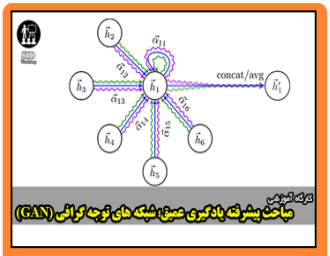
کارگاه های آموزشی مرکز اطلاعات علمی جهاد دانشگاهی

کارگاه آنلاین مکالمه روزمره انگلیسی

کارگاه آنلاین آموزش استفاده از وب آو ساینس



مباحث پیشرفته یادگیری عمیق؛
شبکه های توجه گرافی
(Graph Attention Networks)

قوانین، مقررات و راهکارهای تامین امنیت در شهر الکترونیکی

لیلا ناصری
کارشناس ارشد حقوق عمومی– جهاددانشگاهی استان مرکزی

چکیده

هسته اصلی زیرساختهای شهر الکترونیکی، اینترنت است که در ابتدا برای استفاده مشترک از اطلاعات طبقه‌بندی شده محققان ایجاد گردید. می‌دانیم که هرگونه فعالیت و خلاقیت شهروندان معلول ایمن بودن از هرگونه تعدی و تجاوزگری دیگران است و امنیت از حیات و فعالیت انسانها غیر قابل انفکاک است. مقوله امنیت به همان میزان که در جامعه واقعی مورد نیاز است، در فضای مجازی نیز تضمین کننده منافع و مطلوب‌های کاربران است. توسعه و پیشرفت کسب و کار در فضای مجازی بیش از هرچیز معلول وجود فضای ایمن و مصون از تعدی است و این مقوله امری است که مورد تائید همگان می‌باشد. بحث امنیت اطلاعات با امنیت ارتباطات در حریم خصوصی و حریم اجتماعی امنیت‌هایی که در جوامع مطرح می‌شود، گره می‌خورد. مساله حریم خصوصی و حمایت از داده نیز از جمله دغدغه‌های مهم کاربران و فعالان در فضای مجازی به ویژه متولیان و سیاستگذاران کسب و کار الکترونیکی است. زیرا اگر کاربران از مصون بودن حریم خصوصی و داده‌های شخصی خود در فضای مجازی اطمینان نیابند به فعالیت و کسب و کار در این عرصه تن در نخواهند داد. این وضعیت ناشی از آنست که میل به حفظ محرمانگی و مصونیت حریم خصوصی (به ویژه حریم خصوصی اطلاعاتی) از تمایلات نوع بشر است.

فناوریهای دفاع در برابر تهدیدکنندگان شبکه‌های رایانه‌ای با سرعت کمتری در حال توسعه است. آسیب‌پذیری‌ها بیشتر ناشی از وابستگی سایر بخشها به فناوری اطلاعات و سهولت استفاده از فناوری اطلاعات توسط گروهها و افراد تهدیدکننده فضای مجازی است. آسیب‌ها می‌تواند شامل از کارافتادن زیرساختهای اساسی، از کارافتادن خدمات اجتماعی، تهاجم فرهنگی، بحران اقتصادی مانند تعطیلی خدمات اجتماعی، تعطیلی بانکهای الکترونیکی و خریدوفروش از طریق شبکه باشد. درحقوق داخلی ما، قوانین مناسبی که بتواند در پیشگیری و مبارزه با این جنایت موثر باشد، کمتر دیده می‌شود و بیشتر قوانین، جوانب سنتی خود را حفظ کرده‌اند. بنابراین در این زمینه به تدوین قوانین مناسب و تقویت قدرت اطلاعاتی، امنیتی و اجرایی نیازمندیم.

واژگان کلیدی

امنیت، حریم خصوصی، داده، اطلاعات، شبکه، تدبیر پیشگیرانه.

۱- مقدمه

حمایت از جریان آزاد اطلاعات، گسترش روزافزون فناوری 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. به طور کلی، امنیت یکی از بنیادی‌ترین و اساسی‌ترین مواردی است که به سبب وجود سیستم‌های اطلاعاتی مختلف، امکان دسترسی‌های از راه دور به اطلاعات، اشتراک اطلاعات و وجود داده‌های محرمانه و حساس شهروندان و کسب و کارها در شهر الکترونیک، توجه مدیران و بانیان آن را از یک سو و شهروندان را به عنوان کاربران الکترونیکی این امکانات از سوی دیگر به خود جلب کرده است. این مهم زمانی تحقق می‌یابد که اطلاعات به صورت مطمئن، با صحت و سقم کامل و با حفظ امنیت و محرمانگی منتقل، نگهداری و یا در دسترس افراد قرار گیرد.

با توجه به ناشناس بودن کاربران و سهولت استفاده از اینترنت تجاوز به حریم خصوصی افراد به سرعت افزایش یافته و صاحب نظران و دولتمردان را در جهت حمایت از حریم خصوصی افراد سوق داده است. از اینرو ،این سوال به ذهن متبادر می‌شود که آیا برای پوشش دادن این دو دغدغه مهم فعالان کسب و کار الکترونیکی، تدوین قوانین و مقررات مستقل برای هریک از این دو حوزه ضروری است یا آنکه می‌توان با تدوین قوانین یک کاسه و واحد هر دو موضوع را تحت پوشش و حمایت قانونی قرار داد؟

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 جنبه 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.

در بسیاری از موارد، هزینه افشای اطلاعات و داده‌ها جبران ناپذیر است و در بسیاری موارد دیگر سازمان را متحمل ضررهای بسیاری می‌کند. مسائل امنیتی اغلب به سادگی دیگر بخشهای فن آوری اطلاعات، توجیه اقتصادی قابل لمس ندارند.

از اینرو، گرچه فضای سایبر ـ این پدیدهٔ شگفت‌انگیز قرن بیست و یکم ـ بسیاری از عرصه‌ها را با تحولات بنیادین مواجه کرده، سوء استفاده‌های فراوان از آن موجب پیش‌بینی تدابیر کیفری در این زمینه شده است. اما با توجه به مشکلات بسیاری که فراروی تدابیر کیفری وجود دارد، سیاست پیشگیری از وقوع این جرائم مناسب‌ترین تدبیر سیاست جنایی است .

از آنجا که امروزه با گسترش ابزارهای اطلاع رسانی و استفاده گسترده از اینترنت، حریم خصوصی به یکی از چالش انگیزترین مسائل حقوق بشر تبدیل شده، لذا در این مقاله سعی داریم به تحلیل و بررسی مقوله حریم خصوصی و امنیت داده، اطلاعات و شبکه پرداخته تا به نتیجه‌ای مطلوب جهت تدوین قوانین مناسب در زمینه مقوله‌های مذکور برسیم و در ادامه به پیشگیری وضعی به عنوان یکی از راهکارهای مناسب در کنار تدوین قانون اشاره می‌کنیم.

۲- تعریف مفاهیم

۲-۱- حریم خصوصی

حریم خصوصی با آنکه یکی از ملموس ترین و پرکاربردترین حق برای هر فردی شناخته شده، ولی صاحب نظران برجسته دنیا نتوانسته اند بر سر یک تعریف واحد به توافق برسند .ازاینرو، تعاریف مختلف از حریم خصوصی را می‌توان در شش دسته تقسیم بندی کرد :

۱- حق تنها ماندن .۲-دسترسی محدود دیگران به انسان و توانایی ایجاد مانع در برابر دسترسی‌های ناخواسته به انسان.۳- محرمانگی و پنهان ساختن برخی امور از دیگران.۴- کنترل بر اطلاعات شخصی. ۵-حمایت از شخصیت و کرامت انسان.۶- حق بر عالم صمیمیت انسان

۲-۲- امنیت

گفته شده که امنیت متشکل از دورکن است: ۱- صحت (حفظ تمامیت)۲-محرمانگی.

از این توصیف کوتاه می‌توان نتیجه گرفت که امنیت یک پدیده، یعنی از یکسو سلامت و تمامیت آن یا حقوق مترتب بر آن مورد تعدی قرار نگیرد. بعنوان مثال، رکن صحت در امنیت خانه یک شخص یعنی دیگری آن را مورد صدمه قرار ندهد (جرم علیه اموال) و همچنین کسی نتواند حقوق مالکانه مالک را مثلا از طریق سرقت اشیاء قیمتی آن، از او سلب کند (جرم علیه مالکیت). از سوی دیگر، امنیت یک پدیده، یعنی کسی بدون رضایت دارنده و صاحب اختیار آن پدیده بر آن وقوف نیافته و ابعاد آن برای دیگری مکشوف نگردد (مثلا بدون رضایت مال وارد خانه نشود).

دو رکن اساسی تشکیل دهنده فضای مجازی، شبکه (بعنوان کالبد و جسم این موجود) و داده‌ها (بعنوان روح و حیات جاری در این کالبد) می‌باشند، لذا هرگونه تعدی و تجاوزگری در فضای مجازی پیش از هرچیز نیازمند نقض امنیت یکی از ایندو یا به طریق اولی هردوی آنهاست. از سوی دیگر، هرچند آنچه در واقع در فضای مجازی جریان دارد، داده است و اطلاعات در واقع معنایی است که از داده افاده می‌شود (و هرچند اطلاعات به لحاظ مفهومی از داده استقلال دارد و بدون وجود داده، اطلاعات نیز وجود ندارد) اما بعضا خود اطلاعات، نیز در فضای مجازی مطلوبیت ذاتی یافته و امنیت آنها در معرض تهدید قرار می‌گیرد و لذا بحث از امنیت اطلاعات نیز ضرورت داشته و به دو شق پیشین افزوده می‌شود.

با لحاظ مقدمات فوق، می‌توان چنین نتیجه گرفت که با توجه به اینکه ارکان و عناصر سازنده فضای مجازی عبارتند از: داده، اطلاعات و شبکه و با توجه به اینکه در خصوص هریک از این سه عنصر نقض صحت (اعم از مالیت و مالکیت) و محرمانگی قابل تصور و تحقق می‌باشد، لذا برای وقوف به نسبت میان امنیت با حریم خصوصی در هریک از آنها بررسی مستقل صحت و محرمانگی هریک از آنها ضروری است:

۲-۲-۱- امنیت داده و حریم خصوصی

امنیت داده یعنی وضعیتی که طی آن اشخاص نسبت به هرگونه تعرض و تجاوز دیگران به داده‌هایی که مربوط به ایشان است، احساس مصونیت می‌کنند.

حریم خصوصی اطلاعاتی از یکسو به معنی منع سایرین از وقوف به داده‌هایی است که اختصاص به یک شخص دارد و از سوی دیگر به مفهوم منع دیگران از هرگونه تصاحب و تخصیص داده‌های این چنینی به خود و همچنین منع ایشان از تغییر و دست کاری کردن این گونه داده‌ها است.

بنا بر مراتب فوق، تردیدی باقی نمی‌ماند که در حوزه فناوری اطلاعات و ارتباطات، امنیت داده و حریم خصوصی (اطلاعاتی) دو اصطلاح مترادف و دارای مفهوم واحد می‌باشند. لذا هر جا سخن از مفهوم، اصول، قلمرو و نقض حریم خصوصی اطلاعاتی است، می‌توان از امنیت داده نیز سخن گفت و کلیه اعمالی که ناقض یکی تلقی می‌شوند، ناقض دیگری نیز می‌باشند. بعنوان مثال، افشای داده‌های مربوط به بیماری‌های شخص، تخلفی است که هم ناقض حریم خصوصی اطلاعاتی اوست و هم امنیت شخص را از جهت مصون ماندن از تعرض داده‌های شخصی (امنیت داده) او نقض نموده است.

در نتیجه کلیه قوانینی که برای حمایت از حریم خصوصی اطلاعاتی شهروندان وضع شوند، جملگی ناظر بر امنیت داده‌ها نیز می‌باشند و مآلا تدوین قوانین جداگانه برای این دو ضرورتی نخواهد داشت.

۲-۲-۲- امنیت اطلاعات و حریم خصوصی

مفهوم اطلاعات در معنی اخص خود با مفهوم داده تفاوت‌هایی دارد و اطلاعات به معنی، مفهومی است که از داده تحصیل می‌شود .

از منظر امنیت نیز، باید گفت که حفظ صحت (مالیت و مالکیت) اطلاعات و حفظ محرمانگی آنها تامین کننده امنیت اطلاعات است. یعنی اینکه اولا: اطلاعات شخصی یک فرد دچار تغییر و اصلاح غیر مجاز قرار نگرفته و اطلاعات نادرست تولید نشود، و ثانیا: اطلاعات شخصی افراد بدون مجوز قانونی تصاحب نشوند و ثالثا: بدون مجوز قانونی کسی مبادرت به افشاء یا وقوف بر آنها نکند. از منظر حریم خصوصی اطلاعاتی، آنچه بیش از همه مد نظر است صیانت از اطلاعات واقعی و صحیح منتسب به اشخاص است نه لزوما تامین و تضمین صحت اطلاعات.

از آنجا که نقض هریک از دو مولفه صحت و محرمانگی در خصوص اطلاعات ممکن است توام با نقض حریم خصوصی اطلاعاتی به مفهوم پیش گفته باشد یا نباشد، لذا در باب نسبت امنیت اطلاعات به مفهوم اخص کلمه با حریم خصوصی اطلاعاتی نمی‌توان قائل به انطباق کامل میان ایندو شد و نسبت آنها را تساوی تلقی نمود. بعنوان مثال، در حالی که هر گونه تحصیل و پردازش اطلاعات شخصی واقعی شهروندان در عین حال که نقض حریم خصوصی اطلاعاتی ایشان است، نقض امنیت اطلاعاتی (نقض محرمانگی) آنها نیز محسوب می‌شود، لیکن عکس این رابطه لزوما برقرار نیست و به عنوان مثال ایراد تهمت و افترا از طریق منتسب نمودن وصفی خاص به شخص (مثلا ارتکاب یک قتل) نقض امنیت اطلاعاتی شخص محسوب می‌شود (نقض صحت)، لیکن نقض حریم خصوصی اطلاعاتی شخص محسوب نمی‌شود. زیرا این اطلاعات واقعا به آن شخص انتساب ندارد تا افشای آن به این دلیل ممنوع باشد.

نتیجه اینکه برای پوشش دادن حریم خصوصی و امنیت در این دو حوزه نیازمند قوانین مجزا و جامع در هریک از این دو زمینه هستیم.

۲-۲-۳- امنیت شبکه و حریم خصوصی

اگر بخواهیم دو مولفه اصلی امنیت یعنی صحت و محرمانگی را در خصوص شبکه در نظر بگیریم، خواهیم دید که صحت آن منوط به عدم تخریب یا تصاحب تجهیزات آن از یکسو و از سوی دیگر عدم تعرض به جنبه‌های نرم افزاری آن که کارکرد صحیح و کامل آن را تامین می‌کند، بوده و محرمانگی آن نیز منوط به منع سایرین از ورود به حیطه‌های ممنوعه آن می‌باشد. لذا نسبتی میان این مفهوم از امنیت با حریم خصوصی اطلاعاتی وجود نداشته و با یکدیگر متباینند.

اما در باب شق دیگر امنیت، یعنی محرمانگی باید گفت که در مفهوم عام، هدفمند بودن و پیوند (اتصال) داشتن از مختصات اصلی شبکه می‌باشد که بدون آنها شبکه به مفهوم واقعی محقق نخواهد بود. برقراری اتصال به معنی امکان دستیابی دیگر مشترکان شبکه به داده‌هایی است که در بخش‌های اختصاصی شبکه قابل دستیابی می‌باشد و امکان دستیابی بالقوه برهم زننده امنیت در شبکه است.

کمال محرمانگی و مصونیت در شبکه زمانی حاصل می‌شود که همه اتصالات و کابل‌ها را قطع نمائیم. لیکن این امر از یکسو غیر ممکن است و از سوی دیگر نقض غرض می‌باشد، زیرا هدف از ایجاد

هرشبکه‌ای اتصال است. از این رو، منطقا نمی‌توان تمامی زوایای شبکه و داده‌های عرضه شده بر روی آن را به روی همگان مفتوح نمود و منع کاربران از ورود به بخش‌هایی از شبکه (از جمله بخش‌های امنیتی، داده‌های شخصی حساس، داده‌های مالی و....) اجتناب ناپذیر است.از سوی دیگر، محرمانگی شبکه به مفهوم امکان دسترسی افراد مجاز به شبکه نیز می‌باشد و هرگونه ایجاد اختلال در مسیر دسترسی کاربران مجاز نیز به نوعی مختل کننده امنیت می‌باشد.

لذا، می‌توان گفت که محرمانگی و امنیت شبکه دارای یک مفهوم ایجابی (امکان دسترسی افراد مجاز) و یک مفهوم سلبی (منع دسترسی افراد غیر مجاز) می‌باشد. براین اساس، در مقام ارائه یک تعریف ساده میتوان گفت که مولفه محرمانگی امنیت شبکه به معنی مصون بودن آن از هرگونه دسترسی غیر مجاز و مصون بودن از ایجاد مانع در جهت دسترسی مجاز می‌باشد.

از آنجا که بنا بر مراتب مذکور، منع برخی کاربران از دسترسی به برخی نقاط یک شبکه و تسهیل دسترسی برخی دیگر از کاربران امری لازم و البته اجتناب ناپذیر است و نادیده گرفتن این ممنوعیت‌های قانونی همواره بنا به دلائل مختلف برای عده‌ای مطلوبیت دارد، لذا امنیت شبکه امری است که نیازمند قاعده گذاری و تدوین مقررات است تا هم کاربران حدود آزادی‌ها خود و ضمانت اجراهای مترتب بر آن را بشناسند و هم دارندگان شبکه از ایمنی آن اطمینان نسبی حاصل کنند.

در خصوص نسبت میان دو مفهوم امنیت (صحت و محرمانگی) شبکه و حریم خصوصی می‌توان گفت اگر مقصود، مقایسه این مفهوم با حریم خصوصی اطلاعاتی باشد، نسبت میان ایندو از نسب اربعه تباین است. زیرا همانطور که گفته شد، داده‌ها به منزله روح و شبکه به منزله کالبد فضای مجازی می‌باشند و حریم خصوصی اطلاعاتی ناظر بر داده‌ها (روح) و امنیت شبکه ناظر بر کالبد (شبکه) است.

لیکن، در صورتی که مقصود مقایسه مفهوم امنیت شبکه با حریم خصوصی ارتباطاتی باشد، می‌توان گفت که رابطه میان این دو مفهوم از نسب اربعه عموم و خصوص مطلق می‌باشد. زیرا ارتباطات اعم است از ارتباطات شبکه‌ای و لذا امنیت ارتباطاتی از امنیت ارتباطات شبکه‌ای عام تر بوده و در نتیجه حریم خصوصی ارتباطاتی اعم از امنیت شبکه است.

در واقع، می‌توان گفت که هر ارتباطی که از طریق شبکه انجام می‌گیرد، نوعی از ارتباطات است. لیکن، همه اشکال ارتباطات از طریق شبکه صورت نمی‌گیرند.

بر این اساس، چنین نتیجه می‌گیریم که برای تدوین قواعد و مقررات تام و کامل برای تامین امنیت شبکه، اختصاص دادن بخشی از مقررات ناظر بر حریم خصوصی ارتباطاتی به این بحث ضرورت دارد و به لحاظ ابعاد فنی و پیچیدگی‌ها و ظرافت‌های خاص این حوزه نمی‌توان انتظار داشت که مقررات عام ناظر بر حریم خصوصی ارتباطاتی، تامین کننده امنیت شبکه به نحو مطلوب باشند.

در پایان، ذکر این نکته ضروری است که تفکیکی که میان مباحث مربوط به امنیت داده و امنیت شبکه در این قسمت ارائه شد، به معنی منفک و مجزا بودن تام و تمام این دو حوزه نمی‌باشد، بلکه برعکس، این دو حوزه در تعامل مستقیم و دائمی با یکدیگر هستند. زیرا غالبا به خطر افتادن امنیت شبکه و امنیت داده در فضای مجازی، لازم و ملزوم یکدیگرند.از همین رو، در اغلب تخلفات و جرائم اینترنتی ملاحظه می‌شود که عمل ارتکاب یافته همزمان ناقض امنیت شبکه و امنیت داده است و هماهنگی مقررات این دو حوزه را اقتضاء دارد.

ازجمله مواردی که عمل شخص در عین حال که امنیت شبکه را نقض می‌کند، ناقض امنیت داده‌ها نیز می‌باشد، می‌توان به موارد ذیل اشاره کرد: سرقت اینترنتی، کلاهبرداری اینترنتی، افترای عملی در فضای سایبر (ورود به سایت اختصاصی دیگری و قراردادن مطالب ممنوع بر روی سایت برای مجرم جلوه دادن او)، خرابکاری اینترنتی، جعل اینترنتی، تخریب داده‌ها از طریق اینترنت. با اینحال، مواردی وجود دارد که تنها نقض امنیت شبکه محسوب می‌شود، مثل نفوذ و جاسوسی اینترنتی و حمله‌های مختل کننده سیستم.. در مقابل، مواردی نیز وجود دارد که تنها نقض امنیت داده بوده و امنیت شبکه را نقض نمی‌کند. مثل، تحصیل داده‌های محرمانه و شخصی دیگری و تغییر دادن یا انتشار آنها بدون استفاده از شبکه.

۳- پیشگیری وضعی از جرم

یعنی ابزار و فرصت ارتکاب جرم را از مجرم سلب می‌کند. توجه به مثلث جرم می‌تواند به درک این موضوع کمک کند. برای ارتکاب یک جرم، سه عامل باید جمع شوند. مهم‌ترین آنها که قاعدهٔ مثلث جرم را هم تشکیل می‌دهد، انگیزهٔ مجرمانه است. انگیزه باعث بیدار شدن میل درونی در افراد و به تبع آن قصد مجرمانه می‌شود. برای

از بین بردن این عامل، ضروری است تدابیر پیشگیرانهٔ اجتماعی اتخاذ گردد. اما اگر به هر دلیل مجرمان واجد انگیزه شدند، باید از اجتماع دو ضلع دیگر این مثلث، یعنی فرصت و ابزار ارتکاب جرم جلوگیری کرد. از میان این دو، سلب فرصت از مجرمان اهمیت بیشتری دارد. زیرا متصدیان امر هرچه بکوشند ابزارهای ارتکاب جرم را از سطح جامعه جمع‌آوری کنند، باز هم مجرمان باانگیزه خواهند توانست به آنها دست یابند. هرچند در عین حال نباید اهمیت جمع‌آوری این ابزارها را در کاهش جرائم نادیده گرفت.

به هر حال، آنچه در پیشگیری وضعی از جرائم اولویت دارد، حفظ آماجها و بزه‌دیدگان از تعرض مجرمان است. (صفاری، ۱۳۸۰: ۲۹۲)در این زمینه، شیوه‌های مختلفی از سوی جرم‌شناسان ارائه شده که از مهم‌ترین آنها می‌توان به شیوه‌های دوازده‌گانهٔ کلارک، جرم‌شناس انگلیسی، اشاره کرد که آنها را در سه گروه چهارتایی قرار داده است :

۱-دشوار ساختن ارتکاب جرم از طریق: الف. حفاظت از آماجها و قربانیان جرم؛ ب.کنترل و ایجاد محدودیت در دسترسی به موقعیتهای جرم‌زا؛ ج. منحرف کردن مجرمان؛ د. برچیدن ابزار ارتکاب جرم.

۲-افزایش خطرپذیری مجرمان از طریق: الف. مراقبت از ورودیها و خروجیها؛ ب. مراقبت رسمی؛ ج. مراقبت غیررسمی؛ د. مراقبت طبیعی.

۳-کاهش جاذبه از آماجها و قربانیان جرم از طریق: الف. حذف آماجهای جرم؛ ب.علامت‌گذاری اموال؛ ج. تقلیل فرصتهای وسوسه‌انگیز؛ د. وضع قواعد خاص.

امروزه جرایم سایبری به حدی اوج گرفته که سازمان‌های بین المللی و منطقه ای، شورای حکام، پارلمان اروپا و... را به شدت درگیر کرده است، تا آنجا که سازمان ملل از کنگره هفتم به بعد به طور مرتب قطعنامه‌ای را در خصوص این جرایم و راهکارهای قانونی پیشگیری و مجازات آن داشته است.

۴- انواع تدابیر پیشگیری وضعی از جرائم سایبر

به طور کلی، تدابیر پیشگیرانهٔ وضعی از جرائم سایبر را می‌توان در چهار گروه بررسی کرد:

۴-۱- تدابیر محدودکننده یا سلب‌کنندهٔ دسترسی

این تدابیر، در زمرهٔ مهم‌ترین تدابیر پیشگیرانهٔ وضعی از جرائم سایبر قرار دارند که نمونه‌های اولیهٔ آن برای جلوگیری ازجرائم نسل اول نیز به کار می‌رفت. دراینجا سعی می‌شود با نصب سیستمها یا برنامه‌های خاص بر روی گرههای دسترسی به شبکه، یعنی کامپیوترهای شخصی، مسیریاب‌ها، سیستمهای ارائه‌دهندگان خدمات شبکه‌ای و از همه مهم‌تر ایجادکنندگان نقطهٔ تماس بین‌المللی، از ورود یا ارسال برخی داده‌های غیرمجاز یا غیرقانونی جلوگیری شود. این سیستم‌ها و برنامه‌ها عمدتاً در سه قالب دیوارهای آتشین، فیلترها و پراکسیها هستند. این ابزارها حاوی فهرستی از موضوعات مجاز یا غیرمجاز هستند و بر اساس فرایند انطباق عمل می‌کنند. بعضی از آنها مانند فیلترها و دیوارهای آتشین یک سویه عمل می‌کنند، یعنی فقط از ورودیهای غیرمجاز جلوگیری می‌کنند، اما بعضی دیگر دوسویه عمل می‌کنند و علاوه بر ورودیها، از خروجیها هم مراقبت می‌نمایند.

۴-۲- تدابیر نظارتی

نظارت شبکه‌ای شاید بیش از آنکه یک اقدام پیشگیرانه باشد، از لحاظ بازدارندگی مورد توجه قرار می‌گیرد. این اقدام به دو شکل فنی و انسانی قابل اجراست.

۴-۲-۱- در حالت فنی، ابزارها یا برنامه‌هایی بر روی سیستم نصب می‌شوند و کلیهٔ فعالیتهای شبکه‌ای اشخاص، حتی ضرباتی که بر روی صفحه کلیدشان زده‌اند یا نقاطی را که به وسیلهٔ ماوس بر روی آنها کلیک کرده‌اند ضبط می‌کنند. سپس مأمور مورد نظر می‌تواند با بررسی این سوابق، موارد غیرقانونی را تحت پیگرد قرار دهد. شایان ذکر است در صورتی نظارت شبکه‌ای اثر بازدارنده خواهد داشت که کاربر بداند فعالیتهایش تحت نظارت قرار دارد، زیرا همان‌طور که می‌دانیم، نظارت مخفی فقط برای جمع‌آوری ادله علیه متهم به کار می‌رود و هیچ اثر پیش‌گیرانه‌ای ندارد.

اکنون بسیاری از محیطهای گپ شبکه‌ای، به ویژه آنها که مورد اقبال قشر جوان و نوجوان است، تحت نظارت فنی یا زنده قرار دارند. اما مهم‌ترین مزیت این اقدام نسبت به اقدامات محدودکننده یا سلب‌کنندهٔ دسترسی این است که در عین اثرگذاری بازدارنده که پیشگیرانه نیز تلقی می‌شود، در فعالیت کاربران خللی ایجاد نمی‌کند و از این لحاظ اشکالی به وجود نمی‌آورد.

۴-۲-۲- در حالت انسانی، از جمله این تدابیر، نهاد پلیس سایبر به عنوان یک ضرورت ملی و بین المللی است که در ذیل به طور مختصر به آن اشاره می‌کنیم:

۴-۲-۲-۱- پلیس سایبر

در فضای سایبر، همانگونه که فعالیت‌ها سریع‌تر و ارزان‌تر انجام می‌شود، جرایم نیز پیچیده‌تر، سریع‌تر و کم‌هزینه‌تر است. به عنوان مثال در دنیای واقعی، محیط فیزیکی محدودیت‌ها و موانع بزرگی را برای مجرمان و تبهکاران ایجاد می‌کند؛ اما در فضای سایبر چنین موانع فیزیکی وجود ندارد.به دلیل ویژگی‌های خاص فضای سایبر، این فضا به قوانین کارآمد نیاز دارد. از سوی دیگر، اجرای قانون نیازمند سیستمی است که بر فعالیت‌های شبکه نظارت کند و به تعقیب و دستگیری مجرمان و امحای امور مجرمانه در محیط سایبر بپردازد. به چنین سیستمی، "پلیس سایبر "می‌گوییم.

۴-۲-۲-۲- ویژگی‌های پلیس سایبر

پلیس سایبر باید بتواند به ردیابی، شناسایی و ایجاد محدودیت برای مجرمان در فضای سایبر بپردازد. این امر مستلزم داشتن وجاهت قانونی، حرفه‌ای بودن و تسلط بر فنون نفوذگری و همچنین، داشتن ابزارهای پیشرفته عملیات در فضای سایبر و در نهایت نیازمند همکاری است.

دامنهٔ فعالیت پلیس سایبر، متناسب با گسترهٔ فضای سایبر، سرتاسر جهان است و احتمالاً در آینده، این پلیس زیر نظر سازمان ملل یا کشورهای غربی تشکیل خواهد شد. در صورتیکه فعالیت پلیس‌های دنیای واقعی به یک منطقهٔ جغرافیایی یعنی یک کشور محدود است. پلیس‌های دنیای واقعی اگرچه در سطح بین‌الملل با یکدیگر ارتباط دارند و پلیس بین‌الملل نیز وجود دارد، اما فعالیت‌های بین‌المللی آنها معمولاً تابع سیاست‌ها و روابط کشورها است.یکی از کارهایی که پلیس سایبر انجام می‌دهد، محدود کردن دامنهٔ فعالیت مجرمان در فضای سایبر است.

هم‌اکنون امکانی فراهم شده که آدرس‌های اینترنتی که از طریق آنها به فعالیت‌های خرابکارانه مثل ارسال ویروس، نفوذ غیرمجاز و ارسال پیغام‌های مزاحم می‌پردازند، شناسایی و هرگونه فعالیت از طریق این آدرس‌ها به شدت محدود شود. برای مثال، امروزه سرورهای پست‌الکترونیک به صورت خودکار با پلیس سایبر برای دریافت یا حذف پیغام‌های ورودی مشورت می‌کنند.

۴-۲-۲-۳- تجربهٔ سایر کشورها

پلیس سایبر با اسامی مختلفی چون پلیس شبکه، پلیس وب و غیره در کشورهای مختلف شکل گرفته است و حتی برخی کشورها این وظیفه را به تیم واکنش سریع به مشکلات رایانه‌ای واگذار کرده‌اند. از جمله کشورهای پیشرو در ایجاد پلیس سایبر می‌توان به آمریکا، فرانسه، چین، ژاپن، هند و کره اشاره کرد. کره تا قبل از سال ۲۰۰۰ فقط به جرایم رایانه‌ای اهمیت می‌داد، اما در این سال، تیم واکنش سریع به مشکلات رایانه‌ای را برای مقابله با جرایم سایبری ایجاد کرد. هند نیز اولین ایستگاه پلیس سایبر خود را در سال ۲۰۰۱ در بنگلور ایجاد کرد. پلیس سایبر هند وظیفه دارد با جرایم فضای سایبر از قبیل نفوذ غیرمجاز، خرابکاری اطلاعات و کلاهبرداری اینترنتی مقابله کند .ایجاد پلیس سایبر در هند در شرایطی است که این کشور در سال ۲۰۰۰ قانونی را برای مقابله با جرایم رایانه‌ای تصویب کرده بود.

۴-۲-۲-۴- تجربهٔ کشور ما

در کشور ما نیز چند سالی است که اداره کل مبارزه با جرایم رایانه‌ای در معاونت آگاهی نیروی انتظامی ایجاد شده است. پرواضح است که جرایم فضای سایبر محدود به جرایم رایانه‌ای نیست و ابزارها، نیروی انسانی و اختیارات خاص خود را می‌طلبد. پلیس سایبر قطعه‌ای از پازل گمشدهٔ توسعهٔ فناوری اطلاعات در کشور است. با توجه به این نکته که نیروی انتظامی مسئول برقراری نظم در جامعه است، این ارگان می‌تواند با در دست گرفتن ابتکار عمل و از دست ندادن فرصت‌ها، مسئولیت نظم و امنیت در این حوزه بزرگ اجتماعی را نیز بر عهده بگیرد. البته باید برای مقابله قانونی با جرایم فضای سایبر، قوانین لازم و شایسته تدوین گردد.

۴-۳- تدابیر صدور مجوز

در اینجا تلاش می‌شود بر اساس معیارهایی خاص، از ورود اشخاص ناشناس یا فاقد اعتبار جلوگیری شود. نمونهٔ سادهٔ این اقدام، به کارگیری گذرواژه است که در گذشته و اکنون جایگاه خود را حفظ کرده است. به این ترتیب، تنها کسانی حق بهره‌برداری از یک سیستم یا سایت را خواهند داشت که پس از طی مراحل شناسایی و کسب اعتبار لازم، گذر واژهٔ مربوط را دریافت کنند. ممکن است این مجوز بر اساس سن، جنس، ملیت، مذهب یا

گرایشهای خاص فکری داده شود. امروزه در این حوزه پیشرفتهای بسیاری صورت گرفته است.

به عنوان مثال، برای ارتقای هرچه بیشتر امنیت، چندی است از شیوه‌های بیومتریک نیز استفاده می‌شود. یعنی به جای یا علاوه بر گذرواژه، از اسکن عنبیه یا شبکیهٔ چشم یا اثر انگشت نیز برای شناسایی فرد استفاده می‌شود تا ضریب خطا به حداقل برسد.

به نظر می‌رسد تدابیر این حوزه نسبت به دو حوزهٔ دیگر ایرادات اساسی ندارد، اما خالی از اشکال هم نیست و حداقل به دو نقص مهم آن می‌توان اشاره کرد:

۱- نسبت به تمامی حوزه‌های فضای سایبر قابل اجرا نیست و موارد استفادهٔ آن بسیار محدود است. ۲- این ایراد که البته راجع به دیگر ابزارهای پیشگیرانه نیز صادق است، به پیشرفت لحظه‌شمار فناوریهای موجود در فضای سایبر مربوط می‌شود. ممکن است یک سیستم اکنون با بهره‌گیری از ابزارهای صدور مجوز، از ایمنی قابل قبولی برخوردار باشد، اما به نظر نمی‌رسد هیچ متخصصی بتواند این ایمنی را تا مدت مشخصی تضمین نماید، زیرا این فناوری در معرض آزمون و خطای هزاران نفر از سراسر جهان قرار دارد و به زودی نقاط ضعف آن کشف می‌شود.

۴-۴- ابزارهای ناشناس‌کننده و رمزگذاری

این دو اقدام تا حدی از لحاظ کارکرد با یکدیگر تفاوت دارند، اما از آنجا که یک هدف را دنبال می‌کنند، در اینجا با هم بررسی می‌شوند. همان گونه که از این اصطلاحات پیداست، این ابزارها ماهیت اصلی یک مفهوم را پنهان یا غیرقابل درک می‌کنند تا غیرقابل شناسایی و تشخیص گردد. ناشناس‌کننده‌ها هویت اشخاص را در فضای سایبر پنهان می‌کنند و از این طریق به آنها امکان می‌دهند با ایجاد حریم بیشتر به فعالیت شبکه‌ای بپردازند. این اقدام به ویژه برای زنان و کودکان یا به طور کلی اشخاصی که به هر دلیل آسیب‌پذیرند، سودمند است، زیرا بی‌آنکه فرصت شناسایی خود را به مجرمان سایبر بدهند، می‌توانند به فعالیتهای شبکه‌ای بپردازند.

اما از ابزارهای رمزنگاری بیشتر برای محتوای ارتباطات استفاده می‌شود. در اینجا بر اساس کدهای خاصی متن اصلی به رمزنوشته تبدیل می‌شود و گیرنده در مقصد به وسیلهٔ کلیدی که در اختیار دارد، آن را رمزگشایی می‌کند. متأسفانه ابزارهای متنوع و بسیاری در فضای سایبر برای شنود و دستیابی به ارتباطات افراد وجود دارد که بهره‌گیری از برنامه‌های رمزنگاری می‌تواند خطر این گونه تعرضات را کاهش دهد.

با این حال، نباید از یاد برد که امکان استفاده از این ابزارها برای مجرمان نیز وجود دارد. آنها با پنهان کردن هویت یا رمزنگاری محتوای مجرمانهٔ ارتباطاتشان، امکان شناسایی خود را کاهش می‌دهند. لذا این گزینه نسبت به سه تدبیر پیشگیرانهٔ قبل از این ضعف برخوردار است که در کنار از بین بردن برخی از فرصتهای ارتکاب جرم، زمینهٔ ارتکاب ایمن برخی دیگر از جرائم را هم فراهم می‌آورد.

۵- نتیجه

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. 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.

گرچه 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.

لازم است برای حفظ امنیت شهر الکترونیکی افراد اقداماتی چون راهکارهای قانونی، خود مقررات گذاری، مقررات گذاری‌های مشترک، تامین منابع مالی برای طرح‌های پژوهشی مربوط به فنون جدید رمزگذاری و ناشناختگی صورت گیرد .اما دراین میان تشویق شهروندان به مشارکت فعالانه در فرایند تصمیم گیری چه در مرزهای ملی و چه بین المللی می‌تواند در حفاظت از این حریم کار سازتر باشد.

پیشرفت فناوری، نیروی جوان تحصیل کرده، بیکاری تحصیل کردگان، بی ثباتی سیاسی و اقتصادی، فقدان قوانین و وجود خریداران ثروتمند برای خدمات مجرمان سایبری زمینه‌های اجتماعی گسترش جرایم سایبری را تشکیل می‌دهد .

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. 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.

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.

جرایم رایانه‌ای و شبکه‌ای از حیث تعقیب و دادرسی نیز با چالش و تحول مواجه می‌باشد .آئین دادرسی کیفری می‌بایستی به حمایت از آزادیهای مدنی و مظنونین و شهود بپردازد و در زمینه تعقیب بین المللی جرایم می‌بایست بر مبنای تعاون و همکاری بین المللی با رعایت اصول حاکمیت و امنیت کشور مقابل صورت گیرد .

به نظر می‌رسد برای یک استراتژی جامع امنیت داده پردازی و کنترل جرم راه حل قانونی بایستی توسط ابزارها و تدابیر فراقضایی همچون تدابیر امنیتی اختیاری توسط کاربران رایانه به کار گرفته شود .ضمن اینکه اجرای تدابیر امنیتی و جلوگیری از جرایم باید با توسعه تکنولوژی همگام باشد.

برای سالم‌سازی فضای سایبر دو دسته اقدام باید صورت گیرد: یک دسته "اقداماتی برای دوران گذر "از قبیل: ایجاد تنوعی از دسترسی‌ها برای کاربران خاص و استفاده خاص، بازنگری در فهرست سیاه آدرس‌ها، بازنگری و محدودسازی فهرست کلید واژگان و در نهایت حذف این روش، تهیه برنامه‌های آگاه‌سازی و آموزش‌های تلویزیونی به کاربران و خانواده‌ها، آگاهی دادن به شرکتها و ادارات در خصوص قابلیت خطر پذیری سیستم‌های رایانه‌ای و تشویق آنان به بکارگیری تدابیر امنیتی.

دسته دوم "اقداماتی برای ایجاد شرایط ایده‌آل" مثل: نهادسازی برای ایجاد یک مرکز فرماندهی سیاستگذاری و اجرا برای سالم‌سازی، مطالعات مستمر رفتار کاربران، ترغیب و تسهیل بروز انگیزش‌های مشروع و سودمند، تولید محتوای فارسی و پشتیبانی فنی از محتوای فارسی، ضمانت اجراهای غیرکیفری (اداری) علیه ارائه‌دهندگان خدمات متخلف، ضمانت اجراهای کیفری علیه جرایم سایبری (تولیدکنندگان محتوای غیرمجاز)، کاهش موقعیت‌های جرم زا و فرصت‌های استفاده از ابزار فنی در ارتکاب جرم، تشویق بزه دیدگان به اعلام وقوع جرم، اتخاذ استراتژی فرهنگی کلان در مورد صنایع فرهنگی جدید، اتخاذ سیاست ملی مخابراتی یعنی اولویت‌بندی در مورد گسترش تلفن ثابت، همراه و مخابرات داده‌ها و تعیین میزان ظرفیت دولت در پذیرش مشارکت بخش خصوصی در وارد کردن و توزیع اینترنت، اتخاذ سیاست روشن گمرکی در مورد مجاز یا ممنوع بودن واردات تجهیزات، دریافت و ارسال ماهواره‌ای برای خدمات اینترنت، اتخاذ سیاست ملی اطلاع‌رسانی، اتخاذ سیاستهای نظارتی و امنیتی(بعبارتی 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 تولید شده و قابل دسترس در کشور است؟)، تاسیس رسمی پلیس سایر در نیروی انتظامی، برنامه ریزی پلیس سایبر برای مقابله با جرایم طبق اولویتی مشخص، گسترش پلیس سایبر در مراکز استان‌ها و سایر نقاط کشور، تأکید پلیس سایبر بر مبارزه با تروریست‌ها و تهدیدکنندگان خارجی و داخلی فضای سایبر ملی و نهایتا همکاری آگاهانه و فعالانه پلیس سایبر ملی با کشورهای دیگر.

مراجع

[۱]- بوزان، باری. مردم، دولتها و هراس. تهران: پژوهشکده مطالعات راهبردی. ۱۳۷۸.

[۲]- تاجیک، محمدرضا. قدرت و امنیت در عصر پسامدرنیسم. گفتمان، شماره صفر. ۱۳۷۷.

[۳]- رنجبر، مقصود. ملاحظات امنیتی در سیاست خارجی جمهوری اسلامی ایران. تهران: پژوهشکده مطالعات راهبردی. ۱۳۷۹.

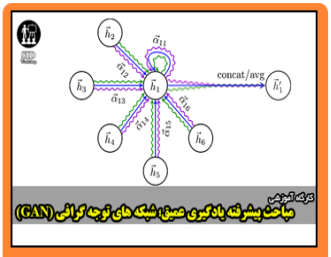
[۴]- رابرت، ماندل. چهره متغیر امنیت ملی. تهران: پژوهشکده مطالعات راهبردی. ۱۳۷۷.
[۵]- محسنیان‌راد، مهدی. ارتباط جمعی در کشورهای اسلامی. دانشگاه امام صادق، انتشار محدود. ۱۳۷۷.
[۶]- محسنیان‌راد، مهدی. انتقاد در مطبوعات ایران. مرکز مطالعات و تحقیقات رسانه‌ها، انتشار محدود. ۱۳۷۶.
[۷]- محمدی، مجید. سیمای اقتدارگرایی تلویزیون دولتی ایران. تهران: جامعه ایرانیان. ۱۳۷۹
[۸]- مولانا، حمید. جریان بین‌المللی اطلاعات. ترجمهٔ یونس شکرخواه. تهران: مرکز مطالعات و تحقیقات رسانه‌ها. ۱۳۷۹.
[۹]-بروجردی، مهدخت. حریم خصوصی در جامعه اطلاعاتی. www.bashgah.net
[۱۰]- لوراستین و نیکیل سینا، رسانه‌های نوین جهانی و سیاستگذاری ارتباطات، نقش دولت در قرن ۲۱ .ترجمه لیدا کاووسی، فصلنامه رسانه، سال پانزدهم، شماره ۲، ص ۱۳۰.
[۱۱]- هلن نیس بام، حمایت از حق خلوت آدمیان در عصر اطلاعات، ترجمه عباس ایمانی، مجله پژوهشها، پاییز و زمستان۸۱، ص ۹۹.
[۱۲]- کارل هارلو، شبه جرم، مترجم کامبیز نورزوی، چاپ اول، تهران :نشر میزان بهار ۸۳.ص ۱۶۶ .
[۱۳] -هاناآرنت، توتالیستاریسم، ترجمه محسن ثلاثی، تهران.انتشارات جاویدان، ۱۳۶۶ .ص ۲۲۹ .
[۱۴] -مارک روتنبرگ، حفظ حریم شخصی در جامعه اطلاعاتی، چالشهای حقوقی اخلاقی و اجتماعی فضای رایانه‌ای به کوشش بابک دربیگی، چاپ دوم بهمن۸۰، نشر خانه کتاب، ص ۱۶۱ .
[۱۵] -بیانیه اصول اجلاس عالی سران درباره جامعه اطلاعاتی /۱۲ دسامبر ۲۰۰۳، :ش سندWSIS: ۳/ doc/ genevae/ ۴ E.
[۱۶] -گارن کوهن، اینترنت و مسائل نظارتی بین المللی -چالشهای حقوقی و اطلاعاتی و اجتماعی، فصلنامه رایانه ای، چاپ دوم بهمن ۸۰، نشر خانه کتاب، ص ۳۷ .
[۱۷] -محسنی منوچهر، جامعه شناسی جامعه اطلاعاتی، موسسه انتشارات آگاه، چاپ اول، ۸۰ ص ۷۷ .
[۱۸] -فرانسس کار نکراس، زوال فاصله ها،چگونه انقلاب ارتباطات زندگی ما را تغییر خواهد داد،مترجم نصرا ..جهانگرد و همکاران .تهران : شورای عالی اطلاع رسانی، چاپ اول ۸۴، ص ۱۵۷ .
[۱۹] -اجلالی، علی اکبر، شهر الکترونیک، انتشارات دانشگاه علم و صنعت ایران، چاپ اول، ۸۲، ص ۵۷ .
[۲۰] -کدخدایی عباسی، همان .
[۲۱] -جان ون دایک، سیاست گذاری در جامعه شبکه ای، ترجمه پیروز ایزدی، فصلنامه رسانه، سال پانزدهم، شماره۲، ص ۱۱۱ .
[۲۲] -دنیس مک کوئیل، سیاستگذاری‌های رسانه ای، ترجمه مریم بنی هاشمی، فصلنامه رسانه همان، ص ۴۳ .
[۲۳]ـ فاطمه، مطلبی ،استفاده از نهان نگاری برای حفاظت از حقوق نشر دیجیتال، ماهنامه مخابرات و ارتباطات،سال چهارم،شماره ۴۰،مرداد۱۳۸۶.
[۲۴]ـ دیوید جی پست، هرج ومرج، دولت واینترنت، جستاری در باب قانون گذاری در فضای شبکه ای، ترجمه پرویزعلوی، فصلنامه علمی ـ پژوهشی دانشگاه آزاد اسلامی واحد آشتیان، پیش شماره ۱، پاییز ۱۳۸۵
[۲۵]- پرویزی، رضا. جرائم کامپیوتری و اینترنتی، نشریه آسیا.۱۳۸۱.
[۲۶]- دانش کیا، ماهرخ. گسترش جرائم اینترنتی و رایانه ای، نشریه صدای عدالت. ۱۳۸۳.
[۲۷]- حاتمی، سوگل. اجرای طرح ویزه مبارزه با جرایم رایانه‌ای، روزنامه جهان اقتصاد. ۱۳۸۵
[۲۸]- دنیای اقتصاد. پیشگیری یا برخورد گفتگو با رضا پروزی دبیر کمیته مبارزه با جرائم رایانه‌ای و اینترنتی.۱۳۸۱.
[۲۹]- دیداری، اکرم. جنگ آخر، جرائم رایانه‌ای ۶۴ در صد رشد سالانه، نشریه دنیای اقتصاد. ۱۳۸۱
[۳۰]- خبر گزاری‌های خارجی (خبرهایی پیرامون سوء استفاده ار اینترنت در جهان، پیدایش صنعت ۲۰ میلیار دلاری و ...) واحد مرکزی خبر، ۱۳۸۵.
[۳۱]- شهریاری ،حمید .اخلاق فناوری اطلاعات، ره آورد نور. شماره ۷.

[32]-Sick, Gary. Middle East Studies Association Bulletin, December, 1999.
[33]-Us Dept of State 2000. A National security Strategy for a new centry, 2000.
[34]-Tehranian, Majid. Global Communication and World Politics:

کارگاه های آموزشی مرکز اطلاعات علمی جهاد دانشگاهی

کارگاه آنلاین مکالمه روزمره انگلیسی

کارگاه آنلاین آموزش استفاده از وب آو ساینس



مباحث پیشرفته یادگیری عمیق؛ شبکه های توجه گرافی (Graph Attention Networks)