نگاهی به چالش ها و راهکارها در امنیت شبکه

● الهه حسین زاده،
بابک زاهدی، مهدی صالحی،
بهروز وفا داری

اینترنت یک شبکهٔ عظیم اطلاع رسانی و یک بانک وسیع اطلاعاتی است که در آینده نزدیک دسترسی به آن برای تک‌تک افراد ممکن خواهد شد. کارشناسان ارتباطات، بهره‌گیری از این شبکه ارتباطی را یک ضرورت در عصر اطلاعات می دانند.

این شبکه که از هزاران شبکه کوچک‌تر تشکیل شده، فارغ از مرزهای جغرافیایی، سراسر جهان را به هم مرتبط ساخته است. طبق آخرین آمار، بیش از شصت میلیون رایانه از تمام نقاط جهان در این شبکهٔ گسترده به یکدیگر متصل شده‌اند که اطلاعات بی‌شماری را با موضوعات مختلف به اشتراک گذارند، گفته می‌شود نزدیک به یک میلیارد صفحه اطلاعات از سوی افراد حقیقی و حقوقی روی این شبکه قرار داده شده است.

این اطلاعات با سرعت بسیار زیاد در بزرگراه های اطلاعاتی بین کاربران رد و بدل می‌شود و تقریباً هیچ گونه محدودیت و کنترلی بر وارد کردن یا دریافت کردن داده‌ها اعمال نمی‌شود.

حمایت از جریان آزاد اطلاعات، گسترش روزافزون فن‌آوری اطلاعات و بسترسازی برای اتصال به شبکه‌های اطلاع رسانی شعار دولت‌هاست. این در حالی است که گستردگی و تنوع اطلاعات آلوده روی اینترنت، موجب بروز نگرانی در بین کشورهای مختلف شده است. انتشار تصاویر مستهجن، ایجاد پایگاه‌هایی با مضامین پورنوگرافی و سایت‌های سوءاستفاده از کودکان و انواع قاچاق در کشورهای پیشرفته صنعتی به‌خصوص در خاستگاه این شبکهٔ جهانی یعنی آمریکا، کارشناسان اجتماعی را به شدت نگران کرده، به گونه‌ای که هیأت حاکمه را مجبور به تصویب قوانینی مبنی بر کنترل این شبکه در سطح آمریکا کرده است. هشدار، جریمه و بازداشت برای برپاکنندگان پایگاه‌های مخرب و فسادانگیز تدابیری است که کشورهای مختلف جهان برای مقابله با آثار سوء اینترنت اتخاذ کرده‌اند.

ترس و بیم از تخریب مبانی اخلاقی و اجتماعی، ناشی از هجوم اطلاعات آلوده و مخرب از طریق اینترنت، واکنشی منطقی است، زیرا هر جامعه‌ای چارچوب‌های اطلاعاتی خاص خود را دارد و طبیعی است که هر نوع اطلاعاتی که این حد و مرزها را بشکند می‌تواند سلامت و امنیت جامعه را به خطر اندازد. علی‌رغم وجود جنبه‌های مثبت شبکه‌های جهانی، سوء استفاده از این شبکه‌های رایانه‌ای توسط افراد بزهکار، امنیت ملی را در کشورهای مختلف با خطر روبه روساخته است. از این رو به‌کارگیری فیلترها و فایروال‌های مختلف برای پیشگیری از نفوذ داده‌های مخرب و مضر و گزینش اطلاعات سالم در این شبکه‌ها رو به افزایش است. خوشبختانه با وجود هیاهوی بسیاری که شبکهٔ اینترنت را غیرقابل کنترل معرفی می‌کند، فناوری لازم برای کنترل این شبکه و انتخاب اطلاعات سالم روبه گسترش و تکامل است.

امنیت شبکه‌های اطلاعاتی و ارتباطی

امروزه امنیت شبکه‌های اطلاعاتی و ارتباطی با نفوذ به اطلاعات، دستخوش اختلال شده است ودیگر کاربران نمی‌توانند از مزیت‌های بی‌شمار آن بهره برند. مزیت های پول و تجارت الکترونیک، خدمات به کاربران خاص، اطلاعات شخصی، اطلاعات عمومی و نشریات الکترونیک همه و همه در معرض دستکاری و سوءاستفاده‌های مادی و معنوی قرار گرفته است. هم‌چنین دستکاری اطلاعات، به‌عنوان زیربنای فکری ملت‌ها توسط گروه‌های سازماندهی شده بین‌المللی، به نوعی مختل ساختن امنیت ملی و تهاجم علیه دولت‌ها و تهدیدی ملی محسوب می‌شود.

برای کشور ما که بسیاری از نرم‌افزارهای پایه از قبیل سیستم عامل و نرم‌افزارهای کاربردی و اینترنتی، از طریق واسطه‌ها و شرکتهای خارجی تهیه می‌شود، بیم نفوذ از طریق راه های مخفی وجود دارد. در آینده که بسیاری از بانک‌ها و نهادها و دستگاه‌های دیگر از طریق شبکه به فعالیت می‌پردازند، جلوگیری از نفوذ عوامل

مخرب به شبکه به‌صورت مسأله‌ای استراتژیک درخواهد آمد که نپرداختن به آن باعث واردشدن خساراتی خواهد شد که بعضاً جبران‌ناپذیر است. چنانچه یک پیغام خاص، مثلاً از طرف شرکت مایکروسافت، به‌کلیه‌سایت‌های ایرانی ارسال‌شود وسیستم عامل‌ها در واکنش به این پیغام سیستم‌ها را خراب کنند و از کار بیندازند، ضررهای هنگفتی به امنیت و اقتصاد مملکت وارد خواهدشد.

با توجه به اینکه شعبه اصلی شرکت چک پوینت بزرگ‌ترین شرکت تولید نرم‌افزارهای امنیت شبکه، در اسرائیل است. امنیت شبکه‌برای‌کشورها، به‌صورت مسأله‌ای استراتژیک‌نمودپیدامی‌کند. کشور ما نیز برای درامان ماندن از نفوذ اطلاعات باید به آخرین تکنولوژی‌های امنیت شبکه مجهز شود، از آنجایی که این تکنولوژی‌ها به صورت محصولات نرم‌افزاری قابل خریداری نیستند، محققان کشور می‌باید در زمینه این مسأله مهم فعالیت کنند.

سهولت‌دسترسی‌به‌اینترنت‌آن‌رادرمعرض‌خطراتی‌چون‌گم‌شدن اطلاعات، ربوده‌شدن، مخدوش‌شدن یا سوءاستفاده از اطلاعات موجود درآن قرار می‌دهد. اگر اطلاعات روی کاغذ چاپ شده بود و در قفسه‌ای از اتاق‌های محفوظ اداره مربوطه نگهداری می‌شد، برای دسترسی به آنها افراد غیرمجاز می‌بایست از حصارهای مختلف عبور می‌کردند، اما اکنون چند اشاره به کلیدهای رایانه‌ای برای این منظورکافی است.

اینترنت در سال ۱۹۶۹ به‌صورت شبکه‌هایی به‌نام آرپانت که مربوط به وزارت دفاع آمریکا بود راه‌اندازی شد. هدف این بودکه با استفاده‌ازرایانه‌های متصل به‌هم، شرایطی ایجادشودکه حتی اگر، بخش‌های عمده‌ای از سیستم اطلاعاتی به هر دلیلی از کار بیفتد، کل‌شبکه بتواند به‌کار خود ادامه دهد، تا این اطلاعات حفظ شود. از همان ابتدا، فکر ایجاد شبکه، برای جلوگیری از اثرات مخرب حملات اطلاعاتی بود.

درسال ۱۹۷۱ تعدادی از رایانه‌های دانشگاه‌ها و مراکز دولتی به این شبکه متصل شدند و محققان از این طریق شروع به تبادل اطلاعات کردند.

با بروز رخدادهای غیرمنتظره در اطلاعات، توجه به مسأله امنیت بیش از پیش اوج گرفت. درسال ۱۹۸۸، آرپانت برای اولین بار با یک حادثه امنیتی سراسری درشبکه، مواجه‌شدکه بعداً، «کرم موریس» نام گرفت. رابرت موریس که یک دانشجو در نیویورک بود، برنامه‌هایی نوشت که می‌توانست به یک رایانه‌ای دیگر راه یابد و در

آن تکثیر شود و به همین ترتیب به رایانه‌های دیگر هم نفوذ کند و به صورت هندسی تکثیر شود. آن زمان ۸۸۰۰۰ رایانه به این شبکه وصل بود. این برنامه سبب شد طی مدت کوتاهی ده درصد از رایانه‌های متصل به شبکه در آمریکا از کار بیفتد.

به دنبال این حادثه، بنیاد مقابله با حوادث امنیتی (IRST) شکل گرفت که در هماهنگی فعالیت‌های مقابله با حملات ضد امنیتی، آموزش و تجهیز شبکه‌ها و روش‌های پیشگیرانه نقش مؤثری داشت. با رایج‌تر شدن و استفاده عام از اینترنت، مسأله امنیت خود را بهتر و بیشتر نشان داد. از جمله این حوادث، اختلال در امنیت شبکه، WINK/OILS WORM در سال ۱۹۸۹، Sniff packet در سال ۱۹۹۴ بود که مورد اخیر از طریق پست الکترونیک منتشر می‌شد و باعث افشای اطلاعات مربوط به اسامی شماره رمز کاربران می‌شد. از آن زمان حملات امنیتی ــ اطلاعاتی به شبکه‌ها و شبکه جهانی روزبه‌روز افزایش یافته است.

گرچه اینترنت در ابتدا، با هدف آموزشی و تحقیقاتی گسترش یافت، امروزه کاربردهای تجاری، پزشکی، ارتباطی و شخصی فراوانی پیدا کرده است که ضرورت افزایش ضریب اطمینان آن را بیش از پیش آشکار می‌کند.

جرائم رایانه‌ای و اینترنتی

ویژگی برجسته فناوری اطلاعات، تأثیری است که بر تکامل فناوری ارتباطات راه دور گذاشته و خواهد گذاشت. ارتباطات کلاسیک همچون انتقال صدای انسان، جای خود را، به مقادیر وسیعی از داده‌ها، صوت، متن، موزیک، تصاویر ثابت و متحرک داده است. این تبادل و تکامل نه تنها بین انسان‌ها بلکه مابین انسان‌ها و رایانه‌ها، و هم‌چنین بین خود رایانه‌ها نیز وجود دارد. استفاده وسیع از پست الکترونیک، و دستیابی به اطلاعات از طریق وب‌سایت‌های متعدد در اینترنت نمونه‌هایی از این پیشرفت‌ها است که جامعه را به طور پیچیده‌ای دگرگون ساخته‌اند.

سهولت در دسترسی و جست‌وجوی اطلاعات موجود در سیستم‌های رایانه‌ای توأم با امکانات عملی نامحدود در مبادله و توزیع اطلاعات، بدون توجه به فواصل جغرافیایی، منجر به رشد سرسام‌آور مقدار اطلاعات موجود در آگاهی که می‌توان از آن به دست آورد، شده است.

این اطلاعات موجب افزایش تغییرات اجتماعی و اقتصادی

پیش‌بینی نشده گردیده است، اما پیشرفت‌های مذکور جنبهٔ خطرناکی نیز دارد که پیدایش انواع جرایم و هم‌چنین بهره‌برداری از فناوری جدید در ارتکاب جرایم بخشی از آن به‌شمار می‌رود. به علاوه عواقب و پیامدهای رفتار مجرمانه می‌تواند خیلی بیشتر از قبل و دور از تصور باشد چون که محدودیت‌های جغرافیایی یا مرزهای ملی آن را محدود نمی‌کنند حتی فناوری جدید مفاهیم قانونی موجود را نیز دچار چالش‌هایی ساخته است زیرا جنایتکاران غالباً در مکان‌هایی به غیر از جاه‌هایی که آثار و نتایج اعمال آنها ظاهر می‌شود، قرار دارند.

سوءاستفاده گسترده مجرمان، به ویژه گروه‌های جنایتکار سازمان نیافته از فناوری اطلاعات سبب شده است که سیاست‌گذاران جنایی اغلب کشورهای جهان با استفاده از ابزارهای سیاست جنایی درصدد مقابله با آنها برآیند. تصویب کنوانسیون جرایم رایانه‌ای در اواخر سال ۲۰۰۱ و امضای آن توسط ۳۰ کشور پیشرفته، تصویب قوانین مبارزه با این جرایم توسط قانون‌گذاران داخلی و تشکیل واحدهای مبارزه با آن در سازمان پلیس بیشتر کشورهای پیشرفته و تجهیز آنها به جدیدترین سخت‌افزارها و نرم‌افزارهای کشف این گونه جرایم و جذب و به‌کارگیری بهترین متخصصان در واحدهای مذکور، بخشی از اقدامات مقابله‌ای را تشکیل می‌دهد.

در مورد زمان دقیق پیدایش جرم رایانه‌ای نمی‌توان اظهارنظر قطعی کرد زیرا این جرم زائیده تکنولوژی اطلاعاتی و انفورماتیکی است، و به طور طبیعی و منظم بعد از گذشت مدت کوتاهی از شیوع و کاربرد تکنولوژی اطلاعات، باب سوءاستفاده نیز قابل طرح است. شیوع استعمال این تکنولوژی و برابری کاربران آن حداقل در چند کشور مطرح جهان به صورت گسترده، امکان بررسی اولین مورد را دشوار می‌کند.

برای اولین بار آلدون رویس حسابدار یک شرکت آمریکایی باعث شد تا اذهان عمومی متوجه سوء استفاده های رایانه ای شود. چون به گمان وی، شرکت حق او را پایمال کرده بود، بنابراین با تهیه برنامه ای، قسمتی از پول های شرکت را اختلاس کرد. انگیزهٔ رویس در این کار انتقام گیری بود.

مکانیزم کار بدین گونه بود که شرکت محل کار وی یک عمده فروش میوه و سبزی بود. محصولات متنوعی را از کشاورزان می خرید و با استفاده از تجهیزات خود از قبیل کامیون ها، انبار و بسته بندی و سرویس دهی به گروه های فروشندگان، آنها را عرضه می کرد. به دلیل وضعیت خاص این شغل، قیمت ها در نوسان بود و ارزیابی امور تنها می توانست از عهدهٔ رایانه برآید تا کنترل محاسبات این شرکت عظیم را عهده دار شود.

کلیه امور حسابرسی و ممیزی اسناد و مدارک و صورت حساب ها به صورت اطلاعات مضبوط در نوارهای الکترونیکی بود.

رویس در برنامه ها، دستورالعمل های اضافی را گنجانده بود و قیمت کالا ها را با ظرافت خاصی تغییر می داد. با تنظیم درآمد اجناس، وی مبلغی را کاهش می داد و مبالغ حاصله را به حساب های مخصوص واریز می کرد. بعد در زمان های خاص، چکی به نام یکی از هفده شرکت جعلی و ساختگی خود صادر و مقداری از مبالغ را برداشت می کرد. بدین ترتیب وی توانست در مدت ۶ سال بیش از یک میلیون دلار برداشت کند. اما او نمی توانست مکانیسمی برای توقف عملکرد سیستم خود بیندیشد. بنابراین در نهایت خود را به مراجع قضایی معرفی و به جرم خود اعتراض کرد و به مدت ده سال به زندان محکوم شد. از این جا بود که مبحث جدیدی به نام جرم رایانه ای ایجاد شد.

تاکنون تعریف های گوناگونی از جرم رایانه ای از سوی سازمان ها، متخصصان و برخی قوانین ارائه شده، که وجود تفاوت در آنها بیانگر ابهامات موجود در ماهیت و تعریف این جرائم است.

جرم رایانه ای یا جرم در فضای مجازی (سایر جرایم) دارای دو معنی و مفهوم است. در تعریف مضیق، جرم رایانه ای صرفاً عبارت از جرایمی است که در فضای سایبر رخ می دهد. از این نظر جرایمی مثل هرزه نگاری، افترا، آزار و اذیت سوء استفاده از پست الکترونیک و سایر جرایمی که در آنها رایانه به عنوان ابزار و وسیله ارتکاب جرم به کار گرفته می شود، در زمرهٔ جرم رایانه ای قرار نمی گیرند.

در تعریف موسع از جرم رایانه ای هر فعل و ترک فعلی که در اینترنت یا از طریق آن یا با اینترنت یا از طریق اتصال به اینترنت، چه به طور مستقیم یا غیرمستقیم رخ می دهد و قانون آن را ممنوع کرده و برای آن مجازات در نظر گرفته شده است جرم رایانه ای نامیده می شود. براین اساس این گونه جرایم را می توان به سه دسته تقسیم کرد:

دسته اول: جرایمی هستند که در آنها رایانه و تجهیزات جانبی آن موضوع جرم واقع می شوند. مانند سرقت، تخریب و غیره.

دسته دوم: جرایمی هستند که در آنها رایانه به عنوان ابزار و وسیله توسط مجرم برای ارتکاب جرم به کار گرفته می شود.

دسته سوم: جرایمی هستند که می توان آنها را جرایم رایانه ای محض نامید. این نوع از جرایم کاملاً با جرایم کلاسیک تفاوت دارند و در دنیای مجازی به وقوع می پیوندند، اما آثار آنها در دنیای واقعی ظاهر می شود. مانند دسترسی غیرمجاز به سیستم های رایانه ای.

در سال ۱۹۸۳ «او.ای.سی.دی.بی» مطالعه امکان پذیری اعمال بین المللی و هماهنگی قوانین کیفری را به منظور حل مسأله جرم یا سوءاستفاده های رایانه ای متعهد شد. این سازمان در سال ۱۹۸۶ گزارشی تحت عنوان جرم رایانه ای، تحلیل سیاست های قانونی منتشر ساخت که به بررسی قوانین موجود و پیشنهادهای اصلاحی چند کشور عضو پرداخت و فهرست حداقل سوءاستفاده هایی را پیشنهاد کرده بود که کشورهای مختلف باید با استفاده از قوانین کیفری، مشمول ممنوعیت و مجازات قرار دهند. بدین گونه اولین تقسیم بندی از جرایم رایانه ای در سال ۱۹۸۳ ارائه شد و طی آن پنج دسته اعمال را مجرمانه تلقی کرد و پیشنهاد کرد در قوانین ماهوی ذکر شود.

این پنج دسته عبارت اند از:

الف- ورود، تغییر، پاک کردن و یا متوقف سازی داده های رایانه ای و برنامه های رایانه ای که به طور ارادی با قصد انتقال غیرقانونی وجوه یا هر چیز باارزش دیگر صورت گرفته باشد.

ب- ورود، تغییر، پاک کردن، و یا متوقف سازی داده های رایانه ای و برنامه های رایانه ای که به صورت عمدی و به قصد ارتکاب جعل صورت گرفته باشند، یا هرگونه مداخله دیگر در سیستم های رایانه ای که به صورت عمدی و با قصد جلوگیری از عملکرد سیستم رایانه ای و یا ارتباطات صورت گرفته باشد.

ج- ورود، تغییر، پاک کردن و متوقف سازی داده های رایانه ای و یا برنامه های رایانه ای.

د- تجاوز به حقوق انحصاری مالک یک برنامهٔ رایانه‌ای.
حفاظت شده با قصد بهره‌برداری تجاری از برنامه‌ها و ارائه آن به بازار.

هـ- دستیابی یا شنود در یک سیستم رایانه‌ای و یا ارتباطی که آگاهانه و بدون کسب مجوز از فرد مسئول سیستم مزبور یا تخطی از تدابیر امنیتی و چه با هدف غیر شرافتمندانه و یا موضوع صورت گرفته باشد.

طبقه‌بندی اینترپول

سال‌هاست که اینترپول در مبارزه با جرایم مرتبط با فناوری اطلاعات فعال است. این سازمان با بهره‌گیری از کارشناسان و متخصصان کشورهای عضو، اقدام به تشکیل گروه‌های کاری در این زمینه کرده است و رؤسای واحدهای مبارزه با جرایم رایانه‌ای کشورهای باتجربه عضو سازمان در این گروه کاری گردهم آمده‌اند.

گروه‌های کاری منطقه‌ای در اروپا، آسیا، آمریکا و آفریقا مشغول به کارند و زیر نظر کمیتهٔ راهبردی جرایم فناوری اطلاعات، مستقر در دبیرخانهٔ کل اینترپول فعالیت می‌کنند.

گروه کاری اروپایی اینترپول با حضور کارشناسان هلند، اسپانیا، بلژیک، فنلاند، فرانسه، آلمان، ایتالیا، سوئد و انگلیس در سال ۱۹۹۰ تشکیل شد. این گروه‌ها هر سال سه بار تشکیل جلسه می‌دهند و در ژانویه سال ۲۰۰۱ سی امین گردهمایی آن در دبیرخانه کل تشکیل شد.

تهیه کتابچهٔ راهنمای پی‌جویی جرایم رایانه‌ای، کتاب و سی‌دی راهنمای جرایم رایانه‌ای، تشکیل دوره‌های آموزشی برای نیروهای پلیس در طول ۵ سال گذشته، تشکیل سیستم اعلام خطر که مرکب از سیستم‌های پاسخگوی شبانه‌روزی، نقاط تماس دائمی شبانه‌روزی، تبادل پیام بین‌المللی در قالب فرم‌های استاندارد در زمینهٔ جرایم رایانه‌ای واقعه و انجام چندین پروژه تحقیقاتی پیرامون موضوعات مرتبط با جرایم رایانه‌ای از جمله اقدامات گروه کاری مذکور است. گروه کار آمریکایی نیز جرایم مرتبط با تکنولوژی اطلاعات، مرکب از کارشناسان و متخصصان کشورهای کانادا، ایالات متحده، آرژانتین، شیلی، کلمبیا، جامائیکا و باهاماست.

گروه کاری آفریقایی جرایم مرتبط با تکنولوژی اطلاعات، مرکب از کارشناسان آفریقای جنوبی، زیمبابوه، نامبیا، تانزانیا، اوگاندا، بوتسوانا، سوازیلند، زنگبار، لسوتو و رواندا در ژوئن سال ۱۹۹۸ تشکیل شد. آنها کارشان را با برگزاری یک دوره آموزشی آغاز

کردند و دومین دوره آموزشی آنها با مساعدت مالی سفارتخانه‌های انگلیس برگزار شد.

گروه کاری جنوب اقیانوس آرام، و آسیا در نوامبر سال ۲۰۰۰ در هند تشکیل شد و کارشناسانی از کشورهای استرالیا، چین، هنگ کنگ، هند، ژاپن، نپال، وسر یلانکا عضو آن هستند. این گروه کاری با الگو قرار دادن کمیته راهبردی جرایم مربوط به فناوری اطلاعات به منظور ایجاد و هماهنگی میان اقدامات گروه‌های کاری منطقه‌ای در محل دبیرخانه کل اینترپول تشکیل شده است.

کنوانسیون جرایم سایبرنتیک در اواخر سال ۲۰۰۱ به امضای ۳۰ کشور پیشرفته رسیده است و دارای وظایف زیر است:

هماهنگ کردن ارکان تشکیل دهنده جرم در حقوق جزای ماهوی داخلی کشورها و مسائل مربوطه در بخش جرایم سایبراسپیس.

الف- فراهم آوردن اختیارات لازم آیین دادرسی کیفری داخلی برای پی‌جویی و تعقیب چنین جرائمی علاوه بر جرایم دیگر که با استفاده از سیستم‌های رایانه‌ای ارتکاب می‌یابند.

ب- تدوین سیستم سریع و مؤثر همکاری بین‌المللی.

ج- کنوانسیون بین‌المللی جرایم رایانه‌ای بوداپست (۲۰۰۱) جرم را موارد زیر تعریف کرده است:

- نفوذ غیرمجاز به سیستم‌های رایانه‌ای
- شنود غیرمجاز اطلاعات و ارتباطات رایانه‌ای
- اخلال در داده‌های رایانه‌ای
- اخلال در سیستم‌های رایانه‌ای
- جعل رایانه‌ای

– کلاه‌برداری رایانه‌ای
– سوءاستفاده از ابزارهای رایانه‌ای
– هرزه‌نگاری کودکان
– تکثیر غیرمجاز نرم‌افزارهای رایانه‌ای و نقض حقوق ادبی و هنری

شش نشانه از خرابکاران شبکه‌ای

۱. در صورت نفوذ یک خرابکار به شبکهٔ شما ممکن است حساب بانکی‌تان تغییر کند.

۲. خرابکاران شبکه‌ای آن قدر تلاش می‌کنند تا بالاخره موفق به ورود به اینترانت شما شوند. لازم به ذکر است که در برخی موارد در صورتی که یک خرابکار بتواند به حساب بانکی شما نفوذ کند فایل آن به طور خودکار بسته نمی‌شود.

۳. گاهی اوقات خرابکاران برای نفوذ به یک رایانه ناچارند کد جدیدی به آن وارد کنند. برای این کار لازم است رایانه دوباره راه‌اندازی شود. بنابراین راه‌اندازی‌های مجدد رایانه، که به طور غیرمنتظره انجام می‌شود، می‌تواند نشانه‌ای از نفوذ خرابکاران شبکه‌ای به رایانه شما باشد.

۴. بعضی اوقات خرابکاران شبکه‌ای تنها با حذف بخش هایی از یک فایل می‌توانند راه نفوذ خود در آن را مخفی نگه دارند. بنابراین قسمت‌های حذف شده از یک فایل می‌تواند نشان‌دهندهٔ مسیر نفوذ خرابکاران شبکه‌ای به یک فایل از رایانه باشد.

۵. گاهی با این که انتظار می‌رود ارتباط بین دو رایانه از طریق شبکه، در زمان هایی مشخص، بسیار کم باشد ترافیک زیادی در آن مسیر ملاحظه می‌شود. چه بسا خرابکاران شبکه‌ای در حال تلاش برای نفوذ به آن سیستم‌ها باشند و همین امر موجب ترافیک سنگین بین آنها شود.

۶. بخش هایی در سیستم هر شرکت وجود دارد که جدا از بقیه سیستم بوده و تنها افراد معدودی به آن دسترسی دارند، گاهی می‌توان خرابکاران شبکه‌ای را در چنین بخش هایی پیدا کرد.

راهکارهای امنیتی شبکه

کنترل دولتی

علاوه بر بهره‌گیری از امکانات فنی، روش‌های کنترل دیگری نیز برای مهار اینترنت پیشنهاد شده است. در این روش، سیاست کلی حاکم بر کشور اجازه دسترسی به پایگاه‌های مخرب و ضد اخلاقی را نمی‌دهد و دولت شبکه‌های جهانی را از دروازه اتصال و ورود به کشور با فیلترهای مخصوص کنترل می‌کند.

کنترل سازمانی

روش دیگر، کنترل سازمانی است که معمولاً سازمان، اداره یا تشکیلاتی که مسئولیت سرویس‌دهی و اتصال شهروندان را به اینترنت به عهده می‌گیرد، خود موظف به کنترل شبکه و نظارت بر استفاده صحیح از آن می‌شود تا با الزامات قانونی و اخلاقی انجام این وظیفه را تضمین کند.

کنترل فردی

کنترل فردی روش دیگری است که قابل انجام است. در این نوع کنترل، تمام تضمین‌های اجرایی، درون فردی است و شخص با بهره‌گیری از وجدان فردی و مبانی اخلاقی و تعهد دینی، مراقبت‌های لازم را در ارتباط با شبکه‌های جهانی به عمل می‌آورد. این اعتقاد و فرهنگ در محدودهٔ خانواده نیز اعمال می‌شود و چه بسا اطرافیان را نیز تحت تأثیر قرار دهد. البته شیوهٔ اخیر در صورتی ممکن خواهد بود که واگذاری خط اشتراک IP پس از شناسایی کامل افراد و با ملاحظه خصوصیات اخلاقی آنان انجام پذیرد. در غیر این صورت تصور چنین اعمال کنترلی از سوی تک تک افراد جامعه صرفاً در حد آرزو باقی خواهد ماند. آرزویی که نمی‌تواند بسیاری از تأثیرات سوء این شبکه را از بین ببرد و آن را به سوی شبکه سالم سوق دهد.

تقویت اینترانت‌ها

از سوی دیگر تقویت شبکه‌های داخلی که به اینترانت معروف است می‌تواند نقش بسزایی در کاهش آلودگی‌های فرهنگی و اطلاعاتی اینترنت یاری کند. قرار دادن اطلاعات مفید اینترنت به صورت ناپیوسته و روی شبکه‌های داخلی یا اینترانت‌ها، علاوه بر ارائهٔ خدمات و اطلاع‌رسانی سالم، پس از چندی، بایگانی غنی و پربار از انواع اطلاعات فراهم‌آمده از چهارگوشه جهان را در اختیار کاربران قرار می‌دهد که با افزایش اطلاعات داخلی و یا روزآمد کردن آن، به عنوان زیربنای اطلاعاتی کشور قابل طرح است. به هر حال سرعت بالا و هزینه کم در استفاده از اینترانت‌ها، دو عامل مورد توجه کاربران به شبکه‌های داخلی است که به نظر نمی‌رسد محمل

مناسبی برای اطلاعات گزینش شده اینترنت باشد.

وجود یک نظام قانونمند اینترنتی

موردی دیگر که کارشناسان از آن به عنوان پادزهر آسیب‌های اینترنتی (تهاجم فرهنگی، اطلاعات نادرست و یا پیامدهای ضد اخلاقی) نام می‌برند، وجود یک نظام قانونمند اینترنتی در جامعه است که ادارهٔ آن از سوی یک متولی قدرتمند و کاردان می‌تواند اینترنت سرکش و افسار گسیخته را مهار کند و از آن به نحو شایسته بهره‌برداری کند.

این نظام اگر با یک نظام حقوقی و دادرسی جامع و عمیق توأم باشد، موارد تخلف و سوء استفاده از این ابزار به راحتی قابل تشخیص و پیگیری قضایی خواهد بود.

کارگسترده فرهنگی برای آگاهی کاربران

بهترین روش، برای آگاهی کاربران گسترش فرهنگ استفاده مناسب از اینترنت است.

فایروال ها

فایروال یا بارو شبکه‌های کوچک خانگی و شبکه‌های بزرگ شرکتی را از حملات احتمالی رخنه‌گرها (هکرها) و وب‌سایت‌های نامناسب و خطرناک حفظ می‌کند و مانع و سدی است که متعلقات و دارایی‌های شما را از دسترس نیروهای متخاصم دور نگاه می‌دارد.

بارو یک برنامه یا وسیله سخت‌افزاری است که اطلاعات ورودی به سیستم رایانه و شبکه‌های اختصاصی را تصفیه می‌کند. اگر یک بسته اطلاعاتی ورودی به وسیلهٔ فیلترها نشان‌دار شود، اجازه ورود به شبکه و رایانه کاربر را نخواهد داشت.

به عنوان مثال در یک شرکت بزرگ بیش از صد رایانه وجود دارد که با کارت شبکه به یکدیگر متصل هستند. این شبکهٔ داخلی توسط یک یا چند خط ویژه به اینترنت متصل است. بدون استفاده از یک بارو تمام رایانه‌ها و اطلاعات موجود در این شبکه برای شخص خارج از شبکه قابل دسترسی است و اگر این شخص راه خود را بشناسد می‌تواند یک یک رایانه‌ها را بررسی و با آنها ارتباط هوشمند برقرار کند. در این حالت اگر یک کارمند خطایی را انجام دهد و یک حفره امنیتی ایجاد شود، رخنه‌گرها می‌توانند وارد سیستم شده و از این حفره سوء استفاده کنند.

اما با داشتن یک بارو همه چیز متفاوت خواهد بود. بارو ها روی خطوطی که ارتباط اینترنتی برقرار می‌کنند، نصب می‌شوند و از یک سری قانون‌های امنیتی پیروی می‌کنند. به عنوان مثال یکی از قانون‌های امنیتی شرکت می‌تواند به صورت زیر باشد:

از تمام پانصد رایانه موجود در شرکت فقط یکی اجازه دریافت صفحات ftp را دارد و بارو باید مانع از ارتباط دیگر رایانه‌ها از طریق ftp شود.

این شرکت می‌تواند برای وب سرورها و سرورهای هوشمند و غیره نیز چنین قوانینی در نظر بگیرد. علاوه بر این، شرکت می‌تواند نحوهٔ اتصال کاربران کارمندان به شبکه اینترنت را نیز کنترل کند به عنوان مثال اجازه ارسال فایل از شبکه به خارج را ندهد.

در حقیقت با استفاده از بارو یک شرکت می‌تواند نحوهٔ استفاده از اینترنت را تعیین کند. باروها برای کنترل جریان عبوری در شبکه‌ها از سه روش استفاده می‌کنند:

Packet Filtering

یک بسته اطلاعاتی با توجه به فیلترهای تعیین شده مورد تحلیل و ارزیابی قرار می‌گیرند. بسته‌هایی که از تمام فیلترها عبور می‌کنند به سیستم‌های موردنیاز فرستاده شده و بقیه بسته‌ها رد می‌شوند.

Proxy Services

اطلاعات موجود در اینترنت توسط بارو اصلاح می‌شود و سپس به سیستم فرستاده می‌شود و بالعکس.

Stateful Inspection

این روش جدید محتوای هر بسته با بسته‌های اطلاعاتی ویژه‌ای از اطلاعات مورد اطمینان مقایسه می‌شوند. اطلاعاتی که باید از درون بارو به بیرون فرستاده شوند، با اطلاعاتی که از بیرون به درون ارسال می‌شود، از لحاظ داشتن خصوصیات ویژه مقایسه می‌شوند و در صورتی که با یکدیگر ارتباط منطقی داشته باشند اجازه عبور به آنها داده می‌شود و در غیر این صورت امکان مبادلهٔ اطلاعات فراهم نمی‌شود.

سیاست‌گذاری ملی در بستر جهانی

بدون ملاحظه چند الگوی ملی در برخورد با اینترنت نمی‌توان از سیاست‌گذاری مبتنی بر فهم جهانی سخن گفت. لذا معرفی اجمالی

چند نمونه که با سه رویکرد تحول گرا، ثبات گرا، و اعتدال گرا تناسب بیشتری دارند ضروری است.

الگوی آمریکایی

اینترنت در آمریکا هم به عنوان تهدید امنیتی و هم به عنوان بزرگ‌ترین فرصت ملی تلقی می‌شود. کاخ سفید در پنجم ژانویه سال ۲۰۰۰ بیانیه‌ای را تحت عنوان «استراتژی امنیت ملی در قرن جدید» منتشر کرد. در این بیانیه ضمن برشمردن منافع حیاتی آمریکا، از اینترنت به عنوان مهم‌ترین ابزار دیپلماسی مردمی نام برده شده است.

پیشرفت جهانی تکنولوژی‌های آزاد و اطلاع‌رسانی چون اینترنت توانایی شهروندان و مؤسسات را برای تأثیرگذاری بر سیستم‌های دولت‌ها تا حد غیرقابل تصوری بالا برده است. دیپلماسی مردمی یعنی تلاش برای انتقال اطلاعات و پیام‌هایمان به مردم جهان یکی از ابعاد مهم استراتژی امنیت ملی ماست. برنامه‌ریزی ما باید به گونه‌ای باشد که توانایی ما را برای اطلاع‌رسانی و تأثیرگذاری بر ملل کشورهای دیگر در جهت منافع آمریکا تقویت کند و گفت‌وگوی میان شهروندان و مؤسسات آمریکایی را با نظایرشان در دیگر کشورها توسعه ببخشد. توسعهٔ اینترنت در داخل و استفاده از آن برای تأثیرگذاری بر دیگران بخش مهمی از سیاست‌های استراتژیک آمریکاست.

افزایش جرایم رایانه‌ای در آمریکا از جمله حمله به سایت‌های Amazon و yahoo، ریس FBI را واداشت تا در فوریه ۲۰۰۰ از کنگره بخواهد ۳۷ میلیون دلار به بودجه ۱۰۰ میلیون دلاری وزارت دادگستری برای مبارزه با جرایم رایانه‌ای بیفزاید و کلینتون در همان ماه درخواست یک بودجه ۹ میلیون دلاری برای تأسیس مرکز امنیت ملی، مشارکت شرکت‌های اینترنتی و تجارت الکترونیک علیه حمله‌کنندگان به سایت‌های رایانه‌ای را به کنگره ارائه داد.

الگوی فلسطین اشغالی

این کشور در فاصله سال ۱۹۹۴ تا ۲۰۰۰ تبدیل به یک غول صنعت اینترنت شده است این کشور در سطح داخلی چنین سیاست هایی اتخاذ کرده است:

– اختصاص ۳٪ از GDP کشور معادل ۹۰ میلیارد دلار به تحقیق و توسعه در زمینه تکنولوژی پیشرفته

– آموزش مهارت های پیشرفته رایانه‌ای در دوران سربازی و تداوم آموزش در دوران خدمت احتیاط.

تولید Checkpoint با پیشینه و ریشه در کاربردهای نظامی و به عنوان یکی از قابل اطمینان‌ترین و پرفروش‌ترین باروهای جهان که کشورهای عربی نیز به آن متکی هستند، یکی از سیاست‌های جهانی کشور مذکور است.

الگوی چینی

چین رسماً اعلام کرده است به دنبال برقراری توازن میان جریان آزاد اطلاعات و صیانت فرهنگ و ارزش های اجتماعی خود است. پیتر پیت معاون شرکت دولتی اینترنت چین گفته است:

ما علاقه به قمار، پورنوگرافی و موارد حساسیت برانگیز سیاسی نداریم اما حتی با محتوای فیلترشده، اینترنت را تنها و مهم‌ترین نیرویی می‌دانیم که درهای چین را بر روی دنیا می‌گشاید و راه تغییرات اقتصادی را هموار می‌کند.

در اجرای این استراتژی، چین اقدامات زیر را انجام داده است:

– سرمایه‌گذاری عظیم در صنایع الکترونیک، مخابرات و رایانه

– اقدامات وسیع و سازمان یافته برای تکثیر، شکستن قفل و شبیه‌سازی نرم‌افزارها و برنامه‌های کاربردی رایانه‌ای و تقویت صنعت عظیم نرم‌افزار

– تأسیس شرکت دولتی اینترنت چین و انحصار ورود اینترنت به کشور از طریق این شرکت

– همکاری شرکت با غول های اینترنتی آمریکا برای ایجاد خدمات مبتنی بر وب با استانداردهای کیفی AQL و استانداردهای

اخلاقی و قانونی چین
– جلب همکاری AQL و Netscape برای تولید یک پویشگر اینترنت به زبان چینی
– هزینه عظیم برای فیلترکردن محتوای نامناسب اخلاقی و سیاسی در اینترنت

الگوی کشورهای عربی حاشیه خلیج فارس

تقریباً در تمام کشورهای حاشیه خلیج فارس کنترل قوی دولتی بر محتوا و توزیع اطلاعات وجود دارد. این کنترل ها به علل مذهبی، سیاسی و فشارهای داخلی صورت می‌گیرد. روش اصلی کنترل اطلاعات الکترونیک، در این کشورها انحصار مخابرات در شرکت های دولتی است. یکی از پیامدهای اصلی این کنترل دولتی تأخیر در رسیدن اینترنت و کندی در همه‌گیرشدن آن در این کشورهاست. در کشورهای عربی منطقه خلیج فارس دولت و بخش دانشگاهی عامل گسترش اینترنت نبوده‌اند، در عوض تجارت آزاد و بازرگانان خارجی مقیم، بیشترین مشتاقان و کاربران اینترنت را تشکیل می‌دهند. در واقع هیچ شخص، سازمان، و تجارت مدنی نمی‌تواند بدون اتکاء به وب و اینترنت در رقابت جهانی برای دسترسی به منابع طبیعی و اقتصادی خلیج فارس به بقاء خود ادامه دهد. اقتصاد وابسته و ادغام منطقه در اقتصاد جهانی، اتصال به اینترنت را گریزناپذیر می‌کند. بازار مصرف اینترنت در کشورهای عربی خلیج فارس، اساساً تجاری است.

کشورهای خلیج فارس از نظر سیاست‌گذاری در مورد اینترنت روی یک طیف قرار دارند که یک طرف آن عراق و طرف دیگر آن یمن و قطر است.

عراق تاکنون رسماً به اینترنت متصل نشده است و مودم های شخصی را ممنوع کرده است. از طرف دیگر یمن و قطر با حذف هرگونه کنترلی بر روی اینترنت و سرمایه‌گذاری برای گسترش زیرساخت ها به منافع اینترنت بیشتر از خطرات آن بها داده‌اند.

کویت با برخورداری از سیستم مخابراتی کاملاً پذیرفته در سال ۱۹۹۴ ارائه خدمات عمومی اینترنت را آغاز کرد. وزارت مخابرات کویت امتیاز ISP را ابتدا به گلف نت و سپس به یک کمپانی دیگر واگذار کرد. گلف نت از طریق ماهواره Sprint به آمریکا متصل است. دانشجویان کویتی بدون هیچ گونه هزینه به اینترنت دسترسی دارند.

عمان به واسطه جبران عقب ماندگی نسبی از دیگر کشورهای خلیج فارس، بازسازی سیستم مخابراتی را در اولویت های خود قرار داده است. در چارچوب یک طراحی ملی برای زیرساخت‌ها و خدمات مخابراتی GTO سازمان عمومی مخابرات طرحی را برای سال ۲۰۰۰ ارائه کرد که در آن امکان دسترسی به هر اطلاعی در هر زمانی در هر کجا و به هر شکل برای دولت و بخش خصوصی پیش‌بینی شده‌اند. GTO در سال ۱۹۹۵ یک مناقصه بین‌المللی را برای ISP اعلام کرد. در این مناقصه Sprint آمریکا برگزیده شد و علاوه بر ایجاد سایت، اداره آن را به مدت ۵ سال تعهد کرد. دسترسی عمومی به اینترنت از دسامبر ۱۹۹۶ فراهم شد و کاربری تجاری آن به سرعت توسعه یافت.

قطر مدرن ترین شبکهٔ مخابراتی منطقه را ایجاد کرده است و انحصار مخابرات دولتی توسط Qtel اعمال می شود که تنها ISP کشور را دارد، ولی بررسی هایی به منظور خصوصی‌سازی، ولی به صورت غیررقابتی در حال انجام است. دولت در کنار اینترنت، یک سیستم اطلاعاتی ژئوفیزیکی را با اهداف توسعه بخشی عمومی و خصوصی به‌سرعت توسعه داده است ولی آموزش عالی و دانشگاه بهره چندانی از آن نبرده‌اند. قطر تنها کشور حاشیه خلیج فارس است که خود را منطقه فارغ از سانسور اطلاعات معرفی کرده و هیچ‌گونه کنترلی بر محتوای اینترنت اعمال نمی‌کند. تنها حساسیت دولت مسأله پورنوگرافی است که با استفاده از باروها تا حدی کنترل می شود.

امارات متحده عربی از سال ۱۹۹۵ ارزان قیمت‌ترین و نظارت شده‌ترین خدمات اینترنت منطقه را ارائه می‌کند و نسبت به جمعیت دارای بیشترین تعداد رایانه متصل به اینترنت است. دولت و بخش تجاری و دانشگاهها همه پشتیبان اینترنت هستند و از آن به خوبی بهره‌برداری می‌کنند. وزارت مخابرات با راه‌اندازی چند پراکسی سرور گران قیمت تمام تبادلات داده‌ها را فیلتر و کنترل می‌کند. در عین حال امارات شاهد بیشترین مباحثات افکار عمومی درباره خطرات استفاده از اینترنت بوده است.

عربستان سعودی بزرگ ترین و محافظه‌کارترین کشور منطقه است و به موارد غیراخلاقی و فعالیت های تبعیدیان خارج نشین بسیار حساس است. هنوز اینترنت در سعودی توسعهٔ چندانی پیدا نکرده است و دسترسی عمومی در اینترنت همگانی نشده است، اما برخی از بخش های دولتی، پزشکی و دانشگاهی از طریق یک اتصال ماهواره‌ای به آمریکا از خدمات اینترنت استفاده می‌کنند. سعودی گران‌ترین طرح مطالعاتی در مورد کاربردها و استلزامات اینترنت را به مدت دو سال پیگیری کرد و در نتیجه روش مدیریت

کاملاً متمرکز برای ورود اینترنت به کشور و کنترل کل ورودی توسط یک باروی ملی برای جلوگیری از دسترسی به محتوای نامناسب از طرف دولت پذیرفته شد.

جمع‌بندی

به نظر می‌رسد تهدید اصلی و بالفعل کشور در مورد اینترنت، فقدان گفتمان امنیتی در مورد این پدیده است. اینترنت که به‌طور بالقوه می‌تواند هم تهدید و هم فرصتی طلایی برای امنیت فرهنگی و سیاسی باشد، به وسیله‌ای برای فشار سیاسی و اقتصادی تبدیل شده است.

فقدان دانش جامع‌نگر در مورد صورت مسأله و عدم وجود مطالعات سیاست‌گذاری مقایسه‌ای در کشور، حاکمیت روش آزمون خطا و اعمال سلایق فردی و سازمانی را به دنبال داشته است.

مسئولیت‌پذیری دولت در سیاست گذاری علمی، کارشناسانه و همه‌سونگر و بهره‌گیری از تمام توان علمی کشور، شرط اصلی تحقق بیشترین منافع و کمترین آسیب‌ها از صنعت اینترنت در ایران است.

برای جلوگیری از اثرات مخرب ارتباط با پایگاه‌های ضداخلاقی باید به سمتی حرکت کنیم که سایت های مفید، جذابیت پیدا کند. یعنی ابتدا در حد توان باید در زمینهٔ سایت‌های مفید و درعین حال جذاب سرمایه‌گذاری کنیم. از طرف دیگر هم باید موارد منفی را سد کنیم، یعنی از نفوذ سایت‌های مخرب، به این سو جلوگیری کنیم. چون در کشورهای غربی، مثل انگلیس، مسأله استفاده از سایت های مستهجن توسط دانش‌آموزان مدارس به صورت یک بحران درآمده است و آنها به این نتیجه رسیده‌اند که دو راه در پیش رو دارند: بستن راه‌های دسترسی به اینترنت یا کنترل آن از مباحث مطروحه نتایج ذیل به دست می‌آید:

۱. اینترنت به عنوان یک پدیدهٔ مثبت ارزیابی می‌شود.

۲. سوءاستفاده از شبکهٔ جهانی نباید مانع از بهره‌برداری از این رسانه دوسویه شود.

۳. امکان گزینش اطلاعات سالم و ارائهٔ آن برای عموم وجود دارد.

۴. امکان کنترل این شبکه تا حدود زیادی با روش های فنی، سازمانی و فرهنگی وجود دارد.

۵. همه کشورهای جهان در پی مسدود کردن نفوذ اطلاعات آلوده هستند و سعی در تدوین قوانین و مقرراتی برای جلوگیری از بهره‌برداری سوء از شبکهٔ جهانی‌اند.

در هر حال نیاز اساسی جوامع در حال رشد به دریافت اطلاعات مفید و سازنده را نمی‌توان نادیده گرفت. و این در حالی است که از تخریب مبانی اعتقادی و اجتماعی جامعه نیز می‌باید با حساسیت تمام جلوگیری کرد.

نفوذ اطلاعات آلوده به شبکه‌های اطلاع رسانی به مثابه سرایت سموم مهلک و خطرناک به شبکهٔ آب آشامیدنی سالم شهری است. این درحالی است که آلاینده‌های روحی و اخلاقی ضرباتی جبران‌ناپذیرتر از آلاینده‌های جسمی بر پیکر اجتماعات انسانی وارد می‌سازند.

منابع:

– بوزان، باری. (۱۳۷۸). مردم، دولت‌ها و هراس، تهران: پژوهشکده مطالعات راهبردی، ۱۳۷۸.

– تاجیک، محمدرضا. قدرت و امنیت در عصر پسامدرنیسم، گفتمان، شماره صفر، ۱۳۷۷.

– رنجبر، مقصود. ملاحظات امنیتی در سیاست خارجی جمهوری اسلامی ایران، تهران: پژوهشکده مطالعات راهبردی، ۱۳۷۹.

– رابرت، ماندل. چهره متغیر امنیت ملی، تهران: پژوهشکده مطالعات راهبردی، ۱۳۷۷

– محسنیان‌راد، مهدی. ارتباط جمعی در کشورهای اسلامی، تهران: دانشگاه امام صادق، انتشار محدود، ۱۳۷۷.

– محسنیان‌راد، مهدی. انتقاد در مطبوعات ایران، مرکز مطالعات و تحقیقات رسانه‌ها، انتشار محدود، ۱۳۷۶.

– محمدی، مجید. سیمای اقتدارگرایی تلویزیون دولتی ایران، تهران: جامعه ایرانیان، ۱۳۷۹.

– مولانا، حمید. جریان بین المللی اطلاعات، ترجمهٔ یونس شکرخواه، تهران: مرکز مطالعات و تحقیقات رسانه‌ها، ۱۳۷۹.

- Mohammadi Annabelle Sreberny, Ali. Small media, Big Revolution: Communication, Culture, and the Iranian Revolution.Univ of Minnesota Press.

- Sick, Gary.Middle East Studies Association Bulletin, December, 1999.

- A National security Strategy for a new centry,Us Dept of State, 2000.

-Tehranian, Majid. Global Communication and World Politics: Domination Development and Discourse Lynne Rienner Publisher.