فصلنامهٔ پدافند غیرعامل و امنیت (پژوهشی)
سال نهم: شمارهٔ ۳۵- تابستان ۱۴۰۰
صص: ۳۱ - ۵۳

Quarterly of Passive Defense & Security
Vol.9, No.35,Summer 2021
P-P: 31 - 53

تاریخ دریافت: ۱۴۰۰/۳/۱۱
تاریخ پذیرش: ۱۴۰۰/۷/۶

تهدیدات امنیتی نوین فراروی جمهوری اسلامی ایران در حوزه سایبری

داود رضایی[۱]
محمود واحدی[۲]

چکیده:

تغییر نگرش دولت ها به استفاده از فضای سایبر و استفاده از خدمات دولت الکترونیک به عنوان یک اصل برای کشورهای توسعه یافته و همچنین یک راهبرد برای کشورهای کمتر توسعه یافته می باشد. مسأله حائزاهمیت در این زمینه، امنیت این بستر ارتباطی است. این پژوهش در صدد است تا تهدیدات نوین امنیتی سایبری فراروی جمهوری اسلامی ایران را بررسی و راهکارهایی برای کاهش آنها ارائه دهد. لذا از نظر هدف، کاربردی می باشد و با روش توصیفی تحلیلی انجام شده است. جامعه آماری بکارگرفته شده طیفی از متخصصین و خبرگان موضوعات سایبری و امنیت سایبری است که ضمن انجام مصاحبه با آنان، نسبت به کشف تهدیدات نوین سایبری فرآروی جمهوری اسلامی که مستعد ظهور و بروز در آینده می باشند اقدام گردیده است که مجموعاً ۱۱ تهدید احصا و مورد شناسایی قرار گرفته است و این تهدیدات جهت اعتبار سنجی و رتبه بندی از طریق پرسشنامه به طیفی از جامعه هدف ارائه و نتجیه آن از طریق نرم افزار SPSS مورد تجزیه و تحلیل قرار گرفته است. در پایان نیز ۱۶ راهکار به منظور مدیریت پیشگیری از وقوع این تهدیدات و یا کاهش آسیب های آنان ارائه شده است.

واژگان کلیدی:

تهدیدات – تهاجم سایبری – تهدیدات نوین – حملات سایبری – فضای سایبری

۱. استادیار امنیت ملی دانشکده علوم و فنون فارابی
۲. دکتری امنیت ملی دانشگاه عالی دفاع ملی، نویسنده مسئول
rezaiedavood@gmail.com

جستارگشایی

مسیر توسعهٔ کشورها ناگزیر از کاربست فناوریهای نوین از جمله بکارگیری زیرساختها و تجهیزات سخت افزاری و نرم افزاری سایبری است و دولتها با اهداف مختلفی از جمله تامین حداکثر رفاه برای ملتهای خود، مدیریت و نظارت بر تحولات سیاسی و اجتماعی، صیانت فرهنگی از ارزشها و هنجارهای اصیل ملت، حفظ رشد اقتصادی و برتری صنعتی در قیاس با رقبای خود و کاهش هزینه‌های سنتی ارتباطات و آموزش و ... در تلاشند تا ضمن بکارگیری فناوریهای به روز سایبری و ایجاد زیرساختهای پایدار تحت نظارت و اشرافیت خود، از گزند آسیبها و تهدیدات فضای سایبری نیز مصون بماند. اما برخی ویژگیهای این فضا نظیر خصلت گمنامی کاربران، فرامرز بودن ابعاد آن، خزنده بودن تهدیدات در بستر آن و سلطه دولتها و شرکتهای صاحب فناوری بر مدیریت کلان فضای سایبر موجب گردیده که حاکمیت و امنیت دولتها و ملتها در معرض تهدیدات این فضا قرار گیرد و حملات سایبری به تاسیسات هسته ای نطنز، سامانه راه آهن، شبکه هوشمند کارت سوخت و حتی صدا و سیما نشان داد که غفلت از تهدیدات فضای سایبر چالشی مهم فراروی ابعاد مختلف امنیت دولتها و ملتها ایجاد خواهد نمود و پویا و توسعه محور بودن این فضا بیانگر بروز و ظهور تهدیدات نوینی در آینده در بستر آن علیه امنیت ملی و مساله‌ای مستلزم بررسی در حوزه مطالعات امنیتی خواهد بود که در این پژوهش ضمن برشماری مصادیق تهدیدات سایبری گذشته، در صدد کشف و بررسی تهدیدات نوین سایبری فراروی نظام جمهوری اسلامی ایران بعنوان یک مساله حائز توجه خاص می باشد.

نتایج این تحقیق به شناسایی تهدیدات امنیتی نوین سایبری علیه ج.ا.ایران و ایجاد آمادگی و برنامه ریزی برای پیشگیری از تبعات این تهدیدات و تقابل با آنها کمک خواهد نمود.

غفلت از تهدیدات امنیتی سایبری منجر به غافلگیری در مواجه با این تهدیدات ناشناخته و ایجاد چالش امنیتی برای ج.ا.ایران در حوزه سایبری در آینده خواهد گردید.

تهدیدات امنیتی نوین فراروی جمهوری اسلامی ایران در حوزه سایبری شامل چه تهدیداتی می شوند؟

مهمترین پژوهش های مرتبط با ادبیات پژوهش به شرح زیر اشاره می گردد.

۱- مقاله پژوهشی «ارائه مدل مفهومی منطقی طبقه بندی تهدیدات سایبری زیرساختهای حیاتی» (آقایی محسن و دیگران، فصلنامه‌امنیت‌ملی، سال‌نهم، شماره‌دوم، تابستان ۱۳۹۸)

در این مقاله با اشاره به اثرگذاری تهدیدات سایبری در سطح ملی علیه برخی زیرساختهای حیاتی و تحمیل هزینه های غیرقابل جبران به جوامع، در صدد است از طریق شناسایی تهدیدات سایبری و گونه شناسی این تهدیدات در سطح زیرساختهای حیاتی، به ارائه مدل مفهومی برای طبقه بندی تهدیدات سایبری دست یابد که در نهایت این مدل را با ابعاد شش گانه «تهدیدات، عوامل تهدید، مشخصات تهدید، نگاه از دید

نفوذگر، توصیف سیستم و منابع شناسایی تهدیدات» معرفی می نماید.

۲ – مقاله پژوهشی «ارتقاء امنیت سایبری در نبرد پست مدرنیسم» (هوشی محمدرضا، اولین همایش علمی پژوهشی یافته های نوین علوم مدیریت کارآفرینی و آموزش ایران ۱۳۹۴)

در این مقاله به استفاده بازیگران دولتی و غیر دولتی از قدرت سایبری جهت دست یابی به اهداف اجتماعی، ایدیولوژیک، سیاسی، نظامی و مالی اشاره شده و ذکر شده که این اهداف از طریق انین شیوه ها حاصل می گردد: «جنگ سایبری، حمله های سایبری، جایم سایبری» سپس با مقایسه میان حمله سایبری، جرم سایبری و جنگ سایبری، به تاثیر تهدیدات سایبری بر امنیت ملی و تشریح وضعیت امنیت در عصر جدید و رویارویی با تهدیدات سایبری پرداخته و اینگونه نتیجه گیری کرده که مقابله با تهدیدات سایبری نیازمند همکاری موثر دولتها و بخش خصوصی می باشد.

۳– مقاله پژوهشی «طرح راهبردی دفاع سایبری جمهوری اسلامی ایران در حوزه بازدارندگی» (احدی محمد و دیگران، فصلنامه علمی پژوهشی مطالعات بین رشته‌ای دانش راهبردی، سال هشتم، شماره ۳۱، تابستان ۱۳۹۷ صص ۲۲۵-۲۵۲)

در این مقاله ذکر شده است که گسترش فضای سایبری منجر به آسیب پذیری زیرساختهای کشور شده که بازدارندگی نسبت به سایر طرحهای دفاعی واجد اولویت برتر است. در همین راستا در یک فرآیند پژوهشی اهمیت اصول و ارزشهای حاکم در حوزه بازدارندگی را از طریق توزیع و تحلیل پرسشنامه ارزشگذاری نموده و نهایتاً نتیجه گیری نموده است که مهمترین و موثرترین راهبرد بازدارندگی سایبری شامل «تولید ظرفیت و قدرت پاسخ گویی به تهدیدات سایبری و نمایش قدرت و اقتدار سایبری از طریق رزمایش و تولید پیام اقتدار طی فرآیند متمرکز و انتقال پیام» می باشد.

٤ – مقاله پژوهشی «مطالعه تطبیقی ساختار دفاع سایبری کشورها» (حسینی پرویز، فصلنامه پژوهشهای حفاظتی – امنیتی دانشگاه جامع امام حسین علیه السلام، سال دوم، شماره ۵، بهار ۱۳۹۲ صص ٤١–٦٨)

این مقاله ضمن برشماری ویژگیهای فضای سایبر و تبیین مفهوم دفاع و حمله در حوزه سایبری، ساختار دفاع سایبری برخی کشورها نظیر آلمان، آمریکا، انگلیس و فرانسه را مورد مطالعه قرار داده و نهایتاً نتیجه گیری نموده که برای مقابله با تهدیدات سایبری، ایجاد سازمان دفاع سایبری جمهوری اسلامی ایران ذیل شورای عالی فضای مجازی ضروری است.

در بررسی تحقیقات بعمل آمده، ادبیات و مفاهیم مربوط به تهدیدات تا حدودی مشترک است که در این تحقیق هم می‌تواند مورد استفاده قرار گیرد. در تحقیقات قبلی بیشتر به تهدیدات شناخته شده و عمدتاً در حوزه حملات سایبری اشاره شده که کشورها. از جمله ایران تجربه مواجهه با آن را داشته اند ولی به تهدیدات امنیتی نوین و تهدیداتی که فرآروی جمهوری اسلامی ایران می باشد اشاره ای نشده است. نوآوری این تحقیق

نسبت به تحقیقات مذکور و گذشته در این است که این پژوهش به تهدیدات نوینی پرداخته که مستعهد ظهور و بروز در آینده نزدیک می باشند.

مفاهیم و مبانی نظری

امنیت ملی: اصطلاح امنیت ملی یعنی مصون بودن مولفه‌های تشکیل‌دهنده یک کشور در برابر آسیب‌های شدید داخلی و تهدیدات فوری خارجی. علاوه بر این تعبیر سلبی (در خطر نبودن مولفه‌های تشکیل‌دهنده کشور)، عده‌ای از محققان نگاهی ایجابی به مفهوم امنیت ملی دارند و آن را به توانمندی یک بازیگر سیاسی (کشور) در تعقیب آسان و کم هزینه اهداف ملی و صیانت از مولفه‌های کشور می‌شمارند هم در تعبیر سلبی و هم در نگاه ایجابی (افتخاری، ۱۳۸۱) رابرت ماندل در تعریف امنیت ملی میگوید:»امنیت ملی شامل تعقیب روانی و مادی ایمنی است و اصولا جزو مسئولیت حکومتهای ملی است، تا از تهدیدات مستقیم ناشی از خارج، نسبت به بقای رژیمها، نظام شهروندی و شیوه زندگی شهروندان خود ممانعت به عمل آورند». در این تعریف تهدیدات همیشه در دستور کار امنیت است و دامنه آن بسیار فراتر از نیروی نظامی بوده و شامل تهدیدات منابع/محیطی، اقتصاد و سیاسی/فرهنگی میشود، البته در صورتی که آنها بقای کل حکومت، مردم یا شیوه زندگی ملت را مستقیما» تهدید کنند. (ماندل، ۱۳۷۷،۱۸)

تهدید: تهدید، یک حالت، وضعیت خاص، رفتار و پدیده‌ای است که برداشت‌های گوناگونی از آن وجود دارد و حد و مرز آن، اعتباری و به عبارتی، زمان‌مند و مکان‌مند است. ممکن است پدیده و یا مسئله ای برای جامعه ای، پدیده ای عادی و یا مسئله‌ای اجتماعی باشد، در حالی که همان پدیده و وضعیت برای جامعه دیگر، مسئله ای غیرعادی، خطر یا بحران امنیتی به شمار آید. بنابراین، ماهیت، نوع، شدت، سطح تهدیدها، تابع عقاید و نگرش بازیگران، محیط اجتماعی و ملی و محل وقوع تهدید باشد. (تریف تری و دیگران، ۱۳۸۳:۴۸).

تهدیدات امنیتی

تهدیداتی که اهداف و ارزش‌های حیاتی یک کشور را به‌گونه‌ای در معرض خطر قرار دهند که بیم آن رود در آن اهداف و ارزش‌های حیاتی که هر نظام و هر ملتی دارد، تغییرات اساسی صورت گیرد. تهدید زمانی به یک موضوع امنیتی تبدیل می‌شود که با سه موضوع مردم–کشور و حکومت ارتباط داشته باشد. (مرادیان، ۱۳۸۸: ۳۲) به آن دسته از وضعیت‌هایی اطلاق می گردد که موجودیت یک نظام را نشانه رفته باشد. در واقع تفاوت آن با تهدیداتی عمومی در این نکته نهفته است که تهدیدات امنیتی با موجودیت و بقای یک نظام سیاسی مرتبط است و در حالی که تهدیدات عمومی از چنین ویژگی برخوردار نیست. (زرگر، ۱۳۸۵: ۵۴) در تعریف عملیاتی تهدیدات امنیتی نوین می توان گفت که تهدیداتی امنیتی نوین، تهدیداتی امنیتی هستند که با توجه به پیشرفت فناوری و تغییر پرشتاب محیط، در آینده در محیط امنیتی

جمهوری اسلامی ایران تاثیرگذار هستند و شامل تهدیداتی نوپدید و یا تهدیداتی می‌شوند که از گذشته وجود داشته و در آینده ماهیت آنها تغییر یافته و شکل جدیدی به خود می گیرد.

مفهوم فضای سایبری[1]:

فضای سایبر را می توان شبکه ای متصل به هم از زیر ساخت های فناوری اطلاعات دانست که اینترنت، شبکه های مخابراتی، سیستم های کامپیوتری و پردازشگرها و کنترلگرهای داخلی صنایع مهم را شامل می شود و نگرشی فناورانه بر پایه مولفه هایی چون سخت افزار، نرم افزار، کیفیت و کمیت انتقال داده ها و نهایتاً شکل گیری شبکه‌ای مشخص تحت مدیریت انسان است که بستری را خلق می کند تا فرایند انتقال داده را در حداقل زمان و در گسترهٔ تصور مارواییی انسان ممکن سازد. در سند پدافند سایبری کشور، فضای سایبر اینگونه تعریف شده است: شبکه های وابسته به یکدیگر، از زیرساختهای فناوری اطلاعات، شبکه های ارتباطی، سامانه های رایانه ای، پردازنده های تعبیه شده (جاگذاری شده)، کنترلگرهای صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط وانسان به منظورتولید، پردازش، ذخیره سازی، مبادله، بازیابی و بهره برداری از اطلاعات می باشد (سند راهبردی پدافند سایبری کشور) همچنین در سند راهبرد امنیت سایبری آلمان، دراین خصوص گفته شده «فضای سایبر یک فضای مجازی از همه سیستم های *IT* مرتبط با هم در سطح دیتا و مقیاس جهانی است. پایه فضای مجازی اینترنت است که اتصال جهانی عمومی و قابل قبولی از شبکه انتقال در حال توسعه را فراهم آورده است. (*Cyber security strategy for Germany,2011*)

امنیت سایبری: امنیت سایبری شامل چند بُعد یا الزام می گردد: امنیت برنامه؛ امنیت اطلاعات؛ امنیت شبکه و زیرساخت؛ لذا به دلیل آنکه از فناوری سایبری می توان همانند ابزارهای جنگ متعارف، برای حمله به تشکیلات دولتی، نهادهای مالی، زیرساخت های انرژی و حمل و نقل ملی و روحیه عمومی استفاده کرد، بنابراین ناامنی در فضای سایبری، صرفاً شامل ناامنی در سیستم های اطلاعاتی نیست، بلکه شامل تمام زیرساخت هایی می شود که به نحوی با فناوری اطلاعات درارتباطند. بعنوان مثال در حمله سایبری تحت عنوان ویروس استاکس نت در سال ۲۰۱۰ به تاسیسات اتمی ایران؛ یک بدافزار توانست در سیستم کنترل سانترفیوژها نفوذ و از طریق تغییر در سرعت چرخش آنها، موجب تخریب بخشی از زنجیره سانتریفیوژ گردد. (خلیلی پور رکن آبادی،۱۳۹۱)

تاثیر فضای سایبر بر امنیت ملی: گسترش حملات سایبری فرامرزی، امنیت سایبری رابه یکی از نگرانی های عمدهٔ جهانی درقرن بیست ویکم تبدیل کرده است. با توجه به روندها و رویدادهای گذشته و تجربه سایر کشورها، پیچیدگی و مشکل‌بودن شناخت فضای سایبر، کاربربودن در تمامی عرصه‌ها، ضعف در اعتماد عمومی نسبت به دولت در حوزه سایبری، نداشتن راهبرد جامع و کارآمد سایبری و جزیره‌ای عمل کردن و

1. *Syber space*

همگام‌نبودن با فضای انقلاب سایبری از جمله مهم‌ترین آسیب‌پذیری‌ها و چالش‌های کشور در حوزه سایبر هستند. اما تهدیدات فضای سایبر محدود به موارد مذکور نیست بلکه در شرایط حاضر و شرایط حاکم بر جایگاه جمهوری اسلامی ایران در منطقه و چالشها و تهدیدات امنیتی مترتب بر آن، تهدیدات سایبری از گستردگی و تنوع نوین برخوردار است که شاید برخی از آنها تاکنون مشمول هیچ دولت و کشوری نبوده است و امروزه برخی از تهدیدات سایبری علیه جمهوری اسلامی ایران در قالب جنگهای سایبری تجلی یافته است و دول و رژیمهای متخاصم بعضاً اقدام به حمله یا جنگی سایبری علیه زیرساختهای صنعتی ایران نموده‌اند. درخصوص جایگاه این فضا در نزد دولتها می توان گفت فضای سایبر به دلیل قابلیتها، امکانات، رفاه و توسعه‌ای که برای بشر ایجاد نموده، یک سرمایه تلقی می گردد که این سرمایه می تواند ترکیبی از سخت افزاز، نرم افزار و پدیدآورندگان و مدیران آن باشد و لذا صیانت از این سرمایه در مقابل تهدیدات مربوط به خود، امروزه یک ضرورت خاص قلمداد می گردد. (شفیع پور و پورقهرمانی،۱۳۹۳)

تهدیداتی امنیتی نوین سایبری: تهدیداتی هستند که با توجه به پیشرفت فناوری و تغییر پرشتاب محیط، در آینده در محیط امنیتی جمهوری اسلامی ایران تاثیرگذار هستند و شامل تهدیداتی نوپدید و یا تهدیداتی سایبری می‌شوند که از گذشته وجود داشته و در آینده ماهیت آنها تغییر یافته و شکل جدیدی به خود می گیرد. (مطالعه گروهی: تهدیدات نوین امنیتی فراروی ج.ا.ایران، ۱۳۹۹)

نظریه‌های مطرح در حوزه تهدیدات سایبری

(۱) پروفسور اریک گارتز[1] (استاد دانشگاه سن دیگو آمریکا و پژوهشگر جنگ) در مقاله‌ای در مجله امنیت بین الملل[2] معتقد است به دلیل اینکه فضای سایبر سه ویژگی ضروری موردنظر کلازویتس، فیلسوف جنگ پروسی، را نداشته و فاقد این عناصر است (خشونت بار/ ابزاری/سیاسی)، نمی‌توان به آن به عنوان موضوعی جنگی نگریست. لذا «سایبر یک ضمیمه به جنگ های جدید است، نه یک جایگزین و تا زمانی که جنگ به صحنه زمین نیاید، معلوم می شود که مسئله زیاد مهم نیست و در جای دیگری می گوید: «در صورت عدم برخورداری از قدرت در سایر حوزه ها، سایبر امکان پیروزی و ایجاد بی ثباتی را ندارد» و در نهایت، معتقد است که «نظر به موارد فوق، نبرد سایبری شایستگی بررسی ذیل موضوعات استراتژیک امنیت بین الملل را ندارد». در طرف دیگر این مباحثه نیز گروه دیگری از اندیشمندان قرار دارند. (*Gartzke*, 2013)

(۲) لوکاس کلو[3] (مدیر مرکز فناوری و امور جهانی در بخش سیاست و روابط بین‌الملل دانشگاه آکسفورد) در مقاله‌ای در مجله امنیت بین الملل می گوید: «برخی از جنبه های سایبر قادر به تطابق با «چارچوب های امنیت سنتی است و برخی دیگر برای آن چالش ایجاد می کنند؛ از جمله: گسترش تهدید غیرفیزیکی بر

1. *Erik A. Gartzke*
2. *International Security*
3. *Lucas Kello*

امنیت ملی، توان مندی بازیگران غیردولتی در ایجاد بحران دیپلماتیک، از بین رفتن تمایز میان جنگ محلی و جنگ از راه دور، نفوذ دشمنان ناشناس و غیره. شکاکان این ویژگی های امنیت در عصر حاضر را در نظر نمی گیرند و فقط می‌خواهند موضوع را با استفاده از منطق سابق توضیح دهند. آنها به دنبال این هستند تا تأثیر سلاح مجازی را تا سطح مسائل متعارف کشورداری پایین بیاورند؛ چراکه فکر می کنند با این کار به عنوان خدمت کاران راستین رشته روابط بین الملل معرفی خواهند شد. کارل فون کلازویتس از اهمیت تکنولوژی در عصر خود غفلت کرده است. این اشتباه است که فکر کنیم مفاهیم او قادر به رمزگشایی از تکنولوژی جدید عصر ما هستند» (Kello ,2013)

(۳) تیموتی جی جونیو[1] (پژوهشگر مرکز امنیت و همکاری بین المللی دانشگاه استنفورد) در مجله مطالعات راهبردی[2] در موافقت با استحقاق این عرصه و در جهت بذل توجه و ایجاد مکتب سایبر در مطالعات امنیت بین‌الملل استدلال می کند. تأکید وی بر اشتباه بودن این نظر شکاکان است که «جنگ سایبری رخ نخواهد. سایبر بیشتر از سایر تکنولوژی ها شانس شرکت در عملیات تهاجمی را دارد. سلاح های سایبری بسیاری از سازوکارهای تشدید خشونت را دارند. در سازوکارهای سنتی شروع عملیات بسیار مشکل و پرهزینه بود، ولی در این جا آسان و کم هزینه است. لذا می بایست به سایبر توجه بیشتری شود. (Junio,2013)

(٤) کاربست نظریه *Principal-agent* (کارگزار کارفرما) در علل جنگهای سایبری: این نظریه توضیح میدهد که چگونه اختلاف انگیزه ها و ترجیحات افراد و سازمان ها می تواند به بروز جنگ در راستای منافعی خاص دامن بزند و با توجه به طبیعت مسائل سایبری، شروع نبرد سایبری بین دولتها بسیار محتمل و آسان تر از جنگهای نظامی است. این در حالی است که شروع عملیات نظامی متعارف به دلیل هزینه بالا به راحتی قابل انتخاب نیست. همچنین در مقایسه بین تکنولوژی‌های هسته‌ای و سایبری به دلیل هزینه های جنگ، شروع تهاجم سایبری در قیاس با جنگهای هسته ای بسیار سهل الوصول است و به دلیل ماهیت تهاجمی سایبر، سازمان های سایبری نظامی بسیار تهاجمی‌تر از سایر بروکراسی ها رفتار می کنند. لذا می توان نتیجه گرفت که دولتها یا بازیگران در تعارضات بین خود به دلیل ویژگیهای موصوف جنگهای سایبری، قبل از توسل به تسلیحات نظامی و هسته ای، از ظرفیتهای تهاجمات سایبری استفاده خواهند کرد.

(٥) ریچارد کلارک و رابرت ناک[3] دو تن از اولین اندیشمندان آمریکایی حوزه امنیت سایبری، اعتقاد دارند که «از بین تمام مفاهیم استراتژی هسته ای، بازدارندگی کمترین امکان را برای انتقال به نبرد سایبر دارد». یک استراتژی مؤثر در عصر سایبر، نیازمند فهمی گسترده تر و چندبعدی از مفهوم بازدارندگی بوده

1. *Timothy J. Junio*
2. *Strategic Studies*
3. *Richard A. Clarke and Robert K. Knake*

و اشتباه است حوزه سایبر را تنها ببینیم. نیاز نیست که پاسخ یک حمله سایبری را تنها با ابزار سایبری ارائه دهیم. بازدارندگی سایبری به این معناست که در پاسخ به یک حمله سایبری می توانیم از طریق تمامی عرصه ها پاسخ دهیم. در استراتژی سایبری آمریکا در ۲۰۱۱ تصریح شده است که آمریکا حق استفاده از کلیه ابزارهای دیپلماتیک، اطلاعاتی، نظامی و اقتصادی را برای خود محفوظ می داند. (دهقانی، ۱۳۹۷)

(٦) ریچارد. ال. کلوگلر[1] (پژوهشگر آمریکایی در حوزه امنیت ملی و استراتژی دفاعی) در مقاله خود تحت عنوان «بازدارندگی حملات سایبری» درخصوص الزامات تئوری بازدارندگی می نویسد: «نیازمندیهای یک تئوری بازدارندگی موثر چیست؟ یک پاسخ ساده این است: دفاع قوی که بتواند حملات سایبری را دفع کند و آفندهای سایبری را تقویت نماید که بتواند خسارات تلافی جویانه انبوه را تحمیل نماید. بدین ترتیب، در چنین رویکرد قابلیت پایه‌ای فرض می شود جنگهای سایبری در حالت ایزوله از سایر وقایع بزرگتر پیرامون آن، اتفاق بیافتد و بتواند با آن به عنوان خود حاکم، تابع منطق و نیازهای خود رفتار شود. بدین ترتیب، احتمال بیشتر این است که برخی حملات سایبر عمده احتمالاً بعنوان یک ابزار در دستیابی به اهداف سیاسی و راهبردی، نه فقط تحمیل خسارات به طرف مقابل می نماید بلکه بعنوان ابزار چانه زنی و اجبار مورد استفاده قرار می گیرند تا کشور هدف را وادار به تسلیم در مقابل خواسته های سیاسی – راهبردی مهاجمین نمایند (احدی و شاه‌محمدی، ۱۳۹۶)

اسناد بالادستی درخصوص فضای سایبری در جمهوری اسلامی ایران

در رابطه با فضای سایبر، اسناد بالادستی زیادی وجود دارد که مهمترین اسناد بالادستی فضای سایبری، شامل موارد ذیل می گردند:

- «سند راهبردی امنیت فضای تولید و تبادل اطلاعات» مصوب ۱۳۷۸/۱۲/۱ ابلاغ توسط رئیس جمهور
- سند «سیاستهای کلی امنیت فضای تولید و تبادل اطلاعات مصوب ۱۳۸۹/۱۱/۲۹ مجمع تشخیص مصلحت نظام
- «سند راهبردی پدافند سایبری کشور» مصوب ۱۳۹٤/۳/۲۱ ابلاغ توسط فرماندهی کل قوا
- «سیاست های کلی برنامه ششم توسعه، بخش امور فناوری اطلاعات و ارتباطات» مصوب ۱۳۹٤ «نظام ملی پیشگیری و مقابله با حوادث فضای مجازی» مصوب شورای عالی فضای مجازی ۱۳۹۶/۸/۱۵

ابعاد تهدیدات سایبری (تهدید و آسیب پذیری سایبری):

آسیب پذیری سایبری به ضعف، نقص و عیب موجود در داخل یک سرمایه ملی سایبری، رویه های امنیتی یا کنترلهای داخلی، یا پیاده سازی آن سرمایه ملی سایبری که قابلیت بهره برداری یا فعال شدن تهدیدات داخلی و خارجی به منظور تهاجم یا جنگ سایبری را داشته باشد اطلاق می گردد. (سند راهبردی فضای

1. *Richard L. Kugler*

سایبری کشور). وجه افتراق تهدید و آسیب پذیری در منشاء آنان بروز می نماید، لذا تهدیدات فضای سایبری فراسرزمینی و منبعث از دشمنان یا مهاجمان خارجی و عمدتاً در حوزه های فنی خلاصه می شود. تهدید سایبری در سند راهبردی پدافند سایبری اینگونه تعریف شده است: هررویداد یا واقعه با قابلیت واردنمودن ضربه به مأموریتها، وظایف، تصویر (پنداره) یا اشتهار دستگاه متولی، سرمایه ملی سایبری یا پرسنل دستگاه به واسطه یک سامانه اطلاعاتی، ازطریق دسترسی غیرمجاز، انهدام (تخریب)، افشاء، تغییراطلاعات و / یا ممانعت از (ایجاداختلال در) ارائه خدمت.

ویژگیهای تهدیدات سایبری

منشاء اغلب تهدیدات سایبری قابل شناسایی نیست و غالباً از خارج از مرزهای جغرافیایی کشور برنامه ریزی و اجرا می‌شوند و دارای ویژگیهای متنوعمی می باشند که مهمترین آنها:

۱. فراسرزمینی بودن: تهدیدات سایبری در مرزهای جغرافیایی نمی گنجند.

۲. رهیافتهای غیر نظامی: مدیریت، تقابل و دفع تهدیدات سایبری مستلزم طیفی از رهیافتهای غیر نظامی و مبتنی بر دانش سایبری است.

۳. خصلت خزندگی و نامشخص بودن: تهدیدات سایبری رفتاری خزنده و پنهان دارند.

٤. عدم انتساب یا خصلت گمنانی: منشاء تهدید یا مهاجم قادر به کتمان هویت خود می باشندو انکار وجه قالب پذیرش مسولیت از جانب مظنونین به انجام این تهدیدات یا حملات است. (مرتضوی، مصاحبه:۱۳۹۹)

«مؤلفه های ذیل، مدل دیگری از بیان ویژگیهای تهدیدات سایبری می باشند:

۱) تعدد بازیگران در فضای سایبری ۲) هزینه کم ورود، صرف زمان کم و سرعت بالای اقدام ۳) ناشناس ماندن افراد و عدم قابلیت ردیابی ۴) تاثیر گذاری زیاد و عمیق ۵) کمرنگ شدن نقش جغرافیای کشورها ۶) ساختار فضای اینترنت ۷) پایین بودن احتمال تنبیه یا بازخواست اقدام های مجرمانه در فضای سایبری»(خلیلی پور و نورعلی وند. یاسر؛ ۱۳۹۰)

تهاجم سایبری: «تهاجم سایبری، مجموعه اقداماتی است که به منظور ایجاد اختلال، قطعی، کاهش کیفیت یا نابودی اطلاعات موجود در رایانه‌های متصل به فضای سایبری صورت می‌پذیرد»(۲۵: ۲۰۱۱، *Andress and Winterfield*). جنگ سایبری در ذیل تهاجم سایبری تعریف می گردد اما در شدت عمل و پیامدهای آن سطح بالاتر و خشن تری نسبت به اشکال مختلف تهاجم به خود می گیرد. «اگر با نظر کلازویتز موافق باشیم که جنگ عمل صرفاً سیاسی نیست، بلکه ابزار سیاسی برای رسیدن به اهداف سیاسی است، می توانیم بگوییم که جنگ در فضای مجازی توسط بازیگرانی صورت می گیرد که به دنبال استفاده از این فضا برای رسیدن به اهداف سیاسی خود هستند. به منظور درک اینکه آیا عمل خصمانه

در فضای مجازی جنگ قلمداد می شود یا نه، لازم است قصد بازیگر را درک کنیم.»(Cornish-2010 and Et al) منشاء جنگهای سایبری را می توان دولتهای متخاصم یا رقیب و یا گروه های سازماندهی شده تحت حمایت آن دولتها دانست.

انواع حملات سایبری:

حملات سایبری بسته به اهمیت و ارزش اهدافی که مورد هدف قرار می گیرند، توانمندی فنی مهاجم، هویت حقیقی یا حقوقی مهاجم، عوارض و پیامدهای کنترل شده و یا غیر قابل پیش بینی و تصور عملیات، به طرق گونان دسته بندی می گردند:

۱. استراق سمع و جاسوسی از طریق بستر شبکه
۲. اختلال، انهدام یا قطع شبکه های اطلاع رسانی، ارتباطی، زیرساختی و خدمات عمومی
۳. دسترسی غیر مجاز، سرقت، تغییر یا از بین بردن داده های داده‌های حاکمیتی یا حائز اهمیت
٤. تهدید حریم خصوصی افراد و سرقت و افشای داده های شخصی مردم عادی جامعه (فلی پور، مصاحبه،۱۳۹۹)

پیامدهای جنگ یا تهاجم سایبری:

- ✓ اختلال در اداره امور کشور یا یک سازمان و احتمال وقوع شورش یا اعتراضات عمومی
- ✓ سلب اطمینان عمومی نسبت به توانایی حاکمیت برای اداره کشور یا حمایت از آنان
- ✓ خسارتهای ملی و منطقه ای در اقتصاد و صنعت
- ✓ تخریب سرمایه های ملی شامل زیرساختهای حیاتی و حساس
- ✓ احتمال وقوع جنگ نظامی یا تنش دیپلماتیک بین کشور مهاجم و قربانی
- ✓ تخریب وجهه و اعتبار کشور در سطح بین المللی
- ✓ احتمال وقوع مخاطرات زیست محیطی یا سلامت عمومی ناشی از ایجاد آلودگیهای هسته ای و شیمیایی (بابایی، مصاحبه،۱۳۹۹)

مصادیقی از سوابق حملات سایبری علیه جمهوری اسلامی ایران

- حمله سایبری به تاسیسات غنی سازی نطنز در خرداد ۱۳۸۸ توسط یک رایانه‌ای بنام استاکس‌نت[1] که از طریق تغییر فرکانس دستگاه های سانتریفیوژ، موجب تخریب زنجیره غنی سازی اورانیوم گردید.
- حمله به رایانه های وزارت نفت و شرکتهای وابسته در اردیبهشت سال ۱۳۹۱ توسط ویروسی بنام «فلیم» که منجر به سوختن مادربرد رایانه ها و باعث پاک شدن اطلاعات و در نتیجه اخلال در سیستم های رایانه ای و اینترنتی وزارت نفت و مناطق عملیاتی خارک، بهرگان، سیری، لاوان، قشم و کیش گردید.

1. *Stuxnet*

- حمله به شبکه مخابراتی کشور در ١٤ آبان ١٣٩٧ که بنابر اظهارات وزیر وقت ارتباطات، از مبداء شرکت گلدن لاین اینترنت اسرائیل بوده و منجر به حذف پیکربندی تجهیزات روتر و سوئیچ شرکت سیسکو گردید.
- حمله به سامانه های دولت الکترونیک کشور در ٢٤ آذرماه ١٣٩٨ که بنابر اظهارات وزیر وقت ارتباطات، در قالب حملات شناخته شده و پیچیده $APT_{٢٧}$ دسته بندی و برای جاسوسی از اطلاعات صورت گرفته بود.
- حمله سایبری به سیستم های رایانه ای شرکت راه آهن در ١٨ تیر ١٤٠٠ که منجر به اخلال در فعالیت و برنامه حرکت قطارها، مراکز خرید بلیط، خدمات الکترونیک مسافری و باری و سایت شرکت راه آهن گردید.
- هک دوربینهای زندان اوین و انتشار تصاویر برخی دوربینهای زندان در اوایل شهریور ١٤٠٠ که موجب راه افتادن موج تبلیغاتی علیه قوه قضائیه و سازمان زندانها را در رسانه های معاند و خارجی گردید.
- حمله به سامانه هوشمند کارت سوخت در ٤ آبان ١٤٠٠ که منجر به اخلال در سامانه مدیریت کارتهای سوخت وسائط نقلیه و توزیع سهمیه بنزین با نرخ دولتی، توقف سوختگیری در جایگاههای سراسر کشور و تبعاتی نظیر تشکیل صفهای طولانی، ایجاد نارضایتی عمومی و بروز شایعات مختلف گردید.
- هک چندین شبکه تلویزیونی و رادیویی صدا و سیما در ٦ بهمن ١٤٠٠ که درپی آن تصاویر و صدای سران گروهک منافقین و شعار علیه مقامات نظام به مدت ١٠ ثانیه از شبکه یک سیما و شبکه های رادیویی قرآن، پیام و جوان پخش گردید.

تهدیدات نوین سایبری فراروی علیه ج.ا.ایران

١- تروریسم سایبری

تروریسم سایبری، تهدیدی در آینده نیست بلکه در گذشته شروع شده و در آینده نیز ادامه خواهد داشت و به معنی «بکارگیری ابزارهای سایبری برای حمله به ساختارهای اطلاعاتی و ارتباطی یك کشور، حزب، گروه، توسط گروه های تروریستی به منظور خربکاری یا نفوذ» می باشد». (کریمی پاشایی و دیگران، ١٣٩٤)

٢- گسترش کاربری هوش مصنوعی

هوش مصنوعی را «دانش و مهندسی ساخت ماشین‌های هوشمند» تعریف نموده اند و مجرمان سایبری از این دانش برای مدیریت هوشمند حملات سایبری استفاده می کنند را مدیریت بکنند. بسیاری از دانشمندان و کارشناسان بر این باورند که توسعه هوش مصنوعی در کنار تمام فرصت‌های جدیدی که در صنعت به وجود می‌آورد، تهدید نیز به شمار می‌رود و به مجرمان و دولتها این امکان را می دهد تا با سرعت و دقت

بیشترو احتمال کمتر ردیابی، نسبت به انجام جرایم سایبری (نظیر سرقت، کلاهبرداری، تخریب و ...) اقدام نمایند. اما هوش مصنوعی از این حیث خطرناک تر که خارج از کنترل انسان عمل نموده و با توانایی فکر کردن و سازگاری با محیط اطراف، تهدیدی خارج از کنترل بشر تولید نماید. (هادی، مصاحبه،۱۳۹۹)

۳- ارزهای دیجیتال

ارز دیجیتال یا *Cryptocurrency* شکل خاصی از پول دیجیتال است که بر پایه علم رمزنگاری ایجاد شده است. اولین ویژگی ارزهای دیجیتال غیرقابل برگشت بودن تراکنش‌هاست. دومین ویژگی ارزهای دیجیتال ناشناس بودن یا نیمه ناشناس بودن آن‌هاست. سومین ویژگی ارزهای دیجیتال جهانی یا فرامرزی بودن آن‌هاست. چهارمین ویژگی امنیت ارزهای دیجیتال و پنجمین ویژگی انحصاری نبودن آن‌هاست. تهدید این ارزها اینجاست که منجر به دور زدن حاکمیت‌های ملی و سلب قدرت اقتصادی سیاسی کشور شده و در اختیار حاکمان کمپانی‌های فراملی این فناوری قرار خواهد گرفت. لذا بخش عمده نوسانات بازار پول به سیاست‌های این کمپانی‌ها بستگی خواهد داشت. همچنین شکل گیری بازار زیرزمینی پول و عدم امکان رصد و مالیات‌ستانی بر اساس تراکنش‌های مالی افراد، انجام معامله در بازارهای غیررسمی و غیرقانونی مانند موادمخدر، قاچاق و بازارهای زیرزمینی یا وب تاریک و فقدان مسئولیت پذیری از دیگر اشکالات ارزهای دیجیتال می باشند. (ملک پور، ۱۳۹۸/۴/۲۵)

٤- حکمرانی قدرتهای جهانی بخصوص آمریکا بر اینترنت:

حکمرانی شامل فرایندهای اعمال حاکمیت به‌وسیله دولت یا هر سیستم واجد قدرت بر سیستمی دیگر شامل نهادهای اجتماعی و سیاسی (خانواده، قبیله، یک قلمرو و...) است؛ این فرایند از طریق گسترهٔ وسیعی از ابزارها شامل قوانین و هنجارها شکل می گیرد. شبکه جهانی اینترنت نیز از این قاعده مستثنی نیست. شکل گیری مؤسسه غیرانتفاعی و عمومی *ICANN* توسط وزارت بازرگانی آمریکا در سال ۱۹۹۸ جهت هماهنگی دامنه و تخصیص آدرس و سازمان *IANA* بعنوان مسئول اختصاص منابع عددی اینترنت به خاطر وابستگی کامل به وزارت دفاع آمریکا مورد هجوم منتقدین جهانی قرارگرفت. کشورها با انتقاد از حکمرانی انحصاری و یک‌طرفه ایالات‌متحده، تصمیم گیری مستقل آیکان در مورد مسائل عمومی جهانی، فنی بودن صرف آیکان و عدم پرداختن به مشکلات اجتماعی و نوظهور اینترنت، مشروعیت *ICANN* را موردنقد قراردادند و نهایتاً انجمن چندذینفعی حکمرانی اینترنت ((*IGF*را شکل گرفت. اما علی‌رغم وجود نهادهای بین‌المللی، یکه‌تاز بودن ایالات‌متحده در اپراتوری و رگولاتوری اینترنت نیز گمان نمایشی بودن این‌گونه نهادها را قوت می‌بخشد. با توجه به مخاصمات میان ج.ا.ایران و آمریکا، تداوم حاکمیت آمریکا بر اینترنت می‌تواند ابزاری در اختیار آمریکا برای اعمال فشار، محدودیت و حتی محرومیت از برخی جنبه‌ها و خدمات اینترنتی برای سایتهای اینترنتی و هاستهای ایرانی باشد. (زیبنده مراد، ۱۳۹۷/۵/۲۰)

۵– تهدیدات ناشی از اینترنت ماهواره‌ای

اینترنت ماهواره ای یکی از انواع روش های دسترسی به شبکه اینترنت است که از طریق ارتباطات ماهواره‌ای برقرار و بیشتر برای مواردی مورد استفاده قرار می گیرد که دسترسی به اینترنت زمینی و معمولی امکان پذیر نمی باشد یا از کیفیت بسیار پایینی برخوردار است. در حال حاضر شرکت آمریکایی «اسپیس اکس»[1] پیشتاز پرتاب ماهواره به فضا برای ارائه خدمات اینترنت ماهواره‌ای است که اعلام کرده است در نظر دارد هزاران ماهواره ارائه دهنده خدمات اینترنتی به مدار اطراف کره زمین در طول چند سال آینده ارسال کند که بخشی از این ماهواره‌ها پرتاب شده‌اند. تحقق ارائه خدمات اینترنت ماهواره‌ای یعنی ارائه این خدمات خارج از مالکیت و حاکمیت دولتها و به تبع آن ایجاد چالش در قوانین فیلترینگ دولتها بر محتوای اینترنت خواهد بود. (قلی پور، مصاحبه ۱۳۹۹)

۶– عملیات روانی ناشی از فضای مجازی (در بستر فضای سایبری):

عملیات روانی، قدرت مبتنی بر مولفه‌های نرم و درحقیقت تاثیر گذاری بر روان اشخاص یا مخاطب از طریق قدرت نرم است. فضای سایبر به واسطهٔ فناوریهای نوین ارتباطی که از طریق شبکه‌های اجتماعی ایجاد نموده است (اپلیکیش های رایج در ایران نظیر *watsApp*، *Telegram*، *Instagram*، *ooVoo*، *Skyp* و...) به رکنی اساسی در مدیریت افکار عمومی و جهت دهی به افکار مخاطبین و ذهنیت آنان تبدیل شده است. این شبکه‌ها ضمن ایجاد دسترسی آسان و زودهنگام و برخط کاربران به اخبار واقعی و غیر واقعی جاری، کاهش اعتبار رسانه‌های داخلی سنتی در ذهن مخاطبین را در پی داشته که از همین طریق، مدیریت این شبکه‌ها نسبت به القای مطالبی مورد نظر خود به افکار عمومی، فضاسازی و شایعه سازی صورت می گیرد. (امیری،۱۳۹۲)

۷– تهدیدات ناشی از محاسبات کوانتومی:

محاسبات کوانتومی یعنی توسعه کامپیوتر هایی بر مبنای نظریه کوانتوم که طبیعت و رفتار انرژی و ماده را در سطح کوانتومی (اتمی و زیراتمی) مورد بررسی قرار می دهد. پیشتازی دولتها در دست یابی به توانمندی محاسبات کوانتومی، برتری آنها را در فناوریهایی نظیر «ذخیره سازی اطلاعات، رمز کردن اطلاعات، انتقال اطلاعات، پردازش اطلاعات، تولید اطلاعات» نسبت به سایر کشورها تضمین خواهد نمود که بطور مستقیم بر فضای مجازی بخصوص در رمز نمودن داده ها (در شبکه‌های اجتماعی، ایمیل‌ها، رمز ارزها) تاثیرگذار خواهد بود. بنابر این کشورهایی که عموماً کاربر فضای سایبری و فضای مجازی هستند تابع قوانین و شرایطی خواهد بود که در فضای فناوریهای نوظهور کوانتومی و توسط دولتها و شرکتهای تولید کننده وضع خواهد شد. (قلی پور، مصاحبه،۱۳۹۹)

1. *Space Exploration Technologies Corporation*

شکل گیری کلان داده‌ها از کاربران، سازمانها و شرکتها[1]:

کلان داده به مجموعه داده های بسیاربزرگ، متنوع، با ساختار پیچیده گفته می شود که ذخیره سازی، تحلیل و پردازشهای آنها فراتر از حدی است که با نرم افزارهای معمول بتوان آنها را در یک زمان معقول اخذ، دقیق سازی، مدیریت و پردازش کرد. این داده ها از تراکنشهای برخط، پستهای الکترونیکی، ویدئوها، صوتها، کلیک کردن ها، log ها و ارسالها، درخواستهای جستجو، یادداشتهای درست، تعاملات شبکه های اجتماعی، داده های علمی، سنسورها و تلفنهای همراه و برنامه های کاربردی آنها تولید میشوند. از تحلیل این داده‌ها اطلاعات ذیل قابل حصول است:

-علایق و سلیقه‌های مردم یک کشور، گروه‌های سنی و جنسیتی، قومیت، منطقه جغرافیایی و... (ذائقه سنجی)

-اطلاعات شخصی (عکس، فیلم، چت، جستجوها و...)

-نوع واکنش مردم به مسائل و اخبار منتشره در فضای مجازی و عالم حقیقی (برانگیختگی و بی‌تفاوتی)

-نوع نگرش نسبت به مسائل مختلف سیاسی و اجتماعی و فرهنگی و...(قابلیت پذیری و تقابل) و ... (آسمانی، ۱۳۹۵)

۹- تهدیدات ناشی از تکنولوژیهای جدید ارتباطهای اینترنتی نظیر *Black chain*، *wikitalk*

واژه بلاک چین [2]ترکیبی از دو کلمه *Block* (بلوک) و *Chain* (زنجیره) و در حقیقت زنجیره‌ای از بلوک‌ها و یک نوع سیستم ثبت اطلاعات و گزارش است که تفاوت آن با سیستم‌های دیگر این است که اطلاعات ذخیره شده روی این نوع سیستم، میان همه اعضای شبکه به اشتراک گذاشته می‌شوند و با استفاده از رمزنگاری امکان حذف و دستکاری اطلاعات ثبت شده تقریبا غیرممکن است. داده‌های بلاک چین در یک کامپیوتر یا سرور خاص ذخیره نمی‌شوند. هر کامپیوتر یا سیستمی که به شبکه وصل شود، یک نسخه از اطلاعات را دریافت می کند. به هر کامپیوتری که به شبکه متصل می‌شود و یک کپی از بلاک چین را دریافت می کند، نود (*Node*) می گویند. وقتی شما به یک بلاک چین متصل می‌شوید، یک نسخه از کل داده‌های آن را دریافت می کنید. هیچ تغییری در اطلاعت امکان پذیر نیست مگر اینکه بیش از ۵۰ درصد از داده‌های رایانه‌های متصل به شبکه تغییر کند. در شبکه «بلاک‌چین» نظارت دولتی بر اینترنت محدود می‌شود و امکان اعمال فیلتر ضعیف می‌شود. در مجموع بلک چین قابلیت ایجاد یک اینترنت محلی، در محدودهٔ رایانه‌ها و گوشی‌های همراه در یک محدوده جغرافیایی مشخص را دارد به گونه‌ای که تجهیزات موصوف امکان ارتباط گیری در شعا خاصی نظیر ۳۰۰ متر را با یکدیگر داشته باشند. نرم افزارهایی نظیر *wikitalk* نیز بر همین قاعده استوارند و افرادی که در یک محدودهٔ شهری یا منطقه‌ای برای هدف خاصی

1. Big Data
2. Blockchain

نظیر اعتراض یا اغتشاش تجمع می کنند، می‌توانند بدون اینکه نگران قطع شدن اینترنت توسط حاکمیت باشند، از طریق قابلیتهای مذکور و نصب نرم افزارهایی که بر پایهٔ بلک چین فعالیت می کنند، نسبت به ارتباط با یکدیگر و ایجاد هماهنگی و انتقال پیام اقدام کنند. این نوع ارتباط به دلیل آنکه مستقل از نظارت و کنترل حاکمیت است در زمان نا آرامیها و اعتراضات می‌تواند یک تهدید برای دولتها محسوب گردد. (آذرنیوار،۱۳۹۹/۱/۲۳)

۱۰- مدیریت افکار و ذائقه عمومی توسط شبکه‌های اجتماعی

شبکه های اجتماعی به دلیل قابلیتهای خدماتی خود مورد اقبال و توجه طیف بسیار کثیر و شاید همهٔ کاربران اینترنت قرار گرفته است و امروزه کمتر کسی را می‌توان یافت که حداقل عضور یکی از شبکه های اجتماعی نباشد. شبکه های اجتماعی با ظرفیتهای ایجاد گروه و کانال و سیستم توزیع پیام بطور هماهنگ و سریع در بین اعضا و مخاطبین از طرق ذیل توانمندی مدیریت افکار و ذائقه عمومی را پیدا نموده که درصورت عدم مدیریت یا نظارت، می تواند تولید آسیب یا تهدید را در پی داشته باشد:

۱. قابلیت سازماندهی (ساماندهی) کاربران در قبال موضوعی خاص
۲. امکان انتقال سریع خبر، مطلب یا پیامی به طیف وسیعی از کاربران در حداقل زمان
۳. توانایی القای مطلب یا نظر خاصی به کاربران در قالب شایعه یا پیامهای فاقد منبع مشخص
٤. عدم امکان راستی آزمایی مطالب منتشره در شبکه‌ها در زمان کوتاه و استناد بسیاری از کابران به آن مطالب
٥. امکان بازنشر اخبار، مطالب و پیامها توسط کاربران در کوتاه ترین زمان ممکن قبل از بررسی صحت (کریمی و دیگران،۱۳۹۷)

۱۱- ایجاد محدودیت در دسترسی به خدمات ایترنتی (تحریم و...)

ایجاد محدودیت شرکتهای گوگل پلی و سامسونگ در ارئه خدمات به کاربران ایرانی ناشی از تحریمهای ثانویه دولت آمریکا علیه جمهوری اسلامی ایران منجر به ایجاد نارضایتی عمومی در ایرانیان و طرح این سوال شد که «علت و منشاء این تحریمها چیست؟» و عموماً توسط رسانه های خارجی و معاند اینگونه پاسخ داده می شود که رفتارهای ج.ا.ایران در قبال موضوعات منطقه‌ای و بین‌الملل موجب وضع تحریمهای مذکور و محرومیت مردم ایران از خدماتی و امکاناتی گردیده است که عموم مردم جهان از آن برخوردارند. اینترنت به دلیل ظریب نفوذ بالا و تعدد کثیر کاربران و قابلیتهای متنوع گوشی‌های هوشمند موجب گردیده که هرنوع محرومیت و تحریم بر خلاف سایر تحریمها که جامعیت فراگیری ندارند بلافاصله اثرات حس محرومیت بر طیف کثیری از مردم ظاهر می شود و لذا نارضایتی نسبت به حاکمیت ج.ا.ایران در اذهان و رفتار مردم ایجاد گردد. (بابایی، مصاحبه،۱۳۹۹)

۱۲- وابستگی زیرساختهای ملی به فضای سایبری

امروز بسیاری از خدمات عمومی نظیر خدمات پولی و بانکی، تبلیغات، کسب و کارهای اینترنتی در بستر فضای سایبری در حال ارائه می باشد. خدمات عمومی نظیر مخابرات، برق و آب و...در بستر فضای سایبری مدیریت و کنترل می گردند. تسلط به فضای سایبری بطور مطلق برای هیچ کاربر یا کشوری ممکن نیست، اما شرکتها و دولتهایی که صاحب تکنولوژی هستند قواعد مسلط بر فضای سایبر و مجازی را تعیین و امنیت دولتها و کشورهای ضعیف تر را به چالش خواهند کشید. (خلیلی پور رکن آبادی،۱۳۹۱)

روش شناسی: تحقیق مورد نظر بر مبنای هدف، کاربردی و رویکرد پژوهش تلفیقی است. روش به کارگرفته در این پژوهش از نوع توصیفی تحلیلی است. روش گردآوری اطلاعات بر محورهای گردآوری کتابخانه‌ای و اینترنتی، و روش‌های میدانی متمرکز بوده است. برای دستیابی به روایی تحقیق نیز ابتدا سؤال‌های پرسشنامه از خبرگانی نظرخواهی و سپس بر اساس آنها مصاحبه انجام شده است. جامعه آماری این پژوهش ٢٦ نفر است (بخش کمی (١٤ نفر) و کیفی (١٢ نفر). در بخش کیفی جامعه آماری، ١٢ نفر از معاونین حوزه سایبری کشوری و لشگری که دارای جایگاه های شغلی ١٨ به بالا و حداقل ٢٠ سال سابقه کار در این حوزه داشته و دارای مدرک کارشناسی ارشد به بالا هستند، مورد استفاده قرار گرفته است. مصاحبه با این افراد تا اشباع نظری و به شیوه گلوله برفی انجام شده است. در بخش کمی نیز تعداد ١٤ نفر از مدیران ارشد امنیتی حوزه سایبری و فناوری که دارای مدرک کارشناسی ارشد به بالا، حداقل ١٥ سال سابقه مدیریتی و اجرایی در حوزه امنیت سایبر بوده، به عنوان جامعه آماری در نظر گرفته شد و بصورت تمام شمار از آنها در حجم نمونه آماری استفاده گردید.

پس از بررسی ادبیات موضوع و احصا و تبیین تهدیدات سایبری نوین، ابتدا با انجام مصاحبه نیمه ساخت یافته با خبرگان موضوع، ادبیات احصاء شده کامل تر گردید و لیستی از تهدیدان نوین امنیتی در حوزه سایبری بدست آمد. در مصاحبه های انجام شده سه سوال اساسی مطرح شد. ١-مهم‌ترین تهدیدات امنیتی نوین سایبری فراروی ج.ا.ایران ٢- اولویت‌بندی این تهدیدات ٣- راهکارهای مقابله با این تهدیدات.

لیست تهدیدات نوین سایبری احصا شده از ادبیات موجود و نتایج حاصل از مصاحبه با خبرگان موضوع که بدست آمده است، شامل موارد ذیل می باشد:

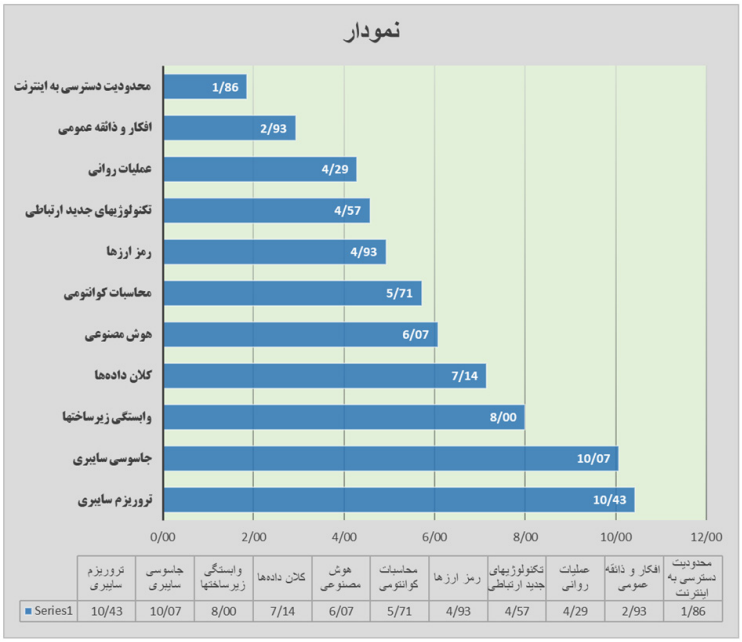
ردیف	تهدیدات نوین سایبری
١	تروریزم سایبری (تهاجمات سایبری)
٢	عملیات روانی در بستر فضای سایبری علیه ج.ا.ایران
٣	رمز ارزها
٤	تحقق محاسبات کوانتومی (کوانتوم کامپیوتینگ) و اثرات آن بر تحولات فضای سایبری
٥	شکل گیری کلان داده‌ها از داده‌های مربوط به کاربران ایرانی

ردیف	تهدیدات نوین سایبری
۶	جاسوسی سایبری (جمع آوری اطلاعات)
۷	فراگیر شدن هوش مصنوعی در ابعاد مختلف زندگی بشر
۸	**فراگیرشدن تکنولوژیهای جدید ارتباطهای اینترنتی (*Black chain wikitallk*، ماهواره‌ای و ...)**
۹	مدیریت افکار و ذائقه عمومی کاربران ایرانی توسط شبکه‌های اجتماعی
۱۰	ایجاد محدودیت در دسترسی ج.ا.ایران و کاربران ایرانی به خدمات اینترنتی (تحریم و ...)
۱۱	وابستگی زیرساختهای ملی به فضای سایبری

پرسشنامه اولیه پس از احصاء از طریق ارائه به جمعی از خبرگان مورد تایید روایی محتوایی قرار گرفت و نظرات این جمع در تصحیح پرسشنامه مورد استفاده قرار گرفت. پرسشنامه در اختیار ١٤ نفر از حجم نمونه آماری اشاره شده قرار گرفت که نتایج به شرح ذیل می باشد. به منظور سنجش پایایی پرسش نامه، از روش باز آزمایی یا آزمون مجدد استفاده شد. در این روش پرسشنامه در دو نوبت با فاصله زمانی به گروه واحدی از جامعه آماری ارائه شد و نمرات حاصل را با هم مقایسه گردید و نسبت به پایایی یا اطمینان نسبت به پرسشنامه حاصل گردید.

جمع بندی (پیاده سازی) داده‌های حاصل از پاسخ به سوالات پرسشنامه:

پرسشنامه‌های جمع آوری شده با استفاده از نرم افزار SPSS و از طریق آزمون فریدمن مورد جمع بندی و تجزیه و رتبه بندی قرار گرفتند که نتایج ذیل را در بر داشت:



عنوان تهدید	امتیاز	رتبه	درصد
تروریسم سایبری	۱۰،٤۳	۱	۱۶%
جاسوسی سایبری	۱۰،۰۷	۲	۱۵%
وابستگی زیرساختهای ملی به فضای سایبری	۸،۰۰	۳	۱۲%
شکل گیری کلان داده‌ها از داده‌های مربوط به کاربران ایرانی	۷،۱٤	٤	۱۱%
فراگیر شدن هوش مصنوعی در ابعاد مختلف زندگی بشر	۶،۰۷	۵	۹%
تحقق محاسبات کوانتومی (کوانتوم کامپیوتینگ) و اثرات آن بر تحولات فضای سایبری	۵،۷۱	۶	۹%
رمز ارزها	٤،۹۳	۷	۷%
فراگیرشدن تکنولوژیهای جدید ارتباطهای اینترنتی (*wikitallk*، *Black chain*، ماهواره‌ای و ...)	٤،۵۷	۸	۷%
عملیات روانی در بستر فضای سایبری علیه ج.ا.ایران	٤،۲۹	۹	۷%
مدیریت افکار و ذائقه عمومی کاربران ایرانی توسط شبکه‌های اجتماعی	۲،۹۳	۱۰	٤%
ایجاد محدودیت در دسترسی ج.ا.ایران و کاربران ایرانی به خدمات اینترنتی (تحریم و ...)	۱،۸۶	۱۱	۳%

نمودار توصیفی								
عنوان تهدید	تعداد نمونه	متوسط	انحراف معیار	مینیمم	ماکزیمم	*Percentiles*		
						25th	*50th (Median)*	*75th*
تروریزم سایبری	۱٤	۲۱،٤۲۸۶	۰،۶٤۶۲۱	۲۰،۰۰	۲۲،۰۰	۲۱،۰۰۰۰	۲۱،۵۰۰۰	۲۲.۰۰۰۰
عملیات روانی	۱٤	۱۵،۲۸۵۷	۱،۸۵۷۵۷	۱۲،۰۰	۱۸،۰۰	۱۳،۷۵۰۰	۱۵،۵۰۰۰	۱۷.۰۰۰۰
تهدید ناشی از رمز ارزها	۱٤	۱۵،۹۲۸۶	۱،۸۱۷۲۰	۱۳،۰۰	۱۹،۰۰	۱٤،۷۵۰۰	۱۵،۵۰۰۰	۱۸.۰۰۰۰
تهدید ناشی از محاسبات کوانتومی	۱٤	۱۶،۷۱٤۳	۲،٤۶۲۹۱	۱۳،۰۰	۲۱،۰۰	۱٤،۷۵۰۰	۱۶،۰۰۰۰	۱۹.۲۵۰۰
تهدید ناشی از تشکیل کلان داده‌ها	۱٤	۱۸،۱٤۲۹	۱،۸۷۵۲۳	۱٤،۰۰	۲۲،۰۰	۱۷،۰۰۰۰	۱۸،۰۰۰۰	۱۹.۰۰۰۰
جاسوسی سایبری	۱٤	۲۱،۰۷۱٤	۰،۷۳۰۰۵	۲۰،۰۰	۲۲،۰۰	۲۰،۷۵۰۰	۲۱،۰۰۰۰	۲۲.۰۰۰۰

نمودار توصیفی								
عنوان تهدید	تعداد نمونه	متوسط	انحراف معیار	مینیمم	ماکزیمم	Percentiles		
						25th	50th (Median)	75th
تهدید ناشی از هوش مصنوعی	١٤	١٧,٠٧١٤	٢,٨۶٧٩٧	١٣,٠٠	٢٢,٠٠	١٤,٧٥٠٠	١٧,٠٠٠٠	١٩.٢٥٠٠
تکنولوژیهای جدید ارتباطی اینترنتی	١٤	١٥,٥٧١٤	١,٧٤١٥٤	١٢,٠٠	١٩,٠٠	١٤,٧٥٠٠	١٥,٥٠٠٠	١۶.٢٥٠٠
تاثیر بر افکار و ذائقه عمومی	١٤	١٣,٩٢٨۶	٢,٧٨۶٣٥	١٢,٠٠	١٩,٠٠	١٢,٠٠٠٠	١٣,٠٠٠٠	١٤.٥٠٠٠
ایجاد محدودیت دسترسی به خدمات اینترنت	١٤	١٢,٨٥٧١	١,٠٢٧١١	١٢,٠٠	١٥,٠٠	١٢,٠٠٠٠	١٢,٥٠٠٠	١٤.٠٠٠٠
وابستگی زیرساختها به فضای سایبر	١٤	١٩,٠٠٠٠	١,٠٣٧٧٥	١٧,٠٠	٢٠,٠٠	١٨,٠٠٠٠	١٩,٠٠٠٠	٢٠.٠٠٠٠

نتیجه گیری

موضوع سایبر و تهدیدات سایبری به دلیل ساختار شبکه محور زیرساختهای سایبری، قابلیت تفکیک موضوعی ندارد و راهکارهای پیشگیری از تهدیدات و مقابله با آن نیز در ساختاری منسجم و پیوسته جای می گیرد، لذا برای هر تهدید، امکان ارائه راهکاری مستقل وجود ندارد. به معنای دیگر، خنثی سازی تهدیدات مستلزم هماهنگی کامل در بخشهای پدافندی و IT و همچنین اتخاذ راهبردها و راهکارهای پیوسته و هماهنگ است. از این رو راهکارهای ذیل که برگرفته از نتایج حاصل از مصاحبه با متخصصین و خبرگان موضوع بصورت مصاحبه مستقیم و از طریق سوال مطروحه در پرسشنامه‌های می باشد مورد تشریح قرار می گیرد، اما بنابر توصیه متخصصین، پیشگیری از تهدیدات سایبری، مستلزم اجرای هماهنگ آنان است:

١. ارتقای دانش سایبری کشور و تربیت متخصص امنیت سایبری متناسب با تهدیدات نوین سایبری
٢. راه اندازی شبکه ملی اطلاعات
٣. اتخاذ سیاستهای بازدارنده و تدوین قوانین بازدارنده درحوزهٔ تروریزم سایبری و سرقت اطلاعات جهت تقابل با حملات سایبری در سطح بین المللی
٤. تدوین سند امنیت سایبر ملی مبتنی ترسیم پروتکل‌های دقیق امنیت سایبری و الزام اشخاص حقوقی و حقیقی به رعایت آن پروتکل‌ها
٥. تشکیل مرکز یا کمیته‌ای خاص جهت هماهنگی بین سازمانی در زمان بحرانهای سایبری گسترده نظیر حملات سایبری

۶. آموزش عمومی مردم درخصوص حفاظت و صیانت از اطلاعات خود و عضویت در شبکه های اجتماعی
۷. فرهنگ سازی عمومی درخصوص چگونگی برخورد با شایعات و اخبار منتشره در فضای مجازی
۸. بالابردن اعتماد ملی به حاکمیت درخصوص مدیریت اینترنت و شبکه های اجتماعی داخلی.
۹. آینده پژوهی درخصوص اولویت بندی تهدیدات سایبری
۱۰. توجه خاص به پدافند سایبر و اجرای دستورالعملهای پدافند سایبری
۱۱. بازدارندگی سایبری از طریق انجام حملات متقابل علیه دولتها یا گروههای مهاجم
۱۲. ارتقاء استانداردهای ایمنی زیرساخت‌های حیاتی و حساس کشور در برابر تهدیدات و آسیب پذیری های سایبری و به روزرسانی مستمر ان استانداردها
۱۳. بومی سازی تجهیزات و نرم افزارهای مورد کاربرد در ایجاد امنیت سایبری و زیرساختهای سایبری
۱۴. ایجاد محدودیت در بکارگیری سامانه های فنی غیر بومی در مراکز حساس و حیاتی
۱۵. توجیه و آگاه سازی مستمر سازمانهای موثر بر فضای سایبری و مجازی کشور در خصوص اهمیت و ضرورت رعایت دستورالعملهای پدافند غیر عامل سایبری با هدف ممانعت از کاهش حساسیت آنان در طول زمان
۱۶. فراهم نمودن سازوکارهای تشویقی و حقوقی به منظور ترغیب مراکز تحقیقاتی و شرکتهای دانش بنیان داخلی در تولید محصولات و سامانه های سایبری

منابع

- آزادی، جواد (۱۳۹۶/۱۱/۸) **تفاوت فضای سایبری و فضای مجازی**، قابل دسترسی در http://cpolicy.ir
- آسمانی، ناصر (۱۳۹۵) **آشنایی با مفاهیم کلان داده ها**، مدیریت آمار وفناوری اطلاعات دانشگاه علوم پزشکی تبریز
- آذرنیوار محمد (۱۳۹۹/۱/۲۳) **بلاک چین چین چیست؟** قابل دسترسی در https://arzdigital.com/what-is-blockchain-technology/
- احدی محمد. شاه محمدی محمد (۱۳۹۶) **طرح راهبردی دفاع سایبری جمهوری اسلامی ایران در حوزه بازدارندگی**، فصلنامه علمی پژوهشی مطالعات بین رشته‌ای دانش رهبردی، سال هشتم، شماره ۳۱، تابستان ۱۳۹۶ صص ۲۵۲-۲۲۵
- امیری، گلاره،۱۳۹۲، **بررسی ابزارها و عوامل زمینه ساز جنگ نرم به عنوان رویکردی سیاسی**، اولین کنفرانس بین المللی حماسه سیاسی (با رویکردی بر تحولات خاورمیانه) و حماسه اقتصادی (با رویکردی بر مدیریت و حسابداری)، رودهن https://civilica.com/doc/495669
- بابایی حسین (پژوهشگر حوزه امنیت سایبری)، مصاحبه مورخ ۱۳۹۹/۲/۲۲، با موضوع: **تهدیدات نوین سایبری**
- جعفری لاری. علی اصغر (۱۳۹٤) **امنیت سایبری و جنگ سایبری**، پندارپارس، تهران
- حسینی، پرویز. ظریف منش حسین (۱۳۹۲) **مطالعه تطبیقی ساختار دفاع سایبری کشورها**، فصلنامه پژوهش های حفاظتی حسین امنیتی دانشگاه جامع امام (علیه السلام) سال دوم شماره ۵، بهار ۹۲، صص ٦٨ - ٤١
- خانیکی، هادی. بابائی، محمود. (۱۳۹۰) **فضای سایبر مفهوم و شبکه های اجتماعی مفهوم و کارکردها**. فصلنامه علمی _پژوهشی جامعه اطلاعاتی شماره ۱ پائیز و زمستان صص ۷۱-۹٦
- خبرگزاری مشرق نیوز (۱۳۹۷/۸/۱٤)، **حمله سایبری علیه ایران دفع شد**، قابل دسترسی در https://www.mashreghnews.ir
- خبرگزاری مهر (۹۸/۹/۲٤) **حمله سایبری به سامانه های دولت الکترونیک دفع شد**، کد خبر ٤٧٩٧٨٧٤
- خلیلی پور، علی. نورعلی وند، یاسر (۱۳۹۰) **تهدیدات سایبری و تاثیر آن بر امنیت ملی**. فصلنامه مطالعات راهبردی، سال پانزده، شماره دو،
- خلیلی پور رکن آبادی، علی. نورعلی وند، یاسر (۱۳۹۱) **تهدیدات سایبری و تاثیر آن بر امنیت ملی**، فصلنامه مطالعات راهبردی، تابستان ۱۳۹۱، شماره مسلسل ٥٦، صص ۱٦٨-۱۹٦
- خلیلی علی و دیگران (۱۳۹۹) **معماری کلان فضای سایبر جمهوری اسلامی ایران با رویکرد دفاعی امنیتی**. مطالعات گروهی، دانشگاه عالی دفاع ملی _ دانشکده امنیت ملی
- دستوار محمد (۱۳۹٤) **بررسی تهدیدات سایبری بر امنیت زیرساختهای کشور**، کنفرانس بین‌المللی پژوهشهای کاربردی در فناوری اطلاعات کامپیوتر و مخابرات، تربت حیدریه، ۲۸ آبان ۱۳۹٤

- دهقانی، علی اصغر (۱۳۹٦) **بازدارندگی سایبری در امنیت نوین جهانی: تهدید سایبری روسیه و چین علیه زیرساختهای حیاتی آمریکا**، نشریهٔ رهیافتهای سیاسی و بین‌المللی، سال هشتم، شماره ۴، تابستان، صص ۱۲۱ _ ۱٤۷
- سند راهبردی پدافند سایبری کشور – مصوب ۱۳۹٤/۹/۲۲؛ **کمیته پدافند غیر عامل کشور**
- **سند راهبردی سیاست های کلی نظام در حوزه پدافند غیرعامل**، مصوب ۱۳۹٦/۸/۱۲، مجمع تشخیص مصلحت نظام
- شفیع پور. بنفشه، پورقهرمانی. بابک (۱۳۹۳)، **تهدیدهای سایبری علیه ایران و چالش های مقابله، همایش ملی ازران و چالشهای حقوق بین‌الملل**. مراغه، دانشگاه آزاد اسلامی
- عباسی قادی. مجتبی، خلیلی کاشانی. مرتضی، (۱۳۸۸)، **تاثیر اینترنت بر هویت ملی**، تهران، پژوهشکده مطالعات راهبردی
- زینده مراد حسین (۱۳۹۷/۵/۲۰) **رژیم حکمرانی اینترنت**، قابل دسترسی در https://cpolicy.ir/727
- کیانوش کریمی، جلال غفاری قدیر، ۱۳۹۷، **مدل تأثیرگذاری بر افکار عمومی در فضای مجازی به کمک قابلیت‌های بازی وارسازی**، فصلنامه مطالعات رسانه‌های نوین، سال پنجم، شماره ۱۷
- کریمی پاشایی، سجاد؛ و منعم، روح‌الله؛ و کاظمی‌پور، علی. (۱۳۹۴). **تحلیلی بر مولفه‌های دکترین سایبری کشورها (مطالعه موردی: جمهوری اسلامی ایران)**. فصلنامه پژوهشهای بین الملل، شماره ۱۵ (دوره ۵)، ۲۲۰-۱۹۳
- قلی پور حجت (پژوهشگر حوزه امنیت سایبری)، مصاحبه مورخ ۱۳۹۹/۲/۲۲، با موضوع: **تهدیدات نوین سایبری**
- ملک پور نیما (۱۳۹۸/۴/۲۵) **ارز دیجیتال چیست؟** قابل دسترسی در https://arzdigital.com/what-is-cryptocurrency/
- مرتضوی علی (پژوهشگر حوزه امنیت سایبری) مصاحبه مورخ ۱۳۹۹/۲/۱۷، با موضوع: **تهدیدات نوین سایبری**
- موسسه فرهنگی و مطالعات و تحقیقات ابرار معاصر تهران (۱۳۹۱) **امنیت و جنگ سایبری ۲**، موسسه ابرار معاصر تهران، تهران
- میردامادی، مهرداد (۱۳۸۰)، **فضای سایبرنتیک به مثابه فضای شهری**، پایان نامه کارشناسی ارشد تهران دانشگاه تهران دانشکده علوم اجتماعی
- هادی احمدرضا (پژوهشگر حوزه هوش دیجیتال)، مصاحبه مورخ ۱۳۹۹/۲/۲۲، با موضوع: **تهدیدات نوین سایبری**
- همشهری آنلاین (۱۳۹۱/۳/۹) **جزئیات جدید از ویروس مهاجم به صنعت نفت**، کدخبر ۱۷۲۴۸۱
- J. Andress and S. Winterfeld, (2011),Cyber Warfare**: Techniques, Tactics and Tools for Security Practitioners, Elsevier Syngress**
- CACI International Inc. and U.S Naval Institute (July ۲۰۱۰); "**Cyber Threats to National Security, Symposium One: Countering Challenges to the Global Supply Chain**", www.caci.com,2011/05/20

- *Lord and Sharp, Travis (2011); "**America's Cyber future Security and Prosperity in the Information Age**",Center for a New American Security, Volume I*
- *Cornish, Paul&Livingstone, David.(2011) "On Cyber Warfare" www.chathamhouse.org.uk.*
- *Gartzke, Erik. "**The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth.**" Quarterly Journal: International Security, vol. 38. no. 2. (Fall 2013): 41-73*
- *Kello, Lucas. (2013). The Meaning of the Cyber Revolution: perils to theory and statecraft, International Security, vol 38*
- *New Zealand, New Zealand Cyber Security Strategy,2011*
- *Junio, Timothy J, "**The politics and strategy of cyber conflict**" (2013). Dissertations available from ProQuest. AAI3609184.*
- *William J.Board , Jogn Markoff and David E.Sanger(Jan. 15, 2011) Israeli Test on Worm Called Crucial in Iran Nuclear Delay , NewYork Times*