توسعه شبکه ملی دیتا، چالش‌های فراروی و تهدیدهای متوجه امنیت ملّی

دکتر ابراهیم حسن‌بیگی*

چکیده

فناوری اطلاعات؛ مانند هر دستاورد بشری واجد فرصت‌های بی‌نظیر و در همان حال حامل چالش‌های مختص خود است. سرقت اطلاعات، خرابکاری، از کاراندازی سیستم رایانه‌ای، کلاهبرداری و جاسوسی از جمله تأثیرات مخرب فناوری اطلاعات برای حیات بشری است. توسعه اینترنت و جهان شمولی آن در حوزه‌های گوناگون زندگی بشر در سطوح فروملّی، ملّی و فراملّی، سازمان‌ها و دولت‌ها را با چالش‌های جدیدی روبه‌رو ساخته است.

در مقاله‌ی حاضر با عنایت به گسترش فزایندهٔ فناوری اطلاعات و ارتباطات و پیامدهای[1] آن، تلاش شده است که به توسعه شبکه ملّی دیتا، چالش‌های فراروی؛ و تهدیدهای متوجه امنیت ملّی جمهوری اسلامی ایران از زاویه‌ی امنیتی توجه شود.

---

* - پژوهشگر و جانشین ریاست دانشگاه عالی دفاع ملی

1 -Impacts

مقدمه

دنیا در حال گذار است. دستاوردهای علمی بشر که تحولات و دگرگونی‌های شتاب‌زا و شتاب‌زی را در ساخت‌های گوناگون زندگی بشر ایجاد می‌کنند، آثار و پیامدهای خود را بر حوزه‌های گوناگون حیات فردی، خانوادگی، اجتماعی، ملّی، منطقه‌یی و بین‌المللی بر جای می‌گذارند و بخش‌های مختلف حیات انسان را دستخوش بسامدها و پیامدهای مختلف می‌سازند.

یکی از مهم‌ترین دستاوردهای بشر گسترش فزاینده فناوری اطلاعات و ارتباطات است که به دگرگونی در ابعاد مختلف مؤلفه‌های اقتصادی، سیاسی، اجتماعی، فرهنگی و نظامی منجر خواهد شد؛ و مجموعه فعالیت‌ها در زمینه‌های تولید، بهره‌برداری، بانکداری و برقراری ارتباطات با رایانه‌های شبکه‌بندی شده را دستخوش تغییرات جدی قرار خواهد داد. هرچه زمان می‌گذرد ابعاد وابستگی زیرساخت‌های حیاتی در زمینه‌های اقتصادی، مسایل اجتماعی ـ فرهنگی، دفاعی و امنیتی به اطلاعات و ارتباطات، آشکارتر می‌شود.

چنین فرآیندی، علاوه بر آسیب‌پذیری‌های داخلی ناشی از زیرساخت‌های فنی و نیز کمبودها و ضعف‌های آموزشی، طیف وسیعی از عوامل مهاجم را نیز با خود به همراه دارد؛ و علاوه بر نگرش اثباتی معطوف به زمینه‌سازی و زمینه‌پروری مناسب جهت دستیابی به زیرساخت‌های فنی، رفع کمبودها و ضعف‌های آموزشی به نگرش سلبی معطوف به آماده‌سازی و مهیا شدن در برابر تهدیدهای ناشی از بهره‌برداری‌های منفی از آن نیز توجه می‌نماید.

قدر مسلم آن است که همگان با توسعه روزافزون فناوری اطلاعات؛ ابزارها و شیوه‌های آن، از فرصتی طلایی بهره‌مند شده‌اند؛ اما همگام با توسعه روزافزون فناوری اطلاعات؛ شیوه‌های مختلف تهاجمی نیز به سرعت گسترش یافته و توان تخصصی و درجه پیچیدگی نفوذگران عامل تخریب یا غارت سیر صعودی پیدا کرده است. علاوه بر پیچیدگی روزافزون ابزارهای مورد استفاده در حملات رایانه‌یی، بر شمار عاملانی که قدرت یورش علیه زیرساخت‌ها را دارند، هم روز به روز افزوده می‌شود.

این یورش تنها در فضا و زمانه‌ی جنگی صورت نمی‌پذیرد بلکه در زمان صلح نیز فعال است. در زمان جنگ یا بحران دشمن می‌تواند به اتکای اطلاعات جمع‌آوری شده به زیرساخت‌های حیاتی و فعالیت‌های اقتصادی عمده حمله و یا با مخدوش کردن اعتبار و سیستم‌های اطلاعاتی نزد افکار عمومی و نیز ایجاد نگرانی و هراس عمومی، شورش‌های گسترده و براندازی را تدارک نماید. در دوران صلح و آرامش احتمال جاسوسی دشمنان درباره اوضاع عمومی کشور و دستیابی به اطلاعات طبقه‌بندی شده و نیز جمع‌آوری اطلاعات در مورد مواضعی از قبیل اهداف کلیدی و رخنه در زیرساخت‌ها به طرق و سایر شیوه‌های دستیابی به اطلاعات به منظور تدارک تهاجم‌های سایبری، متصور، بلکه مسلم است.

یکی از ویژگی‌های فناوری اطلاعات و به ویژه اینترنت، امکان ساماندهی و تدارک تهاجم سازمان یافته از فواصل دور علیه اهداف از پیش تعیین شده می‌باشد و به مهاجمان این امکان را می‌دهد تا علیه اهداف خود اقدام و ایجاد اختلال کنند. این فناوری علاوه بر اینکه موجب آشکار شدن نقاط ضعف موجود در زیرساخت‌های حیاتی می‌شود با ایجاد ارتباط مخرب مانع از واکنش‌های دفاعی و یا ایجاد تأخیر در آنها می‌گردد. در تهاجم از طریق شبکه اینترنت حتی کشورهایی که به دلیل موقعیت جغرافیایی از بسیاری از تهاجم‌های فیزیکی مصون بودند، دیگر، در امان نخواهند بود. زیرا در فضای مجازی مرزهای کشورها مفهوم چندانی نداشته و اطلاعات بی‌محابا از مرزبندی‌های سیاسی، اخلاقی و اجتماعی عبور کرده و تبادل می‌شود.

امروزه، اهمیت درک چنین فضایی در ارتباط با مفهوم امنیت ملّی، از مهمترین ادراکات ضروری برای جوامع مختلف است؛ و به تبع این اهمیت، تلاش‌های همه جانبه محققان و پژوهشگران را در بازتابش روشنایی بر ابعاد مختلف موضوع طلب می‌کند. آنچه در این مجال کوتاه در پی آن خواهیم بود؛ بررسی اجمالی موضوع توسعه‌ی شبکه ملّی دیتا، چالش‌های فراروی و تهدیدهای متوجه امنیت ملّی است.

فناوری اطلاعات : "تهدید و امنیت ملّی"چشم‌اندازی از چالش‌های فراروی

سرقت اطلاعات، خرابکاری، از کارانداختن سیستم‌های رایانه‌یی، کلاهبرداری و

اینترنت ـ فارغ از وجوه مثبت و فرصت‌های حاصل از آن ـ در جوامع و گسترش آن حتی به درون منازل و محل کار مردم و نیز جهان شمول بودن و وجود خطرات بالقوه آن، سازمان‌ها و دولت‌ها را با چالش‌های جدید روبه‌رو ساخته است. این چالش‌ها در سه ساحت: ۱ ـ دسترسی غیرمجاز ۲ ـ استفاده غیرمجاز ۳ ـ ریزش ناخودآگاه «اطلاعات» موجد چالش‌های جدید در برابر دولت‌ها شده است.

در راستای مقابله با پیامدهای ناشی از بروز چنین چالش‌هایی است که مکانیزم‌های متفاوتی نیز در تقابل با این پیامدها به وجود آمده است؛ از جمله دیوارهای آتش، سیستم تشخیص نفوذ و سیستم فیلتر؛ برنامه‌ریزی و در کنار این سیستم‌ها، مکانیزم‌های شنود، مراقبت و مانیتورینگ نیز گسترش یافته‌اند که با اهداف گوناگون مراقبتی یا جاسوسی به کار می‌روند.

در چنین فضایی بررسی عالمانه‌ی ارتباط میان توسعه شبکه ملی دیتا، «چالش‌های فراروی» و «امنیت ملی» در مرحله نخست مبتنی بر تعریف مفهوم تهدید و ارتباط آن با دانشواژه‌ی تلفیقی «امنیت ملّی» است.

در حوزه‌ی ادبیات سیاسی ـ امنیتی دو گفتمان «امنیت منفی» و «امنیت مثبت» از یکدیگر قابل تمییز هستند. در هر دو گفتمان مذکور مفهوم امنیت؛ دانشواژه‌یی مستقل نیست بلکه فهم آن در گرو ادای مفهوم تهدید است؛ به تبع این وابستگی مفهوم «تهدید» نیز در کنار پدیدگی مفهوم «دشمن» قرار می‌گیرد؛ هر دو گفتمان امنیت منفی و مثبت بر این نکته نیز صحه می‌گذارند؛ اما در گفتمان امنیت منفی وجوه بیرونی و سخت‌افزاری مفهوم تهدید و دشمن مدنظر قرار می‌گیرد؛ مفهوم تهدید در حوزه‌ی فرامرزی مورد عنایت واقع می‌شود؛ و دشمن در پیکره‌ی «تهدید کننده‌ی تمامیت ارضی و استقلال ملی» غالباً با اسلحه و بهره‌برداری از قدرت نظامی رخ نشان می‌دهد.

این درحالی است که درگفتمان امنیت مثبت، «تهدید» درقالب مجموعه‌ی عوامل نرم‌افزاری و سخت‌افزاری‌یی چهره می‌نمایاند که موجب تضعیف و کاهش «توان و قدرت ملی» برای دستیابی به «منافع و اهداف ملّی» می‌شود. در این نگرش «تهدید» در همه‌ی ابعاد تضعیف‌کننده‌ی قدرت ملی و در حوزه‌های مختلف فعالیت‌های انسانی در

محیط داخلی و بیرونی و در جنبه‌های فردی، اجتماعی، ملی، منطقه‌یی و بین‌المللی قابل توجه است. لذا؛ در ارتباط با پیوند میان توسعه شبکه ملّی دیتا، چالش‌های فراروی و امنیت ملّی؛ «مفهوم تهدید»؛ دربرگیرنده‌ی پیامدهای ناشی از توسعه فناوری اطلاعات در تضعیف و کاهش توان و قدرت ملّی برای دستیابی به اهداف ملّی تعریف شده در فضا و زمانه‌ی تاریخی معین است.

به خاطر اهمیت جهانی فضای مجازی ـ ارتباطات رایانه‌یی ـ آسیب‌پذیری‌های موجود در سراسر جهان کاملاً قابل پیش‌بینی است و هرکس در هر نقطه جهان به صرف دارا بودن توان آشکارسازی و در اختیار داشتن ابزارهای لازم می‌تواند مبادرت به حمله و آسیب رساندن به فضای مجازی هدف نماید. لذا مهاجمان رایانه‌ای قادرند بدون هیچگونه هشداری به شبکه‌های ملّی یورش آورده و با آنچنان سرعتی گسترش یابند که بسیاری از مواضع هدف حتی فرصت شنیدن صدای آژیر خطر را نیز پیدا نکنند و حتی درصورت هشدار قبلی هم به احتمال زیاد فرصت لازم برای محافظت از خود را نداشته باشند.

دربخش مربوط به قوانین، مسایل حقوقی و قضایی نیز، اینترنت قواعد سنتی حاکم بر رسیدگی‌های قضایی را دستخوش تحولات اساسی کرده است. تعریف از جرایم در محیط‌های مجازی انطباق چندانی با تعاریف کلاسیک نداشته و در بسیاری از موارد متفاوت است. در سیستم امنیتی متعارف برای اجرا و اعمال مقررات جزایی یک محدوده و مرز جغرافیایی وجود دارد که همیشه و به طور اصولی محدود به خاک یک کشور و تحت حاکمیت یک دولت می‌شود. به عبارت دیگر اعمال حاکمیت از سوی یک دولت مطرح است. همچنین شرایط استرداد مجرمین عدم تعارض این عمل با حاکمیت دولت‌ها در عرصه‌های سیاسی و قضایی است.

بنابراین رسیدگی به جرایم ارتکابی در محیط‌های مجازی ـ از تعریف جرایم مجازی گرفته تا شیوه‌های مجازات جرایم و... ـ در ابعاد داخلی و بین‌المللی با کمبودها و چالش‌هایی اساسی مواجه است ـ جرایمی درمحیط‌های مجازی به وقوع پیوسته که سیستم قضایی کشورهای مختلف نتوانسته‌اند با آنها برخورد جدی نمایند. همین امر باعث شده که شبکه اینترنت فارغ از سلطه قوانین در دنیا و فضای

از دیدگاه حقوق خصوصی نیز اینترنت چالش‌هایی از قبیل صلاحیت محلی دادگاه‌ها، قانون حاکم بر قضیه و تعارض قوانین کشورهای مختلف را فراروی همهٔ کشورها قرارداده است. همچنین، در تجارت الکترونیکی مسایل مربوط به تصدیق امضای الکترونیک و تضمین صحت داده‌ها، مشکلات جدیدی ایجاد کرده است.

در ابعاد حقوقی، پیدایش و تکامل تهدیدهای اینترنتی موجب بروز جرایم جدید و بالطبع آیین دادرسی خاصی شده و از سویی برخی رشته‌های علوم جنایی را با چالش مواجه کرده است. این تهدیدها کاملاً در بستر و فضای مجازی ـ محیط دیجیتالی محض ـ ارتکاب می‌یابند و از حیث میزان خطر، حجم ضرر و زیان و سهولت ارتکاب بزه‌دیدگان از جرم با افزایش ناگهانی مواجه شده است. این جرایم بسته به هدف و موضوع جرم، متمایز از دیگر جرایم محسوب می‌شوند.

به عنوان شاخص‌ترین این اهداف می‌توان از هدف ضدیت با امنیت ملّی ـ داخلی یا خارجی ـ یا علیه اموال، آسایش عمومی، اخلاق، عفت عمومی و... یاد کرد. از این‌رو، یکی از اهداف تحت تأثیر جرایم مذکور، چالش‌های امنیتی کلانی است که به واسطه‌ی ویژگی‌های یادشده‌ی بالا خطرات بسیاری را برای کشور درپی خواهد داشت.

این جرایم یا تهدیدها، گاه به طور مستقیم علیه امنیت کشور ارتکاب می‌یابند که شاخص‌ترین آنها جاسوسی کامپیوتری؛ و سابوتاژ کامپیوتری است و گاه به طور غیرمستقیم رویکرد امنیتی داشته و امنیت ملی را به چالش می‌کشند. تهدیدهای خارجی از ناحیه کسانی است که به بخش‌های نظامی و آژانس‌های امنیتی کشورهای خارجی و حتی شرکت‌هایی که وابستگی زیادی به آن کشورها دارند، وابسته‌اند.

آسیب‌پذیری خطوط اطلاعاتی دیجیتالی به وضعیت کشورها بستگی دارد، طبیعتاً در کشورهایی که امنیت و استاندارد شبکه در سطوح عالی رعایت نمی‌شود، مجرمین راحت‌تر اطلاعات محرمانه ملّی را کسب می‌کنند و از سویی افشای آنچه در تعارض با مصالح امنیتی می‌شود، نیز آسان‌تر صورت می‌گیرد.

قوانین کیفری در عین داشتن ابهام، هرگز باتحولات همراه نشده است؛ و از این‌رو یک طیف بسته از اصطلاحات تحت حمایت آنها قرار می‌گیرد؛ در حالیکه طیف جاسوسی سیاسی و نظامی به جاسوسی صنعتی، تجاری، اقتصادی، مالی و... تسری

یافته و از سویی شکل‌های جدید موجب فرار برخی افراد از دامنه جرایم می‌شود، نوع ارتکاب نیز در طول زمان تکامل یافته و شکل جدید آن به صورت دیجیتالی روی می‌دهد.

سابوتاژ فی‌حد ذاته تهدید خطرناکی است که امنیت کشورها را به چالش می‌کشد، مصادیقی همچون انفجار در خطوط لوله انتقال نفت و گاز، کابل‌های مخابراتی، خطوط راه‌آهن، صنایع هواپیمایی و... یا دیگر اقدامات مجرمانه چالش‌های امنیتی زیادی را ایجاد می‌کند. از آنجائیکه درحال حاضر کنترل عملکردهای اداری ـ حکومتی توسط کامپیوتر صورت می‌گیرد، چنانچه، هدف اقدامات خرابکارانه مجرمین قرار بگیرد، حوادث مهمی روی می‌دهد.

برخی تهدیدها اگرچه فی‌حد ذاته به عنوان جرایم مستقیم علیه امنیت دسته‌بندی نمی‌شود، اما گاه به علت رویکرد امنیتی از حیث هدف و انگیزه‌ی تهدیدکنندگان و گاه از حیث نتیجه کار جزء تهدیدات علیه امنیت نیز می‌توانند مورد بحث واقع شوند.

سطوح چالش‌ساز فناوری اطلاعات و تهدیدهای متوجه امنیت ملّی

با عنایت به درجه‌بندی اتحادیه بین‌المللی مخابرات ITU در ارتباط با درجه‌بندی میزان گسترش اینترنت در یک کشور، میزان گسترش اینترنت در ایران، در تراز «دو» یعنی «نوپا» قرار می‌گیرد (پیام ارتباط، شمارهٔ ۲۶، ۱۳۸۱).

تراز/ درجه	نام	توضیح
تراز صفر	ناموجود	در چنین کشوری هیچ رایانه‌ای از طریق خط تلفن شهری به اینترنت وصل نیست. کاربران انگشت‌شماری از طریق تلفن بین‌المللی به فراهم آوردن خدمات اینترنتی خارجی وصل می‌شوند.
تراز یک	جنینی	ضریب نفوذ اینترنت کمتر از ۰/۱ درصد
تراز دو	نوپا	ضریب نفوذ اینترنت بزرگتر یا مساوی ۰/۱ درصد
تراز سه	تثبیت شده	ضریب نفوذ اینترنت بزرگتر یا مساوی ۱ درصد

با عطف توجه به نیاز آینده کشور به توسعه شبکه فناوری اطلاعات، و از سویی دیگر چالش‌ها و تنگناهای موجود در این ارتباط، می‌توان به دسته‌بندی چالش‌های موجود پرداخت؛ و سپس با تعمق درچنین فضایی، تأثیرات و پیامدهای آنرا بر حوزه‌ی امنیت ملّی مورد توجه قرار داد؛ در بررسی و حیطه‌شناسی چالش‌های موجود، حوزه‌های چالش برانگیز ذیل قابل احصا هستند:

الف ـ چالش‌های قانونی:

(۱). ابهامات موجود در مورد به رسمیت شناختن حقوق مالکیت‌های معنوی.

(۲). تعریف نشدن حقوق پدید آورنده در قوانین.

(۳). فقدان قانون جامع تجارت الکترونیک.

(٤). نقض قوانین در مورد جرایم مرتبط با فناوری اطلاعات و ارتباطات.

(٥). تحریم‌های بین‌المللی و قوانین ناشی از آن در بهره‌مندی از توسعه فناوری اطلاعات.

(٦). به رسمیت شناخته نشدن امضای الکترونیکی.

(۷). عدم وجود ضمانت اجرایی درجهت حمایت از حقوق مصرف کننده.

ب ـ چالش‌های مربوط به ساختار بازارها:

(۱). مشکلات ناشی از انحصار دولتی مخابرات.

(۲). موانع فعالیت بخش خصوصی.

(۳). ساختار سنتی بازارها.

ج ـ چالش‌های اجتماعی و فرهنگی:

(۱). سطح پایین دانش عمومی در زمینه فناوری اطلاعات و ارتباطات.

(۲). عدم اعتماد عمومی در مورد امنیت اطلاعات.

هـ ـ چالش‌های مربوط به زیرساخت‌های نرم‌افزاری و سخت‌افزاری:

(۱). عدم تناسب آموزش‌های تخصصی با نیازهای جامعه.

(۲). امنیت پایین شبکه‌های مخابراتی.

(۳). ضعف زیرساخت‌های مخابراتی.

(٤). نبود استانداردهای مناسب در ارتباط با:

۱/٤ ـ استانداردهای تبادل اطلاعات

۲/٤ ـ استانداردهای کدگذاری کالا و خدمات

۳/٤ ـ استانداردهای کدمکان

٤/٤ ـ استانداردهای فونت فارسی

(٥). نبود ابزارهای داد و ستد الکترونیکی و عدم گسترش بانکداری الکترونیکی.

توضیح هرکدام از این چالش فرصتی مقتضی را طلب می‌نماید؛ اما با عنایت به وجود چالش‌های موجود در سطوح چهارگانه فوق و شاخصه‌های وابسته به آن می‌توان اذعان نمود که فضای بهره‌مندی از فناوری اطلاعات در ایران به واسطه‌ی چالش‌های موجود براساس تقسیم‌بندی‌های سیستم‌ها به سه دسته‌ی: ۱) در حال تعادل ۲) نزدیک به تعادل و ۳) دور از تعادل؛ در موقعیتی که در میان فضاهای دور از تعادل و نزدیک به تعادل در حال نوسان است و با توجه به تعریف «تهدید» در نگرش حاضر، به تبع قرار گرفتن در چنین فضایی، اتلاف انرژی حاصل و پیامدهای ناشی از این اتلاف انرژی در دستیابی به توان ملی در این زمینه بستر اصلی تهدیدهای متوجه امنیت ملّی را فراهم می‌سازد.

از دریچه‌ی چنین نگاهی ضرورت دارد تا به تهدیدهای متوجه امنیت ملی توجه داشته باشیم. در گذشته ذهن بشر مفهوم «تهدید» را در کنار پدیده‌ی «تقدیر و سرنوشت» مورد توجه قرار داده است؛ و آنرا با دانشواژه‌ی «مخاطره» هم‌نشین و جانشین ساخته است. واژه‌ی «مخاطره» به معنای خطرکردن و از میان سخره راه بازکردن، از کلمات مورد استفاده در میان دریانوردان اسپانیایی بود؛ که در قرن هفده میلادی به زبان انگلیسی راه یافت؛ و واجد دو جنبه‌ی طبیعی و انسانی شد؛ به عبارتی

مفهوم مخاطره از شناخت این واقعیت نشأت گرفت که تحولات نامطلوب ممکن است، نه تنها از طبیعت، بلکه در اثر فعالیت‌ها و تصمیمات ابناء بشر نیز رخ دهد.

همسو با تحول جوامع بشری و پیدایش فرآیند دولت‌سازی، به تدریج دال مخاطره مدلول‌های خاصی را به اذهان متبادر نمود و در این فراگرد مفهوم تهدید از بطن تطورات مزبور سربرآورد. عده‌یی هرگونه تجاوز به حق حاکمیت دولت‌ها در ادارهٔ امور داخلی و خارجی را تهدید تلقی نمودند و برخی مخاطراتی که اهداف و ارزش‌های حیاتی یک کشور را به گونه‌یی در معرض خطر قرار می‌دهد که بیم آن رود در اهداف و ارزش‌های مذکور تغییر اساسی صورت پذیرد؛ را تهدید خواندند. تهدیدها در دوره‌های کهن به طور معمول از مؤلفه‌های ذیل تأثیر می‌پذیرفته‌اند :

۱ ـ عمدتاً با منشأ خارجی تصور می‌شدند،

۲ ـ مبتنی بر قدرت نظامی بودند،

۳ ـ متکی بر حضور فیزیکی دشمن بودند،

٤ ـ آگاهی از تهدیدها گسترده نبود،

٥ ـ دامنه تهدیدها محدود بود،

٦ ـ دراکثر تهدیدها دولت‌ها نقش بسیار مؤثری داشتند

۷ ـ تهدیدها به راحتی قابل تشخیص بودند،

به واسطه‌ی پهنا و گستره‌ی تغییر و تحولات در سپهر فعالیت‌های گوناگون و وجوه مختلف حیات بشر، مفهوم تهدید نیز از صیرورت دور نماند و شکل و ماهیتی نوین یافت. این چهرهٔ نوین با وجود فقدان ماهیت شفاف، از شاخصه‌های قابل تعمقی برخوردار است:

۱ ـ اکثر این تهدیدها دولت محور نیستند؛ ۲ ـ فاقد فضای جغرافیایی معین هستند ۳ ـ نمی‌توان آنها را با اتکاء به سیاست‌های دفاعی سنتی مدیریت نمود؛ این در حالی است که با ورود به عصر جهانی شدن، مفهوم تهدید از برخی زوایای دیگر نیز قابل بررسی است:

الف) بسط جهانی محیط‌ها و فضاهای تهدید.

ب) تهدیدهای برآمده از محیط ساخته شده یا طبیعت اجتماعی شده.

ج) گسترش محیط تهدیدهای نهادی
د) جهانی شدن تهدید از نظر تراکم
هـ) آگاهی جهانی نسبت به تهدیدها
و) تهدیدهای ناشی از مشروعیت و اقتداریابی بازیگران فراملی
ز) تهدیدهای ناشی از اقتصاد جهانی؛
ح) ابهام در شناسایی کشورهای تهدید کننده.

در چنین شرایطی اکثر دولت‌ها به ویژه دول جهان سوم در مواجهه با تهدیدات باید سه مؤلفه را به طور همزمان درنظر بگیرند:

(۱). محیط امنیتی: این مؤلفه معیار اساسی درخصوص تهدید خارجی و مدل‌های همکاری و اتحاد است.

(۲). سخت‌افزارها: مقدورات فیزیکی، دکترین‌های عملیاتی، ساختار قدرت و گزینش جنگ‌افزارها را دربر می‌گیرد.

(۳). نرم‌افزارها: که اشاره به شاخص‌های مشروعیت‌سیاسی، وحدت ملّی و توان سیاست‌گذاری عمومی دارد.

اگرچه در فضای مناسبات دوقطبی، توجهات معطوف به محیط امنیتی و سخت‌افزارها بود؛ امروزه، درک واقع بینانه از تهدیدات در گرو توجه به نرم‌افزارها است که در مقام حلقه‌ی واسطه بین محیط امنیتی و سخت‌افزارها قرار می‌گیرد. در این دیدگاه، نادیده انگاشتن وجه نرم‌افزاری درک دولتمردان را از پیچیدگی روابط میان عوامل دروندادی تهدیدات و ظرفیت‌های داخلی از یک طرف و کل بروندادهای سیاسی و ساماندهی امور امنیتی از سوی دیگر، تضعیف می‌کند (تاجیک، ۱۳۷۷، ص ۱۱۸).

تهدیدسازان فضای مجازی

مهم‌ترین تهدیدکنندگان فضای مجازی درچهار گروه عمده قابل دسته‌بندی است: گروه نخست تهدیدات ناشی از عوامل خارجی هستند. این تهدید از ناحیه کلیه کسانی صورت می‌پذیرد که به یک کشور خارجی از قبیل بخش‌های نظامی و آژانس‌های

دوم، تروریست‌ها و گروه‌های افراطی هستند. این افراد ممکن است به دولت خاصی وابسته نباشند، ولی در راستای اهداف خود به خرابکاری مبادرت ورزند. تهدید سوم از ناحیه گروهی است که شامل جنایتکاران و سازمان‌های جنایی است؛ این گروه نه تنها جرایم سازمان یافته‌ی بزرگ را در فضای مجازی مرتکب می‌شوند، بلکه به صورت انفرادی نیز اقدام می‌کنند. ویژگی خاص فضای سایبر باعث شده که یک فرد به تنهایی بتواند جرایم بزرگی را مرتکب شود. چهارمین گروه از تهدیدسازان فضای مجازی را کاربران داخل سازمان‌ها و نیروهای خودی تشکیل می‌دهند.

هر تهدید از دو مؤلفهٔ «قصد و نیت» و «قابلیت» تشکیل می‌شود. قابلیت از دو شاخصه‌ی سازماندهی و ابزار تأثیرپذیری و ابزار نیز از تجهیزات و مهارت در کار متأثر می‌گردد. در چنین فضایی از شاخصه‌های تودرتو، مفاهیم تلفیقی «عملیات اطلاعاتی» و «جنگ اطلاعات» در فضای مجازی از اهمیت کلیدی برخوردار می‌گردند.

اهمیت فضای مجازی برای عملیات نظامی به گونه‌یی است که سازمان‌های نظامی از هم‌اکنون برای آن برنامه‌ریزی می‌کنند. برای مثال وزارت دفاع آمریکا در چشم‌انداز ۲۰۲۰ خود این موضوع را درنظر گرفته و از عبارت‌های جدیدی از قبیل «عملیات اطلاعاتی» (IO) برای نمایش زمینه‌های تهاجمی ـ تدافعی در محیط اطلاعاتی استفاده کرده است.

عملیات اطلاعاتی و جنگ اطلاعاتی

به کلیه فعالیت‌های لازم برای حمله به اطلاعات و سیستم‌های اطلاعاتی دشمن و همچنین دفاع از اطلاعات و سیستم‌های اطلاعاتی خودی، عملیات اطلاعاتی گویند. در تعریف جنگ اطلاعات ـ IW ـ نیز آمده است: جنگ اطلاعاتی بخشی از عملیات اطلاعاتی است و به هر فعالیت نظامی که در زمان جنگ اتفاق بیافتد و در محیط اطلاعاتی، انجام شود، اطلاق می‌شود.

نگرانی ازحملات کشورهای خارجی و جنگ اطلاعات به قدری زیاد است که حتی کشوری مثل آمریکا را که خود حرف اول را در فناوری اطلاعات می‌زند نیز، به چاره‌اندیشی وادار کرده است (Serabian.2000).

هزینه کم، سهولت دسترسی، کامپیوترهای قدرتمند و ابزارهای قوی موجود، برخی از قابلیت‌های مهمی هستند که در اختیار سازمان‌ها در راستای انجام عملیات اطلاعاتی قرار می‌گیرند. ابزارهایی چون کدهای خطرناک، ویروس‌ها و کرم‌ها، اسب‌های تروا، بمب‌های منطقی و... نمونه‌هایی از این ابزارها هستند. سلاح‌های در دسترس دیگری که جریان داده‌ها و اطلاعات را تخریب می‌کنند از قبیل تفنگ‌های فرکانس رادیویی پرانرژی که با یک سیگنال فرکانس بالا وسایل الکترونیکی را از کار می‌اندازد؛ نیز به صورت محدودتر قابل استفاده‌اند.

با چنین امکانات و ابزاری جنگ اطلاعاتی در یک فضای غیرایزوله انجام می‌پذیرد. جنگ اطلاعات یک فعالیت سجزا «ایزوله» محسوب نمی‌شود. این جنگ هم در حیطه‌ی فعالیت‌های دولت‌ها و هم در حوزه‌ی برخوردهای انسانی قرار می‌گیرد. در یک دسته‌بندی کلی این فعالیت‌ها را می‌توان در چهار قلمرو : ۱) امنیت ملّی ۲) جرایم ۳) حقوق فردی ٤) دستیابی غیرمجاز بررسی نمود. در مهم‌ترین بخش این قلمروهای چهارگانه یعنی «امنیت ملّی» رویکردهای پنج‌گانه‌ی ذیل قابل تعمق است:

۱ ـ حمله به شبکه‌های رایانه‌یی؛ عملیات برای خرابی، حذف، تغییر و به هم ریختن اطلاعات کامپیوترها و یا شبکه‌های کامپیوتری دشمن.

۲ ـ جنگ الکترونیک متوجه بهره‌برداری از امواج الکترومغناطیس و انرژی متمرکز در حوزه‌ی فعالیت‌های نظامی برای کنترل طیف الکترو مغناطیسی.

۳ ـ عملیات روانی؛ مبتنی بر برنامه‌ریزی‌های متوجه انتقال اطلاعات گزینشی به مردم کشورهای خارجی برای تأثیرگذاری بر دولت‌ها، سازمان‌ها، گروه‌ها و حتی اشخاص خارجی می‌باشد.

٤ ـ فریب نظامی متوجه طراحی عملیات عمدی برای گمراه کردن تصمیم‌گیرندگان ارتش دشمن استفاده می‌گردد.

۵ ـ جنگ اطلاعات رایانه‌یی که متوجه فراگیر نمودن، امکان حمله به فضای مجازی با مقیاس بزرگ است.

براساس گزارشات سازمان جاسوسی آمریکا، چین یکی از بازیگران مطرح در توسعه‌ی قابلیت‌های جنگ اطلاعات است. پس از پایان جنگ خلیج‌فارس در سال

تشکیل گروه‌هایی که آمادگی جنگ در محیط مجازی را داشته باشند، تلاش کرده است (bristow, 1998).

قلمرو امنیت ملّی در محیط سایبر شامل مسایلی در سطح ملّی از قبیل عملیات جاسوسی کشورهای خارجی، جنگ و برخورد نظامی، تروریسم و عملیات برعلیه یک کشور از طرف سازمان‌های غیردولتی می‌شود. باید به یاد داشته باشیم که این قلمروها از یکدیگر جدا نیستند؛ به طور مثال نفوذ رایانه‌ای معمولاً جرم تلقی شده و حقوق فردی را نقض می‌کند و در مواقعی که از حالت بازی و تفنن خارج شده و در اختیار جانیان سازمان یافته، گروه‌های جاسوسی، گروه‌های تروریستی یا واحدهای نظامی قرار می‌گیرد. نقض حقوق فردی، خود یک جرم محسوب می‌شود. این تعاریف و دسته‌بندی‌ها حالت جامع و مانع ندارد و یک نگاه کلی را عرضه می‌نماید.

با توجه به آنچه آمد اهداف و لایه‌های جنگ اطلاعاتی در سه سطح قابل تعمق است:

۱ ـ لایه سیستم اطلاعات: این سطح شامل عناصر مادی تولید، انتقال و ذخیره اطلاعات می‌باشد و حملات علیه سیستم‌های اطلاعاتی باعث پیامدهای تکنیکی می‌شود.

۲ ـ لایه مدیریت اطلاعاتی: این سطح روندهای پردازش و اطلاعات، مدیریت می‌شود و حمله در این سطح باعث پیامدهای عملی می‌گردد.

۳ ـ لایه تصمیم‌گیری: این سطح مربوط به تصمیم‌گیری و استفاده از اطلاعات در امر تدوین و تنظیم سیاست و تصمیم است. حملات در این لایه موجب پیامدهای عملیاتی می‌شود.

از نقطه‌نظر دفاعی مشکل است که بتوان مشخص نمود حمله از کدام قلمرو برخاسته است: اگر سیستم کامپیوتری مورد هجوم قرار گرفته است آیا در اثر بازی جوانان سرکش و ماجراجوست یا یک سازمان جنایی مشغول دزدیدن شماره کارت‌های اعتباری است و یا یک شرکت رقیب داخلی یا خارجی می‌خواهد اسرار تجاری را به دست آورد و یا یک گروه خرابکاری می‌خواهد به زیرساخت حیاتی کشور آسیب برساند؟

FBI با مطالعه و تحقیق در بین ۵۲۰ سازمان یا شرکت در سال ۱۹۹۸، انواع حملات و سوء استفاده‌ها را به ترتیب دسته‌بندی کرده است (نمودار ۱):

۱ ـ ویروس

۲ـ سوء استفاده از شبکه توسط کارکنان سازمان

۳ ـ سرقت Laptop

٤ ـ دسترسی غیرمجاز توسط کارکنان داخل سازمان

۵ ـ نفوذ غیرمجاز به سیستم

٦ ـ سرقت اسرار تجاری

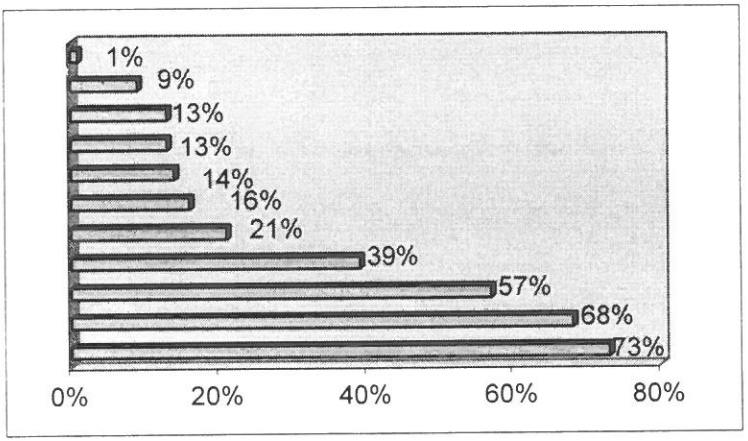
۷ ـ کلاهبرداری مخابراتی

۸ ـ کلاهبرداری مالی

۹ ـ خرابکاری

۱۰ ـ دسترسی غیرمجاز به سیگنال «غیرفعال»

۱۱ ـ دسترسی غیرمجاز به سیگنال «فعال»



نمودار ۱- انواع حملات و سوء استفاده‌های بررسی شده توسط FBI در سال ۱۹۹۸ از ۵۲۰ سازمان

گسترش فناوری اطلاعات، حوزه‌ی جنایات را از حیطه‌ی مرزها خارج می‌سازد و به جنایت‌های سازمان یافته‌ی فراملّی تسری می‌بخشد.

جنایت سازمان‌یافته فراملی در ابعاد گوناگون آثار مختلفی از خود برجای

نظم جهانی را مختل می‌کند و با این امر جامعهٔ جهانی و نهادهای آن را تحلیل می‌برد. بطور کلی، تزلزل نهادهای مدنی به نوبهٔ خود بی‌ثباتی و ضعف حکومت و جامعه را در برخورد با جرم و جنایت موجب می‌شود. از سوی دیگر، بر سیستم‌های اقتصادی اعم از ملی و بین‌المللی تأثیر می‌گذارد.

همچنین با قاچاق غیرقانونی زنان و کودکان و سوء استفاده‌های جنسی از آنان، افزون بر نقض حقوق بشر، آثار انسانی و فرهنگی درخور توجهی از خود برجای می‌گذارد. صحبت از ابعاد مختلف سیاسی اجتماعی، اقتصادی و فرهنگی این آثار مجال بیشتری را طلب می‌نماید.

استفاده از فناوری‌های اطلاعاتی منحصر به امور جنایی نمی‌شود. مجریان قانون نیز به گونه‌ای فزاینده از این فناوری‌ها استفاده می‌کنند و در آینده نیز چنین خواهد بود. مثلاً در زمینهٔ تحول نرم‌افزارهای پیشرفته گام‌های مهمی برداشته شده تا به روندهای تحلیلی اجرای قانون کمک شود. نرم‌افزارهایی از قبیل لیدز اوریونز[1]، دفتر یادداشت تحلیلگران و هارلکونیز دکتر واتسون[2] قابلیت‌هایی را برای موارد ذیل فراهم می کنند:

تحلیل صدای افراد در تلفن (توانمند کردن تحلیلگران برای تعیین الگوهای رابطه)، تحلیل پیوند یا رابطه (شناسایی و بصری کردن روابط بین افراد و موجودات و نیز ردیابی حرکت غیرمجاز کالاها و پول) و تحلیل تجسسی بصری (شناسایی خطوط زمانی و الگوهای تلاقی یا همگرایی).

ابزارهای دیگر کارهای ذیل را انجام می‌دهند: نظارت الکترونیکی و به گونه‌ای فزاینده شناسایی الکترونیکی نقل و انتقال‌های سیمی یا تلگرافی. سوء استفادهٔ مجریان قانون از فناوری‌های اطلاعاتی نباید حیرت‌آور باشد زیرا یک رابطهٔ رقابت‌آمیز میان مجریان قانون و سازمان‌های جنایی وجود دارد که هر دو طرف می‌کوشند با پیشرفت و کارآزمودگی دیگری برابری کنند. یکی از عوامل تعیین‌کنندهٔ سرنوشت این رقابت، رمزگذاری است. کارگزاران اجرای قانون، در عمل موفق نمی‌شوند که دولت و

1 - Leads Orions
2 - Harlequins Dr. Watson

قوهٔ مقننه را متقاعد سازند که برای روز مبادا «کلیدهایی» را تعبیه کنند تا به منظور غلبه بر رمزگذاری مورد استفاده قرار گیرند؛ در نتیجه سازمان‌های جنایی شکلی از تفوق راهبردی را بدست خواهند آورد که تعدیل و یا رویارویی با آن مشکل خواهد بود. حتی اگر سازمان‌های جنایی منافع سرنوشت‌سازی بدست نیاورند با این حال آنها به گونه‌ای فزاینده به مخالفانی قهار و نیرومند تبدیل خواهند شد. فناوری‌های اطلاعاتی فرصت‌های نوین فراوانی به سازمان‌های جنایی داخلی و فراملی می‌دهد و این امکان را برای آنها فراهم می‌سازد تا قدرت و ثروت خویش را افزایش دهند. فناوری‌های اطلاعاتی این امکان را برای شبکه‌های کوچکتر فراهم می‌سازد که با منابع کمتری جرائم فراوانی را انجام دهند که در نتیجهٔ آن درآمد زیادی نیز بدست آورند این فناوری‌ها حتی این امکان را به شبکه‌های بزرگتر می‌دهد که از طریق مدیریت بسیار کارآمد قابلیت‌های عملیاتی پیشرفته و مجموعهٔ وسیعتری از سلاح‌ها و راهبردهای تهاجمی و تدافعی، ثروت و قدرت بیشتری انباشته کنند. علاوه بر این فناوری‌های اطلاعاتی این امکان را به سازمان‌های جنایی فراملی می‌دهند که از طریق ذیل خطرات مرتبط با اعمالشان را کاهش دهند:

استفاده از قابلیت‌های ضد اطلاعات، استفاده از ارتباطات پیشرفته راه دور برای اداره کردن کار آفرینی‌های غیرمجاز و انجام اعمال غیرمجاز. بطور خلاصه این فناوری‌ها ظرفیت سازمان‌های جنایی فراملی را برای به چالش کشیدن امنیت داخلی و بین‌المللی افزایش می دهند. همچنانکه سازمان‌های جنایی قدرت اقتصادی خویش را افزایش می‌دهند، آنها نه توانایی خویش را در زمینهٔ گریز از قواعد حقوقی افزایش می‌دهند بلکه ظرفیت خویش را در عرصه‌های ذیل نیز ارتقاء می‌بخشند:

فاسد کردن اعضای حکومت، به جمع خود راه دادن اعضاء حکومتی (و حل کردن درخود)، رویارویی با حکومت و اعمال فشار بر حکومت. چنین دورنمایی وسیله‌ای برای جنجال‌آفرین بودن نیست کما اینکه نمی‌تواند ما را از هشیار شدن مأیوس کند.» (پیکارتی، جان تی، آگوست ۲۰۰۰، ص ۳۷).

تروریست‌ها و گروه‌های افراطی

تروریسم از آن دسته تهدیدات نوینی است که در جهان معاصر بسیار حائز اهمیت می‌باشد. حوادث یازدهم سپتامبر فارغ از منشاء آن نمونهٔ بارز اخیر این نوع تهدید محسوب می‌شود. اهمیت حوادث تروریستی اخیر در آمریکا از آن جهت است که:

۱ ـ این‌اتفاق درعصر رسانه‌ای شدن جوامع، یک اجماع‌جهانی را درمورد مقابله‌با تروریسم شکل داده است.

۲ ـ رخداد مذکور نمونهٔ عینی تهدیدات ناشی از به هم وابستگی‌های جهانی می‌باشد.

۳ ـ این واقعه نشان داد، که تهدیدات آینده بدون پیش‌بینی و با امکانات درونی کشورها رخ خواهد داد.

٤ ـ حادثه مزبور مهر تأییدی بر تحول مفاهیمی همچون امنیت و تهدید بود.

٥ ـ اتفاقات آمریکا نشان‌داد به‌دلیل مبهم بودن فاعل و مصدر تهدید، واکنش‌نشان‌دادن به‌آن‌دشوارمی‌باشد.

از جمله گروه‌های تروریستی نوین تهدیدکنندگان امنیت ملی کشورها در فضای سایبر هستند. این گروه‌ها به زیرساخت‌های فناوری اطلاعات با هدف دستیابی به مقاصد خود حمله می‌کنند. گسترش تعداد این گروه‌ها و بهره برداری از شرایط جدید، زمینه‌های تهدید آنها را بیشتر نموده است. ماهیت شبکه‌ای و به هم پیوستهٔ دنیا و امکان خرابکاری از طریق این شبکه باعث می‌شود که گروه‌های تروریستی بسیاری به وجود آیند. شرایط خرابکاری در فضای سایبر که بیشتر مبتنی بر دانش است باعث کوچکتر اما کاراتر شدن این گروه‌ها می‌گردد؛ این در حالی است که استفاده از سلاح‌های پیشرفته هم گران و هم خطرناک است و این خود در گذشته مانع توسعهٔ این گروه‌ها بود.

ـ نیات

انگیزه‌ای که تروریست‌ها را به استفاده از فضای سایبر برای عملیات تروریستی

حداقل، امکان هماهنگی حداکثر، ارزان بودن و کم خطر بودن استفاده از این شرایط به وجود آمده‌است. این افراد می‌توانند بدون اینکه نیاز به اخذ ویزا از یک کشور خارجی برای مسافرت به آن باشند، به عملیات خود جامهٔ عمل بپوشانند و حتی ردی هم از خود باقی نگذارند.

ـ قابلیت‌ها

مسلماً تروریست‌ها از اینترنت برای اهداف خود استفاده می‌کنند. تروریسم سایبری به تاکتیک‌هایی که با هدف از کار انداختن عملیات زیرساخت‌های بحرانی یک کشور انجام می‌شوند اطلاق می‌شود. بنابراین تروریست‌ها که از راه دور قصد چنین خرابکاری‌هایی را دارند از فناوری اطلاعات و ارتباطات بهره می‌گیرند. برخی از روش‌های مورد استفاده در مقاصد این افراد به شرح زیر می‌باشد:

الف ـ بمب‌های پست الکترونیکی

حملات بمب پست الکترونیکی به این صورت است که به مقصد فرد موردنظر خود در یک لحظه میلیاردها پیغام الکترونیکی ارسال می‌کنند. در واقع بمباران اطلاعاتی باعث ایجاد نقص در فعالیت‌های فرد مورد نظر می‌گردد. شخصی که با پست الکترونیک فرد به کارهای تجاری و امور شغلی و اجتماعی خود می‌پردازد و زمان برایش ارزش زیادی دارد در صورت مواجهه با این حجم پیغام، مسلماً باید وقت زیادی صرف نماید تا پیغام‌های مفید را از میان پیغام‌های مزاحم تشخیص دهد.

گاهی اوقات نیز بمباران پست الکترونیکی باعث سرریز شدن صندوق پستی مخاطب و برگشت خوردن سایر مراسلات می‌گردد که این مسأله نیز مضرات خود را دارا است.

مثالی از این جمله در سال ۱۹۹۷ م توسط چریک‌های تامیل علیه سفیر سریلانکا صورت گرفت که در آن این گروه ابتدا به شبکهٔ کامپیوتر دانشگاه شفیلد انگلیس نفوذ کرده حملهٔ خود را از آنجا ترتیب دادند به این صورت که به یکباره هزاران پیغام را به مقصد مورد نظر ارسال نمودند (Michael Vatis, April 1998).

ب ـ ایجاد ترافیک(Sit-in)

خدمات به سایرین می‌شود. یکی از اولین نوع این حملات در سال ۹۵ وقتی که سیستم‌های کامپیوتر دولت فرانسه به خاطر سیاست‌هایش در قبال مسائل هسته‌ای مورد حمله قرار گرفت، اتفاق افتاد. اگرچه این حملات توسط تروریست‌ها انجام نشد ولی خود نشانگر قابلیتی است که می‌تواند در دسترس تروریست‌ها باشد (Dorothy E. 1999).

ج ـ خرابکاری‌های فیزیکی در فضای سایبر

تروریسم سنتی همچنان ادامه خواهد یافت و زیرساخت‌های فیزیکی را مورد هجوم قرار خواهد داد. اما حملاتی وجود دارند که از ترکیب روش‌های تروریسم سنتی و تروریسم سایبری تشکیل می‌شوند. البته به علت اینکه حمله به یک زیرساخت، زیرساختهای دیگر را می‌تواند مختل کند حملات سنتی نیز گاهی فعالیت‌های سایبری را متوقف می‌نمایند. برای مثال ارتش ایرلند بین سالهای ۹۶ تا ۹۷ تعداد ۳۷ بمب را در اطراف مراکز برق خارج لندن با هدف از کار انداختن شبکهٔ برق کار گذاشت. اگرچه هدف این افراد مستقیماً زیر ساخت IT نبوده معهذا زیر ساخت IT نیز آسیب دیده است (Schwartz, 1999).

د ـ ویروس‌ها و کرم‌های رایانه‌ای

ویروس‌ها و کرم‌ها ابزارهایی هستند که جهت خرابکاری کامپیوتر و شبکه‌های مقصد مورد استفاده قرار می‌گیرند. ایجاد و طراحی یک ویروس نسبتاً ساده است. یک گروه تروریستی ممکن است یک ویروس بی‌آزار طراحی کند و آنرا در شبکهٔ اینترنت انتشار دهد و برای خود نوعی مصونیت بدست آورد و یا اینکه با ویروسی خطرناک کلیهٔ اطلاعات کامپیوترها را از بین ببرد (http://www.Whashington post.com, 2000 ju14).

متخصصان جنگ پنتاگون تخمین زده‌اند که با بودجه‌ای کمتر از ۱۰ میلیون دلار و کمتر از ۳۰ کامپیوتر می‌تواند یک عملیات خطرناک علیه زیرساخت‌های آمریکا طراحی نماید.

هکرها

به برنامه‌نویسان و کاربرانی که می‌توانند به صورت غیرمجاز با استفاده از خطاهای نرم‌افزاری و یا انسانی به سیستم‌های رایانه‌ای نفوذ کنند، هکر می‌گویند.

ـ نیات

انگیزه‌های مختلفی برای فعالیت‌های هکری وجود دارد. برای مثال نتیجهٔ یک بررسی از ۱٦٤ هکر نشان داد که:

٤۹ درصد با انگیزهٔ چالش، دانش و یا سرگرمی این کار را انجام می‌دهند.

۲٤ درصد انگیزهٔ کنجکاوی، هیجان و یا رفاقت داشته‌اند.

۲۷ درصد نیز با انگیزه‌های خطرناکی مثل خود ارضایی، اعتیاد، جاسوسی، سرقت، انتقام و خرابکاری فعالیت کرده‌اند (Dorothy E. Denning, 1999.p 47).

اگرچه ممکن است برخی از هکرها آسیب جدی به کسی یا جایی وارد نکنند اما همین مسأله که آنها می‌خواهند قابلیت‌های خود را به نمایش گذاشته و یا آزمایش کنند، آنها را به سوی حمله به زیرساخت‌های اساسی هدایت می‌کند. خطر استخدام این افراد توسط گروه‌های تروریستی جنایی نیز قبلاً مورد بررسی قرار گرفت.

مثال معروف حملهٔ هکرها مربوط به سال ۹۸ است که سه پسر ۱٦، ۱۷ و ۱۸ ساله با نام‌های مستعار ماکیاول، قد کوتاه و تحلیل‌گر، برنامه‌ریزی شده‌ترین حمله علیه زیرساخت‌های نظامی آمریکا در فضای سایبر را انجام دادند. اگرچه انگیزهٔ این افراد سیاسی و یا نظامی نبود ولی آنها توانستند به شبکه‌های پنتاگون، دانشگاه برکلی، دانشگاه MIT و کتابخانه‌های ملی نفوذ کنند.

نمونهٔ دیگر مربوط به یک جوان کانادایی است که حملاتی از نوع منع خدمت را علیه سیاست‌های معروف آمازون، یاهو، CNN، ebay و ... انجام داد.

ـ قابلیت‌ها

توانایی هکرها همراه با رشد ابزارهای نفوذگری افزایش می‌یابد. امروزه این ابزارهای نرم‌افزاری آنقدر پیشرفت کرده‌اند که نسخه‌های کاملاً خودکار آن نیز به وجود آمده است. بنابراین حتی یک هکر تازه کار هم می‌تواند امنیت سیستم‌های

کشور را از طریق فناوری اطلاعات مختل سازد. هکرها به سه گروه بچه‌ها[1]، کاربران پیشرفته[2] و تولیدکنندگان[3] تقسیم می‌شوند.

گروه بچه‌ها که ساده‌ترین اما با سابقه‌ترین گروه است و اکثر هکرها به خاطر داشتن مهارت کار با تعدادی ابزار شناخته شده در این گروه دسته‌بندی می‌شوند، تنها از راه‌های شناخته شده بهره‌برداری می‌کنند و حملات شناخته شده‌ای را ترتیب می‌دهند.

گروه کاربران پیشرفته علاوه بر استفاده از ابزارهای گروه بچه‌ها از زبان‌های برنامه‌نویسی نیز برای حمله به سیستم‌ها بهره می‌گیرند. این افراد به علل نفوذ به یک شبکه واقفند و می‌فهمند چرا عملیات‌شان موفق یا ناموفق بوده است. یکی از تفاوت‌های اساسی این دو گروه هدف‌گیری و یا هدف‌یابی است. گروه بچه‌ها به اهدافی که سیستم‌هایشان در آن تأثیر نماید حمله می‌کنند، در حالیکه کاربران پیشرفته هدف مشخصی داشته، سپس سیستم را انتخاب می‌کنند.

تولیدکنندگان نیز خود، برنامه نویسان ماهری هستند که ابزارهای جدید را با توجه به شرایط سیستم‌های هدف طراحی می‌کنند. تعداد هکرهایی که در این رده باشند اندک است. اما اینها هکرهای خلاق هستند و از روش‌های ناشناخته برای حمله بهره می‌گیرند. گروه‌های مختلف هکرها در شبکهٔ اینترنت اطلاعات خود را عرضه می‌کنند. اگرچه این اطلاعات به تولیدکنندگان نرم‌افزار برای رفع خطاهای خود کمک می‌کند اما ابزار بسیاری از هکرها برای حمله به سیستم‌ها می‌شود. ممکن است هکر خود مستقیماً به عملیات علیه زیرساخت‌های ملی اقدام نورزد، اما ابزارهایی که تولید می‌کند می‌تواند در این راه مورد بهره‌برداری قرار گیرد.

1 - Script Kiddies
2 - Advanced Users
3 - Developers

کارمندان و نیروهای داخلی

آمارها نشان می‌دهد که ۸۷ درصد حملات به سازمان بزرگ توسط کارمندان و کسانی که در آن مشغول به کار هستند انجام می‌گیرد. بنابراین این افراد تهدید بزرگی برای فعالیت‌های سازمان‌های مختلف محسوب می‌شوند. چنانچه این افراد توسط گروه‌های تروریستی استخدام شوند در راستای منافع آنها و علیه سازمان اقدام می‌کنند. از آنجائیکه اکثر شبکه‌ها از دیوارهٔ آتش برای محافظت از حملات بهره می‌گیرند، حملات داخلی که در پشت این دیوار اتفاق می‌افتد، تهدیدی بزرگ محسوب می‌شود.

تعریف خودی در دنیای سایبر تغییر یافته است. خودی یا داخلی لزوماً کسی نیست که به صورت فیزیکی در داخل سازمان قرار دارد و در صورت تخلف توسط حراست شناسایی می‌شود بلکه در شرایط جدید خودی‌ها حتی از بیرون به سیستم وصل می‌شوند و با آن کار می‌کنند.

ـ نیات

کارمندان داخلی انگیزه‌های مختلفی برای نفوذ به سیستم دارند که از آن جمله می‌توان به انتقام، بهره‌برداری اقتصادی و غیره اشاره کرد. این افراد معمولاً به ٦ گروه با انگیزه‌های مختلف تقسیم می‌شوند:

کارمندان ناراضی: کارمندانی هستند که از شغل خود رضایت ندارند و یا برخورد سازمان را با خودشان نامناسب می‌دانند؛ حتی ممکن است از حقوق خود ناراضی باشند. انگیزهٔ این کارمندان انتقام جویی است.

فروشندگان اطلاعات: افرادی هستند که اطلاعات سازمان را به دلالان اطلاعات، جاسوسان صنعتی، سازمان‌های جنایی و سازمان‌های امنیتی می‌فروشند. انگیزهٔ این افراد کسب درآمد است.

کارمندان مجبور یا مصالحه‌گر: کسانی هستند که به اطلاعات یا منابع حساس سازمان دسترسی دارند و توسط گروه‌های تروریستی، جنایی و یا امنیتی کشورهای دیگر تهدید شده‌اند تا اطلاعات را در دسترس آنان قرار دهند. انگیزهٔ این افراد ترس است.

کارمندان سابق: کارمندان سابق ممکن است دسترسی به شبکه‌های کامپیوتری سازمان را حفظ کرده باشند. این افراد می‌توانند از این دسترسی‌ها برای مقاصد خرابکارانه استفاده کنند. انگیزهٔ این کارمندان پول یا انتقام است.

شبه کارمندان: کسانی هستند که با سازمان یا شرکتی کار می‌کنند اما کارمندان آن نیستند. در شرایط جدید امکان کار این افراد افزایش یافته است. شبه کارمندان انگیزه‌های مختلفی چون کسب درآمد و پول، انتقام، ترس و غیره دارند.

شرکای تجاری: تغییر محیط تجاری توسط اینترنت، افرادی جدید را به عنوان خودی به وجود آورده است. مشتری‌ها، رقبا و فروشندگان برخی از این افراد هستند. این گروه نیز مانند گروه قبل از انگیزه‌های متعددی برخوردارند.

ـ قابلیت‌ها

به خاطر دسترسی فیزیکی به داخل سازمان و حفاظت محدودتر از منابع داخلی، دست این افراد در مقاصد مربوطه نسبت به سایر گروه‌ها بازتر است. به همین علت طبیعت کار این گروه با سایر گروه‌ها تفاوت دارد. این افراد ممکن است رمز عبور سایر کاربران را یافته، از آن به نفع مقاصد خویش استفاده نمایند. ابزارهای موجود هکینگ نیز به عنوان توانایی‌های این گروه محسوب می‌گردد.

آشنایی این افراد با سازمان و منابع آن مهمترین توانایی آنها تلقی شده و آنها را در زمانی سریعتر به سمت اهداف‌شان راهنمایی می‌کند.

نتیجه‌گیری

با عنایت به اهمیت شبکه جهانی اطلاع‌رسانی به عنوان یک پدیده‌ی غیرقابل انکار عصر فرامدرن که واجد فرصت‌های بسیاری و حامل تهدیدهای جدی است، طراحی استراتژی نظام جمهوری اسلامی ایران در ارتباط با فناوری اطلاعات و بهره‌مندی از فرصت‌ها و تهدیدها به موازات تقویت نقاط قوت و تدبیر در ترمیم نقاط ضعف در این حوزه از اهمیتی ویژه برای امنیت ملی جمهوری اسلامی ایران برخوردار است.

منابع و مأخذ

منابع فارسی

۱ - آردی،مک کین لای، آر.لیتل.(۱۳۸۰). «**امنیت جهانی رویکردها و نظریه‌ها**»، (ترجمهٔ اصغر افتخاری)، تهران: انتشارات پژوهشکدهٔ مطالعات راهبردی.

۲- آزر، ادوارد و چونگ این مون.(۱۳۷۹). «**بسوی اندیشهٔ بدیل**» (ترجمهٔ پژوهشکدهٔ مطالعات راهبردی)، تهران: پژوهشکده مطالعات راهبردی.

۳- بوزان، باری.(۱۳۷۸). «**مردم، دولتها و هراس**»، (ترجمهٔ پژوهشکدهٔ مطالعات راهبردی)، تهران: پژوهشکده مطالعات راهبردی.

٤ - پیکارتی، جان تی و ویلیامیز.(آگوست ۲۰۰۰). فیل، گزیده‌های عصر اطلاعات : **الزامات امنیت ملی در عصر اطلاعات**، سی‌سی‌آرپی، ص ۳۷.

٥ - تاجیک. محمدرضا.(۱۳۷۷). «**انتظام و پراکندگی : بحثی در امنیت ملی ایران**»، فصلنامه مطالعات راهبردی، پیش شماره دوم، ص ۱۱۸.

٦ - درویشی سه تلانی، فرهاد .(۱۳۷٦). «**تأملی نظری برامنیت ملی**»، تهران: معاونت تحقیق و پژوهش دانشکده فرماندهی و ستاد سپاه پاسداران انقلاب اسلامی.

۷- دزیانی،محمدحسن.(-). «**مسئولیت کیفری برای انتقال داده‌ها در سایبراسپیس**»، شورای عالی انفورماتیک، سازمان مدیریت و برنامه‌ریزی، چاپ محدود.

۸ - زرکلام، ستار.(۱۳۸۰). «**قراردادهای انفورماتیک**»، شورای عالی انفورماتیک تهران: انتشارات سازمان مدیریت و برنامه‌ریزی، تهران.

۹- زرکلام،ستار.(۱۳۸۰). «**قراردادهای انفورماتیکوجرائم آن**»، اولین همایش تخصصی‌ناجا، تهران.

۱۰ - زیبر، اولریش. (-). «**سایبرلا: توسعه در آلمان**»، ترجمهٔ احمدی، هما، خبرنامهٔ انفورماتیک شماره‌های ۷۱ و ۷٤.

۱۱ - قاجارقیونلو، سیامک.(۱۳۸۱). «**ارزش اثباتی ادله در محیطهای دیجیتال در حقوق ایران**»، چاپ محدود، شورای عالی انفورماتیک، تهران.

۱۲ ـ قاجارقیونلو، سیامک.(۱۳۸۱). «**جریان آزاد اطلاعات**»، تهران: شورای عالی انفورماتیک.

۱۳ ـ قاجارقیونلو، سیامک. (۱۳۷۵). «**گروه بررسی مسائل حقوقی و جزایی کاربرد کامپیوتر**»، دبیرخانه شورای عالی انفورماتیک کشور.

منابع لاتین

1-Caleb Pringle.(1999). "Terrorist Organizations' Use of Information Age Capabilities," *Defense and Foreign Affairs* Strategic Policy, January.

2-Denning ,Dorothy E.(1999). **Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy**, Nautilus Institute.

3-Denning ,Dorothy E. (1999). **Information Warfare and Security**, Addison-Wesley, p. 47.

4-Schwartz John.(2000)."**No Love for Computer Bugs**", Washington Post,July5.

http://www.washingtonpost.com/cgi...ni/print&articled= a47155-2000jul4

5-Vatis, Michael .(1998). "**Seminar on Cyber-Terrorism and Information Warfare: Threats and Responses**," Proceedings Report, Potomac Institute for Policy Studies, April 16.

د ـ فهرست منابع اینترنتی

1- http : // www . aba . gov . au/internet/ industry/ codes/index.html
2- http: // www . abc . gov . au / what/ online/ complaints/ index.asp
3- http: // www. aph.gov .au/library/ pubs/bd/1999-2000/2000bd
4- http : // www . aph.gov. au/library/pubs/rp/1997-98/98rp18.
5- http : // www. austlii . edu . au/legis/ cth/num – act/pasa 2000 n 1552000373. html
6- http : // www . austlii .edu . au/legis/nsw/consol-act
7- http: // www. austlii . edu . au/legis/ cth/consol– act/ca 2002 . html
8 - http : // www . australianit.news.com.au
9- http: // ww.cnnfn.com/digitaljam/9802/24/robber/
10- http: // www . dcita . gov . au
11- http : // www. handotimes . com

13- http : // www . noie . gov .au
14- http : // www . oflc . gov . au
15- http : // www . Privacy . gov. au/ Publications/pia - html
16- http : // www.Privacy .gov. au/Publications/Is 13 – 01 .html.
17- http : // www. Scaleplus. Law.gov. au
18- http: // www.sec.gov/news/uclaenf.htm
19- http: // www .scaletext. Law . gov . au/htm/Comact.