تبیین آسیب‌های امنیتی در حوزه فن‌آوری اطلاعات و استخراج عوامل مؤثر بر آن

عباسعلی مقدم نژاد [1]

تاریخ دریافت: ۱۳۹۱/۲/۱۸
تاریخ تأیید: ۱۳۹۱/۳/۳۱

چکیده

در این تحقیق، ابتدا، چارچوب بعضی از آسیب‌های امنیتی حوزه فن‌آوری اطلاعات با ذکر مصادیقی از انواع حملات انجام‌شده به شبکه‌های رایانه‌ای، تبیین شده است. سپس آسیب‌های امنیتی فن‌آوری اطلاعات در حوزه‌های جمع‌آوری، پردازش، ذخیره‌سازی و انتقال اطلاعات استخراج گردیده است و سرانجام عوامل مؤثر بر آن بیان شده است.

داده‌های این پژوهش با استفاده از آمار توصیفی (شامل میانگین، واریانس، انحراف معیار) و آمار استنباطی (شامل تحلیل عوامل، آزمون آماره استنباطی، آزمون فریدمن با استفاده از نرم‌افزار SPSS) مورد تجزیه و تحلیل قرار گرفته است. اعتبار پرسشنامه از طریق به دست آوردن ضریب آلفای کرانباخ با استفاده از نرم‌افزار SPSS صورت گرفته است. بومی‌سازی سامانه‌های فن‌آوری اطلاعات به معنای واقعی با رویکرد تاکتیک‌های نوآوری و خلاقیت در این حوزه، کنترل فریب سایبری حریفان، کنترل ساختاریافته دقیق فضای انتقال اطلاعات و همچنین تبیین سناریوی چگونگی پردازش اطلاعات حریفان در آینده، از نتایج مهم این پژوهش است.

کلیدواژه‌ها: *آسیب‌شناسی امنیتی، فن‌آوری اطلاعات، نوآوری و خلاقیت*

۱. مدرس دانشکده فارابی و دانشجوی دکتری دانشگاه عالی دفاع ملی Aamn64@gmail.com

مقدمه

فن‌آوری، یک محرک اصلی در انقلاب اطلاعاتی قرن بیستم است. مشهودترین تأثیر آن، در روش‌های جمع‌آوری اطلاعات است و به دنبال آن تغییرات اساسی در ارتباطات، به ویژه پیدایش رادیو، قبل از جنگ جهانی اول، امکان تبادل اطلاعات سریع را به وجود آورد. اطلاعات مخابراتی در طول جنگ جهانی اول تولد یافت، شکوفا شد و همچنان به عنوان جوهره اصلی اطلاعات در بقیه قرن بیستم باقی ماند. آزمایش‌های برادران رایت در تپه‌های ماسه‌ای کیتی‌هاوک در کارولینای شمالی، حوزه جاسوسی را به آسمان‌ها کشاند. اطلاعات تصویری نیز به موازات اطلاعات مخابراتی، به عنوان یک روش اصلی جمع‌آوری اطلاعات شکل گرفت و توسعه یافت. اما جمع‌آوری اطلاعات، تنها جنبه‌ای نبود که تحت تأثیر فن‌آوری واقع شد. الگوی چرخه اطلاعات، دارای چهار مرحله اساسی است که شامل جمع‌آوری، تحلیل و پردازش، ارزیابی، توزیع و انتشار اطلاعات است. طی جنگ جهانی دوم، خدماتی که فن‌آوری، در راستای ارائه اطلاعات تصویری و دیداری ارائه کرد، توان پشتیبانی تصمیم خود را در این حوزه نشان داد (ادوارت، ۱۳۸۷، ۲۹).

انقلاب رایانه‌ای و در پی آن انقلاب اینترنتی، شیوه‌های ذخیره‌سازی و بازیابی داده‌های اطلاعاتی را تغییر داد؛ به‌ویژه اینترنت، گستره وسیعی از اطلاعات را در قالب اطلاعات آشکار به روی سازمان‌های اطلاعاتی گشود و همچنین فرصت‌های بی‌بدیلی را (در کنار تهدیدات گسترده) تقدیم کرد. امروزه، فراوانی بیش از حد اطلاعات، خود به یک مشکل بزرگ در سازمان‌های اطلاعاتی تبدیل شده است. چگونگی به‌کارگیری سامانه‌های فن‌آوری اطلاعات و شناسایی تهدیدات و آسیب‌های آن و یافتن راهکار درست، یکی از دغدغه‌های سازمان‌های اطلاعاتی امروزی است. در حقیقت، فن‌آوری، با افزایش دادن دامنه پیچیدگی و کمک به کمال‌ناپذیری اطلاعات، بیش از پیش به مشکل افزوده است. میزان مشارکت سامانه‌های فنی، در افزایش قدرت جمع‌آوری اطلاعات، فراتر از تصور است؛ اما کمال‌پذیری اطلاعات، همچنان تخیلی بیش نخواهد بود (اخوان، ۱۳۸۴: ۸۶).

محیط امنیتی – اطلاعاتی ساحفاهای نیروهای مسلح، مبتنی بر جمع‌آوری اطلاعات، پردازش و به‌کارگیری اطلاعات است. از آنجایی که جمع‌آوری اطلاعات، با به‌کارگیری فناوری اطلاعات، آسیب‌های خاص خود را دارد و برابر شواهد موجود، حریفان به شدت در این محیط فعالیت می‌کنند؛ بنابراین شناسایی آسیب‌ها و ارائه راهکارهای عملی، از اهم مواردی است که در این تحقیق مد نظر است.

تشریح مسئله

از دیرباز تاکنون، تبادل اطلاعات در راستای رشد و توسعه جوامع، نقش بسیار مهمی داشته است و این رشد بدون در نظر گرفتن حوزه‌های امنیتی و آسیب‌شناسی آن، امکان‌پذیر نخواهد بود. حجم زیاد اطلاعات و اهمیت آن، دولت‌مردان را بر آن داشته است تا از طریق تجهیزات فنی و سامانه‌های فن‌آوری اطلاعات، نسبت به تبادل آن اقدام کنند.

با نگاهی گذرا به کشورهای جهان سوم در طول سه دهه گذشته، ویژگی‌های زیر به چشم می‌خورد (محقق):

۱) هیچ‌کدام تولیدکننده قطعات اصلی تجهیزات فنی نیستند. (اغلب کشورهایی که توانایی تولید قطعات اصلی تجهیزات فنی مانند مدارهای مجتمع[1] را داشته باشند، از حوزه کشورهای جهان سوم رهایی پیدا می‌کنند).

۲) از علم تولید قطعات سخت‌افزاری اصلی، آگاهی ندارند و به گونه‌ای ارزان و آسان در اختیار آنان گذاشته می‌شود که این کشورها، تولید آنها را مقرون به صرفه نمی‌دانند.

۳) به سیاست رشد و توسعه فن‌آوری اطلاعات، دسترسی ندارند و همواره سعی بر تبعیت از آن دارند.

۴) به طور کامل، مصرف‌کننده تجهیزات فنی و سامانه‌های فناوری اطلاعات هستند.

1. IC: Integrated Circuit

۵) این کشورها، پیشرفت، رشد و توسعه خود را در به‌کارگیری تجهیزات فنی و سامانه‌های فن‌آوری اطلاعات سایر دولت‌ها می‌دانند.

۶) کشورهای تولیدکننده تجهیزات فنی و سامانه‌های فن‌آوری اطلاعات، به‌گونه‌ای تولیدات خود را توسعه می‌دهند که مقبولیت و مشروعیت لازم و کافی را در کشورهای مصرف‌کننده داشته باشد.

این مصرف‌کنندگی صرف کشورهای جهان سوم، هرگز آنان را از این خصلت (جهان سومی) رهایی نداده است و از آنجایی که ضامن رشد و توسعه اطلاعات نامیده می‌شود، به طور حتم، از طریق تجهیزات و سامانه‌های فن‌آوری اطلاعات، مورد هجوم تولیدکنندگان قرار می‌گیرند. به عبارت دیگر، بیشتر تولید و رشد تجهیزات فنی و سامانه‌های فن‌آوری اطلاعات، همواره در راستای اهداف جمع‌آوری اطلاعات، در اختیار سایر کشورها قرار می‌گیرد؛ هر چند که سایر سیاست‌ها از قبیل وابستگی، سودجویی و... نیز محتمل است.

بر اساس تجربیات گذشته، جمهوری اسلامی ایران، همواره مورد تهاجم نیروهای فرامنطقه‌ای قرار گرفته و این وضعیت در طول ۵۰۰ سال گذشته، به شکل‌های مختلف به وجود آمده است و هم اکنون نیز ادامه دارد. تداوم این وضعیت، بسیار محتمل است و محقق با این دیدگاه که فن‌آوری اطلاعات برای نیل به اهداف دشمنان جمهوری اسلامی ایران واگذار می‌گردد، این تحقیق را انجام داده است.

مسائل امنیتی در به‌کارگیری این‌گونه وسایل، ناشی از دو سامانه نرم‌افزاری و سخت‌افزاری است و راه‌های عملی برای رفع مشکلات امنیتی، به دو طریق همگون و ناهمگون، با استفاده از روش‌های نوآوری فنی بسیار حائز اهمیت است. مسئله اصلی تحقیق این است که آسیب‌های امنیتی تجهیزات جمع‌آوری اطلاعات چیست و چگونه می‌توان نسبت به رفع آن اقدام کرد؟

اهمیت و ضرورت تحقیق

محیط امنیتی پیرامون جمهوری اسلامی ایران و تهدیدهای بالقوه و بالفعل از سوی دشمنان آن (به سرکردگی ایالات متحده آمریکا و رژیم اشغالگر قدس) علیه تمامیت ارضی کشور، به‌ویژه از ناحیه جمع‌آوری اطلاعات، تفکر در ظرفیت‌های ارائه راهکارهای دفاعی مؤثر در مقابل یک هجوم همه‌جانبه را ضروری ساخته است. دشمنان جمهوری اسلامی ایران، همواره با شیوه و شگردهای مختلف، نسبت به جمع‌آوری اطلاعات اقدام می‌کنند و در کنار عوامل انسانی، به‌کارگیری تجهیزات فنی و سامانه‌های فن‌آوری اطلاعات را در اولویت خود قرار داده‌اند. به طور کلی، در هر زمان، ارائه جدیدترین تجهیزات فنی و سامانه‌های فناوری اطلاعات، در راستای جمع‌آوری موثر اطلاعاتی و امنیتی است؛ هر چند که سایر جوانب سیاسی، اقتصادی و فرهنگی اجتماعی را نیز شامل می‌گردد. سازمان‌های حفاظت اطلاعات نیروهای مسلح، باید در برابر هرگونه تهدید احتمالی از سوی به‌کارگیری تجهیزات فنی و سامانه‌های فن‌آوری اطلاعات، آمادگی لازم را به‌دست آورند و توان مقابله با انواع شگردها، ترفندها و حملات مربوط را داشته باشند؛ بنابراین ضرورت دارد که متخصصان و مسئولان رده بالای سازمان‌های حفاظت اطلاعات نیروهای مسلح، با شناسایی و پیش‌بینی آسیب‌های احتمالی در آینده (نرم‌افزاری و سخت‌افزاری)، نیروهای رزمی را در برابر پیامدهای آن تهدیدها و آسیب‌پذیری‌ها، ایمن سازند و این کار مستلزم این است که قبل از مواجهه با تهدیدهای احتمالی، نسبت به اتخاذ تاکتیک‌های همگون و ناهمگون در راستای ارائه راه‌کارهای عملی، برای رفع آسیب‌ها اقدام کنند.

اهداف تحقیق

هدف کلی

آسیب‌شناسی امنیتی تجهیزات جمع‌آوری اطلاعات برای ارائه راه‌حل‌های عملی و پاسخگو به‌منظور رفع آنها.

اهداف فرعی

۱) رفع آسیب‌های امنیتی سامانه‌های جمع‌آوری اطلاعات.

۲) ارائه راهکارهای مناسب برای رفع آسیب‌های امنیتی تجهیزات و سامانه‌های فن‌آوری اطلاعات، پس از تجزیه و تحلیل داده‌ها و اطلاعات.

سوال تحقیق

آسیب‌های امنیتی تجهیزات جمع‌آوری اطلاعات کدامند و راه‌حل‌های عملی و پاسخگو به‌منظور رفع آنها چیست؟

فرضیه تحقیق

غیربومی بودن سامانه‌ها در تولید و چرخه مربوط به اطلاعات، از اهم آسیب‌های امنیتی است و به‌کارگیری شیوه‌های مدیریتی (خلاقیت و نوآوری، کارآفرینی) در حوزه‌های درون‌سازمانی و برون‌سازمانی، برای رفع آسیب‌ها مؤثر است.

نوع و روش تحقیق

این تحقیق، از نوع کاربردی و به روش توصیفی – تحلیلی صورت گرفته است. به این ترتیب که با جمع‌آوری اطلاعات به روش کتابخانه‌ای و میدانی، تأثیر مؤلفه‌های متغیر مستقل (اثرگذار) بر متغیر تابع (وابسته) مورد شناسایی قرار گرفته است و با انتخاب نمونه آماری، از بین خبرگان و صاحب‌نظران، با طراحی سوال‌های مناسب که می‌تواند شاخص‌های مورد نظر را مورد سنجش قرار دهد، نظرهای خبرگان، به روش دلفی دریافت شده است و پس از انجام محاسبات آماری(توصیفی و استنباطی)، پاسخ‌ها با به‌کارگیری آزمون آماره استنباطی، با بهره‌برداری از نرم‌افزار SPSS و EXCEL، مورد تجزیه و تحلیل قرار گرفته است. بر این اساس، پاسخ سوالات حاصل و فرضیه‌های تحقیق مورد تأیید قرار گرفته است. به منظور اولویت‌بندی متغیرها و شناسایی متغیرهای اهم و بیشترین تأثیرگذار، از آزمون فریدمن، تحت نرم‌افزار اکسل استفاده شده است.

جامعه آماری

تحقیق حاضر، در حوزه اطلاعاتی امنیتی اجرا شده است. جامعه آماری تحقیق، کارشناسان فنی و عملیاتی سازمان حفاظت اطلاعات ارتش ج.ا.ا، کارشناسان معاونت‌های اطلاعات، عملیات و فاوای ستاد ارتش ج.ا.ا و کارشناسان فنی ستاد کل نیروهای مسلح هستند که تعداد آنها، ۱۰۰ نفر و به شرح جدول زیر است:

شرح مشاغل	کارشناسان فنی ساحفاجا	کارشناسان عملیاتی ساحفاجا	کارشناسان معاونت اطلاعات ستاد آجا	کارشناسان فاوای ستاد آجا	کارشناسان فنی ستاد کل نیروهای مسلح	جمع کل
جامعه آماری	۳۵	۲۰	۱۵	۱۵	۱۵	۱۰۰

نظر به اهمیت موضوع، محقق به صورت تمام‌شمار، کلیه جامعه آماری را به صورت جامعه نمونه آماری تلقی کرده است.

اعتبار پرسشنامه

در این پژوهش، اعتبار پرسش‌نامه با نرم‌افزار SPSS از طریق آلفای کرونباخ alpha=0/8413 محاسبه گردیده است که اعتبار قابل توجهی محسوب می‌شود و نشان‌دهنده پایایی پرسش‌نامه است.

شواهد مربوط به روایی

در این پژوهش، به‌منظور روایی صوری پرسش‌نامه که در واقع مناسب، بامعنی و مفید بودن وسیله اندازه‌گیری است، از نظر استادان راهنما، مشاور و تعدادی از کارشناسان مرتبط استفاده گردیده و نشان داده شده است که سؤال‌های پرسش‌نامه از روایی قابل قبولی برخوردار است.

چارچوب نظری آسیب‌شناسی امنیتی

واژه‌هایی چون امنیت، امنیت ملی، محیط امنیتی، آسیب‌شناسی و... در علوم سیاسی، دارای معانی و تعابیر مختلفی است. از آنجایی که مقاله حاضر، بیشتر به آسیب‌های امنیتی توجه دارد، ناچار از تفکیک میان امنیت و امنیت ملی هستیم. در واژگان علوم سیاسی،«امنیت» را به معنای تضمین ایمنی؛ یعنی قرارهای تنظیمی سیاسی برای کاهش احتمال بروز جنگ، برقراری مذاکره به جای محاربه، مصونیت از تعرض و تصرف اجباری و وجود اطمینان به سلامت جان، مال و ناموس مردم تعریف کرده‌اند. اما«امنیت ملی»، به حالتی گفته می‌شود که در آن، مصونیت نسبی یا مطلق یک کشور از حمله مسلحانه یا خرابکارانه سیاسی یا اقتصادی احتمالی همراه با وارد کردن ضربه کاری و مرگبار، مد نظر است. امنیت ملی، بیان‌کننده تمام مقاصد دفاعی کشور؛ یعنی آمادگی برای مخاصمه به‌علت بازداشتن آن یا دوری گزیدن از آن است (افتخاری، ۱۳۸۱: ۳۳).

درک امنیتی، همواره با مشکلات خودمحوری قومی، واقعگرایی نظری، بنیادگرایی ایدئولوژیکی و تقلیل‌گرایی به معنی تبدیل شدن پدیده‌های ذهنی به اصطلاحات ساده‌اندیشانه همراه بوده است. کاربرد گسترده واژه«امنیت»در حوزه‌های گوناگون و تحت تأثیر قرار دادن آن در معادلات منافع، باعث گردیده است تا این مفهوم از دقت علمی لازم که نتیجه نگرش انتقادی

است، کمتر بهره‌مند شود و از آن مفهومی توسعه‌نیافته، مبهم، نارسا، جدال‌برانگیز، متباین و متناقض درآورد (heleh, 2006: 75-76).

از مجموع تعاریف فوق، می‌توان این نتیجه را استخراج کرد که در تمامی آنها، منظور از امنیت، به نوعی دربرگیرنده این واژه در بُعد داخلی و خارجی یا به عبارت مناسب‌تر، ذهنی و عینی است. بعد ذهنی، معطوف به احساس امنیت است و اشعار ذهنی را بر وجود، ایمن می‌نمایاند و بعد عینی معطوف به نبود تهدید و خطر بیرونی و موجبی برای ایجاد مخاطره و ناامنی را مورد توجه قرار می‌دهد. در هر صورت، در این بخش، از تکرار مکررات در زمینه تعاریف مختلف امنیت و امنیت ملی پرهیز می‌شود و بیشتر به مباحث کاربردی می‌پردازیم.

در کنار مسائل فوق، باید میان واژه‌هایی چون آسیب‌های امنیتی، چالش‌های امنیتی، تهدیدات امنیتی، معضلات امنیتی، بحران‌های امنیتی و... نیز تفکیک قائل شد. یکی از مشکلاتی که در مقوله «آسیب‌شناسی امنیتی» وجود دارد، تفکیک نبودن و غیرتمایز بودن سطوح تحلیل است؛ یعنی برخی از مسائل، بیشتر جنبه نظری دارند یا در سطوحی هستند که چالش‌آفرین نیستند؛ ولی در حد مشکل تلقی می‌شوند. برخی آسیب‌ها نیز، بیشتر جنبه داخلی دارند؛ اما در عین حال از شدت چندانی برخوردار نیستند، ولی به صورت تهدید نمایان می‌گردند که در نهایت سطح تحلیل «بحران» که نقطه اوج سطوح قبلی است، به ستیزه و درگیری می‌انجامد و می‌تواند باعث فروپاشی سیاسی و اجتماعی گردد.

یکی از مشکلاتی که وجود دارد، متمایز نبودن بین این سطوح است که با هر سطح، متناسب با آن برخورد نمی‌شود؛ یعنی گاه با «مشکل» مقابله‌ای می‌شود که باید با «بحران» انجام داد، و گاه با «بحران» چنان ساده برخورد می‌شود که در سطح یک «مشکل» تقلیل می‌یابد. از این رو ابتدا، باید موضع و دیدگاه خود را در مورد عنوان مقاله یعنی آسیب‌های امنیتی تعیین نمود.

منظور ما از چالش‌های امنیتی (داخلی و خارجی) شامل معضل‌ها، خطرها، تهدیدها و نیز بحران‌های امنیتی به‌طور هم‌زمان است و با تلفیق میان چهار سطح تحلیل فوق، به بررسی آسیب‌های امنیتی تجهیزات جمع‌آوری اطلاعات می‌پردازیم و در ضمن لازم است تفکیکی

دیگر نیز قائل شویم و آن هم دیدگاه سنّت‌گرایان و نوگرایان از مقوله امنیت است. اصولاً دو دیدگاه در مقوله امنیت و محیط امنیتی وجود دارد. یک دیدگاه با رویکردی سلبی به امنیت می‌نگرد و تحقق آن را در نبود عامل دیگر (تهدید) تعریف می‌کند؛ این دیدگاه بیشتر به زور و اجبار و در نهایت نیروی نظامی تأکید دارد؛ البته برخی در همین دسته که به فراسنتی‌ها معروف هستند، با گفتمان چندبعدی، به متغیرهای دیگر، غیر از نیروی نظامی مانند؛ تحریم اقتصادی، زیست محیطی، سیاسی و فرهنگی توجه نموده‌اند (چپ در ایران، ۱۳۷۸: ۳۷).

در مقابل گفتمان سلبی (برامویی، ۱۳۷۸: ۱۰)، دیدگاه دیگری وجود دارد که«گفتمان ایجابی» است(استمپل، ۱۳۷۷: ۷۱) و به جوهره و ماهیت امنیت توجه دارد. در این رویکرد، نظام سیاسی توان پاسخ‌گویی به تقاضاها را دارد و بر اساس رضایت، منافع ملی را حفظ و نگهداری می‌کند. به عبارت دیگر، در گفتمان سلبی، محیط، صرفاً امنیتی است و به مقولاتی چون فرهنگ، اقتصاد و سیاست از دید امنیتی نگریسته می‌شود (سیاست‌های انقباضی). اما در گفتمان ایجابی، چه در مرحله راهبردی امنیتی و چه در سایر مراحل، مانند برنامه‌ریزی امنیتی یا سیاست امنیتی، به مقوله‌های مختلف فقط از جنبه نظامی و امنیتی نگریسته نمی‌شود و محیط بین‌الملل نیز مورد توجه قرار می‌گیرد.

بنابراین ما در این مقاله، از کلیه مبانی نظری مذکور، به صورت تلفیق استفاده می‌کنیم و با یک دیدگاه سلبی - ایجابی سعی می‌نماییم تا آسیب‌های امنیتی تجهیزات جمع‌آوری اطلاعات را به نقد و بررسی بگذاریم.

مروری بر پیشینه تحقیق

نقش اطلاعات در فن‌آوری و صنایع حساس و مهم که جنبه راهبردی دارند، اهمیت فوق‌العاده‌ای دارد و هر کشوری که سازمان اطلاعاتی قوی‌تر و کاراتری داشته باشد، موفق‌تر خواهد بود؛ زیرا چنین سازمانی با کسب اطلاعات پنهانی از فن‌آوری‌های پیشرفته، از طریق نفوذ یا سرقت اسرار، عقب‌ماندگی کشور خود را نسبت به سایر کشورها جبران می‌کند و بر

دشمنان واقعی یا فرضی تفوق می‌یابد. نمونه عالی چنین اهمیتی، کسب دانش هسته‌ای یا سرقت آن از سوی کشورهای فاقد این فن‌آوری است (علوی‌فر، ۱۳۸۲: ۲۲).

انواع حمله در شبکه‌های رایانه‌ای

الف - حملات غیرعامل[1]

حملات غیرعامل، شامل کنترل ارتباطات مخابراتی توسط حامل‌های عمومی (مانند رادیو، ماهواره، ماکروویو، شبکه‌های سوئیچی عمومی) است. برای مقابله با حملات غیرعامل، از شبکه اختصاصی مجازی، شبکه‌های حفاظت‌شده، مبتنی بر رمزنگاری و شبکه‌های توزیع حفاظت‌شده (مانند شبکه‌های توزیع سیمی که به صورت فیزیکی حفاظت می‌شوند) استفاده می‌گردد. روش‌های این نوع حمله عبارتند از:

(۱) مونیتورینگ[2]: حمله‌کننده، با مونیتور شبکه می‌تواند اطلاعات کاربران را که از انتشار غیرمجاز محافظت نشده است، استخراج کند.

(۲) رمزگشایی ترافیک رمزشده ضعیف.

(۳) کشف کلمه عبور[3]: در این نوع حمله، با استفاده از تحلیل گره‌ای پروتکل، کلمات عبور برای استفاده‌های غیرمجاز استخراج می‌شود.

(۴) تحلیل ترافیک[4]: مشاهده پترن‌های ترافیک می‌تواند اطلاعات بسیار خوبی را در اختیار دشمن قرار دهد؛ حتی اگر نتواند اطلاعات رمزشده را رمزگشایی کرد. برای نمونه گسترش شبکه به صحنه نبرد تاکتیکی، ممکن است قریب‌الوقوع بودن عملیاتی از طرف کشور مهاجم را نشان دهد و مانع غافل‌گیر شدن عناصر خودی شود(مؤسسه آموزشی و تحقیقاتی صنایع دفاعی، ۱۳۸۷).

1. passive
2. PlainText
3. PassWorrd Sniffing
4. Traffic Analysis

ب- حملات عامل[1]

حملات عامل، شامل تلاش‌هایی برای شکستن یا به خطر انداختن جنبه‌های امنیتی شبکه، وارد کردن کدهای مضر (مانند ویروس)، از بین بردن دیتا و صحت عملکرد سامانه است. برای مقابله با این نوع حمله، باید به کمک فایروال‌ها، گاردها و دست‌یابی افرادی که مدیریت شبکه را انجام می‌دهند، از طریق تصدیق هویت، کنترل شود و از ابزارهای آشکارسازی خودکار ویروس، بازرسی و آشکارسازی نفوذ به شبکه استفاده گردد. انواع حملات عامل به شرح زیر هستند(سادوسکای، ۱۳۸۴: ۲۱):

(۱) تغییر اطلاعات در حال انتقال.

(۲) وارد کردن دیتا.[2]

(۳) جعل کاربر یا سرور مجاز.

(۴) سوءاستفاده از سامانه عامل‌ها و نرم‌افزارهای کاربردی.

(۵) سوءاستفاده از اجرای دیتا.

(۶) وارد کردن کدهای مضر(اسب تراوا، ویروس، کرم، در تله[3]، ...).

(۷) سوءاستفاده از پروتکل و اشکال‌های موجود در زیرساخت‌ها.

(۸) جعل سرویس.

ج- حمله تقرب[4]

در این حمله، افراد غیرمجاز با نزدیک شدن فیزیکی به شبکه‌ها، سامانه‌ها و تسهیلات، سبب تغییر، جمع‌آوری یا ممانعت از دست‌یابی افراد به اطلاعات می‌شوند. نزدیک شدن به منابع سامانه‌های اطلاعاتی از طریق ورود پنهانی، دست‌یابی آزاد یا ترکیب هر دو به شرح زیر حاصل می‌شود (سادوسکای، ۱۳۸۴: ۲۱):

1. Active
2. Replaying
3. Trap Door
4. Close-In

(۱) تغییر داده جمع‌آوری اطلاعات.

(۲) تحریف سامانه.[1]

(۳) خرابی فیزیکی.

د - حمله‌های داخلی[2]

حمله‌های داخلی، توسط افراد مجاز موجود در محدوده فیزیکی سامانه‌های پردازش امنیت اطلاعات یا افرادی که دسترسی مستقیم به سامانه‌های پردازش امنیت اطلاعات دارند، به وجود می‌آید. حمله‌های داخلی به دو دسته تقسیم می‌شود:

(الف) بدخواهانه و غیربدخواهانه.

(ب) حالت دوم به این علت حمله در نظر گرفته می‌شود که عمل کاربر، نتیجه امنیتی به شرح زیر به دنبال دارد(Doty,1997: 23):

(۱) تغییر دیتا یا سامانه‌های امنیتی.

(۲) ایجاد ارتباط شبکه‌ای غیرمجاز.

(۳) کانال‌های پنهان.

(۴) آسیب یا خرابی فیزیکی.

ه- حمله توزیع[3]

این حمله به تغییرات عمدی سخت‌افزار و نرم‌افزار بین مراحل تولید و نصب آن، یا هنگام انتقال آن از یک سایت به سایت دیگر گفته می‌شود. آسیب‌پذیری‌های ممکن در کارخانجات با به‌کارگیری روش‌های کنترل پیکربندی سامانه می‌تواند به حداقل برسد. با استفاده از سامانه‌های کنترل، دست‌یابی، توزیع کنترل‌شده و نرم‌افزارهای تأییدشده، می‌توان آسیب‌های این نوع حمله را کاهش داد. روش‌های این نوع تهدید عبارتند از(Hutt,1995: 34):

(۱) تغییر نرم‌افزار و سخت‌افزار در محل تولید.

1. System Tampering
2. Insider
3. Distribution

(۲) تغییر نرم‌افزار و سخت‌افزار در طول فرآیند توزیع.

اقدامات تهاجمی	اقدامات متقابل دفاعی
۱- ویروس اصلی: همتاساز کد (آلوده‌کننده)	۲- اسکن‌کننده ویروس: جستجوی فراگیر برای علائم متوالی کد
۳- ویروس ایستای ضدآشکارکننده: کد همتاساز، رمزکننده، کد خفته برای پنهان - کردن علائم ایستا، تغییرات کلید رمز برای برنامه بهبودبخش (جز افشای رمز) به طور پویا به‌منظور تغییر علائم	۴- اسکن‌کننده ویروس: جستجوی فراگیر برای باز کردن رمز علائم جاری ایستا. مشاهده رفتار
۵- ویروس پویای ضدآشکارکننده (چندریختی): کد همتاساز، رمزگذاری و افشای رمز، کد ویروس و کلید پویا، موتور تغییردهنده جهشی برای تغییر دادن کد بازکننده رمز	۶- تست رفتار ویروس: کد اجرایی در فرآیند رایانه مجازی (امنیت و مشاهده رفتار)

جدول ۲: سه فرآوری توسعه ویروس (Opplinger, 2006: 23)

آسیب‌های کلان به‌کارگیری فن‌آوری در حوزه جمع‌آوری اطلاعات

شاید بهره‌گیری از واژه منفی، در ارزشیابی تأثیر به‌کارگیری فن‌آوری اطلاعات نادرست باشد؛ زیرا اگر هر ابزاری در جای خود به کار گرفته نشود، آثار زیان‌باری به دنبال خواهد داشت. بخشی از کاربردهای منفی ارتباطات در جهان سوم عبارتند از:

(۱) توانایی تجزیه گروه‌های اجتماعی و اخلال در جریان وحدت ملی جوامع، نظیر بحران یوگسلاوی، تجزیه اتحاد جماهیر شوروی سابق یا ایجاد شورش‌ها و ناآرامی‌های قومی و

منطقه‌ای همچون ناآرامی‌های تبت در جمهوری خلق چین و شمار زیادی از کشورهای افریقایی و همچنین در انقلاب‌های رنگی.

(۲) انتقال فن‌آوری نامناسب و وابستگی به شرکت‌های چندملیتی به ویژه غربی.

(۳) ایجاد اختلاف و شکاف میان ملت‌ها، برای توسعه ملی‌گرایی افراطی، ایدئولوژی‌های متضاد و در نتیجه بروز شکاف فرهنگی.

(۴) تغییر الگوهای مصرف و روش‌های زیستی، از طریق افزایش خواسته‌ها و ایجاد دنیای پرزرق و برق، همراه با دام‌های جذاب جامعه مصرفی.

تجزیه و تحلیل ادبیات تحقیق

✓ **با توجه به سطح نفوذ فن‌آوری‌های ویژه در حوزه اطلاعات، امکان جمع‌آوری اطلاعات در موارد زیر وجود دارد:**

(۱) استفاده از ریزپردازنده‌ها در پردازش محیط اطلاعات کارساز است.

(۲) استفاده از امکان فن‌آوری در شناسایی و دسته‌بندی کاربران، کاربرد متوسطی دارد.

(۳) دسته‌بندی‌های بیومتریک در جمع‌آوری‌های اطلاعات، نفوذ دارند.

(۴) از تمامی علائم و سیگنال‌های موجود در فضای اطلاعات، برای جمع‌آوری استفاده می‌شود.

(۵) از سلاح‌های نرم و فاقد تخریب فیزیکی، در نفوذ اطلاعاتی استفاده می‌شود.

(۶) مالکیت فضای الکترومغناطیس در جمع‌آوری اطلاعات، در اختیار حریفان قرار دارد.

(۷) از تمامی ابزارهای فن‌آوری به‌منظور جمع‌آوری، از فضا تا عمق زمین بهره‌برداری می‌شود.

(۸) امکان نامرئی‌سازی جمع‌آوری، با استفاده از فن‌آوری وجود دارد.

(۹) تولید اغلب فن‌آوری‌ها، در قالب سیاست‌های جمع‌آوری اطلاعات هوشمند در محیط اطلاعاتی صورت می‌گیرد.

(۱۰) امکان جمع‌آوری فن‌آورانه از هزاران مایل فاصله وجود دارد.

(۱۱) ارتقای سرعت و کیفیت در انتقال اطلاعات در سناریوی جمع‌آوری اطلاعات از سوی حریفان همچنان ادامه دارد.

(۱۲) تمامی ابزار و تجهیزات اطلاعاتی کوچک‌سازی می‌شوند.

(۱۳) امکان شبیه‌سازی تمامی رخدادها در فضای مجازی وجود دارد.

(۱۴) نقش ریزپردازنده‌ها در تصمیم‌سازی نظامی در محیط عملیات در حال افزایش است.

آزمون استنباطی فرضیه

مرحله اول - تبدیل فرضیه پژوهشی به فرضیه آماری:

ادعا=H_1

غیربومی بودن سامانه‌ها در تولید اطلاعات و چرخه مربوط به آن اطلاعات، از اهم آسیب‌های امنیتی است و به‌کارگیری شیوه‌های مدیریتی (خلاقیت و نوآوری، کارآفرینی) در حوزه‌های درون‌سازمانی و برون‌سازمانی به منظور رفع آسیب‌ها موثر است.

نقیض ادعا =H_0

غیربومی بودن سامانه‌ها در تولید اطلاعات و چرخه مربوط به آن اطلاعات، از اهم آسیب‌های امنیتی است و به‌کارگیری شیوه‌های مدیریتی (خلاقیت و نوآوری، کارآفرینی) در حوزه‌های درون‌سازمانی و برون‌سازمانی به منظور رفع آسیب‌ها موثر نیست.

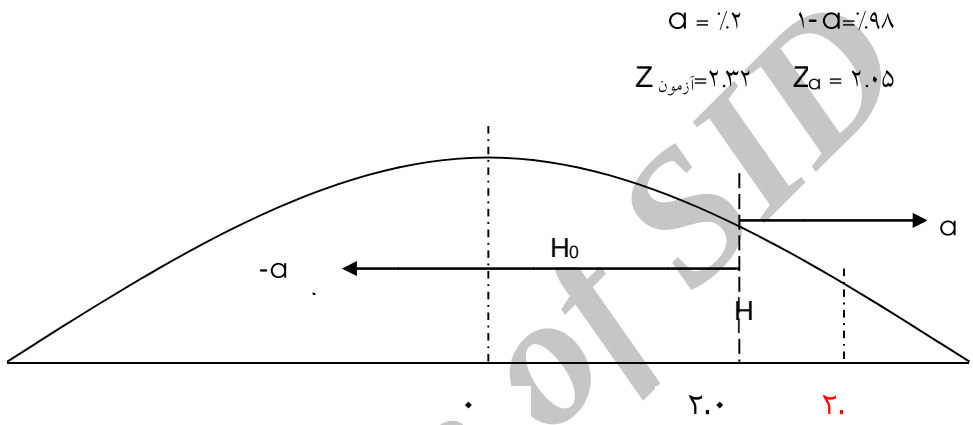
مرحله دوم - تعیین آماره آزمون فرضیه:

طیف	خیلی زیاد	زیاد	متوسط	کم	خیلی کم	جمع
فراوانی	467	382	70	77	44	1040
درصد	44.90	36.73	6.73	7.40	4.23	100
$\overline{P}$	۸۱.۶۳					

$$Z = \frac{\overline{P} - P_0}{\sqrt{P_0 \frac{1-P_0}{n}}} = \frac{\%81.63 - \%70}{\sqrt{\%70 \frac{1-\%70}{65}}} = \frac{\%11.63}{\sqrt{\frac{0.21}{65}}} = \frac{0.1163}{.05} = +2.32$$

$P_0 = \%70$ و $\overline{P} = \%81.63$

مرحله سوم تعیین سطح زیر منحنی و نقطه بحرانی:



مرحله چهارم - تحلیل:

چون مقدار آماره آزمون (۲.۳۲) از Z_α (مقدار بحرانی ۲.۰۵) بزرگ‌تر است و در ناحیه H_1 قرار گرفته است، فرضیه H_1 پذیرفته می‌شود و فرضیه مقابل آن یعنی H_0 رد می‌گردد. به عبارت دیگر، با اطمینان ۹۸٪ می‌توان گفت که غیربومی بودن سامانه‌های جمع‌آوری اطلاعات، از اهم آسیب‌های امنیتی است و به‌کارگیری شیوه‌های مدیریتی (خلاقیت و نوآوری، کارآفرینی) در حوزه‌های درون‌سازمانی و برون‌سازمانی به‌منظور رفع آسیب‌ها موثر است.

تحلیل توصیفی فرضیه (استخراج‌شده از آزمون فریدمن تحت نرم‌افزار SPSS)

✓ **با توجه به چگونگی انتقال اطلاعات مبتنی بر سامانه‌های فن‌آوری اطلاعات غیربـومی، آسیب‌های زیر محتمل است:**

(۱) انباشت و تمرکز اطلاعات در فضای سایبر ناشی از انتقال اطلاعات.

(۲) قابلیت جمع‌آوری اطلاعات به همراه اطمینان و امنیت کافی در حوزه حریف.

(۳) قابلیت توزیع، انتقال و پردازش هوشمند اطلاعات.

(۴) امکان فراوان ایجاد اختلال و فریب‌زایی در انتقال اطلاعات.

(۵) توان تولید نارضایتی در سطح گسترده.

(۶) خودکنترلی و هوشمندی.

✓ **با توجه به چگونگی پردازش اطلاعـات مبتنـی بـر سـامانه‌هـای فـن‌آوری اطلاعـات غیربومی، آسیب‌های زیر محتمل است:**

(۱) توان پردازش اطلاعات علائم به جا مانده از کوچک‌ترین تحرک و جابجایی‌ها.

(۲) توان پردازش از علائم و نشانه‌های موجود محیطی.

(۳) قدرت پردازش بسیار بالا با حجم فراوان در کم‌ترین زمان ممکن.

(۴) پردازش اطلاعات بر اساس نیل به اهداف از قبل تبیین‌شده(عملیات روانی).

(۵) پردازش اطلاعات بر اساس حفظ کیفیت و امنیت اطلاعاتی.

(۶) پردازش اطلاعات بر اساس هم‌خوانی با فضای سایبر خودی.

(۷) در اختیار داشتن مالکیت سامانه‌های پردازش اطلاعات.

(۸) پایش حوزه دما، لرزه، فشار، گاز، موج، بو و طعم، صدا، انرژی، ذرات مواد عایق الکترومغناطیس از فاصله صدها مایلی.

(۹) سیاست‌گذاری همراه با شبیه‌سازی در حوزه پردازش اطلاعات.

(۱۰) حفاظت ارتباطات بر اساس کیفی‌ترین سامانه پردازش اطلاعات.

✓ **با توجه به غیربومی بودن سامانه‌های ذخیره‌سازی اطلاعات و مالکیت حریفان، آسیب‌های زیر محتمل است:**

(۱) درگاه‌های فیزیکی (ورودی و خروجی) تعریف معینی ندارند و بهره‌برداری‌های مختلفی می‌توان از آنها به عمل آورد. درگاه USB رایانه‌ها، قابلیت اتصال به ۱۲۸ دستگاه مختلف را دارا است. در بسیاری از موارد، سامانه‌های ارتباطی جاسوسی، امکان اتصال از این درگاه را دارا هستند.

(۲) امکان تجهیز سامانه‌های فناوری اطلاعات به وسایل ارتباطی جاسوسی، با استفاده از حافظه‌های جانبی وجود دارد که امکان شناسایی آنها به‌راحتی صورت نمی‌گیرد.

(۳) رشد و پیشرفت سامانه‌ها و تجهیزات ذخیره‌کننده اطلاعات فنی، نشان‌دهنده تبادل اطلاعات سریع، مطمئن و امن است. این موضوع از سیاست‌های مالکان و تولیدکنندگان فن‌آوری است.

(۴) نامرئی‌سازی در حوزه جمع‌آوری اطلاعات بر اساس اصول جمع‌آوری غیرعامل با استفاده از تجهیزات ذخیره‌کننده اطلاعات.

(۵) رشد کم‌حجم فیزیکی سامانه‌های جمع‌آوری اطلاعات بر اساس سناریوهای از قبل تهیه‌شده برای کنترل‌ناپذیر کردن مسائل امنیتی این سامانه‌ها.

✓ **عوامل موثر زیر در حوزه جمع‌آوری اطلاعات، از اولویت بیشتری نسبت به سایر متغیرها برخوردار هستند:**

(۱) بومی‌سازی ریزپردازنده‌ها.

(۲) ایجاد شبکه بومی جمع‌آوری اطلاعات.

(۳) کنترل فریب سایبری حریفان.

(۴) ایجاد امکان کشف و کنترل نفوذ اطلاعاتی مجازی.

(۵) بومی‌سازی سامانه‌های بیومتریک.

عوامل موثر زیر در حوزه انتقال اطلاعات، از اولویت بیشتری نسبت به سایر متغیرها برخوردار هستند:

(۱) کنترل ساختاریافته دقیق فضای انتقال اطلاعات.

(۲) ایجاد امکان حذف آنی اطلاعات از فضای سایبر.

(۳) خروج از سامانه‌های انتقال اطلاعات کشوری.

(۴) ایجاد بخش سازمانی امنیت فضای سایبری در نیروهای مسلح.

(۵) رعایت اصل حیطه‌بندی در انتقال اطلاعات.

✓ **عوامل موثر زیر در حوزه پردازش اطلاعات، از اولویت بیشتری نسبت به سایر متغیرها برخوردار هستند:**

(۱) تبیین سناریوی چگونگی پردازش اطلاعات حریفان در آینده.

(۲) کیفیت‌بخشی و اطمینان‌پذیری پردازش اطلاعات خودی.

(۳) پایش تحولات محیطی و مدیریت تغییرات سریع.

(۴) تقویت حوزه نظارتی و عملکردی سازمانی.

(۵) کنترل عوامل مورد پایش حریفان.

✓ **عوامل موثر زیر در حوزه ذخیره‌سازی اطلاعات، از اولویت بیشتری نسبت به سایر متغیرها برخوردار هستند:**

(۱) تبیین تاکتیک‌های پیشگیری از خرابکاری، سرقت و نفوذ (فعال و غیرفعال) به اطلاعات ذخیره‌شده.

(۲) نفوذناپذیر ساختن دسترسی‌های غیرمجاز به اطلاعات ذخیره‌شده.

(۳) کنترل دسترسی به اطلاعات ذخیره‌شده.

(۴) استفاده از تجهیزات بدون درگاه USB.

(۵) پیشگیری از انبوه یکپارچگی اطلاعات در سامانه‌های خاص.

پیشنهادهای اجرایی

۱ - فاواهای ستاد نیروهای مسلح، با همکاری معاونت جهاد خودکفایی آن نیرو، معاونت فنی و معاونت حفاظت و پیشگیری ساحفاهای نیروهای مسلح، نسبت به بومی‌سازی تجهیزات فناوری در حوزه نظامی برای رفع آسیب‌های محتمل اقدام جدی به عمل آورند و ضمن بررسی، چگونگی عملیاتی کردن راهکارهای زیر را مورد مداقه قرار دهند:

(۱) گوش به فرمان بودن عملی و جدی به اوامر فرماندهی معظم کل قوا (مدّظلّه‌العالی) در تمامی حوزه‌ها به‌ویژه در زمینه اتاق‌های فکر، علم‌محوری، خلاقیت و نوآوری، جنبش نرم‌افزاری و ...

(۲) توجه به متغیرهای مشترک بین تفکر سالم و طراحی و تولید فناوری (قدرت اندیشه و تفکر، تفکر راهبردی، دانش تفکر، کامل‌اندیشی با تشکیل کارگروه تخصصی، هماهنگ بودن با سازمان اجرایی، همسو بودن با زمان).

(۳) توجه کافی و جدی به زنجیره چگونگی طراحی و تولید فن‌آوری.

(۴) به‌کارگیری شیوه‌های خلاقیت و نوآوری در طراحی و تولید فن‌آوری.

(۵) ایجاد اتاق فکر مبتنی بر متغیرهای مشترک به‌ویژه عناصر گزینش، عناصر متخصص، با تجربه و متعهد سازمانی.

(۶) رفع موانع تفکر سالم، خلاقیت و نوآوری، تولید علم و فناوری.

(۷) تبیین سناریونویسی چگونگی طراحی و تولید فناوری حفاظتی در اتاق‌های فکر حداقل در ۲ سال آینده.

(۸) بر اساس زنجیره تفکر، به‌منظور اعمال مدیریت کارآفرینی و شکوفایی خلاقیت و نوآوری برای طراحی و تولید فن‌آوری حفاظتی.

(۹) رفع موانع موجود در حوزه‌های اتاق فکر، خلاقیت، نوآوری، توسعه، طراحی و تولید.

منابع

۱. احمدپور، محمود(۱۳۸۶). **ماهنامه تدبیر، کارآفرینی، استراتژی مناسب برای بهره‌وری**، شماره ۷۷، آبان ماه، تهران: ماهنامه الکترونیکی.

۲. اخوان، مریم(۱۳۸۴). **بررسی علل شکست پروژه‌های فناوری اطلاعات و ارائه راهکارهای پیشگیری از آن**، کنفرانس IKT 2005.

۳. ادوارت، والترز(۱۳۸۶). **عملیات و اصول جنگ اطلاعات**، ترجمه غلامعلی جان‌گداز، تهران: دانشکده امام باقر علیه‌السلام.

۴. آزاده دل، رمضان علی(۱۳۸۴). **معماری سازمانی فن‌آوری اطلاعات و چالش‌های آن**، نخستین همایش سراسری مشترک انجمن‌های علمی C4I &ICT وزارت دفاع، تهران: وزارت دفاع و پشتیبانی نیروهای مسلح.

۵. استمپل، جان ری(۱۳۷۷). **درون انقلاب ایران**، ترجمه منوچهر شجاعی، تهران: رسا.

۶. افتخاری، اصغر(۱۳۸۱). «سیاست امنیتی ایران»، **فصلنامه دفاعی امنیتی**، سال نهم، شماره ۳۳.

۷. برامویی، نرجس(۱۳۷۸). «سرزمین و فرهنگ مردم بلوچستان»، **فصلنامه مطالعات ملی**، پاییز، شماره ۱۰.

۸. **بررسی مکانیزم‌های امنیت در سامانه‌های C4I**(۱۳۸۷)، مؤسسه آموزشی و تحقیقاتی صنایع دفاعی.

۹. بررسی اسناد تاریخی (۱۳۷۸). **چپ در ایران**، جلد اوّل، تهران: مرکز اسناد تاریخی جمهوری اسلامی ایران.

۱۰. حسنوی، رضا و محمد مجتهدی نژاد(۱۳۸۳). «درآمدی بر جنبش نرم‌افزاری یا فناوری نرم»، **فصلنامه راهبرد دفاعی**، سال دوم، شماره ششم.

۱۱. رزمخواه، محمدرضا(۱۳۸۳). «نقش اطلاعات در نیروهای مسلح و تأثیر آن بر بنیه دفاعی کشور»، **فصلنامه مطالعات دفاعی راهبردی**، سال ششم، شماره نوزدهم.

۱۲. سادوسکای، جورج دمپزی، جیمز اکس، گرین‌بگ، آلن، جی، مک، باربارا، شوارتز، آلن(۱۳۸۴). **راهنمای امنیت فناوری اطلاعات**، ترجمه مهدی میردامادی و گروه مترجمین، تهران: دبیرخانه شورای عالی اطلاع‌رسانی.

۱۳. علوی‌فر، سید ناصر(۱۳۸۲). **جهان زیر سلطه سازمان‌های اطلاعاتی**، تهران: نشر دواوین.

14.Doty ،T(1997). "**Internet Security: Vulnerabilities ،Threats and Mitigation** ،" ACM Professional Development Seminar ،University of Maryland ،Nov.
15. Gosselin ،R.J(1997). "**External Threats to Computer Security in Networked systems** ،" pp. 63-80.
16.Hutt ،A. e. s. Bosworth ،and D. B Hoyt(1995). **Computer Security Handbook** ، New York: John Wiley & Sons ،3d ed.
17. Opplinger ،R.(1996**). Authentication Systems for Secure Networks** ،Norwood ، MA: Artech House.
18. Duyvesteyn sabelle & Angstorm Jan (2005). "**Rethinking the Nature of war**" ، London: Routledge.
19.**Trusted Database Management System Interpretation**(1991) "NCSC-TG-021 ، Version 1 ،Apr.
20. Afshar Heleh (2006). "**An Assessment of Agricultual DeveLoment Policiesim in Iran**" in Heleh Afshar.cd. Iran a Revolution in Tumoil.