امنیت شبکه: چالشها و راهکارها

نوشته: علیرضا گنجی*

چکیده

این مقاله به طور کلی به چالشها و راهکارها در امنیت شبکه می‌پردازد. در ابتدای مقاله به مباحثی چون: امنیت شبکه‌های اطلاعاتی و ارتباطی، اهمیت امنیت شبکه، سابقهٔ امنیت شبکه، پیدایش جرایم رایانه‌ای، طبقه‌بندی جرایم رایانه‌ای، و راهکارهایی که برای این چالش پیشنهاد شده است از جمله کنترل دولتی، کنترل سازمانی، کنترل فردی، تقویت اینترانتها، وجود یک نظام قدرتمند و کار گسترده فرهنگی برای آگاهی کاربران و فایروالها پرداخته می‌شود. در آخر نیز به مسأله «اینترنت و امنیت فرهنگی در ایران» و چالشهایی که در این زمینه مطرح گردیده پرداخته شده و برای رفع این مشکل پیشنهاداتی نیز ارائه گردیده است.

۱. مقدمه

اینترنت یک شبکهٔ عظیم اطلاع‌رسانی 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 را یک ضرورت در عصر اطلاعات می‌دانند.

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 در تمامی زمینه‌ها از هر سنخ و نوعی به اشتراک گذاشته‌اند. گفته می‌شود نزدیک به یک میلیارد صفحه اطلاعات با موضوعات گوناگون از سوی افراد حقیقی و حقوقی روی این شبکه قرار داده شده است.

این اطلاعات با سرعت تمام در بزرگراههای اطلاعاتی بین کاربران رد و بدل می‌شود و تقریباً هیچ گونه

* کارشناس ارشد کتابداری و اطلاع‌رسانی دانشگاه فردوسی مشهد

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 اطلاع‌رسانی 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 بخصوص در خاستگاه این شبکهٔ جهانی یعنی آمریکا، کارشناسان اجتماعی را بشدت نگران کرده، به گونه‌ای که هیأت حاکمه را مجبور به تصویب قوانینی مبنی بر کنترل این شبکه در سطح آمریکا نموده 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. علی‌الرغم وجود جنبه‌ای مثبت شبکه‌های جهانی، سوء استفاده از این شبکه‌های رایانه‌ای توسط افراد بزهکار، امنیت ملی را در کشورهای مختلف با خطر روبرو ساخته است. از این رو بکارگیری فیلترها و فایر وال‌های 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.

۲. امنیت شبکه‌های اطلاعاتی و ارتباطی

۲-۱: اهمیت امنیت شبکه

چنانچه به اهمیت شبکه‌های اطلاعاتی (الکترونیکی) و نقش اساسی آن دریافت اجتماعی آینده پی برده باشیم، اهمیت امنیت این شبکه‌ها مشخص می‌گردد. اگر امنیت شبکه برقرار نگردد، مزیتهای فراوان آن نیز به خوبی حاصل نخواهد شد و پول و تجارت الکترونیک، خدمات به کاربران خاص، اطلاعات شخصی، اطلاعاتی عمومی و نشریات الکترونیک همه و همه در معرض دستکاری و سوءاستفاده‌های مادی و معنوی هستند. همچنین دستکاری اطلاعات- به عنوان 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 راههای مخفی وجود دارد. در آینده که بانکها و بسیاری از نهادها و دستگاههای دیگر از طریق شبکهٔ به فعالیت می‌پردازند، جلوگیری از نفوذ عوامل مخرب در شبکه بصورت مسئله‌ای استراتژیک درخواهد آمد که نپرداختن به آن باعث ایراد خساراتی خواهد شد که بعضاً جبران‌ناپذیر خواهد بود. چنانچه یک پیغام خاص، مثلاً از طرف شرکت مایکروسافت، به کلیه سایتهای ایرانی ارسال شود و سیستم عاملها در واکنش به این پیغام سیستمها را خراب کنند و از کار بیندازند، چه ضررهای هنگفتی به امنیت و اقتصاد مملکت وارد خواهد شد؟

نکته جالب اینکه بزرگترین شرکت تولید نرم‌افزارهای امنیت شبکه، شرکت چک پوینت است که شعبهٔ اصلی آن در اسرائیل می‌باشد. مسأله امنیت شبکهٔ برای کشورها، مسأله‌ای استراتژیک است؛ بنابراین کشور ما نیز باید به آخرین تکنولوژیهای امنیت شبکه مجهز شود و از آنجایی که این تکنولوژیها به صورت محصولات نرم‌افزاری قابل خریداری نیستند، پس می‌بایست محققین کشور این مهم را بدست بگیرند و در آن فعالیت نمایند.

امروزه اینترنت آنقدر قابل دسترس شده که هرکس بدون توجه به محل زندگی، ملیت، شغل و زمان میتواند به آن راه یابد و از آن بهره ببرد. همین سهولت دسترسی آن را در معرض خطراتی چون گم شدن، ربوده شدن، مخدوش شدن یا سوءاستفاده از اطلاعات موجود در آن 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 منظور کافی است.

۲-۲: سابقه امنیت شبکه

اینترنت در سال ۱۹۶۹ بصورت شبکه‌های بنام آرپانت که مربوط به وزارت دفاع آمریکا بود راه‌اندازی شد. هدف این بود که با استفاده از رایانه‌های متصل به هم، شرایطی ایجاد شود که حتی اگر، بخشهای عمده‌ای از سیستم اطلاعاتی به هر دلیلی از کار بیفتد، کل شبکه بتواند به کار خود ادامه دهد، تا این اطلاعات حفظ شود. از همان ابتدا، فکر ایجاد شبکه، برای جلوگیری از اثرات مخرب حملات اطلاعاتی بود.

در سال ۱۹۷۱ تعدادی از رایانه‌های دانشگاهها و مراکز دولتی به این شبکه متصل شدند و محققین از این طریق شروع به تبادل اطلاعات کردند.

با بروز رخدادهای غیرمنتظره در اطلاعات، توجه به مسأله امنیت بیش از پیش اوج گرفت. در سال ۱۹۸۸، آرپانت برای اولین بار با یک حادثه امنیتی سراسری در شبکه، مواجه شد که 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 بصورت 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- 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 روشن نموده است.

۳- 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 می‌باشد که جامعه را بطور پیچیده‌ای دگرگون ساخته‌اند.

سهولت در دسترسی و جستجوی 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 بدست 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 به شمار می‌رود. بعلاوه 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. فناوری جدید مفاهیم قانونی موجود را دچار چالشهایی ساخته است. اطلاعات و ارتباطات راه دور به راحت‌ترین وجه در جهان جریان پیدا کرده و مرزها دیگر موانعی بر سر این جریان به شمار نمی‌روند. جنایتکاران غالباً در مکانهایی به غیر از جاههایی که آثار و نتایج اعمال آنها ظاهر می‌شود، قرار دارند.

سوءاستفاده گسترده مجرمین، به ویژه گروههای جنایتکار سازمان نیافته از فناوری اطلاعات سبب گشته 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 بکارگیری بهترین متخصصین در واحدهای مذکور، بخشی از اقدامات مقابله‌ای را تشکیل می‌دهد.

۳-۱: پیدایش جرایم رایانه‌ای

در مورد زمان دقیق پیدایش جرم رایانه‌ای نمی‌توان اظهارنظر قطعی کرد. این جرم زائیده تکنولوژی اطلاعاتی و انفورماتیکی است، بنابراین بطور 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 بصورت گسترده، امکان بررسی اولین مورد را دشوار می‌سازد. در نهایت آن چه مبرهن است اینکه در جامعه آمریکا رویس موجب شد برای اولین بار اذهان متوجه سوءاستفاده‌های رایانه‌ای شود.

۳-۲: قضیه رویس:

آلدون رویس حسابدار یک شرکت بود. چون به گمان وی، شرکت حق او را پایمال کرده بود، بنابراین با تهیه برنامه‌ای، قسمتی از پولهای شرکت را اختلاس کرد. انگیزهٔ رویس در این کار انتقام‌گیری بود.

مکانیزم کار بدین گونه بود که شرکت محل کار وی یک عمده‌فروش میوه و سبزی بود. محصولات متنوعی را از کشاورزان می‌خرید و با استفاده از تجهیزات خود از قبیل کامیونها، انبار و بسته‌بندی و سرویس‌دهی به گروههای فروشندگان، آنها را عرضه می‌کرد. به دلیل وضعیت خاص این شغل، قیمتها در نوسان بود و ارزیابی امور تنها می‌توانست از عهدهٔ رایانه برآید تا کنترل محاسبات این شرکت عظیم را عهده‌دار شود.

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

رویس در برنامه‌ها، دستورالعمل‌های اضافی را گنجانده بود و قیمت کالاها را با ظرافت خاصی تغییر می‌داد. با تنظیم درآمد اجناس وی مبلغی را کاهش می‌داد و مبالغ حاصله را به حسابهای مخصوص واریز می‌کرد. بعد در زمانهای خاص چکی به نام یکی از هفده شرکت جعلی و ساختگی خودش صادر و مقداری از مبالغ را برداشت می‌کرد. بدین ترتیب وی توانست در مدت ۶ سال بیش از یک میلیون دلار برداشت کند. اما او بر سر راه خودش مشکلی داشت و آن این بود که مکانیسمی برای توقف عملکرد سیستم نمی‌توانست 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 رایانه‌ای ایجاد شد.

۳-۳: تعریف جرم رایانه‌ای

تاکنون تعریفهای گوناگونی از جرم رایانه‌ای از سوی سازمانها، متخصصان و برخی قوانین ارائه شده که وجود تفاوت در آنها بیانگر ابهامات موجود در ماهیت و تعریف این جرائم است.

جرم رایانه‌ای یا جرم در فضای مجازی (سایر جرایم) دارای دو معنی و مفهوم است. در تعریف مضیق، جرم رایانه‌ای صرفاً عبارت از جرایمی است که در فضای سایبر رخ می‌دهد. از این نظر جرایمی مثل هرزه‌نگاری، افترا، آزار و اذیت سوءاستفاده از پست الکترونیک و سایر جرایمی که در آنها رایانه به عنوان ابزار و وسیله ارتکاب جرم بکار گرفته می‌شود، در زمرهٔ جرم رایانه‌ای قرار نمی‌گیرند.

در تعریف موسع از جرم رایانه‌ای هر فعل و ترک فعلی که در اینترنت یا از طریق آن یا با اینترنت یا از طریق اتصال به اینترنت، چه بطور مستقیم یا غیرمستقیم رخ می‌دهد و قانون آن را ممنوع کرده و برای آن مجازات در نظر گرفته شده است جرم رایانه‌ای نامیده می‌شود. براین اساس اینگونه جرایم را می‌توان به سه دسته تقسیم نمود:

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

دسته دوم: جرایمی هستند که در آنها رایانه به عنوان ابزار وسیله توسط مجرم برای ارتکاب جرم بکار گرفته می‌شود.

دسته سوم: جرایمی هستند که می‌توان آنها را جرایم رایانه‌ای محض نامید. این نو ع از جرایم کاملاً با جرایم کلاسیک تفاوت دارند و در دنیای مجازی به وقوع می‌پیوندند اما آثار آنها در دنیای واقعی ظاهر می‌شود. مانند دسترسی غیرمجاز به سیستم‌های رایانه‌ای.

۳-۴: طبقه‌بندی جرایم رایانه‌ای

طبقه‌بندی‌های مختلفی از جرایم رایانه‌ای توسط مراجع مختلف انجام گرفته است. برای آشنایی شما با آنها موارد مهم بشرح زیر اکتفا می‌شود.

۳-۴-۱: طبقه‌بندی OECDB

در سال ۱۹۸۳ «او.ای.سی.دی.بی» مطالعه امکان پذیری اعمال بین‌المللی و هماهنگی قوانین کیفری را به منظور حل مسئله جرم یا سوءاستفاده‌های رایانه‌ای متعهد شد. این سازمان در سال ۱۹۸۶ گزارشی تحت عنوان جرم رایانه‌ای، تحلیل سیاستهای قانونی منتشر ساخت که به بررسی قوانین موجود و پیشنهادهای اصلاحی چند کشور عضو پرداخته و فهرست حداقل سوءاستفاده‌هایی را پیشنهاد کرده بود که کشورهای مختلف باید با استفاده از قوانین کیفری، مشمول ممنوعیت و مجازات قرار دهند. بدین گونه اولین تقسیم‌بندی از جرایم رایانه‌ای 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 عبارتند از:

الف: ورود، تغییر، پاک کردن و یا متوقف‌سازی داده‌های رایانه‌ای و برنامه‌های رایانه‌ای که بطور ارادی با قصد انتقال غیرقانونی وجوه یا هر چیز باارزش دیگر صورت گرفته باشد.

ب: ورود، تغییر، پاک کردن، و یا متوقف‌سازی داده‌های رایانه‌ای و برنامه‌های رایانه‌ای که بصورت عمدی و به قصد ارتکاب جعل صورت گرفته باشند. یا هرگونه مداخله دیگر در سیستمهای رایانه‌ای که بصورت عمدی و با قصد جلوگیری از عملکرد سیستم رایانه‌ای و یا ارتباطات صورت گرفته باشد.

ج: ورود، تغییر، پاک کردن و متوقف‌سازی داده‌های رایانه‌ای و یا برنامه‌های رایانه‌ای.

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

ه- 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.

۳-۴-۲: طبقه‌بندی شورای اروپا:

کمیتهٔ منتخب جرایم رایانه‌ای شورای اروپا، پس از بررسی نظرات «او.ای.سی.دی.بی» و نیز بررسیهای حقوقی- فنی دو لیست تحت عناوین لیست حداقل و لیست اختیاری را به کمیته وزراء پیشنهاد داد و آنان نیز تصویب کردند. این لیستها بدین شرح هستند:

الف: کلاه‌برداری رایانه‌ای

ب: جعل رایانه‌ای
ج: خسارت زدن به داده‌های رایانه‌ای یا برنامه‌های رایانه‌ای
د: دستیابی غیرمجاز
ه: ایجاد مجدد و غیرمجاز یک برنامهٔ رایانه‌ای حمایت شده
- ایجاد مجدد غیرمجاز یک توپوگرافی.
- لیست اختیاری
الف: تغییر داده‌های رایانه‌ای و یا برنامه‌های رایانه‌ای
ب: جاسوسی رایانه‌ای
ج: استفاده غیرمجاز از رایانه
د: استفاده غیرمجاز از برنامهٔ رایانه‌ای حمایت شده.

۳-۴-۳: طبقه‌بندی اینترپول:

سالهاست که اینترپول در مبارزه با جرایم مرتبط با قناوری اطلاعات فعال می‌باشد. این سازمان با بهره‌گیری از کارشناسان و متخصصین کشورهای عضو اقدام به تشکیل گروههای کاری در این زمینه کرده است. 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 می‌نمایند.

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 سی‌امین گردهمایی آن در دبیرخانه کل تشکیل گردید.

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 می‌باشد و انجام چندین پروژه تحقیقاتی پیرامون موضوعات مرتبط با جرایم رایانه‌ای از جمله اقدامات گروه کاری مذکور می‌باشد. گروه کار آمریکایی جرایم مرتبط با تکنولوژی اطلاعات مرکب از کارشناسان و متخصصین 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 گردید. آنها کارشان را با برگزاری یک دوره آموزشی آغاز نمودند 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، و سریلانکا 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 گردیده است.

سازمان پلیس جنایی بین‌المللی جرایم رایانه‌ای را به شرح زیر طبقه‌بندی کرده است:

۱: دستیابی غیرمجاز
۱-۱: نفوذغیرمجاز
۱-۲: شنود غیرمجاز
۱-۳: سرقت زمان رایانه
۲: تغییر داده‌های رایانه‌ای
۲-۱: بمب منطقی
۲-۲: اسب تروا
۲-۳: ویروس رایانه‌ای
۲-۴: کرم رایانه‌ای
۳: کلاه‌برداری رایانه‌ای
۳-۱: صندوقهای پرداخت
۳-۲: جعل رایانه‌ای
۳-۳: ماشینهای بازی

۳-۴: دستکاریها در مرحله ورودی/ خروجی
۳-۵: ابزار پرداخت (نقطه فروش)
۳-۶: سوءاستفاده تلفنی

۴: تکثیر غیرمجاز

۴-۱: بازیهای رایانه‌ای
۴-۲: نرم‌افزارهای دیگر
۴-۳: توپوگرافی نیمه هادی

۵: سابوتاژ رایانه‌ای

۵-۱: سخت‌افزار
۵-۲: نرم‌افزار

۶: سایر جرائم رایانه‌ای

۶-۱: سیستمهای تابلوی اعلانات الکترونیک
۶-۲: سرقت اسرار تجاری
۶-۳: سایر موضوعات قابل تعقیب

۳-۴-۴: طبقه‌بندی در کنوانسیون جرایم سایبرنتیک

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

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 نموده 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

۳-۵: 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 صورتیکه یک خرابکار بتواند به حساب بانکی شما نفوذ کند فایل آن بطور 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 بطور غیرمنتظره انجام می‌شود، می‌تواند نشانه‌ای از نفوذ خرابکاران شبکه‌ای به رایانه شما باشد.

۴: بعضی اوقات خرابکاران شبکه‌ای تنها با حذف بخشهایی 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 زمانهایی 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: بخشهایی 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 بخشهایی پیدا کرد.

۴: راهکارهای امنیتی شبکه

۴-۱: 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.

۴-۲: کنترل سازمانی

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

۴-۳: 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 آورد. 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 خواه بود که واگذاری خط اشتراک IP پس از شناسایی کامل افراد و با ملاحظه خصوصیات اخلاقی آنان انجام پذیرد. در غیر این صورت تصور اعمال چنین 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 بسوی شبکه سالم سوق دهد.

۴-۴: تقویت اینترانت‌ها

از سوی دیگر تقویت شبکه‌های داخلی که به اینترانت معرو ف 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 پرباری از انواع اطلاعات فراهم آمده از چهار گوشه جهان را در اختیار کاربران قرار می‌دهد که با افزایش اطلاعات داخلی و یا روزآمد کردن آن، به عنوان زیربنای اطلاعاتی کشور قابل طرح می‌باشد. 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.

۴-۵: وجود یک نظام قانونمند اینترنتی

مورد دیگر که کارشناسان از آن به عنوان پادزهر آسیبهای اینترنتی از قبیل 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 نماید.

این نظام اگر با یک نظام حقوقی و دادرسی جامع و عمیق توأم باشد، موارد تخلف و سوءاستفاده از این ابزار به راحتی قابل تشخیص و پیگیری قضایی خواهد بود. در این صورت امکان سوءاستفاده و تأثیرپذیری از فرهنگهای بیگانه که عموماً مغایر با اصول اخلاقی ماست، به طرز چشمگیری کاهش می‌یابد.

۴-۶: کار گسترده فرهنگی برای آگاهی کاربران

اما بهترین روش، کار گستردهٔ فرهنگی، برای آگاهی کاربران است. کافی است که آنها آگاه شوند که گرایش و ارتباط با پایگاههای غیرمتعارف جز ضلالت و تباهی ثمره‌ای ندارد. باید تقوای درونی و اعتقادات دینی کاربران را رشد داد و آنها را تقویت کرد. بنابراین بهترین بارو (فایروال) برای ممانعت از خطرات اینترنت و جلوگیری از تأثیر ابعاد منفی آن، وجدان درونی و ایمان هر نسل است که بخشی از این ایمان را علمای دین باید در وجود نسل جوان و انسانهای این عصر بارور سازند.

۴-۷: فایروالها

در حقیقت فایروال یا بارو شبکه‌های کوچک خانگی و شبکه‌های بزرگ شرکتی را از حملات احتمالی رخنه‌گرها (هکرها) و وب سایتهای نامناسب و خطرناک حفظ می‌کند و مانع و سدی است که متعلقات و دارایهای 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. باروها 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:

۱: 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.

۲: Proxy Services

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

۳: 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 داشتن اجازه عبور به آنها داده می‌شود و در غیر اینصورت امکان مبادلهٔ اطلاعات فراهم نمی‌شود.

۴-۷: سیاست‌گذاری ملی در بستر جهانی

واقعیت این است که 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 تحول‌گرا، ثبات‌گرا، و اعتدال‌گرا تناسب بیشتری دارند ضروری است.

۴-۷-۱: 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 گفتگوی میان شهروندان و مؤسسات آمریکایی را با نظائرشان 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.

۴-۷-۲: 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 سیاستهایی اتخاذ کرده است:

- اختصاص ۳٪ از GDP کشور معادل ۹۰ میلیارد دلار به تحقیق و توسعه در زمینه تکنولوژی پیشرفته
- آموزش مهارتهای 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.

۴-۷-۳: الگوی چینی

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

ما علاقه به قمار، پورنوگرافی و موارد حساسیت برانگیز سیاسی نداریم اما حتی با محتوای فیلتر شده، اینترنت را تنها و مهمترین نیرویی می‌دانیم که درهای چین را بر روی دنیا می‌گشاید 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 در چین
- تأسیس شرکت دولتی اینترنت چین و انحصار ورود اینترنت به کشور از طریق این شرکت
- همکاری شرکت با غولهای 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 فیلتر کردن محتوای نامناسب اخلاقی و سیاسی در اینترنت

۴-۷-۴: الگوی کشورهای عربی حاشیه خلیج فارس

تقریباً در تمام کشورهای حاشیه خلیج فارس کنترل قوی دولتی بر محتوا و توزیع اطلاعات وجود دارد. این کنترلها به علل مذهبی، سیاسی و فشارهای داخلی صورت می‌گیرد. روش اصلی کنترل اطلاعات الکترونیک، در این کشورها انحصار مخابرات در شرکتهای دولتی است. یکی از پیامدهای اصلی این کنترل دولتی تأخیر در

رسیدن اینترنت و کندی در همه‌گیر شدن 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 مودمهای شخصی را ممنوع کرده است. از طرف دیگر یمن و قطر با حذف هرگونه کنترلی بر روی اینترنت و سرمایه‌گذاری برای گسترش زیر ساختها 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 اولویتهای 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 مدرن‌ترین شبکهٔ مخابراتی منطقه را ایجاد کرده است و انحصار مخابرات دولتی توسط Qtel اعمال می‌شود که تنها ISP کشور را دارا می‌باشد، ولی بررسیهایی 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 به سرعت 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 می‌شود.

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 بزرگترین و محافظه‌کارترین کشور منطقه است و به موارد غیراخلاقی و فعالیتهای 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 بخشهای 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.

۵- اینترنت و امنیت فرهنگی ایران

در بحبوحه جنگ نگرشها، این واقعیت را نباید از نظر دور داشت که در حال حاضر اینترنت در ایران نقش بسیار مهمی از لحاظ امنیت فرهنگی ایفاء می‌کند. از نظر علمی افزایش توانایی دسترسی دانشجویان، اساتید، و محققان ایرانی به منابع الکترونیک و تماسهای علمی با دانشمندان دیگر کشورها کاملاً مرهون اینترنت دانشگاهیان است. از نظر افزایش توان کسب آگاهیهای سیاسی و اجتماعی و دریافت آراء مختلف و امکان گفتگو نمی‌توان نقش اینترنت را انکار کرد. امروزه سایتهای مختلف ایرانی با تشکیل گروههای مباحثاتی بسیار جدید در مورد مسائل جهانی و ملی عرضه وسیعی را برای آگاهی جویی و اعلام نظرهای تخصصی و عمومی فراهم کرده‌اند (سیک، ۱۹۹۹). پیگیری نظرسنجی‌های اینترنتی در مورد انتخاب مجلس ششم، انتخاب رئیس مجلس، فایده یا ضرر ارتباط با آمریکا، انتخاب مهمترین شخصیت قرن اخیر ایران، نشان می‌دهد که اینترنت برای ایرانیان امکانات کاملاًمساعدی برای ابراز آزادانه عقاید و مشارکت سیاسی و فرهنگی فراهم آورده است. حتی برخی احزاب و داوطلبان نمایندگی برای تبلیغات انتخاباتی خود، از اینترنت استفاده کرده‌اند. به این ترتیب می‌توان نقش مهمی برای اینترنت در گسترش آزادیها و مشارکت سیاسی و دمکراسی فرهنگی قائل شد.

۵-۱: معیارهای امنیت فرهنگی در سیاستگذاری

برای تحلیل فرآیند سیاستگذاری در مورد اینترنت در ایران، پاسخ به سؤالاتی در مورد آزادی بیان، کنترل جریان اطلاعات، قوانین مربوط و در یک بیان نظریه هنجاری حاکم بر رسانه‌های جدید ضروری است. این سؤالات به ۵ حیطه اصلی قابل تحلیل است:

حق ارتباط خصوصی
حق ارتباط ناشناس
حق رمزگذاری در ارتباط
معافیت کانال ارتباطی از مسئولیت محتوی
دسترسی عمومی و ارزان

با توجه به تحقیق محسنیان راد (۱۳۷۶) نظریه حاکم بر رسانه‌های مرسوم در ایران در سال ۱۳۷۶، آمیزه‌ای از نظریه مسئولیت اجتماعی، توسعهٔ بخش و ایدئولوژیک بوده است. تغییرات سیاسی سال ۷۶ به بعد نقش نظریه مسئولیت اجتماعی را تقویت کرده است. ولی در مورد اینترنت وضع کاملاً متفاوت است و حاکمیت تئوری آزادی‌گرا بر دسترسی و انتشار از طریق اینترنت کاملاً ملموس است. تا اواخر نیمه اول سال ۱۳۸۰، دولت هیچ گونه نظارت و دخالت ملموسی در مورد آن نداشته است. زیرا:

۱.قوانین مربوط به مطبوعات که عمده‌ترین قانون در حوزهٔ محدوده محدودیتهای آزادی بیان است شامل گفتار روی شبکه نمی‌شود.
۲.افراد، سازمانها و شرکتها امکان دسترسی به سرویس دهندگان اینترنت را از طریق خطوط تلفن دارند.
۳.برای دسترسی به اینترنت هیچ گونه مجوز دولتی لازم نیست.
۴.دسترسی به اینترنت با پست یا پست الکترونیک نیاز به هیچ گونه تأییدای از طرف هیچ سازمان دولتی ندارد.
۵.هیچ دستورالعمل یا بخشنامه‌ای وجود ندارد که سرویس دهندگان را موظف کند اطلاعات مربوط به مشترکان، کاربران و محتوای داده‌های تبادل شده را به سازمانهای دولتی ارائه دهند.
۶.هیچ قانون یا دستورالعملی برای منع رمزگذاری محتوای داده‌های مبادله شده وجود ندارد.
۷.هیچ قانونی وجود ندارد که سرویس‌دهندگان ملزم به کنترل محتوا نماید.
۸.هیچ سیاست و اقدام مشخصی در مورد سانسور یا بلوک کردن سایتها، گروههای مباحثاتی و آدرسهای پست الکترونیکی وجود ندارد و ایران فاقد یک بارو و سیستم فیلترینگ ملی و مرکزی است.

۹.هیچ قانونی وجود ندارد که سرویس‌دهندگان را مسئول محتوای سایتهای روی سرویس بداند.

۱۰. کافه‌های اینترنتی به سرعت در حال رشد است و هیچ قانون خاصی برای نحوهٔ تأسیس و نحوهٔ اداره وجود ندارد، این کافه‌ها تابع قانون اماکن عمومی هستند.

۱۱. خدمات اینترنت در ایران به سرعت ارزان شده است و دولت برای دسترسیهای دانشگاهی سوبسید قابل ملاحظه‌ای را پذیرفته است. سیاست گسترش فیبر نوری و افزایش ظرفیت تبادل بین‌المللی داده‌ها از سیاستهای جاری دولت است.

۵-۲: مشکلات فعلی سیاستگذاری در امنیت فرهنگی و اینترنت

در جریان سیاستگذاری برای اینترنت در کشور ما موانع جدی وجود دارد. این موانع را می‌توان به شرح زیر مرتب کرد:

۱.فقدان استراتژی فرهنگی کلان در مورد صنایع فرهنگی جدید

۲.فقدان سیاست ملی مخابراتی

- روشن نبودن اولویت‌بندی در مورد گسترش تلفن ثابت، همراه و مخابرات داده‌ها
- روشن نبودن میزان ظرفیت دولت در پذیرش مشارکت بخش خصوصی در وارد کردن و توزیع اینترنت

۳. فقدان سیاست روشن گمرکی

در مورد مجاز یا ممنوع بودن واردات تجهیزات، دریافت و ارسال ماهواره‌ای برای خدمات اینترنت

۴.وجود رقابت تخریبی میان ارگانهای عمومی

متولی اینترنت در کشور از جمله فیزیک نظری، شرکت مخابرات، صدا و سیما

۵. فقدان سیاست ملی اطلاع‌رسانی

علی‌الرغم تشکیل شورای عالی اطلاع‌رسانی این شورا به سیاست‌گذاری تفصیلی و اعلام شده‌ای در زمینهٔ اطلاع‌رسانی دست نیافته است. وجود مدعیان و متولیان متعدد در مدیریت ملی اطلاعات و عدم تفکیک وظایف آنها موجب کندی و بلکه عقب‌ماندگی جدی ایران در تولید و سازماندهی اطلاعات الکترونیک شده است. امروزه به علت عدم سازماندهی اطلاعات علمی کشور، دسترسی به کتابخانه کنگرهٔ آمریکا بسیار ساده‌تر و مفیدتر از دسترسی به کتابخانه‌های ملی، مجلس و دانشگاه تهران است.

۶. فقدان سیاستهای نظارتی و امنیتی

هم اکنون بایستی روشن شود که مسئول حفاظت از داده‌های موجود در سامانه‌های نظامی، امنیتی، اقتصادی کشور کیست؟

چه سازمانی مسئول جلوگیری، پیشگیری و پیگیری حملات الکترونیکی و نقش امنیت سامانه‌های ملی است؟

چه سازمانی متولی سیاستگذاری و تعیین موارد ممنوعه در تبادل داده‌ها است؟

کدام سازمان مسئول نظارت بر کیفیت فرهنگی و محتوای سایتهای تولیدشده و قابل دسترس در کشور است؟

۵-۳: ملاحظات فرهنگی در سیاستگذاری

به نظر می‌رسد ملاحظات اساسی فرهنگی در سیاستگذاری آتی در مورد اینترنت در ایران به شرح زیر می‌باشد:

- گسترش اینترنت در کشور ایران باید به گونه‌ای باشد که به خلاقیت‌گستری مدد رسانده، نه اینکه موجبات خلاقیت‌زدایی را فراهم آورد. سیاستگذاری در مورد توسعه اینترنت نباید به توسعه مصرف یا باز تولید محتوای آن محدود شود، بلکه باید گسترش فرهنگ بومی و مذهبی و مقاومت فرهنگی را به دنبال داشته باشد.
- بیش و پیش از توسعه اینترنت باید به نظام تولید و سازماندهی الکترونیک اطلاعات علمی، اداری و مالی براساس استانداردهای قابل تبادل در شبکهٔ اهتمام داشت و بودجه‌های کلانی را به این امر اختصاص داد.
- تدوین و اجرای قوانین موردنیاز و روزآمد در حوزهٔ ارتباطات شبکه‌ای بسیار اساسی است این قوانین به خصوص موضوع حقوق تکثیر و مالکیت آثار فرهنگی

و نرم‌افزارها و اطلاعات الکترونیک تأثیر قطعی در تشویق تولید فرهنگی بر روی شبکه دارد.

- در سیاستگذاری فرهنگی باید چگونگی کاربرد تکنولوژی توسط مؤسسات فرهنگی و تأثیر آن را بر مخاطبان در نظر گرفت. معلوم نیست که هرگونه استفاده از تکنولوژی جدید لزوم به افزایش تأثیرپذیری مخاطبان منجر شود.
- نظام نظارت فرهنگی بر محتوای داده‌های مبادله شده و ثبت ملی نقش اساسی در پیشگیری از گسترش فساد، تهدیدات امنیتی، رسوخ جاسوسی و خرابکاری الکترونیک و عملیات روانی دارد.

جمع‌بندی

به نظر می‌رسد تهدید اصلی و بالفعل کشور در مورد اینترنت، فقدان گفتمان امنیتی در مورد این پدیده است. اینترنت که بطور 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 سیاستگذاری علمی، کارشناسانه و همه سو نگر 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 سایتهای 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 سایتهای 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

بطور کلی آنچه را که از مطالب بالا می‌توان نتیجه‌گیری کرد می‌توان در پنج بند خلاصه نمود:

۱) اینترنت به عنوان یک پدیدهٔ مثبت ارزیابی می‌شود.
۲) سوءاستفاده از شبکهٔ جهانی نباید مانع از بهره‌برداری از این رسانه دو سویه شود.
۳) امکان گزینش اطلاعات سالم و ارائه آن برای عموم وجود دارد.
۴) امکان کنترل این شبکه تا حدود زیادی با روشهای 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 اطلاع‌رسانی به مثابه سرایت سموم مهلک و خطرناک به شبکهٔ آب آشامیدنی سالم شهری است. این درحالی است که آلاینده‌های روحی و اخلاقی ضرباتی دهشتناکتر و جبران‌ناپذیرتر از آلاینده‌های جسمی بر پیکر اجتماعات انسانی وارد می‌سازند.

منابع:

بوزان، باری. (۱۳۷۸). ***مردم، دولتها و هراس***. تهران: پژوهشکده مطالعات راهبردی.
تاجیک، محمدرضا. (۱۳۷۷). ***قدرت و امنیت در عصر پسامدرنیسم***. گفتمان، شماره صفر.

رنجبر، مقصود. (۱۳۷۹). ***ملاحظات امنیتی در سیاست خارجی جمهوری اسلامی ایران***. تهران: پژوهشکده مطالعات راهبرد.ی

رابرت، ماندل. (۱۳۷۷). ***چهره متغیر امنیت ملی***. تهران: پژوهشکده مطالعات راهبردی.

محسنیان‌راد، مهدی. (۱۳۷۷) ***ارتباط جمعی در کشورهای اسلامی***. دانشگاه امام صادق، انتشار محدود.

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

محمدی، مجید. (۱۳۷۹) ***سیمای اقتدارگرایی تلویزیون دولتی ایران***. تهران: جامعه ایرانیان.

مولانا، حمید. (۱۳۷۹). ***جریان بین‌المللی اطلاعات***. ترجمهٔ یونس شکرخواه. تهران: مرکز مطالعات و تحقیقات رسانه‌ها.

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.

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

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