از این‌رو وزارت امنیت داخلی و آژانس امنیت ملی به تقویت شبکه‌های بانکی برای مواجه با حملات سایبری آینده پرداختند. بعد از این حادثه، جیم لویس[4] عضو ارشد مرکز مطالعات استراتژیک و بین‌الملل گفت: «این (قدرت سایبری ایران) مانند برنامه هسته‌ای است، پیچیدگی خاصی ندارد، اما می‌تواند هر سال پیشرفت داشته باشد» (Finkle and Rothacker, 2012). در فوریه ۲۰۱۴ حمله سایبری دیگری به سندزکازینوی لاس و گاس[5] انجام شد که هکرها بطور کامل شبکه‌های این شرکت را از کار انداختند. این حمله چند ماه بعد از این اتفاق افتاد که مدیر این شرکت، شِلدون آدلسون[6] پیشنهاد داده بود که آمریکا باید تهران را در صورت عدم توقف ساخت سلاح هسته‌ای، به حمله اتمی تهدید کند. برخی کارشناسان برای عقیده بودند که این حمله پاسخ هکرهای ایران بود (Sabotka, 2015: 5).

واکنش آمریکا به ایران: ایالات متحده نیز در پاسخ به فعالیت‌های ایران دست به اقداماتی زد. دولت اوباما از سال ۲۰۰۹ فضای سایبر را در مرکز تمرکز سیاسی قرار داد و آن را بعنوان عرصه جدید منازعه می‌دید. اما این توجه بیشتر معطوف به چین و روسیه بود و کمتر به قدرت سایبری ایران برای جنگ سایبری توجه می‌شد. ولی به تدریج متخصصین به تهدید ایران و عدم طرح‌ریزی جدی برای این کشور پی‌بردند. از این‌رو برخی از بخش‌های اداره فدرال مثل فرماندهی استراتژیک آمریکا[7] شروع به بررسی تهدیدات بالقوه ایران در حوزه سایبر کردند. زیرا بر این باورند که ایران به دنبال آماده شدن برای یک جنگ سایبری و به فکر ضربه زدن به زیرساخت‌های حیاتی آمریکا است (Berman, 2012). زیرا زمانی که آمریکا ویروس استاکس نت را

[1] JP Morgan
[2] Bank of America Corp
[3] Citigroup Inc
[4] Jim Lewis
[5] Las Vegas Sands Casino
[6] Sheldon Adelson
[7] US Strategic Command

برای تأسیسات هسته‌ای ایران طراحی کرد، قصد نفوذ در سایر برنامه‌های نظامی و علمی ایران را هم داشت (Bussing, 2013: 9). استاکس نت به برخی از کشورهای دیگر هم ورود کرد ولی آسیب فیزیکی نداشت و این نشان می‌دهد که این ویروس فقط برای ایران ساخته شده است (Bussing, 2013: 10).

در موردی دیگر و در سال ۲۰۱۶ وزارت دادگستری آمریکا در همکاری با اداره تحقیقات فدرال (اف.بی.آی) پرونده هفت نفر از هکرهای سپاه پاسداران (احمد فتحی، حمید فیروزی، امین شکوهی، صادق احمدزادگان، امید غفارنیا، سینا کیسر، نادر ساعدی) را مطرح کرد. در این پرونده ذکر شده است که تیم آی.تی.سک[1] و شرکت مرصاد از جانب دولت ایران حملاتی از نوع دی.داس را به خاک آمریکا داشته‌اند. این حملات با هدف نفوذ به وبسایت‌های بانکی، ناسا و برخی از صنایع آمریکا از سال ۲۰۱۱ تا ۲۰۱۳ انجام شد که هزینه‌های زیادی را بر دوش این کشور گذاشت. وزارت دادگستری اعلام کرد که از این پس رویه خود را در برابر این گروه‌ها تغییر داده و اجازه تهدیداتی از این نوع را نخواهد داد و از ابزارهای لازم برای پیگیری اتهامات این مجرمان استفاده خواهد کرد (Department of Justice, 2016). این رویه وزارت دادگستری ادامه یافت و در سال‌های ۲۰۱۷ و ۲۰۱۸ نیز چندین هکر دیگر را به سرقت و نفوذ سایبری متهم کرد. در جولای ۲۰۱۷، دو نفر دیگر (محمدرضا رضازاده و محمد سعید آجیلی) به اتهام نفوذ به شرکت‌های نرم‌افزای آمریکا، سرقت اطلاعات و فروش آنها به دیگر کشورها، اعلام شدند. در نوامبر همین سال، فردی دیگری (بهزاد مصری) را که سابقا یکی از اعضای نظامی ایران بود، به هک کردن سیستم‌ها و سرقت دارایی‌های اطلاعاتی آنها متهم نمود. در مارس ۲۰۱۸ نیز نه نفر از هکرهای سازمان مبنا، متهم به سرقت دارایی‌های اطلاعات بیش از ۱۴۴ دانشگاه آمریکا شدند (NCSC, 2018: 10).

در سال ۲۰۱۸ نیز، زمانی که ترامپ تحریم‌های اقتصادی دولت اوباما را مجددا اعمال کرد، بسیاری از نهادهای مالی و بانکی آمریکا و حتی سایر بخش‌های مهم این کشور، نگران موج تازه‌ای از حملات ایران، همانند آنچه که در سال‌های ۲۰۱۱ تا ۲۰۱۳ رخ داد، بودند. گرچه بعد از آن حملات، آمریکا به تقویت توانایی‌های دفاعی زیرساخت‌های حیاتی خود بویژه نهادهای مالی و انرژی پرداخت و وزارت دفاع نیز در موقعیتی تهاجمی نسبت به تهدیدات آینده ایران قرار گرفت، اما امکان وقوع حادثه‌ای مشابه آمریکا را در حالت آماده‌باش نگه داشت (Pagliery, 2018). ایران با این اقدامات نشان می‌دهد که چطور می‌تواند از عملیات سایبری تهاجمی به مبارزه علیه رقبایی بپردازد که از خودش پیشرفته‌تر هستند. عملیات سایبری تهران تاکنون اغلب در قالب

[1] Ti Sec

مبازرات جاسوسی و خرابکارانه بوده است و کمتر به سرقت اقتصادی می‌پردازد. چنین اقداماتی توانایی اعمال هزینه‌های تلافی‌جویانه بر دشمنانش را آشکار می‌کند (Anderson and Sadjadpour, 2018).

در سال ۲۰۱۹، یک هفته بعد از اعلام ترامپ درخصوص پشتیبانی از کاربرد سلاح‌های متعارف علیه ایران، حمله سایبری دیگری را به این کشور انجام داد. در واقع این تصمیم آمریکا، پاسخی به افزایش فعالیت سایبری ایران و انهدام پهپاد آمریکایی بود. این حمله توسط فرماندهی سایبری آمریکا با دستور مستقیم ترامپ انجام شد. فرماندهی سایبری آمریکا در این حمله، سیستم‌های رایانه‌ای نظامی مورد استفاده در لانچرهای راکت و موشک‌انداز ایران را هدف قرار داد. زیرا این سیستم‌ها از طرف سپاه پاسداران انقلاب هدایت می‌شوند که آمریکا آن را یک سازمان تروریستی می‌داند. دلیل دیگر این حمله، تلاش‌های فزاینده ایران برای هدف قرار دادن زیرساخت‌های حیاتی آمریکا است که به دنبال تنش‌زا شدن روابط دو کشور صورت گرفت (Cimpanu, 2019). بعد از انهدام پهپاد آمریکایی توسط ایران و حمله سایبری آمریکا به سیستم‌های موشکی این کشور، مقامات دولتی آمریکا نسبت به حمله‌های سایبری آینده ایران برای تلافی این کار هشدار دادند (NBC news 2019: June 20).

۳-۴- کره شمالی

معرفی قدرت سایبری کره شمالی: کره شمالی یکی از معدود کشورهایی است که کمترین حضور اینترنتی در جهان را دارد و دسترسی اندک آن به اینترنت هم از طریق کشور چین انجام می‌گیرد و دارای شبکه‌های داخلی است. گرچه نخبگان و افراد خارجی دسترسی بیشتری به اینترنت دارند، ولی به شدت توسط دولت این کشور تحت نظارت هستند. یکی از ابهامات و سوالاتی که در مورد این کشور وجود دارد این است که آیا قابلیت‌های تکنیکی خود را برای هدایت حملات مخرب توسعه می‌دهد یا خیر. در این بین کره جنوبی مهمترین قربانی حملات سایبری کره شمالی می‌باشد اما امروزه، حملات‌اش را به دیگر کشورهای جهان هم توسعه داده است و طیف حملات آن از نهادهای مالی بزرگ آمریکا گرفته تا بانک جهانی و سایر بانک‌های جهان، حتی اوروگوئه را نیز تهدید می‌کند. عمده این فعالیت‌ها تحت اجرای اداره کل شناسایی[1] و خصوصا اداره ۱۲۱ این کشور است که مسئول انجام عملیات‌های مخفیانه می‌باشد. تعداد نیروی سایبری این کشور بین ۳۰۰۰ تا ۶۰۰۰ نفر تخمین زده شده است (CRS, 2017: 1, 2).

[1] Reconnaissance General Bureau (RGB)

علاقه رهبر کره شمالی، کیم.جونگ.اون[1] به جنگ سایبری به قبل از شروع ریاست وی باز می‌گردد. کیم جونگ ایل[2] رهبر سابق کره شمالی، مزیت‌های داشتن ارتشی شبکه‌ای را دریافته بود و بر اهمیت ایجاد توانایی‌های سایبری تأکید می‌کرد. سند راهنمای جنگ الکترونیک[3](۲۰۱۵) ارتش کره از قول وی چنین نقل می‌کند که: «اگر اینترنت یک اسلحه است، حملات سایبری مانند بمب‌های اتمی هستند». او بر اهمیت اطلاعات در قرن ۲۱ تأکید می‌کرد و معتقد به برتری نسبت به رقیب در این حوزه بود. کیم جونگ اون نیز براساس کار پدرش واحدهای سایبری ویژه‌ای را تأسیس و گسترش داد (Jin Young, Kyoung Gon And Jong In, 2019: 2). از آنجائیکه یکی از اهداف کره شمالی، توسعه قدرت نظامی نامتقارن است، سربازان نخبه‌ای را برای اِعمال توانایی‌های سایبری‌اش بکار می‌برد و در سال بین ۵۰ تا ۶۰ نخبه را برای آموزش‌های علوم کامپیوتر به خارج اعزام می‌کند و احتمالا بعنوان مهاجمان سایبری در واحدهای نظامی این کشور گماشته می‌شوند (Jin Young, Kyoung Gon And Jong In, 2019: 3).

توانایی‌های دفاعی و تهاجمی کره شمالی شامل مولفه‌های جنگ الکترونیک و سایبری است، مانند عملیات‌های سایبری تهاجمی، عملیات‌های شبکه‌ای رایانه‌ای، حملات دی.داس، نظارت ماهواره‌ای، پهپادها و ... (HP security research, 2014: 28). جنگ سایبری یکی از ابعاد نامتقارن مهم از نبرد این کشور به‌شمار می‌آید که به دلیل قابلیت انکار و هزینه نسبتا کم آن، اهمیت زیادی دارد (HP security research, 2014: 27). اغلب تاکتیک‌های کره شمالی نیز براساس استراتژی نظامی حمله برق‌آسا بوده است که حملاتی سریع با نیروی گسترده و بدون دادن زمان به قربانیان برای مقابله انجام می‌گیرد. اما تاکتیک‌های نیروهای سایبری اکنون پنهانی و بلندمدت شده‌اند، چون محیط سایبری نیازمند زمان کافی برای مهاجمین به منظور درک و هجوم به سیستم‌های اطلاعاتی است.کره شمالی زمان زیادی را صرف شناسایی اهدف خود می‌کند و از طریق ابزارهای مختلف مثل ارسال ایمیل‌های فیشینگ برای آلوده کردن رایانه‌های هدف بهره می‌برد (Jin Young, Kyoung Gon And Jong In, 2019: 13).

یکی از حملات سایبری معروف کره شمالی به شرکت سونی پیکچرز بود که در این پرونده اف.بی.آی مأمور رسیدگی به آن شد و منجر به تحریم‌های بیشتر آمریکا، علیه کره شمالی گردید (Sabotka, 2015: 25). مورد پرونده سونی یکی از حملات سایبری بود که آمریکا به یک کشور نسبت داد. این شرکت شعبه فرعی شرکت سونی ژاپن، مستقر در آمریکا است، که محصولات دیجیتالی، فیلم و ... را تولید و منتشر می‌کند.

[1] Kim Jong Un
[2] Kim Jong Il
[3] Electronic Warfare Reference Guide

هکرها ادعا کردند که به سرورهای ورودی این شرکت دست یافتند و بیش از ۱۰۰ترابایت از اطلاعات محرمانه، شامل ایمیل‌های شخصی، شماره‌ها و ... را به سرقت برده و آنها را در وبسایت‌های عمومی قرار دادند. بعد از آن، این شرکت تمام سیستم‌های خود را موقتا خاموش کرد. هکرها خواستار این بودند که این شرکت، اکران فیلم خود در مورد ترور رهبر کره شمالی را متوقف کند و مدتی بعد هکرها، مردم آمریکا را به عواقبی مشابه یازده سپتامبر تهدید کردند. در پایان تحقیقات اف.بی.آی، مشخص شد که این حملات مشابه حملاتی است که کره شمالی، قبلا هم به بانک‌ها و رسانه‌های کره جنوبی داشته است و در نهایت مسبب پرونده سونی نیز، پیونگ یانگ معرفی گردید (CEA, 2018: 16).

واکنش آمریکا به کره شمالی: در واکنش به اقدام علیه شرکت سونی، اوباما این رویداد را خرابکاری سایبری نامید و اعلام کرد که پاسخی متناسب با این حمله کره شمالی را در نظر دارد که در زمان و به روش مناسب خود پاسخ می‌دهد. روز بعد از سخنرانی اوباما، سرویس‌های خدمات اینترنتی کره شمالی برای ۱۰ ساعت ازکار افتادند، اما مقامات آمریکایی درباره اینکه آیا این کار مربوط به پاسخ متناسب بوده یا نه توضیحی ندادند (CRS, 2017: 7). بعلاوه، این حمله تأثیرات بدی بر روابط بین آمریکا و کره شمالی داشت و بر سیاست‌گذاری‌های امنیت سایبری آمریکا موثر بود، از این‌رو اوباما تحریم‌های جدیدی را بر افراد و شرکت‌های مختلف مربوط به بخش‌های نظامی و تکنولوژیک کره شمالی وضع کرد، همچنین تمهیدات قانونی بیشتری را برای پاسخ به این حمله اعمال نمود. وی به اشتراک‌گذاری هرچه بیشتر اطلاعات امنیت سایبری و نوسازی قانون پاسخ اجرایی به فعالیت‌های بدخواهانه نیز تأکید کرد (CEA, 2018: 16, 17).

در سال ۲۰۱۹ آژانس امنیت ملی (ان.اس.اِی) آمریکا تصمیم گرفت تا بخش امنیت سایبری جدیدی را برای مقابله با دشمنان خارجی راه‌اندازی کند. یکی از دلایل این اقدام ان.اس.اِی، تمرکز ویژه بر افزایش قدرت سایبری کره شمالی (و ایران) بود. این سازمان که با نام گروه ریاست امنیت سایبری[1]شناخته می‌شود، با هدف ادغام اطلاعات خارجی و مأموریت‌های دفاعی سایبری عمل می‌کند. این واحد جدید به همکاری با فرماندهی سایبری، وزارت امنیت داخلی و اداره تحقیقات فدرال کمک می‌نماید (Afif-Sabet, 2019).

[1] Cybersecurity Directorate

نتیجه‌گیری

این پژوهش به دنبال پاسخ به این سوال بود که بازیگران دولتی چه تأثیری بر تحول استراتژی ایالات متحده آمریکا در برابر تهدیدات امنیت سایبری داشته‌اند. آنطور که در فرضیه اشاره شد، افزایش اثرگذاری فناوری‌های سایبری بر امنیت ملی و ظهور بازیگران دولتی، بر تحول استراتژی آمریکا در برابر تهدیدات سایبری تأثیرگذار بوده‌اند و مسبب کنار گذاشتن حالت تدافعی و اتخاذ رویکرد تهاجمی شده‌اند. اشاره شد که فضای سایبری جای خود را در بخش‌های مختلف مدیریتی کشورها باز کرده است و به یکی از مولفه‌های مهم امنیت ملی تبدیل شده و به شدت آمریکا را درگیر خود ساخته است. امنیت ملی با هدف حفظ استقلال، رفاه و جلوگیری از تهدیدات داخلی و خارجی پایه‌گذاری می‌شود. باتوجه به رشد فناوری و گسترش دامنه امنیت به حوزه سایبر، اهمیت این عرصه بعنوان یکی از حوزه‌هایی که آماج تهدیدات مختلف است، بیش از پیش مورد توجه آمریکا و امنیت ملی آن واقع شده است. از آنجائیکه ایالات متحده از پیشتازان این عرصه می‌باشد، موضوع امنیت سایبری به یکی از مولفه‌های مهم در تدوین استراتژی‌های امنیت ملی این کشور به‌شمار می‌آید. از دیدگاه آمریکا، کشورهایی مانند چین، روسیه، ایران و کره شمالی از جمله مهم‌ترین و فعال‌ترین کشورها در عرصه سایبری به‌شمار می‌آیند و فعالیت‌های این بازیگران تهدیدی مهم برای امنیت این کشور می‌باشد.

افزایش اهمیت سایبر در امنیت ملی و تحول در استراتژی‌های امنیتی این کشور را می‌توان با یک مقایسه مشاهده کرد. واژه سایبر در استراتژی امنیت ملی ۲۰۰۲ یعنی در دوران ریاست جمهوری بوش، وجود ندارد، اما این واژه و مشتقات دیگر آن در نسخه ۲۰۱۰ دوران ریاست اوباما، ۲۴ مرتبه تکرار شده و در استراتژی امنیت ملی در زمان ترامپ یعنی سال ۲۰۱۷، ۴۶ بار مطرح می‌شود، که اینها نشان دهنده اهمیت روزافزون این عرصه در سطوح کلان امنیتی این کشور است. این افزایش اهمیت، حاکی از نیاز به تغییر در سیاست‌گذاری برای مدیریت این فضا بود. بطورکلی امنیت ملی بعنوان اولین هدف کشورها با رشد فناوری، اهمیت روزافزون یافته و فضای سایبر نیز یکی از ابعاد آن به‌شمار می‌آید. بازیگران مختلفی در این عرصه ظهورکرده‌اند که هرکدام برای ایالات متحده خطرساز هستند و این کشور برای مقابله و حفظ امنیت ملی خود نیازمند تحول در سیاست‌گذاری و استراتژی‌های خود است. در مجموع به نظر می‌رسد که افزایش اثرگذاری فناوری‌های سایبری بر امنیت ملی و ظهور بازیگران دولتی بر تحول استراتژی آمریکا و اتخاذ رویکردی تهاجمی این کشور در برابر تهدیدات سایبری تأثیرگذار بوده‌اند.

فهرست منابع

فارسی:

۱- عبداله خانی، علی (۱۳۸۳)، **نظریه های امنیت؛ مقدمه‌ای بر طرح‌ریزی دکترین امنیت ملی (۱)**، تهران: انتشارات ابرار معاصر.

۲- کریمی مله، علی.(۱۳۹۱)، «تأملی نظری در نسبت حکمرانی خوب و امنیت ملی»، **فصلنامه مطالعات راهبردی**، س ۴، ش ۱۵.

۳- لرد، کریستین ام و تراویس شارپ (۱۳۹۲)، **آینده سایبری آمریکا؛ امنیت و رفاه در عصر اطلاعات**، تهران: مرکز راهبردی سپاه پاسداران انقلاب اسلامی.

۴- ماندل، رابرت (۱۳۷۷)، **چهره متغیر امنیت ملی**، ترجمه: پژوهشکده مطالعات راهبردی، تهران: پژوهشکده مطالعات راهبردی.

لاتین:

5- Afif-sabet, Keumars (2019). NAS to Create New Division to Bolster Us Cyber Defences. Available At:https://www.itpro.co.uk/security/34077/nsa-to-create-new-division-to-bolster-us-cyber-defences.

6- Anderson, Collin and Karim, Sadjadpour (2018). Iran Cyber Threat: Espionage, Sabotage and Revenge, Available at: https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-introduction-pub-75138

7- Ben, Israel and Lior, Tabansky (2014). An International Look at Security Challenges in the Informaton Age. Cyberspace and National Security. Siboni, Gabi(ed). Telaviv university: INSS.

8- Berman, Ilan (2013). The Iranian Cyber Threat, Revisited, Statement Before the U.S House of Representatives Committee On Homeland Security Subcommittee On Cybersecurity, Infrastructure Protection and Security Technology. Available at: https://docs.house.gov/meetings/HM/HM08/20130320/100523/HHRG-113-HM08-Wstate-BermanI-20130320.pdf.

9- Berman, Ilan (2012). The Iranian cyber threat to the U.S homeland. Statement Before the U.S House of Representatives Committee on Homeland Security Subcommittee On Cybersecurity, Infrastructure Protection and Security Technology and Subcommittee on Counterterrorism and Intelligence. Available at: https://www.afpc.org/about/experts/ilan-i-berman

10- Brown, Michael and Pavneet, Singh (2018). China`s Technology Transfer Strategy. Defense Innovation Unit Experiment. Silicon Valley.

11- Bussing, Joseph (2013). The Degrees of Force Exercised in the Cyber Battlespace. Connection, 12(4), pp 1-14.
12- CEA (2018). The Cost of Malicious Cyber Activity to The U.S Economy, The Council of Economic Advisers, Executive Office Of The President Of The United States. Available at: https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf
13- Cimpanu, Catalin (2019). US Launches Cyber-Attack Aimed at Iranian Rocket and Missile Systems. Available at: https://www.zdnet.com/article/us-launches-cyber-attack-aimed-at-iranian-rocket-and-missile-systems/
14- CNN (2019). Presidential Campaign Hacking Fast Facts, 31 October. Available at: https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html
15- Coats, Daniel R (2017). Statement for the Worldwide Threat Assessment of the US Intelligence Community. Senate Select Committee on Intelligence. Available at: https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf
16- Connell, Michael and Sarah, Volger (2017). Russia`s Approach to Cyber Warfare. CAN Analysis & Solution.
17- CRS. (2017). North Korean Cyber Capabilities. Congressional Research Service, R44912.At: https://fas.org/sgp/crs/row/R44912.pdf
18- Carroll, Oliver (2019). US cyberattack: Did America really try to override the Russian power grid? Independent, June 19, Available at: https://www.independent.co.uk/news/world/europe/us-cyber-attack-russia-power-grid-war-kremlin-a8964506.html
19- Dale, Catherine (2013). National Security Strategy: Mandates, Execution to Date, and Issues for Congress. CRS, Congressional Research Service, R 43174. Available at: https://fas.org/sgp/crs/natsec/R43174.pdf
20- DCAF (2005). National Security Policy. Backgrounder, Security Sector Governance and Reform. Available at: https://www.eldis.org/document/A22260.
21- Department of Defense (2018). Cyberspace Operations. Joint Publication 3-12. Available at: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf
22- Department of Justice (2016). Seven Iranians Working for Islamic Revolutionary Guard Corps Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S Financial Sector. Available at: https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged

23- Department of Justice (2014). U.S Charges Five Chinese Military Hackers for Cyber Espionage Against U.S Corporations and A Labor Organization for Commercial Advantage. Available at: https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.
24- Department of State (2016). International Cyberspace Policy Strategy. Available at: https://2009-2017.state.gov/documents/organization/255732.pdf.
25- Finkle, Jim and Rick, Rothacker (2012). Iranian Hackers Target Bank of America, Jp Morgan, Citi. Reuters, September 21, Available at: https://www.reuters.com/article/us-iran-cyberattacks/exclusive-iranian-hackers-target-bank-of-america-jpmorgan-citi-idUSBRE88K12H20120921
26- Fryer-Biggs, Zakhary (2018). Center for public integrity. Available at: https://publicintegrity.org/national-security/future-of-warfare/the-pentagon-has-prepared-a-cyber-attack-against-russia/
27- Hjortdal, Magnus (2011). China`s Use of Cyber Warefare: Espionage Meets Strategic Deterrence". Journal of Strategic Security, 4(2).
28- HP Security Briefing (2014). Profiling and Enigma: The Mystery of North Koreas cyber Threat Landscape. HP Security Research, 16.
29- Ji young, Kong, Kim, Kyoung Gon and lim, Jong in (2019). The All-Purpose Sword: North Korea`s Cyber Operations and Strategeis. Tallin. Available at: https://ccdcoe.org/uploads/2019/06/Art_08_The-All-Purpose-Sword.pdf
30- Klimber, Alexander (2011). Mobilising Cyber Power. Survival, 53(1), pp 41-60. Available at: https://doi.org/10.1080/00396338.2011.555595
31- Lee, Weknke and Bo Rotoloni (2017). Emergence Cyber Threats, Trends & Technologies. Georgia Tech. The Institute for Information Security & Privacy.
32- Libicki, Martin C (2013). Brandishing Cyberattack Capability. National Defense Research Institute. Available at: https://www.rand.org/pubs/research_reports/RR175.html
33- Lieberthal, Kenneth and Peter W. Singer (2012). Cybersecurity and U.S-China Relations. China Center,Brookings.Availableat:https://www.brookings.edu/wp,content/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf.
34- Limmergard, Robeert (2018). State Sponsored Cyber Attacks. Swedish Security & Defence Industry Association.Available,at:https://soff.se/wpcontent/uploads/2018/03/Cybersecurity_statsunderst%C3%B6ddaakt%C3%B6rer.pdf.
35- Maker, Simran R (2017). New Frontier in Defense: Cyber Space and U.S Foreign Policy. National Committee on American Foreign Policy Report. Available at: https://www.ncafp.org/new-frontier-defense-cyberspace-u-s-foreign-policy-report/

36- Moscowtimes (2019). Russia Thawarts U.S Cyber Attacks on Its Infrastructure. June 17, Available at: https://www.themiscowtimes.com/2019/06/17/russia-uncovers-attempted-us-cyberattack-on-its-infrastructure-ria-a66034
37- National Cyber Strategy of the United States of America (2018). White House. Available at: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
38- National Strategy to Secure Cyberspac (2003). White House. Available at: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf
39- NBC News (2019). U.S. drone shot down by Iran in international space, U.S. officials say, June 20, Available at: https://www.nbcnews.com/news/world/military-official-says-no-u-s-drones-iranian-airspace-after-n1019566.
40- NCSC (2018). Foreign Economic Espionage in Cyber Space. National Counter Intelligence and Security Center. Available at: https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf
41- Pagliety, Jose. (2018). Us Banks Prepare for Iranian Cyberattacks as Retaliation for Sanctions. CNN, Noveember 9. Available at: https://edition.cnn.com/2018/11/09/tech/iran-sanctions-us-banks-cyber-hack-invs/index.html
42- Perlroth, Nicole, David E. Sanger and Scott Shane. (2019). How Chinese Spies Got the NSA`s Hacking Tools, and Used Them for Attacks**.** Available at: https://www.nytimes.com/2019/05/06/us/politics/china-hacking-cyber.html.
43- Regester, Virginia C (2015). An Assessment of Botnets as an Offensive Cyber Weapon for the United States. ProQuest. Utica College.
44- Rubenstein, Dana (2014). Nation State Cyber Espionage and Its Impacts. Available at: https:// www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage/index.html
45- Sabotka, Sarah S. (2015). An Assessment of Historical and Emerging Nation-State Cyber Threats: China, Russia, North Korea and Iran. ProQuest. Utica College.
46- Sigholm, Johan (2016). Non-State Actors in Cyberspace Operations, Swedish National Defence College.
47- Softness, Nicole (2017). How Should the U.S Respond to Russian cyberattack? Yale Journal of International Affairs, 12, pp 99-113.
49- Spade, Jayson M (2012). China`s Cyber Power and America`s National Security. Pennsylvania: U.S Army War College.
50- Sullivan, Kate (2019). New York Times: US Ramping Up Cyber Attacks On Russia. CNN, June 15. Available at: https://editon.cnn.com/2019/06/15/politics/us-ramping-up-cyberattacks-russia/index.html

51- Watson, Cybthia A (2008). U.S National Security. England. Oxford. ABC Clio.
52- Windrem, Robert (2016). Timeline: Ten Years of Russian Cyber Attacks on Other Nations. NBC News, December 18, Available at: https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111
53- Wortzel, Larry (2013). Cyber Espionage and the Theft of US Intellectual Property and Technology. Testimony before the House of Representatives, July 9.
54- Yang, Jia-hao (2016). Development of the U.S Cybersecurity Strategy Legislation and the Enlightment for China. China Zhongnan University of Economics and law.