فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره اول | بهار ۱۴۰۲
وبگاه مجله: https://cyberlaw.maragheh.iau.ir

Situational Prevention Approaches of Iran's Criminal Policy Against Cyber SecurityViolations in the Light of International Documents

Eraj Negahdar
Ph.D Student in Criminal Law and Criminology, Maragheh Branch, Islamic Azad University, Maragheh, Iran
Babak Pourghahrmani
Associate Professor, Department of Criminal Law & Criminology, Maragheh Branch, Islamic Azad University, Maragheh, Iran
Jamal Beigi
Associate Professor, Department of Criminal Law & Criminology, Maragheh Branch, Islamic Azad University, Maragheh, Iran
pourghahramani@iau-maragheh.ac.ir

DOI: 10.30495/CYBERLAW.2023.701662

Keywords:
international cyber documents, state prevention, criminal policy, cyber security breach.

Abstract

Prevention of security breaches today depends on understanding the concepts and examples of cyber security breaches And Examining measures by governments to adopt preventive criminal policy is appropriate. This is a relatively new but important issue Why so; The most important component in expressing the desired governance of countries Ability to deal with cyber security breaches. And since, according to the evidence, the cyberspace is the target of complex security-violating actions by individuals and even governments, has involved those involved both in the domestic arena and in the international arena With the application of efficient and effective approaches and guidelines of active and comprehensive preventive criminal policy Seek to find a suitable solution for a cyber security breach From this point of view, this article follows descriptive-analytical method Reading the preventive approaches of Iran's cyber security violations in laws and documents Upstream and its review in international cyber documents .It seems that despite the fact that the governing systems and international decision makers In laws and agreements and conventions that are somewhat scattered Several cyber security approaches have been proposed and implemented in order to prevent cyber security violations; However, Iran's criminal policy despite efforts to strengthen the security foundations of cyber encounters and aligning with global measures and taking advantage of current knowledge and approving numerous regulations, It lacked the necessary differentiation bases And so far, it has not succeeded in adopting a centralized and efficient criminal policy for the prevention of cyber security violations.

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره اول | بهار ۱۴۰۲

رهیافت‌های پیشگیری وضعی سیاست جنایی ایران در قبال نقض امنیت سایبری در پرتو اسناد بین‌المللی

ایرج نگهدار

دانشجوی دکتری تخصصی حقوق جزا و جرم‌شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران

بابک پورقهرمانی*

دانشیار، گروه آموزشی حقوق جزا و جرم‌شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران

جمال بیگی

دانشیار، گروه آموزشی حقوق جزا و جرم‌شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران

pourghahramani@iau-maragheh.ac.ir

تاریخ دریافت: ۰۸ دی ۱۴۰۱ تاریخ پذیرش: ۰۲ اردیبهشت ۱۴۰۲

چکیده

پیشگیری از نقض امنیت در جهان امروز در گرو شناخت مفاهیم و مصادیق نقض امنیت سایبری و تدابیر دولت‌ها جهت اتخاذ سیاست جنایی پیشگیرانه مناسب است. این امر موضوعی نسبتاً نوین ولی حائز اهمیت است چراکه؛ مهم‌ترین مؤلفه در بیان حاکمیت مطلوب کشورهاست و ازآنجایی‌که حسب شواهد، فضای سایبری آماج اقدامات پیچیده ناقض امنیت است، دولت‌ها را چه در عرصه داخلی و چه بین‌المللی بر آن داشته تا با اتخاذ و تدوین سیاست جنایی پیشگیرانه فعال و همه‌جانبه در پی یافتن راهکار مناسب مقابله با نقض امنیت سایبری باشند. این مقاله با روش توصیفی-تحلیلی در پی خوانش رهیافت‌های پیشگیرانه وضعی در قبال نقض امنیت سایبری ایران در قوانین و اسناد بالادستی و بررسی آن در اسناد بین‌المللی سایبری است. به نظر می‌رسد علی‌رغم اینکه نظام حقوقی رویکردهای سایبری امنیتی متعددی در قبال پیشگیری وضعی از نقض امنیت سایبری اتخاذ نموده است؛ لکن سیاست جنایی ایران علی‌رغم تلاش در تقویت بنیان‌های امنیتی مقابلات سایبری، فاقد مبانی افتراقی و کارسازی مناسب بوده و تابه‌حال موفق به اتخاذ سیاست جنایی متمرکز و کارآمدی در قبال پیشگیری از نقض امنیت سایبری نگردیده است.

کلید واژگان: اسناد بین‌المللی سایبری، پیشگیری وضعی، سیاست جنایی، نقض امنیت سایبری.

مقدمه

سیاست جنایی در رویکرد فرانوگرایانه در حقیقت تلفیقی از سیاست‌گذاری عمومی و سیاست جنایی است که بر اساس داده‌های نوین دانش بشری در پی پیشگیری وقایع برمی‌آید تا از طریق اصلاح روش‌ها و حذف عوامل مؤثر از وقوع پدیده‌های که ظرفیت تبدیل به پدیده جنایی را دارد، جلوگیری نماید. در سیاست جنایی، برای پیشگیری از جرم مبارزه با آن از وسایل مختلف دولتی و غیردولتی کمک گرفته می‌شود (وطنی و اسدی، ۱۳۹۵: ۹۹). بااین‌حال گفتمان سیاست جنایی در پی فراخوان نگاهی همه‌جانبه به مبارزه با پدیده‌های آسیب‌زای اجتماعی است و به‌عنوان الگوی نوین در تحلیل پدیده‌های جنایی جایگاه بسیار مهمی را در عرصه حقوق کیفری کسب نموده است (نجفی ابرندآبادی، ۱۳۹۶: ۵۴۴). امنیت فضای سایبر به‌عنوان کی از عرصه‌های نوظهور در امنیت بین‌الملل و به خاطر ویژگی‌های منحصربه‌فرد این حوزه، به نگرانی مشترک و درعین‌حال فزاینده کارشناسان فنی، حقوقی، سیاسی، امنیتی و بازیگران ملی و فراملی بدل شده و جایگاه مهمی در گفتمان امنیت ملی و بین‌المللی یافته است و موجب ظهور واژگان جدیدی امنیت سایبری، حاکمیت سایبری، جرائم سایبری، جاسوسی سایبری، حملات سایبری، تروریسم سایبری و... در گفتمان امنیتی کشورها در سطوح ملی و بین‌المللی شده است (سلطانی، ۱۳۹۶: ۱۵). بحث پیشگیری از نقض امنیت ملی در فضای سایبر ازآن‌رو اهمیت مضاعف دارد که تهدیدها علیه امنیت ملی در این فضا با امکانات پیچیده چون فناوری اطلاعات یا فناوری هسته‌ای به نسبت تهدیدات گذشته متنوع‌تر شده و دولت‌ها را در مسیر پرمخاطره‌ای قرار داده است (بهره‌مند و داودی، ۱۳۹۷: ۲۸).

با بیان مختصری از سیاست جنایی پیشگیرانه وضعی، مشخص است که در آن کلیت یک ساختار اعم از تقنین و نظارت و اعمال و اجرا مدنظر قرار می‌گیرد. حال ازاین‌رو با روش مطالعه تحلیلی-اسنادی[1] برآنیم تا با مراجعه به نوشتگان حوزه حقوق امنیت سایبری و شناسایی و تحلیل اسناد موجود، پس‌ازآن، نمودهای پیشگیری وضعی، آثار و تبعات این رهیافت‌ها بر دو نظام حقوقی ایران و نظام بین‌الملل را در اتخاذ رویکردهای پیشگیرانه مورد کنکاش قرار دهیم. از دیدگاه حقوقی و از منظر حقوق بین‌الملل نیز برای مقابله با معضل جهانی نقض امنیت سایبری و تعیین تکالیف اعضای جامعه بین‌المللی در برخورد با این پدیده چالش‌های متعددی وجود دارد. نه کنوانسیون خاصی و نه عرف بین‌المللی واحدی که دولت‌های قربانی حملات سایبری بدانند در برابر آن‌ها به چه اقداماتی متوسل شوند وجود ندارد و آنچه مسلم است، حملات سایبری نیازمند قانون‌مند شدن و ایجاد رویه واحد در عرصه بین‌المللی است (جوینرو لوترینت، ۸۶۴:۲۰۰۱ به نقل از (کتانجی و ذاکری، ۱۳۹۸: ۶۱۷). لازم به ذکر است که نقض امنیت سایبری در اوج اهمیت مورد اغفال دولت‌ها بوده و آن‌چنان‌که به جرم سایبری پرداخته‌شده به امنیت سایبری و بالطبع آن‌چنان‌که به پیشگیری از جرم توجه گردیده به پیشگیری از نقض امنیت سایبری امعان نظر نشده است. با این اوصاف سؤال اصلی تحقیق حول این محور است که در اسناد و قوانین ایران چه اقدامات و تدابیر پیشگیرانه‌ای مبتنی بر رویکردهای وضعی در قبال نقض امنیت سایبری وجود دارد و این تدابیر در پرتو اسناد بین‌المللی چگونه ارزیابی می‌گردند؟ به نظر می‌رسد مدیریت کلان پیشگیری از تهدیدات امنیتی سایبری در سیاست جنایی ایران فاقد رویکرد افتراقی پیشگیرانه وضعی سایبری مناسبی است. لذا ضمن تطابق رهیافت‌های مدنظر در سیاست جنایی ایران و جهان نگارنده بر این عقیده است که پیشگیری وضعی در بطن اسناد بالادستی و قوانین موردتوجه نسبی قانون‌گذار ایرانی قرارگرفته، لکن بعد امنیت فضای سایبری نیازمند شناختی بسیار غامض‌تر و درنتیجه اقدامات پیشگیرانه بسیار فنی‌تر است.

[1] روش اسنادی را تحلیل آن دسته از اسنادی می‌دانند که شامل اطلاعات دربارهٔ پدیده‌هایی است که قصد مطالعهٔ آن‌ها را داریم. روش اسنادی مستلزم جستجویی توصیفی و تفسیری است و علاقه پژوهش‌گر این است که از فهم مقاصد و انگیزه‌های اسناد و متون یا تحلیل‌های تأویلی یک متن خارج شود و آن را به‌عنوان زبان مکتوب و گفتمان نوشتاری نویسنده، پذیرفته و مورد استناد قرار دهد (صادقی و عرفان منش، ۱۳۹۴: ۶۵)

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره اول | بهار ۱۴۰۲

۱. مفهوم شناسی

مفاهیم مندرج در این نگارش خوانشی از عناوین عالم حقوق کیفری و نظام حقوقی سایبری با ابتناء بر رویکردهای امنیتی در آن است. این موضوع هرچند دامنه پرتکراری از عناوین حقوقی و فنی را در برمی‌گیرد، اما ماحصل آفرینش ترکیبی نوین و ازجمله مباحث بسیار جدی جهان جدید مجازی است. فلذا با بازخوانی این مفاهیم نگارنده در پی تقریب عنوان در ذهن خواننده ناآشنا با حقوق امنیت سایبری و تقابل با نقض آن در خواستگاه سیاست جنایی است.

۱،۱. نقض امنیت سایبری

شورای عالی فضای مجازی در مصوبه «توسعه فضای مجازی سالم، مفید و امن» این فضا را این‌گونه تعریف می‌کند: «فضایی است متشکل از شبکه‌های ارتباطی که در آن محتوا و خدمات مفید در چارچوب مبانی و ارزش‌های اسلامی و قوانین و مقررات کشور ارائه می‌شود و کاربران می‌توانند بر اساس ویژگی‌های جمعیتی از محتوا و خدمات مورد نیاز بهره‌مند شوند و حتی‌الامکان در برابر محتوا و رفتارهای آسیب‌زا محفوظ بماند» و هدف از این امر را تولید و توزیع محتوا و خدمات سالم مفید و امن موردنیاز و ممانعت از نشر محتوا و خدمات مضر و ناسالم و ناایمن ذکر می‌نماید[۲]. کمیته دائمی پدافند غیرعامل در «سند راهبردی پدافند سایبری کشور» در ذیل ماده یک این سند، فضای سایبری را: «شبکه‌های وابسته به یکدیگر از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی سامانه‌های رایانه‌ای، پردازنده‌های تعبیه‌شده، کنترل‌کننده‌های صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط و انسان به‌منظور تولید، پردازش، ذخیره‌سازی، مبادله، بازیابی و بهره‌برداری از اطلاعات که ممکن است در ارتباط مستقیم و مداوم با سامانه‌های فناوری اطلاعات و شبکه‌های ارتباطی اعم از شبکه اینترنت باشد و یا تنها قابلیت اتصال به محیط پیرامونی، در آن تعبیه‌شده باشد»[۳] تعریف نموده است؛ و نیز از نگاه دیوید بل[۴]، فضای سایبر[۵] یک شبکه گسترده جهانی است که شبکه‌های مختلف رایانه‌ای در اندازه‌های متعدد و حتی رایانه‌های شخصی را با استفاده از سخت‌افزارها و نرم‌افزارهای گوناگون و با قراردادهای ارتباطی به یکدیگر وصل می‌کند (شریفی هولاسو،۵۲:۱۳۸۷) به نقل از (پورقهرمان و فهیمی، ۱۳۹۸: ۴۱۰). در همین باره لازم است به تعریف آکادمی حکمرانی الکترونیک[۶] از شاخص کلی امنیت سایبری نگاهی بیندازیم. این آکادمی شاخص مذکور را یک شاخص جهانی اعلام که آمادگی کشورها را برای جلوگیری از تهدیدهای سایبری و مدیریت حوادث سایبری اندازه‌گیری می‌کند. این آکادمی شاخص‌های چون سیاست و خط‌مشی امنیت سایبری، تحلیل و اطلاع‌رسانی تهدیدات سایبری، آموزش و تربیت امنیت سایبری، مشارکت در امنیت سایبری جهانی، حمایت از خدمات دیجیتال و حمایت از خدمات حیاتی را به‌عنوان ابعاد اصلی ارزیابی آمادگی امنیت سایبری لحاظ نموده است. حرکت کشورها به سمت نوگرایی باعث ایجاد انقلاب صنعتی چهارم[۷] است، این نشان می‌دهد که امنیت سایبری به دلیل رشد سریع فناوری دیجیتال در کشورهای مدرن در سطح جهان به‌عنوان موضوع تحقیقاتی انتخاب می‌شود (کتانچی و پورقهرمانی،۱۴۰۰: ۱۴۰). امنیت[۸] سایبری یکی از دسته‌بندی‌های امنیت بر پایه

---

[۲] مصوبه دوم جلسه ۲۲ مورخ ۱۳۹۳/۱۲/۱۰ شورای عالی فضای مجازی

[۳] کمیته دائمی پدافند غیرعامل کشور، سند راهبردی پدافند سایبری کشور، ۱۳۹۴/۲/۲۹

[4] -David Belle

[۵] مع‌الوصف فضای سایبری، فضای غیرمادی و ناملموس است که متشکل از صدها هزار رایانه، سرویس، روتر، سویچ و کابل فیبر نوری است که به هم متصل گشته و موجب عملکرد زیرساخت‌های فناوری اطلاعاتی، اینترنتی، شبکه‌های مخابراتی، سیستم‌های رایانه‌ای، کنترل‌کننده‌ها و پردازشگرها است (کمیته دائمی پدافند غیرعامل کشور، سند راهبردی پدافند سایبری کشور، مصوب ۱۳۹۴/۲/۲۹).

[6] EGovernance Academy (EGA)

[7] Industrial Revolution (IR4.0)

[۸] در زمینه تأثیر فناوری اطلاعات و ارتباطات بر مفهوم امنیت دو دسته از نظریه‌پردازان وجود دارند. گروهی بر این عقیده‌اند که این ابزار به بهترین وجه می‌تواند مفهوم امنیت را کمرنگ و مفهوم صلح را جایگزین آن کند. گروه دوم که همان نظریه‌پردازان رئالیسم کلاسیک هستند؛ معتقدند که هرچند فناوری اطلاعات و ارتباطات گسترش‌یافته است اما مفهوم کلاسیک امنیت به معنای امنیت دولت در قالب نظامی و جریان اطلاعات رسمی همچنان جایگاه خود را حفظ کرده است (Eriksson & Giacomello, 2006: 222-223)

فضای سایبری است که در چهره درون سایبری بر دو دسته امنیت اطلاعات و امنیت سامانه تقسیم و ناظر بر سه دسته امنیت کاربران، امنیت زیرساخت‌های نهادهای عمومی و امنیت ملی است (محمود زاده و اسماعیلی، ۱۳۹۷: ۲۱۳). فلذا امنیت در عصر جهانی‌شدن را باید در تعامل و تقابل با موضوعاتی چون «رژیم‌های بین‌المللی»، «هنجارها»، «توسعه»، «وابستگی متقابل»، «بازیگران بین‌المللی»، «سازمان های غیردولتی» تفسیر کرد (علایی، ۱۳۹۱: ۱۲۱). به تعبیری امنیت سایبری را می‌توان به‌عنوان راحل‌های پیشنهادی (شامل قوانین، دستورالعمل‌ها، حراست‌های فناوری) برای تهدیدات ناشی از هک و به خطر انداختن سیستم‌های رایانه‌ای تعریف کرد (Brunot, 2018: 3).

۲,۱. پیشگیری از نقض امنیت سایبری

صیانت امنیتی فضای سایبر موضوع بسیار مهمی است و بسیار جلوتر از امنیت فضای سایبراست، زیرا در امنیت فضای سایبر به دنبال یک سری از الزامات برای ایمنی و امنیت این فضا هستیم، درحالی‌که صیانت امنیتی به دنبال موضوعاتی شامل ارزش‌ها، حریم خصوصی، سرمایه‌های مادی و معنوی، اسرار و اطلاعات، تخلفات و جرائم، خدمات و سرویس‌ها، قوانین و مقررات، پیاده‌سازی مراکز عملیات امنیت است (حسینی، ۱۳۹۵: ۲۸۶). در سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور اشاره شده است که: «فضای تبادل اطلاعات در معرض چالش‌ها، آسیب‌ها و تهدیدهای گوناگونی نظیر ارتکاب جرائم سازمان‌یافته، تخریب بانک‌های اطلاعاتی، حملات مختل‌کننده خدمات، جاسوسی، خرابکاری، نقض حریم خصوصی و نقض حقوق مالکیت معنوی قرار دارد». با این اوصاف نقض امنیت سایبری را می‌توان: «تجاوز یا هنجارشکنی یا تهدید نسبت به یکی از پنج موضوع داده‌ها و اطلاعات، شبکه‌ها و سیستم‌های رایانه‌ای و مخابراتی، کاربران و مشترکان اینترنتی و نهایتاً موضوعات بیرون از دنیای سایبر که مرتکب به‌واسطه محیط سایبر درصدد تجاوز به آن برمی‌آید» (عالی پور، ۱۳۹۲: ۷) قلمداد کرد. با این مقدمه اشاره به این نکته ضروری است که این مقاله اصولاً درپی یافتن جرائم علیه امنیت مندرج در قانون مجازات اسلامی چون تبلیغ علیه نظام و... در فضای سایبری نیست. امنیت سایبری بازخوردی گسترده در تمامیت نظام سایبری و مختص به ماهیت این فضاست که نقض آن سبب بروز تهدیدات گسترده در زیرساخت‌ها و استقلال سایبری و تمامیت ساختار امن مستقل آن و فراتر از مفاهیمی چون جنگ سایبری و تروریسم سایبری و جاسوسی سایبری است و لازم به ذکر است که سیاست جنایی بین‌المللی رفتارهای منجر به نقض امنیت سایبری را ناقض حقوق بین‌الملل عمومی می‌داند و ناتو طی توافقی در زمینه خط‌مشی مشترک سایبری اعلام نمود که هرگاه حمله سایبری علیه یکی از دولت‌های عضو ناتو به وقوع بپیوندد مطابق ماده ۴ معاهده سازمان پیمان آتلانتیک با آن برخورد خواهد شد.

۲. سند شناسی سیاست جنایی سایبری

برای یافتن بافت[9] امنیت سایبری ملی و بین‌المللی شناخت مفاهیم مرتبط و بررسی رویکردهای قانونی و انسجام بخش نظام سیاست جنایی در قبال نقض آن نیازمند احصاء اسناد داخلی و جهانی در این عرصه هستیم که در دو بخش زیر مراجع دخیل و اسناد مهم را بازخوانی خواهیم نمود تا شاکله تدابیر پیشگیرانه سایبری وضعی در این اسناد در قبال نقض امنیت را شناسایی نماییم.

۱,۲. اسناد سایبری داخلی

رهیافت‌های نظام حکمرانی جمهوری اسلامی ایران در حیطه مقابله با نقض امنیت سایبری در سند چشم‌انداز ایران ۱۴۰۴ و سیاست کلی شبکه اطلاع‌رسانی و سیاست کلی نظام برای رشد و توسعه فناوری در کشور[10] و نیز نظام جامع توسعه فناوری اطلاعات کشور[11] و

[9] Context

[10] طی ۴ ماده و ۲۵ بند در ۱۳۸۶ به تصویب هیئت‌وزیران رسید.

[11] در جلسه ۸۶/۸/۱۹ کمیسیون راهبردی شورای عالی فناوری اطلاعات کشور مدنظر قرارگرفته است.

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره اول | بهار ۱۴۰۲

سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور[۱۲] و قانون برنامه پنجم و ششم توسعه جمهوری اسلامی ایران و همچنین شرح وظایف پلیس فضای تولید و تبادل اطلاعات و قانون جرائم رایانه‌ای و نظام جامع توسعه فناوری اطلاعات کشور و سند تبیین الزامات شبکه ملی اطلاعات و مصوبات سازمان تنظیم مقررات و ارتباطات رادیویی و سند سیاست‌ها و اقدامات ساماندهی پیام‌رسان‌های اجتماعی[۱۳] و سند راهبردی پدافند سایبری کشور[۱۴] و سند نظام هویت معتبر در فضای مجازی کشور مصوب شورای عالی فضای مجاز و طرح امن‌سازی زیرساخت‌های حیاتی در قبال حملات سایبری سال ۱۳۹۷ مرکز مدیریت راهبردی افتا[۱۵] نهاد ریاست جمهوری در این اسناد به چشم می‌خورند که هریک به‌نوعی موضوعاتی را بیان اما تاکنون سیاست جنایی جامعی در قبال نقض امنیت سایبری تدوین‌نشده است. شیوه حکمرانی کنونی فضای مجازی از رویکردی غیر مشارکتی و از بالا به پایین پیروی می‌کند (خوشنویس، ۱۳۹۸: ۳۷). واقعیت موجود نقض گسترده امنیت سایبری در ابعاد گوناگون آن است و جامعه جهانی با این معضل دست به گریبان است حتی حکمران این عرصه. بنابراین توسعه راهبردها و رهنامه‌هایی به منظور مواجه فعال و پیش دستانه با این رخدادها با هدف آماده سازی زیرساخت ها و ایجاد هماهنگی به منظعور حفظ امنیت ملی و در صورت نیاز، واکنش در برابر این گونه تهدیدات انجاه شده است (Katrina , Lewis,2011)

۲،۲. اسناد سایبری خارجی

صحبت از نقض امنیت سایبری مستلزم صیانت از داده‌ها و اطلاعات سایبری است. ازاین‌رو، کشورهای پیشرو در صیانت از داده‌های شخصی را در دستور کار خود قرار داده و ضمانت اجراهای حقوقی و کیفری متعددی را وضع کرده‌اند. سرآمد و پیشتاز قوانین حمایت از داده را می‌توان در اتحادیه اروپا مشاهده کرد. نخستین دستورالعمل شورای اروپا درباره حمایت از داده در سال ۱۹۹۵، با عنوان «حمایت از اشخاص در جریان پردازش داده‌های شخصی و جریان آزاد اطلاعات» به تصویب رسید[۱۶]. در بررسی اسناد و مقاوله نامه‌های بین‌المللی به نظر می‌رسد سیاست جنایی بین‌المللی در قبال نقض امنیت سایبری با سرگردانی مواجه است. به‌عنوان‌مثال سازمان‌ها و مجامع جهانی که ناظر بر «هنجارهای رفتار مسئولانه دولت‌ها در فضای سایبری» می‌باشند شامل کنوانسیون بوداپست (۲۰۰۴)، تلاش‌های علمی گروه خبرگان حکمرانی سازمان ملل متحد[۱۷]، سند راهبرد بین‌المللی ایالات‌متحده برای فضای سایبری (۲۰۱۱)، یافته‌های موسسه مطالعات امنیتی شرق و غرب[۱۸] (۲۰۱۱)، مطالعات تطبیقی کنوانسیون‌های لاهه و ژنو در حوزه موردبحث، دستورالعمل تدوین‌شده در سازمان پیمان آتلانتیک شمالی (ناتو) تحت عنوان «تالین ۲۰۱۳»، طرح بلوک چین و روسیه با عنوان «کدهای رفتاری بین‌المللی برای امنیت اطلاعات» (۲۰۱۵)، استراتژی وزارت امور خارجه امریکا در حوزه سیاست‌های بین‌المللی (۲۰۱۶)، اعلامیه گروه ۷ در خصوص «رفتار مسئولانه دولت‌ها در فضای سایبری» در ایتالیا (۲۰۱۷)، فرمان اجرایی ترامپ در حوزه تقویت امنیت سایبری شبکه‌ها و زیرساخت‌های فدرال (۲۰۱۷) برخی از اسناد قابل‌توجه می‌باشند[۱۹]. در اسناد و اقدامات بین‌المللی در حوزه امنیت سایبری، سندی که در اجلاس سران ناتو در

---

[۱۲] معاونت فناوری اطلاعات دفتر امور زیربنایی فناوری اطلاعات در سال ۱۳۸۶ به استناد بند «ج» ماده ۴۴ قانون برنامه چهارم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی ایران، سند راهبردی امنیت فضای تبادل اطلاعات را به‌منظور تضمین هم‌گرایی و نظام‌بندی برنامه‌های کشور در زمینه امنیت فضای تبادل اطلاعات را به‌عنوان سند بالادستی برای کلیه برنامه‌های بخشی و فرابخشی تدوین نمود.

[۱۳] اهمیت پیام‌رسان‌های اجتماعی و توان در نقض امنیت سبب شد شورای عالی فضای مجازی سند «سیاست‌ها و اقدامات ساماندهی پیام‌رسان‌های اجتماعی» را در تاریخ ۱۳۹۶/۳/۱۳ تصویب نماید؛ که هدف از آن، تعیین سیاست‌ها و اقدامات لازم برای ساماندهی فعالیت پیام‌رسان‌های اجتماعی، باهدف فراگیری پیام‌رسان‌های اجتماعی داخلی و ساماندهی پیام‌رسان‌های خارجی عنوان‌شده است.

[۱۴] کمیته دائمی شورای عالی پدافند غیرعامل کشور در جلسه مورخ ۱۳۹۴/۲/۲۹ به استناد ماده ۸ اساسنامه سازمان پدافند غیرعامل کشور مصوب مقام معظم رهبری «**سند راهبردی پدافند سایبری کشور**» را تصویب نمود.

[۱۵] لالالالا لا لالالا لالا لالا لالاعات

[16] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data

[17] UNGGE2010

[18] East West Institute (EWI)

[۱۹] به نقل از سایت مرکز ملی فضای مجازی،۱۳۹۹

۲۰ نوامبر ۲۰۱۰ در لیسبون پرتغال به تصویب رسید ازجمله موارد حائز اهمیت است و فعالیت‌های مؤثری را در سه زمینه دفاع دسته جمعی، مدیریت بحران و همکاری امنیتی متمرکز ساخته است (احمدیان، بلوکی صارمی‌فر،۱۳۹۱:۱). اتحادیه بین‌المللی مخابرات[۲۰] ازجمله نهادهای بین‌المللی دیگر در زمینه امنیت سایبری است. اجلاس جهانی سران درباره جامعه اطلاعاتی[۲۱] در سال ۲۰۱۹ که در آن فرم چند ذینفعی اجلاس سالانه جامعه اطلاعاتی، پیاده‌سازی خطوط اقدامات را برای اهداف توسعه پایدار تسهیل و موضوعات مهمی مانند حذف شکاف دیجیتالی، امنیت سایبری و اخلاق و همچنین فناوری‌های نوین نظیر هوش مصنوعی، اینترنت اشیاء، بلاکچین، در اجلاس سالانه جامعه اطلاعاتی ۲۰۱۹ مطرح شد[۲۲] (وامالا، ۱۳۹۶: ۱۲).

۳. سیاست جنایی پیشگیرانه در قبال نقض امنیت سایبری

در کشور ما هرچند تا حدودی ماهیت پیشگیری از نقض امنیت سایبری و موانع و چالش‌های موجود روشن است، اما اجرای سیاست‌های پیشگیرانه با محدودیت خاص خود همراه است چراکه به دلیل شفاف نبودن مقررات موجود، نحوه به‌کارگیری این ابزارهای پیشگیرانه نیز مشخص نیست (جزایری و نعمت‌الهی و امیربان فارسانی، ، ۱۳۹۸: ۱۳). با این اوصاف فقدان راهبرد مشخص در زمینه توسعه الکترونیک و امنیت فضای مجازی، فقدان متولی مشخص در حفاظت از داده‌های موجود در سامانه‌های نظامی، امنیتی کشور، فقدان سیاست مشخص ملی در آموزش، اطلاع‌رسانی و افزایش جرائم پنهانی در فضای مجازی و حرفه‌ای شدن مجرمین با افزایش استفاده از شبکه‌های مجازی در دستگاه‌ها و نهادهای دولتی و خصوصی و فقدان سیاست‌های نظارتی و امنیتی مشخص در کشور از چالش‌های پیشرو است (هاتف، ۱۳۸۸: ۱۴) به نقل از: (ظفری و فروغی‌نیا و باوند، ۱۳۹۹: ۱۹).

۳-۱ پیشگیری وضعی

با توجه به این چالش‌ها انتظار از اقدامات پیشگیرانه این است که فرصت نقض امنیت را از طریق دشوار ساختن ارتکاب و افزایش خطرپذیری و کاهش آماج و قربانیان کاهش دهند. لذا گرچه سیاست جنایی پیشگیرانه مبتنی بر رویکردهای مختلفی است اما در این مقاله از میان تدابیر گوناگون، الگوی پیشگیری پیشگیری وضعی به سبب بعد فنی و کاربردی و رهیافت‌های مندرج در ارتباط با پیشگیری از نقض امنیت سایبری بررسی می‌گردد. به‌طور خلاصه پیشگیری وضعی عبارت است از: «ایجاد تغییر نظام‌مند و دائمی در محیط، به‌منظور کاهش فرصت‌های مجرمانه و افزایش خطر ارتکاب جرم» (بهره‌مند، کوره‌پز و سلیمی، ۱۵۴:۱۳۹۱). بنابراین پیشگیری وضعی بر کاهش فرصت‌ها و موقعیت‌های ناقض امنیت تکیه دارد. درواقع به‌جای پرداختن به انگیزه و نیات درونی افراد که تغییر آن‌ها دشوار است سعی دارد راه‌های دست‌یابی مرتکب به موضوع جرم یا بزه دیده و افزایش زحمت و خطر برای مرتکب بپردازد تا از این رهگذر راهکاری عملی برای پیشگیری از وقوع جرم ارائه نماید. با این توصیف در ادامه ضمن برشماردن مصادیق این نوع پیشگیری، رهیافت‌های مذکور در سیاست جنایی ایران را بررسی خواهیم کرد.

---

[۲۰] این اتحادیه از زمان شکل‌گیری در سال ۱۸۶۵، نقش مهمی در زمینه ارتباطات راه دور، امنیت اطلاعات و تعیین استانداردهای جهانی با ظرفیت‌های مختلف ایفا کرده است. فعالیت‌های زیر ازجمله اقدامات این اتحادیه قلمداد می‌شود: اجلاس جهانی در مورد جامعه اطلاعاتی و دستور کار امنیت سایبری جهانی (GCA) و اقدام سطر (C5) در اجلاس جهانی جامعه اطلاعاتی و ابتکار عمل حفاظت از «کودکان برخط». این سند مسائلی را موردتوجه قرار می‌دهد که کشورها در بازنگری یا فرآیند پربار کردن و غنی‌سازی راهبردهای امنیت ملی سایبری، باید به آن بپردازد (وامالا، ۱۳۹۶: ۱۶).

[21] Information Society

[۲۲] همچنین درنتیجه نشست‌های عمومی سازمان ملل نیز این نهاد در پنج قطعنامه مهم، به بازتاب نظر خود درباره امنیت سایبری پرداخته است که شامل A/RES/55/63: مبارزه با استفاده مجرمانه از فناوری ارتباطات و اطلاعات و A/RES/56/121: مبارزه با استفاده مجرمانه از فناوری ارتباطات و اطلاعات و A/RES/57/239: فرهنگ امنیت سایبری و A/RES/57/239: زیرساخت‌های حیاتی و A/RES/57/239: فرهنگ جهانی امنیت سایبری می‌باشند.

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره اول | بهار ۱۴۰۲

۲،۳. مصادیق سیاست جنایی پیشگیرانه وضعی در قبال نقض امنیت سایبری

در قوانین و مقررات مربوط به فضای سایبر قانون‌گذار به استفاده از تدابیر فنی جهت تحقق امنیت فضای سایبر پرداخته که در ادامه به آن‌ها اشاره می‌شود. نخست، مصوبات شورای عالی فضای مجازی است: این شورا موظف گردید تا به‌طور کامل و روزآمد بر فضای درونی و بیرونی اینترنت اشراف داشته و امنیت این فضا را تأمین سازد. در مصوبه این شورا با موضوع توسعه فضای مجازی سالم، مفید و امن به شماره ابلاغیه ۱۰۰۱۵۱/۹۴ش مصوب ۱۴۰۱/۱/۳۰ به تعریف فضای مجازی سالم، مفید و ایمن پرداخته شده است. در مصوبه دیگر، این شورا با موضوع سیاست‌های ساماندهی خدمات پیامکی ارزش‌افزوده و پیامک انبوه در شبکه‌های ارتباطی به شماره ۱۰۳۶۸۱/۹۳ش مورخ ۱۳۹۳/۱۱/۱ که در بند ۴ آن آمده است: «به‌منظور حفظ و صیانت از اطلاعات خصوصی مخاطبان پیام و بر اساس قوانین به‌ویژه قانون جرائم رایانه‌ای، ارائه‌دهندگان خدمات ارتباطی و ارائه‌دهندگان خدمات محتوایی، حق واگذاری، فروش و یا در اختیار قرار دادن این اطلاعات به دیگران را ندارند». همچنین در طرح‌های کلان مرکز ملی فضای مجازی کشور جهت تدوین لایحه بودجه و تصویب‌نامه این شورا در خصوص شرح وظایف، اختیارات و اعضای کمیسیون عالی فضای مجازی، به ارتقای امنیت سایبری پرداخته‌شده است. در مصوبه دیگر، این شورا در خصوص تعریف و الزامات حاکم بر تحقق شبکه ملی اطلاعات و بودجه سال ۱۳۹۳ نیز در بند چهارم مقرره دوم به ایجاد شبکه‌ای با قابلیت عرضه انواع خدمات امن اعم از رمزنگاری و امضای دیجیتال پرداخته و در سیاست‌های حاکم بر برنامه‌های رایانه‌ای، در بند۱۰ به حفظ حریم خصوصی و حمایت از حقوق مصرف‌کننده اشاره‌شده، اما تدابیر واسطه‌ای پیش‌بینی‌شده نیز تنها ناظر به حفظ حریم خصوصی است و اطلاعات مالی اشخاص حقوقی تحت شمول این مقرره قرار نمی‌گیرند. بابیان این مقدمه در ذیل به بررسی رویکردهای وضعی در قبال نقض امنیت سایبری اقدام خواهیم نمود.

۱،۲،۳. ایجاد سامانه‌ها و زیرساخت‌های الکترونیکی

در دنیای جدید، مهم‌ترین عامل توانایی و قدرت، حفاظت از اطلاعات در مقابل تهدیدات دشمنان، تبادل و اشتراک‌گذاری امن اطلاعات درجهت افزایش توانمندی است .جنگ اطلاعاتی، تروریسم سایبری و جنگ نفوذگرها ازجمله این تهدیدات است و بومی نبودن این فنّاوری و عمل نمودن به دستورات صاحبان فنّاوری منجر به افزایش تأثیرگذاری تهدیدات زیرساخت و شریان‌های اطلاعاتی شده است (کیان‌خواه و علوی وفا، ۱۳۹۰: ۷). سند راهبردی کشور استرالیا نیز وزارت دفاع را مسئول امنیت زیرساخت‌های حیاتی فناوری اطلاعات و ارتباطات و دفاع و پاسخگویی هماهنگ به تهاجمات سایبر را از جمله موضوعات مهم تلقی نموده است (Commonwealth of Australia,2009)

بنا به تعریف یک زیرساخت، مجموعه ساختاریافته‌ای از شبکه‌ها و سیستم‌های وابسته به هم است که در بسیاری از سطوح مختلف با یکدیگر پیوند دارند (نامدار، ۱۳۹۸: ۳۱)[۲۳]. وزارت امنیت داخلی امریکا[۲۴] در ۱۴ فوریه ۲۰۰۳ سندی را به نام «استراتژی ملی برای فضای سایبر[۲۵]» منتشر نمود. در این سند زیرساخت‌های حساس ملی بدین‌گونه تعریف گردیده است: «اموال و دارایی‌های فیزیکی (مادی) و سایبری تأسیسات خصوصی و عمومی در زمینه‌های کشاورزی، غذا، آب، سلامت عمومی، سرویس‌های اورژانس، حمل‌ونقل، پولی و بانکی، مواد شیمیایی و سمی، امور پستی و کشتیرانی». در سند مصوبه جلسه ۳۵ و مورخ ۱۴۰۰/۹/۲۰ شورای عالی فضای مجازی با نام «تبیین الزامات شبکه ملی اطلاعات» شبکه ملی اطلاعات به‌عنوان زیرساخت ارتباطی فضای مجازی کشور یکی از مهم‌ترین پروژه‌های ملی در عرصه فضای قلمداد و در مصوبه اول جلسه ۱۵ این شورا در فراز بند ۱ ماده ۴ این مصوبه آمده است که: «شبکه ملی اطلاعات

[23] UN General Assembly Resolution, A/RES/58/199:Creation of a global culture of cybersecurity and the protection of critical information infrastructures (23 December 2003)
[24] Department of Homeland security
[25] The national strategy to secure cyberspace

زیرساخت همه شبکه‌های کشور است این شبکه در چارچوب قوانین جمهوری اسلامی ایران به نحوه مطلوب و مطمئن، تأمین‌کننده کلیه نیازهای ارتباطی برای ذینفعانی که حداقل یکی از آن‌ها در داخل کشور قرار دارند، است». در بخشی دیگر از سند طرح امن‌سازی زیرساخت‌های حیاتی در قبال حملات سایبری به زیرساخت محرمانگی و استنادپذیری پرداخته و اشاره‌شده که زیرساخت محرمانگی و استنادپذیری نیازمند تدوین سیاست‌ها، ضوابط، رویه‌ها در بعد مدیریتی و بهره‌گیری از ابزارهای امنیت اطلاعات و ارتباطات در بعد فنی بوده که محرمانگی اطلاعات را برای سازمان تضمین می‌نماید. لزوم استقرار زیرساخت محرمانگی و استنادپذیری در سازمان، جلوگیری از افشای داده‌ها و اطلاعاتی است که باید محافظت شوند و در اختیار افراد غیرمجاز قرار نگیرند. سیاست‌های پیشنهادی در این راستا قابل تأمل و دارای بار حقوقی هستند، ازجمله: تبعیت از سیاست‌های بالادستی در حوزه زیرساخت محرمانگی و استناد پذیری که به مرکز افتا ابلاغ می‌گردد.

در سند تبیین الزامات شبکه ملی اطلاعات مصوب شورای عالی فضای مجازی شبکه ملی اطلاعات به‌عنوان زیرساخت توسعه خدمات الکترونیکی و هوشمندسازی و همچنین زیرساخت ارتباطی فضای مجازی کشور، ازجمله مهم‌ترین طرح‌های ملی در عرصه فناوری اطلاعات و ارتباطات به شمار می‌آید که تحقق آن بنابر ضرورت‌های ملی همچون «ارائه خدمات زیرساختی پیشرفته» و «بهره‌مندی از مزایای زیست‌بوم ملی فضای مجازی متناسب با فرهنگ اسلامی- ایرانی» در کنار «حفاظت از حریم خصوصی کاربران ایرانی» و «تحقق استقلال و کاهش وابستگی کشور» در اسناد بالادستی نظام آمده است.

مبنا در سند راهبردی جمهوری اسلامی ایران در فضای مجازی در افق ۱۴۱۰ ارزش‌ها، چشم‌اندازها، اهداف و راهبردها عنوان شده است. این سند از طریق مطالعه اسناد راهبردی و چشم‌انداز سایر کشورها در حوزه فضای مجازی، تحلیل وضع موجود و مطلوب، تحلیل اسناد بالادستی در مورخ ۱۴۰۰/۳/۱۷ تصویب‌شده است. در چشم‌انداز مطرح‌شده در بند «ب» این سند فضای مجازی ایران در سال ۱۴۱۰ در امتداد فضای واقعی، سالم، ایمن، مفید پیشران پیشرفت سایر حوزه‌ها، متکی بر ظرفیت درون‌زای کشور، برخوردار از منابع انسانی متخصص، ماهر مؤثر و کارآمد و... و در فراز پایانی آن دارای زیرساخت مطمئن، امن، پایدار، یکپارچه و گسترده در سراسر کشور بر بستر شبکه ملی اطلاعات و در ارتباط با شبکه جهانی مدنظر قرارگرفته است.

مجمع دولت‌های آسیای جنوبی یا آ.سه.آن در سال ۱۹۶۷ از اجتماع ۱۰ کشور تشکیل گردید. اهمیت وجود زیرساخت‌های اطلاعاتی ایمن در این منطقه در سال ۲۰۰۸ و در «برنامه کاری جامعه اقتصادی آ.سه.آن» مورد تأکید قرار گرفت. در سال ۲۰۱۲ «آ.سه.آن» در نوزدهمین مجمع منطقه‌ای خود بیانیه‌ای از سوی وزرای امور خارجه کشورهای عضو خود در مورد همکاری در حوزه تضمین امنیت سایبری صادر نمود و در جولای سال ۲۰۱۳ و در طول بیستمین مجمع خود نیز موضوع امنیت سایبری در ارتباط با جرائم فراملی و مبارزه با تروریسم و تأکید بر تقویت همکاری‌ها در این حوزه مدنظر قرار داد. به‌هرحال بیانیه‌ها و مصوبات این سازمان جنبه ارشادی دارند و برای اعضا الزام‌آور نمی‌باشند (تقی زاده، ۱۴۸:۱۳۹۵) به نقل از (کتانچی و پورقهرمانی ،۷۸:۱۳۹۵). در سال ۲۰۰۰ کنوانسیون امنیت سایبری و محافظت از اطلاعات شخصی اتحادیه آفریقا با هدف ایجاد هماهنگی در قوانین مرتبط با امنیت سایبری دستورالعمل گسترده‌ای ارائه و در سال ۲۰۱۲، قانون امنیت سایبری آفریقا را مشتمل بر چهار فصل معاملات الکترونیکی، حفاظت از اطلاعات شخصی، ارتقاء امنیت سایبری و مبارزه با جرایم سایبری و مقررات نهایی بازخوانی و در ماده ۲۸، همکاری بین‌المللی را لازمه تحقق امنیت سایبری دانسته و چهار شاخص هماهنگی، کمک حقوقی متقابل، تبادل اطلاعات و ابزار همکاری را برای آن پیش‌بینی کرد (AFRICAN UNION,2014). در اسناد راهبردی کشور فرانسه با هدف حفظ استقلال داخلی، محافظت سامانه‌های اطلاعاتی کشور و گردانندگان زیرساخت حیاتی برای پایداری بهتر ملی از بخش‌های مهم ماموریتی دفاع سایبری تلقی شده‌اند. بعلاوه توسعه همکاری‌های بین‌المللی در حوزه‌های امنیت سامان‌های اطلاعاتی، واکنش در مقابل با حملات سایبری و دفاع سایبر، به منظور محافظت بهتر از سامانه‌های اطلاعات ملی نیز از دیگر موضوعات راهبردی مورد تاکید کشور فرانسه است (Manuel Valls,2015).

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره اول | بهار ۱۴۰۲

در اجلاس هفتادم مجمع عمومی سازمان ملل متحد در ۲۲ جولای ۲۰۱۵ قطعنامه شماره A/۷۰/۱۷۴ در بند چهارمین گروه کارشناسان دولتی موضوع در بند ح مقدمه گزارش خود به این مسئله پرداخته است که: «دولت‌ها باید به درخواست‌های کمک متعارف از سوی دولتی دیگر که زیرساخت‌های حیاتی آن مورد تهدیدات مخرب در حوزه فناوری اطلاعات و ارتباطات قرارگرفته پاسخ دهند. دولت‌ها همچنین باید به درخواست‌های مناسب برای کاهش فعالیت‌های مخرب در حوزه فناوری اطلاعات و ارتباطات با هدف زیرساخت‌های حیاتی دولت دیگری که از سرزمین آن‌ها نشأت‌گرفته است، با توجه به حق حاکمیت پاسخ دهند» در بند ط نیز تأکید شده است که دولت‌ها باید گام‌های مسئولانه برای اطمینان از یکپارچگی زنجیره تأمین انجام دهند تا کاربران نهایی بتوانند به امنیت محصولات حوزه فناوری اطلاعات و ارتباطات اطمینان داشته باشند. دولت‌ها باید به دنبال پیشگیری از گسترش ابزارهای مخرب در حوزه فناوری اطلاعات و ارتباطات و تکنیک‌ها و استفاده از کاربردهای پنهان مضر باشند.

۲،۲،۳. توسعه شبکه ملی سایبری

همکاری بین‌المللی برای کاهش خطر و افزایش امنیت ضروری است. پیشرفت بیشتر همکاری در سطح بین‌المللی، مستلزم اقداماتی برای فراهم آوردن یک محیط صلح‌آمیز، امن و آزاد و در دسترس برای فناوری‌های اطلاعاتی و ارتباطی است که شامل هنجارها، قوانین و اصول مربوط به رفتار مسئولانه توسط دولت‌ها، اقدامات داوطلبانه برای افزایش شفاف‌سازی و اقدامات مربوط به اعتمادسازی، مسئولیت‌پذیری و ظرفیت‌سازی میان کشورها است (قطعنامه شماره A/۶۸/۹۸ اجلاس ۶۸۹ مجمع عمومی سازمان ملل متحد مورخ ۲۴ ژوئن ۲۰۱۳). ددر سیاست‌های کلی برنامه‌ی ششم توسعه ابلاغی مقام معظم رهبری به امور مرتبط با فناوری اطلاعات و ارتباطات بر ایجاد، تکمیل و توسعه‌ی شبکه ملی اطلاعات و تأمین امنیت آن، تسلط بر دروازه‌های ورودی و خروجی فضای مجازی و پالایش هوشمند آن و ساماندهی و احراز هویت تأکید گردیده است. مطابق سیاست‌های ابلاغی فوق توسعه فناوری اطلاعات و ارتباطات در تعامل با وضعیت جهانی این پدیده با نظر به اهمیت امنیت سایبری رویکرد عملیاتی در کشور خواهد بود. طرح مفاهیمی همانند هماهنگی، یکپارچه‌سازی و هدایت فعالیت‌های عملیاتی در فضای سایبر در اسناد راهبردی کشورهای مختلف، مرتبط با سامانه‌های فرماندهی و کنترل این فضا بوده و به‌عنوان خروجی‌های ایجاد و استقرار سامانه‌های مزبور تلقی می‌گردند (محمود زاده، و نیک نفس و مهدی قوچانی، ۱۳۹۶: ۲۳۲). کشور آلمان نیز با توسعه سند ملی راهبردی امنیت سایبر به موضوعات راهبردی از قبیل تضمین امنیت سایبر، اعمال حقوق و حفاظت از زیرساخت‌های اطلاعات حیاتی ملی با مشارکت دولت، صنعت و جامعه بر اساس یک رویکرد جامع و عمدتاً متمرکز بر رویکردها و اقدامات پیشگیرانه، تقویت امنیت سایبر با اعمال قواعد بین‌المللی رفتار، استانداردها و هنجارها با همکاری شرکای بین المللی و مقابل با رشد سریع جرائم اینترنتی با همکاری نزدیک بین مقامات اعمال قانون در سراسر جهان و اطمینان از امنیت سایبر توجه نموده است (German Government,2011)

در بندهای ۳۳ و ۳۴ و ۳۶ و .....از سیاست‌های کلی برنامه ششم توسعه کشور به امنیت فضای سایبری اشاره شده است:

بند ۳۳- توسعه محتوای در فضای مجازی بر اساس نقشه مهندسی فرهنگی کشور تا حداقل پنج برابر وضعیت کنونی و بومی‌سازی شبکه‌های اجتماعی.

بند ۳۴- ایجاد، تکمیل و توسعه شبکه ملی اطلاعات و تأمین امنیت آن، تسلط بر دروازه‌های ورودی و خروجی فضای مجازی و پالایش هوشمند آن و ساماندهی، احراز هویت و تحول در شاخص ترافیکی شبکه به‌طوری‌که ۵۰ درصد آن داخلی باشد.

بند ۳۶- حضور مؤثر و هدفمند در تعاملات بین‌المللی فضای مجازی؛ که در موادی از قانون برنامه ششم توسعه کشور نیز همین رویکرد لحاظ شده است:

ماده ۶۷- بندهای (الف، ب، پ، ت، ث، ج) شامل موضوع‌های: افزایش انتقال پهنای باند، زیرساخت‌های خدمات الکترونیکی و افزایش بهره‌وری زیرساخت‌های ارتباطی کشور، الکترونیکی کردن کلیه فرآیندها و خدمات با الکترونیکی و... است.

ماده ۶۸- بندهای (الف، ب، پ، ت، ث، ج، چ، ح، خ و د) شامل موضوع‌های: ایجاد نظام اطلاعات استنادپذیر الکترونیکی و گسترش متوازن زیرساخت‌های فنی محتوا و خدمات و دولت الکترونیک و... است.

ماده ۶۹- هوشمندسازی مدارس، امکان دسترسی الکترونیک؛ که در بند ۲ از سطر (پ) سیاست‌های کلی اقتصاد مقاومتی پیشتازی اقتصاد دانش‌بنیان، پیاده‌سازی و اجرای نقشه جامع علمی کشور و ساماندهی نظام ملی نوآوری به‌منظور ارتقاء جایگاه جهانی کشور و افزایش سهم تولید و صادرات محصولات و خدمات دانش‌بنیان و دستیابی به رتبه اول اقتصاد دانش‌بنیان در منطقه اشاره شده است.

۳،۲،۳. تدابیر محدودکننده دسترسی

نقض امنیت سایبری غالباً ناشی از دسترسی غیرقانونی به داده‌ها و اطلاعات دارای دامنه بالای اعتبار کشوری است. محدودنمودن دسترسی یکی از مهم‌ترین راهکارهای پیش‌بینی‌شده در این راستاست. ایجاد محدودیت در فضای مجازی و اعمال پالایش[۲۶]، منحصراً ترفند رژیم‌های سیاسی مقتدر و تمامیت‌خواه نیست؛ بلکه امروز پالایش به‌عنوان یک قاعده جهانی جهت تثبیت حق حاکمیت دولت‌ها در قلمرو برخط تلقی می‌شود، به‌طوری‌که تقریباً همه کشورهای جهان، بنا به ملاحظات سیاسی، عقیدتی، فرهنگی و اقتصاد خود جهت مبارزه و کنترل جرم و آسیب‌های اجتماعی در فضای مجازی، به پالایش می‌پردازند (پور نجفی قوشچی و فخر و پورقهرمانی، ۱۳۹۹: ۳۶).

نظام ملی پیشگیری و مقابله با حوادث فضای مجازی نیز با ایجاد ساختار مناسب، تقسیم‌کار، هماهنگی و همکاری ملی، وقوع حوادث در فضای مجازی کشور را کاهش داده و در کمترین زمان ممکن حوادث رخ‌داده را مدیریت می‌نماید. این نظام به حوادث شبکه‌ها و سیستم‌های فنی سخت‌افزاری و نرم‌افزاری پرداخته و حوادث حوزه محتوا را شامل نمی‌شود. ازجمله الزامات مطرح در طرح امن‌سازی سطح بلوغ امنیتی آن است که می‌تواند بر اساس سطح قابل‌پذیرش مخاطرات سازمان تعیین گردد که در سطح برنامه عملیاتی سازمان تصریح و به تأیید مرکز افتا خواهد رسید و شامل موضوعات مهمی چون: پایش و کنترل سایبری، مدیریت تهدیدات بدافزاری، مدیریت زنجیره تأمین، مدیریت هویت دسترسی، زیرساخت محرمانگی و استنادپذیری، آموزش و فرهنگ‌سازی، مدیریت تداوم کسب‌وکار، مدیریت حوادث سایبری (IT/OT) می‌شوند.

در بخش ۲-۲ طرح امن‌سازی زیرساخت‌های حیاتی در قبال حملات سایبری موضوع کنترل و پایش سایبری بیان و در سیاست‌های قابل‌بررسی در این خصوص لازم است خط‌مشی پایش و کنترل سازمان و پیشگیری و حفاظت در مقابل حملات و تهدیدات سایبری، مرکز عملیات امنیت مناسب با مأموریت‌های سازمان با استفاده از ظرفیت‌های داخل سازمان و استفاده از ظرفیت‌های سازمان بالادستی و طراحی امن شبکه و تجهیزات و برقراری ارتباط مرکز عملیات امنیت حوزه‌های زیرساختی به‌صورت امن را با مرکز عملیات امنیت کشور تحت مدیریت مرکز افتا در اهداف مدنظر خود بگنجاند.

از پیش‌بینی‌های قابل‌توجه دیگر در طرح فوق پرداختن به مدیریت هویت و دسترسی است. کاربران در سازمان به‌عنوان مهم‌ترین بازیگران در فرآیندهای سازمان، دارای دسترسی به منابع مختلف سازمان هستند. ایجاد، کنترل و مدیریت این دسترسی‌ها از وظایف اصلی تعریف‌شده در مدیریت هویت و دسترسی است. مدیریت هویت و دسترسی، چهارچوبی است که در آن سازمان سیاست‌ها و فرآیندهای خود در چرخه حیات هویت‌های دیجیتال را تبیین می‌نماید. این چرخه موارد زیر را در برمی‌گیرد: تعریف هویت دیجیتال؛ ایجاد و مجاز شماری دسترسی به منابع و دارایی‌های دیجیتال و فیزیکی آسان؛ حذف هویت و دسترسی‌ها در موقعی که کارمند مسئولیت خود را به هر دلیلی از دست می‌دهد. طرح در ادامه سیاست‌های در این جهت بیان می‌دارد: لازم است سازمان خط‌مشی مدیریت هویت و دسترسی شامل مدیریت چرخه حیات هویت‌های دیجیتال، کنترل دسترسی، تجهیزات قابل‌حمل شامل رسانه‌های قابل‌حمل سازمانی و دستگاه‌های شخصی، مدیریت رسانه‌های دیجیتال و غیر دیجیتال، ارتباطات راه دور و همچنین حفاظت فیزیکی خود را تدوین و اجرایی نماید.

[26] Filtering

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره اول | بهار ۱۴۰۲

۴،۲،۳. تدابیر سلب‌کننده دسترسی

علیرغم تأکید اسناد بالادستی نظام جمهوری اسلامی ایران بر توسعه فضای مجازی در ابعاد مختلف، امّا بسیاری از این اهداف آن‌گونه که باید محقق نشده است و هنوز کاستی‌ها و ناکارآمدی‌هایی دراین‌باره به چشم می‌خورد. در این نقصان و ناکارآمدی، می‌توان نقش عمده‌ای را برای سیاست‌گذاری‌های مربوطه در این خصوص که مبتنی بر نگاه از بالا به پائین، در دو طیف مجزای ایجابی و سلبی از سوی حاکمیت طرح‌ریزی گردیده‌اند، قائل شد (فرهنگی و میر ترابی گلشنی، ۱۳۹۸: ۱۱۳). در شرایط اضطراری علی‌رغم پروتکل‌های جهانی گردش آزاد اطلاعات شرایط خاص امنیتی می‌طلبد که اقدامات پیشگیرانه منجر به سلب دسترسی دائم یا مقطعی وضعیت نقض‌کننده امنیت باشد. اقدامات لحاظ شده تدابیر فنی و اثرگذار با استفاده از نرم‌افزارها یا هر اقدام تخصصی دیگری را در چارچوب قوانین توجیه می‌نماید. هدف از اجرای تدابیر سلب‌کننده دسترسی، مجموعه اقداماتی است که از ورود یا ارسال برخی از داده‌های غیرمجاز جلوگیری به عمل می‌آورد. درصورتی‌که این تدابیر به‌طور مناسبی اجرا شوند تا حد قابل قبولی می‌تواند از افشای اطلاعات تجاری ممانعت نماید (جوان جعفری، سودمندراد، ۱۹۴۳: ۴۲). ازجمله تدابیر فنی لحاظ شده در راستای سلب دسترسی اقدامات مختلفی مانند دیواره آتش[۲۷]، سیستم تشخیص تجاوز[۲۸]، نرم‌افزارهای ضد پیام‌های ناخواسته[۲۹]، نرم‌افزارهای ضد پایش، پراکسی‌ها[۳۰]، فیلترها[۳۱]، ناشناس کننده[۳۲] و رمزنگارها[۳۳] هستند. با این اوصاف به نظر می‌رسد سیاست پیشگیرانه فضای مجازی در کشور از نوع سلبی است که باید شامل سیاست‌ها و برنامه‌هایی معطوف به حذف، کنترل و نظارت دانست. در طیف سیاست‌های سلبی جوامع و دولت‌ها در حوزه سیاست‌گذاری و برنامه ریزی در خصوص فضای مجازی، شاید بتوان چهار گروه عمده از اقدامات را جای داد که عبارت‌اند از: تشویق به استفاده از سامانه‌های نظارتی و مسدودسازی سطح خرد، استفاده از سامانه‌های نظارتی و مسدودسازی سطح کلان، برنامه‌ریزی بازدارنده در حوزه قانون‌گذاری و جلوگیری از استفاده از اینترنت. پس این نگاه از بالا به پائین و دارای دو سازوکار عمده است؛ برنامه‌ریزی بازدارنده در حوزه قانون‌گذاری مبتنی بر تنظیم مقررات و پالایش فضای مجازی «مسدودسازی، فیلترینگ» (فرهنگی و میرترابی و گلشنی، ۱۳۹۸ ۱۱۶). در ماده «۱۰»توصیه‌نامه ارتقاء و استفاده چندزبانه و دسترسی جهانی به سایبر یونسکو، اکتبر ۲۰۰۳ تصریح‌شده است که کشورها می‌بایست دستیابی تمام سطوح جامعه را به فناوری اطلاعات و ارتباطات به‌نحوی‌که هزینه دسترسی کاربران به خدمات اینترنتی کاهش یابد را فراهم آورند. بر این اساس، همگان می‌بایست با دسترسی به اینترنت از آن بهره‌مند شوند و همچنین، در ماده «۲» منشور حفظ اسناد دیجیتالی یونسکو، اکتبر ۲۰۳۳ با تأکید بر اصل فوق، لزوم تعادل منصفانه بین حقوق سازندگان و سایر صاحبان حقوق، ازجمله حقوق و منافع عمومی از یک‌سو و حفظ حقوق و اطلاعات شخصی کاربران از هر گزند و نفوذ، مطالبه هنجارهای بین‌المللی، مورد تأکید قرارگرفته است (خادم رضوی و انصاریان، ۱۳۹۸: ۹).

۵،۲،۳. تدابیر صدور مجوز[۳۴]

امروزه فضای سایبر ابعاد مختلف داده‌های شخصی نظیر اطلاعات ژنتیکی، هویتی، فیزیولوژیکی، رفتاری و اعتقادی را مورد هدف قرار داده است تا با جمع‌آوری آن‌ها بتواند به پایش‌ها و برنامه‌ریزی‌های سیاسی، اقتصادی و اجتماعی دست یابد. در مقابل متولیان سیاست تقنینی در بیشتر جوامع مقررات متنوعی در راستای حمایت از حریم خصوصی و داده‌های اشخاص تدوین و تصویب نموده‌اند (قناد و علیقلی، ۱۳۹۸: ۱). شورای عالی فضای مجازی در جلسه ۵۴ مورخ ۱۳۹۷/۹/۲۴ آیین‌نامه اجرایی احصای کلیه استعلامات و ایجاد نظام

[27] Fire Walls
[28] Intrusion Detection System(IDS)
[29] Unsolicited Commercial Mail(UCM) or Spam
[30] Proxy
[31] Filtering
[32] Anonymizers
[33] Encryption
[34] Verification or Authentication Technologies

استانداردسازی و تبادل اطلاعات بین دستگاهی را که توسط مرکز ملی فضای مجازی با همکاری وزارت ارتباطات و فناوری اطلاعات و سایر دستگاه‌های اجرایی ذی‌ربط تدوین‌شده بود تصویب نمود و در این آیین‌نامه پایگاه‌های اطلاعاتی پایه را کلیه پایگاه‌های که داده و اطلاعات آن‌ها برای احراز هویت اشخاص، دارایی‌های منقول و غیرمنقول، فعالیت اقتصادی، اجتماعی و علمی و صحت تبادل اطلاعات پولی، مالی و سرمایه‌ای ضروری است معرفی و در ادامه بنده ۱-۳ ماده ۱ این آیین‌نامه پایگاه هویت ایرانیان، پایگاه اسناد و املاک و حدنگاری کشور و پایگاه ثبت‌نام الکترونیک قوه قضائیه و حدود ۲۲ پایگاه دیگر را ذکر که برابر ماده ۳ آن تبادل اطلاعات و استعلامات را صرفاً از طریق مرکز کلی تبادل اطلاعات (NIX) موضوع تبصره «۲» بند «ث» ماده ۶۷ قانون برنامه پنج‌ساله ششم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی ایران و مطابق دستورالعمل‌های صادره انجام خواهند داد. نکته قابل‌توجه وظایف و اختیاراتی است که در ماده ۶ آیین‌نامه برای کارگروه تعامل‌پذیری دولت الکترونیکی ذیل مرکز ملی فضای مجازی و با عضویت دبیر شورای اجرایی فناوری اطلاعات بدان پرداخته است که شامل این موارد می‌شوند: تعیین ضوابط و استانداردهای لازم نظیر قالب شناسنامه‌های فنی، ارزیابی شناسنامه فنی تکمیل‌شده توسط دستگاه‌های اجرایی، استعلام و نحوه دسترسی به آن‌ها، تعیین دادگان برای دولت الکترونیک، تدوین توافق‌نامه تبادل اطلاعات بین دستگاه‌های مبدأ، مقصد و مرکز ملی تبادل اطلاعات، تعیین مدل پیاده‌سازی تبادل اطلاعات و استعلام الکترونیکی بین دستگاهی، به‌روزرسانی فهرست پایگاه‌های اطلاعات‌پایه و... درمجموع این آیین‌نامه درصدد حذف استعلامات مکتوب و انتقال آن‌ها به مرکز ملی تبادل اطلاعات است که بیانگر رصد و پایش مکاتبات و نیز محافظت از داده‌های مذکور و اتخاذ سیاست جنایی پیشگیرانه البته با اتخاذ تدابیر مناسب است.

دومین مصوبه جلسه ۵۳ مورخ ۱۳۹۷/۷/۳۰ با عنوان الزام حاکم بر اینترنت اشیاء ضمن ارائه مفاهیم و تعاریف مدنظر مختصات فعلی فضای مجازی را مبتنی بر «کلان داده‌ها[۳۵]» و «ارتباط از نوع ماشینی[۳۶]» و «هوشمندسازی[۳۷]» اعلام و در بند ۳ ماده ۲ در باب الزامات عمومی به تدوین نیازمندی‌های حقوقی با رویکرد تعریف اشیاء، تعیین جایگاه و همچنین تنظیم روابط آن‌ها در تعامل با یکدیگر و انسان نیم‌نگاهی دارد و در ادامه از اصول ایمنی کاربران در اتصال به شبکه اینترنت اشیاء، به‌منظور تضمین امنیت و سلامت فردی و عمومی سخن به میان آورده است.

در این سند تبیین الزامات شبکه ملی اطلاعات در باب ۴ از ماده ۴ تحت عنوان خدمات شبکه ملی اطلاعات ویژگی‌های مدیریتی و امنیتی و دارای تعامل با لایه‌های مدیریتی و امنیتی این شبکه را در ۴ محور خدمات ارتباطی، خدمات پایه کاربردی، خدمات سالم‌سازی امنیتی و پشتیبانی از خدمات رصد کمی، کیفی و هوشمندی تجاری، فرهنگی دفاعی ذکر کرده است و در فراز ۵ آن با عنوان سالم‌سازی و امنیت شبکه ملی اطلاعات را به تعامل با دیگر شبکه‌ها، بر اساس نظامات یکپارچه قابل تأمین و اصولی را برای آن بدین شرح در نظر گرفته است: ۱- حفاظت و مدیریت تعاملات در شبکه ملی اطلاعات؛ ۲- شبکه‌های اختصاصی امن و ارتباطات دستگاه؛ ۳- خدمات ایمن. در هریک از این موارد فروعاتی را مورد نظر دارد. در بند ۱ بخش اول تصویب‌کنندگان تأمین امنیت همه‌جانبه فرهنگی، اقتصادی، سیاسی، قضائی و اجتماعی و امنیت در سطح داده‌ها، اطلاعات در لایه‌های مختلف شبکه ملی اطلاعات در حوزه زیرساخت فضای مجازی کشور و امکان اعمال سیاست‌های حاکمیتی متفاوت و در بند ۲ حفاظت در مقابل تهدیدات بالقوه و بالفعل درونی و بیرونی شامل تهدیدات از دیگر شبکه‌ها و از شبکه ملی علیه خود و یا علیه لایه‌های فضای مجازی و علیه ذینفعان و برعکس را لحاظ و در پی چاره اندیشی و مدیریت و پیشگیری و مقابله قانونی با وقوع و گسترش حوادث و انواع جرائم و دفاع سایبری و مقابل با تروریسم و تأمین

[۳۵] Big-Data

[۳۶] Machin Type Communication (MYC)

[۳۷] Smartness

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره اول | بهار ۱۴۰۲

امنیت عمومی و پشتیبانی از مشارکت‌های اجتماعی کاهنده جرائم و ارتقاء بخش سالم‌سازی امنیت و تأمین امنیت در مدیریت منابع، زیرساخت‌ها و خدمات شبکه ملی اطلاعات در بندهای بعدی است.

۶،۲،۳. تدابیر نظارتی و حفاظتی[۳۸]

ابزارهای نظارت الکترونیکی، وظیفه کنترل فعالیت شبکه‌ای افراد را با به‌کارگیری تجهیزات و برنامه‌هایی بر عهده‌دارند. نقض امنیت سایبری را می‌توان با تدابیر پیشگیرانه ازجمله پیشگیری وضعی محدود کرد. یکی از روش‌های پیشگیری موقعیت مدار که به افزایش خطر ارتکاب بزه منجر می‌شود، کاربست تدابیر نظارتی است. از دیرباز، نظارت جایگاه ویژه‌ای در سیاست‌های پیشگیری از بزهکاری داشته و با توجه به نقش بازدارنده آن ارتکاب بزه، همچنان در اشکال مختلف مورداستفاده قرار می‌گیرد. نظارت مادی و الکترونیکی ازجمله تقسیم‌بندی‌های قابل‌ذکر است که تدابیر نظارت الکترونیکی رسمی است که از سوی مقامات مسئول پیشگیری از جرم، در راستای پیشگیری موقعیت مدار از جرائم سایبری صورت می‌گیرد (فرهادی آلاشتی و جعفری، ۱۳۴۹۵: ۷۶-۷۸).

یکی از سیاست‌های قابل‌اعمال در حیطه نقض امنیت سایبری داده‌کاوی[۳۹] حداکثری و نقض محرمانگی داده‌های کاربران است. با پیشرفت فناوری‌های هوش مصنوعی، امروز داده‌کاوی به‌عنوان یکی از قدرتمندترین و مؤثرترین ابزارهای موردنیاز مجریان قانون برای شناخت فرصت‌های بزهکارانه احتمالی تبدیل‌شده است ازاین‌رو، این روش‌ها را «شیوه‌ای مؤثر برای استخراج اطلاعات و داده‌های مهم از میان انبوه داده‌ها» تعریف کرده‌اند (Taniar, 2008: 119) به نقل از: (فرهادی آلاشتی و جعفری، ۱۳۹۵: ۸۱)

آیین‌نامه نحوه ارائه خدمات اطلاع‌رسانی و اینترنت، شرکت‌ها و یا مؤسسات و مراکز ارائه‌کننده خدمات اطلاع‌رسانی و اینترنت را به‌عنوان اشخاص حقوقی تعریف و حدود فعالیت‌ها و وظایف آن‌ها را برشمرده است. آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی مصوب ۱۳۹۳ نیز در بند الف ماده ۱ ارائه‌دهندگان خدمات دسترسی را اشخاصی دانسته که امکان ارتباط کاربران را با شبکه‌های رایانه‌ای یا مخابراتی و ارتباطی داخلی یا بین‌المللی یا هر شبکه مستقل دیگر فراهم می‌آورند از قبیل تأمین‌کنندگان، توزیع‌کنندگان، عرضه‌کنندگان خدمات دسترسی به شبکه‌های رایانه‌ای یا مخابراتی. همچنین مطابق ماده ۶۶۷ قانون آیین دادرسی کیفری، ارائه‌دهندگان خدمات دسترسی موظف‌اند داده‌های ترافیک را حداقل تا شش ماه پس از ایجاد حفظ نمایند و اطلاعات کاربران را حداقل تا شش ماه پس از خاتمه اشتراک نگهداری کنند و بر اساس ماده ۶۶۸ قانون آیین دادرسی کیفری ارائه‌دهندگان خدمات میزبانی داخلی موظف‌اند اطلاعات کاربران خود را حداقل تا شش ماه پس از خاتمه اشتراک و محتوای ذخیره‌شده و داده ترافیک حاصل از تغییرات ایجاد شده را حداقل تا پانزده روز نگهداری کنند. همچنین در خصوص اپراتورهای تلفن همراه نیز پیش‌بینی مواردی جهت نظارت این ارائه‌دهندگان خدمات بر محتوای سایبری پیش‌بینی‌شده است. به‌عنوان‌مثال در پیش‌نویس نقشه مهندسی فرهنگی شرکت خدمات ارتباطی رایتل، اپراتور رایتل به‌عنوان فراهم‌کننده خدمات در ایران بر اساس ضوابط مقرر توسط شورای عالی انقلاب فرهنگی خط‌مشی خود را در زمینه نحوه ارائه خدمات به مشترکین تنظیم کرده است. بخشی از خط‌مشی این فراهم‌کننده خدمات صراحتاً همکاری مشارکتی در تنظیم مقررات در زمینه کنترل و نظارت بر محتوا است. ازجمله این خط‌مشی‌ها می‌توان به تدوین سازوکار نظارتی بر محتوا، تبلیغات و خدمات اشاره نمود. این فراهم‌کننده خدمات هیئت متخصصی را برای تعیین محتوا و پایش آن تشکیل داده است که ازجمله وظایف این هیئت تدوین سازوکار نظارتی بر محتوا، تبلیغات و خدمات تعیین ضوابط فرهنگی انتخاب و همکاری با شرکت‌های همکار در موضوعات محتوا، خدمات و تبلیغات، پایش فرهنگی مطبوعات و... محتوای چندرسانه‌ای، پایش فرهنگی خدمات ارزش‌افزوده، پایش فرهنگی تبلیغات تلویزیونی، چاپ، پایش فرهنگی فروشگاه‌های عرضه خدمات رایتل، پایش اخبار مرتبط با تبلیغات، خدمات و محتوا، رصد اخبار مرتبط با تبلیغات، خدمات و

[۳۸] Monitoring Measures
[۳۹] Data Mining

محتوا است مجموعه اقدامات جلوگیری از دستیابی مجرمان بالقوه به فرصت و ابزار ارتکاب جرم تحت شمول تدابیر پیشگیرانه وضعی از جرم می‌توان برشمرد. برنامه پیشگیرانه قابل‌ذکر دیگر طرح دژفا که سپر امنیتی شبکه ملی اطلاعات است و همراه با توسعه فناوری از حریم شخصی افراد محافظت می‌کند و هدف آن مقابله با حمات سایبری، حمایت از تداوم خدمات دیجیتال، جلوگیری از کلاهبرداری، نشر اطلاعات و شناسایی بدافزارهاست و جهت حفظ امنیت اطلاعات و زیرساخت‌های دیجیتال کشور به‌عنوان «سپر امنیتی شبکه ملی اطلاعات» عمل خواهد کرد. دژفا مجموعه از سامانه‌ها است که برای رصد وضعیت تهدیدات و افزایش توان مقابله با آسیب‌ها در فضای سایبری کشور توسط مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌های کشور که نقش (cert) ملی ایران را بر عهده دارد در دست توسعه است. در طرح دژفا الزاماتی را در قالب حدود ۱۰ سامانه در نظر گرفته‌اند که قرار است در آینده به ۱۸ سرویس افزایش یابد ازجمله: سامانه‌های ملی تله افزار بومی کاوشگر و بومی سمات و بومی بینا و بومی چکاپ و بومی سایمان و بومی دانا و عمومی سینا و بومی سویه چتر امن (ناظمی، میثم، ۱۳۹۸: ۵۸).

علی‌رغم این در سطح جهانی تنها توافق‌نامه بین‌المللی چندجانبه در موردحفاظت از داده‌ها با تعداد قابل‌توجهی از طرفین، کنوانسیون شورای اروپا برای حمایت از اشخاص در رابطه با پردازش خودکار داده‌های شخصی (کنوانسیون ۱۰۸) سال ۱۹۸۱ است که همه اعضا شورای اروپا به‌استثناء ترکیه طرف این کنوانسیون هستند. در ماده ۶ کنوانسیون دسته‌های ویژه داده مورد حفاظت باید قرارگرفته و پردازش آن‌ها ممنوع است؛ اما در بند دوم ماده ۹ استثنائات این ممنوعیت را تنها در مواردی که توسط قانون ملی پیش‌بینی‌شده است مجاز می‌داند و این اقدام در جامعه دموکراتیک به‌منظور حفاظت از امنیت کشور، امنیت عمومی، منافع ملی کشور و یا سرکوب جرائم جنایی یا حفاظت از موضوع داده یا حقوق و آزادی دیگران محافظت، یک اقدام ضروری اعلام می‌کند. فراتر از آن کشورهای منطقه اقیانوس آرام و آسیا تحت عنوان سازمان همکاری اقتصادی آسیا و اقیانوسیه (APEC)، چارچوب حفظ حریم خصوصی را در سال ۲۰۰۵ تصویب کرده است. در رابطه با پاسخ گوئی، یک کنترل‌کننده اطلاعات شخصی باید از نظر مطابقت با اقدامات مؤثر اصولی، پاسخگو باشد. در صورت انتقال اطلاعات شخصی به شخص یا سازمان دیگری، چه در داخل کشور و چه در سطح بین‌المللی، کنترل‌کننده «باید» رضایت فرد را جلب کرده یا مراقبت‌های لازم اقدامات منطقی را انجام دهد تا اطمینان حاصل کند که شخص یا سازمان، اطلاعات را پس از انتقال، مطابق با اصول مربوطه محافظت می‌کند (کریانگ‌ساک، ۱۴۰۰: ۱۰۷). در ماده ۸ از کنوانسیون مصوب ۱۹۸۱ شورای اروپا در حمایت از افراد در رابطه با پردازش خودکار اطلاعات، امکان حذف، اصلاح، پاک‌سازی و جلوگیری از پردازش اطلاعات را از ناحیه دارنده اطلاعات در فرض وجود هرگونه نقض از ناحیه کنترل‌کننده پیش‌بینی نموده است. علاوه بر آنچه بیان شد در سال ۲۰۱۵ گروه جی ۲۰ با تصویب اینکه کشورهای عضو این گروه حق هیچ‌گونه نقض امنیت مجازی برای دستیابی به اهداف تجاری خود را ندارند، مبادرت به تصمیم‌گیری بازدارنده نمود که این امر می‌تواند از اقدامات ناقضان این اعضا در زمینه‌های دیگر مانند نظامی یا پشتیبانی پیشگیری نماید (کریانگ‌ساک، ۱۴۰۰:۴۰۸)

نتیجه‌گیری

در این پژوهش اسناد و مدارک مهم و بالادستی جمهوری اسلامی ایران ازجمله: سیاست‌های کلی برنامه ششم و پنجم توسعه، سیاست های کلی نظام در امور امنیت فضای تولید و تبادل اطلاعات ملاحظه شده‌اند تا رویکرد سیاست جنایی ایران در قبال نقض امنیت سایبری در تقابل با قوانین و کنوانسیون‌ها و اسناد ناظر بر امنیت سایبری در نظام بین‌الملل ارزیابی گردد. با مداقه در راهبردهای پدافند سایبری رویکردهای متنوعی در رهیافت‌های مدنظر کارگزاران سایبری کشور با ابتناء بر آموزه‌های سیاست جنایی پیشگیرانه به چشم می‌خورد ازجمله: توسعه آمادگی دفاعی و بازدارندگی در مقابل تهدیدات و حملات سایبری، دستیابی به‌نظام جامع فرماندهی و کنترل مقتدر و هوشمند دفاع سایبری، رصد، پایش، مراقبت و تشخیص و هشدار تهدیدات و حملات سایبری، حفظ و پایداری سازی زیرساخت‌های حیاتی و حساس کشور در مقابل تهدیدات و حملات سایبری، توسعه زیست‌بوم سایبری بومی، امن و پایدار، توسعه مفاهیم دفاع سایبری،

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره اول | بهار ۱۴۰۲

توسعه نظام حقوقی و تعاملات بین‌المللی در حوزه دفاع سایبری، تدوین قوانین و مقررات، دستورالعمل‌ها و استانداردهای بومی در حوزه دفاع سایبری، توسعه قابلیت‌های صیانت از اطلاعات، افراد و سرمایه‌های سایبری، درک هوشمندانه و پیش‌دستانه تهدیدات، نفوذناپذیری و استحکام و ایمنی زیرساخت‌های حیاتی و حساس، عدم به‌کارگیری غیرهوشمندانه سامانه‌های خارجی در مراکز دارای اهمیت بالا. با این اوصاف و از سوی دیگر در حال حاضر کنوانسیون بین‌المللی در حوزه امنیت سایبری به رشته تحریر در نیامده است لذا قطعنامه‌های سازمان ملل یا پروتکل منطقه‌ای و یا اسناد کشورهای دارای هژمونی سایبری ازجمله کشورهای اروپای مطالعه و در نهایت اینکه، تدقیق در مجموعه قوانین و مقررات مربوطه، حکایت از این دارد که سیاست جنایی ایران در قبال نقض امنیت سایبری، سیاستی غیر افتراقی و مبهم و فاقد مبنای منسجم حقوقی و بعضاً مغایر و ناهماهنگ با اصول بین‌المللی است.

آنچه در دوران کنونی به‌عنوان مهم‌ترین موضوع و چالش غیرقابل‌انکار از آن می‌توان یاد کرد ابهام و چندگانگی در تعریف روشن از فضای سایبر و امنیت سایبر و شناسایی چالش‌های گوناگون موجود در این عرصه است. هنگامی‌که سخن از سیاست جنایی است، می‌بایست دریابیم که ما در کجای جهان سایبریم و آیا آنچه تعریف ما از سایبر است و آنچه در مفاهیم این پدیده در نظام قانونی و حقوقی جهان سایبر وجود دارد به همان صورت در نظام حقوقی و اجتماعی ما قابل تسری است. در بعد داخلی و بین‌الملل طلاقی این مفاهیم و تطبیق نظام واژگان موجود خود چالش مهمی است که به سبب تنوع قوانین بعضاً ضعیف موجود در داخل، گریبان‌گیر نظام حقوقی ماست. تدوین و اجرای سیاست‌های مناسب در حوزه حکمرانی دیجیتال می‌تواند باعث افزایش اعتماد عمومی، افزایش سطح کیفیت خدمات دولت، افزایش رفاه و آسایش عمومی، خلق منابع ثروت جدید برای کشور و درعین‌حال تمدن‌سازی در جهت نیل به آرمان‌های بیانیه گام دوم انقلاب اسلامی گردد. در این میان، نهادهای متولی سیاست‌گذاری در کشور در سالیان گذشته نقش خود را برای ترسیم و تحقق حکمرانی فضای مجازی در تراز انقلاب اسلامی را به‌درستی ایفا نکرده‌اند. تحقق حکمرانی منوط به هم‌گرایی نهادهای سیاست‌گذار و وزارت ارتباطات و فناوری اطلاعات به‌عنوان مجری و تنظیم‌گر و ارائه واقع‌بینانه نیازمندی‌ها و مطالبات حاکمیت در جهت تحقق مدل حکمرانی مطلوب است. باید افزود که حاکمیت بر اینترنت شامل مدیریت و هماهنگی زیرساخت‌های فنی اینترنت است. مثل نام‌های دامنه، آدرس‌ها، استانداردها پروتکل‌هایی که اینترنت را قادر به انجام وظایفش می‌کند. تعریف موسعی از حاکمیت بر اینترنت ارائه شده است: «عوامل مختلفی که موضوعات مرتبط با سیاست‌گذاری اینترنت را شکل می‌دهند، مثل مالکیت فکری،حریم خصوصی، آزادی اینترنت، تجارت الکترونیک، امنیت سایبری و....»[۴۰]

از سویی دیگر همگرایی ایران با کشورهای منطقه، کشورهای اسلامی، جنبش عدم تعهد و قدرت‌های همسو می‌تواند باعث برون‌رفت کشور از مواجهه منفرد با سیاست‌های یک‌جانبه‌گرایانه، ایجاد ظرفیت‌های اقتصاد دیجیتال در منطقه، پیگیری تصویب معاهدات و قوانین پیشنهادی توسط ایران در مجامع و نهادهای قانون‌گذار بین‌المللی و... گردد. علاوه بر این، امکان پیگیری حقوقی حمات سایبری به زیرساخت‌های کشور (نظیر استاکسنت و سامانه سوخت)، نقض حریم خصوصی شهروندان ایرانی، مسدودسازی صفحات کاربران ایرانی توسط سکو (پلتفرم) های خارجی و تحریم زیرساخت‌ها و ابزارهای توسعه فناوری اطلاعات، از طریق پویایی بیشتر حوزه روابط بین‌الملل وزارت ارتباطات مقدور خواهد بود..

ما قادر به حذف خود و جامعه و محدود کردن و عدم دسترسی و حکم به عدم خویش به‌عنوان یک نظام حاکمیت آنهم با داعیه‌های اقتدار ایران اسلامی به‌عنوان بازیگری تأثیرگذار و فعال در بعد داخلی و منطقه‌ای و بین‌المللی نیستیم و از سوی بودن ما آنهم در این ابهام لایتناهی سایبر بدون اتخاذ چهارچوب‌های حقوقی که برگرفته از یک نظام سیاست جنایی قدرتمند امنیت‌مدار باشد، ممکن نیست. پس در وهله اول شناخت تمامی ابعاد جهان فضای سیال، فعال، تغییرپذیر و پویا که اساساً خواستگاهی غیر ایرانی نیز دارد و ترسیم خطوط و

[40]- Lennard G. Kruger Internet Governance and the Domain Name System: Issuse for Congress November 18, 2016. P.۱

نقشه راه‌های با چشم‌انداز امنیتی بر اساس قواعد حقوق اسلامی و ایرانی و منطبق با آموزه‌های دنیای نوین از اهم مهمات است که نیازمند بررسی و تفحصی اندیشمندانه در تمام اسلوب‌های تأثیرگذار آن است. نه پذیرش هرچه هست و نه رد هر چه هست. ما بخشی از این دنیای گسترده بی‌مرز پر رمزورازیم که می‌بایست آینده اقتدار خویش را در آیینه هزارتویی واقعیت نوین دنیای سایبر و دهکده نوین جهانی بیابیم. در این مقال بحث از امنیت سایبری بود نه امنیت با تعاریف معمول آن که البته آنهم بعدی از موضوع بحث ماست.

در این میان چالش‌های متعددی وجود دارد که می‌توان به آن‌ها اشاره کرد: عدم توجه به نقش محوری شورای عالی فضای مجازی در حوزه سیاست‌گذاری و تصمیم‌گیری حکمرانی دیجیتال (فضای مجازی)، فقدان نگاه جدی به اهمیت و موضوع حکمرانی دیجیتال و ضعف دانشی این حوزه در بین مسئولین مربوطه، خلاء وجود مدل حکمرانی دیجیتال مطلوب مبتنی بر ارزش‌های ایرانی–اسلامی، عدم سیاست‌گذاری فعال در مواجهه با فناوری‌های جدید و به‌تبع، عدم استفاده حداکثری از ظرفیت‌های آن‌ها برای پیشرفت کشور، نبود زیرساخت‌های سخت‌افزاری و نرم‌افزاری لازم برای تحقق حکمرانی دیجیتال، عدم حضور مؤثر و فعال در تدوین معاهدات بین‌المللی حاکم بر نظامات فناوری اطلاعات و ارتباطات، عدم توفیق در راه‌اندازی و بهره‌برداری کامل از شبکه ملی اطلاعات، عدم وجود زیرساخت‌های قانونی لازم برای احقاق حقوق تضییع‌شده کاربران ایرانی در سکو (پلتفرم) های خارجی. این ایرادات را بر اساس نظام حاکم سیاست‌های فضای مجازی می‌بایست راهبری نمود و ازجمله اینکه با اتخاذ تدابیری شامل موضوعات ذیل رهیافت‌های سیاست سایبری کارآمد را پیش گرفت: همگرایی ساختارهای بعضاً موازی و تعیین خطوط فاصل بین وظایف هریک از ساختارهای موجود، اصلاح، یکپارچه‌سازی و استقرار نظام جامع تنظیم مقررات فضای مجازی، پیشنهاد تشکیل کمیسیون تخصصی فضای مجازی در مجلس شورای اسلامی، تلاش برای همراهی هرچه بیشتر وزارت ارتباطات و فناوری اطلاعات با شورای عالی فضای مجازی با اجرای مصوبات شورا، پیشنهاد مدل حکمرانی مطلوب فضای مجازی در تراز بیانیه گام دوم انقلاب اسامی و پیگیری تصویب و پیاده‌سازی آن، تدوین دکترین فضای مجازی و نقشه راه جمهوری اسلامی ایران در راستای نیل به قدرت سایبری اول منطقه و تأثیرگذاری در سطح جهان در تعامل با نهادهای سیاست‌گذار، توجه ویژه به تحلیل کلان داده‌ها[41] برای تصمیم‌گیری‌های کلان کشور، نگاه فرصت محور به فناوری‌های نوظهور نظیر هوش مصنوعی[42]، بلاک چین[43]، اینترنت اشیاء[44] و...، ایجاد بسترهای جلب سرمایه‌گذاری خارجی جدید از طریق پیش‌بینی برنامه همکاری بلندمدت با رویکردهای جدید تأثیرناپذیر از تحریم‌های خارجی، تدوین برنامه اقدام همکاری مؤثر با سازمان‌های منطق‌های و جهانی حوزه فناوری اطلاعات، جبهه مقاومت و کشورهای همسو برای مقابله با انحصارگرایی نظام سلطه در حکمرانی اینترنت، افزایش ظرفیت ترانزیت مرز به مرز بین‌الملل با هدف فعال نمودن بازارهای اقتصادی و کسب‌وکار دیجیتال مرزی، استفاده از ظرفیت قدرت‌های همسو در تأمین امنیت زیرساخت‌های حساس سایبری و انتقال دانش و فناوری به کشور، مواجهه ایجابی، توسعه گرایانه، فناورانه، اشتغال آفرین با فناوری‌های نوین ارتباطی نظیر منظومه ماهواره‌ای، توزیع پهنای باند و دسترسی به اینترنت، عملیاتی سازی اسناد بالادستی نظام در همه ارکان و شئونات وزارت ارتباطات و فناوری اطلاعات در جهت تحقق حکمرانی دیجیتال، تهیه و ارائه لوایحی برای بروز رسانی قوانین و مقررات حوزه فناوری اطلاعات و فضای مجازی ازجمله مالیات، بیمه، مطبوعات، تبلیغات، تجارت متناسب با توسعه و نیازهای فضای مجازی شود.

[41] Big Data Analytics
[42] Artificial Intelligence
[43] Block chain
[44] Internet of Things

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره اول | بهار ۱۴۰۲

منابع

- احمدیان، قدرت و بلوکی، صالح و صارمی‌فر، مریم .(۱۳۹۱). «مفهوم نوین استراتژیک ناتو(۲۰۱۰ (و پیامدهای امنیتی آن در روابط ناتو و روسیه»، فصلنامه آسیای مرکزی و قفقاز، شماره ۸، صص ۳۰-۱
- بهره‌مند، حمید و کوره‌پز، حسین محمد و سلیمی، احسان.(۱۳۹۱). «راهبردهای وضعی پیشگیری از جرائم سایبری»، آموزه‌های حقوق کیفری، دانشگاه علوم اسلامی رضوی، ش۷.
- بهره‌مند، حمید و داوودی، ذوالفقار.(۱۳۹۷). «پیشگیری اجتماعی از جرائم امنیتی سایبری»، مطالعات حقوق کیفری و جرم‌شناسی،دوره ۴۸، شماره ۱، صص۴۶-۲۷
- پور نجفی قوشچی، لیلا و فخر، حسین و پور قهرمانی، بابک، ۱۳۹۹، پالایش فضای مجازی در پرتو اسناد حقوق بشری، آموزه‌های حقوق کیفری، دوره هفدهم، شماره ۱۹، صص۶۷-۳۵
- پورقهرمانی، بابک و عظیمی، فهیمه .(۱۳۹۸). «نقش فضای سایبری در توسعه امنیت گردشگری»، مجموعه مقالات دومین کنفرانس ملی پدافند سایبری، آدربایجان شرقی، دانشگاه آزاد اسلامی واحد مراغه.صص ۴۲۳-۴۰۸
- تقی زاد، مهرداد.(۱۳۹۵). «سازمان‌های بین‌المللی و قاعده‌مند سازی فضای سایبری»، چاپ اول، تهران: انتشارات خرسندی
- جوان جعفری، عبدالرضا و سودمندراد، امیر .(۱۳۹۴). «پیشگیری وضعی از نقض اسرار تجاری در فضای سایبر»، دو فصلنامه دانشنامه حقوق اقتصادی (دانش و توسعه سابق)، دوره جدید، سال بیست و یکم، شماره۶، صص۵۰-۳۱
- شریفی‌هولاسو، اسماعیل .(۱۳۸۷). «بررسی تجربه جامعه‌پذیری در میان سه نسل با مطالعه دانش آموزان دبیرستان‌های پسرانه شهر تهران»، پایان نامه کارشناسی ارشد، دانشگاه تربیت مدرس.
- خادم رضوی، قاسم و انصاریان، جواد.(۱۳۹۸). «الزامات حقوقی حاکم بر تبلیغات تجاری سایبری و ضمانت اجرای کیفری آن با رویکرد تطبیقی»، فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف، سال اول، شماره سوم، صص۲۳-۷
- صادقی‌فسایی، سهیلا و عرفان‌منش، ایمان .(۱۳۹۴). «مبانی روش‌شناختی پژوهش اسنادی در علوم اجتماعی»، مجله راهبرد فرهنگ، شماره ۲۹، صص ۹۱-۶۱
- جزایری، سید عباس و نعمت‌الهی، میثم و امیربان فارسانی، امین .(۱۳۹۸). «پیشگیری از جرائم سایبری و محدودیت‌های حاکم بر آن»، فصلنامه علمی-حقوقی قانون‌یار، دوره سوم، شماره ۱۱، صص۲۴-۹
- حسینی، پرویز.(۱۳۹۵). «ارائه الگوی راهبردی در حوزه امنیت فناوری اطلاعات و ارتباطات بر اساس گفتمان امام (ره) و رهبری، قانون اساسی، تجارب جمهوری اسلامی ایران، بهره‌گیری از تجارب موفق بشری»، تهران :دانشگاه عالی دفاع ملی، دانشکده امنیت ملی.
- خوشنویس، یاسر.(۱۳۹۸). «حکمرانی چند ذیربطی فضای مجازی»، پژوهشگاه مرکز ملی فضای مجازی-گروه مطالعات فرهنگی و اجتماعی، تهران، گزارش شماره۳.
- عالی پور، حسن .(۱۳۹۲). «بزه های امنیتی سایبری»، جزوه حقوق جزای اختصاصی کارشناسی ارشد (درآمد بزه های رایانه ای)، دانشگاه اصفهان
- علایی، حسین .(۱۳۹۱). «امنیت پایدار در سند چشم‌انداز بیست‌ساله جمهوری اسلامی ایران، علوم سیاسی»، آفاق امنیت، شماره ۱۵،صص ۱۴۸-۱۱۹
- -فرهادی آلاشتی، زهرا و جوان جعفری بجنوردی، عبدالرضا .(۱۳۹۵). «بررسی تعارض رهیافت‌های تدابیر موقعیت مدار نظارت سایبری با حریم خصوصی کاربران»، مجلس و راهبرد، سال ۲۳، شماره ۸۷، صص۱۰۰-۷۵

دانشگاه آزاد اسلامی واحد مراغه

- فرهنگی، محمدمهدی و میر ترابی، سعید و گلشنی، علیرضا .(۱۳۹۸). «تبیین سیاست‌گذاری فضای مجازی در جمهوری اسلامی ایران (الزامات و اصلاح، در چارچوب اهداف موردنظر در اسناد بالادستی)» ،فصلنامه پژوهش‌های انقلاب اسلامی، انجمن علمی انقلاب اسلامی ایران، سال هشتم، شماره ۳۰، صص ۱۳۲-۱۱۱
- قناد، فاطمه و علیقلی، امیره.(۱۳۹۸). «حمایت از حریم خصوصی در فضای وب در پرتو قانون اروپایی حمایت از داده‌های شخصی و نظام حقوقی ایران» ،پنجمین کنفرانس وب پژوهشی، صص۹-۱
- کتانچی، الناز و پورقهرمانی، بابک.(۱۳۹۵).«نقش نهادهای بین‌المللی در قاعده‌مند سازی فضای سایبر»، کنفرانس ملی پدافندغیرعامل در قلمرو فضای سایبر، دانشگاه آزاد اسلامی واحد مراغه، ص۷۹-۷۲
- کتانچی، الناز و ذاکری، رضا .(۱۳۹۸). «شیوه‌های مقابله حقوقی با حملات سایبری در حقوق بین‌الملل»، مجموعه مقالات دومین کنفرانس ملی پدافند سایبری، آذربایجان شرقی، دانشگاه آزاد اسلامی واحد مراغه، صص ۶۲۰-۶۱۱
- ظفری، ایوب و فروغی‌نیا، سعید و باوند، موسی .(۱۳۹۹). «تأثیر فضای سایبری بر منافع ملی جمهوری اسلامی ایران از منظر جنگ نرم»، فصلنامه دانش انتظامی بوشهر، سال یازدهم، شماره ۴۱، صص۱۰۶-۸۰
- کتانچی، الناز و پور قهرمانی، بابک .(۱۴۰۰). «چالش‌های امنیتِ سایبری در کشورهایِ فصلنامه مطالعات بین‌المللی»، سال ۱۸، شماره ۱ (۶۹)
- کریانگ ساک، کیتی چایساری .(۱۴۰۰). حقوق بین‌الملل عمومی فضای مجازی، ترجمه: صادقی، حسین و همکاران، تهران، انتشارات حقوق‌یار.
- کیان‌خواه، احسان و علوی وفا، سعید.(۱۳۹۰). «مفهوم شناسی امنیت سایبری»، مجموعه مقالات نخستین همایش ملی دفاع –سایبری، تهران، پژوهشکده فناوری اطلاعات و ارتباطات جهاد دانشگاهی، صص۷-۱
- منفرد، محبوبه، جلالی فراهانی، امیرحسین.(۱۳۹۱). «کدهای رفتاری و پیشگیری از بزهکاری»، پژوهشنامه حقوق کیفری، سال سوم، شماره ۲، صص ۱۳۴-۱۰۵
- محمود زاده، ابراهیم و نیک‌نفس، علی و مهدی قوچانی، مهدی.(۱۳۹۶). «اولویت‌بندی راهبردهای توسعه سامانه‌ی فرماندهی و کنترل (C41) فضای سایبر کشور»، فصلنامه علمی پژوهشی مطالعات بین‌رشته‌ای دانش راهبردی، سال هفتم، شماره ۲۷، صص ۲۴۸-۲۲۹.
- محمود زاده، ابراهیم و اسماعیلی، کیوان.(۱۳۹۷). «الگوی راهبردی صیانت امنیتی فضای سایبر نیروهای مسلح»، فصلنامه امنیت ملی، سال هشتم، شماره سی، صص ۲۳۷-۲۰۳
- نجفی ابرندآبادی، علی حسین،۱۳۹۶، سیاست جنایی، مدخل در: دانشنامه علوم جنایی اقتصادی، به کوشش امیرحسن نیازپور، تهران: میزان، چاپ اول.
- ناظمی، میثم، ۱۳۹۸، سپر امنیتی شبکه ملی اطلاعات، نشریه تخصصی امنیت سایبری مرکز آپا دانشگاه کردستان، شماره چهارم، ۶۰-۵۸
- نظری، سیدغنی و جعفرزاده، سیامک و نیک‌خواه‌سرنقی، رضا.(۱۴۰۰). «نقش سیاست جنایی مشارکتی در پیشگیری از جرائم سایبری در ایران»، پژوهش‌های سیاسی جهان اسلام، انجمن مطالعات جهان اسلام، سال یازدهم، شماره چهارم، صص۱۷۴-۱۵۱
- نصرالله، سلطانی.(۱۳۹۶).به‌سوی کنوانسیون سایبری: جریان‌شناسی هنجارها و پایش روندها، جلد یک، انتشارات سپند قلم.
- نامدار، سعید.(۱۳۹۸). حملات سایبری و حقوق بین‌الملل عمومی، تهران: موسسه آموزشی و تحقیقاتی صنایع دفاعی
- وامالا، فردریک.(۱۳۹۶).سند راهنمای اتحادیه بین‌الملل مخابرات در حوزه راهبرد ملی امنیت سایبری، ترجمه: مرتضی واحدی و علی‌اصغر حقیری، انتشارات مؤسسه آموزشی و تحقیقاتی صنایع دفاعی، تهران.
- وطنی، امیر و اسدی، حمید.(۱۳۹۵). «سیاست جنایی جمهوری اسلامی ایران در جرائم سایبری با تأکید بر ویژگی‌های خاص این جرائم»، پژوهشنامه حقوق اسلامی، سال هفدهم، شماره اول، صص۱۲۶-۹۹
- هاتف، مهدی.(۱۳۸۸). «چالش ها و چشم اندازهای امنیت در فضای مجازی» ،دوماهنامه توسعه انسانی پلیس، سال ششم، شماره ۲،صص۱۷۷-۹۳

- Brunot, R. (2018). United Nations Security Council Background Guide, at: http://www.ccwa.org/wp-content/uploads/2018/09/UNSC-Final.pdf:1-11
- Christopher C. Joyner &Catherine Lotrionte, "information warfare as international coercion: Elements of a legal framework?" European Journal of international law, Vol.12 2001: 863-864
- Eriksson, J. G, Giacomello. 2006. The Information Revolution. Security, and International Relations: (IR). Relevant Theory. 27 (3), P224.
- German Government. (2011). ***National cyber security strategy, Cyber Securit Strategy for Germany Federal Ministry of interior.***
- James A. Lewis و Katrina Timlin. (2011). Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization. Center forStrategic and International Studies .
- Manuel Valls. (2015). French ***National Digital Security Strategy***. French Government.
- Commonwealth of Australia. (2009). ***National Cyber Security Strategy Australian Government.***
- Global-cybersecurityindex. aspx (accessed .08 /05/2020
- Lennard G. Kruger Internet Governance and the Domain Name System: Issuse for Congress November 18, 2016. P.۱
- Taniar, David (2008). Data Mining and Knowledge Discovery Technologies, UK and USA, IGI Publishing
- AFRICAN UNION. 2014. AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION. AFRICAN UNION.