راهبردهای وضعی پیشگیری از جرایم سایبری*

□ حمید بهره‌مند[۱]
□ حسین‌محمد کوره‌پز[۲]
□ احسان سلیمی[۳]

چکیده

پیشگیری از جرم، نخستین گام برای تحقق عدالت کیفری است. فضای سایبر[۴] به اقتضای ویژگی‌های خاصی که دارد، برای پیشگیری وضعی بسیار مساعد است. رهایی بستر، گمنامی کاربران، آسیب‌پذیری آماج، دشواری شناسایی بزهکاران، سهولت ارتکاب جرم، گستردگی خسارت، کثرت بزه‌دیدگان و کم سن بودن اغلب کاربران، ضرورت پیشگیری وضعی از این جرایم را دو چندان ساخته است، لذا با اِعمال شیوه‌های فنیِ پیشگیری از جرم، می‌توان تا حدّ مطلوبی از این جرایم پیشگیری نمود. مقالهٔ پیش رو می کوشد تا تدابیر وضعی مختلف را ـ با

* تاریخ دریافت: ۱۳۹۲/۸/۱ ـ تاریخ پذیرش: ۱۳۹۳/۲/۱۸.

۱. استادیار دانشگاه تهران (نویسندهٔ مسئول) (bahrmand@ut.ac.ir).
۲. دانشجوی کارشناسی ارشد حقوق کیفری و جرم‌شناسی (kourepaz@ut.ac.ir).
۳. دانشجوی کارشناسی ارشد حقوق کیفری و جرم‌شناسی (ehsansalimi1367@ut.ac.ir).

4. Cyber space.

تکیه بر رهنمودهای ۲۵گانهٔ کلارک- در فضای سایبر تبیین نماید و از این طریق، راهکارهایی را برای کاهش فرصت‌های مجرمانه و افزایش خطر ارتکاب جرم ارائه کند. روش تحقیق در این مقاله توصیفی ـ تحلیلی است و برایند آن، معرفی راهکارهای لازم برای پیشگیری وضعی از جرایم سایبر می‌باشد.
واژگان کلیدی: پیشگیری فنی از جرم، راهبردهای وضعی پیشگیری از جرم، جرایم سایبری، کاهش فرصت‌های مجرمانه.

مقدمه

در عصر حاضر، پیدایش و رشد بی‌سابقهٔ فناوری‌های رایانه‌ای شبکه‌محور، تحولات شگرف و دستاوردهای سترگی را در جهت پیشروی جامعهٔ انسانی به سوی قلّه‌های پیشرفت اجتماعی همراه داشته است. بی‌تردید، عمده‌ترین دلیل شکل‌گیریِ این دنیای جدید، رهایی از این قالب خاکی بوده است که محدودیت‌ها و موانع، بشر را بر آن داشت تا به آرمان خود که دستیابی به دنیایی بی‌مرز است، دست یابد. با این همه، این ارمغانِ ستودنی در کنار امتیازات بی‌همتایی که دارد، گسترهٔ بی‌پایانی از فرصت‌های منحرفانه و مجرمانه را نیز فراهم آورده است که نه تنها بزهکاران را بر شیوه‌های جدید ارتکاب جرم توانمند ساخته است، بلکه افرادی را که پیشتر منحرف نبودند نیز به رفتارهای مجرمانه واداشته است (ویلیامز، ۱۳۹۱: ۴۶). این فضای بی‌پاسبان و رها که هر لحظه بر گسترهٔ آن افزوده می‌شود، فرصت بسیار مناسبی را برای ارتکاب و اختفای جرایم سایبری[1] که تهدیدهای آن به مراتب در مقایسه با محیط واقعی بیشتر است، به مرتکب اعطا می‌کند. علاوه بر این، گمنامیِ هر کاربر اینترنتی کشف و شناسایی

۱. از ابتدای پیدایش جرایم سایبری، حقوق‌دانان و نهادهای دولتی / غیر دولتی و بین‌المللی، تعاریف گوناگونی از آن ارائه کرده‌اند. در تعاریف نخستین به جرم سایبری بیشتر به عنوان جرایم نوظهوری که علیه محرمانگی، صحت و تمامیت داده‌ها ارتکاب می‌یابد، نگریسته می‌شد. در واقع، تا پیش از سال ۲۰۰۱، بیشتر تعاریف، جرم سایبری را به عنوان واسطه‌ای برای حمله به فعالیت‌های اقتصادی ـ تجاری و روش‌های نفوذ در امنیت تبیین می‌کردند. با تصویب کنوانسیون جرایم سایبر در سال ۲۰۰۱، با گنجاندن اصطلاح هرزه‌نگاری کودکان، جرایم «مرتبط با محتوا» را در گسترهٔ جرم‌انگاری قرار داد تا به نوعی حمله به عواطف انسانی را نیز ممنوع سازد. با این توضیح، به نظر می‌رسد تعریف زیر می‌تواند به عنوان تعریف عملیاتی از جرایم سایبری که گونه‌های متفاوت آن را پوشش دهد، به کار رود: «جرمی علیه داده‌ها یا سامانه‌های رایانه‌ای ارتکاب یافته است یا اینکه داده‌ها یا سامانه‌های رایانه‌ای وسیلهٔ ارتکاب آن بوده است» (جهت آشنایی با سایر تعاریف ر.ک: عالی‌پور، ۱۳۹۰: ۱۲۰ـ۱۲۲).

مرتکب را ـ اگر نگوییم غیر ممکن ـ بسیار دشوار ساخته است، به نحوی که این انحرافات، یکی از چالش‌های اصلی تمامی جوامع بشری شده است؛ زیرا می‌توان به تعداد فرصت‌های آن، تهدیدهای اجتماعی، اخلاقی، حقوقی و سیاسی برشمرد (Kizza, 2013: 107). از این رو، آنچه اخیراً ذهن سیاست‌گذاران را به خود مشغول داشته است، این است که «سودمندترین تدبیر» در قبال جرایم سایبری چیست؟

رهیافت غیر کیفری با تکیه بر عامل‌های وضعی ـ فنیِ بزهکاری ـ یعنی وضعیت‌های پیش‌جنایی ـ در صدد است تا از گذر انحراف در فرایند گذار اندیشه به عمل، زمینهٔ تحقق فرصت‌های ارتکاب جرم را خنثی سازد و از آماجِ آسیب‌پذیر محافظت نماید (نجفی ابرندآبادی، ۱۳۸۸: ۷۱۷). بنابراین، در دهه‌های اخیر، بار دیگر پیشگیری وضعی ـ البته بر خلاف شیوهٔ خودجوش و سنتی گذشتهٔ خود ـ مطرح گردید؛ زیرا مدیریت وضعی پیشگیرانه، بر این نکته تأکید دارد که بزهکاری، تنها محصول عوامل اجتماعی ـ روانی نیست و شرایط موقعیتی، تأثیر به سزایی در بروز رفتارِ مجرمانه دارند. چه بسا، پیشگیری وضعی، اثربخش‌تر از پیشگیری اجتماعی نیز باشد. فرضیهٔ این مدعا آن است که در تقابل شخصیت با وضعیت، آنچه زودتر از پای درمی‌آید، وضعیت است و پیچیدگی‌های انسانی، مانع شکست شخصیت می‌شود. این مقاله، نگاهی بر ایمن‌سازی آماج جرم دارد تا از گذر آن، آماج‌های در معرض خطر و آسیب‌دیده را تقویت کند. به همین منظور، باید از خود فضای سایبر ـ به مثابهٔ پادزهر ـ استمداد جست.[۱]

اگرچه هیچ آمار قطعی در زمینهٔ جرایم سایبری وجود ندارد، شواهدِ روایی از جمله پیمایش صورت‌گرفته توسط ادارهٔ تحقیقات فدرال (آمریکا)[۲] و مؤسسهٔ امنیت رایانه[۳] با قاطعیت حکایت از آن دارند که بازدارندگی سنتی در پیشگیری از جرایم سایبری

---

۱. عبارت اخیر بدان معناست که با پیشرفت فناوری‌های نوین و گسترش آن در عرصه‌های گوناگون، تدابیر وضعی نیز باید همگام با آن به‌روزرسانی شده و با بهره‌برداری از همین فناوری‌ها، به مبارزه با جرایم برخاست. بدین خاطر، امروزه دیگر پیشگیری وضعی، چهره‌ای فنّی پیدا کرده و با عنوان «پیشگیری فنّی از جرم» (Technical prevention of crime) شناخته می‌شود (خانعلی‌پور واجارگاه، ۱۳۹۰: ۱۳). در این مقاله نیز منظور ما از پیشگیری وضعی، «پیشگیری وضعیِ فناورانه» یا «پیشگیری فنّی» است.

2. Federal Bureau of Investigation (FBI).

3. Computer Security Institute (CSI).

ـنسبت به جرایم سنتی ـ حتی تأثیر کمتری دارد (Turrini, 2010: 369). لذا اقدامات پیشگیرانهٔ موقعیت‌مدار در برابر جرایم سایبری ـحتی بیش از جرایم سنتی ـ بیش از هر اقدام دیگری، ضروری به نظر می‌رسند.

با این حال نباید تصور شود که تنها با کاربستِ تدابیر وضعی می‌توان از جرایم سایبری پیشگیری نمود؛ زیرا این اقدامات مصون از محدودیت و ایراد نیستند که جابه‌جایی و محدودیت‌های حقوق بشری از مهم‌ترین آن‌هاست (دربارهٔ محدودیت‌های پیشگیری وضعی ر.ک: گسن، ۱۳۷۶: ش۱۹ـ۶۱۳/۲۰ به بعد). دربارهٔ جابه‌جایی در فضای سایبر باید گفت که هرچند امکان وقوع انواع جابه‌جایی وجود دارد، جابه‌جایی شیوهٔ ارتکاب، مرسوم‌ترین روشی است که بزهکاران سایبری به منظور دور زدن و از میان برداشتن موانع، از آن بهره می‌برند و به محض شکست یا ناکامی در یک روش، به سرعتْ شگردی روزآمد یا جدید را اتخاذ می‌نمایند. این امر موجب می‌شود تا بزهکاران بتوانند در این بازهٔ زمانی ـاز شگردهای جدید تا کاربست تدابیر وضعیِ محدودکننده‌ـ، هر نوع بهره‌برداری را از فضای سایبر داشته باشند. پس حداقل، این دسته تدابیر برای مبارزه با این جرایم در مقطعی ناتوان هستند.[۱]

تدابیر پیشگیری وضعی حتی در شکل حداقلی خود، موجب محدودسازی آزادی‌های فردی می‌گردند. بارزترین نمونهٔ این امر در فضای سایبر، فیلترینگ نامناسب و غیر کارشناسی است که صرفاً به خاطر استعمال یک یا چند واژهٔ غیر مجاز در یک متن علمی، بخشی از جامعه از یافته‌های آن اثر محروم می‌شوند. این امر، علاوه بر اینکه ناشی از کاربستِ غیر اصولی و بی‌برنامه است، به ماهیت تدابیر وضعی نیز که میان بزهکار و ناکرده بزه تفکیک قائل نیست، برمی‌گردد (پاک‌نهاد، ۱۳۸۸: ۲۶۶). همچنین می‌توان به ابزارهای ردیابی ـ نظارتی متهمان و نیز سرویس‌های تصدیق هویت ـکه اطلاعات کاربران را در اختیار ارائه‌دهندگان خدمات اینترنتی قرار می‌دهد و زمینهٔ

۱. به عبارت دیگر، تدابیر وضعی در قبال بزهکاران مختلف، به یک شکل عمل نمی‌کند. در این راستا، بزهکاران حرفه‌ای هرچند در وهلهٔ نخست از آنچه در سر می‌پرورانند، منصرف می‌شوند، این امر پایدار نیست و آن‌ها با ادامه دادن به مسیر بزهکاری تلاش می‌کنند تا به استقبال این موانع رفته و به اهداف خود جامهٔ عمل بپوشانند (بابایی و نجییان، ۱۳۹۰: ش۱۵۸/۷۵).

سوءاستفادهٔ آن‌ها را فراهم می‌آورد- اشاره نمود. بنابراین در راستای بعضی از اقدامات وضعیِ پیشگیرانه، ارائه‌دهندگان خدمات شبکه‌ای، مأموران اجرای قانون و سایر افراد، به بهانهٔ نظارت و دفع تهدیدهای احتمالی، بدون ضابطهٔ مشخص در حریم خصوصی افراد دخالت می‌نمایند. نظریهٔ جرم‌شناختیِ پایه‌ای که در این مقاله طرح می‌شود، نظریهٔ «فعالیت روزانه» است. از آنجا که نظریهٔ «فعالیت روزانه» به تبیین دقیق نقشِ فرصت‌های مجرمانه می‌پردازد و برای آماجِ آسیب‌پذیر، اصالت ویژه‌ای در تحلیلِ رفتار مجرمانه قائل است، می‌تواند درک مطلوبی از رفتار مجرمانه در فضای سایبر -حتی بیش از جرایم واقعی- به ما ارائه نماید. از این رو، به نظر می‌رسد که این نظریه، دیدگاهی مناسب برای پیشگیری وضعی از جرایم سایبری است.

در این دیدگاه، لورنس کوهن[1] و مارکوس فلسون[2] پس از آنکه رویداد مجرمانه[3] را محصول فعالیت‌های روزانه، همکنش‌های اجتماعی عادی میان بزهکار و بزه‌دیده و ناشی از تحولات بنیادین -نظیر رشد فناوری- دانستند، وجود سه متغیر را امری کلیدی در شکل‌گیری آن رویداد ارزیابی کردند:[4] ۱. مجرم باانگیزه؛[5] ۲. آماج مناسب؛[6] ۳. فقدان مانع (محافظ)[7] (Felson, 2008: 70). بنابراین، این نظریه نشان می‌دهد که افزایش و کاهش جرایم، تابعی از شمار آماج‌های مناسب جرم یا تعداد موانع موجود بر سر راه ارتکاب جرم است.

دربارهٔ متغیر نخست باید اشاره کرد که ویژگی‌هایی مانند ناشناختگی[8] و مخفی ماندن هویت در فضای سایبر سبب می‌شوند بزهکاران و حتی کسانی را که قبلاً

1. Lawrence Cohen.
2. Marcus Felson.
3. Criminal event.
۴. این نظریه بیشتر به اوضاع و احوال یا شرایط مشرف به ارتکاب جرم توجه دارد. فعالیت‌های عادی یا روزانه، به معنای هر فعالیت اجتماعی عادی است که برای برآوردن نیازهای اساسی -نظیر کار رسمی، تربیت فرزند، تفریح کردن، یافتن محل سکونت و غیره- انجام می‌پذیرد (ویلیامز و مک‌شین، ۱۳۸۸: ۲۴۳).
5. Motivated offender.
6. Suitable targets.
7. Absence of capable guardian.
8. Anonymity.

منحرف نبودند، به ارتکاب جرم تحریک نمایند.

در این دیدگاه، مناسب بودن آماج، نقش کلیدی در درک رفتار مجرمانه ایفا می‌نماید. این مناسب بودن، در معیارهای چهارگانهٔ زیر تبیین می‌شود.[۱]

الف) ارزشمند بودن:[۲] این معیار، بسته به نوع نگرش و انگیزهٔ مجرم متفاوت است و ارزشمند بودن یک هدف، امری شخصی محسوب می‌شود. فضای سایبر که سرشار از داده‌ها و اطلاعات متنوع و گران‌بها و زمینه‌های ارتکاب جرایم مالی است، ممکن است افراد را به انگیزه‌های مختلف به خود مجذوب سازد.

ب) مقاومت‌پذیری:[۳] مقاومت یا سستی شخص یا هدف در برابر حملات، مقادیر متنوعی دارد. هر چه یک هدف مقاوم‌تر باشد، میل به تهاجم نسبت به آن نیز کمتر خواهد بود. در فضای سایبر نیز چنانچه سامانه‌ها و شبکه‌ها مقاوم‌سازی نشوند، به راحتی مورد حمله قرار می‌گیرند.

ج) رؤیت‌پذیری:[۴] به این معناست که مجرمان پس از آنکه نشانه‌هایی را از هدف خود ملاحظه کردند، به سمت آن حمله می‌کنند. شاید هیچ محیطی مانند فضای سایبر، تا این اندازه مشاهده‌شدنی نباشد. از این جهت نیز بزهکاران احتمالی را به ارتکاب جرم برمی‌انگیزد.

د) دسترس‌پذیری:[۵] در فضای سایبر، همه چیز را می‌توان به اشتراک گذاشت و این مزیت در این فضا بیش از هر جای دیگر قابل ملاحظه است. افراد علاوه بر اینکه به راحتی می‌توانند به داده‌ها دست یابند، به آسانی نیز می‌توانند آن‌ها را دستکاری نمایند

---

۱. در این نظریه، انتخاب واژهٔ هدف (Target) به جای لفظ بزه‌دیده (Victim) به این خاطر است که در زمان طرح این نظریه (۱۹۷۰)، در استفاده از لفظ بزه‌دیده، تمایزی میان حمله به یک شخص (نظیر مورد ضرب و جرح واقع شدن) یا حمله به یک شیء (سرقت از یک منزل خالی از سکنه) قائل نمی‌شد و ذهنْ تنها منصرف به مورد اول می‌شد؛ زیرا در دههٔ هفتاد میلادی تحقیقات بزه‌دیده‌شناسی به اوج خود رسید و انتخاب واژهٔ «بزه‌دیده» تنها بزه‌دیده واقع شدن یک شخص را به ذهن متبادر می‌ساخت (Felson, 2008: 71).

2. Value.

3. Inertia.

4. Visibility.

5. Accessibility.

.(McLaughlin, 2001: 253)

فقدان مانع (محافظ): گسترهٔ فضای سایبر دارای اهداف مناسبِ بی‌شماری است و این امر، برانگیختگی مضاعف هر بزهکاری را در پی دارد. از این رو، این متغیر در مقایسه با دو متغیر پیشین (مجرم باانگیزه و آماج مناسب)، اهمیت فراوانی دارد. در واقع، کاربست نظریهٔ «فعالیت روزانه» در فضای سایبر، ما را به این رهنمون می‌سازد که میزان بزه‌دیدگی با میزان محافظت، همبستگی و ارتباط بیشتری دارد (زررخ، ۱۳۹۰: ش۱۴۶/۶۴).

در فضای سایبر، تدابیری که موجب دشواری دسترسی به آماج یا بزه‌دیده و ایمن‌سازیِ هدف می‌شوند، از طریق نرم‌افزارهای امنیتی ـ نظیر دیوار آتشین[1] و ضد ویروس‌ها[2] ـ یا ارتقای میزان دانش و تخصص از فناوری‌های رایانه‌محور تأمین می‌گردد (Ngo & Paternoster, 2011: 776). دربارهٔ مورد اخیر باید گفت که در بسیاری از موارد، فرد از اینکه مورد حمله واقع شده، بی‌خبر است (برای مطالعهٔ بیشتر ر.ک: جلالی فراهانی و منفرد، ۱۳۹۲: ش۱۶۵/۷۳ به بعد). در گفتار سوم، به تفصیل به راه‌های ایمن‌سازی خواهیم پرداخت.

انتقاد وارد به این نظریه آن است که در تحلیل پدیدهٔ مجرمانه، به عوامل روانی ـ اجتماعیِ شخصیت توجه نشده است. در پاسخ به این ایراد باید گفت که این نظریه، در بستر شکستِ پیشگیریِ اجتماعی مطرح شده و به هیچ عنوان ادعای متعالی کردن جامعهٔ خود را نداشته است. ضمن اینکه این انتقاد نه تنها به این نظریه، بلکه به مجموعهٔ اندیشه‌هایی که فرصت‌محورند، وارد است (برای مطالعهٔ بیشتر ر.ک: صفاری، ۱۳۸۱: ش۲۳۴ـ۱۹۳/۳۶ـ۳۵).

باید اشاره کرد که هرچند این نظریه، بر اساس فضای واقعی مطرح شده است، با کاربست آن در فضای سایبر روشن می‌شود که حتی بیش از جرایم واقعی، در توصیف و تبیین جرایم سایبری موفق بوده است؛ زیرا هر یک از عناصر سه‌گانهٔ بیان‌شده، به طور چشم‌گیرتر و ملموس‌تری در فضای سایبر ملاحظه می‌شوند.[3]

---

1. Firewall.
2. Antivirus.
۳. شایان ذکر است که به منظور علت‌شناسیِ جرایم سایبری، نمی‌توان صرفاً به نظریه‌های جرایم کلاسیک بسنده کرد، بلکه باید در کنار آن‌ها، رویکرد جرم‌شناختیِ مستقلی را متناسب با این فضا طراحی کرد (نجفی ابرندآبادی، ۱۳۹۰: ۱۴).

کلارک،[1] پیشگیری وضعی را شامل تدابیری به منظور کاهش فرصت‌های مجرمانه می‌داند که: اولاً، به سوی اَشکال خاصی از جرایم معطوف شده‌اند. ثانیاً، شامل مدیریت، طراحی و دستکاری در محیط به صورت نظام‌مند و دائمی می‌باشند و در نهایت، برای دشوارتر و پرخطر کردن ارتکاب جرم یا کاهش منافع به دست‌آمده از آن استفاده می‌شوند (Clarke, 1997: 4). به طور خلاصه پیشگیری وضعی عبارت است از: «ایجاد تغییر نظام‌مند و دائمی در محیط، به منظور کاهش فرصت‌های مجرمانه و افزایش خطر ارتکاب جرم».[2]

کُرنیش و کلارک، پنج راهبرد اصلی[3] را برای پیشگیری وضعی از جرایم پیشنهاد می‌کنند که هر یک از این راهبردها، پنج راهکار ـ راهکارهای ۲۵گانهٔ پیشگیری وضعی ـ را در بر می‌گیرند. این پنج راهبرد اصلی، به شرح زیر هستند: ۱. افزایش میزان تلاش به منظور ارتکاب جرم؛[4] ۲. افزایش خطرهای ارتکاب جرم؛[5] ۳. کاهش دستاوردها؛[6] ۴. کاهش عوامل محرک؛[7] ۵. سلب توجیه‌ها[8] (Cornish & Clarke, 2003: 90). در مقالهٔ پیش رو، این راهبردهایِ پنج‌گانه، ذیل دو دستهٔ «راهبردهای ایجابی» و «راهبردهای سلبی» بررسی می‌شوند.

فراگیر بودن این راهبردها سبب می‌شود تا در انواع مختلف جرایم ـ حتی جرایم نوینی

---

1. Clarke.

۲. معمولاً در تعاریفی که از پیشگیری وضعی ارائه می‌شود، بر دو دسته از تدابیر تأکید می‌شود. نویسندگان، یا به تدابیری که در صدد دشوارسازیِ دسترسی به آماج یا بزه‌دیدگان است، اشاره می‌کنند یا اساس تعریف خود را بر کاهشِ عوامل محرک و جذاب قرار می‌دهند (میرخلیلی، ۱۳۸۸: ۳۶). البته باید اشاره کرد که با کاربست تدابیر دستهٔ نخست ـ بالا بردن هزینهٔ ارتکاب جرم و کاهش عواید حاصل از آن ـ خودبه‌خود می‌توان موجبات عدم تمایل و کشش مرتکب نسبت به آماج را فراهم آورد. از این رو، در تعریف خود تنها به چنین تدابیری اشاره کردیم.

۳. در اینجا کرنیش و کلارک، واژهٔ راهبرد (Strategy) را به معنای تدابیر اصلی و کلّی‌ای به کار برده‌اند که هر یک از آن‌ها شامل پنج راهکار می‌شود.

4. Increase the effort.

5. Increase the risks.

6. Reduce the rewards.

7. Reduce provocations.

8. Remove excuses.

چون جرایم سایبری- بتوان آن‌ها را به کار بست.

جستار حاضر تلاش می‌کند تا بر مبنای الگویی که کلارک ارائه کرده است، گونه‌های راهبردهای وضعی را که می‌توانند در پیشگیری از جرایم سایبری مؤثر باشند، در دو قالب راهبردهای ایجابی و سلبی بررسی کند.

۱. راهبردهای ایجابی

راهبردهای ایجابی، مجموعهٔ تدابیری هستند که با تأسیس و کاربستِ آن‌ها می‌توان موجبات ایمن‌سازی محیطی را فراهم آورد. از میان راهبردهای کلارک، تدابیر دشوارکننده و خطرافزا، به نحو ایجابی سعی در پیشگیری محیطی دارند که در زیر به آن‌ها اشاره می‌گردد:

۱ـ۱. افزایش میزان تلاش برای ارتکاب جرم

مقصود از افزایش میزان تلاش برای ارتکاب جرم آن است که اقداماتی صورت بگیرد تا هزینهٔ مادی ارتکاب جرم برای مرتکب بالا رود. یکی از ویژگی‌های ممتاز و در عین حال ارزشمند فناوری اطلاعات و ارتباطات الکترونیکی نسبت به دیگر فناوری‌ها، سهولت استفاده از آن است (جلالی فراهانی، ۱۳۸۹: ۱۵). بنابراین ارتکاب جرم در محیط سایبر نیز کاری بسیار راحت است. افراد با داشتن یک رایانهٔ متصل به اینترنت و سواد رایانه‌ای اندک می‌توانند مجرمی بالقوه باشند. عدم مجاورت فیزیکی بزهکار و بزه‌دیده نیز ارتکاب این جرایم را آسان‌تر کرده است. در ادامه، سازوکارهای دشوارسازیِ ارتکاب جرایم سایبری بررسی می‌شوند.

۱ـ۱ـ۱. تقویت آماج‌ها[1]

با استفاده از تدابیر امنیتی می‌توان به میزان قابل توجهی دسترسی به آماج‌های جرم را محدود نمود. منظور از تدابیر امنیتی، «ایجاد ممنوعیت یا محدودیت دسترسی به داده‌ها و اطلاعات برای افراد غیر مجاز با توجه به طبقه‌بندی و ارزش محتویات آن‌هاست»

1. Target harden.

(الهی‌منش و سدره‌نشین، ۱۳۹۱: ۱۴). پالایه/ فیلترینگ، شیوهٔ مناسبی برای دشوارسازی دسترسی به آماج جرم است که برای کنترل و محدود کردن دسترسی به شبکه و برخی خدمات اِعمال می‌شود (خانعلی‌پور واجارگاه، ۱۳۹۰: ۱۲۷). بنابراین پالایش نظام‌مند می‌تواند تا حدّ زیادی از ارتکاب جرایم رایانه‌ایِ از پیش تعیین‌نشده ـ به وسیلهٔ مجرمان اتفاقی ـ جلوگیری کند.

با پیشرفت شیوه‌های فنیِ دسترسی غیر مجاز به رایانه‌ها و شبکه‌ها، به کارگیری نرم‌افزارهای مقابله با این شیوه‌ها بسیار ضروری است. برنامه‌های هک‌کنندهٔ سامانه‌ها با نام «اسب‌های تروا»،[1] رایج‌ترین و بهترین نمونه برای بیان پیشرفت فنیِ شیوه‌های دسترسی غیر مجاز است. استفاده از برنامه‌های ضد ویروس و به‌روزرسانی مرتب این برنامه‌ها، تا حد زیادی می‌تواند در مقابله با حملات اسب‌های تروا مؤثر باشد. با این حال، حتی اگر اکثر برنامه‌های ضد ویروس به طور کامل به‌روزرسانی شوند، همچنان در برابر همهٔ ویروس‌های رایانه‌ای و اسب‌های تروا، مصونیت کافی ندارند. در واقع، نباید برنامه‌های ضد ویروس را مهم‌ترین حصار امنیتی سامانه دانست؛ زیرا آن‌ها صرفاً ابزارهایی هستند که ضریب و احتمال آلوده شدن سیستم را کاهش می‌دهند.

برای اطمینان از بالا بودن ضریب امنیت یک سامانهٔ رایانه‌ای می‌توان میزان نفوذپذیری آن را با آزمون نفوذپذیری[2] سنجید. در آزمون نفوذپذیری که برای اعطای گواهی امنیت به سامانه انجام می‌شود، ارزیاب‌ها تلاش می‌کنند تا با فریب سامانهٔ امنیتی، راه‌های نفوذ به لایه‌های مختلفِ منابع سامانه را کشف کنند (سادوسکای و دیگران، ۱۳۸۴: ۵۵).

۱ـ۱ـ۲. کنترل ورودی‌ها

کلارک این راهکار را تحت عنوان «کنترل دستیابی به اهداف»[3] مطرح می‌نماید. البته مثال‌های وی ـ نظیر استخدام نگهبان برای آپارتمان، استفاده از رمز عبور برای کارت‌های الکترونیکی ـ بیانگر چیزی جز کنترل ورودی‌ها نمی‌باشد. کنترل ورودی، اهمیت

1. Trojan horses.
2. Penetration test.
3. Control access to facilities.

فراوانی در پیشگیری از جرایم رایانه‌ای دارد. بسیاری از سامانه‌ها، اطلاعات مربوط به تلاش‌های موفق یا ناموفق افراد را در ورود به سیستم ثبت می‌کنند. با کنترل ورودی‌ها باید از میزان داده‌های واردشده، نوع و منشأ آن‌ها ـ به ویژه در حالت‌هایی که به دلیل بالا بودن هزینه، امکان به کارگیری کنترل‌های دو لایه و تفکیک‌های تهیهٔ مجوز وجود نداشته باشد ـ اطلاع و اطمینان حاصل نمود (زیبر، ۱۳۹۰: ۲۱۹). راه‌های گوناگونی برای کنترل ورودی‌ها وجود دارد که ساده‌ترین آن‌ها، استفاده از رمز عبور در رایانه است. بدیهی است که بالا بردن ضریب کنترل می‌تواند به مثابهٔ مانعی در برابر مجرمان باانگیزه عمل کند و آن‌ها را در دستیابی به آماج جرم ناکام بگذارد.

از دیگر راهکارهایی که می‌تواند به عنوان کنترل ورودی عمل کند، استفاده از شبکه‌های مجازیِ کاوشگرهای الکترونیک است. این کاوشگرها ـ که از آن‌ها به پلیس مجازی تعبیر می‌شود ـ وظیفهٔ تشخیص هویت‌های مجازی، اعتبارسنجی امضاهای الکترونیک، کنترل دسترسی‌های مجاز به محتوای محرمانهٔ داده‌ها و حتی تشخیص مصادیق محرمانهٔ منتشرشده را به عهده دارند (خالقی پوستچی، ۱۳۸۸: ۴۶). تجهیز شرکت‌ها و سازمان‌ها به این سیستم‌های نظارتی و کنترلی، شیوهٔ مناسبی برای پیشگیری از جرم است. این بازرسی‌های خودکار رایانه‌ای، به ویژه برای انجام بررسی‌های متوالی، بررسی‌های مربوط به معقول بودن ورودی‌ها، بازرسی‌های مربوط به حدود بالا و پایین و بازرسی‌های ویژهٔ مربوط به تصحیحات تعدیل‌کننده، باید به صورت گسترده و موردی به کار گرفته شوند (زیبر، ۱۳۹۰: ۲۱۹).

یکی از بهترین شیوه‌های پیشگیری وضعی، استفاده از «دیوار آتشین» است. دیوار آتشین، یک سیستم حفاظتی است که جریان ترافیک ورودی به شبکه‌ها و گاهی میان آن‌ها را کنترل می‌کند. برای دیوار آتشین، پیکربندی‌ها و کاربردهای مختلفی وجود دارد که صافی‌ها، تقویت‌کننده‌ها، برنامه‌های کاربردی، رمزگذاری،[1] ایجاد منطقهٔ غیر نظامی[2] و... از جملهٔ آن‌هاست. دیوارهای آتشین به دو شکل وجود دارند: نخست، دیوار آتشین می‌تواند یک برنامهٔ نرم‌افزاری باشد که بر روی رایانه اجرا می‌شود. دوم، ممکن است

1. Encryption.
2. Demilitarized zone (DMZ).

یک قطعهٔ مجزای سخت‌افزاری باشد که بر آنچه روی شبکه فرستاده و دریافت می‌شود، نظارت می‌کند. آن‌ها قادرند ارتباطات میان کاربر و دنیای خارج را کنترل نمایند یا از انتقالات پیش‌بینی‌نشده یا غیر مجاز جلوگیری کنند (سادوسکای و دیگران، ۱۳۸۴: ۴۵۹).

۱ـ۱ـ۳. کنترل و بازرسی خروجی‌ها[1]

هرچند کنترل ورودی‌ها، اهمیت فراوانی دارد؛ زیرا با دور زدن و خنثی‌سازی کنترل‌های ورودی، ضمن دسترسی به داده‌های محرمانه، احتمال خروج را با موفقیت بیشتری همراه می‌سازد، اما کنترل و بازرسی خروجی‌ها نیز مکمّل کنترل ورودی‌هاست. با کنترل خروجی‌ها باید همهٔ داده‌هایی که منشأ خود را ترک می‌کنند، بررسی و نظارت کامل شوند. در این کنترل، علاوه بر اینکه باید تمامی راهکارهای قانونیِ خروج اطلاعات مد نظر قرار گیرد، باید به احتمال نشت اطلاعات به خارج ـبه ویژه در ارتباطات راه دور و انتشار الکترونیکیـ توجه کرد. همچنین، تمامی داده‌های ذخیره‌شده باید از علایم متمایزکننده ـبه ویژه علایم حق نشر، علایم شناسایی مخفی و شماره‌های سریالیـ که اصالت داده‌ها را به اثبات می‌رسانند، برخوردار باشند (زیبر، ۱۳۹۰: ۲۲۳).

برای پیشگیری از جرایم علیه محرمانگیِ[2] داده‌ها می‌توان با انجام فراگردِ رمزگذاری داده‌ها، به بالا رفتن هر چه بیشتر امنیت خروجی‌ها کمک نمود. در این راستا، با روش الگوریتم رمزگذاری می‌توان برای پنهان‌سازی اطلاعات اقدام نمود، به صورتی که پیامِ داده‌ها ـبه جز برای دریافت‌کنندگان مورد نظرـ به سادگی دریافت نشود. در این روش، با تغییر یک رشته از حروف به یک رشتهٔ دیگر، محتویات پرونده‌ها و برنامه‌ها به سختی قابل درک می‌باشد. در ساده‌ترین نوع رمزگذاری، یک «کلید» وجود دارد که برای مخفی نمودن اطلاعات، از آن استفاده می‌شود. بدیهی است که رمزگشایی[3] از این اطلاعات نیز تنها در سایهٔ کشفِ این کلید ممکن است.

1. Screen exits.
2. Confidentiality.
3. Decryption.

۱ـ۱ـ۴. تغییر مسیر بزهکاران[1]

تغییر مسیر به معنایِ کاربستِ تدابیری است که از ایجاد ارتباط و ملاقات میان بزهکاران احتمالی با بزه‌دیدگان و آماج‌های آسیب‌پذیر جلوگیری می‌کند (ابراهیمی، ۱۳۹۱: ۱۲۳). بدین‌سان باید مسیرهایی را که موجبات تماس و تنش میان بزهکاران احتمالی با آماج ــ یا بزه‌دیده ـ را فراهم می‌آورد، مسدود کرد. آموزش بزه‌دیدگان آسیب‌پذیر ـ کودکان و زنان ـ برای عدم برقراری ارتباط با افراد مظنون، یکی از بهترین شیوه‌های تغییر مسیر مجرمانه به شمار می‌رود.

آمارهای موجود بیانگر این واقعیت هستند که از یک سو، جوانان ۱۶ تا ۲۴ ساله بیشترین حضور را در فضای مجازی دارند[2] و از سوی دیگر، در فضای مجازی ـ از میان همهٔ گروه‌های سنی ـ آسیب‌پذیرترند؛ زیرا جوانان و نوجوانان، خودشان را بیشتر در معرض این تهدیدها قرار می‌دهند.

اتاق‌های گپ،[3] یکی از ناامن‌ترین قسمت‌های دنیای مجازی برای نونهالان و نوجوانان هستند که باید به شدت از آن‌ها محافظت کرد.[4] بر اساس بررسی انجام‌شده در ایالات متحدهٔ آمریکا، تقریباً ۳۴ درصد افراد بیان کردند که در اتاق‌های گپ مورد تهاجم قرار گرفته‌اند و مهاجمان، فشارهای روانی مختلفی را بر آن‌ها تحمیل کرده‌اند (Katzer, Fetchenhauer & Belschak, 2009: 25). یکی از شیوه‌های ایجاد مانع در برخورد بزه‌دیده با بزهکار، تفکیک سنّی اتاق‌های گپ و جداسازی نوجوانان از بزرگسالان است. راهکارهای عملیِ متفاوتی را برای این امر می‌توان به کار گرفت که یکی از

---

1. Deflect offenders.

۲. سنجشی که در سال ۲۰۰۳ میان برخی از کشورها، پیرامون ردهٔ سنی کاربران اینترنت انجام شد، نشان داد که در کشورهایی نظیر کره (۹۵ درصد)، ایالات متحدهٔ آمریکا (۹۱ درصد)، ژاپن (۸۱ درصد) و انگلستان (۸۰ درصد)، کودکان و نوجوانانِ ۱۶ تا ۲۴ ساله، بیشترین استفاده از اینترنت را داشته‌اند (توکل و کاظم‌پور، ۱۳۸۴: ۱۲۰).

3. Chat room.

۴. بنا بر گزارش ایران آی‌تی که از آمار وبگاه یاهو مسنجر به دست آمده است، جوانان ایرانی سالانه حدود ۵ میلیارد ریال صرف گپ اینترنتی می‌کنند و به طور متوسط در شبانه روز حدود ۲۰۰ نفر در اتاق‌های گپ ایرانی حضور دارند که این تعداد در هیچ اتاق گپ دیگری در سایر کشورها مشاهده نمی‌شود (سالاری، ۱۳۸۶: ۲۷۸).

آن‌ها، نظام‌مند کردن اتاق‌های گپ و الزام کاربران به ثبت‌نام حضوری است. راه دیگری که جنبهٔ عملی بیشتری دارد این است که اجازهٔ ورود به محیط گپ، تنها در صورت پاسخ‌گویی به پرسش‌هایی باشد که معمولاً یک کودک از پاسخ به آن‌ها ناتوان است.

۱ـ۱ـ۵. کنترل ابزارها[1]

مقید به وسیله بودنِ جرایم سایبری، پیشگیری از آن‌ها را تسهیل می‌کند؛ زیرا بدون استفاده از رایانه و ورود به فضای سایبر، ارتکاب آن‌ها ممکن نیست. در نتیجه، با اِعمال محدودیت‌های لازم بر وسیله، می‌توان ارتکاب این جرایم را به نحو چشمگیری کاهش داد. این امر، امتیازی برای پیشگیری وضعی از جرایم سایبری محسوب می‌شود ـ که پیشگیری وضعی از جرایم سنتی از آن بی‌بهره است ـ؛ زیرا در جرایم سنتی، کمتر عامل مؤثری را می‌توان میان آماج جرم و مجرم قرار داد. مقید به وسیله بودنِ جرایم رایانه‌ای و امکان ساماندهی و تنظیم ارتباطات، امکان کنترل ابزارهای ارتکاب جرم را فراهم نموده است؛ به عنوان مثال، برای جلوگیری از تداخل باند و رعایت مسائل ایمنی و فنی و برخی ملاحظات امنیتی، می‌توان به راحتی با کنترل استفادهٔ غیر قانونی از پهنای باند بین‌المللی، از وقوع برخی جرایم پیشگیری نمود.

۱ـ۲. افزایش خطر ارتکاب جرم[2]

این راهبرد می‌کوشد تا با کاربستِ تدابیر نظارتی ـ مراقبتی، خطرات ارتکاب جرم را افزایش دهد و از این رهگذر، مانع از وقوع جرایم یا کاهش احتمال ارتکاب آن‌ها شود.

۱ـ۲ـ۱. توسعهٔ محافظت‌ها[3]

محافظت در فضای مجازی تا حدّ زیادی متمایز از حفاظت در دنیای واقعی است. بدیهی است که در فضای مجازی نیز باید از محافظ‌های متناسب با ماهیت آن استفاده نمود. دیوار آتشین و برنامه‌های ویروس‌یاب از شیوه‌های محافظتیِ پیشگیرانه در برابر تهدیدهای سایبری می‌باشند. همان طور که اشاره شد، دیوار آتشین، ترکیبی از سخت‌افزار و نرم‌افزار است

1. Control tools.
2. Increase the risks.
3. Extend guardianship.

که یک شبکه را از لحاظ امنیتی به دو یا چند بخش تقسیم می‌کند. به کارگیری این دیواره‌های دفاعی، بهترین راه برای کاهش هرزنامه‌هاست[1] (داتن، ۱۳۸۴: ۷۱).

استفاده از پیشکار / پروکسی‌ها[2] را نیز باید روش دیگری برای پیشگیری وضعی از این جرایم دانست. از جمله کاربردهای پیشکار می‌توان به ارتقای امنیت رایانه اشاره کرد. با استفاده از پیشکارها، کاربران به جای اینکه مستقیم به اینترنت متصل شوند، همگی از طریق یک پیشکار به اینترنت متصل می‌شوند. یک سرور / کارساز پیشکار، تماس با اینترنت را میان تمام رایانه‌هایی که به شبکهٔ محلّی متصل می‌باشند، تقسیم می‌کند. به طور کلّی پیشکار، کارسازی است که به عنوان یک واسط بین کاربر و کارساز عمل می‌کند. هنگامی که رایانه‌ای از طریق پیشکار به اینترنت وصل است و می‌خواهد به یک پرونده دسترسی پیدا کند، باید ابتدا درخواست خود را به یک کارسازِ پیشکار ارسال نماید. آنگاه پیشکار به رایانهٔ مقصد متصل می‌شود و پروندهٔ درخواستی را دریافت می‌کند.

یکی دیگر از شیوه‌های محافظت، مراقبت از داده‌هایی است که حمله به آن‌ها بسیار محتمل است. در واقع می‌توان با اِعمال نظارت مداوم نسبت به چنین مواردی، از آن‌ها حمایت کرد. این حمایت مداوم، از آسیب‌پذیری آماج می‌کاهد و این هشدار را به مرتکب خواهد داد که در صورت ارتکاب جرم مورد نظر، احتمالاً شناسایی و دستگیر خواهد شد. مزیت مهم ردیابی رفتار از طریق آماج بالقوه در مقایسه با ردیابی از طریق خود مجرم، تضییق کمترِ حق آزادی و حریم خصوصی وی است (خانعلی‌پور واجارگاه، ۱۳۹۰: ۱۰۹).

۱ـ۲ـ۲. کاهش ناشناختگی[3]

بی‌چهرگی و ناشناختگی بزهکاران سایبری، یکی از ویژگی‌های ممتاز فضای سایبر

---

1. Spam.
2. Proxy.
۳. Reduce anonymity؛ کلارک، ذیل راهبرد افزایش خطرات ارتکاب جرم، پیش از اشاره به راهکار کاهش ناشناختگی، از روش افزایش نظارت طبیعی (Assist Natural Surveillance) ـنظیر افزایش روشنایی خیابان‌هاـ یاد می‌کند. بدیهی است که این راهکار به دلیل مجازی بودن محیط سایبر، اعمال‌شدنی نیست.

است که به خطر مضاعف این جرایم دامن می‌زند. به بیان دیگر، از یک سو ناشناخته ماندن مجرم، موجب دشواری کشف جرم می‌شود و از سوی دیگر، این گمنامی تجرّی بزهکاران را به همراه دارد. جعل پروتکل اینترنتی[۱] و استتار برخط،[۲] شیوه‌های مرسوم تغییر هویت می‌باشند که از لحاظ سهولت، با شیوه‌های مشابه آن در جرایم سنتی ـ نظیر گریم، جراحی پلاستیک و جعل سند ـ قابل مقایسه نیستند (جوان جعفری، ۱۳۸۵: ۲۷).

کاهش گمنامی کاربران، به طور چشمگیری از ارتکاب جرایم رایانه‌ای می‌کاهد. برای این امر، سازوکارهای مختلفی را می‌توان در نظر گرفت. یکی از این روش‌ها استفاده از تصدیق هویتِ دو عاملی[۳] است. در واقع، تصدیق هویتْ این امکان را فراهم می‌کند که رایانه بداند کاربر کیست. برای استفاده از تصدیق هویتِ دو عاملی، دو روش وجود دارد: روش نخست، استفاده از کارت‌های هوشمندِ مبتنی بر نشانه است که اطلاعات زیستی افراد را در خود ذخیره می‌کنند. روش دوم، استفاده از سرویس‌دهنده‌ها و برنامه‌هایی است که مثل نگهبان یک سالن، عبور و مرور را کنترل می‌کنند. آن‌ها پس از بررسی و تأیید اطلاعات کاربر، به وی اجازهٔ دسترسی به خدمات شبکه را می‌دهند (مشهدی تفرشی، ۱۳۸۳: ۱۱۸). به طور کلّی، روند سرویس‌های تصدیق هویت به این صورت است که اگر نشانه‌ای که کاربر وارد می‌کند، با نشانهٔ ذخیره‌شده در این برنامه‌ها یکسان باشد، کاربر به همهٔ خدمات دسترسی پیدا می‌کند. این امر، سبب مقاوم‌سازی ارتباطات در برابر حملات شنود و گمراه‌سازی می‌شود (خانعلی‌پور واجارگاه، ۱۳۹۰: ۱۳۶).

۱ـ۲ـ۳. استفاده از مدیریت مکان[۴]

هرچند سیستم‌های خودکارِ نظارتی، دقت و سرعت بسیار بالایی دارند، در برخی موارد، این سیستم‌ها به دلیل نداشتن هوش و درک لازم نتوانسته‌اند در برابر حملات هوشمندانه

۱. IP (internet protocol) spoofing؛ جعل پروتکل اینترنتی دیگران به منظور دسترسی غیر قانونی به سیستم رایانه‌ای. در این روش، مجرم از پوشش رایانه‌ای برای ارتکاب اَعمال خلاف قانون خود استفاده می‌کند.

۲. Online camouflage؛ استفاده از انواع نرم‌افزارها برای استتار در فضای سایبر که مرتکب قابل شناسایی نباشد.

3. Two factor authentication.

4. Utilize place managers.

مقاومت نمایند و بزهکاران حرفه‌ای از سدّ این تدابیر نظارتی ـ امنیتی عبور کرده‌اند. بدین‌سان، استفاده از افراد نگهبان و حسابرس در مراکز امنیتی ـ اطلاعاتی و تجاری ـ بازرگانی می‌تواند مکمّل مناسبی برای این سیستم‌های خودکار باشد؛ برای مثال، بانک‌ها و فروشگاه‌های اینترنتی برای جلوگیری از سرقت اینترنتی می‌توانند برای نظارت بر عملیات‌های تجاری، حسابرسی و کنترل حساب‌های خود از نیروی انسانی استفاده کنند؛ زیرا همان طور که گفته شد، برنامه‌های نظارتی علی‌رغم دقت و سرعت بالایی که دارند، کماکان یک برنامه هستند و امکان تجاوز و مخدوش کردن این برنامه‌ها به وسیلهٔ افراد فنی و ماهر وجود دارد؛ برای مثال، یک نوجوان ۱۵ ساله که به حساب شرکت‌های دیگر مبلغ ۸۹ هزار دلار مکالمهٔ تلفنی انجام داده بود، شناسایی و دستگیر شد. این بزهکار نوجوان با استفاده از یک دستگاه مودم و رایانهٔ شخصی، وارد سیستم‌های رایانه‌ای شرکت‌های تجاری می‌شد و گذرواژهٔ آن‌ها را به دست می‌آورد و با استفاده از آن، در هر مکانی می‌توانست از حساب آن شرکت تلفن کند (*ماهنامهٔ گزارش رایانه*، ۱۳۸۱: ش۱۱۹/۱۴).

۱ـ۲ـ۴. ارتقای نظارت رسمی[1]

نظارت در محیط سایبر ـهمچون نظارت در محیط مادی‌ـ از جمله راهکارهایی است که علاوه بر کشف سریع جرم، از ارتکاب آن نیز جلوگیری می‌کند. تدابیر مراقبتی را می‌توان از دو طریق اعمال کرد: شیوهٔ نخست، کاربستِ تدابیر فیزیکی در دنیای فیزیکی ـآن گونه که در سایر جرایم اعمال می‌شود‌ـ می‌باشد؛ برای مثال، نصب دوربین‌های مداربسته در کافی‌نت‌ها و سازمندی صفحهٔ نمایش رایانه‌ها به صورتی که در معرض دید عموم باشد. اما روش دیگر، نظارت الکترونیکی است که با ویژگی‌های این محیط، سازگاری بیشتری دارد. در این شیوه با به کارگیری تجهیزات و برنامه‌های خاص، فعالیت‌های شبکه‌ایِ افراد تحت نظر قرار می‌گیرد (جلالی فراهانی، ۱۳۸۳: ش۱۱۴/۴۷). لازم به ذکر است در صورتی نظارت شبکه‌ای اثر بازدارنده خواهد داشت که کاربر بداند فعالیت‌هایش تحت نظارت قرار دارد؛ زیرا نظارت مخفی فقط برای جمع‌آوری ادله علیه متهم به کار می‌رود و هیچ اثر پیشگیرانه‌ای ندارد (همو، ۱۳۸۴: ش۱۴۴/۶).

1. Strengthen formal surveillance.

بنابراین، استفاده از ابزارهایی که تحت محافظت بودن شبکه و تحت نظارت بودن کاربر را اعلام کنند، می‌تواند ابزارهای نظارتی را تکمیل نماید.

۲. راهبردهای سلبی

راهبردهای کاهش دستاوردهای حاصل از جرم، تحدید و حذف عوامل محرک و نیز سلب توجیه‌ها و به عبارتی بهانه‌های ارتکاب جرم، در این امر مشترک می‌باشند که لازمهٔ آن ایجاد و تأسیس در محیط نیست، بلکه می‌توان تنها با تغییر و دستکاری یا حذف مواردی، از آماج در برابر حملات دفاع نمود. در ادامه، این سه راهبرد به تفصیل بررسی می‌شوند:

۲ـ۱. کاهش دستاوردها

هدف این راهکارها، کاهش منافع حاصل از ارتکاب جرم است؛ زیرا زمانی که بزهکار بداند از ارتکاب جرم منفعتی عاید وی نخواهد شد، از انجام آن منصرف می‌شود. کلارک، ذیل این راهبرد، به پنج راهکار پنهان کردن آماج،[1] جابه‌جا کردن (برداشتن) آماج،[2] هویت‌دار کردن اموال،[3] برچیدن بازارها[4] و از بین بردن منافع[5] اشاره می‌کند. از آنجا که برخی از این راهکارها در فضای سایبر قابل اجرا نیستند[6] یا برخی به توضیح زیاد نیاز ندارند،[7] تنها به تبیین دو راهکار نخست اکتفا می‌شود.

---

1. Conceal targets.
2. Remove targets.
3. Identify property.
4. Disrupt markets.
5. Deny benefits.

۶. برای نمونه، روش برچیدن بازارها، در فضای مجازی معنا پیدا نمی‌کند. برچیدن بازار راهکاری است که به نظارت بر دستفروش‌ها و بازارهای محلّی اشاره دارد؛ زیرا بزهکاران در آنجا اموال ربوده‌شده را با قیمتی کمتر از مورد مشابه به فروش می‌رسانند. بدیهی است چنانچه نظارتی جدی در رابطه با این بازارها صورت گیرد، کمتر بزهکاری نفعی برای سرقت خود متصور می‌شود.

۷. از بین بردن منافع، ناظر بر روش‌هایی است که جذابیت ارتکاب جرم را برای بزهکار از بین می‌برد. مثلاً در صورت رمزگذاری‌های پیچیده، داده‌های هک‌شده از حیّز انتفاع خارج می‌شوند. در ارتباط با هویت‌دار کردن اموال نیز همان طور که اشاره شد، باید تا جای ممکن از علایم متمایزکننده ـ نظیر شماره‌های سریالی برای داده‌های ذخیره‌شده ـ استفاده نمود.

۲ـ۱ـ۱. پنهان کردن آماج

یکی از راه‌های پیشگیری از وقوع جرم، پنهان نمودن آماج جرم یا بزه‌دیدهٔ احتمالی از دید بزهکاران است. در فضای مجازی، مخفی نمودن آماج به کمک ناشناس‌کننده‌ها[1] و رمزنگارها[2] امکان‌پذیر است. این دو اقدام با آنکه با یکدیگر تفاوت دارند، یک هدف را دنبال می‌کنند. کارکرد اصلی آن‌ها این است که با پنهان کردن هویت یا محتوای اطلاعات افراد، از بزه‌دیدگی آن‌ها جلوگیری کنند (خانعلی‌پور واجارگاه، ۱۳۹۰: ۱۲۹). ناشناس‌کننده‌ها، هویت افراد مبدأ و مقصدِ مبادلهٔ اطلاعات را پنهان می‌کنند، اما رمزنگارها محتوای ارتباطات را نامفهوم می‌سازند. دلیل به کارگیری فرایند رمزنگاری این است که از یک سو، کلیهٔ پیام‌هایی که در وب دریافت و ارسال می‌شوند، به صورت متن ساده هستند و از سوی دیگر، ابزارهای بسیاری در این محیط برای شنود و دستیابی به ارتباطات افراد وجود دارند (جلالی فراهانی، ۱۳۸۳: ش۱۱۶/۴۷). در حقیقت، ناشناس‌کننده‌ها هویت افراد را در محیط سایبر پنهان می‌کنند و از این طریق، به آن‌ها امکان می‌دهند با ایجاد حریم بیشتر، به فعالیت شبکه‌ای بپردازند. از آنجا که رمزنگاری، پیام را تغییر می‌دهد، برای افراد غیر مجاز بسیار سخت یا حتی غیر ممکن خواهد بود که بتوانند پیام رمزگذاری‌شده را بخوانند. پروتکل‌های رمزگذاری‌شده نیز تنها زمانی کار می‌کنند که مرورگر بداند مخاطب آن چه کسی است. این امر به کمک گواهی امنیتی[3] و امضای دیجیتالی[4] صورت می‌پذیرد.

در میان انحرافات سایبری، جرایم ویژه‌ای به چشم می‌خورد که بزه‌دیدگی در آن، مختص زنان و کودکان می‌باشد. این جرایم، بیشتر در ارتباط با آنچه امروزه از آن با عنوان صنعت مقاربت جنسی یاد می‌شود، هستند. این صنعت، از ماهیت متخلّفانهٔ محتوای هرزه‌نگاری زنان و کودکان بهره می‌گیرد و چیزهایی را که در زمان قدیم فقط در بازی‌های کثیف و فرعیِ هرزه‌نگاری یافت می‌شد، قابل قبول می‌سازد.

---

1. Anonymizers.
2. Cryptography.
3. Security certificate.
۴. امضای دیجیتالی، مبتنی بر روش‌های رمزنویسی از طریق کلیدهای عمومی و خصوصی است.

نگران‌کننده‌ترین موضوع در مورد تمام این اطلاعات این است که ایـن صـنعت نـه تنهـا تجارت بزرگی است، بلکه فروش محصولات آن ـهرزه‌نگـاری، خودفروشـی، سـیاحت جنسی و عروس‌های پستی‌ـ اکثراً به زنان و کودکان مربوط می‌شود (زینـالی، ۱۳۸۸: ۲۸۵). این قبیل تدابیر، به ویژه برای زنان، کودکان و یا به طور کلّی اشخاصی که به هـر دلیلـی آسیب‌پذیرند، سودمند است؛ زیرا بی‌آنکه فرصت شناسایی خـود را بـه بزهکـاران سـایبر بدهند، می‌توانند به فعالیت‌های شبکه‌ای بپردازند (جلالی فراهانی، ۱۳۸۴: ش۱۴۵/۶).

۲ـ۱ـ۲. جابه‌جا کردن آماج

برخی روش‌ها، منافع حاصل از جرم را از بین می‌برند. بنابراین تدابیر وضعی باید تا جای ممکن معادلات را بـه ضـرر بزهکـار رقـم زننـد. جابـه‌جـا کـردن آمـاج، حملـه را بـرای بزهکارانْ بی‌جاذبه جلوه می‌دهد و آن‌ها را از انجام آن باز می‌دارد؛ بـرای نمونـه هکرهـا می‌توانند به آسانی از طریق امـواج الکترومغناطیـسی منتـشرشده در محـیط، خـود را بـه عنوان عضوی از شبکه تلقی کنند و از این طریق به شنود اطلاعات در حال انتشار اقدام نمایند. بنابراین تا جایی که ممکن است، باید از ارتباطات سیمی بـرای برقـراری ارتبـاط بین سامانه‌های رایانه‌ای و مخابراتی استفاده نمود.

۲ـ۲. کاهش عوامل محرک[1]

گاهی عوامل مساعد بزهکاری به قدری تحریک‌کننده‌اند که افراد زیادی را به ارتکاب بزه وسوسه می‌کنند. همان طور که اشاره شد، این حالـت در فـضای سـایبر بـه وضـوح دیـدنی است. پس، طبق این راهبرد باید در اوضاع و احوال ناظر به جرم، به گونه‌ای دخالـت نمـود که عوامل محرک را ـحداقل بزهکاران اتفاقی‌ـ به کمترین حد ممکن رسـاند. پـنج راهکـار پیش‌بینی‌شده در این راهبرد ـکه بیشتر بر کُنش‌های روان‌شناختی بزه‌دیدگان احتمـالی تکیـه دارد‌ـ به ترتیب عبارت‌اند از: کاهش استرس،[2] اجتناب از اغتشاش،[3] کاهش برانگیختگی،[4]

1. Reduce provocation.
2. Reduce frustrations and stress.
3. Avoid disputes.
4. Reduce emotional arousal.

خنثی کردن فشار گروه همسالان[1] و ممانعت از تقلید ارتکاب جرم.[2] از آنجا که روش اجرای برخی از راهکارها با جرایم واقعی مشابه است، لذا فقط راهکارهای دوم و سوم بررسی می‌شوند.

۲ـ۲ـ۱. اجتناب از اغتشاش

هکرها در فضای سایبر اغلب به دنبال سرگرمی و محک زدن میزان دانش و مهارت خود دربارهٔ چگونگی کارکرد سامانه‌ها و کشف آسیب‌پذیری‌های یک رایانه یا شبکه هستند. در بیشتر موارد، این افراد قصد ارتکاب بزه را ندارند، اما گاه تحریکات اشخاص یا حتی دستگاه‌های دولتی می‌تواند زمینه‌ساز تهدیدات سایبری آن‌ها شود. بنابراین در صورت بروز رفتار غیر معمول از طرف هکرها و بزهکاران احتمالی، رفتارهایی از قبیل مقابله به مثل یا انتشار بیانیه در رسانه‌های گروهی، بستر را برای شکل‌گیری حملات سایبری فراهم می‌کنند؛ زیرا این اقدام، باعث ترغیب بیشتر بزهکاران به انجام رفتارهای غیر قانونی می‌شود؛ نمونهٔ بارز اقدامات تحریک‌آمیز را می‌توان در کشورهایی که دارای ساختار قومیتی هستند، ملاحظه کرد. هر گونه تبعیض نژادی یا اختلافات مذهبی ـ عقیدتی می‌تواند بزهکاران سایبری را برای حمله به تارنماهای دولتی و حتی زیرساخت‌های حیاتی یک دولت تحریک کند تا به همگان ثابت کنند که در این جنگ سایبری، آن‌ها فاتح بلامنازع می‌باشند. لذا باید از هر گونه اقدامات تنش‌زا و محرک اجتناب ورزید.

۲ـ۲ـ۲. کاهش برانگیختی

هر جرم، اهداف مجرمانهٔ خاص خود را داراست. به بیان دیگر، بنا بر نوع جرم، هدف مجرمانه نیز متفاوت است؛ برای مثال، در جرایم منافی عفت، دسترسی به صور مستهجن یک هدف مجرمانه است. حال در صورتی که هدف و موضوع جرم ـ که در مثال فوق، صور و آثار مستهجن می‌باشد ـ حذف و معدوم شود، میزان ارتکاب جرم نیز کاهش می‌یابد؛ زیرا اهداف محرک، منشأ بسیاری از جرایم است. این امر نیز در محیط

1. Neutralize peer pressure.
2. Discourage imitation.

سایبر به دلایل مختلف و از جمله اهداف تجاریِ شرکت‌های تولیدکنندهٔ کالا، ناشناس بودن کاربران و سهولت تحریک، نمود بیشتری دارد. استفاده از تصاویر برهنه و نیمه‌برهنهٔ زنان برای تبلیغ و فروش بیشترِ محصولات بازرگانی، امری رایج در عرصهٔ فضای مجازی است. این امر علاوه بر اینکه طبق قانون بسیاری از کشورها جرم است، دارای خصیصهٔ تحریک‌کنندگی کاربران برای ورود به وبگاه‌های مستهجن نیز می‌باشد. بنابراین با حذف چنین تبلیغات تحریک‌آمیزی از طریق پالایش و اِعمال محدودیت‌های دیگر، می‌توان تا حدّ زیادی از ارتکاب جرایم دیگر هم پیشگیری نمود. لذا پالایش، یکی از ابزارهای قوی برای از بین بردن اهداف مجرمانه است.

راه دیگری که برای حذف اهداف مجرمانه می‌توان پیشنهاد کرد، جاذبه‌زدایی از داده‌ها و سامانه‌های محرمانه است. با نگهداری نکردن داده‌هایی که سبب محرمانگی آن شده‌اند، می‌توان در پیشگیری از جرایم علیه محرمانگی داده‌ها و سامانه‌ها موفق بود. برای اینکه محتوای رایانامه‌ای یا کلامی که از طریق ابزارهای مخابراتی و اینترنتی منتقل می‌شود مورد دسترسی غیر مجاز یا شنود قرار نگیرد، می‌توان تا حدّ امکان، داده‌ها و محتویات محرمانه را از آن کاست.

۲ـ۳. تدابیر آموزشی ـ آگاهی‌ساز

راهبرد پنجم و پایانی کلارک، به سلب توجیه‌ها اختصاص دارد. سلب توجیه‌ها به این معناست که افراد همواره برای کارهایشان توجیه‌هایی را مطرح می‌کنند. بزهکاران نیز ممکن برای اعمال خود، توجیه‌ها یا بهانه‌هایی را جهت رفع مسئولیت از خود بیان دارند.[۱] راهکارهای وضعی این راهبرد، به منظور دفع چنین توجیه‌هایی است. وضع مقررات،[۲] تحریک وجدان،[۳] نصب تابلوهای هشداردهنده،[۴] تسهیل رعایت مقررات[۵] و

۱. دیوید ماتزا در چارچوب نظریهٔ فنون خنثی‌سازی خود، چنین توجیهاتی را موجب تضعیف سازوکارهای کنترل اجتماعی می‌داند به گونه‌ای که رفتار بزهکار را از حالت رفتار متعارف، به رفتار انحرافی سوق می‌دهد (McLaughlin, 2001: 186).

2. Set rules.

3. Post instructions.

4. Alert conscience.

5. Assist compliance.

کنترل مواد مخدر و الکل[1] از جملهٔ آن‌هاست؛ برای نمونه، نصب تابلو و علایم هشداردهنده، در جهت سلب توجیهِ «من نمی‌دانستم» است یا اعمال کنترل بر مواد مخدر برای دفعِ بهانهٔ «من مست بودم و متوجه اعمالم نبودم» و... می‌باشد.

راهکارهای سلب توجیه در همهٔ جرایم از جمله جرایم سایبری، کارکرد ویژه‌ای دارد، اما از آنجا که پیاده‌سازی این راهکارها در فضای سایبر، تفاوت چندانی با سایر جرایم ندارد، همچنین به جهت پرهیز از اطالهٔ کلام، از تبیین آن‌ها صرف‌نظر می‌کنیم.

اما با توجه به اهمیت فراوان بحث آموزش در پیشگیری از جرایم سایبری، در این بند تا آنجا که در راستای پیشگیری وضعی است، به این مقوله اشاره می‌شود. شایان ذکر است که راهبردِ تدابیر آموزشی ـ آگاهی‌ساز، به طور جداگانه در رهنمودهای کلارک مطرح نشده است.

یکی از دلایل اولیهٔ رشد انحرافات سایبری آن است که عموم مردم از ممنوعیت این دسته اَعمال آگاهی ندارند. از این رو، شاید مهم‌ترین ابزار مبارزه با جرایم سایبری، آموزش همگانی باشد. همان طور که اشاره شد، با توجه به عدم درک پیامدهای گرانبار تهدیدات سایبری و تقبیح نکردن ارتکاب این قبیل جرایم از سوی جامعه، ضرورتِ نقش آموزش در پیشگیری از جرایم سایبری، بیش از سایر جرایم احساس می‌شود. ساده‌ترین نوع آموزش در ارتباط با این جرایم، همان تدابیری است که برای سایر انحرافات اجتماعی به کار می‌روند.

بیان این نکته ضروری است که هرچند نقش آموزش در پیشگیری، ذیلِ پیشگیری اجتماعی بحث می‌شود، با این حال نباید تصور شود که پیشگیری وضعیت‌مدار[2] با آن بیگانه است. بحث از آموزش تا آنجا که در راستای تقویت آماج جرم ـ بزه‌دیدگان احتمالی ـ می‌باشد، ذیل پیشگیری وضعی می‌گنجد؛ زیرا امر آموزش و اقدامات آگاهی‌ساز می‌تواند ضمن تقویت آماج جرم، در مسلّح‌سازی و هوشیاری بزه‌دیدگان احتمالی، نقش کلیدی ایفا نماید؛ برای نمونه، کلارک مثالی را که ذیل راهکار استفاده

1. Control drugs and alcohol.

2. Situational crime prevention (SCP).

از مدیریت مکان مطرح می‌کند، به صراحت به کاربستِ آموزش برای پیشگیری از بزه‌دیدگی کارمندان مؤسسه اشاره می‌کند یا در راهکار نصب تابلوهای هشداردهنده، علاوه بر سلب توجیه‌ها، به دنبال آنیم که با تکیه بر تدابیر آگاهی‌ساز، از ورود بزه‌دیدگان به موقعیت‌های پرخطر پیشگیری کنیم. بنابراین با آنکه خاستگاه تدابیر آموزشی ـ آگاهی‌ساز در پیشگیری اجتماعی است، در پیشگیری وضعی نیز برای تقویت آماج ـ در معنای وسیع ـ به کار گرفته می‌شود. کثرت بزه‌دیدگان در جرایم سایبری، اهمیت این تدابیر را دوچندان می‌سازد.

۲ـ۳ـ۱. اعلان جرم بودن یک عمل و اطلاع‌رسانی نسبت به آن

تعداد زیادی از کاربران اینترنت، تنها برای گذران وقت و سرگرمی، گام در فضای مجازی می‌گذارند.[۱] 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 غیر مجاز متمایل شوند، بسیار زیاد است. مجازی بودن، فقدان نمود خارجی و ملموس نبودن آثار جرم، یکی از عوامل سوق یافتن کاربران به ارتکاب این گونه جرایم است. لذا با آگاه‌سازی و هشدارهای لازم نسبت به جرم بودن عمل و میزان مجازات اَعمال ارتکابی می‌توان تا حد زیادی از ارتکاب جرایم دنیای سایبر، پیشگیری نمود؛ برای نمونه، هر یک از این شبکه‌ها می‌توانند در وبگاه‌های خود بر اساس نوع خدماتی که ارائه می‌دهند، مخاطبان خود را با خطرها و آسیب‌هایی که ممکن است متوجه آن‌ها باشد، آشنا کنند. از سوی دیگر، با هشدارهای لازم و تبیین این موضوع که سوءاستفاده از خدماتشان با چه عواقبی مواجه می‌باشد، از بروز جرایم رایانه‌ای جلوگیری کنند (جلالی فراهانی، ۱۳۸۳: ش۱۱۰/۴۷).

۲ـ۳ـ۲. آگاه‌سازی کاربران و آمادگی مقابله با جرایم سایبری

آگاه‌سازی و استفادهٔ بهینه از راهبردهای حساس‌سازی مردم برای پیشگیری از جرم می‌تواند به پیشگیری از جرایم سایبری کمک کند. حساس‌سازی مردم برای ایجاد

۱. بر اساس آمار سازمان ملّی جوانان، بیش از ۴۴ درصد کاربران ایرانی با هدف تفریح و سرگرمی وارد فضای مجازی می‌شوند (حاجیلی، ۱۳۸۸: ۱۲۸).

فرهنگ قانون‌مداری، مقولهٔ مهمی است که با تحقق آن، بار دستگاه عدالت کیفری در امر پیشگیری از جرم بسیار سبک خواهد شد. به فرایند مشارکت مردم در پیشگیری از جرم، در راهبرد سند پیشگیری از جرم سازمان ملل متحد نیز توجه شده است. در رهنمود پیشگیری از جرمِ سازمان ملل متحد آمده است:

> در برنامه‌های پیشگیری، با توجه به تنوع علل ایجاد جرم، مشارکت تمامی افراد و نهادهایی که در زمینهٔ پیشگیری از جرم، دارای مهارت و مسئولیت هستند امری اجتناب‌ناپذیر است. به همین دلیل، برنامه‌های پیشگیری را نمی‌توان در یک وزارتخانه محدود ساخت و وزارتخانه‌های مختلف، مقامات، نهادهای محلّی، سازمان‌های غیر دولتی، تجار و شهروندان، همه و همه باید با همکاری یکدیگر برنامه‌های پیشگیری را به اجرا درآورند (جوان جعفری و سیدزاده ثانی، ۱۳۹۱: ۲۸۶).

ارتقای فرهنگ استفادهٔ صحیح از رایانه و مقولهٔ آموزش، به نوبهٔ خود می‌تواند به پیشگیری از جرایم سایبری منجر شود. با توجه به اینکه جرایم سایبری بیشتر توسط گروه‌های سازمان‌یافته و با طراحی و نقشهٔ قبلی و همچنین توسط اشخاص رقیب یا اخراج‌شده از سازمان‌های مزبور صورت می‌گیرد (رضوی، ۱۳۸۶: ش۱/۱۲۴)، آموزش به اشخاص و شرکت‌های در معرض تهدیدهای سایبری، آن‌ها را برای مقابله با این جرایم تجهیز می‌کند. علاوه بر این، آموزش‌های عمومی در رسانه‌های گروهی برای مقابله با ویروس‌ها و کرم‌های رایانه‌ای نیز بسیار سودمند است؛ زیرا چنانچه به سرعت مقابلهٔ عمومی با این ویروس‌های رایانه‌ای صورت پذیرد، هزینه‌های پیشگیری از این جرایم به مراتب کاهش می‌یابد.

نتیجه‌گیری

بین وابستگیِ فزایندهٔ جامعه به فناوری‌های اطلاعاتی و ارتباطی (ICTs) و توانایی دولت‌ها در صیانت از فضای سایبر، شکافی پدید آمده است که بزهکاران را به سوی دنیای سایبر گسیل داشته است؛ زیرا آن‌ها دریافته‌اند که ابزارهای مرسوم، فاقد کارایی لازم است و دلایل دیجیتالی به دست‌آمده، تاب پیگرد آن‌ها را ندارد. همچنین نوظهور بودن این فناوری‌ها سبب شده تا اقدامات مقطعی و ضربتی ـ برای کنترل کوتاه‌مدت جرایم

سایبری-، مطلوبِ سیاست‌گذاران و نظام عدالت کیفری قرار گیرد؛ چرا که این اقداماتِ کم‌هزینه سبب می‌شود تا چنین به نظر آید که دستگاه عدالت کیفری برای برخورد با منحرفان، فاقد برنامهٔ لازم نمی‌باشد؛ نمونهٔ بارز این گونه اقدامات، تدابیر وضعی است که با اثرگذاری بر موقعیت‌های جرم‌زا به دنبال آن است که در سایهٔ تدابیر محدودکننده و نظارتی، بزه را برای بزهکار دشوار جلوه دهد و با تغییر در معادلهٔ هزینه ـ فایده، او را از ارتکاب جرم باز دارد. البته دستگاه عدالت کیفری برای مبارزه با جرم، همواره از کیفر بهره جسته است، اما دربارهٔ جرایم سایبری ـ به دلیل ویژگی‌های حاکم بر فضای سایبر ـ سیاست‌گذاران دریافته‌اند که الگوی بازدارندگی سنتی، حتی کمتر از سایر جرایم در پیشگیری و ارعاب این دسته جرایم مؤثر واقع می‌شود. از این رو، اقدامات کُنشی را بر هر نوع تدبیر دیگر مقدم داشته‌اند.

شاید جامع‌ترین و فراگیرترین برنامهٔ پیشگیری وضعی، رهنمودهای کلارک ـ راهکارهای ۲۵گانه ـ باشد. گرچه او این رهنمودها را در چارچوب جرایم سنتی مطرح کرد، با این حال می‌توان با پیاده‌سازی و اجرای این رهنمودها، به نحو مطلوبی از جرایم سایبری نیز پیشگیری نمود. با آنکه کلارک هیچ‌گاه یک راهبرد مستقل را به بحث آموزش بزه‌دیدگان اختصاص نداد، می‌توان در میان برخی راهکارهای وی به طور صریح اهمیت آن را دریافت. نوظهور بودن جرایم سایبری، کثرت بزه‌دیدگان در فضای سایبر و عدم درک دقیق آثار تهدیدهای سایبری، ضرورت تکیه بر تدابیر آموزشی ـ آگاهی‌ساز را در این دسته جرایم موجه می‌نماید.

باید دانست که تدابیر وضعی، بارِ کم‌کاریِ دستگاه‌های مختلفِ مسئول در امر مبارزه و کنترل جرم را به عهده می‌گیرند و تدابیر پیشگیری وضعی در کنار برنامه‌های پیشگیری اجتماعی، سبب بالندگی در پیشگیری و کنترل بزهکاری می‌شوند؛ زیرا رسالت پیشگیری وضعی، ریشه‌کنی اصولیِ جرم نیست و اثرگذاری برنامه‌های آن، بیشتر جنبهٔ آرام‌بخشی دارد. بنابراین لازم است سیاست‌گذاران در کنار بهسازی محیطی ـ توسعه و به‌روزرسانی تدابیر وضعی-، نسبت به تقویت سازوکارهای خودکنترلی و آموزش مهارت‌های اجتماعی به شهروندان، اهتمام داشته باشند.

البته برخی ایرادهای ناظر بر پیشگیری وضعی ناشی از کاربست نادرست این تدابیر

و راهبردها می‌باشد؛ برای نمونه، انتقادات بـر محـدودیت‌هـای اخلاقـی ـ حقـوق بـشری بیشتر ناظر بر اجرای چنین تدابیری است. همچنین دربارهٔ هزینه‌های سنگین اقتـصادی، عده‌ای معتقدند که به دلیل محرومیت‌های مالیِ طبقات فرودست، این پیشگیری تنها به سود طبقهٔ فرادست می‌باشد و نتیجهٔ این امر، آپارتاید امنیتی است. در پاسخ بایـد گفـت که این ایراد نیز به نحوهٔ اجرای برنامه‌ها وارد است، نه به اصـل پیـشگیری وضـعی؛ زیـرا دولت می‌تواند با دخالت در این زمینه بـه یـاریِ بخـش محـروم جامعـه آیـد و در قالـب طرح‌های حمایتی ـبا اختصاص بخشی از بودجهٔ کـشورـ تـوازن امنیـت را برقـرار سـازد. پس چنانچه این برنامه‌ها به طور همه‌جانبه مورد نظر واقع شوند و به طور علمـی بـه کـار گرفته شوند، کمتر با چالش اخلاقی مواجه خواهند شد.

در پایـان بایـد توجـه داشـت کـه در کنـار اقـدامات پیـشگیرانه، نهادهـای مـسئول قانون‌گذاری، سیاست‌گذاران، قضات و نهادهای مردمـی بایـد درک و شـناخت کـافی دربارهٔ این جرایم کسب کنند. شاید علت اصـلیِ رشـد بـی‌رویـهٔ تهدیـدهای سـایبری را بتوان در عدم شناخت دقیق واقعیت این جرایم و نیز عقب‌ماندگی دستگاه‌های مختلـفِ سیاست‌گذاری ـ اجرایی از تحولات آن دانست؛ برای نمونه، قضاتْ برای درک مفهـوم «نفوذ غیر مجاز (هک) به سامانه‌ها»، آن را با «ورود غیر مجاز به منزل دیگری» تطبیـق می‌دهند! این امر نشان می‌دهد که هنوز برخی، از واقعیت و چیستی این جـرایم، اطـلاع دقیقی ندارند. بنابراین بایسته اسـت در کنـار پـژوهش‌هـای مبنـایی و کـاربردی در ایـن حوزه، دربارهٔ قانون‌گذاری متناسب با بـزهِ سـایبری و کیفرگـذاری متناسـب بـا بزهکـارِ سایبری، واکاوی و مطالعات منسجمی صورت گیرد.

کتاب‌شناسی

۱. ابراهیمی، شهرام، *جرم‌شناسی پیشگیری*، چاپ دوم، تهران، میزان، ۱۳۹۱ ش.
۲. الهی‌منش، محمدرضا و ابوالفضل سدره‌نشین، *محشای قانون جرایم رایانه‌ای*، تهران، مجد، ۱۳۹۱ ش.
۳. بابایی، محمدعلی و علی نجیبیان، «چالش‌های پیشگیری وضعی از جرم»، *مجلهٔ حقوقی دادگستری*، شمارهٔ ۷۵، ۱۳۹۰ ش.
۴. پاک‌نهاد، امیر، *سیاست جنایی ریسک‌مدار*، تهران، میزان، ۱۳۸۸ ش.
۵. توکل، محمد و ابراهیم کاظم‌پور، *دگرگونی‌های اجتماعی در یک جامعهٔ اطلاعاتی*، تهران، کمیسیون ملی یونسکو، ۱۳۸۴ ش.
۶. جلالی فراهانی، امیرحسین، «پیشگیری از جرایم رایانه‌ای»، *مجلهٔ حقوقی دادگستری*، شمارهٔ ۴۷، ۱۳۸۳ ش.
۷. همو، «پیشگیری وضعی از جرایم سایبر در پرتو موازین حقوق بشر»، *مجلهٔ فقه و حقوق*، شمارهٔ ۶، ۱۳۸۴ش.
۸. همو، *درآمدی بر آیین دادرسی کیفری جرایم سایبری*، تهران، خرسندی، ۱۳۸۹ ش.
۹. جلالی فراهانی، امیرحسین و محبوبه منفرد، «حمایت قانونی از آسیب‌دیدگان سایبری»، *مجلهٔ مجلس و راهبرد*، سال بیستم، شمارهٔ ۷۳، ۱۳۹۲ ش.
۱۰. جوان جعفری، عبدالرضا، «جرایم سایبر و چالش‌های نوین سیاست کیفری»، *مجموعه مقالات همایش جهانی شدن حقوق و چالش‌های آن*، مشهد، ۱۳۸۵ ش، قابل دسترسی در: <http://confbank.um.ac.ir/modules/conf_display/conferences/hoghogh/pdf/hamayesh-02pdf>.
۱۱. جوان جعفری، عبدالرضا و مهدی سیدزاده ثانی، *رهنمودهای عملی پیشگیری از جرم*، معاونت پیشگیری از وقوع جرم قوهٔ قضاییه، تهران، میزان، ۱۳۹۱ ش.
۱۲. حاجیلی، محمود، *وضعیت فناوری ارتباطات در حوزهٔ جوانان*، تهران، دبیرخانهٔ شورای عالی اطلاع‌رسانی، ۱۳۸۸ ش.
۱۳. خالقی پوستچی، علی، «پیشگیری از جرایم سایبری با بهره‌گیری از فناوری اطلاعات و ارتباطات»، *مقاله‌های همایش ملیِ علمی ـ کاربردی پیشگیری از جرم* (قوهٔ قضاییه، مشهد)، تهران، میزان، ۱۳۸۸ ش.
۱۴. خانعلی‌پور واجارگاه، سکینه، *پیشگیری فنی از جرم*، تهران، میزان، ۱۳۹۰ ش.
۱۵. داتن، ویلیام، *دگرگونی‌های اجتماعی در جامعهٔ اطلاعاتی*، ترجمهٔ محمد توکل و ابراهیم کاظمی‌پور، تهران، کمیسیون ملّی یونسکو، ۱۳۸۴ ش.
۱۶. رضوی، محمد، «جرایم سایبری و نقش پلیس در پیشگیری از این جرایم و کشف آن‌ها»، *فصلنامهٔ دانش انتظامی*، سال نهم، شمارهٔ ۱، ۱۳۸۶ ش.
۱۷. زررخ، احسان، «بزه‌دیده‌شناسی سایبری»، *فصلنامهٔ مجلس و پژوهش*، سال هفدهم، شمارهٔ ۶۴، ۱۳۹۰ ش.
۱۸. زیبر، اولریش، *جرایم رایانه‌ای*، چاپ دوم، تهران، گنج دانش، ۱۳۹۰ ش.
۱۹. زینالی، امیرحمزه، «حمایت کیفری از کودکان در برابر هرزه‌نگاری؛ از واکنش‌های جهانی تا پاسخ‌های نظام‌های کیفری ملی»، *حقوق فناوری اطلاعات و ارتباطات* (مجموعه مقالات)، گردآوری امیرحسین جلالی فراهانی، تهران، روزنامهٔ رسمی، ۱۳۸۸ ش.
۲۰. سادوسکای، جورج، جیمز اکس دمپزی، آلن گرین‌برگ، جی‌مک باربارا و آلن شوارتز، *راهنمای امنیت فناوری اطلاعات*، ترجمهٔ مهدی میردامادی، زهرا شجاعی و محمدجواد صمدی، تهران، دبیرخانهٔ شورای عالی اطلاع‌رسانی، ۱۳۸۴ ش.
۲۱. سالاری، مهدی، *کلاهبرداری*، تهران، میزان، ۱۳۸۶ ش.

۲۲. صفاری، علی، «انتقادات وارده به پیشگیری وضعی از جرم»، *مجلهٔ تحقیقات حقوقی*، شماره‌های ۳۵ـ۳۶، ۱۳۸۱ ش.
۲۳. عالی‌پور، حسن، *حقوق کیفری فناوری اطلاعات*، تهران، خرسندی، ۱۳۹۰ ش.
۲۴. گسن، ریمون، «روابط میان پیشگیری وضعی و کنترل بزهکاری»، ترجمهٔ علی‌حسین نجفی ابرندآبادی، *مجلهٔ تحقیقات حقوقی*، شماره‌های ۱۹ـ۲۰، ۱۳۷۶ ش.
۲۵. *ماهنامهٔ گزارش رایانه*، تهران، شمارهٔ ۱۱۹، ۱۳۸۱ ش.
۲۶. مشهدی تفرشی، شکوه، «امنیت پایگاه‌های اطلاعاتی»، *مجلهٔ اطلاع‌شناسی*، شمارهٔ ۳، ۱۳۸۳ ش.
۲۷. میرخلیلی، سیدمحمود، *پیشگیری وضعی از بزهکاری با نگاهی به سیاست جنایی اسلام*، تهران، سازمان انتشارات پژوهشگاه فرهنگ و اندیشهٔ اسلامی، ۱۳۸۸ ش.
۲۸. نجفی ابرندآبادی، علی‌حسین، «از جرم‌شناسی حقیقی تا جرم‌شناسی مجازی»، دیباچه در: *جرم‌شناسی*، نوشتهٔ ژرژ پیکا، ترجمهٔ علی‌حسین نجفی ابرندآبادی، چاپ دوم، تهران، میزان، ۱۳۹۰ ش.
۲۹. همو، *تقریرات درس جرم‌شناسی (پیشگیری)*، دورهٔ دکتری، تهران، دانشگاه تربیت مدرس، نیم‌سال دوم تحصیلی ۱۳۸۰ ش، قابل دسترسی در: <www.lawtest.ir>.
۳۰. همو، «کیفرشناسی نو ـ جرم‌شناسی نو؛ درآمدی بر سیاست جنایی مدیریتی خطرمدار»، *تازه‌های علوم جنایی* (مجموعه مقاله‌ها)، زیر نظر علی‌حسین نجفی ابرندآبادی، تهران، میزان، ۱۳۸۸ ش.
۳۱. ویلیامز، فرانک پی. و ماری لین دی. مک‌شین، *نظریه‌های جرم‌شناسی*، ترجمهٔ حمیدرضا ملک‌محمدی، چاپ سوم، تهران، میزان، ۱۳۸۸ ش.
۳۲. ویلیامز، ماتیو، *بزهکاری مجازی؛ بزه، انحراف و مقررات‌گذاری برخط*، ترجمهٔ امیرحسین جلالی فراهانی و محبوبه منفرد، تهران، میزان، ۱۳۹۱ ش.
33. Clarke, Ronald V., "Introduction", ***Situational Crime Prevention: Successful Case Studies***, 2nd Ed., New York, Criminal Justice Press, 1997.
34. Cornish, Derek B. & Ronald V. Clarck, "Opportunities, Precipitators and Criminal Decisions: A Reply to Wortley's Critique of Situational Crime Prevention", ***Crime Prevention Studies***, Vol. 16, 2003.
35. Felson, Marcus, "Routine Activity Approach", Ed. by: Richard Wortley & Lorraine Mazerolle, ***Environmental Criminology and Crime Analysis***, 1st Ed., Willan Publishing, 2008.
36. Katzer, Catarina, Detlef Fetchenhauer & Frank Belschak, "Cyberbullying: Who Are the Victims? A Comparison of Victimization in Internet Chatrooms and Victimization in School", ***Journal of Media Psychology***, Vol. 21(1), Hogrefe & Huber Publishers, 2009.
37. Kizza, Joseph M., ***Guide to Computer Network Security***, London, Springer Publications Ltd., 2013.
38. McLaughlin, Eugene, "Routine Activity Theory", Ed. by: Eugene McLaughlin & John Muncie, ***The Sage Dictionary of Criminology***, 1st Ed., London, Sage Publications Ltd., 2001.

39. Ngo, Fawn T. & Reymond Paternoster, "Cybercrime Victimization: An Examination of Individual and Situational Level Factors", ***International Journal of Cyber Criminology***, Vol. 5, Issue 1, 2011.
40. Turrini, Elliot, "Increasing Attack Costs and Risks and Reducing Attack Motivations", Ed. by: Sumit Ghosh & Elliot Turrini, ***Cyber Crimes: A Multidisciplinary Analysis***, 1st Ed., London, Springer Publications Ltd., 2010.