فصلنامه علمی امنیت ملی
سال دهم، شماره سی‌وهشتم، زمستان ۱۳۹۹
مقاله دهم از صفحات ۳۳۰-۲۹۳

مقاله پژوهشی: تهدیدهای سایبری و اقدامات امنیتی در فضای مجازی؛ بررسی رویکردهای ایالات‌متحده آمریکا و جمهوری اسلامی ایران

محمدکاظم صیاد[۱]، آرمین امینی[۲]، ابوالقاسم طاهری[۳]

تاریخ دریافت: ۹۸/۰۹/۱۶ **تاریخ پذیرش: ۹۹/۱۰/۰۳**

چکیده

امروزه فناوری، اینترنت و تجارت رایانه‌ای، نقش به‌سزایی در ارتباطات جهانی ایفا می‌کند. این پدیده، مرز جدیدی میان دنیای سایبری و دنیای حقیقی به وجود آورده است، ولی ضعف ذاتی فناوری ارتباطات، این سامانه را در معرض تهدیدهای امنیتی بی‌شماری قرار داده است. استفاده دولت‌ها از فضای ناامن سایبری، زمینه را برای تهدیدات امنیتی ازجمله خرابکاری، اخلال، ترور، جاسوسی و دیگر جرائم مرتبط هموار ساخته است. هدف از این پژوهش، بررسی راهبردها و رویکردهای دو کشور ایران و آمریکا و همچنین کشف نقاط ضعف و یا کاستی‌های موجود در حوزه امنیت سایبری با توجه به تهدیدات موجود در فضای مجازی است. در این پژوهش ضمن بررسی تهدیدات امنیتی متأثر از فضای مجازی در دو کشور ایران و آمریکا، اقدامات امنیتی در مواجهه با این تهدیدات بررسی شده است. نتایج پژوهش نشان داد که متخصصان فضای سایبری در ایران به شناسایی تهدیدهای سایبری از پیش توجه کمتری داشته و درنتیجه در حوزه امنیت ملی، به‌رغم فعالیت‌ها و تدابیر خوب اندیشیده‌شده پیشین، راهکارهای مقابله با تهدیدهای سایبری با توجه به روند تهدیدات باید به‌روزرسانی‌شده و تدابیر جدیدی اتخاذ شود. در این زمینه بایستی در زمینه بسترسازی فناوری، قانون‌گذاری و فرهنگ‌سازی، برنامه‌هایی مشخص تدوین شود و اقدامات مؤثری صورت پذیرد.

کلیدواژه‌ها: اینترنت، فضای سایبری، شبکه‌های اجتماعی، امنیت ملی.

۱. **دکتری تخصصی علوم سیاسی، دانشگاه آزاد واحد علوم تحقیقات،** kazemsayad02@gmail.com
۲. دکتری تخصصی روابط بین‌الملل، دانشگاه آزاد واحد علوم تحقیقات، arminamini@gmail.com(نویسنده مسئول)
۳. دکتری تخصصی علوم سیاسی، دانشگاه آزاد واحد علوم تحقیقات، Dr.taheri@yahoo.com

مقدمه

ایران در صدر کشورهای استفاده‌کننده از اینترنت در خاورمیانه قرار دارد (عبدی، سوران؛ اسدالله الوندی‌زاده و نسرین مالکی، ۱۳۹۱) و ضریب نفوذ فیس‌بوک در میان کاربران ۵.۶۸ درصد می‌باشد (سایت اقتصادنیوز[۱] ۱۳۹۵/۱۲/۲۰). آمارهای موجود در سال ۱۳۹۸ نشان می‌دهند، در حالی که تعداد کاربران اینترنت در سراسر دنیا ۴ میلیارد و ۳۸۸ میلیون نفر با ضریب نفوذ ۶۷ درصد اعلام شده است، در ایران با جمعیتی بیش از ۸۲ میلیون نفر، بالغ بر ۶۷ میلیون نفر از اینترنت استفاده می‌کنند و ضریب نفوذ اینترنت در کشورمان حدود ۸۲ درصد برآورد شده است (وب‌سایت خبرگزاری میزان[۲] ۱۳۹۸/۹/۹). نتایج نظرسنجی ملی مرکز افکارسنجی دانشجویان ایران[۳]نیز که در تیرماه ۹۸ به‌صورت تلفنی و با جامعه آماری شهروندان کل کشور (اعم از شهر و روستا) انجام شده است، نشان می‌دهد که ۷۰ درصد مردم ایران، حداقل از یکی از شبکه‌های اجتماعی مجازی استفاده می‌کنند. در رابطه با همین موضوع، یکی دیگر از نظرسنجی‌های ایسپا که در اسفند ۹۷ انجام شد، نشان داد که ۷۱ درصد جوانان ۱۸ تا ۲۹ ساله از تلگرام[۴]و ۴۹ درصد این جوانان از اینستاگرام[۵]استفاده می‌کنند(وب‌سایت ایسپا،[۶] ۱۳۹۸/۰۷/۲۵).

امروزه فضای مجازی به بخش تفکیک‌ناپذیری از زندگی انسان‌ها تبدیل شده و با سرعت شتابان، تمامی شئون و عرصه‌های زیست بشر را تحت تأثیر قرار داده است. از این رو ماهیت‌شناسی این فضا و تشخیص شرایط و الزام‌های تبدیل شدن به بازیگری توانمند در این عرصه، نخستین گام است و هرگونه بی‌توجهی و غفلت نسبت به این پدیده، صدمه‌ها و آسیب‌های خطرناکی را متوجه جامعه خواهد نمود (قدسی، ۱۳۹۲: ۱۵۱)، «فضای مجازی» به‌عنوان پدیده‌ای نوظهور در زندگی بشر، محصول عملکرد شبکه جهانی

---

۱. www.eghtesadnews.com
۲. https://www.mizanonline.com/
۳. Iranian Students Polling Agency(ISPA)
۴. Telegram
۵. Instagram
۶. Ispa.ir

«اینترنت» است که امکان گردآوری، تمرکز، جابه‌جایی، پردازش و کاربری اطلاعات را با استفاده از فناوری اطلاعات بین کاربران اینترنت و بازیگران فضای مجازی در سراسر جهان فراهم می‌کند (حافظنیا، ۱۳۹۴: ۱). فضای سایبری محیط الکترونیکی واقعی است که ارتباطات انسانی به شیوه‌ای سریع و فراتر از مرزهای جغرافیایی و با ابزار خاص، زنده و مستقیم روی می‌دهد. از ویژگی‌های دیگر آن جهانی و فرامرزی بودن و دستیابی آسان به آخرین اطلاعات می‌باشد (سلیمانی فارسانی، ۱۳۸۸: ۴۱).

ضعف ذاتی فناوری ارتباطات، این سامانه را در معرض تهدیدهای امنیتی بی‌شماری قرار داده است (المرابت[1] و همکاران، ۲۰۱۸: ۴۸۹). اینترنت و ابزار فناوری اطلاعات، با همه جذابیت‌ها و محبوبیت‌های خود، فضای مجازی برای تبلیغات ضد هویتی برای دانشجویان و جوانان مسلمان ایرانی به شمار می‌آید. در این میان، آگاهی از اهداف و سوءنیت‌ها در تبلیغات گروه‌های انحرافی و التزام به آگاهی برای حفظ امنیت[2] کاربری در شبکه جهانی وب، از نکات مهم و ضروری کاربران فضای سایبری، به‌ویژه نسل جوان است و امنیت پایدار دیجیتالی را نه‌فقط به‌عنوان توسعه فنی بلکه می‌توان به‌مثابه حالتی روحی، طرز تفکر و حرکت عمومی جهانی توصیف کرد (خلیلی جو لرستانی، ۱۳۹۶: ۱۵۹)، فناوری اطلاعات و ارتباطات، تغییرات و دگرگونی‌های بسیاری را در زندگی بشر ایجاد کرده و از این طریق منجر به تحولات عمده‌ای در دانش روابط و هنجارهای بشری شده است. در عصر ارتباطات الکترونیک، مفاهیم نیز به تغییر و تحول دچار شده‌اند که یکی از آن‌ها مفهوم «هویت» و «احساس امنیت» است (پورنقدی، ۱۳۹۷: ۸۹). در عصر اطلاعات موضوع‌ها و مسئله‌های متنوع‌تری نسبت به گذشته در زمره مسائل امنیت ملی تلقی می‌شود. در این عصر، گردش آزاد اطلاعات در سراسر جهان که از راه اینترنت صورت می‌گیرد، موضوع امنیت اطلاعات را تا سطح مسائل امنیت ملی بالا می‌برد و درنتیجه تعریف امنیت ملی بسط و گسترش می‌یابد (پالیزیان، ۱۳۹۴: ۶۴۲).

---

۱. El Mrabet
۲. Security

مطابق بررسی‌ها کاربران ایرانی در فضای مجازی با تهدیدهایی در خصوص حریم خصوصی مواجه هستند. همچنین، به‌طور کلی برجسته‌ترین تهدیدها و آسیب‌های امنیتی در فضای مجازی، جعل و سرقت هویت، انتشار بدافزارها، سرقت و سوءاستفاده از افشای اطلاعات و داده‌های شخصی، دسترسی غیرمجاز به داده‌های محافظت‌شده، سرقت مالی، اعتیاد الکترونیکی، گسترش روابط نامشروع، شایعه‌پراکنی، ایجاد شبهات دینی و سیاسی، تمایل به ارتکاب جرائم، کمرنگ شدن هنجارهای اجتماعی و هویت فردی و دیگر موارد مشابه است. در سال‌های اخیر، با گسترش استفاده از شبکه‌های اجتماعی مجازی در بین جوانان و دانشجویان، مشاهده می‌شود که فرصت‌ها و تهدیدهای جدیدی در این عرصه ایجاد شده‌اند (پورنقدی، ۱۳۹۷: ۸۹).

شالوده و بنیاد هر کشوری بر اساس مجموعه‌ای از زیرساختارهای حیاتی آن کشور در بخش‌های ارتباطات، دفاع، انرژی، حمل‌ونقل، کشاورزی، بهداشت و امور اقتصادی است که فضای سایبر به‌مثابه یک سیستم عصبی آن‌ها را به‌هم مرتبط می‌سازد. امروزه اقدامات تروریستی فراوانی در فضای سایبر متوجه دولت‌ها است که از ویژگی‌های این حملات می‌توان به ناشناخته بودن و سرعت حملات مذکور اشاره نمود و اغلب این‌گونه حملات پس از وقوع مورد شناسایی قرار می‌گیرند؛ بنابراین با ایجاد یک راهبرد ملی در استقرار حداکثر امنیت در فضای سایبر می‌توان به کاهش آسیب‌پذیری کشور در مقابل حملات پرداخته و از بروز خسارت به زیرساخت‌های اطلاعاتی پایه و حیاتی و همچنین دارایی‌های ملی جلوگیری نمود.

تجاربی مانند واقعه ۱۱ سپتامبر نشان داد که در صورت وقوع هر تهدیدی از ناحیه فضای سایبر، دو اقدام باید به‌سرعت انجام شود. نخست ارائه یک واکنش مثبت جهت تحدید بحران و آماده کردن فضای مناسب برای مدیریت اوضاع و دوم تهیه و اعمال سیاست‌هایی که بتواند مانع از تکرار وضعیت شود. با توجه به تخصصی بودن هر دو فعالیت، لازم است که گروه‌های کارشناسی تحلیل راهبردی، تحلیل تاکتیکی و آسیب‌شناسی فضای مجازی، کاملاً فعال باشند و با کمترین خطر موجود و در زمان کوتاه، بیشترین بهره را ببرند (تهامی، ۱۳۹۰: ۲).

در میان کشورهای بزرگ، ایالات‌متحده آمریکا ازجمله کشورهایی است که با تهدیدهای امنیتی سایبری زیادی مواجه است؛ به‌طوری که زنگ خطر این تهدیدها در تمام نهادهای مرتبط با امنیت ملی به صدا درآمده است. این امر ایالات‌متحده آمریکا را ملزم به ارائه راهکارها و کاربست شیوه‌های مختلفی برای مقابله با تهدیدهای سایبری کرده است. جمهوری اسلامی ایران نیز همانند برخی از کشورها، بارها مورد هجوم حملات سایبری قرار گرفته است و به همین دلیل علاوه بر نرخ بالای حملات سایبری، رتبه نخست توان سایبری منطقه می‌باشد (خبرگزاری صداوسیما[۱]، ۱۳۹۸/۳/۸). گاهی این حملات سایبری از سوی دشمنان و با هدف تخریب و اختلال در مراکز مهم همچون تأسیسات هسته‌ای و سیستم بانکی کشور صورت گرفته است. سال‌ها است که متخصصان فضای سایبری در ایران متوجه حملات سایبری شده و به نهادهای مرتبط هشدارهای لازم را داده‌اند. در این رابطه، بالا بردن ضریب امنیت فضای سایبری و پیشگیری از حملات سایبری، امری ضروری است. درواقع پرسش اساسی این است که آیا جمهوری اسلامی ایران توانسته است یک شیوه مناسب در مقابله با این تهدیدها را همچون کشورهای پیشرفته اتخاذ کند و از تهدیدهای سایبری در امان بماند؟ در این پژوهش با مقایسه رویکرد دو کشور جمهوری اسلامی ایران و ایالات‌متحده آمریکا، به دنبال پاسخگویی به این سؤال هستیم که جمهوری اسلامی ایران تا چه اندازه توانسته امنیت سایبری خود را در مقابل تهدیدهای سایبری حفظ کند؟

مبانی نظری

فضای سایبر: اصطلاح فضای سایبر یا دنیای مجازی آنلاین، اصطلاحی است که نخستین بار توسط ویلیام گیبسون[۲] در سال ۱۹۸۴ م مورد استفاده قرار گرفت. فضای سایبر در این تعریف، شبکه‌هایی است که از طریق شاهراه‌های اطلاعاتی مثل اینترنت به‌هم وصل هستند و تمام اطلاعات راجع به روابط افراد، فرهنگ‌ها، ملت‌ها، کشورها و به‌طور کلی هر

۱. Iribnews.ir
۲. William Gibson

آنچه در کره خاکی به‌صورت فیزیکی و ملموس وجود دارد، در این فضا به شکل دیجیتالی وجود داشته و قابل استفاده و دسترسِ کاربران بوده و از طریق رایانه، اجزای آن و شبکه‌های بین‌المللی به‌هم مرتبط باشند (وطنی و اسدی، ۱۳۹۵: ۱۰۲).

امنیت: پس از دهه ۱۹۸۰ م و ناتوانی مکاتب رئالیسم[۱] و ایدئالیسم[۲] در پیش‌بینی جنگ سرد، افرادی همچون باری بوزان[۳] و الی ویور[۴] تعریف جدیدی از امنیت ارائه کردند که با عنوان مکتب کپنهاگ شناخته می‌شود. علت نام‌گذاری این مکتب فکری با عنوان کپنهاگ نیز به دلیل گردهمایی اندیشمندان آن در شهر کپنهاگ بود (احمدی‌نژاد، ۱۳۸۹: ۱۹). اصطلاح مکتب کپنهاگ توسط بیل‌مک‌سوئینی[۵] که خود از اندیشمندان این مکتب می‌باشد، برای آثار و دیدگاه‌های باری بوزان، الی ویور و دو ویلد[۶] و افراد دیگر به کار برده شده است. این مکتب تنها رهیافتی است که به مطالعات امنیتی می‌پردازد و امنیت را از حالت راهبردی دوران جنگ سرد خارج کرده و آن را در زیرمجموعه روابط بین‌الملل[۷] قرار داده است. ازجمله آثار این حوزه می‌توان به کتاب «مردم، دولت‌ها و هراس» و «امنیت چهارچوبی جدید برای تحلیل» و «امنیتی ساختن و ناامنی» اشاره کرد (عبدالله خانی، ۱۳۹۲: ۱۱۹). امنیت به مفهوم کلی آزادی و رهایی از ترس و خطر و احساس ایمنی از هرگونه تهدید و یکی از نیازهای اولیه و اساسی انسان‌ها از آغاز زندگی اجتماعی بوده است (محبوبی منش، ۱۳۸۱: ۱۴۲)، برداشت متفکران سیاسی از امنیت جهانی و امنیت بین‌المللی همانند مفهوم امنیت، همواره با تحولات نظام جهانی، متحول و سیال هستند؛ به‌طوری که دستیابی به توسعه بدون برخورداری از امنیت ناممکن است و توسعه نیز در برقراری امنیت به‌طور به‌سزایی نقش دارد و این پیوستگی در مقیاس‌های مختلف محلی، ملی، منطقه‌ای و جهانی مصداق پیدا می‌کند. در طول تاریخ، خطوط مرزهای سیاسی به دلیل جداسازی واحدهای مستقل و گاهی

---

۱. Realism
۲. Idealism
۳. Barry Buzan
۴. Ole Waever
۵. Bill McSweeney
۶. De Wilde
۷. International relations

نیمه‌مستقل سیاسی برای اعطای هویت ملی به دولت‌های ملی و محلی از نظر سیاسی، نظامی، اقتصادی و فرهنگی به شکل خاصی اهمیت داشته‌اند (گادال و جنسولین[۱] ۲۰۰۰: ۱۴). تعریف امنیت به‌عنوان کنش کلامی یا اقدام گفتاری مرکز ثقل این بحث است. امنیت عملی است که سیاست را به آن‌سوی قوانین تثبیت‌شده بازی می‌برد. برای این منظور طیفی سه‌درجه‌ای شامل موضوعات غیرسیاسی (مسائل خارج از حوزه دولت)، موضوعات سیاسی[۲] (تصمیم‌گیری و اختصاص منابع توسط دولت) و موضوعات امنیتی[۳]ترسیم می‌شود. امنیتی‌سازی به خارج کردن یک موضوع از دستور کار طبیعی و عادی، به دستور کار فوق‌العاده و اضطراری که استفاده از وسایل و ابزار غیرمعمول را توجیه می‌کند، دلالت دارد. از طرفی دیگر امنیتی‌سازی یعنی اینکه دیگر یک موضوع را نمی‌توان در معرض چانه‌زنی سیاسی قرار داد (چگنی‌زاده و آثارتمر، ۱۳۸۸: ۱۹۱).

«نایف رودهان»[۴] در بررسی مؤلفه‌های پایداری امنیت، بر مواردی همچون این مسائل تأکید می‌کند: مجموع اصول چندگانه امنیتی بر اساس عدالت در تمام سطوح، چندجانبه‌گرایی و نگرش چندبعدی[۵](شامل بشر، محیط، ملیت و امنیت فراملی، چندفرهنگی و چندتمدنی)، رئالیسم هم‌زیست‌گرایانه[۶]در روابط بین‌الملل و فضای مجازی و همکاری چندجانبه فرهنگی. به موجب این رئالیسم، همکاری چندجانبه ملت‌ها و دولت‌ها (که از نداشتن برخورد مطلق حاصل می‌شود) پدید می‌آید و همکاری چندجانبه فرهنگی[۷]نتیجه احترام چندجانبه، چندفرهنگی و جهان‌شهرگرایی[۸]است و به عدالت و امنیت منجر خواهد شد (رودهان[۹] ۲۰۰۹: ۱۵).

---

۱. Gadal & Jeansoulin
۲. Political Issues
۳. Security Issues
۴. Nayef Rodhan
۵. Multidimensional
۶. Symbiotic Realism
۷. Multilateralism
۸. Cosmopolitanism
۹. Rodhan

نظریه‌های امنیت: «بوزان» امنیت را موضوعی بین ذهنی تعریف می‌کند و آن را مبتنی بر تصمیم بازیگر می‌داند؛ اما بیان می‌کند که امنیت در اجتماع شناخته می‌شود. درواقع این نظریه ترکیبی از رهیافت‌های مادی و سازه‌انگارانه[۱] می‌باشد (داداندیش وکوزه‌گرکالجی، ۱۳۸۹: ۷۸). مکتب کپنهاگ تعریف موسعی از امنیت ارائه می‌دهد، به‌ویژه اینکه امنیت اقتصادی و امنیت زیست‌محیطی را بررسی کرده و تنها امنیت نظامی را مورد توجه قرار نمی‌دهد. به عبارتی دیگر امنیت ابعاد گوناگونی دارد که باید همه این ابعاد بررسی شوند (بوزان، ۱۱: ۱۳۷۹).

به‌طور کلی امنیت ملی و تهدیدها نسبت به آن، مهم‌ترین موضوع در مکتب کپنهاگ است. بوزان تهدیدها نسبت به امنیت ملی را به پنج دسته تقسیم می‌کند که عبارت‌اند از؛ تهدید سیاسی[۲] که متوجه ثبات سازمانی دولت است، تهدید اجتماعی[۳] که به هویت ملی مربوط است، تهدید اقتصادی،[۴] تهدید زیست‌محیطی[۵] که به پایگاه مادی دولت لطمه می‌زند و تهدید نظامی[۶] که می‌تواند همه اجزای دولت را تهدید کند که در عمل نیز همین‌گونه است(بوزان، ۱۳۸۹: ۱۵۹).

بوزان در انتقاد به نگاه سنتی درباره امنیت، آن را به پنج بعد نظامی، سیاسی، اقتصادی، اجتماعی و زیست‌محیطی گسترش می‌دهد. وی برای این امر دلایلی ذکر می‌کند؛ ازجمله اینکه افزایش سطح روابط میان کنشگران نظام بین‌الملل باعث تغییر و دگرگونی چهره تهدیدها گردیده و انواع دیگری از تهدیدها، به‌جز تهدیدهای نظامی ظهور یافته‌اند. دلیل دیگر، ویژگی سیاسی امنیت است و دلیل سوم به ویژگی چندبعدی بودن امنیت از لحاظ فکری برمی‌گردد. در این چهارچوب مفهوم امنیت به‌عنوان پیونددهنده تئوری و تحلیل در نظر گرفته می‌شود، به‌طور کلی مکتب کپنهاگ معتقد است که باید تلاش شود تا از امنیتی کردن بیش‌ازحد موضوعات و گنجاندن آن‌ها در دستور کار امنیت پرهیز شود و این رسالت یک سیاست موفق است (صادقی و نادری، ۱۳۹۵: ۱۷۰).

---

۱. Constructivism
۲. PoliticalThreat
۳. Social Threat
۴. Economy Threat
۵. Element Threat
۶. Military Threat

استفن والت[1] در چهارچوب مکتب واقع‌گرایی تدافعی ادعا می‌کند که مطالعات امنیتی بایستی بر روی «پدیده جنگ» که به‌وسیله قدرت‌های نظامی که تحت کنترل سیاسی بازیگران دولتی اداره می‌شوند، تمرکز کند. این مطالعات همچنین می‌تواند شامل کنترل تسلیحات و مدیریت بحران که به‌طور مستقیم در ارتباط با مسائل نظامی هستند، باشد. بنابراین نوواقع‌گرایان در مقابل توسعه دستور کار مطالعات امنیتی، شامل امنیت سایبری، مادامی که هنوز درباره تأثیرگذاری واقعی حمله‌های سایبری بر امنیت فیزیکی دولت‌ها و ظرفیت نظامی‌شان مشاجره وجود دارد، بحث می‌کنند. در هر صورت، به نظر می‌رسد نوواقع‌گرایان بر روی جایگاه تهدید سایبری در این زمینه توافق ندارند (هیر[2] ۲۰۱۰: ۲۱۵)، در معدود تفسیرهای برسازانه‌ای که در حال حاضر درباره امنیت در دوران دیجیتال وجود دارد، به‌طور عمده بر این تأکید می‌شود که چگونه جنگ اطلاعات، مجموعه متعددی از مرزبندی‌ها را به‌ویژه در مرزهای هویت به چالش می‌کشد. ادویرارد[3] جنگ اطلاعات‌پایه را نوع خاصی از «جنگ هویت» می‌داند که در آن تمامی انواع مرزبندی‌ها ازجمله تفکیک قدیمی داخلی- بین‌المللی به چالش کشیده می‌شود. بر این اساس، هویت دولت ملی به خطر می‌افتد. البته این امکان وجود دارد که دولت به‌جای تسلیم شدن در برابر رخنه مداوم به مرزهای رسمی حاکمیت خویش و سر برآوردن و ابراز هویت‌های جدید در فضای مجازی، خود را با آن سازگار کند. تحلیل برسازانه قدرت و امنیت در جهان مجازی، متضمن تأکید بر اهمیت تصورات و نمادها در کنار واقعیت‌های مادی رایانه‌ها و کابل‌ها است (روزنا و دیگران، ۱۳۹۰: ۳۰).

نظریات دیگری نیز در خصوص امنیت مطرح شده است، مطابق با نظریه «ساختاری- کارکردی»، همه رخدادهای اجتماعی از قبیل تداوم، نظم، یکپارچگی، انگیزه، هدایت و سازگاری را بر اساس نیازهای جامعه توجیه می‌کند. رسانه‌های همگانی یکی از عناصر زیرمجموعه نظام محسوب می‌شوند که هر عنصری در آن، به‌صورت ویژه‌ای کارکرد دارد.

---

۱. Stephen Walt
۲. Hare
۳. Edverard

رسانه‌های همگانی بخش‌های مختلف نظام را به‌هم مرتبط می‌کنند و نظم آن را در بحران‌ها افزایش و نیازهای شهروندان را پاسخ می‌دهند (پورنقدی، ۱۳۹۷: ۹۱). بر اساس نظریه «تغییر در ارزش‌های فردی»، رسانه‌های همگانی ارزش‌هایی را در جامعه انتشار می‌دهند که در فرد سبب نوآوری، تحرک اجتماعی، روانی و ذهنی می‌شوند و وجدان کار را تقویت می‌کنند و سرانجام، به افزایش احساس امنیت منجر می‌شوند و همچنین زمینه پیشرفت‌های فردی و اجتماعی را فراهم می‌کنند.

در این پژوهش با توجه به اهمیت امنیت ملی برای هر کشور با بهره‌گیری از نظریه مکتب کپنهاگ و بوزان، جایگاه امنیت سایبری را در سیاست‌های دو کشور ایران و آمریکا مورد بررسی قرار خواهیم داد. از نقاط مثبت این نظریه توجه به ابعاد مختلف امنیت ملی و کاربست تمهیدات لازم توسط دولت‌ها به‌عنوان بازیگران اصلی در تأمین امنیت است.

مروری بر پیشینه تحقیق

واگنر[۱] و همکاران (۲۰۱۹ م) طی تحقیقی، به‌اشتراک‌گذاری اطلاعات تهدیدهای فضای سایبری را به‌عنوان یکی از روش‌های خنثی کردن افزایش مداوم حملات سایبری معرفی نمودند. در این تحقیق به بررسی آیین‌نامه‌ها و روش‌هایی پرداختند که از یک روند اشتراک‌گذاری اطلاعات در مورد تهدیدات فضای مجازی پشتیبانی می‌کند.

المرابت[۲] و همکاران (۲۰۱۸ م)، امنیت سایبری و چالش‌های آن را در شبکه‌های هوشمند مورد بررسی قرار دادند. به اعتقاد ایشان، در حال حاضر اقدامات متقابل موجود بر روی مقابله با برخی از حملات خاص یا محافظت از برخی از اجزای خاص تمرکز دارد، اما هیچ رویکرد جهانی برای تأمین امنیت کل سامانه وجود ندارد.

عسگری و گلی (۱۳۹۷) طی تحقیقی به این نتیجه دست یافتند که فضای مجازی بر امنیت ملی جمهوری اسلامی ایران تأثیرگذار است که این مسئله خود در قالب اقدامات

---

۱. Wagner
۲. El Mrabet

مخل امنیت و برانداز، گسترش نابسامانی‌های اجتماعی، شکاف بین اقلیت‌های قومی، مذهبی، زبانی و... نمایان می‌گردد.

نتایج تحقیق پورنقدی (۱۳۹۷) که با عنوان «فرصت‌ها و تهدیدهای امنیت در شبکه‌های اجتماعی مجازی برای دانشجویان» انجام شد، حاکی از آن بود که تهدیدهای نظم و امنیت در شبکه‌های اجتماعی مجازی برای دانشجویان، بحران هویت، هنجارهای اخلاقی، ترویج فساد، روابط غیراخلاقی، اعتیاد الکترونیک و کاهش انگیزه تحصیل و نقاط قوت و فرصت، گسترش آموزش‌های، مجازی، توسعه ارتباطات علمی و تجارت الکترونیک است.

نتایج تحقیق خلیلی جو لرستانی (۱۳۹۶)، حاکی از آن بود که نبودِ آموزش و اطلاع‌رسانی به دانشجویان و کاربران اینترنت، دسترسی به سایت‌های مخاطره‌انگیز، دوست‌یابی و فریب‌دهنده، باعث اغفال و آسیب و تهدید امنیت اجتماعی در فضای سایبر و فضای واقعی جامعه می‌شود.

عسگری (۱۳۹۶) طی تحقیقی که با هدف بررسی جایگاه نبرد سایبری در راهبرد امنیتی آمریکا بعد از ۱۱ سپتامبر انجام داد، به این نتیجه رسید که به‌طور کلی ایالات‌متحده در ارتباط با بسیاری از خدمات مهم و حیاتی به اینترنت و سامانه‌ها و داده‌های فضای مجازی متکی است. برتری نظامی آمریکا در کنار وابستگی ارکان دفاعی و اطلاعاتی این کشور به فضای سایبر موجب گشته برخی کشورها روی به ابزارهای غیرمتقارن جهت به چالش کشیدن آن ارکان بیاورند تا از این طریق میزان آسیب‌پذیری آمریکا را افزایش دهند؛ بنابراین تهدیدها و حملات سایبری در راهبرد امنیت ملی آمریکا جایگاه پراهمیتی دارد.

پالیزیان (۱۳۹۴) در مطالعه‌ای که با هدف بررسی رابطه اینترنت و امنیت ملی جمهوری اسلامی ایران انجام داد، به این نتیجه رسید که ماهیت اینترنت و محیط امنیتی و راهبردی متأثر از آن، به‌گونه‌ای است که در کنار فرصت‌های فراوان، قابلیت ایجاد تهدید و ناامنی داشته، الزام‌های خاص خود را در حوزه امنیت ملی طلب می‌کند. از این منظر، مشخص می‌شود که امنیت ملی کشور با اینترنت و امنیت فضای مجازی پیوستگی مثبتی دارد.

قدسی (۱۳۹۲) طی تحقیقی با عنوان «تأثیر فضای مجازی بر امنیت ملی ج.ا.ایران و ارائه راهبرد، با تأکید بر نقش شبکه‌های اجتماعی» مهم‌ترین راهکارهای مقابله با تهدیدات فضای مجازی را که بر اساس دیدگاه‌های ۲۰ نفر از صاحب‌نظران جمع‌آوری شد، به شرح زیر نام برد: تأسیس مرکز سیاست‌گذاری به‌منظور مدیریت یکپارچه، بهره‌گیری از ظرفیت‌های جامعه و تقویت سرمایه اجتماعی.

نجفی علمی (۱۳۹۱)، در تحقیقی که با هدف بررسی روند تحولات فضای سایبر و نقش آن در تهدیدات ناشی از جرم در محیط سایبر در ج.ا.ا انجام داد، به این نتیجه رسید که «قابلیت و ظرفیت سازگاری روند تحولی جرم، همگام و همسو با روند تحولات فضای سایبر (در سه عرصه کلی و با هفت تغییر ماهوی)»؛ الگوی تهدید جرم (اهداف و راهبردها، نوع، ماهیت، فرآیند، گستره، محیط، آثار و پیامدها) را در کشور از قابلیت و ظرفیت‌های پیچیده و نوینی برخوردار کرده است. این اتفاق پیچیده و نرم، به معنی آن است که «تهدیدات جرم با استفاده از قدرت فناوری به فناوری قدرت نرم تبدیل شده است» که این موضوع ضمن بی‌سابقه بودن در تاریخ تهدیدات جرم، می‌تواند سبب چالشی جدی در شناخت تهدیدات و مدیریت آن در محیط سایبر و تحول در نگاه به مفهوم نظم و امنیت در وضعیت کنونی کشور گردد.

فضای سایبر و فناوری‌هایی که استفاده از این فضا را برای ما ممکن می‌سازد، به تمام مردم جهان از هر ملیت، نژاد، دین و دیدگاه اجازه می‌دهد تا با یکدیگر ارتباط برقرار کرده، همکاری کنند و به پیشرفت و شکوفایی برسند. امروزه یک شرکت آمریکایی می‌تواند در هر نقطه از جهان از طریق ارتباطات اینترنتی به تجارت بپردازد، از مشاغل بی‌شماری حمایت به عمل آورد و فرصت مناسبی را در اختیار مردم آمریکا قرار دهد (لرد وشارپ، ۲۰۱۱: ۹). زمانی می‌توان از فضای سایبر به‌عنوان پیونددهنده زیرساخت‌های حیاتی کشور استفاده نمود که مسئله امنیت آن به‌طور کامل حل شده باشد، وجود هرگونه شکاف امنیتی در این فضا و همچنین در اجزایی که در این فضا عمل می‌نمایند، ضربات جبران‌ناپذیری را به کشور وارد خواهد کرد (حسن‌بیگی، ۱۳۸۴: ۲).

نشت اطلاعات، سرقت داده‌های حیاتی کشور و آسیب‌پذیری شبکه‌های جامع اطلاع‌رسانی به‌عنوان مهم‌ترین اشکالات امنیتی در این فضا می‌باشد که اگر از طرف حکومت توجه ویژه‌ای به آن نشود، به‌عنوان یک تهدید جدی برای منافع پایه‌ای کشور تلقی می‌شود. وجود شبکه جهانی اینترنت که امکان دسترسی‌های مختلف را برای همه افراد در سرتاسر جهان میسر ساخته است، واقعیتی انکارناپذیر است که به‌عنوان مهم‌ترین بستر فضای سایبر و مهم‌ترین عامل در امنیت ملی و زیرساخت‌های کشورهای توسعه‌یافته است که تهدیدات مجازی درون آن شکل گرفته و فعال می‌شوند (حسن‌بیگی، ۱۳۸۶: ۲۵۲).

تهدیدات سایبری و اقدامات امنیتی ایالات‌متحده آمریکا

در این قسمت ابتدا به بررسی تهدیدات سایبری متأثر از فضای مجازی در ایالات‌متحده آمریکا پرداخته شده و سپس راهبردهای امنیتی این کشور در مواجهه با تهدیدات امنیتی برشمرده شده است.

الف) تهدیدات سایبری و نهادهای امنیتی آمریکا

بر اساس بررسی‌ها و بازبینی‌های به‌عمل‌آمده قضایی بر روی اسناد و مدارک حقوقی موجود، دولت‌ها نگرانی ویژه‌ای را در بروز برخی از جرائم از قبیل کلاهبرداری‌های مالی، پورنوگرافی، (هرزه‌نگاری) کودکان و دسترسی غیرقانونی به اطلاعات رایانه‌ای در فضای سایبری دارند. اکثر کشورها در حال تهیه پیش‌نویس و یا بحث و تبادل‌نظر در مورد برخی از تغییرات در قوانین خود در موضوع جرائم سایبری و توسعه واحدها یا سازمان‌های جدید برای پرداختن به موضوع حملات سایبری هستند. در بررسی خط‌مشی‌ها، موافقت‌نامه‌ها و اقدامات راهبردی، آنچه قابل مشاهده است این است که کشورها با یک همبستگی شدید اقدام به شروع ایجاد تمایز میان حملات سایبری از جرائم سایبری کرده‌اند. این تمرکز راهبردی شامل تغییر در رویکرد امنیت سایبری از کشف ساده جرم و مبارزه با جرائم جنایی در فضای سایبری به‌صورت موضعی تا چالش‌های پیچیده‌تر ازجمله حفاظت از زیرساخت‌های ملی در برابر حملات سایبری، از منظر خارجی و یا داخلی به کشور است.

در جوامع پیشرفته مانند آمریکا که به شبکه‌های الکترونیکی متکی هستند، آسیب‌پذیری در برابر حملات تروریستی، سرقت و خرابکاری در سطح ملی مطرح است؛ بنابراین تأکید زیادی بر تروریسم اطلاعاتی و سایبرنتیک صورت می‌گیرد. به‌گونه‌ای که حتی یک مقام امنیتی آمریکا گفته است «که با یک میلیارد دلار و بیست نفر متخصص خبره رایانه می‌تواند کل آمریکا را فلج کند، یک تروریست نیز می‌تواند به این توانایی دست یابد». از این رو تأثیر حمله به شبکه‌های رایانه‌ای از تأثیر حملات شیمیایی و میکروبی بیشتر است (رایش، ۱۳۸۲: ۵۵).

جنبش‌های اجتماعی جدید، از مهم‌ترین جنبه‌های نرم‌افزاری تهدید امنیت ملی هر کشوری محسوب می‌گردند و حتی در خاستگاه اصلی آن یعنی ایالات‌متحده، جنبشی مانند «جنبش تسخیر وال‌استریت»[۱] توانست هشدارهای جدی به نظام سرمایه‌داری غرب دهد. عموم حاضران در این جنبش از طریق شبکه‌های اجتماعی مجازی به‌هم مرتبط شده و سازمان‌یافته بودند. به اعتقاد امانوئل کاستلز،[۲] بازیگران سیاسی از طریق رسانه‌های جدید، در بازی قدرت حضور دارند و از آنجا که اطلاعات و ارتباطات، بیشتر از طریق شبکه جهانی اینترنت، ماهواره‌ها و خبرگزاری‌ها انتشار می‌یابد، بازی سیاسی، به‌گونه فزاینده‌ای در فضای رسانه‌ها انجام می‌شود (کاستلز، ۱۳۸۹: ۲۶). بیمبر[۳](۱۹۹۸ م) می‌گوید: لازمه توفیق جنبش‌های یادشده، توانمندی در سه عرصه «شکل دادن به هویت جسمی»، «متقاعد ساختن پیروان خود» و «بسیج» آن‌ها است و فناوری‌های جدید ارتباطی به‌راحتی قادرند امکانات مورد نیاز برای تحقق این سه هدف را در اختیار جنبش‌ها قرار دهند. در جریان حوادث سال ۸۸ تهران نیز هیلاری کلینتون، وزیر امور خارجه وقت آمریکا حمایت رسمی کشورش از نقش توییتر و فیس‌بوک در اغتشاش‌ها را اعلام نمود و کمک مالی قابل توجهی را در اختیار گردانندگان این وبگاه‌ها قرار داد.

ایالات‌متحده آمریکا کنوانسیون شورای اروپا را در بحث مقابله با جرائم سایبری در سال ۲۰۰۶ م تصویب نمود. بخش اداره امنیت داخلی، سامانه هشدار ملی سایبری و گروه

---

۱. Occupy Wall Street Movement
۲. M. Castells
۳. Bimber

هماهنگی واکنش سایبری ملی را در قالب دو برنامه مهم در صیانت از آمریکا در برابر تهدیدات سایبری راه‌اندازی نمود. علاوه بر این اداره امور امنیت داخلی بر روی طرح‌ها و مانورهای امنیتی در فضای سایبری در مقابله با هجوم حملات سایبری به‌طور مداوم نظارت خواهد نمود.

یگان فرماندهی ارتش سایبری ایالات‌متحده[۱] در سال ۲۰۰۹ م تأسیس شد که زیرمجموعه و تابع دستور فرماندهی راهبردی ایالات‌متحده می‌باشد. عناصر عملیاتی و خدماتی سازمان سایبری آمریکا عبارت‌اند از: نیروهای فرماندهی ارتش سایبری[۲] یگان بیست و چهارم نیروی هوایی ارتش، فرماندهی سایبری ناوگان دریایی[۳] و فرماندهی سایبری نیروهای دریایی.[۴] در بیانیه مربوط به مأموریت فرماندهی سایبری ایالات‌متحده[۵] آمده است که «برنامه‌ها، طرح‌ها، هماهنگی‌ها، همبستگی‌ها، همگامی‌ها، هم‌زمانی‌ها و اجرای فعالیت‌ها برای هدایت برنامه‌های عملیاتی و حمایت از بخش‌های مشخص‌شده از شبکه‌های اطلاعاتی محافظت‌شده و آماده‌سازی آن‌ها، برای انجام طیف کامل عملیات ارتش در فضای سایبری به‌منظور فعال کردن اقدامات در همه حوزه‌ها، اطمینان‌بخشی به آزادی آمریکا و متحدانش از اقدام در فضای سایبری و انکار آن برای دشمنان ما» است(مستندات وزارت دفاع آمریکا؛[۶] ۲۰۱۰).

قانون جرائم سایبری در ایالات‌متحده تحت عنوان قانون شماره ۱۸ در خصوص مجازات و جرائم جنایی می‌باشد. در این قانون مجازاتی برای جرائمی مانند سرقت هویت اینترنتی، هک کردن، نفوذ به سامانه‌های رایانه‌ای و استفاده جنسی از کودکان در نظر گرفته شده است. قانون حریم خصوصی ۱۹۸۶ بحث ارتباطات الکترونیکی، الزامات مورد نیاز در افشای داده‌ها و چگونگی شرایط ردیابی و نظارت دستگاه‌های تلفن همراه و ره‌گیری

---

۱. USCYBERCOM or CYBERCOM
۲. ARFORCYBER
۳. FLTCYBERCOM
۴. MARFORCYBER
۵. USCYBERCOM
۶. Department of Defense fact sheet

داده‌های ارتباطی را بیان می‌کند. این قانون، ارتباطات تلگرافی، الکترونیکی و ارتباطاتی را که از طرق مذکور ذخیره یا افشاء شده، پوشش می‌دهد. در سال ۱۹۹۴ م ایالات‌متحده آمریکا قابلیت‌های ره‌گیری ارتباطات را به‌صورت قانونی با تصویب کمک به ارتباطات برای اجرای بهتر قانون، به‌روزرسانی نمود.

همه موارد فوق نیاز به نظارت قضایی دارد. با این حال از سال ۲۰۰۱ م ایالات‌متحده آمریکا برای رهگیری و ردیابی ارتباطات بدون نیاز به هرگونه حکم یا دستور قضایی طبق نظارت بر اطلاعات خارجی عمل می‌نموده است. این قانون در سال ۲۰۱۳ م مورد بررسی قرار گرفت (جهانشیری، تقی‌پور و پورمنافی، ۱۳۹۴: ۱۶۵).

کشور آمریکا به‌شدت به دستگاه‌های رایانه‌ای وابسته است. حوادث ۱۱ سپتامبر به‌طور خاصی به افزایش آگاهی از آسیب‌پذیری‌ها و مسئله فوریت در پاسخگویی تخریب یا اختلال در زیرساخت‌های حساس منجر شد. همچنین دولت تدابیر امنیتی در اینترنت را تشدید کرد. جورج بوش، رئیس‌جمهور وقت آمریکا، دستور داد ۱/۵ میلیارد دلار بر بودجه تدابیر امنیتی شبکه‌های رایانه‌ای و اینترنت و همچنین آموزش متخصصانی که با حملات اینترنتی احتمالی تروریست‌ها مقابله می‌کنند، افزوده شود (ضیایی‌پور، ۱۳۸۹: ۱۱۴). حملات ۱۱ سپتامبر، مسلم ساخت که مسئله حفاظت از زیرساخت‌های حساس به هسته اصلی امنیت ملی تبدیل شده است و این در حالی بود که دولت کلینتون تهدیدهای سایبری را یکی از خطرات عمده قرن بیست و یکم تعریف می‌کرد. دولت بوش با چرخش از یک تمرکز بسیار قوی بر ابزارهای سایبری و روش‌های شکل‌گیری تهدید سایبری به سمت ادغام با دیدگاه‌هایی در باب تروریسم پیش رفت. تهدیدهای سایبری در ارتباط مستقیم با بحث حفاظت از زیرساخت‌های حساس است (دان کاولتی، ۱۳۸۹: ۱۲۶)، برخی زیرساخت‌های حیاتی ازجمله حوزه مسائل مالی، بخش برق و شبکه‌های ارتباطاتی به‌طور فزاینده‌ای در برابر حملات سایبری آسیب‌پذیر هستند. بخش خصوصی در ایالات‌متحده در حدود ۸۵ تا ۹۰ درصد زیرساخت‌های حیاتی این کشور را در اختیار دارد و فعالان این بخش‌ها برای کنترل و اداره این فرآیندهای حساس از فضای سایبری استفاده می‌کنند. وقوع یک حمله سایبری

و بروز اختلال در شبکه‌ها حتی برای مدت‌زمان اندکی می‌تواند موجب از بین رفتن اموال، منابع و کشته شدن انسان‌های بی‌گناه شود (خبرگزاری صداوسیما[۱] به نقل از بختیاری ۱۳۹۷).

آمریکا به هنگام حفاظت از زیرساخت‌های بنیادی نباید بسیار خام و بیش‌ازحد مقرراتی عمل کند و باید از راه‌حل‌های بازار تا حد ممکن جانب‌داری کند. این هدف فراگیر باید تأمین‌کنندگان زیرساخت‌های بنیادی و پیشرفته را قادر سازد تا از امنیت بیشتری نسبت به مجموعه گسترده‌ای از تهدیدها برخوردار باشند، در حالی که برای تأمین‌کنندگان کمترتوسعه‌یافته این امکان را فراهم می‌سازد تا به سطح بالایی از امنیت دست یابند. برای دستیابی به اهداف فوق و برای دفاع از زیرساخت‌های ملی، دولت ایالات‌متحده گام‌های متعددی برداشته است. اگرچه پرداختن به تمام آن گام‌ها از دامنه این مطلب خارج است، اما چند مورد، ارزش مطرح شدن دارد. گام اول، تأسیس یک مرکز هماهنگی تیم پاسخ اضطراری رایانه‌ای در دانشگاه کارنگی- ملون است. این مرکز در سال ۱۹۹۸ م پس از آنکه یک رویداد مهم در اینترنت، هزاران رایانه را دست‌خوش اختلال کرد، تأسیس شد. اداره پروژه‌های پیشرفته وزارت دفاع که اینترنت را بنا نهاد، مرکز هماهنگی گروه پاسخ اضطراری رایانه‌ای را طوری بنیان نهاده که ایالات‌متحده برای رویدادهای آتی بهتر آماده باشد. مرکز فوق دارای یک نقطه تماس ۲۴ ساعته و یک نقطه مرکزی برای مشخص کردن آسیب‌پذیری‌ها و رفع آن‌ها به کمک فروشنده است (عبدالله خانی، ۱۳۹۲: ۱۳۶)، گام دوم، تشکیل کمیسیون ریاست جمهوری درباره حفاظت زیرساخت‌های اساسی در ژوئیه ۱۹۹۶ م است. از این کمیسیون خواسته شد آن گروه از زیرساخت‌های حساس که سامانه‌های حمایت از نخبگان را تشکیل می‌دهند، مطالعه کنند و آسیب‌پذیری‌های آن‌ها را در برابر گستره وسیعی از تهدیدها مشخص نمایند و برای محافظت از آن‌ها در آینده، راهبردی پیشنهاد کنند. سال‌های ۱۹۹۷ و ۱۹۹۸ م درواقع سال‌های آستانه ارائه دیدگاه‌های مختلف در باب تهدیدهای سایبری بوده است. در گزارش کمیسیون ریاست جمهوری درباره حفاظت زیرساخت‌های اساسی تهدیدهای سایبری، حتی از تهدیدهای جدید نیز خطرناک‌تر

---

۱. Iribnews.ir

توصیف شده بودند (دان‌کاولتی، ۱۳۸۹: ۱۲۶). گام سوم، کنگره باید در قانون امنیت داخلی سال ۲۰۰۲ م تجدیدنظر کند تا وزارت امنیت داخلی از اختیارات بیشتری در حفظ زیرساخت‌های بنیادی آمریکا در فضای سایبری برخوردار شود. این موضوع باید اختیار در مورد قواعد موضوعی تحت صلاحیت را شامل شود که بر اساس آن تهیه‌کنندگان زیرساخت‌های بنیادی، مبنای محکمی را برای اقدامات امنیتی می‌پذیرند. اگرچه رئیس‌جمهور اختیارات فوق را از طریق دستورالعمل‌های مشخصی ارائه کرده است، اما این اختیارات باید بر اساس قانون مدون شود تا درنهایت به تقویت امر پاسخگویی منتهی شود، همچنین کنگره با وضع قوانین سایبری باید زمینه را برای راهبردهای نظارتی دقیق فراهم کند که با اهداف و نیازهای بخش‌های خاص متناسب باشد (لرد و شارپ، ۲۰۱۱: ۴۸).

ب) راهبردهای دولت آمریکا برای ارتقای امنیت سایبری

راهبرد آمریکا در جنگ نرم بر اساس دیپلماسی سیاه بیشتر از طریق مؤسسه «خطر جاری» و مؤسسه «هوور» که به دنبال شکل‌دهی به انقلاب‌های مخملی است، صورت می‌پذیرد. دیپلماسی سیاه از سال هزار و نهصد و هشتاد کار خود را آغاز کرد و در همه انقلاب‌های مخملی تأثیرگذاری آن دیده می‌شود. در این دیپلماسی، دولت آمریکا بدون جنگ و خونریزی، حکومتی را ساقط و حکومت دیگری را جانشین آن می‌کند. روش اجرای این سیاست به‌گونه‌ای است که شرایط کاملاً عادی است، روابط دیپلماسی بدون هیچ‌گونه اعمال تحریمی برقرار است و شرکت‌های تجاری روابط دوطرفه دارند. در چنین شرایطی مشکل به داخل کشور برمی‌گردد و مردم، دولت‌مردان خود را عامل بروز نارضایتی می‌دانند. دموکرات‌های آمریکا بیشتر از این روش در مقابله با کشورهای هدف، بهره‌برداری می‌کنند (خلیلی جو لرستانی، ۱۳۹۶: ۱۵۵).

در ژانویه سال ۲۰۰۸ م، دولت بوش طرح جامع امنیت سایبری ملی[1] را جهت تلاش برای امن‌تر ساختن ایالات‌متحده در مقابل تهدیدهای سایبری آغاز کرد. این طرح جامع،

---

1. CNCI

ایجاد سیاست، راهبرد و راهنمایی‌هایی برای سامانه‌های امنیتی فدرال بود. همچنین رویکردی بود که تهدیدهای آینده اینترنتی و فناوری و نیازهای دولت فدرال به ادغام بسیاری از توانایی‌های فنی و سازمانی آن را برای پاسخ بهتر به تهدیدهای پیچیده، پیش‌بینی می‌کرد (تئوهری ورولینز[1] ۲۰۰۹: ۳). در سال ۲۰۰۹ م دولت اوباما، مجموعه‌ای از راهبردها را برای امنیت سایبری به‌منظور مقابله با تهدیدها، تدوین و صورت‌بندی کرد. این ابتکار دوازده دستورالعمل نظامی، غیرنظامی، شبکه‌های دولتی و سامانه‌های زیرساخت را پوشش می‌دهد. در قدم نخست تأکید رئیس‌جمهور به کار هماهنگ بخش خصوصی، جامعه پژوهشی و شهروندان برای ایجاد زیرساخت‌های اینترنتی قابل اعتماد و انعطاف‌پذیر برای حفظ پیشرفت‌های ملی و امنیت میهنی است (استون[2] ۲۰۱۰: ۶).

ده برنامه کلیدی برای تقویت امنیت سایبری ایالات‌متحده در هم‌نشستی که در ۲۰۱۰/۳/۲ از سوی مؤسسه بین‌المللی CACI و مؤسسه مطالعاتی نیروی دریایی ایالات‌متحده با عنوان «تهدیدهای سایبری امنیت ملی و مقابله با چالش‌های پیش روی زنجیره عرضه جهانی» برگزار شد، ارائه شده است:

۱) سازمان و رهبری منسجم برای تلاش‌های فدرال برای امنیت سایبری و شناسایی امنیت سایبری به‌عنوان یک اولویت ملی؛

۲) شفاف‌سازی هرچه بیشتر برای امنیت سایبری بهتر در زیرساخت‌های حیاتی و توسعه راه‌های جدید برای کار با بخش خصوصی؛

۳) سیاست خارجی که تمام ابزار قدرت ایالات‌متحده برای ایجاد هنجارها، رویکردهای جدید به حکومت و عواقب اقدامات مخرب در فضای مجازی را در برمی‌گیرد. سیاست جدید باید چشم‌اندازی را برای آینده اینترنت جهانی روشن کند؛

۴) توانایی گسترش استفاده از هوش توانایی‌های نظامی برای دفاع در برابر تهدیدهای پیشرفته خارجی؛

---

۱. Theohary & Rollins
۲. Stone

۵) نظارت برای تقویت حریم خصوصی و آزادی‌های مدنی با قوانین و فرآیندهای روشن و سازگار با فناوری‌های دیجیتالی؛

۶) بهبود تشخیص هویت برای زیرساخت‌های حیاتی؛

۷) ایجاد یک نیروی کار گسترده با مهارت کافی امنیت سایبری؛

۸) تغییر سیاست مالکیت برای اداره بازار به سمت امنیت بیشتر تولیدات و خدمات؛

۹) سیاست تجدیدنظرشده و چهارچوب قانونی برای هدایت اقدامات امنیت سایبری دولت؛

۱۰) پژوهش، توسعه و تمرکز بر روی مشکلات امنیت سایبری و فرآیند برای شناسایی این مشکلات و تخصیص بودجه در یک روش هماهنگ شده است.

علاوه بر این وزارت دفاع، راهبرد خود را برای فعالیت در فضای سایبری (مصوب جولای ۲۰۱۱) در پنج طرح راهبردی برای ایالات‌متحده در فضای سایبری به شرح زیر مطرح نموده است:

الف) سالم‌سازی فضای سایبری به‌عنوان یک حوزه عملیاتی با استفاده از سازمان‌دهی، آموزش و تجهیز به‌طوری که وزارت دفاع آمریکا بتواند بهره‌برداری کامل از فضای سایبری را به‌صورت بالقوه داشته باشد.

ب) به‌کارگیری ایده عملیاتی دفاع جدید برای محافظت از سامانه‌ها و شبکه‌های وزارت دفاع.

ج) همکاری با سایر ادارات دولتی ایالات‌متحده، سازمان‌ها و بخش خصوصی به‌منظور مقدور نمودن راهبرد کامل دولت در امنیت‌بخشی به فضای سایبری.

د) ایجاد روابط مستحکم با متحدان ایالات‌متحده و شرکای بین‌المللی برای تقویت امنیت سایبری به‌صورت جمعی و گروهی.

ه) ابتکار عمل راهبردی: افزایش و تقویت نوآوری در کشور از طریق نیروی کار فوق‌العاده و بااستعداد در فضای سایبر و استفاده از فناوری‌های نوین و سریع (وزارت دفاع آمریکا، ۲۰۱۱).

به‌طور کلی تمرکز اصلی دولت آمریکا برای محافظت از ایالات‌متحده در برابر حمله سایبری است و مسئولیت آن به‌طور انحصاری به ارتش واگذار شده است. آمریکایی‌ها به دلیل وابستگی زیرساخت‌های حیاتی کشورشان به اینترنت، برای دولت نقش برجسته‌ای قائل‌اند و هدایت امنیت ملی در فضای سایبری را وظیفه دولت می‌دانند. آن‌ها بر همکاری و مشارکت بخش‌های خصوصی و دولتی تأکید داشته و این همکاری را از نوع اشتراک اطلاعات، امکانات و آموزش می‌دانند و دولت مرکزی را نیز به‌عنوان هماهنگ‌کننده اصلی در نظر گرفته‌اند.

اکثر کشورهای توسعه‌یافته ازجمله آمریکا برای تأمین امنیت در فضای مجازی خود، راهبردهای ملی خود را تدوین نموده‌اند که در کشور آمریکا سه هدف زیر مدنظر قرار داشته است:

۱. از حملات فضای سایبر به زیرساخت‌های اساسی کشور (که شاید منجر به منع استفاده آزادانه دیگران از فضای مجازی شود) ممانعت به عمل آید.
۲. زمینه‌های آسیب‌پذیری داخلی را که می‌توانند موضوع تهدیدات سایبر قرار گیرند، کاهش داده و از بین ببرند.
۳. در صورت وقوع حملات سایبر، ترتیبی اتخاذ شود تا خسارات وارده به حداقل رسیده و زمان بهبود شرایط کاهش یابد.

این راهبرد که پس از حادثه ۱۱ سپتامبر و با توجه به آسیب‌پذیری‌های جدی جامعه آمریکا ناشی از مخاطرات در فضای سایبر تدوین شده، به شرح زیر است: (پاک‌نظر، ۱۳۸۳: ۲)

۱. طراحی یک سامانه واکنش ملی، ویژه مقابله با تهدیدات در فضای سایبر؛
۲. طراحی برنامه واکنش در قبال تهدیدات و آسیب‌ها در فضای سایبر؛
۳. طراحی برنامه ارتقای سطح آگاهی و مهارت عمومی برای فعالیت در فضای سایبر؛
۴. اهتمام به ایمن‌سازی جایگاه مجازی حکومت در شبکه ارتباطی؛
۵. ایجاد همکاری و همگرایی بین دو بخش امنیت ملی و امنیت مجازی بین‌المللی.

تهدیدات سایبری و اقدامات امنیتی جمهوری اسلامی ایران

در این قسمت نیز ابتدا به بررسی تهدیدات سایبری متأثر از فضای مجازی در جمهوری اسلامی ایران پرداخته شده و سپس راهبردهای امنیتی این کشور در رویارویی با تهدیدات امنیتی برشمرده شده است.

الف) تهدیدهای امنیتی متأثر از فضای مجازی در جمهوری اسلامی ایران

ابرقدرت‌ها با استفاده از ویژگی‌ها و رشد روزافزون و فراگیر شدن فضای سایبری و با در نظر گرفتن نقاط ضعف و قوت دولت و ملت‌ها و چالش‌های فراروی آن‌ها، از ابعاد گوناگون در تضعیف نقاط قوت و جهت‌دهی و پررنگ نمودن نقاط ضعف آن‌ها، تلاش‌های بسیاری نموده‌اند. الگوهایی که توسط آن‌ها مانند آندلسی[۱] سکولاری[۲] و ... تعریف و تقسیم‌بندی شده، با همین نگرش صورت پذیرفته است. با کمی دقت در فضای اطراف و زندگی جوامع بشری خواهیم دید که به دلیل جایگاه دین، تعالیم و دستورات آن در برخی از کشورها که اسباب موفقیت را برای آن‌ها در برهه‌های مختلف به ارمغان آورده است، اقدام به تضعیف رویکردهای دینی و بی‌قیدوبند نمودن افراد در این امور می‌نمایند. بدون شک جامعه‌ای که اهداف عالیه آن در راستای منویات دینی‌اش تعریف شده باشد، با این آسیب‌پذیری تحت تأثیر قرار خواهد گرفت و جامعه انسانی آن مسیر تعریف‌شده را به‌درستی طی نخواهند نمود و حتی می‌تواند تضعیف شدن استقلال و آزادگی کشور همچنین دفاع از تمامیت ارضی را در پی داشته باشد (عسگری و گلی، ۱۳۹۷: ۱۲).

شیوه‌های سیاست‌گذاری در خصوص «رسانه‌های اجتماعی مجازی» از بیش از یک دهه گذشته، برای سیاست‌گذاران فضای مجازی در ایران، مسئله‌ای چالش‌برانگیز بوده است(بصیریان جهرمی، ۱۳۹۳: ۴). در این میان، به‌رغم اینکه طراحان راهبردها، با استفاده از رسانه‌ها سعی دارند تا با ایجاد چهارچوب منسجم، مطابق با موازین بوم خود، سیاست مصرف پاک و بهینه را شکل دهند (کاستلز، ۱۳۸۹: ۳۸۸) که از این دست راهبردها می‌توان

---

۱ Andalucía
۲ Seculari

به سندهای پدافند سایبری کشور و یا سند راهبردی افتا در ایران نیز اشاره نمود، ایران کشوری است که در خصوص مسدودسازی و فیلترینگ رسانه‌های اجتماعی مجازی در جهان، در جایگاه اول قرار گرفته است (بصیریان جهرمی، ۱۳۹۳: ۶۱)؛ اما با وجود همه محدودیت‌های سلبی اعمال‌شده از سوی سیاست‌گذاران رسانه‌ای که البته با هدف شفاف‌سازی و پالایش فضای مجازیِ کاربران ایرانیِ اینترنت در داخل ایران ایجاد شده است، کاربران ایرانی در استفاده از امکاناتی مانند وب‌نویسی و فعالیت در رسانه‌های اجتماعی مجازی، دارای فعالیت و رشد چشمگیری بوده‌اند (رسولی و مرادی، ۱۳۹۱). این مسئله در کنار گزارش‌هایی مبنی بر کسب رتبه چهارم وب‌نویسی جهان در سال‌های ۱۳۸۴ و ۱۳۸۵ (سایت تبیان، ۱۳۹۱) و جایگاه سوم جهان در شبکه اجتماعی اورکات (کوثری، ۱۳۸۶)، گویای این واقعیت است که کاربران ایرانی رسانه‌های اجتماعی، با استفاده از خط‌مشی‌های تعیین‌شده به این آمارها دست یافته‌اند. با این حال، از آنجا که سیاست‌گذاری در قبال این گروه از رسانه‌ها، بخشی از سیاست‌های فرهنگی هر کشور تلقی می‌شود، انتظار می‌رود که سیاست‌گذاران تنها در تقابل با عضویت، شیوه استفاده و کنشگری کاربرانی که قوانین و رویه‌های موجود را برنمی‌تابند، قرار گرفته باشند؛ اما چالش و دغدغه دیگری که پیشِ روی نهادهای سیاست‌گذار قرار گرفته، این است که برخی از مقامات سیاسی نظیر رئیس‌جمهور، وزرا، اعضای کابینه، نمایندگان مجلس و حتی بسیاری از سازمان‌های حقوقی و افراد سرشناس حقیقی و رهبران فکری به‌رغم این محدودیت عمومی و قانونی، از مدت‌ها پیش در رسانه‌های اجتماعی فیلترشده‌ای همچون فیس‌بوک، توییتر، یوتیوب و ... عضویت داشته و به فعالیت می‌پردازند؛ بنابراین سیاست‌های رسانه‌ای اتخاذشده، همچون مسدودسازی (فیلترینگ) رسانه‌های اجتماعی مجازی در ایران، برای کاربران و مصرف‌کنندگان، از آن جهت متناقض و غیرقابل قبول می‌نماید که به‌رغم سخت‌گیری‌های موجود پیشین در قالب وسایل ارتباطی یک‌سویه همچون رادیو، ویدئو، ماهواره و نظایر آن، رسانه‌های اجتماعی مجازی در جامعه شبکه‌ای حاضر و با بهره‌گیری از شبکه‌های جهان‌گستر اینترنتی از تعامل دوسویه برخوردارند و به این اعتبار، محبوبیت بیشتری نیز پیدا کرده‌اند.

به اعتقاد تاجیک (۱۳۸۲) تهدیدهای امنیتی متأثر از فضای مجازی در ایران عبارت‌اند از:

– اقدام‌های مخل امنیت و برانداز گروه‌های مسلح و غیرمسلح؛

– گسترش نابسامانی‌های اجتماعی از قبیل مواد مخدر، فساد اخلاقی، جرائم اجتماعی، سرقت و...؛

– شکاف بین اقلیت‌های قومی، مذهبی، زبانی با نظام و افزایش گرایش‌های تجزیه‌طلبانه قومی؛

– اقدام‌های تروریستی، خرابکاری و هکتیویسم؛

– آماده‌سازی افکار عمومی جهان علیه جمهوری اسلامی ایران در زمینه پرونده هسته‌ای و تشدید اقدام‌ها و تحریم‌ها علیه ایران؛

– اقدام سرویس‌های اطلاعاتی بیگانه به عملیات جاسوسی اینترنتی علیه جمهوری اسلامی ایران.

ب) اقدامات امنیتی در برابر تهدیدات فضای مجازی در ایران

به‌طور طبیعی، هرگونه نقش‌آفرینی مؤثر و مواجهه فعال و هوشمند، در گرو شناخت ابعاد و زوایای تأثیرگذاری این پدیده بر امور جاری است و بدون درک و شناخت هرچه کامل‌تر، نتیجه مطلوب حاصل نخواهد شد.

در ادامه راهبردهای مواجهه فعال در فضای مجازی کشور مورد بررسی قرار می‌گیرد.

۱– ساماندهی و مدیریت یکپارچه فضای مجازی کشور: با توجه به تشکیل شورای عالی فضای مجازی کشور، ضروری‌ترین اقدام‌ها عبارت‌اند از:

۱) واگذاری وظایف شوراهای موازی شورای عالی فناوری اطلاعات، شورای عالی انفورماتیک و نظایر آن به این شورا؛

۲) برخورداری تدابیر و راهبردهای این شورا از ضمانت اجرا برای قوای سه‌گانه؛

۳) رفع خلأ قانون‌گذاری در این حوزه؛

۴) همراه و هماهنگ شدن سایر قوا با این شورا و ایجاد ظرفیت‌ها و ساختارهای جدید در درون خود.

۲- اعتمادسازی و تقویت سرمایه اجتماعی: اگرچه تحقیق در مورد ارتباط میان سرمایه اجتماعی و شبکه‌های اجتماعی مجازی همچنان ادامه دارد، اما شواهد موجود حاکی از ارتباط مثبت میان سرمایه اجتماعی و اینترنت است، «سرمایه اجتماعی» که موضوعی «فرهنگ‌مدار» بوده و کلیدواژه‌های ادبیات آن بر اعتماد، آرمان و ارزش‌های اخلاقی استوار است، از جایگاه قابل توجهی در قدرت نرم برخوردار می‌باشد. قدرت نرم، یعنی توانایی تعیین اولویت‌ها، به‌گونه‌ای که با دارایی‌های نامریی، مانند جذابیت‌های فرهنگی، شخصیتی و ارزش‌ها، همسو بوده و اعتبار معنوی پدید آورد. برای مثال، اگر یک رهبر ارزش‌هایی را ارائه کند که دیگران، خود مایل به پیروی از آن باشند، هزینه اداره کردن آن جامعه به‌مراتب کمتر خواهد شد. این اعتبار معنوی باعث خواهد شد انسان‌ها با اراده و علاقه خود، کاری را انجام دهند که اعمال‌کنندگان قدرت نرم، آن را می‌خواهند (قدسی، ۱۳۹۲: ۱۴۲).

۳- مشارکت‌آفرینی: شبکه‌های اجتماعی مجازی، بسترهای بسیار مناسب و مغتنمی را برای ایجاد مشارکت افراد و اقشار مختلف جامعه فراهم ساخته است و «مشارکت»، عاملی مؤثر در ایجاد و تقویت قدرت ملی و قدرت نرم می‌باشد.

یافته‌های یک تحقیق نشان می‌دهد «جمهوری اسلامی ایران بیشترین کاربرد مؤلفه‌های قدرت نرم را در میان کشورهای اوراسیای مرکزی (۹۶٪/۳) و کمترین میزان (۲۸٪/۷۶) را نسبت به آمریکای لاتین داشته است. همچنین مشخص شد که بالاترین میزان اِعمال قدرت نرم ج.ا.ایران در مناطقی است که ساکنان آن بیشتر با زبان فارسی در ارتباط هستند. در ضمن، جمهوری اسلامی ایران بیشترین موفقیت را در کاربرد عوامل متغیر قدرت نرم، در زمینه بهره‌گیری از مؤسسه‌های ایران‌شناسی در سایر کشورها داشته است» (هرسیچ و تویسرکانی، ۱۳۸۸: ۲۲۵).

۴- آگاه‌سازی: رسانه‌ها با همان روش‌ها می‌توانند منابع قدرت نرم یک کشور، یعنی کارآمدی حکومت، سرمایه اجتماعی، اقتدار و جذابیت را تقویت کرده و با افزایش سطح رضایت، حساسیت و اعتماد سیاسی، میزان مشارکت نهادمند، مستمر و قانونی مردم را افزایش و مشروعیت دولت را افزایش دهند. نوع نگاه و دید راهبردی مسئولان در این

زمینه می‌تواند بسیار تأثیرگذار باشد، بنابراین فضای مجازی را به‌عنوان یک واقعیت باید پذیرفت و به‌جای نگاه امنیتی به این پدیده و اجرا و تجویز اقدام‌های سلبی (مانند پالایش، در وسیع‌ترین شکل ممکن)، به اقدام‌های ایجابی، مانند اعتمادآفرینی در اشکالی مانند افزایش سعه‌صدر و انتقادپذیری در مسائل اجتماعی و فرهنگی از منظر آگاه‌سازی مبادرت ورزید.

۵- اقدام‌های پژوهش‌محور: بسیار ساده‌لوحانه است که اقدام‌های دشمنان در عرصه جنگ نرم را اقدام‌هایی در سطح و فاقد عقبه علمی فرض کرد. بدون شک موفقیت چشمگیر حاصل‌شده در این فضا، مرهون تلاش‌های مجدانه عناصر فکری و پشتیبانی‌های بی‌دریغ صاحبان قدرت و نظام سلطه نوین جهانی در قالب مؤسسه‌های قدرتمند علمی و پژوهشی بوده است. از این رو مقابله و مواجهه مؤثر نیز تنها از این طریق امکان‌پذیر بوده و توسل به شیوه‌های غیرعلمی و منفعلانه، راه به جایی نخواهد برد. جمهوری اسلامی ایران به‌عنوان داعیه‌دار حضور در خط مقدم مبارزه با نظام سلطه جهانی و علاقه‌مند به ظهور جهانی انسانی به‌عنوان یک آرمان مقدس الهی، نیازمند ورود مقتدرانه در عرصه پژوهش با ایجاد و تقویت مؤسسه‌های پژوهشی در حوزه فضای مجازی می‌باشد. نتیجه تحقق این راهبرد آن است که به‌جای غافلگیر شدن، همواره در مواجهه با پدیده‌های نوظهور اجتماعی در این حوزه و توسل جستن به اقدام‌های سلبی و منفعلانه، به بازیگری فعال، آینده‌پژوه و آینده‌ساز تبدیل گردید. در شرایط کنونی، جامعه نیازمند تولید و راه‌اندازی شبکه‌های اجتماعی بومی است تا افزون بر برخورداری از قابلیت‌های شبکه‌های اجتماعی جهانی، مرزهای ملی و مذهبی کشورمان نیز در آن لحاظ شده باشد.

۶- مدیریت هوشمند: نظریه‌پردازان در دهه‌های اخیر، قدرت را با توجه به شاخص‌ها و معیارهای متکثر مورد بررسی قرار داده تا بتوانند زوایای مختلف آن را مورد کنکاش قرار دهند. بارنس[۱] در نظریه‌پردازی‌های خویش از واژه و اصطلاح قدرت ترکیبی استفاده

---

۱. Barness

کرد(بارنس[۱] ۱۹۹۸: ۳۷). سوزان ناسل[۲]معتقد است: توانایی‌ها وبرتری‌های نظامی، اقتصادی، فرهنگی و ایدئولوژیک باید در یک جهت هماهنگ شوند تا برآیند آن، تداوم برتری یک کشور را تضمین کند (فرهادی و مرادیان، ۱۳۸۷: ۱۴۷)، نظریه‌پردازان قدرت هوشمند بر این باورند که کشوری مانند ایالات‌متحده برای ایفای نقش جهانی نیازمند آن است که به اقدام‌های سازمان‌یافته برای دستیابی به سیطره دست زند. این امر، ماهیت منحصربه‌فرد و چندبعدی داشته و امکان پیوند ابزارهای دیپلماتیک، امنیتی و راهبردی را فراهم می‌سازد (متقی، ۱۳۸۷: ۶۴).

به اعتقاد جراحی (۱۳۸۳) اقداماتی که باید در راستای مقابله با تهدیدات امنیتی انجام داد عبارت‌اند از: ایجاد نهادهای تصمیم‌گیر دولتی در بالاترین سطح، بسیج بخش‌های غیردولتی و نگرش تخصصی، بومی‌سازی فناوری، استقرار مقطعی و با برنامه، ارتقای آموزشی، برنامه‌ریزی کاهش تهدیدها، تعاملات بین‌المللی و واکنش به تهدید در حداقل زمان ممکن (جراحی، ۱۳۸۳: ۲).

با توجه به آنکه موضوع امنیت در فضای سایبر در ارتباط مستقیم با امنیت ملی کشور قرار دارد، دولت باید از طریق وزارت اطلاعات وظیفه برنامه‌ریزی راهبردی برای این مسئله را بر عهده داشته باشد و از تخصص و توان موجود در شرکت‌های خصوصی و نهادهای غیردولتی[۳]نهایت استفاده را بنماید.

به اعتقاد قدسی (۱۳۹۲)، باید در طراحی فضای مجازی، ج.ا.ایران در پی ایجاد قدرت بزرگ مجازی در پرتو یکپارچه‌سازی فعالیت در فضای مجازی و طراحی نهادهای یکپارچه فرهنگی در این فضا، بر اساس نیازهای فرهنگی، سیاسی و اقتصادی بومی بود. این حقیقت غیرقابل‌انکار است که فضای مجازی – با وجود تهدیدها- فرصت‌های مغتنمی را برای معرفی توان‌ها و قابلیت‌های فرهنگی، ایجاد و افزایش سرمایه اجتماعی از طریق بهبود و سلامت ارتباط‌های اجتماعی افراد، آگاه‌سازی و آموزش‌های اجتماعی و درنهایت، تولید قدرت نرم در اختیار ملت‌ها و دولت‌ها قرار داده است و ج.ا.ایران نیز می‌تواند با

---

۱. Barnes
۲. Suzanne Nossel
۳. Non Government Organization (NGO)

ظرفیت‌سازی و مدیریت هوشمند، به بازتولید قدرت نرم در این فضا اقدام نماید. با این نگاه، راهبردهای پیشنهادی نیز عبارت است از:

۱- آگاه‌سازی سایبری: همگام با پیشرفت فناوری اطلاعات آسیب‌پذیری‌ها نیز افزایش یافته و اهمیت ارتقای آموزش و دانش سایبری عمومی اهمیت روزافزون پیدا کرده است و برای رسیدن به این مهم ضروری است در رشته‌های دانشگاهی و دروس نوین تحصیلات تکمیلی، در دانشگاه‌ها گنجانده شود. در بخش‌های تحقیق و توسعه همه سازمان‌ها اهمیت موضوع تبیین گردد و تحقیقات مرتبط با مقولات جنگ‌های نوین، دارای اولویت گردد. همچنین به‌عنوان دوره‌های آگاه‌سازی در مجامع عمومی، آموزش‌های کافی برگزار گردد.

۲- ایجاد امنیت در شبکه: اقدامات تأمینی لازم برای حفاظت از سامانه‌های اطلاعاتی و ارتباطات نیروهای مسلح و روش‌های اثربخش همچون استقرار مرکز عملیات امنیتی[۱].

۳- خودکفایی تجهیزاتی: برای دستیابی به امنیت واقعی چاره‌ای جز اجتناب از به‌کارگیری تجهیزات وارداتی، به‌خصوص تجهیزات حساس ارتباطاتی، شبکه‌ای و امنیتی نداریم. به همین دلیل مسئولین کشور و فرماندهان نیروهای مسلح باید به‌عنوان یک دغدغه مهم به این معضل نگاه کرده و بیش‌ازپیش به فکر تولید تجهیزات فناوری و ارتباطات بومی باشند و تولید سیستم‌عامل‌ها و نرم‌افزارهای داخلی بسیار ضروری به نظر می‌رسد.

۴- اتخاذ خط‌مشی فعال جنگ اطلاعاتی سایبری: نقاط ضعف سامانه‌های مخابراتی و الکترونیکی دشمن را باید شناسایی نموده و در حوزه جنگ سایبری، مشی فعال را اتخاذ نموده و تجربه و تبحر کافی را در زمینه به‌کارگیری ویروس، بدافزار، تروجان، کدهای رمزشکن، نفوذگری، ارسال پارازیت و ... کسب نمود.

۵- آموزش خبرگان و نخبگان: در این زمینه باید از نخبگان و چهره‌های برتر علمی و ظرفیت دانشگاه‌ها و فضای اجتماعی استفاده نماییم.

---

۱. SOC

۶- شناسایی و به‌کارگیری کلیه امکانات بالقوه سایبری در کشور: شرکت‌های پیش رو در تولید نرم‌افزار، دانشگاه‌های صنعتی معتبر و دانشگاه‌های نظامی، کارخانه‌های الکترونیکی پیشرفته، مراکز تحقیقاتی نظامی و صنعتی و غیر صنعتی، جشنواره‌های علمی معتبر، همایش‌ها و نمایشگاه‌های تخصصی و نظایر آن، بستر و زمینه‌های علمی و فنی مورد نیاز کشور را اداره و ارائه می‌نمایند که لازم است در راستای نیازمندی‌های کشوری و نیروهای مسلح کشور شناسایی شوند و از آنان بهره‌برداری به عمل آید. ترکیبی از خبرگان و متخصصین فناوری اطلاعات و سایر عرصه‌های اقتصادی و فرهنگی در بخش‌های یادشده می‌توانند زمینه لازم برای تشکیل یک نیروی واکنش سریع سایبری را فراهم آورده و در مواقع لزوم در اسرع وقت نسبت به انجام عملیات آفندی و یا پدافندی متناسب اقدام نمایند.

۷- ایجاد ساختار سازمانی مناسب در کشور: به‌منظور ورود در عرصه فرصت‌ها و تهدیدات سایبری و هماهنگی عملیاتی، ایجاد ساختارهای هماهنگ‌کننده ستادی و یگان‌های عملیاتی در همه سطوح لشکری و کشوری ضروری است (توکل، ۱۳۸۵).

۸- کاهش اقدام‌های تصدی‌گرایانه دولتی و افزایش سطح مشارکت‌های مردمی برای مدیریت شبکه‌های اجتماعی و بهره‌گیری بهینه از ظرفیت‌های جامعه (قدسی، ۱۳۹۲: ۱۸۴).

به این ترتیب با استفاده از مدل SWOT با رویکرد تقویت نقاط قوت و کاهش تهدیدها و آثار آن[۱] می‌توان اولویت‌های اساسی امنیت فضای سایبر را جهت نیل به راهبردهای پیشنهادی جهت تقویت داشته‌های استحکام‌بخش داخلی و تهدیدات متصور در این محیط به‌صورت زیر دسته‌بندی نمود:

۱) سامانه پاسخگویی امنیت فضای سایبر ملی؛

۲) برنامه کاهش آسیب‌پذیری و تهدید امنیت فضای سایبر ملی؛

۳) برنامه آموزش و اطلاع‌رسانی امنیت فضای سایبر ملی؛

۴) تأمین فضای سایبر دولتی؛

۵) همکاری بین‌المللی.

---

۱. ST

اولویت اول در مورد ارائه واکنش لازم به حوادث سایبر به‌منظور کاهش خسارات احتمالی است. اولویت‌های دوم، سوم، چهارم آسیب‌پذیری و خطر تهدید حملات سایبری را کاهش می‌دهند و اولویت پنجم نیز برای اجتناب از حملات سایبر خارجی که بر امنیت ملی تأثیر داشته و همچنین برای بهبود مدیریت بین‌المللی و پاسخگویی به چنین حملاتی در نظر گرفته شده است.

برای عملکرد به‌هنگام و سریع در مدیریت امنیت ملی در فضای مجازی، باید به شرایط حال و آینده آگاه بود، متغیرهای اثرگذار و محوری در امنیت ملی را آن‌گونه که هستند، درک و استخراج کرد و در چهارچوب نظام ارزشی و قانونی، به ترسیم راهبردها و کشف و معرفی راهکارها پرداخت، بر این اساس، راهکارهای زیر برای تأمین امنیت فضای مجازی توصیه می‌شود:

۱- به نظر می‌رسد تهدید اصلی کشور از ناحیه اینترنت، فقدان گفتمان امنیتی درباره این پدیده است. متأسفانه نگاه مدیران و دستگاه‌های مربوط در توسعه فناوری اطلاعات بدون در نظر گرفتن الزام‌های امنیت فضای مجازی، سبب ایجاد تبعات منفی داخلی و خارجی زیادی شده است؛ بنابراین توسعه فناوری اطلاعات باید همراه با لحاظ کردن الزام‌های امنیت فضای مجازی صورت گیرد.

۲- تقویت امنیت و حفاظت از اطلاعات حساس و سامانه‌های ارتباطاتی نهادها، سازمان‌ها و ارگان‌های مهم که به نحوی در خدمات‌رسانی عمومی دخالت دارند؛ زیرا هرگونه اخلال در انجام گرفتن مأموریت این سازمان‌ها، ممکن است آسیب‌های جبران‌ناپذیری را در پی داشته باشد.

۳- از آنجا که تهدیدها و آسیب‌های مجازی به‌سرعت تحول و تغییر می‌یابند، لازم است نهادهای متولی مدیریت آن‌ها، از انعطاف‌پذیری مناسب و مطمئن در برنامه، سازمان و مأموریت برخوردار باشند.

۴- فرآیند مدیریت امنیت ملی در فضای مجازی و مواجهه با تهدیدهای آن، فرایندی در حال شدن است و نباید آن را پایان‌یافته تلقی کرد. این امر، اصلاح و تکمیل هرساله

نظام جامع امنیت را در فضای مجازی با توجه به شرایط و یافته‌های نو ضروری می‌کند.

۵- اینترنت از دو جهت با آزادی‌های مدنی و خصوصی در ارتباط است: از یک‌سو، امکان سوءاستفاده از این ابزار نو برای تروریست‌ها، خرابکاران و دیگر بازیگران فروملی و فراملی وجود دارد و از سوی دیگر، این امکان وجود دارد که برنامه مبارزه با تهدیدها و مدیریت امنیت فضای مجازی به تهدید آزادی‌های مدنی به بهانه تأمین امنیت منجر شود. تصمیم‌سازی در این حوزه، بسیار دشوار است و لحاظ کردن هر دو جنبه آن در مدیریت امنیت فضای مجازی و تدوین قوانین مربوط به جرائم رایانه‌ای، ضروری است.

نتیجه‌گیری

یکی از اتفاقات مهم در پایان هزاره دوم، ظهور فناوری‌های ارتباطی است که برجسته‌ترین آن اینترنت و شبکه‌های اجتماعی است. این پدیده از یک‌سو فرصت‌هایی را به وجود آورده و امکان دسترسی افراد به اطلاعات را بسیار آسان نموده و از سوی دیگر تهدیدهای متعددی را به وجود آورده و فضای تا حدودی ناامن را در اختیار سودجویان برای دسترسی به اطلاعات دیگران و یا آسیب زدن به زیرساخت‌های ملی به وجود آورده است. از این نظر برخی کشورها بر آن شده‌اند تا محیط سایبری خود را تا حد زیادی امن کرده و میزان خسارات ناشی از تهدیدهای فضای مجازی را به حداقل ممکن برسانند. ایالات‌متحده آمریکا ازجمله کشورهایی است که در این زمینه به موفقیت‌هایی رسیده است. البته اگرچه این کشور همچنان ازجمله کشورهای آسیب‌پذیر در حوزه سایبری است، اما میزان توجه و درگیری نهادهای مختلف این کشور در این زمینه شایان توجه است.

ایجاد توانایی ضربه زدن به تأسیسات حیاتی بازیگران رقیب در فضای نبردهای سایبر از متغیرهای مهم در به تصویر کشیدن جایگاه فضای سایبر در راهبرد امنیتی آمریکا است. اقدامات صورت‌گرفته برای تحقق این هدف شامل هنجارسازی‌های بین‌المللی در زمینه سایبر و ایجاد همکاری‌های بین‌المللی با محوریت آمریکا است. درواقع این نوع

هنجارسازی‌ها به ایالات‌متحده این فرصت را می‌دهند تا برای واکنش به حملات صورت‌گرفته از همه گزینه‌های خود ازجمله گزینه نظامی استفاده کند. همان‌گونه که تنها یک سازمان دولتی در آمریکا نمی‌تواند از تمامی شهروندان حمایت کند، یک سیاست تنها نیز نمی‌تواند امنیت سایبری کاملی ارائه دهد. از این رو دولت آمریکا نیاز به این دیده است که برای تقویت امنیت سایبری خود اقدام به یک برنامه‌ریزی جامع در سطح بین‌المللی در این زمینه بنماید. فضای مجازی، قدرتی را به‌عنوان قدرت نرم‌افزارها و فناوری اطلاعات و ارتباطات به وجود آورده است و این فناوری، بسیاری از عرصه‌های تقابل را متفاوت از گذشته ساخته است. اگر امروز یک میلیارد جمعیت دنیا در فیس‌بوک عضو می‌شوند، این، عضویت در یک نظام قدرت است. اگر امروز ۹۵ درصد جست‌وجوی اطلاعات در جست‌وجوگرهای آمریکا انجام می‌شود و این اطلاعات از مسیر آن‌ها عبور می‌کند، این به معنای یک سلطه قدرت نرم در این محیط است.

جمهوری اسلامی ایران نیز که ازجمله کشورهای مورد هدف جاسوسان سایبری است، به‌ویژه اینکه پس از ورود فضای مجازی و شبکه‌های اجتماعی به این کشور، به میزان فعالیت‌های خرابکارانه افزوده شده است، علاوه بر اینکه بودجه‌های هنگفتی توسط کشورها، نهادها و شرکت‌های چندملیتی جهت محقق شدن اهداف در این فضا هزینه می‌شود که البته نباید تلاش‌های متخصصان فضای سایبری در بالا بردن امنیت سایبری را در صیانت از مرزهای سایبری نادیده گرفت.

در این میان اگرچه سیاست فیلترینگ می‌تواند مانع دسترسی به شبکه‌های اجتماعی باشد، ولی ممکن است موجب آسیب‌های جدی‌تری گردد، بنابراین بایستی با توجه به پیشروندگی فضای سایبر، به‌رغم اقدامات مثبت انجام‌شده در کشورمان، راهکارهای نوینی با توجه به مقتضیات جدید ایجادشده در این محیط، همانند تحولات انجام‌شده در فناوری بدافزارها که ازجمله جنگ‌افزارهای این حوزه محسوب می‌شوند، برای مقابله با تهدیدهای سایبری به‌ویژه در فضای مجازی در دستور کار متخصصان داخلی قرار گیرد.

پیشنهادها

جهت استقرار ایمن فضای سایبر، راهکارهای زیر توصیه می‌گردد:

۱- جایگاه مرکز ملی فضای مجازی به‌عنوان بازوی شورای عالی فضای مجازی در جهت تحقق تصمیمات آن شورا با وظایفی همچون رصد وضعیت جاری فضای مجازی و پیش‌بینی و آینده‌نگری تحولات در این فضا در سطح ملی و بین‌المللی، ایجاد هماهنگی و هم‌افزایی میان وزارتخانه‌ها، سازمان‌ها و نهادهای مختلف ذی‌ربط در ابعاد علمی، فنی، اقتصادی، بازرگانی، حقوقی، انتظامی، امنیتی و دفاعی مرتبط با فضای مجازی و نظارت مستمر بر عملکرد دستگاه‌ها و بخش‌های ذی‌ربط در چهارچوب مصوبات شورای عالی تثبیت و تقویت شود.

۲- همکاری مستمر بین بخش‌های دولتی و خصوصی به وجود آید، به‌گونه‌ای که بخش خصوصی توان مقابله با مشکلات امنیتی را دارا باشد و بتواند در زمان بحران ملی به کمک دولت بیاید.

۳- بومی‌سازی فناوری در بخش‌های مهم مانند دیواره‌های آتش، تجهیزات شبکه‌ای مانند مسیریاب‌ها و ... صورت پذیرد، زیرا مهم‌ترین عامل نشت و سرقت اطلاعات از کشورهای مصرف‌کننده فناوری از ناحیه تجهیزات واگذارشده به آن کشورها است.

۴- در راه‌اندازی شبکه ملی اطلاعات، پس از تصویب طرح آن در شورای عالی تسریع شود و مرکز ملی بر مراحل راه‌اندازی و بهره‌برداری از آن نظارت مستمر و مؤثری انجام دهد.

۵- هنجارها، ارزش‌ها و سبک زندگی اسلامی- ایرانی و ممانعت از رخنه‌ها و آسیب‌های فرهنگی و اجتماعی در این حوزه ترویج داده شود و با تهاجم همه‌جانبه فرهنگی مقابله مؤثری صورت پذیرد.

۶- محتوا و خدمات کارآمد و رقابتی منطبق بر ارزش‌ها و فرهنگ اسلامی ـ ایرانی در تمامی قلمروهای مورد نیاز جامعه توسعه یابد و مشارکت‌های مردمی و به‌کارگیری ظرفیت‌های بخش خصوصی در این زمینه جلب شود.

۷- نظام‌های امنیتی، حقوقی، قضایی و انتظامی مورد نیاز در فضای مجازی تدوین و

تصویب گردد.

۸- اقدام‌های پژوهش‌محور و ساخت عقبه‌های علمی برای تولید ایده و انتشار محتوا در فضای مجازی و پرهیز از فعالیت‌های مقطعی و سطحی صورت پذیرد.

۹- اقدام‌های تصدی‌گرایانه دولتی کاهش یابد، سطح مشارکت‌های مردمی برای مدیریت شبکه‌های اجتماعی افزایش یابد و از تمامی ظرفیت‌های جامعه بهره‌گیری شود.

فهرست منابع ومآخذ

الف. منابع فارسی

- عبدی، سوران؛ الوندی‌زاده، اسدالله و مالکی، نسرین (۱۳۹۱)، بررسی تأثیر اینترنت بر رشد اقتصادی در کشورهای منتخب عضو(OIC)، اولین همایش بین‌المللی اقتصادسنجی، روش‌ها و کاربردها، سنندج، دانشگاه آزاد اسلامی واحد سنندج، https://www.civilica.com/Paper-ECONOMETRICS01-ECONOMETRICS01_035.html
- احمدی‌نژاد، حمید (۱۳۸۹)، حضور ناتو در محیط پیرامونی ایران و امنیت ملی جمهوری اسلامی ایران. پایان نامه کارشناسی ارشد، دانشگاه علامه طباطبایی، دانشکده حقوق و علوم سیاسی.
- بصیریان جهرمی، حسین (۱۳۹۳)، سیاست و مصرف رسانه‌های اجتماعی مجازی در ایران: چالش‌ها، الگوها و تبیین یک مدل پیشنهادی، رساله دکتری علوم ارتباطات، دانشگاه علامه طباطبایی.
- بوزان، باری (۱۳۸۹)، مردم، دولت‌ها و هراس، تهران، ترجمه پژوهشکده مطالعات راهبردی.
- پاک‌نظر، ثریا (۱۳۸۳)، دایرةالمعارف کامپیوتر، مؤسسه فرهنگی هنری دیباگران تهران.
- پالیزبان، محسن (۱۳۹۴)، بررسی رابطه اینترنت و امنیت ملی جمهوری اسلامی ایران، فصلنامه سیاست، مجله دانشکده حقوق و علوم سیاسی، ۴۵ (۳): ۶۳۵-۶۴۵.
- پورنقدی، بهزاد (۱۳۹۷)، فرصت‌ها و تهدیدهای امنیت در شبکه‌های اجتماعی مجازی برای دانشجویان، پژوهش‌های راهبردی مسائل اجتماعی ایران، ۷ (۲): ۸۷-۹۸.
- تاجیک، محمدرضا (۱۳۸۲)، مقدمه‌ای بر استراتژی‌های امنیت ملی ج.ا.ا رهیافت‌ها و راهبردها، نشر فرهنگ گفتمان.
- تهامی، سید مجتبی (۱۳۹۰)، امنیت ملی، داکترین و سیاست‌های دفاعی – امنیتی، سازمان عقیدتی سیاسی ارتش جمهوری اسلامی ایران.
- جانسون، لنا (۱۳۸۹)، امنیت در آسیای مرکزی: چهارچوب نوین بین‌المللی، ترجمه محمدرضا دبیری، نشر وزارت امور خارجه .
- جراحی، محمدحسین (۱۳۸۳)، دولت الکترونیکی، فرصت‌ها، چالش‌ها و روند آینده، دانشگاه شهید بهشتی.
- جهانشیری، جواد؛ تقی‌پور، رضا و پورمنافی، ابولفضل (۱۳۹۴)، مقایسه بین‌المللی جرائم سایبری، فصلنامه علمی- ترویجی مطالعات بین‌المللی پلیس، ۶ (۲۱): ۱۴۷-۱۸۵.
- چگنی‌زاده، غلامعلی و آثارتمر، محمد (۱۳۸۸)، «تحرکات قومی کردها و امنیت ملی ترکیه»، فصلنامه علوم سیاسی، شماره دوم.
- چگنی‌زاده، غلامعلی و آثارتمر، محمد (۱۳۸۸)، تحرکات قومی کردها و امنیت ملی ترکیه، روابط خارجی، ۲ (۳۷): ۱۸۵-۲۱۸.

- حافظ‌نیا، محمدرضا (۱۳۹۴)، جغرافیای سیاسی فضای مجازی، تهران، سمت.
- حسن‌بیگی، ابراهیم (۱۳۸۴)، توسعه شبکه ملی دیتا، چالش‌های فراروی و تهدیدهای متوجه امنیت ملی، مطالعات مدیریت (بهبود و تحول)، ۱۲ (۴۸): ۱-۲۷.
- حسن‌بیگی، ابراهیم (۱۳۸۴)، حقوق و امنیت در فضای سایبر، تهران، مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر.
- خلیلی جولرستانی، سید احمد (۱۳۹۶)، نگاهی دوباره به چالش‌ها و تهدیدات فضای مجازی بر امنیت پایدار، بصیرت و تربیت اسلامی، ۱۴ (۴۲): ۱۴۷-۱۷۶.
- داداندیش، پروین و کوزه‌گر کالجی، ولی (۱۳۸۹)، «بررسی انتقادی نظریه مجموعه امنیتی منطقه‌ای با استفاده از محیط امنیتی منطقه قفقاز جنوبی»، فصلنامه راهبرد، ۱۹ (۵۶): ۷۳-۱۰۷.
- دان‌کاولتی، میریام (۱۳۸۹)، سیاست‌های تهدید و امنیت سایبری، محبوبه بیات، تهران، مرکز آموزشی و پژوهشی شهید صیاد شیرازی.
- رایش، والتر (۱۳۸۲)، ریشه‌های تروریسم، ترجمه سید حسین محمدی نجم، تهران، دوره عالی جنگ، دانشکده فرماندهی و ستاد سپاه.
- رسولی ز، محمدرضا و مرادی، مریم (۱۳۹۱)، میزان مشارکت دانشجویان ارتباطات در تولید محتوای رسانه‌های اجتماعی، فصلنامه مطالعات فرهنگ – ارتباطات، ۱۳ (۱۹): ۱۱۳-۱۴۰.
- روزنا، جیمز و دیگران (۱۳۹۰)، انقلاب اطلاعات، امنیت و فناوری‌های جدید، مترجم علیرضا طیب، تهران، پژوهشکده مطالعات راهبردی.
- سلطانی‌فر، محمد (۱۳۹۰)، دیپلماسی عمومی نوین و روابط عمومی الکترونیک، نشر سیمای شرق.
- صادقی، سید شمس الدین و نادری، مسعود (۱۳۹۵)، تحلیل ابعاد امنیت دولت در ایران قرن بیست و یکم، فصلنامه دولت‌پژوهی، مجله دانشکده حقوق و علوم سیاسی، ۲ (۵): ۱۶۵-۲۰۲.
- ضیایی‌پور، حمید (۱۳۸۳)، جنگ نرم؛ ویژه جنگ رایانه‌ای، تهران، انتشارات مؤسسه فرهنگی مطالعه‌ها و پژوهش‌های بین‌المللی ابرار معاصر.
- عبدالله خانی، علی (۱۳۹۲)، نظریه‌های امنیت، جلد اول، تهران، مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر.
- عسگری، بصیر و گلی، سمانه (۱۳۹۷)، تأثیر فضای مجازی بر امنیت ملی جمهوری اسلامی ایران، نخستین همایش واکاوی تهدیدهای نوپدید دفاعی- نظامی، دانشگاه ستاد فرماندهی و ستاد آجا.
- عسگری، محمدعلی (۱۳۹۶)، جایگاه نبرد سایبری در استراتژی امنیتی آمریکا بعد از ۱۱ سپتامبر، پایان‌نامه برای دریافت درجه کارشناسی ارشد روابط بین‌الملل، دانشگاه علامه طباطبایی، دانشکده حقوق و علوم سیاسی.

- فرهادی، محمد و مرادیان، حسن (۱۳۸۷)، درک قدرت نرم با نگاهی به ج.ا.ایران، تهران، پژوهشکده مطالعات و تحقیقات بسیج.
- قدسی، امیر (۱۳۹۲)، تأثیر فضای مجازی بر امنیت ملی ج.ا.ایران و ارائه راهبرد (با تأکید بر نقش سرمایه اجتماعی)، فصلنامه راهبرد دفاعی، ۱۱ (۴۴): ۱۸۶-۱۴۹.
- کاستلز، مانوئل (۱۳۸۹)، عصر اطلاعات: اقتصاد، جامعه و فرهنگ، ترجمه افشین خاکباز و احد علیقلیان، جلد ۲، تهران، طرح نو.
- کوثری، مسعود (۱۳۸۶)، جهان فرهنگی کاربران ایرانی در شبکه دوست‌یابی اورکات، تهران، پژوهشگاه فرهنگ، هنر و ارتباطات.
- متقی، ابراهیم (۱۳۸۷)، قدرت هوشمند و استراتژی تغییر چهره آمریکا در دوران اوباما، فصلنامه مطالعات بسیج، شماره ۴۱.
- محبوبی منش، حسین (۱۳۸۱)، امنیت و انحرافات اجتماعی، مطالعات راهبردی زنان، ۳ (۱۸): ۱۳۳-۱۵۹.
- موحدی‌صفت، محمدرضا (۱۳۸۶)، امنیت ملی در فضای سایبر، فرصت‌ها و تهدیدها با تأکید بر استقرار دولت الکترونیکی، فصلنامه مطالعات دفاعی استراتژیک، ۸ (۳): ۲۴۶-۲۷۶.
- میزان استفاده جوانان از تلگرام و اینستاگرام، ispa.ir، تاریخ بازیابی ۱۳۹۸/۷/۲۵.
- نجفی علمی، مرتضی (۱۳۹۱)، روند تحولات فضای سایبر و نقش آن در تهدیدات ناشی از جرم در محیط سایبر در ج.ا.ا رساله جهت دریافت دکتری جامعه‌شناسی، دانشگاه علامه طباطبایی، دانشکده علوم اجتماعی.
- هرسیچ، حسن و تویسرکانی، مجتبی (۱۳۸۸)، ژئوپلیتیک قدرت نرم ایران، پژوهشنامه علوم سیاسی، ۴ (۲): ۲۶۹-۲۲۵.
- وطنی، امیر و اسدی، حمید (۱۳۹۵)، سیاست جنایی جمهوری اسلامی ایران در جرائم سایبری با تأکید بر ویژگی‌های خاص این جرائم، پژوهشنامه حقوق اسلامی، ۱۷ (۴۳): ۹۹-۱۲۶.

الف. منابع انگلیسی

- Al-Rodhan, N. R. (2009). The Three Pillars of Sustainable National Security in a Transnational World. Lit Verlag.
- Bimber, Bruce (1998), The Internet and Political Transformation: Populism, Community, and Accelerated Pluralism, Conference: ACM Policy - ACM Policy.
- Buzan, B., Wæver, O., Wæver, O., & De Wilde, J. (1998). Security: A new framework for analysis. Lynne Rienner Publishers.
- Department of Defense fact sheet – 2010: http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20 replaces %20May%2021%20Fact%20Sheet.pdf

- Department of Defense, USA. (2019, July). Department of Defense Strategy for Operating in Cyberspace. Available at http://www.defense.gov/news/ d20110714cyber.pdf.
- El Mrabet, Z., Kaabouch, N., El Ghazi, H., & El Ghazi, H. (2018). Cyber-security in smart grid: Survey and challenges. Computers & Electrical Engineering, 67, 469-482.
- Gadal, S., & Jeansoulin, R. (2000). Borders, frontiers and limits: some computational concepts beyond words. Cybergeo: European Journal of Geography.
- Hare, Forrest (2010); "The Cyber Threat to National Security: Why Can't We Agree?" CCD COE Publications, Tallinn, Estonia.
- Theohary, Catherine A. & Rollins, Johan (2009), Cyber Security: Current Legislation, Executive Branch Initiative, and Options for Congress, Congressional Research Service.
- Wagner, T. D., Mahbub, K., Palomar, E., & Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. Computers & Security, 87, 101589.