پلیس و چالش‌های اجرایی تامین امنیت سایبری[1]

فرید محسنی[2]، محسن صوفی زمرد[3]

تاریخ دریافت:۹۶/۷/۳۰ تاریخ پذیرش:۹۶/۱۰/۲۳

چکیده:

زمینه و هدف: به موازات نفوذ گسترده فضای مجازی در هر دو سطح کلان (حاکمیّتی) و خرد (شهروندان)، تأمین امنیّت آن نیز در کانون توجّه قرار گرفته است. هر چند همه فعالیت‌های بزهکارانه در فضای مجازی از جهت موضوع، انگیزه بزهکار، اهمیت و آثار رفتار ارتکابی یکسان نیستند اما از این جهت که تمام رفتارهای بزهکارانه به نوعی امنیت را در این فضا خدشه دار می سازد با رفتارهای بزهکارانه در فضای حقیقی اشتراک دارند. برخی رفتارهای بزهکارانه در فضای مجازی نیز به طور مستقیم امنیت یک کشور، زیرساخت‌های حیاتی یا اطلاعات حساس آن را هدف گرفته است. بنابراین علاوه بر ضرورت تقنین در مقابله با تهدیدات سایبری، نهادهای اجرایی کشور به ویژه پلیس در راستای تطبیق و اجرای سیاست جنایی اتخاذ شده از سوی قوه مقننه برای پاسخ‌دهی مناسب به این رفتارها و تامین امنیت آن نیازمند سیاستگذاری هستند که چالش های پیش‌رو در این زمینه نیازمند بررسی و تبیین است.

روش: روش این تحقیق از نظر جمع آوری داده‌ها اسنادی با استفاده از منابع مکتوب کتابخانه‌ای و نشریات الکترونیکی بوده و از نظر هدف کاربردی و از نظر نوع تحقیق نیز توصیفی - تحلیلی است.

یافته‌ها و نتیجه‌گیری: هر چند سیاست‌های تقنینی در حوزه امنیت فضای مجازی تا حدودی جرایم و پاسخ‌های کیفری را تبیین نموده و متناسب با آن سیاست قضایی نیز شکل گرفته اما بسیاری از تدابیر کنشی نیازمند سیاست‌گذاری و تعیین وظایف برای نهادهای اجرایی است. از طرفی موانع عقیدتی و ایدئولوژیک، ابهام در معیارهای حاکم بر سیاست‌گذاری، ضعف نهادهای اجرایی و دسترسی های فنی ، عدم تمایل بخش های خصوصی و عمومی به مشارکت با پلیس ، محدودیت‌های ساختاری و عدم توازن در بهره‌گیری از فناوری‌ها مانع از شکل‌گیری یک رویکرد هماهنگ و فراگیر برای مقابله با تهدیدات سایبری شده است.

واژگان کلیدی

امنیت سایبری، پیشگیری از جرم، سیاست جنایی، جرایم سایبری.

---

۱. این مقاله برگرفته از رساله دکتری با عنوان «پلیس و سیاست جنایی اجرایی ایران در قبال امنیت فضای مجازی با نگاهی به اسناد بین المللی» می باشد.

۲- عضو هیئت علمی حقوق دانشگاه علوم قضایی و خدمات اداری دادگستری (نویسنده مسئول)، mohseni@afranet.com

۳- دانشجوی دکتری دانشگاه علوم قضایی و خدمات اداری و عضو هیئت علمی دانشگاه علوم انتظامی امین(m.sufi61@gmail.com).

مقدمه

بشر از آغازین روزهای حیاتش در معرض آسیب، تعرض و تهدید قرار داشته و از ابتدا به فکر امنیت، آرامش و آسایش بوده است. امنیت در لغت از ریشه امن به معنای در امان بودن و مصون بودن از هر گونه تهدید و ترس است(جهان بزرگی ، ۱۳۸۸: ۳۱). امنیت مصونیت از تعرض ، تجاوز ، بر اساس حیطه‌ای است که پیرامون آن طرح می‌شود. فضای سایبر به علت ماهیت و کارکرد خود فضای تهدیدزایی را خلق نموده که باعث چالش امنیت در سطوح مختلف می‌شود. سطوح امنیت در این فضا، تحت تاثیر سه پارامتر انسان، اعتقادات و جامعه در مواجهه با فضای مجازی و سایبری شکل می‌گیرد. افراد و کاربران این فضا تجربه اجتماعی از تعامل، تبادل و اشتراک گذاری اطلاعات ، کسب و کار، بازی و تفریح، بحث-های گروهی که به صورت غیر فیزیکی است، دست پیدا می نمایند. فضای سایبری به مانند فضای حقیقی و ژئوپلوتیکی دارای تهدیدها و آسیب‌پذیری هایی است که انسان در برخورد با آن شرایطی را برای مصونیت در یک چرخه دائمی شکل می‌دهد. فضای سایبر هم از آن جهت که همه امور آدمی را در بر می‌گیرد و هم از آن جهت که مبانی انسان شناختی فضای تولید تکنولوژی و محتوی را در برگرفته مخاطراتی را متوجه انسان و جامعه می نماید. فضای جدید که در حال در برگرفتن همه شئون زندگی آدمی از تلاش، تفریح و اداره خانواده و محیط زندگی، تربیت فرزند و حتی فکر کردن را در بر می‌گیرد.

امنیت در پارادایم فضای مجازی تابع دو عنصر کلیدی انسان و فضای سایبری است. انسان و جامعه در مقابل فضای سایبری جهانی با ویژگی‌های خود فضای تهدیدزایی را شکل داده است. تهدیدات فضای سایبر، ضرورت حفاظت از انسان، جامعه و حاکمیت را در بر می گیرد. در واقع این تهدیدات نیازمند سه سطح امنیت است. سطح اول امنیت در فضای سایبر، امنیت در حوزه زیرساخت و شریان های اطلاعاتی است. فرصت جدید ایجاد شده برای حرفه ها و کشورها در فضای اتوماسیون، تبادل و همکاری، تجارت الکترونیکی، تولید هدفمند منجر به تولید، ذخیره‌سازی و بهره‌برداری از اطلاعات حساس و حیاتی شده است و وابستگی به شبکه‌های پرسرعت و پردازشگرهای قدرتمند روز به روز افزایش می‌یابد که

سیستم ها را در معرض مخاطراتی از آتش وطوفان تا بزهکاری وتروریسم سایبری قرارداده، که نیاز به مدیریت و نظارت دارد (کیان خواه ، ۱۳۸۹:). در دنیای جدید، مهمترین عامل توانایی و قدرت، حفاظت از اطلاعات در مقابل تهدیدات دشمنان، تبادل و اشتراک گذاری امن اطلاعات در جهت افزایش توانمندی است. جنگ اطلاعاتی، تروریسم سایبری و جنگ نفوذگرها از جمله این تهدیدات است و بومی نبودن این تکنولوژی و عمل نمودن به دستورات صاحبان تکنولوژی منجر به افزایش تاثیر گذاری تهدیدات زیر ساخت و شریان های اطلاعاتی شده است.

سطح دوم امنیت در فضای سایبر، امنیت در حوزه فرد و اجتماع است. در این حوزه با توجه به تفاوت در کارکرد انسان و حقوق او در ایدئولوژی اسلامی با ایدئولوژی غرب چالش هایی را ایجاد می نماید. ابعاد این چالش در بعد فردی و اجتماعی ضرورت طرح ریزی برای امنیت فرهنگی و امنیت اخلاقی و دینی را ایجاب می نماید.

سطح سوم امنیت در فضای سایبر، امنیت در حوزه ملی و حاکمیتی است. تهدیدات در حوزه ملی و حاکمیتی، مجموعه تهدیداتی است که حیاتی ترین منافع ملی و حاکمیتی یک نظام را به چالش می کشاند. این حوزه از تهدیدات بخش در حوزه زیرساخت و شریان های اطلاعاتی قرار داشته بخشی در حوزه امنیت سیاسی و اقتصادی است. فضای سایبری که ذاتاً ابزاری برای تعامل و ارتباط افراد و جوامع است فضایی را برای جنگ روانی ایجاد می نماید. در این جنگ اطلاعات بر علیه فکر و ذهن افراد استفاده می شود و منجر به عملیات علیه اراده ملی، عملیات علیه عناصر نظامی، ایجاد تضاد فرهنگی و ایجاد تنش و هرج و مرج می شود(آلبرتس، ۱۳۸۵: ۱۰۴). امروزه به هم پیوستگی زیرساخت‌های دیجیتالی نهادهای مختلف از قبیل سازمان‌ها، کسب و کارها، دولت ها، افراد و... باعث شده است که این فضا با چالشی جهانی از سوی حملات سایبری روبرو شود. دامنه و گستردگی این حملات که از یک بدافزار ساده گرفته تا حملات مداوم پیشرفته و هدفمند به گونه‌ای است که اطلاعات حساس افراد و زیرساخت های حیاتی سازمان‌ها و کشورها را با تهدید جدی مواجه کرده است. به علت همبستگی بین نهادها و موجودیت‌های مختلف در جهان این تهدیدات به طور قراردادی

و تکنیکی به عنوان «تهدیدات سایبری جهانی» شناخته می‌شوند. این تهدیدات دامنه وسیعی از جرایم سایبری را در بر می‌گیرد و همواره خسارات جدی را به سازمان‌ها و افراد وارد می‌کند. تهدیدات در بیشتر مواقع به طور ذاتی مخرب و تهاجمی است. قربانیان ممکن است دارایی‌های فکری و مالکیت معنوی خود را از دست بدهند یا حساب‌های بانکی آنها افشا شود، یا به طور ناخواسته باعث انتشار ویروس به رایانه‌های دیگر شبکه شوند. در سطح بالاتر هکرها اطلاعات محرمانه کسب و کارها را بدست آورده و حتی زیرساخت های حیاتی کشورها را تهدید و از کار می‌اندازند.

هزینه کم ورود، ناشناس بودن، مشخص نبودن قلمرو جغرافیایی تهدیدکننده، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری، موجب شده بازیگران قوی و ضعیف اعم از دولت‌ها، گروه‌های سازمان‌یافته و تروریستی و حتی افراد به این فضا وارد شده و تهدیدهایی همچون جنگ سایبری، جرایم سایبری، تروریسم سایبری، جاسوسی سایبری و مانند آنها را به وجود آورند. همین نکته، تهدیدهای سایبری را از تهدیدهای سنتی امنیت ملی که تا حدود زیادی از ماهیت شفافی برخوردارند و بازیگران آن را دولت- ملت هایی تشکیل می‌دهند که در یک قلمرو مشخص جغرافیایی قابل شناسایی هستند، متمایز کرده و سبب شده است امنیت ملی به مفهوم سنتی آن در این فضا به چالش کشیده شده و ناکارآمد به حساب آید. آسیب-پذیری امنیت ملی کشور در برابر کارکرد سیاسی فضای مجازی نیز در اولویت نخست تهدیدات قرار گرفته است.

در سیاست های امنیت سایبری سعی بر قابل در دسترس بودن؛ یکپارچگی ای که شامل اعتبار و صحت است؛ و نیز محرمانه بودن است. مبارزه با جرایم مرتبط با امنیت سایبری نیازمند یک روش جامع است. ارائه معیارهای تکنیکی به تنهایی نمی‌تواند از هیچ جرمی جلوگیری کند، قطعاً به نمایندگی‌های اجرای قانون اجازه داده شده است که جرایم سایبری را مورد تحقیق و پیگرد قرار دهند. در این فضا ، همانند فضای حقیقی تأمین امنیّت و صیانت از کاربران آن مورد توجّه قرار گرفته و برخی از آموزه‌های عمومی تأمین امنیّت محیط مادّی نیز در این محیط بکار می‌رود. لیکن، به علّت ماهیّت متفاوت فضای مجازی از فضای مادّی، تأمین امنیّت

و پیشگیری از جرایم ارتکابی در فضای جدید شیوه‌ها و تکنیک‌های خاصّی را می‌طلبد که باید به صورت دقیق‌تری مورد بررسی قرار گیرد (فرهادی آلاشتی،۱۳۹۵، ۱۴).

روش

روش تحقیق در این پژوهش، توصیفی - تحلیلی است که روش گردآوری اطلاعات و داده‌ها با استفاده از منابع کتابخانه‌ای، با مراجعه به منابع تالیفی شامل کتاب‌ها و مقاله‌های تالیفی و ترجمه‌ای، اسناد بین‌المللی موجود، قانون، رویه قضایی و از طریق فیش‌برداری انجام می‌شود. این تحقیق فاقد جامعه آماری است و روش تجزیه و تحلیل داده‌ها به صورت کیفی و مبتنی بر استدلال و استنتاج نگارنده از اطلاعات موجود خواهد بود.

یافته‌ها

هماهنگ نبودن هنجارهای ملی و بین المللی

تنوع نظام‌های سیاسی، اقتصادی، اجتماعی و فرهنگی کشورها، مانعی اساسی در راه ایجاد این وفاق برای هنجارگذاری در فضای مجازی محسوب می‌شود. برای رفع این مانع و موارد مشابه، باید سیاست گذاری فراتر از حوزه صلاحیت های داخلی و ملی صورت گیرد. در پرتو سیاست‌گذاری است که تفکر حاکم برای ایجاد امنیت سایبری مشخص می شود.

سیاست جنایی عموم کشورها در قبال جرایم سایبری به ویژه از نوع جرایم اینترنتی به این نتیجه رسیده است که رویکرد ملی به تنهایی برای مقابله با این جرایم کافی نیست. ناتوانی سیاست جنایی در قبال این جرایم نه به جهت مشکلات مرتبط با روش تعیین و اعمال تدابیر سیاست جنایی در رویارویی با جرایم سایبری که به دلیل چالشهای مرتبط با ماهیت این جرایم است. این جرایم در بستری جهانی و فراتر از مرزها و با کیفیاتی جدید ارتکاب می یابند که رویکرد ملی در مقابله به آن ها محکوم به ناکامی و ناتوانی است. در واقع با توجه به تحولات و توسعه‌هایی که به ویژه در قرن گذشته و حاضر در عرصه‌های مختلف اتفاق افتاده است، دولت‌ها نیازمند ایجاد تشکیلات مستمر و منظمی هستند تا بتوانند با همکاری و همبستگی

بین‌المللی، در رسیدن به اهداف مشترک یکدیگر را یاری کنند (مشهدی و تسخیری، ۱۳۹۲، ۱۵۱۶-).

تلاش‌های متعددی برای تعریف واحد از جرایم سایبری به عمل آمده است که نمونه آن را می توان در فرایند شکل گیری کنوانسیون بوداپست مشاهده کرد. اما جرم سایبری آن‌قدر پویاست که کنوانسیون بوداپست را می‌توان ناکارآمد دانست زیرا برای مثال، تحولات مدرن و مسایلی از قبیل هرزنامه‌ها، سرقت هویت، اقدامات آماده‌سازی و حملات سایبری بزرگ مقیاس و هماهنگ علیه زیرساخت‌های حساس اطلاعاتی، تروریسم سایبری، فیشینگ و فارمینگ، جوانبی از امنیت سایبری، پیشگیری فنی، جوانب سازمانی، مشارکت‌های خصوصی - عمومی و ... در این کنوانسیون یا درنظر گرفته نشده‌اند یا به طور مناسب با آنها برخورد نشده است (مقیمی،۱۳۹۵: ۳۱).

خلاهای سیاست تقنینی

اینترنت به صورت لجام گسیخته گسترش یافته است، اما ملاحظات آن نادیده گرفته شده است. جهانی سازی خود یکی از عوامل گسترش فن آوری اطلاعات بوده است. مشکل از آن جا ناشی می شود که اینترنت از ابتدا با هدف بهره برداری نظامی و کنترل خارجی ابداع شده بود. حتی کسانی که مدافع توسعه اینترنت هستند، بر این باورند که زمانی اینترنت می تواند به ظرفیت کامل خود برسد که از آنارشی موجود خارج شده و قواعد مسلمی بر آن حاکم شود(ریج، ۲۰۱۵: ۲۲).

پیشرفت کافی در قانون‌گذاری و در این روش پیشرفت چهارچوب قانونی مربوط به جرایم سایبری بخش اصلی از استراتژی امنیت سایبری است. برای امنیت سایبری ابتدا نیازمند تهیه قوانین صریح برای جرم دانستن مصدایق نقض کننده امنیت این فضا است. جرم انگاری های

- کنوانسیون جرایم سایبری معروف به «کنوانسیون جرایم سایبری بوداپست» و یا به اختصار «کنوانسیون بوداپست» نخستین معاهده بین‌المللی است که به **جرائم رایانه‌ای** و اینترنتی می‌پردازد و می‌کوشد قوانین ملی را سازگار کرده، روش‌های تحقیقات را ارتقا دهد و همکاری بین کشورها را بهبود بخشد.

مانند کلاهبرداری رایانه ای، دسترسی غیرقانونی، تداخل اطلاعات، تخلفات مربوط به حق مالکیت معنوی و جرایم علیه عفت عمومی .... .

شورای عالی فضای مجازی طی حکمی توسط مقام معظم رهبری در تاریخ تأسیس شد که در آن روسای قوا و برخی دیگر از مسئولان نظام عضو هستند. مسئولیتی که به عهدهٔ این نهاد گذاشته شده است، ناشی از خلأی بود که در مسألهٔ فضای مجازی و گسترش آن در جامعه و نفوذ آن در زندگی شخصی و اجتماعی افراد احساس می شد. مقام رهبری طی حکمی دلایل تشکیل شورا را بیان کردند: گسترش فزاینده فناوری های اطلاعاتی و ارتباطاتی به ویژه شبکهٔ جهانی اینترنت و آثار چشمگیر آن در ابعاد زندگی فردی و اجتماعی، و لزوم سرمایه گذاری وسیع و هدفمند در جهت بهره گیری حداکثری از فرصت های ناشی از آن در جهت پیشرفت همه جانبه کشور و ارائه خدمات گسترده و مفید به اقشار گوناگون مردم و همچنین ضرورت برنامه ریزی و هماهنگی مستمر به منظور صیانت از آسیب های ناشی از آن اقتضا می کند که نقطهٔ کانونی متمرکزی برای سیاست گذاری، تصمیم گیری و هماهنگی در فضای مجازی کشور به وجود آید.

تشکیل این شورا برای امور خطیری که بر عهدهٔ آن نهاده شد است، اقتضا دارد تصمیمات و مصوبات اعضای آن از چنان موقعیتی برخوردار باشد که مورد تبعیت تمام دستگاه های ذیربط قرار گیرد و الزام مناسب را به همراه داشته باشد. به همین خاطر مقام معظم رهبری مصوبات این نهاد تازه تأسیس را لازم الاجرا دانسته و بیان داشتند: «به این مناسبت شورای عالی فضای مجازی کشور با اختیارات کافی به ریاستِ رئیس جمهور تشکیل می‌گردد و لازم است به کلیهٔ مصوبات آن ترتیب آثار قانونی داده شود». به همین جهت کلیهٔ دستگاه ها می بایست از تصمیمات این نهاد که به حکم رهبری لازم الاتباع می باشد، پیروی کرده و خود را ملزم به رعایت آنها بدانند. این نهاد بر پایهٔ اصول ۷۱ و ۸۸ قانون اساسی تشکیل شده است، بر این اساس نهادهای دیگر حق رد و یا تأیید مصوبات این شورا را نداشته، بلکه کلیهٔ نهادها ملزم به اجرای آنها هستند. قائل شدن اختیار تصویب قانون یا مصوبات لازم الاجرا به شورای عالی فضای مجازی، باعث شده است تا این نهاد نیز در زمرهٔ نهادهای متعدد قانون

گذاری در جمهوری اسلامی ایران درآید و مصوباتش در حیطهٔ صلاحیت آن در حدی باشد که نهادهای دیگرِ قانون گذاری امکان تزاحم و تداخل در آنها را نداشته باشند و به نوعی از حیث سلسله مراتبی مصوباتش در موارد مربوط به فضای مجازی در مرحله‌ای برتر و مُشرف بر دیگر نهادها قرار گیرد.

به نظر می‌رسد به رغم اقدامات انجام شده در حوزه تقنین و تشکیل شورای عالی فضای مجازی هنوز نقشه راه یکپارچه برای مدیریت کل فضای مجازی وجود ندارد. این موضوع می‌تواند ناشی از تاخیر در نهادسازی و قانونگذاری و سرعت تحولات این فضا باشد. هرچند تشکیل شورای عالی فضای مجازی می تواند امیدبخش باشد اما به جهت انفعال دوره اول آن و مستمر نبودن جلسات و مغفول ماندن برخی مولفه های موثر پیشگیرانه تاثیر مدیریت کلان این شورا را با چالش مواجه کرده است.

تعدد نهادها و موازی کاری

در سطح ملی، در ایران شورای عالی فضای مجازی از تاریخ ۱۷ اسفند ۱۳۹۰ به فرمان رهبر معظم انقلاب اسلامی تشکیل و موظف به راه‌اندازی مرکز ملی فضای مجازی کشور شد. «شورای عالی فضای مجازی» با نظارت رئیس جمهور تشکیل و بالاترین نهاد حاکمیتی برای فضای سایبری ایران است که برای اجرای سیاست‌ها، تصمیمات و مصوبات خود، مرکزی با نام «مرکز ملی فضای مجازی» تشکیل داده است. ۳ کمیسیون عالی نیز در ذیل مرکز ملی فضای شامل کمیسیون عالی تنظیم مقررات فضای مجازی کشور، کمیسیون عالی ارتقا تولید محتوای فضای مجازی و کمیسیون عالی امنیت فضای مجازی نیز تشکیل شده است.

موضوع انحلال شوراهای موازی اواخر شهریور ۹۴ از سوی رهبر معظم انقلاب در قالب حکم جدید انتصاب اعضای شورای عالی فضای مجازی مورد تاکید قرار گرفته بود، ایشان در این حکم جدید ضمن تأکید بر مفاد حکم اولیه تشکیل شورا و پیوست آن توجه به نکات و موارد جدیدی از جمله «انحلال شوراهای عالی مصوب در گذشته که موازی این شورا هستند را به منظور تحکیم جایگاه فراقوه‌ای و موقعیت محوری و کانونی شورای عالی و نیز انتقال وظایف آن شوراها به شورای عالی فضای مجازی» مورد تاکید قرار دادند. موضوعی که

سرانجام در آغاز سال ۱۳۹۵ و با برگزاری نخستین جلسه شورای عالی فضای مجازی تعیین تکلیف شد. اما باز هم به نظر می‌رسد نوعی ناهماهنگی یا تداخل وظایف با سایر نهادها و سازمان‌ها وجود دارد. به طور مثال درباره امنیت فضای مجازی نیروی انتظامی، وزارت فناوری اطلاعات و ارتباطات، سپاه پاسداران انقلاب اسلامی ، ارائه دهندگان خدمات میزبانی و اپراتورهای تلفن همراه، سازمان تنظیم مقررات و ارتباطات رادیویی و دارای نقش هستند.

پراکندگی و تعدد نهادهای متولی پیشگیری از جرم در ایران، ناهماهنگی بین نهادهای ذی ربط و نیز نبود یک سیاست علمی، هماهنگ و سنجیده در این زمینه باعث هدر رفتن امکانات و ظرفیت های سازمان ها و نیز خنثی شدن فعالیت های بخش های مختلف سیاست جنایی در پیشگیری از جرم خواهد شد(منصورآبادی و ابراهیمی، ۱۳۸۷:).

به طور خاص برای امنیت فضای مجازی نیز به نظر می رسد یک راهبرد منسجم در این باره هنوز شکل نگرفته است و حتی اگر اولویت‌های راهبردی را منحصر در حکم رهبری بدانیم لازمه اجرای آن تدوین برنامه و سیاست‌های هماهنگ ساز برای اجرا است. بنابراین شورای عالی فضای مجازی باید وظایف را میان دستگاه ها تقسیم و آن ها را هماهنگ کند که به نظر می رسد در حال حاضر در این باره چندان موفق نبوده است.

فرهنگ سایبری و پیشگیری جامعه مدار

در حیطه تدابیر جامعه مدار مولفه‌های فرهنگی برای جهت‌دهی و معنابخشی به تغییرات و تحولات فضای سایبر به منظور تامین امنیت در راهبردهای امنیت سایبری کشور و به طور خاص جایگاه تدابیر پیشگیری اجتماعی و امکان بهره گیری پلیس از این ظرفیت باید مورد بحث و مطالعه قرار گیرد تا جایگاه و الویت آن در سیاست های پیشگیرانه پلیس برای تامین امنیت سایبری به خوبی درک شود.

فرهنگ سایبری در بند ۷ حکم اعضای شورای عالی مجازی در تاریخ ۱۴ شهریور ۱۳۹۴ توسط رهبری بدین ترتیب بحث فرهنگ مورد توجه قرار گرفته است: «ترویج هنجارها، ارزش‌ها و سبک زندگی اسلامی ایرانی و ممانعت از رخنه‌ها و آسیب‌های فرهنگی و اجتماعی

در این عرصه و مقابله مؤثر با تهاجم همه‌جانبه فرهنگی و نیز ارتقای فرهنگ کاربری و سواد فضای مجازی جامعه».

در رویکردهای پیشگیرانه کنشی نقش اجتماع و فرهنگ بی بدیل است. آموزش و فرهنگ به عنوان بستر حرکت جوامع و الگوهایی که انعکاس دهنده ارزش‌ها، سنت‌ها و هنجارهای پایدار جامعه‌اند در مباحث امنیت در فضای سایبری بایستی مورد توجه باشد. برای این منظور می‌توان فرهنگ‌سازی سایبری را وارد نظام آموزشی خود چه در مدارس و چه در دانشگاه‌ها و مراکز علمی کرد. مدرسه و محیط آموزشی بخش اعظمی از زندگی یک فرد را به خود اختصاص می دهد بنابراین نقش مهمی در تکوین شخصیت فرد و نهادینه شدن بسیاری از هنجارها در درون فرد دارد. اما برای نهاد اجرایی مانند پلیس کم ترین نقش در این حوزه دیده شده و میزان مشارکت نهادهای فرهنگی و آموزشی با این نهاد به اقداماتی نمادین و محدود است.

حریم خصوصی و چالش‌های نظارت

ارتباط تنگاتنگ جرایم سایبری با استفاده از اطلاعات شخصی و محرمانه، حریم خصوصی اشخاص، به طور مستقیم و غیرمستقیم، آماج فعالیت های غیرقانونی قرار می‌گیرد. بنابراین، اتخاذ راهکارهای پیشگیرانه مؤثر و روزآمد در این راستا از مهم ترین پیش نیازهای توسعه در جامعه اطلاعاتی است. اگرچه فناوری اطلاعات، معمولاً یکی از عمده ترین دلائل نقض حریم خصوصی تلقی می گردد، راه های گوناگونی نیز وجود دارد که از طریق آن ها این فناوری، خود قادر به حمایت از محرمانگی و پیشگیری از نقض آن می باشد. امروزه رهنمودها و شیوه های محافظت از حریم خصوصی که به روش های علمی طراحی شده‌اند مورد استفاده قرار می گیرند. این امکانات، طیف وسیعی از تمهیدات و راهکارها از روش شناسی های طراحی شده بر مبنای اطلاع رسانی اخلاقی تا رمزنگاری به منظور محافظت از اطلاعات شخصی در مقابل استفاده غیرمجاز را دربرمی گیرد(محسنی،۱۳۹۵: ۹۳).

اجرای تدابیر پیشگیرانه وضعی، همانند بسیاری از سایر تدابیر پیشگیرانه، ممکن است محدودیت هایی ایجاد کند. از این رو، هدف پیشگیری، نمی‌تواند کاربرد هر وسیله، فن، اقدام

و روش‌های خاص فراقانونی شود (نجفی ابرندآبادی، ۱۳۸۲، ص ۵۶۷). در بند دوم و سوم اصل ۲۶ «رهنمود پیشگیری از جرم[1]» سازمان ملل متحد سال ۲۰۰۲ به بهره‌گیری از تدابیر پیشگیری وضعی که به قابلیت و بدنه‌ی محیط اجتماعی لطمه وارد نکند و دسترسی آزاد به مکان‌های عمومی را محدود ننماید، تأکید شده است. در ارتباط با بند ۱ لازم به توضیح است که از نظر فنی و تخصصی، ممکن است با کاربرد تدابیر پیشگیری وضعی در فضای سایبری، شاهد برخی اختلالات همچون کاهش سرعت شبکه، بسته شدن اشتباهی برخی از سایت‌ها و وبلاگ‌ها به جهت پالایه، محدودیت‌های بی‌جهت برای ورود به برخی فضاها، اعمال محدودیت در دسترسی به شبکه‌های بین‌المللی و غیره بود. نتیجه‌ی اعمال این شرط رهنمود، بهره‌گیری از رویکردی سنجیده و ملایم‌تر نسبت به ممنوعیت کامل شبکه‌های اجتماعی مجازی، مسئله‌ی پالایه و افزایش دقت و هوشمندی سامانه‌های پالایه است. بند ۲ این رهنمود نیز با تفویض تصمیم‌گیری به سازمان ها، نهادها یا اشخاصی که صلاحیت قانونی چنین امری را دارند یا بر روند و نحوه اجرا این گونه تدابیر نظارت مستقیمی دارند قابل اجرا است.

پیشگیری پایدار از نقض حریم خصوصی کاربران، تنها در غالب یک سیاست جنایی جامع امکان پذیر است که مشتمل بر راهکارهای روزآمد، پویا و مبتنی بر همکاری بخش های تخصصی، تقنینی و اجرایی باشد و در آن آموزش مستمر به سطوح مختلف اجتماع به ویژه در مدارس و دانشگاه ها به منظور تعامل و مشارکت اجتماعی پیش‌بینی شده باشد.

نظارت بر محتوی

درمصوبه شورای عالی فضای مجازی با موضوع توسعه فضای مجازی سالم، مفید و امن به شماره ی ۹۴/۱۰۰۱۵۱/ش مصوب ۹۴/۱/۳۰ به تعریف فضای مجازی ایمن پرداخته شده است. در این مصوبه آمده: «فضای ایمن فضایی است متشکل از شبکه‌های ارتباطی که در آن محتوا و خدمات مفید در چارچوب مبانی و ارزش های اسلامی و مقررات کشور ارائه می شود و کاربران می توانند بر اساس ویژگی های جمعیتی از قبیل سن، جنس، شغل و تحصیلات از محتوا و خدمات مورد نیاز بهره مند شوند و حتی الامکان در برابر محتوا و رفتارهای آسیب زا

1. The guidelines for the prevention of crime

محفوظ بمانند». در عنوان این مصوبه هر چند به توسعه ی فضای مجازی سالم، مفید و ایمن پرداخته شده است اما در تعریفی که از فضای ایمن ارائه شده، به نظر می‌رسد فضای ایمن به لحاظ محتوایی مدنظر بوده یعنی فضایی که محتوای آن در چارچوب مبانی اسلامی باشد به عبارت بهتر در این مقرره قانون گذار صرفا به پالایش محتوا توجه داشته در حالی که پالایه یک اقدام حفاظتی محسوب نمی شود(فضلی، ۱۳۸۹: ۱۱۱). دلیل این امر این است که پالایه همواره از سوی مقامات دولتی و برای پاک سازی یک وب سایت یا سایت از اطلاعاتی که به لحاظ مضمون با مبانی اخلاقی و اسلامی ناسازگار اند به کار رفته و جنبه حفاظتی ندارد در حالی که آن چه در حفاظت از اطلاعات مالی مدنظر است این است که از اطلاعات مالی حفاظت به عمل آید تا این اطلاعات افشاء، تخریب و محو و غیره نشوند که این حفاظت می-تواند هم از سوی اشخاص حقیقی و هم حقوقی باشد. در مصوبه دیگر این شورا با موضوع سیاست های سامان دهی خدمات پیامکی ارزش افزوده و پیامک انبوه در شبکه های ارتباطی به شماره ۹۳/۱۰۳۶۸۱/ش مورخ ۹۳/۱۱/۱ در بند ۴ آمده: «به منظور حفظ و صیانت از اطلاعات خصوصی مخاطبان پیام و بر اساس قوانین به ویژه قانون جرائم رایانه ای، ارائه دهندگان خدمات ارتباطی و ارائه دهندگان خدمات محتوایی حق واگذاری، فروش و یا در اختیار قرار دادن این اطلاعات به دیگران را ندارند». در این مصوبه نیز هرچند به حفاظت و حراست از اطلاعات اشاره شده، اما تنها به حفاظت از اطلاعاتی که مربوط به حریم خصوصی شهروندان است، پرداخته شده و به سایر حوزه ها از جمله اطلاعات مالی به طور خاص توجهی نشده است(جاوید نیا، ۱۳۸۸: ۵)

در مصوبه دیگر این شورا درباره طرح های کلان مرکز ملی فضای مجازی کشور جهت تدوین لایحه بودجه و در تصویبنامه ی این شورا درباره شرح وظایف، اختیارات و اعضای کمیسیون عالی فضای مجازی، به ارتقای امنیت سایبری پرداخته شده است. در این مصوبه قانون گذار به تولید محتوای فضای مجازی به صراحت توجه نموده است در حالی که مفهوم امنیت و ابعاد آن در این جا تشریح نشده است. از منظر حقوقی، امنیت سایبری در دو مفهوم مضیق و موسع به کار می رود. در مفهوم مضیق به معنای اتخاذ تدابیر فنی پیش گیرانه برای

حفاظت و حراست از اطلاعات در بستر سامانه های رایانه‌ای و مخابراتی است(احسانی موید، ۱۳۸۹: ۱۲). در این مفهوم اقدامات غیر فنی جایگاهی نداشته و اشخاص موضوع مستقیم تدابیر امنیتی قرار نمی گیرند اما در مفهوم موسع، دو قسم از تدابیر را برای تامین امنیت در محیط سایبر می توان برشمرد: نخست تدابیر واسطه‌ای که تعریف آنها پیش تر اشاره شد و دوم تدابیر مستقیم یا اصلی. تدابیر اخیر به تدابیر پیش گیرانه ی وضعی اعم از تدابیر نظارت انسانی یا فنی گفته می‌شود که برای تامین امنیت دو موضوع زیر به کار می رود: نخست اطلاعات رایانه ای که از مرحله ورود یا تولید تا ذخیره و انتشار و مورد استفاده قرار گرفتن در معرض انواع رفتارهای مخرب و مختل کننده است که این رفتارها موجب نابودی یا افشای اطلاعات مالی در این فضا می شود و دوم: سیستم ها و شبکه های رایانه ای و مخابراتی که سیستم و شبکه نیز همچون اطلاعات آسیب پذیر بوده و از آن جا که که مقوم آنها اطلاعات است، اقداماتی نظیر انتشار ویروس، اختلال در کارکرد و بازدهی، ممانعت از ترافیک و دسترسی به اطلاعات و غیره امنیت آنها را به شدت تهدید می کند، از این رو برای امنیت اطلاعات و سیستم، از اقدامات پیش گیرانه وضعی استفاده می شود. امنیت اطلاعات نیز به فرایند حفاظت از اطلاعات در برابر کارهای غیر مجاز شامل دسترسی، استفاده، افشاء، اختلال، تغییر، مطالعه، بازرسی و ضبط گفته می شود(حسن بیگی، ۱۳۸۴: ۱۱).

لزوم مشارکت بخش عمومی و خصوصی

امنیت، مفهومی چندوجهی داشته و همزاد با مفاهیمی مانند قدرت، تهدید و آسیب است. ابعاد مختلف امنیت ملی در فضای مجازی همانند فضای حقیقی می‌تواند نیز در سطوح امنیت اجتماعی، اقتصادی، فرهنگی، کسب و کار و ... مورد توجه باشد که میزان مداخله و نقش پلیس در هریک به یک میزان نیست و بیشتر ساحت عمومی امنیت را مد نظر دارد. برابر مصوبه شورای عالی فضای مجازی در تاریخ ۱۳۹۶/۰۸/۱۵ نیروی انتظامی جمهوری اسلامی مسئول رسیدگی به حوادث فضای مجازی است که در حوزه عمومی به وقوع می‌پیوندد. البته این به معنای نادیده گرفتن سایر ساحت‌های امنیت فضای مجازی و تعامل با سایر نهادهای مرتبط نیست.

بخش‌هایی که هریک به نحوی از فضای مجازی و جرایم ارتکابی در این فضا تاثیرپذیرند می‌توانند در تامین امنیت داری سهم و نقش باشند. به طور کلی می‌توان فعالان فضای مجازی را عبارت دانست از سیاست‌گذاران، تولیدکنندگان محصولات، ارائه‌دهندگان خدمات و کاربران فضای سایبری. سیاست‌گذاران فضای سایبری اشخاص حقیقی و حقوقی هستند که به نوعی در تصمیم‌سازی و تصمیم‌گیری برای این فضا نقش دارند. به همین ترتیب تولیدکنندگان فناوری‌های نیز اشخاصی هستند که با توجه به نظام سیاست‌ها و تصمیم‌های جاری، به تولید فناوری سایبری می‌پردازند. برای تامین امنیت و به طور خاص امنیت در فضای مجازی باید همه فعالان بخش های دولتی و خصوصی مشارکت داشته باشند. باید درنظر داشت که هیچ سیاستی در قبال جرایم سایبری بدون مشارکت تمام بخش‌های مرتبط یعنی حکومت، بخش خصوصی، جامعه و به طور کلی، تمام کسانی که به نحوی از فضای سایبر ذی‌نفع و متأثر می‌باشند، قابلیت اجرا و تداوم نخواهد داشت (حاجی‌ده‌آبادی و سلیمی، ۱۳۹۳: ۸۳ و ۸۴).

در سطح کلان قانون پیشگیری از وقوع جرم مصوب سال ۱۳۹۴ برای ورود بخش خصوصی به عرصه تصمیم گیری سازوکاری پیش بینی نکرده است. ماده ۲ این قانون شورای عالی پیشگیری از وقوع جرم را شامل اعضایی دانسته که هیچ یک از آنها بخش خصوصی نیست. در شورای عالی مجازی نیز همین امر مشاهده می شود.

هر چند شورای‌عالی فضای مجازی، مشارکت با بخش خصوصی را در جلسه بیست و ششم مورخ ۱۳۹۴/۰۹/۲۵، به صورت یک امر مستقل و به عنوان یک سیاست با تصویب «سیاست‌های حاکم بر برنامه ملی بازی‌های رایانه‌ای»، (در بند ۳ و ۶ «ماده ۱: سیاست‌ها») تلقی کرده است ولی مشارکت بخش خصوصی منحصر موضوع بازی های رایانه ای نیست.

دانشگاه‌ها و موسسه‌های پژوهشی معمولاً متخصصان فنی، حقوقی و مدیریتی مورد نیاز برای طراحی و اجرای راهبرد پیشگیری از جرم سایبری را آموزش می‌دهند. از سویی معمولا دانشگاه‌ها پیشگام در تحقیق و توسعه راه حل‌ها و سامانه‌های پیشگیری از جرم سایبری هستند. در حقیقت موسسات پژوهشی و دانشگاهی می‌توانند شریک مهمی در پیشگیری از تهدیدات سایبری از خلال تسهیم دانش؛ مشاوره برای وضع قانون و توسعه سیاست‌ها و خط مشی‌ها؛

توسعه فناوری و معیارهای فنی؛ ارائه مساعدت فنی و همکاری با مراجع اجرای قانون باشند؛ بنابراین ضروری است با ایجاد یک ساختار مناسب، از این ظرفیت علمی بهره برداری کرد.

هر چند پلیس، مخابرات، بخش های خصوصی و.. دارای مراکز واکنش به حملات سریع هستند ولی به نظر می رسد در زمینه امنیت فضای مجازی یک نهاد منسجم، یکپارچه و هماهنگ‌ساز برای برای پیشگیری، شناسایی، تحلیل و ارزیابی ریسک و پاسخ به تهدیدات و حملات سایبری ضروری است. این نهاد می‌تواند ضمن جلوگیری از جزیره‌ای عمل کردن سایر مراکز واکنش سریع، به اشتراک اطلاعات آنها و تسریع پاسخ‌ها کمک کند(مقیمی،۱۳۹۵: ۱۳۵).

شرکای متعدد بین المللی در ارائه خدمات اینترنتی

حملات سایبری ممکن است که از سوی یک دولت برای هدف قرار دادن زیرساخت‌های اساسی یک دولت از جمله سیستم بانکی، انرژی و حمل و نقل عمومی که به شبکه رایانه‌ای متصل هستند انجام شود. حمله سایبری توسط افراد خصوصی در صورتی که در استخدام دولت یا تحت کنترل دولت باشند به دولت منتسب می‌شود و حمله سایبری با همکاری شرکت‌های ارائه‌دهنده خدمات اینترنتی تا جایی که در چارچوب اقتدار عمومی یا تحت کنترل دولت عمل می‌کنند به دولت منتسب می‌شود. حملات سایبری اگر مصداقی از تجاوز یا توسل به زور محسوب نشوند می‌تواند به عنوان مداخله در امور داخلی دولت یک تخلف بین‌المللی تلقی شود.

در دوره ای که فضای مجازی درست به اندازه زمین و دریا اهمیت دارد امنیت سایبری باید توسط همه کشورهای جهان محافظت شود وگرنه به پاشنه آشیل در توسعه اینترنت تبدیل می شود. به همین دلیل باید به دنبال ایجاد سیستم حاکمیت اینترنت شفاف بین المللی، دموکراتیک و چندجانبه ای بود که بتواند به کل دنیا نفع بیشتری برساند. افزایش استفاده از اینترنت در سطح جهان چالش هایی را در زمینه مدیریت و قانونمندسازی بوجود آورده است. راهبری اینترنت شامل موضوعات گسترده ای از اداره فنی آن تا مباحث عمومی تر چون نظارت بر محتوی می شود. علی رغم ماهیت بین المللی اینترنت، دشواری

توافق در سطح جهانی بر سر این مقررات باعث تدوین بیشتر این قوانین در سطح ملت ها شده است که مجموع این تلاش ها به تشکیل مجمع راهبری اینترنت برای استفاده از نظرات سه بخش دولتی، عمومی و خصوصی کشورهای عضو رأی تدوین و تصویب قوانین مرتبط منجر شده است. در نهایت در سال۲۰۱۵ راهبری اینترنت بدین صورت تعریف گردید: «راهبری اینترنت توسعه و استفاده به وسیله دولت ها، بخش خصوصی و عمومی در قالب قوانین، و ارزش های مشترکشان برای ایجاد چارچوبی برای ارزیابی و استفاده از اینترنت است(دناردیس، ۲۱۱: ۵۱).

ضرورت همکاری های بین‌المللی

ترویج همکاری‌های بین‌المللی با توجه به ماهیت فراملی جرایم سایبری ضرورتی انکار ناپذیر است که به صرف همکاری‌های سنتی در عرصه بین‌المللی مانند استرداد مجرمان کفایت ننموده و تعامل مستقیم و به هنگام نهادها اجرایی را مطالبه می‌کند. اما تکثّر نظام‌های حقوقی، موانع عقیدتی و ایدئولوژیک، نبود یک معاهده فراگیر و الزام آور بین‌المللی، ابهام در معیارهای حاکم بر سیاست‌گذاری، ضعف نهادهای اجرایی و هنجارگذار بین‌المللی، عدم تمایل به مشارکت، محدودیت‌های ساختاری و عدم توازن در بهره‌گیری از فناوری‌ها مانع از شکل‌گیری یک رویکرد هماهنگ و فراگیر در عرصه بین‌المللی در پیشگیری و مقابله با جرایم سایبری شده است(مقیمی،۱۳۹۵: ۱۳۱).

پلیس نهادی مبتنی بر رویه و عمل است و نسبت به نهادهای دولتی و ملی دیگر، قابلیت های مناسب تر و بیشتری برای برقراری های ارتباط و همکاری با پلیس دیگر کشورها دارد. حتی اگر الزامات جرایم سایبری نیز در نظر گرفته نشود، ماهیت اقدام پلیسی چنان حساس و چالش آفرین نیست که همکاری های بین المللی پلیسی با اما و اگر همراه باشد ولی وقتی پای جرایم سایبری در بستری جهانی به میان بیاید، در این صورت وضعیتی که برای نیروهای پلیس کشورها مطرح می شود این است که اقدام فراملی آن ها بر اقدام ملی اشان می چربد.

به طور کلی، همکاری پلیس به تعاملات خواسته یا ناخواستهای گفته می شود که بین دو یا چند نهاد پلیسی (شامل سازمانهای دولتی و خصوصی) با هدف اشتراک اطلاعات جنایی،

انجام تحقیقات و نهایتاً توقیف مظنونها صورت می گیرد. همکاری بین المللی پلیس حرکتی است که طی آن اطلاعات جنایی در سطح ملی و مرزهای جغرافیای سیاسی به اشتراک گذاشته می شود (لیموکس، ۲۰۱۰: ۲۸۶).

همکاری‌ها در سطح نهادهای اجرایی به ویژه در حوزه ماموریت های پلیس از طریق سازمان هایی نظیر اینترپل امکان‌پذیر است. سازمان اینترپل نقشی محوری در هماهنگ نمودن اقدامات پلیسی در این زمینه عهده‌دار است. نتایج سوء ناشی از عدم هماهنگی سطح دانش نیروهای پلیس در سال‌های اخیر از نظر نهادهای بین‌المللی و منطقه‌ای مسئول مبارزه با جرایم سایبری پوشیده نمانده و آنان نیز به این اجماع دست یافته‌اند که هر گونه تلاش برای ایجاد فضای امن و پیشگیری مؤثّر از جرایم سایبری در گام نخست نیازمند قادر ساختن طرفین درگیر در قضیه برای پاسخگویی به درخواست سایر طرفین است و این امر در وهله اول نیازمند دانش و به عبارت بهتر آگاهی از نیازهای یکدیگر است. اعضای مجمع عمومی سازمان اینترپل در سال ۲۰۱۰ در هفتاد و نهمین نشست خود با قطعنامه تشکیل مجموعه جهانی اینترپل برای نوآوری[1] (IGCI) در کشور سنگاپور موافقت کردند که در سال ۲۰۱۴ عملیاتی شد. یکی از اهداف مهم این مرکز ایجاد کانال‌های جدید بین پلیس‌های کشورهای عضو جهت مبارزه با جرایم سایبری است.

ضرورت تشکیل یک نهاد پلیسی بین‌المللی برای امور پلیسی مرتبط با جرم سایبری یعنی تشکیل پلیس جهانی اینترنتی، در سال ۲۰۰۵ توسط سازمان ملل نیز مطرح شده است[2] علاوه بر آن تدابیر خاص پلیسی درباره تروریسم و مباحث اینترنتی مرتبط با آن «نیروی ضربتی اجرایی ضد تروریسم[3]» توسط دبیرکل سازمان ملل با هدف تضمین اقدام هماهنگ برای مبارزه با تروریسم در سال ۲۰۰۵ تاسیس شد.

1 - INTERPOL Global Complex for Innovation
2- A/CONF.203/14
3-The Counter-Terrorism Implementation Task Force s

استنادپذیری ادله

مشکل جمع آوری ادله و ارزیابی آن ها در جرایم فضای مجازی در اکثر کشور ها وجود دارد. به طور کلی مشکلات ناشی از ادله الکترونیک را به سه قسم مشکلات ناشی از کشف و شناسایی ادله، مشکلات قضایی و مشکلات تخصصی تقسیم می‌شوند. به علت ماهیت غیر ملموس و غیر مادی ادله الکترونیک مشکلات زیادی در فرآیند کشف و شناسایی ادله وجود دارد. از آن جمله می توان به اخفای جرم، نامرئی بودن، کد گذاری مدارک، امحاء مدارک و فراوانی داده‌ها اشاره کرد. مشکلات تخصصی شامل کمبود نیروی انسانی آموزش دیده در نیروی انتظامی، دادسرا و دادگاه ها است. مشکلات قضایی می تواند مرتبط با قدرت دستیابی و قابلیت جمع آوری ادله باشد(جوانمرد،قاضی میرسعید و امیرآبادی، ۱۳۹۵: ۴۶۳). هم چنین میزان اعتبار ادله جمع آوری توسط ضابطان از دیگر چالش های بحث است. هر چند به نظر می رسد ادله الکترونیکی در چارچوب نظرات کارشناس اعتبار می‌یابند اما نوع نگاه مراجع رسیدگی کننده به جرایم سایبری و میزان تخصص و آشنایی آنها با ادله الکترونیکی نقشی تعیین کننده در سرنوست تعقیب و اثبات این جرایم دارد.

موانع فنی و محدودیت تدابیر فنی

پیشگیری وضعی رویکردی است که با تمرکز بر محیط هایی که جرم در آن محقق می شود تنها به دنبال کاهش فرصت های مجرمانه و ایجاد تغییر در آنهاست. منظور از ایجاد تغییر ، جاذبه زدایی از سیبل جرم، بالا بردن هزینه، سخت کردن ارتکاب جرم و خطرناک کردن آن است(صفاری، ۱۳۸۰: ۱۴). دراین نوع از پیش گیری جهت افزایش هزینه ی جرم و حفظ آماج جرم اقداماتی صورت می گیرد که این اقدامات دارای اشکالی است. از جمله این اشکال می توان به: استفاده از شیوه های سنتی نظارت و کنترل، حفاظت های فیزیکی واقدامات مادی، کنترل ورودی ها و خروجی ها، کنترل ابزاری که ارتکاب جرم را تسهیل می کند و ایجاد مانع برای برقراری تماس بین بزهکار بالقوه و آماج جرم اشاره کرد. در فضای واقعی برای حفاظت از سیبل جرم بیش تراز تدابیر فیزیکی و سنتی کنترل استفاده می شود که ماهیتا ملموس و عینی هستند مثلا با نصب دزدگیر بر روی ماشین از سرقت آن جلوگیری می شود. اما در فضای

سایبر برای حفاظت از سیبل جرم می‌بایست اکثرا از تدابیر فنی امنیتی متناسب با این فضا و از جنس آن استفاده شود. این تدابیر بیش تر ناظر به کنترل ورودی و خروجی ها و کنترل ابزاری است که ارتکاب جرم را تسهیل می کندو دارای ماهیتی فنی است(خانعلی پور، ۱۳۹۰: ۱۷).

جرایم سایبری بیشتر مواقع ماهیتی فنی و تخصصی دارند. ارائه دهندگان خدمات سایبری در بسیاری اوقات اشخاص حقیقی/حقوقی غیردولتی هستند. از این رو کارایی اقدامات پیشگیرانه، به مشارکت مسئولانه و همراه شدن نهادهای غیردولتی با دولت در فرآیند پیشگیری از جرم وابسته است. شرکت‌های تولیدکننده و واردکننده سخت‌افزارهای رایانه‌ای، شرکت‌های ارتباطی، توزیع‌کنندگان کلی و جزیی نرم‌افزار، شرکت‌های دسترسی به خدمات، اتحادیه‌ها و اصناف مرتبط، کافی‌نت‌ها، آموزشگاه‌های رایانه و همه اشخاص و نهادهای مرتبط با فعالیت‌های سایبری می‌توانند به طور مستقیم در امر پیشگیری از جرم مشارکت کنند.

از طرفی چنانچه کشورها بصورت مستقل مبادرت به آموزش واحدهای فنّی خود نمایند و "هماهنگی و تعامل کارآمد و اثربخش میان تمامی دست‌اندکاران این حوزه به وجود نیاید و یک مرکز فرماندهی واحد برای آنها پیش‌بینی نشود، بیش از همه کاربران فنّاوری اطلاعات و ارتباطات یا به عبارت بهتر شهروندان سایبری لطمه خواهند دید" (جلالی فراهانی، ۱۳۸۸: ۹۳).

نتیجه‌گیری و پیشنهادها

افزایش استفاده از اینترنت در سطح جهان، چالش هایی را در زمینه مدیریت و قانونمندسازی بوجود آورده است. راهبری اینترنت شامل موضوعات گسترده‌ای از اداره فنی آن تا مباحث عمومی تر چون نظارت بر محتوی می شود. با توجه به وسعت مباحث امنیت فضای مجازی و گستره تهدیدات، ذینفعان و بازیگران متعدد در این فضا، به طور برجسته‌ای واکاوی نقش پلیس در زمینه تامین امنیت در فضای مجازی حایز اهمیت است. زیرا پلیس به عنوان نماد حاکمیت و ضابط قضایی در پیشبرد سیاست جنایی اجرایی نقش مهمی دارد. جایگاهی که نهاد پلیس برای تامین امنیت در فضای مجازی دارد تعیین کننده مدل سیاست جنایی است که حاکم بر روابط پلیس با سایر نهادهای عدالت کیفری است. در واقع آن چه مهم است درک و برداشت پلیس از نوع ناهنجاری‌هایی که نیازمند پاسخ تلقی شده و ماهیت

پاسخ های پلیس به ناهنجاری‌های حوزه فضای مجازی و مباحث مرتبط با امنیت است. بنابراین برای مقابله همه‌جانبه و کارآمد با جرم سایبری، ضرورت بهره‌گیری از یک سیاست جنایی فراگیر با مشارکت گسترده جامعه مدنی، کاربران سایبری و سازمان‌های مردم‌نهاد آشکار می‌شود. تبیین نقش پلیس در سیاست‌های تامین امنیت در فضای مجازی، با شناختی جامع از آسیب‌ها و چالش‌های پیش روی پلیس در مقابله با تهدیدات فضای مجازی، منطبق با سیاست‌های کلی امنیت در تعامل با سایر نهادها (اعم از خصوصی و دولتی) امکان‌پذیر است. البته پلیس به عنوان یکی از اجزا اصلی در پیاده‌سازی سیاست‌های اجرایی می‌تواند در تصمیم‌سازی و در نهایت سیاست‌گذاری نیز دارای نقش باشد.

پلیس به عنوان یکی از اصلی‌ترین نهادهای مقابله و پیشگیری از تهدیدات فضای مجازی اگر شناخت دقیقی از هنجارهای حاکم بر فضای مجازی، الویت‌های تامین امنیت، ماهیت و ویژگی‌های تهدیدات و تاثیر این تهدیدات بر امنیت فضای حقیقی داشته باشد بهتر می‌تواند در تحقق سیاست‌های کلان امنیت فضای مجازی گام بردارد. هر چند سیاست جنایی اجرایی در فضای مجازی از مبانی ارزشی و گفتمان تقنینی و قضایی تاثیر می‌پذیرد، یافته‌های علمی و جرم شناختی می‌تواند به تدوین راهبردی اصولی در این زمینه کمک کند. بنابراین با توجه به تقسیم‌بندی رایج از پیشگیری(به معنای عام)، ابعاد مختلف سیاست جنایی اجرایی حداقل در دو سطح تدابیر واکنشی یا به عبارتی کیفرگرا و تدابیر پیشگیرانه (به معنای خاص) یا کنشی در راهبردهای پلیس و سایر نهادهای اجرایی قابل بحث است. در ارتباط با رویکردهای پیشگیرانه دو طیف تدابیر موقعیت‌مدار و تدابیر جامعه‌مدار مطرح خواهد بود. هر چند یکی از بهترین و کارآمدترین روش‌های پیشگیری در فضای سایبری، پیشگیری غیرکیفری است ولی بیشترین چالش نیز در حوزه تدابیر موقعیت‌مدار مطرح می‌گردد. تدابیر پیشگیرانه‌ی موقعیّت‌مدار می‌تواند از خسارات کلان سایبری پیشگیری نماید و فضای نسبتاً امن سایبری را برای کاربران شبکه ایجاد نماید، چرا که؛ در این حالت مبارزه و پیشگیری با ابزارهای خود بزهکاران صورت می‌گیرد. بنابراین، باید سیاست‌های جامعی برای تأمین امنیّت شبکه از طریق تکنیک‌های پیشگیرانه تدوین شود و با توجّه به روند تکامل جرایم به روز شود، زیرا در این نوع از

جرایم، هر دو طرف درگیر در قضیه (بزهکار و مجریان عدالت کیفری) از فنّاوری واحدی برای نیل به مقصود خود استفاده می‌نمایند و تنها تفاوت آنها در روزآمدی و استفاده حداکثری از فنّاوری‌های موجود است. در ارتباط با تدابیر موقعیت‌مدار برای تامین امنیت فضای مجازی به علت احتمال تعارض با منافع فردی افراد به جهت نادیده گرفتن حریم‌های خصوصی مسئله-ای چالش برانگیز است. به رغم کارآمدی نسبی تکنیک‌های پیشگیری موقعیّت‌مدار سایبری و بهره‌گیری از این تدابیر توسط پلیس برای امنیت فضای مجازی، تهدیدات سایبری در حال افزایش هستند و بسیاری از تصمیم‌گیری‌ها و فعالیّت‌های کاربران با اختلال روبرو شده‌اند و این خود، به معنی ضعف بخشی از تدابیر پیشگیرانه است. تدابیر پیشگیرانه‌ی موقعیّت‌مدار با برخی چالش‌ها از قبیل تحدید حقوق بنیادین بشر در نتیجه استفاده فزاینده از این تدابیر در فضای سایبر مواجه‌اند. در کنار این چالش که برای جرایم سنتی نیز صدق می‌کند، چالش‌ها و دغدغه‌های جدیدی که صرفاً منحصر به فضای مجازی هستند، نیز وجود دارند. بنابراین بررسی علل ناکارآمدی یا عدم کارایی اثربخش این تدابیر توسط مجریان قانون و ارائه الگوهایی که از کارایی حداکثری برخوردار بوده و با کمترین چالش مواجه باشند ضرورتی انکارناپذیر است. نقش آن دسته از تدابیر امنیت سایبری با محوریت تدابیر موقعیت‌مدار که منجر به نقض حقوق حریم خصوصی، آزادی بیان و آزادی جریان اطلاعات می‌شوند و آنچه که اجرای این تدابیر بر سر حقوق و آزادی‌های فردی خواهد آورد موضوعاتی است که باید مورد توجه باشد. از سوی دیگر، باید توجه داشت، در صورت عدم اتخّاذ این تدابیر، فرآیند امنیت فضای مجازی در مواجه با تهدیدات فزاینده سایبری با چه چالش‌هایی مواجه خواهد شد. در واقع پلیس به عنوان نگهبان حقوق و آزادی‌های فردی و از سویی به عنوان یک نهاد دولتی بایستی به مقوله امنیت فضای مجازی، نگاهی مبتنی بر پیشبرد منافع ملی داشته باشد.

در حیطه تدابیر جامعه‌مدار نیز مولفه‌های فرهنگی برای جهت‌دهی و معنابخشی به تغییرات و تحولات فضای سایبر به منظور تامین امنیت در راهبردهای امنیت سایبری کشور و به طور خاص جایگاه تدابیر پیشگیری اجتماعی و امکان بهره گیری پلیس از این ظرفیت باید مورد بحث و مطالعه قرار گیرد تا جایگاه و الویت آن در سیاست های پیشگیرانه پلیس برای تامین

امنیت فضای مجازی به خوبی درک شود. بنابراین ضمن حفظ رویکردهای موقعیت‌مدار بایستی رویکردهایی جامعه‌مدار هم که از عمق و پایداری بیشتری برخوردارند مورد بررسی قرار گیرند. در رویکردهای پیشگیرانه کنشی نقش اجتماع و فرهنگ بی بدیل است. آموزش و فرهنگ به عنوان بستر حرکت جوامع و الگوهایی که منعکس کننده ارزش‌ها، سنت‌ها و هنجارهای پایدار جامعه‌اند در مباحث امنیت در فضای مجازی بایستی مورد توجه باشد.

در نهایت برای پیشگیری و ایجاد امنیت در فضای مجازی، همکاری به موقع و مؤثر بین کشورها ضروری است. بنابراین دنبال نمودن ایجاد وفاق بین‌المللی در مقابله با جرایم سایبری و حضور فعال و مؤثر در پی ریزی ساختارها، راهبردها و رویه‌ها و تدابیر لازم و تعهد به اجرای آن عنصری اساسی در موفقیت راهبردهای امنیت سایبری است. تبیین نوع و چارچوب همکاری‌های بین‌المللی در سطح کلان کشور می تواند به راهبرد مشخص و موثر پلیس نیز بیانجامد.

منابع

- خالقی پوستچی، علی (۱۳۸۸). پیشگیری از جرایم سایبری با بهره‌گیری از فناوری اطلاعات و ارتباطات، همایش ملی علمی ـ کاربردی پیشگیری از جرم (قوه قضاییه، مشهد مقدس)، چاپ نخست، تهران، بنیاد حقوقی میزان.
- رزونا، جیمز و دیگران (۱۳۹۰). انقلاب اطلاعات، امنیت و فناوری های جدید، ترجمه علیرضا طیب، تهران، انتشارات پژوهشکده مطالعات راهبردی.
- زیبر، اولریش (۱۳۹۰). جرایم رایانه‌ای، ترجمه‌ی محمدعلی نوری، رضا نخجوانی، مصطفی بختیاروند و احمد رحیمی، تهران، انتشارات گنج دانش .
- عالی‌پور، حسن (۱۳۹۰). حقوق کیفری فناوری اطلاعات، تهران، انتشارات خرسندی.
- عبدالله‌خانی، علی (۱۳۸۶). جنگ نرم ۳، نبرد در عصر اطلاعات، تهران، نشر مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی معاصر.
- فضلی، مهدی (۱۳۸۹). مسئولیت کیفری در فضای سایبر، چاپ اول، تهران، انتشارات خرسندی.

- گاتن، ویلیام (۱۳۸۴). دگرگونی‌های اجتماعی در جامعه اطلاعاتی، چاپ نخست، ترجمه‌ی محمد توکل و ابراهیم کاظمی‌پور، تهران، نشر کمیسیون ملی یونسکو.
- ملزوماتی، الهام و یاری، علیرضا (۱۳۸۴). امنیت مرکز خدمات اینترنت، چاپ نخست، مجموعه مقالات همایش نقش مراکز داده در توسعه‌ی فناوری اطلاعات و ارتباطات، تهران، نشر دبیرخانه‌ی شورای عالی اطلاع‌رسانی.
- نای، جوزف (۱۳۸۷). قدرت در عصر اطلاعات (از واقع گرایی تا جهانی شدن)، ترجمه سعید میرترابی، تهران، انتشارات پژوهشکده مطالعات راهبردی.

مقالات

- بهره‌مند، حمید و حسین محمد کوره‌پز، احسان سلیمی (۱۳۹۳). راهبردهای وضعی پیشگیری از جرایم سایبری، فصلنامه آموزه‌های حقوق کیفری، سال چهارم، شماره ۷، بهار و تابستان.
- جلالی فراهانی، امیرحسین (۱۳۸۳). پیشگیری از جرایم رایانه‌ای، نشریه حقوقی دادگستری، سال دوازدهم، شماره‌ی ۴۷.
- جلالی فراهانی، امیرحسین (۱۳۸۴). پیشگیری وضعی از جرایم سایبر در پرتو موازین حقوق بشر، نشریه‌ی فقه و حقوق، سال پنجم، شماره ۱۷.
- جلالی فراهانی، امیرحسین و رضا باقری اصل (۱۳۹۳). پیشگیری اجتماعی از جرایم سایبری، راهکاری اصولی برای نهادینه سازی اخلاق سایبری، فصلنامه مرکز پژوهش لهای مجلس شورای اسلامی، دفتر ارتباطات و فناوری نوین، سال سوم، شماره ۴.
- حاجی ده‌آبادی، احمد، احسان سلیمی و علیرضا نوریان (۱۳۹۳). اصول جرم‌انگاری در فضای سایبر (با رویکردهای انتقادی به قانون جرائم رایانه‌ای)، فصلنامه مجلس و راهبرد، سال بیست و یکم، شماره هشتاد، زمستان.
- خرم‌آبادی، عبدالصمد (۱۳۸۶). کلاهبرداری رایانه‌ای از دیدگاه بین‌المللی و وضعیت ایران، فصلنامه حقوق دانشکده حقوق و علوم سیاسی دانشگاه تهران، سال ۳۷، شماره ۲، تابستان.

- خلیلی‌پور رکن‌آبادی، علی و نورعلی‌وند، یاسر (۱۳۹۱). تهدیدات سایبری و تأثیر آن بر امنیت ملی، فصلنامه مطالعات راهبردی، سال پانزدهم، شماره دوم، تابستان.
- رایجیان اصلی، مهرداد، سلیمی، احسان و نوریان علیرضا (۱۳۹۳). پیشگیری از جرایم رایانه‌ای از رهیافت‌های نظری تا رهیافت جهانی در پرتو رهنمود پیشگیری از جرم سازمان ملل متحد، فصلنامه مطالعات راهبردی جهانی شدن، سال پنجم، شماره ۱۳، پاییز .
- سلیمی، احسان (۱۳۹۱). خطر مضاعف جرائم رایانه‌ای، مجموعه مقالات اولین کنگره فضای مجازی و آسیب‌های اجتماعی نوپدید، تهران، انتشارات وزارت رفاه و تأمین اجتماعی.
- ضیایی، یاسر (۱۳۹۲). حمایت از حقوق بشر در فضای سایبر، نشریه پژوهشهای حقوقی، سال هشتم، شماره ۲۱.
- عاملی، سعیدرضا و حسنی، حسین (۱۳۹۱). دوفضایی شدن آسیب ها و ناهنجاری های فضای مجازی: مطالعه تطبیقی سیاست گذاری های بین المللی، فصلنامه تحقیقات فرهنگی، دوره پنجم، شماره ۱، بهار.
- کرمانی، روح الله (۱۳۹۰). درآمدی بر پدیدارشناسی فضای مجازی، فصلنامه مطالعات رسانه ای، سال ششم، شماره ۱۲.
- مایلی، محمدرضا و بهمنی، محمدسعید (۱۳۹۱). جنگ سرد نوین و رقابت بین قدرت‌های جهانی در فضای سایبری، پژوهشنامه روابط بین الملل، سال سوم، شماره ۱۴، پاییز .
- یزدانی زنور، هرمز (۱۳۸۸). حریم خصوصی در فضای سایبر، مجموعه مقالات حقوق فناوری اطلاعات و ارتباطات؛ گرامیداشت مرحوم دزیانی، گردآوری امیرحسین جلالی فراهانی، چاپ اول.

پایان نامه ها

- آریانی، امیر (۱۳۹۲).زمینه های جرم شناسی جرایم سایبری علیه کودکان، پایان‌نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد تهران مرکزی، دانشکده حقوق و علوم سیاسی.

- باقری حسین آبادی، علی (۱۳۹۳).سیاست جنایی قضائی ایران در قبال جرایم رایانه‌ای، پایان‌نامه کارشناسی ارشد، دانشگاه تربیت مدرس،دانشکده ادبیات و علوم انسانی.
- رشیدی، پدرام (۱۳۹۰).بررسی جرایم علیه تمامیت و صحت داده‌ها در فضای سایبر،پایان‌نامه کارشناسی ارشد،دانشگاه قم.
- عرب زاده، آزاده (۱۳۹۱).تاثیر پیشگیرانه قانون گذاریهای نظام تقنینی ایران در حوزه جرایم (IT)،پایان‌نامه کارشناسی ارشد دانشگاه پیام نور ، استان البرز – دانشکده الهیات و معارف اسلامی.
- کرمی، داود (۱۳۹۴).سیاست کیفری افتراقی در جرایم سایبر با تأکید بر حقوق کیفری ایران، پایان نامه دکترا دانشگاه قم،دانشکده حقوق و علوم سیاسی.
- فارسیان، محمد رضا (۱۳۹۴).بررسی فقهی و حقوقی وظایف و اختیارات شورای عالی فضای مجازی کشور، پایان‌نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد تهران مرکزی،دانشکده ادبیات و علوم انسانی.
- فرهادی آلاشتی، زهرا (۱۳۹۴).چالش های فراروی پیشگیری موقعیت مدار از جرایم سایبری،پایان‌نامه کارشناسی ارشد، دانشگاه فردوسی مشهد، دانشکده علوم اقتصادی.
- معصومی، اردشیر (۱۳۹۳). صلاحیت کیفری در جرائم سایبری بین‌المللی، پایان‌نامه کارشناسی ارشد، دانشگاه پیام نور، مرکز کرج.
- مقیمی، مهدی(۱۳۹۵).سیاست‌ها و تدابیر سازمان ملل متحد برای پیشگیری از جرم سایبری، پایان نامه دکتری دانشگاه شهیدبهشتی،دانشکده حقوق.
- هوشیارحسینی، سیدمهرداد (۱۳۹۱).نقش پلیس در پیشگیری از جرایم سایبری، پایان نامه کارشناسی ارشد، دانشگاه شیراز، دانشکده آموزشهای الکترونیکی.

منابع لاتین

- Barnett, Michael N., and Liv Coleman (2005). Designing Police: Interpol, and the Study of Change in International Organizations, International Studies Quarterly, 49.
- Duncan B. Hollis (2011). Why States Need an International Law for Information Operations, Lewis & Clark Law Review, No. 1

- March, James G., and Johan P. Olsen (2014). The Institutional Dynamics of International Political Orders, 5th edition, International Organizations Pub.
- K. Govinda; E. Sathiyamoorth. (2011). **Multilevel Cryptography Technique Using Graceful Codes**, Journal of Global Research in Computer Science, Vol. 2, No. 7, pp. 1-5.

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی