دوره ۴۸، شماره ۱، بهار و تابستان ۱۳۹۷
صفحات ۲۷ تا ۴۶

پیشگیری اجتماعی از جرایم امنیتی - سایبری

حمید بهره‌مند*
استادیار دانشکده حقوق و علوم سیاسی دانشگاه تهران
ذوالفقار داودی
دانش‌آموخته کارشناسی ارشد حقوق جزا و جرم‌شناسی دانشگاه اصفهان
(تاریخ دریافت: ۱۳۹۶/۵/۳ - تاریخ تصویب: ۱۳۹۷/۳/۲۸)

چکیده

بی‌گمان گسترش و نفوذ فناوری‌های اطلاعات و ارتباطات و در پی آن پدیدار شدن فضای سایبر، تغییرات اساسی را در تمامی ابعاد زندگی آدمی و ازجمله امنیت ملی جوامع ایجاد کرده است. فضای مجازی با برخورداری از ویژگی‌های منحصربه‌فرد، با توسل به فناوری تبادل اطلاعات امنیت ملی را با چالش‌های جدید و جدی مواجه کرده که صیانت از آن به شیوهٔ سنتی دشوار و ناکافی است. هرچند مقابلهٔ کیفری در خصوص این جرایم اجتناب‌ناپذیر است، با توجه به واکنشی بودن این اقدام و اتخاذ آن پس از ارتکاب، نمی‌توان آثار سوء این جرایم را خنثی کرد. ازاین‌رو لازم است اقداماتی را موردتحقیق قرار داد که به‌جای واکنش به این جرایم، از وقوع آنها پیشگیری کند. به‌نظر می‌رسد با توجه به ایرادات پیشگیری وضعی که به‌کلی مانع از ارتکاب جرایم نمی‌شود، بلکه هزینهٔ آنها را افزایش می‌دهد و موجب جابه‌جا شدن سیبل مجرمانه می‌شود، سیاست جنایی پیشگیرانه، بتواند راهبرد مؤثرتری برای مقابله با این تهدیدات نوین به‌شمار رود. این مقاله با روش توصیفی- تحلیلی ضمن شناسایی مفهوم و مصادیق جرایم امنیتی - سایبری به بررسی برنامه‌های پیشگیرانهٔ اجتماعی برای رویارویی با جرایم سایبری علیه امنیت ملی می‌پردازد و بدون آنکه تأثیر سایر اقدامات پیشگیرانه را به‌کلی نفی کند، برنامه‌های پیشگیرانهٔ اجتماعی را پیشنهاد و آثار مثبت آنها را معرفی می‌کند. در این میان می‌توان به برنامه‌های خانواده‌مدار، تدابیر آموزشی - سایبری، بالا بردن سواد رسانه‌ای، تنظیم کدهای رفتاری، اطلاع‌رسانی و اطلاع‌گیری، توجه به حکمرانی خوب و شاخص‌های آن، مشارکت و اجماع‌گری، ارتقای پاسخگویی و شفافیت، فرهنگ‌سازی و تولید رسانه‌ای اشاره کرد.

کلید واژگان

پیشگیری اجتماعی، جرایم امنیتی - سایبری، حکمرانی خوب، فضای سایبر، کدهای رفتاری.

* bahrmand@ut.ac.ir

مقدمه

یکی از موضوعات بی‌نظیر بشر که زندگی او را در تمامی شئون فردی و اجتماعی با تحولات گسترده‌ای مواجه کرده، رایانه و فضای سایبری است. محتوای سامانه‌های رایانه‌ای را اطلاعات تشکیل می‌دهد. امروزه این اطلاعات به‌حدی زندگی بشر را تغییر داده و الگوی گسستی را در بنیاد اقتصاد، جامعه و فرهنگ ایجاد کرده است که از آن به‌عنوان شاخص مستقلی برای تعریف عصر جدیدی در تاریخ تحولات بشر یاد می‌شود. البته ورود به این دوره، به معنای از بین رفتن کامل نظم گذشته نیست؛ دنیای جدید با دنیای قدیم همپوشانی دارد و قدرت در آن همچنان به نهادهای مبتنی بر جغرافیا وابسته است (روزنا و سینگ،[1] ۱۳۹۱: ۳۷).

فضای سایبری روزبه‌روز در حال پیشرفت و گسترش است و در کنار دستاوردهای مفیدی که برای بشر داشته، مشکلاتی نیز برای وی به ارمغان آورده است؛ ازجمله دستاویزی برای اعمال جرایم علیه امنیت ملی کشورها شده است. بحث پیشگیری از امنیت ملی در فضای سایبر ازآن‌رو اهمیت مضاعف دارد که تهدیدها علیه امنیت ملی در این فضا با امکانات پیچیده و خیره‌کننده‌ای چون فناوری اطلاعات یا فناوری هسته‌ای به نسبت تهدیدات گذشته متنوع شده و دولت‌ها را در مسیر پرمخاطره‌ای قرار داده است. امروزه دیگر امنیت ملی فقط با جنگ یا کودتا نمی‌شکند که دفاع نظامی در برابر آن لازم آید، بلکه با تهدیدهای متنوع و ناملموسی سست و لرزان می‌شود که صیانت از آن از عهدهٔ آرایش نظامی خارج است، در عوض به‌نظر می‌رسد اقدامات پیشگیرانه و به‌خصوص پیشگیری اجتماعی ــ نظر به ویژگی‌های خاص این جرایم ازجمله پنهان و پوشیده بودن و بین‌المللی بودن ــ می‌تواند مؤثرترین راه برای مقابله با این تهدیدات نوین به‌شمار رود.

در تقسیم‌بندی‌های جدید به‌عمل‌آمده از اقدامات پیشگیرانه، پیشگیری به اجتماعی و وضعی تقسیم‌بندی شده است (محمدنسل، ۱۳۹۳: ۵۴). پیشگیری اجتماعی شامل مجموعه اقدامات پیشگیرانه از جرایم است که به دنبال حذف یا خنثی کردن آن دسته از عواملی است که در تکوین جرم مؤثر است. این نوع پیشگیری بر مبنای علت‌شناسی جرایم استوار است و با دخالت در محیط‌های اجتماعی مانع از شکل‌گیری رفتارهای بزهکارانه و خنثی‌سازی عوامل جرم‌زا می‌شود. به‌عبارت دیگر، پیشگیری اجتماعی از جرم راهبردی است که برخورد با علل ریشه‌ای اقدامات مجرمانه و بزه‌دیدگی را مدنظر قرار می‌دهد (Grant, 2015: 5). این نوع پیشگیری در پی تغییر انگیزه‌های جنایی است و برخلاف پیشگیری وضعی به‌جای اشیا به افراد در محیط اجتماعی توجه می‌کند (Gilling, 1997: 4).

پیشگیری اجتماعی با ایجاد تغییرات و اصلاحات در محیط اجتماعی عمومی و شخصی فرد در پی جلوگیری از جرم به‌صورت پایدار و همیشگی است. پیشگیری مزبور، درصدد است اعضای جامعه را از طریق آموزش، تربیت، تشویق و تنبیه با قواعد اجتماعی آشنا و هم‌نوا کند. به دیگر سخن،

1. Rosenau & sink

رویکرد پیشگیری اجتماعی، تقویت روابط اجتماعی، افزایش سطح کنترل غیررسمی و درنتیجه بازدارندگی بالقوه و بالفعل از ارتکاب جرم است (محمدنسل، ۱۳۹۳: ۶۷).

در این مقاله دو پرسش مورد توجه قرار خواهد گرفت: ۱. مفهوم و مصادیق جرایم امنیتی‌ـ سایبری چیست؟ ۲. چه اقداماتی را می‌توان برای پیشگیری از این جرایم اتخاذ کرد؟ ازاین‌رو با روشی توصیفی ـ تحلیلی ابتدا مفهوم جرایم امنیتی ـ سایبری و مصادیق آنها بیان و سپس برنامه‌های پیشگیری اجتماعی جهت جلوگیری از این جرایم و اقسام این برنامه‌ها معرفی می‌شود.

۱. شناسایی جرایم امنیتی – سایبری

۱-۱. مفهوم‌شناسی

فرهنگ علوم سیاسی امنیت ملی را چنین تعریف می‌کند: امنیت ملی عبارت است از احساس آزادی کشور در تعقیب هدف‌های اساسی و فقدان ترس و خطر جدی نسبت به منافع سیاسی، اساسی و حیاتی کشور (آقابخشی، ۱۳۶۳: ۱۷۳). امنیت ملی - سایبری یکی از دسته‌بندی‌های امنیت ملی است که با معیار فضای سایبری سنجیده می‌شود. امنیت ملی در فضای سایبر منوط به امنیت اطلاعات است و تا زمانی‌که امنیت اطلاعات مخدوش نشود، امنیت ملی نیز تهدید نمی‌شود. جرایم علیه امنیت ملی در این فضا را می‌توان چنین تعریف کرد: هرگونه «تجاوز یا هنجارشکنی یا تهدید نسبت به یکی از پنج موضوع داده‌ها و اطلاعات، شبکه‌ها و سیستم‌های رایانه‌ای و مخابراتی، کاربران و مشترکان اینترنتی، ارائه‌دهندگان خدمات اینترنتی و نهایتاً موضوعات بیرون از محیط سایبر که مرتکب باواسطه محیط سایبر درصدد تجاوز به آن برمی‌آید» (عالی‌پور، ۱۳۹۲: ۷).

۱-۲. مصادیق جرایم امنیتی – سایبری

برای جرایم رایانه‌ای دسته‌بندی‌های مختلفی پیشنهاد شده است که مشهورترین آن، براساس نقش رایانه صورت گرفته و با توجه به اینکه در اینجا این رایانه است که مفهوم و مصادیق جرم را در فضای سایبر دگرگون ساخته، دسته‌بندی نیز با محوریت نقش آنها ارائه شده است. در بیشتر نوشته‌ها، بزه‌های رایانه‌ای را بزه‌هایی دانسته‌اند که در تحقق آنها، رایانه و فضای سایبر یا نقش موضوع جرم دارد یا نقش وسیلهٔ جرم. در اولی یعنی موضوع جرم، رایانه نقش منفعل و پذیرا دارد و موضوع رفتار مجرمانه قرار می‌گیرد، اما در وسیلهٔ جرم نقشی فعال دارد و جرم با کمک آن ارتکاب می‌یابد» (عالی‌پور، ۱۳۹۳: ۱۴۶ـ ۱۴۵). در این مقاله با توجه به این تقسیم‌بندی، به برخی جرایم علیه امنیت در فضای سایبر اشاره می‌شود.[۱]

---

۱. شایان ذکر است در ادبیات حقوق کیفری، نگارندگان بیشتر تمایل دارند از عناوینی مانند جاسوسی رایانه‌ای که در قانون به‌کار رفته است، استفاده کنند (برای مثال، ر.ک.: محمدنسل، ۱۳۹۵: ۴۰) و استفاده از عناوینی چون جرایم امنیتی ـ سایبری کمتر به‌کار می‌رود.

۱-۲-۱. جرایم امنیتی ـ سایبری با استفاده از فضای سایبر

معیار وسیله‌محور جرایمی را بررسی می‌کند که در آن «رایانه و فضای سایبر به‌عنوان ابزاری برای ارتکاب جرم در نظر گرفته می‌شود نه هدف» (Dashora, 2011: 241). این دسته از جرایم می‌تواند شامل همهٔ جرایمی که امنیت ملی را در فضای فیزیکی تهدید می‌کند، شود. در ادامه برخی از مصادیق جرایم علیه امنیت ــ که اغلب جرایم سنتی‌اند ــ با توجه به محیط سایبر بررسی می‌شود.

۱-۱-۲-۱. فعالیت‌های تبلیغی علیه نظام

ضرورت صیانت از کلیت نظام حکومتی و ارزش‌های آن سبب شده است در برخی کشورها فعالیت تبلیغی علیه نظام، با ضمانت اجرای کیفری روبه‌رو شود. پیش از انقلاب اسلامی، در ایران هرگونه تبلیغ در مقام ضدیت با سلطنت مشروطه یا حمایت از مرام و رویهٔ اشتراکی، یا تبلیغ به نفع مجرمان چنین جرایمی طبق مادهٔ ۵ قانون مجازات مُقدِمین علیه امنیت و استقلال مملکت (مصوب ۱۳۱۰)، جرم و قابل مجازات اعلام شده بود. پس از انقلاب اسلامی با تصویب قانون تعزیرات سال ۱۳۶۲، از سوی قانونگذار در زمینهٔ تبلیغ علیه نظام جرم‌انگاری صورت نپذیرفت. اما از سال ۱۳۷۵ و با تصویب قانون تعزیرات جدید، قانونگذار در قالب مادهٔ ۵۰۰ قانون مجازات اسلامی که در واقع رکن قانونی تشکیل‌دهندهٔ جرم است، انجام هرگونه فعالیت تبلیغی علیه نظام جمهوری اسلامی ایران یا به نفع گروه‌ها و سازمان‌های مخالف نظام را جرم دانسته و برای آن مجازات تعیین کرده است. امروزه با گسترش شبکه‌های ارتباطی انجام دادن جرم فعالیت تبلیغی علیه نظام بسیار سهل شده است و افرادی می‌توانند با استفاده از سایت‌ها و شبکه‌های اجتماعی رایگان اقدام به تبلیغات سوء علیه مقدسات اسلامی و نظام می‌کنند.

۲-۱-۲-۱. تشکیل جمعیت، دسته، گروه در فضای سایبر با هدف برهم زدن امنیت کشور

در فضای سایبر گروه‌ها، انجمن یا اتاق گفت‌وگوی مجازی یک سرویس مجانی است که برخی از سایت‌ها در اختیار بازدیدکنندگان خود قرار می‌دهند که از طریق آنها افراد می‌توانند جمعیت، دسته و گروه تشکیل دهند. به‌این‌ترتیب، امکان تحقق جرم تشکیل یا ادارهٔ جمعیت، دسته، گروه با هدف برهم زدن امنیت کشور از طریق امکانات رایانه‌ای، امری ممکن و آسان است؛ برای نمونه بارز گروه تکفیری ــ تروریستی داعش است که توانسته با استفاده از امکانات فضای سایبری هزاران نفر را از کشورهای مختلف جهان جذب کند و به‌منظور اهداف خود آموزش دهد و به‌کار رود. همچنین با گسترده شدن استفادهٔ کاربران فضای سایبری از شبکه‌های اجتماعی، تشکیل چنین گروه‌هایی به‌سادگی ممکن شده است. عنصر قانونی این جرم مادهٔ ۴۹۸ قانون مجازات اسلامی قسمت تعزیرات است که مقرر می‌دارد: «هر کس با هر مرامی، دسته، جمعیت یا شبه‌جمعیتی بیش از دو نفر در داخل یا خارج از کشور تحت هر اسم یا عنوانی تشکیل دهد یا اداره کند که هدف آن برهم زدن امنیت کشور باشد و محارب شناخته شود به حبس از دو تا ۱۰ سال محکوم می‌شود». در این ماده

دو جرم پیش‌بینی شده است: اولاً جرم تشکیل گروه جمعیتی که هدفش برهم زدن امنیت کشور است و ثانیاً جرم ادارهٔ گروه جمعیتی که هدفش برهم زدن امنیت کشور باشد.

۲-۲-۱. جرایم امنیتی ـ سایبری علیه فضای سایبر

جرایم رایانه‌ای در این دسته، جرایمی‌اند که در آن خود رایانه مورد هدف قرار می‌گیرد و موضوع رفتارهای مجرمانه است. این دسته، بزه‌های هستند که جدیدند و واقعیت جدید دارند. روی‌هم‌رفته می‌توان دو تهدید برجستهٔ امنیتی را برشمرد که در قانون‌های کیفری ایران چه به‌طور روشن و چه به‌طور پوشیده، عنوان مجرمانه یافته‌اند: تروریسم و جاسوسی سایبری.

۱-۲-۲-۱. تروریسم سایبری

تروریسم بزرگ‌ترین خطر برای صلح و امنیت ملی و بین‌المللی شمرده می‌شود. این پدیده به سبب پیوند با فناوری‌های نوین به یک گرفتاری راهبردی تبدیل شده و توانسته است گروه‌هایی کوچک، اما با ساختارهای پیچیده را به بازیگران برجسته در پهنهٔ بین‌المللی تبدیل کند (محسنی، ۱۳۹۰: ۲۰۰). تروریسم سایبری که درواقع نقطهٔ تلاقی تروریسم با فضای رایانه‌ای است، «عبارت است از فعالیت‌های اخلالگرانهٔ از پیش برنامه‌ریزی‌شده در فضای سایبر به‌منظور پیشبرد اهداف اجتماعی، ایدئولوژیک، مذهبی، سیاسی و غیره یا ارعاب افراد در پیشبرد این اهداف»[1] (Dashora , 2011: 251).

اصولاً حملات سایبری به طریقی دنبال می‌شود که خسارات حاصله به حداکثر برسد و موج رسانه‌ای گسترده‌ای تولید شود، مانند حمله به تأسیسات دولتی یا به زیرساخت‌های حساس جامعه. اقدامات تروریست‌ها در فضای سایبر به‌اندازه‌ای می‌تواند گسترده باشد که فضای سایبر هم نقش افزار را برای آنها داشته باشد. چنانکه تروریست‌ها به کمک آن گذشته از رساندن تبلیغات تروریستی امکانات عضوگیری و تأمین منافع مالی خود را گسترش می‌دهند و هم نقش موضوع و هدف جرم را که در اینجا اطلاعات یا سامانه‌ها یا شبکه‌ها مورد هجوم تروریست‌ها قرار می‌گیرد و دچار آشفتگی می‌شوند.

مثال معروف برای اقدامات تروریستی به کرم رایانه‌ای نیمدا[2] مربوط می‌شود (Nimda top of 2001 malware list, 2002: p.20.) که به‌دلیل تأثیرگذاری مخرب بالای آن و همچنین برخورداری از قابلیت‌های دیگر، مانند تروجان[3]، به کرم چهارسر[4] معروف بود. البته معروفیت بیشتر این کرم به زمان انتشار آن مربوط می‌شود که درست یک هفته پس از واقعهٔ یازدهم سپتامبر ۲۰۰۱ منتشر شد و خسارات زیادی را به‌ویژه به سامانه‌های رایانه‌ای ایالات متحده، بریتانیا و هنگ‌کنگ وارد آورد.

---

۱. برای مطالعهٔ بیشتر در مورد تعاریف ارائه‌شده در خصوص تروریسم سایبری، ر.ک:

Hill, J. & Marion, N. (2016). *Introduction to cybercrime : computer crimes, laws, and policing in the 21st century*. Santa Barbara, CA: Praeger.

2. Nimda
3. Trojan
4. Four Headed Worm

بااین‌حال، دادستان کل آمریکا، جان اشکرافت[1] اظهار داشت دلیلی مبنی بر ارتباط این کرم با حملات یازدهم سپتامبر در دست نیست (جلالی فراهانی، ۱۳۸۵: ۹۶).

۲-۲-۲-۱. جاسوسی سایبری

جاسوسی سایبری از غالب‌ترین اقسام جرم رایانه‌ای است. اهمیت این جرم به‌ویژه از حیث مرتکب و خطرها برای دولت متضرر از آن جهت است که در مراکز رایانه‌ای بیشتر سازمان‌ها و حتی شرکت‌ها اطلاعات ارزشمند ذخیره می‌شود (حسن‌بیگی، ۱۳۸۴: ۲۱۱). در این جرم، داده‌های رایانه‌ای به‌منزلهٔ موضوع جرم، جزء رکن مادی است. به عبارتی، در جاسوسی رایانه‌ای داده‌ها و اطلاعات یا به عبارتی موضوع جرم در مرحلهٔ مقدماتی انجام جرم دارای پایه و قالب مادی نیست که قابل‌لمس باشد و دارای وجود خارجی نیست و صرفاً در فضای سایبر وجود دارند؛ بدون اینکه به‌صورت خارجی مثل سی دی درآمده باشد (رهامی و پرویزی، ۱۳۹۱: ۱۸۰). در جاسوسی سایبری از رایانه‌ها و سامانه‌های مربوط به آن استفاده می‌کند تا اطلاعات محرمانه جمع‌آوری شود.

برخلاف سایر جرایم سایبری که مسائل مالی و اقتصادی محرک اصلی مجرمان است، جاسوسی سایبری بیشتر تأثیرات سیاسی است و جامعه را تهدید می‌کند. محرک‌های اصلی جاسوسی سایبری متفاوت است، اما شامل کسب منافع نظامی، صنعتی، سیاسی و فنی است (خلیلی‌پور رکن‌آبادی و نورعلی وند، ۱۳۹۱: ۱۷۴). به‌هرحال جاسوسی سایبر خواه با هدف برملا کردن اطلاعات مهم حکومتی باشد یا دزدیدن اطلاعات بخش نظامی و بازرگانی، یک عملیات نظامی است که به‌منظور کسب برتری اطلاعاتی برای دستیابی به موفقیت‌های بزرگ‌تر با صرف کمترین هزینه صورت می‌پذیرد (ماه پیشانیان، ۱۳۹۰: ۱۰۲). نمونه‌ای از جاسوسی «حملات باران»[2] تایوان در سال ۲۰۰۷ یکی از گسترده‌ترین موارد نفوذ به ادارات دولتی آمریکا و انگلیس، ازجمله وزارت دفاع آمریکا و ادارهٔ خارجی مشترک‌المنافع انگلیس بود که به چین نسبت داده شد و ظاهراً از سال ۲۰۰۲ در جریان بوده است (مؤسسهٔ فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر ایران، ۱۳۹۱: ۵۵).

عنصر قانونی جاسوسی رایانه‌ای مادهٔ ۷۳۱ قانون مجازات اسلامی در ذیل مبحث جاسوسی رایانه‌ای است. علاوه‌بر این ماده، مادهٔ ۷۳۲ نیز در مورد نقض تدابیر امنیتی سامانه‌های رایانه‌ای مقرراتی را پیش‌بینی کرده است. به‌علاوه مادهٔ ۷۳۳ جرمی غیرعمدی را برای کارکنان دستگاه‌های اجرایی پیش‌بینی کرده که نتیجهٔ آن با نتیجهٔ جرم جاسوسی که جرمی عمدی است، یکسان است، لکن از این نظر که مرتکب با ارتکاب خطای کیفری خود چنین نتیجه‌ای را ایجاد می‌کند، قانونگذار این جرم را ذیل عنوان جاسوسی رایانه‌ای ذکر کرده است.

1. John Ashcroft
2. Rain attacks

۲. شناسایی تدابیر پیشگیرانهٔ اجتماعی

همان‌طور که در مقدمه بیان شد، با توجه به تقسیم‌بندی پیشگیری اجتماعی به پیشگیری رشدمدار و اجتماع‌مدار اقدامات این مدل را برای پیشگیری از جرایم امنیتی ـ سایبری در دو بحث با همین عناوین پی می‌گیریم.

۲-۱. پیشگیری رشدمدار

امروزه نسل کودک و نوجوان ما به نسبت نسل گذشته با فضای سایبری اُنس بهتری گرفته است. کودک و نوجوان امروز با این فضا بزرگ شده و از همان ابتدا هر آنچه پیرامون خود مشاهده کرده‌اند، رنگ و بوی سایبری داشته است و به موازات آن از خطرهای این فضا ـ همچون فعالیت‌های علیه امنیت کشور مانند تبلیغ علیه نظام و مذهب رسمی کشور و ایجاد اختلاف و تنفرات قومی ـ نیز دور نبوده‌اند؛ ازاین‌رو باید آنها را از خطرها و آسیب‌های فراوان این فضا آگاه کرد تا با گرفتار شدن در آنها، نتیجه مغایر نشود. در این زمینه پیشگیری رشدمدار تنها گونهٔ پیشگیری است که به‌صورت تخصصی در پی جلوگیری و ممانعت از منحرف شدن کودکان و نوجوانان است.

پیشگیری رشدمدار به‌دنبال بهبود پایدار توانایی اجتماعی اطفالی است که خطر گرایش آنان به دنیای بزهکاری و بزه‌دیدگی زیاد است. این نوع پیشگیری بر این اندیشه مبتنی است که رفتار و آداب اکتسابی دوران رشد، یعنی از تولد تا بزرگسالی، زمینه‌ساز ارتکاب اعمال مجرمانه و منحرفانه می‌شود (ابراهیمی، ۱۳۹۱: ۷۳)؛ ازاین‌رو اقدام‌ها و مداخله‌های معمول باید جلوی عوامل خطری را که صغار در معرض آن‌اند، بگیرد (کاری یو، ۱۳۸۱: ۲۷۳). در این مدل قدرت شناخت و تمیز کودکان و نوجوانان تقویت مشده و مهارت‌های زندگی اجتماعی به آنان آموزش داده می‌شود تا بتوانند به‌هنگام مواجهه با معضلات، به‌ویژه طیف گستردهٔ جرایم و انحرافاتی که علیه امنیت ملی کشور است، از خود واکنش منطقی نشان دهد.[۱]

۲-۱-۱. انواع برنامه‌های پیشگیری رشدمدار

این مدل برای پیشگیری از کجروی، بزهکاری و بزه‌دیدگی برنامه‌هایی پیش‌بینی کرده است که در زیر با توجه به موضوع مقاله برخی از آنها را برمی‌شماریم.

۲-۱-۱-۱. برنامه‌های خانواده‌مدار

یکی از مهم‌ترین اقدامات پیشگیرانه، به تقویت کنشگران اجتماعی توجه به نقش و جایگاه خانواده مربوط می‌شود (محمدنسل، ۱۳۹۳: ۱۰۷). در همهٔ انسان‌ها ممکن است تمایلات ضداجتماعی وجود داشته باشد که می‌تواند به صورت‌های مختلف برانگیخته و به کجروی منجر شود. خانواده به‌عنوان

۱. برای آگاهی بیشتر در مورد پیشگیری زودرس ر.ک: مهدوی، ۱۳۹۰.

نخستین نهاد پرورشی فرد، نقش تعیین‌کننده‌ای در این تمایلات ایفا می‌کند، به‌گونه‌ای که می‌توان گفت کلیهٔ حالات و رفتارهای آیندهٔ کودک چه بهنجار باشد چه ناهنجار، به محیط داخلی و تربیت خانوادگی وی بستگی دارد.

برنامه‌های پیشگیری مبتنی بر خانواده عوامل خطر بزهکاری و انحرافات آیندهٔ کودک را که با خانواده همخوانی دارد، هدف قرار می‌دهد (welsh, 2007: 18). یافته‌های ناشی از مداخلات خانواده-مدار برای پیشگیری از رفتارهای منحرفانه از طریق بهبود رشد فکری، عاطفی و آموزشی طرح‌ریزی شده‌اند. ازجمله مسائل زیربنایی این برنامه‌ها، نحوهٔ آموزش کودک و جوان در انتخاب عاقلانهٔ گزینه‌ها، نحوهٔ انجام فعالیت‌های آنلاین تحت کنترل دیگران، واکنش به پیام‌های تبلیغاتی و تصاویر نامناسبی که امنیت ملی را هدف قرار می‌دهند، است. در همین زمینه برای مثال، یک برنامهٔ آموزشی برای والدینی که فرزندانشان با اینترنت کار می‌کنند، می‌تواند حاوی این نکات باشد: ۱. ایجاد حس مسئولیت‌پذیری و توانایی انتخاب گزینه‌های سالم به‌هنگام استفاده از اینترنت (به‌عبارت بهتر نحوهٔ استفادهٔ صحیح از اینترنت)؛ ۲. ایجاد تصمیمات به‌جا و مناسب دربارهٔ محتوایی که قرار است مشاهده کنند؛ و ۳. آموزش نحوهٔ رویارویی با محتوای نامناسبی که امنیت ملی را مورد هجمه قرار می‌دهد یا کاهش عواقب آن. در واقع در اینجا ابتدا باید به خود والدین آموزش داد تا بدانند چگونه این رهیافت‌ها را نسبت به اشخاص جوان خود اتخاذ کنند.

۲-۱-۱-۲. تدابیر آموزشی ـ سایبری

منظور از تدابیر آموزشی ـ سایبری آن دسته اقداماتی است که نسبت به کودکان و نوجوانان به کار می‌رود تا آنها درک مناسبی در مورد تهدیدهای سایبری پیدا کنند و هنجارهای اخلاقی در آنها درونی شود و در برابر این آسیب‌ها ایمن شوند. زمانی می‌توان گفت این اقدامات با موفقیت انجام گرفته است که بتوانند کودکان و نوجوانان را به‌مانند فضای مادی/دنیای خاکی نسبت به مخاطبان خود هُشیار کنند، اخلاق سایبری‌شان را ارتقا دهند و نیز رفتارهای آنان را حسابگرایانه‌تر سازند (رضوی فرد و کوره‌پز، ۱۳۹۴: ۹۲). کودکان و نوجوان در خصوص هرگونه اطلاعات دریافتی از اینترنت اعم از جرایم علیه امنیت ملی خنثی هستند؛ ازاین‌رو تدارک برنامه‌های آموزشی مفید خواهد بود. این تدابیر به کودکان یاد می‌دهد برای عدم مواجهه با موقعیت‌های ناامن، چه کارهایی انجام دهند و چه کارهایی انجام ندهند. همچنین، به آنها مهارت‌های تفکر را می‌آموزد (جلالی‌فراهانی و باقری‌اصل، ۱۳۸۶: ۱۴۴). نوظهور بودن جرایم سایبری، کثرت بزه‌دیدگان در فضای سایبر و عدم درک دقیق آثار تهدیدهای سایبری، ضرورت تکیه‌بر تدابیر آموزشی را موجه می‌کند (بهره‌مند و دیگران، ۱۳۹۳: ۱۷۲). به‌واقع در این فضا به‌علت عدم توان کنترل دقیق بر آن، به جولانگاه بزهکارانی مبدل شده که امنیت ملی کشور را به‌نحو مستقیم و غیرمستقیم هدف قرار داده است.

۳-۱-۱-۲. سواد رسانه‌ای

سواد رسانه‌ای شامل مهارت و توانایی تحلیل شایسته و به‌کارگیری ماهرانهٔ پیام‌ها و مبادلات

رسانه‌ای ـ سایبری است. سواد رسانه‌ای به مخاطب می‌آموزد هنگام برخورد با پیام‌هایی که امنیت ملی را هدف قرار داده است، سؤالات اساسی بپرسد و برخورد نقادانه داشته باشد، مدیریت اطلاعات داشته باشد و تسلیم ابزارهای چندرسانه‌ای قدرتمند فرهنگ رسانه نشود و نیز استفاده‌کننده‌ای متفکر در برخورد با رسانه باشد. در همین زمینه می‌توان به نتیجهٔ تحقیق تقی‌زاده استناد کرد که اشاره می‌دارد سواد رسانه‌ای می‌تواند نقش بسزایی در کاهش آسیب‌ها و استفادهٔ نقادانه و هوشمندانه از اینترنت داشته باشد (تقی‌زاده، ۱۳۹۱: ۱). همچنین آناپانگ[1] در مطالعه‌ای با روش پیمایشی روی ۲۹۲ جوان معتقد است افرادی که در دوره‌های آموزش سواد رسانه‌ای شرکت کرده بودند، آگاهی بیشتر و تفکر انتقادی بالاتری نسبت به افرادی که در دوره‌های مزبور شرکت نکرده بودند، داشتند (تقی‌زاده، ۱۳۹۱: ۴). جامعه‌ای که افراد آن سواد رسانه‌ای دارند، از توسعهٔ انسانی و اجتماعی بیشتری در مقابله با هجوم رسانه‌ای برخوردار است و افراد آن دیگر مخاطبِ صرف، منفعل و تحت کنترل رسانه‌های تهدیدکنندهٔ امنیت نیستند؛ بلکه به‌طور فعال با پیام‌ها برخورد می‌کنند و به مخاطب انتخاب‌گر و گزینشگر مبدل خواهند شد. نظر به اهمیت سواد رسانه‌ای در برخی کشورهای دنیا ازجمله کانادا، ژاپن، آلمان، انگلیس، استرالیا و آفریقای جنوبی سواد رسانه‌ای به‌عنوان یک واحد درسی در نظام آموزشی آنها در حال تدریس است. همچنین پلیس کانادا در وب‌سایت خود اقدامات مناسب برای پیشگیری از جرایم سایبری را به اطلاع مردم رسانده است (http://www.rcmp-grc.gc.ca/to-ot/tis-set/cyber-tips-conseils-eng.htm). همچنین با توجه به اینکه مرتکبان جرایم برای مخفی ماندن هویت واقعی خود اقدام به سرقت هویت می‌کنند، در ایالات‌متحده برای افزایش آگاهی‌های مردم کمیسیون فدرال تجارت اقدام به راه‌اندازی وب‌سایتی کرده است که در آن شیوه‌های ارتکاب سرقت هویت، راه‌های پیشگیری از آن و اقداماتی که باید پس از کشف توسط بزه‌دیده اتخاذ شود، معرفی شده است (Scheb & Scheb, 2011: 221).

در راستای آموزش رسانه‌ای براساس بند «ب» مادهٔ ۱۰ قانون برنامهٔ پنجسالهٔ پنجم توسعهٔ جمهوری اسلامی ایران دولت موظف است سازوکارهای اجرایی لازم را برای ارتقای آگاهی، دانش و مهارت همگانی به‌منظور ساماندهی فضای رسانه‌ای کشور، مقابله با تهاجم فرهنگ بیگانه و جرایم و ناهنجاری‌های رسانه‌ای فراهم و اجرایی کند.

۲-۲. پیشگیری اجتماع‌مدار

پیشگیری اجتماع‌مدار از جرایم امنیتی ـ سایبری به معنای اتخاذ تدابیر همگانی و عمومی برای ایجاد بستری است که این جرایم ارتکاب نیابند یا میزان آن کاهش یابد. این مدل در تلاش است برای از بین بردن یا کاهش عوامل جرم‌زا بر محیط اجتماعی و عمومی اثر گذارد و به‌دنبال مداخله در محیط اجتماعی عمومی مانند محیط فرهنگی، اقتصادی، سیاسی است که در مورد همه مشترک است (نجفی ابرندابادی، ۱۳۹۱: ۷۶۱). این مدل بر مبنای رویکرد عوامل بزهکاری و بزه‌دیدگی مبتنی است و به‌دنبال تعیین عوامل بزهکاری ـ بزه‌دیدگی و سازماندهی برنامه‌هایی به‌منظور مقابله با آن و تغییر

1. Anna Phang

شرایط اجتماعی - اقتصادی نامناسبی است که فرد در آن زندگی می‌کند و منشأ رفتارهای ضداجتماعی وی می‌شود (ابراهیمی، ۱۳۹۱: ۵۱). باید این نکته را مدنظر داشت که در پیشگیری اجتماع‌مدار از جرایم امنیتی سایبری بار اصلی پیشگیری اجتماعی بر دوش دولت است که باید هم در راستای اصلاح ساختار خویش و هم آگاهانیدن کارمندان و شهروندان از جرایم امنیتی سایبری و عواقب آن دست به ارائهٔ برنامه و پیشنهاد بزند.

۱-۲-۲. کدهای رفتاری

برای بشر دوران گذشته آشکار شده بود که نقل سینه‌به‌سینهٔ هنجارها، ولو به شکل فراگیر تا هنگامی‌که در یک کالبدی نمایان نشود و مردم آن را در پیکره‌ای یکپارچه نبینند و یادآوری نکنند، نمی‌توان به اجرای شایستهٔ آنها امیدوار بود. ازاین‌رو کتابت احکام که نخستین بار بر روی الواح سنگی صورت گرفت، با همین رویکرد در دستور کار حاکمان گذشته قرار گرفت (صدر توحیدخانه، ۱۳۸۳: ۱۵۹). در کنار این کالبدیابی و پیکرتراشی هنجاری، محتوای هنجارها نیز دگرگون و ازآن‌پس بر پایهٔ قواعد ویژه‌ای نگارش شد تا همگی آنها جلوهٔ یکپارچه و هماهنگ یابند و بتوانند به‌طور اثربخش‌تر مخاطبان خود را تحت تأثیر قرار دهند. برگزیدن این رویه‌ها سبب شد این مجموعه‌های هنجاری عنوان کد یا قانون‌نامه بیابند و به‌دلیل برخورداری از شکل و محتوای متمایز، نگاه‌های متفاوت همهٔ افراد جامعه را به‌سوی خود جلب کنند (منفرد و جلالی، ۱۳۹۱: ۱۰۹) ؛ به‌این‌ترتیب مجموعه هنجارهایی که امروز با عناوینی چون قانون، آیین‌نامه، مقررات یا بخشنامه از سوی مراجع صلاحیت‌دار، برای رعایت همه یا بخشی از اعضای جامعه وضع و ابلاغ می‌شود، کدهایی هستند که برای بهنجارسازی رفتارها پدید آمده‌اند و بنابراین، از یک نگاه می‌توان همهٔ آنها را زیر عنوان کدهای رفتاری گنجانید (همان).

به‌تدریج با گذشت زمان، به‌کارگیری کدهای رفتاری به‌عنوان ابزاری برای تبلیغ و ترویج اخلاق حرفه‌ای شیوع یافت. ازآنجاکه سامانه‌های رایانه‌ای در ابتدا در بنگاه‌های اقتصادی و بخش‌های حسابداری و حسابرسی مشاغل به کار گرفته شدند، سوءاستفاده‌های رایانه‌ای نیز در میان آنها مشاهده شد. ازاین‌رو متصدیان امر و صاحبان تصمیم ابتدا در این حوزه تصمیم گرفتند برای خنثی‌سازی انگیزه‌های مجرمانه اقدام کنند. یکی از مهم‌ترین اقداماتی که در دستور کار قرار گرفت، تدوین کد رفتاری مسئولان و متصدیان شاغل در بخش‌های مختلف بهره‌برداری از سامانه‌های رایانه‌ای بود (دزیانی، ۱۳۷۶: ۷۴) تا از طریق وضع این کدها، مسئولان سمت‌های حساس مرتبط با سامانه‌های رایانه‌ای، با تنبیه‌ها و تشویق‌های بالقوه آشنا شوند که انتظار می‌رفت به‌این‌ترتیب، از میزان سوءاستفاده‌های رایانه‌ای کاسته شود.

۱-۱-۲-۲. مفهوم‌شناسی کدهای رفتاری

کد رفتاری یا ضوابط رفتاری، مجموعه‌ای از قواعد است که اساس و پایهٔ قبول مسئولیت‌ها یا انجام رفتارهای شایسته از سوی افراد یا سازمان‌هاست. کارکرد مبنایی و مستقیم کدهای رفتاری به

آگاهی‌بخشی و شفاف‌سازی بایدها و نبایدهای رفتاری در حوزه‌های تخصصی برمی‌گردد. افزایش آگاهی گروه‌های مختلف شغلی و حرفه‌ای از قوانین و مقررات مربوط، شفافیت و مسئولیت‌پذیری را بالا می‌برد و آنها را از پیامدهای نقض رفتارهای مورد انتظار مطلع می‌گرداند (منفرد و جلالی فراهانی، ۱۳۹۱: ۱۱۲).

اساس کدهای رفتاری بر آگاهی و هشدار دهی و نیز آموزش استوار است؛ درواقع تدوین کدهای رفتاریِ رایانه‌ای راهکاری است که از یک‌سو بر آگاهی افراد از پیامدهای رفتار مجرمانهٔ رایانه‌ای می‌افزاید و از سوی دیگر، از بزه‌دیدگی‌های ناشی از کاستی دانش و ناآگاهی در این فضایِ پرخطر می‌کاهد. آگاهی، هشدار دهی و آموزش موجب خواهد شد تا افراد با آگاهی از تهدیدهای سایبری و گسترهٔ آن، به این آسیب‌ها حساسیت نشان دهند و به‌طور خودجوش نسبت به مقابله با آن اقدام کنند.

۲-۱-۲-۲. گونه‌شناسی کدهای رفتاری

برای پیشگیری از جرایم سایبری ـ امنیتی با کدهای رفتاری با دو گروه از اشخاص حقیقی و حقوقی مواجهیم؛ گاه مخاطبان کدهای رفتاری کاربرانی هستند که در گروه‌های سنی گوناگون و با خطرپذیری‌های مختلف، آماج بزه‌دیدگی و بزهکاران سایبری قرار می‌گیرند و گاه نیز مخاطبان کدهای رفتاری کارکنان و کارمندان سازمان‌های مختلف و حساس کشوری هستند؛ بر این اساس کدهای رفتاری به دو دستهٔ عام و خاص قابل تقسیم‌بندی هستند.

۱-۲-۱-۲-۲. کدهای رفتاری عمومی

فضای سایبر با دارا بودن ظرفیت‌های فراوانی که دارد، به شیوه‌های گوناگونی می‌تواند مورداستفادهٔ مجرمانِ جرایم امنیتی قرار گیرد. در این فضا از سویی ارتکاب جرایم امنیتی همچون تحریک و تشویق افراد و گروه‌ها به ارتکاب اعمال علیه امنیت یا تبلیغ به نفع گروه‌های مخالف نظام بسیار آسان است و از سوی دیگر با استفاده از روش‌های پیشگیری چون فیلترینگ نمی‌توان از آنها جلوگیری کرد، ازاین‌رو توسل به کدهای رفتاری عمومی ضرورت دارد. این کدهای رفتاری صرف‌نظر از حوزه و محیطی که برای آن تدوین می‌شوند، صرفاً در مقام تعیین رهنمودهای مورد انتظار ظاهر می‌شوند و بر فهرستی از بایدها و نبایدها به‌عنوان یک الگوی عام تأکید می‌کنند. درواقع افزایش آگاهی این کاربران از انگیزه‌های بزهکاران و موقعیت‌های مجرمانهٔ رایانه‌ای و آشنایی با تدابیر امنیتی و نحوهٔ حفاظت از خود در فضای سایبر و نیز ارائهٔ دستورالعمل‌های کاربردی شیوهٔ تأمین امنیت، رسالتی است که بر عهدهٔ این کدهای رفتاری قرار دارد. این آگاهی می‌تواند در توانمندی آنها در حفاظت از خود و برنامه‌ریزی برای به‌کارگیری ابزارهای امنیتی نقش شایان توجهی را بازی کند (منفرد، ۱۳۹۱: ۱۵۸).

در همین زمینه، شورای عالی اطلاع‌رسانی در سال ۱۳۷۹ در سندی با عنوان «راهبردهای کلان ارائهٔ خدمات اطلاع‌رسانی و اینترنت در کشور»، تدوین کدهای رفتاری برای کاربران شبکه‌های

اطلاع‌رسانی رایانه‌ای را پیش‌بینی کرده بود و در سال ۱۳۸۰، پیرو تصویب و ابلاغ سیاست‌های کلی شبکه‌های اطلاع‌رسانی رایانه‌ای از سوی رهبر معظم انقلاب اسلامی، شورای عالی انقلاب فرهنگی به‌منظور انتظام امور و فعالیت‌های اطلاع‌رسانی و توسعهٔ خدمات دسترسی به اینترنت در کشور مقررات و ضوابط شبکه‌های اطلاع‌رسانی رایانه‌ای را تصویب کرد.

۲-۲-۱-۲-۲. کدهای رفتاری خاص

نبود دانش و اطلاعات لازم کاربران شبکه‌های کامپیوتری و استفاده‌کنندگان اطلاعات حساس در یک سازمان، همواره به‌عنوان مهم‌ترین تهدید امنیتی مطرح و عدم پایبندی و رعایت اصول امنیتی تدوین‌شده، می‌تواند زمینهٔ ایجاد پتانسیل‌هایی شود که توسط مهاجمان استفاده و سبب بروز مشکل در سازمان شود. مهاجمان همواره در پی چنین فرصت‌هایی هستند تا با اتکا به آنان به اهداف خود نائل شوند. اگر سعی کنیم بر اساس یک روش مناسب، درصد بروز اشتباهات خود را کاهش دهیم، به همان نسبت نیز شانس موفقیت مهاجمان کاهش پیدا خواهد کرد (حسن‌زاده و جهانگیری، ۱۳۹۰: ۸۸). برخی جرایم سایبری همچون رخنه دادن ویروس به اتوماسیون مراکز مهم یا اخلال در روند کار شبکه‌های برق و گاز ضررها و خسارات زیادی را به امنیت کشور وارد می‌کنند (مثال بارز ایجاد اخلال در جریان برق در آمریکاست که درست یک روز بعد از واقعهٔ ۱۱ سپتامبر ۲۰۰۱ رخ داد) که به‌منظور جلوگیری از آنها آموزش کارکنان و متخصصان این مراکز لازم است تا پیش از تأثیرگذاری این جرایم از آنها پیشگیری شود، در این زمینه کدهای رفتاری خاص می‌تواند راهگشا باشد. این کدها «در جهت آشنایی هرچه بیشتر این افراد با شغل خطیری که در اختیار دارند، درک حساسیت‌های حاکم بر آن مشاغل، خطرهای احتمالی که آنها را تهدید می‌کند و شیوه‌های مقابله با آنها و همچنین امتیازاتی را که می‌توانند به‌دنبال حسن انجام کار از آنها بهره‌مند شوند، دربردارد. به‌عبارت‌دیگر، از طریق وضع این کدها، مسئولان سمت‌های حساس مرتبط با سامانه‌های رایانه‌ای، با تنبیه‌ها و تشویق‌های بالقوه آشنا می‌شدند که انتظار می‌رود به‌این‌ترتیب، از میزان سوءاستفاده‌های رایانه‌ای کاسته شود. درواقع، مهم‌ترین هدفی که از تدوین این کدهای رفتاری دنبال می‌شد، از بین بردن انگیزه‌های سودجویانهٔ مادی بود که ممکن است کارمندان را تحریک کرده و وادار به انجام اعمالی از قبیل سرقت اسرار تجاری یا صنعتی و فروش به رقبا کند» (جلالی فراهانی، ۱۳۸۴: ۴۴). به‌منظور تحقق اهداف کدهای رفتاری خاص برای جلوگیری از جرایم امنیتی سایبری شایسته است متصدیان مراکز حساس مورد آموزش تخصصی قرار گیرند و آموزش لازم برای جلوگیری از این جرایم به آنها داده شود. به‌علاوه افرادی که تخصص بیشتری در فضای سایبر دارند، به‌عنوان دیدبان محیط سایبری مراکز مهم جذب شوند تا ضمن رصد کردن کارکرد درست اتوماسیون‌ها و فناوری‌های مرتبط سایبری از بزهکاری‌های احتمالی علیه امنیت در فضای سایبر جلوگیری شود.

۲-۲-۲. اطلاع‌رسانی و اطلاع‌گیری

اطلاع‌رسانی و اطلاع‌گیری در مورد فضای ناشناختهٔ سایبر از راهکارهای اساسی برای پیشگیری از تهدیدات امنیتی ـ سایبری است.

۱-۲-۲- ۲. اطلاع‌رسانی

تعداد زیادی از کاربران اینترنت، تنها برای گذران وقت و سرگرمی، گام در فضای مجازی می‌گذارند. بسیاری از کاربران نیز به برخی از جرایم سایبری به دیدهٔ سرگرمی می‌نگرند. با توجه به بی‌هدف بودن این تعداد از کاربران، احتمال اینکه آنها به سمت ارتکاب جرایم سایبری یا وبگاه‌های غیرمجاز متمایل شوند، بسیار زیاد است. مجازی بودن، فقدان نمود خارجی و ملموس نبودن آثار جرم، یکی از عوامل سوق یافتن کاربران به ارتکاب این‌گونه جرایم است (بهره‌مند و دیگران، ۱۳۹۳: ۱۷۰). بر این اساس پیشگیری اطلاعی در خصوص جرایم امنیتی - سایبری در فضای سایبر می‌تواند تأثیر بسزایی بر پیشگیری از این جرایم داشته باشد. اطلاع‌رسانی در خصوص تهدیدات سایبری می‌تواند جنبهٔ آموزشی و هشداردهی داشته باشد. این وظیفه اغلب بر عهدهٔ نهادها و سازمان‌هایی است که نقش رسانه‌ای دارند. بر اساس بند ۲ اصل ۳ قانون اساسی بالا بردن سطح آگاهی‌های عمومی در همهٔ زمینه‌ها با استفادهٔ صحیح از مطبوعات و رسانه‌های گروهی و وسایل دیگر، از وظایف اساسی دولت جمهوری اسلامی ایران است. حق اطلاع‌رسانی و کسب اطلاع پیش‌تر در اسناد بین‌المللی که ایران به آنها ملحق شده است نیز به‌عنوان حقوق بشر مورد پذیرش قرار گرفته است؛ از جمله مادهٔ ۱۹ اعلامیهٔ جهانی حقوق بشر که مقرر می‌دارد: «هر کس حق آزادی عقیده بیان دارد و حق مزبور شامل آن است که از داشتن عقاید خود بیم و اضطرابی نداشته باشد و در کسب اطلاعات و افکار و در اخذ و انتشار آن به تمام وسایل ممکن و بدون ملاحظات مرزی آزاد باشد». «اطلاع‌رسانی می‌تواند از طریق رسانه‌های سنتی مانند تلویزیون، رادیو، روزنامه‌ها و شبکه‌های محلی در کنار اینترنت، اعلامیه‌های خدمات عمومی یا ویدئوها برای دادن اطلاعات کلی راجع به مسائل مربوط به جرم، اطلاعات مربوط به خدمات یا تغییرات جدید راهبردها و پیشرفت‌های پروژه انجام شود» (جوان جعفری و سیدزاده ثانی، ۱۳۹۱: ۲۴۶-۲۴۵). جرایم امنیتی در فضای سایبر دامنه‌های گسترده‌ای دارند که ضرورت اطلاع‌رسانی چندوجهی را آشکار می‌کند. برخی دولت‌ها مراکز اطلاع‌رسانی آنلاینی تأسیس کرده‌اند که اقدام به ارائهٔ مشاوره و توصیه‌های عملی به سیاست‌گذاران، متصدیان و پژوهشگران شاغل در ارکان مختلف دولت می‌کند.

در ایالات‌متحده، وظیفهٔ اطلاع‌رسانی برای پیشگیری از جرایم امنیتی بر عهدهٔ پلیس این کشور نهاده شده است. درواقع به‌منظور پیشگیری غیرکیفری از جرایم دولت ایالات متحدهٔ آمریکا شماری از برنامه‌های آموزشی و آگاهی‌رسانی را برای مقابله با جریم سایبری، صرف‌نظر از هویت یا مقاصد مرتکبان، پشتیبانی می‌کند. برای مثال، وب‌سایت اف بی آی اطلاعات و منابع مربوط به محفوظ

داشتن رایانه‌ها از تأثیرات جرایم سایبری را ارائه می‌کند (پاکزاد، ۱۳۸۸: ۲۹۹).[1] در انگلستان نیز وزارت کشور سایتی را برای کاهش جرم طراحی کرده است که توسط آن به حمایت از مجریان قانون، همکاری در جهت کاهش جرم و بی‌نظمی و طرح مشارکت در امنیت جامعه می‌پردازد (جوان جعفری و سیدزاده ثانی، ۱۳۹۱: ۱۱۳ – ۱۱۲).

در ایران طرح آپا به‌منظور ارتقای دانش فنی کشور و توسعهٔ دانش مدیریت حوادث امنیتی از سال ۱۳۸۴ در پژوهشکدهٔ امنیت ارتباطات و فناوری اطلاعات مرکز تحقیقات مخابرات ایران شروع و بهره‌برداری آن اواخر سال ۱۳۸۶ آغاز شده است.[2] (https://esfahan.ict.gov.ir/fa/hozahayfaliat/fanavari/apa-%D9%85%D8%B1%DA%A9%D8%B2-%D8%A2%D9%BE%D8%A7) در این طرح آگاهی‌های امنیتی برای مقابله با اختلالات و حوادث فضای رایانه‌ای ارائه می‌شود. علاوه‌بر این یک گروه امداد امنیت کامپیوتری ایران هم به‌عنوان یک بخش خصوصی همانند بخش خصوصی بسیاری از کشورها اقدام به راه‌اندازی پرتالی کرده که هدف از آن عبارت است از: الف) اطلاع‌رسانی (مستند و قابل اطمینان بودن اطلاعات)، ب) آموزش (اعتبار مدارک و دوره‌ها)، ج) مشاوره، پیشگیری و پاسخگویی (ایجاد اطمینان در زیرساخت‌ها)، د) تست و ارزیابی امنیتی (شبکه‌ها و سایت‌های تأییدشده) و ه) ارتباط و هماهنگی با مؤسسات، سازمان‌ها و شرکت‌های بین‌المللی و داخلی (http://www.ircert.com/aboutus.htm) .

۲-۲-۲-۲. اطلاع‌گیری

در کنار اطلاع‌رسانی، اطلاع‌گیری یا خبرگیری نیز یکی از تدابیر مهم پیشگیری است. فضای سایبر به‌علت گستردگی، پیچیدگی و نیز پنهان بودن آن امکان ارتکاب انواع جرایم امنیتی ـ سایبری را فراهم می‌سازد؛ ازاین‌رو تدارک برنامه‌ای جامع در جهت اطلاع‌گیری در این فضا لازم است. در این زمینه می‌توان برای نمونه در کوشه مرورگرهای مختلف لینکی را قرار داد تا چنانچه کاربران در صفحات فراخوانده‌شده محتوایی حاوی جرایم امنیتی را مشاهده کردند، آن را گزارش کنند و «اینکه نهادهای امنیتی در سطح شهر یا از طریق رسانه شمارهٔ تلفن یا مشخصات دیگری در فضای سایبر ارائه دهند که در صورت برخورد شهروندان با هرگونه واقعهٔ مشکوک اینترنتی یا حملهٔ اینترنتی، جریان را به مرجع تعقیب اطلاع دهند. اطلاع‌گیری عمومی به این نحو که شماره یا مشخصات دیگر را به مردم ارائه دهند، خود سبب احساس ناامنی مجرمین جرایم امنیتی سایبری از اطرافیان یا کسانی که با آنها ارتباط برقرار می‌کنند، می‌شود و نقش بسزایی در پیشگیری دارد» (پاکزاد، ۱۳۸۸: ۳۰۱). در همین زمینه در انگلستان نهادی به نام سیاست‌گذاری مبتنی بر خبرگیری تأسیس شده که به‌عنوان مدل سیاست‌گذاری در امور مربوط به اطلاعات معرفی شده و نخستین بار

---

۱. ر.ک: وب‌سایت اف بی آی به نشانی زیر:

http://www.fbi.gov/cyberinvest/protect_online.htm

۲. در حال حاضر هشت مرکز تخصصی آپا به‌ترتیب زیر ایجاد شده‌اند که به مرور دامنهٔ خدمات خود را پس از طی کردن مراحل راه‌اندازی و تجهیز، گسترش می‌دهند.

در سال ۲۰۰۰ با توجه به مدل خبرگیری ملی انگلستان و در ذیل آن ایجاد شد (Ratcliffe, 2003: 6). در این مدل، فرایندی سه‌مرحله‌ای برای تحلیل اطلاعات در راستای پیشگیری یا کاهش جرایم و مبارزه با باندهای جنایی پیش‌بینی شده است: مرحلهٔ نخست تفسیر و تحلیل محیط جنایی توسط مدیر عالی خبرگیری؛ مرحلهٔ دوم معرفی اطلاعات کسب‌شده از سازمان‌های جنایی به مراجع تصمیم‌گیر؛ و مرحلهٔ سوم تصمیم‌گیری مراجع مافوق جهت پیشگیری یا کاهش جرم. به‌تدریج شبیه نهاد فوق، در سایر کشورها، نظیر ایالات‌متحده، استرالیا و کانادا نیز تأسیس شد (عالی‌پور، ۱۳۸۷: ۱۱۸).[۱]

۳-۲-۲. حکمرانی خوب در فضای سایبر

حکمرانی خوب ازجمله مباحث تازه‌ای است که در دو دههٔ اخیر توجه محافل علمی و بین‌المللی را به خود جلب کرده است. «در اواخر دههٔ ۱۹۸۰ و اوایل دههٔ۱۹۹۰ اصطلاح حکمرانی خوب توسط بانک جهانی مطرح شد و تأکید آن بر تصمیماتی بود که امکان تأثیرگذاری بر عملکرد اقتصادی کشورها را فراهم می‌ساخت. بعدها علاوه بر بعد اقتصادی، یک بعد سیاسی نیز به آن افزوده شد که شامل ویژگی‌های مشروعیت دولتی، پاسخگویی دولتی، تحقق حقوق بشر از طریق حاکمیت قانون و شایستگی دولتی است» (دباغ و نفری، ۱۳۸۸: ۵).

ازآنجاکه ریشه‌های جرایم امنیتی ــ سایبری در وضعیت سیاسی، اقتصادی، اجتماعی و فرهنگی جوامع نهفته است و بدون توجه به این علل و تلاش برای از بین بردن نابرابری‌ها در سطح ملی و جهانی نباید امیدی به پیروزی در مبارزه با این جرایم امنیتی داشت، ازاین‌رو توجه به توسعهٔ همه‌جانبه و معیارهای حکمرانی خوب حائز اهمیت است.

۱-۳-۲- ۲. مشارکت و اجماع‌گری

مشارکت گروه‌های مختلف می‌تواند سبب انسجام ملی و وحدت شود که این خود زمینه را برای پیشگیری و مقابله با حرکت‌هایی چون تبلیغ علیه نظام، رواج بی‌بندوباری، اسلام‌ستیزی و خود انزجاری‌های فرهنگی و علاقه به فرهنگ غیر داشتن که بنیاد امنیت کشور را مخدوش می‌کند، شود. به‌علاوه مشارکت سبب آگاهی اقشار مختلف جامعه و پیشگیری از مورد سوءاستفاده قرار گرفتن افراد در فضای سایبر در جهت خدشه به امنیت ملی می‌شود. برای نمونه در فضای سایبر با تحریکات از افراد برای جمع‌آوری پول برای ضربه زدن به امنیت ملی و نیز تشکیل گروه‌های مجرمانه با هدف برهم زدن امنیت و... استفاده می‌شود.

---

۱. در انگلستان بر پایهٔ قانون تنظیم اختیارات بازپرسی انگلستان مصوب ۲۰۰۰ مأموران دولت به بهانهٔ بایسته‌های امنیت ملی، می‌توانند به فراگیری یا افشای داده‌های ارتباطی (مادهٔ ۲)، خبرگیری از داده‌های در حال تراکنش (مادهٔ ۲۸) و انجام جاسوسی‌های سرزده دست زنند (عالی‌پور، ۱۳۹۲: ۲۶).

نظر به اینکه جرایم علیه امنیت در فضای سایبر از تنوع بسیاری برخوردار است، به شکلی که برخی زیرساخت‌های مادی ـ انسانی حساسِ کشور را هدف قرار می‌دهند، برخی از بعد تبلیغات علیه ارزش‌های اساسی و ایجاد دسته‌بندی‌های غیرقانونی فعالیت می‌کنند و... بر این اساس مشارکت بین سازمان‌های دولتی و غیردولتی، بخش خصوصی و افراد جامعه باید از ارکان اساسی پیشگیری در این حوزه به‌حساب آید، زیرا «این گروه‌ها می‌توانند بر اساس تجربیات خود دانش عمیق، بینش خلاقانه و راه‌حل‌های ابتکاری در واکنش به مشکلات ارائه کنند. در همین زمینه مادهٔ ۹ رهنمودهای پیش‌گیری از جرم سازمان ملل تأکید می‌کند که برنامه‌های پیشگیری را نمی‌توان در یک وزارتخانه محدود ساخت و وزارتخانه‌های مختلف، مقامات، نهادهای محلی، سازمان‌های غیردولتی، تجار و شهروندان همه و همه باید با همکاری یکدیگر برنامه‌های پیشگیری را به اجرا درآورند» (جوان جعفری، ۱۳۹۱: ۶۴ و ۲۴۴). شایان‌ذکر است دولت باید برای مشارکت گروه‌ها و نهادهای مختلف نقش اساسی را در بعد مدیریت، هماهنگی و تأمین منابع لازم ایفا کند.

۲-۳-۲- ۲. پاسخگویی و شفافیت

بسیاری از کودتاها و انقلاب‌های نرمی که ریشهٔ درونی دارند و مورد استقبال عمومی مردم قرار می‌گیرند، ناشی از ارتکاب جرایمی چون سوءاستفاده از قدرت و ثروت از سوی دولتمردان و هیأت حاکمه است. این امور به‌خصوص با شایعه‌پراکنی‌های سایبری که امنیت ملی را متزلزل می‌کند و دسترسی آحاد و آنی مردم به آنها بسیار خطرناک است. این موارد و نیز بسیاری از مواردی که احساس تجزیه‌طلبی را در جامعه تقویت می‌کند و عدم‌وفوق بین دولت و مردم و فرهنگ‌گریزی‌ها را بین اقشار جامعه بسط می‌دهد و امنیت ملی را تضعیف می‌کند، ناشی از پاسخگو و شفاف نبودن مسئولان کشور در مورد امور مختلف کشور است. «برای تحقق این امر لازم است مردم امکان نظارت بر اعمال دولت را داشته باشند و در جریان چندوچون فعالیت‌های دولت و عوامل آن قرار گیرند؛ ازاین‌رو دولت باید قانوناً متعهد به افشای آمار و اطلاعات در خصوص فعالیت‌های خود باشد و آمار و اطلاعات معنی‌دار و دقیق که امکان ارزیابی فعالیت‌های دولت را بدهد. از این نظر دسترسی به اطلاعات معتبر و شفافیت بیشتر، لازمهٔ اجتناب‌ناپذیر از فرایندی است که بتوان دولت و عوامل آن را در قبال اعمالشان به پاسخگویی فراخواند» (یزدانی زنور، ۱۳۸۸: ۵۴).

یکی از ابزارها برای تحقق شفاف‌سازی و علنی کردن تصمیمات مسئولان و نیز مورد سؤال واقع شدن آنها، آزادی اطلاعات و اجبار دولت به ارائهٔ اطلاعات است. آزادی اطلاعات به معنای داشتن حق دسترسی به اطلاعات به‌ویژه اطلاعات عمومی و اسناد دولتی است. ضرورت آزادی اطلاعات موجب تصویب قانون انتشار و دسترسی آزاد به اطلاعات در سال ۱۳۸۸ شد. قانون مزبور حق دسترسی را در دو قالب کنشی و واکنشی به‌صورت اجباری پیش‌بینی کرده است. در قالب کنشی، مؤسسات عمومی مکلف‌اند درهرحال و بدون آنکه درخواستی صورت گیرد، اطلاعاتی را که متضمن حق و تکلیف برای مردم است، انتشار دهند و در قالب واکنشی در صورت درخواست از سوی متقاضی یا متقاضیان و نبود ممنوعیت قانونی مؤسسات عمومی مکلف به ارائهٔ اطلاعات هستند.

درواقع آنچه رأساً در قبال اطلاعات عمومی صورت می‌گیرد، انتشار و آنچه با درخواست متقاضی است، ارائهٔ اطلاعات نامیده می‌شود» (پاکزاد، ۱۳۸۸: ۳۱۰).

۳-۳-۲- ۲. فرهنگ‌سازی و تولید رسانه‌ای

بسیاری از جرایم علیه امنیت در فضای سایبر را می‌توان با فرهنگ‌سازی چه در بعد داخلی چه در بعد بین‌المللی خنثی کرد. در بعد داخلی تقویت فرهنگ قانون‌مداری، ایجاد اعتماد به ظرفیت‌های خود در افراد جامعه، حمایت از ارزش‌های اجتماعی و نیز فرهنگ پذیرش برنامه‌های پیشگیری، زمینهٔ پیشگیری از این دسته جرایم را فراهم می‌کند، زیرا چنانچه مردم بدانند که برنامه‌های پیشگیری به بهبود فضای زندگی و کاهش بزه‌دیدگی منجر می‌شود، بهتر و بیشتر در برنامه‌های پیشگیری مشارکت خواهند کرد.

در بعد بین‌المللی با لحاظ فرامرزی بودن جرایم امنیتی ـ سایبری، پیشگیری و فرهنگ‌سازی نیز باید چهرهٔ جهانی به خود بگیرد. دلیل این امر هم آن است که فضای سایبر و ارزش‌ها و هنجارهای آن جهانی است و درنتیجه باید یک فرهنگ مطلوب و صحیح جهانی بر فضای سایبر حاکم شود. بر همین اساس طبق قطعنامهٔ ۵۸/۱۹۹ مجمع عمومی سازمان ملل، امنیت سایبری در گرو یک فرهنگ جهانی شناخته شده است (پاکزاد، ۱۳۸۸: ۱۰۹).

موضوع آخر در خصوص حکمرانی خوب توسعهٔ تولیدات رسانه‌ای و حضور فعال داشتن در فضای سایبر است. به شکلی کاربران ایرانی در مورد موضوعات مختلف با تولیدات داخلی کافی روبه‌رو شوند. به‌منظور تحقق این هدف مادهٔ ۳ قانون برنامهٔ پنجم توسعه یکی از وظایف دولت را حمایت لازم از «طراحی، تولید، توزیع، انتشار و صدور خدمات و محصولات فرهنگی، هنری، رسانه‌ای، صنایع‌دستی و میراث فرهنگی» دانسته است. همچنین مادهٔ ۲۰۹ قانون مزبور دولت موظف است سازوکارهای اجرایی لازم را برای «بهره‌گیری و هماهنگ‌سازی اقدامات فرهنگی، آموزشی، تربیتی، تبلیغی و رسانه‌ای برای مقابله با ناهنجاری‌های فرهنگی و اجتماعی» فراهم کند.

نتیجه‌گیری

انقلاب در فناوری ارتباطات و اطلاعات فرصت‌های بدیعی را در اختیار افراد و دولت‌ها نهاده است که بتوانند امورشان را به نحو بهتر تدبیر کنند؛ اما از طرفی تهدیدآمیز نیز بوده و آسیب‌پذیری‌ها را افزون‌تر ساخته است. استعمارگران دنیا برای به قدرت رسیدن در جهان و به زیر سلطه در آوردن کشورهای جهان از اینترنت بیشترین بهره را می‌گیرند؛ بدین شکل که از یک سو در جنگی نرم جوانان را از ارزش‌ها و اهداف اصلی زندگی دور می‌کنند و خود نیز با برنامه‌ریزی هدفمند افکار عمومی جهان را تحت تأثیر قرار می‌دهند و از سوی دیگر به زیرساخت‌های حیاتی کشورهای هدف هجوم می‌برند و بدین گونه امنیت ملی کشوها را مخاطره‌آمیز می‌کنند. این فناوری توانسته منابع

تهدیدکنندهٔ امنیت ملی را از سطح دولت‌ها فراتر برد و در کنار دولت‌ها افراد، گروه‌ها و سازمان‌های فرو ملی و فراملی نیز وارد عرصهٔ ارتکاب جرایم امنیتی شدند.

جرایم امنیتی که در فضای سایبر ارتکاب می‌یابد، جدیدترین و پیچیده‌ترین تهدید علیه زندگی بشر به‌شمار می‌آید. این جرایم در سیاههٔ کیفری نظام حقوقی ایران شامل جرایم امنیتی ـ سایبری استفاده‌کننده از فضای سایبر و علیه فضای سایبر می‌شود. این جرایم در فضای سایبر در بستری متفاوت و با کیفیتی منحصربه‌فرد ارتکاب می‌یابند و بالطبع هر اقدام کنترلی، مقابله‌گرایانه و پیشگیرانه نیز باید متناسب با این فضا تدارک دیده شود. درواقع در فضای سایبر که مرزهای مشخصی برای آن ترسیم نشده است، نمی‌توان از اقدامات سنتی برای پاسبانی امنیت ملی در فضای سایبر سود جست. جهانی و بدون مرز بودن این فضا و امکان انجام انواع جرایم با توسل به فناوری تبادل اطلاعات، امنیت ملی را با چالشی جدید و جدی مواجه کرده و تهدیداتی را وارد این حوزه کرده است که ماهیتاً با نظایر فیزیکی متفاوت است که اقدامات پیشگیرانه می‌تواند مؤثرترین راه برای مقابله با این تهدیدات نوین به‌شمار رود؛ بر این اساس سیاست جنایی در رویارویی با جرایم سایبری علیه امنیت ملی نیازمند اتخاذ تدابیر پیشگیرانه خاص و در قالب پیشگیری اجتماعی است.

پیشگیری اجتماعی ازنظر دارا بودن آثار مثبت و سازنده در قیاس با پیشگیری وضعی و کیفری به‌مراتب امیدوارکننده است. با این توضیح که در پیشگیری وضعی که تأکید بر عواملی چون رمزنگاری، دیوارهای آتش، فیلترینگ و... دارد، به‌علت تحول و پیشرفت سریع فناوری اینترنتی ــ سایبری و همچنین از این نظر که به‌طورکلی مانع از وقوع این جرایم نمی‌شوند و تنها هزینهٔ ارتکاب آنها را بالاتر می‌برند و درنهایت سبب جابه‌جایی سیبل مجرمانه می‌شوند. ازاین‌رو، چندان نمی‌توان به کارایی آنها امیدوار بود. به‌علاوه پیشگیری کیفری که پس از وقوع جرم با بهره جستن از تدابیر و اقدامات نظام عدالت کیفری برای کاهش نرخ جرم مداخله می‌کند نیز چون جرایم امنیتی ــ سایبری با دارا بودن ویژگی‌هایی چون جهانی و فرامرزی ـ به‌گونه‌ای که بیشتر از جانب کشورهای آمریکایی و اروپایی ارتکاب می‌یابند ـ و نیز پوشیده بودن، قابلیت کارایی چندان ندارد. در مقابل به نظر می‌رسد پیشگیری اجتماعی می‌تواند بسیار مؤثر باشد. هدف در این مدل پیشگیری از بین بردن آن دسته از عوامل خطرِ جرم است که افراد را مستعد بزهکاری یا بزه‌دیدگی می‌کنند. این مدل از راه‌هایی مانند آموزش کاربران و حکمرانی خوب در فضای سایبر و... که پیش‌تر اشاره شد، اعمال می‌شود. در اقدامات پیشگیرانهٔ اجتماعی تلاش می‌شود با کمک از ظرفیت کاربران مانع تحقق جرایم امنیتی سایبری شد. در میان اقدامات پیشگیرانهٔ اجتماعی که می‌تواند به کاهش جرایم امنیتی ـ سایبری کمک کند، می‌توان به برنامه‌های خانواده‌مدار، تدابیر آموزشی ـ سایبری، بالا بردن سواد رسانه‌ای، تنظیم کدهای رفتاری، اطلاع‌رسانی و اطلاع‌گیری، توجه به حکمرانی خوب و شاخص‌های آن، مشارکت و اجماع‌گری، ارتقای پاسخگویی و شفافیت، فرهنگ‌سازی و تولید رسانه‌ای اشاره کرد.

منابع

الف) فارسی

۱.آقابخشی، علی (۱۳۶۳). *فرهنگ علوم سیاسی: انگلیسی ـ فارسی*، تهران: انتشارات بهرنگ.
۲.ابراهیمی، شهرام (۱۳۹۱). جرم‌شناسی پیشگیری از جرم، چ ۱، چ اول، تهران: میزان.
۳.بهره‌مند، حمید؛ کوره‌پز، حسین‌محمد؛ سلیمی، احسان (۱۳۹۳). «راهبردهای وضعی پیشگیری از جرایم سایبری»، *آموزه‌های حقوق کیفری*، دانشگاه علوم اسلامی رضوی، ش ۷.
۴.پاکزاد، بتول (۱۳۸۸). *تروریسم سایبری*، رسالهٔ نامهٔ دکتری حقوق جزا و جرم‌شناسی، دانشگاه شهید بهشتی، تهران.
۵.تقی‌زاده، عباس (۱۳۹۱). ارتقای سواد رسانه‌ای زمینهٔ کاهش آسیب‌های اجتماعی نوپدید فضای مجازی، نخستین کنگرهٔ ملی فضای مجازی و آسیب‌های اجتماعی نوپدید، تهران: وزارت تعاون، کار و رفاه اجتماعی، http://www. civilica. com/Paper-NOPADID01-NOPADID01_030. html
۶.جلالی فراهانی، امیرحسین (۱۳۸۴). *پیشگیری از جرایم رایانه‌ای*، پایان‌نامهٔ کارشناسی ارشد حقوق جزا و جرم‌شناسی، تهران: دانشگاه امام صادق (ع).
۷.جلالی فراهانی، امیرحسین؛ باقری اصل، رضا (۱۳۸۶). «پیشگیری اجتماعی از جرائم و انحرافات سایبری»، *مجلهٔ مجلس و پژوهش*، سال چهاردهم، ش ۵۵.
۸.---------- (۱۳۸۷). «پیشگیری اجتماعی از جرائم و انحرافات سایبری راهکاری اصولی برای نهادینه‌سازی اخلاق سایبری»، *فصلنامهٔ ره‌آورد نور*، پاییز، سال هفتم، ش ۲۴.
۹.جلالی فراهانی، امیرحسین (۱۳۸۵). «تروریسم سایبری»، *فصلنامهٔ فقه و حقوق*، ش ۱۰.
۱۰. جوان جعفری، عبدالرضا؛ سیدزاده ثانی، سید مهدی (۱۳۹۱). *رهنمودهای عملی پیشگیری از جرم*، چ اول، تهران: میزان.
۱۱. حسن‌زاده، محمد؛ جهانگیری، نرگس (۱۳۹۰). *امنیت اطلاعات: از آگاهی تا آموزش*، چ اول، تهران: نشر کتابدار.
۱۲. حسن بیگی، ابراهیم (۱۳۸۴). *حقوق و امنیت در فضای سایبر*، چ اول، تهران: مؤسسهٔ فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران.
۱۳. خلیلی پور رکن‌آبادی، علی؛ نورعلی وند، یاسر (۱۳۹۱). «تهدیدات سایبری و تأثیر آن بر امنیت ملی»، *فصلنامهٔ مطالعات راهبردی*، سال پانزدهم، ش دوم.
۱۴. خبرگزاری فارس، کد خبر ۹۴۸۹۸، تاریخ انتشار، ۲۰ بهمن ۱۳۹۴
۱۵. خبرگزاری دانشجویان ایران (ایسنا)، کد خبر ۴۲۶۷۵۰، ۰۸ بهمن ۱۳۹۴
۱۶. دزیانی، محمدحسن (۱۳۷۶). *جرایم کامپیوتری*، ج ۲، چ اول، سازمان مدیریت و برنامه‌ریزی، دبیرخانهٔ شورای عالی انفورماتیک کشور.
۱۷. دباغ، سروش؛ نفری، ندا (۱۳۸۸). «تبیین مفهوم خوبی در حکمرانی خوب»، *نشریهٔ مدیریت دولتی*، دورهٔ اول، ش ۳.
۱۸. رضوی فرد، بهزاد؛ کوره‌پز، حسین محمد (۱۳۹۴). «راهبردهای پیشگیرانهٔ آموزشی آگاهی ساز: ضرورتی پیش روی برنامه‌های کنترل انحرافات سایبری»، *فصلنامهٔ کارآگاه*، دورهٔ دوم، سال هشتم، ش ۳۲.
۱۹. روزنا و سینگ (۱۳۹۱). فناوری اطلاعات و سیاست جهانی، ترجمهٔ احمد سلطانی‌نژاد و احمد محقر، چ اول، تهران: دانشگاه امام صادق (ع).
۲۰. رضاعلی، لنی (۱۳۹۰). «بازشناسی و تحلیل پدیدهٔ تروریسم»، *فصلنامهٔ مطالعات سیاسی*، سال سوم، ش ۱۲.
۲۱. رهامی، محسن؛ پرویزی، سیروس (۱۳۹۱). «جاسوسی رایانه‌ای در حقوق ایران و وضعیت بین‌المللی آن»، *فصلنامهٔ حقوق*، دورهٔ ۴۲، ش ۳.
۲۲. صدر توحیدخانه، محمد (۱۳۸۳). «کدهای باستانی و قداست بخشی به آنها»، *مجلهٔ حقوقی دادگستری*، ش ۴۷.
۲۳. عالی‌پور، حسن (۱۳۸۷). *توازن میان امنیت ملی و آزادی‌های فردی در مقابله با جرایم تروریستی*، رسالهٔ دکتری حقوق جزا و جرم‌شناسی، تهران.
۲۴. ---------- (۱۳۹۲). *بزه‌های امنیتی سایبری، جزوهٔ حقوق جزای اختصاصی کارشناسی‌ارشد (درآمد بزه‌های رایانه‌ای)*، دانشگاه اصفهان.
۲۵. ---------- (۱۳۹۳). *حقوق کیفری فناوری اطلاعات*، چ سوم، تهران: خرسندی.
۲۶. کاری یو، روبر (۱۳۸۱). «مداخلهٔ روان‌شناختی- اجتماعی زودرس در پیشگیری از رفتارهای مجرمانه»، ترجمهٔ علی‌حسین نجفی ابرندآبادی، *مجلهٔ تحقیقات حقوقی*، ش ۳۶-۳۵.

۲۷. مؤسسهٔ فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران (۱۳۹۱). *امنیت و جنگ سایبر (۱) (ویژهٔ مفاهیم و مبانی)*، چ اول، ابرار معاصر ایران.
۲۸. منفرد، محبوبه؛ جلالی فراهانی، امیرحسین (۱۳۹۱). «کدهای رفتاری و پیشگیری از بزهکاری»، *پژوهشنامهٔ حقوق کیفری*، سال سوم، ش ۲.
۲۹. ماه پیشانیان، مهسا (۱۳۹۰). «فضای سایبر و شیوه‌های نوین درگیری ایالات متحدهٔ آمریکا با جمهوری اسلامی ایران»، *نامهٔ پژوهش فرهنگی*، سال دوازدهم، ش ۱۳.
۳۰. محمدنسل، غلامرضا (۱۳۹۳). *کلیات پیشگیری از جرم*، چ اول، تهران: میزان.
۳۱. ---------- (۱۳۹۵). *حقوق جزای اختصاصی؛ جرایم رایانه‌ای در ایران*، چ دوم، تهران: میزان.
۳۲. منفرد، محبوبه (۱۳۹۱). *پیشگیری از جرایم رایانه‌ای از گذر کدهای رفتاری رایانه‌ای*، پایان‌نامهٔ کارشناسی‌ارشد، مؤسسهٔ آموزش عالی شهید اشرفی اصفهانی.
۳۳. نجفی‌ابرندآبادی، علی‌حسین (۱۳۹۱). *جرم‌شناسی (پیشگیری)*، تهیه‌کننده محمدعلی بابایی، در مجموعه تقریرات، به کوشش شهرام ابراهیمی، ویراست ششم.
۳۴. نمک‌دوست تهرانی، حسن (۱۳۸۳). *آزادی اطلاعات و حق دسترسی؛ بنیان دمکراسی*، مرکز پژوهش‌های مجلس شورای اسلامی.
۳۵. یزدانی زنور، هرمز (۱۳۸۸). «بررسی نقش شفافیت در تحقق حکمرانی مطلوب»، *حقوق عمومی*، ش ۵.

ب) انگلیسی

36. Gilling, D. (1997). *Crime* prevention *: theory, policy and practice*. London: UCL Press.
37. Grant, H. (2015). *Social crime prevention in the developing world: exploring the role of police in crime prevention*. Switzerland: Springer.
38. Hill, J. & Marion, N. (2016). *Introduction to cybercrime: computer crimes, laws, and policing in the 21st century*. Santa Barbara, CA: Praeger.
39. Nimda top of 2001 malware list. (2002). *Computer Fraud & Security*, 2002 (1) , p.20.
40. Dashora, K. (2011) , Cyber Crime in the Society: Problems and Preventions, *Journal of Alternative Perspectives in the Social Sciences*, Vol 3, No 1, 240-259
41. Ratcliffe, J.H. (2003) 'Intelligence-led policing', *Trends and Issues in Crime and Criminal Justice*, 248, p. 6.
42. Scheb, J. and Scheb, J. (2011). *Criminal law and procedure*. Belmont, CA: Wadsworth Cengage Learning.
43. Von Solms, R. and Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, pp.97-102.
44. Welsh, B. (2007). *Evidence-based crime prevention: scientific basis, trends, results and implications for Canada*. Ottawa: National Crime Prevention Centre.

ج) اینترنتی

45. http://www.rcmp-grc.gc.ca/to-ot/tis-set/cyber-tips-conseils-eng.htm
46. http://www.ircert.com/aboutus.htm
47. https://esfahan.ict.gov.ir/fa/hozahayfaliat/fanavari/apa-%D9%85%D8%B1%DA%A9%D8%B2-%D8%A2%D9%BE%D8%A7
48. http://www.fbi.gov/cyberinvest/protect_online.htm
49. http://www.cyberpolice.ir/page/2551