سنجش تهدیدات سایبری

علی عبداله خانی[1]

پرویز حسینی[2]

تاریخ دریافت: ۹۳/۱۲/۱۲ **تاریخ پذیرش: ۹٤/۰۲/۲۰**

چکیده

امروزه توجه به مخاطرات امنیتی فضای سایبر یعنی واقع‌شدن در وضعیتی که بتوان از آسیب‌پذیری ارکان نظام در مواجهه با تهدیدات داخلی و خارجی حوزه سایبر فروکاست، از عنایت ویژه‌ای برخوردار است. دلیل این توجه از یک‌سو متأثر از رشد روزافزون وابستگی جوامع به فضای سایبر به‌عنوان بستر اصلی اطلاعات و از سوی دیگر گوناگونی تهدیدات در حوزه مذکور است. با سنجش تهدیدات سایبری می‌توان توجه مسئولین فضای سایبر را به قسمت‌هایی معطوف کرد که ازنظر امنیتی در وضعیت مناسبی قرار نداشته و می‌توانند آسیب‌های جدی به اهداف مرجع و دارائی‌های کلیدی حوزه سایبر وارد نموده و پیامدهای خطرناکی را در پی داشته باشند. در این تحقیق که باهدف سنجش تهدیدات سایبری انجام گرفت، وضعیت و میزان تهدیدات خطرناک امنیتی سایبری مشخص گردید. بر این اساس اهداف مرجع و دارائی‌های کلیدی حوزه سایبر ازنظر امنیتی در برابر بعضی از تهدیدات سایبری در وضعیت هشدار قرار داشته که توجه بیشتری را می‌طلبد.

واژه‌های کلیدی:

تروریسم سایبری، تهدیدات سایبری، جاسوسی سایبری، جرائم سایبری، جنگ سایبری، سنجش تهدید، صدمه سایبری

---

[1] استاد دانشگاه عالی دفاع ملی

[2] نویسنده مسئول و دانشجوی دکتری امنیت ملی، دانشگاه عالی دفاع ملی

۵.۲. مقدمه:

امنیت و ناامنی از موضوعات دیرینه‌ای است که هم‌زمان با داستان آفرینش و پس‌ازآن با هبوط انسان به زمین مطرح بوده و از این حیث دغدغه‌ای مهم ارزیابی می‌شود. سیر تحول جوامع بشری نیز حکایت از آن دارد که امنیت کالایی عمومی و بس ارزشمند است که تمامی ملت‌ها و دولت‌ها در پی تحصیل و تقویت آن هستند. (افتخاری، ۱۳۹۱: ۲۰) امنیت واژه‌ای مبهم بوده و تاکنون تعریف جامع‌ومانعی از آن، ارائه نشده است. در مقابل امنیت تهدید قرار دارد که امنیت را به مخاطره می‌اندازد. ره‌پیک تهدید را یک امر ثانوی می‌داند زیرا اول مبنای امنیت و ارزش به خطر می‌افتد و در این صورت تهدید به وجود می‌آید. (ره‌پیک، ۱۳۹۰)

نیمه‌ی پایانی قرن بیستم و پس از جنگ جهانی دوّم، دوره‌ی طلایی دانش و فنّاوری بشر و دوره‌ی انتقال از عصر صنعت و ماشین به عصر فنّاوری اطلاعات است. توسعه‌ی شبکه‌ها با کارکردهای نظامی در ابتدا و به دنبال آن توسعه و تعریف کارکردهای جدید و ایجاد امکان اتّصال مراکز دانشگاهی، پژوهشی، علمی و تبادل اطلاعات با یکدیگر در این نیمه اتّفاق افتاده است. تجاری‌سازی فنّاوری اطلاعات و ارتباطات و به‌تبع آن کاهش هزینه‌های رایج و امکان استفاده‌ی عموم از این فنّاوری، اینترنت را به معنای امروز آن در دهه‌ی پایانی قرن بیستم به مردم معرفی نمود و امروزه این فنّاوری عظیم با میلیاردها رایانه، میلیون‌ها خدمات‌دهنده و صدها هزار شاه‌راه ارتباطی اصلی در برابر بشر قرار دارد تا از مواهب و مزایای بی‌بدیل آن استفاده کند و یا خود را با پلیدی‌ها و آسیب‌های آن به نابودی کشد. فنّاوری اطلاعات و ارتباطات ضمن تأثیرگذاری بر تمامی جنبه‌ها و شئون زندگی اجتماعی بشر، بر جرائم، تهدیدها و آسیب‌ها نیز تأثیر گذاشته است. تهدیدات سایبری در چنین فضائی بروز و ظهور پیدا کرده است و شناخت تهدیدات سایبری، تشخیص و ارزیابی ماهیت، نوع، شدت، دامنه و عمق آن در دستیابی به امنیت مطلوب و موردنظر در جامعه مبتنی بر فناوری امروزی می‌تواند تأثیر بسزایی داشته باشد.

۵.۳. بیان مسئله:

تهدید ذاتاً مبهم و نامعلوم بوده و شناسایی آن بسیار دشوار است. بوزان معتقد است اکثر تهدیدات موجود درصحنه جهانی شامل تعداد زیادی عوامل پیچیده‌اند که برآیند و نتایج آن‌ها را به‌شدت نامعلوم می‌سازند. (بوزان، ۱۳۷۸: ١٦٦)

شناسایی و سنجش اهمیت، شدت و دامنه تهدیدات مطرح علیه یک کشور و نظام سیاسی از

موضوعات مهمی است که به دلیل اهمیت و ضرورت این موضوع در تعیین راهبردها و سیاست‌ها، تخصیص منابع و اتخاذ تدابیر لازم، از دغدغه‌های همیشگی مسئولین و سیاست‌مداران و اداره‌کنندگان کشورها بوده است. ازاین‌رو، تهیه الگو و مدل‌های کارآمد برای این فرایند، همواره موردتوجه بوده است.

با گسترش روزافزون استفاده از رایانه در دنیا، تشکیل و گسترش فضای مجازی و غیر فیزیکی به وقوع پیوسته است که ورود به این فضا ناگزیر هر فرد و جامعه‌ای است. اکنون با استفاده همه‌جانبه از رایانه‌ها، فضای سایبر گستره بسیار زیادی پیدا کرده است و در این فضا اطلاعات ارزشمندی تولید، پردازش، نگهداری و توزیع می‌شود که همواره در معرض تخریب، دست‌کاری، سرقت و افشاء قرار دارد.

تاکنون اقدامات و تلاش‌های مؤثری برای ارزیابی و سنجش تهدیدات که فوق‌العاده مهم و حیاتی می‌باشند صورت پذیرفته، لیکن جهت سنجش و ارزیابی تهدیدات سایبری و فاکتورهای اساسی آن کار جدی و قابل توجهی انجام نگرفته و در دست نیست.

گستردگی استفاده از فضای سایبر باعث به وجود آمدن تهدیدات متعدد در این فضا شده است که ضرورت سنجش تهدیدات برای ارزیابی و سنجش شدت، دامنه، میزان وقوع تهدیدات سایبری بیشتر نمود می‌یابد. مسئله‌ای که ذهن محقق را به خود مشغول نموده این است که تهدیدات سایبری در چه وضعیتی قرار دارد تا علاوه بر تعیین شدت، دامنه و میزان تهدیدات، نسبت به رفع اشکالات و ارتقاء امنیتی فضای سایبر اقدام نمود. لذا این تحقیق بر آن است که با بررسی الگوهای موجود، به سنجش تهدیدات سایبری بپردازد.

۵.٤. اهمیت و ضرورت انجام تحقیق:

سنجش تهدیدات می‌تواند نقش مؤثری در محاسبه‌ی احتمال وقوع تهدید و ارزیابی شدت آن ایفاء نموده و در سیاست‌گذاری موضوعات امنیتی نقش تأثیرگذاری داشته باشد.

با توجه به گسترش تهدیدات سایبری علیه نظام مقدس جمهوری اسلامی ایران در سال‌های اخیر و عدم سنجش تهدیدات سایبری، ارزیابی مناسبی درباره احتمال وقوع و شدت تهدیدات سایبری در دست نیست. لذا این پژوهش می‌تواند کمک مؤثری در ارزیابی بهتر و دقیق‌تر تهدیدات سایبری به دولت‌مردان باشد تا در اتخاذ تدابیر و تصمیمات خود با آگاهی بیشتری عمل نموده و به‌موقع، تصمیمات مقتضی را برای حفظ امنیت و مصالح و منافع ملی کشور اتخاذ نمایند.

فقدان سنجش و ارزیابی تهدیدات سایبری می‌تواند:

۱- روند صحت و کارآمدی تصمیمات را دچار مشکل نماید.

۲- مقابله با تهدیدات سایبری و به‌تبع آن نظام سیاسی را با مشکل مواجه سازد.

۳- آمادگی برای مقابله با تهدیدات سایبری را کاهش دهد.

و در مقابل سنجش تهدیدات سایبری می‌تواند:

۱- باعث تحلیل‌های منطقی، کارآمد و هشداردهنده به سیاست‌گذاران شود.

۲- منجر به اتخاذ تدابیر مناسب دفاعی و هجومی جهت مقابله با تهدیدات سایبری گردد.

۳- به تکمیل مباحث نظری سنجش تهدیدات سایبری کمک نماید.

۵.۵. روش‌شناسی تحقیق:

هدف تحقیق:سنجش تهدیدات سایبری

سؤال تحقیق:وضعیت و میزان تهدیدات خطرناک امنیتی سایبری در چه حدی است؟

این تحقیق به روش توصیفی و با بررسی اسناد و مدارک علمی[1] و مصاحبه با خبرگان، با رویکرد کاربردی و توسعه‌ای انجام شده و برای انجام تحقیق، جمع‌آوری اطلاعات به روش کتابخانه‌ای تخصصی و میدانی صورت گرفته و اطلاعاتِ موردنیاز از طریق جستجوی کتابخانه‌ای، اینترنتی و مصاحبه با صاحب‌نظران به‌دست‌آمده است. روش بکار رفته برای تحلیل مباحث در این تحقیق، روش «تکیه بر موضوعات نظری و تجربیات صاحب‌نظران» با هدف دست یافتن به دیدگاه‌های جدید و ژرف‌نگری در وضعیت و میزان تهدیدات خطرناک امنیتی سایبری است.

نوع تحقیق:با توجه به ماهیت موضوع تحقیق و استفاده‌ای که می‌توان از نتایج حاصله در راستای بهینه نمودن مدیریت تهدیدات سایبری و شناخت ابعاد تهدیدات سایبری و ارزیابی احتمال وقوع و شدت آن بُرد، این تحقیق از نوع کاربردی-توسعه‌ای با تأکید بر جنبهٔ کاربردی آن، است.

۵.٦. جامعه آماری، جمعیت نمونه و روش نمونه‌گیری:

جامعه آماری، خبرگان و مدیران موجود در حوزه سایبر و امنیت فضای سایبر بودند که در قالب نمونه‌گیری به روش گلوله برفی تا رسیدن به اشباع نظری نمونه‌گیری انجام شد.

[1] – Document & Archival Method

با توجه به اینکه در این تحقیق از روش گلوله برفی استفاده شد، از تعداد ۱۰ نفر دکتری، دانشجوی دکتری و کارشناسی ارشد مصاحبه انجام شد تا اینکه اشباع نظری حاصل گردید. تمام صاحب‌نظران دارای تحصیلات، تجربه مدیریتی و سابقه اجرائی در حوزه سایبر و امنیت فضای سایبر بودند.

۵.۷. ادبیات تحقیق:

۵.۸. ۱.۵. امنیت

امنیت به معنای «ایمن شدن، در امان بودن و بی‌بیمی»، (معین، ۱۳۶۳: ۳۵۲)، «ایمنی، آرامش و آسودگی» (عمید، ۱۳۷۹: ۲۳۳) و «اطمینان و آرامش خاطر» (المنجد، ۱۹۷۳: ۱۸) بیان شده است. در فرهنگ آکسفورد، امنیت به معنای «در حفظ بودن، فراغت از خطر یا اضطراب و تشویش» آمده است. (Oxford, 1997) فرهنگ لغات و بستر نیز مفهوم امنیت را کیفیت احساس تأمین و احساس دوری از خطر، ترس و عدم اطمینان بیان نموده است. (Webster, 2001) «ریشه امنیت در لغت از امن، استمان، ایمان و ایمنی است که به مفهوم آرامش در برابر خوف و ترس و نگرانی و ناآرامی است. به عبارت دیگر امنیت را به اطمینان و فقدان خوف تفسیر، تعریف و ترجمه کرده‌اند. که تاحدودی زیادی به واقعیت نزدیک و شامل دو بعد ایجابی و سلبی در تعریف است. از یک‌سو اطمینان، آرامش فکری و روحی و از سوی دیگر فقدان خوف دلهره و نگرانی که موجب سلب آرامش و اطمینان می‌گردد». (دری، ۱۳۷۹:۲۸۲)

«از گذشته تا به حال تلاش‌های زیادی جهت تعریف امنیت انجام گرفته است؛ برخی امنیت را فقدان تهدید تعریف کرده‌اند. بعضی امنیت را مترادف با صلح تعریف کرده‌اند و معتقد گشتند امنیت جنبهٔ تأمین دارد. برخی دیگر معتقد شده‌اند فقدان تهدید نسبت به منافع ملی یک کشور مساوی با امنیت است» (عبدالله‌خانی، ۱۳۸۵: ۱۲۳).

امنیت در فضای داشته‌ها و خواسته‌های بازیگران مطرح است. به بیان دیگر امنیت وقتی معنا می‌یابد که مجموعه‌ای از بازیگران با یکدیگر ارتباط پیدا کرده و داشته‌ها و خواسته‌های آنان در ارتباط باهم معنا یابند. (عبداله‌خانی، ۱۳۸۲: ۲۶۰) داشته‌ها درواقع دارایی‌ها و به بیان کلی‌تر منافع بازیگران قلمداد می‌شود و خواسته‌ها به انتظارات و به بیان کلی‌تر اهداف بازیگران قابل تعریف است.

در تعریف امنیت می‌توان به این نکته اشاره نمود که «در ادبیات روابط بین‌الملل، امنیت غالباً

به معنی احساس آزادی در تعقیب اهداف ملّی و فقدان ترس و خطر جدی **از خارج نسبت به منافع اساسی و حیاتی کشور آمده است» (بهزادی، ۱۳٦۸: ۱۰٤)** و ریچارد کوپر می‌گوید: «امنیت به معنی توان جامعه در حفظ و بهره‌گیری از فرهنگ و ارزش‌هایش است». وی برای امنیت دو جنبه قائل است: «شرایط عینی و برداشت‌های ذهنی». شرایط عینی عبارتنداز عوامل فیزیکی و وضعیتی که کمترین بایستگی‌ها را برای تأمین امنیت کشور معین می‌کنند. برداشت‌های ذهنی نیز پدیده‌هایی هستند روانی که ممکن است حتی باوجود شرایط عینی، وجود نداشته باشند. (بوزان، ۱۳۷۸: ۱٤)

۵.۹. تهدید

ارائه یک تعریف دقیق از تهدید به دلیل چندوجهی بودن و ارتباطش با امنیت، منافع و اهداف و استراتژی‌ها، پیچیده و مشکل است. تهدید در لغت به معنای بیم دادن، ترسانیدن و عقوبت کردن است. فرهنگ معین تهدید را ترسانیدن و بیم دادن معنی کرده است و لرنر تهدیدات را عبارت از هر چیزی که بتواند ثبات و امنیت را در یک کشور به خطر اندازد، دانسته و معتقد است تهدیدات، منافع را هدف قرار می‌دهند. مفهوم تهدید در نگرش سیستمی، عدم تعادل در سیستم، بیان شده است. یعنی عاملی که اجازه نمی‌دهد سیستم به اهداف خویش برسد. در پاره ای از متون نیز تهدید به معنای توانایی‌ها، نیات و اقدامات دشمنان بالفعل و بالقوه برای ممانعت از دستیابی خودی به مقاصد امنیتی، تعریف شده است. (عبداله‌خانی، ۱۳۸۲: ۸٤)

از نظر اولمان، نوع و شدت تهدید، دو عنصر اصلی تهدید امنیتی محسوب می‌شوند. با توجه به این تعریف، به نظر می‌رسد تهدید، زمانی تبدیل به یک موضوع امنیتی می‌شود که با سه موضوع: مردم، کشور و حکومت در ارتباط باشد. «هم‌چنین می‌توان تهدیدات امنیتی را تهدیداتی دانست که اهداف و ارزش‌های حیاتی یک کشور را به‌گونه‌ای در معرض خطر قرار دهند که در آن‌ها، تغییر ماهوی و اساسی صورت پذیرد. تهدیدات را می‌توان میزان توانمندی‌های حریف نیز دانست. این توانمندی‌ها، عمدتاً از ابعاد سیاسی- نظامی برخوردار بوده و علیه یک نظام به کار می‌روند.»(درویشی، ۱۳۷٤: ۱٤٦)

در نگاه سنتی به امنیت و تلقی آن به‌عنوان «وضعیت مبنی بر نبود تهدید» فرض این است که تهدید مفهومی واضح و شفاف است. اما این رویکرد در پی تحول جوامع بشری و ظهور اذهان نقادی که خواهان دستیابی به تعاریفی دقیق و مستقل از واژگان و پدیده‌ها بودند، به‌شدت مورد نقد واقع

شده و لذا مباحث زبان‌شناسانه‌ای مطرح می‌شود که از معنا و مصداق تهدید پرسش می‌نماید. در این چشم‌انداز است که ابهام واژه امنیت نه‌تنها کمتر از امنیت ارزیابی نمی‌شود، بلکه به‌مراتب پیچیده‌تر و مبهم‌تر معرفی می‌گردد. (افتخاری،۱۳۸۵: ۲٦۰)

معناسازی تهدید با قدرت حمله یکی دیگر از تعاریف است. از نگاه دیوید بریور[1]، بر این اساس تهدید عبارت است از «سنجش قدرت حمله که با توجه به پارامترهایی نظیر توانایی و انگیزه تهدیدگر یا مهاجم و چگونگی اعمال آن بیان می‌گردد». (عبدالله‌خانی، ۱۳۸٦: ۲٤)

۵.۱۰. فضای سایبری[2]

ویلیام گیبسون در رمان علمی تخیلی نورومنسر (۱۹۸٤) اصطلاح فضای سایبر را ابداع نمود. (Gibson،۱۹۸٤: ٦۹) گیبسون در شرایطی که شبکه‌ها و سامانه‌های کامپیوتری جهانی امروزی نبود فضای سایبری را این‌گونه معرفی کرد: «فضای سایبر یک توهم مورد وفاق است که روزانه میلیاردها اپراتور و کودکانی که مفاهیم ریاضی به آن‌ها داده می‌شود آن را تجربه می‌کنند. فضای سایبر نوعی بازنمایی گرافیکی از داده‌هایی است که از بانک‌های تمامی کامپیوترها در سیستم انسانی تصویرسازی شده است. پیچیدگی‌ای که قابل‌تصور نیست». (بل، ۲۰۰۱: ٤٦)

فضای سایبری استعاره‌ای برای تشریح سرزمین غیرفیزیکی، تشکیل شده توسط سیستم‌های کامپیوتری است. برخلاف فضای حقیقی، سیر و گشت در این سرزمین بدون هیچ‌گونه حرکت فیزیکی مقدور است، تنها با حرکت موشواره یا فشردن کلیدی در صفحه‌کلید. (سیدمفیدی، ۱۳۸۳: ٦)

در بعد چیستی فضای سایبر از دیدگاه سخت‌افزاری، شبکه‌ای جهانی از کامپیوترهای به‌هم‌پیوسته است که از طریق کانال‌های ارتباطی پرسرعت تارعنکبوتی را شکل داده که سریع‌تر از مصنوعات دیگر انسان در حال گسترش است. ارتباطات سریع قابلیت ارسال پیام؛ ارائه سرویس‌های ارتباطی؛ تبادل اطلاعات با فرمت‌های مختلف از خدمات متنوع این ابر شبکه است. اینترنت به‌عنوان یکی از جلوه‌های فضای سایبر، قابلیت‌های ویژه‌ای را برای تجارت الکترونیکی، بازاریابی، تبلیغات و بانکداری الکترونیکی پدید آورده است. (Mutula،۲۰۰۷: ۱۵).

در سطح معنایی فضای سایبر، فضای مجازی افراد و کاربران در شبکه‌های اجتماعی، محیط‌های

[1] David Brewer
[2] Cyber Space

گفتگو، فروشگاه و... با یکدیگر ارتباط برقرار نموده، به گشت‌وگذار، خرید فروش، بحث و تبادل‌نظر می‌پردازند بدون اینکه هیچ‌گونه حرکتی داشته باشند. فضای سایبر برای توصیف هر مفهومی که در ارتباط با شبکه‌های رایانه‌ای، فناوری اطلاعات، اینترنت و جامعه اطلاعاتی بکار برده شده و افراد و کاربران این فضا تجربه اجتماعی از تعامل، تبادل و اشتراک‌گذاری اطلاعات، کسب‌وکار، بازی و تفریح، بحث‌های گروهی که به‌صورت غیر فیزیکی است، دست پیدا می‌نمایند. فضای سایبر چیزی فراتر از اینترنت است که اینترنت این مفهوم را در حال گسترش دادن است. با شکل‌گیری فضای سایبر و رشد سریع آن مفاهیم عرصه زندگی نیز به سمت تغییر ماهوی گام برمی‌دارد. همه‌چیز از هویت، فرهنگ، حکمرانی، روابط و تعاملات خصوصی و گروهی در حال تغییر است. فضای سایبری یکی از ویژگی‌های زندگی مدرن است که در آن افراد و جوامع در سراسر جهان باهم مرتبط شده و معاشرت و همکاری می‌نمایند. (DOD، ۲۰۱۱: ۱)

۵.۱۱. زیرساخت حیاتی فضای سایبری

تعیین عناصر فضای سایبری که باید تمرکز امنیت سایبری بر آن‌ها باشد دارای اهمیت اساسی است. یک مجموعه از مؤلفه‌ها که توافق سراسری در مورد آن وجود دارد، شامل آن‌هایی است که با زیرساخت حیاتی کشور مرتبط هستند. ازجمله این موارد عبارتنداز:

۱- **صنایع تولیدی**: انرژی، شیمیایی، پایگاه‌های صنعتی دفاعی.

۲- **صنایع خدماتی**: بانکداری و مالی، حمل‌ونقل، پست و ارسال محموله.

۳- **تغذیه و بهداشت**: کشاورزی، غذا، آب و بهداشت عمومی.

٤- **ملی و دولتی**: خدمات دولتی و اورژانس.

۵- **فناوری اطلاعات و سایبر**: اطلاعات و مخابرات. (Fischer، ۲۰۰۵: ٥٦)

۵.۱۲. تهدیدات سایبری[1]

مخاطرات موجود در فضای سایبری را تهدید سایبری گویند. فضای سایبری به‌مانند فضای حقیقی و ژئوپلیتیکی دارای تهدیدها و آسیب‌پذیری‌هایی است که انسان در برخورد با آن شرایطی را برای مصونیت در یک چرخه دائمی‌شکل می‌دهد. فضای سایبر هم از آن جهت که همه امور آدمی را در برمی‌گیرد و هم ازآن‌جهت که مبانی انسان‌شناختی فضای تولید تکنولوژی و محتوی را در برگرفته

[1] Cyber Threats

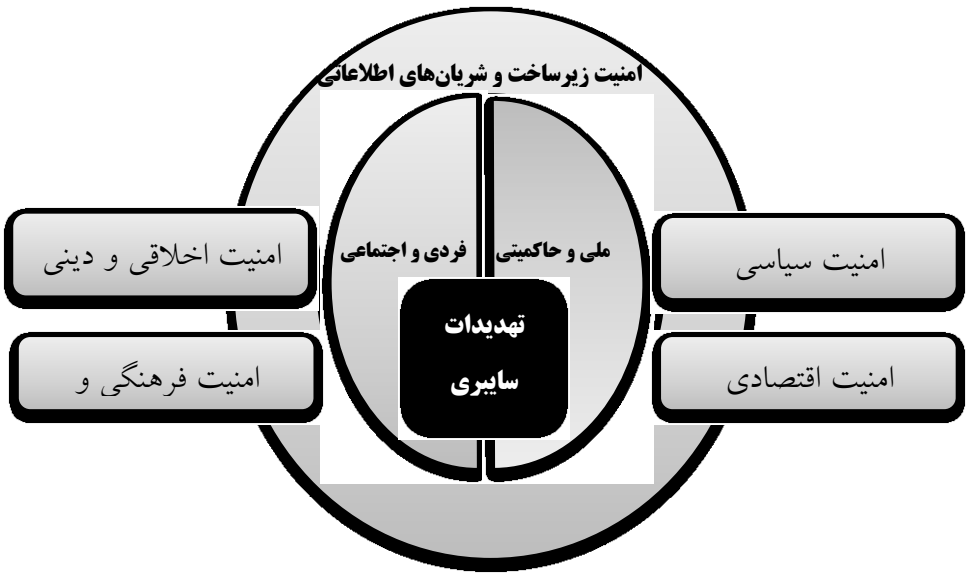
مخاطراتی را متوجه انسان و جامعه می‌نماید.

تهدیدات سایبری نیازمند سه سطح امنیت به قرار زیر است.

سطح اول امنیت در فضای سایبر، امنیت در حوزه زیرساخت و شریان‌های اطلاعاتی است. وابستگی به شبکه‌های پرسرعت و پردازشگرهای قدرتمند روزبه‌روز افزایش می‌یابد که سیستم‌ها را در معرض مخاطراتی از آتش و طوفان تا بزهکاری و تروریسم سایبری قرارداده، که نیاز به مدیریت و نظارت دارد. (کیان‌خواه،۱۳۸۹: ۳۵) در دنیای جدید، مهم‌ترین عامل قدرت، حفاظت از اطلاعات در مقابل تهدیدات، تبادل و اشتراک‌گذاری امن اطلاعات در جهت افزایش توانمندی است. جنگ اطلاعاتی، تروریسم سایبری و نفوذگرها ازجمله این تهدیدات است و بومی‌نبودن و عمل نمودن به دستورات صاحبان تکنولوژی منجر به افزایش تأثیرگذاری تهدیدات زیرساخت و شریان‌های اطلاعاتی شده است.

سطح دوم امنیت در فضای سایبر، امنیت در حوزه فرد و اجتماع است. ابعاد چالش در بعد فردی و اجتماعی موجب طرح‌ریزی امنیت فرهنگی و هویتی و امنیت اخلاقی و دینی می‌شود. امنیت اخلاقی و هویتی فرد و اجتماع در فضای سایبر حافظ دین و اخلاق انسان پایبند به فطرت الهی است. امنیت فرهنگی و هویتی، حافظ انسانیت انسان است که هویت و فرهنگش ریشه در آداب و سننی است که بر اساس ویژگی‌ها و نژاد و قومش شکل‌گرفته است.

سطح سوم امنیت در فضای سایبر، امنیت در حوزه ملی و حاکمیتی است. تهدیدات در حوزه ملی و حاکمیتی، مجموعه تهدیداتی است که حیاتی‌ترین منافع ملی و حاکمیتی یک نظام را به چالش می‌کشاند. این حوزه از تهدیدات بخشی در حوزه زیرساخت و شریان‌های اطلاعاتی قرار داشته و بخشی در حوزه امنیت سیاسی و اقتصادی است. فضای سایبری که ذاتاً ابزاری برای تعامل و ارتباط افراد و جوامع است فضایی را برای جنگ روانی ایجاد می‌نماید. در این جنگ اطلاعات علیه فکر و ذهن افراد استفاده می‌شود و منجر به عملیات علیه اراده ملی، عملیات علیه عناصر نظامی، ایجاد تضاد فرهنگی و ایجاد تنش و هرج‌ومرج می‌شود. (آلبرتس،۱۳۸۵: ۱۰٤) در بعد اقتصادی، تحریم‌های اطلاعاتی در حال بروز چالش جدید در تبادلات اقتصادی است و منجر به آسیب رسیدن در تعاملات اقتصادی کشورها شود.



(کیان‌خواه، علوی‌وفا، ۱۳۸۹: ۸)

۵.۱۳. جنگ سایبری[1]

جنگ سایبری عبارت است از حالت تشدید برخورد سایبری مابین کشورها که در آن حملات سایبری به‌وسیله عوامل یک کشور به‌عنوان بخشی از عملیات جنگی علیه زیرساخت سایبری کشور دیگر انجام می‌شود، که ممکن است به‌صورت رسمی به‌وسیله مسئولین یک‌طرف مخاصمه اعلان شود، یا آنکه به‌طور رسمی اعلان نشود. (Rauscher، ۲۰۱۱: ۸۳)

جنگ سایبر به قصد کارهای سیاسی و یا آرمانی انجام می‌گیرد و مکان‌ها و تأسیسات حیاتی مانند انرژی، حمل‌ونقل، ارتباطات، سرویس‌های ضروری (مانند پلیس و خدمات پزشکی) را هدف قرار می‌دهد و از شبکه‌های کامپیوتری به‌عنوان بسترهایی جهت انجام این اعمال خرابکارانه استفاده می‌کند. (سازمان پدافند، بی‌تا: ۵)

۵.۱٤. تروریسم سایبری[2]

تروریسم را این‌گونه تعریف می‌کنند: به‌کارگیری خشونت علیه اشخاص، دولت‌ها یا گروه‌ها برای

[1] Cyber warfare
[2] cyber terrorism

پیشبرد زورمندانه اهداف سیاسی یا عمومی. سایبر تروریسم در حقیقت همان تعریف را دارد، با این تفاوت که این بار هدف متمرکز روی منابع موجود در فضای مجازی است. سایبر تروریسم می‌تواند ابعاد داخلی داشته باشد یا شامل موارد بین‌المللی شود. سایبر تروریسم امروز خطرناک‌تر از تروریسم سنتی است به این دلیل که ساختار اقتصادی و خدمات‌رسانی بسیاری از کشورها مبتنی بر فناوری‌های اطلاعاتی و ارتباطی شده است با این توضیحات می‌توان سایبر تروریسم را چنین تعریف کرد: "اقدامات برنامه‌ریزی شده و هدفمند با اغراض سیاسی و غیرشخصی که علیه رایانه‌ها و امکانات و برنامه‌های ذخیره‌شده در درون آن‌ها از طریق شبکه جهانی صورت می‌گیرد و هدف از چنین اقدامی نابودی یا وارد آوردن آسیب‌های جدی به آن‌هاست." به‌عبارت‌دیگر تروریسم سایبری عبارت است از استفاده از فضای سایبری در جهت مقاصد تروریستی، به‌صورتی که در قوانین ملی یا بین‌المللی تعریف شده است. (Rauscher، ۲۰۱۱: ۱۱۲)

با توجه به مطالب ذکر شده درباره سایبر تروریسم، می‌توان ویژگی‌هایی مانند: هدف قرار دادن تعداد بیشتری از مردم، استفاده از گروه‌های رایانه‌ای ناشناخته در سطح بین‌المللی، نداشتن محدودیت جغرافیایی، پنهان ماندن هویت، تبلیغ و عضوگیری بین‌المللی، گسترش دامنه تروریسم به مسائل مالی بانکی و اقتصادی و خدمات شهری برای آن ذکر کرد.

۵.۱۵. جاسوسی سایبری[1]

جاسوسی سایبری عبارت است از پیگرد، تحلیل و مقابله با تهدیدهای امنیتی در فضای سایبری. این نوع جاسوسی ترکیبی از خبرگیری و دفاع فیزیکی با فناوری‌های مدرن اطلاعاتی است. اقدامات جاسوسی سایبری شامل ویروس‌ها، هکرها و تروریست‌ها است که در فضای سایبری باهدف سرقت اطلاعات حساس فعالیت می‌کنند. (www.wisegeek.com)

جاسوسی سایبری به معنای عام آن یعنی به دست آوردن اطلاعات سری بدون اجازه مالک آن؛ حال در معنی خاص این مالکیت می‌تواند درزمینه‌های مختلف تعریف و نیز به مالکیت‌های متفاوت تعمیم داده شود.

انحصار این مالکیت‌ها نیز می‌تواند فردی، سازمانی، حزبی و دولتی باشد. درزمینه دولتی این جاسوسی سایبری خود تقسیم‌بندی‌های مختلف دارد که می‌توان سه دسته سیاسی، اقتصادی و

[1] cyber intelligence

نظامی را از مهم‌ترین آن‌ها دانست.

۵.۱٦. جرائم سایبر[1]

هرگونه دخل و تصرف غیرمجاز از طریق ورود یا خروج، ضبط و ذخیره، پردازش و کنترل داده‌ها و نرم‌افزارهای رایانه‌ای و ایجاد یا واردکردن انواع ویروس‌های رایانه‌ای و امثال آن جرم محسوب می‌شود. (سازمان پدافند، بی‌تا: ۵)

هم‌زمان با توسعه و کاربردپذیری رایانه و سیستم‌های رایانه‌ای، جرائم رایانه‌ای هم به وجود آمده‌اند. اگرچه دامنه و حوزه‌ی وقوع جرم در هر حوزه با توجّه به ویژگی‌ها و وسعت کاربرد و استفاده متفاوت بوده است. از سال ۱۹٦۰ میلادی تاکنون سه نسل از جرائم رایانه‌ای برشماری شده‌اند. نسل اوّل که مقارن سال‌های دهه‌ی هشتاد، هفتاد و اوایل دهه‌ی هشتاد میلادی است و چون استفاده از اینترنت در آن زمان شیوع نداشت، عمده‌ی جرائم مرتبط با رایانه‌ها بود و ازاین‌رو این دسته از جرائم صرفاً به «جرائم رایانه‌ای» یاد می‌شوند. نسل دوّم جرائم رایانه‌ای از اوایل دهه‌ی هشتاد تا اوایل دهه‌ی نود به وقوع پیوستند که به «جرائم علیه داده‌ها» تعبیر می‌شوند. در این نسل، «داده» صرف‌نظر از این‌که در رایانه قرار داشته باشد، در واسط‌ها و ابزارهای انتقال مورد توجّه قرار گرفت و دیگر تأکیدی بر رایانه نبود. نسل سوّم رایانه‌ای نیز هم‌زمان با فراگیر شدن اینترنت از اوایل دهه‌ی ۱۹۹۰ میلادی به وجود آمدند. این جرائم که با گسترش کاربرد شبکه و اینترنت به وجود آمدند نام «جرائم سایبری» را به خود گرفتند. (www.syberpolice.ir)

۵.۱۷. صدمه سایبری[2]

هکتیویسم که از آن به صدمه سایبری یا آسیب سایبری تعبیر می‌شود، ترکیبی از کلمات هک (hack) و اکتیویسم (activism) است. منظور از هک یا نفوذ، به عملی که هر شخص یا برنامه‌ای که انجام می‌دهد تا بدون اجازه وارد یک دستگاه شود، گفته شده و عملیات و اقداماتی است که رایانه‌ها را به شیوه‌های غیرمعمول مورداستفاده قرار می‌دهند. این شیوه عموماً غیرقانونی و با استفاده از نرم‌افزارهای خاصی (ابزارهای هک) صورت می‌گیرد.

هکتیویسم شامل نافرمانی مدنی الکترونیکی است که مقدمه‌های نافرمانی را به فضای سایبر می‌کشاند.

---

[1] Cyber crime
[2] Hacktivism

هکتیویسم‌ها از برنامه‌نویسی رایانه‌ای، شبکه و مبادلات اینترنتی برای انجام آشوب‌های سیاسی در اینترنت سود می‌برند. این آشوب‌ها می‌تواند از حملات به‌قصد متوقف ساختن (DOS[1])، وب سایت‌ها تا سرقت و انتشار اطلاعات خصوصی در اینترنت، متنوع باشد برخی از محققان طیف اقدامات هکتیویسم‌ها را به چهار قسم تقسیم کرده‌اند:

۱) تحصن‌ها و محاصره‌های اینترنتی و مجازی

۲) بمب‌های اتوماتیک ایمیلی

۳) هک کردن وب سایت‌ها

٤) ورود به رایانه و استفاده از کرم‌ها و ویروس‌های رایانه‌ای. (http://www.aftabir.com)

۵.۱۸. مراحل یک حمله سایبری

۱- ابتدا یک هدف مشخص تعیین می‌شود که می‌تواند قسمتی از یک زیرساخت حیاتی مانند شبکه راه‌آهن، شبکه برق، شبکهٔ ATM و یا وب سایت‌های دولتی باشد.

۲- مهاجم‌ها شروع به جمع‌آوری اطلاعات می‌کنند.

- از طریق شبکه اینترنت/ مقالات/ مطالعات و ...
- از طریق وب سایت‌های هدف.
- انجام آزمایش‌های تست نفوذ[2] بر روی وب.
- شناسایی مؤلفه‌های تکنیکی هدف مانند سیستم‌عامل و ...
- جمع‌آوری اطلاعات از طریق مهندسی اجتماعی (توسط کارکنانی که در آن ساختار کار می‌کنند)

۳- حملهٔ سایبر اتفاق می‌افتد.

- بعدازاینکه دسترسی حاصل شد، ممکن است که حمله تا مدتی نگه‌داشته شود.
- ممکن است که حمله موفقیت‌آمیز بوده و یا شکست بخورد.
- اگر حمله موفقیت‌آمیز باشد، هکر آن را از طریق مالتی مدیا منتشر و یا ردپا و اثر خود را مخفی می‌کند.

٤- تحقیق و بررسی جهت حملات دیگر انجام می‌گیرد. (سازمان پدافند، بی‌تا: ١٦)

---

[1] denial of service
[2] Pen- testing

۵.۱۹. مراحل دفاع سایبری

۱- جلوگیری[1]

عبارت است از شناسایی راه‌های نفوذ و حمله و مقابله با آن‌ها جهت افزایش ضریب امنیت، ایمنی و پایداری. ازجمله روش‌های جلوگیری می‌توان به موارد ذیل اشاره نمود:

- طراحی امن و ایمن و پایدار سیستم‌ها[2]

درصورتی‌که امنیت جزو معیارها و اصول طراحی سیستم‌ها، قرار بگیرد، سیستم‌ها بسیار امن‌تر و ایمن‌تر و پایدارتر از قبل خواهند بود.

- متوقف نمودن حملات[3]

از دیگر راه‌های جلوگیری از حملات، متوقف نمودن آن‌ها است این روش از طریق استفاده از تجهیزات پیشرفته امنیتی و وضع قوانین لازم، میسر است.

۲- مدیریت حادثه[4]، محدود کردن خرابی‌ها[5]

روش‌های مدیریت حوادث و محدود نمودن اثرات زیان‌بار حوادث، راه‌هایی هستند که با استفاده از آن‌ها می‌توانیم اثر حملات صورت گرفته را در کمترین زمان کاهش دهیم.

- تعیین آثار، نشانه‌ها و هشدارها

بدین معنی که وقتی حمله ای اتفاق می‌افتد، ابتدا در گام اول باید آثار و خطراتی که این حمله می‌تواند داشته باشد را شناسایی کنیم، زیرا با شناسایی آثار یک حمله می‌توانیم از پیامدهای حملات دیگر و خطراتی که ممکن است ایجاد شوند، جلوگیری کنیم.

- امن، ایمن و پایدار کردن سیستم‌ها[6]

جهت جلوگیری از نفوذهای بیرونی، ضروری است تا موانعی ایجاد کنیم. از قدیمی‌ترین موانع نفوذ، استفاده از کلمه عبور است که البته روش‌های جدیدتر، استفاده از تکنیک‌هایی مانند دیوار آتش و یا پروکسی سرورها[7] است. البته همان‌طور که شیوه‌های رمزنگاری شکست خوردند، شیوه‌های جدید نیز می‌تواند منجر به شکست شوند. در مورد حملات فیزیکی نیز لازم است که

---

[1] Prevention
[2] Embed Security into design
[3] Ban attacks
[4] Incident management
[5] damage limitation
[6] harden the system
[7] proxy servers

ابتدا تمام حملات و نفوذهایی که می‌تواند انجام شود را، شناسایی کنیم. مثلاً در مورد یک شبکه اطلاعاتی، باید استراتژی‌های فیزیکی مناسب جهت امن، ایمن و پایدار نمودن مراکز داده آن اتخاذ نمود.

- خاموشی و تخصیص مجدد[1]

یک‌راه حل دیگر این است که سیستم به‌طور کامل یا به‌طور جزئی خاموش شود و دوباره تخصیص مجدد شود. سیستمی که متوجه شود تحت یک حمله قرار دارد، باید موانع و دفاع‌هایی از خود را بنا نهد که شاید در مواقع عادی از آن‌ها استفاده نمی‌کند و سعی کند قسمت‌هایی از سیستم را که مواجه با حمله شده‌اند، ایزوله کند. البته مراحل خاموش کردن و تخصیص دهی مجدد باید به‌صورت بلادرنگ[2] و به‌سرعت انجام گیرد.

- پشتیبانی[3]

نکتهٔ قابل‌توجه این است که باید همواره از اطلاعات جمع‌آوری شده، قبل از هر حمله‌ای پشتیبانی کنیم. این تاکتیک از طریق تهیه نسخه پشتیبان اطلاعاتی که ذخیره شده‌اند، به دست می‌آید. بسیاری از روش‌های دفاع، نیاز به این دارند که حالت صحیح سیستم قبل از حمله را، جهت تسهیل در بازیابی و تجدید مجدد بدانند. این روش برای مواقعی است که حملات براساس نقطهٔ شروع دقیق و مشخصی انجام می‌شود و پشتیبان‌ها به‌طور منظم گرفته می‌شوند. بسیاری از حملات موذیانه به‌کندی و به‌طور محرمانه، مشکلات زیادی را نسبت به زمانی که اطلاعات سالم بودند، ایجاد می‌کنند (یعنی در این‌گونه از حملات ما زمان دقیق سالم بودن اطلاعات را نداریم و تأثیر حملات هنوز ایجاد نشده است). در این حالت، جهت ایجاد فضای سالم، سیستم‌های سازمان باید خودشان برنامه‌هایی برای تهیه نسخه پشتیبان داشته باشند. (سازمان پدافند، بی‌تا: ۱۷)

۵.۲۰. سنجش تهدید

برای سنجش یک مفهوم کیفی باید آن را به مجموعه‌ای از شاخص‌های عینی (معرف‌ها، مظاهر و نشانگان) تبدیل نمود، زیرا مفاهیم برای قابل‌استفاده و سنجش بودن، باید قابل‌اندازه‌گیری و دارای شاخص‌های تجربی باشند. تبدیل مفهوم به شاخص همواره باید مبتنی بر اصول و مبانی علمی باشد. «شاخص‌سازی تابع اصولی مانند صراحت، جامعیت، وزن‌پذیری و نسبت است. (ساروخانی،

---

[1] Shutdown and reallocation
[2] real time
[3] Backup

۱۳۷۷: ۹۵) زیرا شاخص که به معنای «نمودار، نمونه، الو و سرمشق» (عمید، ۱۳۷۹: ٦۷۸) است، نمایانگر تحولات بوده و ابزاری ساده و قابل‌اتکا را برای نشان دادن تغییرات فراهم می‌کنند.
استفاده از اصول و ملاک‌هایی کـه خصوصـیات کیفـی را در قالـب کمیـت بیـان کـرده و آن‌هـا را قابل‌بررسی و ارزشیابی می‌کند، شاخص نام دارد. به عبارت دیگر شاخص بیان کمی‌رابطـه موجـود بین دو کمیت را نشان می‌دهد. شاخص‌ها معمولاً از نظریه‌ها، نگرش‌ها و یا موقعیت‌هـا سرچشـمه گرفته و مانند علائمی که مسـیر را مشـخص مـی‌کننـد، مورداسـتفاده قـرار مـی‌گیرنـد. بـه کمـک شاخص‌ها می‌توان به تشریح وضعیت موجود پرداخته و روند تغییرات را بررسی نمود.

شاخص‌سازی می‌تواند نقش ارزنده‌ای در هدف‌گذاری و جهت‌دهی به سیاست‌گذاری‌ها و راهبردها داشته باشد. با کمک شاخص‌ها، معیارها و مقیاس‌های غیرقابل انکاری در ارزیابی عملکردها به دست می‌آید که می‌توان به کمک آن‌ها سیاست‌ها، مفاهیم و تصورت را از حالت انتزاعی و تجریدی خارج ساخته و به عالم واقع پیوند زد. (عسکری، ۱۳۸٦: ٤۹)
پس از شاخص‌سازی، فرایند اجرایی مطالعه انجام و پس از جمع‌آوری داده‌ها، بررسی آن‌ها صورت می‌پذیرد. به‌عبارت‌دیگر، تعریف تعیین ویژگی‌های موردسنجش، فرآیند اجرای سنجش و بررسی فرآورده‌ها سه بخش مهم سنجش و اندازه‌گیری به شمار می‌روند. بر این اساس سنجش و اندازه‌گیری را در سه بخش عمده مرحله طراحی، مرحله اجرا و مرحله بررسی فرآورده‌ها می‌توان خلاصه کرد.
تهدید ذاتاً مبهم و نامعلوم بوده و سنجش و ارزیابی آن بسیار دشوار است، لیکن علیرغم این دشواری، سنجش و ارزیابی تهدید امری ضروری است زیرا انجام هدفمند و منطقی اقداماتی که به‌منظور مقابله با تهدید و تأمین امنیت موردنظر و مطلوب صورت می‌گیرند، به شناخت ابعاد، عمق و شدت تهدید بستگی دارند.
به‌منظور سنجش امنیت، کارشناسان و اندیشمندان مسائل امنیتی برای اقدام به مفهوم‌سازی و شناخت بیشتر تهدید و زمان وقوع و تفکیک و دسته‌بندی مفاهیم آن نموده و با شاخص سازی سعی در کمی‌کردن و سنجش آن نموده‌اند که کاری بس دشوار و با نتایج مورد تردید است. راه برون‌رفت از این وضعیت دشوار، چنان‌که «گار» بیان داشته و خود در مقام سنجش پدیده محرومیت نسبی آن را به کار بسته است، «طراحی سیستم سنجشی است که بر شاخص‌های متعدد کمی- کیفی استوار باشد». (گار، ۱۳۷۷: ٦-۳۳)

ماندل معتقد است که «ما در حال ورود به دوران بی‌سابقه‌ای ازلحاظ عدم امکان پیش‌بینی هستیم. البته اگر این سخن را به‌طور کامل بپذیریم، آنگاه سیاست‌ها همگی فلج خواهند شد» (ماندل، ۱۳۷۹: ١٦) و بوزان می‌گوید «اکثر تهدیدات موجودات در صحنه جهانی شامل تعداد زیادی عوامل پیچیده است که برآیند مستقیم و نتایج گسترده آن‌ها را به‌شدت نامعلوم می‌سازد، وقتی این تهدیدات را با تدابیری که برای رویارویی آن‌ها اتخاذ می‌گردد، ترکیب کنید؛ قضیه پیچیده‌تر می‌شود.» (بوزان، ۱۳۷۸: ١٦٦)

«دیوید اپتر»[1] و «چارلز اف. آندریین»[2] از این وضعیت به «لغزندگی» مفاهیمی چون تهدید تعبیر نموده‌اند که از ناحیه ماهیت سه وجهی «فرهنگ- ساختار- رفتار» این مقولات حاصل می‌آید. (اپتر و آندریین، ۱۳۸۰: ٤٠-٣٥) البته نتیجه طرح ادعاهایی از این قبیل انصراف از اصل ضروری «سنجش تهدیدات» نیست؛ چرا که عمده استدلال‌های ارائه شده حکایت از صعوبت سنجش و نه نفی امکان سنجش شدت تهدیدات دارد، دلیل این امر آن است که به گفته «رابرت ماندل»، پذیرش این باور به فلج شدن حوزه سیاست عملی و تعطیل سیاست‌گذاری منتهی خواهد شد؛ چیزی که هیچ اندیشه‌گر و دولت‌مردی قادر به قبول آن نیست. (افتخاری، ۱۳۸۵: ۸۹)

بوزان برای ارزیابی جدی بودن تهدید به مشخص بودن هویت تهدید، قریب‌الوقوع بودن یا نزدیکی آن از لحاظ زمانی، شدت احتمال وقوع تهدید و اوضاع و شرایط تاریخی که باعث تقویت تهدید می‌شوند، توجه می‌نماید. (بوزان، ۱۳۷۸::۱۵۹) از نظر بوزان عوامل مؤثر بر سنجش شدت و ضعف تهدیدات که اثرات تعیین کننده‌ای بر آن‌ها دارند، عبارت‌اند از:

نوع تهدید / شرایط	شدید	ضعیف
تراکم و گستره	خاص و متراکم	پخش و پراکنده
فوریت مکانی	نزدیک	دور
فوریت زمانی	قریب	بعید
میزان اثر	زیاد	کم
عمق	زیاد	کم

(بوزان، ۱۳۷۸: ۱۶۶)

[1] – David Apter

[2] – Chalres Andrain

۵.۲۱. شاخص‌های مؤثر در سنجش تهدیدات

در بحث تهدید شناسی با فرض شناخت ماهیت و موضوع تهدید، عامل تهدید و حوزه آن باید با برخی شاخص‌های کیفی و کمی نسبت به ارزیابی، اولویت و اهمیت تهدید را موردسنجش قرار داد. به تعبیر باری بوزان فوریت، اولویت و جدی بودن تهدید بسیار مهم است. بوزان شاخص‌های کمی و کیفی تهدید را عمدتاً ذیل محور "شدت تهدید" تقسیم‌بندی می‌کند که خود در برگیرنده عمق، گستردگی، مکان، توان بازیگر، اهمیت منافع مورد تهدید و احتمال وقوع است. (بوزان، ۱۳۷۸: ۱٦٤)

افراد دیگری مثل مایکل اشمیت، شاخص‌های کمی و کیفی تهدید را در چهار متغیر اصلی، اهمیت موضوع تهدید، احتمال وقوع، فوریت تهدید و نهایتاً شدت لطمه وارد شده به منافع یا اهداف خلاصه می‌کنند. اما کامل‌ترین شاخص بندی سنجش تهدید را در تقسیم‌بندی دکتر اصغر افتخاری در کتاب کالبدشکافی تهدید می‌توان یافت که در دو سطح درونی شامل شاخص توان ملّی و منافع ملّی و سطح بیرونی با شش شاخص بیرونی به‌منظور ارزیابی تهدید و سنجش کمی و کیفی، اشاره می‌کند که عبارت است از: (عمق تهدید، دامنه تهدید، زمان تهدید، مکان تهدید، قدرتمندی تهدیدگر و موقعیت تهدیدات (افتخاری، ۱۳۸۵: ۱۱٤)

در یک الگوی دیگر، سنجش تهدیدات ازدیدگاه علی عبدالله خانی در کتاب تهدیدات امنیت ملّی و روش سنجش تهدیدات بر پایه چهار گام ذیل پایه‌گذاری شده است (عبدالله خانی، ۱۳۸٦: ۲۵۳)

۱ – برآورد حوزه تهدید

۲ – عامل تهدید و تحلیل آسیب‌پذیری

۳ – ارزیابی تهدید

٤ – الگوسازی و ایجاد سناریو

۵.۲۲. الگوها و مدل‌های سنجش تهدید:

تاکنون الگوها و مدل‌های متعددی برای سنجش تهدیدات ارائه شده است که در این نوشتار سه مدل ارائه شده از سوی متخصصین و نخبگان ایرانی موردمطالعه و بررسی قرار می‌گیرند.

۵.۲۲.۱. مرادیان معیارهای سنجش امنیت خارجی ج.ا.ا را در دو بخش وجود تهدیدات و اندازه (شدت و اهمیت) تهدیدات بررسی نموده و معتقد است «سنجش تهدید در هر یک از

شاخص‌های فوریت، عمق، آثار و تراکم را می‌توان از طریق روش‌های مختلف کمّی یا کیفی انجام داد تا نتیجه آن در تصمیم‌گیری‌ها و قضاوت‌ها مورداستفاده قرار گیرد.

همچنین با عنایت به شرایط نظام سیاسی می‌توان برای ابعاد مختلف امنیت خارجی، ضریب اهمیت تعیین کرد تا تهدیدات در شرایط یکسان نسبت به اهمیت هر بعد، وزن متناسب را نشان دهند. به‌طور مثال در جمهوری اسلامی ایران ضریب بعد فرهنگی– اجتماعی در مقایسه با بعد فناوری اطلاعات بالاتر و بیشتر است».

بر اساس این الگو، درصورتی‌که رصد حوادث و رفتارهای خارجی با شاخص‌ها و مظاهر تهدیدات انطباق داشته باشد، وجود تهدید محرز و مدل سنجش امنیت فعال خواهد شد. در این مدل با استفاده از پرسشنامه، ابتدا ابعاد، شاخص‌ها و نشانگان و مظاهر تهدیدات (زیر شاخص‌ها) به کمک خبرگان و جمع‌آوری نظرات آنان وزن دهی شده و اهمیت هر یک از این الگو، درصورتی‌که رصد حوادث و رفتارهای خارجی با شاخص‌ها و مظاهر تهدیدات انطباق داشته باشد، وجود تهدید محرز و مدل سنجش امنیت فعال خواهد شد. در این مدل با استفاده از پرسشنامه، ابتدا ابعاد، شاخص‌ها و ن مشخص شده است. در مراحل بعد، با ورود داده‌ها و تعیین میزان تراکم، اثر، عمق و فوریت مظاهر و نشانگان تهدید که هر ساله یا طی پریودهای خاص، به کمک خبرگان صورت می‌گیرد و ضرب اعداد حاصله در وزن هر یک از نشانگان و جمع ارقام حاصل، عدد کلی که نشان دهندهٔ میزان امنیت خارجی باشد، به دست می‌آید. (نک مرادیان، ۱۳۸۸)

۵.۲۲.۲. افتخاری برای سنجش شدت تهدید، مکانیزم سنجش دولایه‌ای را پیشنهاد می‌نماید که در دو سطح بیرونی و درونی به بررسی میزان شدت تهدید می‌پردازد.

در سطح نخست که ظرفیت‌های بیرونی را بررسی می‌کند، با مدنظر قرار دادن دو اصل محدودیت «خیر» و ضعف سازمان قانونی نتیجه می‌گیرد که تکوین و ظهور تهدیدات پدیده‌ای کاملاً طبیعی در سیاست بین‌الملل است؛ چراکه کمبود امکانات در حالت افزایش نیازمندی‌ها، موجد انگیزه «تجاوز» خواهد بود و چون سازمان قانونی معتبری (چون حکومت ملی) برای مهار این خواسته در نظام بین‌الملل وجود ندارد، لذا «تهدید» موضوعیت و اصالت می‌یابد. در این چشم‌انداز تهدیدات به دلیل داشتن صبغه «خارجی» از عینیت و ظهور بیشتری برخوردارند.

وی با استفاده از تحلیل‌های ارائه شده از سوی کارشناسان امنیتی و همچنین با مطالعه موردی تجارب موجود، می‌کوشد تا به شاخص‌های عمومی تهدیدات خارجی که بیشترین روایی را برای

شناخت و سنجش تهدید دارا هستند، دست یابد. برای این منظور، وی شاخص‌های شش‌گانه عمق تهدید، دامنه تهدید، زمان تهدید، مکان تهدید، قدرتمندی تهدیدگر و موقعیت تهدیدات را پیشنهاد می‌کند و معتقد است این شاخص‌ها در کنار دو شاخص مربوط به ظرفیت‌های درونی، یعنی توان ملی (توانمندی) و منافع ملی، درمجموع تصویر نسبتاً جامعی را از تهدید به نمایش می‌گذارند. (افتخاری، ۱۳۸۵: ۹۱-۹۵).

۵.۲۲.۲.۱. در این روش پیشنهادی، در خصوص شاخص توان ملی (توانمندی) یافتن پاسخی برای این سؤال مدنظر است که «آیا عامل A فارغ از توان X می‌تواند تهدید باشد یا خیر؟» دکتر افتخاری با اشاره به نسبی بودن تهدید و تأکید بر این‌که «منظور از «نسبی» آن است که یک پدیده در «نسبت» با بازیگر و توانمندی اوست که «تهدید» یا «فرصت» ارزیابی می‌شود «، معتقد است در مقام یک تهدید نمی‌توان از گزاره ساده «عامل A تهدیدی برای بازیگر Y است» استفاده نمود، بلکه جهت افزایش ضریب دقت و راستی این گزاره باید آن را این‌گونه تبیین نمود «عامل Ac برای بازیگر B در شرایط C یک تهدید است.» به‌عبارت‌دیگر، در این مدل، عامل تهدیدکننده، شرایط موجود و توانمندی تهدیدشونده سه رکن مقوم یک تهدید بشمار می‌آیند.

۵.۲۲.۲.۲. در خصوص شاخص منافع ملی (وضعیت منافع)، با تکیه بر اصل «همسویی یا تعارض پدیده‌ها با منافع ملی» در ارزیابی آن‌ها، به‌عنوان یک شاخص مستقل، تهدیدآمیز یا فرصت بودن یک پدیده را در قالب وضعیت‌های منافع متعارض که در آن پدیده‌ها از قابلیت بالای تبدیل‌شدن به تهدید برخوردارند، منافع منطبق که در آن ابعاد تهدیدآمیز پدیده به حداقل رسیده و فرصت‌های آن افزایش می‌یابد، منافع مخالف که بیانگر موقعیتی است که در آن ابعاد تهدیدآمیز بر ابعاد فرصت‌آمیز غلبه نسبی دارد ولی امکان مدیریت موقعیت جهت تبدیل آن به وضعیتی فرصت‌ساز منتفی نیست و منافع هم‌سو که در آن ریسک تهدیدات احتمالی قابل‌توجه است اما احتمال مدیریت کردن آن‌ها و تحصیل اهدافی ارزشمند هم می‌رود، بررسی می‌شود.

۵.۲۲.۲.۳. در شاخص عمق تهدید، که معرف میزان ارزشمندی منفعت موضوع تهدید برای بازیگر است، درجه‌بندی منافع به منافع بنیادین، حیاتی، مهم و حاشیه‌ای معیار ارزش‌گذاری تهدیدات گوناگون برحسب میزان عمق آن‌ها است.

در مدل فوق، منافع بنیادین[1] دربرگیرنده آن دسته از اهدافی هستند که با هویت یک واحد سیاسی در ارتباط می‌باشند و هرگونه آسیب و یا تعرضی به آن‌ها از آن حیث که هویت بازیگر را به «غیر» آن تبدیل می‌سازد، غیرقابل تحمل می‌نماید. هر اقدامی که به نقد، نفی و یا نقض منافع بنیادین منجر شود، در حکم «تهدید» بوده، از حیث قانونی ممنوع می‌باشند. در این تلقی سه گونه عمومی رفتار به‌مثابه اقدامات تهدیدآمیز تلقی شده‌اند که عبارتنداز:

۱. **رفتار مبتنی بر نقض:** در این حالت منافع بنیادین اگرچه از حیث نظری مورد تأیید و قبول بازیگر خاطی قرار دارد، اما در مقام عمل پاس داشته نشده و درنتیجه «منافع بنیادین» عملاً، و نه نظراً، تهدید می‌شوند.

۲. **رفتار مبتنی بر نفی:** در این حالت بازیگر خاطی ضمن عدم پذیرش حجیت نظری منافع مذکور، در مقام عمل به نقض و از حیث نظری به عدم تأیید آن‌ها همت می‌گمارد، بر این اساس «نفی» دربردارنده موضع‌گیری تهدیدآمیز نظری و عملی، به‌صورت توأمان، است.

۳. **رفتار مبتنی بر نقد:** در این حالت بازیگر خاطی التزام عملی نسبت به منافع بنیادین دارد، اما از حیث نظری اعتقاد به مرجعیت این منافع را درست ندانسته و در مقام اظهار این دیدگاه برآید. هر سه بالا از مصادیق «تهدیدات» با «عمق زیاد» ارزیابی می‌شوند.

در «**منافع بنیادین**» نقد، نفی و نقض هیچ کدام موضوعیت ندارد و اصل اولیه بر صیانت و پاسداشت آن‌ها است. لذا هر اقدامی که از یکی از کانون‌های سه‌گانه بالا ناشی شود، در الگوی عمومی «تهدید» قرار می‌گیرد که از حیث «عمق» در ذیل «تهدیدات با عمق زیاد» ارزیابی می‌گردند، البته تهدیدات فهرست شده در این عمق دارای گونه‌های متفاوتی می‌باشند که با عنایت به تعارض نظری یا عملی به دودسته «تهدیدات پیچیده»[2] و «تهدیدات ساده»[3] تقسیم می‌شوند- تهدیدات از یک ناحیه با منافع بنیادین تعارض دارند، اما تهدیدات پیچیده از هر دو ناحیه (نظر و عمل) دارای تعارض هستند.

---

[1] – Fundermental / Basic Interests

[2] –Complex Thrrats

[3] – Simple Threats

منافع حیاتی[1] در نزدیک‌ترین ارتباط با منافع بنیادین بازیگر قرار دارند؛ با این تفاوت که در حالت قرار گرفته در وضعیت «اضمحلال»، منافع بنیادین ارجح هستند؛ حال آن که منافع حیاتی یک مجال اندک از چانه‌زنی را تا قبل از پذیرش «اضمحلال» فراسوی نظام سیاسی قرار می‌دهند. تهدیداتی که متوجه «منافع حیاتی» هستند از عمق کمتری نسبت به «منافع بنیادین» برخوردارند، اما در سیاست عملی به دلیل وجود مکانیزم‌های متعارف و جاافتاده‌ای برای «تعریف و اثبات منافع بنیادین» و «عادی شدن آن‌ها» وجود دارد، منافع حیاتی هستند که در عمل موضوع تصمیم‌گیری سیاسی در سطح ملی قرار می‌گیرند.

منافع مهم[2] قابلیت مصالحه‌پذیری دارند و در عرصه سیاست هر بازیگر با محاسبه هزینه – فایده آن‌ها اقدام به طرح، تصویب و پی‌گیری آن‌ها می‌نماید، بدیهی است که در صورت تحصیل اهداف مشابه با هزینه کمتر و یا طرح اهداف مهم‌تری، این دسته از اهداف به نفع گزینه‌های جدید کنار گذاشته می‌شوند. تهدیدات مطرح علیه این منافع، از هزینه‌های به‌مراتب کمتری نسبت به دودسته قبلی برخوردارند و لذا ارزش و عمق کمتری دارند.

منافع حاشیه‌ای[3] در حکم «محافظ» منافع مهم بوده و ذاتاً برای «مصالحه» وضع شده‌اند. تهدیدات مطرح علیه این منافع به نحوی مدیریت می‌شوند که به منافع مهم‌تر آسیبی نرسد.

۵.۲۲.۲.۴. شاخص «دامنه تهدید» به‌صورت سنتی در ارزیابی تهدیدات پیوسته موردتوجه بوده، اما تلقی بسیط به عمل آمده باعث شد تا ابعاد جدید، و درنتیجه اهمیت فزاینده این شاخص، کمتر لحاظ شود، منظور از دامنه تهدید عبارت است از: «میزان شیوع یک تهدید از حیث عاملی – ارزشی».

در این تعریف دو سطح اصلی برای «گستره تهدید» شناسایی شده است:

اول: در هر رابطه تهدیدآمیز موضوعی وجود دارد که تهدید با توجه به آن معنا و مفهوم می‌یابد، بر این اساس دامنه تهدید را می‌توان با توجه به موضوع تهدید مشخص ساخت. در این تقسیم‌بندی تهدیدات به سه دسته تهدیدات با دامنه اندک، تهدیدات با دامنه متوسط، و تهدیدات با دامنه بالا تفکیک می‌شوند.

---

[1] – Vital Interests

[2] – Important Interests

[3] – Matginal Interests

دوم: سطح عددی که در آن منظور از دامنه تهدید، تعداد بازیگران درگیر در یک «تهدید» است که معمولاً به‌عنوان یک شاخص اصلی از سوی برخی از تحلیل‌گران به آن اشاره شده است.

۵.۲۲.۲.۵. شاخص و عنصر زمان به توسعه دیدگاه تحلیل‌گر در مقام شناخت تهدید کمک می‌نماید و به عبارتی چشم‌انداز تازه‌ای را فراسوی وی ترسیم می‌نمایند که به او امکان آن را می‌دهد تا پیش از ظهور تهدیدات به شناخت و به‌تبع آن به مدیریت تهدیدات نائل آیند، بر این اساس می‌توان تهدیدات را به دو دسته اصلی تقسیم نمود:

۱. تهدیدات مترقبه که دارای هویت اجتماعی مشخص بوده و به دلیل شکل‌گیری تدریجی طی زمان، از بنیادهای تاریخی لازم ظهور جدی در مرحله بعدی برخوردارند. این دسته از تهدیدات دارای شناسنامه تاریخی هستند و لذا پرسش از ریشه‌های اجتماعی آن‌ها بسیار حساس و مهم است.

۲. تهدیدات غیرمترقبه دربرگیرنده مصادیقی است که بنا به دلایل مختلف، تکوین تاریخی لازم را طی نکرده‌اند و به‌صورت جهش و به یک‌باره ظاهر شده‌اند. این تهدیدات، هویت اجتماعی دارند، اما آن‌قدر این هویت کند، پوشیده و مخفی است که به طور طبیعی امکان شناخت و پیش‌بینی ظهور آن وجود ندارد.

تأثیر زمان بر روند تهدید و توجه به سیکل حیاتی «سازواره‌ها» (ارگانیسم) و مراحل سه‌گانه تولد، بلوغ و مرگ هر پدیده، تأثیر زمان و سرعت دگردیسی تهدید نیز ازجمله موارد موردنظر در این شاخص هستند.

۵.۲۲.۲.۶. شاخص مکان ازجمله شاخص‌های ارزیابی شدت تهدیدات است که از فضای جدید حاکم بر مناسبات بین‌المللی، موسوم به جهانی‌شدن (Globalization)، تأثیرپذیری و تحولات چشم‌گیری را تجربه نموده است. در این شاخص تقسیم‌بندی تهدیدات به تهدیدات داخلی، تهدیدات مرزی و تهدیدات خارجی موردنظر هستند و میزان شدت تهدید از داخل به خارج به‌طور طبیعی کاهش می‌یابد.

۵.۲۲.۲.۷. در شاخص قدرتمندی، چهارعنصر اصلی بازیگر عامل (که به دنبال اعمال قدرت است)، بازیگر رقیب (که موضوع اعمال قدرت واقع می‌شود)، هدف (که به صورت انجام دادن یا

ترک فعلی از سوی بازیگر رقیب تعریف می‌شود) و ابـزار (کـه توسـط عامـل بـرای تحمیـل اراده خویش بر رقیب، کاربرد دارد) موردتوجه واقع می‌شود.

در این شاخص، تصویر «عامل» از «توان» و «امکان» خویش و تصویر «رقیب» از «توان» و «امکان» عامل. که به‌صورت هم‌زمان ایجاد و عمل می‌نمایند، شدت تهدید را مشخص می‌سازند. هر چه تصویر از «توان» عامل به سمت مثبت تمایل یابد، شدت تهدید افزوده می‌گردد و هر چه تصویر از «امکان» عامل به سمت مثبت تمایل یابد، شدت تهدید افزوده می‌گردد.

۵.۲۲.۲.۸. در شاخص موقعیت، وضعیت مناسبات بین عوامل تأثیرگذار برحسب شرایط زمـانی و مکانی در نظر گرفته می‌شوند. با توجه به این‌که توالی تهدیدات و هم‌زمانی آن‌ها می‌تواند مدیریت تهدیدات را مشکل ساخته و درنتیجه توان آن‌ها را بیش‌ازحد و اندازه واقعـی آن‌هـا بنمایانـد، ایـن «نسبت سنجی» بین تهدیدات مختلف، ضرورتی امنیتی بوده و در بـرآورد میـزان شـدت تأثیرگـذار است. در این رابطه سه وضعیت متفاوت مطرح هستند که عبارتنداز:

۱. تعارض: موقعیتی که در آن «تهدیدگران» در مناسباتشان بـا یکـدیگر در خصـوص اهـداف و یـا روش‌های اعمال تهدید به توافق نرسیده‌اند. این وضعیت بسته به نتـایج حاصـل از تعـارض، بـه کاهش شدت تهدید برای «تهدیدشونده» منتهی می‌شود.

۲. تقاطع: موقعیتی که در آن «تهدیدگران» در سطح اهداف یا روش‌هـا اخـتلاف‌نظـر دارنـد، امـا در مبانی و اصول با یکدیگر مشترک می‌باشند. «تقاطع تهدیدات» به پیدایش یـک تهدیـد بـا شـدت کمتر برای «تهدیدشونده» (که بر حداقل مشترک بین دو تهدیدگر استوار است) منتهی می‌شود.

۳. تراکم: موقعیتی که در آن «تعدد و انباشت تهدیدات در واحد زمان، مکان و موضوع مطـرح و بـه افزایش شدت تهدید منجر می‌شود. (افتخاری، ۱۳۸۵: ۱۵۲)

در این مدل پیشنهادی، شاخص‌های سنجش تهدید به دو دسته اصلی درونی و بیرونی تقسیم و درمجموع هشت شاخص تعیین‌شده است که شامل (۱) توانمندی (ضعف یا قوت بازیگر)، (۲) وضعیت منافع (تعارض، انطباق و ...)، (۳) عمق تهدید (منافع بنیادین، حیاتی، حاشیه‌ای و...)، (٤) دامنه تهدید (اندک، متوسط، بالا)، (۵) زمان تهدید (مترقبه و غیرمترقبه و...)، (٦) مکان تهدید (داخلی، خارجی...)، (۷) قدرت و امکان اعمال قدرت و (۸) موقعیت (تعارض، تقاطع و تراکم) هستند. اما سنجه‌ها و نشانگان (مظاهر) مورد نظر برای سنجش این شاخص‌ها و همچنین مدل و

الگوی این فرایند معین نگردیده و مشخص نیست که فرمولاسیون این مدل چگونه شکل می‌گیرد.

۵.۲۲.۳. عبداله‌خانی تهدید را تشکیل شده از سه بخش اساسی

(الف) کارگزار یا عامل تهدید[1]: هویت (شخصی یا سازمانی) یا چیزی که به طور بالفعل یا بالقوه توانایی ایجاد انتقال و یا پشتیبانی از تهدید را دارد،

(ب) حوزه تهدید، هویت یا چیزی است که موجودیت و یا دارایی‌های حیاتی آن در معرض خطر قرار گرفته است (پ) موضوع تهدید[2]: وضعیت، پدیده، فعالیت یا رخدادی است که به نظر می‌رسد قابلیت درونی و بیرونی انتقال، پشتیبانی یا ایجاد خطر در موجودیت با دارایی‌های حیاتی بازیگر مورد آماج را در خود دارد، دانسته و قرار گرفتن یک موضوع در مجموعه موضوعات تهدیدآمیز را مستلزم سه شرط:

(الف) وجود رابطه میان عامل تهدید، حوزه تهدید و هدف مرجع تهدید (مشروط بر آن‌که موضوع تهدید، هدف یا اهداف مرجع امنیتی را نشانه گرفته باشد، موضوع تهدید از سوی تهدیدشونده امنیتی شده و واجد شرایط تهدید امنیتی شناخته شده باشد و بتوان برای موضوع تهدید، عامل تهدید شناسایی کرد و عامل تهدید به‌صورت بالقوه یا بالفعل توانایی ایجاد انتقال یا پشتیبانی از تهدید را داشته باشد)،

(ب) موضوع تهدید باید هویتی مستقل پیدا کرده باشد

(پ) نیروی لازم برای به خطر انداختن بقای اهداف مرجع امنیتی یا دارایی‌های کلیدی حوزه تهدید (تهدیدشونده) در درون پدیده، وضعیت یا روند به‌عنوان موضوع تهدید وجود داشته باشد، معرفی نموده است.

ایشان عوامل تهدید را بر مبنای هویت عامل، در سه گروه ذیل طبقه‌بندی می‌نمایند:

- ✓ طبقه عامل تهدید (دولت‌ها و ملت‌های دشمن، شرکت‌ها و افراد به‌عنوان عامل قدرتمند کوچک)
- ✓ طبقه توانایی عامل تهدید (ابرقدرت، قدرت‌های بزرگ، قدرت‌های منطقه‌ای و قدرت‌های ملی و قدرت‌های ورشکسته)
- ✓ طبقه انگیزه عامل تهدید شامل:

---

[1] – threat agents

[2] – Key threat

الف- انگیزه‌های ایدئولوژیک (اعتقادی، دینی، مذهبی، نظریه سیاسی)
ب- انگیزه‌های منفعت محور (سود) (برای حفظ دارایی‌های مادی، توسعه آن‌ها)
پ- انگیزه‌های مزدی (انگیزه‌های شخصی بازیگران)
ت- انگیزه‌های ملی (انگیزه‌های مربوط به مسئله بقاء سرزمین، یکپارچگی و هویت ملی)

ایشان با تأکید بر این‌که الگوسازی تهدیدات امنیتی، موجب میسر شدن درک تهدیدات شده و توانمندی‌های بازیگران حافظ سیستم را درزمینه تدوین الزامات امنیتی افزایش می‌دهد، دو روش کلی الگوی مهاجم محور و الگوی سیستم محور را ذکر کرده و خاطرنشان می‌سازد که در الگوسازی تهدید مهاجم محور، عاملان تهدید موردتوجه بوده و موضوعات، پدیده‌ها، روندها، ساختارها، سازمان‌ها و دولت‌های تهدیدگر سیستم تعیین می‌شوند ولی در الگوی سیستم محور، دارایی‌های کلیدی مبنای شناسایی تهدیدات قرار می‌گیرند. شناسایی تهدیدات، درک تهدیدات، دسته‌بندی تهدیدات، آزمایش تهدیدات و شناخت استراتژی‌های مقابله با تهدیدات امنیتی، وجوه اصلی الگوسازی تهدیدات امنیتی بشمار می‌آیند و بررسی چالش‌ها (تهدیدات بالقوه)، شناسایی تهدیدات امنیتی، تعیین تهدیدات امنیتی خطرناک، تحلیل و ارزیابی تهدیدات خطرناک امنیتی و واکنش به تهدید نیز پنج گام اساسی فرایند الگوسازی می‌باشند.

در روش پیشنهادی، برای تعیین تهدیدات خطرناک امنیتی سه روش پیشنهاد شده است:

روش اول: شناسایی تهدید خطرناک امنیتی برحسب اهداف مرجع تهدید. در این روش، با سنجش تأثیر هر یک از تهدیدات شناسایی شده بر اهداف مرجع تهدیدات امنیتی، خطرناک بودن یا نبودن تهدیدات مشخص می‌شود.

معیارهای اساسی و اصلی این روش، «میزان آسیب‌پذیری در برابر تهدیدات شناسایی شده» و «پیامدهای این تهدیدات» هستند. مراحل اجرای این روش عبارت‌اند از:

۱) تعیین اهداف مرجع و دارایی‌های آن‌ها
۲) مشخص نمودن تهدیدات شناسایی‌شده
۳) تعیین وزن اهداف مرجع (برای اولویت‌بندی آن‌ها ازنظر اهمیت)
٤) تشکیل ماتریس برای هر زوج تهدید- اهداف مرجع جهت سنجش میزان آسیب‌پذیری در مقابل تهدید (بسیار بالا، بالا، متوسط و یا کم) و پیامدهای تهدید (ویرانگر، شدید، قابل‌توجه، اندک)

۵) تعیین میزان خطرناک بودن هر تهدید برای اهداف مرجع در قالب وضعیت‌های پنج‌گانه (بحرانی، خطرناک، هشدار، چالش‌برانگیز و قابل‌کنترل) توسط نخبگان

٦) تعیین میزان خطر شناسایی‌شده از طریق محاسبه مرکز ثقل نظرات نخبگان

درروش فوق برای اندازه‌گیری آسیب‌پذیری از سه معیار و شاخصه «توان بازدارندگی»، «توان حفاظتی» و «توان ترمیمی» استفاده شده و سطوح آسیب‌پذیری بر اساس موارد ذیل تعیین می‌شود:

- ❖ آسیب‌پذیری بسیار بالا: توان بازدارندگی خیلی ضعیف، توان حفاظتی خیلی ضعیف و توان ترمیمی خیلی ضعیف.
- ❖ آسیب‌پذیری بالا: توان بازدارندگی خیلی ضعیف، توان حفاظتی تاحدودی ضعیف و توان ترمیمی تاحدودی ضعیف.
- ❖ آسیب‌پذیری متوسط: توان بازدارندگی تاحدودی ضعیف، توان حفاظتی تاحدودی ضعیف و توان ترمیمی خوب.
- ❖ آسیب‌پذیری کم: توان بازدارندگی خوب، توان حفاظتی خوب و توان ترمیمی خوب.

پیامدهای تهدید نیز از طریق سه شاخصه شدت تهدید، گستره تهدید و عمق تهدید ارزیابی پیامدها تعیین‌شده و به چهار گروه ویرانگر، شدید، قابل‌توجه و اندک تقسیم می‌شوند.

روش دوم: تعیین تهدیدات خطرناک امنیتی از طریق طراحی سناریو: در این روش، سناریوهای احتمالی هر تهدید ترسیم و سپس با توجه به سناریوهای موجود، خطرناک بودن یا نبودن تهدید تعیین می‌شود.

روش سوم: اولویت‌بندی تهدیدات شناسایی‌شده. در این روش، با استفاده از فهرست تهدیدات شناسایی‌شده و برخی معیارهای اساسی که از سوی نخبگان موردپذیرش قرار گرفته‌اند، تهدیدات اولویت‌بندی شده و سپس براساس وزن و ارزش مشخص‌شده برای معیارهای هر یک از تهدیدات موردنظر، میزان مخاطره‌آمیز بودن هر تهدید مشخص و درنهایت تهدیدات خطرناک معین می‌شوند. روش تحلیل سلسله مراتبی[1] و روش تاپسیس[2] ازجمله روش‌هایی هستند که می‌توان برای اولویت‌بندی تهدیدات شناسایی‌شده استفاده نمود.

---

[1] - Analytic Hiearchy Processes

[2] - Technique for order Preference by Similarity to Ideal Solution (TOPSIS)

دکتر عبدا...خانی روش ماتریس تحلیل و ارزیابی تهدیدات امنیتی را که ترکیبی از دو روش «تعیین تهدیدات امنیتی» و «تحلیل و ارزیابی تهدیدات خطرناک امنیتی» است را برای کالبدشکافی تهدیدات امنیتی مناسب می‌داند. در این روش، ابتدا تحلیل و ارزیابی تهدیدات خطرناک امنیتی با استفاده از سه مؤلفه «توان بالقوه آسیب‌رسانی»، «هشدار استراتژیک» و «احتمال استراتژیک» انجام می‌گیرد.

در مؤلفه «توان بالقوه آسیب‌رسانی» معیارهای عمق (شدت آسیب‌های وارده به اهداف حمله)، گستره (محدوده جغرافیایی آسیب‌های اولیه)، آثار موجی (تأثیرات دومینوی حوادث) و زمان بازیابی (زمان بازسازی یا جایگزینی موارد آسیب‌دیده از تهدید) سنجیده شده و تهدیدات به یکی از سطوح مختلف آن (تهدیدات فاجعه‌آمیز، تهدیدات حیاتی، تهدیدات تأثیرگذار، تهدیدات ناچیز و تهدیدات بی‌اهمیت) تقسیم می‌شوند.

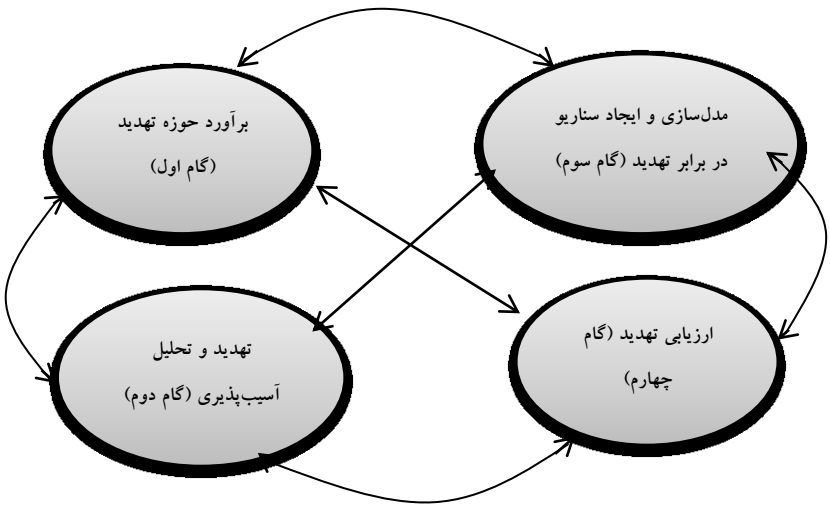
در مؤلفه «هشدار استراتژیک» که می‌توان آن را به دو صورت هشدار تاکتیکی و استراتژیکی و یا به‌صورت پیوسته درنظر گرفت، از زمانی که بروز تهدید قطعیت یافته باشد تا زمان مورد هدف قرار گرفتن در نظر گرفته و سنجیده می‌شود. این زمان برای تهدیدات مختلف، تغییر بوده و با توجه به نوع تهدید، تجهیزات و تسلیحات بکار گرفته شده، گستردگی تهدید و ... تعیین می‌شود. به‌طور مثال می‌توان از معیار زیر استفاده نمود: زمان هشدار کمتر از یک دقیقه، زمان هشدار کمتر از یک ساعت، زمان هشدار یک روز تا یک هفته، زمان هشدار چند هفته تا چند ماه و زمان هشدار بیش از چند ماه.

در شاخصه «احتمال استراتژیک»، احتمال رخداد تهدید مورد ارزیابی قرار می‌گیرد. سابقه منازعه و بروز تهدید در گذشته، رویکرد بازیگر یا بازیگران امنیتی‌ساز، نوع سیستم‌عامل درگیر در تهدید مدنظر قرار گرفته شده و احتمال وقوع (وقوع مکرر، وقوع محتمل، وقوع موردی، وقوع اندک و وقوع بعید) تعیین می‌گردد. درنهایت میانگین نهایی تهدید از محاسبه نمرات شاخصه‌های سه‌گانه فوق محاسبه می‌شود.

دکتر عبدا.. خانی درنهایت مدلی را برای سنجش تهدیدات ارائه می‌نماید که بر پایه چهارگام زیر استوار است:

- برآورد حوزه تهدید
- عامل تهدید و تحلیل آسیب‌پذیری

- ارزیابی تهدید
- مدل‌سازی و ایجاد سناریو



(عبداله‌خانی، ۱۳۸٦: ۲۵۳)

این مدل دارای پنج ویژگی به شرح ذیل است:

تحلیل‌گر می‌تواند نحوه کار و تفکر خود را در گام‌های مختلف تغییر دهد؛ یعنی می‌تواند برای مدل‌سازی و ایجاد سناریو از یک روش‌شناسی و برای ارزیابی از روش‌شناسی دیگر استفاده کند.

رسیدن به بالاترین حد انسجام در میان گام‌های مختلف و پرهیز از قرار گرفتن در یک گام، خود یک هدف اصلی است؛ به معنای آنکه باید میان گام‌های مختلف نوعی هماهنگی و هم‌افزایی وجود داشته باشد و گام‌های چهارگانه به‌صورت چهار جزیره نمی‌توانند عمل نمایند.

مدل باید به‌تمامی مراحل پنج‌گانه الگوسازی تهدید پاسخگو باشد؛ یعنی هم بتواند به شناسایی تهدید بپردازد و هم بتواند راهکارهای واکنش به تهدید را نشان دهد.

لازم نیست همه گام‌های چهارگانه را طی کرد؛ اما قانون طلایی می‌گوید «گام بیشتر، نتایج بهتر» نقطه خروجی مدل، گام ارزیابی تهدید است. (عبداله‌خانی، ۱۳۸٦: ۲۵٤)

۵.۲۳. مراحل انجام تحقیق:

در این تحقیق با استفاده از الگویی که آقای دکتر عبدا...خانی در کتاب تهدیدات امنیت ملی ارائه

داده است به سنجش تهدیدات سایبری پرداخته شد. (عبدا...خانی، ۱۳۸٦: ۲۰۹)

در این روش، با سنجش تأثیر هر یک از تهدیدات شناسایی شده فضای سایبر بر اهداف مرجع تهدیدات امنیتی و دارائی‌های کلیدی حوزه سایبر، خطرناک بودن یا نبودن تهدیدات مشخص شد. معیارهای اساسی و اصلی این روش، «میزان آسیب‌پذیری در برابر تهدیدات شناسایی‌شده» و «پیامدهای این تهدیدات» هستند که گام‌های ذیل برای انجام تحقیق برداشته شد.

۱- گام اول: تعیین اهداف مرجع و دارایی‌های کلیدی حوزه سایبر

برای تعیین اهداف مرجع و دارایی‌های کلیدی حوزه سایبر پس از مطالعات اکتشافی و بررسی ابعاد مختلف تهدیدات سایبری، با توجه به موقعیت خاص کشور ایران اهداف مرجع و داریی‌های کلیدی به‌دست‌آمده به صاحب‌نظران و متخصصین حوزه سایبر ارائه گردید که پس از بحث و بررسی موارد ذیل به جمع‌بندی رسید.

- اطلاعات و ارتباطات (هدف مرجع حوزه سایبر)
- انرژی (دارائی کلیدی حوزه سایبر)
- بانک‌ها (دارائی کلیدی حوزه سایبر)
- خدمات دولتی (دارائی کلیدی حوزه سایبر)
- صنایع تولیدی (دارائی کلیدی حوزه سایبر)

۲- گام دوم: مشخص نمودن تهدیدات شناسایی‌شده حوزه سایبر

برای تعیین تهدیدات شناسایی‌شده حوزه سایبر به روش فوق اقدام و تهدیدات سایبری (جنگ سایبری- تروریسم سایبری- جاسوسی سایبری- جرائم سایبری- صدمه سایبری) جهت انجام گام‌های بعدی نهائی گردید.

۳- گام سوم: تشکیل ماتریس برای هر زوج تهدیدات شناسایی‌شده- اهداف مرجع و دارایی‌های کلیدی جهت سنجش میزان آسیب‌پذیری در مقابل تهدید (بسیار بالا، بالا، متوسط و یا کم) و پیامدهای تهدید (ویرانگر، شدید، قابل‌توجه، اندک)

✓ در این مرحله با توجه به جمع‌بندی انجام شده در راستای تهدیدات شناسایی‌شده و اهداف مرجع و دارایی‌های کلیدی حوزه سایبر، جهت مشخص نمودن میزان آسیب‌پذیری در مقابل تهدید، از سه معیار و شاخصه «توان بازدارندگی»، «توان حفاظتی» و «توان ترمیمی» در مقابل

تهدیدات شناسایی‌شده سایبری سؤال گردید که درنهایت مصاحبه‌شوندگان علاوه بر تعیین سطح میزان آسیب‌پذیری (آسیب‌پذیری بسیار بالا، آسیب‌پذیری بالا، آسیب‌پذیری متوسط و آسیب‌پذیری کم) عددی را بین صفر و یک به شرح ذیل انتخاب نمودند.

- آسیب‌پذیری بسیار بالا (۱ – ۰/۷۶) آسیب‌پذیری بالا (۰/۷۵ – ۰/۵۱)
- آسیب‌پذیری متوسط (۰/۵ – ۰/۲۶) آسیب‌پذیری کم (۰/۲۵ — ۰)

✓ برای تعیین پیامدهایی که تهدیدات سایبری می‌توانند برای اهداف مرجع و دارایی‌های کلیدی حوزه سایبر داشته باشند، از سه شاخصه شدت تهدید، گستره تهدید و عمق تهدید سؤال شد که درنهایت مصاحبه‌شوندگان علاوه بر تعیین نوع پیامد تهدید (ویرانگر، شدید، قابل‌توجه، اندک) عددی را بین صفر و یک به شرح ذیل برای پیامد تهدیدات سایبری انتخاب نمودند.

- پیامد ویرانگر (۱ – ۰/۷۶) پیامد شدید (۰/۷۵ – ۰/۵۱)
- پیامد قابل توجه (۰/۵ – ۰/۲۶) پیامد اندک (۰/۲۵ — ۰)

٤- گام چهارم: تعیین میزان خطرناک بودن هر تهدید برای اهداف مرجع و دارایی‌های کلیدی حوزه سایبر در قالب وضعیت‌های پنج‌گانه (بحرانی، خطرناک، هشدار، چالش‌برانگیز و قابل کنترل)

بر اساس مصاحبه‌های انجام‌شده با صاحب‌نظران و نمراتی که هر کدام از آن‌ها به میزان آسیب‌پذیری و پیامد تهدید داده بودند، برای تعیین وزن تهدیدات خطرناک امنیتی از فرمول زیر استفاده شد. (عبدا...خانی، ۱۳۸٦: ۲۱۳)

$$DT = \frac{\sum I * V}{\mathrm{n}}$$

در این فرمول: DT تهدیدات خطرناک امنیتی، I پیامدها، V آسیب‌پذیری‌ها و n تعداد قضاوت کنندگان است. حال با توجه به قرارداد ذیل تهدیدات خطرناک امنیتی تعیین وضعیت گردیدند.

- وضعیت بحرانی (۰/۹۰ تا ۰/۹۹) وضعیت خطرناک (۰/۸۰ تا ۰/۸۹)
- وضعیت هشدار (۰/٦۵ تا ۰/۷۹) وضعیت چالش‌برانگیز (۰/۵۰ تا ۰/٦٤)
- وضعیت قابل‌کنترل (زیر ۵۰)

۵.۲٤. تجزیه‌وتحلیل و نتیجه‌گیری:

تهدیدات سایبری واقعیتی انکارناپذیر بوده و یکی از اساسی‌ترین تهدیدات متصوره علیه

زیرساخت‌های کشورهای توسعه‌یافته است. در ورود به دنیای جدید، باید تمام زوایا خصوصاً تهدیدات آن را بشناسیم. اگرچه امنیت مطلق در محیط‌های واقعی و محیط‌های مجازی امکان‌پذیر نیست، ولی ایجاد سطحی از امنیت که به‌اندازه کافی و متناسب با نیازها و سرمایه‌گذاری انجام‌شده باشد تقریباً در همه شرایط محیطی ممکن است. لذا در این مقاله سعی شد تا با بررسی میزان آسیب‌پذیری اهداف مرجع و دارایی‌های کلیدی حوزه سایبر و پیامدهایی که تهدیدات سایبری می‌توانند برای اهداف مرجع و دارایی‌های کلیدی داشته باشند، میزان خطرناک بودن هر تهدید برای اهداف مرجع و دارایی‌های کلیدی را تعیین نماییم تا مسئولین ذی‌ربط بر اساس یافته‌های این تحقیق تمهیدات امنیتی خاص آن را اتخاذ نمایند.

بر اساس جمع‌بندی که از نظرات مصاحبه‌شوندگان و نمراتی که به میزان آسیب‌پذیری و پیامد تهدیدات سایبری داده بودند، میزان پذیرش خطر تهدیدات سایبری طبق تهدیدات شناسایی‌شده جهت اهداف مرجع و دارایی‌های کلیدی حوزه سایبر به‌صورت ذیل مشخص گردید.

جدول نهایی نتایج به‌دست‌آمده از وضعیت امنیتی تهدیدات سایبری نسبت به اهداف مرجع و دارایی‌های کلیدی حوزه سایبر:

اهداف مرجع و دارائی کلیدی / تهدیدات سایبری	اطلاعات و ارتباطات	انرژی	بانک‌ها	خدمات دولتی	صنایع
جنگ سایبری	۰/٦۱ چالش‌برانگیز	۰/۷٦ هشدار	۰/۷٤ هشدار	۰/٦۳ چالش‌برانگیز	۰/٦۸ هشدار
تروریسم سایبری	۰/۷۱ هشدار	۰/۷۲ هشدار	۰/۵۹ چالش‌برانگیز	۰/۵٤ چالش‌برانگیز	۰/۵٤ چالش‌برانگیز
جاسوسی سایبری	۰/۷۵ هشدار	۰/٦۵ هشدار	۰/۵٤ چالش‌برانگیز	۰/۵٤ چالش‌برانگیز	۰/٦۵ هشدار
جرائم سایبری	۰/۵۲ چالش‌برانگیز	۰/٤۵ قابل‌کنترل	۰/٦۱ چالش‌برانگیز	۰/٦٦ هشدار	۰/٤۷ قابل‌کنترل
صدمه سایبری	۰/۳۸ قابل‌کنترل	۰/٤۳ قابل‌کنترل	۰/۳۹ قابل‌کنترل	۰/۵۲ چالش‌برانگیز	۰/٤۵ قابل‌کنترل

پس از جمع‌بندی یافته‌های تحقیق مشخص گردید که تهدیدات سایبری ذیل جهت اهداف مرجع و دارایی‌های کلیدی حوزه سایبر وضعیت هشدار را ایجاد نموده است و بایستی مسئولین حوزه سایبر توجه بیشتری را به آن‌ها معطوف نموده تا از وضعیت هشدار بیرون بیایند، در غیر این صورت احتمال تبدیل‌شدن آن‌ها به وضعیت خطرناک امنیتی و بحرانی متصور است.

۱- جاسوسی سایبری و تروریسم سایبری برای اطلاعات و ارتباطات که اهداف مرجع حوزه سایبر می‌باشند، در حد بالائی از وضعیت هشدار قرار دارند.

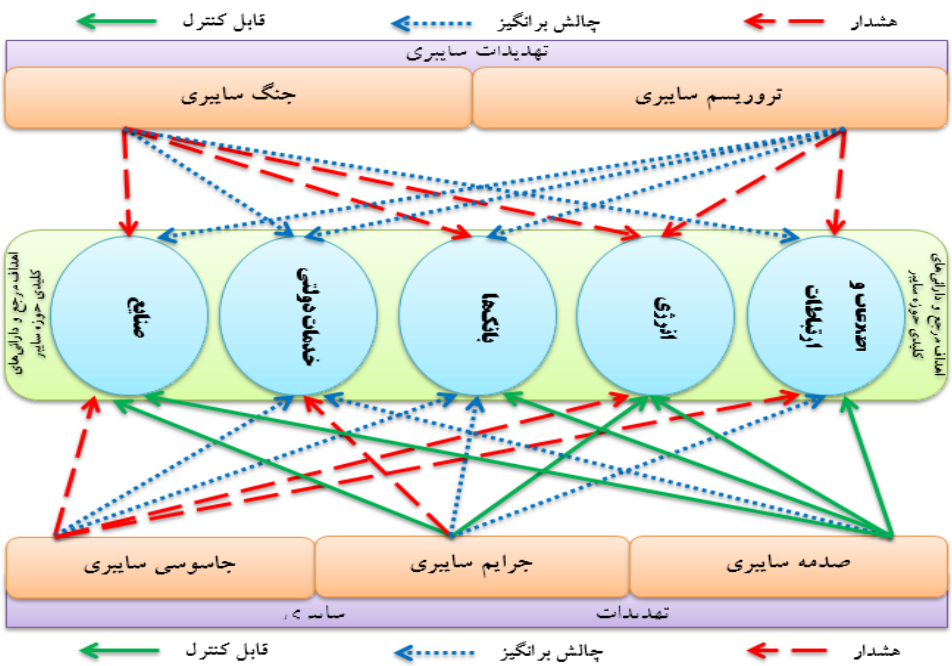
۲- جنگ سایبری، تروریسم سایبری و جاسوسی سایبری برای حوزه انرژی در وضعیت هشدار بوده که از این بین جنگ سایبری و تروریسم سایبری به وضعیت خطرناک امنیتی نزدیک‌ترند.

۳- جنگ سایبری برای بانک‌ها وضعیت هشدار امنیتی بالائی را ایجاد نموده است.

٤- جرائم سایبری برای خدمات دولتی

۵- جنگ سایبری و جاسوسی سایبری برای صنایع کشور

نتایج به دست آمده از تحقیق را می‌توان به‌صورت مدل ذیل نمایش داد:



۵.۲۵. منابع:

- آلبرتس دیوید، پاپ دانیل، (۱۳۸۵)، الزامات امنیت ملی در عصر اطاعات، پژوهشکده مطالعات راهبردی
- «المنجد فی اللغه» (۱۹۷۳)، تهران، انتشارات اسماعیلیان، افست از روی دارالمشرق، بیروت، چاپ بیست و سوم.
- اپتر، دیوید و آندریین، چارلز (۱۳۸۰)، «اعتراض سیاسی و تغییر اجتماعی»، مترجم محمدرضا سعیدآبادی، تهران، پژوهشکده، مطالعات راهبردی.
- افتخاری، اصغر (۱۳۸۵)، «کالبدشناسی تهدید»، تهران، دانشگاه امام حسین (علیه السلام).
- افتخاری، اصغر (۱۳۹۱)، «امنیت»، تهران، دانشگاه امام صادق (علیه السلام)
- بل دیوید، (۲۰۰۱)، درآمدی بر فرهنگ سایبر ترجمه مسعود کوثری، حسین حسنی، چاپ اول انتشارات جامعه شناسان
- بوزان، باری (۱۳۷۸)، «مردم، دولت‌ها، هراس»، ترجمه و انتشارات پژوهشکده مطالعات راهبردی، تهران.
- بهزادی، حمید (۱۳٦۸)، «اصول روابط بین‌الملل و سیاست خارجی»، انتشارات دهخدا، چاپ دوم، تهران.
- خلیلی شورینی، سیاوش (۱۳۸۹)، «روش‌های پژوهش آمیخته»، تهران، انتشارات یادوراه کتاب
- درویشی سه تلانی؛ (۱۳۷٤)، تهدیدات امنیت ملی یک چارچوب نظری، مجله سیاست دفاعی، شماره 10 و 11 سال سوم – بهار و تابستان.
- درّی نجف‌آبادی، قربان‌علی (۱۳۷۹)، «نگاهی به امنیت از منظر امیر مؤمنان (علیه السلام)»، فصلنامه حکومت اسلامی، شماره ۱۸، سال پنجم.
- رابرت گار، تد (۱۳۷۷)، «چرا انسان‌ها شورش می‌کنند»، مترجم علی مرشدی زاده، تهران، پژوهشکده مطالعات راهبردی.
- رشاد، علی اکبر، (۱۳۸۸)، معنا منهای معنا، تهران: انتشارات پژوهشگاه فرهنگ و اندیشه اسلامی
- ره‌پیک، (۱۳۹۰)، تقریرات کلاسی «تهدیدات نرم: چالش‌ها و آسیب‌های داخلی»
- ساروخانی، باقر (۱۳۷۷)، «روش‌های تحقیق در علوم اجتماعی، بینش‌ها و فنون»، ج ۲، تهران، پژوهشگاه علوم انسانی و مطالعات فرهنگی.

- سازمان پدافند غیر عامل، پدافند غیر عامل در حوزه جنگ سایبر
- سید مفیدی، کاوه، (۱۳۸۳)، جنگ سایبری،
- عبداللّه خانی، علی (۱۳۸٦)، تهدیدات امنیت ملی، تهران: انتشارات ابرار معاصر تهران.
- عبداللّه خانی، علی (۱۳۸۲)، نظریه‌های امنیت، مقدمه‌ای بر طرح‌ریزی دکترین امنیت ملی، تهران: انتشارات ابرار معاصر تهران.
- عبدالله خانی، علی (۱۳۸۵)، «عدالت و امنیت»، فصل‌نامه علوم سیاسی، شماره ۳۳، سال نهم، بهار ۱۳۸۵.
- عسکری، محمود (۱۳۸٦)، «شاخص‌های قدرت منطقه‌ای»، تهران، فصل‌نامه راهبرد دفاعی، سال پنجم شماره ۱۸، زمستان.
- عمید، حسن (۱۳۷۹)، «فرهنگ فارسی»، تهران: انتشارات امیرکبیر، چاپ نوزدهم.
- کیان خواه احسان، (۱۳۸۹)، مدیریت امنیت اطلاعات، انتشارات ناقوس
- کیان‌خواه، احسان، علوی‌وفا، سعید، (۱۳۸۹)، مفهوم شناسی امنیت سایبری، مجموعه مقالات نخستین همایش ملی دفاع سایبری
- ماندل، رابرت (۱۳۷۹)، «چهره متغیر امنیت‌ملی»، مترجم و ناشر پژوهشکده مطالعات راهبردی، تهران.
- مرادیان، محسن، (۱۳۸۸)، تهدید و امنیت، تهران: انتشارات مرکز آموزش شهید صیاد شیرازی آجا
- معین، محمد (۱۳٦۳)، «فرهنگ فارسی»، تهران: انتشارات امیرکبیر، چاپ ششم.

- Oxford Advanced Learner's Dictionary (2005), 7th edition: Londen, Oxford Press; Threat.
- Dod, Department Of Defense Strategy For Operating In Cyberspace, (2011), http://www.defence.gov
- Mutula,Stephen M.,2007,Web Information Management, UK: Cahndos Publication
- E. A. Fischer, Creating a National Framework for Cybersecurity: An Analysis of Issues and Options, CRS Report for Congress, Order Cide RL32777, Feb. 2005.
- GibsonWilliam,1984, Neuromancer, US: Ace Books
- K.F. Rauscher and V. Yaschenko (Eds.), Russia-U.S. Bilateral on Cybersecurity Critical Terminology Foundations, EastWest Institute and the Information Security Institute of Moscow State University, 2011.

- www.syberpolice.ir
- http://www.industryinfobase.ir/cofarsi/cofarsi/index.asp
- http://www.aftabir.com/articles/view/politics/political_science/c1c1280312433_internet_p1.php "بررسی پدیده هکتیویسم- آشوب دراینترنت"
- http://www.wisegeek.com/what-is-cyber-intelligence.htm, Visited: 2012-01-20."What Is Cyber Intelligence?,"