American Strategic Studies Journal

8

Vol. 4
winter 2023

Research Paper

Received:
29 September 2022
Accepted:
15 Octorber 2023
P.P: 75-104

A comparison of cyber security policies of U.S presidents (2000-2020)

Seyedah Zohra Makhmelbaf [1] | Shirzad Azad [2]

Abstract

Today, cyber space has been turned into one of the most important dimensions of security in our world. With the development and growth of cyber technology, we face an increase in threats of this arena. According to their goals, governmental and non- governmental actors have taken actions against U.S national security. Therefore, change and evolution in the national security with considering cyberspace and its possible threats, from George W. Bush time, has borne different characteristics. The paper tries to review the characteristics of policy and strategies of the U.S presidents against the threats. To answer the paper`s central question, we show that the U.S cyber strategy, under Bush, was defensive and marginal; had domestic and international development under Obama; and was openly offensive under Trump. This paper has been written by library resources and documents in content analysis method and descriptive approach.

Keywords: Cyber security, US, Bush, Obama, Trump.

1. Corresponding Author: Master of International Relations, Ferdowsi University of Mashhad, Mashhad, Iran. z.nastaran57@gmail.com
2. Associate Professor, Department of Political Science and International Relations, Ferdowsi University of Mashhad, Mashhad, Iran.

نشریه علمی مطالعات راهبردی آمریکا

۸

سال دوم
زمستان ۱۴۰۱

مقاله پژوهشی

تاریخ دریافت:
۱۴۰۱/۰۷/۰۶
تاریخ پذیرش:
۱۴۰۲/۰۷/۲۳
صص: ۱۰۴-۷۵

مقایسه سیاست‌های امنیت سایبری رؤسای جمهور آمریکا (۲۰۰۰-۲۰۲۰)

سیده زهره مخملباف[۱] | شیرزاد آزاد[۲]

چکیده

امروزه، فضای سایبر به یکی از مهم‌ترین ابعاد امنیت بدل گشته است به‌طوری که با رشد و توسعه‌ی فناوری سایبری، شاهد افزایش خطرات در این عرصه هستیم. بازیگران مختلفی اعم از دولتی و غیردولتی در این حوزه ظهور کردند و هر کدام به نحوی و بر اساس اهداف خود علیه امنیت ملی آمریکا دست به اقداماتی زده‌اند. از این رو موضوع امنیت سایبری در سیاست‌گذاری رهبران آمریکا جایگاه شایان توجهی یافت. لذا از دوران ریاست جرج بوش پسر تغییر و تحولات در امنیت ملی با نگاه به کنترل فضای سایبر و تهدیدات احتمالی آن تا به امروز، دارای ویژگی‌هایی بوده است. در دوره‌ی ریاست جمهوری اوباما و ترامپ نیز رویدادهایی در این عرصه به وقوع پیوست. لذا در این نوشتار به دنبال این هستیم که نشان دهیم نوع سیاست و استراتژی رؤسای جمهور آمریکا در قبال این گونه تهدیدات از چه ویژگی‌هایی برخوردار بوده است. در پاسخ به این سؤال نیز، نشان می‌دهیم که استراتژی سایبری آمریکا در دوران بوش، حالتی تدافعی و حاشیه‌ای داشت، در دروان اوباما به سمت گسترش و توسعه‌ی داخلی و بین‌المللی رفت و نهایتا در دوران ریاست ترامپ، علنا رویکردی تهاجمی برای آن اتخاذ شد. این پژوهش با رویکرد توصیفی-تحلیلی و با روش مطالعه اسنادی و استفاده از منابع کتابخانه‌ای اعم از مکتوب و الکترونیکی و تحلیل محتوای کیفی آن‌ها نگاشته شده است.

کلیدواژه‌ها: آمریکا، امنیت سایبری، بوش، اوباما، ترامپ

۱. نویسنده مسئول: کارشناسی ارشد روابط بین‌الملل، دانشگاه فردوسی مشهد، مشهد، ایران.
z.nastaran57@gmail.com
۲. دانشیار، گروه علوم سیاسی و روابط بین‌الملل، دانشگاه فردوسی مشهد، مشهد، ایران.

مقدمه

برای بیش از دو دهه، اینترنت نقشی بسیار مهم و درخور توجه در ارتباطات جهانی بازی کرده و به شکلی فزاینده با زندگی همه انسان‌ها در سرتاسر جهان پیوند یافته است. نوآوری‌ها و هزینه پایین در این عرصه کاربرد اینترنت را افزایش داده است به‌طوری که امروزه، این فناوری بیش از ۳ میلیارد کاربر در جهان دارد. پرواضح است که بیشتر فعالیت‌های اقتصادی، تجاری، فرهنگی، اجتماعی و... در تمام سطوح فردی، دولتی و غیردولتی، در بستر فضای سایبر صورت می‌گیرد. لذا این گستردگی فضای سایبر، شرایطی را برای رشد تهدیدات و خطرات آن نیز فراهم کرده است. در کنار ابعاد مثبت این فناوری، شاهد سوءاستفاده از آن علی‌الخصوص در حوزه امنیت ملی هستیم تا جایی که امنیت سایبری، به عنوان بخش مهمی از امنیت کشورها، جایگاه ویژه‌ای یافته است. برای مثال، یک حمله سایبری می‌تواند همه بخش‌های حیاتی و مهم یک کشور را شدیدا تحت تاثیر قرار دهد. مواردی همچون سرقت اطلاعات، آسیب به زیرساخت‌ها و اخلال در عملکرد سازمان‌ها و بخش‌های متصل به اینترنت، تنها بخشی از این تهدیدات به شمار می‌آیند (لیو و لی[1]، ۲۰۲۱: ۸۱۷۶-۸۱۷۷).

در این میان آمریکا به عنوان کشور مبدع اینترنت و فضای سایبر جایگاه ویژه‌ای دارد. بررسی اقدامات رؤسای جمهور آمریکا نشان می‌دهد که از زمان ظهور وسایل ارتباطی، به ویژه اینترنت موضوع امنیت اطلاعات و امنیت ملی نیز برجسته‌تر می‌گردد. پس از آن تمامی رؤسای جمهور در دوران ترومن، کارتر، ریگان، بوش پدر و کلینتون فرامین ریاست جمهوری مختلفی را برحسب شرایط و زمان، برای حفظ حوزه ارتباطات و فضای سایبر صادر نموده‌اند (آرشیو امنیت ملی[2]، ۲۰۱۸). در دوران ریاست جمهوری ریگان، کنگره این کشور رؤسای جمهور را موظف کرد که بعد از انتخابات ریاست جمهوری استراتژی امنیت ملی خود را ارائه دهند. بعد از این تصمیم، رؤسای جمهور آمریکا بعد از انتخاب شدن، سندی را تحت عنوان *استراتژی امنیت ملی* منتشر می‌نمایند(عبدالله خانی، ۱۳۸۳: ۳۴).

در حال حاضر و طبق استراتژی‌های سایبری ایالات متحده، فرصت‌ها و چالش‌های زیادی در فضای سایبر ایجاد شده است و امنیت این کشور به نحوه استفاده و واکنش نسبت به این فرصت‌ها

1. Liu And Li
2. National Security Archive

و چالش‌ها بستگی دارد. از آنجایی که زندگی روزمره انسان‌ها در همه ابعاد به فناوری سایبر ارتباط پیدا کرده است، حفظ امنیت ملی و زندگی شهروندان از اولویت‌های این کشور به‌شمار می‌آید. از این رو، هر دولتی در آمریکا می‌بایست بر اساس تغییر و تحولات این عرصه، اقدامات مختلفی را جهت حفظ کشور انجام دهد. آمریکا معتقد است که فناوری سایبری در کنار محاسن خود، زمینه ساز سواستفاده برخی بازیگران دولتی (به‌ویژه روسیه، چین، ایران و کره شمالی) و غیردولتی نیز شده که هر کدام بر طبق منافع خود تلاش دارند تا نهایت استفاده را از این عرصه داشته باشند. با این اوصاف، شناسایی خطرات، راه‌های مقابله با آن‌ها و نیز نقاط ضعف و آسیب‌پذیری‌های این کشور، در استراتژی‌های مربوط به امنیت، جزء وظایف دولت آمریکا می‌باشد (استراتژی امنیت ملی[1]، ۲۰۱۸: ۲-۱).

بر این اساس می‌توان گفت از دوران ریاست جرج بوش پسر تا کنون تغییراتی که در امنیت ملی این کشور صورت گرفته و امنیت سایبری به یکی از ابعاد مهم آن بدل گردیده است، به‌طوری که در هر دوره شاهد تفاوت‌هایی در استراتژی های امنیت سایبری این کشور هستیم. از این‌رو، در این پژوهش نشان داده شده که نوع سیاست و استراتژی رؤسای جمهور آمریکا در قبال این‌گونه تهدیدات از چه ویژگی‌هایی برخوردار بوده است. در مقام پاسخ به این سؤال نیز، مشخص می‌شود که استراتژی سایبری آمریکا در دوران بوش، حالتی تدافعی و حاشیه‌ای داشت، در دروان اوباما به سمت گسترش و توسعه‌ی داخلی و بین‌المللی رفت و نهایتا در دوران ریاست ترامپ، علنا رویکردی تهاجمی برای آن اتخاذ شد و به شکلی تخصصی بر کشورهای رقیب آمریکا یعنی روسیه، چین، ایران و کره شمالی و همچنین تروریست‌ها توجه شد. این تحقیق در چارچوب مفهوم امنیت ملی و بعد امنیت سایبری آن با رویکرد توصیفی انجام گرفته و با استفاده از اطلاعات اسناد بالادستی آمریکا، مانند استراتژی‌های امنیت ملی، امنیت سایبری، دفاع ملی و نظامی و همچنین منابع کتابخانه‌ای، و مقالات اینترنتی تهیه شده است.

پیشینه پژوهش

به‌طورکلی در خصوص پیشینه این مقاله باید گفت که پژوهش‌هایی که صریحا بررسی استراتژی‌های امنیتی رؤسای جمهور آمریکا در عرصه سایبری بپردازند بسیار محدود می‌باشد و

1. National Cyber Strategy

عمده تحقیقات بر اساس رابطه سیاست خارجی و امنیت سایبر و اهمیت فناوری‌های سایبری است. با این حال به برخی از مقالات مهم‌تر اشاره می‌شود.

مقاله‌ی *تکنولوژی و امنیت ملی؛ ایالات متحده در یک تقاطع بحرانی*[1]، از وارتون و کادک[2] (۲۰۱۸) به دوران ریاست جمهوری ترامپ تمرکز دارند و به بحث امنیت ملی و تکنولوژی سایبری می پردازند. نویسندگان معتقدند که توسعه فناوری و رشد آن در ابعاد مختلف، قطعا برای حفظ امنیت ملی کشورها در جهان امروز مهم است. سمران آر میکر[3] (۲۰۱۷) در پژوهشی با نام *جبهه دفاعی جدید: فضای سایبر و سیاست خارجی آمریکا*[4]، به قدرت گرفتن سایر کشورها در عرصه سایبری اشاره می کند و تهدیدات آن ها را علیه آمریکا مورد بررسی قرار می‌دهد. وی عملکرد این کشور را در قبال این گونه تهدیدات و از نگاهی تدافعی نشان می‌دهد.

در پژوهشی دیگر در مرکز مطالعات رند[5] و وزارت دفاع آمریکا تحقیقی با عنوان *اعلام توانمندی های حمله سایبری*[6] از مارتین سی لیبیکی[7] (۲۰۱۳) منتشر شد. این اثر به توانایی‌های نظامی این کشور درعرصه سایبری می‌پردازد و با بررسی اسناد مربوطه به اهمیت بازدارندگی در این عرصه اشاره می کند. ویلیام کی تیرل[8] (۲۰۱۲)، در مقاله‌ی *استراتژی امنیت سایبر آمریکا، سیاست و سازمان*[9]، به بررسی اسناد مربوط به عرصه سایبری از دوران ریاست جمهوری کلینتون تا اوباما می‌پردازد. تمرکز اصلی وی در این پژوهش به ابعاد تخصصی این اسناد مربوط می‌شود.

اما در این مقاله، سیاستگذاری‌ها و تغییرات در دوران ریاست جمهوری بوش، اوباما و ترامپ بررسی شده و تغییر در استراتژی‌های سایبری هر دوره بر اساس برخی از اسناد مربوط به آن را نشان داده می‌شود. باید گفت که در این زمینه منبع مشابهی که صریحا به موضوع پیشنهادی این مقاله با این محوریت اشاره کند به چشم نمی‌خورد. لذا با بررسی کیفی محتوای اسناد مربوط به

1. Technology And National Security : The United States At A Critical Crossroads
2. Wharton And Kadtke
3. Simran R Maker
4. New Frontier In Defense: Cyberspace And U.S. Foreign Policy
5. Rand Institute
6. Brandishing Cyberattack Capabilities
7. Martin C. Libick
8. Wiliam K. Tirrel
9. Nited States Cybersecurity Strategy, Policy, And Organization: Poorly Postured To Cope With A Post-9/11 Security Environment?

امنیت ملی و سایبری آمریکا در دوران‌های مختلف ریاست جمهوری این کشور، به این تغییرات اشاره گردیده به‌طوری که بر طبق آن می‌توان این روند را با توجه به شرایط هر دوره ارزیابی نمود.

روش‌شناسی پژوهش

در بخش مربوط به روش شناسی این پژوهش، به تحلیل محتوای کیفی اسنادی همچون استراتژی امنیت سایبری، استراتژی نظام، استراتژی دفاع ملی، امنیت ملی و فرامین ریاست جمهوری اشاره می‌شود. تحلیل محتوا در واقع یک تکنیک پژوهشی برای ایجاد تفاسیر معتبر از متن براساس زمینه کاربرد آن‌ها می‌باشد. این روش شامل روندهای تخصصی بوده و بینش تازه‌تری را به خواننده منتقل کرده و فهم محقق را از یک پدیده خاص افزایش می‌دهد (کریپندروف[1]، ۲۰۰۴: ۱۸). جایگاه تحلیل محتوا در پژوهش‌ها و الگوهای ارتباطی مشخص می باشد. در بین عناصر ارتباط، محتوای پیام اهمیت خاصی دارد. این روش در زمینه‌های گوناگون مانند جامعه شناسی، روانشناسی، تاریخ و علوم سیاسی مورد استفاده است. با این روش می‌توان مقایسه تطبیقی را بین پیام‌های تولید شده در یک مقطع یا زمان‌های گوناگون انجام داد (بدیعی، ۱۳۸۰: ۶-۷). از این رو در این پژوهش با استفاده از همین روش به بررسی اسناد مربوطه پرداخته شده و در انتها با مقایسه آن‌ها، ویژگی سیاستگذاری‌های سایبری رؤسای جمهور آمریکا مطرح می‌گردد. در بررسی محتوای کیفی اسناد نیز با انتخاب واژه سایبری و مشتقات آن همچون امنیت سایبری، حملات سایبری، فضای سایبر و... به کدگذاری باز، اشباع مفاهیم و سپس کدگذاری محوری جملات مربوطه پرداخته شده و با انتخاب مقوله های مناسب، تحلیل محتوای آن‌ها بصورت داده بنیاد صورت پذیرفته است.

چارچوب مفهومی امنیت ملی(بعد امنیت سایبری)

چارچوب در نظرگرفته شده برای این پژوهش، امنیت ملی و در واقع بعد سایبری آن می‌باشد. همانطور که می‌دانیم امنیت ملی عبارتی بود که بعد از پایان جنگ جهانی دوم، ابداع شد تا توصیف‌کننده‌ی حوزه‌ای از سیاست عمومی باشد که معطوف به صیانت از استقلال و آزادی عمل دولت است (شیهان، ۱۳۸۸: ۱۸). اما با گذشت زمان ابعاد جدیدی از امنیت مطرح شد. همان‌طور

1. Krippendroff

که باری بوزان سابقا به آن اشاره کرد، مفهوم امنیت دارای ابعاد گوناگونی است و با توجه به تغییر و تحولات و افزایش سطح روابط میان کنشگران نظام بین‌الملل، تهدیدات جدیدی به غیر از تهدیدات صرفا نظامی پیش روی جهان قرار گرفته است (بوزان، ۱۳۷۸: ۴۰۴-۴۰۵). شرایط امروز فناوری‌های نوین، امنیت سایبری را در کنار سایر ابعاد امنیت جای داده است و به خطرات آن به عنوان ابزاری برای نبرد میان کشورها اشاره می‌کند. خطرات این عرصه جدید در امنیت ملی، موضوعی است که دارای اهمیت زیادی می‌باشد. زیرا تمامی بخش‌های مهم کشور به این فناوری وابسته است. لذا اخلال در امنیت سایبری یعنی اخلال در روند امنیت کشور. به‌علاوه این‌که بازیگران تازه‌ای نیز در این عرصه وارد شده اند که هر کدام براساس منافع خود از این فناوری استفاده می‌کنند و امکان گسترش خطرات سایبری نیز به امری رایج تبدیل شده است (استراتژی امنیت ملی[1]، ۲۰۱۷: ۱۲). از این‌رو، کارشناسان تهدیدات سایبری را در دسته‌بندی‌های مختلفی قرار می‌دهند. اما به‌طورکلی چهار نوع تهدید سایبری در مقابل امنیت ملی وجود دارد که عبارتند از: جنگ سایبری، جرایم سایبری، تروریسم سایبری و جاسوسی سایبری (لرد و شارپ، ۱۳۹۲: ۹۶) که به ترتیب معرفی می‌شوند.

الف) *جنگ سایبری*[2]: جنگ سایبری بالاترین سطح و پیچیده‌ترین نوع از حمله سایبری به شمار می‌آیند که برضد منافع سایبری ملی کشورها صورت می‌گیرد و عواقب سنگینی را برای کشور هدف دارد (لیو و لی، ۲۰۲۱: ۸۱۷۸)

ب) *جرایم سایبری*[3]: مجموعه اقداماتی که با انگیزه‌های مجرمانه و به صورت عمدی علیه شهرت یک فرد یاگروه و یا به منظور آسیب فیزیکی و روانی، از طریق شبکه های ارتباطی مدرن مثل اینترنت به صورت مستقیم یا غیرمستقیم انجام می‌شود (جیانتاس و سرجیو[4]، ۲۰۱۸: ۴).

پ) *تروریسم سایبری*[5]: سایبر تروریسم یا تروریسم سایبری، نوعی از جرایم سایبری بوده که عنصر اصلی آن ترور می‌باشد. حمله‌ی یک تروریست سایبری، باعث وحشت و حس نا امنی شدید می‌شود و ویژگی عمده ی آن اهداف سیاسی عاملان افراط گرای آن است

1. National Security Strategy
2. Cyber war
3. Cyber crimes
4. Giantas and Srergiou
5. Cyber terrorism

(جیانتاس و سرجیو[1]، ۲۰۱۸: ۵-۴). در معنای دیگر، استفاده تروریست ها از هرگونه فناوری های اطلاعاتی را، سایبر تروریسم گویند(بیدا و هالاوی[2]، ۲۰۱۵: ۳۷).

ت) *جاسوسی سایبری*[3]: جاسوسی سایبری به اقداماتی گفته می‌شود که با هدف کسب اسرار از افراد، دولت‌ها، دشمنان، شرکت ها و رقبا به منظور بهره‌برداری های سیاسی، اقتصادی و سیاسی و با استفاده از فضای سایبر انجام می‌شود. در تعریف دیگری هم جاسوسی سایبری را به‌دست آوردن اطلاعات سری بدون اجازه‌ی مالک آن معنا می کنند. این مالک می تواند فرد، دولت، شرکت یا هر بازیگر دیگری باشد (صدیق، ۱۳۹۵: ۸۰).

یافته‌های پژوهش

۱. سیاست امنیت سایبری در سه دوره‌ی بوش، اوباما و ترامپ

در ابتدا باید خاطر نشان کرد که اسناد مختلفی مربوط به فضای سایبر و امنیت ملی در آمریکا وجود دارد. این اسناد در رابطه با امنیت ملی، در دوران ریاست هر رئیس جمهوری در آمریکا منتشر می‌شوند که همه‌ی آن‌ها بخشی را به بحث چالش‌ها و سیاست‌های مرتبط با فضای سایبر اختصاص داده‌اند. این اسناد اصلی شامل استراتژی امنیت ملی (ان. اس. اس)[4]، استراتژی دفاع ملی (ان. دی. اس)[5]، استراتژی نظامی ملی (ان ام اس)[6] و سند بازنگری دفاعی چهار ساله (کیو دی آر)[7] می‌باشند(دیل[8]، ۲۰۱۳: ۹-۳). به غیر از موارد ذکر شده، استراتژی‌های دیگری هم مثل فرمان‌های ریاست جمهوری و سایر طرح‌هایی نظیر *طرح ملی برای حفاظت سیستم های اطلاعاتی*[9] هم در درک سیاست امنیت سایبری آمریکا مؤثر هستند (تیرل، ۲۰۱۲: ۲۰).

---

1. Giantas and Srergiou
2. Beida and Halawi
3. Cyber epionage
4. National Security Strategy (NSS)
5. National Defense Strategy (NDS)
6. National Military Strategy (NMS)
7. Quadrennial Defense Review (QDR)
8. Dale
9. National Plan for Information Systems Protection (NPISP)

از آنجایی که اسناد استراتژی امنیت ملی، دفاع ملی، نظامی به موضوعات مختلفی هم چون خطرات هسته‌ای، بیولوژیکی، مسائل اقتصادی و ... نیز اشاره می‌کنند و امنیت سایبری تنها بخشی از این استراتژی‌ها می‌باشد، لذا در تحلیل آن‌ها صرفاً بخش‌ها و پاراگراف‌های مربوط به موضوع سایبری مورد تحلیل قرار گرفت و با انتخاب کلمه سایبر و مشتقات آن همچون امنیت سایبری، حمله سایبری و ... بررسی اسناد صورت پذیرفت. اسناد امنیت سایبر و فرامین ریاست جمهوری نیز به صورت کامل بررسی شد که در مجموع ۱۳ سند مورد بررسی و تحلیل قرار گرفت و در سه دوره ریاست جمهوری، در جدول شماره (۱) دسته‌بندی شده است. بررسی اسناد مربوط با انجام کدگذاری اولیه، کدگذاری محوری و انتخاب زیرمقوله‌ها و سپس مقوله‌های اصلی و سرانجام اجرا و تحلیل آنها صورت گرفته است.

جدول شماره ۱. کدگذاری و مقوله‌یابی

رئیس‌جمهور	سند	برچسب‌ها	مقوله	مقوله اصلی
۱.جرج دبلیو بوش	۱. استراتژی سایبری ملی ۲۰۰۳	– اهمیت تقویت و ایمن‌سازی زیرساخت‌های اساسی – ضرورت شناخت بازیگران خطرناک سایبری – همکاری و هماهنگی بین ارگان‌های مربوطه – آگاه‌سازی و آموزش مردم و نهادها – ضرورت شناخت و مقابله با فناوری‌های جدید در حوزه سایبر – دفاع و جلوگیری از حملات و کاهش آسیب‌ها – رفع نقاط ضعف	– ایمن سازی داخلی – همکاری نهادها – ضرورت شناخت و آگاهی – جلوگیری و کاهش خطرات	تامین امنیت و دفاع سایبری برای کاهش تهدیدات
	۲. استراتژی امنیت ملی ۲۰۰۶	– خطرات بازیگران سایبری – خطرات فناوری‌های جدید برای امنیت آمریکا	– بازیگران سایبری – امنیت آمریکا	تامین امنیت علیه تهدیدات سایبری

رئیس‌جمهور	سند	برچسب‌ها	مقوله	مقوله اصلی
۱.جرج دبلیو بوش	۳. استراتژی دفاع ملی	در دوره وی این استراتژی تدوین نشد.		
	٤. استراتژی نظامی ۲۰۰٤	– تامین امنیت مشترک – تنوع و گستردگی تهدیدات سایبری و بازیگران آن – اهمیت نقش بازدارندگی	– امنیت مشترک – بازیگران خطرناک سایبری – اقدامات حفاظتی	تامین امنیت و دفاع سایبری علیه تهدیدات
	۵. استراتژی بین‌المللی سایبری	در دوره وی این استراتژی تدوین نشد.		
	٦. فرمان ریاست جمهوری ان اس پی دی ٥٤[1]	– شروع بررسی ابعاد فناوری سایبری – برنامه ریزی و آغاز به کار ارگان‌های مختلف برای مقابله با تهدیدات سایبری – هماهنگی و تعیین دستور کار مقامات مربوطه	– طرح ریزی سایبری – هماهنگی ارگان‌ها – تهدیدات سایبری	تامین امنیت علیه تهدیدات سایبری
۲. باراک اوباما	۱. استراتژی امنیت سایبری	در دوره ریاست وی، این استراتژی تدوین نشد.		
	۲. استراتژی امنیت ملی ۲۰۱۰	– استراتژی‌های جدید برای مقابله با چالش‌های شبکه سایبری – لزوم ایجاد بازدارندگی – آسیب پذیری بخش‌های مختلف نسبت به فناوری سایبری – آمادگی آمریکا برای مقابله با استفاده دشمنان از	– استراتژی‌های جدید – همکاری داخلی و بین‌المللی – تهدیدات سایبری	تقویت توان سایبری و همکاری همه جانبه

1. NSPD54

رئیس‌جمهور	سند	برچسب‌ها	مقوله	مقوله اصلی
۲. باراک اوباما	۲. استراتژی امنیت ملی ۲۰۱۰	فضای سایبر – ابعاد مثبت و منفی این فناوری – گستردگی و تنوع بازیگران و خطرات سایبری – ضرورت افزایش آگاهی و دانش سایبری برای همگان – همکاری‌های بین المللی برای افرایش امنیت و مقابله با مجرمین سایبری – ایجاد قانونمندی جدید برای همکاری جهانی برای کاربرد مناسب از شبکه‌های دیجیتال	– نقاط ضعف و قوت	
	۳. استراتژی دفاع ملی۲۰۰۸	– آمادگی و واکنش به انواع تهدیدات به ویژه سایبری – خطر سایبری بازیگران غیردولتی – خطر بازیگران مختلف علیه آمریکا – رشد همه جانبه رقبای سایبری آمریکا	– خطر بازیگران سایبری – آمادگی همه جانبه	تقویت توان سایبری
	٤. استراتژی نظامی۲۰۱۱ و ۲۰۱۵	:۲۰۱۱	:۲۰۱۱	:۲۰۱۱
		– ضرورت همکاری داخلی و بین‌المللی	– همکاری همه جانبه	تقویت توان سایبری و همکاری همه جانبه ۲۰۱۵
		– توجه به بازیگران جدید متخاصم	– بازیگران متخاصم سایبری	

رئیس‌جمهور	سند	برچسب‌ها	مقوله	مقوله اصلی
۲. باراک اوباما	٤. استراتژی نظامی ۲۰۱۱ و ۲۰۱۵	۲۰۱۱: – برنامه‌ریزی همه‌جانبه برای رفع نقاط ضعف – خطر بروز حمله سایبری –کنترل کشورهای متخاصم	۲۰۱۱: – طرح ریزی جدید – آسیب‌ها و خلاءها	۲۰۱۱:
		۲۰۱۵: – نگرانی شدید از رشد تهدیدات نوین سایبری و قدرت گرفتن رقبا – اهمیت آمادگی و مشارکت همه بخش‌ها – راه اندازی بخش‌های جدید و تدوین سیاستگذاری‌های به روز – همکاری مشترک داخلی و خارجی	۲۰۱۵: – رشد تهدیدات نوین سایبری – آمادگی همه جانبه – سیاستگذاری‌های جدید	۲۰۱۵: تقویت توان سایبری با سیاستگذاری جدید و همکاری همه جانبه
	۵. استراتژی سایبری بین‌المللی ۲۰۱۱	–ضرورت توسعه اینترنت –اهمیت حفاظت داخلی و بین المللی –لزوم همکاری بین‌المللی برای تدوین هنجار و قوانین سایبری –بهره‌گیری از فضای‌سایبر برای پیشرفت در همه زمینه‌ها و برای همه کشورها –ضرورت مقابله با مجرمین و تهدیدات سایبری به صورت بین‌المللی	–توسعه فضای سایبر برای پیشرفت –تدوین قوانین داخلی و بین‌المللی سایبری –همکاری جهانی برای دفع تهدیدات سایبری –تقویت امنیت سایبری از طریق همکاری و مشارکت	همکاری ومشارکت برای استفاده بهینه و تامین امنیت سایبری

رئیس‌جمهور	سند	برچسب‌ها	مقوله	مقوله اصلی
۲. باراک اوباما	٦. فرمان ریاست جمهوری پی پی دی ۲۰[1]	– ناکارامدی سیاست های دولت‌های قبل – اراده ابعاد جدید تدافعی و تهاجمی از فناوری سایبری – اهمیت نقش رئیس جمهور برای اجرای عملیات سایبری – افزایش حساسیت نسبت به حملات سایبری – ابلاغ دستورالعمل های لازم برای عملیات سایبری	–ناکارامدی و ضعف رویکرد دفاعی و تهاجمی –سیاستگذاری جدید –نقش رئیس جمهور –همکاری همه جانبه	سیاستگذاری جدید و همکاری همه جانبه
۳. دونالد ترامپ	۱. استراتژی سایبری ملی۲۰۱۸	– رشد بازیگران جدید سایبری – لزوم قانونگذاری داخلی و بین المللی – ضرورت مبارزه و واکنش به حملات سایبری – اهمیت نظارت و ایمن سازی داخلی – استفاده از تمام ابزارهای لازم برای واکنش به حملات – همکاری داخلی و بین‌المللی برای نفوذ سایبری آمریکا	–خطر بازیگران متخاصم –مبارزه سایبری –ایمن سازی داخلی –همکاری سایبری	تقویت توان سایبری برای واکنش و نبرد سایبری
	۲. استراتژی امنیت ملی۲۰۱۷	– گسترش فعالیت‌های خصمانه – بازیگران دولتی وغیر دولتی	–تهدیدات جدید سایبری – بررسی آسیب‌ها و نقاط ضعف	تقویت توان سایبری همه جانبه برای واکنش و نبرد

1. PPD 20

رئیس‌جمهور	سند	برچسب‌ها	مقوله	مقوله اصلی
۳. دونالد ترامپ	۲. استراتژی امنیت ملی۲۰۱۷	– وجود تهدید برای ارزش‌های داخلی وجهانی – اشکال جدید درگیری‌های مدرن در قالب حملات سایری – آمادگی همه جانبه آمریکا برای ترمیم خلاء ها و نقاط ضعف – ضرورت تقویت شناسایی حملات و واکنش سریع به آن‌ها – تقویت همگرایی همه مسئولان مربوطه – ارتقای ابزارهای لازم حقوقی و اطلاعاتی برای نبرد سایبری	– آمادگی همه جانبه – واکنش سریع به تهدیدات	سایبری
	۳ .استراتژی دفاع ملی۲۰۱۸	– بازیگران جدید سایبری من جمله تروریست‌ها – اهداف بدخواهانه بازیگران متخاصم سایبری برای ضربه به آمریکا – ضرورت واکنش به نبردها و حملات سایبری – اهمیت شتاب گیری در نوسازی – برنامه‌های جدید و اختصاص بودجه برای پیش‌گیری از تهدید رقبا – سرمایه‌گذاری در همه بخش‌های مختلف برای	– تشدید تهدیدات سایبری بازیگران متخاصم – عملیات واکنشی نظامی سایبری – توسعه سایبری همه جانبه	تقویت توان سایبری نظامی برای واکنش علیه تهدیدات سایبری
		بهره‌گیری از توانایی سایبری در عملیات نظامی		

رئیس‌جمهور	سند	برچسب‌ها	مقوله	مقوله اصلی
	٤. استراتژی نظامی ملی ۲۰۱۸	– اهمیت افزایش هوشیاری در مورد تهدیدات کشورهای متخاصم – لزوم بررسی نقاط ضعف و خلاءها – تاسیس ارگان‌های موردنیاز برای هماهنگی در نبرد سایبری	– افزایش آگاهی سایبری – نقاط ضعف وآسیب‌ها – طرح ریزی جدید سایبری	تقویت توان سایبری برای مبارزه
	۵. استراتژی سایبری بین المللی	در دوره وی این استراتژی تدوین نشد.		
	٦. فرمان ریاست جمهوری	این استراتژی هنوز از رده فوق سری خارج نشده و اصل سند در هیچ‌جا در دسترس نیست. اما تحلیل‌ها، رویکرد حاکم بر این فرمان را تهاجمی ذکر کرده‌اند که در متن مقاله به منابع آن اشاره می‌گردد.		

در ادامه رویه و عملکرد هرکدام از رؤسای جمهور آمریکا به ترتیب در دوران ریاست جمهوری جرج بوش، باراک اوباما و دونالد ترامپ را مطرح می‌شود.

۱.۱ سیاست سایبری دوران جرج دبلیو بوش

در ابتدا باید گفت که پیشرفت‌هایی که در دوران ریاست جمهوری بیل کلینتون در عرصه سایبری انجام شد، در دوران بوش بشدت کاهش یافت و در واقع سرعت این پیشرفت ها کم گردید. کلینتون به مسائل مختلف امنیتی توجه می کرد، ولی دولت بوش بیشتر درگیر اقدامات ضد تروریستی و مسائل مربوط به جنگ عراق و افغانستان بود. با این وجود مسائل سایبری به طورکامل از دستور کار استراتژی ملی آمریکا حذف نشد و پیشرفت‌هایی هر چند اندک در ادامه‌ی مسیر کلینتون انجام گرفت و تمام اسناد استراتژیک ملی دولت قبل را به روز رسانی شد (تیرل، ۲۰۱۲: ۳۵-۳۶).

سال ۲۰۰۲: آنچه که در این سال باعث شد تا انگیزه برای تغییرات سازمانی گسترده در وزارت دفاع فراهم شود و بر توانایی ارتش برای اقدام کردن و دفاع در برابر جنگ سایبری موثر باشد، حملات تروریستی به سازمان تجارت جهانی و پنتاگون در سال ۲۰۰۱ بود (جانشکی و

کلاریک، ۱۳۸۹: ۳۹۴) اما باید گفت که در استراتژی امنیت ملی (۲۰۰۲) که بر بحث تروریسم متمرکز بود اشاره‌ای به فضای سایبر نشد (تیرل، ۲۰۱۲: ۳۷).

سال ۲۰۰۳: در این سال اقدامات دیگر در دولت بوش صورت گرفت. در فرمان ریاست جمهوری ۶۸، بیل کلینتون رئیس‌جمهور قبل از بوش، دستور حفظ کشور را در مقابل حملات سایبری صادر کرده بود که جرج بوش این تصمیم را با استراتژی امنیت سایبری (۲۰۰۳) توسعه داد. تمرکز اصلی این استراتژی بر کاهش آسیب‌پذیری آمریکا در برابر تهدیدات سایبری قبل از هرگونه ضربه به سیستم‌های این کشور است. وزارت دفاع، وزارت دادگستری، اداره تحقیقات فدرال، جامعه اطلاعاتی و سایر آژانس‌های مرتبط، سازمان‌ها و بخش‌هایی را برای تعامل با مسائل فضای سایبر و نقش‌های مرتبط با ماموریت‌های حفظ امنیت ملی تاسیس کردند. وزارت امنیت داخلی به طور ویژه به بحث مقابله با حملات تروریستی سایبری پرداخت و در این سال واحد امنیت سایبری ملی خود را راه اندازی نمود (راتاری[1] ۲۰۰۹: ۲). اما باید گفت که بوش تحت تأثیر حادثه ۱۱ سپتامبر قرار داشت و اندیشه‌ی ضد تروریسم آن راهنمای تنظیم استراتژی امنیت سایبری بود (یانگ[2]، ۲۰۱۶: ۲۱۰).

به‌طورکلی گرچه سیاستگذاری‌هایی در حوزه‌ی امنیت سایبری انجام گرفت ولی مسئولیت آژانس‌ها و نهادهای مختلف مربوط به این عرصه، دارای ابهام و محدودیت بودند (هاوری[3]، ۲۰۱۶: ۱۰-۹). با توجه به این که تمرکز اصلی دولت بوش بر مقابله با تروریسم بین‌المللی و داخلی بود، حفاظت از زیرساخت‌های حیاتی را از زاویه‌ی مقابله با تروریسم می‌دید. اما روی هم رفته، پیشرفت نامتوازنی را در این حوزه وجود داشت و سایر اسناد استراتژیک نیز منسجم و هماهنگ نبودند (تیرل، ۲۰۱۲: ۱۰۱-۱۰۲). به‌طوری که مایکل هیدن[4] رئیس سابق سازمان سیا در دوران ریاست جمهوری جرج بوش گفت: «سایبر آنچنان با سرعت حرکت می‌کند که ما همیشه در سیاست‌گذاری، از آن یک قدم عقب تر هستیم» (آذری، ۱۳۹۱: ۲۱۸).

---

1. Rattary
2.Yang
3.Harvey
4. Michael Hayden

۲.۱ سیاست سایبری دوران باراک اوباما

با روی کار آمدن باراک اوباما، طرح‌ها و برنامه‌های زیادی با توجه به تحولات فناوری سایبری مطرح شد. وی اهداف متعددی برای حفظ امنیت سایبری آمریکا درنظر داشت و اقدامات بیشتری نسبت به جرج دبلیو بوش انجام داد. بررسی اقدامات وی نشان می‌دهد که او در زمینه حل مشکلات سایبری این کشور بسیار فعال بود و از تمام راه‌های قانونی ممکن برای توسعه سیاست‌های مرتبط با این حوزه بهره گرفت. با این وجود آمریکا در دروان ریاست وی ضربات امنیتی بدی مانند حمله سایبری روسیه در انتخاب ریاست جمهوری سال۲۰۱۶، جاسوسی‌های اقتصادی چین و چندین مورد هک سازمانی را متحمل شد (موسسه امنیت دیجیتال سی اس او[1]، ۲۰۱۷). با این حال اقدامات مثبتی نیز در جهت تغییر در این حوزه و محیط امنیتی داخلی و بین‌المللی صورت گرفت. همان‌طور که فضای سایبر به منبع مهم تهدید برای امنیت ملی آمریکا تبدیل شده بود، جایگاه استراتژی امنیت ملی در اسناد مرتبط به آن هم افزایش یافت (یانگ، ۲۰۱۶: ۲۱۰). یکی از دلایلی که دولت اوباما به سمت به‌روز رسانی استراتژی خود کرد، این بود که آنچه تاکنون انجام گرفته است را کافی نمی‌دانست. از این‌رو، نیاز بود وزارت امنیت داخلی و شورای امنیت ملی که نه فقط برای پیشگیری، سازمان یابند بلکه باید آمادگی واکنش سریع به حملات را برای حفظ امنیت ملی داشته باشند. لذا حفظ شهروندان و امنیت کشور در حوزه‌ی سایبری به‌خاطر نامحسوس بودن آن دشوارتر است (استون[2]، ۲۰۱۰: ۴).

سال ۲۰۰۹: در دسامبر این سال دولت اوباما چندین طرح ابتکاری را آغاز کرد. دولت اولین مسئول هماهنگ کننده‌ی امنیت سایبری کاخ سفید را منصوب نمود که *تزار سایبری*[3] لقب داشت، وی فعالیت‌های امنیت سایبری فدرال را هدایت می کرد. اما کنترل مستقیم بر بودجه‌ی آژانس را نداشت و نفوذ آژانس امنیت ملی بسیار بیشتر از آن بود (فیشر[4]، ۲۰۱۴: ۴۵). با تأکید اوباما بر حفظ امنیت ملی به عنوان یکی از اولویت‌های آمریکا، در سیاست ملی و نظامی، بحث بازدارندگی را به

1. CSO (Chief Security Officer)
2. Stone
3. Cyber Czar
4. Fishcer

عنوان یک هدف شناخته شده در برابر دشمنان مطرح کرد (تروجیلو[1]، ۲۰۱۴: ۴۴) ، لذا آمریکا باید از بازدارندگی به عنوان یکی دیگر از استراتژی‌های اقدامات متقابل، در برابر تهدیدات سایبری استفاده کند. بازدارندگی یعنی کشوری دشمن خود را متقاعد می‌سازد که توانایی و قصد پاسخ به نفوذهای سایبر را با استفاده از نیروی نظامی دارد. هدف این‌کار این است که دیگر کشورها را از ارتکاب حملات سایبری باز داشته از عمل متقابل آنها جلوگیری کند (رابنشتاین[2]، ۲۰۱۴: ۶). در واکنش به رشد تهدیدات سایبری، وزارت دفاع نیز بخش تازه‌ای در فرماندهی نظامی را ایجاد کردکه به فعالیت‌های سایبری اختصاص یافته بود. فرماندهی سایبری ایالات متحده اکنون زیر مجموعه فرماندهی استراتژیک آمریکا است که ماموریت آن هدایت عملیات‌ها و دفاع از شبکه‌های اطلاعاتی وزارت دفاع و آماده‌سازی برای عملیات‌های سایبری تمام عیار در تمام حوزه‌ها است (جیکارن[3]، ۲۰۱۸: ۷).

سال ۲۰۱۰: با تأکید وی در مورد اهمیت فضای سایبر در امنیت ملی، سیاست و دکترین برای فضای سایبر و موضوع بازدارندگی به طرز قابل توجهی افزایش یافت و این بازدارندگی در اسناد و استراتژی‌های مختلفی از جمله استراتژی امنیت ملی (۲۰۱۰) به آن پرداخته شد (تروجیلو، ۲۰۱۴: ۴۶). استراتژی بازدارندگی کاخ سفید به دنبال این بود تا اجماعی بین‌المللی را برای واکنش‌های مناسب به حملات سایبری ترتیب دهد. اوباما حتی تلاش کرد در جلسه‌ی سران گروه جی ۲۰ توافقی را برای هنجارسازی در فضای سایبر انجام دهد (کولتون[4]، ۲۰۱۷: ۱۳۱).

در ادامه اقدامات دولت اوباما، طرح ابتکار امنیت سایبری در مارس ۲۰۱۰ منتشر شد. تغییرات و اهداف مهم در این سند عبارت‌اند از: استحکام نقاط دسترسی خارجی به سیستم‌های فدرال، استقرار سیستم‌های حفظ و ردیابی نفوذ، ارتقای اولویت‌بندی و همکاری تحقیق و توسعه فناوری نسل آینده، اشتراک‌گذاری اطلاعات و آموزش و آگاهی بخشی در امنیت سایبری، کاهش خطرات مرتبط با فناوری اطلاعاتی جهانی و شفاف سازی نقش فدرال در حفظ جامعه اطلاعاتی (فیشر، ۲۰۱۴: ۳-۴).

1.Trujillo
2. Rubenstein
3. Jaikaran
4. Kolton

سال ۲۰۱۱: استراتژی نظامی ملی (۲۰۱۱) در این سال بر پایه استراتژی‌های امنیت ملی و سند دفاعی چهارساله تنظیم شد که بر تقویت فضای سایبر به عنوان یک حوزه‌ی جنگی در ارتباط با زمین، دریا و فضا تاکید دارد. ولی در مورد نسبت دادن حمله‌ی خصمانه به دشمنان حرفی نزده و نامی از رقبا نمی‌برد (تیرل، ۲۰۱۲: ۴۱-۴۳). بعد از آن، در جولای ۲۰۱۱، استراتژی وزارت دفاع برای عملیات در فضای سایبر تدوین گردید و شامل پنج ابتکار استراتژیک می‌شد. این ابتکارات عبارتند از: برخورد با فضای سایبر به عنوان یک حوزه‌ی عملیاتی به منظور سازماندهی، آموزش و تجهیز وزارت دفاع به منظور بهره‌برداری کامل از توانایی فضای سایبر، به‌کار بردن جنبه‌های عملیانی جدید برای حفظ شبکه‌ها و سیستم‌های وزارت دفاع، مشارکت با سایر وزارتخانه‌ها و آژانس‌های بخش خصوصی و ایجاد پیوندهای قوی بین متحدین آمریکا و شرکای بین‌المللی برای تقویت فضای سایبری جمعی، تقویت استعداد کشور از طریق نیروی کاری سایبری ویژه و نوآوری‌های فناورانه‌ی سریع (وزرات دفاع آمریکا[1]، ۲۰۱۱). بعد از این تصمیمات این وزارت خانه، فرماندهی سایبری خود را گسترش داد و تعداد کارکنان این بخش را پنج برابر و به نزدیک ۵۰۰۰ نفر رساند(سیگام[2]، ۲۰۱۶: ۳).

موضوع دیگری که در دوران ریاست جمهوری اوباما به آن توجه زیادی شد، موضوع همکاری است. در واقع وی رویکردی چند جانبه در این حوزه داشت و معتقد به همکاری‌های بین‌المللی با شرکای خود به منظور بهبود چالش‌های پیش‌رو بود(فارول و روزینسکی[3]، ۲۰۱۱: ۳۱). در دولت وی، اثرگذاری سیاسی بین‌المللی و ایجاد مکانیسم‌هایی در این حوزه شدت گرفت و دولت آمریکا بر استراتژی امنیت سایبری در سطح بین‌المللی هم تمرکز نمود (یانگ، ۲۰۱۶: ۲۱۰). لذا اولین استراتژی بین‌المللی سایبری(۲۰۱۱) در این سال منتشر شد که نشان داد زیرساخت‌های دیجیتال عصر امروز، تبدیل به ستون فقرات اقتصادهای شکوفا، تحقیقات، ارتش‌های قوی و دولت شفاف شده است(استراتژی بین‌المللی فضای سایبر آمریکا[4]، ۲۰۱۱: ۶-۳).

1. Department of Defense
2. Sigholm
3. Farwell and Rohozinski
4. International Strategy For Cyber Space

سال ۲۰۱۲: اوباما به وزارت دفاع ماموریت دیگری داد تا حفاظت از کشور و آژانس‌های دولتی را در برابر حملات سایبری تقویت کند. لذا استراتژی سایبری وزارت دفاع (۲۰۱۲) بر این نکات متمرکز شد: دفاع از سیستم‌ها، شبکه‌ها و اطلاعات وزارت دفاع، دفاع از منافع ملی و خاک آمریکا در برابر حملات سایبری، فراهم آوری حمایت سایبری برای عملیات‌های نظامی و طرح‌های احتیاطی. بر طبق این استراتژی، وزارت دفاع شروع به ایجاد نیروی ماموریت سایبری (سی. ام. اف)[1] برای اجرای ماموریت‌های سایبری کرد (جیکارن، ۲۰۱۸: ۶-۷).

سال ۲۰۱۳: در دوران ریاست اوباما، سازمان ان. اس. ای. هشدار داد که در طی سال‌های آینده، هکرها توانایی این را خواهند داشت تا کل شبکه‌ی برق این کشور را ازکار بیندازند. این نگرانی باعث شد تا دولت بر روی چندین استراتژی امنیت سایبری جدید کار کند (ترووبیش[2]، ۲۰۱۴: ۳۹). وی از جامعه تکنولوژیک آمریکا هم خواست تا مسیری را برای کمک به اجرای قانون در دستیابی به رمزنگاری اطلاعات و پیشرفت در ارتقای اجرای توانایی‌های تکنولوژیک، توسعه دهد (جیکارن، ۲۰۱۸: ۱۳).

سال ۲۰۱۵: فرمان اجرایی دیگری هم در سال ۲۰۱۵ امضا شد که تحریم‌هایی را بر افراد خاصی که در فعالیت های سایبری بدخواهانه مشارکت دارند، وضع می‌کرد. این فرمان اجرایی، اولین برنامه تحریمی است که به دولت اجازه می‌دهد تا جریمه‌هایی را بر افرادی که در خارج، در حملات سایبری مخرب و جاسوسی‌های تجاری در فضای سایبر مشارکت دارند، اعمال شود. لذا وزارت خزانه‌داری می‌تواند دارایی‌های این افراد را بلوکه کرده و معاملات تجاری آن ها را مسدود کند (جیکارن، ۲۰۱۸: ۲۳). در این سال وزارت دفاع راهبرد جیدید داشت که بر اساس آن، استراتژی بازدارندگی می‌تواند دشمنان را از انجام حملات سایبری باز دارد، عوامل و نقاط حمله را شناسایی کند و آمریکا را قادر به واکنش علیه آن‌ها نماید (رجیستر[3]، ۲۰۱۵: ۱۲).

در واقع نگاه وی استفاده از ابزار سایبری، محتاطانه و محدود بود. حتی زمانی که این کشور از ویروس استاکس نت علیه سیاست‌های هسته‌ای ایران استفاده کرد، وی به شدت نگران عواقب آن بود و بر رویکرد تدافعی در فضای سایبر تأکید داشت (نیویورک تایمز[4]، ۲۰۱۸)، به‌طوری که در

1. Cyber Mission Force (CMF)
2. Trobisch
3. Regester
4. The Newyorktimes

دوران وی، عملیات سایبری تحت قاعده بودند تا تشدید خطرها را محدود سازند و این عملیات در کنار مجموعه اقدامات دیپلماتیک برای هدایت روابط با قدرت‌های بزرگ انجام می شد. برای مثال، این کشور در پاسخ به فعالیت‌های روسیه، ترکیبی از تحریم، رویه‌های دیپلماتیک و فعالیت‌های سایبری را انجام داد و از واکنش میان سازمانی برای هکرهای چین استفاده کرد که شامل عمل متقابل پنهانی و هم دنبال کردن قرارداد برای محدودسازی جنگ اقتصادی سایبری بود(والریانو و جنسن[1]، ۲۰۱۹).

۳.۱ سیاست سایبری دونالد ترامپ

افزایش قدرت رقابتی کشورهای دیگر، تدوین‌کنندگان استراتژی امنیت ملی را به فعالیت وا داشت، زیرا نگرانی‌هایی در خصوص عدم توجه کافی به امنیت ملی در مقایسه با دیگر بازیگران که پیوسته طرح‌های بلندمدتی را برای به چالش کشیدن آمریکا انجام داده و برنامه‌های خود را در تضاد با اهداف آمریکا و متحدانش انجام می‌دهند، وجود داشت (ناکاسون، ۲۰۱۹: ۱۱). در استراتژی امنیت ملی این دوره، آشکارا ازکشورهای روسیه، چین، ایران و کره شمالی به‌عنوان بازیگرانی یاد شده است که از فضای سایبر برای به چالش کشیدن ایالات متحده و متحدین و شرکای آن استفاده می‌کنند (استراتژی سایبری ملی، ۲۰۱۸: ۲). آمریکا حملات سایبری متعددی را به این کشورها نسبت می‌دهد که به چند مورد اشاره می‌شود. برای مثال حملات سایبری معروفی با عنوان باران تایتان[2] و یا نفوذ به آژانس امنیت ملی آمریکا در سال ۲۰۱۶ نمونه‌هایی از تهدیدات چین نسبت به آمریکا می‌باشد (پرلروث، سینگر و شین[3]، ۲۰۱۹). روسیه هم به نفوذ سایبری در انتخابات سال ۲۰۱۶ و چندین حمله سایبری دیگر متهم است (کتس[4]، ۲۰۱۷: ۱). درخصوص ایران نیز، آمریکا چندین حمله سایبری من جمله به بانک‌ها و نهادهای مالی خود را در سال ۲۰۱۱ به این کشور نسبت می‌دهد (فینکل و راثکر[5]، ۲۰۱۲). کره شمالی

1. Valeriano and Jensen
2. Titan Rain
3. Perlroth, Sanger and Shane
4. Coats
5. Finkle and Rothacker

هـم همیشـه جـزء یکـی از مهم‌تـرین تهدیـدات آمریکـا بـه شـمار می‌آیـد. مهم‌تـرین حملـه سـایبری ایـن کشـور بـه آمریکـا پرونـده سـونی پیکچـرز[1] بـود کـه شـامل سـرقت اطلاعـات زیـادی از آمریکـا می‌شد(سـی. ایـی. ای[2]، ۲۰۱۸: ۱۶). درایـن میـان آمریکـا نیـز واکنش‌هـای مختلفـی را نسـبت بـه ایـن حمـلات داشـته اسـت. بـرای مثـال وزارت امنیـت داخلـی قـانونی الزامـی را صـادر نمـود کـه براسـاس آن، تمـام آژانس‌هـای فـدرال بایـد همـه محصـولات شـرکت کاسپراسـکای[3] روسـیه را از سیسـتم‌های خـود حـذف کننـد، چـون احتمـال نفـوذ و جاسوسـی مسـکو از ایـن طریـق وجـود دارد.کنگـره نیـز چنـین لایحـه‌ای را تصـویب نمـود و قـانون منـع اسـتفاده از تجهیـزات ارتبـاطی چـین را، در دسـتگاه‌های دولتـی صـادر کـرد، تـا جـایی کـه کمیسـیون ارتباطـات فـدرال هـم محـدودیت‌هایی را بـرای تجهیـزات مـرتبط بـا شـرکت هـواوی[4] اعمـال نمـود (هانـا و ادنسـیک[5]، ۲۰۱۹: ۸۴). در خصـوص ایـران نیـز بایـد گفـت پـس از افـزایش فعالیت‌هـای سـایبری ایـران و انهـدام پهپـاد آمریکـا در سـال۲۰۱۹، فرمانـدهی سـایبری آمریکـا در منطقـه بـا دسـتور مسـتقیم ترامـپ سیسـتم‌هـای رایانـه‌ای نظـامی مورد استفاده در لانچرهای موشکی ایران را مورد هدف قرار داد (سیمپانو[6]، ۲۰۱۹).

سال ۲۰۱۷: در استراتژی امنیت ملی (۲۰۱۷) در این سال، به تجدید توانایی‌ها و مزیت های رقابتی این کشور اشاره می‌شود و در کنار ابعاد نظامی، هسته‌ای، فضایی و اطلاعاتی، به فضای سایبر هم توجه دارد. این سند به نقش بازیگران دولتی و غیردولتی که از ابزارها و فناوری‌های سایبری برای تقویت و گسترش نفوذ خود استفاده می‌کنند نیز اشاره دارد. سه راهبرد اصلی در این سند برای عملکرد آینده‌ی فضای سایبر آمریکا در نظر گرفته شده است: بهبود توانایی نسبت دادن، مسئولیت و واکنش،ارتقای ابزارها و تخصص سایبری، پیشبرد هماهنگی و سرعت عمل (استراتژی امنیت ملی، ۲۰۱۷: ۳۱-۳۲).

سیاست سایبری دولت ترامپ از اولویت به اجرای قانون، به سمت رویکردی حرکت کرده است که در آن بین اجرای قانون و پرداختن به دشمنان در فضای سایبری و ایجاد بازدارنگی،

1. Sony Pictures
2. CEA
3. Kaspersky
4. Huawei
5 . Hannah and Adesnik
6. Cimpanu

توازن ایجاد کند. مهم‌ترین مفهوم این تغییر جهت در استراتژی سایبری ملی، خودش را در این جمله نشان می‌دهد که دولت آمریکا به دنبال تشخیص هویت، مقابله، ایجاد اختلال، تضعیف و بازدارندگی در فضای سایبر است و با فعالیت‌هایی که منافع ملی این کشور را به خطر می‌اندازد، مقابله می‌کند. از طرفی هم دولت ترامپ، سیاست سایبری فرمان ریاست جمهوری(پی.پی.دی-۲۰)[1] سال ۲۰۱۳ را به ارث برده است. طبق این فرمان سیاست سایبری، آمریکا باید فعالیت‌های لازم برای کاهش تهدیدات و اولویت دادن به دفاع از شبکه‌ها و همچنین اجرای قانون انجام دهد. اما در دوران ترامپ، مقامات ارشد آمریکا ارزیابی‌های تندی را نسبت به رویکرد دولت قبلی نشان دادند. طبق گفته‌های مایک راجرز[2]، فرمانده‌ی آژانس امنیت ملی و فرمانده‌ی سایبری آمریکا، توانایی‌های سایبری این کشور، سرعت و قابلیت کافی در برابر دشمنانش را ندارد و این در حالی است که رقبا و دشمنان آمریکا، نسبت به گذشته بسیار جسورتر شده‌اند، زیرا هیچ مسئولیتی در قبال عواقب فعالیت‌های سایبری خود ندارند. در همین حین که وزارت دفاع در استراتژی سایبری خودش بر بازدارندگی و مبارزه‌ی پیوسته با فعالیت‌های سایبری معاندانه تأکید داشت، به طور همزمان دولت نیز اختیارات جدیدی را برای عملیات‌های سایبری فراهم کرد و فرمان ریاست جمهوری (پی. پی. دی- ۲۰) سابق را ملغی نمود (هانا و ادنسیک، ۲۰۱۹: ۸۳) تا محدودیت‌های مربوط به حمله سایبری را بردارد. این قواعد روند و هماهنگی بین سازمانی پیش از انجام حملات سایبری به ویژه علیه کشورهای متخاصم را تشریح می‌کند (خبرگزاری صدا و سیما، ۱۳۹۷).

این فرمان سایبری جدیدکه با نام *ان اس پی ام ۱۳*[3] شناخته می‌شود، برای حفاظت از آمریکا در مقابل حملاتی شبیه آنچه که در شرکت سونی پیکچرز[4] و یا در فرایند انتخابات ۲۰۱۶، اتفاق افتاد است (بلیک[5]، ۲۰۱۹). منطق این کار این است که فرماندهی سایبری باید اختیار انجام فعالیت در مقایسه با سایر فرماندهی‌های جنگی را داشته باشد (بورگارد و لانجرگان[6]، ۲۰۱۸). زیرا عملیات تهاجمی سایبری می‌توانند ارزش استراتژیک قابل توجهی را برای کشورها ایجاد کنند.

1. Presidential Policy Directive (PPD 20)
2. Mike Rogers
3. National Security Presidential Memorandum (NSPM)
4. Sony Pictures
5. Blake
6. Borghard and Longergan

توانایی تهاجم سایبری می‌تواند گزینه‌های انتخابی رهبران کشورها را در موقعیت‌های زیادی گسترش داده و از لحاظ مادی و روانی تأثیرگذار باشند (اسمیت[1]، ۲۰۱۸: ۹۲).

سال ۲۰۱۸: انتشار سند استراتژی سایبری ملی آمریکا بعد از پانزده سال، به چهار موضوع مهم اشاره می‌کند. اول، حفاظت از مردم، کشور و سبک زندگی آمریکایی از طریق تقویت حفظ زیرساخت‌های حیاتی و مبارزه با جرایم سایبری؛ دوم، ارتقای شکوفایی آمریکا از طریق ایجاد اقتصادی پویا و دیجیتالی؛ سوم، محافظت از صلح از طریق ثبات و بازدارندگی و چهارم نیز افزایش نفوذ آمریکا می‌باشد (استراتژی سایبری ملی، ۲۰۱۸). طبق این سند، ایالات متحده به طور پیوسته، قربانی فعالیت‌های بدخواهانه سایبری است که توسط بازیگران دولتی و غیردولتی، نایبان آن‌ها و تروریست‌ها انجام می‌گیرد. در این راستا، این سند اقداماتی را برای مبارزه با جرایم سایبری در اولویت قرار می‌دهد: ارتقای گزارش‌دهی حوادث و واکنش به آن‌ها، به روز رسانی نظارت الکترونیک و قوانین جرایم کامپیوتری، کاهش تهدیدات از سمت سازمان‌های جنایی فراملی، ارتقای رهگیری مجرمان خارجی، تقویت ظرفیت اجرای قوانین ملی شرکا برای مبارزه با فعالیت‌های سایبری مجرمان (استراتژی سایبری ملی، ۲۰۱۸: ۱۰-۱۱).

وزارت دفاع هم در این سال استراتژی سایبری خودش را منتشر کرد که به ارتش اجازه می‌دهد تا به دنبال برتری اطلاعاتی و ضربه به اهداف تهدیدات‌آمیز باشد. از این‌رو، اشاره می‌کند رقبای آمریکا که شامل تروریست‌ها، مجرمان و دشمنان خارجی اند، از فضای سایبر برای ضربه زدن و سرقت از فناوری‌ها به منظور اخلال در اقتصاد و تهدید زیرساخت‌های آمریکا استفاده می‌کنند. لذا نیاز است از طریق این استراتژی، برتری سایبری آمریکا را حفظ کرده و حملات سایبری را قبل از ضربه به شبکه‌های مختلف دفع نمود. بر این اساس، پنج راهبرد اصلی استراتژی سایبری وزارت دفاع عبارتند از: تشکیل یک نیروی مهلک، مبارزه و بازدارندگی در فضای سایبر، تقویت متحدین و جذب شرکای جدید، اصلاح وزارت خانه، پرورش استعدادها (لانج[2]، ۲۰۱۸).

جان بولتون[3] مشاور امنیت ملی وقت، در توضیح این استراتژی جدید این‌طور گفت که چون دستگاه‌های مختلف امنیتی که بیشترشان در معرض حملات سایبری قرار دارند، در اجرای عملیات

1. Smeet
2. Lange
3. John Bolton

دفاعی و تهاجمی مشروع علیه دیگر کشورها محدودیت داشتند، اما اکنون دونالد ترامپ در عمل محدودیت‌ها را برداشته و عملیات تهاجمی سایبری را مقدور کرده است و دیگر مثل دولت اوباما دست آمریکا در این زمینه بسته نیست (خبرگزاری بی. بی. سی، ۱۳۹۷). در همین سال وزارت امنیت داخلی نیز استراتژی سایبری مجزای خودش را منتشر می‌کند. راهبردهای عملیاتی این سند عبارت‌اند از: شناسایی خطرات، کاهش آسیب پذیری‌ها، کاهش تهدیدات، سبک کردن عواقب و فعال سازی داده‌های امنیت سایبری (وزارت امنیت داخلی آمریکا[1]، ۲۰۱۸).

به‌طورکلی، آنچه که در دوران ریاست جمهوری ترامپ در خصوص تغییر در استراتژی‌های سایبری این کشور رخ داده است، عمدتا حول تقویت سیستم‌های داخلی و رویکردی تهاجمی عمل می‌کند. تغییر در روند برنامه‌ریزی و تصمیم‌سازی نسبت به دورهٔ قبلی، ویژگی بارز در راهبردهای کلان سیاست سایبری این کشور است. دیگر گزینه‌ی حمله‌ی سایبری، موضوعی سری در دستور کار آمریکا نیست و این کشور آشکارا از فضای سایبر به عنوان ابزاری برای سیاست خارجی خود استفاده می‌کند.

با توجه به آنچه تا اینجا بدان پرداخته شد، شباهت‌ها و تفاوت‌هایی در سیاستگذاری‌ها و تدوین استراتژی‌های هر دوره وجود دارد. از آنجایی که فناوری سایبر نسبت به بسیاری از علوم دیگر دارای رشد زیادی است، این موضوع در تمام استراتژی‌ها به آن پرداخته شده و متناسب با آن به موارد به روز و نوینی در همه ارگان‌های مربوطه برمی‌خوریم. یکی دیگر از نقاط تشابه این استراتژی‌ها توجه به ظرفیت‌های داخلی و رقبای آمریکا است که توجه همه جانبه به نقش آنها، موضوعی مهم می‌باشد. از نقاط تمایز این استراتژی‌ها نیز می‌توان به چند مورد اشاره کرد. در دوران ریاست جرج بوش پسر، موضوع فناوری سایبری در وزارت امنیت داخلی متمرکز بود و توجه خاصی به این عرصه در استراتژی‌های امنیت ملی، دفاع ملی، نظامی و بین‌المللی نشد. اما در دوران اوباما، توجه بیشتری را در این زمینه وجود داشت. در این دوره ضمن استفاده از استراتژی‌های دوره قبل، به نوآوری و تنوع بخشی در کاربرد فضای سایبر در همه بخش‌ها توجه شد و تدوین یک استراتژی بین‌المللی نشان از نگاهی گسترده و همکاری‌جویانه به این مسئله داشت. در دوران ریاست ترامپ نیز تمرکز جدی بر تقویت و حفظ امنیت داخلی آمریکا شده و

1. Department of Homeland Security

صریحا صحبت از مقابله تهاجمی با دشمنان سایبری آمریکا شده است. نام بردن از کشورهایی همچون روسیه، چین، کره شمالی و ایران در استراتژی امنیت سایبر، تدوین مجدد این استراتژی بعد از ۱۵ سال، اتخاذ رویکرد تهاجمی بدون نیاز به فرمان رئیس جمهور و کاربرد فناوری سایبری به عنوان یک سلاح از جمله تحولات دوران ترامپ و اهمیت مضاعف این عرصه می‌باشد.

نتیجه‌گیری

همان‌طور که اشاره شد، با رشد سریع فناوری در عرصه‌ی فضای سایبر و گستردگی این حوزه در بسیاری از ابعاد مختلف زندگی، این موضوع به مسئله‌ای حیاتی برای امنیت ملی کشورها تبدیل شده است. تمام کشورها به مسئله‌ی امنیت ملی خود حساسیت ویژه‌ای دارند و با توجه به توسعه سریع فناوری، به دنبال به‌روزرسانی آن هستند. فناوری سایبری یکی از عجیب‌ترین عرصه‌های علمی امروز است که با رشد این فناوری، موضوع امنیت سایبری و ارتباط آن با امنیت ملی کشورها نیز پررنگ‌تر می‌گردد بطوری که به یکی از نگرانی‌های همه کشورها و سازمان‌ها تبدیل شده است. با توسعه این فناوری، نیاز به امنیت سایبری نیز برای همه برجسته‌تر خواهد شد. تهدیدات و خطرات این فناوری همراستا با جنبه های مثبت آن پیش می‌رود و لذا نیاز به طرح‌ریزی و سیاستگذاری برای آن نیز ضروری است. ارتباط این فناوری در کنار هوش مصنوعی، خطرات این فناوری را چند برابر کرده است و همین موضوع بعد امنیتی این فناوری را برجسته می‌کند.

در این پژوهش نشان داده شد که در هر دوره از ریاست جمهوری رؤسای جمهور آمریکا، بر اساس نیازها و شرایط داخلی و بین‌المللی، تدابیر و سیاست‌های خاصی اتخاذ شده و استراتژی‌های هر دوره بر اساس آن تدوین گردیده است. در دوران ریاست جرج بوش دفاع سایبری و تأمین امنیت کشور مدنظر بود. در دوران ریاست باراک اوباما، تقویت توان سایبری و همکاری در همه بخش‌ها و مشارکت بین‌المللی، موردتوجه ویژه قرار داشت. دولت دونالد ترامپ نیز بر مبارزه و رویکردی تهاجمی در قبال تهدیدات امنیت سایبر تأکید نمود. نقش رقبای آمریکا نیز به عنوان تهدیدکنندگان امنیت ملی و امنیت سایبری این کشور یکی از موضوعات مهم در این استراتژی‌ها به شمار می‌رود که در برخی از این اسناد به طور مشخص از چین، روسیه، ایران و کره شمالی نام

برده شده، تهدیدات سایبری مختلفی را به آن‌ها نسبت داده و از طرق نظامی و قضایی بـه مقابلـه بـا این کشورها پرداخته است.

از این‌رو، روشن است که با نوآوری‌های پرسرعت در فضای سایبر، دامنه تهدیدات سایبری نیز گسترش یابد و جنگ‌های سایبری به یکی از مهم‌ترین ابعاد جنگ‌های ترکیبی بـدل شـوند. آنچـه که برای آمریکا و سایر کشورها مهم است این می‌باشد که در فضای سایبر و فناوری‌های وابسته به آن، پیشرو بود و به روزرسـانی امـری ضـروری اسـت. همـانطور کـه آمریکـا بـرای هـر سـازمان و وزارتخانه، استراتژی خاص خود را دارد و هر رئیس‌جمهور چندین استراتژی را مشخص می‌کنـد، سایر قدرت‌های سایبری نیز به این سمت حرکت می‌کنند. یافتن نقاط ضـعف و خلاءهـای امنیتـی، شناخت تهدیدات نوظهور و بازیگران دولتی و غیردولتـی جدیـد، از جملـه ابعـادی هسـتند کـه در آینده سایبری، بخشی از نگرانی آمریکا و سایر کشورها را تشکیل می‌دهد.

منابع

آذری، منیره. (۱۳۹۱الف). *امنیت و جنگ سایبری ۱؛ ویژه مفاهیم و مبانی*. تهران: ابرار معاصر.

بوزان، باری. (۱۳۷۸). *مردم، دولت ها و هراس*. تهران: پژوهشکده مطالعات راهبردی.

بدیعی، تعیم. (۱۳۸۰). *تحلیل محتوا*. تهران؛ اداره کل تبلیغات.

جالینوسی، احمد. ابراهیم، شهروز و قنواتی، طیبه. (۱۳۹۳). جایگاه فضای سایبر و تهدیدهای سایبری در استراتژی امنیت ملی ایالات متحده آمریکا»، *فصلنامه دانش سیاسی و بین الملل*، ۲(۵)، ۲٤-۹.

جانشکی، لچ جی و آندره ام. کلاریک. (۱۳۸۹). *مقدمه ای بر جنگ سایبر و تروریسم سایبر(جلد دوم)*. تهران: دانشگاه جامع امام حسین.

خبرگذاری بی بی سی. (۱۳۹۷). تغییر استراتژی سایبری آمریکا از دفاع به حمله. ۳۰ شهریور، از:
https://www.bbc.com/persian/world-45600472

خبرگزاری صدا و سیما. (۱۳۹۷). رویکرد تهاجمی استراتژی ملی سایبری آمریکا. ۵ مهر ۱۳۹۷، از:
https://www.iribnews.ir/fa/news/2237732/

شیهان، مایکل. (۱۳۸۸). *امنیت بین الملل*. ترجمه سید جلال دهقانی فیروز آبادی، تهران :پژوهشکده مطالعات راهبردی.

صدیق، میر ابراهیم. (۱۳۹۵). انقلاب سایبری و تحول در پدیده ی جاسوسی. *مطالعات راهبردی*، ۱۹(۱)، ۹۲-۷۱.

عبدالله خانی، علی. (۱۳۸۳). *نظریه‌های امنیت؛ مقدمه‌ای بر طرح ریزی دکترین امنیت ملی(۱)*. تهران: ابرار معاصر.

Beida, David And Leila Halawi. (2015). *Cyberspace : Avenue For Terrorism*. *Issues In Information Systems*, 16(3), pp 33-42.

Blake, Andrew. (2019). *Bolton: Trump Cyber Policy Broadening Ability Conduct Offensive Campaigns*. Washington Times, June 12, Available at: https://m.washingtontimes.com/news/2019/jun/12/john-bolton-trump-cyber-policy-broadening-ability-/

Borghard, Erica D. and Shawn W. Longergan. (2018). *Confidence Building Measures for the Cyber Domain*. *Strategic Studies Quarterly*, 12(3), pp 10-49.

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

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/

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

CSO. (2017). Obama`s cybersecurity legacy: Good intentions, Good legacy, limited results. Available at:

https://www.csoonline.com/article/3162844/obama-cybersecurity-legacy-good-intentions-good-efforts-limited-results-html

Dale, Catherine. (2013). *National Security Strategy: Mandates, Execution to Date, and Issues for Congress. CRS, Congressional Research Service,* R 43174. Available at: https://apps.dtic.mil/sti/pdfs/ADA584684.pdf

Farwell, James P. and Rafal Rohozinski. (2012). *The New Reality of Cyber War. Servival*, 54(4), pp 107-120.

Farwell, James P. and Rafal Rohozinski. (2011). *Stuxnet and the Future of Cyber War. Survival,* 53(1), pp 23-40.

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

Fischer, Eric A .(2014). *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws and Proposed Legislation*. *Congressional Research Service*. Available at: https://fas.org/sgp/crs/natsec/R42114.pdf

Giantas, Dominika and Dimitrios Stergiou. (2018). *From Terrorism to Cyber-terrorism: The Case of ISIS*. Greece. University of Peloponnese. Hellenic Institute of Strategic Studies.

Hamby, Janic M. and Thomas C. Wingfield. (2016). *Cyberpolicy.* pp 149-170.

Hannah, John and David Adesnik. (2019). *Midterm Assessment: The Trump Administration`s Foreign Policy and National Security Policies*. Foundation for Defense of Democracies. Available at:https://www.fdd.org/wp-content/uploads/2019/01/fdd-report-trump-midterm-assessment.pdf

Harvey, John. (2016). *Cybersecurity Policy Tenets: Yesterday and Today*. *CSEC,* 635.

Hjortdal, Magnus. (2011). China`s Use of Cyber Warefare: Espionage Meets Strategic Deterrence. *Journal of Strategic Security*, 4(2).

International Strategy For Cyberspace (2011). *White House*. Available at: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Jaikaran, Chris. (2018). Cybersecurity: Selected Issues for The 115th Congress. *Congressional Research Service.* Available at: https://fas.org/sgp/crs/misc/R45127.pdf

James, Kevin(2023). What is the future of cybersecurity? Predictions & trends for 2022-2023. Cyber security. Available at: https://cybersecurityforme.com/what-is-the-future-of-cybersecurity

Kolton, Michael. (2017). Interpreting China`s Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence. *Cyber Defense Review,* 2(1).pp 119-154.

Krippendorff, Klaus(2004). Content Analysis; An introduction to its methodology, University of Pennsylvania.

Libicki, Martin C.(2013). Brandishing Cyberattack Capability. *National Defense Research Institute.* Available at: https://www.rand.org/pubs/research_reports/RR175.html

Liu, Qinghui and Li Yuchong(2021). A comprehensive review study of cyber attacks and cyber security: Emerging trends and recent developments. Elsevier Ltd .Energy reports.

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/

National security Archive(2018),Presidential orders. Availabel at: https://nsarchive.gwu.edu/news/cyber-vault/2018-11-07/presidential-orders

Nakasone, Paul M. (2019). Cyber Force for Persistence Operations. JFQ, 92, pp 10-14.

O`Niel, Willian. (2009). Cyberspace and Infrastructures. In Franklin et al. (Ed.). *Cyberpower*. National Defense University press.

Regester, Virginia C. (2015). An Assessment of Botnets as an Offensive Cyber Weapon for the United States. *ProQuest.* Utica College.

Schimidt, Lara. (2015). Perspective on 2015 DOD Cyber Strategy. *RAND* CT439. Available at: https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT439/RAND_CT439.pdf

Spade, Jayson M. (2012). *China`s Cyber Power and America`s National Security*. Pennsylvania: U.S Army War College.

Stone, Marianne. (2010). Obama`s Cyber Security. *Security Technology Policy Pares Series 1*. New York: Columbia University.

Tirrell, Willian K. (2012). *United States Cybersecurity Strategy, Policy and Organization.* Washington DC: U.S Army Command and General Staff College.

Trobisch, Jan. (2014). *Challenges In The Protection Of Us Critical Infrastructure In The Cyber Realm.* United States Army Command And General Staff College. Available at: https://www.hsdl.org/?view&did=791151

The Newyork Times(2018), Trump`s Reckless Cybersecurity Strategy. February 10. Avalaible at: https://www.nytimes.com/2018/10/02/opinion/trumps-reckless-cybersecurity-strategy.html

Trujillo, Clorinda. (2014). The Limits of Cyberspace Detterance. *JFQ*: 75, pp 42-52.

Valeriano, Brandon and Benjamin Jensen. (2019). *The Myth of the Cyber Offense: The Case for Restraint.* Cato Institute. 862. Available at: https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint

Yang, Jia-hao. (2016). *Development of the U.S Cybersecurity Strategy Legislation and the Enlightment for China*. China Zhongnan University of Economics and law.

Department of Defense. (2011). *Strategy for Operating in Cyberspace*. Available at: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

Department of Homeland Security. (2018). Available at: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf

Department of State. (2016). *International Cyberspace Policy Strategy.* Available at: https://2009-2017.state.gov/documents/organization/255732.pdf

International Strategy For Cyberspace .(2011). *White House*. Available at: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Lange, Katie. (2018). *DOD`s Cyber Strategy*. Available at: https://www.defense.gov/explore/story/Article/1648425/dods-cyber-strategy-5-things-to-know/

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

National Security Strategy. (2017). *White House.* Available at: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

National Strategy to Secure Cyberspace. (2003). *White House*. Available at: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

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

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