فصلنامه تخصصی علوم سیاسی
دوره ۱۹، شماره ۶۲، بهار ۱۴۰۲
نوع مقاله: علمی پژوهشی
صفحات: ۲۴-۱

تهدیدات جنگ سایبری و امنیت ملی ایران

بهروزنصیری[۱]
قاسم ترابی[۲]
علیرضارضایی[۳]

چکیده

فضای سایبر بستر اصلی اطلاعات محسوب می‌شود. ضرورت توجه به امنیت فضای سایبر نگاه ویژه‌ای را می‌طلبد. بدون شک امروزه زیرساخت‌های اصلی کشور اعم از اقتصادی، صنعتی، اطلاعاتی، امنیتی و...در این فضا قرارگرفته‌اند و گریزی از آن نیست و هرروزه شاهد افزایش کاربرد نرم‌افزارها در بستر این فضا هستیم؛ بنابراین هرگونه مشکل امنیتی در این فضا باعث تهدید جدی در امنیت ملی کشور خواهد شد. جنگ‌های پیش رو، در فضای مجازی شکل می‌گیرد. فضای مجازی را به‌عنوان پنجمین میدان جنگ پس از دریا، زمین، هوا و فضا نامیده‌اند. برخی معتقدند جنگ در فضای مجازی می‌تواند به سمتی پیش برود که در عرض یک‌لحظه سامانه‌های کنترلی یک کشور یا چند کشور از دست دولت‌های آن کشورها خارج‌شده و دنیای مدرن امروزی در کمتر از چند ثانیه از حرکت و پویایی بازایستد و فاجعه‌ای بسیار مصیبت‌بارتر از فاجعه اتمی پیش آورد. در هر جنگی، شرط اولیه شناخت صحنه نبرد است. ابتدا صحنه و فضای سایبر را باید به‌درستی بشناسیم تا بتوانیم در آن صحنه قدرت مانور، جنگ و دفاع داشته باشیم. هدف از این پژوهش، بررسی تأثیرات فضای سایبری بر امنیت ملی جمهوری اسلامی ایران در حوزه‌های مختلف به‌ویژه حوزه‌های سیاسی-امنیتی می‌باشد. همچنین کشف نقاط ضعف و یا کاستی‌های موجود در حوزه امنیت سایبری با توجه به تهدیدات موجود در فضای مجازی از دیگر اهداف پژوهش حاضر می‌باشد که به‌صورت روش تحلیلی-توصیفی به این پرسش اساسی می‌خواهد پاسخ دهد که تهدیدات سایبری چگونه بر امنیت جمهوری اسلامی ایران تأثیر می‌گذارد؟ امری که یافته‌های تحقیق بیانگر آن است که جمهوری اسلامی ایران یکی از مهم‌ترین کشورهای هدف حملات سایبری در حوزه‌های مختلف بوده و از این نظر تسریع در تجهیز زیرساخت‌ها و سرمایه‌گذاری در حوزه مقابله با تهدیدات سایبری ازجمله رویکردهای راهبردی ایران در این حوزه بشمار می‌رود که در این پژوهش به واکاوی ابعاد بیشتر آن پرداخته می‌شود.

کلمات کلیدی

فضای سایبر، تهدیدات امنیتی، جنگ سایبری، امنیت ملی، ایران

۱-دانشجوی دکتری تخصصی روابط بین‌الملل، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران. 1364behnasiri@gmail.com
۲-دانشیار روابط بین‌الملل، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران. (نویسنده مسئول) ghasemtoraby@yahoo.com
۳-دانشیار روابط بین‌الملل، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران. Alirezarezaei@gmail.com

مقدمه

فناوری، همواره نقش تعیین‌کننده‌ای در شکل‌دهی به زندگی بشر ایفا کرده، اما باگذشت زمان و پیشرفت فناوری، تأثیرپذیری زندگی بشر از این پدیده تشدید شده است. بسیاری انقلاب صنعتی در سده هجدهم را نقطه عطفی در این راستا می‌دانند. پیامد انقلاب صنعتی، ظهور فناوری‌های پیچیده‌تری بود که بیش‌ازپیش بر تحولات جوامع انسانی سایه افکندند. این فناوری‌ها بر تبادلات و پیچیدگی نسبی ارتباطات انسانی افزودند. ویژگی تمامی انقلاب‌های فناورانه این است که تمامی قلمرو فعالیت انسانی را تحت تأثیر قرار می‌دهند، به این معنا که به‌عنوان بافتاری که فعالیت انسانی در آن جاری است، عمل می‌کند. (کاستلز،۱۳۸۵: ۶۰)

از دهه ۱۹۷۰، پیشرفت فناوری به نحو طوفان‌آسایی شتاب گرفت، به‌طوری‌که حالا دیگر می‌توان گفت که ماشین به‌عنوان زیربنای تولید تسلیحات برای تأمین امنیت، جای خود را به فناوری‌های اطلاعات و ارتباطات داده و درنتیجه، در استراتژی پردازی‌های نظامی محوریت یافته است. این وضعیت، آسیب‌پذیری‌های جوامع را به نحو خطرناکی افزایش داده و تهدیدهای امنیتی را بیش‌ازپیش پیچیده‌تر ساخته است. علاوه بر این، امکان ظهور کنشگران جدید در عرصه جهانی را فراهم ساخته و ظرفیت تأثیرگذاری کنشگران غیردولتی بر روندها و پویش‌های بین‌المللی ازجمله امنیت را با بهره‌گیری از فناوری‌های نوین اطلاعاتی و ارتباطاتی تقویت کرده است.

درعین‌حال، در کنار جهان واقعی، جهان مجازی ظهور کرده که کنشگران دولتی و غیردولتی، فارغ از محدودیت‌های جهان واقعی در آن نقش‌آفرینی می‌کنند. مهم‌ترین ویژگی فضای جدید کنترل‌ناپذیری تعاملات و تغییر ماهیت بسیاری از مفاهیم مانند جنگ و پیروزی است. دگرگونی در ابزارها و شیوه‌های نبرد، شکل‌های جدیدی از جنگ مانند جنگ اطلاعاتی را در فضای مجازی به وجود آورده که بر اساس آن، پیروزی نیز دیگر به معنای دستیابی به اهداف از طریق شکست دشمن با توسل به ابزارهای خشونت‌آمیز نیست؛ بلکه پیروزی به معنای دستیابی به اهداف بدون خونریزی و درگیری است. (نورمحمدی، ۱۳۹۰: ۱۲۹)

برخی، حوزه مجازی را پنجمین حوزه از نبرد می‌دانند. تحلیل‌گران نظامی، حوزه مجازی را به‌عنوان یک دامنه جدید در حوزه جنگ به رسمیت شناخته‌اند که اهمیت آن اکنون در حال فزونی گرفتن از سایر حوزه‌ها است. وجود نداشتن قوانین بین‌المللی باعث شده که هر کشوری به خود اجازه دهد تا بر ضد کشور دیگر وارد جنگ مجازی یا سایبری شود.

هدف ازجمله سایبری دست‌یابی به اطلاعات سایر کشورها، ایجاد وقفه در تجارت و یا ایجاد خدشه در زیرساخت‌هایی مانند آب، برق، حمل‌ونقل و ... است به‌گونه‌ای که هزینه‌های اقتصادی را افزایش دهند. در سال‌های گذشته میزان حملات سایبری در سطح جهان، بسیار افزایش‌یافته است. نقطه شروع جنگ مجازی را جنگ بالکان می‌دانند که نیروهای متخاصم سعی در نفوذ به اطلاعات یکدیگر داشتند. امروزه رشد شبکه‌های رایانه‌ای، بسیار سریع‌تر از رشد نرم‌افزارهای امنیتی مرتبط به آن‌ها است. هنوز زیرساخت‌های کافی برای جلوگیری از حملات سایبری در سیستم‌های رایانه‌ای کشورها تعبیه نشده است. فضای مجازی به یک مکان بالقوه برای جرائم این‌چنینی تبدیل‌شده است. میلیاردها دلار بدون کمترین امنیتی در فضای سایبر روزانه جابجا می‌شوند و بخشی از مهم‌ترین اطلاعات دولتی و شخصی بدون کمترین امنیتی در فضای مجازی وجوددارند که خطر حملات سایبری را افزایش می‌دهند. (واحدی فرد، ۱۳۹۱: ۳)

بیان مسأله

هم‌زمان با نقش فراگیر فضای مجازی و گستره شبکه‌های اینترنتی در زندگی مردم، این بستر نقش مهمی در ارتباطات جهانی ایفا می‌کند به‌گونه‌ای که نوآوری‌های صورت گرفته در کنار هزینه‌های کم در این بستر باعث دسترسی بیشتر و استفاده روبه گسترش مردم شده است. امروزه اینترنت شبکه وسیع جهانی در حوزه‌های مختلف ارتباطی و کسب‌وکارهای گوناگون بوجود آورده است که سالانه میلیاردها دلار برای اقتصاد جهانی سودآوری و نقش مهمی در توسعه کشورها داشته است. باوجوداین همه مزایای بستر فضای اینترنتی یا سایبری، دولت‌ها را در مقابل چالش‌های جدید امنیتی نیز قرارداده است که بیش ازهر چیزی ناشی از تهدیدات سایبری می‌باشد.

تهدیدات سایبری پدیده‌های جدید در دهه‌های اخیر می‌باشد که با تحول فن‌آوری اطلاعات و گسترش ارتباطات جهانی از طریق شبکه وسیع اینترنت در سراسر جهان به‌صورت انواع ویروس‌ها، کرم‌ها، جرم‌ها، هکرها و حملات اینترنتی ظهور و رشد پیداکرده است به‌گونه‌ای که امروزه چالش تهدیدهای سایبری، هم مهم وهم پیچیده به نظرمی‌رسد. تهدیدهای سایبری ویژگی‌های منحصربه‌فردی دارند. از یک‌سو، این تهدیدها گستره وسیعی اعم از موانع قانونی، فنی، سازمانی و فرهنگی را شامل می‌شوند و از سوی دیگر، هزینه کم، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری، موجب شده بازیگران زیادی به این عرصه وارد شوند. مهم‌ترین ویژگی‌های تهدیدهای سایبری در مؤلفه‌هایی چون؛

- تعدد بازیگران در فضای سایبری؛ هزینه کم فن‌آوری رایانه‌ای، اتصال گسترده بـه اینترنت و سهولت ایجاد یا به دست آوردن نرم‌افزارهای مخرب و... خلاصه می‌شود که به این معناست که تقریباً هرکسی

می‌تواند به این فضا وارد شود. این بازیگران شامل افراد، گروه‌های سازمان‌یافته جنایی، گروه‌های تروریستی، شرکت‌های خصوصی و دولت– ملت هستند (Charney,۲۰۰۹: ۵)

- هزینه کم ورود، صرف زمان کم و سرعت‌بالای اقدام، هر فرد برای انجام حمله سایبری تنها به یک رایانه، یک ارتباط اینترنتی و دانش فنی محدود در زمینه فضای سایبری نیاز دارد. درنتیجه، فضای سایبری شرایطی را فراهم کرده است که با هزینه پایین می‌توان اقدامات خطرناکی را در مدت‌زمان کم و با سرعت‌بالایی انجام داد. البته، انجام حملات پیچیده‌تر سایبری نیازمند صرف هزینه‌های بالاتری است.

- ناشناس ماندن بازیگران وعدم قابلیت ردیابی: اینترنت به‌عنوان سیستم نامتمرکز طراحی‌شده و کاربران آن، غالباً شناخته‌شده نیستند. همین ناشناختگی باعث می‌شود هیچ اثری از برخی از جمله‌های سایبری باقی نماند. افراد فعال درعرصه اینترنت می‌توانند از اقصی نقاط دنیا، بدون هشدار و در عرض چند ثانیه و بدون آنکه اثر یا نامی از خود بر جای بگذارند، اهداف دیجیتالی را مورد هدف قرار دهند

- تأثیرگذاری شگرف: ماهیت خاص فضای سایبری شرایطی را به وجود آورده است که بروز هر اختلال یا وقفه می‌تواند تأثیرات و پیامدهای به‌مراتب بیشتری از حادثه اولیه درپی داشته باشد. وقوع حمله‌های سایبری و درنتیجه آن، بروز اختلال در شبکه‌ها می‌تواند موجب ایجاد خسارت به اموال، زمان، محصولات و تولیدات، اعتبار، اطلاعات حساس و حتی از دست دادن جان انسان‌ها شود، زیرا در این‌گونه مواقع، زیرساخت‌ها و سامانه‌های مهم دچار آسیب می‌شوند

- کمرنگ شدن نقش جغرافیا: فضای سایبری سرعت انتقال به سراسر جهان را در لحظه کوتاهی فراهم کرده است. بنابراین، تهدیدکنندگان قادر به فراتر رفتن از محدوده جغرافیایی خود و رسیدن به اهداف کلیدی‌شان هستند (Starr ,۲۰۰۹: ۱۸)

- ساختار فضای اینترنت: اینترنت، دامنه مشترک و یکپارچه است. استفاده از این فضا توسط شهروندان، شرکت‌ها و دولت‌ها به شیوه‌ای است که جداسازی آن‌ها بسیار دشوار است. توانایی محدود برای جدا کردن بازیگران و فعالیت‌های آن‌ها، پاسخ مناسب به تهدید را بسیار دشوارتر کرده است (Charney,۲۰۰۹: ۶-۵) از سوی دیگر، ساختار اینترنت، دولت‌ها و شرکت‌های خصوصی را با عدم اطمینان در قبال خطرات فضای اینترنتی مواجه کرده است. این عدم قطعیت ناشی از پیچیدگی‌ها و فن‌آوری در حال تکامل برای پشتیبانی از سیستم‌های حیاتی است.

- پایین بودن احتمال تنبیه یا بازخواست اقدام‌های مجرمانه در فضای سایبری: احتمال تنبیه یا بازخواست اقدام‌های مجرمانه در فضای سایبری پایین است. درنتیجه، افراد و سازمان‌ها نیز این فضا را در مقایسه با گزینه‌های جایگزین غیر سایبری مطمئن‌تر و دارای خطرات کمتری می‌بینند.

با توجه به مؤلفه‌های فوق، اهمیت و پیچیدگی‌های ناشی از ماهیت تهدیدهای سایبری و ویژگی‌ها و نمودهای منحصربه‌فرد آن، شناخت و چگونگی مقابله با آن برای جلوگیری از آثار سوء و منفی بر حوزه‌های مختلف همچون امنیت ملی کشورها را به امری ضروری و اجتناب‌ناپذیر تبدیل کرده است به نظر می‌رسد در این میان هزینه‌های کم ورود، ناشناس بودن افراد، مشخص نبودن قلمرو جغرافیایی تهدیدکننده یا تهدیدکنندگان در این فضا، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری، موجب شده بازیگران قوی و ضعیف اعم از دولت‌ها و گروه‌های سازمان‌یافته و تروریستی و حتی افراد واردشده به این فضا؛ تهدیدهایی همچون جنگ سایبری، جرائم سایبری، تروریسم سایبری، جاسوسی سایبری و مانند آن‌ها را به وجود آورند. همین نکته، تهدیدهای سایبری را از تهدیدهای سنتی امنیت ملی که تا حدود زیادی از ماهیت شفاهی برخوردارند و بازیگران آن را دولت –ملت‌هایی تشکیل می‌دهند که دریک قلمرو مشخص جغرافیایی قابل‌شناسایی هستند، متمایز کرده و سبب شده است امنیت ملی به مفهوم سنتی آن در این فضا به چالش کشیده شده و ناکارآمد به‌حساب آید.

در این راستا در پژوهش حاضر با توجه به ظرفیت‌های فضای سایبری، به بررسی و واکاوی این مهم می‌پردازیم که تهدیدات سایبری چه تأثیرات مخربی می‌توانند بر امنیت ملی کشور داشته باشند و این تهدیدات، امنیت ملی را با چه تغییرات مهمی مواجه می‌کنند.

پیشینه تحقیق

با توجه به سابقه نه‌چندان زیاد تهدیدات سایبری نسبت به دیگر تهدیدات سنتی در این حوزه به‌ویژه موضوع پژوهش‌کارهای صورت گرفته به‌صورت محدود و نگاه اجمالی بوده که به برخی از مهم‌ترین آن‌ها در این بخش اشاره می‌شود:

احمدی و رفسنجانی (۱۴۰۰)، در کتاب «بایسته‌های راهبرد ایران در حکمرانی دیجیتال و حکمرانی سایبری، نویسندگان پژوهش حاضر، با توجه به پیچیدگی‌های ناشی از انقلاب دیجیتال و تأثیر این تغییرات در مناسبات سیاست‌گذاری داخلی و بین‌المللی و از سوی دیگر فقدان راهبرد درزمینه حکمرانی سایبری کشور، مرکز بررسی استراتژیک ریاست جمهوری در شش نشست با محوریت موضوع «حکمرانی سایبری و راهبرد جمهوری اسلامی ایران» طی سال ۱۳۹۹ به بررسی موضوع مذکور پرداخته‌اند. سلسله‌نشست‌ها درقالب کتابی با عنوان «بایسته‌های راهبردایران در حکمرانی دیجیتال و حکمرانی سایبری» منتشرشده است.

لسان طوسی و همکاران (۱۳۹۹) در پژوهش خود با عنوان «فضای سایبر و آیندهٔ هویت ملی: هشدارهای راهبردی برای امنیت ملی با رویکرد تحلیل لایه‌ای علّی که باهدف مشخص نمودن شاخص‌های

تبیین‌کننده هویت ملی در برابر شاخص‌های متضاد هویت ملی در فضای سایبر تعیین انجام‌شده تا تصویر کلان هویت ملی از سطح مسئله تا سطوح عمیق مشخص شود. به این نتیجه رسیدند که هویت ملی مردم ایران در سطوح مختلف مورد تهدید قرارگرفته است. اگرچه این تهدید تا حدی ناشی از ضعف سیستم‌های سیاسی و اقتصادی است، اما به دلیل به‌کاررفته شدن قدرت نرم غرب علیه ایران، این تهدید در لایه‌های جهان‌بینی و استعاره‌ها تشدید می‌شود تا حدی که منجر به تحقیر کشور و انکار پیشرفت‌ها توسط کاربران داخلی و باورپذیری افکار ترویج شده از سوی غرب می‌شود

Chris Jay HoofnaglE در کتاب Cybersecurity in Context "امنیت سایبری در متن" که در سال ۲۰۲۲ نوشته است:

تهدید سایبری را به‌عنوان یک مشکل "شرور" تعریف می‌کند، به این معنی که تهدید سایبری فقط قابل مدیریت است، نه حل کردن. همچنین امنیت سایبری به آموزش چند رشته‌ای نیاز دارد تا بتوان خطوط آن را درک کرد؛ بنابراین می‌توان برای پیچیدگی زیاد امنیت سایبری از روانشناسی، اقتصاد، علوم کامپیوتر و تئوری اطلاعات در کنار رشته حقوق کمک گرفت.

در این کتاب بر این نکته تأکید خواهدشد که چگونه چارچوب‌های اخلاقی، قانونی و اقتصادی فناوری‌ها، سیاست‌های امنیتی را توانا نموده و یا محدود می‌کنند. برخی از مهم‌ترین عناصر کلان (مانند ملاحظات امنیت ملی و منافع دولت-ملت‌ها) و عناصر خرد (مانند بینش‌های اقتصادی رفتاری در مورد چگونگی درک افراد و تعامل با ویژگی‌های امنیتی) را معرفی می‌کند. موضوعات خاص شامل سیاست‌گذاری (در سطح ملی، بین‌المللی و سازمانی)، مدل‌های کسب‌وکار، چارچوب‌های قانونی (شامل وظایف امنیتی، حریم خصوصی، مسائل دسترسی مجری قانون، هک کامپیوتر، جاسوسی اقتصادی/نظامی، و جنگ سایبری)، توسعه فنی استانداردها و نقش کاربران، دولت و صنعت است.

Yuchong Li و Qinghui Liu در سال ۲۰۲۱ در مقاله A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments مطالعه مروری جامع حملات سایبری و امنیت سایبری؛ روندهای نوظهور و تحولات اخیر بیان می‌دارند در حال حاضر بیشتر فعالیت‌های اقتصادی، تجاری، فرهنگی، اجتماعی و دولتی و تعاملات کشورها، در تمام سطوح، اعم از افراد، سازمان‌های غیردولتی و دولتی و نهادهای دولتی، در فضای مجازی انجام می‌شود.

هدف این پژوهش بررسی و بررسی جامع پیشرفت‌های استاندارد ارائه‌شده در حوزه امنیت سایبری و بررسی چالش‌ها، نقاط ضعف و قوت روش‌های پیشنهادی است. انواع مختلف حملات نسل جدید با جزئیات درنظر گرفته‌شده است. چارچوب‌های امنیتی استاندارد با تاریخچه و روش‌های امنیت سایبری

نسل اولیه موردبحث قرار می‌گیرند. علاوه بر این، روندهای نوظهور و تحولات اخیر امنیت سایبری و تهدیدها و چالش‌های امنیتی ارائه‌شده است. انتظار می‌رود که مطالعه مرور جامع ارائه‌شده برای محققان فناوری اطلاعات و امنیت سایبری مفید باشد.

اغلب این مطالعات به‌ویژه آنچه در داخل انجام‌شده است با در نظر گرفتن یک تعداد محدودی از تأثیرات عرصه سایبری رو تهدیدات متأثر از آن بر امنیت ملی موردبررسی و تحلیل قرارگرفته است به‌نوعی که در بیشتر پژوهش‌ها به دنبال ارزیابی آن و چگونگی اثرپذیری آن از محتوای فضای سایبر هستند. ارزش کاربردی مؤلفه‌های امنیت ملی در بخش‌های مختلف آن که توجه به آن‌ها لازمه حفظ جنبه‌هایی از امنیت ملی است در این پژوهش‌ها نادیده گرفته‌شده است. همچنین این پژوهش‌ها در مراحل سطحی به مسئله پرداخته و به علل عمیقی که منجر به اثرگذاری تهدیدات سایبری بر حوزه‌های حساس زیرساخت نظامی، هسته‌ای و صنعتی چندان توجهی نشده است. صحبت از مؤلفه‌های شکل‌دهنده به امنیت ملی، مبحث گسترده‌ای است که نیازمند پژوهش‌ها و تحقیقات تخصصی‌تر است. در این پژوهش به‌به بررسی تأثیرات منفی تهدیدات سایبری در تغییر ابعاد امنیت ملی و بحران امنیتی حاصل از آن و درنهایت هشدارهای راهبردی لازم برای غلبه بر این بحران امنیتی متأثر از تهدیدات سایبری پرداخته می‌شود و سعی بر این است کاستی‌های تحقیقات پیشین برطرف گردد.

چارچوب نظری تحقیق

نظریه واقع‌گرایی، در تبیین و تفسیر امنیت ملی در فضای مجازی می‌تواند تأثیر فناوری اطلاعات به‌خصوص اینترنت را بر امنیت ملی توضیح دهد: لذا در این پژوهش ازنظریه واقع‌گرایی استفاده کرده‌ایم.

نظریه واقع‌گرایی

واقع‌گرایان معتقدند در سطح سیاست داخلی، مسئله‌ای به نام امنیت وجود نداشته و امنیت صرفاً در سطح بین‌المللی معنا می‌یابد. به‌بیان‌دیگر، امنیت ملی نزد آنان چیزی جز امنیت بین‌الملل نیست و در این راستا ناامنی ویژگی بارز نظام بین‌الملل است. (عبدالله خانی، ۱۳۸۲: ۷۰) ازنظر واقع‌گرایان، عدم امنیت اصلی‌ترین مسأله، قدرت مهم‌ترین ابزار، دولت مهم‌ترین بازیگر و جنگ، بارزترین جلوه بروز ناامنی در عرصه بین‌المللی است. (یزدان فام، ۱۳۸۶: ۷۳۱؛ خلیلی پور رکن‌آبادی، نورعلی وند، ۱۳۹۱)

بنابراین، محور تمرکز واقع‌گرایی در موضوع امنیت، نظامی است.

همان‌طور که استفن والت تعریف می‌کند، مطالعات امنیتی، مطالعه تهدید، استفاده و کنترل نیروی نظامی است. (Williams and Krause و ۱۹۹۶: ۲۳۰) جدای از مسائل نظامی، سایر عوامل هم در بحث

امنیت می‌توانند مهم باشند، اما واقع‌گرایان و نو واقع‌گرایان معمولاً تنها تا جایی آن‌ها را مهم می‌شمارند که به توسعه توانایی‌های نظامی کمک کند. ازنظر واقع‌گرایان، هر چیزی ممکن است بر امنیت تأثیرگذار باشد، اما موضوع امنیت هر چیزی نمی‌تواند باشد. به باور واقع‌گرایان، چون دولت‌ها بازیگران اصلی در نظام بین‌الملل می‌باشند، بنابراین آنان مرجع امنیت قرار خواهند گرفت. (عبدالله خانی،۱۳۸۲: ۸۳؛ خلیلی پور رکن‌آبادی، نورعلی وند، ۱۳۹۱)

تعریف واژگان تخصصی تحقیق

الف) فضای سایبر

واژه "فضای سایبر[۱]" را نخستین بار ویلیام گیبسون،[۲] نویسنده داستان علمی تخیلی در کتاب نورومنسر[۳] در سال ۱۹۸۴ به‌کاربرده است. فضای سایبر در معنا به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق کامپیوتر و وسایل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود. (صدیق بنای،۱۳۸۵:۱)

مفهوم فضای سایبر، معطوف به فضای ساختگی و خیالی واقعیت مجازی و اینترنت است که انسان از طریق آن به فضای واقعیت مجازی وارد می‌شود. بدون فن‌آوری، فضای سایبر بی‌معنا خواهد بود. برخی، فضای سایبر را با موضوعات علمی ـ تخیلی مقایسه می‌کنند .این نوعی ناکجاآباد است که در آن می‌توان هویت‌های چندگانه داشتHaney 35:2006)). درواقع، اینترنت دروازه فضای سایبر است، اما فضای سایبر، با ویژگی‌هایی چون میزان و چگونگی دسترسی، راهبری، فعالیت اطلاع‌یابی، بالندگی و اعتماد شناخته می‌شود. (Folsom, ۲۰۰۷:۷۷)

ب) مفهوم امنیت

تعریف فرهنگ‌های لغات از «امنیت»، عبارت است از: در معرض خطر نبودن یا از خطر محافظت شدن. «امنیت» همچنین عبارت است از: رهایی از تردید، آزادی از اضطراب و بیمناکی و داشتن اعتماد و اطمینان موجّه و مستند. امنیت خواه فردی، ملّی یا بین‌المللی، در زمره مسائلی است که انسان با آن مواجه است. امنیت به‌صورت وسیع، در مفهومی به کار گرفته‌شده است که به صلح، آزادی اعتماد، سلامتی و دیگر شرایطی اشاره می‌کند که فرد و یا گروهی از مردم احساس آزادی از نگرانی، ترس، خطر یا تهدیدات ناشی از داخل یا خارج داشته باشند (ربیعی، ۱۳۸۳: ۴۴).

واژه «امنیت» ابتدا در ادبیات سیاسی آمریکا شدیداً متداول گردید. سپس تغییرات مهمی که پس از جنگ جهانی دوم در سیاست بین‌الملل پدید آمد، موجب شدند این مفهوم کارایی بیشتری پیدا

کند. بوزان[۴] که رهیافت مفهومی وسیعی از مسئله امنیت ارائه می‌دهد، اصطلاح «امنیت» را یک مفهوم توسعه‌نیافته تلقّی می‌کند. (بوزان، ۱۳۷۸: ۱۵).

دریکی از کامل‌ترین تلاش‌ها، برای تحلیل مفهوم امنیت (پیش از بوزان)، آرنولد ولفرز امنیت را به‌عنوان یک نشان و نماد مبهم توصیف نمود و به وجود نیروهای بالقوّه مبهم و استفاده سیاست‌مداران از آن اشاره کرد. پس ابهام مفهومی می‌تواند پیامدهای سیاسی مهمی در پی داشته باشد; زیرا رجوع به ملزومات امنیت می‌تواند برای توجیه اقدامات استثنایی مورداستفاده قرار گیرد. طبق نظر وی، امنیت در معنای عینی، فقدان تهدید در برابر ارزش‌های کسب‌شده را مشخص می‌کند، و در معنای ذهنی، فقدان ترس و وحشت از حمله به ارزش‌ها را معیّن می‌نماید. این دووجهی بودن مفهوم امنیت در تعاریف لغت‌نامه‌ها که از یک‌سو به معنای ایمنی، استواری و نفوذناپذیری، قابلیت اعتماد، اطمینان از عدم شکست و از سوی دیگر، به معنای عدم اضطراب از تشویش و خطر اشاره دارد، منعکس است. ازاین‌رو، تعریف واحد و مطلقی از «امنیت» وجود ندارد و این واژه دارای یک مفهوم ذاتاً نسبی است (عبدالله خانی،(357 :1387

به باور برخی سطح و عمق تأثیرگذاری انقلاب سایبری بر جوامع در حدی است که باید قرن بیست‌ویک را قرن سایبری نامید افزون بر این فضای سایبر چنان جوامع را تحت تأثیر بنیادین قرارداده است که دیگر زندگی انسان بدون آن قابل‌تصور نیست. به‌واقع تأثیرگذاری انقلاب سایبری بر زندگی انسان چنان گسترده است که برخی حتی آن را فراتر از اختراع خط و آغاز مدنیت بشر ارزیابی می‌کنند. به‌هرحال این‌یک واقعیت غیرقابل کتمان است که انقلاب سایبری موجی ایجاد کرده است که هرروز بعد جدیدی از زندگی انسان را دچار تغییر و تحولات گسترده‌ای می‌کند و شکل تازه‌ای به آن می‌دهد (۴۵ :۲۰۱۹,Torabi)

پ) جنگ سایبری

اگر با نظر کلازویتز موافق باشیم که جنگ عمل صرفاً سیاسی نیست، بلکه ابزار سیاسی برای رسیدن به اهداف سیاسی است، می‌توانیم بگوییم که جنگ در فضای مجازی توسط بازیگرانی صورت می‌گیرد که به دنبال استفاده از فضا برای رسیدن به اهداف سیاسی خود هستند. برای اینکه آیا عمل خصمانه در فضای مجازی جنگ قلمداد می‌شود یا نه، لازم است قصد بازیگر را درک کنیم. به‌عنوان‌مثال، اگر هدف از یک حمله اینترنتی سود مالی یا شخصی از طریق روش‌های مجرمانه مانند سرقت، تقلب و اخاذی باشد، باید با آن به‌عنوان عمل مجرمانه برخورد شود، اما اگر هدف مهاجم با جاه‌طلبی‌های به‌مراتب بزرگ‌تر همچون واردکردن آسیب به دولت یا شهروندان آن همچون تخریب، تضعیف و غیرفعال کردن

زیرساخت‌های نظامی و غیرنظامی باشد، چنین رفتاری درواقع چیزی نزدیک به اقدام جنگی در مفهوم سنتی است.

در سال ۲۰۰۸، استونی به‌عنوان کشور کوچک مدرن در مقیاس بزرگ موردحمله‌های اینترنتی قرار گرفت. فناوری بالای این کشور زمینه ای مناسب برای حمله‌های اینترنتی باانگیزه‌های سیاسی بود. همان‌طور که ریچارد کلارک استدلال می‌کند جنگ سایبری شکل جدیدی از مبارزه است که ما هنوز نمی‌توانیم آن را به‌طور کامل درک کنیم. درعین‌حال روشن است که در دنیای امروز، میدان جنگ حوزه خود را به فضای مجازی گسترش داده و باید آن را به‌عنوان پنجمین عرصه جنگ در کنار عرصه‌های سنتی زمین، هوا، دریا و فضا در نظر گرفت. (خلیلی پور و نورعلی وند، ۱۳۹۱: ۱۷۹)

انواع تهدیدهای سایبری

تهدیدهایی را که به‌صورت سایبری متوجه کشورها می‌شود می‌توان در دسته‌بندی زیر قرارداد:

۱-تهدیدهای مستقیم نظامی در فضای سایبر

تکنولوژی‌های سایبر با دارا بودن عملکردهای بسیار مشخص نظامی می‌توانند به‌طور مستقیم بر میدان نبرد تأثیرگذار باشند. بخش نظامی هر کشوری برای آموزش و تجهیز نیروها، سیستم‌های جنگ‌افزاری، ماهواره‌ها و شبکه‌های ارتباطی یا داده‌پردازی اطلاعات به تکنولوژی‌های سایبری وابسته است. درواقع می‌توان گفت فضای اطلاعاتی و سایبری به همان نسبت که می‌تواند فرصت‌های بسیار زیادی را برای نیروهای نظامی هر کشور به وجود آورد، به همان میزان نیز می‌تواند تهدیدهای بزرگی را برای این بخش ایجاد کند. بنابراین امروزه سرنوشت جنگ را دیگر تخریب‌ها، انفجارها و عملیات فرسایشی تعیین نمی‌کنند بلکه ازهم‌گسیختگی ظرفیت‌های فرماندهی و کنترل در فضای مجازی می‌تواند بسیار برای نتیجه برخوردها تعیین‌کننده باشد. علاوه بر این، امروزه بُعد اطلاعاتی به‌عنوان یکی از ابعاد محوری جنگ در همه عملیات‌ها، رزم‌ها و نبردهای آینده دخیل خواهد بود. همچنین در جنگ‌های آینده، کسب برتری سریع در حوزه اطلاعاتی یکی از عوامل مهم موفقیت خواهد بود. Rollins, J. & Henning,2009:8))

۲-تهدیدهای سایبری غیرمستقیم و غیرنظامی

در سال ۲۰۱۰ جدیدترین نمونه این‌گونه از حملات سایبری به‌وسیله حمله کرم (استاکس‌نت) شکل گرفت. این حمله نشان داد بازیگران جنگ‌های سایبری می‌توانند بدون نیاز به درگیری‌های نظامی به اهداف استراتژیک و سیاسی خود دست یابند. همچنین حمله این کرم خطرناک نشان داد که

ماهیت مبهم و نامشخص جنگ‌های سایبر سبب می‌شود که اقدامات مقابله‌به‌مثل با مشاجره‌های سیاسی همراه شود و چه‌بسا هزینه‌های بسیار زیادی را برای دولت‌ها به وجود آورد. همچنین در جنگ‌های سایبر مرز بین اهداف نظامی و غیرنظامی مبهم است. (ماه‌پیشانیان، ۱۳۹۰: ۱۰۱)

عموماً تهدیدهایی که در فضای سایبر در حوزه غیرنظامی وجود دارد و می‌تواند باعث صدمه در زیرساختارهای کشورها شود، عمدتاً در ۴ حوزه زیر قرار دارند:

۱. کاربران خانگی که در زمان اتصال به شبکه می‌توانند با ورود به سامانه‌های موجود تهدیداتی را به وجود آورند. معمولاً با توجه به آنکه اثر خاصی از آن‌ها در شبکه ثبت نمی‌شود، شناسایی آن‌ها دشوار می‌باشد.

۲. مؤسسات بزرگ مانند شرکت‌ها و دانشگاه‌ها که به بخش‌هایی از زیرساخت‌ها دسترسی دارند و انگیزه کافی در کارکنان و دانشجویان برای نفوذ به شبکه‌ها وجود دارد.

۳. بخش‌های مهم دولتی و مؤسسات ملی که بنا به اقتضا باید برخی از اطلاعات را به‌صورت اشتراکی در اختیار کاربران قرار دهند و خطر نفوذ از این ناحیه وجود دارد.

۴. کاربران شبکه اینترنت که بانفوذ به سرورهای موجود در زیر ساختارها می‌توانند تهدیدی برای آن‌ها به شمار آیند. (موحدی صفت، ۱۳۸۶: ۲۵۳)

۳-تروریسم و افراط‌گرایی

ماهیت نامتقارن، مخفیانه و مجازی فضای سایبر سبب شده است که این فضا، فرصت بسیار مناسبی را برای گروه‌های تروریستی و مجرمان سازمان‌یافته به وجود آورد. اگرچه هنوز شواهد محکمی در دست نیست که سازمان‌های تروریستی همانند القاعده و داعش بتوانند حملات گسترده نظامی را طراحی نمایند، اما این گروه‌ها از فضای سایبر برای انتشار پیام‌ها، آموزش و سربازگیری، بیشترین استفاده را می‌کنند. فضای اینترنت این امکان را برای گروه‌های تروریستی فراهم می‌کند که تکنیک‌های خود را با یکدیگر به اشتراک گذاشته، پیام‌های خود را اشاعه داده، سربازگیری نموده و به آموزش آن‌ها بپردازند. آنچه موفقیت این گروه‌ها را در فضای سایبر تسریع می‌نماید، ارزان و در دسترس بودن این تکنولوژی‌ها است

.نمونه بارز استفاده از جنگ سایبری را در عصر حاضر در منطقه خاورمیانه می‌توان توسط گروه تروریستی داعش مشاهده کرد.

در تروریسم کلاسیک مواد منفجره و سلاح‌های گرم اصلی‌ترین ابزار تروریسم هستند، ولی مهم‌ترین ابزار تروریست‌های سایبری، رایانه است. رایج‌ترین روش‌های این نوع تروریسم عبارت‌اند از هک کردن، شیوع ویروس‌های رایانه‌ای، جاسوسی الکترونیک، دزدی هویت و تخریب یا دست‌کاری اطلاعات. نرم‌افزارهای مخرب رایانه‌ای که تروریست‌های سایبری برای پیشبرد اهداف خود استفاده می‌کنند، متنوع هستند که ازجمله آن‌ها می‌توان به ویروس‌ها، کرم‌ها، تروجآن‌ها، اسپم‌ها اشاره کرد.

۴-جاسوسی سایبر

جاسوسی سایبر رایج‌ترین شکل فعالیت در فضای مجازی می‌باشد. جاسوسی سایبر خواه باهدف برملا نمودن اطـلاعات مهم حکومتی باشد یا دزدیدن اطلاعات بخش نظامی و بازرگانی، یک عـملیات مجازی است که به‌منظور کسب برتری اطلاعاتی برای دستیابی به موفقیت‌های بزرگ‌تر با صرف کمترین هزینه صورت می‌پذیرد. برای مثال چین تلاش می‌کند که با استفاده از جاسوسی سایبر در ساختارهای مهم سیاسی، اقـتصادی و نـظامی ایالات‌متحده امریکا و روسیه نفوذ نماید. در کـل می‌توان گفت، جاسوسی اینترنتی سبب سایش توازن اطلاعاتی بین دولت‌های مختلف می‌شود. البته هدف جاسوسی سایبر تنها دولت‌ها نیستند بـلکه شرکت‌های دفاعی، بازرگانی و سازمان‌های غیردولتی بین‌المللی نیز، می‌توانند هدف حملات جاسوسان سایبری قرار گیرند. ((Mueller, 2007:3

۵-جـنگ روانـی سایبر

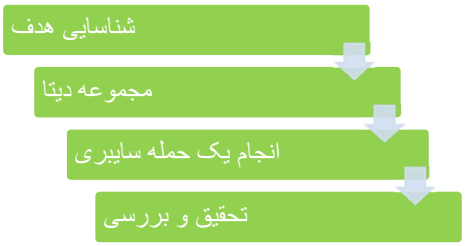
مهم‌ترین بعد جنگ‌های سایبر در جهان امروز بعد روانی آن است. عملیات روانی در فضای سایبر اقدامات برنامه‌ریزی‌شده برای انتقال اطلاعات و شاخص‌های منتخب به مخاطبان خارجی است که هـدف تأثیرگذاری بر احساسات، انگیزه‌ها، قدرت تفکر و استدلال و نهایتاً تغییر رفتار سازمان‌ها، گروه‌ها و اراده آن‌ها را شامل می‌شود. همچنین ممکن است طراحی عملیات دزدیدن اطلاعات در فضای سایبر باهدف ایجاد تشویش و نگرانی روانی طـراحی شـود. نمونه این مسئله را می‌توان در مورد کرم استاکس‌نت در ایران نام برد. مهم‌ترین هدف این کرم خطرناک افزایش ناامنی روانی در میان دولتمردان ایرانی بود. (ماه‌پیشانیان، ۱۳۹۰: ۱۰۴)

ت) دامنه حملات سایبری

حملات سایبری دامنه متنوعی دارند، از شوخی‌های معمولی تا کرم‌های مخرب رایانه‌ای که توسط حافظه‌های قابل‌حمل جابه‌جاشده و امنیت کلی کشوری را به مخاطره می‌کشند، جزو گستره این حملات قرار می‌گیرند. این تهاجم‌ها می‌توانند در سطح فردی و بر روی رایانه شخصی افراد یا تلفن همراه و یا در

سطح کلان بر روی سیستم‌های دفاعی و امنیتی کشوری تأثیرهای مخرب بگذارند. (عطیه طالب پور، ۱۳۹۸:۲)

حملات سایبری در زمینه وسیع‌تری نسبت به آنچه که به‌طور سنتی عملیات اطلاعاتی نامیده می‌شود قرار می‌گیرند. عملیات اطلاعاتی با استفاده یکپارچه از قابلیت‌های اصلی جنگ الکترونیک، روانی، شبکه کامپیوتری، ترفند نظامی و عملیات امنیتی با هماهنگی با پشتیبانی ویژه و توانایی‌های مربوطه و برای نفوذ، توقف، تخریب یا ربودن تصمیمات انسانی و یکی از فرآیندهای تصمیم‌گیری نهادهای ملی است. (Hart و همکاران، ۶:۲۰۲۰). شکل زیر تشریح آناتومی یک حمله سایبری است. از استراتژی USNM برای عملیات فضای سایبری، عملیات شبکه کامپیوتری از حمله، دفاع و امکان استفاده تشکیل‌شده است (Ma et al. ۲۰۲۱:۳). مورد دوم با حملات شبکه و دفاع شبکه متفاوت است، زیرا این نوع عملیات بیشتر بر جمع‌آوری و تجزیه‌وتحلیل اطلاعات متمرکز است تا قطع کردن شبکه‌ها و ممکن است خود مقدمه یک حمله باشد (Alghamdie:۴، ۲۰۲۱). این عملیات می‌تواند باهدف انتشار اطلاعات و تبلیغات انجام شود (Thomson، ۲۰۱۵:۴۸). عملیات فعال‌سازی بهره‌برداری از شبکه رایانه‌ای نیز می‌تواند باهدف سرقت داده‌های مهم رایانه انجام شود. در چنین زمینه‌ای، Sniffers و Doors Trap ابزارهای سودمندی برای فضای مجازی هستند (Liu et al،Trap Doors 2021:2) به یک کاربر خارجی اجازه می‌دهد تا در هر زمان بدون اطلاع کاربر رایانه به نرم‌افزار دسترسی داشته باشد. Sniffers ابزاری برای سرقت نام کاربری و رمز عبور است (Karbasi, & Farhadi،3؛ Yuchong &Qinghui، ۲۰۲۱)



آناتومی یک حمله سایبری از (Qinghui،Yuchong، ۲۰۲۱)

ایران و تهدیدات سایبری

الف) فضای مجازی در ایران

ایران در سال ۱۹۹۳ میلادی (۱۳۷۲ شمسی) به اینترنت و دنیای مجازی متصل شد. از آن زمان، تعداد کاربران اینترنت در ایران روند فزاینده‌ای داشته است. بر اساس آخرین آمار اعلام‌شده از سوی وزارت ارتباطات بر اساس محاسبه مرکز مدیریت توسعه ملی اینترنت (متما)، ضریب نفوذ اینترنت در کشور در سه ماه نخست ۱۳۹۳ عدد ۸۲/۱۲ درصد است که برمبنای سرویس‌های اینترنتی ارائه‌شده، محاسبه‌شده است. در این محاسبه تعداد کاربران اینترنت درسه ماه نخست آن سال ۶۱ میلیون و ۷۰۹ هزار و ۹۲۹ نفر و تعداد کل مشترکان اینترنت در کشور برمبنای جمعیت ۷۵ میلیون و ۱۴۹ هزار نفر در ایران، ۴۳ میلیون و ۲۶ هزار و ۲۷۹ نفر اعلام‌شده است. در گزارش ضریب نفوذ اینترنت در ایران، بیشترین اتصالات کاربران ایرانی مربوط به اینترنت تلفن همراه است و پس از اینترنت ADSL، بیشترین کاربر را به خود اختصاص داده است. براین اساس، ضریب نفوذ اینترنت ADSL در کشور به ۲۲/۰۷ درصد و ضریب نفوذ اینترنت تلفن همراه با توسعه‌تری جی در کشور به ۳۸/۶۷ درصد رسیده است که نشان می‌دهد حداقل ۲۹ میلیون ایرانی با تلفن همراهشان به اینترنت متصل می‌شوند. برآوردها از سایر شاخص‌های اتصالات در کشور نشان می‌دهد که همچنان ۶ میلیون و ۹۳۴ هزار و ۷۶۰ نفر در ایران از طریق تلفن (دایل آپ) به اینترنت متصل می‌شوند (عاملی، ۱۳۸۷: ۴۳؛) آمارهای موجود در سال ۱۳۹۸ نشان می‌دهند، درحالی‌که تعداد کاربران اینترنت در سراسر دنیا ۴ میلیارد و ۳۸۸ میلیون نفر با ضریب نفوذ ۶۷ درصد اعلام‌شده 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[۵]، ۱۳۹۸/۹/۹؛). همچنین بر اساس اعلام مرکز پژوهش‌های مجلس شورای اسلامی، هزینه اینترنت در ایران دو برابر افغانستان و ۳۵۰۰ برابر ژاپن است. در رابطه با نوع رفتار ایرانیان در فضای مجازی، رئیس مرکز فناوری اطلاعات و رسانه‌های دیجیتال وزارت فرهنگ و ارشاد اسلامی در مردادماه ۱۳۹۴ آمارهایی از میزان و نوع حضور ایرانی‌ها در فضای مجازی ارائه داد. به لحاظ نوع استفاده، کاربران ایرانی به ترتیب از وبگاه‌های ارائه‌کننده خبر، تبلیغات بازی، کتاب‌های الکترونیکی و فیلم‌های آموزشی و درسی بیشترین استفاده را دارند. این حجم از حضور و ظرفیت، ضرورت توجه به فضای مجازی را به‌عنوان یکی از ابعاد مهم زندگی فردی و اجتماعی نشان می‌دهد (سلامی، ۱۳۹۲: ۴۴؛)

ب) تهدیدات فضای سایبری بر امنیت ملی ایران

متأثر از تهدیدات فضای سایبری می‌توان بیان داشت که حاکمیت جمهوری اسلامی نیز، به لحاظ ژئوپولیتیکی با چالش‌های ویژه قرن حاضر مواجه است؛ چراکه امروزه انگیزه‌های زیادی از قبیل ژئوپولیتیکی، جغرافیایی، اقتصادی، مذهبی، سیاسی و ... برای مبارزه با نظام جمهوری اسلامی ایران از سوی کشورهای منطقه‌ای و فرامنطقه‌ای و گروه‌های مخالف نظام جمهوری اسلامی ایران وجود دارد که دشمنان را ترغیب به جاسوسی سایبری، خرابکاری سایبری، حمله‌های سایبری یا هدف ضربه به زیرساخت‌های جمهوری اسلامی و تلاش برای براندازی و تغییر حاکمیت آن می‌نماید. ساده‌ترین روش مبارزه با جمهوری اسلامی ایران، سعی در عدم توسعه‌یافتگی و اختلال در زیرساخت‌های حیاتی آن است که اجباراً باید در فضای سایبری قرار گیرند (موحدی صفت،۱۳۸۶:۲۴)

امنیت امروزه با تهدیدهای بی‌شماری مواجه است، اما در این میان، تهدیدهای سایبری پدیده جدیدی است که همراه با فناوری اطلاعات و گسترش ارتباطات گریبان گیر دولت‌ها شده است. این پدیده آن‌قدر جدید است که بررسی پیامدهای آن برای امنیت ملی دولت‌ها تا حد زیادی مورد غفلت واقع‌شده است. در دو دهه اخیر، یک طیف، گرایش به زیر سؤال بردن رویکرد رایجی که درباره امنیت در چارچوب مطالعات راهبردی در طول دوره جنگ سرد توسعه داده‌شده است، دارند. (کلارک، ۱۳۸۶: ۲۳۶)

ازنظر این گروه، امروزه دیگر تهدیدهای امنیتی صرفاً نظامی نیست، بلکه مسائل زیست‌محیطی، فقر جهانی، مهاجرت و اخیراً تهدیدهای سایبری بیش از تهدیدهای نظامی، امنیت دولت‌ها را به خطر انداخته است. بحث درباره تهدیدهای سایبری تأثیر گرفته از انقلاب مداوم اطلاعات می‌باشد که ناشی از پویایی انتشار اطلاعات و تکنولوژی‌های ارتباطات در همه جنبه‌های زندگی انسان است. به‌موازات افزایش ابعاد خدمات‌رسانی اینترنت در حوزه‌های مختلف زندگی بشر و به‌ویژه در امور تجاری و بازرگانی، مهاجمان رایانه‌ای، سارقان و جاسوسان اطلاعاتی، حجم تهدیدها و آسیب‌های ناشی از این فناوری را به‌شدت افزایش داده‌اند. این تهدیدها امروزه علاوه بر اینکه روزبه‌روز گسترش می‌یابند و پیچیده‌تر می‌شوند امنیت ملی دولت‌ها را به‌طور مستقیم تحت تأثیر قرار می‌دهند. (میرمحمدی و محمدی‌لرد، ۱۳۸۷: ۳۶)

مفاهیم سنتی جنگ بر اساس حمله و دفاع، توسط پیچیدگی‌های فضای مجازی، به چالش کشیده شده‌اند و با سرعت تغییر پیدا می‌کنند و این تهدید به‌نوعی مفاهیم سنتی جنگ را تغییر داده است. تهدید سایبر نامتقارن است و ازاین‌رو، نیاز به سرمایه‌گذاری بزرگی برای استفاده از آن یا حمله از طریق آن وجود ندارد. در مقابل، دفاع در برابر تهدید سایبر باید تمام جوانب را در نظر بگیرد که هزینه‌های آن امروزه در حال افزایش است.

شالوده و بنیاد هر کشوری بر اساس مجموعه‌ای از زیرساختارهای حیاتی آن کشور دربخش‌های ارتباطات، دفاع، انرژی، حمل‌ونقل، کشاورزی، بهداشت و امور اقتصادی است که فضای سایبر به‌مثابه یک سیستم عصبی آن‌ها را به هم 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 (صیاد و همکاران، ۱۳۹۹: ۲۹۷)

ازاین‌رو، امنیت سایبری در ارتباط مستقیم با امنیت ملی کشور است. امروزه دیگر نمی‌توان امنیت ملی را منحصراً در ارتباط با مرزهای خارجی و حفاظت از جان شهروندان به‌وسیله نیروهای نظامی تعریف کرد. امروزه به لطف اینترنت و یک دستگاه رایانه، دشمن بدون اینکه متوجه حضور فیزیکی‌اش باشیم تا خانه‌های ما رخنه کرده است. (خلیلی پور رکن‌آبادی و نورعلی وند، ۱۳۹۱: ۱۸۹)

بیشترین تهدیدات ناشی از فضای سایبری بر ضد امنیت ملی ایران را می‌توان ناشی از تخاصم برخی قدرت‌ها با جمهوری اسلامی و استفاده ابزاری از فضای سایبری برعلیه ایران در قالب جنگ سایبری دانست به‌گونه‌ای که فقط در یک مورداستفاده ابزاری غرب از این فضا برای به چالش کشاندن امنیت ایران در دو بعد رسانه‌ای و جنگ سایبری به مقابله با جمهوری اسلامی پرداختند.

بدین‌سان جمهوری اسلامی ایران همانند برخی از کشورهای دیگر، بارها مورد هجوم حملات سایبری قرارگرفته است و به همین دلیل علاوه بر نرخ بالای حملات سایبری، رتبه نخست توان سایبری منطقه می‌باشد (خبرگزاری صداوسیما،۱۳۹۸/۳/۸)

گاهی این حملات سایبری از سوی دشمنان و باهدف 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. در میان حملات مهم سایبری علیه ایران که یکی از بزرگ‌ترین تهدیدات امنیتی آن را می‌توان در سایبری محسوب کرد، جمله سایبری بود که از طریق کرم رایانه‌ای، «استاکس‌نت » اتفاق افتاد. کرم خطرناکی که تلاش کرد اطلاعات سیستم‌های کنترل صنعتی را به سرقت برده و آن‌ها را روی اینترنت قرار دهد با اهداف سیاسی و به‌منظور فشار بر ایران برای توقف طرح غنی‌سازی اورانیوم، نیروگاه‌های اتمی بوشهر و نطنز را مورد هدف قرارداد (ماه‌پیشانیان، ۱۳۹۰: ۱۰۴)

ماجرا به این شکل روی داد که در سال ۲۰۱۰ یک کرم رایانه‌ای قدرتمند جدید، بر صنعت هسته‌ای و دیگر تأسیسات صنعتی ایران تأثیر گذاشت. کار این کرم که «استاکس نت» نامیده شده است، نوعی

خـرابکاری صنعتی یا جنگ سایبری غیرقانونی بود که نه توسط هکرهای غیردولتی، بلکه توسط یک دولت ساخته و رهاسازی شد. استاکس نت ویروسی بسیار تخصصی است و «فقط تجهیزات ساخته‌شده توسط «زیمنس» که لوله‌های نـفتی، تأسیسات الکتریکی، تأسیسات هـسته‌ای و دیگر مکان‌های صنعتی بزرگ را کنترل می‌کنند»، هدف می‌گیرد.

آلودگی به استاکس نت توسط **VirusBlokAda** که یک شرکت امنیت رایانه‌ای بلاروسی است، در ماه جولای ۲۰۱۰ ردگیری شد. همچون سایر اشکال جنگ، حمله با استاکس نت نیز موجب صدماتی جانبی می‌شود و دامنه آلودگی به آن، به شبکه‌های رایانه‌ای خارج از ایران نیز تسری می‌یابد. ویروس استاکس نت بر تأسیسات اتمی ایران در بوشهر که بـه دسـت روس‌ها ساخته‌شده نیز تأثیر گذاشت. (دریفوس، ۱۳۸۷: ۸۹)

این ویروس قادر به تخریب لوله‌های گاز و اختلال در فعالیت‌های تأسیسات هسته‌ای بود. همچنین توانست در سیستم کنترل‌های ساخته‌شده توسط شرکت زیمنس که در تأسیسات صنعتی و همچنین تأمین آب شرب، چاه‌های نفت، نیروگاه‌های برق و دیگر تأسیسات صنعتی نصب‌شده‌اند، نفوذ کند. استاکس با کپی شدن در درایوهای **USB** و **Email** های آلوده و یا فایل‌های به اشتراک گذاشته‌شده در شبکه‌های رایانه‌ای که دارای نقاط آسیب هستند، منتشر می‌شود. ویروس استاکس‌نت زمانی فعالیت‌های هسته‌ای ایران را هدف قرارداد که تهران در مرحله سوخت‌گذاری در قلب رآکتور نیروگاه هسته‌ای بوشهر قرار داشت و محموله سوخت هسته‌ای را از روسیه دریافت کرده بود. با تأیید تهاجم سایبری به تأسیسات هسته‌ای ایران و اعلام تأخیر در راه‌اندازی نیروگاه هسته‌ای بوشهر گمانه‌ها از پیامدهای این جنگ اعلام نشده، بالا گرفت.

حمله سایبری به زیرساخت‌های ایران با استاکس نت اولین و آخرین مورد تهدیدات امنیتی علیه جمهوری اسلامی ایران نبود به‌طوری‌که در طول سال‌های فراگیر شدن اینترنت در ایران بارها ویروس‌های مختلف جاسوس و بدافزارهای مخرب زیرساخت‌های کشورمان را موردحمله قرار داده‌اند. استارس و دوکو نیز دو نمونه دیگر از ویروس‌هایی هستند که اخبار حمله آن‌ها به ایران رسانه‌ای شده است

در راستای این وقایع، آنچه موردنیاز است، امنیت سایبری است که طیف گسترده‌ای از فناوری‌ها را در برمی‌گیرد. آنتی‌ویروس‌ها، سامانه‌های پیشگیری از نفوذ، رمزگذاری اطلاعات و دیوار آتش چند نمونه از این فناوری‌ها هستند. هدف این فناوری‌ها مقابله با تهدیدات پیشرفته و دائمی موجود در دنیای سایبری است. چنین فناوری‌هایی می‌توانند از انتشار ویروس در کل سیستم جلوگیری کرده و بقای یک کسب‌وکار را پس از حملات سایبری تضمین کنند. کسب‌وکارهای امروزی برای حذف محدودیت‌های جغرافیایی و

رشد توان تولید، به‌شدت به اینترنت وابسته هستند. درنتیجه امنیت سایبر، امینت چارچوب داخلی یک سازمان را در مقابل تهدیدات خارجی تأمین می‌کند. (صنعت بیمه، ۱۳۹۴: ۱) و با کشف استاکس نت در ایران، به نظر می‌رسد ایران نیاز مبرمی به این تدابیر دارد.

اساساً تهاجمات تروریستی و تخریبی در هر سطح و قالبی زمینه‌ساز ظهور توانمندی‌های کشور هدف در دفاع و مقابله با منشأ تهدید است. همان‌طور که در دکترین امنیت ملی جمهوری اسلامی بیان‌شده، ایران به هرگونه تهدید و تهاجم واکنش نشان داده و شدت این واکنش نیز متناسب با سطح تهاجم دشمن خواهد بود. لذا برخی از کارشناسان آمریکایی اصولاً مخالف شدید حملات سایبری علیه تأسیسات نظامی و هسته‌ای ایران هستند، زیرا که به اعتقاد آن‌ها چنین اقداماتی درنهایت منجر به واکنش متقابل جمهوری اسلامی خواهد شد و با توجه به ضعف‌های موجود در حوزه دفاعی این عرصه از مخاصمات و گستردگی شبکه‌های اینترنتی آمریکا، می‌تواند نتایج فاجعه‌باری رقم بزند. در گزارش همین دست از کارشناسان حوزه امنیت و سایبر به کمیته امنیت ملی مجلس نمایندگان به‌صراحت از سرمایه‌گذاری و تدارک ایران بعد از حمله ویروسی به تأسیسات هسته‌ای خود در سال ۱۳۸۹ سخن رفته و بابت عواقب سنگین این اقدامات هشدار داده‌شده است. (دیدبان، ۱۳۹۴: ۱)

یکی از اهداف سایبری رسانه‌های غربی در خصوص کرم رایانه‌ای، «استاکس‌نت »، تبلیغات و بزرگنمایی آن، بیش از قدرت اعمال تخریبی آن بود چنان‌که برخی، با بزرگ‌نمایی، سعی کرده‌اند حدود ۶۰ درصد از رایانه‌های آلوده در جهان را متعلق به ایران بدانند و برخی دیگر قصد دارند نشان دهند که ایران دیر متوجه نفوذ ویروس جاسوسی به سیستم‌های خود شده و اکنون توان مقابله با این معضل را ندارد. (اشرافی، ۱۳۹۰: ۶۵)

پ) الزامات راهبردی ایران برای مقابله با تهدیدات امنیتی سایبری

تقویت شیوه‌های بازدارندگی متقابل

یکی از بهترین شیوه‌های بازدارندگی، اقدام متقابل است که با اصطلاح «مقابله‌به‌مثل» از آن یاد می‌شود؛ همان‌طور که آمریکا در پروتکل‌های امنیت سایبر خود به‌طور صریح ابراز داشته که: «آمریکا در مقابل اعمال خصمانه در فضای مجازی به‌عنوان تهدیدی برعلیه منافع کشور پاسخ خواهد داد. همه کشورها دارای حق ذاتی برای دفاع از خود هستند و به اعمال خصمانه‌ای که از طریق فضای مجازی صورت می‌گیرد با توجه به تعهدات ما در قبال هم‌پیمانان نظامی خود با اقدامات نظامی به آن‌ها پاسخ خواهیم داد»، ایران نیز این حق را برای خود باید محفوظ بدارد تا بتواند حمله سایبری قدرتمندی را

جهت آسیب جدی به زیرساخت‌های آمریکا انجام دهد که این امر نیازمند نوآوری در طراحی یک سلاح سایبری قدرتمند است تا دشمنان ایران را از فکر حمله سایبری بیرون بیاورد. (۸۰۲۲۹/tanvir.ir/fa/news)

ت) تهدید سایبری در ایران

متأثر از تهدیدات فضای سایبری می‌توان بیان داشت که حاکمیت جمهوری اسلامی نیز، به لحاظ ژئوپولیتیکی با چالش‌های ویژه قرن حاضر مواجه است؛ چراکه امروزه انگیزه‌های زیادی از قبیل ژئوپولیتیکی، جغرافیایی، اقتصادی، مذهبی، سیاسی و ... برای مبارزه با نظام جمهوری اسلامی ایران از سوی کشورهای منطقه‌ای و فرامنطقه‌ای و گروه‌های مخالف نظام جمهوری اسلامی ایران وجود دارد که دشمنان را ترغیب به جاسوسی سایبری، خرابکاری سایبری، حمله‌های سایبری یا هدف ضربه به زیرساخت‌های جمهوری اسلامی و تلاش برای براندازی و تغییر حاکمیت آن می‌نماید. ساده‌ترین روش مبارزه با جمهوری اسلامی ایران، سعی در عدم توسعه‌یافتگی و اختلال در زیرساخت‌های حیاتی آن است که اجباراً باید در فضای سایبری قرار گیرند (موحدی صفت، ۱۳۸۶؛ موسی زاده و همکاران، ۱۴۰۰)

نتیجه‌گیری و پیشنهادها

فضای سایبر فضایی واقعی در عرصه‌ای جدید برای تأثیرگذاری و تأثیرپذیری و درنتیجه دوستی، همکاری، رقابت، دشمنی و حتی جنگ بین کشورها و سایر بازیگران است. این موارد به‌خوبی نشان می‌دهد که اینترنت و فضای سایبر عرصه‌ای جدید برای سیاست مهیا نموده‌اند؛ فضایی که در آن افراد، گروه‌های مختلف و دولت‌ها در حال بازیگری و سیاست‌ورزی هستند. در عرصه روابط بین‌الملل، تحت تأثیر سنت واقع‌گرایی، مسائل بین‌المللی به مسائل بسیار مهم و حیاتی همچون امنیت و مسائل کمتر مهم مثل موضوعات اقتصادی تقسیم می‌شود. برخی از کارشناسان بر این باورند که به دلیل اهمیت فضای سایبر، باید امنیت سایبری را جزء مسائل بسیار مهم، حیاتی و امنیتی یا سیاست عالی قرار دارد. بااین‌وجود پیشنهاد می‌شود در کنار طراحی یک سلاح سایبری قدرتمند سایبری، ایجاد واحدهای عملیاتی سایبری در نیروهای مسلح کشور و دستگاه‌های "اطلاعاتی-امنیتی- انتظامی"، تحت تدوین «استراتژی امنیت ملی سایبری» ضرورت دومی است که این نیاز با توجه به وابستگی روزافزون زیرساخت کشور به فضای سایبر، بسیار استراتژیک محسوب می‌شود. در این رابطه، تدوین «استراتژی امنیت ملی سایبری» دربرگیرنده ۴ حوزه امنیت ملی: سیاسی-امنیتی، فرهنگی-اجتماعی، اقتصادی و نظامی که نحوه تصمیم‌گیری، هدایت و کنترل امور را از سطح تکنیک تا استراتژیک در حوزه‌های سلبی- ایجابی، آفندی- پدافندی و خارجی-داخلی کشور را پوشش دهد، بسیار ضروری به نظر می‌رسد.

راهکارهای مقابله با تهدیدات سایبری

شاید اصلی‌ترین راهکار برای داشتن اینترنتی ایمن، اجرای یک طرح جامع امنیت ملی در حوزه سایبری باشد. طرحی که شبکه ملی اطلاعات هم می‌تواند از اجزای آن باشد. در این طرح می‌بایست به حوزه‌های آموزش عمومی، تقویت سیستم‌های دفاعی و توان مقابله و اجرای عملیات در هر سطح علیه مهاجم موردتوجه قرار گیرد. همچنین نیاز است ملاحظات مربوط به پدافند غیرعامل در همه طرح‌های مربوط به شبکه‌های ارتباطی و الزام دستگاه‌های اجرایی به استفاده از توان داخلی (تا حد امکان) مدنظر باشد.

از سوی دیگر به نظر می‌رسد تقویت رویه‌های دیپلماتیک در قالب افزایش مشارکت و فعالیت برای یافتن راه‌های پیگیری حقوقی بین‌المللی حملات سایبری به ایران ضرورتی اجتناب‌ناپذیر است

همچنین تلاش برای سهیم شدن در مدیریت اینترنت جهانی از طریق حضور در مجامع مؤثر و مرتبط، اقداماتی است که نیازمند تحرک و پویایی بیشتر وزارت امور خارجه در این راستا می‌باشد.

با توجه به وجود نگاه نوآور در مسئولان ارشد نظامی- امنیتی، انتظار می‌رود که هرچه زودتر فرماندهی سایبری در ایران تأسیس شود تا این نهاد جدید بتواند در تحقق ساخت سلاح‌های سایبری، تدوین استراتژی امنیت ملی سایبری و تقویت زیرساخت‌های کشور در قبال حملات سایبری در راستای امنیت بیشتر کشور عمل کند.

منابع

۱) احمدی، بهزاد و سیما رفسنجانی نژاد (۱۴۰۰)، بایسته‌های راهبرد ایران در حکمرانی دیجیتال و حکمرانی سایبری، مرکز بررسی‌های استراتژیک ریاست جمهوری

۲) اشرافی، مرتضی و اشرافی، مجتبی (۱۳۹۰)، «تحلیلی بر جاسوسی و جنگ سایبری»، مجله درس‌هایی از مکتب اسلام، شماره ۵۹۹، فروردین.

۳) بوزان، باری (۱۳۷۸)، مردم، دولت‌ها و هراس، ترجمه پژوهشکده مطالعات راهبردی. تهران: پژوهشکده مطالعات راهبردی.

۴) ترابی، قاسم (۱۳۹۷)، چالش‌ها و آسیب‌پذیری‌های جمهوری اسلامی ایران در فضای سایبر، مطالعات راهبردی سال بیست‌ویکم بهار شماره ۱ (پیاپی ۷۹)

۵) خلیلی پور رکن‌آبادی، علی و نورعلی وند، یاسر (۱۳۹۱)، «تهدیدات سایبری و تأثیر آن بر امنیت ملی»، فصلنامه مطالعات راهبردی، شماره دوم، سال پانزدهم، تابستان.

۶) دریفوس، رابرت (۱۳۸۹)، «آیا ما به‌طور محرمانه درگیر یک جنگ سایبری با ایران هستیم؟»، مجله سیاحت غرب، شماره ۸۷، آبان.

۷) ربیعی، علی، (۱۳۸۳). مطالعات امنیت ملّی، دفتر مطالعات سیاسی و بین‌المللی وزارت امور خارجه، تهران، مرکز چاپ و انتشارات وزارت امور خارجه.

۸) طالب پور، عطیه، تاریخچه حملات سایبری در ایران و جهان، خبرگزاری باشگاه خبرنگاران جوان ۲۱ بهمن ۱۳۹۸

۹) سلامی، محمدمهدی،۱۳۹۲، فرصت‌ها و تهدیدهای فضای مجازی تهران: نشر توزیع پیام دیدار.

۱۰) صیاد، محمدکاظم و دیگران (۱۳۹۹) تهدیدهای سایبری و امنیت در فضای مجازی؛ بررسی ایالات‌متحده آمریکا و جمهوری اسلامی ایران، فصلنامه علمی امنیت ملی، دوره ۱۰، شماره ۳۸، زمستان

۱۱) عاملی، سعید رضا، ۱۳۸۷، مطالعات شهر مجازی تهران: رویکرد تحلیلی به فضاهای عمومی تهران: انتشارات قلم.

۱۲) عبدالله خانی، علی، (۱۳۸۲)؛ "نظریه‌های امنیت: مقدمه‌ای بر طرح‌ریزی دکترین امنیت ملی (۱)"، جلد اول، تهران: موسسه فرهنگی مطالعات و تحقیقات ابرار معاصر تهران.

۱۳) عبدی، سوران؛ الوندی زاده، اسدالله و مالکی، نسرین (۱۳۹۱)، بررسی تأثیر اینترنت بر رشد اقتصادی در منتخب عضو (OIC)، اولین همایش بین‌المللی اقتصادسنجی، روش‌ها و کاربردها، سنندج، دانشگاه آزاد اسلامی واحد سنندج

۱۴) کاستلز، مانوئل (۱۳۸۵)، عصر اطلاعات: اقتصاد، جامعه و فرهنگ (ظهور جامعه شبکه‌ای)، ترجمه احد علیقلیان و افشین خاکباز، تهران: انتشارات طرح نو.

۱۵) کلارک، یان (۱۳۸۶)، جهانی‌شدن و نظریه روابط بین‌الملل، ترجمه فرامرز تقی لو، تهران: دفتر مطالعات سیاسی و بین‌الملل.

۱۶) لسان طوسی، فهیمه، مانیان، امیر، تقوی، مصطفی، ذوالفقارزاده، محمدمهدی، (۱۳۹۹)، فضای سایبر و آینده هویت ملی: هشدارهای راهبردی برای امنیت ملی با رویکرد تحلیل لایه‌ای علّی، دو فصلنامه آینده‌پژوهی ایران، مقاله پژوهشی، سال پنجم، شماره اول، بهار و تابستان ۱۳۹۹ صفحه ۳۰۵-۳۲۹

۱۷) ماه‌پیشانیان، مهسا (۱۳۹۰)، «فضای سایبر و شیوه‌های نوین درگیری ایالات‌متحده با جمهوری اسلامی ایران»، مجله نامه پژوهش فرهنگی، شماره ۴۵، بهار.

۱۸) موحدی صفت، محمدرضا (۱۳۸۶)، «امنیت ملی در فضای سایبر؛ فرصت‌ها و تهدیدها با تأکید بر استقرار دولت الکترونیکی»، مجله مطالعات دفاعی استراتژیک، شماره ۳۰، تابستان و پاییز.

۱۹) میرمحمدی، مهدی و محمدی لرد، عبدلامحمود (۱۳۸۷)، سیاست و اطلاعات: مطالعه موردی ایالات‌متحده امریکا، تهران: مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران.

۲۰) نورمحمدی، مرتضی (۱۳۹۰)، «جنگ نرم فضای سایبر و امنیت جمهوری اسلامی ایران»، مجله راهبرد فرهنگ، شماره ۱۶، زمستان.

۲۱) واحدی فرد، سعید (۱۳۹۱)، «جنگ سایبری، بررسی ابعاد نوین فضای مجازی»، ره‌آورد نو، سال یازدهم، شماره ۳۹، تابستان.

۲۲) یزدان فام، محمود (۱۳۸۶)، "دگرگونی در نظریه‌ها و مفهوم امنیت بین‌المللی"، فصلنامه مطالعات راهبردی، شماره ۳۸، صص ۷۲۵-۷۵۰

۲۳) صدیق بنای، هلن (۱۳۸۵)، مفاهیم: فضای سایبر چیست؟ مرکز مطالعات و تحقیقات رسانه‌ای روزنامه همشهری، نشانی بازیابی اینترنتی: https://www.hamshahrionline.ir/news/4411

۲۴) دیدبان (۱۳۹۴)، «سایبر تروریسم و ابعاد تهدید امنیت ملی»، ۱۰ تیر، به آدرس اینترنتی: http://www.didehbancenter.com/

۲۵) صنعت بیمه (۱۳۹۴)، «امنیت سایبری، دغدغه اصلی موسسه‌های تجاری در خاورمیانه»، ۵ خرداد، به آدرس اینترنتی: http://www.sanatebime.ir/fa/news/44820/

۲۶) سلاح سایبری؛ پاسخ ایران به حملات سایبری آمریکا: http://www.tanvir.ir/fa/news/80229/

۲۷) وبسایت خبرگزاری میزان، https://www.mizanonline.com

28) Alghamdi, M.I. 2021. Determining the impact of cyber security awareness on employee behaviour: A case of Saudi Arabia. Mater. Today: Proc.

29) Charney, Scott (2009); "Rethinking the Cyber Threat A Framework and Path Forward", Microsoft Corp. • One Microsoft Way • Redmond, WA 98052-6399 • USA.

30) Jay Hoofnagle, Chris, (2022), Cybersecurity in Context, PUBLISHER TBD, BOOK-WEBSITE.COM

31) Judge, M.A. et al. 2021. Price-based demand response for household load management with interval uncertainty. Energy Rep.

32) Hart, S. et al. 2020. Riskio: A serious game for cyber security awareness and education. Comput. Secur. 95, 101827.

33) Haney, William S. (2006). Cyberculture, Cyborgs and Science Fiction: Consciousness and the Posthuman. The Netherlands: Rodopi B.V. Hine, Christine (2000) Virtual Ethnography. SAGE Publications

34) Liu, X. et al. 2021. Quantitative cyber–physical security analysis methodology for industrial control systems based on incomplete information Bayesian game. Comput. Secur. 102, 102138.

35) Folsom, Thomas C. (2007) Defining Cyberspace (Finding Real Virtue in the Place of Virtual Reality) (2006). Tulane Journal of Technology & Intellectual Property, Vol. 9, p. 75

36) Krause, Keith and Williams, Michael c. (1996); "Broadening the Agenda of Security Studies: Politics and Methods", *Mershon International Studies Review.*

37) Mueller, R. S. (2007, January 11), "Testimony Before the Senate Select Committee on Intelligence", Retrieved from The Investigative Project on Terrorism.

38) Rollins, J. & Henning, A. C. (2009, March 10). "Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations". Retrieved from Congressional Research Service.

39) Starr, Stuart H. (2009); "Towards an Evolving Theory of Cyber power", National Defense University, Center for Technology and National Security Policy

40) . Thomson, J.R. 2015. Cyber security, cyber-attack and cyber-espionage. In: Thomson, J.R. (Ed.), High Integrity Systems and Safety Management in Hazardous Industries. Butterworth-Heinemann, Boston, pp. 45–53 (Chapter 3).

41) Torabi,Ghasem, (2019), Cyber revolution and chang in the nature of power and national security,Journal of National Security Studies,76(1),45

42) Yuchong، Li، Qinghui،Liu، 2021 A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments، journal homepage: www.elsevier.com/locate/egyr، Energy Reports،

یادداشت‌ها :

1 -Cyberspace
2 - William Gibson
3 - Neuromancer
4 - buzan
5 https://www.mizanonline.com