گزارش راهبردی فارس

شماره۲

راه‌کارها و راهبردهای ایالات متحده برای امنیت سایبر

خبرگزاری فارس
FARS NEWS AGENCY
معاونت آموزش و پژوهش

بهار ۹۲

سرشناسه	:	ایزدی، فواد
عنوان و نام پدیدآور	:	راهکارها و راهبردهای ایالات متحده برای امنیت سایبر/نویسنده فواد ایزدی، مهسا ماه‌پیشانیان ؛ تهیه و تنظیم معاونت آموزش و پژوهش خبرگزاری فارس.
مشخصات نشر	:	تهران: خبرگزاری فارس، ۱۳۹۲.
مشخصات ظاهری	:	۷۱ص.
فروست	:	گزارش راهبردی فارس؛ شماره ۲.
شابک	:	۹۷۸-۶۰۰-۹۰۸۰۸-۷-۸
وضعیت فهرست نویسی	:	فیپا
موضوع	:	فضای مجازی-- ایالات متحده -- سیاست دولت.
موضوع	:	فضای مجازی-- ایالات متحده -- اقدامات تأمینی
شناسه افزوده	:	ماه‌پیشانیان، مهسا
شناسه افزوده	:	خبرگزاری فارس. معاونت آموزش و پژوهش
رده بندی کنگره	:	HM۸۵۱/الف۹ر۲ ۱۳۹۲
رده بندی دیویی	:	۳۰۳/۴۸۳۴
شماره کتابشناسی ملی	:	۳۱۲۳۸۷۲

راهکارها و راهبردهای ایالات متحده برای امنیت سایبر

گزارش‌های راهبردی فارس - ۲

نویسندگان : دکتر فواد ایزدی، مهسا ماه‌پیشانیان

ناشر: انتشارات خبرگزاری فارس

شمارگان: ۱۱۰۰ نسخه

چاپ و صحافی: پیام‌آوران نشر روز

نوبت چاپ: اول، بهار ۱۳۹۲

قیمت: ۲۵۰۰ تومان

تلفن: ۸-۸۸۹۱۳۲۷۷

نمابر: ۸۸۹۱۳۲۷۹

www.farsnews.com

publications@farsnews.ir

نشانی: تهران، میدان فردوسی، بن‌بست شاهرود، پلاک ۲

معاونت آموزش و پژوهش خبرگزاری فارس

فهرست مطالب

مقدمه

تکنولوژی ارتباطات و اطلاعات یکی از قوی‌ترین نیروها در شکل‌بخشی به قرن بیست‌ویکم بوده و تغییرات اساسی حاصل از آن، در روش زندگی افراد، آموزش، کار و نیز روش حکومت دولت‌ها تأثیرگذار می‌باشد. در واقع، عصر حاضر را باید تلفیقی از ارتباطات و اطلاعات دانست؛ عصری که بشر در آن بیش از گذشته خود را نیازمند برقراری ارتباط برای کسب اطلاعات مورد نیاز می‌داند. بنابراین، تردیدی در این واقعیت نمی‌توان داشت که جهان درحال خیز تازه‌ای به‌سمت یک تحول دوران‌ساز است. جانمایه این تحول در حوزه اطلاع‌رسانی و دانایی استقرار یافته است. البته تغییراتی که اکنون به‌واسطه انقلاب ارتباطات و فناوری‌های نوین اطلاعاتی سراسر دنیا را فراگرفته است، اگرچه می‌تواند به ایجاد جامعه‌ای علمی منتهی شود که در آن، جریان پیوسته اطلاعات، انتشار سریع عقاید و افکار صورت می‌پذیرد و تأثیرات مثبتی نیز در زمینه سیاسی، اقتصادی و اجتماعی دارد، اما به‌همان نسبت در منابع، نوع و ابزارهای تهدید تحولی شگرف ایجاد نموده و هم از لحاظ کمی (تعدد و تنوع منابع تهدید) و هم از لحاظ کیفی (پیچیده‌تر و کارآمدشدن ابزارهای سنتی تهدید) ابزارهای تهدیدات امنیت ملی را متحول نموده است. به‌کلام دیگر، در گذشته منابع تهدید امنیت دولت‌ها مشخص بود، اما امروزه دیگر چنین نیست.

به‌طورکلی می‌توان گفت فناوری‌های نوین اطلاعاتی تهدیدات و آسیب‌پذیری‌های امنیتی متعددی را متوجه کشورها اعم از بزرگ یا کوچک، پیشرفته یا در حال توسعه ساخته است. زیرا گسترش تکنولوژی‌های ارتباطی ـ اطلاعاتی فاصله موضوعات داخلی و خارجی را محو و افراد جوامع را با

تهدیدات فراملی پیوند داده است. همچنین این تکنولوژی‌ها با خلق موجودیت‌های بدون ساختار فیزیکی و مجازی و فارغ از محدودیت‌های طبیعی نه‌تنها حاکمیت ملی در برخورد با تهدیدات امنیتی را تضعیف نموده، بلکه قدرت تأثیرگذاری و عدم تشخیص تهدیدات را نیز افزایش داده‌اند.

در این میان، آمریکا یکی از کشورهایی است که با تهدیدات روبه‌گسترش سایبری علیه زیرساخت‌های حیاتی نظامی و غیرنظامی خود روبرو می‌باشد (Meyers, Powers, & Faissol, 2009: 10). تهدیدات پیش‌روی ایالات متحده در حوزه زیرساخت‌های سایبری و ارتباطات از راه دور، روبه افزایش و تکامل بوده و افراد و گروه‌های مختلفی روز به‌روز بر حملات خود با استفاده از توانایی سایبری در راستای ضربه‌زدن به منافع امنیت ملی این کشور می‌افزایند. به‌طور اساسی، نگرانی‌ها در این زمینه از دهه ۱۹۹۰ مطرح شده است. این نوع حملات پیامدهای نامطلوبی به‌همراه دارند که شامل نفوذ غیرمجاز برای دسترسی و مشاهده داده‌های محافظت‌شده، سرقت یا دستکاری اطلاعات در پایگاه‌های اطلاعاتی و حمله به دستگاه‌های ارتباطاتی برای تخریب داده‌ها یا آسیب رساندن به زیرساخت‌ها می‌شود. جنگ اطلاعاتی، جاسوسی سایبری، خرابکاری رایانه‌ای، جعل کامپیوتری، سرقت نرم‌افزاری و تروریسم سایبری از مهمترین چالش‌ها و تهدیداتی است که آمریکا در «فضای سایبر»[1] با آن روبرو می‌باشد. سرویس‌های اطلاعاتی خارجی، گروه‌های جنایی، هکرها و تروریست‌ها نیز مهم‌ترین گروه‌های شکل‌دهنده به تهدیدات سایبر برای این کشور محسوب می‌گردند (Kark, 2010: 2).

در این رابطه، مهم‌تر از هر چیزی برای آمریکا تهدید حمله‌ی سایبری علیه زیرساخت‌های حیاتی این کشور می‌باشد ـ سیستم‌ها و دارایی‌های فیزیکی یا

[1] Cyberspace

مجازی حیاتی برای ایالات متحده که ناتوانی یا نابودی آن‌ها تأثیری تضعیف‌کننده بر امنیت ملی، امنیت اقتصادی، بهداشت و سلامتی عمومی و یا ترکیبی از این موارد خواهد داشت (Rollins & Henning, 2009).

هرچند داده‌ها نشان از آن دارد که اکثریت تلاش‌ها و حملات سایبری موفق تا به امروز تنها منابع اطلاعاتی مجازی را هدف قرار داده‌اند و نه زیرساخت‌های فیزیکی، ولی بسیاری از کارشناسان آمریکایی بر این باورند که در آینده شاهد این نوع حملات به اهداف فیزیکی در جهت از کار انداختن موقت یا دائمی شبکه‌های ارتباطاتی خواهیم بود. از دید آن‌ها، این امر با ناتوانی آمریکا در شناسایی عاملان چنین حملاتی عجین شده است (همان).

ازسوی دیگر، برخی کارشناسان بر این نظرند که اگرچه تاحدی این تهدیدات وجود دارند، اما سیاست بزرگ‌نمایی تهدیدات سایبری که به‌وسیله مقامات سیاسی، امنیتی و نظامی ایالات متحده درپیش گرفته شده است، این تهدیدات را بیش از اندازه جلوه می‌دهد (Kark, 2010: 2).

البته با افزایش تهدیدات سایبری و پیچیدگی آن، دولت آمریکا نیز دست به اقداماتی برای مقابله با آن‌ها زده است. در این راستا، «فرمان شماره ۶۳ رئیس‌جمهوری»[2] که در سال ۲۰۰۳ به واسطه انتشار «استراتژی ملی در باب ایمن‌سازی فضای سایبر»[3] به روز شد، «فرمان شماره ۷ رئیس‌جمهور در زمینه امنیت کشور»[4] و دیگر فرمان‌های محرمانه ریاست‌جمهوری و اسناد برنامه‌ریزی استراتژیک، همگی بازتابی از سیاست دولت فدرال در واکنش به تهدیدات سایبر می‌باشند. اگرچه اوباما نیز توصیه‌هایی برای اصلاح سیاست‌های سایبر در سال ۲۰۰۹ عنوان نمود، اما از میان ۲۴ توصیه وی در این سال، فقط دو توصیه به‌طور

[2] Presidential Decision Directive 63
[3] National Strategy to Secure Cyberspace
[4] Homeland Security Presidential Directive 7

کامل و ۲۲ توصیه دیگر به‌صورت ناقص اجرایی شده‌اند یا اساساً اجرا نشده‌اند. بسیاری معتقدند دلیل اصلی این مسئله، عملکرد کُند و آهسته سازمان‌های مسئول به‌علت مشخص نبودن نقش و مسئولیت دقیق آن‌ها در قبال اجرای این توصیه‌ها بوده است. در مجموع می‌توان گفت ایالات متحده در زمینه تأمین «امنیت سایبر»[5] با یک انفعال استراتژیک روبرو می‌باشد (Lewis, 2008).

با این توضیح، در متن حاضر که بخش نخست «راه‌کارها و راهبردهای ایالات متحده برای امنیت سایبر» محسوب می‌گردد، تلاش شده تا ضمن ارائه تعاریفی از فضای سایبر و برشمردن ویژگی‌ها، چالش‌ها و تهدیدات این فضا برای آمریکا، به بررسی سیاست‌های دولت فدرال در راستای تأمین امنیت سایبر پرداخته شود. بنابراین سعی می‌شود به این سؤالات پاسخ داده شود:

۱. منابع مستقیم و غیرمستقیم تهدیدات آمریکا در فضای سایبر چیست؟
۲. بازیگران اصلی عرصه جنگ سایبر چه کسانی بوده و از چه ماهیتی برخوردارند؟
۳. هدف حملات سایبری به این کشور چیست؟
٤. آیا هدف حملات سایبری کسب سلطه، برتری سیاسی یا استراتژیک بوده یا این حملات تنها با هدف وارد آوردن ضربات امنیتی بر دولت یا شهروندان طراحی شده است؟

در واقع، در اینجا بیشتر تأکید بر راه‌کارهای دفاعی ایالات متحده در حوزه سایبر می‌باشد. عملیات‌های تدافعی در فضای سایبر شامل اقدامات مستقیم و هم‌زمانی است که به‌منظور کشف، تجزیه و تحلیل، مقابله و تعدیل تهدیدات و آسیب‌پذیری‌ها در فضای سایبر به‌منظور پیش‌افتادن از حریفان در این فضا صورت می‌پذیرد. این دسته از اقدامات می‌توانند زمینه شکل گرفتن اقدامات

[5] Cybersecurity

دفاعی ایالات متحده در فضای سایبر یا دیگر اقدامات واکنشی لازم برای دفاع از شبکه‌های اطلاعاتی این کشور در مقابله با اقدامات خرابکارانه را به‌وجود آورد (U.S. Cyber Command, USCYBERCOM Concept of Operations, 2010).

عملیات‌های تهاجمی که در بخش دوم و در شماره آتی مورد توجه قرار خواهند گرفت، دربرگیرنده ظرفیت‌هایی برای حمایت مستقیم از اهداف فرماندهی جنگی و ملی، دفاع فعال از وزارت دفاع و دیگر شبکه‌های اطلاعاتی می‌باشد (همان). بنابراین، ضمن بررسی تعاریف، طرح‌ها، دکترین و تسلیحات «جنگ سایبری»[6] آمریکا، به اقدامات آفندی (تهاجمی) این کشور در فضای سایبر پرداخته خواهد شد.

در کلیت امر نیز هدف از تدوین چنین گزارشی، یافتن راه‌کارهای مناسب برای کشورمان در حوزه دفاع سایبری می‌باشد. در اصل، از آنجایی‌که ایالات متحده در دهه اخیر با حملات سایبری فراوانی مواجه بوده است، اقدامات دفاعی آن در این زمینه می‌تواند الگویی باشد برای تمهیداتی که قرار است در ایران به اجرا درآید.

[6] Cyber War or Cyber Warfare

بخش اول – فضای سایبر: مفهوم، ویژگی، اهداف

۱) تعریف فضای سایبر

فضای سایبر یک محیط سیال بشرساخته است. فرهنگ لغت «مِریَم–وبستر»[1] فضای سایبر را «جهان آنلاین از شبکه‌های کامپیوتری و به‌خصوص اینترنت تعریف می‌کند» (Merriam-Webster, 2000). وزارت دفاع آمریکا نیز این فضا را یک قلمرو جهانی در محیط اطلاعات می‌داند که دربرگیرنده شبکه‌ای به‌هم مرتبط از زیرساخت‌های تکنولوژی اطلاعاتی بوده و شامل اینترنت، شبکه‌های ارتباطات از راه دور، سیستم‌های کامپیوتری، کنترل‌گرها و پردازنده‌ها می‌شود (Defense Department Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities, 2011).

جدای از این، کسانی همچون «چیپ مُرنینگستار[2]» و «اِف. رَندِل فارمر[3]» از کارشناسان سیستم‌های نرم‌افزاری در حوزه ارتباطات، فضای سایبر را بیشتر با توجه به تعاملات اجتماعی صورت‌گرفته و نه بُعد فنی آن تعریف می‌کنند. از دید آن‌ها، رسانه کامپیوتر در فضای سایبر تقویت کانال ارتباطی میان مردم واقعی می‌باشد و بنابراین ویژگی اصلی فضای سایبر آن است که محیطی را ایجاد می‌کند که شامل افراد بسیاری می‌شود که از توانایی تأثیرگذاری و نفوذ بر یکدیگر برخوردارند (Morningstar & Farmer, 2003: 46).

۲) ویژگی‌های فضای سایبر

■ *کاهش اختلاف قدرت میان بازیگران*

[1] Merriam-Webster
[2] Chip Morningstar
[3] F. Randall Farmer