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

● دکتر ابراهیم حسن بیگی*

چکیده:

فناوری اطلاعات فرصت‌های بی نظیری در اختیار بشریت قرار داده است ولی مشابه با هر فناوری نوظهور در جهان، چالش هایی نیز به دنبال دارد. سرقت اطلاعات، خرابکاری از کاراندازی سیستم‌های رایانه‌ای، کلاهبرداری و جاسوسی از جمله تأثیرات مخرب فناوری اطلاعات برای حیات بشری است. توسعه اینترنت در جوامع و گسترش آن حتی به درون منازل و محل‌های کار مردم و نیز جهان شمول بودن و وجود خطرات بالقوه آن، سازمان‌ها و دولتها را با چالش‌های جدیدی روبه‌رو ساخته است.

گسترش فزاینده فناوری اطلاعات و ارتباطات به تحول و دگرگونی در ابعاد مختلف مؤلفه‌های اقتصادی، سیاسی، اجتماعی، فرهنگی و نظامی منجر خواهد شد و مجموعه فعالیت‌ها در زمینه‌های تولیدی، بهره‌برداری، بانکداری، برقراری ارتباطات با رایانه‌های شبکه‌بندی شده را دستخوش تغییرات جدّی قرار خواهد داد...

قدر مسلم آن است که همگام با توسعه روزافزون فناوری اطلاعات، ابزارها و 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

* پژوهشگر و جانشین ریاست دانشگاه عالی دفاع ملّی

رایانه‌ای، بر شمار عاملانی که قدرت یورش علیه زیرساخت‌ها را دارند هم روز به روز افزوده می‌شود.

در مقاله حاضر به عنوان چکیده‌ای از یک رساله حجیم تلاش شده است که به توسعه شبکه ملّی دیتا، چالش‌های فراروی و تهدیدهای متوجه امنیت ملّی عنایت شده و در ضمن بذل توجه به این مهمّ، آن را در حوزه امنیت ملّی جمهوری اسلامی ایران مطمح نظر قرار دهد.

پیشگفتار

گسترش فزاینده فناوری اطلاعات و ارتباطات به تحول و دگرگونی در ابعاد مختلف مؤلفه‌های اقتصادی، سیاسی، اجتماعی و فرهنگی و نظامی منجر خواهد شد و مجموعهٔ فعالیت‌ها در زمینه‌های تولید، بهره‌برداری، بانکداری، برقراری ارتباطات با رایانه‌های شبکه‌بندی شده را دستخوش تغییرات جدی قرار خواهد داد. در آینده نزدیک زیرساخت‌های حیاتی در زمینه‌های اقتصادی، مسائل اجتماعی فرهنگی و دفاعی و امنیت ملی کشورها به فناوری اطلاعات و ارتباطات وابستگی پیدا خواهد نمود این زیرساخت‌ها عبارتند از: انرژی (نیروی برق، نفت و گاز)، حمل‌ونقل (راه‌آهن، هوایی و دریائی)، بانکداری، مخابرات، بهداشت عمومی، خدمات فوریتی، آبرسانی، صنایع دفاعی، تغذیه، کشاورزی، امور بارگیری کالا و....

علاوه بر آسیب‌پذیری‌های داخلی ناشی از ضعف زیرساخت‌های فنی و نیز کمبودها و ضعف‌های آموزشی، طیف وسیعی از عوامل مهاجم وجود دارند که می‌توانند علیه زیرساخت‌های اطلاعاتی حساس دست به تهاجم بزنند. مهم‌ترین نگرانی در این‌باره تهدید ناشی از حملات سایبری سازمان‌یافته است که قادر به تحمیل لطمه‌های جبران‌ناپذیر بر زیرساخت‌های حیاتی کشور می‌باشد.

قدر مسلم آن است که همگام با توسعهٔ روزافزون فناوری اطلاعات، ابزارها و شیوه‌های مختلف تهاجمی نیز به سرعت گسترش یافته و توان تخصصی و درجهٔ پیچیدگی نفوذگران عامل تخریب یا غارت سیر صعودی پیدا کرده است.

علاوه بر پیچیدگی روزافزون ابزارهای مورد استفاده در حملات رایانه‌ای، بر شمار عاملانی که قدرت یورش علیه زیرساخت‌ها را دارند هم روزبه‌روز افزوده می‌شود.

در دوران صلح و آرامش احتمال جاسوسی دشمنان دربارهٔ 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 مخفی و سایر شیوه‌های دستیابی به اطلاعات به منظور تدارک تهاجم‌های سایبری متصور بلکه مسلم 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 سیستم‌های اطلاعاتی نزد افکار عمومی و نیز ایجاد نگرانی و هراس عمومی شورش‌های گسترده و براندازی را تدارک نماید.

از ویژگی‌های فناوری اطلاعات و بویژه اینترنت، امکان ساماندهی و تدارک تهاجم سازمان‌یافته از فواصل دور علیه اهداف از پیش تعیین‌شده 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 برقراری ارتباط مخرب مانع از واکنش‌های دفاعی و یا ایجاد تأخیر در آنها نیز می‌گردد. در تهاجم از طریق شبکه اینترنت حتی کشورهایی که بدلیل موقعیت جغرافیائی از بسیاری از تهاجم‌های فیزیکی مصونیت دارند نیز 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.

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

از این جهت لازم است تا در سطح ملی ضمن شناسایی نقاط ضعف و قوت و نیز آسیب‌پذیری‌های احتمالی و با درنظر گرفتن فرصت و فشارها در محیط بین‌الملل،

اقدامات بازدارندهٔ متناسب، پیش‌بینی و چاره‌اندیشی شود.

آنچه مسلم است ایجاد شبکهٔ امن و محافظت از زیرساخت‌های فناوری اطلاعات مستلزم تلاش همهٔ دستگاههای مسؤول مبتنی بر راهبرد مشخص است که بایستی توسط مسؤولین تعیین خط‌مشی پس از احصاء آسیب‌پذیری‌ها و تهدیدات احتمالی طراحی و به مرحله اجرا درآید.

از آنجایی که کلیهٔ اقدامات مربوط به طراحی شبکه، اقدامات به هم پیوسته‌ای است که بروز ضعف در هر یک موجب آسیب‌پذیری سایر اقدامات می‌شود لذا این عملیات از قبیل استفاده از نرم‌افزار، معماری شبکهٔ مدیریت اطلاعات و امنیت شبکه، استانداردسازی و اقدامات کاربرها، مستلزم هماهنگی و پیش‌بینی راهکارهای علمی و امنیتی می‌باشد.

در بخش مربوط به قوانین، مسائل حقوقی و قضایی نیز، اینترنت قواعد سنتی حاکم بر رسیدگی‌های قضایی را دستخوش تحولات اساسی کرده است. تعریف از جرائم 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 بطور اصولی محدود به خاک یک کشور و تحت حاکمیت یک دولت می‌شود به عبارت دیگر اعمال حاکمیت از سوی یک دولت مطرح است. همچنین شرط استرداد مجرمین، عدم تعارض این عمل با حاکمیت دولت‌ها در عرصه‌های سیاسی و قضایی است.

بنابراین رسیدگی به جرائم ارتکابی در محیط‌های مجازی در ابعاد داخلی و در ابعاد بین‌المللی با کمبودها و چالش‌های اساسی مواجه است.

با گسترش شبکه جهانی اطلاع‌رسانی (اینترنت) به لحاظ مشکلاتی که به آنها اشاره شد جرائمی در محیط‌های مجازی به وقوع پیوسته که سیستم قضایی کشورهای مختلف نتوانسته‌اند با آنها برخورد جدی نمایند. همین امر باعث شده که شبکهٔ اینترنت فارغ از سلطهٔ قوانین در دنیا و فضای مستقر خود به راه خود ادامه دهد.

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 قرار داده است.

همچنین در تجارت الکترونیکی مسائل مربوط به تصدیق امضای الکترونیک و تضمین صحت داده‌ها مشکلات جدیدی ایجاد کرده است.

بنابراین از آنجا که درگذار از جامعه صنعتی به فراصنعتی و ورود به دوره پست مدرن، حقوق نیز از حقوق صنعتی به حقوق اطلاعات و به تبع آن فناوری اطلاعات و ارتباطات تغییر و تحول یافته از اینرو شاخصه‌ها و بحث‌های خاصی را دارا شده است. بخشی از این تحول در خصوص فناوری اطلاعات ناظر به ابعاد مدنی و تجارت (حقوق خصوصی)، بخشی ناظر به حقوق عمومی (اساسی و اداری)، بخشی ناظر به حقوق جزا و بخشی دیگر ناظر به جنبه‌های بین‌المللی یا حقوق بین‌الملل است. در مقاله‌ی حاضر به عنوان چکیده‌یی از یک رساله حجیم تلاش شده است که به توسعه شبکه ملّی دیتا، چالش‌های فراروی و تهدیدهای متوجّه امنیت ملّی عنایت شده و در ضمن بذل توجه به این مهمّ آن را در حوزه‌ی امنیت ملّی جمهوری اسلامی ایران مطمح نظر قرار دهد.

بیان مسأله

فناوری اطلاعات فرصت‌های بی‌نظیری در اختیار بشریت قرار داده است ولی مشابه هر فناوری نوظهور در جهان، چالش‌هایی نیز به دنبال دارد. سرقت اطلاعات، خرابکاری، از کاراندازی سیستم‌های رایانه‌ای، کلاهبرداری و جاسوسی از جمله تأثیرات مخرب فناوری اطلاعات برای حیات بشری است. توسعهٔ اینترنت در جوامع و گسترش آن حتی به درون منازل و محل‌های کار مردم و نیز جهان شمول بودن و وجود خطرات بالقوهٔ آن، سازمان‌ها و دولت‌ها را با چالش‌های جدیدی روبرو ساخته است.

اهم مشکلاتی که سازمان‌ها با نقاط تاریک فناوری اطلاعات دارند، عبارتند از:

- دسترسی غیرمجاز افراد (بیگانه یا داخلی) به سیستم‌ها و اطلاعات یک سازمان و خرابکاری یا جاسوسی و یا دستکاری داده‌ها.
- استفاده غیرمجاز از اینترنت
- نشت ناخودآگاه اطلاعات

برای مقابله با تهدیدات فناوری اطلاعات مکانیزم‌های متعددی بوجود آمده است از جمله دیوارهای آتش، سیستم تشخیص نفوذ، سیستم فیلتر که به‌طور سیستماتیک به مقابله با مسائل فوق برمی‌خیزد.

در کنار این سیستم‌ها، مکانیزم‌های شنود، مراقبت و مانیتورینگ نیز گسترش یافته‌اند که با اهداف گوناگون مراقبتی یا جاسوسی به کار می‌روند.

در ابعاد حقوقی پیدایش و تکامل تهدیدهای اینترنتی موجب بروز جرائم جدید و بالطبع آئین دادرسی خاصی شده و از سویی برخی رشته‌های علوم جنایی را با چالش مواجه کرده است.

این تهدیدها کاملاً در بستر و فضای مجازی (محیط دیجیتالی محض) ارتکاب می‌یابند و از حیث میزان خطر، حجم ضرر و زیان و سهولت ارتکاب بزه دیدگان از جرم با افزایش ناگهانی مواجه شده است. این جرائم بسته به هدف و موضوع جرم، متمایز از دیگر جرائم محسوب می‌شوند.

بعنوان شاخص‌ترین این اهداف می‌توان از هدف ضدیت با امنیت ملّی (داخلی و خارجی) یا بر علیه اموال، آسایش عمومی، اخلاق، عفت عمومی و... یاد کرد. از این رو یکی از اهداف تحت‌تأثیرِ جرائم مذکور، چالش‌های امنیتی کلانی است که بواسطهٔ ویژگی‌های یادشدهٔ بالا خطرات بسیاری را برای کشور در پی خواهد داشت.

این جرائم یا تهدیدها گاه بطور مستقیم علیه امنیت کشور ارتکاب می‌یابند که شاخص‌ترین آنها جاسوسی کامپیوتری و سابوتاژ کامپیوتری است و گاه بطور غیرمستقیم رویکرد امنیتی داشته و امنیت ملّی را به چالش می‌کشند.

تهدیدهای خارجی از ناحیهٔ 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 محرمانهٔ 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 با تحولات همراه نشده است و از این رو 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 دامنهٔ جرائم می‌شود. نوع ارتکاب نیز

در طول زمان تکامل یافته و شکل جدید آن بصورت دیجیتالی روی می‌دهد.

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

برخی تهدیدها اگرچه فی حد ذاته بعنوان جرائم مستقیم علیه امنیّت دسته‌بندی نمی‌شوند اما گاه بعلت رویکرد امنیّتی از حیث هدف و انگیزهٔ تهدیدکنندگان و گاه از حیث نتیجهٔ کار جزء تهدیدات علیه امنیت نیز می‌توانند مورد بحث واقع شوند.

از این منظر در بستر و فضای دیجیتالی می‌توان مصادیقی را ذکر کرد که طبیعتاً نیازمند بررسی و سیاست‌گذاری است.

جنگ اینترنت

این جنگ کوششی است که جهت تخطی از امنیت توسط مزاحم و یا عملی نمودن تهدید در اثر آشکار شدن آسیب‌پذیری صورت می‌گیرد. این ابزار بصورت مفصل و با جزئیات دقیق در دستور کار برخی کشورهای متخاصم قرار گرفته و با ارتکاب اعمال مختلف سعی در به چالش کشاندن موضوعات امنیتی دارند. البته مصادیق و روش‌های این کار نیز به وسعت خود اینترنت گسترده است.

ساده‌ترین روش، ایجاد رعب و وحشت در جامعه در جهت ضدیت با نظام و یا ایجاد نارضایتی عمومی است.

برنامه‌های توسعهٔ زیرساخت و شبکهٔ ملی دیتای کشور و امنیت شبکه

برنامه‌های توسعه در کشور براساس مفروضات زیر صورت گرفته است:

۱ ـ امور دیتا ایجاد زیرساخت و شبکهٔ دیتا را بر عهده دارد.

۲ ـ ارائهٔ سرویس خدمات شبکهٔ دیتا بصورت عمده فروشی [۱] انجام شده و فروش جزئی [۲] بر عهدهٔ ISPاها و مؤسسات ذیربط [۳] واگذار می‌شود.

۳ ـ کاربران خانگی [۴] مگر در موارد استثنایی بطور مستقیم به شبکهٔ دیتا متصل نمی‌شوند

۴ ـ تعداد پورت‌های ارتباطی شبکه، کم، ظرفیت آنها نسبتاً زیاد و ضریب اشتغال کانال در آنها بالا خواهد بود.

۵ ـ تعداد محدودی اتصال کاربر انتهایی [۵] برای مشترکین خاص پیش‌بینی می‌شود.

مشخصات اصلی شبکهٔ دیتا در مرحلهٔ اول برنامهٔ سوم:

ـ ارائهٔ سرویس‌های شبکه در ۴۲۰ نقطه در بیش از ۱۸۰ شهر کشور.

ـ دریافت و توزیع خدمات اینترنتی برای ۱۰۰۰۰ پورت IP با ظرفیت ۸ میلیون کاربر اینترنت در کل کشور.

ـ امکان ایجاد ارتباط به نقطهٔ دیتا و شبکهٔ خصوصی VPN در سطح کشور بدون پروتکل و یا با پروتکل بازپخش چارچوب [۶] با ظرفیت ۷۰۰۰ نقطه و سرعت‌های ۶۴ کیلوبیت در ثانیه تا ۲ مگابیت در ثانیه.

ـ ارائهٔ بیش از ۲۰۰ پورت نامتقارن ADSL با سرعت تا ۸ مگابیت بر ثانیه درهشت شهر بزرگ کشور برای سرویس‌های مالتی مدیا و ویدئویی زنده.

مراکز اصلی در فاز اول برنامهٔ سوم شامل شهرهای تهران، اصفهان، شیراز، مشهد، تبریز، همدان، اهواز و بابل است. فاز اول در بازهٔ زمانی ۱۳۷۹ تا انتهای سال ۱۳۸۱ باید اجرا می‌شد و فاز دوم نیز طبق برنامه در سال‌های ۱۳۸۱ الی ۱۳۸۴ اجرا می‌شود در فاز اول سرعت لینکهای هستهٔ شبکه STM1 و در فاز دوم STM4/STM-1/E(622/34Mbps) پیش‌بنی شده بود. همچنین در این برنامه در فاز اول سرعت لینکهای دسترسی در مراکز اصلی 64K/2M/8Mbps و در فاز دوم در مراکز استانها 64/2M/8Mbps پیش‌بینی شده است در این برنامه مشترکین مستقیم شبکه موارد زیر می‌باشند:

ـ فروشندگان خدمات اینترنتی یا ISPها.

ـ مراکز اطلاع‌رسانی کامپیوتری.

ـ مؤسسات، شرکت‌ها و سازمان‌هایی که در سطح کشور یا شهر، شعب مختلف

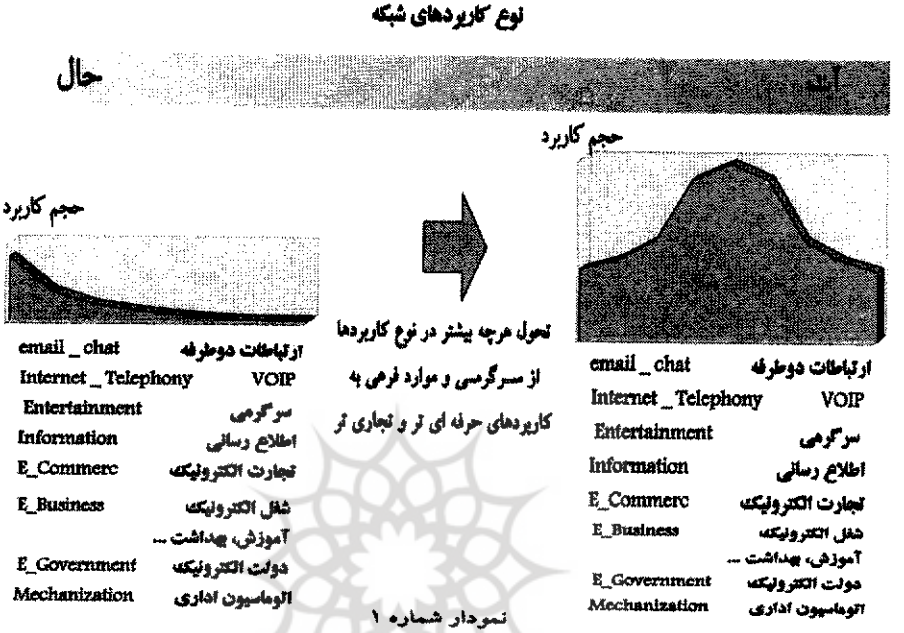
داشته و مایل به شبکه کردن شعب خود می‌باشند.

- عرضه‌کنندگان تلفن راه دور ارزان.
- فروشگاه‌های الکترونیک، بانک‌ها، آژانس‌های رزرو بلیط، هتل، جهانگردی و....
- نیروهای نظامی و انتظامی، هواپیمایی، راه‌آهن، کشتیرانی و سازمان حمل و نقل جاده‌ای.
- وزارت بهداشت، بیمارستانها و مؤسسات بیمه.
- دانشگاه‌ها، پژوهشگاه‌ها، دبیرستان‌ها، مدارس و سایر مراکز آموزشی.

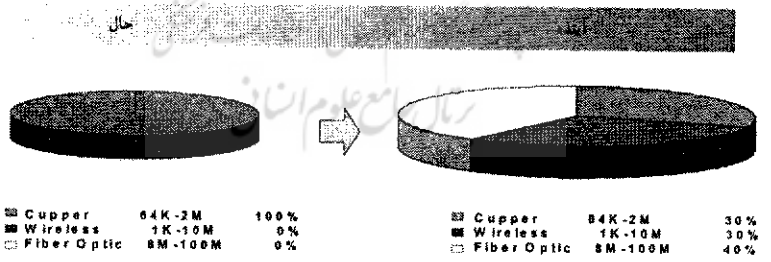
اهداف کلان طرح توسعهٔ ایجاد شبکهٔ ملی دیتا با مشخصات زیر است:

- توزیع یکنواخت ترافیک اینترنتی پرظرفیت با قیمت یکسان در سراسر کشور.
- برقراری ارتباطات پرظرفیت و با کیفیت بالا با شبکهٔ اینترنت جهانی.
- تحت پوشش قراردادن کلیه شهرهای کشور و ارائهٔ سرویس‌های دیتا.
- تحت پوشش قرار دادن کلیهٔ نقاط مهم و استراتژیک کشور مانند نقاط مرز، مناطق آزاد، بنادر و شهرک‌های صنعتی.
- مشارکت هرچه بیشتر بخش خصوصی و ایجاد محیط رقابتی در عرصهٔ خدمات دیتا به کاربران انتهایی.
- استفاده از توان بخش خصوصی در توسعهٔ شبکهٔ ملی دیتا.
- ارائهٔ خدمات شبکه‌های خصوصی جهت ارتباطات بیرونی سازمان در سراسر کشور.

در این شبکه کاربردهای زیر در حال و آینده بصورت نمودارهای شماره ۱ و ۲ زیر تعریف شده است:



نمودار شماره ۱



نمودار شماره ۲

مشخصات فاز دوم توسعهٔ دیتا:

- تحت پوشش قرار گرفتن کلیه شهرهای صنعتی، مناطق آزاد، بنادر، مرزها و جزایر

کیش، قشم، خارک و غیره...

- ظرفیت پردازش ۱۵,۰۰۰,۰۰۰ کاربر اینترنت بطور غیرمستقیم.

- ظرفیت انتقال ترافیک صدا بین شهری و بین‌المللی شامل ۱۰,۰۰۰ کانال تلفنی بصورت فناوری انتقال صدا در شبکه‌های دیتا[۷].

ضمناً وضعیت سیستم‌های ارتباطی در کشورهای آسیایی در ماه مارس ۲۰۰۲ میلادی به شرح جدول شماره ۱ بوده است:

جدول شماره ۱ - وضعیت ICT کشورهای آسیایی (مارس ۲۰۰۲)[۸]

کشور	تعداد موبایل (میلیون)	تعداد کاربران اینترنتی از طریق موبایل	جمعیت (میلیون)	ضریب نفوذ اینترنت (درصد)
ژاپن	۶۹	۵۲	۱۲۶	۴۵/۵
کره	۳۰	۲۷	۵۰	۵۱/۷
مالزی	۴	۲/۵ اینترنت ۱/۷	۲۲	۲۴
ایران	۲	اینترنت ۱/۷	۶۵	۲/۵

همچنین روند توسعهٔ کاربری از اینترنت طی سال‌های ۸۰ تا ۸۵ در ایران به شرح جداول شماره ۲ و ۳ می‌باشد:

جدول شماره ۲ - برنامه دستیابی به ضریب نفوذ ۲۸ درصد در سال ۱۳۸۶ (۲۰۰۷ میلادی)

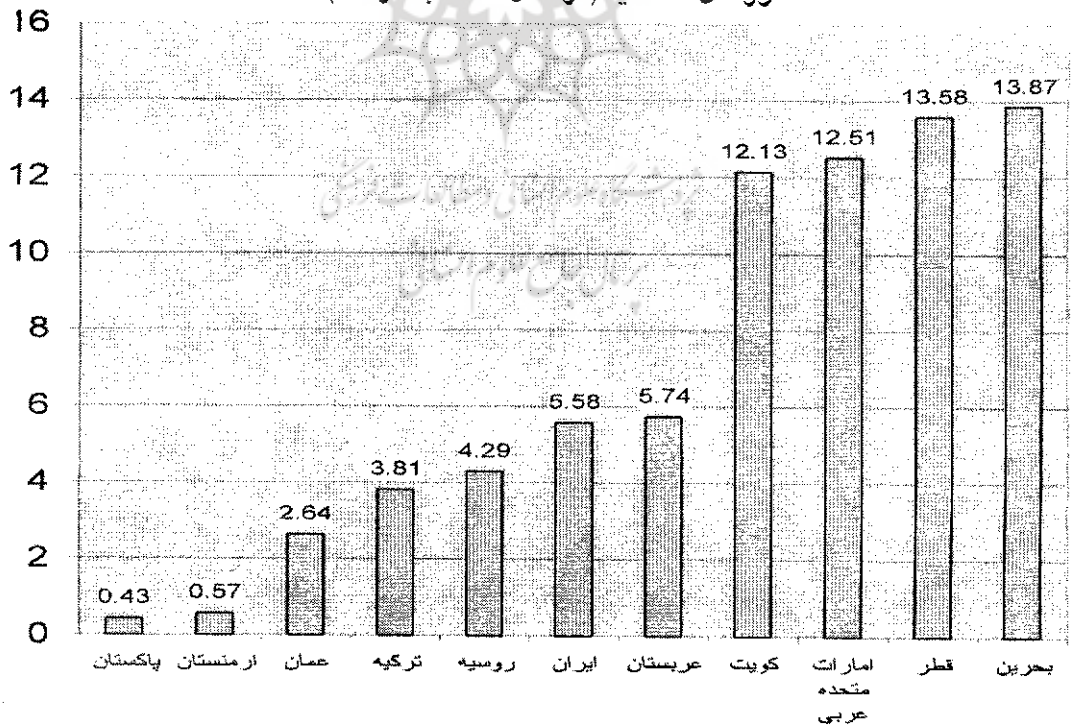
سال	ضریب نفوذ (درصد)	تعداد کاربران اینترنتی	ضریب رشد (درصد)
۸۰	۲/۵	۱۷۰۰۰۰۰	۱۰۰
۸۱	۴	۲۸۰۰۰۰۰	۶۰
۸۲	۸	۵۶۰۰۰۰۰	۱۰۰
۸۳	۱۸	۱۲۰۰۰۰۰۰	۱۱۴
۸۵	۲۸	۲۰۰۰۰۰۰۰	۶۷

جدول شماره ۳ ـ پیش‌بینی رشد و ضرورت برنامه‌ریزی برای ایران تا سال ۲۰۰۷ (پیشنهاد برنامه پنج‌ساله چهارم)

تعداد تلفن (میلیون)	تعداد موبایل (میلیون)	تعداد کاربران اینترنتی از طریق موبایل و تلفن ثابت (میلیون)	ضریب نفوذ اینترنت (درصد)
۳۵	۲۰	۲۰	۲۸

در جدول شماره ۴ میزان نفوذ رایانه‌های شخصی در ایران و برخی از کشورهای همسایه مورد مقایسه قرار گرفته است:

جدول شماره ۴ ـ نمودار ضریب نفوذ رایانهٔ شخصی در ایران و برخی کشورهای همسایه (در سال ۲۰۰۰ به درصد)[۹]



جدول شماره ٤

درجه‌بندی میزان گسترش اینترنت

اخیراً اتحادیهٔ بین‌المللی مخابرات ITU، اقدام به درجه‌بندی میزان گسترش اینترنت در یک کشور کرده است که خلاصهٔ آن را در جدول شمارهٔ ۵ ارائه می‌کنیم:

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
تراز چهار	متداول	ضریب نفوذ اینترنت بزرگتر یا مساوی ۱۰ درصد

بنابراین میزان گسترش اینترنت در ایران، تراز «دو» یعنی «نوپا»ست.[۱۰]

هـ ـ چالش‌ها و تنگناهای توسعهٔ فناوری اطلاعات و ارتباطات

«پس از بررسی اجمالی توسعهٔ شبکهٔ ملی دیتا به معرفی چالش‌ها و تنگناهای اصلی پیش‌روی توسعهٔ فناوری اطلاعات و ارتباطات در کشور می‌پردازیم:

چالش‌های قانونی

۱ ـ ابهامات موجود در مورد به رسمیت شناختن حقوق مالکیت معنوی: یکی از چالش‌های عمدهٔ مطرح در اقتصاد کشور احساس عدم امنیت در زمینهٔ مالکیت خصوصی افراد است. گرچه با توجه به قانون حمایت از مؤلفان و محققان سال ۱۳۴۸، قانون ترجمه سال ۱۳۵۲ و قانون حمایت از نرم‌افزارهای رایانه‌ای که اخیراً تصویب شده می‌توان مشکلات حادث در این حوزه را پاسخ داد معهذا بطور کلی و قاطع نمی‌توان

آن را کافی دانست و ابهاماتی در اجرا وجود دارد. فناوری اطلاعات و ارتباطات با گسترش خود باعث شفاف‌تر شدن صورت دارایی‌های افراد می‌شود. به منظور همراهی و همکاری مردم در جهت توسعهٔ این فناوری لازم است در ابتدا، آحاد جامعه نسبت به محترم شمرده شدن حقوق مالکیت معنوی خود مطمئن گردند.

۲ـ **تعریف نشدن حقوق پدیدآورنده در قوانین:** یکی از چالش‌های اساسی خدمات اطلاع‌رسانی، تعریف و به رسمیت شناختن حقوق مالکیت پدیدآورنده است. محترم شمردن حقوق مالکیت معنوی، پدیدآورنده را جهت ایجاد و گسترش محصولات جدید ترغیب می‌نماید. بدیهی است در صورتیکه هزینهٔ کپی‌برداری از محصولات دیجیتالی صفر باشد، پدیدآورنده انگیزه‌ای جهت ایجاد و توزیع محصولات جدید نخواهد داشت لذا به رسمیت شناختن حقوق مالکیت پدیدآورندگان محصولات اطلاعاتی در داخل کشور، جهت رشد و توسعهٔ این فعالیت‌ها و گسترش تولید اینگونه محصولات، ضروری به نظر می‌رسد. جنبهٔ دیگر این مسأله، جنبهٔ بین‌المللی موضوع است، زیرا به منظور حمایت از صادرات نرم‌افزار، لازم است کشور به عضویت سازمان جهانی حقوق پدیدآورنده درآید. البته تعیین ورود یا عدم ورود و زمان ورود به این سازمان نیاز به کار کارشناسی دارد.

۳ـ **قانون جامع تجارت الکترونیک:** با توجه به تغییر فضای تجاری در صورت توسعهٔ تجارت الکترونیک، لازم است قوانین تجاری متناسب طراحی و تصویب گردد.

۴ـ **نقض قوانین در مورد جرائم مرتبط با فناوری اطلاعات و ارتباطات:** با توجه به تفاوت ماهوی جرائم الکترونیکی با جرائم معمولی، ساختار قضایی کشور در شرایط حاضر از لحاظ قوانین، دانش قضات و ضمانت اجرایی در قبال جرائم الکترونیکی دچار اشکالات اساسی شده است.

۵ـ **تحریم‌های بین‌المللی:** با توجه به نیاز کشور به خارج (به خصوص آمریکا) در زمینهٔ فناوری‌های سخت‌افزاری و نرم‌افزاری مرتبط با اطلاعات و ارتباطات، تحریم‌های بین‌المللی می‌تواند به صورت یک تهدید جدی در روند توسعهٔ فناوری اطلاعات و ارتباطات به شمار آید.

۶ـ **به رسمیت شناخته نشدن امضای الکترونیکی:** در راستای گسترش کاربرد و استفاده از فناوری اطلاعات و ارتباطات در امور اداری، تجاری، مالی و حقوقی به

رسمیت شناختن امضای الکترونیکی در قوانین مربوطه، یکی از ضرورت‌های اساسی بشمار می‌رود. به رسمیت شناخته نشدن امضای الکترونیکی در شرایط حاضر یکی از معضلات عمدهٔ پیش روی این فناوری است. عدم استفاده از امضای الکترونیکی در شرایط موجود ممکن است به دلیل عدم وجود امنیت لازم در شبکه‌های ارتباطی کشور باشد.

۷ ـ **عدم وجود ضمانت اجرایی در جهت حمایت از حقوق مصرف‌کننده**: از آنجا که توسعهٔ تجارت الکترونیکی باعث کاهش برخورد رویاروی طرفین مبادلات تجاری می‌گردد، احتمال تخطی فروشنده در مورد مشخصات تعهد شدهٔ کالای مورد مبادله افزایش می‌یابد. در شرایطی که حقوق مصرف‌کننده به دقت تعریف نشده و یا از ضمانت اجرایی لازم برخوردار نیست، گسترش استفاده از این فناوری با مشکل مواجه خواهد شد.

۸ ـ **قوانین نقل و انتقال ارز**: یکی از تبعات گسترش فناوری اطلاعات و ارتباطات، لزوم انتقال ارز برای خرید کالا و خدمات و همچنین سرمایه‌گذاری و یا برداشت از عایدی سرمایه است که قوانین فعلی از موانع عمده در این راه بشمار می‌رود.

چالش‌های مربوط به ساختار بازارها

۱ ـ **مشکلات ناشی از انحصار دولتی مخابرات**: رشد چشمگیر شبکه‌های اطلاع‌رسانی همچون اینترنت محرک مهمی را جهت بهبود کارآیی در این حوزه فراهم آورده است. عدم وجود رقابت در برخی از بخش‌های این بازار، باعث ناکارآیی بازار در ارتباط با فناوری اطلاعات و ارتباطات در کشور شده است. رشد بی‌رویه شرکت‌های دولتی وابسته به مخابرات و اختلاف فاحش بین نسبت تعداد خطوط تلفن به تعداد کارکنان این شرکت‌ها در ایران در مقایسه با شرکت‌های معتبر خارجی دلیلی بر این مدعاست.

۲ ـ **موانع فعالیت بخش خصوصی**: سود به عنوان یک محرک مؤثر، بخش خصوصی را به حرکت در جهت گسترش و شکوفایی فعالیت‌های خود در بازارهای مختلف ترغیب می‌نماید، فعالیت این بخش در صورتی می‌تواند رشد قابل توجهی ایجد کند که زمینهٔ لازم برای فعالیت آن مهیا گردد.

وجود تنگناهای فراوان بر سر راه بخش خصوصی در زمینهٔ فناوری اطلاعات و

ارتباطات چالش عمده‌ای در مسیر توسعهٔ این فناوری به شمار می‌رود.

۳ ـ **ساختار سنتی بازارها**: با توجه به ساختار سنتی بازارها در کشور ما تغییر نظام تجاری با مخالفت‌های عمده‌ای مواجه خواهد شد. برنامه‌ریزی در جهت توسعهٔ تجارت الکترونیکی بدون توجه به ساختار قبلی و بدون همکاری فعالان نظام تجاری قبلی دشوار یا غیرممکن خواهد بود.

چالش‌های اجتماعی و فرهنگی

۱ ـ **سطح پایین دانش عمومی در زمینهٔ فناوری اطلاعات و ارتباطات**: سطح پایین دانش عمومی آحاد جامعه در زمینه‌های مرتبط با فناوری اطلاعات و ارتباطات یکی از موانع گسترش استفاده از این فناوری است. هر چند نسل جوان با اقبال خوبی به استفاده از این فناوری روی آورده‌اند، لیکن این آموزش‌های موردنیاز به نحو کارآمدی در آموزش پیش از دانشگاه گنجانده نشده است. از دیگر روی افزایش خدمات و امکانات مورد ارائه با استفاده از این فناوری، افراد را به فراگیری بیشتر در مورد آن تشویق می‌نماید. سطح پایین دانش برخی از مدیران نیز در زمینهٔ فناوری اطلاعات و ارتباطات به عنوان یک مانع جدی مطرح است.

۲ ـ **عدم اعتماد عمومی در مورد امنیت اطلاعات**: یکی از الزامات عصر اطلاعات، اطمینان مردم به عدم سوءاستفاده از اطلاعات شخصی موجود در شبکه‌های اطلاعاتی است. ایجاد جو امنیتی در جامعه باعث اطمینان افراد در روی آوردن به فناوری‌های نوین اطلاعاتی می‌گردد.

چالش‌های مرتبط با زیرساخت‌های نرم‌افزاری و سخت‌افزاری

۱ ـ **عدم تناسب آموزش‌های تخصصی با نیازهای جامعه**: در زمینهٔ آموزش علوم و تکنیک‌های مرتبط با فناوری اطلاعات، آموزش‌های دانشگاهی در برخی از موارد با دستاوردهای جدید تکنیکی متناسب نیست، پیشرفت سریع فناوری می‌باید در آموزش‌های ارائه شده لحاظ شود.

۲ ـ **امنیت پایین شبکه‌های مخابراتی**: یکی از نیازهای اساسی در زمینهٔ گسترش استفاده از فناوری اطلاعات و ارتباطات امنیت قابل قبول شبکه‌هاست. هرچه ارزشمندی

اطلاعات موجود در شبکه و نوع مبادلات انجام شده در آن افزایش یابد، سطح امنیت موردنظر نیز باید ارتقا یابد. متأسفانه در این زمینه یکی از موانع نیز کم دانشی متخصصین تربیت شده در نظام دانشگاهی در زمینه فناوری اطلاعات است.

۳ ـ ضعف زیرساخت‌های مخابراتی: طراحی زیرساخت‌های مخابراتی کشور عمدتاً به منظور کاربری‌های ارتباطات تلفنی و بر مبنای فناوری قدیمی صورت گرفته است. این زیرساخت‌ها طبیعتاً پاسخگوی نیازهای فناوری اطلاعات و ارتباطات کشور نیست.

۴ ـ نبود استانداردهای موردنیاز: در توسعهٔ فناوری اطلاعات و ارتباطات وجود استانداردهای زیر ضروری به نظر می‌رسد:

ـ استانداردهای تبادل اطلاعات

ـ استانداردهای کدگذاری کالا و خدمات

ـ استانداردهای کد مکان

ـ استانداردهای فونت فارسی

۵ ـ نبود ابزارهای داد و ستد الکترونیکی و عدم گسترش بانکداری الکترونیکی: گسترش تجارت الکترونیکی به ایجاد زیرساخت‌هایی وابسته است که از آن جمله پول الکترونیکی و بانک الکترونیکی را می‌توان نام برد.

عدم وجود این زیرساخت‌ها از موانع عمدهٔ توسعهٔ فناوری اطلاعات و ارتباطات در کشور است.» [۱۱] همانطوریکه در بندهای ۱ و ۲ چالش‌های قانونی عنوان گردید ابهاماتی در زمینه اجرای قوانین موجود بویژه با توجه به پیشرفت فوق‌العاده فن‌آوری اطلاعات حادث گردیده که این ابهامات در مورد سایر مباحث فوق نیز کاملاً مشهود می‌باشد و مستلزم بازنگری و کارشناسی در قوانین و مقررات مربوطه خواهد بود.

آسیب‌شناسی در فرآیند شناخت تهدیدهای امنیتی

در مطالعات راهبردی بویژه در سطح کلان ملّی و فراملّی، بررسی محیط (محیط دور و نزدیک) از عمده‌ترین پارامترهای ذی‌مدخل در تدوین راهبردها می‌باشد. به طور اعم، در مدل‌های گوناگونی که در خصوص فرآیند مدیریت استراتژیک توسط صاحب‌نظران طراحی و ارائه گردیده است، حاصل مطالعات محیط نزدیک (محیط ملی ـ محیط درون

سازمانی) بایستی به نقاط ضعف و نقاط قوت سیستم برسد. این نتایج برای تدوین راهبرد در سطوح غیرامنیتی قابل استفاده است لیکن برای سطح امنیتی، مسائل مرتبط با امنیت ملی و منافع حیاتی کافی نیست و بایستی دقیقاً مورد ارزیابی مجدد قرار گیرند. توضیح اینکه صرف وصول به نقاط قوت نمی‌تواند برای تدوین راهبرد کافی باشد چرا که تمام نقاط قوت یا پتانسیل‌های موجود توسط دولتی که قادر به بهره‌برداری از آنها نیست نمی‌تواند مورد استفاده قرار گیرد و لذا نمی‌توان روی آنها حساب نمود. به عنوان مثال اگر یک دولت ضعیف از نظر منابع طبیعی دارای معادنی از فلزات استراتژیک باشد ولی فناوری استخراج و بهره‌برداری از آنها را نداشته باشد ضمن اینکه دارا بودن این معادن جزو پتانسیل‌های بالقوه آن کشور محسوب می‌شود معهذا نمی‌توان آن را به عنوان یک عامل در دسترس، برای مقابله با مشکلات و تهدیدات مورد استفاده قرار داد لذا این عامل از دایرهٔ محاسبات ملی کنار می‌رود.

همچنین در احصای نقاط ضعف ملی هم نمی‌توان به‌طور کلی اظهارنظر نمود که تمام نقاط ضعف را باید در تدوین راهبردها لحاظ کرد چرا که برخی از این نقاط ضعف ممکن است توسط برخی از پتانسیل‌ها برطرف گردند. لذا برغم وجود چنین ضعفی در سیستم، ممکن است با اندکی توجه به امکانات موجود بتوان پاره‌ای از آنها را کنار گذاشت.

به منظور شناخت تهدیدات امنیتی لازم است پارامترهای مؤثر در فرآیند بخوبی تشریح گردند. بنابراین این مفاهیم را می‌توان بشکل زیر تعریف نمود:

۱ـ پتانسیل‌ها و نقاط قوت:

آنچه که یک سیستم به طور بالقوه در ابعاد مختلف دارا می‌باشد جزو پتانسیل‌های سیستم محسوب می‌گردد. قدرت ملی شامل ابعاد سیاسی، اقتصادی، نظامی، اجتماعی، فرهنگی، زیست محیطی و تکنولوژیکی می‌تواند از این پتانسیل‌ها برخوردار باشد.

۲ـ توانایی‌های ملی:

آنچه که از میان پتانسیل‌ها و نقاط قوت با ایجاد زمینهٔ لازم می‌تواند به کار گرفته شود توانایی‌های ملی است. با اندکی تسامح، بیشتر نقاط قوت را می‌توان جزو توانایی‌ها

دانست لیکن دامنهٔ توانایی‌ها وسیعتر از پتانسیل‌ها می‌تواند باشد. به عنوان مثال دسترسی کشور به آب‌های آزاد یکی از پتانسیل‌ها و نقاط قوت جمهوری اسلامی ایران است. از این نقطه قوت می‌توان استفاده‌های فراوانی کرد که از آنها به عنوان توانایی‌ها یاد می‌کنیم.

۳ـ قابلیت‌های ملی:

گاهی در بالفعل کردن نقاط قوت با اشکال مواجه می‌گردیم، موانعی بر سر راه خواهد بود که اجازه نمی‌دهد تمام نقاط قوت و توانایی‌ها مورد بهره‌برداری قرار گیرند. عواملی که مانع از تحقق این امر است «نامحتمل‌ها و موانع» خوانده می‌شوند. این عوامل در محاسبات راهبردی بایستی مورد توجه قرار گیرند.

نقاط قوت و پتانسیل‌های ملی توانائی‌های ملی حذف نامحتمل‌ها قابلیت‌های ملی

اگر ثروت ملی را جزو پتانسیل‌ها و نقاط قوت ملی کشورمان تلقی نماییم، درآمد ملی بالا، از توانایی‌های ما خواهد بود. لیکن یکی از موانع مهم در تحقق این امر وابستگی به فروش نفت است که باعث می‌گردد نتوانیم از تمام ثروت‌های خود بهره ببریم. لذا این توانایی نمی‌تواند تبدیل به قابلیت ملی گردد. در مورد نفت که یک ثروت ملی است این مثال کاملاً قابل تطبیق است. یعنی نوسانات قیمت نفت، نفوذ قدرت‌ها در اوپک برای تثبیت یا کاهش قیمت نفت، عوامل و موانعی هستند که نمی‌گذارند این توانائی ملی دقیقاً تبدیل به قابلیت ملی گردد و لذا درصد کمی از این توانایی تبدیل به قابلیت ملی می‌گردد که همان مقدار بایستی در تدوین راهبردها لحاظ گردد. زیرا اگر تمام پتانسیل خود را در بخش نفت جزو قابلیت‌های ملی به حساب آوریم آن وقت راهبرد حاصله نمی‌تواند از دقت و روانی مناسب برخوردار باشد.

بنابراین برای مفهوم قابلیت‌ها گفته می‌شود که: به آن بخش از توانایی‌های یک کشور یا چند کشور متحد برای اجرای راه‌های کار معینی اطلاق می‌شود که انجام آن محتمل و امکانپذیر باشد.

۴ـ نقاط ضعف ملی:

بررسی‌های محیط ملی ممکن است ما را در ابعاد گوناگون با وجود نقاط ضعف مواجه

سازد. این نقاط ضعف ممکن است به علت وجود پاره‌ای محدودیت‌ها باشد که موجبات پدید آمدن ضعف‌ها را فراهم ساخته است.

محدودیت‌های محیطی نقاط ضعف ملی آسیب‌پذیری‌های ملی

در مثال صنایع مونتاژ یکی از نقاط ضعف ملی در بخش صنعت می‌باشد. اگر نتوانیم فناوری جدید را در این زمینه وارد و بومی کنیم و یا تحت تأثیر تحریم‌ها قرار داشته باشیم کم‌کم این ضعف به یک معضل مبدل خواهد شد که ما را به شدت آسیب‌پذیر خواهد کرد.

در تعریف مفهوم آسیب‌پذیری نیز گفته می‌شود:

آسیب پذیری عبارت است از ظرفیت و زمینه و شرایطی در اجزا یا کل سیستم که در صورت وجود عامل خارجی و یا تأثیر نیروی خارجی در جزء و یا کل سیستم ایجاد گسل و ناپایداری نموده و عدم تعادل ایجاد نماید.

در جای دیگر گفته شده است:

آسیب‌پذیری آن دسته از نقاط ضعف هستند که در اثر هر نوع اقدام دشمن و یا کاربرد هر وسیله‌ای، شدیداً متأثر شده و باعث کاهش قابلیت‌ها و در نتیجه عدم تحقق اهداف ملی گردند.

بنابراین در این تعریف هم «اقدام دشمن» به عنوان یک «عامل خارجی» که بر نقاط ضعف تأثیر می‌گذارد، برشمرده شده است.

۵ـ نیات:

نیات به تصمیم یک کشور یا ائتلافی از چند کشور برای بکارگیری قابلیت‌های خود به طرق معین و در زمان‌ها و مکان‌های معین اطلاق می‌گردد. معمولاً نیات، اغراض پشت اهداف دولت‌هاست. هیچ دولتی به وضوح نیات خود را برملا نمی‌سازد.

مفسّرین و محققین معمولاً با بررسی روندها و برگزاری مصاحبه‌ها و تحلیل سخنرانی‌ها و موضع‌گیری‌های مقامات دولتی، میزان خریدها و سفارشات تسلیحاتی، میزان تخصیص بودجه‌های عملیاتی برای قوای نظامی، افزایش ظرفیت بنادر، خطوط راه‌آهن و راه‌های مواصلاتی، میزان بودجه‌های تحقیق و توسعه، پیام‌های دیپلماتیک، قراردادهای سیاسی و اقتصادی، جبهه‌گیری‌ها، استقرار و جابجایی نیروها و... در مورد

راهبرد، اهداف و نیات یک کشور به گمانه‌زنی می‌پردازند.

یکی از مأموریت‌های اساسی سیاست خارجی یک کشور عبارت است از: فراکرد مستمر ارزیابی ظرفیت و توانایی و نیت دیگر کشورها، و این کاری است بس مشکل که نیاز به مهارت و هوشمندی کارشناسان دارد.

برای تشخیص نیات کشورهای دیگر موارد زیر باید مورد بررسی قرار گیرد:

۱ـ منافع ملی کشور هدف

۲ـ اهداف کشور هدف

۳ـ سیاست‌های کشور هدف

۴ـ دکترین واصول پذیرفته شده کشور هدف

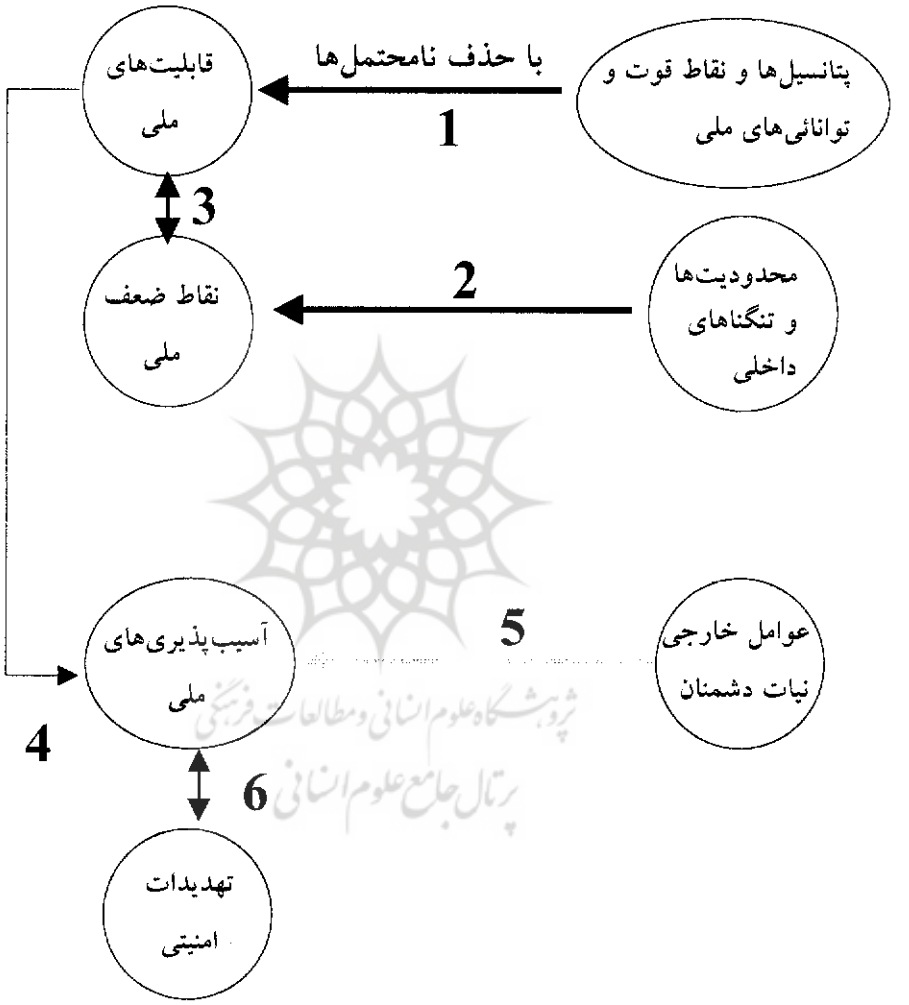
۵ـ تعهدات کشور هدف نسبت به دیگر کشورها

۶ـ ارادهٔ ملی کشور هدف

۷ـ عملکردها

با این توضیحات، ملاحظه می‌گردد که در محیط مجازی (سایبر) برای شناخت آسیب‌پذیری‌های ملی و سپس پی بردن به تهدیدهای آن، لازم است در این فضا یک بررسی جامع از وضعیت محیط ملی داشته باشیم و از رهگذر این بررسی‌ها نقاط قوت و ضعف داخلی را در برخورد با این پدیده بدست آوریم. چنانچه امکانات داخلی (نرم‌افزاری و سخت‌افزاری) قادر به برطرف کردن نقاط ضعف نگردند در آن صورت است که آسیب‌پذیری‌های ملی در این محیط برملا می‌گردد و کافی است دشمنان نسبت به این نقاط ضعف آگاهی یابند. بنابراین هر فشاری از طریق دشمنان و یا سوء استفاده‌کنندگان بر این آسیب‌پذیری‌ها وارد شود موجب بروز تهدیدهای امنیتی برای کشور خواهد شد. فلذا لازم است در بررسی‌های آتی با بررسی همه جانبهٔ محیط داخلی و محیط خارجی و پی بردن به نیات دشمن، راهکارهای کاهش آسیب‌پذیری‌ها را یافته و راه‌حل‌های مناسبی را برای مقابله با عملکرد دشمنان بیابیم.

بنابراین می‌توان از تعامل منطقی پارامترهای فوق، چگونگی شکل‌گیری آسیب‌پذیری‌ها و سپس تهدیدات امنیتی را دریافت. تأثیر و تأثر پارامترهای فوق در یک تصویر شماتیک در شکل (۱) خواهد بود:



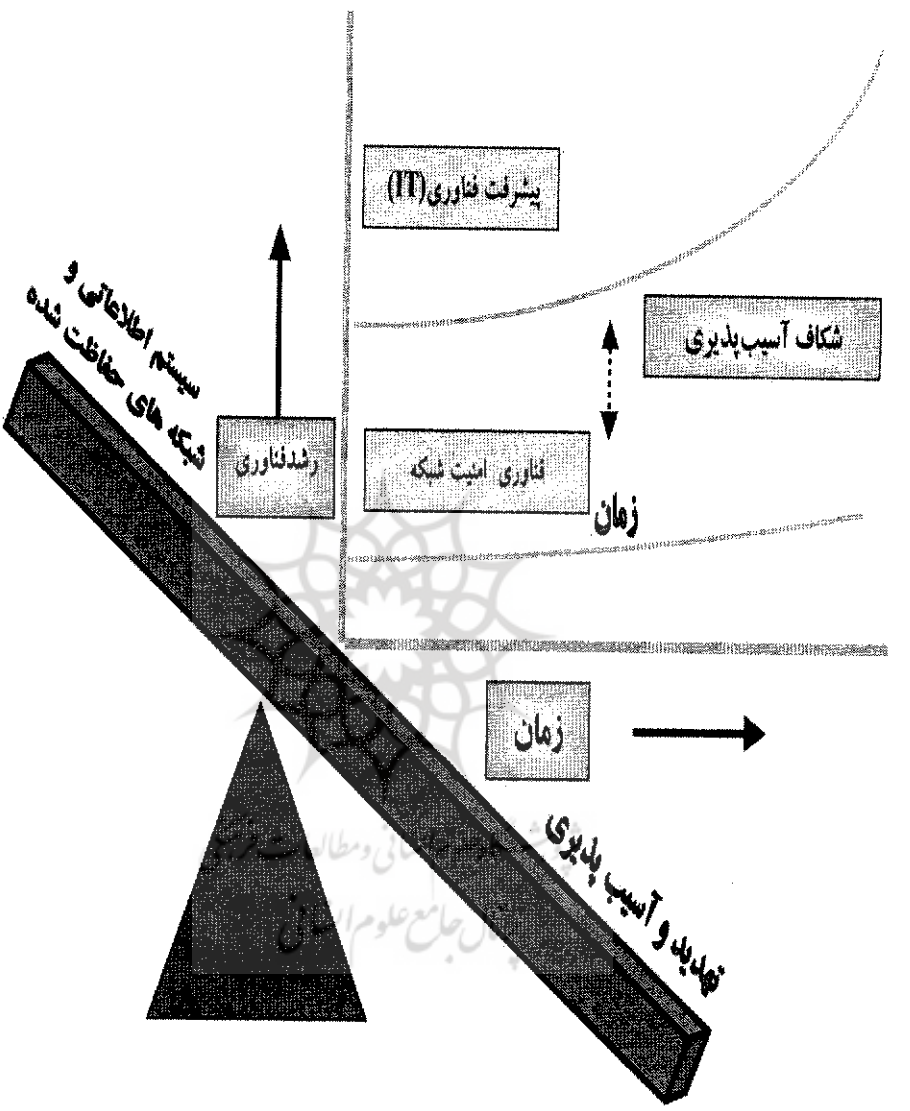
«شکل شماره ۱» چگونگی شکل‌گیری آسیب‌پذیری‌ها و تهدیدات را نشان می‌دهد.

الف ـ آسیب‌پذیری شبکه‌های رایانه‌ای

در اثر پیشرفت و توسعهٔ فناوری اطلاعات، امنیت ملی و اقتصادی کشور وابستگی روزافزونی به فناوری اطلاعات و زیرساخت‌های اطلاعاتی پیدا می‌کند. هستهٔ اصلی زیرساخت‌های اطلاعاتی، اینترنت است که در ابتدا برای استفادهٔ مشترک از اطلاعات طبقه‌بندی شدهٔ محققین ایجاد گردید. این شبکه امروزه شامل میلیونها کامپیوتر است که از طریق آنها خدمات و فعالیت‌های بسیاری انجام می‌پذیرد. در کشورهای پیشرفته از طریق این شبکه همچنین موضوعات فیزیکی از قبیل، انتقال الکتریسته، قطارها، خطوط لوله، مخازن شیمیائی، رادارها و بازارهای سهام کنترل می‌شوند.

فناوری اطلاعات روزبه‌روز توسعه پیدا کرده و کاربردهای آن فراگیرتر می‌شوند، افراد بیشتری به آن روی آورده و خدمات اجتماعی گسترده‌تری در بستر آن ارائه می‌گردد. سرعت توسعهٔ فناوری اطلاعات تأییدی است بر این ادعا، که براساس آن سرعت رشد کاربران اینترنت و اطلاعات و خدمات ارائه شده در آن قابل اثبات است. از سوی دیگر چنانچه در شکل (شماره ۲) نشان داده شده، فناوری‌های دفاع از تهدیدکنندگان شبکه‌های رایانه‌ای با سرعت کمتری در حال توسعه است. بنابراین بین گسترهٔ کاربردهای فناوری اطلاعات و فناوری‌های امنیتی آن فاصله‌ای وجود دارد که به آن شکاف آسیب‌پذیری گویند. همانطوری که در شکل ملاحظه می‌شود با گذشت زمان، شتاب توسعهٔ فناوری اطلاعات از شتاب توسعهٔ فناوری‌های امنیت شبکه بیشتر بوده و در نتیجه اختلاف آسیب‌پذیری به عنوان یک معضل جدی کشورها روزبه‌روز در حال افزایش است.

مدل شکاف آسیب‌پذیری نیز با هدف بررسی آیندهٔ آسیب‌ها در شکل ارائه شده است. همانگونه که در این مدل ملاحظه می‌شود با افزایش زمان، روند توسعهٔ فناوری اطلاعات از روند توسعهٔ فناوری‌های دفاعی مربوطه سبقت گرفته و این اختلاف را بوجود آورده است.



Websit : http://www.niser.org.my _ http://www.mycert.org.my

شکل شماره ۲ - شکاف آسیب‌پذیری

همانطوری که در این مدل مشاهده می‌شود، کشورهایی که در آنها فناوری اطلاعات به عنوان بستر اصلی فعالیت‌ها درآمده، آسیب‌پذیری‌هایی هم پیدا نموده‌اند. این آسیب‌پذیری‌ها بیشتر ناشی از وابستگی سایر بخش‌ها به فناوری اطلاعات و سهولت استفاده از فناوری اطلاعات توسط گروه‌ها و افراد تهدیدکنندهٔ فضای مجازی است. برخی از این آسیب‌پذیری‌ها در ادامه معرفی شده‌اند:

علل آسیب‌پذیری شبکه‌های رایانه‌ای

حال این سؤال مطرح می‌شود که چرا سیستم‌ها آسیب‌پذیر هستند؟ در خصوص علل آسیب‌پذیر بودن سیستم‌ها در برابر حمله چند دلیل وجود دارد که در ادامه به تشریح آنها می‌پردازیم:

شبکه به علل مختلف فنی و یا غیرفنی نیز آسیب‌پذیر است. برخی از موارد جزئی‌تر آسیب‌پذیری بشرح زیر می‌باشد:

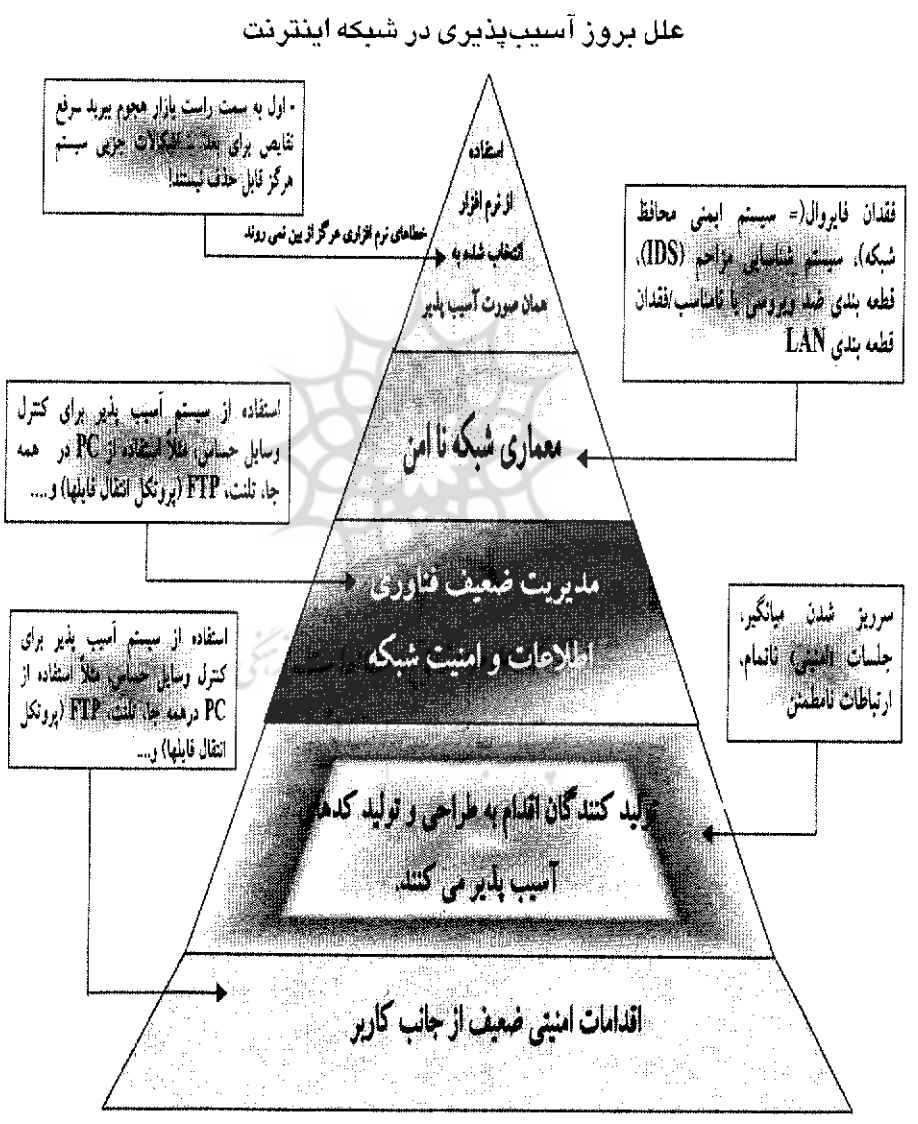
ـ ضعف دانش کاربران یکی از نقاط آسیب‌پذیر است. کاربران شبکه با انتخاب رمزهای ساده و عدم انجام دستورالعمل‌های امنیتی به‌طور ناخواسته باعث سهولت در کار نفوذگران می‌شوند.

ـ ضعف فناوری و وابستگی فناوری به شرکت‌های خارجی، محصولات این شرکت‌ها را به صورت بالقوه آسیب‌پذیر نموده است. برای مثال شنود تلفن‌های یک کشور از کشور دیگر، قسمت عمده‌اش به خاطر فناوری وارداتی و غیرشفاف است.

ـ ضعف در فناوری‌های امنیت شبکه، دفاع از شبکه و ردیابی نفوذگران عرصه را برای فعالیت آنها باز می‌گذارد.

گسترهٔ آسیب‌پذیری‌ها بسیار متنوع است و می‌تواند از امنیت فیزیکی ضعف شبکه‌ها تا خطاهای ناشناخته نرم‌افزاری را شامل شود. در اکثر اوقات مدیریت ضعیف، باعث آسیب‌پذیری سیستم می‌شود. ادارهٔ ضعیف یک سیستم، مشکلی عمومی است که وقتی در کنار آسیب‌پذیری‌های دیگر قرار گیرد، بسیار خطرناک خواهد شد.(شکل شماره ۳)

طبق شکل شماره ۳ ـ علل ضعف سیستم‌ها در پنج شاخه خلاصه می‌شود: اطلاعات کاربران ضعیف است ـ برنامه‌های مورد استفاده نفوذپذیر طراحی شده‌اند ـ مدیریت امنیت شبکه ضعیف است ـ معماری شبکه ناامن است و برنامه‌های کاربردی خطا داشته و لذا نفوذناپذیرند.



شکل شماره ـ ۳

علل افزایش آسیب‌پذیری شبکه‌های رایانه‌ای از نظر فنی

عوامل مختلفی از نظر فنی وجود دارند که آسیب‌پذیری شبکه‌های رایانه‌ای را افزایش می‌دهد در این بخش به مواردی از آن اشاره می‌شود:

الف ـ ویروس

برای اولین بار در دوم نوامبر ۱۹۸۸، یک ویروس رایانه‌ای در آمریکا، سبب از کار افتادن رایانه‌ها در مراکز حساس از جمله MIT و لابراتوارهای لورنس لیورمور [۱۲] گردید.

ویروس رایانه‌ای در حالت معمولی برنامه‌ای کوتاه است که خود را ضمیمهٔ یک برنامهٔ دیگر می‌کند. رفتار ویروس‌های رایانه‌ای شبیه به ویروس آنفولانزا می‌باشد که پس از ورود به بدن، شروع به تکثیر کرده و در صورت فقدان مراقبت لازم، سیستم دفاعی بدن را از کار می‌اندازد.

ب ـ کرم

اولین و مشهورترین ویروس، کرم [۱۳] نام دارد که بطور تصادفی در دوم نوامبر ۱۹۸۸ وارد شبکه‌های رایانه‌ای شد. طبق ادعای طراح آن، هدف او از این کار تنها اثبات ضعف سیستم‌های امنیتی رایانه‌ها بوده است.

کرم‌ها زیر مجموعه‌ای از ویروس‌های رایانه‌ای می‌باشند که برخلاف ویروس‌ها که خود را به صورت پست الکترونیکی برای کاربران اینترنت ارسال می‌کنند، به طور مستقل اجرا شده و پس از سوراخ کردن سیستم رایانه به طرف مغز رایانه پیش می‌روند.

ج ـ اسب تروا

در طی جنگ تروا، به گفته هومر، یونانیان اسب چوبی باشکوهی را بیرون دیوارهای تروا جا گذاشتند. مردم تروا آن را وارد شهر و در نهایت کشف کردند که سربازان یونانی در درون اسب توخالی مخفی شده‌اند. بر همین اساس برخی از برنامه‌نویسان و نویسندگان باهوش برنامه‌های ویروسی، ویروس خود را درون پاکت‌هایی قرار داده و آنها را ضمیمهٔ برنامه‌های نرم‌افزاری باارزش می‌کنند.

د ـ SPAM

Spam یک نامهٔ الکترونیکی آزاد و بطور کامل ناشناس است که صندوق پستی کاربران را از نامه‌ها و نوشته‌های بی‌مصرف پر می‌کند. گروهی فکر می‌کنند که با خرید از

سایت‌های تجاری مانند آمازون و یا از طریق ISPها خطر ورود Spam به رایانهٔ خود را بالا برده‌اند، در صورتی که هرگز این چنین نیست؛ زیرا این سایت‌ها، فیلترهایی بسیار قوی برای جلوگیری از ورد spamها در رایانه و شبکه‌های خود قرار داده‌اند تا بتوانند مشتریان و همچنین اطلاعات آنها را حفظ کنند.

هـ ـ درهای پشتی

در پاره‌ای از موارد، برنامه‌نویسان یا طراحان سیستم‌ها، راه‌هایی را درون سیستم امنیتی، برای ورود خود لحاظ می‌کنند که باعث کاهش امنیت سیستم می‌شود. به عنوان مثال، آنها می‌توانند از طریق وارد کردن یک رمز عبور سری، وارد رایانه‌ها شده، علاوه بر دسترسی به اطلاعات، آنها را به‌طور دلخواه تغییر دهند.

و ـ خطاهای نرم‌افزاری

یکی از راه‌های ورد مزاحمان به داخل سیستم اشکالات نرم‌افزاری است. مهمترین خطاهای نرم‌افزاری مورد استفادهٔ نفوذگران، سرریز بافر است که مزاحم با استفاده از این راه نفوذی وارد سیستم می‌شود. به عنوان مثال، برنامه‌نویس جهت نام کاربر بطور معمول از ۲۵۶ کاراکتر استفاده می‌نماید. به‌طور حتم در این حالت برنامه‌نویس تصور می‌کند که هیچ کاربری از بیش از ۲۵۶ کاراکتر برای نام کاربر استفاده نمی‌کند؛ اما هکرها به این موضوع فکر می‌کنند که اگر نام کاربر را نادرست و بزرگتر از ۲۵۶ کاراکتر وارد نمایند، چه اتفاقی خواهد افتاد و در این صورت کاراکترهای اضافی کجا خواهند رفت.

وقتی که بافر سرریز شود، امکان اجرای هر دستوری وجود دارد؛ بنابراین، هکرها از این روش استفاده کرده و وارد سیستم شده و اطلاعات را مطالعه و یا دستکاری می‌کنند.

تهدیدهای متوجه امنیت ملی

ـ مفهوم تهدید

در گذشته ذهن بشر مفهوم «تهدید» را با مفهوم «تقدیر و سرنوشت» مرتبط می‌دانست به تعبیر روشنتر می‌توان رابطه‌ای محسوس بین علم بشر و تلقی از تهدید مشاهده کرد. در واقع اگر تقسیم‌بندی اگوست کنت را بپذیریم، «شناخت تقدیر محور» با مرحلهٔ

متافیزیکی علم بشری قرین بود. این مرحله بدین معنی بود که چون انسان هنوز به ماهیت واقعی مناسبات بین پدیده‌ها وقوف نیافته بود، دلیل رخداد حوادث را ماورایی می‌پنداشت و آن را در قالب واژهٔ «تقدیر» صورت‌بندی نموده و چون چیستی پدیده برایش در هاله‌ای از ابهام بود فلذا دریچه‌ای برای نگریستن به ابعاد و علل مستور آن وقایع فراروی خود نمی‌یافت.

هرچند بیان می‌شود واژهٔ «مخاطره» (به معنای خطر کردن و از میان صخره راه باز کردن، که از کلمات مستعمل در دریانوردی مردم اسپانیا بود) در قرن ۱۷ به زبان انگلیسی راه یافت، لیکن تحول در نظام اندیشگی انسان به معنای درک روابط بین پدیده‌ها و تحلیل عقلانی و روایی‌تر امور را می‌توان به عنوان عامل بنیادین این دگردیسی مفهومی در نظر گرفت. به عبارتی مفهوم مخاطره از شناخت این واقعیت نشأت می‌گیرد 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 فرایند دولت‌سازی، بتدریج دال مخاطره، مدلول‌های خاصی را به اذهان متبادر نمود ودراین فراگرد مفهوم تهدید از بطن تطورات مزبور سربرآورد. عده‌ای هرگونه تجاوز به حق حاکمیت دولت‌ها در ادارهٔ امور داخلی و خارجی را تهدید تلقی می‌نمایند. برخی، مخاطراتی که اهداف و ارزش‌های حیاتی یک کشور را به گونه‌ای در معرض خطر قرار دهد که بیم آن رود در اهداف و ارزش‌های حیاتی یک کشور را به گونه‌ای در معرض خطر قرار دهد که بیم آن رود در اهداف و ارزش‌های مذکور تغییر اساسی صورت پذیرد را تهدید می‌دانند.»[۱۴]

«تهدید، امنیت ملی یک نظام را که متضمن حیاتی‌ترین منافع آن است به خطر می‌اندازد. به هر حال شناخت و تشخیص این تهدیدها به راحتی میسور نمی‌باشد. دو دلیل عمدهٔ این مسأله عبارتست از:

۱ـ مسأله عینی یا ذهنی قضیه[۱۵] به عبارتی آیا تهدیدات، واقعی هستند یا تخیلی؟

۲ـ دشواری تمایز تهدیدات جدی از لحاظ امنیت ملی.

اساساً تهدیدها موضوع تعریف و بازتعریف هستند و نه موضوع شناخت. از اینرو می‌توان تهدیدات معطوف به نظام ارزشی، فرهنگ، اهداف، هویت ملی و... را در کنار تهدیدات ناظر بر «ساختار»، «مولفه‌های مختلف قدرت»، «کنشگران سیاسی / اجتماعی»،

«تمامیت ارضی»، «مؤسسات و تأسیسات حیاتی» و... مورد شناسایی قرار داد. درجهٔ فوریت و جدیت تهدیدات نیز درهم تنیدگی خاصی با شدت و میزان تهدید شوندگی کلیت و مرکزیت یک سیستم را دارد.»[۱۶]

ـ بازشناسی تهدیدها

همانگونه که بیان شد تهدید مفهومی نسبی و ذهنی بوده که در هر جامعه‌ای به مدلول خاصی ارجاع می‌دهد و شناخت و درک آن به مؤلفه‌های گوناگونی بستگی دارد. با این وجود اگر خواسته باشیم معنایی را که در گذشته، از مفهوم تهدید در اذهان تداعی می‌شد را بطور خلاصه بیان کنیم به این جمع‌بندی خواهیم رسید که تهدیدها در دوره‌های پیشین:

۱ ـ عمدتاً با منشاء خارجی تصور می‌شدند،

۲ ـ مبتنی بر قدرت نظامی بودند،

۳ ـ متکی بر حضور فیزیکی دشمن بودند،

۴ ـ آگاهی از تهدیدها گسترده نبود،

۵ ـ دامنهٔ تهدیدها محدود بود،

۶ ـ در اکثر تهدیدها، دولت‌ها نقش بسیار مؤثری داشتند،

۷ ـ تهدیدها به راحتی قابل تشخیص بودند.

ویژگی تهدیدها

«بواسطهٔ همبسته و پیوسته بودن متن و زمینهٔ همزمان با تحولات جهانی، مفاهیم نیز دستخوش دگردیسی گشته‌اند و در این راستا تهدیدها نیز با صیرورت بافت و ترکیب بسترها، شکل و ماهیتی نوین یافته‌اند. علیرغم آنکه تهدیدات، ماهیتی شفاف نداشته و چند وجهی هستند معهذا می‌توان در شرایط نوین، ویژگی تهدیدات را اینگونه برشمرد:

۱ ـ اکثر این تهدیدها دولت محور نیستند. به عبارت دیگر این قبیل مخاطرات از عوامل و بازیگرانی که خصلتی فروملی یا فراملی دارند، ساطع می‌گردد. در نتیجه آنها به راحتی قابلیت تطبیق با نظریه‌ها و تحلیل‌های دولت محور را ندارند.

۲ ـ این چالش‌ها، فضای جغرافیایی خاصی ندارند. تمرکزی که در گذشته حول

تهدیدها وجود داشت به وسیلهٔ قدرت نظامی ایجاد می‌شد و شرایطی را جهت تلاش برای مهار این قبیل مخاطرات فراهم می‌نمود. بهرحال چالش‌های غیرسنتی نشانگر آن می‌باشد که تهدیدها متنوع، چندسویه و چندجهتی است ضمن اینکه آنها را باید در سه سطح جهانی، منطقه‌ای و ملی نگریست.

۳ ـ این تهدیدها را نمی‌توان تنها با اتکاء به سیاست‌های دفاعی سنتی مدیریت کرد. سازمان‌های نظامی / دفاعی امکان دارد به ویژه در کشمکش‌های خشونت‌آمیز نقش داشته باشند، ولی باید در نظر داشت مدیریت مؤثر مستلزم طیفی از رهیافت‌های غیرنظامی است. [۱۷]

جدا از ویژگی‌های مذکور بنظر می‌رسد در عصر جهانی شدن می‌توان مفهوم تهدید را از برخی زوایای دیگر نیز مورد تدقیق قرار داد که در ادامه به پاره‌ای از آنها اشاره می‌شود:

الف ـ جهانی شدن تهدید از جهت تراکم: جنگ‌های اطلاعاتی مصداق بارز این موضوع است. [۱۸]

ب ـ بسط جهانی محیط‌ها و فضاهای تهدید: به عبارتی رخدادهایی که بخش عمده‌ای از بشریت را مورد تهدید قرار می‌دهد، متکثر و فزاینده شده است.

ج ـ تهدیدهای برآمده از محیط ساخته شده یا طبیعت اجتماعی شده: در واقع بحث بر سر آن است که با عنایت به تحول رابطهٔ «انسان و محیط» که به شدّت متأثر از افزایش توانمندی‌های بشر و دانش انسانی می‌باشد، مخاطرات نوینی را فراروی امنیت انسان قرار داده است. پدیده‌هایی همچون گازهای گلخانه‌ای، زباله‌های هسته‌ای و... نمودهایی در این زمینه هستند. [۱۹]

د ـ گسترش محیط تهدیدهای نهادی: در این رابطه می‌توان به بازارهای سرمایه‌گذاری که قابلیت تأثیرگذاری بر سرنوشت تعداد بیشماری از انسان‌ها را دارد، اشاره کرد.

هـ ـ آگاهی جهانی نسبت به تهدیدها: امروزه بسیاری از تهدیدات برای عامهٔ مردم شناخته شده هستند. [۲۰]

و ـ تهدیدهای نشأت گرفته از مشروعیت / اقتداریابی بازیگران فراملی: مداخلهٔ سازمان‌های بین‌المللی در امور داخلی کشورها در مواردی نظیر عدم رعایت حقوق

بشر و یا تحمیل قواعد و قوانین این نهادها به کشورها، نمونه‌های بارز این تهدید می‌باشد.

ز ـ تهدیدهای ناشی از اقتصاد جهانی: نظام بدور از عدالت اقتصاد بین‌المللی در واقع حکم «خشونت ساختاری» را داشته که در آن فقر و نابرابری تهدیدات جدی و آنی محسوب می‌شوند.

ح ـ ابهام در شناسایی کشورهای تهدید کننده: بدین مفهوم که به واسطهٔ پیچیدگی و تناقضات مناسبات و درهم تنیدگی روابط، ممکن است دولتی در یک زمینه، تهدید و در عرصه‌ای دیگر متحد به نظر آید.

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

الف ـ محیط امنیتی: که معیار اساسی در خصوص تهدید خارجی و مدلهای همکاری و اتحاد می‌باشد.

ب ـ سخت‌افزارها: که مقدورات فیزیکی، دکترین‌های عملیاتی، ساختار قدرت و گزینش جنگ‌افزارها را دربرمی‌گیرد.

ج ـ نرم‌افزارها: که اشاره به شاخص‌های مشروعیت سیاسی، وحدت ملی و توان سیاست‌گذاری عمومی دارد.

در فضای مناسبات دو قطبی، توجهات معطوف به محیط امنیتی و سخت‌افزارها بود. امروزه مشخص گردیده اگرچه کشورها بتوانند درک واقع‌بینانه‌ای از تهدیدات داشته باشند و توانمندی‌های فیزیکی مناسبی فراهم نمایند، لیکن بدون مشروعیتی پایدار، وحدتی فراگیر و انعطاف در توان سیاست‌گذاری، قابلیت‌ها و پتانسیل‌ها، مجال و زمینه‌ای برای ظهور نمی‌یابند. به تعبیر روشن‌تر، نرم‌افزارها حلقهٔ واسط بین محیط امنیتی و سخت‌افزارها می‌باشند. نادیده انگاشتن وجه نرم‌افزاری، درک دولتمردان را از پیچیدگی روابط میان عوامل درونادی تهدیدات و ظرفیت‌های داخلی از یک طرف و کل برونداد سیاسی و ساماندهی امور امنیتی از سوی دیگر، تضعیف می‌کند.

همچنین هر چند هنر نخبگان فکری / ابزاری تقلیل کمی و کیفی تهدیدات می‌باشد، لیکن بهره‌مندی از قابلیت بالا و ظرفیت سیاسی قابل تطبیق، می‌تواند محیطی با ثبات را فراهم نماید. اکثر تهدیدات موجود در عرصهٔ جهانی دربرگیرندهٔ مولفه‌های پیچیده‌ای

است و زمانی که تدابیر مقابله کننده را نیز مدنظر قرار دهیم، قضیه پیچیده‌تر خواهد شد.

ـ تهدیدکنندگان فضای مجازی

در این بخش مهمترین تهدیدکنندگان فضای مجازی در چهار گروه عمده (تهدید) معرفی می‌شوند. اولین تهدید: عوامل خارجی هستند. این تهدید از ناحیهٔ کلیهٔ کسانی است که به یک کشور خارجی از قبیل بخش‌های نظامی و آژانس‌های امنیتی و حتی شرکت‌هایی که وابستگی زیادی به آن دولت دارند وابسته‌اند. تهدید دوم تروریست‌ها و گروه‌های افراطی هستند. این افراد ممکن است وابستگی به دولت خاصی نداشته باشند ولی در راستای اهداف خود به خرابکاری مبادرت ورزند. تهدید سوم شامل جنایتکاران و سازمان‌های جنایی است. این گروه نه تنها جرائم سازمان یافتهٔ 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 جرائم بزرگی را مرتکب شود. تهدید چهارم کاربران داخل سازمان‌ها و نیروهای خودی می‌باشند.

با توجه به اینکه هر تهدید از دو مؤلفهٔ قصد و نیت [۲۱] و قابلیت [۲۲] تشکیل می‌شود. قابلیت خود شامل دو مؤلفهٔ سازماندهی [۲۳] و ابزار [۲۴] تهدید است. ابزار نیز از تجهیزات و مهارت کار با آن تشکیل می‌شود. در این میان واژگان ترکیبی عملیات اطلاعاتی و جنگ اطلاعات در فضای مجازی از اهمیت برخوردارند.

اهمیت فضای مجازی برای عملیات نظامی به گونه‌ای است که سازمان‌های نظامی از هم اکنون برای آن برنامه‌ریزی می‌کنند. برای مثال وزارت دفاع آمریکا در چشم‌انداز ۲۰۲۰ خود این موضوع را در نظر گرفته و از عبارت‌های جدیدی از قبیل «عملیات اطلاعاتی» (IO)[۲۵] برای نمایش زمینه‌های تهاجمی ـ تدافعی در محیط اطلاعاتی استفاده کرده است.

عملیات اطلاعاتی:[۲۶]

به کلیهٔ فعالیت‌های لازم برای حمله به اطلاعات و سیستم‌های اطلاعاتی دشمن و همچنین دفاع از اطلاعات و سیستم‌های اطلاعاتی خودی، عملیات اطلاعاتی گویند. و در

تعریف جنگ اطلاعات (IW) گفته‌اند:[۲۷] جنگ اطلاعاتی بخشی از عملیات اطلاعاتی است و شامل هر فعالیت نظامی که در زمان جنگ اتفاق بیفتد و در محیط اطلاعاتی انجام شود می‌گردد.[۲۸]

نگرانی از حملات کشورهای خارجی و جنگ اطلاعات به قدری زیاد است که حتی کشوری مثل آمریکا که خود حرف اول را در فناوری اطلاعات می‌زند نیز به چاره‌اندیشی وادار کرده است.

براساس گزارش سازمان جاسوسی امریکا (سیا) برخی کشورها برای جنگ اطلاعات برنامه دارند و در حال آماده شدن هستند.[۲۹]

قابلیت‌ها

هزینهٔ کم، سهولت دسترسی، کامپیوترهای قدرتمند و ابزارهای قوی موجود، برخی از قابلیت‌های مهم سازمان‌های خارجی هستند. این سازمان‌ها بسیاری از ابزارها را به راحتی از طریق اینترنت دریافت می‌کنند و به کار می‌گیرند. که 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 وسائل الکتریکی را از کار می‌اندازد و وسائل پالس الکترو مغناطیس که در مجاورت سیستم مقصد منفجر شده و کلیهٔ تجهیزات ارتباطی منطقه را از کار می‌اندازد، نیز به صورت محدودتر قابل استفاده‌اند.

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

۲ ـ **جنگ الکترونیک**: هر نوع فعالیت نظامی که از امواج الکترومغناطیس و انرژی متمرکز برای کنترل طیف الکترو مغناطیس بهره بگیرد.

۳ ـ **عملیات روانی**: عملیات برنامه‌ریزی شده برای انتقال اطلاعات گزینشی به مردم کشورهای خارجی برای تأثیرگذاری بر دولت‌ها، سازمان‌ها، گروه‌ها و حتی اشخاص خارجی می‌باشد.

۴ ـ **فریب نظامی:** عملیاتی عمدی که برای گمراه کردن تصمیم گیرندگان ارتش دشمن استفاده می‌گردد. [۳۰]

۵ ـ **جنگ اطلاعات رایانه‌ای:** اگرچه برخی معتقدند که در حال حاضر امکان حمله به فضای مجازی در مقیاس بزرگ امکانپذیر نیست ولی بررسی‌ها نشان‌دهندهٔ رشد حملات می‌باشد.

براساس گزارشات سازمان جاسوسی آمریکا، چین یکی از بازیگران مطرح در توسعهٔ قابلیت‌های جنگ اطلاعات است. پس از پایان جنگ خلیج‌فارس در سال ۹۱، کشور چین به کاربردهای دفاعی فناوری اطلاعات علاقمندی نشان داده، برای تشکیل گروه‌هایی که آمادگی جنگ در محیط مجازی را داشته باشند تلاش کرده است. [۳۱]

قلمرو جنگ اطلاعات رایانه‌ای (جنگ مجازی)

جنگ اطلاعات یک فعالیت مجزا (ایزوله) نیست، این جنگ هم در حیطهٔ فعالیت‌های دولت‌ها و هم برخوردهای انسانی قرار دارد. در یک دسته‌بندی کلی این فعالیت‌ها را می‌توان در چهار قلمرو: امنیت ملی، جرائم ۷ حقوق فردی و دستیابی غیرمجاز بررسی نمود. مهمترین مسئله دراین بحث برای ما قلمرو امنیت ملی می‌باشد:

در محیط سایبر این قلمرو شامل مسائلی در سطح ملی از قبیل عملیات جاسوسی کشورهای خارجی، جنگ و برخورد نظامی، تروریسم و عملیات علیه یک کشور از طرف سازمان‌های غیردولتی می‌شود. البته این قلمروها کاملاً مجزا نیستند. مثلاً نفوذ رایانه‌ای[۳۲] 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.

هر کشوری دارای سازمانی است که به جمع‌آوری اطلاعات در مورد متحدان و مهاجمان، کشورهای خارجی، سازمان‌های تروریستی و سایر تهدیدات علیه امنیت ملی مشغول است. یکی از مهمترین زمینه‌های فعالیت جاسوسان خارجی، سرقت اسرار علمی، فناوری پیشرفته و سلاح‌های مدرن می‌باشد البته هنوز مدارکی از فعالیت‌های

نفوذ رایانه‌ای به قصد جاسوسی در اختیار عموم قرار نگرفته ولی مسلماً هم به این مقصود و هم به منظور تأثیرگذاری بر رسانه‌های خبری و ساخت ذهنیت استفاده می‌شود.

لایه‌های جنگ اطلاعاتی

اصولاً اهداف جنگ اطلاعاتی را در سه سطح و لایه می‌توان برشمرد:

۱ ـ **لایهٔ سیستم اطلاعات؛**[۳۳] این سطح شامل عناصر مادی تولید، انتقال و ذخیره اطلاعات می‌باشد و حملات علیه سیستم‌های اطلاعاتی باعث پیامدهای تکنیکی[۳۴] می‌شود.

۲ ـ **لایهٔ مدیریت اطلاعاتی؛**[۳۵] دراین سطح، روندهای پردازش و اطلاعات، مدیریت می‌شود و حمله در این سطح باعث پیامدهای عملی[۳۶] می‌گردد.

۳ ـ **لایهٔ تصمیم‌گیری؛**[۳۷] 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[۳۸] می‌شود.

اقدامات پدافندی

از نقطه نظر 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 بدست آورد و یا یک گروه خرابکاری می‌خواهد به زیرساخت حیاتی کشور آسیب برساند؟ خوشبختانه بسیاری از روش‌های دفاعی در مقابل طیفی از حملات، کارساز می‌باشند و نیازی به تعیین قلمرو برای اقدام دفاعی متناسب با آن نیست.

شکل ۲ انواع حملات و سوء استفاده‌ها را در بین ۵۲۰ سازمان یا شرکتی که توسط FBI در سال ۱۹۹۸ بررسی شده‌اند نشان می‌دهد. انواع حملات و سوء استفاده‌ها به ترتیب از بالا به پائین عبارتند از:

۱ ـ ویروس

۲ ـ سوء استفاده از شبکه توسط کارکنان سازمان

۳ ـ سرقت Laptop

۴ ـ دسترسی غیرمجاز توسط کارکنان داخل سازمان

۵ ـ نفوذ غیرمجاز به سیستم

۶ ـ سرقت اسرار تجاری

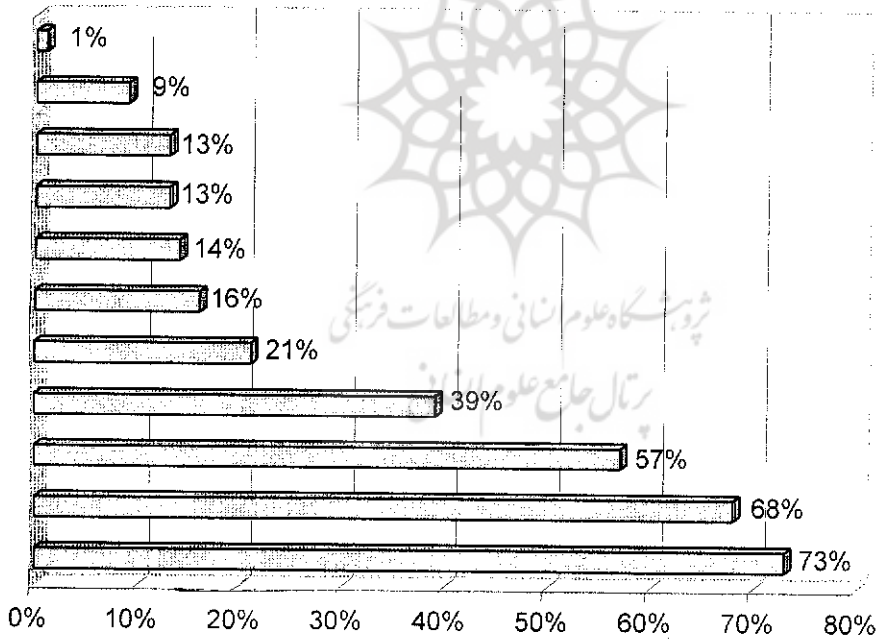
۷ ـ کلاهبرداری مخابراتی

۸ ـ کلاهبرداری مالی

۹ ـ خرابکاری

۱۰ ـ دسترسی غیرمجاز به سیگنال (غیرفعال)

۱۱ ـ دسترسی غیرمجاز به سیگنال (فعال)



شکل ۲ ـ انواع حملات و سوء استفاده‌های بررسی شده توسط FBI در سال ۱۹۹۸ از ۵۲۰ سازمان

هدف نهایی

اصولاً هدف نهایی رویارویی، روند تصمیم‌گیری‌های رقیب و دشمن[۳۹] است. در تعریف گستردهٔ مشترک از رویارویی اطلاعاتی، اهداف واقعی حملات جنگ اطلاعاتی صرفاً بر روی سیستم‌های تهاجمی دشمن نمی‌باشد، بلکه بر روی روندهای تصمیم‌گیری دشمن نیز طراحی می‌شود. به همین دلیل باید گفت طراحی حملات جنگ اطلاعاتی براساس مشخصات سیستم‌های تهاجمی نیست، بلکه بر پایهٔ تأثیرگذاری در سطوح بالای فرماندهی است. مثلاً در یک عملیات جنگ الکترونیکی، حملات مختل کننده، علیه حساس‌گرها براساس دانستن مشخصات تکنیکی و عملیاتی حساس‌گرها می‌باشد، در حالی که در جریان حملهٔ جنگ اطلاعاتی، طراحی و هدایت آن علیه اطلاعاتی که حساس‌گرها از وضعیت منطقه برای نیروهای مهاجم و عملیات بدست می‌آورند، مدنظر می‌باشد.

جنایتکاران و گروه‌های جنایی[۴۰]

گروه‌ها و افرادی که از شبکهٔ اینترنت برای مقاصد مجرمانه خود استفاده می‌کنند نیز فرصت‌های جدیدی بدست آورده‌اند. این افراد به دلایل متعددی تمایل به استفاده از زیرساخت‌های فناوری اطلاعات در جهت مقاصد خود دارند. برخی از این دلایل عبارتند از:

- جهانی سازی بازارهای جهانی قلمرو این افراد را گسترش داده است. در گذشته فعالیت این افراد در مناطق جغرافیایی محدود انجام می‌گرفت؛ در حالیکه امروز فرصت کار گروه‌های مختلف جنایی در سرتاسر دنیا به وجود آمده است. برای مثال هم‌اکنون سازمان‌های جنایی روسی از طریق اینترنت با تریادز[۴۱] در چین و یاکوزا[۴۲] در ژاپن همکاری می‌کنند.[۴۳]
- افزایش دسترسی مستقیم به دارایی‌های تجاری فرصت گرانبهایی را برای این افراد ایجاد کرده است.
- خود اینترنت نیز زمینه‌های جدید بسیاری برای مجرمین فراهم کرده است. حتی بسیاری از فعالیت‌های مجرمانه که در شرایط فیزیکی قابل انجام نبوده در محیط اینترنت وضعیت جدیدی پیدا کرده است.

● ردیابی دشوار مهاجمین اینترنت نیز به عنوان یک دلیل دیگر مطرح است.

استفاده از پایگاه‌های ناشناس[۴۴]، شناسه‌های کاربری رایگان و یا نفوذ به کامپیوترهای دیگران، پیچیدگی ردیابی را افزایش می‌دهد.

نکته‌ای که در اینجا لازم است ذکر شود تفاوت نفوذگری و جرم در فضای سایبر می‌باشد. نفوذگر کسی است که به یک سیستم کامپیوتری وارد شده و اطلاعاتی را تغییر می‌دهد و یا اسم خودش را درج می‌کند. در حالیکه مجرم سعی می‌کند شماره حساب و کارت اعتباری و اطلاعات مشابه را سرقت نماید.

جنایات و جرائم سازمان‌یافته بعنوان تهدید ملی و فراملی

ـ تعاریف و مفاهیم

«جنایات سازمان یافته به آن دسته از اعمال مجرمانه‌ای اطلاق می‌شود که گروه‌های جنایتکار با اعمال نفوذ در ارکان حکومت، از راه ارتشاء یا خشونت و قتل، معمولاً با سازماندهی خاصی و به قصد تحصیل منافع مالی یا مادی مرتکب می‌شوند.»[۴۵] این گروه‌های جنایتکار گاه تشکیلات وسیع و بودجهٔ بسیار کلانی دارند که از بودجهٔ سالانهٔ بسیاری از دولت‌ها نیز بیشتر است. امروزه، این گروه‌ها دامنهٔ فعالیت خود را گسترش داده و برای تحصیل منافع بیشتر، در کشورهای مختلف فعالیت می‌کنند و از خلأهای موجود در سطح بین‌المللی بهره می‌برند. جامعهٔ بین‌المللی این امر و همچنین ضرورت همکاری دولت‌ها را در این زمینه متوجه شده و کنوانسیون ملل متحد علیه جنایات سازمان‌یافتهٔ فراملی را تهیه و در تاریخ ۱۵ نوامبر ۲۰۰۰، طی قطع‌نامه ۵۵/۲۵ در اجلاس پنجاه و پنجم به تصویب مجمع عمومی رسید که در دسامبر ۲۰۰۰ در پالرمو، ۱۲۳ دولت (از جمله ایران) و تا اوایل سال ۲۰۰۲ بیش از ۱۴۰ دولت آن را امضا کرده‌اند معهذا تاکنون تنها، شش دولت آن را تصویب نموده‌اند و هنوز تا اجرا شدن فاصله زیادی دارد.

این جنایات حاکمیت دولت‌ها را زیر سؤال برده و بر امنیت سیاسی، اقتصادی و فرهنگی ـ انسانی آثار مخربی دارند. شناخت این آثار و نتایج آن می‌تواند هم در داخل، ضرورت و شکل مبارزه با این جنایات را روشن نماید و هم در تصمیم‌گیری راجع به تصویب یا عدم تصویب کنوانسیون یاد شده مؤثر باشد.

در متن کنوانسیون پالرمو، ضرورت جرم‌انگاری و قابل تعقیب و مجازات تلقی شدن این عناوین تصریح شده است:

۱ ـ ارتکاب شدید؛ ۲ ـ مشارکت در یک گروه جنایتکارانهٔ سازمان یافته؛ ۳ ـ تطهیر (شستشوی) منافع حاصل از ارتکاب جنایت؛ ۴ ـ فساد مالی یا ارتشاء؛ ۵ ـ ممانعت (ایجاد مانع) از اجرای عدالت.

همچنین هر یک از سه پروتکل الحاقی به کنوانسیون نیز، که تصویب آنها برای متعاهدین کنوانسیون اختیاری است، عنوانی جزایی را تعریف و شرایط و تدابیر مبارزه با آن را بیان کرده‌اند. این سه پروتکل عبارتند از: ۱ ـ پروتکل پیشگیری، سرکوب و مجازات قاچاق اشخاص، بویژه زنان و کودکان؛ ۲ ـ پروتکل علیه قاچاق مهاجران از راه زمینی، دریایی و هوایی؛ ۳ ـ پروتکل علیه تولید و قاچاق غیرقانونی سلاح‌های گرم، قطعات و اجزاء آنها و مهمات مربوطه.

به هر حال نام نبردن از سایر مصادیق در این اسناد به منزله جرم نبودن و حتی کم اهمیت بودن آنها نیست، بلکه به آن علت است که پیش از این، دربارهٔ برخی موارد (مثل قاچاق موادمخدر) اسنادی تنظیم شده و دربارهٔ برخی دیگر نیز یافتن اتفاق‌نظر بین دولت‌ها مشکل بوده است.

کنوانسیون پالرمو جنایت سازمان‌یافتهٔ فراملی را تعریف نکرده، اما ماده ۵ این کنوانسیون به تعریفی تحت عنوان «جرم‌انگاری مشارکت در یک گروه جنایتکارانهٔ سازمان‌یافته» پرداخته که علت آن را باید در ارتباط تامّ جنایت سازمان‌یافتهٔ فراملی و گروه جنایتکارانهٔ سازمان‌یافته که لازم و ملزوم یکدیگرند جستجو کرد.

ماده ۵ کنواسیون پالرمو:

۱ ـ هر دولت متعاهدی سایر اقدامات ضروری را اتخاذ خواهد کرد تا اعمال زیر را در صورتی که بطور عمدی ارتکاب یابند، جرم تلقی کند. این اعمال عبارتند از:

الف ـ هر یک از جرائم جنایی زیر یا هر دوی آنها، صرف‌نظر از اینکه فعالیت جنایتکارانه را شروع کرده یا اینکه آن را به پایان رسانیده باشد (جرم تامّ).

ـ جرمی که توافق با یک یا چند شخص دربارهٔ ارتکاب جنایت شدیدی که بطور مستقیم یا غیرمستقیم برای تحصیل یک نفع مالی یا نفع مادی دیگری ارتکاب یابد و در

صورتی که حقوق داخلی چنین اقتضا کند، یا متضمن عملی است که یکی از شرکا در انجام توافق بر عهده گرفته یا متضمن عمل یک گروه جنایتکارانهٔ سازمان‌یافته است.

ـ رفتار کسی که خواه با علم به هدف و فعالیت جنایتکارانهٔ عمومی یک گروه جنایتکارانهٔ سازمان‌یافته و خواه با علم بر قصد ارتکاب در جنایات مزبور در موارد زیر شرکت فعال کند:

ـ فعالیت‌های جنایتکارانهٔ گروه جنایتکارانهٔ سازمان‌یافته.

ـ فعالیت‌های دیگر گروه جنایتکارانهٔ سازمان‌یافته با علم بر اینکه مشارکت وی در دستیابی به هدف جنایتکارانهٔ مزبور مؤثر است.

ب ـ سازماندهی، هدایت، کمک، مساعدت، تسهیل یا مشاوره دادن در ارتکاب جنایت شدیدی که متضمن یک گروه جنایتکار سازمان‌یافته باشد.

۲ ـ علم، قصد، هدف، مقصود یا توافق مورد اشاره در بند ۱ این ماده را می‌توان از اوضاع و احوال موضوعی استنباط کرد.

۳ ـ دول متعاهدی که حقوق داخلی آنها برای تحقق جرائم مندرج در بند ۱ قسمت الف این ماده وجود یک گروه جنایتکار سازمان‌یافته را لازم می‌دانند تضمین خواهند کرد که حقوق داخلی آنها تمام جنایات متضمن گروه‌های جنایتکار سازمان‌یافته را شامل شود. چنین دولت‌هایی و دولت‌های متعاهدی که حقوق داخلی آنها وجود عملی را برای تحقق توافق انجام شده در راستای ارتکاب جرائم مندرج در بند مزبور لازم می‌دانند، چنین امری را به موقع امضا خواهند کرد و یا تودیع سند، تصویب، پذیرش، تصدیق و یا الحاق به این کنوانسیون را به دبیرکل سازمان ملل متحد اطلاع خواهند داد.

نخستین مطلبی که با مطالعهٔ نام ماده و صدر آن جلب توجه می‌کند این است که این ماده مانند سایر مواد این کنوانسیون و پروتکل‌های الحاقی و اسناد مشابه بین‌المللی دیگر رأساً عنوان مجرمانه‌ای ایجاد نمی‌کند بلکه دولت‌های متعاهد را ملزم می‌نماید تا قوانین و سایر اقدامات مقتضی را تصویب کنند. با مراجعه به کارهای مقدماتی این معاهده و مذاکرات مربوطه متوجه می‌شویم که منظور از سایر اقدامات مندرج در مواد ۵، ۶ و ۲۳ این کنوانسیون اقداماتی افزون بر اقدامات قانون‌گذاری، مسبوق بر آن و در راستای تکمیل آن هستند.

ارتکاب جنایت سازمان‌یافتهٔ فراملی را به دلیل ماهیتش، شرکای جرم مرتکب

می‌شوند نه مباشر. منظور از مباشر کسی است که به تنهایی و بطور مستقل رکن مادی را مرتکب می‌شود و منظور از شرکای جرم دو یا چند نفر از افراد هستند که بطور مشترک و با همکاری یکدیگر رکن مادی جرم را انجام می‌دهند. این معنی را در حقوق داخلی ایران با مطالعهٔ ماده ۴۲ قانون مجازات اسلامی (مصوب ۱۳۷۰) می‌توان دریافت.

با توجه به تعریف و مصادیق ارائه شده در این ماده، بنظر می‌رسد که رکن مادی جنایت سازمان‌یافته همیشه به صورت انجام فعل (عمل مثبت) است و با ترک فعل (عمل منفی) محقق نمی‌شود. به عبارت دیگر کسی به اتهام مشارکت در ارتکاب این جنایت مسؤلیت کیفری دارد که عملی انجام داده باشد و طبق این ماده، صرف انجام ندادن کاری (مثلاً عدم اعلام به مقامات و...) جرم محسوب نمی‌شود.

ـ آثار جنایت سازمان‌یافتهٔ فراملی

جنایت سازمان‌یافته فراملی در ابعاد گوناگون آثار مختلفی از خود بر جای می‌گذارد. از طرفی ساختار سیاسی حکومت و بطور کلی حاکمیت، دموکراسی و حتی 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 در خور توجهی از خود بر جای می‌گذارد. صحبت از ابعاد مختلف سیاسی اجتماعی، اقتصادی و فرهنگی و... این آثار مجال بیشتری را طلب می‌نماید.

نتیجه

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[۴۶]، دفتر یادداشت

تحلیلگران و هارلکونیز دکتر واتسون [۴۷] قابلیت‌هایی را برای موارد ذیل فراهم می‌کنند: 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 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 به منابع کمتری جرائم فراوانی را انجام دهند که در نتیجهٔ آن درآمد زیادی نیز بدست اورند 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 و 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 می‌دهند. 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 در خود)، رویارویی با حکومت و اعمال فشار بر حکومت. چنین دورنمایی وسیله‌ای برای جنجال‌آفرین بودن نیست کمااینکه نمی‌تواند ما را از هشیار شدن مأیوس کند.»[۴۸]

تروریست‌ها و گروه‌های افراطی

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

۱ ـ این اتفاق در عصر رسانه‌ای شدن جوامع، یک اجماع جهانی را در مورد مقابله با 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.

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

۵ ـ اتفاقات آمریکا نشان داد به دلیل مبهم بودن فاعل و مصدر تهدید، واکنش نشان دادن به آن دشوار می‌باشد.

از جمله گروه‌های تروریستی نوین تهدیدکنندگان امنیت ملی کشورها در فضای سایبر هستند. این گروه‌ها به زیر ساخت‌های فناوری اطلاعات با هدف دستیابی به مقاصد خود حمله می‌کنند. گسترش تعداد این گروه‌ها و بهره‌برداری 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 وامی‌دارد شرایط جدیدی است که به علت گستردگی حوزهٔ عملیات، نیاز به زمان حداقل، امکان هماهنگی حداکثر، ارزان بودن و کم خطر بودن استفاده از این شرایط به وجود آمده است. 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 زیر ساخت‌های 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 موردنظر 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 پست‌الکترونیکی 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 موردنظر ارسال نمودند.[۴۹]

ب ـ ایجاد ترافیک (Sit _ in)

همانگونه که از اسم این روش پیدا است تروریست با ارسال تعداد زیادی پیغام درخواست خدمات، دستگاه خدمات دهنده را به خود مشغول داشته و مانع ارائهٔ 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.[۵۰]

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 زیرساخت IT نبوده معهذا زیرساخت IT نیز آسیب دیده است.[۵۱]

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[۵۲]. 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.

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 بررسی‌از ۱۶۴ هکر نشان داد که:

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

۲۴ 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. [۵۲]

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 ۱۶، 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 سایتهای معروف آمازون، یاهو، ebay،CNN 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 [۵۴]، کاربران پیشرفته [۵۵] و تولیدکنندگان [۵۶] 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، برنامه‌نویسان 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 واز 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.

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 [۵۷]. 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 ۶ گروه با انگیزه‌های مختلف تقسیم می‌شوند [۵۸].

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 محافظت 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.

برآیند:

به نظر می‌رسد با عنایت به اهمیت شبکه جهانی اطلاع‌رسانی به عنوان یک پدیده‌ی غیرقابل انکار عصر فرامدرن که واجد فرصت‌های بسیار و حامل تهدیدهای جدّی است. طراحی استراتژی نظام جمهوری‌اسلامی ایران در ارتباط با فن‌آوری اطلاعات و بهره‌مندی از فرصت‌ها و تحدید تهدیدها به موازات تقویت نقاط قوت و تدبیر در ترمیم نقاط ضعف در این حوزه از اهمیتی ویژه برای امنیت ملّی جمهوری اسلامی ایران برخوردار است.

پی‌نوشت‌ها:

1. Whole Saling
2. Retailing.
3. Business User.
4. Home Users.
5. End User.
6. Frame Relay.
7. Voip: Voice over Internet Protocot.

۸. ماهنامه پیام ارتباط، نشر نظر، مشاره ۲۳، بهمن و اسفند ۱۳۸۰

۹- ماهنامه پیام ارتباط، نشر نظر، شماره ۲۳، بهمن و اسفند ۱۳۸۰

۱۰- ماهنامه پیام ارتباط، شماره ۲۴، فروردین و اردیبهشت ۱۳۸۱.

۱۱- هفته‌نامه عصر ارتباط، دوشنبه ۲۶ اسفندماه ۱۳۸۱.

12. Lawrence Livermore Labs

13. Worm

۱۴- درویشی سه تلانی، فرهاد، تأملی نظری بر امنیت ملی، تهران: معاونت تحقیق و پژوهش دانشکده فرماندهی و ستاد سپاه پاسداران انقلاب اسلامی، ۱۳۷۶، صص ۴۱ ـ ۴۰.

15. Objective / Subjective.

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

17. Terriff, Terry , op. cit, pp 115 _ 116.

18. Didds , Klaus, Geopolitics in a Changing World , (London: Prentice Hall, 2000) , pp 92 _ 107.

19. Terriff, Terry, Op.cit. pp 115 _ 134.

۲۰. گیدنز، آنتونی، پیامدهای مدرنیت، ترجمهٔ محسن ثلاثی، تهران: نشر مرکز، ۱۳۸۰.

21. Motivation

22. Capability

23. Organization

24. Tool

25. IO: Information

26. U. S. joint Chiefs Of Staff, joint Doctrine for Information Operations, joint pub 3 _ 13 , October9, 1998.

27. IW: Information War.

۲۸. در ادامهٔ این بخش به تفصیل به تشریح جنگ اطلاعات خواهیم پرداخت.

29. John A. Serabian, Jr, Information Poerations Issue Manager, Centeral Intelligence Agency, Tatement For the Record Before the joint Economic on Cyber Threats and U. S Economy, February 23 , 2000.

30. U.S. Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Pub 3 _ 13 , October 9, 1998.

31. Damon Bristow, Information Warfare Grips China , Janes Intelligence Review, November 1 , 1998.

32. Hacking

33. Information System Layer

34. Technical Effect

35. Information Management Layer

36. Functional Effect

37. Decidion _ Process Layer

38. Operational Effect

39. Adversary's Decision Process

۴۰. با توجه به اهمیت جرائم و جنایات سازمان‌یافته در ادامهٔ این بند به تشریح اینگونه جرائم و جنایات می‌پردازیم.

41. Teryads

42. Yahoza

43. Galeotti, Mark, Inside the Russian Mafiya , Janes Intelligence Review, March 2000, p. 8.

44. Anonymous remailers

۴۵. نشریهٔ نگاه، سال سوم شماره ۲۳، تهران: مؤسسهٔ مطالعات سیاسی فرهنگی اندیشه ناب، خرداد ۱۳۸۱، ص ۵۵.

46. Leads Orions.

47. Harlequins Dr. Watson.

۴۸. پیکارتی، جان تی و ویلیامین، فیل، گزیده‌های عصر اطلاعات: الزامات امنیت ملی در عصر اطلاعات، سی‌سی‌آرپی، آگوست ۲۰۰۰، ص ۳۷.

49. Michael Vatis, Seminar on Cyber _ Terrorism and Information Warfare: Threats and Responses, Proceedings Report, Potomac Institute for Policy Studies, April 16 , 1998.

50. Dorothy E. Denning, Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, Nautilus Institute, 1999.

51. Caleb Pringle, Terrotist Organizations' Use of Information Age Capabilities, Defense and Foreign Affairs Strategic Policy, January 1999.

52. John Schwartz, No Love for Computer Bugs Washington Post, July 5 . 2000. http://www. Washingtonpost.com/cgi_...ni/print&articled=a47/155_2000jul4

53. Dorothy E. Denning, Information Warfare and Security, Addison _ Wesley, 1999. p. 47.

54. Script Kiddies

55. Advanced users

56. Developers

57. DoD Insider Threat Mitigation, Final Report of the Insider Threat Integrated Process Team, April 26, 2000

58. The Insider Threat to Information Systems : A Framework for Understanding and Managing the Insider Threat in Today's Business Environment, Government and National Security Telecommunications Advisory Committee (NSTAC) Network Security Information Exchanges (NSIE), 1998, p. 6 _ 9