فصلنامه پژوهش‌های حفاظتی ـ امنیتی دانشگاه جامع امام حسین (علیه‌السلام)
سال ششم، شماره ۲، شماره پیاپی ۲۲ (تابستان ۱۳۹۶): صص ۱۲۲- ۹۱

تهدید شناسی امنیت فضای سایبری حوزه دفاع موشکی در پسا برجام

مصطفی عباسی[۱]
سامان کشوری[۲]
عبدالرحمن کشوری[۳]
محمدرضا حسنی آهنگر[۴]

تاریخ دریافت: ۱۳۹۶/۰۷/۱۵
تاریخ پذیرش: ۱۳۹۶/۱۰/۱۵

چکیده

با توجه به گسترش روزافزون فضای سایبر، بهره‌برداری از قابلیت‌های آن در حوزه‌های مختلف، به خصوص صنایع نظامی و دفاعی افزایش یافته است. به‌دلیل کمبود زیرساخت‌های فناوری، دانشی و صنایع مورد نیاز در حوزه‌های طراحی و ساخت تجهیزات الکترونیکی، تمایل و نیاز به تسهیلات خارجی، گسترش یافته است؛ درنتیجه، امنیت فضای سایبری در زیرساخت‌های مختلف به خصوص موشکی بیش از گذشته در معرض تهدید و نفوذ قرارگرفته است. با توجه به تعاملات اخیر با کشورهای هم‌راستا با دشمنان نظام و انعقاد برجام، دشمنان نظام سعی دارند تا با بهره‌برداری از قابلیت‌ها و آسیب پذیری‌های فضای سایبری، شرایط لازم را جهت نفوذ، جاسوسی و تخریب در لایه‌های مختلف حوزه موشکی کشور مهیا نمایند. در این پژوهش بر اساس مدل سه شاخه‌ای ذهن عوامل ساختاری، زمینه‌ای، رفتاری مرتبط با امنیت فضای سایبری موشکی تعیین شده، همچنین ضمن تشریح روش‌های نفوذ در این فضا در پسابرجام، راه‌کارهای مقابله‌ای آن بر اساس منابع آشکار ارائه شده است. بنابراین می‌توان با بهره‌گیری از نتایج این پژوهش، با مصون سازی زیرساخت‌ها، کارکنان و شبکه‌های اطلاعاتی حوزه موشکی مانع نفوذ دشمنان و مزدوران وابسته شد.

کلید واژگان: *امنیت، فضای سایبری، تروجان سخت‌افزاری، حوزه موشکی، پسا برجام، مدل سه شاخه‌ای ذهن*

---

[۱] دانشجوی دکتری کامپیوتر دانشگاه جامع امام حسین (ع) moabbasi@ihu.ac.ir
[۲] کارشناس ارشدکامپیوتر دانشگاه جامع امام حسین (ع)
[۳] استادیاردانشگاه جامع امام حسین (ع)
[۴] دانشیاردانشگاه جامع امام حسین (ع)

مقدمه

امروزه مسئله نفوذ یکی از داغ‌ترین و مهم‌ترین مسائل اخبار و خبرگزاری‌ها در کنار مسئله هسته‌ای و موشکی است. هشدارهای متعدد مقام معظم رهبری گواه عمق نگرانی ایشان از این مسئله و نزدیک بودن خطر است. ایشان در تعدادی از سخنرانی‌های خود مسئله نفوذ و انواع آن را تشریح نموده‌اند. به اعتقاد مقام معظم رهبری، دشمنان نظام میلیاردها دلار هزینه می‌کنند تا در کشور ما اقدام به‌نفوذ نمایند. این اقدام نه‌فقط در زمینه‌ای خاص، بلکه در عرصه‌های متعدد صورت می‌پذیرد.

یکی از موضوعات اختلافی بین ایران و سایر کشورها در برجام (برنامه جامع اقدام مشترک) که جزء خطوط قرمز نظام جمهوری اسلامی است، حوزه‌های مختلف موشکی بوده و دشمنان نظام سعی دارند از هر طریقی پیشرفت موشکی را متوقف نماید. با توجه به گسترش تهدیدهای سایبری در حوزه‌های مختلف، به خصوص زیرساخت‌های حساس و همچنین روابط دیپلماتیک بین ایران و کشورهای ۵+۱ (آمریکا، روسیه، چین، بریتانیا، فرانسه و آلمان)، یکی از بهترین روش‌ها و گزینه‌های نفوذ به‌حوزه موشکی کشور، بهره‌برداری از ویژگی‌ها و ظرفیت‌های فضای سایبری و محیط اطلاعاتی است. با توجه به زیر بخش‌های مختلف فضای سایبری که شامل ادراکی و اطلاعاتی و فیزیکی است، متناسب با حوزه موشکی می‌توان هرکدام از این لایه‌ها را بررسی کرد و روش‌های نفوذ دشمن را بیان نمود. به‌عنوان نمونه در لایه ادراکی، نفوذ می‌تواند از طریق تغییر در تصمیم‌گیری و تصمیم سازی مسئولان و متخصصان حوزه موشکی و مرتبط انجام شود. در لایه اطلاعاتی جاسوسی و تخریب سامانه‌های اطلاعاتی زیرساخت‌های موشکی از طریق نفوذ سایبری به این سامانه‌ها صورت می‌پذیرد. در لایه فیزیکی با تخریب و تغییر کارکردها در زیرساخت و سامانه‌های موشکی، ضمن بهره‌برداری از آسیب پذیری‌های تعبیه شده آن‌ها را در شرایط خاص فعال کرد (Cordesman،2002).

در بخش ادبیات موضوع و مفاهیم نظری در راستای شناخت بهتر موضوع، مفاهیم و مؤلفه‌های مختلف محیط اطلاعاتی و فضای سایبر، روش‌های مختلف نفوذ و مدل سه شاخه‌ای ذهن مورد بررسی قرارگرفته است. در بخش مروری بر کارهای مرتبط با امنیت سخت‌افزاری زیرساخت‌های حساس، در راستای نفوذ از طریق لایه فیزیکی فضای سایبری، امنیت سخت‌افزاری، مفهوم تروجان سخت‌افزاری و آسیب پذیری‌های آن در زیرساخت‌های گوناگون مرتبط با زیرساخت‌های سخت‌افزاری موشکی عنوان گردیده است. بخش تهدید شناسی امنیت سایبری حوزه موشکی بر مبنای مدل سه شاخه‌ای ذهن، تهدید شناسی در خصوص امنیت سایبری حوزه موشکی و پیامدهای آن در پسابرجام، راه‌کارهای مقابله‌ای بر اساس مدل سه شاخه‌ای ذهن، نظر متخصصان و منابع آشکار بیان شده است. در پایان، بحث، پیشنهادها و نتیجه‌گیری پژوهش ارائه شده است.

ادبیات موضوع و مفاهیم نظری

با توجه به اهمیت تهدید شناسی امنیت فضای سایبری حوزه دفاع موشکی در پسابرجام و نفوذ از طریق آن، نیاز است مطابق با اسناد کشورهای پیشرو در حوزه فناوری و دانش، مروری بر محیط اطلاعاتی و فضای سایبری انجام شود تا متناسب با قابلیت‌های فضای سایبری، روش‌های نفوذ سایبری دشمنان در زمان‌های مختلف به خصوص زمان صلح معرفی شود. همچنین نیاز است تا متناسب با ویژگی‌های نفوذ از دیدگاه مقام معظم رهبری، روش‌های نفوذ در حوزه امنیت و سایبری بسترهای موشکی بررسی گردد. برای بررسی و تحلیل مسئله نفوذ و تهدید شناسی سایبری حوزه موشکی، از مدل سه شاخه‌ای ذهن استفاده شده است.

ویژگی‌های (عملیات) محیط اطلاعاتی و سایبری

بر اساس تعاریف وزارت دفاع آمریکا، محیط اطلاعاتی عبارت است از: «مجموعه‌ای از افراد، سازمان‌ها و سیستم‌هایی که اطلاعات خود و دیگران را جمع‌آوری، پردازش یا منتشر می‌کنند یا بر اساس اطلاعات، اقدام می‌کنند. محیط اطلاعاتی یک مجموعه به هم مرتبط از اطلاعات، زیرساخت‌های اطلاعاتی و فرایندهای مبتنی بر اطلاعات است. یک سیستم اطلاعاتی تلفیقی از حسگرها، شبکه‌ها، پردازشگرها، مراکز فرماندهی و اپراتورها است» (STAFF،I-1:2012).

لذا بر اساس تعریف فوق و مستندات منتشر شده آمریکایی‌ها، محیط اطلاعاتی شامل بخش‌های زیر است:

قلمرو فیزیکی: جایی است که حمله، حفاظت و مانور در محیط‌های زمینی، دریایی، هوایی و فضایی به‌صورت فیزیکی انجام می‌شود. در این قلمرو سکوهای فیزیکی و شبکه‌های ارتباطی که آن‌ها را به یکدیگر پیوند می‌دهند، وجود دارند. سنجش عناصر و مؤلفه‌های این قلمرو نسبتاً آسان بوده و قدرت نظامی به‌طور سنتی بر اساس توجه به این قلمرو تعیین شده است.

قلمرو اطلاعاتی: جایی است که اطلاعات تولید، مدیریت و به اشتراک گذاشته می‌شود. در این قلمرو اطلاع رسانی به رزمندگان تسهیل می‌شود و دستورات نظامی از طریق نظام فرماندهی و کنترل منتقل می‌شوند. این لایه شامل اطلاعات ذخیره شده در تجهیزات و اطلاعات در جریان هست.

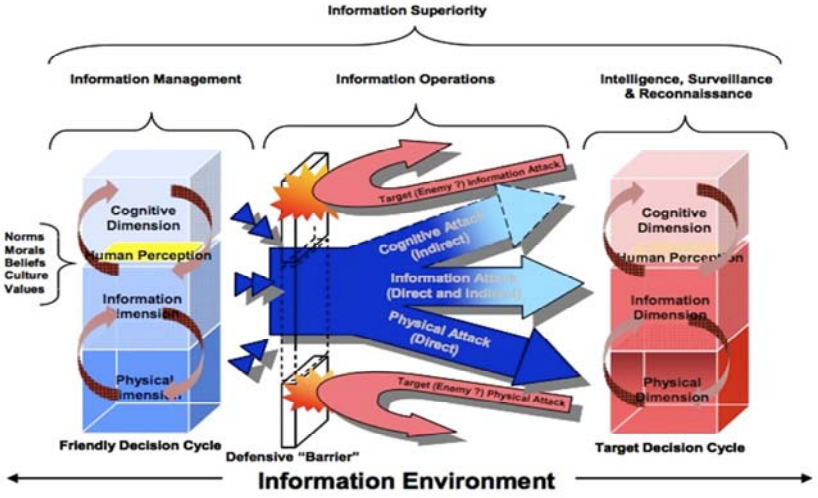
قلمرو شناختی: نیز درون ذهن افراد قرار دارد. در این قلمرو درک، برداشت، باورها و ارزش‌ها حضور دارند و بنیان تصمیم‌گیری را تشکیل می‌دهد. قلمرو شناختی را باید جایگاه امور نامحسوس و ناملموسی مانند توان رهبری، روحیه جنگجوئی، انسجام یگان‌ها، سطح آموزش و تجربه و آگاهی موقعیت دانست. تعیین و سنجش ویژگی‌های این قلمرو بسیار دشوار است و شامل زیرمجموعه‌هایی با عنوان ذهن افراد می‌شود که هریک از آن‌ها منحصربه‌فرد هستند (Romanych،2005:14).

همان‌طور که در شکل ۱

شکل نشان داده شده، در محیط اطلاعاتی، علاوه بر تأثیرگذاری هرکدام از دامنه‌ها بر دامنه‌های زیرین و بالایی خود، توانایی اثرگذاری مستقیم و غیرمستقیم بر سایر دامنه‌ها را دارند. از ویژگی‌های این دامنه‌ها می‌توان در چرخه تصمیم‌گیری و اقدام نیروهای خودی، یا ضد چرخه تصمیم‌گیری دشمن و عملیات‌های اطلاعاتی آن‌ها استفاده کرد. لذا برای جلوگیری از تأثیرات اقدامات دشمن می‌بایست از راه‌کارهای امنیتی و دفاعی متناسب با قابلیت‌های هر دامنه بهره‌جویی نمود تا ضمن خنثی سازی

اقدامات و راهبردهای دشمن، نسبت به رقبا، برتری اطلاعاتی داشته باشیم (Staff، 2012:I-1; Williams،2010).

در دامنه فیزیکی مجموعه اقدامات و مأموریت‌های تعریف شده با استفاده از زیرساخت‌ها و تجهیزات مورد نیاز، پیاده سازی و اجرا می‌گردد. در دامنه اطلاعاتی، اطلاعات از حوزه فیزیکی جمع‌آوری، پردازش و جهت بهره‌برداری تصمیم گیران انتشار می‌یابد. در حوزه شناختی بر اساس اطلاعات حوزه اطلاعاتی، آگهی وضعیتی از شرایط محیطی برای تصمیم گیران به وجود می‌آید، سپس آن‌ها بر اساس شرایط و آگهی کسب شده تصمیم‌گیری می‌نمایند. پس از تعیین تصمیمات در حوزه شناختی، مجدداً تصمیم‌ها در حوزه اطلاعاتی پردازش و انتشار یافته و این اطلاعات منتشر شده در حوزه فیزیکی به کمک تجهیزات و فناوری‌ها اجرا می‌شود (Denning،Libicki; 1999، 1995).



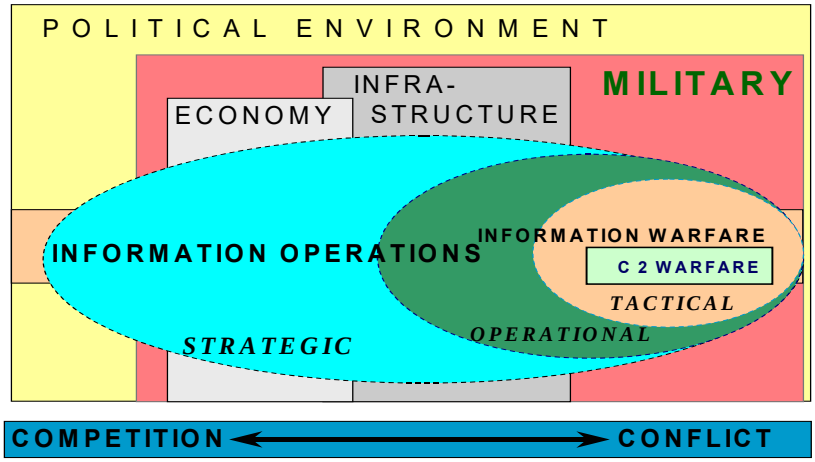
شکل (۱) محیط اطلاعاتی و نحوه تأثیرگذاری هر عملیات اطلاعاتی در دامنه‌های مختلف (Armistead،2004)

هدف اصلی عملیات در محیط اطلاعاتی و سایبری، منابع اطلاعاتی و زیرساخت‌های[1] حیاتی و ملی است، به‌طوری‌که نتیجه خرابی ممکن است به‌صورت یک‌دفعه ظاهر نشود؛ به همین جهت به این نوع حملات حمله نرم[2] نیز گفته می‌شود. یکی از اهداف جنگ اطلاعاتی نفوذ آرام به سیستم‌های اطلاعاتی و مخابراتی به‌منظور به‌دست گرفتن کنترل ارتباطات، دست‌کاری و بهره‌برداری از اطلاعات، ایجاد عدم قطعیت در آن‌ها و یا فریب سیستم‌های رقیب است. در جنگ اطلاعات ناشناخته بودن هویت حمله کنندگان، محل فیزیکی آن‌ها و سرعت زیاد جابه‌جایی و توسعه آن‌ها یک ویژگی بارز محسوب می‌شود. طبق تعاریف اسناد آمریکا، عملیات اطلاعاتی را می‌توان به‌کارگیری یکپارچه قابلیت‌های اصلی محیط اطلاعاتی شامل جنگ الکترونیک[3]، عملیات شبکه رایانه‌ای[4]، عملیات روانی[5]، فریب نظامی[6] و امنیت عملیات[7] و سایر قابلیت‌های مرتبط و پشتیبانی برای تأثیرگذاری[8]، اختلال[9]، تخریب[10] یا غصب کردن[11] فرآیند تصمیم سازی انسانی و خودکار دشمن[12]، در عین حفاظت از آنچه خود داریم، بیان کرد (Staff،2010:175).

با توجه به ویژگی‌های بیان شده برای محیط اطلاعاتی و مطابق با شکل ۲، عملیات اطلاعاتی در زمان‌ها (صلح، رقابت، بحران، جنگ و بازگشت به صلح)، سطوح اقدام (تاکتیک، عملیات و استراتژیک) و حوزه‌های مختلف (سیاسی، اقتصادی، زیرساخت‌ها و نظامی) قابل پیاده سازی و اجرا است. این عملیات‌ها، در زمان‌های مختلف متناسب با نوع به‌کارگیری در مؤلفه‌های قدرت ملی[13] متفاوت هستند؛ به‌عنوان نمونه، جنگ فرماندهی و کنترل در سطح تاکتیک و حوزه نظامی و در زمان

[1] Infrastructures
[2] Softkill
[3] electronic warfare
[4] computer network operations
[5] psychological operations
[6] military deception
[7] operations security
[8] influence
[1] disrupt
[2] corrupt
[3] usurp
[4] human and automated decision making
[5] DIME(Diplomatic, Informational, Military, and Economic)

جنگ کاربرد دارد، اما عملیات اطلاعاتی در همه سطوح تاکتیکی، عملیاتی و راهبردی و در همه مؤلفه‌های قدرت ملی در همه زمان‌های صلح تا درگیری کاربرد دارد (Armistead،2004).



شکل (۲) وضعیت عملیات اطلاعاتی از لحاظ سطوح درگیری و مؤلفه‌های قدرت ملی (Armistead،2004:20)

فضای سایبری یک قلمرو جهانی در محیط اطلاعاتی است که از شبکه وابسته به هم از زیرساخت‌های فناوری اطلاعات، شامل اینترنت، شبکه‌های مخابراتی، سیستم‌های رایانه‌ای و پردازشگرها و کنترلرهای جاسازی شده[1] تشکیل شده است. همان‌طور که در خصوص محیط اطلاعاتی عنوان شد، فضای سایبر دارای ابعاد زیر است:

بعد فیزیکی: فضای سایبر یک شبکه ارتباطی گسترده جهانی متشکل از زیرساخت‌های ارتباطی و فناوری اطلاعات است.

بعد اطلاعاتی: فضای سایبر یک منبع اطلاعاتی توزیع شده حاوی انواع و سطوح مختلف داده، اطلاعات و دانش، از خودی و غیرخودی است.

بعد انسانی: فضای سایبر یک جامعه مجازی است که اعضای آن، قابلیت انجام فعالیت‌های اجتماعی، اقتصادی، سیاسی و فرهنگی را دارند. لذا متناسب با دسته‌بندی بیان شده، سه دسته تهدید و اقدامات دفاعی متقابل در فضای سایبر وجود دارد:

[1] embedded

– تهدیدات سخت متوجه بعد فیزیکی فضای سایبر بوده و اختلال در قابلیت‌های فنی سخت‌افزاری یا نرم‌افزاری آن را هدف قرار می‌دهند.

– تهدیدات نیمه سخت متوجه بعد اطلاعاتی فضای سایبر شده و بهره‌برداری حداکثری اطلاعاتی از این منبع را مقصود خود قرار می‌دهند.

– تهدیدات نرم نیز متوجه بعد انسانی فضای سایبر است و اهداف خود را در این جامعه مجازی جستجو کرده و اقدامات جنگ نرم را روی آن‌ها انجام می‌دهند.

برای عملیات در محیط فضای مجازی، می‌توان از اقدامات هجوم، دفاع و شناسایی یا بهره‌برداری سایبری استفاده نمود. در بخش‌های سخت‌افزاری، نرم‌افزاری و شبکه به‌دلیل آسیب پذیری‌های متعدد شناخته شده و ناشناس، زمینه این‌گونه اقدامات متنوع‌تر است و باعث نگرانی سازمان‌ها در حوزه‌های مختلف، به خصوص زیرساخت‌های مهم و حساس شده است (Army،Andress & Winterfeld ;2013، 2010).

مدل سه شاخه‌ای ذهن

مهم‌ترین ویژگی عصر حاضر برای سازمان‌ها عدم اطمینان، پیچیدگی، جهانی‌سازی و تغییرات فزاینده فناوری از یک‌سو و تنوع خواسته‌ها و نیازهای ذی‌نفعان و نیز سرعت بالای تغییرات الگوی خواسته‌ها از سوی دیگر است. عوامل مؤثر در سازمان‌ها چه عوامل درونی و چه عوامل بیرونی، منجر به تصمیم‌گیری مؤثر، بهبود انعطاف، قابلیت تطبیق، تلفیق و همگونی می‌گردد. این عوامل در قالب مدل سه‌شاخه‌ای شامل عوامل ساختاری، زمینه‌ای و رفتاری تعریف می‌شود. علت نام‌گذاری مدل این است که ارتباط بین عوامل ساختاری، رفتاری و زمینه‌ای به‌نحوی است که هیچ پدیده‌ای نمی‌تواند خارج از تعامل این سه‌شاخه انجام گیرد. در واقع، رابطه میان این سه‌شاخه یک رابطه تنگاتنگ ناگسستنی است که در عمل از هم جدایی ناپذیرند. به‌عبارتی بین سه‌شاخه به‌هیچ‌وجه سه‌گانگی حاکم نیست؛ بلکه سه‌گونگی حاکم است و تمایز و تشخیص این سه جنبه صرفاً نظری و به‌منظور تجزیه‌وتحلیل و شناخت مفاهیم پدیده‌ها است (دهقان و همکاران، ۱۳۹۱: ۲۵).

عوامل ساختاری: دربرگیرنده تمام عناصر، عوامل و شرایط فیزیکی و غیرانسانی سازمان است که بانظم، قاعده و ترتیب خاص و به‌هم‌پیوسته، چارچوب، قالب، پوسته و بدنه فیزیکی و مادی سازمان

را می‌سازد؛ بنابراین تمام منابع مادی، مالی، اطلاعاتی و فنی که با ترکیب خاصی در بدنه کلی سازمان جاری می‌شوند، جزء شاخه ساختاری قرار می‌گیرند.

عوامل زمینه‌ای: شرایط و عوامل محیطی برون‌سازمانی هستند که محیط سازمان را احاطه می‌کنند، با سازمان تأثیر متقابل دارند و خارج از کنترل سازمان هستند. هر نظام یا سازمانی در جایگاه ویژه خود همواره با نظام‌های محیطی در کنش و واکنش دائمی است. ازاین‌رو، همه علل و عواملی که امکان برقراری، تنظیم و واکنش به‌موقع و مناسب سازمان نسبت به سایر نظام‌ها را فراهم می‌آورند، زمینه یا محیط نامیده می‌شوند.

عوامل رفتاری: شامل عوامل و روابط انسانی در سازمان است که هنجارهای رفتاری، ارتباط غیررسمی و الگوهای ویژه به‌هم‌پیوسته و محتوای اصلی سازمان را تشکیل می‌دهند. این عوامل محتوایی در واقع عامل پویایی بخش و زنده کردن سازمانی تلقی می‌شوند و هرگونه عوامل و متغیرهایی که به‌طور مستقیم مربوط به نیروی انسانی باشند در این شاخه قرار می‌گیرند. عوامل ساختاری و رفتاری، درون‌سازمانی و محصور در مرزهای سیستم سازمان هستند (میرزایی و همکاران، ۱۳۸۴: ۷۳).

بررسی نفوذ از دیدگاه مقام معظم رهبری (مدظله العالی)

مقام معظم رهبری در مقاطع زمانی مختلف متناسب با شرایط، برخی از استراتژی‌های دشمن در مورد نفوذ و انواع آن را، بیان فرموده‌اند. از نمونه‌های نفوذ از دید ایشان می‌توان نفوذ موردی (فردی)، نفوذ امنیتی، نفوذ سایبری، نفوذ فرهنگی و نفوذ سیاسی را نام برد. دشمن در این عرصه اهداف مختلفی را دنبال می‌کند. دشمن در بخشی سعی می‌کند تا به باورها و ارزش‌های ایرانی اسلامی حمله کند، در بخش دیگر می‌کوشد مردم کشور را از وضعیت کشور ناامید کند و این‌گونه القا کند که کشور وضع آشفته‌ای دارد. در بخش دیگر تلاش می‌کند تا با حملات هکرهای خود سایت‌های دستگاه‌ها و نهادهای مختلف کشور را هک کرده و به اطلاعات لازم خود برسد. این عرصه از نفوذ مکمل نفوذ فرهنگی و امنیتی است. مطابق با بیانات مقام معظم رهبری (مدظله العالی) در مراسمات مختلف، می‌توان این استدلال را داشت که در زمان کنونی متناسب با شرایط و وضعیت سیاسی پیش‌آمده،

دشمن سعی دارد با بهره‌برداری مناسب از محیط اطلاعاتی و فضای سایبر، نفوذ خود را در حوزه‌های ادراکی، تصمیم‌گیری نظام و زیرساخت‌های مهم اطلاعاتی و فیزیکی افزایش دهد تا در زمان مناسب به‌نحو مطلوبی از آن‌ها استفاده نماید. لذا متناسب با اهداف و استراتژی‌های دشمن برای نفوذ به خصوص با بهره‌برداری از فضای سایبری، در بخش‌های بعدی یکی از روش‌های نفوذ احتمالی دشمن در زیرساخت‌های فیزیکی اساسی کشور با توجه به بومی نبودن قطعات و تجهیزات الکترونیکی، بیان می‌شود. این تهدید برای زیرساخت موشکی کشور که یکی از سناریوهای جذاب و مطلوب برای دشمن است، قابل پیش‌بینی است (بیانات مقام معظم رهبری، ۱۳۹۴ (۱ و ۲)).

مروری بر کارهای مرتبط با امنیت سخت‌افزاری زیرساخت‌های حساس

یکی از تهدیدهای اساسی در سخت‌افزار زیرساخت‌های نظامی و غیرنظامی، وجود تروجان‌های سخت‌افزاری است که امنیت سخت‌افزار مربوطه را متناسب با شرایط برنامه‌ریزی شده طراح، تهدید می‌کند. استفاده از سامانه‌های تعبیه شده در کاربردهای با نیاز امنیتی بالا، تبدیل به امری اجتناب ناپذیر شده است. طراحی سامانه‌های تعبیه شده اساساً به دو صورت مبتنی بر طراحی کامل توسط مشتری و یا مبتنی بر قطعات از قبل ساخته شده تجاری، انجام می‌پذیرد. ازآنجاکه در کشور در حال حاضر فنّاوری ساخت تراشه مبتنی بر فنّاوری نیمه هادی وجود ندارد و یا حداقل بخشی از فرآیند ساخت می‌بایست در خارج از کشور انجام گردد باید از قطعات از قبل ساخته شده تجاری با به‌کارگیری تمهیدات امنیتی و حفاظتی استفاده نمود. درهرصورت چه بخشی یا تمام سخت‌افزار از فاز طراحی تا ساخت توسط شرکت ثالث انجام‌پذیرد، این احتمال وجود دارد که سخت‌افزار ساخته شده راه‌کارهای نفوذ را برای رقبا ایجاد نماید. برای افزایش امنیت سامانه‌ها و زیرساخت‌های سخت‌افزاری آن‌ها، نیاز است ضمن شناسایی انواع تروجان‌های سخت‌افزاری و راه‌کارهای شناسایی و مقابله با آن‌ها بررسی گردد.

مروری بر بهره‌جویی از آسیب پذیری‌های سخت‌افزاری در حوزه‌های مختلف

گزارش‌های مختلفی از وجود تروجان‌های سخت‌افزاری و فعال شدن آن‌ها در زیرساخت‌های نظامی و غیرنظامی و آسیب‌های وارد شده به آن‌ها در مراجع آشکار گزارش شده است که در ادامه برخی از این گزارش‌ها بررسی می‌گردد تا تهدیدات آن در حوزه سایبری موشکی نمایان‌تر شود.

– در سپتامبر ۲۰۰۷، جنگنده‌های اسرائیلی به یک نیروگاه هسته‌ای در شمال غرب سوریه حمله کردند که در این حمله رادارهای سامانه پدافندی سوریه هیچ‌گونه هشداری را در مورد رخداد این حمله گزارش نکردند. پس از مدتی وبلاگ نویسان نظامی و فناوری نتیجه‌گیری کردند که این حادثه به‌دلیل یک جنگ‌افزار الکترونیک، با استفاده از آسیب پذیری‌های سخت‌افزاری بوده است (Bilzor et al.، 2011:1).

– بر اساس گزارش یک پیمانکار نظامی آمریکایی، بر اساس درخواست پیمانکاران دفاعی فرانسه، شرکت‌های سازنده تراشه اروپایی، درون ریز پردازنده‌هایشان یک کلید کشنده قرار داده‌اند تا درصورتی‌که این تجهیزات در آینده در دست دشمن قرار بگیرد، فرانسوی‌ها بتوانند آن‌ها را غیرفعال نمایند (Adee، 2008:2).

– در ماه ژوئن ۲۰۱۱ اعلام شد که در سال ۲۰۱۰ نیروی دریایی آمریکا بیش از ۵۹۰۰۰ تراشه خریداری شده از چین را به این کشور بازگشت داده است. بر اساس گزارش سایت وایرد[1] دلیل این اتفاق علاوه بر بی‌کیفیتی تراشه‌ها، وجود درهای پشتی[2] در این تراشه‌ها عنوان شده است. درهای پشتی این امکان را به حمله کنندگان می‌دادند که هر زمان که خواستند تراشه‌ها را به حالت خاموش برده و آن‌ها را از کار بیندازند. پس‌ازاین اتفاق وزارت دفاع آمریکا پروژه‌ای برای بررسی و ارزیابی امنیت تراشه‌های خریداری شده از سازندگان خارجی تعریف و اجرا کرد (Johnson، 2011).

– بر اساس اطلاعاتی که در سال ۲۰۰۷ منتشر شد، حافظه‌های جانبی خارجی شرکت سیگات[3] حاوی تروجان‌های از پیش نصب شده‌ای بودند که پسوردهای ذخیره شده را به یک سرور ارسال می‌کردند (Alkabani & Koushanfar، 2008:1).

[1] www.wired.com
[1] Backdoor
[2] Seagate

– شرکت اینتل نسخه‌ای از پردازنده‌های تولیدی خود[1] را ارائه کرده که برای پیشگیری از سوءاستفاده از اطلاعات کاربران، از یک فناوری ضد سرقت در آن استفاده شده است. در هنگام سرقت رایانه با استفاده از یک کلید کشنده که در پردازنده آن تعبیه شده، کاربر می‌تواند پردازنده مورد نظر را از راه دور خاموش و غیرفعال نماید (Gomez، 2010).

– از دیگر نمونه‌های تروجان می‌توان به نتیجه پژوهش تعدادی از محققان دانشگاه کمبریج انگلستان بر روی میزان حساسیت تراشه برنامه‌پذیر[2] مخصوص کاربردهای نظامی[3] ساخت شرکت اکتل[4] مدل A3P250 ProASIC Microsemi اشاره کرد. طبق مستندات ارائه شده توسط سازنده، این تراشه دارای میزان امنیت بالا در مقابل انواع حملات امنیتی است. در واقع شرکت مذکور این محصول را مخصوص کاربردهای حساس نظامی به بازار عرضه کرده است. تحقیقات پژوهشگران دانشگاه کمبریج نشان می‌دهد که درون قسمت کنترل‌کننده JTAG این تراشه‌ها ماژولی وجود دارد که اجازه دسترسی مخفی به داده‌های پیکربندی تراشه FPGA را می‌دهد (Skorobogatov & Woods، 2012:24).

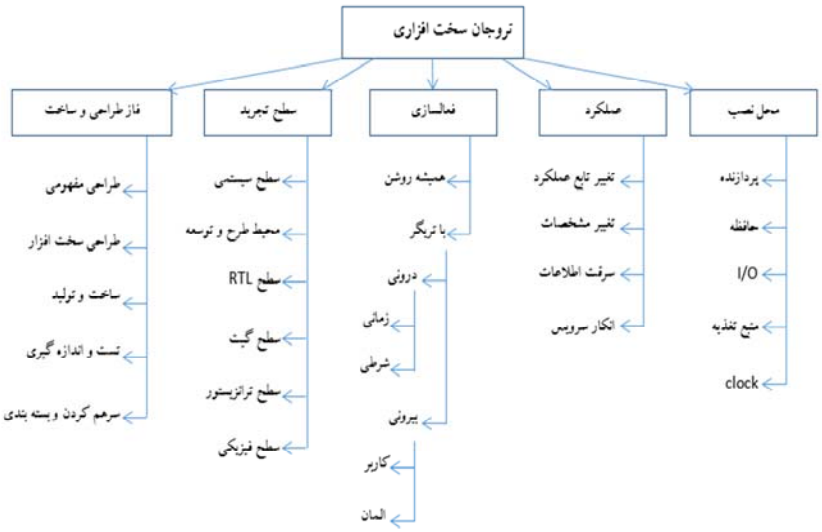
– طبق اخبار منتشر شده پنتاگون در حال بررسی و طراحی نوعی حمله سایبری قبل از پرتاب موشک است تا از این طریق ضمن غیرفعال سازی عملکرد موشک قبل از شلیک، کنترلی بر موشک جهت اجرای اهداف از پیش تعریف شده خود داشته باشد (Bill، 2016).

– کرم استاکس‌نت[5] که با تکیه بر تروجان‌های سخت‌افزاری موجود در زیرساخت‌های صنعتی هسته‌ای، توانست در PLC های زیمنس، صنایع هسته‌ای اخلال ایجاد نماید و خسارت‌های به زیرساخت‌ها هسته‌ای وارد نماید (Falliere et al.، 2011: 4).

با توجه به گزارش‌ها و پژوهش‌های فوق به‌عنوان بخش جزئی از خسارت‌های وارده شده از طریق امنیت سخت‌افزار و تروجان‌های سخت‌افزاری، می‌توان به اهمیت شناخت وجود تروجان سخت‌افزاری در لایه‌های فیزیکی محیط اطلاعاتی و فضای سایبری پی برد. تروجان‌های سخت‌افزاری عملکردی

[3] Sandy Bridge
[4] FPGA
[5] Military Grade
[6] ACTEL
[1] Stuxnet

معمولاً از دو بخش محرک و بار تشکیل شده‌اند. مدار محرک ذاتاً یک مدار غیرفعال با کاربری نظارتی، بدون اثر عملکردی بر کارایی مدار هست و در زمان بهره‌برداری از سامانه هدف، متناسب با رخداد شرایط خاص یا شرایط از پیش تعریف شده برای آن، بخش بار تروجان را فعال می‌نماید. بخش بار تروجان سخت‌افزاری مسئولیت پیاده سازی وظیفه تعریف شده برای تروجان را بر عهده دارد. مطابق با شکل دسته‌بندی نسبتاً جامعی متناسب با خصوصیات تروجان‌های سخت‌افزاری ارائه شده است که این خصوصیات شامل: فاز تزریق تروجان به مدار، سطح انتزاع تروجان، مکانیسم فعال‌سازی تروجان، تأثیر و عملکرد تروجان و مکان تروجان است.



شکل (۳) دسته‌بندی تروجان‌های سخت‌افزاری بر اساس خصوصیات مختلف (Tehranipoor & Wang،2011: 327)

همان‌طور که در دسته‌بندی شکل ۳ نشان داده شده تروجان‌های سخت‌افزاری می‌توانند در فازهای مختلف طراحی تا اسمبل کردن در سامانه هدف، جایگذاری و سپس به‌وسیله حسگرهای مختلفی فعال شوند. تروجان‌ها از لحاظ عملکردی، آسیب‌های مختلفی را متناسب با مأموریت‌های تعریف شده و خسارت‌های ناشی از اعمال تغییرات، به سامانه هدف وارد می‌نمایند. محل نصب و تزریق تروجان متناسب با نوع اهداف و شرایط لازم برای جایگذاری متفاوت هستند. برخی تروجان‌ها به‌گونه‌ای طراحی شده‌اند که همیشه روشن باشند یا ممکن است تا زمان تحریک شدنشان توسط شرایط تعریف شده برای محرک، خاموش بمانند. یک تروجان همیشه روشن، در تمام زمان‌ها، تراشه را تحت تأثیر قرار می‌دهد. یک تروجان تحریک شونده برای فعال شدن، نیاز به یک رویداد داخلی یا خارجی دارد؛ زمانی که برای اولین بار محرک تروجان فعال شود، می‌تواند برای همیشه فعال بماند یا پس از مدتی مجدد به حالت خاموش بازگردد (Tehranipoor & Wang،2011).

پیامدها و راه‌کارهای شناسایی تروجان‌های سخت‌افزاری

تروجان‌های سخت‌افزاری بسته به هدف سازنده و مدار مورد هدف تروجان می‌توانند اهداف متفاوتی را دنبال نمایند و شدت اثرات آن‌ها بر روی سخت‌افزار یا سامانه هدف می‌تواند در بازه‌ای از اختلال‌های ظریف تا خرابی‌های فاجعه‌آمیز سامانه قرار گیرد. دسته‌ای از آن‌ها می‌توانند همیشه فعال بوده و تنها از طریق یک کانال مخفی، موجب نشت اطلاعات سرّی سامانه شوند. دسته دیگر می‌توانند با رخداد در شرایطی بسیار نادر موجب تغییر عملکرد سامانه شوند و از سوی دیگر تغییر در خصوصیات ساخت مدار نیز می‌تواند موجب کاهش اطمینان‌پذیری مدار طراحی شده شود. اساساً تروجان‌های سخت‌افزاری به صورت‌های مختلف می‌تواند عمل کنند:

۱. در زمان مشخص و یا در یک وضعیت مشخص سیستم را از کار بیندازند.

۲. باعث نشت اطلاعات در زمان اجرا با استفاده از یک واسط انتقال اطلاعات در سامانه شوند.

۳. باعث ایجاد تغییرات در روند اجرای برنامه و هدایت سامانه به اجرای برنامه‌های مخرب از قبل تعبیه شده شود.

۴. باعث ایجاد تغییرات در روند اجرای برنامه و دور زدن یکسری دستورالعمل‌های کنترل دسترسی مانند کلمات عبور شوند.

۵. باعث تغییر در روند داده‌های بحرانی سامانه شده و به اطلاعات محرمانه دسترسی پیدا می‌کنند.

یک تروجان می‌تواند با تغییر عمدی پارامترهای دستگاه موجب کاهش کارایی آن شود. این نوع عملکرد عمدتاً توسط تروجان‌های پارامتری صورت می‌گیرد. آن‌ها ممکن است خصوصیات عملکردی، واسط یا پارامتری همچون توان مصرفی و تأخیر را تغییر دهند. تروجان‌های پارامتری با تغییر در خصوصیات مدار موجب وارد شدن خرابی‌هایی همچون خرابی‌های Stuck-at یا خرابی اتصال کوتاه و نیل مدار مجتمع به تولید خروجی‌های خطادار می‌شوند. برای مثال، یک تروجان ممکن است تعداد بافرهای بیشتری را در ارتباطات تراشه وارد کند؛ درنتیجه موجب مصرف توان بیشتر گردد که باطری را به‌سرعت تخلیه خواهد کرد.

تروجان گاهی عامل نشت اطلاعات حساس از سیستم است. این نوع عملکرد تروجان‌های سخت‌افزاری مستلزم ایجاد تغییرات سخت‌افزاری در مدار اصلی باهدف ارسال اطلاعات حساس از سامانه اطلاعاتی به دشمن، بدون اطلاع یا همکاری سامانه اطلاعاتی یا کاربر سامانه است. این کار می‌تواند از طریق کانال‌های مخفی یا آشکار صورت پذیرد. مکانیسم‌های ارسال نیز ممکن است از مسیرهای داخلی یا خارجی خود سامانه استفاده کرده یا از طریق کانال‌های جانبی اقدام به ارسال اطلاعات نمایند. ارسال اطلاعات از طریق کانال جانبی می‌تواند از طریق رسانه‌هایی همچون فرکانس رادیویی، نور، دما، توان مصرفی و زمان‌بندی صورت پذیرد. ارسال‌ها همچنین می‌توانند در حاشیه نویز خصوصیات فیزیکی یا عملکردی مدار مجتمع مخفی شوند. جین و ماکریس (Jin & Makris، 2010) کلیدهای رمزنگاری را از طریق حاشیه‌های دامنه انتقال بی‌سیم یا فرکانس‌هایی که به‌دلیل تغییرات روند به وجود می‌آید نشت داده‌اند و لین و همکارانش (Lin et al.، 2009) داده‌ها را از طریق یک تکنیک کانال جانبی طیف گسترده در زیر سطح نویز روند CMOS نشت داده‌اند.

یک تروجان می‌تواند در کارایی دستگاه هدف تغییر ایجاد نموده و موجب به روز خطاهای ظریفی شود که به‌سادگی قابل‌کشف نیستند. برای مثال، یک تروجان ممکن است باعث شود یک ماژول کشف خطا، ورودی‌هایی را که نباید بپذیرد، قبول نماید. این دسته همچنین شامل تروجان‌هایی می‌شود که خصوصیات طراحی را به‌نحوی تغییر می‌دهند که موجب ایجاد عملکردی متفاوت از عملکرد مطلوب در سامانه می‌شود. مثال تغییر عملکرد رادار سوریه که در مقالات مختلفی بیان شده از این دسته است (Adee، 2008: 2; Bilzor et al.، 2011:1).

تروجان‌های تکذیب سرویس[1] می‌توانند مانع از انجام کار یک تابع یا منبع شوند. یک تروجان ممکن است باعث تمام شدن منابع حیاتی و کمیابی همچون پهنای باند، توان محاسباتی و توان باتری شود. یک تروجان ممکن است موجب تخریب فیزیکی، غیرفعال شدن یا تغییر پیکربندی دستگاه شود. برای مثال تروجانی باعث نادیده‌گیری پردازنده درخواست وقفهٔ یک دستگاه جانبی خاص می‌شود. در نهایت تروجان‌های سخت‌افزاری می‌توانند برای کمک به اجرای حملات مبتنی بر نرم‌افزار، همچون حملات ارتقای سطح دسترسی، ورود از طریق درب پشتی، سرقت کلمه عبور و حملات تکذیب سرویس طراحی شوند.

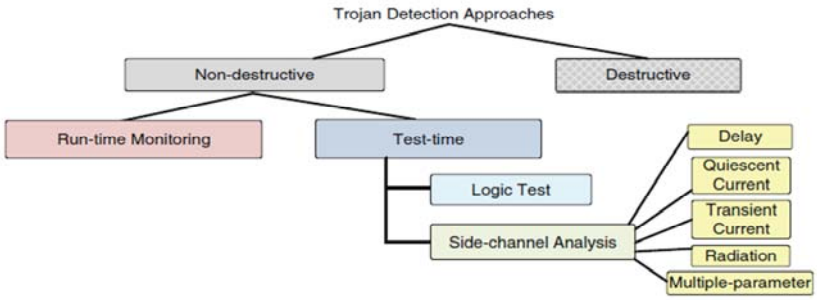
روش‌های تشخیص تروجان‌های سخت‌افزاری به دودسته کلی روش‌های تخریبی و روش‌های غیر تخریبی تقسیم می‌شوند. در روش تخریبی برای شناسایی مدارات تروجان ابتدا مواد بسته‌بندی با استفاده از سایش مکانیکی–شیمیایی برداشته شده و سپس با پویش میکروسکوپ الکترونی[2]، تصاویر لایه به لایه مدار مجتمع استخراج می‌شود. در نهایت با روش‌های پردازش تصویر و تشخیص الگو ساختار کل مدار استخراج می‌شود. روش‌های تخریبی به‌شدت زمان‌گیر و پرهزینه هستند به‌طوری‌که تحلیل تخریبی یک تراشه چندین ماه وقت خواهد برد. علاوه بر این با افزایش چگالی مجتمع سازی تراشه‌ها، استفاده از این روش‌ها بسیار سخت و در خیلی موارد غیرممکن می‌شود. همچنین، نتایج به‌دست‌آمده از یک آزمایش نمی‌تواند به تمام تولیدات تعمیم داده شود زیرا در برخی موارد درصدی از تراشه‌های تولید شده آلوده هستند، بنابراین هر مدار

[1] Denial of service (DOS)
[1] Scanning Electron Microscope

مجتمع برای جلب اعتماد، نیاز به آزمون جداگانه دارد. مطابق شکل ۴ روش‌های غیر تخریبی خود به دودسته تقسیم می‌شوند:

۱) روش‌های زمان آزمون: این روش‌ها به دو دسته آزمون منطقی و تحلیل کانال جانبی تقسیم‌بندی می‌شوند.

۲) روش‌های زمان اجرا: این دسته به روش‌هایی اطلاق می‌شود که فرآیند تشخیص تروجان پیش از قرار گرفتن مدار مجتمع مورد نظر در مدار اصلی‌اش انجام می‌شود



شکل (۴) دسته‌بندی روش‌های کشف تروجان (Tehranipoor & Wang،342 :2011)

روش‌های آزمون منطقی بر تولید و اعمال بردارهای آزمون برای فعال‌سازی مدار تروجان و مشاهده اثر مخرب آن در خروجی‌های اصلی تمرکز می‌کنند. در مقابل، روش‌های تحلیل کانال جانبی بر این واقعیت استوارند که درج بداندیشانه هر المانی در مدار مجتمع باید حضورش را در برخی پارامترهای کانال جانبی از جمله جریان نشتی، جریان منبع ساکن[1]، توان پویا، خصوصیات تأخیر مسیر، تشعشعات الکترومغناطیسی به‌واسطه فعالیت کلیدزنی، یا در ترکیبی از این پارامترها منعکس نماید. مزیت مهم استفاده از تحلیل کانال جانبی برای کشف تروجان‌ها عدم نیاز به فعال‌سازی کامل تروجان و مشاهده اثر مخرب آن در خروجی سامانه است؛ همچنین این روش برای کشف تروجان‌هایی که تنها برای نشت اطلاعات سامانه به‌کار رفته‌اند نیز مناسب است، درحالی‌که روش آزمون منطقی قادر به کشف این‌گونه تروجان‌ها نیست. هر چه مدار تروجان بزرگ‌تر باشد کشف آن آسان‌تر خواهد بود چراکه اثر آن بر پارامترهای کانال جانبی واضح‌تر است. درعین‌حال، وجود پدیدهٔ تغییرات فرآیند

[1] Quiescent Supply Current

ساخت[1] در مدارت مبتنی بر ابعاد نانومتری که خود منجر به تغییرات قابل‌توجه در پارامترهای مدارات می‌شود و همچنین وجود نویزهای اندازه‌گیری باعث شده است روش‌های مبتنی بر تحلیل پارامترهای کانال جانبی به‌خصوص برای مدارهای تروجانی کوچک کارآمدی خود را از دست بدهند.

روش‌های مبتنی بر زمان اجرا یکی از رویکردهای مقابله با تروجان‌های سخت‌افزاری است که در دسته روش‌های غیر تخریبی قرار می‌گیرند. ایده اصلی این روش‌ها استفاده از رفتارهای زمان اجرای سیستم برای کشف مدارهای تروجانی است. در این روش‌ها یک یا چند رفتار سطح کاربرد سامانه به‌عنوان امضا انتخاب و در زمان قبل از اجرا استخراج می‌گردند. سپس، با استفاده از یک سامانه نظارتی، امضاهای تولید شده در زمان اجرا با امضاهای تولید شده قبلی مقایسه می‌شوند. در صورت مشاهده مغایرت، سامانه نظارتی وجود یک رفتار ناهنجار را تشخیص می‌دهد و سامانه اصلی را برای جلوگیری از اثرات احتمالی وجود تروجان‌ها غیرفعال می‌کند.

تهدید شناسی امنیت سایبری حوزه موشکی بر مبنای مدل سه شاخه‌ای ذهن

همان‌طور که در بخش‌های قبل، اهمیت و کاربردهای فضای سایبری و روش‌های نفوذ و مدل سه شاخه‌ای ذهن در ادبیات موضوع تشریح شد، در این بخش تهدیدهای فضای سایبری حوزه موشکی بر اساس مدل سه‌شاخه بررسی می‌گردد. ازآنجایی‌که فضای سایبری موشکی بخشی از فضای سایبری نیروهای مسلح و کشور است و با توجه به حساسیت این حوزه در پسابرجام، دشمنان برای نفوذ به بخش‌ها و لایه‌های مختلف آن، از قابلیت‌ها، ابزارها و روش‌های نفوذ به فضای سایبری و عملیات اطلاعاتی در دوران صلح استفاده خواهند کرد. لذا در ادامه برمبنای مدل سه شاخه‌ای ذهن، تهدید شناسی فضای سایبری حوزه موشکی صورت می‌گیرد و در هر شاخه روش‌های نفوذ، تأثیرت و پیامدها و راه‌کارهای مقابله‌ای بر اساس منابع آشکار علمی و خبری و نظر خبرگان حوزه ارائه می‌گردد.

نفوذ زمینه‌ای و ساختاری

[2] Process Variations (PVs)

روش‌ها

۱. غرب به‌جای آنکه ماهیت واقعی خود به‌عنوان «مولد بحران تروریسم» در منطقه را جلوه‌گر سازد، در قالب «حلال بحران‌های امنیتی منطقه» جلوه‌گر می‌شود تا اعتماد شهروندان را برای برنامه‌های آتی خود در پسابرجام جلب نماید.

۲. با مرتبط ساختن مشکلات کشور به مسائل هسته‌ای و موشکی فضای روانی متناسب را جهت آماده سازی افکار عمومی جامعه ایجاد نماید.

۳. ضوابط و اصول سیاست خارجی کشورمان را (که آن‌ها نیز منبعث از آرمان‌های انقلاب اسلامی هستند) به تاکتیک‌هایی قابل انعطاف تقلیل داده و پس از شکستن پوسته و هسته سخت این اصول، آن‌ها را بر اساس اهداف خود انعطاف‌پذیر سازد تا مجموعه اقداماتی در حوزه موشکی شبیه به هسته‌ای انجام دهد.

۴. فعال‌سازی شبکهٔ حامیان غرب در ایران که بهره‌برداری مختلف از این شبکه‌ها به‌عنوان عامل‌های داخلی دشمنان صورت می‌پذیرد.

۵. پیگیری اهداف و مأموریت‌های خود که از طریق گسترش موضوعات مذاکرات به مسائل غیرهسته‌ای مانند حوزه موشکی انجام می‌شود.

۶. نفوذ در زیرساخت‌های هم‌طراز و مرتبط با حوزه موشکی (دانشگاهی و مراکز علمی و مراکز دولتی مرتبط) از طریق سایبری که به این وسیله اطلاعات دانشمندان و خبرگان حوزه موشکی جمع‌آوری می‌شود.

۷. نفوذ دشمن در حوزه فرهنگی با القاء ناکارآمد نشان دادن مدیریت کشور به مردم تا ضمن به چالش کشیدن مدیریت اسلامی، مانع پیشرفت برنامه‌های استراتژیک نظام مانند حوزه موشکی گردد.

۸. قرار دادن نقطه ثقل اقتصادی کشور بر مبنای «برجام»، مانع از تحقق ظرفیت‌های بالقوه نهفته اقتصادی در حوزه‌های دفاعی کشور به خصوص صنعت فضای سایبر می‌گردد.

۹. فعال شدن شرکت‌ها و صنایع سخت‌افزاری و نرم‌افزاری خارجی مرتبط با حوزه موشکی که نفوذ را تسهیل می‌نماید.

۱۰. ورود شرکت‌ها و زیرساخت‌هایی که باعث انتقال و نهادینه‌سازی فرهنگ غربی در کشور می‌شود.

۱۱. نفوذ از راه فرهنگی به‌دنبال تغییر ارزش‌های فرهنگی و اجتماعی و در نهایت دست یافتن به‌مقاصد سیاسی که در این صورت ارزش‌های حاکم بر کشور از محورهای دینی به‌محورهای دنیا گرایانه تغییر یابد و نظام دینی ماهیت خودش را از دست می‌دهد.

تأثیرات و پیامدها

۱. دشمنان با بهره‌برداری از بسترهای فضای مجازی و اجرای عملیات روانی مناسب، ایران را با اجرای برنامه‌های موشکی خود، به‌عنوان حامی تروریسم و کشوری که امنیت منطقه‌ای به خطر می‌اندازد معرفی می‌کنند. تلاش آن‌ها بر این است که دیدگاه ملت را نسبت به برنامه‌های موشکی تغییر داده و از این طریق به سیستم تصمیم‌گیری نظام در حوزه‌های مختلف فشار آورند.

۲. دشمنان برای اجرای این سیاست، علاوه بر فن‌های فریب و نفوذ، از قابلیت و ظرفیت‌های فضای مجازی استفاده بهینه می‌کنند تا ضمن سست کردن و شکستن هسته و پوسته اصول، این رویکرد را به سایر خطوط قرمز نظام– به‌عنوان‌مثال حوزه موشکی– تعمیم دهند تا از این طریق بتوانند به‌راحتی تأثیرات و اهداف مطلوب خود در این حوزه را پیاده سازی کنند.

۳. ازآنجایی‌که آمریکایی‌ها از براندازی نظامی ناامید شده‌اند، جهت تضعیف، براندازی نرم را دنبال کرده تا در روند تصمیم سازی کشور تأثیر بگذارند. از مهم‌ترین این اقدامات، تلاش برای ایجاد گسست میان ملت و حکومت جمهوری اسلامی از طریق ایجاد نارضایتی به‌وسیله تحریم‌های اقتصادی و مرتبط ساختن آن به مسائل هسته‌ای و موشکی است.

۴. یکی دیگر از راهبردهای آمریکا برای نفوذ در ایران کشاندن مذاکرات به مسائل دیگر ازجمله مباحث منطقه‌ای، حقوق بشر و حوزه موشکی است تا از این طریق بتواند در مسائل سیاسی و تصمیم‌گیری نظام دخالت و نفوذ نماید.

۵. کاهش اعتماد به‌نفس مسؤولان که نتیجه آن عقب ماندگی فناوری به خصوص فنّاوری حوزه‌های مختلف سایبری موشکی است.

۶. تضعیف توان دفاعی تسلیحاتی و موشکی جمهوری اسلامی ایران که یکی از اهداف مهم آن‌ها است.

۷. آنان به‌دنبال تضعیف قدرت منطقه‌ای جمهوری اسلامی ایران و شکست محور مقاومت در منطقه هستند.

۸. بانفوذ می‌توانند به اطلاعات، اسناد، سایت‌ها، مواد، افراد، متخصصان موشکی و روندهای آینده آن دسترسی داشته باشند و احتمال اقداماتی نظیر تحریم، ترور و سایر تهدیدات برای متخصصان را متصور بود.

۹. با ورود هدفمند شرکت‌های خاص خارجی در قالب‌های مختلف جهت انتقال فرهنگ غربی به کشور، فرهنگ غنی ایرانی و اسلامی تحت تأثیر قرار می‌گیرد.

۱۰. با اجرای برجام و ضعف‌های موجود در ساختار اقتصادی کشور، با ورود کالاهای خارجی، به‌تدریج ساخت قطعات و تجهیزات داخلی توسط صنایع دفاعی کاهش یافته، صنایع داخلی توجیه اقتصادی خود را از دست داده و مجبور به استفاده از تجهیزات خارجی می‌کند.

۱۱. با ورود تجهیزات و فناوری‌های خارجی در حوزه سایبری، وابستگی این حوزه به خارج افزایش یافته و مانع رشد صنعت بومی سایبری می‌گردد؛ این باعث افزایش تهدیدات بالقوه و بالفعل و کاهش اقتدار کشور در این حوزه می‌شود.

راه‌کارهای مقابله

۱. شناخت دشمن و توطئه‌هایش، تقویت و استحکام روحیه انقلابی، حرکت به‌سمت تحقق آرمان‌های انقلاب اسلامی.

۲. برای خنثی سازی تأثیر اقدامات دشمنان می‌بایست بااطلاع رسانی‌های مناسب و اقدامات به‌موقع توسط نخبگان سیاسی مانع القاء افکار دشمنان و سیاست‌های آنان به افراد جامعه شد تا دیدگاه و نگرش آن‌ها نسبت به برنامه‌های راهبردی نظام مثبت بوده و مانند همیشه پشتیبان نظام باشند.

۳. متخصصان و پژوهشگران حوزه موشکی در دانشگاه‌ها و مراکز علمی توجیه امنیتی شده و از اطلاعات متخصصان در همه سازمان‌ها، محافظت کامل صورت پذیرد.

۴. از مدیران انقلابی، دلسوز و متخصص در حوزه‌های زیرساخت‌های مهم و حیاتی استفاده شود.

۵. از دستاوردهای شرکت‌های دانش‌بنیان داخلی بهره‌برداری شود.

۶. سیاست‌های اقتصاد مقاومتی پیاده سازی شده و شرکت‌های دانش‌بنیان مرتبط با حوزه موشکی به خصوص زیرساخت‌های سایبری با توجه به اهمیت این حوزه و راه‌های محتمل نفوذ تقویت شوند.

۷. باید نسبت به مقوله «اقتصاد درون‌زا» یا همان اقتصاد مقاومتی به‌شکلی که مد نظر مقام معظم رهبری است، به‌مثابه تنها نسخه مقابله بانفوذ اقتصادی غرب از طرق مختلف در دوران پسا برجام نگریست و سیاست تکیه بر دانش بومی در ساخت و به روز نمودن زیرساخت‌های موشکی در اولویت ویژه قرار گیرد.

۸. سیاست‌ها و برنامه‌های استراتژیک جهت مقابله با تهدیدات فرهنگی و رفع آسیب پذیری‌های فرهنگی به خصوص در فضای سایبری اتخاذ و اجرا شوند.

۹. آگاهی بخشی در حوزه‌های مختلف به خصوص فرهنگی جهت مقابله با تبلیغات و عملیات روانی دشمن و تشریح سناریوهای دشمن در مواقع حساس و گرفتار نشدن در دام دشمن به ویژه در حوزه سایبر انجام شود.

نفوذ زیرساختی

روش‌ها

۱. تجهیزات و سامانه‌های نظامی غیربومی در حوزه‌های مختلف و مرتبط با حوزه موشکی خریداری و به‌کارگیری شود.

۲. از مستشاران نظامی خارجی پس از عادی شدن روابط در حوزه‌های مختلف سایبری جهت ارتقا و رفع مشکلات موجود استفاده شود.

۳. هک و نفوذ به زیرساخت‌های سایبری جهت نفوذ و جمع‌آوری اطلاعات صورت پذیرد.

۴. حملات سایبری از طریق نفوذ بدافزار به زیرساخت‌های سایبری از طریق راه‌کارهای مختلف نفوذ انجام شود.

۵. شراکت در فضای سایبری انجام شده و در فضای مشترک سایبری رخنه شود.

تأثیرات و پیامدها

۱. کند شدن و توقف پیشرفت حرکت علمی کشور به خصوص در حوزه موشکی که عقب ماندگی در این حوزه را در پی دارد.

۲. یکی از اهداف ورود مستشاران خارجی، ضمن کمک در حوزه کاری مربوطه، جاسوسی از زیرساخت‌های نظامی به ویژه صنایع بومی به و ارزیابی توان موشکی کشور، جمع‌آوری اطلاعات سامانه‌ها و طراحی سناریوهای مختلف برای نفوذ از مسیرهای متعارف و غیرمتعارف سایبری است.

۳. نفوذ و جاسوسی از طرح‌ها، نقشه و معماری‌های زیرساخت‌های موشکی با سوءاستفاده از آسیب‌پذیرها و تروجان‌های سخت‌افزاری از طریق روش‌های متعارف و غیرمتعارف، همچنین از کار انداختن سامانه‌ها در شرایط عملیاتی انجام می‌شود.

۴. نفوذ و جاسوسی از مجموعه اقدامات و برنامه‌های حوزه موشکی با بهره‌گیری از تروجان‌های نرم‌افزاری و از کار انداختن سامانه‌ها در شرایط عملیاتی صورت می‌پذیرد.

۵. جاسوسی، تخریب، تغییر اطلاعات و کارکرد سامانه‌ها، همچنین فعال‌سازی تروجان‌های سخت‌افزاری و نرم‌افزاری از طریق نفوذ تروجان‌ها به زیرساخت‌ها انجام می‌شود.

۶. هک و نفوذ به سیستم سایبری موشک، همچنین کنترل و هدایت در حین انجام عملیات و بهره‌برداری‌های معکوس از آن استفاده می‌شود.

۷. اخلال و جاسوسی به‌وسیله فضای مشترک سایبری از زیرساخت‌های موشکی به‌وسیله تروجان‌های نرم‌افزاری و سخت‌افزاری که نتیجه آن‌ها اخلال و افشای اطلاعات سایبری و سهل‌الوصول کردن حملات سایبری و پس از آن حملات سخت نظامی است.

راه‌کارهای مقابله

۱. تجهیزات سخت‌افزاری در آزمایشگاه‌های مرجع امنیت سخت‌افزاری، آزمون و ارزیابی شوند.

۲. بهره‌برداری و تولید از روش‌های کشف و تحلیل تروجان‌های سخت‌افزاری نوین به‌صورت بومی انجام شود.

۳. سامانه‌ها و ماژول‌های نرم‌افزاری در آزمایشگاه‌های مرجع تحلیل بدافزار، آزمون و ارزیابی شوند.
۴. بهره‌برداری از روش‌های نوین ارزیابی نرم‌افزار و تولید سامانه‌ها و ماژول‌ها به‌صورت بومی انجام شود.
۵. سامانه‌های امنیتی و دفاعی به‌روز شده، همچنین از آخرین فناوری و سیاست‌های امنیتی حوزه سایبری استفاده شود.
۶. دستورالعمل‌های مناسب حفاظتی امنیتی برای حضور مستشاران نظامی تهیه و ابلاغ شود.
۷. سیاست‌های مناسب امنیتی و حفاظتی در قبال رسانه‌های قابل‌حمل پیاده سازی شود.
۸. سامانه‌های حساس مطابق با سطح محرمانگی آن‌ها جداسازی و ایزوله شوند.
۹. سناریوهای متنوع مقابله با عملیات نفوذ و حملات سایبری دشمن طراحی و اجرا شود.
۱۰. دانش و فناوری‌های کلیدی مرتبط با عملیات اطلاعاتی دشمن توسعه داده شده و بهره‌برداری از ابزارهای کارآمد مرتبط انجام شود.
۱۱. سامانه‌های سایبر الکترونیکی، ضد سامانه‌ها و تسلیحات دشمن، متناسب با هر پیامد تولید یا بومی‌سازی شود.
۱۲. به‌دلیل غیربومی بودن بیشتر سامانه‌های سخت‌افزاری و نرم‌افزاری، در برنامه اقدام مشترک در حوزه‌های سایبری شرکت نشود.
۱۳. آگهی وضعیتی مطلوب از تغییرات و حملات سایبری داخلی و بین‌المللی داشته و سناریوهای مقابله‌ای متناسب با شرایط به روز گردد.

نفوذ رفتاری

روش‌ها

۱. فریب متخصصان سست‌عنصر و ناآگاه به همکاری با دشمنان که در راستای نفوذ صورت می‌پذیرد.
۲. سوءاستفاده و جاسوسی از طریق شبکه‌های اجتماعی و سامانه‌های ارتباطی که از شبکه پژوهشگران و نخبگان حوزه موشکی انجام می‌شود.

۳. پیشنهاد و ترغیب متخصصان به بهره‌برداری از تجهیزات و بردهای غیربومی دارای تروجان‌های سخت‌افزاری، جهت استفاده در زیرسیستم‌های حوزه موشکی با بهره‌برداری از راه‌کارهای مختلف مهندسی اجتماعی صورت می‌پذیرد.

۴. پیشنهاد و ترغیب متخصصان به بهره‌برداری از سامانه‌ها و ماژول‌های نرم‌افزاری غیربومی که شرکت‌های وابسته به دشمنان آن‌ها را تولید کرده‌اند. این سیستم‌ها گاهی دارای اشکالات نرم‌افزاری یا قابلیت کنترل از راه دور جهت استفاده در زیرسیستم‌های حوزه موشکی هستند.

۵. روحیه پژوهشگران و متخصصان حوزه موشکی با اجرای عملیات روانی متنوع بر آن‌ها یا خانواده‌های ایشان تضعیف کرد.

تأثیرات

۱. از زیرساخت‌های حوزه موشکی جاسوسی کرده و تزریق تروجان‌ها به زیرساخت‌های سایبری موشکی جهت کنترل، تخریب و جاسوسی انجام می‌شود.

۲. بهره‌برداری و تحلیل از اطلاعات موجود در شبکه‌های اجتماعی که سرورهای آن‌ها را در اختیار دارند. آن‌ها با بهره‌گیری از ابزارهای خاص می‌توانند کاربران و نخبگان حوزه موشکی را رصد و تحلیل نموده و ضمن جمع‌آوری اطلاعات از طریق نفوذ و نشت اطلاعات توسط کاربران، روندهای آینده حوزه موشکی را به‌طور مستقیم و غیرمستقیم استخراج نمایند.

۳. سامانه‌ها و تجهیزات آلوده به زیرساخت موشکی وارد کرده که در زیرساخت‌ها تأثیرگذار می‌شوند.

۴. پیشرفت علمی و فناوری حوزه موشکی به‌دلیل تخریب و تضعیف روحیه پژوهشگران و متخصصان موشکی از طریق فضای سایبری کاهش پیدا می‌کند.

راه‌کارهای مقابله

۱. تهیه و ابلاغ سیاست‌های امنیتی و حفاظتی مناسب در خصوص عدم بهره‌برداری یا استفاده هوشمند از شبکه‌های اجتماعی برای افراد درگیر در حوزه‌های مختلف موشکی و مصون سازی در مقابل نفوذ از طریق مهندسی اجتماعی انجام شود.

۲. سناریوهای متنوع مقابله با عملیات نفوذ و روانی دشمن به خصوص در حوزه سایبری با توجه با تأثیرات آن بر کاربران طراحی و اجرا گردد.

۳. آموزش و مدیریت دانش و مهارت‌های مرتبط با هر پیامد با توجه به سوابق گذشته و روندهای آینده حملات و نفوذ انجام شود.

۴. مواظبت و مراقبت همیشگی از کارکنان حوزه موشکی و خانواده‌های آن‌ها با برگزاری دوره‌های بصیرت افزایی و تقویت روحیه جهادی کارکنان حوزه موشکی صورت پذیرد.

بحث

بر اساس مدل سه شاخه‌ای ذهن، دشمنان در راستای نفوذ برای هر سه‌شاخه ذکر شده برنامه‌ریزی کرده‌اند. با بهره‌برداری از شبکه‌های اجتماعی، وب‌سایت‌های خبری و سایر رسانه‌ها، تبلیغات زیادی علیه اهداف و استراتژی‌ها و برنامه‌های موشکی خواهند داشت. این اقدامات ضمن تغییر نگرش مردم ایران نسبت به مسائل موشکی، مسؤولان را تحت فشار قرار داده تا علاوه بر رخنه در چرخه تصمیم‌گیری و تصمیم سازی در حوزه‌های مختلف مرتبط با موشکی، شرایط لازم جهت ایجاد نفوذ بیشتر و دودستگی در بین مسؤولان فراهم آورند. در ضمن با بهره‌برداری از تروجان‌های طراحی شده به‌صورت نرم‌افزاری یا سخت‌افزاری توسط دشمنان و سایر کشورهای صاحب فناوری، شرایط لازم جهت جاسوسی از اطلاعات سامانه‌ها و زیرساخت‌های موشکی و سایر سامانه‌های مرتبط را ایجاد می‌کنند. با دسترسی‌های غیرمجاز به شبکه همکاران و نخبگان حوزه موشکی و اطلاعات آن‌ها، در زمان‌های مختلف از آن‌ها بهره‌برداری لازم را خواهند برد.

یکی از اهداف مهم دشمنان نفوذ در لایه‌های اطلاعاتی و فیزیکی سایبری حوزه موشکی است که این مهم می‌تواند از طریق تروجان‌های سخت‌افزاری در تجهیزات سخت‌افزاری وارداتی صورت گیرد. برای بهبود سطوح امنیتی تراشه‌های پردازشی خریداری شده در صنایع نظامی/دفاعی کشور می‌بایست راه‌حلی ارائه گردد تا بتواند وجود تروجان‌های سخت‌افزاری را به توجه به شرایط بومی تشخیص و از اقدامات تخریبی و جاسوسی جلوگیری نماید. برای ارائه روش نوین بومی، می‌توان از یک سامانه نظارتی که به‌صورت مجموعه‌ای از سخت‌افزار و نرم‌افزار ارائه گردد، با انجام مرحله

آموزش مناسب به این سامانه با استفاده از روش‌های مختلف داده‌کاوی و یادگیری ماشین، با بهره‌برداری از رفتارهای گذشته سامانه، به‌صورت برخط از سامانه اصلی در حال کار نظارت نموده و در صورت به روز ناهنجاری آن‌ها را تشخیص و گزارش نماید. سامانه ناظر در صورت تشخیص هر ناهنجاری که نماینده فعالیت تروجان در سامانه اصلی است، اعلام‌خطر خواهد کرد و بنا به کاربرد و تنظیمات انجام شده، می‌تواند سامانه اصلی را از کار بیندازد و یا فعالیت آن‌ها را محدود کند. سامانه سخت‌افزاری/نرم‌افزاری ناظر، با توجه به ناهنجاری‌هایی که یک تروجان سخت‌افزاری در حین فعالیت در رفتار یک سامانه ایجاد می‌کند، فعالیت تروجان‌ها را تشخیص خواهد داد. از همین رو سامانه ناظر می‌تواند در گستره وسیعی از سیستم‌های پردازشی مبتنی بر میکروکنترلر، تراشه‌های پردازشی و یا برنامه‌پذیر، عمل نظارت را انجام دهد. به عبارت دقیق‌تر می‌توان گفت در سامانه‌های به کار رفته در صنایع دفاعی/نظامی شامل سامانه‌های کنترل موشک، کنترل هواپیما، رادارها، کنترلرهای تجهیزات سنگین و نیمه سنگین نظامی مانند تانک، سامانه‌های مخابراتی و شبکه‌ای نظامی، سامانه‌های کنترلی خطوط تولید ادوات نظامی استفاده شود. لذا سامانه ناظر سعی دارد تا با به‌کارگیری روش‌های شناسایی و دفع خطر تروجان‌های سخت‌افزاری، امنیت سامانه‌های به کار رفته در صنایع دفاعی/نظامی را بهبود بخشد. به‌این ترتیب می‌توان امیدوار بود که از بروز حوادثی مانند آنچه در بخش‌های قبل اشاره شد و یا حملات معروف فلیم[1] و استاکس‌نت جلوگیری شود یا حداقل درصد آن‌ها کاهش قابل‌توجهی داشته باشد. در کشور، مواردی از این حملات مثل حمله بدافزارها به زیرساخت‌های حیاتی گزارش شده است که صدماتی هم از دید فنی و هم از دید بین‌المللی به کشورمان وارد نموده است. تحقیقات نشان داده است که این حملات یا تماماً بر اساس تروجان‌های سخت‌افزاری انجام می‌شوند، یا اینکه در روند رخنه و اثرگذاری آن‌ها از تروجان‌های سخت‌افزاری استفاده شده است. خسارات مالی و ملی حاصل از رخنه تروجان‌های سخت‌افزاری در سامانه‌های دفاعی ابعاد پنهانی دارد که تنها پس از بروز تقابل‌های نظامی آشکار می‌گردد.

نتیجه‌گیری

[1] Flame

ازآنجاکه شناخت راهبردهای نفوذ دشمن در ارکان سیاسی، فرهنگی و اقتصادی و ارکان دیگرِ کشور در پسابرجام، از خود برجام هم مهم‌تر است؛ لذا نباید اجازه داد برجام وسیله‌ای برای تأثیرگذاری دشمن در روند تصمیم سازی کشور و حوزه‌های حیاتی و خطوط قرمز نظام مثل حوزه موشکی باشد. بر همین اساس در این پژوهش ضمن بررسی فضای سایبر و مؤلفه‌های مختلف آن، قابلیت‌های این فضا برای نفوذ دشمن در حوزه‌های مختلف بررسی شده است. فضای سایبر شامل سه لایه شناختی، اطلاعاتی و فیزیکی است که در بحث نفوذ در امنیت سایبری حوزه موشکی دشمن سعی دارد از آسیب پذیری‌های این لایه‌ها به اهداف مورد نظر نفوذ نماید. لذا بر این اساس ضمن بررسی و شناخت امنیت سخت‌افزار و تروجان‌های سخت‌افزاری، به‌عنوان یکی از سناریوهای نفوذ دشمن به‌حوزه موشکی، سایر حوزه‌های مرتبط نیز بررسی و نتایج آن ارائه شده است. در این پژوهش با بهره‌برداری از مدل سه شاخه‌ای ذهن، امنیت سایبری حوزه موشکی و تأثیرات آن نیز بررسی شد. در پایان مطابق با نتایج بخش‌های مختلف، پیشنهاد می‌گردد که سیاست‌های لازم امنیتی و دفاعی در کلیه حوزه‌های سایبری مرتبط با زیرساخت‌های موشکی به‌کارگیری شود تا ضمن جلوگیری از رخنه، از تخریب فیزیکی زیرساخت‌ها و اطلاعات سامانه‌های مربوطه جلوگیری گردد. سامانه‌های امنیتی و دفاعی و هشدار دهی در همه لایه‌های فضای سایبری، متناسب با روندهای آینده حوزه سایبری به‌روزرسانی شوند. در ضمن لازم است تحقیقات متناسب با پیشرفت کشورهای پیشرو در دانش و فناوری حوزه‌های سایبری به خصوص موضوع امنیت سخت‌افزار، تعیین و پیش‌بینی شود.

منابع و مآخذ

منابع فارسی

۱. امام خامنه‌ای، سید علی (۹۴/۶/۲۵) (۱). "نفوذ فرهنگی و سیاسی خطرناکتر از نفوذ اقتصادی و امنیتی است/ دشمن بدنبال دگرگون کردن باورهای جامعه و نفوذ در مراکز تصمیم‌گیری و تصمیم سازی است". در دیدار هزاران نفر از فرماندهان سپاه. پایگاه اطلاع رسانی دفتر مقام معظم رهبری. بازیابی شده در ۹۶/۰۹/۲۸ در آدرس: https://goo.gl/YrvbVp

۲. امام خامنه‌ای، سید علی (۹۴/۰۷/۱۵) (۲)، "عده‌ای سهل‌اندیش، مذاکره با شیطان بزرگ را توجیه می‌کنند/ مذاکره با امریکا یعنی باز کردن راه نفوذ و تحمیل". در دیدار فرماندهان و کارکنان نیروی دریایی سپاه. پایگاه اطلاع رسانی دفتر مقام معظم رهبری. بازیابی شده در ۹۶/۰۹/۲۸ در آدرس: https://goo.gl/vn349b

۳. دهقان رضا؛ طالبی کامبیز؛ عربیون ابوالقاسم (۱۳۹۱). پژوهشی پیرامون عوامل مؤثر بر نوآوری و کارآفرینی سازمانی در دانشگاههای علوم پزشکی کشور، پیاورد سلامت (دوره ۶ صص. ۲۲-۳۳)
۴. میرزایی، حسن؛ سرسک، محمد علی (۱۳۸۴). نگاهی به معرفت شناسی سازمانی: سیر تحول، مکاتب و کاربردهای مدیریتی. فصلنامه پیک نور، سال ۳، شماره ۳

منابع انگلیسی

1. Adee، S. (2008). The hunt for the kill switch. Spectrum، IEEE، 45(5)، 1. 34-39.
2. Alkabani، Y.، & Koushanfar،2. F. (2008). Designer's hardware Trojan horse. Paper presented at the Hardware-Oriented Security and Trust، 2008. HOST 2008. IEEE International Workshop on.
3. Andress، J.، & Winterfeld، S. (2013). Cyber warfare: techniques،3. tactics and tools for security practitioners: Elsevier.
4. Armistead، 4. L. (2004). Information operations: Warfare and the hard reality of soft power: Potomac Books، Inc.
5. Army، 5. U. (2010). Cyberspace Operations Concept Capability Plan 2016-2028. US Army Capabilities Integration Center.
6. Bill، 6. G. (2016). Pentagon Developing Pre-Launch Cyber Attacks on Missiles. Retrieved from http://freebeacon.com/national-security/pentagon-developing-pre-launch-cyber-attacks-missiles/

7. Bilzor، M.، Huffmire، T.، Irvine، C.، & Levin، 7. T. (2011). Security checkers: Detecting processor malicious inclusions at runtime. Paper presented at the Hardware-Oriented Security and Trust (HOST)، 2011 IEEE International Symposium on.
8. Cordesman، 8. A. H. (2002). Strategic Threats and National Missile Defenses: Defending the US Homeland: Greenwood Publishing Group.
9. Denning، 9. D. E. R. (1999). Information warfare and security (Vol. 4): Addison-Wesley Reading.
10. Falliere، N.، Murchu، L. O.، & Chien، E. (2011). W32. stuxnet dossier. White paper،10. Symantec Corp.، Security Response، 5.
11. Gomez، 11. D. (2010). Intel to introduce processor with remote kill switch Retrieved from (online) http://www.tgdaily.com/opinion-features/53108-intel-to-introduce-processor-with-remote-kill-switch#kSQLHXf7zvGslGxK.99
12. Jin، Y.، & Makris، 12. Y. (2010). Hardware trojans in wireless cryptographic integrated circuits.
13. Johnson، 13. R. (2011). The Navy Bought Fake Chinese Microchips That Could Have Disarmed U.S. Missiles. Retrieved from http://www.businessinsider.com/navy-chinese-microchips-weapons-could-have-been-shut-off-2011-6
14. Libicki، 14. M. C. (1995). What is information warfare? Retrieved from

15. Lin، L.، Kasper، M.، Güneysu، T.، Paar، C.، & Burleson، 15. W. (2009). Trojan side-channels: lightweight hardware trojans through side-channel engineering Cryptographic Hardware and Embedded Systems-CHES 2009 (pp. 382-395): Springer.
16. Romanych، 16. M. J. (2005). A theory-based view of io. IO Sphere Joint Information Operations Center، 14-18.
17. Rumsfeld، D. H. (2002). Transforming the military. Foreign Affairs،17. 20-32.
18. Skorobogatov، S.، & Woods، 18. C. (2012). Breakthrough silicon scanning discovers backdoor in military chip. Paper presented at the International Workshop on Cryptographic Hardware and Embedded Systems.
19. Staff، 20. J. (2012). Information Operations: Department of Defense (JP 3-13).
20. Staff، 21. J. (2010). Department of Defense Dictionary of Military and Associated Terms (JP 1-02).
21. Tehranipoor، M.، & Wang، 22. C. (2011). Introduction to hardware security and trust: Springer Science & Business Media.
22. Williams، 23. P. A. (2010). Information Warfare: Time for a redefinition.