فصلنامه راهبرد دفاعی، سال سیزدهم، شماره ۵۰، تابستان ۱۳۹۴

فرماندهی معظم کل قوا: مجموعهٔ زنجیرهٔ به هم پیوستهٔ رسانه‌های گوناگون – که حالا اینترنت هم داخلش شده است و ماهواره‌ها و تلویزیون‌ها و رادیوها – در جهت مشخصی حرکت می‌کنند تا سررشتهٔ تحولات جوامع را به عهده بگیرند. (۱۳۸۷/۳/۱۲)

راهکارهای مقابله با تهدیدهای سایبری علیه جمهوری اسلامی ایران با تأکید بر نقش فناوری و منابع انسانی

بهمن ابراهیمیان[۱]، علی توشه[۲]، ابراهیم پورهادی[۳]

تاریخ دریافت: ۹۳/۱۰/۱ تاریخ پذیرش: ۹۴/۴/۲۲

چکیده

ناکامی در عرصهٔ تهدیدهای سخت و هزینه‌بر بودن آن، موجب تغییر راهبرد دشمنان نظام اسلامی شد. استفاده از ظرفیت‌های موجود در فضای سایبری به‌عنوان راهبرد تقابل با ج.ا. ایران، در کانون توجه استکبار جهانی قرار دارد. هدف پژوهش حاضر، شناسایی و ارزیابی تهدیدهای سایبری در دو حوزهٔ نرم و سخت، آسیب‌های موجود، فرصت‌های مقابله و ارائهٔ راهکار است. به این منظور، مؤلفه‌های اساسی در حوزهٔ تهدیدها، آسیب‌ها و فرصت‌ها از طریق مصاحبه با ۵۲ نفر از خبرگان حوزهٔ فضای سایبری، احصا و با تکمیل پرسشنامه‌ای با آلفای کرونباخ ۰/۸۶ مورد ارزیابی قرار گرفت. نتایج تحقیق نشان داد ابعاد اقتصادی، امنیتی و نظامی بیشترین اثرپذیری را در برابر تهدیدهای سایبری دارند و مهم‌ترین آسیب‌پذیری‌ها، استفاده از تجهیزات غیربومی و عدم رعایت پدافند غیرعامل است. همچنین با توجه به نظر خبرگان، در حوزهٔ فناوری، رعایت امنیت فضای تبادل اطلاعات، توسعهٔ مراکز عملیات امنیت شبکه و انتقال مراکز نگهداری داده به داخل کشور پیشنهاد و در حوزهٔ نیروی انسانی، الگویی برای شناسایی، توانمندسازی و شبکه‌سازی فعالان عرصهٔ فضای سایبری ارائه گردید.

واژگان کلیدی: فضای سایبری، تهدیدهای سایبری، آسیب‌پذیری، فناوری، نیروی انسانی.

۱. کارشناس ارشد مهندسی فناوری اطلاعات، پژوهشگر و مدرس دانشگاه. bahman.ebrahimian@modares.ac.ir
۲. دانشجوی دکترای مدیریت استراتژیک، پژوهشگر و مدرس دانشگاه.
۳. کارشناس ارشد جغرافیای سیاسی، پژوهشگر.

۱. کلیات

۱-۱. بیان مسئله

پیروزی انقلاب اسلامی، منافع استکبار جهانی و هم‌پیمانان منطقه‌ای و داخلی آنها را با تهدیدهای جدی مواجه کرد، به همین علت از ابتدای پیروزی انقلاب اسلامی، سلطه‌گران جهانی با بهره‌گیری از توانمندی‌های نظامی، اقتصادی، سیاسی، اجتماعی و فرهنگی، تهدیدهای گوناگونی را متوجه نظام اسلامی کرده تا زمینهٔ براندازی آن را مهیا کنند. در ابتدای کار، بهره‌گیری از تهدیدهای سخت نظامی، کودتا و ترور در سرلوحهٔ اقدام‌های دنیای غرب قرار گرفت که با رهبری داهیانهٔ حضرت امام (ره) و مقام معظم رهبری و حضور گستردهٔ مردم ایران اسلامی در صحنه‌های مورد نیاز، توطئه‌های دشمنان یکی پس از دیگری با شکست مواجه گردید.

ناکامی در عرصهٔ تهدیدهای سخت و هزینه‌بر بودن آن، موجب تغییر راهبرد دشمن شد. دنبال کردن نبردهای نیمه‌سخت و نرم و استفاده از ظرفیت‌های موجود در فضای سایبری به‌عنوان گزینه‌های اولویت‌دار و آزمون‌شده در کشورهای دیگر بود که مورد توجه استکبار جهانی به‌منظور تقابل با جمهوری اسلامی ایران قرار گرفت. تهدیدهای سایبری که علیه کشور، قابلیت وقوع دارد در دو حوزهٔ سخت و نرم قابل دسته‌بندی هستند. از جمله تهدیدهای سایبری در حوزهٔ سخت، تهدیدها علیه مراکز و زیرساخت‌های حساس و مهم مانند تأسیسات هسته‌ای، مراکز نظامی و امنیتی، نهادهای حکومتی و وزارتخانه‌هایی مانند نفت (پالایشگاه‌ها و خطوط انتقال)، نیرو (شبکه‌های توزیع برق، گاز، آب)، اقتصاد (بانک‌ها)، ارتباطات (شبکه‌های تلفن ثابت و همراه)، کشور و زیرمجموعه‌های آن (مانند استانداری‌ها و فرمانداری‌ها) می‌باشد. مهم‌ترین تهدیدها در حوزهٔ نرم نیز عبارتند از انتشار اخبار غیرموثق علیه مسئولان، شخصیت‌ها و نهادها، ایجاد پایگاه‌های اینترنتی هرزه‌نگاری، ترویج خرافات و شیطان‌پرستی، دعوت به تجمع‌های غیرقانونی مغایر با آداب، رسوم و فرهنگ جامعه، دعوت به ایجاد اغتشاش در زمان‌های

خاص با مقاصد سیاسی، اطلاعاتی، امنیتی، فرهنگی، اجتماعی، اقتصادی و یا حتی جاسوسی می‌باشد که تاکنون خسارت‌های فراوانی به کشور وارد کرده است. این مقاله در پی آن است که با احصای تهدیدها و آسیب‌پذیری‌های موجود در فضای سایبری کشور، به ارزیابی آنها پرداخته و راهکارهای بهره‌مندی از فرصت‌های موجود در این عرصه را با لحاظ قرار دادن و تأکید بر نقش فناوری و منابع انسانی ارائه دهد.

۲-۱. اهمیت و ضرورت موضوع تحقیق

حمله‌های سایبری موجب می‌شوند تا با کمترین هزینهٔ ممکن، بیشترین خسارت‌ها به تأسیسات و زیرساخت‌های حساس وارد شده و با ایجاد اخلال در شبکه‌های ارتباطی و سامانه‌های اطلاعاتی، امکان بهره‌برداری کارآمد از این سامانه‌ها فراهم نشود. همچنین استفاده از شیوه‌های جنگ اطلاعاتی یا به عبارت دیگر، نبرد اطلاع‌رسانی، موجب بر هم خوردن نظم و ثبات سیاسی دولت‌ها شده و کشور هدف را با بحران‌های امنیتی، مشروعیتی و ... مواجه می‌کند؛ در این باره، حوادث پس از انتخابات سال ۱۳۸۸ قابل اشاره می‌باشد.

اهمیت و ضرورت پرداختن به پیامدهای ناشی از تهدیدهای سایبری علیه کشور به‌اندازه‌ای است که مقام معظم رهبری در چندین مورد بر آن تأکید داشته‌اند. از جملهٔ آنها می‌توان به بیانات در دیدار با اعضای مجلس خبرگان رهبری در ۱۳۷۹/۱۱/۲۷ در مورد، «استفادهٔ دشمنان از اینترنت برای تهاجم علیه تفکّرات اسلامی و به‌ویژه تفکّرات شیعی با استفاده از روش‌های تخریبی روانشناسانه»، در دیدار با اعضای شورای‌عالی انقلاب فرهنگی در ۱۳۸۱/۹/۲۶ در مورد اینکه «اینترنت یکی از نعم بزرگ الهی است، اما در عین حال یک نقمت بزرگ هم هست؛ یعنی یک چاقوی دو دم و خطرناک است» و دیدار با روحانیان در ۱۳۸۵/۸/۱۷ که فرمودند: «امروزه تهاجم فرهنگی با استفاده از ابزارها و فناوری‌های جدید ارتباطی، خیلی جدی است؛ ... باید در مقابل اینها ایستاد.

امروز نمی‌شود به همان روش‌های قدیمی خودمان اکتفا کنیم»، اشاره نمود، بنابراین بررسی تهدیدهای سایبری علیه ج.ا. ایران و ارائهٔ راهکارهای مقابله، با تأکید بر نقش فناوری و منابع انسانی، از اهمیت و ضرورت دوچندان برخوردار می‌باشد.

۳-۱. هدف‌های تحقیق

۱-۳-۱. هدف اصلی

هدف اصلی تحقیق، شناسایی تهدیدهای سایبری علیه کشور و یافتن راهکارهای بهره‌مندی از توانمندی‌های فنی و نیروی انسانی توانمند برای مقابله با تهدیدها می‌باشد.

۲-۳-۱. هدف‌های فرعی

(۱) شناسایی و تجزیه و تحلیل تهدیدها و آسیب‌پذیری‌های سایبری کشور،

(۲) شناسایی و تجزیه تحلیل توانمندی‌های مبتنی بر فناوری و نیروی انسانی کارآمد در مقابله با تهدیدهای سایبری علیه کشور،

(۳) شناسایی موانع عملیاتی‌شدن توانمندی‌ها در مقابله با تهدیدهای سایبری.

۴-۱. پیشینهٔ تحقیق

«نبرد اطلاعاتی» به‌عنوان یکی از شیوه‌های رایج به‌ویژه در جنگ روانی، قدمتی طولانی دارد. در دهه‌های اخیر به موازات رشد شتابان فناوری‌های ارتباطی و ورود شبکه‌های خبری متکی بر ماهواره، اینترنت و دیگر ابزارهای الکترونیکی، نبرد اطلاعاتی وارد فضای جدیدی شده است و تحول بسیار عمیقی را تجربه می‌کند؛ در واقع آن‌چنان که صدوقی در کتاب «تکنولوژی اطلاعاتی و حاکمیت ملی» بیان می‌کند: نبرد اطلاعاتی، عملیاتی است که منجر به حصول برتری اطلاعاتی با تأثیرگذاری بر روی اطلاعات

دشمن، فرایند پردازش اطلاعات، سامانه‌های اطلاعاتی و شبکه‌های سایبری می‌شود (صدوقی، ۱۳۸۴: ۱۲۹).

بعضی از محققان مراکز تحقیقاتی معتقدند که در یک طبقه‌بندی کلی، ابزارهای حملهٔ سایبری[1] به نسبت سایر ابزارهای جنگی عمومی، بسیار بیشتر در اختیار کشورها قرار داشته و هزینهٔ استفاده از آنها کمتر و روش‌های استفاده از آنها سهل‌تر می‌باشد (عبداله‌خانی، ۱۳۸۹: ۹۶). هدف بیشتر کشورها از تشکیل ارتش سایبری، گرفتن امتیاز در جهت منافع مشخص و مقابله با انواع تهدیدهایی است که در حوزهٔ فضای سایبری اتفاق می‌افتند؛ چرا که بسیاری از تروریست‌ها می‌توانند با استفاده از امکانات قابل توجه این ابزارها، مخاطره‌های بسیار زیادی را برای دولت‌های گوناگون ایجاد کنند (صدوقی، ۱۳۸۴ ,Gray and Head, 2009, Furnell and Warren, 1999, Geers, 2010).

پژوهش‌ها نشان می‌دهد با توجه به حساسیت بیش از اندازهٔ موضوع جنگ اطلاعاتی راهبردی، بیشتر کشورهای دنیا، راهکنش‌ها (تاکتیک‌ها) و برنامه‌های خود را به‌شدت طبقه‌بندی کرده‌اند. بسیاری از این کشورها مانند آمریکا، انگلیس، چین، روسیه، هند، پاکستان و... به ایجاد ارتش‌های سایبری پرداخته و توسعهٔ ابزارها و سلاح‌های سایبری را در رهنامهٔ (دکترین) نظامی خود مورد توجه قرار داده‌اند (اندیشگاه شریف و اندیشکدهٔ کاوشگران آینده، ۱۳۸۴، Mulazzani and Sarcia, 2011, Caton et al, 2011).

بارمستر[2] و همکاران، اولین گام برای یافتن موضوع‌های پدآفندی در حوزهٔ جنگ اطلاعاتی راهبردی را بازبینی نقاط آسیب‌پذیری در برابر تهدیدهای محتمل، بر روی طیف گستردهٔ تهدیدها و برنامه‌ها (سناریوها) مطرح نموده‌اند (Burmester et al, 2012).

بررسی‌های انجام‌شده از سوی محققان داخلی (علیزاده و علیزاده، ۱۳۹۰، خواجوی و جلالی، ۱۳۹۰) و خارجی (Nye, 2010, Wana et al, 2011, Disso et al, 2011) نشان می‌دهد ارتباطات

1. Cyber Attack Tools
2. Burmester

زیرساخت، مهم‌ترین بخش از شبکهٔ ارتباطات هر کشوری می‌باشد؛ چرا که از طریق ارتباطات، زیرساخت تمامی شبکه‌های ارتباطی در سطح کشوری، منطقه‌ای و بین‌المللی برقرار شده و با توجه به کارکرد و جایگاهی که دارند، همواره در معرض آسیب‌های ناشی از تهدیدهای سایبری دشمنان می‌باشند. در صورت وارد شدن آسیب و از دست رفتن امنیت این ارتباطات و یا قطع آنها، با توجه به حوزهٔ کاربردی وسیعی که دارند، احتمال وقوع بحران‌های سیاسی، اجتماعی، فرهنگی، اقتصادی و امنیتی بسیار زیاد است.

توربان[1] و همکاران معتقدند هر کشوری که در آن فناوری اطلاعات و ارتباطات بهتر و بیشتر توسعه‌یافته باشد، هدف و تهدیدی برای دیگر کشورهای مشابه خواهد بود؛ در واقع از نظر آنها کشورهای کمتر توسعه‌یافته که از زیرساخت‌های وابسته به فناوری اطلاعات، آنچنان بهره‌ای ندارند، در مقایسه با کشورهای پیشرفته‌ای که اصول زندگی آنها به نظام فناوری اطلاعات و ارتباطات گره خورده است، آسیب‌پذیری‌های کمتری در جنگ‌های موسوم به جنگ اینترنتی متحمل می‌شوند (توربان و همکاران، ۱۳۸۶: ۱۱۵۶و۱۱۵۷).

مهری و صانعی، بیان می‌کنند ازجمله کارکردهای جنگ سایبری در حوزهٔ نرم را شبکه‌سازی به معنای تعامل افراد با هم در اینترنت، فرهنگ‌سازی (به‌دلیل دگرگونی‌های فناورانهٔ جدید، جریان‌سازی به معنای هدایت افکار عمومی در نوع انتخاب و تصمیم‌گیری، گردش آزاد اطلاعات با وجود مقدار زیاد فاصلهٔ فیزیکی بین افراد، واپایش (کنترل) و نظارت بر آن دانسته‌اند (مهری و صانعی، ۱۳۸۸).

در پژوهشی که توسط حاذق‌نیکرو انجام شد، وی به این نتیجه رسید که نظام سلطه با راه‌اندازی وبلاگ‌ها، پایگاه‌های مختلف اطلاع‌رسانی و بهره‌گیری از وب۲ توانست در ناآرامی‌های پس از انتخابات در ایران از طریق آموزش، اطلاع‌رسانی، هماهنگی و عملیات روانی، تأثیرگذاری داشته باشد (حاذق‌نیکرو، ۱۳۹۰).

1. Turban

با وجود تحقیق‌های انجام‌شده، تاکنون پژوهش جامعی در مورد ارزیابی میزان تهدیدهای سایبری علیه کشور و نیز آسیب‌پذیری‌های سایبری که امکان وارد شدن خسارت را در دو حوزهٔ یادشده فراهم می‌نماید، مشاهده نشده است، از این‌رو تحقیق حاضر، دارای نوآوری و تازه بودن در ارزیابی شدت تهدیدها، میزان آسیب‌پذیری و نیز توانمندی‌های مقابله با این تهدیدها در دو حوزهٔ فناوری و نیروی انسانی می‌باشد.

۵-۱. پرسش تحقیق

۱-۵-۱. پرسش اصلی

راهکارهای مقابله با تهدیدهای سایبری علیه جمهوری اسلامی ایران با تأکید بر نقش فناوری و منابع انسانی کدامند؟

۲-۵-۱. پرسش‌های فرعی

(۱) تهدیدهای سایبری علیه ج. ا. ایران کدامند؟

(۲) آسیب‌پذیری‌های موجود در فضای سایبری ج. ا. ایران کدامند؟

(۳) توانمندی‌های بالقوه و بالفعل ج. ا. ایران در ابعاد فناوری و نیروی انسانی برای مقابله با تهدیدهای سایبری کدامند؟

۶-۱. روش‌شناسی تحقیق

تحقیق حاضر به لحاظ هدف، کاربردی و از نظر روش از زمرهٔ پژوهش‌های توصیفی- تحلیلی است. به این منظور پس از مرور ادبیات و مطالعهٔ کتابخانه‌ای، به بحث و مصاحبهٔ عمیق با چند نفر از کارشناسان پرداخته شده و با توجه به الگوی مفهومی پژوهش، از ابزار پرسشنامه برای گردآوری داده‌ها استفاده گردید.

۱-۶-۱. جامعه و نمونهٔ آماری

جامعهٔ آماری این تحقیق، خبرگان حوزهٔ فضای سایبری هستند که در سطح سازمان‌های نظامی و اداره‌های تخصصی، مرکز ماهر و دانشکدهٔ جنگال و دفاع سایبری دانشگاه جامع امام حسین(ع)، مشغول به فعالیت بودند. تعداد افرادی که ویژگی‌های مورد نظر برای پاسخگویی به گویه‌های پرسشنامه را داشتند، ۶۰ نفر بود که با توجه به جدول مورگان، تعداد ۵۲ نفر به صورت تصادفی ساده (۴۳ نفر مرد و ۹ نفر زن) انتخاب گردیدند.

۱-۱-۶-۱. وضعیت سنی پاسخگویان

وضعیت سنی پاسخگویان در جدول شمارهٔ ۱، ارائه شده است.

جدول شمارهٔ ۱. وضعیت سنی پاسخگویان

بازهٔ سنی	تعداد	درصد
زیر ۲۵ سال	۴	۷/۷
۲۶ تا ۴۰ سال	۳۰	۵۷/۷
۴۱ تا ۵۵ سال	۱۴	۲۶/۹
۵۶ سال به بالا	۴	۷/۷
مجموع	۵۲	۱۰۰

همچنان‌که جدول شمارهٔ ۱ نشان می‌دهد بیشتر پاسخگویان در بازهٔ سنی ۲۶ تا ۵۵ سال (۷۴/۶٪) قرار دارند.

۲-۱-۶-۱. وضعیت تحصیلی پاسخگویان

وضعیت تحصیلی پاسخگویان در جدول شمارهٔ ۲ ارائه شده است.

جدول شمارهٔ ۲. وضعیت تحصیلی پاسخگویان

مقطع تحصیلی	تعداد	درصد
کاردانی	۱۰	٪۱۹
کارشناسی	۱۵	٪۲۹
کارشناسی ارشد	۲۳	٪۴۴
دکتری	۴	٪۸
مجموع	۵۲	۱۰۰

همچنان‌که جدول شمارهٔ ۲ نشان می‌دهد، از میان نمونهٔ آماری شرکت‌کننده در تحقیق حاضر، به میزان ۱۹٪ دارای تحصیلات کاردانی، ۲۹٪ با تحصیلات کارشناسی، ۴۴٪ دارای تحصیلات کارشناسی ارشد و ۸٪ دانش‌آموختهٔ مقطع دکتری بودند. نکتهٔ قابل توجه آن است که بیش از نیمی از پاسخگویان (۵۲٪)، دارای تحصیلات کارشناسی ارشد به بالا هستند.

۳-۱-۶-۱. وضعیت شغلی پاسخگویان

وضعیت شغلی پاسخگویان در جدول شمارهٔ ۳ ارائه شده است.

جدول شمارهٔ ۳. وضعیت شغلی پاسخگویان

نوع اشتغال	تعداد	درصد
نظامی	۱۸	۳۴/۶
امنیتی- انتظامی	۲۱	۴۰/۴
دانشگاهی	۱۳	۲۵
مجموع	۵۲	۱۰۰

همچنان‌که جدول شمارهٔ ۳ نشان می‌دهد بیشترین مشارکت‌کنندگان در تحقیق حاضر، دارای مشاغل امنیتی- انتظامی (۴۰/۴٪) و پس از آن نظامی (۳۴/۶٪) و در نهایت، دانشگاهی (۲۵٪) بوده‌اند.

۲-۶-۱. روش و ابزار گردآوری اطلاعات

ابزار گردآوری اطلاعات در این پژوهش، پرسشنامهٔ محقق‌ساخته بوده که گویه‌های آن بر اساس مطالعهٔ ادبیات و انجام مشاوره با چند نفر از خبرگان تدوین و روایی و پایایی آن تأیید گردید. برای برآورد و کمی‌سازی متغیرها در بخش تهدیدها، ۱۳ گویه و برای آسیب‌پذیری‌ها، ۱۷ گویه مشخص گردیدند. برای ارزیابی گویه‌ها، با توجه به جدول شمارهٔ ۴، معیارهایی در بازهٔ اعداد ۱ تا ۱۰ ارائه شد تا با استفاده از آنها نسبت به وزن‌دهی به گویه‌ها اقدام گردد. سپس جمع اوزان تهدیدها را با هم مقایسه نموده و آنهایی که از وزن بالاتری برخوردار بودند، به‌عنوان تهدیدهای اصلی انتخاب گردیدند.

جدول شمارهٔ ۴. معیار کمّی کردن شدت تهدیدهای سایبری

طیف	نمره	توضیح
خیلی زیاد	۱۰	احتمال بروز تهدید علیه دارایی مورد نظر قریب‌الوقوع است
زیاد	۸ – ۹	انتظار تهدید علیه دارایی می‌رود
متوسط رو به بالا	۷	تهدید علیه دارایی محتمل به نظر می‌رسد
متوسط	۵ – ۶	تهدید ممکن است علیه دارایی عملی گردد
متوسط رو به پائین	۴	تهدید در محدودهٔ دارایی محتمل به نظر می‌رسد
کم	۲ – ۳	تهدید ممکن است در محدودهٔ دارایی عملی گردد
خیلی کم	۱	تهدید قابل اغماض است

همچنین به‌منظور ارزیابی آسیب‌پذیری‌ها، با توجه به معیارهای ارائه‌شده در جدول شمارهٔ ۵، نسبت به کمّی کردن شدّت آسیب‌پذیری‌ها اقدام گردید.

جدول شمارهٔ ۵. معیار کمّی کردن میزان آسیب‌پذیری سایبری

طیف	نمره	توضیح
خیلی زیاد	۱۰	دارای یک یا چند نقص اصلی است که باعث می‌شود دارایی در خطر شدید متجاوز و یا فاجعه قرار گیرد
زیاد	۹-۸	دارای یک یا چند نقص اصلی است که باعث می‌شود دارایی در خطر بالای متجاوز و یا فاجعه قرار گیرد
متوسط رو به بالا	۷	دارای یک نقص مهم است که باعث می‌شود دارایی در خطر زیاد متجاوز و یا فاجعه قرار گیرد
متوسط	۶ - ۵	دارای یک نقص است که باعث می‌شود دارایی به طور مساعد در خطر متجاوز و یا فاجعه قرار گیرد
متوسط رو به پائین	۴	دارای یک نقص است که باعث می‌شود دارایی تا حدی در خطر متجاوز و یا فاجعه قرار گیرد
کم	۳ - ۲	دارای یک نقص کوچک است که باعث می‌شود دارایی تا حدی در خطر متجاوز یا فاجعه قرار گیرد
خیلی کم	۱	ضعف وجود ندارد

۳-۶-۱. سازماندهی تحقیق

به‌منظور پاسخ به پرسش‌های تحقیق، در گام اول به مطالعهٔ کتابخانه‌ای پرداخته شد. در گام دوم، الگوی مفهومی تحقیق از طریق بحث و مشورت با کارشناسان، طراحی و پرسشنامه با اخذ نظر خبرگان در حوزهٔ تهدیدها، آسیب‌پذیری‌ها و توانمندی‌ها بر اساس آن تدوین گردید. در گام سوم، یافته‌های مبتنی بر وزن‌دهی خبرگان به گویه‌ها و در نهایت، نتیجه‌گیری و پیشنهادها ارائه شد.

۲. مبانی نظری

۱-۲. نبرد در فضای سایبری

فضای سایبری، حوزه‌ای عملیاتی است که به‌منظور بهره‌برداری از اطلاعات با استفاده از سامانه‌های به هم پیوسته و زیرساخت‌های یکپارچهٔ آنها با استفاده از علم الکترونیک شکل گرفته است؛ به عبارتی فضای سایبری به معنای یک سرزمین غیرفیزیکی است که از سامانه‌های سایبری تشکیل شده است، بنابراین دنیای سایبری، هر گونه واقعیت مجازی است که توسط مجموعهٔ رایانه‌ها و شبکه‌ها ایجاد می‌شود. هرچند در فضای سایبری نمی‌توان بویید یا چشید، اما این فضا نیز دارای اشیای خاص

خود است. نبرد در فضای سایبری، زیرمجموعه‌ای از جنگ اطلاعاتی است و شامل اقدام‌هایی می‌شود که در دنیای سایبری رخ می‌دهند.

۲-۲. جنگ نرم و سخت در فضای سایبری

جنگ نرم، اقدامی پیچیده و پنهان متشکل از عملیات‌های سیاسی، فرهنگی و اطلاعاتی برای ایجاد تغییرهای مورد نظر در جامعه هدف است. هدف از این جنگ، تغییر ارزش‌ها و فرهنگ ملت‌هاست (ضیایی‌پرور، ۱۳۸۴)؛ به عبارت دیگر، جنگ نرم شامل هرگونه اقدام نرم‌افزارانه از قبیل روانی، تبلیغاتی و رسانه‌ای علیه جامعهٔ هدف است. در جدول شمارهٔ ۶، جنبه‌های مختلف قدرت در جنگ سایبری از ابعاد نرم و سخت ارائه شده است.

جدول شمارهٔ ۶. جنبه‌های مختلف قدرت نرم و سخت در جنگ سایبری

روی اول: قدرت الف قدرت ب را وادار به کاری می‌کند که خود ب در حالت عادی آن را انجام نمی‌داد.	
قدرت نرم	برنامه‌های تبلیغاتی برای تغییر سلایق اصلی نفوذگرها (هکرها)، جذب اعضای سازمان‌های تروریستی
قدرت سخت	تهدیدهای انکار سرویس، جاسازی بدافزارها، دستگیری وبلاگ‌نویسان
روی دوم: واپایش دستورکار: الف با کنار گذاشتن راهبردهای ب، ب را از انتخاب منع می‌کند.	
قدرت نرم	واپایش فراهم‌کنندگان خدمات اینترنت[1] و موتورهای جست‌وجو
قدرت سخت	دیواره‌های آتش، پالایه (فیلترها) و وارد کردن فشار برای کنارگذاشتن برخی عقاید
روی سوم: الف سلایق ب را طوری شکل می‌دهد که برخی از راهبردها حتی مطرح هم نمی‌شود	
قدرت نرم	انتشار اطلاعات برای ایجاد سلایق و اولویت‌ها (مانند تحریک ملی‌گرایی با استفاده از نفوذگرهای میهن‌پرست)، به وجود آوردن هنجارهای انزجار (مانند هرزه‌نگاری کودکان)
قدرت سخت	تهدید به تنبیه وبلاگ‌نویسانی که مطالب حذف (سانسور) شده را منتشر می‌کنند.

Source: Nye, 2010: 7

1. ISP

۳-۲. تهدیدهای سایبری نرم

از جمله تهدیدهایی سایبری که در حوزهٔ نرم، امنیت ملی ج.ا.ایران را تهدید می‌کنند «جهت‌دهی به افکار عمومی برای به خطر انداختن امنیت سیاسی(اعتراض، اعتصاب، شورش)، امنیت اجتماعی (روابط اجتماعی و حقوق شهروندی)، امنیت فرهنگی (عدم رعایت موازین شرعی و فرهنگی)، گردآوری اطلاعات اقلیمی و قومی، شناسایی افرادی که توانایی‌های کلیدی دارند، الهام‌گیری از نظریه‌های ثبت‌شده، مهندسی اجتماعی، کندوسازی اطلاعاتی و شبکه‌ای، کم‌رنگ شدن ارزش‌های مترقی اسلامی، تضعیف اعتقادها و ایجاد شبهه‌های فکری، رواج سطحی‌نگری فکری، ایجاد سردرگمی بین نسل جوان و آسیب‌های روانی، آموزش و تشویق اغتشاشگران برای انجام عملیات تروریستی به‌منظور ایجاد ناامنی در کشور» می‌باشد. در مجموع هدف‌های اصلی دشمنان از این تهدیدها، اختلال در امر ادارهٔ کشور، ایجاد نارضایتی در بین مردم، فشار به کشور و بهره‌برداری‌های سوء در راستای تغییر رفتار مردم یا حاکمیت در جهت منافع خود می‌باشد.

۴-۲. تهدیدهای سایبری سخت

با توجه به رشد و توسعهٔ روزافزونِ فناوری اطلاعات و ارتباطات در تمامی ابعاد جوامع امروزی و نقشِ بسیار مهم آن در توسعه و واپایش زیرساخت‌های حیاتی، حساس و مهم کشورها، از آن به‌عنوان زیرساختِ زیرساخت‌ها نام برده می‌شود (خواجوی و جلالی، ۱۳۹۰). منظور از زیرساخت، مجموعهٔ ساختاریافته‌ای از شبکه‌ها و سامانه‌های وابسته به یکدیگر است که در بسیاری از سطوح مختلف مانند صنایع و سازمان‌ها با هم پیوند خورده‌اند (هالپین، ۱۳۸۹). مهم‌ترین حوزه‌های زیرساخت، شبکه‌های اطلاعات و ارتباطات، انرژی، بانکداری و امور مالی و خدمات‌رسانی می‌باشد. در تهدیدهای سایبری، هدف‌هایی مختلف دنبال می‌شود. این هدف‌ها شامل

جنبه‌های سیاسی، اقتصادی، نظامی، اطلاعاتی، امنیتی و... می‌باشند. به‌دلیل وسعتِ عملکردی اقدام‌های قابل انجام، هدف‌های متفاوتی همچون تأسیسات هسته‌ای، سازمان‌های نظامی و امنیتی، وزارتخانه‌های مهم در حوزهٔ انرژی، مخابرات، اقتصاد و کشور، شبکه‌ها و سامانه‌های اطلاع‌رسانی نهادهای حکومتی قابل تهدید هستند (علیزاده اصانلو و علیزاده اصانلو، ۱۳۹۰، خواجوی و جلالی، ۱۳۹۰).

از آنجا که زیرساخت‌های فیزیکی فضای سایبری به مکان‌های جغرافیایی متصل است، دولت‌ها می‌کوشند تا با صرف هزینه برای ایجاد و تقویت این زیرساخت‌ها، خود را نسبت به سایر رقبا ارتقا بخشند، بنابراین با توجه به نقشِ حیاتیِ ارتباطات زیرساخت در فضای تبادل اطلاعات کشور، وسعت حوزهٔ کارکردی تهدیدهای سایبری و به‌دلیل تغییرهای دائمی در شکل و ماهیت این تهدیدها و به‌عبارتی پویا بودن آنها، هر روزه تهدیدهای جدیدتری ایجاد و مطرح می‌گردد.

۲-۵. آسیب‌پذیری‌های سایبری

به‌دلیل ماهیت فضای سایبر و پویا بودن این فضا، تعداد آسیب‌پذیری‌هایی که در حوزهٔ سایبر وجود دارد، به‌طور دقیق قابل شناسایی نیست. با توجه به تعریف علمی آسیب‌پذیری، می‌توان آسیب‌پذیری سایبری را «عدم توانایی در جلوگیری از خطرات سایبری»، «فقدان آگاهی در مورد چگونگی رفع تهدید سایبری» و «فاقد قدرت بودن در دفع تهدیدهای سایبری» تعریف نمود (محمدی، ۱۳۸۹).

۲-۶. راه‌های مقابله با تهدیدهای سایبری

ویلیامز[1] ملزوم‌های مقابله با تهدیدهای سایبری را «نیروی انسانی متخصص» و «تجهیزات مورد لزوم» معرفی می‌کند (Williams, 2003). در مقولهٔ نیروی انسانی

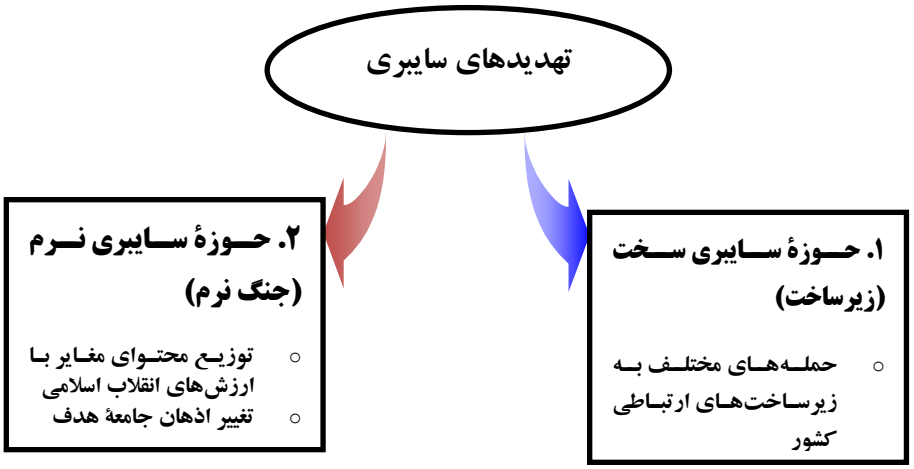
1. Williams

متخصص، کیفیت مهم‌تر از کمیت است؛ چرا که نیروی انسانی، راهبر عملیات سایبری (طرح‌ریزی، گردآوری اطلاعات، تحلیل و اجرای حمله) است. مهم‌ترین توان‌های تخصصی مورد نیاز، دانش شبکه و شناخت اجتماع‌های مختلف (قابلیت مهندسی اجتماعی) است. در بحث فناوری‌های مورد استفاده، لازم است طراحی روش‌ها و سپس ابزارهای مبتنی بر آنها مورد توجه قرار گیرد. از جمله ابزارهای مورد نیاز، ابزارهای شناسایی، وارسی، کنکاش، نفوذ، حمله‌های انکار سرویس و مهندسی اجتماعی می‌باشند.

۷-۲. الگوی نظری

شکل شمارهٔ ۱، الگوی نظری تحقیق را با توجه به مطالعهٔ نظری و مصاحبه با خبرگان، به‌منظور بررسی تهدیدهای سایبری در دو حوزهٔ سایبری سخت (زیرساخت) و سایبری نرم (جنگ نرم) نشان می‌دهد.

شکل شمارهٔ ۱. الگوی نظری تحقیق



ترسیم از: نویسندگان

۳. یافته‌ها

۱-۳. ارزیابی اثر تهدیدهای سایبری از ابعاد کلان

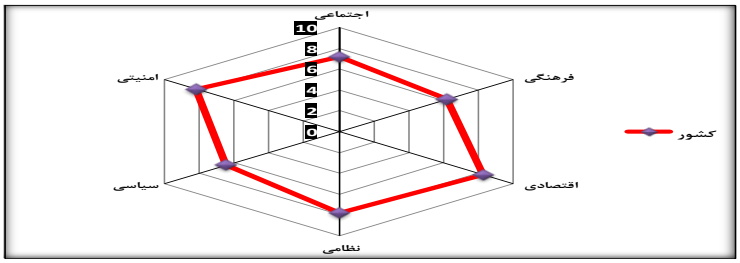
یافته‌های حاصل از ارزیابی اثر تهدیدهای سایبری از ابعاد کلان به شرح جدول شمارهٔ ۷ و شکل شمارهٔ ۲ می‌باشد.

جدول شمارهٔ ۷. ارزیابی اثر تهدیدهای سایبری از ابعاد کلان در سطح کشور

ردیف	ابعاد مورد بررسی	میزان تهدید
۱	اقتصادی	٪۸۳
۲	امنیتی	٪۸۲
۳	نظامی	٪۷۸
۴	اجتماعی	٪۷۲
۵	سیاسی	٪۶۵
۶	فرهنگی	٪۶۲

همچنان‌که جدول شمارهٔ ۶ نشان می‌دهد، حوزهٔ اقتصادی به میزان ۸۳٪، حوزهٔ امنیتی به میزان ۸۲٪، حوزهٔ نظامی به میزان ۷۸٪، حوزهٔ اجتماعی به میزان ۷۲٪، حوزهٔ سیاسی به میزان ۶۵٪ و حوزهٔ فرهنگی به میزان ۶۲٪، از تهدیدهای سایبری، اثرپذیری دارند.

شکل شمارهٔ ۲. برآورد شدت اثر تهدیدهای سایبری از ابعاد کلان در سطح کشور



یافته‌های نمودار ارائه‌شده در شکل شمارهٔ ۲ نیز نشان می‌دهد که ابعاد اقتصادی، امنیتی و نظامی بیشترین اثرپذیری و ابعاد سیاسی و فرهنگی کمترین اثرپذیری را از تهدیدهای سایبری دارند.

۲-۳. ارزیابی شدت اثر تهدیدهای سایبری به شکل جزیی

با توجه به یافته‌های تحقیق، ارزیابی جزیی شدت اثر تهدیدهای سایبری در حوزه‌هایی که احتمال حملهٔ سایبری نسبت به آنها وجود دارد به شرح جدول شمارهٔ ۸ می‌باشد.

جدول شمارهٔ ۸. ارزیابی شدت اثر تهدیدهای سایبری به صورت جزیی

ردیف	حوزه‌ای که ممکن است مورد حمله قرار گیرد	میزان تهدید
۱	حوزه‌های مالی کشور از قبیل شبکهٔ بانکی کشور	٪۹۵
۲	حوزه‌های ارتباطات از قبیل شبکهٔ ارتباطات زیرساخت، شبکهٔ تلفن همراه	٪۸۸
۳	حوزهٔ رسانه از قبیل شبکه‌های صدا و سیما	٪۸۸
۴	حوزه‌های صنعتی از قبیل سامانه‌های واپایش کارخانجات و پالایشگاه‌ها	٪۸۸
۵	حوزه‌های مختلف حمل‌ونقل اعم از ریلی، هوایی و دریایی	٪۸۳
۶	حوزه‌های دفاعی از قبیل سامانه‌های فرماندهی و واپایش	٪۸۲
۷	حوزه‌های خدماتی از قبیل شبکه‌های آب و برق و گاز	٪۷۸
۸	حوزه‌های فرهنگی از قبیل شبکه‌های فرهنگی، هنری، اعتقادی	٪۷۶
۹	حوزه‌های اجتماعی از قبیل گروه‌های مختلف اجتماعی، سیاسی	٪۷۴
۱۰	حوزه‌های علمی و تحقیقاتی کشور از قبیل مراکز علمی تحقیقاتی و دانشگاه‌ها	٪۷۳
۱۱	حوزه‌های اطلاع‌رسانی کشور از قبیل مطبوعات	٪۷۰
۱۲	حوزه‌های آموزشی از قبیل شبکه‌های آموزش مجازی و آموزش از راه دور	٪۶۵
۱۳	از بین بردن حس وفاداری در مخاطبان	٪۶۵

همچنان‌که یافته‌های ارائه‌شده در جدول بالا نشان می‌دهد، بیشترین شدت تبعات ناشی از تهدیدهای سایبری در «حوزه‌های مالی کشور از قبیل شبکهٔ بانکی کشور» می‌باشد که مؤید اطلاعات حاصل در جدول شمارهٔ ۶ می‌باشد. نکتهٔ قابل توجه آن است که از نظر خبرگان، در سطح کشور کمترین اثرپذیری برای گویه «از بین بردن حس وفاداری در مخاطبان» لحاظ شده است، بنابراین با توجه به نوع و فراوانی مخاطبان لازم است با استفاده از تمامی ابزارهای در دسترس، نسبت به کاهش آثار ناشی از تهدیدهای سایبری در این حوزه کوشید. حوزهٔ دیگری که در سطح کشور،

شدت آثار تهدیدهای سایبری نسبت به سایر حوزه‌ها کمتر است، «حوزه‌های آموزشی از قبیل شبکه‌های آموزش مجازی و آموزش از راه دور» می‌باشد.

ارزیابی خبرگان در زمینهٔ میزان توانایی دشمنان در بهره‌مندی از روش‌های مختلف برای انجام تهدیدهای سایبری به شرح جدول شمارهٔ ۹ ارائه گردیده است.

جدول شمارهٔ ۹. ارزیابی توانایی دشمن در استفاده از روش‌های مختلف برای انجام تهدیدهای سایبری

ردیف	روش مورد استفاده	میزان توانایی
۱	اختلال در شبکه‌های مراکز مختلف خدماتی از قبیل مخابرات، بانک‌ها، شبکه‌های حمل و نقل	٪۷۸
۲	تهدیدهای امنیتی از قبیل تروریسم سایبری	٪۷۷
۳	قطع ارتباط با مراکز نگهداری داده در مواقع حساس	٪۷۵
۴	حملهٔ سایبری به مراکز نگهداری داده اعم از بومی و غیربومی	٪۷۳
۵	حمله به وبگاه‌های متعلق به دستگاه‌های کشور به‌منظور جلوگیری از ارائهٔ خدمات به مردم	٪۷۳
۶	تهدیدهای اجتماعی علیه جامعه از قبیل سازماندهی اغتشاش‌ها و ناآرامی‌های مختلف در کشور	٪۷۳
۷	جاسوسی از راه دور و از طریق بستر شبکه	٪۷۲
۸	قطع کامل یا اختلال شبکه‌های ارتباطات تلفنی داخل و یا خارج از کشور	٪۷۲
۹	دسترسی غیرمجاز به بانک‌های اطلاعاتی مختلف سازمان‌ها مانند سازمان ثبت احوال کشور	٪۷۰
۱۰	تهدیدهای سیاسی از قبیل انجام اقدام‌های هماهنگ علیه یک کشور	٪۷۰
۱۱	تهدیدهای اقتصادی و مالی از قبیل اعمال تحریم‌های اقتصادی از طریق فضای	٪۷۰
۱۲	ورود غیرقانونی به حریم خصوصی افراد و امکان ایجاد مشکلات مختلف برای زندگی مردم	٪۶۸
۱۳	عضویت غیرارادی کارسازها (سرورها) و رایانه‌های کشور در گروه‌های نفوذگر و سربازگیری الکترونیکی	٪۶۷
۱۴	ممانعت از استفاده از برخی خدمات شبکهٔ جهانی اینترنت به بهانهٔ تحریم‌ها	٪۶۷
۱۵	تهدیدهای فرهنگی جامعه از قبیل رواج بی بندوباری، ایجاد بی‌اعتقادی، سست کردن باورها	٪۶۷
۱۶	استراق سمع به صورت عام (مکالمه‌ها، اطلاعات، تصویر) به روش‌های مختلف و از راه دور	٪۶۳
۱۷	انهدام و یا آسیب‌رسانی به تأسیسات صنعتی کشور از قبیل پالایشگاه‌ها و نیروگاه‌ها	٪۶۳
۱۸	اختلال یا قطع شبکه‌های اطلاع‌رسانی (مانند قطع خدمات صدا و سیما)	٪۶۲

آنچنان که در جدول شمارهٔ ۹ نشان داده شده است، براساس نظر خبرگان، بیشترین توانمندی‌های دشمنان در انجام تهدیدهای سایبری، استفاده از روش‌های «اختلال در شبکه‌های مراکز مختلف خدماتی از قبیل مخابرات، بانک‌ها، مراکز واپایشی، شبکه‌های حمل و نقل، شبکه‌های توزیع برق و آب» به میزان ۷۸٪، «تهدیدهای امنیتی از قبیل تروریسم سایبری» به میزان ۷۷٪، «قطع ارتباط با مراکز نگهداری داده در مواقع حساس» به میزان ۷۵٪، «حملهٔ سایبری به مراکز نگهداری داده اعم از بومی و غیربومی» به میزان

۷۳٪، «حمله به وبگاه‌های متعلق به سازمان‌ها، نهادها و دستگاه‌های کشور به‌منظور جلوگیری از ارائهٔ خدمات به مردم» به میزان ۷۳٪، «تهدیدهای اجتماعی علیه جامعه از قبیل بسیج و سازماندهی اغتشاش‌ها و ناآرامی‌های مختلف در کشور و یا تشکیل و هدایت گروه‌های منحرف» به میزان ۷۳٪ می‌باشد.

۳-۳. ارزیابی میزان اثر ابزارها و سلاح‌های مورد استفاده در تهدیدهای سایبری

ارزیابی خبرگان از ابزارهایی که امکان استفاده از آنها در انجام تهدیدهای سایبری برای دشمن علیه فضای سایبری در سطح کشور وجود دارد به شرح جدول شمارهٔ ۱۰ می‌باشد.

جدول شمارهٔ ۱۰. ارزیابی میزان اثر ابزارها و سلاح‌های مورد استفاده دشمنان در تهدیدهای سایبری

ردیف	ابزار تهدید	نوع اقدام	هدف	شدت اثر
۱	دروازهٔ پشتی (حفرهٔ نفوذ مخفی)	قرار دادن یک حفرهٔ نفوذ مخفی در تجهیزات تولیدی توسط تولیدکننده	ورود به شبکه در زمان دلخواه و به‌صورت مخفیانه	٪۹۰
۲	شبکه‌های اجتماعی	ساماندهی کاربران در گروه‌های خاص و به‌کارگیری آنها علیه کشور	ایجاد اغتشاش و تلاش برای ایجاد نافرمانی مدنی	٪۸۸
۳	عدم دسترسی به خدمات (سرویس)	قطع دسترسی به وبگاه توسط شرکت ارائه‌کنندهٔ خدمات میزبانی	عدم دسترسی به خدمات (سرویس)	٪۸۷
۴	شبکه‌های بات نت	در اختیار گرفتن غیرقانونی کارسازها و رایانه‌های سازمان‌ها و مردم	شرکت غیرارادی در تهدیدهای سایبری به‌عنوان سرباز الکترونیکی	٪۸۲
۵	ویروس‌های رایانه‌ای	آلوده کردن سامانه‌ها و از کار انداختن آنها	اختلال و یا از کار انداختن کارسازها و تأسیسات از قبیل نیروگاه و پالایشگاه	٪۸۰
۶	نرم‌افزارهای جاسوسی	در پوشش نرم‌افزارهای کاربردی مانند فرهنگ لغت بابیلون	سرقت اطلاعات رایانه‌ها و شبکه‌های کاربران	٪۸۰
۷	تهدیدهای انکار سرویس	بالا بردن کاذب شدوآمد (ترافیک) ارتباطی دسترسی به وبگاه	از کار انداختن کارسازها و جلوگیری از ارائهٔ خدمات به مردم	٪۷۸
۸	اسب‌های تروآ	انتشار از طریق رایانامه، محل‌های اشتراک پرونجا (فایل)	ثبت کلیدهای فشرده شدن صفحه کلید، مشاهده صفحهٔ نمایش کاربر	٪۷۷
۹	حمله و نفوذ	ورود غیرقانونی به شبکه‌ها از طریق درگاه آسیب‌پذیر	اختلال و یا جلوگیری از ارائهٔ خدمات	٪۷۷
۱۰	نرم‌افزارهای تبلیغاتی اینترنتی	قرار گرفتن در رایانهٔ حریف و اصرار بر حداقل یک بار استفاده از آنها	سرقت هویت کاربران و کلمهٔ عبور آنها	٪۶۷

همچنان‌که جدول شمارهٔ ۱۰ نشان می‌دهد مؤثرترین ابزارهای تهدیدهای سایبری، دروازهٔ پشتی(به‌ویژه در بُعد سخت‌افزاری و زیرساختی) و شبکه‌های اجتماعی (در بُعد سایبری نرم) می‌باشد. کمترین تأثیر در میان ابزارهای یادشده عبارت از «نرم‌افزارهای تبلیغاتی اینترنتی» است که البته آن نیز با برآورد شدت اثر ۶۷٪، دارای احتمال متوسط به بالا (محتمل) می‌باشد.

با توجه به یافته‌های تحقیق، دسته‌بندی تهدیدهای موجود در فضای سایبری از ابعاد امنیتی و اجتماعی به شرح جدول شمارهٔ ۱۱ می‌باشد.

جدول شمارهٔ ۱۱. دسته‌بندی تهدیدهای موجود در فضای سایبری از ابعاد امنیتی و اجتماعی

ردیف	دسته‌بندی تهدید	نوع تهدید	کشور
۱	امنیتی	کُدهای مخرب و بدافزارها	٪۷۷
۲	امنیتی	دسترسی غیرمجاز از راه دور	٪۷۵
۳	امنیتی	استفاده از رایانامه جهت نشر بدافزار و شبهه‌پراکنی	٪۷۲
۴	امنیتی	اتصال‌های ناامن به شبکه‌های اینترنت و اینترانت و فیبر نوری	٪۷۲
۵	امنیتی	استفاده از سامانه‌های پایهٔ غیربومی	٪۷۲
۶	اجتماعی	استفاده از شبکه‌های اجتماعی جهت تغییر فرهنگ و اعتقادهای مردم	٪۷۰
۷	امنیتی	اتکای قابل ملاحظه به سامانه‌های ارتباطی بی‌سیم و ماهوارهٔ غیر امن	٪۶۸
۸	امنیتی	اختلال الکترونیکی	٪۶۷
۹	امنیتی	استفاده از شبکه‌های اجتماعی برای اغتشاش‌ها و نافرمانی مدنی	٪۶۷

براساس این دسته‌بندی، بیشتر تهدیدهای در حوزهٔ سایبری به جز یک مورد، تبعات امنیتی دارند که میزان اثر آنها، نزدیک به هم و با احتمالی بین متوسط تا زیاد می‌باشد.

۴-۳. ارزیابی آسیب‌پذیری‌های سایبری

با توجه به احصای آسیب‌پذیری‌ها، ارزیابی آنها بر اساس نظریهٔ خبرگان در جدول شمارهٔ ۱۲ ارائه گردیده است.

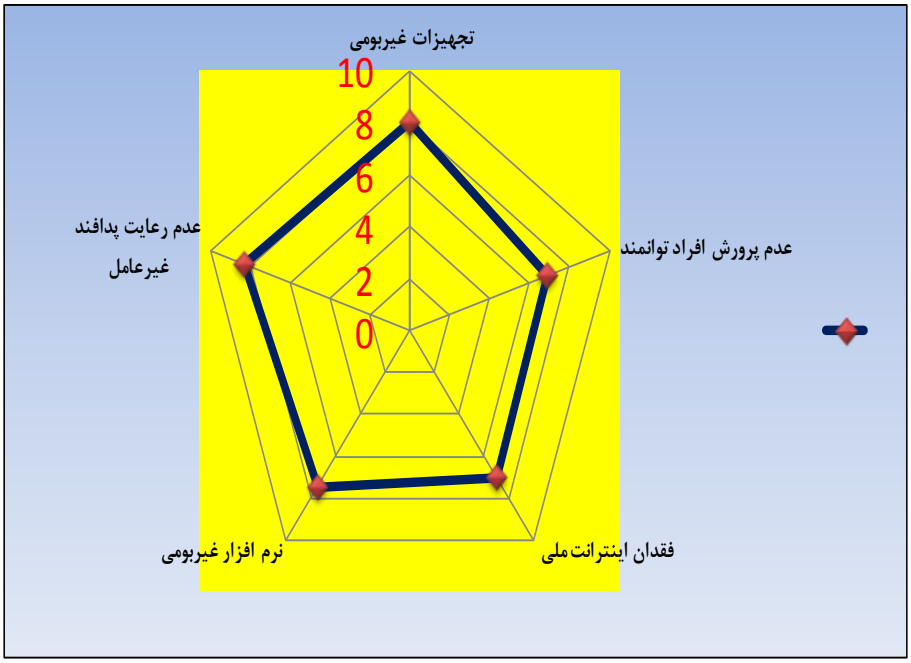
جدول شمارهٔ ۱۲. ارزیابی آسیب‌پذیری‌های موجود فضای سایبری کشور

ردیف	عنوان آسیب‌پذیری	میزان آسیب‌پذیری
۱	عدم توجه کافی به الزام‌های پدافند غیرعامل در طرح‌های فناوری اطلاعات و ارتباطات کشور	٪۸۳
۲	عدم وجود محصول‌های سخت‌افزاری بومی در مورد امنیت فضای سایبری	٪۸۰
۳	استفادهٔ بخش عمده‌ای از زیرساخت‌های ارتباطی حیاتی از سامانه‌ها و تجهیزات غیربومی	٪۸۰
۴	عدم رعایت الزام‌ها و استانداردهای امنیتی در طرح‌های فناوری اطلاعات و ارتباطات کشور	٪۷۸
۵	عدم داشتن مراکز میزبانی داده (Hosting z) در داخل کشور	٪۷۵
۶	عدم وجود نرم‌افزار بومی برای تجهیزات ارتباطی مورد استفاده در شبکه‌های اصلی ارتباطی	٪۷۵
۷	عدم داشتن سامانهٔ عامل بومی و ملی	٪۷۳
۸	صاحب فناوری نبودن در حوزهٔ سایبر	٪۷۰
۹	عدم پیاده‌سازی شبکهٔ ملی اطلاعات کشور (اینترانت ملی) و به صورت مستقل از شبکهٔ اینترنت	٪۷۰
۱۰	عدم داشتن نرم‌افزارهای پایه و نرم‌افزارهای عمومی کاربردی اداری در سازمان‌ها	٪۷۰
۱۱	عدم ارائهٔ آموزش لازم و پرورش کارکنان توانمند در سازمان‌ها	٪۶۹
۱۲	عدم حضور فعال در فضای مجازی	٪۶۹
۱۳	ضعف سامانهٔ موتور جست‌وجوی بومی و ملی در ارائهٔ خدمات متناسب با نیازمندی‌های کاربران	٪۶۳
۱۴	عدم بهره‌مندی صحیح و اصولی از ظرفیت موجود اعم از سخت‌افزاری، نرم‌افزاری و نیروی انسانی تحصیلکرده	٪۶۱
۱۵	عدم وجود فرهنگ استفاده از سامانهٔ رایانامهٔ بومی و ملی	٪۶۰

همچنان‌که یافته‌های جدول شمارهٔ ۱۲ نشان می‌دهد، بر اساس نظر خبرگان، مهم‌ترین آسیب‌پذیری‌ها، «عدم توجه کافی به الزام‌های پدافند غیرعامل در طرح‌های فناوری اطلاعات و ارتباطات کشور و سازمان‌ها به ویژه از نوع نظامی» به میزان ۸۳٪ می‌باشد. آسیب‌پذیری‌های مهم دیگر، «عدم وجود محصولات سخت‌افزاری بومی در مورد امنیت فضای سایبری» به میزان ۸۰٪، «استفادهٔ بخش عمده‌ای از زیرساخت‌های ارتباطی حیاتی کشور از سامانه‌ها و تجهیزات غیربومی در زمینهٔ ارتباطات و شبکه» به میزان ۸۰٪ و «عدم رعایت الزام‌ها و استانداردهای امنیتی در طرح‌های فناوری اطلاعات و ارتباطات کشور» به میزان ۷۸٪ می‌باشد.

با توجه به نتایج جدول بالا، مهم‌ترین آسیب‌پذیری‌های سایبری در سطح فضای سایبری کشور به صورت شکل شمارهٔ ۳ ارائه گردیده است.

شکل شمارهٔ ۳. نمودار تحلیلی مهم‌ترین آسیب‌پذیری‌های سایبری در سطح فضای سایبری کشور



با توجه به نمودار ارائه‌شده، مهم‌ترین آسیب‌پذیری‌ها در حوزهٔ استفاده از تجهیزات غیربومی و عدم رعایت پدافند غیرعامل می‌باشد.

۴. راهکارهای مقابله با تهدیدهای سایبری و اولویت‌بندی آنها

راهکارهای مقابله با تهدیدهای سایبری و اولویت‌بندی آنها با توجه به نظرات اخذ شده از خبرگان، در جدول شمارهٔ ۱۳ ارائه گردیده است.

جدول شمارهٔ ۱۳. راهکارهای مقابله با تهدیدهای سایبری و اولویت‌بندی آنها

راهکار	میزان اهمیت
ایجاد مراکز عملیات امنیت شبکه در مراکز اصلی ارتباطات زیرساخت	٪۸۳
رعایت امنیت فضای تبادل اطلاعات (افتا) در شبکه‌های عمومی و اختصاصی و در سطح ملی و سازمانی	٪۸۰
راه‌اندازی شبکهٔ اطلاعات ملی و سازمانی	٪۷۷
داشتن سامانهٔ موتور جست‌وجوی ملیِ بومی	٪۷۷
ایجاد گروه‌های امداد و نجات سایبری موسوم به CERT	٪۷۷
اتخاذ و به‌کارگیری تدابیر امنیتی مربوط به تجهیزات و شبکه‌های مرتبط و متصل به فضای سایبر	٪۷۳
استفاده از فیبر نوری به‌عنوان بستر ارتباطی و حذف ارتباطات زیرساختی با بستر ماهواره	٪۷۳
استفاده از جانمایی (توپولوژی) مناسب ارتباطی	٪۶۸
داشتن تجهیزات شبکه‌ای بومی	٪۶۷
تهیهٔ شیوه‌نامه‌های امنیتی و پدافندی	٪۶۷
انتقال مراکز متعدد میزبانی داده به داخل کشور و جلوگیری از انتقال شدوآمد (ترافیک) ارتباطی مربوط به خارج	٪۶۵
رصد و پایش دائمی تهدیدهای سایبری و ارائهٔ راهکارهای پدافندی مربوط	٪۶۵
استفاده از سامانه‌ها و ویگاه‌های جایگزین	٪۶۵
داشتن نسخهٔ پشتیبان از اطلاعات موجود	٪۶۵
به‌کارگیری اصول عام پدافند غیرعامل برای تأسیسات فیزیکی در تمامی مراحل از طراحی تا بهره‌برداری	٪۶۵
آموزش مداوم و مستمر تمامی کارکنان مرتبط	٪۶۵
استفاده از سامانه‌های اطلاع‌رسانی به‌منظور تأثیرگذاری بر فضای سایبری	٪۶۳
برگزاری رزمایش‌های دوره‌ای پدافند غیرعاملی	٪۶۲
داشتن سامانهٔ عامل ملیِ بومی	٪۶۰
به‌کارگیری اصول پدافند غیرعامل سایبری متناسب با تهدیدها از قبیل فریب و اختفای سایبری	٪۶۰
سازماندهی کارکنان توانمند به‌منظور انجام دفاع سایبری	٪۶۰
سازماندهی کارکنان توانمند به‌منظور انجام آفند سایبری	٪۵۸
کاهش هزینه‌های مرتبط با مراکز داده از قبیل هزینهٔ اتصال و هزینهٔ ذخیره‌سازی اطلاعات	٪۵۰

همچنان‌که جدول شمارهٔ ۱۳ نشان می‌دهد، مهم‌ترین راهکار مقابله با تهدیدهای سایبری از نظر خبرگان «ایجاد مراکز عملیات امنیت شبکه در مراکز اصلی ارتباطات زیرساخت» با میزان اهمیت ۸۳٪ است. از دیگر راهکارهای مهم به ترتیب، «رعایت امنیت فضای تبادل اطلاعات (افتا) در شبکه‌های عمومی و اختصاصی در سطح ملی و

سازمانی» با میزان اهمیت ۸۰٪، «راه‌اندازی شبکهٔ اطلاعات ملی و سازمانی» با میزان اهمیت ۷۷٪، راهکار ایجاد «سامانهٔ موتور جست‌وجوی ملیِ بومی» با میزان اهمیت ۷۷٪ و «ایجاد گروه‌های امداد و نجات سایبری موسوم به CERT» با میزان اهمیت ۷۷٪ می‌باشد.

۵. نتیجه‌گیری

۵-۱. جمع‌بندی

انقلاب اسلامی ایران به‌عنوان یک اندیشه و الگوی سیاسی نوین، با به چالش کشیدن ارزش‌ها و الگوی سیاسی لیبرال دموکراسی، ضربهٔ سنگینی بر استیلای جهان غرب وارد کرد. نظام سلطه به سردمداری آمریکا، تمامی اشکال براندازی سخت مانند جنگ نظامی و کمک به گروه‌های معاند و نوع نیمه‌سخت آن از قبیل شورش، کودتا و نفوذ را در دههٔ اول انقلاب اسلامی تجربه کرد، اما راه به جایی نبرد و مشاهده کرد که اتحاد و همدلی مردم روزبه‌روز افزایش می‌یابد، بنابراین پس از شکست در این عرصه‌ها، آنان تصمیم گرفتند تا مقابله‌ای پیچیده‌تر از پیش اتخاذ کنند. بدون شک یکی از راهبردی‌ترین ابزارهای مؤثر برای نظام سلطه، بهره‌مندی از فضای سایبری می‌باشد (نایینی، ۱۳۸۹).

با توجه به یافته‌ها، جمهوری اسلامی ایران با دو دسته از تهدیدها در فضای سایبری مواجه است؛ یک دسته، شامل توزیع محتوای مغایر با ارزش‌های انقلاب اسلامی است که به‌منظور تغییر اذهان جامعهٔ هدف و تغییر رفتار مردم عادی و نخبگان در جهت منافع خاص خود و مغایر با منافع ملی کشور انجام می‌شود و می‌توان از آن به‌عنوان جنگ نرم یاد نمود و دستهٔ دوم، تهدیدهای مختلف علیه زیرساخت‌های ارتباطی کشور (زیرساخت توسعهٔ سایر زیرساخت‌ها) می‌باشد.

با توجه به برگزاری انتخابات در ج.ا.ایران و فراهم بودن زمینهٔ مساعد برای فعالیت، دشمنان به‌ویژه غرب را به تکاپو واداشت تا از فضای سایبری در جهت دستیابی به

هدف‌های خود بهره‌برداری کنند. همچنین آنان با انتشار بدافزارها تلاش کردند تا زیرساخت‌های کشور به‌ویژه در حوزهٔ انرژی هسته‌ای و پالایشگاه‌های نفت را مورد هدف قرار دهند. یافته‌های تحقیق در حوزهٔ تهدیدهای سایبری نشان دادند که ابعاد اقتصادی، امنیتی و نظامی، اثرپذیرترین حوزه‌ها از تهدیدهای سایبری در ابعاد کلان محسوب می‌شوند. در سطح جزیی نیز حوزه‌های مالی و اقتصادی، ارتباطات و انرژی آماج بیشترین تهدیدهای سایبری با استفاده از روش اختلال می‌باشند. با توجه به نتایج حاصل از یافته‌های تحقیق، مهم‌ترین آسیب‌پذیری‌ها، استفاده از تجهیزات غیربومی و عدم رعایت پدافند غیرعامل می‌باشد. در صورت عدم توجه کافی به الزام‌های پدافند غیرعامل در طرح‌های فناوری اطلاعات و ارتباطات کشور و سازمان‌ها به‌ویژه از نوع نظامی و نیز عدم وجود محصول‌های سخت‌افزاری بومی در مورد امنیت فضای سایبری، احتمال بروز مخاطره‌های بسیار زیاد خواهد بود، بنابراین با توجه به استفادهٔ بخش عمده‌ای از زیرساخت‌های ارتباطی حیاتی کشور از سامانه‌ها و تجهیزات غیربومی در زمینهٔ ارتباطات و شبکه، لازم است توجه ویژه‌ای به این موضوع شود.

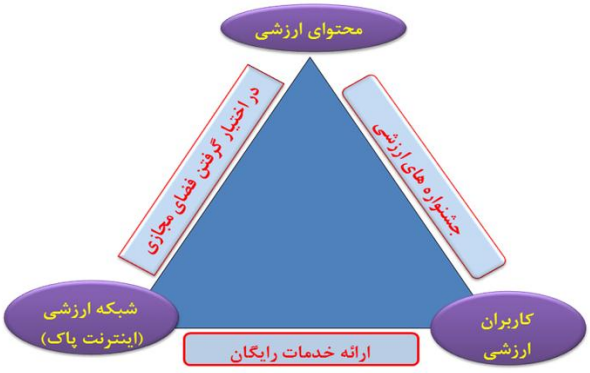
نتایج حاصل از یافته‌ها در مورد توانمندی‌های سایبری نشان داد، امکان ایجاد مراکز عملیات امنیت شبکه در مراکز اصلی ارتباطات زیرساخت یکی از توانمندی‌های بسیار خوب است، همچنان‌که «مرکز ماهر» یک مصداق عینی است و اثربخشی بسیار خوبی در زمینهٔ مقابله با تهدیدهای سایبری داشته است، از سوی دیگر، رعایت امنیت فضای تبادل اطلاعات (افتا) در شبکه‌های عمومی و اختصاصی و در سطح ملی و سازمانی از دیگر توانمندی‌هاست. همچنین راه‌اندازی شبکهٔ اطلاعات ملی یکی دیگر از فرصت‌های بسیار مناسب است که هر چند قدم‌های خوبی در این زمینه برداشته شده است، اما باید بسیار سریع‌تر در این باره اقدام شود؛ چرا که این امر، موجب تقویت سامانهٔ موتور جست‌وجوی ملیِ بومی و هرچه پرطرفدارتر شدن و کاربرد بیشتر آن می‌شود.

۲-۵. پیشنهادها

فضای سایبری با توجه ویژگی‌هایی مانند سایبری بودن، حافظهٔ مجازی، تعاملی بودن، واقعیت مجازی، جهانی و فرامرزی بودن، دستیابی به آخرین اطلاعات، جذابیت و تنوع، آزادی اطلاعات و ارتباطات، در حال تبدیل شدن به جزء جدایی‌ناپذیر زندگی انسان‌ها است و فکر و تخیل ادامهٔ حیات بشری بدون داده‌های فناوری اطلاعات و ارتباطات غیرقابل تحمل است. برای مقابله با تهدیدهای سایبری در حوزهٔ فناوری، لازم است به رعایت امنیت فضای تبادل اطلاعات (افتا) در شبکه‌های عمومی و اختصاصی و در سطح ملی و سازمانی به طور جدی پرداخته شود. همچنین مراکز عملیات امنیت شبکه در مراکز اصلی ارتباطات زیرساخت، توسعه داده شوند، از سوی دیگر، تسریع و تسهیل در انتقال مراکز متعدد نگهداری داده (میزبانی داده) به داخل کشور و جلوگیری از انتقال شدوآمد (ترافیک) ارتباطی مربوط به خارج از کشور که موجب جلوگیری از شنود بخش عظیمی از اطلاعات کاربران توسط دشمن می‌شود، بسیار مؤثر است.

در حوزهٔ بهره‌مندی از نیروی انسانی، شناسایی و سازماندهی فعالان عرصهٔ فضای مجازی برای تولید و انتشار محتوای مطابق با ارزش‌های انقلاب اسلامی به‌منظور هدایت افکار عمومی جامعه، الگوی ارائه‌شده در شکل شمارهٔ ۴ پیشنهاد می‌گردد.

شکل شمارهٔ ۴. الگوی پیشنهادی برای بهره‌مندی از ظرفیت‌های نیروی انسانی



بر اساس این الگو، در گام اول، توسعهٔ زیرساخت و فراهم نمودن تجهیزات سخت‌افزاری و نرم‌افزاری انجام شود و به طور رایگان در اختیار نیروی انسانی خبره و مستعد قرار داده شود. در گام دوم، به‌منظور تصمیم‌سازی و اتخاذ بهترین تصمیم‌ها توسط مدیران برای راهبری نیروی انسانی فعال در فضای سایبری، به‌روزترین اطلاعات در اختیار مدیران قرار داده شود. در گام سوم، شناسایی، توانمندسازی و شبکه‌سازی سایبری افراد علاقه‌مند، مستعد و خبره از طریق فراخوان‌ها و برگزاری جشنواره‌های سایبری انجام شود.

فهرست منابع

۱. منابع فارسی

۱. اندیشگاه شریف و اندیشکدهٔ کاوشگران آینده، (۱۳۸۴)، جنگ و دفاع سایبر، قابل دسترس در:
http://www.vahidthinktank.com/oldArman/Reports/CyberWar/CyberWar.pdf

۲. بیانات امام خامنه‌ای، علی در دیدار با اعضای مجلس خبرگان (۱۳۷۹/۱۱/۲۷)، دیدار با اعضای شورای‌عالی انقلاب فرهنگی (۱۳۸۱/۹/۲۶) و در دیدار با روحانیان (۱۳۸۵/۸/۱۷) قابل دسترسی در ***Khamenei.ir***.

۳. توربان، افرایم و همکاران (۱۳۸۶)، ***فناوری اطلاعات در مدیریت (دگرگونی سازمان‌ها و اقتصاد دیجیتالی)***، ترجمهٔ حمیدرضا ریاحی، تهران، انتشارات دانشگاه پیام نور.

۴. حاذق‌نیکرو، حمید (۱۳۹۰)، «نقش اینترنت در ناآرامی‌های پس از انتخابات دهمین دورهٔ ریاست جمهوری در ایران»، ***فصلنامهٔ عملیات روانی***، شمارهٔ ۳۱.

۵. خواجوی، محسن و غلامرضا جلالی (۱۳۹۰)، «بررسی تهدیدات و آسیب‌پذیری سایبری در حوزهٔ زیرساختی کشور»، ارائه‌شده در: ***همایش ملی دفاع سایبری***، تهران، جهاد دانشگاهی.

۶. صدوقی، مرادعلی (۱۳۸۴)، ***تکنولوژی اطلاعاتی و حاکمیت ملی***، تهران، وزارت امور خارجه.

۷. ضیایی‌پرور، حمید (۱۳۸۴)، «اینترنت در ایران»، در: ***بررسی کارکردهای مثبت و منفی اینترنت و وبلاگ در ایران***، مؤسسهٔ فرهنگی مطالعاتی و تحقیقات بین‌المللی ابرار معاصر تهران.

۸. عبداله‌خانی، علی (۱۳۸۹)، ***جنگ نرم ۳ (نبرد در عصر اطلاعات)***، تهران، مؤسسهٔ فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر.

۹. علیزاده اوصالو، علی و امیر علیزاده اوصالو (۱۳۹۰)، راهبردهای دفاع سایبری در صنایع نفت، گاز و پتروشیمی، ارائه‌شده در: ***همایش ملی دفاع سایبری***، تهران، جهاد دانشگاهی.

۱۰. محمدی، عباس (۱۳۸۹)، «بررسی پیامدهای سیاسی- اجتماعی وبلاگ (فرصت‌ها و چالش‌های جمهوری اسلامی ایران»، ***فصلنامهٔ عملیات روانی***، شمارهٔ ۲۷.

۱۱. مهری، عباس و یدا... صانعی (۱۳۹۰)، «بهره‌گیری غرب از اینترنت در جنگ نرم علیه جمهوری اسلامی ایران»، ***فصلنامهٔ عملیات روانی***، شمارهٔ ۳۱.

۱۲. نایینی، علی‌محمد (۱۳۸۹)، «بررسی تطبیقی تهدیدهای سه‌گانه سخت، نیمه‌سخت و نرم»، ***فصلنامهٔ راهبرد دفاعی***، سال هشتم، شمارهٔ ۳۰.

۱۳. هالپین، تروور (۱۳۸۹)، ***جنگ سایبر، جنگ اینترنتی و انقلاب در امور سایبر***، ترجمهٔ روح اله طالبی آرانی، تهران، مرکز پژوهش‌های مجلس شورای اسلامی.

۲. منابع انگلیسی

1. Burmester, M, Magkos, E, Chrissikopoulos, V (2012), "Modeling Security in Cyber–physical Systems", ***International Journal of Critical Infrastructure Protection***, vol. 5.
2. Jeffrey, L, John H. Greenmyer, Jeffrey L. Groh, William O. Waddell (2011), "Information as Power: An Anthology of Selected United States Army War College Student Papers", Volume 5, available in: ***www.dtic.mil***.
3. Disso, J, Jones, K, Williams, P, Steer, A (2011), A Distributed Attack Detection and Mitigation Framework, Internet Multimedia Systems Architecture and Application (IMSAA), ***2011 IEEE 5th International Conference on***.
4. Furnell, S, M, and Warren, M, J (1999), "Computer Hacking and Cyber Terrorism: the Real Threats in the New Millennium"?, ***Computers & Security***, vol.18.
5. Geers, K (2010), The Challenge of Cyber Attack Deterrence, Computer ***Law & Security Review***, Vol. 26, Issue. 3.
6. Gray, DH, Head, A (2009), The Importance of the Internet to the Post-modern Errorist and its Role as a Form of Safe Haven, ***Journal of Scientific Research,*** vol. 25. No. 3.
7. Mulazzani, F, Sarcia, S (2011), Cyber Security on Military Deployed Networks: A Case Study on Real Information Leakage, ***International Conference on Cyber Conflicts***, Estonia, Tallinn
8. Nye, J (2010), ***America's Cyber Future (Security and Prosperity in the Information Age)***, Washington, Center for a New American Security.
9. Wana, J, Suob, H, Yanb, H, Liub, J (2011), A General Test Platform for Cyber-Physical Systems: Unmanned Vehicle with Wireless Sensor Network Navigation, ***International Conference on Advances in Engineering, Procedia Engineering***.
10. Williams, Ken (2003), National Imagery and Mapping Agency, available at: ***http://www.defense.gov/Contracts/Contract.aspx?ContractID=2607***