امنیت سایبری در چشم‌انداز ۱۴۰۴:
چالش‌ها و راهکارهای حقوقی رویارویی با بزه‌های امنیتی سایبری

حسن عالی پور

استادیار دانشگاه شهرکرد و همکار علمی پژوهشکده مطالعات راهبردی

Hassan.alipour@gmail.com

چکیده

امنیت سایبری یکی از دسته‌های بندی‌های امنیت بر پایه فضای سایبری است که در چهره درون‌سایبری بر دو دسته امنیت اطلاعات و امنیت سامانه و شبکه و در چهره برون‌سایبری بر سه دسته امنیت کاربران و مشترکین (امنیت فردی)، امنیت زیرساخت‌های نهادهای عمومی (امنیت اجتماعی) و امنیت ملی است. پیوند میان امنیت ملی و فضای سایبر به ویژه با آغاز قرن بیست‌ویکم و رایانه‌ای شدن امور، شفاف‌تر شده که امنیت ملی در فضای سایبر منوط به امنیت اطلاعات است و در واقع تا زمانی که امنیت اطلاعات مخدوش نگردد، امنیت ملی نیز تهدید نمی‌شود. امنیت اطلاعات با سه سنجه بنیادین تبلور می‌یابد: نخست قابلیت اعتماد و رازداری تا به واسطه آن اطلاعات به صورت غیر مجاز افشا نشوند. با این معیار سعی در پیشگیری از دسترسی اشخاص ناصالح به اطلاعات می‌شود اعم از آنکه دسترسی برای خواندن اطلاعات باشد یا خواندن و نوشتن (برداشتن) آنها. دوم صحت و تمامیت تا از تغییر یا حذف غیر مجاز اطلاعات پیشگیری شود. سوم قابلیت دسترسی تا با تحقق این معیار، ممانعت غیرمجاز از دسترسی به اطلاعات و منابع آن پیش نیاید. غیر از این سه معیار ماهوی، باید پارامترهای قابلیت استناد (شناسایی قبلی طرفین مبادله)، قابلیت پاسخگویی (تعریف و اجرای مسئولیت‌های طرفین) و رد ناپذیری (اثبات اینکه اطلاعات به دریافت کننده واقعی ارسال شده) نیز مد نظر قرار بگیرد تا از حیث شکلی نیز پشتوانه امنیت اطلاعات تضمین گردد.

در سند چشم انداز ۱۴۰۴ از یک جامعه امن سخن به میان آمده که به جهت رایانه‌ای شدن کارها و برنامه ها، جامعه امن در فضای سایبر را نیز باید در سند چشم‌انداز دید و تامین کرد، همچنانکه در سیاست‌های کلان کشور برای رسیدن به هدف‌های سند چشم انداز، تامین امنیت فضای مجازی نیز پیش‌بینی شده است. این نوشتار در سه گام طولی به امنیت سایبری می‌پردازد: گام نخست شناخت ارزش یعنی همان امنیت سایبری است. گام دوم، شناخت تهدیدها بر ضد ارزش که همان بزه‌های سایبری است و گام سوم، شناخت راهکار پشتیبانی از ارزش است که همان تدبیرهای رویارویی با بزه‌های امنیتی سایبری است.

واژگان کلیدی: فضای سایبر، امنیت سایبری، بزه‌های سایبری، جاسوسی سایبری، تروریسم سایبری، افشای سایبری، سند چشم انداز ۱۴۰۴، تدبیرهای رویارویی

درآمد

جامعه امن به گونه‌ای که در افق ۱۴۰۴ نوید داده شده، جامعه‌ای است که در همه سپهرها و بخش‌های آن، تهدید یا خطری در میان نباشد. از این رو در سند چشم‌انداز بیست ساله، امنیت سایبری یک از مفهوم‌های کلیدی است. امنیت، استقلال و اقتدار به عنوان سه ویژگی برجسته نظام جمهوری اسلامی ایران در سال ۱۴۰۴ است که هر سه پیوند تنگاتنگی با امنیت سایبری برقرار می‌کنند. طبق سند چشم‌انداز، جامعه‌ی ایرانی در افق این چشم‌انداز چنین ویژگی‌هایی خواهد داشت: امن، مستقل و مقتدر با سامان دفاعی مبتنی بر بازدارندگی همه‌جانبه و پیوستگی مردم و حکومت. هرچند به جهت کلی و جهت‌ده بودن سند چشم‌انداز، به فضای سایبر و امنیت فضای تبادل اطلاعات اشاره نشده ولی در سنجه‌ها و راهبردهای سیاست‌های کلی نظام در دوره چشم انداز، به آن پرداخته شده است.

سیاست‌های کلی شبکه‌های اطلاع‌رسانی رایانه‌ای، بخشی از سیاست‌های کلانی است که بر پایه قانون اساسی جمهری اسلامی پیش‌بینی شده تا جامعه امن در فضای سایبر در افق ۱۴۰۴ را ترسیم کند. در این سیاست‌ها با درک فرصت‌ها و تهدیدهای روزافزون فضای سایبر، « *ایجاد، ساماندهی و تقویت نظام ملی اطلاع‌رسانی رایانه‌ای و اعمال تدابیر و نظارت‌های لازم به منظور صیانت از امنیت سیاسی، فرهنگی، اقتصادی، اجتماعی* » از یک سو و « *جلوگیری از جنبه‌ها و پیامدهای منفی شبکه‌های اطلاع‌رسانی* » از سوی دیگر پیش‌بینی شده است. در بخشی دیگر با رویکردی پیشگیرانه به « *ایجاد دسترسی به شبکه‌های اطلاع‌رسانی جهانی صرفاً از طریق نهادها و مؤسسات مجاز*» پرداخته شده تا دسترسی‌ها به فضای سایبر ضابطه‌مند شود. از همه برجسته‌تر، پیش‌بینی سیاست کلان رویارویی به تهدیدهای برجسته سایبری از رهگذر «*ایجاد و تقویت نظام حقوقی و قضایی متناسب با توسعه شبکه‌های اطلاع‌رسانی به ویژه در جهت مقابله کارآمد با جرائم سازمان‌یافته الکترونیکی*» است.

گذارندگان سیاست‌های کلان در حوزه اطلاع رسانی رایانه‌ای با چهره جهانی و فراگیر فضای سایبر آشنایی داشته و از این رو دانسته‌اند که پیش‌بینی سیاست‌های کلان برای دست یافتن به امنیت سایبری، مگر با اندیشه و برنامه فراملی شدنی نیست. بنابراین « *اقدام مناسب برای دستیابی به میثاق‌ها و مقررات بین‌المللی و ایجاد اتحادیه‌های اطلاع‌رسانی با سایر کشورها به ویژه کشورهای اسلامی به منظور ایجاد توازن در عرصه اطلاع‌رسانی بین‌المللی و حفظ و صیانت از هویت و فرهنگ ملی و مقابله با سلطه جهانی* » را به عنوان یکی از شیوه‌های بنیادین در کنار برنامه‌ها و تدبیرهای درون سرزمینی دانسته اند.

فضای سایبر یا فناوری اطلاعات به جهت اینکه پدیده‌ای نو است و دگرگونی‌های بسیاری در همه بخش‌های زندگی فردی و اجتماعی پدید آورده است، جایگاهی شکننده و ناپایدار داشت و شاید پیش‌بینی سیاست‌های کلان در این حوزه در کنار حوزه‌های شناخته شده دیگر، می‌توانست همراه با گمان و اندیشه باشد. با این حال در سیاست‌های کلان در حوزه اطلاع‌رسانی رایانه‌ای به درستی بر دو ویژگی بنیادین فضای سایبر دست گذاشته شده است. نخست آنکه فضای سایبر، سپهر گردش اطلاعات و جایگاهی برای دست یافتن به زندگی بهتر و پیشرفته تر است و به همین صورت امنیت سایبری یک ارزش بنیادین در این راه است. پس فضای سایبر و اینترنت یک تهدید یا دشمن نیست هرچند می-تواند همراه با تهدیدهایی نیز باشد. دوم آنکه فضای سایبر، سپهری جهانی است که نه تنها باید برای ضابطه‌مندی آن با کشورهای دیگر همکاری کرد بلکه باید نسبت به آن همان سیاست‌هایی دنبال شود که بیشتر کشورها دنبال می‌کنند تا بتوان در این همکاری جهانی دستی داشت.

در سنجش میان دو مفهوم امنیت سایبری و دفاع سایبری، امنیت سایبری ارزش و هدف است و دفاع سایبری شیوه و برنامه. دفاع سایبری، برنامه‌های پدافندی نرم در برابر تهدیدهای سایبری است ولی امنیت سایبری حالتی است که در آن تهدیدی نباشد. از این رو امنیت سایبری یک مفهوم ارزشی و همیشگی است ولی دفاع سایبری یک مفهوم سیاسی و چندگاهه است که گاه از آن برداشت-های ناروا نیز صورت می‌گیرد. در این نوشتار به جای پرداختن به دفاع سایبری که جایگاه حقوقی نااستوار و پوشیده‌ای دارد، به امنیت سایبری پرداخته می‌شود. با این حال امنیت سایبری نیز تنها از دریچه حقوقی نگریسته می‌شود که در زیر آن به طور طولی به سه جستار پرداخته می‌شود. نخست شناخت ارزش و پس از آن تهدیدهای ضد این ارزش و در گام پایانی پیش‌بینی تدبیرهایی برای پشتیبانی از ارزش یعنی امنیت سایبری.

الف: شناخت ارزش: امنیت سایبری

امنیت، نبودِ تهدید روانی و جسمی برای فرد و جامعه است. اگر آزادی، ندای انسان در درازی چند سده گذشته است، می‌توان گفت امنیت خواستِ همسان انسان و حیوان در همه زمان‌ها و مکان‌ها بوده است. امنیت‌خواهی بر پایه سرشت انسان است و جدا از اینکه امنیت، بایسته‌ی زندگی باهمادی یا بنیاد گرفتن دولت است، ولی از همان آغاز آفرینش، همواره از آرزوهای آدمیان بوده است. اما وقتی "امنیت " به درون جامعه می‌آید، معنای پیشرفته-تری می‌یابد؛ زیرا از جهت فردی، امنیت، دربردارنده پاسداشتن حقوق و آزادی‌ها و امنیت انسانی در فراهم ساختن زمینه‌های بایای(لازم) بهداشت و سلامت انسان است، ولی از جهت اجتماعی در دید ولفرز، *« امنیت در معنای عینی، فقدان تهدید در برابر ارزش‌های کسب شده را مشخص کرده و در معنای ذهنی، فقدان ترس و وحشت از حمله علیه ارزشها را معین می‌کند.»[۳]* در اینجا پای امنیت ملی و امنیت بین‌المللی برای نگهداری از این ارزشها نیز به میان می‌آید.

در معنای امروزین امنیت، از امنیتِ وابستگی‌های زندگی انسان که چیزهای بی‌جان هستند، نیز سخن به میان می‌آید؛ مانند امنیت پول، امنیت فضای سایبر و امنیت شبکه ارتباطات؛ چه « *ایده امنیت را برای اشیا راحت از افراد می‌توان بکار برد. برای نمونه، امنیت پول در بانک تابع محاسبات مربوط به تهدیدات خاصی از لحاظ تغییر محل غیر مجاز آن یا احتمال اثرات تورم بر ارزش است. اما امنیت افراد را نمی توان به سادگی تعریف کرد. عواملی مثل حیات، ثروت، موقعیت اجتماعی، سلامتی و آزادی بسیار پیچیده هستند و بسیاری از آنها در صورت از دست رفتن، غیر قابل جایگزین‌اند.*»[۱]

پیوند میان امنیت ملی و فضای سایبر به ویژه با آغاز قرن بیست و یکم و رایانه‌ای شدن امور، شفاف‌تر شده است. امنیت ملی در فضای سایبر منوط به امنیت اطلاعات است و در واقع تا زمانی که امنیت اطلاعات مخدوش نگردد، امنیت ملی نیز تهدید نمی شود. امنیت اطلاعات با سه معیار اساسی تبلور می‌یابد:[۱۴] نخست قابلیت اعتماد و رازداری[1] تا بواسطه آن اطلاعات به صورت غیرمجاز افشا نشوند. با این معیار سعی در پیشگیری از دسترسی اشخاص ناصالح به اطلاعات می‌شود اعم از آنکه دسترسی برای خواندن اطلاعات باشد یا خواندن و نوشتن (برداشتن) آنها. دوم صحت و تمامیت تا از تغییر یا حذف غیر مجاز اطلاعات پیشگیری شود. سوم قابلیت دسترسی تا با تحقق این معیار، ممانعت غیرمجاز از دسترسی به اطلاعات و منابع آن پیش نیاید. غیر از این سه معیار ماهوی، باید پارامترهای قابلیت استناد (شناسایی قبلی طرفینی که به مبادله داده می‌پردازند.)، قابلیت پاسخگویی (تعریف و اجرای مسوولیت‌های طرفین) و ردناپذیری (اثبات اینکه اطلاعات به دریافت کننده ارسال شده و ارسال کننده همان شخص است که ارسال کرده است.) نیز مد نظر قرار بگیرد تا از حیث شکلی نیز پشتوانه امنیت اطلاعات تضمین گردد.

امنیت فضای سایبر یکی از مقوله‌های بسیار مهم فناوری اطلاعات است که در آن هم امنیت داده و سیستم از طریق تدابیری چون باروی آتشین مورد توجه قرار می‌گیرد و هم امنیت کاربران و مشترکین از طریق پالایش اطلاعات مضر یا مستهجن. در این میان امنیت ملی در طول امنیت فضای سایبر قرار می‌گیرد؛ زیرا از یک طرف معیار محرمانگی و قابلیت اعتماد موجب بستن روزنه بزه‌هایی مانند جاسوسی رایانه‌ای و معیار تمامیت داده و سیستم یا قابلیت دسترسی به آنها باعث کاهش وقوع اقدامات تروریستی می‌گردد و از سوی دیگر اقدامات پیشگیرانه‌ای همچون باروی آتشین موجب امنیت داده‌ها و سیستم‌های حیاتی و حساس می-گردد. حتی پالایش نیز جلوی گردش اطلاعاتی همچون تبلیغ ضد نظام یا آموزش ارتکاب بزه‌های ضد امنیت را مسدود می‌کند.

ارتباط فضای سایبر و امنیت ملی از جهت مثبت و منفی قابل توجه است: ارتباط مثبت بین آنها در نتیجه طبیعی کارکرد فناوری اطلاعات است. فناوری اطلاعات با نزدیک ساختن مکانها و کوتاه کردن زمان ها و با امکانات خارق العاده‌ای که به دولتها تقدیم کرده، روش‌های نوین پاسداری از امنیت ملی را از طریق خبرگیری هم در سطح بین المللی و هم در سطح داخلی پیش رو قرار داده است. دولتها هرچند هنوز از نزدیک ساختن اطلاعات سری به ساحت اینترنت احتراز می‌کنند اما ناگزیر از رایانه‌ای کردن آنها هستند و این خود علی رغم تهدیدات، زمینه مناسب پردازش سریع اطلاعات و تبادل آنها را فراهم و کسب اطلاع از دیگران و یا اطلاع‌رسانی به دیگران را تقویت می‌کند.

فناوری اطلاعات برای تامین امنیت ملی کارکردهایی فراتر از اطلاع رسانی دارد. برخی از دولتها با استفاده از تکنیک پنهان

1-Confidentiality

نگاری[1] در محیط رایانه سعی در حفظ اطلاعات مرتبط با امنیت ملی نموده اند. رمزنگاری تکنیک کد گذاری اطلاعات در حین انتقال آنهاست تا احتیاطات لازم برای عدم دسترسی به آنها فراهم شود. در ابتدا این شیوه توسط آژانس امنیت ملی آمریکا برای محافظت از اطلاعات امنیت ملی فراهم گردید اما در ادامه طبق دستور العمل تصمیم‌گیری در مورد امنیت ملی مشهور به ان اس دی دی ۱۴۵ [2] آژانس با نام امنیت ملی یا حفاظت از داده‌های حساس مبادرت به کنترل رمز نگاری داده‌های اشخاص نمود بدون آنکه در طبقه بندی خاصی از داده‌های مورد کنترل ارایه دهد.[۱۱]

همین طور دولت‌ها از فناوری اطلاعات برای تامین امنیت داخلی نیز بهره برده و برای مبارزه با مجرمین و بزهکاران از طریق خبرگیری از آنها به کار می‌برند؛ به عنوان مثال در انگلستان نهادی به نام کنترل و نظارت مبتنی بر خبرگیری[3] تاسیس شده که به عنوان مدل سیاستگذاری در امور مربوط به اطلاعات معرفی شده و نخستین بار در سال ۲۰۰۰ با توجه به مدل خبرگیری ملی انگلستان و در ذیل آن ایجاد شد. [۱۵]در این مدل فرایندی سه مرحله‌ای برای تجزیه اطلاعات در راستای پیشگیری یا کاهش بزه‌های و مبارزه با باندهای جنایی پیش‌بینی شده است: مرحله نخست تفسیر و تحلیل محیط جنایی توسط مدیریت عالی خبرگیری، مرحله دوم معرفی اطلاعات کسب شده از سازمان‌های جنایی به مراجع تصمیم گیر و مرحله سوم اعمال تصمیمات مراجع مافوق جهت پیشگیری یا کاهش جرم. شبیه نهاد فوق به تدریج در سایر کشورها نظیر ایالات متحده، استرالیا و کانادا نیز تاسیس شد.

وجه ارتباط منفی میان امنیت ملی با فضای سایبر در تهدیدات یا رفتارهای مجرمانه سایبری ضد امنیت ملی است. فضای سایبر، محیطی امن و با امکانات برای ناقضان هنجارهای آن محسوب می‌شود و هر آنچه که ارتکابش در محیط بیرون مخاطره آمیز به نظر می‌رسد، در فضای سایبر راحت و پنهانی است. در این میان دولتها به دو صورت سعی در مقابله با این تهدیدات داشته اند: نخست پیش‌بینی برخی تکالیف، سختگیری‌ها و کنترل‌ها در قالب اقدامات پیشگیرانه تا حتی‌الامکان ضریب ارتکاب اقدامات مجرمانه ضد امنیت ملی کاهش یابد؛ به عنوان مثال در قانون تنظیم اختیارات بازرسی مصوب ۲۰۰۰ انگلستان به مقامات ارشد پلیس اجازه داده شده تا از ارایه دهندگان خدمات ارتباطی، افشای هرگونه ارتباطات داده تحت نظارت یا مالکیت آنها که ضرورتاً با امنیت ملی مرتبط است، بخواهند. طبق این قانون واژه داده ارتباطات اعم است از داده ترافیک و داده‌های مکانی.[۱۳]

بسیاری از سختگیری‌ها و نظارت‌ها در فضای سایبر به دلیل بستر پنهانی‌اش است. این فضا نه تنها قابلیت بسیار مناسبی برای اختفای مرتکب بزه‌های رایانه‌ای دارد بلکه تهدیدات نهانی در این فضا ضد امنیت ملی در مقایسه با محیط واقعی بیشتر است. رمز نگاری با وجود اینکه یک عمل فنی است یکی از مهمترین روشها برای جاسوس‌ها یا تروریست‌ها است تا با کمک آن مبادله داده و خبرگیری از اطلاعات مورد هدف است به گونه‌ای بسیاری از نویسندگان رمز نگاری دیجیتالی هم عرض خبرگیری دولتی منتها در خدمت مخالفان دولت یا ناقضان قانون تلقی کرده و آن را تهدیدی جدی ضد امنیت ارتباطات دانسته اند. [۷]

پنهان بودن جرم و پنهانی عمل کردن مرتکب آن باعث شده تا کشورهایی که زیرساخت‌های امنیت ملی آنها منوط به سلامت فضای تبادل اطلاعات است، سخت گیری‌هایی در راستای تحدید آزادی‌های فردی به ویژه ضد اتباع خارجی اعمال کرده اند. در ایالات متحده دو فرض ماهوی نسبت به مرتکبین ناشناخته ضد امنیت ملی مطرح شده است: فرض نخست این است که یک شخص یا سازمان در خارج از ایالات متحده یا یک شخص خارجی در داخل ایالات متحده تبعه این کشور محسوب نمی‌شود مگر اینکه با اطلاعات کافی خلاف آن ثابت شود. این فرض نسبت به عدم امکان شناسایی مرتکب و مکان ارتکاب وی می‌تواند سختگیری‌هایی نسبت به اتباع بیگانه به همراه داشته باشد. فرض دوم با توجه به مشکلات فرض نخست در تعیین خودی و غیر خودی، مبتنی است بر اینکه در حملات سایبری اقدام یک شخص که مرتکب دستیابی غیرمجاز به یک سیستم رایانه‌ای حساس شده، به عنوان یک رفتار مهم و حیاتی ضد اقتصاد و امنیت ملی ایالات متحده تلقی می‌شود و البته نسبت به شخصیت مرتکب نیز بنا بر خارجی بودن آن گذاشته می‌شود مگر اینکه خلافش ثابت گردد.[۱۲]

به هر حال واژه امنیت چه به عنوان موضوع و چه در جایگاه یک ویژگی برجسته برای فضای سایبر، بسیار پرکابرد است و از جهت

1-Cryptography
2-NSDD 145 (National security decision directive)
3- Intelligence led policing
4- National Intelligence Model

اندازه به کارگیری واژه دیگری با امنیت سایبری یا امنیت فناوری اطلاعات برابری نمی کند. از این رو گرایش بر پیشنهاد تعریف بسیار گسترده از امنیت سایبری هست. امنیت محیط سایبر عبارت است از فقدان هرگونه تجاوز یا هنجار شکنی یا تهدید به آن نسبت به یکی از پنج موضوع داده‌ها و اطلاعات، شبکه ها و سیستمهای رایانه‌ای و مخابراتی، کاربران و مشترکین اینترنتی، ارایه دهندگان خدمات اینترنتی و نهایتاً موضوعات بیرون از محیط سایبر که مرتکب با واسطه محیط سایبر در صدد تجاوز به آنها بر می‌آید.

در باب تامین امنیت محیط سایبر در قالب طرح مباحث فنی دایره تدابیر تامینی عمدتا محدود به مقولاتی چون مقابله با هکر و کراکرها و اتخاذ فیلترینگ و نصب باروی آتشین یا سایر می‌شود که اساس این وظیفه خطیر بر عهده ارایه دهندگان خدمات اینترنتی قرار می‌گیرد.

از منظر حقوقی امنیت سایبری در دو مفهوم مضیق و موسع به کار می‌رود. در مفهوم مضیق منظور اتخاذ تدابیر فنی و پیشگیرانه برای تامین امنیت شبکه ها و اطلاعات است. در این مفهوم اقدامات غیر فنی جایگاهی نداشته و اشخاص موضوع مستقیم تدابیر امنیتی نیست همچنانکه تامین امنیت فراتر از محیط سایبر را در بر نمی گیرد. این مفهوم منطبق بر امنیتی است که اهل فن در علوم رایانه و اینترنت آن را طراحی و تبیین می‌کنند. اما در مفهوم موسع دو قسم از تدابیر را برای تامین امنیت در محیط سایبر می‌توان سراغ گرفت:

الف) تدابیر مستقیم یا اصلی: این تدابیر به کلیه تدابیر فنی و قانونی گفته می‌شود که برای تامین امنیت چهار موضوع زیر به کار آید: یکم: *داده ها و اطلاعات رایانه ای*: داده و اطلاعات رایانه‌ای خمیر مایه فضای تبادل اطلاعات است که در محیط سایبر به هر دستاویزی از قبیل اتصال به اینترنت، ماهواره، امواج مغناطیسی قابل انتقال اند. داده از مرحله ورودی یا تولید تا ذخیره و انتشار و مورد استفاده قرار گرفتن در معرض انواع رفتارهای مخرب و مختل کننده است که از جمله این رفتار ها که امنیت داده را با خطر مواجه می‌سازد انتشار ویروس و سایر نرم افزارهای مضر، هک، کرک، شنود، تخریب، جعل و غیره است. دوم: *سیستم‌های و شبکه‌های رایانه‌ای و مخابراتی*: سیستم مجموعه‌ای متشکل از نرم افزار و سخت افزار است که برای پردازش اتوماتیک داده‌های دیجیتالی تهیه شده و ممکن است شامل ورودی و خروجی تسهیلات ذخیره اطلاعات باشد. سیستم ممکن است تنها یا به شبکه‌ای از دیگر وسایل مشابه متصل باشد. شبکه رایانه‌ای به رایانه‌های متصل به اطلاق می‌شود که فارغ از محلی یا عمومی بودن در آن مبادله اطلاعات صورت می‌گیرد. سیستم و شبکه نیز همچون داده آسیب پذیر بوده و از آنجا که با موجودیت داده معنا می‌یابند اقداماتی نظیر انتشار ویروس، اختلال در کارکرد و بازدهی، ممانعت از ترافیک و دسترسی داده و غیره امنیت آنها را به شدت تهدید می‌کند و از این رو برای سلامت و امنیت داده و سیستم اقدامات پیشگیرانه‌ای نظیر باروی آتشین، نصب گذرواژه و غیره مورد تاکید قرار می‌گیرد.

ب) تدابیر واسطه‌ای: این تدابیر در پی تنظیم مقررات مناسب برای فضای سایبر است تا به واسطه آن هدف اصلی یعنی امنیت فضای واقعی تامین شود. با رایانه‌ای شدن امور، از یک سو بسیاری از اطلاعات وزارتخانه ها، سازمانها و شرکتها در محیط سایبر قرار گرفته و از سوی دیگر فعالیت این نهادها نیز با محیط سایبر ارتباط تنگاتنگ یافته است. به عنوان مثال امنیت هواپیمایی، امنیت بیماران بیمارستانها، امنیت موسسات ارایه دهنده خدمات عمومی مثل برق، تلفن،آب و غیره جز در خاطر آسوده بودن از سلامت و امنیت محیط سایبر و رایانه و اینترنت نیست.

با این وصف امنیت جامعه پیوند محکمی با امنیت فضای سایبر دارد؛ با رسوخ حیرت انگیز و اجتناب ناپذیر رایانه و اینترنت در جامعه ما از هم اکنون باید به سرعت اقدامات قانونگذاری با توجه به تهدیدها از یک سو و ظرفیتهای موجود از سوی دیگر تحقق یابد. زیرا برای امنیت سایبر باید دست به اقدامات پیشگیرانه زد نه اقدامات چاره ساز. این تدابیر هم باید ناظر به امنیت خود فضای سایبر باشد و هم امنیت فیزیکی که مرتبط با کارکرد محیط سایبر است.

ب: شناخت ضد ارزش: تهدیدهای سایبری امنیتی

تهدید سایبری از جهت مفهومی و مصداقی از بزه‌های سایبری گسترده‌تر است و هر کنشی را در بر می‌گیرد که امنیت سایبری را از میان بردارد یا یا در آستانه آن قرار دهد. با این حال از نگاه قانونی، امنیت ملی و پیرو آن امنیت‌های زیردست آن هنگامی تهدید می‌شوند که دو مقوله جنگ یا بزه در میان باشد و بیرون از

این دو عنوان، هیچ سنجه‌ای نیست تا بتوان بر پایه آن تهدید امنیتی را بازشناخت. با این حال از نگاه سیاسی، تهدیدهای امنیتی تنها در بزه و جنگ نمود نمی‌یابند و بسیار پیرو برداشت سیاستمداران یک کشور است و چه بسا با رویکرد قانونی رویارویی کند. در اینجا رویکرد سیاسی و نیز برداشت‌های فرمانروایان در بنیادگیری مفهوم تهدید امنیتی و گستره آن بسیار تاثیرگذار است و از این رو از سنجه‌های ثابت و پذیرفتنی به دور اند. ولی تهدیدهای سایبری امنیتی با رویکرد قانونی و حقوقی، بیرون از دو حالت بزه و جنگ نیستند و هر کنش یا برنامه‌ای که در دل این دو مفهوم جای نگیرد، تهدید نبوده و انجامش آزاد است. واژه جنگ در فضای سایبر هنوز ساختار و پیکره حقوقی نیافته و تعبیرهای جنگ نرم، جنگ سایبری، دفاع سایبری یا چهره حقوقی ندارند یا بسیار چالش‌پذیراند و درباره آنها باید چندین سال به دور از هیاهو و ادعاهای سیاسی و شخصی بی‌پایه و بنیان، جستارهای فلسفی و حقوقی را پیش کشید تا واژه آفند سایبری و پیرو آن پدافند سایبری در ادبیات حقوقی کشور جای بگیرد. با این حال واژه " بزه سایبری" این چالش را ندارد و با روی آوردن به قانون‌های کیفری کنونی می‌توان چهره حقوق کیفری به تهدیدهای سایبری امنیتی نگریست. روی‌هم‌رفته می‌توان سه تهدید برجسته امنیتی را که در قانون‌های کیفری ایران جه به طور روشن و چه به طور پوشیده، عنوان مجرمانه یافته‌اند، شماره کرد که عبارتند از: جاسوسی سایبری، افشای سایبری و تروریسم سایبری. باید گفت این سه عنوان به جهت پیوند مستقیم با امنیت اطلاعات یا سامانه پیش کشیده می‌شوند وگرنه فضای سایبر، بستر انجام دیگر بزه‌های رایانه‌ای امنیتی مانند تهدید به بمب گذاری یا فعالیت تبلیغی بر ضد نظام و تحریک به کشتار نیز است ولی چون نسبت به چنین بزه هایی، فضای سایبر نقشی بیشتر از افزار یا بستر بزه ندارد، همان جستارهای سنتی درباره بزه‌های ضد امنیت نیز مطرح می‌شود:

۱-جاسوسی سایبری

در فراگیری جاسوسی، پیش از هرچیز، دانستن چیستی و فرآیند تحقق آن است. جاسوسی همچون پولشویی به گونه‌ای فرآیندوار رخ می‌دهد که انجام رفتارهای آن گام به گام در پس هم می‌آیند. روی هم رفته جاسوسی سنتی در سه گام نمود می‌یابد: گام نخست ورود یا دسترسی به مکان یا موضعی است که اطلاعات طبقه بندی شده در آن جای گرفته اند. گام دوم دسترسی به اطلاعاتی است که در مکان یا موضع مربوطه جای گرفته است و گام سوم در دسترس قرار دادن اطلاعات یا افشای آنها به دولتها یا کسانی است که شایستگی دسترسی به اطلاعات یا آگاه شدن به درون مایه آنها را ندارند. (این گام‌های سه‌گانه به گونه‌ای در ماده‌های ۵۰۳، ۵۰۵ و ۵۰۱ قانون مجازات اسلامی بازتاب یافته اند.)

در قانون جرایم رایانه‌ای نیز گام‌های سه گانه پیش گفته را می‌توان به شرح زیر دید: گام نخست، دسترسی به سامانه‌های رایانه‌ای و مخابراتی که داده‌های سری در آنها انباشت یا نگهداری می‌شوند (ماده ۴ قانون جرایم رایانه‌ای یا همان ماده ۷۳۲ قانون مجازات اسلامی) گام دوم، دسترسی به داده‌های سری یا تحصیل یا شنود آنها (بند الف ماده ۳ ق.ج.ر یا ماده ۷۳۱ ق.م.ا) و گام سوم در دسترس قرار دادن کسانی که شایستگی آگاهی از محتوای داده‌های سری را ندارند (بند ب ماده ۷۳۱ ق.م.ا) و یا در دسترس قرار دادن داده‌های سری یا افشای آنها به دولت یا نهادهای بیگانه یا عاملان آنها.(بند ج ماده ۷۳۱ ق.م.ا).

در گام‌های پیش‌گفته، دسترسی به سامانه‌های دربردارنده داده‌ها (گام نخست) و نیز دسترسی به خود داده‌های سری(گام دوم) در اصل همان بزه دسترسی غیرمجاز هستند که در گام دوم، شنود به دسترسی یا تحصیل نیز افزوده شده است. از این رو پیکره اصلی جاسوسی رایانه‌ای، دو بزه دسترسی غیرمجاز و شنود غیرمجاز است که با توجه به برخی ویژگی‌ها از این پدیده جدا می‌گردند؛ به سخن دیگر با شرط موضوع بزه یعنی داده‌های سری، جاسوسی رایانه‌ای از دسترسی غیرمجاز و نیز شنود غیرمجاز جدا می‌شود و دیگر میان این بزه ها تعدد مادی یا معنوی برقرار نمی-شود.

در کنار فرآیند سه مرحله‌ای پیش گفته، قانونگذار بزه دیگری به عنوان فراهم آوردن موجب دسترسی کسان ناشایست به داده‌های سری پیش بینی کرده است که این بزه غیر عمدی است. بدین ترتیب با توجه به پیش بینی کیفر به طور جداگانه در ماده‌های مبحث سوم قانون جرایم رایانه ای، پدیده جاسوسی رایانه‌ای بر پایه پنج رفتار جداگانه بنیاد می‌گیرد که هر یک بزه جداگانه به شمار می‌رود:

یکم، *نقض تدابیر امنیتی سامانه‌های رایانه‌ای و مخابراتی دربردارنده داده‌های سری*: نقض تدابیر امنیتی سامانه‌ها در ماده ۷۳۲ تکرار ماده ۷۲۹ قانون مجازات اسلامی است، با این حال دسترسی در اینجا با قصد خاص دسترسی به داده‌های سری و نسبت به سامانه‌هایی انجام می‌گیرد که داده‌های سری در آن نگهداری می‌شوند. رفتار پیش بینی شده در ماده ۷۳۲، نقض تدابیر امنیتی(که در زبان فنی هک گفته می‌شود) است که همان دسترسی غیرمجاز است. شیوه‌های دسترسی یا ورود به سامانه-های دارنده داده‌های سری بسیار گوناگون است. پخش ویروس و کرم‌های رایانه‌ای رخنه گر، نصب اسب‌های تروا که توانایی درون شدن به درهای پشتی[1] را دارد، بهره گیری از ضبط کننده کلیدهای گزینش شده[2](این نرم افزار به کاربر اجازه می‌دهد تا به اطلاعات محرمانه نوشته شده در دستگاه مانند گذرواژه و داده‌های خصوصی دست یابد)، گیرنده بسته‌ها[3] که توانایی بو کشیدن از بسته‌های در حال انتقال را دارد از جمله راه‌های رخنه به سامانه دیگری است. یکی از روش‌های رایج برای رخنه آن است که رایانامه یک کاربر شناخته شده را برای ویروس تعریف کرده و سپس آن را به نشانی کاربر می‌فرستد بدون آنکه فرستنده یا رخنه گر شناخته شود. این اقدام ممکن است از رهگذر اسپم یا پیام ناخواسته انجام شود که این اسپم ها دربردارنده ویروس‌های رخنه‌گر هستند. یکی دیگر از روش‌ها با نام باز کردن کیف رمزدار است که همانند کسی که رمز کیف اش را فراموش یا گم می‌کند با چینش شماره می‌کوشد به طور ناگهانی به شماره رمز دست یابد. برخی رخنه‌گران با حوصله از این روش برای یافتن نام کاربر، گذرواژه یا دیگر تدبیرهای حفاظتی که بیشتر به صورت رقم است، بهره می‌جویند. همسان با این روش، روش رقص موش است که رخنه گر با بازی با واژگان به کار گرفته برای نمونه در پرداخت و دریافت حساب‌های بانکی، به یکباره و به طور ناخواسته واژه گذری را یافته و به سامانه وارد می‌گردد.

دوم، *دسترسی به داده‌های سری یا تحصیل یا شنود آنها*: دسترسی، تحصیل و شنود همگی در یک معنا به کار برده می-شوند و آن دریافت اطلاعات است. از این رو ذکر این سه رفتار در کنار هم این خوبی را دارد که سبب تخصیص خوردن دسترسی غیرمجاز و شنود غیر مجاز می‌شود. در واقع هر جا موضوع دسترسی و شنود غیرمجاز، داده‌های سری باشند، رفتار مجرمانه از دایره این دو بزه بیرون آمده و در زیر جاسوسی قرار می‌گیرد. گفتنی است میان شنود غیرمجاز و دسترسی غیرمجاز به جهت رفتار، فرقی نیست و در هر دو، مرتکب به داده ها دسترسی می‌یابد و از این راه، محرمانگی آنها را از میان بر می‌دارد. فرق برجسته این دو بزه یکی در گونه داده‌ای است که مرتکب دریافت می‌دارد: در دسترسی، دریافت داده‌های ذخیره شده و در شنود، دریافت محتوای در حال انتقال و دیگری اینکه دسترسی هم نسبت به داده است و هم سامانه ولی شنود تنها نسبت به داده رخ می‌دهد.

سوم، *در دسترس قرار دادن داده‌های سری برای اشخاص فاقد صلاحیت*: در دسترس قرار دادن به معنای در اختیار گذاشتن داده ها در اختیار دیگری و یا آگاهاندن وی از محتوای آنهاست.

چهارم، *افشا یا در دسترس قرار دادن داده‌های سری برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آنها*: افشا به معنای بیان آشکاره و گسترده محتوای داده‌های سری است که این رفتار نسبت به اشخاص فاقد صلاحیت معنا ندارد و به همین دلیل این رفتار نسبت به دولتها یا گروه‌های بیگانه پیش بینی شده است. به سخن دیگر، در دسترس قرار دادن چهره فردی یا دست کم گروهی دارد و مرتکب، داده ها را در اختیار فرد یا کسان ویژه‌ای قرار می‌دهد ولی افشا، چهره همگانی داشته و مرتکب محتوای داده ها را نسبت به همه بازگو می‌کند که چون در این میان دولت ها یا گروه‌های بیگانه پیش و بیش از هر کس دیگر در پی اطلاعات اند، رفتار افشا نیز به واسطه آنها خطرناک می‌باشد.

چهار رفتار پیش‌گفته، همگی آنی‌اند و فرایندی دانستن جاسوسی به معنی به عادت یا مستمر شمردن آن نیست. از این رو همه رفتارهای پیش بینی شده در زیر پدیده جاسوسی به طور آنی رخ می‌دهند و نیز به طور جداگانه بزه به شمار می‌روند. پس اگر کسی در آغاز به قصد دسترسی به داده‌های سری به سامانه‌های مربوطه دسترسی یابد و سپس داده‌های سری را به دست آورد و در پایان آنها را در اختیار کسان ناشایست قرار دهد، سه بزه انجام داده که تعدد مادی از نوع مشابه خواهد بود؛ زیرا هرچند جنس رفتارها از هم جدا هستند ولی با نگاه قانون همه آنها جاسوسی هستند و مرتکب نیز سه بار جاسوسی انجام داده است.

1- Back doors
2- Key loggers
3- Packet sniffer

پنجم، *در دسترس قرار دادن غیرعمدی داده‌های سری برای اشخاص فاقد صلاحیت*: این رفتار هرچند به جهت ماهیت، همان در دسترس گذاری داده‌های سری است ولی این رفتار از روی عمد انجام نمی‌شود، به همین جهت قانونگذار از رفتار " موجب دسترسی شدن" یاد می‌کند. همسان با این بزه، تخلیه اطلاعاتی شدن است که در ماده ۵۰۶ قانون مجازات اسلامی به آن پرداخته شده است. طبق این ماده چنانچه مأمورین دولتی که مسئول امور حفاظتی و اطلاعاتی طبقه‌بندی شده می‌باشند و به آن‌ها آموزش لازم داده شده است در اثربی‌مبالاتی و عدم رعایت اصول حفاظتی توسط دشمنان تخلیه اطلاعاتی شوند به یک تا شش ماه حبس محکوم می‌شوند. با این حال میان بزه پیش بینی شده در ماده ۵۰۶ و ماده ۷۳۳ فرق هست. بزه موضوع ماده ۷۳۳ رایانه‌ای بوده و نسبت به داده‌های سری انباشت شده در سامانه ها است. برای این بزه یکی از دو شرط برخورداری از آموزش لازم یا در اختیار داشتن داده‌های رایانه‌ای بس خواهد بود ولی این دو شرط در ماده ۵۰۶ با هم هستند. همچنین در ماده ۵۰۶، مرتکب، مسئول امور حفاظتی و اطلاعاتی طبقه‌بندی است که با بودن یک جاسوس یا عامل خبرگیری، اطلاعات را از دست می‌دهد ولی بزه موضوع ماده ۷۳۳، با رفتارِ موجب دسترسی شدن رخ می‌دهد که با تخلیه اطلاعاتی فرق می‌کند و نیازی به وجود جاسوس یا عامل نیست. از این رو ماده ۷۳۳ بسیار عام تر از ماده ۵۰۶ است.

موضوع بزه جاسوسی رایانه ای، داده‌های سری هستند. طبق تبصره ۱ ماده ۷۳۱ قانون مجازات اسلامی، داده‌های سری داده‌هایی است که افشای آنها به امنیت کشور یا منافع ملی لطمه می‌زند. سری بودن، ویژگی اطلاعات دارای ارزش سیاسی است. دلیل پیش‌بینی جاسوسی رایانه‌ای در قانون جرایم رایانه‌ای و پیرو آن داده‌ها در قانون ماده پیش‌گفته، خاموشی قانون مجازات انتشار و افشای اسناد محرمانه و سری دولتی مصوب ۱۳۵۳ درباره داده-های سری است. این قانون به اسناد پرداخته و تعریفی که از آن به دست داده است، داده های دارای ارزش اطلاعاتی را در برنمی-گیرد. طبق ماده یک این قانون، اسناد دولتی عبارتند از هر نوع نوشته یا اطلاعات ثبت یا ضبط شده مربوط به وظایف و فعالیتهای وزارتخانه‌ها و مؤسسات دولتی و وابسته به به دولت و شرکتهای دولتی از قبیل مراسلات - دفاتر - پرونده - عکس‌ها - نقشه‌ها - کلیشه‌ها - نمودارها - فیلم‌ها - میکرو فیلم‌ها و نوارهای ضبط صوت که در مراجع مذکور تهیه و یا به آن رسیده باشد.

دلیل پیش‌بینی داده‌های سری نیز بیرون کردن داده‌های محرمانه از تنگنای پشتیبانی کیفری است؛ زیرا گستره داده‌های محرمانه به اندازه ای است که می‌توان هر اطلاعاتی را در زیر آن قرار داد و چون در رویه نیز، برچسب محرمانه بودن بدون نیاز و توجیه بر روی اسناد قرار می‌گیرد، در قانون جرایم رایانه ای به داده‌های سری بسنده شده است. داده‌های سری نیز با پشتوانه قانون مجازات انتشار و افشای اسناد محرمانه و سری تعریف شده است. بر پایه دنباله ماده یک این قانون، اسناد دولتی سری اسنادی است که افشای آنها مغایر با مصالح دولت و یا مملکت باشد. اسناد دولتی محرمانه اسنادی است که افشای آنها مغایر با مصالح خاص اداری سازمانهای مذکور در این ماده باشد.

هرچند آئین‌نامه طرز نگاهداری اسناد سری و محرمانه دولتی و طبقه‌بندی و نحوه مشخص کردن نوع اسناد و اطلاعات مصوب ۱۳۵۴/۱۰/۱ هیأت وزیران، بین اسناد سری و اسناد به کلی سری با توجه به ارایه طبقه‌بندی از اسناد سری و محرمانه دولتی در ماده یک این آئین‌نامه تفاوت قائل شده، اما در قانون مجازات انتشار و افشای اسناد محرمانه و سری دولتی مصوب ۱۳۵۳/۱۱/۲۹، اسناد دولتی سری اعم است از اسناد سری و به کلی سری و بر اساس همین قانون در این ماده، موضوع جرم، داده‌های سری است که اعم است از سری و بکلی سری.

موضوع بزه جاسوسی رایانه‌ای سبب جدایی این بزه از دیگر بزه-های رایانه‌ای می‌گردد. با این حال این خرده را نیز دارد که جاسوسی صنعتی و تجاری که از جاسوسی‌های شایع در فضای سایبر است، را در بر نمی‌گیرد. با این حال می‌توان گفت که نسبت به نظامیان، جاسوسی صنعتی پیش بینی شده است. بر پایه بند ج ماده ۲۴ قانون مجازات جرایم نیروهای مسلح مصوب ۱۳۸۲ هر نظامی که اسرار نظامی ، سیاسی ، امنیتی ، اقتصادی و یا صنعتی مربوط به نیروهای مسلح را به دشمنان داخلی یا خارجی یا بیگانگان یا منابع آنان تسلیم و یا آنان را از مفاد آن آگاه سازد جاسوس محسوب و به مجازات محارب محکوم خواهد شد. پیرو آن طبق ماده ۱۳۱ این قانون ... *همچنین اقداماتی از قبیل تسلیم اطلاعات طبقه‌بندی شده رایانه‌ای به دشمن یا افرادی که*

صلاحیت دسترسی به آن اطلاعات را ندارند... نیز دربردارنده جاسوسی صنعتی سایبری در کنار دیگر گونه‌های جاسوسی است.

۲- افشای سایبری

افشای اطلاعات طبقه‌بندی شده، با توجه قانون مجازات انتشار و افشای اسناد محرمانه و سری دولتی مصوب ۱۳۵۳/۱۱/۲۹ که هنوز نیروی اجرایی دارد، پدیده‌ای جدا از جاسوسی است. بر پایه ماده ۲ این قانون هر یک از کارکنان سازمانهای مذکور در ماده یک (وزارتخانه‌ها و موسسات دولتی و وابسته به به دولت و شرکتهای دولتی) که حسب وظیفه مامور حفظ اسناد سری و محرمانه دولتی بوده یا حسب وظیفه اسناد مزبور در اختیار او بوده و آنها را انتشار داده یا افشا نماید یا خارج از حدود وظایف اداری در اختیار دیگران قرار دهد یا به هر نحو، دیگران را از مفاد آنها مطلع سازد در مورد اسناد سری به حبس جنایی درجه ۲ از دو تا ده سال و در مورد اسناد محرمانه به حبس جنحه ای از شش ماه تا سه سال محکوم می‌شود همین مجازات حسب مورد مقرر است درباره کسانی که این اسناد را با علم و اطلاع از سری یا محرمانه بودن آن چاپ یا منتشر نموده و یا موجبات چاپ یا انتشار آن را فراهم نمایند. در صورتی که افشای مفاد اسناد مذکور در اثر عدم رعایت نظامات یا در اثر غفلت و مسامحه حفاظت آنها صورت گرفته باشد مجازات او سه ماه تا شش ماه حبس جنحه‌ای خواهد بود.

و طبق ماده ۳، هر یک از کارکنان سازمانهای مذکور در ماده ۱ یا اشخاص دیگر که اطلاعات یا مذاکرات یا تصمیمات سری و محرمانه دولتی را به نحوی از انحا به کسی‌که صلاحیت اطلاع بر آن را ندارد به دهد یا موجبات افشا یا انتشار آنها را فراهم نماید عمل مرتکب در حکم افشا یا انتشار اسناد سری یا محرمانه دولتی محسوب می‌شود.

دو ماده پیش‌گفته چهار حالت را برای احراز بزه افشای غیرمجاز اطلاعات طبقه‌بندی شده پیش‌بینی می‌کند. حالت نخست زمانی است که کارمند دولت حسب وظیفه مامور حفظ اسناد سری و محرمانه دولتی باشد؛ مانند کارمند مسوول پاسداری از اطلاعات. حالت دوم هنگامی است که کارمند دولت حسب وظیفه اسناد مزبور در اختیار او بوده است مانند رئیس بخشی‌که اسناد طبقه-بندی شده در آن نگهداری می‌شوند یا هر کسی‌که از جهت مقررات به بخش نگهداری اسناد رفت و آمد دارد، بی‌آنکه مسوول حفظ اسناد باشد. دو حالت پیش‌گفته در ماده ۲ قانون پیش بینی شده اند. حالت سوم دربردارنده هر کارمندی است که اطلاعات سری یا محرمانه را به کسان ناصالح بدهد یا موجبات افشا یا انتشار را فراهم سازد و حالت چهارم نسبت به کسان ناکارمند است که به وجه به تعبیر " یا اشخاص دیگر" که در ماده ۳ قانون پیش گفته آمده به همه کسان بار می‌شود. در حالت سوم و چهارم که قانونگذار از آنها به " در حکم افشا یا انتشار" یاد کرده با بزه جاسوسی هم پوشانی پدید می‌آید؛ زیرا در جایی‌که اطلاعات به امانت به دیگری سپرده نشده یا در اختیار وی نیست، رفتار جاسوسی پیش کشیده می‌شود؛ به سخن دیگر، جدایی بنیادین میان افشای غیرمجاز اطلاعات طبقه بندی شده و جاسوسی در همین ویژگی و سمتی است که مرتکب دارد. در بزه افشا مرتکب امین یا دارای اختیار دسترسی به اسناد است و نیازی به کاوش و جستجو برای اسناد ندارد ولی در جاسوسی مرتکب یک شخص بیگانه یا ناصالح است. بدین حال حالت سوم و چهارم با جاسوسی یکی می‌شوند و شاید از این روست که ماده ۶ قانون مجازات انتشار و افشای اسناد محرمانه و سری دولتی پیش‌بینی می‌کند که هرگاه انتشار یا افشای اسناد دولتی مذکور در این قانون متضمن جاسوسی یا جرایم دیگری باشد که رسیدگی به آن در صلاحیت دادگاههای نظامی است در دادگاههای مزبور رسیدگی خواهد شد. تعبیر " متضمن جاسوسی" یک بار دیگر در ماده ۵۰۱ قانون مجازات اسلامی آمده که می‌گوید: هرکس نقشه ها یا اسرار یا اسناد و تصمیمات راجع به سیاست داخی یا خارجی کشور را عالما" و عامدا" در اختیار افرادی که صلاحیت دسترسی به آنها را ندارند قرار دهد یا از مفادآن مطلع کند به نحوی که متضمن نوعی جاسوسی باشد ، نظر به کیفیات ومراتب به یک تا ده سال حبس محکوم می‌شود. پندار بیشینه بر این است که جاسوسی با خواست و قصد مرتکب شناخته می‌شود ولی درست آن است که بگوییم جاسوسی با افشای غیرمجاز اطلاعات طبقه بندی شده نه از جهت رکن روانی که از جهت رکن مادی تفاوت دارد. نخست اینکه جاسوسی چنانکه پیش از این گفتیم، یک بزه فرآیندی است و از سه گام ورود یا سرکشی، تحصیل یا شنود و افشا یا در اختیار گذاشتن اطلاعات بنیاد می‌گیرد که هر گام برای خود بزهی جداگانه است، در حالی که دو گام نخست در افشای غیرمجاز معنا ندارد؛ زیرا همچنانکه از عنوان این بزه بر می‌آید،

مرتکب تنها رفتار افشا یا انتشار را انجام می‌دهد؛ زیرا به جهت دسترسی پیشین به اطلاعات، دو گام نخست یعنی ورود به موضع های مربوطه یا تحصیل و شنود اطلاعات نمود نمی‌یابد. دوم اینکه از دید قانون سال ۵۳ چهار دسته از مرتکبین جاسوس نیستند و بلکه مرتکب افشای غیرمجاز اند: مامورین نگهدارنده اطلاعات، مامورین دارای اختیار در دسترسی به اطلاعات، همه کارمندان دولت به جهت رابطه عمومی امانت میان آنها و اموال و اطلاعات دولتی هرچند سپرده نشده باشد و سرانجام کسان دیگر یعنی همان‌هایی که به طور اتفاقی و یکباره به اطلاعات دست یابند بی-آنکه در پی آن باشند مانند یافتن اطلاعات. برای تعبیر " کسان دیگر" به جهت پدید آوردن پیوند میان آنها و کارمندان دولت، این برداشت بخردانه به نظر می‌آید و از نگاه در رویه دادگاهی بخش زیادی از اتهام‌های جاسوسی از ریشه افشای غیرمجاز اند و هرچند چالش دادگاه شایسته به رسیدگی پیش می‌آید ولی در هر حال بزه افشای غیرمجاز بزهی سبک‌تر از جاسوسی است؛ در حالی‌که رویه روشن و یکپارچه‌ای در دادگاه‌ها برای بازشناسی این دو بزه نیست.

بازشناسی افشای داده های سری در فضای سایبر از جاسوسی رایانه‌ای نیز چالش پذیر است. هرچند بر پایه ماده ۱۳۱ قانون مجازات جرایم نیروهای مسلح، افشاء غیرمجاز اطلاعات از جاسوسی اطلاعاتی جدا شده و پیرو آن این دو پدیده در این قانون تا اندازه‌ای از عنوان‌های سنتی خود یعنی افشای عمدی و غیر عمدی (ماده ۲۱ و ماده ۲۷) و جاسوسی (ماده ۲۴) پیروی می‌کنند ولی قانون جرایم رایانه‌ای رویکرد ناروشنی دارد. از یک سو می‌توان گفت که دو عنوان افشای غیرمجاز اطلاعات طبقه بندی شده و جاسوسی در این قانون یکی است و با توجه به پیش بینی نشدن عنوان " افشای غیرمجاز رایانه ای" در این قانون، به راستی قانونگذار خواسته تا این دو عنوان را یکی بداند ولی این دیدگاه درباره جایی‌که داده‌های سری به کارمندی سپرده شده یا در اختیار وی بوده، بخردانه نیست؛ زیرا چنین فردی اطلاعات را در اختیار دارد یا به وی سپرده شده است و در صورت افشا آنها، نمی توان به چنین فردی جاسوس گفت. از سوی دیگر می‌توان گفت که قانون جرایم رایانه‌ای تنها به جاسوسی و نیز افشای غیرعمدی اطلاعات (ماده ۷۳۳ ق.م.ا) پرداخته و چهار حالت پیش‌گفته برای جاسوسی و افشای غیرمجاز سنتی در اینجا نیز در جداسازی افشای عمدی سایبری و جاسوسی سایبری همچنان به کار می‌آید. پس اگر چهار حالت زیر پیش آید جاسوسی رایانه ای نیست بلکه افشای داده های سری است که همچنان مشمول قانون سال ۱۳۵۳ خواهد بود. حالت نخست جایی است که داده-های سری برای نگهداری به کارمندی سپرده شده است. حالت دوم جایی است که کارمند دولت، داده های سری را در اختیار داشته یا قانونا به آنها دسترسی دارد. حالت سوم همه کارمندان دولتی که به گونه ای به داده های سری یا سامانه ها دربردارنده این داده‌ها دست یابند و حالت چهارم کسی است که به طور ناگهانی و بدون کاوش و جستجو به داده های سری از رهگذر سامانه‌های رایانه ای و مخابراتی دست یابد.

گزینش یکی از دو دیدگاه پیش‌گفته، پیامدهای جداگانه‌ای به بار می‌آورد؛ هرچند بخردانه آن است که در فضای سایبر نیز میان جاسوسی و افشای داده سری نیز جدایی باشد ولی با مقرره‌های کیفری کنونی بهتر است با دستاویز ماده ۶ قانون سال ۱۳۵۳ که پیش بینی کرده است، اگر افشا یا انتشار جاسوسی به شمار آید پیرو مقرره‌های جاسوسی است، قانون جرایم رایانه ای را در مقام همسان سازی جاسوسی و افشای غیرمجاز بدانیم؛ زیرا یکی از جهت های بنیادین برای پیش‌بینی جاسوسی رایانه‌ای به جهت پیشینه‌مند و کاستی‌دار بودن قانون مجازات انتشار و افشای اسناد محرمانه و سری دولتی مصوب ۱۳۵۳ است که تعریف ارایه شده از اسناد دولتی سری و محرمانه در این قانون، داده‌های رایانه ای را در بر نمی‌گرفت. افزون بر این، ماده ۳ قانون جرایم رایانه ای به طور مطلق به پشتیبانی از داده های سری پرداخته است و چون هر یک از رفتارهای جاسوسی را به طور جداگانه بزه دانسته است، افشا یا انتشار هم در زیر آن جای می‌گیرد. طبق بند ج ماده ۳ قانون جرایم رایانه ای، افشاء یا در دسترس قرار دادن داده‌های سری برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آنها، سزاوار حبس از پنج تا پانزده سال است. از همه برجسته تر، قانون جرایم رایانه ای، چهار حالت پیشین برای احراز افشای اطلاعات طبقه‌بندی شده در برابر جاسوسی را دگرگون کرده است، زیرا در ماده ۲۶ برای بزه های رایانه‌ای موضوع قانون که جاسوسی رایانه‌ای یکی از آنها است، عامل‌های افزایش کیفر را پیش‌بینی کرده است که در بند الف به هر یک از کارمندان و کارکنان اداره‌ها و سازمانها یا شوراها و یا شهرداریها و موسسه‌ها و

شرکت‌های دولتی و یا وابسته به دولت یا نهادهای انقلابی و بنیادها و مؤسسه‌هایی که زیر نظر ولی‌فقیه اداره می‌شوند و دیوان محاسبات و مؤسسه‌هایی که با کمک مستمر دولت اداره می‌شوند و یا دارندگان پایه قضائی و به طور کلی اعضاء و کارکنان قوای سه‌گانه و همچنین نیروهای مسلح و مأموران به خدمت عمومی اعم از رسمی و غیررسمی به مناسبت انجام وظیفه مرتکب جرم رایانه‌ای شده باشند، پرداخته است. در اینجا مرتکب بر پایه صدر ماده ۲۶ حسب مورد مرتکب به بیش از دو سوم حداکثر یک یا دو مجازات مقرر محکوم خواهد شد. بنابراین از نگاه این قانون کارمند دولت خواه داده‌های سری در دستش امانی باشند خواه نباشند و خواه به آنها دسترسی داشته یا نداشته باشد، مشمول افزایش کیفر ماده ۲۶ می‌گردد و همین ماده به گونه‌ای به جای افشای غیرمجاز داده‌های سری از سوی کارمند دولت به جاسوسی از سوی وی گواهی داده است.

۳-تروریسم سایبری

اقدام تروریستی سایبری را بیشتر در زمره بزه‌های رایانه‌ای می‌دانند[۱۶] ، زیرا در بروز کنش تروریستی، همچون دیگر بزه-های رایانه‌ای، رایانه و اینترنت هم در نقش موضوع بزه نمود می-یابد و هم افزار آن. در نگاه دیگر، بسیاری از بزه‌های رایانه‌ای به ویژه دستیابی غیرمجاز و خراب‌کاری، خود شیوه‌های ارتکاب تروریسم سایبری به شمار می‌رود؛ زیرا تروریسم سایبری از رخنه-ی غیرمجاز به سیستم یا شبکه توسط خراب‌کاران رایانه‌ای می-آغازد و به اخلال در سیستم‌های حیاتی و زیرساخت‌های اطلاعاتی و حتی پیامدهای فاجعه باری چون یورش‌های شیمیایی، میکروبی و هسته‌ای می‌انجامد. این ادعا در پرتو این پرسش که « *چرا تبهکاران تروریسم رایانه‌ای (سایبر تروریسم) مرتکب جرایم رایانه-ای نمی‌شوند*»[۴] شفاف‌تر می‌شود و از همین جا روشن می‌گردد که تروریست‌های رایانه‌ای، بزهکارانی نیستند که بتوان ارتکاب بزه‌های رایانه‌ای را از آنها چشم داشت. از این رو برخی تروریسم سایبری را در زیر بزه‌های رایانه‌ای جا نمی‌دهند؛ چون « *بزه چهره شخصی داشته و به دلایل فردی و شخصی ارتکاب می‌یابد، ولی تروریسم جنبه سیاسی دارد و هرچند رفتارها و نشانه‌های آن با بزه جداناشدنی است ولی تنها با انگیزه‌های سیاسی ارتکاب می-یابد.*»[۸] ولی پیش از اینکه پیوند تروریسم سایبری با بزه رایانه-ای پیش آید، باید دانست هستیِ این گونه از تروریسم، خود گمان‌آور است؛ چه تروریست‌ها «*از اینترنت و رایانه برای تبلیغ و خبرپراکنی، گزینش نیروی انسانی، داده‌کاوی*[1] *و دیگر انگیزه‌ها بهره می‌جویند*»[۲۱] وگرنه اقدام‌های برجسته‌ی تروریستی که دربردارنده خشونت و از بین بردن است، در فضای سایبر شدنی نیست.

مرتکب تروریسم سایبری با انگیزه‌های پیوندیافته با باورهای سیاسی، مذهبی، میهن‌پرستانه و مانند آن به اخلال در سیستم‌ها و شبکه‌های رایانه‌ای می‌کوشد و از این رو بر وارونه‌ی بزهکار رایانه‌ای، اقدام‌های آشوبگر و اخلال‌کننده‌ی آنها از پیش تصمیم-گیری شده است. « *برعکسِ آنچه که بزهکار رایانه‌ای بزهش را پنهان نگه می‌دارد، تروریست رایانه‌ای افزون بر شناساندن خود، تلاش دارد خواسته‌های مذهبی، عقیدتی، سیاسی و اجتماعی خود را با پدید آوردن هراس در فضای سایبر یا از رهگذر آن پیش کشد.*»[۱۷]

واژه سایبر تروریسم از دهه هشتاد بر زبانها افتاد، ولی پیش از آن اقدام‌های تروریستی از رهگذر رایانه رخ داده و به دهه هفتاد بر می‌گردد؛ « *زمانی که بریگاد سرخ طی این دهه در ایتالیا ۱۱ عدد از تاسیسات اصلی پردازشگرهای ارتباطی را تخریب کردند. میزان خسارت وارده پانصد هزار دلار تخمین زده شد. این گروه طی انتشار بیانیه‌ای استفاده روز افزون از رایانه را بخشی از یک توطئه جهت بیشینه کردن نظارت‌های اجتماعی برشمردند. به نظر این گروه ، رایانه‌ها به مثابه ابزاری جهت درگیری‌های طبقاتی به شمار می‌رفتند و از این رو لازم بود تا این شبکه‌های نظارت مورد حمله قرار گرفته و از بین بروند.*»[۶]

به هر حال اقدام‌های تروریستی سایبری چهره نوین تروریسم است و بری کالین که گفته می‌شود واژه سایبر تروریسم را برای نخستین بار پیشنهاد داده، آن را این‌گونه تعریف کرده است: « *سوء استفاده عمدی از یک سیستم، شبکه یا مولفه اطلاعاتی رایانه ای برای تحقق هدفی که موید یا تسهیل کننده مبارزه یا اقدام تروریستی است.*»[۴] برخی از نویسندگان نشانه‌ها و نتیجه‌های بیرونیِ کنش‌های تروریستی در فضای سایبر را نیز در تعریف خود

1- Data mining

گنجانده اند؛ به گفته کانوی از نظریه‌پردازان آمریکایی در زمینه تهدیدهای سایبری، « *تروریسم سایبری عبارت است از یورش عمدی و آگاهانه با انگیزه‌های سیاسی به وسیله گروه‌های فروملی یا عامل‌های پنهانی برضد اطلاعات، سیستم‌های رایانه‌ای، برنامه‌های رایانه‌ای و داده، که منتهی به خشونت بر ضد کسان غیر نظامی و دیگر هدف‌ها شود.*»[۱۹]

انجام اقدام تروریستی بر ضد شبکه‌ها، سیستم‌ها و اطلاعات یا بهره‌گیری از فضای سایبر برای تروریسم در جهان فیزیکی، به چهار دلیل برای تروریست‌ها مهم است: « *پایین بودن هزینه‌های ارتکاب از فراهم ساختن رایانه گرفته تا طراحی برنامه های آماده سازی خدمات دروغین، دشواری در ردیابی یا دستگیری مرتکب، نبودِ رویارویی حضوری به دلیل نبود محدوده‌ای مشخص برای انجام اقدام تروریستی و دست‌آخر بودِ هدف‌ها و قربانیان گوناگون در یک زمان.*»[۱۸] از همین رو محدوده‌ی اقدام‌های تروریستی سایبری به اندازه‌ای گسترده است که رایانه در جهت ارتکاب آنها، هم نقش‌افزار را دارد و هم نقش هدف یا موضوع. رایانه زمانی افزار بزه است که تروریست‌ها از رهگذر آن مرام و هدف‌های خود را تبلیغ می‌کنند یا با کمک آن شیوه‌ی انجام اقدام‌های تروریستی را می‌آموزانند. در اینجا اقدام‌های تروریستی سنتی با کمک رایانه ارتکاب می‌یابد؛ برای نمونه « *عبدالله قریشی یکی از هواخواهان اسامه بن لادن، در سال ۲۰۰۰ گروه خادمان بن لادن(OLB) را در اروپا بنیاد نهاد که کار اصلی این گروه طراحی و راه انداختن پایگاه‌های اینترنتی برای آفرینش اطلاعاتی پیرامون ساخت جنگ‌افزار، افزارهای انفجاری دستی و نیز تبلیغ و آگاهی‌رسانی برای گروه القاعده بود.*»[۱۰]

رایانه هنگامی به عنوان موضوع یا هدف اقدام تروریستی مطرح می‌شود که اطلاعات یا سیستم‌ها یا شبکه‌ها در پی یورش مجازی تروریست‌ها دچار آشفتگی شده یا از میان بروند. اقدام‌های تروریستیِ سایبریِ محض، یعنی جایی‌که فضای سایبر خود موضوعِ مستقیم بزه است، ممکن است به صورت‌های گوناگونی انجام یابند. برجسته‌ترین روش، به نام *عامل تشدید کننده وضعیت(یا ضریب افزاینده نیرو[2])* است که کنش‌های تروریستی سایبری به دنبال اقدام‌های خرابکارانه سنتی انجام می‌شود؛ « *مانند یورش دیجیتالی به زیرساخت‌های ارتباطاتی حیاتی به دنبال یک بمب‌گذاری یا حمله شیمیایی.*»[۲۰] روش دیگر، هدف قرار دادنِ سیستم یا شبکه، ناتوان‌سازی از رهگذرِ پخش ویروس-ها، کرم‌ها یا دیگر نرم‌افزارهای پخش‌کننده در فضای سایبر است. مهمترین بخش از یورش‌های ویروسی از طریق پست‌های الکترونیکی آلوده انجام می‌گیرد که اندازه آنها روز به روز در حال افزایش است. کرم‌ها نیز همانند ویروس‌ها توانایی مختل کردن سیستم را دارا هستند؛ برای نمونه، « *کرم رایانه‌ای نیمدا که به دلیل تأثیرگذاری مخرب بالای آن و همچنین برخورداری از قابلیت‌های دیگر، مانند ویروس تروجان به کرم چهارسر معروف است. معروفیت این کرم رایانه‌ای بیشتر به زمان انتشار آن مربوط می‌شود که درست یک هفته پس از واقعه یازدهم سپتامبر ۲۰۰۱ منتشر شد و خسارات زیادی را به ویژه به سیستم‌های رایانه‌ای ایالات متحده، بریتانیا و هنگ‌کنگ وارد آورد. با این‌حال، دادستان کل امریکا، جان اشکرافت اظهار داشت دلیلی مبنی بر ارتباط این کرم با حملات یازدهم سپتامبر در دست نیست.*»[۲]

رخنه‌گری غیرمجاز به سیستم رایانه‌ای و انجام رفتارهای بزهکارانه در آن از دیگر روش‌های شناخته شده برای ارتکاب اقدامات تروریستی است. در این روش مرتکب با نفوذِ فنی (هک) یا با نفوذِ شفاهی (مهندسی اجتماعی) بخش‌های آسیب‌پذیر سیستم یا شبکه را شناسایی کرده تا در زمان مناسب آن را از کار بیندازد یا اطلاعات را دگرگون سازد یا از بین ببرد و یا اینکه مانع دسترسی به داده یا سیستم و در نتیجه کارآیی آنها شود. جدا از مهندسی اجتماعی، هک صرف رخنه‌ی غیر مجاز به سیستم است که در گام نخست چهره کیفری ندارد اما خرابکاری رایانه‌ای چهره کیفری هک است که مرتکب با قصد ربایش داده یا دگرگون ساختن آن یا جابجایی اطلاعات، به اقدام‌های بزهکارانه دست می‌زند و از این رو تروریست سایبری شخصی است که با انگیزه-های سیاسی و اجتماعی، مهارت‌های هک را به خدمت می‌گیرد.

اقدام‌های تروریستی سایبری روی‌هم‌رفته به چهار شیوه انجام می‌شوند: «*الف- یورش به اطلاعات که همان دگرگونی یا از میان بردن محتوای فایل‌های الکترونیکی، سیستم‌های رایانه‌ای یا محتویات گوناگون موجود در آنها است. ب- یورش به زیرساخت که بر پایه آن، مرتکب، سخت‌افزارها، پایگاه‌های عملیاتی یا برنامه‌های محیط رایانه را مختل می‌کند یا از بین می‌برد. ج- معاونت فنی در ارتکاب که عبارت است از به کارگیری ارتباطات*

2- Force Multiplier

الکترونیکی برای فرستادن نقشه‌ها و طرح‌ها به منظور انجام یورش‌های تروریستی یا تحریک به انجام آنها یا توسل به سایر تسهیلات. د- افزایش یا ارتقای منابع مالی که به موجب آن تروریست‌ها با بهره‌گیری از اینترنت برای خشونت سیاسی یا دیگر رفتارها، به گرفتن کمک‌های مالی افراد یا سازمان‌ها می‌کوشند.»[۷]

رکن روانی اقدام‌های تروریستی نیز همچون روش ارتکاب آنها گوناگون بوده و تروریست‌ها با انگیزه‌های چندی در فضای سایبر حضور می‌یابند که از جمله آنها می‌توان به « *طرح‌ریزی (مانند گردآوری اطلاعات، تجزیه و تحلیل آنها و تجهیز به نرم‌افزار پیشرفته و کمک‌رسان)، تامین یا تراکنش‌های مالی (همچون به دست آوردن کمک‌ها و بخشایش‌های هواخواهان، انتقال پول، پولشویی)، هماهنگی برای اجرای عملیات (مانند فرستادن نشانه‌ها یا رمزهای عملیات و بسیجیدن نیروها)، اقدام‌های سیاسی (مانند بازگویی قصدها و هدف‌های سیاسی) و تبلیغ و آموزش انگشت نهاد.*»[۹] گابریل وایمن پژوهشگر اسرائیلی، برای نشان دادن اندازه و شیوه‌های بهره‌گیری از فضای سایبر می‌گوید: «*گروه‌های مسلمان در ابتدای فعالیت روی اینترنت دوازده سایت داشتند اما این تعداد در انتهای سال ۲۰۰۳ به ۴۰۰ سایت افزایش یافت. وی نشان داده که چگونه طراحان یازهم سپتامبر از اینترنت برای یافتن اطلاعات ارزشمندی به منظور هواپیماربایی از قبیل چگونگی سوخت گیری، تعداد مسافران ثبت شده و مانند آن بهره برداری کرده اند.*»[۵]

اقدامات تروریستی سایبری هر چند به طوری که به چشم آید، رخ نداده ولی نمونه‌هایی از آن مانند خاموشی برق در ایالات متحده در سال ۲۰۰۳ در اثر دستکاری در سیستم رایانه‌ای اداره برق هشداری است برای آینده که تروریستها با انگیزه‌های گوناگون می‌توانند وارد سیستم رایانه‌ای جاهای حساس مانند کارخانه‌های داروسازی، بیمارستانها، سازمان‌های مربوط به آب و برق و مانند آن در سیستم‌ها و شبکه‌ها، آشفتگی و پریشانی پدید آورند که چه بسا نشانه‌های وخیمی از جهت سلامت و بهداشت همگانی به همراه داشته باشد. به همین دلیل دولتها جدا از جرم‌انگاری (مانند استرالیا که در ماده ۴۷۷ از قانون جرایم سایبری مصوب ۲۰۰۱ در سرلوحه بزه های برجسته و خطرناک سایبری به ارتکاب آگاهانه رفتارهایی چون رخنه‌گری غیر مجاز، تغییر داده و اختلال در سیستم بر ضد سلامت و بهداشت عمومی و دولت پرداخته است. و یا پاکستان در سال ۲۰۰۸) چاره‌اندیشی‌های ویژه‌ای برای مبارزه با اقدام‌های تروریستی سایبری در دستور کار قرار داده‌اند.

قانونگذار ایران، هنوز به طور راستین اقدام تروریستی را به عنوان یک بزه جداگانه و ناوابسته از دیگر بزه های امنیتی، پیش بینی نکرده است؛ از این رو نمی‌توان چشم داشت که اقدام تروریستی سایبری که خود گونه ای از اقدام تروریستی است، را در قانون‌های کیفری جای داده باشد. با این حال ماده ۱۱ قانون جرایم رایانه‌ای، بدون نام بردن از اقدام تروریستی یا تروریسم، بزهی را پیش‌بینی می‌کند که بسیار نزدیک به تروریسم سایبری است و آن اخلال رایانه ای همراه با قصد است.

ماده۱۱ قانون جرایم رایانه ای (ماده ۷۳۹ ق.م.ا) پیش بینی می‌کند: «هرکس به قصد خطر انداختن امنیت، آسایش و امنیت عمومی اعمال مذکور در مواد (۸)، (۹) و (۱۰) این قانون را علیه سامانه‌های رایانه‌ای و مخابراتی که برای ارائه خدمات ضروری عمومی به کار می‌روند، از قبیل خدمات درمانی، آب، برق، گاز، مخابرات، حمل و نقل و بانکداری مرتکب شود، به حبس از سه تا ده سال محکوم خواهدشد.»

رفتارهای موضوع ماده ۷۳۹، همان رفتارهای پیش بینی شده در ماده های ۸ (حذف یا تخریب یا مختل یا غیرقابل پردازش کردن)، ۹(از کار انداختن و مختل کردن کارکرد) و ۱۰(مانع شدن از دسترسی) قانون جرایم رایانه ای (ماده های ۷۳۶ و ۷۳۷ و ۷۳۸ قانون مجازات اسلامی) است. بدین حال، از جهت رفتاری، بزه موضوع ماده ۷۳۹، هیچ چیزی پیش بینی نکرده است و از جهت منطقی بهتر می‌بود که ماده ۷۳۹ که تنها بر قصد مرتکب و نیز گونه سامانه هایی که تهدید می‌شوند را سنجه ای برای افزایش کیفر بزهکار قرار می‌داد؛ زیرا بزه ها به رفتار شناخته می‌شوند و بزه موضوع ماده ۷۳۹ نیز رفتار جداگانه ای ندارد و برگرفته از همان رفتار بزه های دیگر است. نکته مهم در وابستگی رفتاری بزه موضوع ماده ۷۳۹ این است که در صورتی که این بزه رخ دهد، دیگر به جهت اینکه رفتار مرتکب که به طور جداگانه می‌تواند موضوع یکی از مواد سه گانه پیش گفته باشد، تعدد مادی یا معنوی در کار نیست. پس اگر مرتکب با قصد خاص پیش بینی شده در ماده ۷۳۹، اخلال یا تخریب یا ممانعت از دسترسی را بر

روی سامانه های ارایه دهنده خدمات ضـروری انجـام دهـد، تنهـا مرتکب بزه موضوع ماده ۷۳۹ شده است و گزاره هـای تعـدد بـزه جاری نیست؛ زیرا قانونگذار رفتار بزهی را با پـیش بینـی شـرایط نوین برای بزه دیگر قرار داده است.

با بررسی قانون های ضد تروریسم، روی هم رفته ترویسم سایبری را می‌توان بر دو دسته بزه‌های افزار محور و بزه‌های هدف محور دسته‌بندی کرد. بزه‌های افزار محور، به رفتارهای بزهکارانه سنتی گفته می‌شود که گروه‌های تروریستی از فضای سایبر برای انگیزه‌ها و هدف‌های خود بهره می‌جویند مانند تبلیغ اندیشه‌ها و آرمان‌های گروه، عضوگیری، تامین مالی و حتی تهدید دیگری یا ترساندن همگانی. این رفتار تنها با افزار رایانه انجام می‌شوند و به راستی تروریسم سایبری نیستند ولی در قانون‌های ضد تروریسم از آنها یاد شده و در ادبیات حقوقی نیز در زیر تروریسم سایبری آورده می‌شود. بزه‌های هدف محور همان رفتارهایی است که از سوی گروه‌های تروریستی بر ضد رایانه انجام می‌گردد. از آنجا که سنجه بزه تروریستی یا انگیزه سیاسی است یا پیوند یک رفتار با یک گروه تروریستی، همه رفتارهای نابهنجار رایانه ای مانند دسترسی غیرمجاز، شنود اطلاعات و جعل نیز می‌تواند در دل تروریسم سایبری جای بگیرد ولی آنچه که مفهوم راستین تروریسم سایبری است، جایی است رایانه هدف است نه افزار و در جایی که هدف است باید تمامیت داده یا سامانه، موضوع رفتار تروریست ها قرار بگیرد، نه محرمانگی. بدین حال تنها تخریب داده و اخلال سامانه با انگیزه سیاسی می‌تواند اقدام تروریستی سایبری به شمار آید که با رفتارهایی مانند انتشار ویروس، دست اندازی به نام‌های دامنه، ممانعت از دسترسی به داده و سامانه، اخلال در زیرساخت‌های حیاتی، تحریف اطلاعات نهادهای خدمات رسان یا اخلال در عملکرد نهادهایی که خدمات ضروری به شهروندان می‌دهند، نمود می‌یابد. از همین نگاه است که باید تروریسم سایبری را به دو مفهوم عام و خاص دسته بندی کرد و در جایی که تمامیت داده و یا سامانه موضوع اقدام تروریستی است را تروریسم سایبری خاص یا ناب نامید. با این نگاه، رفتارهای پیش‌بینی شده در ماده ۷۳۹ پیوند نزدیکی با پدیده تروریسم سایبری خواهند داشت.

موضوع تروریسم سایبری به سانی که در ماده ۷۳۹ قانون مجازات اسلامی آمده است، سامانه‌های رایانه‌ای و مخابراتی که برای ارائه خدمات ضروری عمومی به کار می‌روند، است. موردهای تمثیلی پیش بینی شده در ماده مانند خدمات درمانی، آب، برق، گاز، مخابرات، حمل و نقل و بانکداری نشانگر آن است که خدمات ضروری عمومی به خدماتی گفته می‌شود که برای رفع نیازهای حیاتی و ضروری شهروندان به کار می‌آید. اخلال در سامانه‌های ارایه دهنده خدمات ضروری نشان می‌دهد که تروریسم سایبری، از جهت رفتاری در فضای سایبر و از جهت نتیجه ای و پیآمدی در فضای بیرون نمود می‌یابد. هرچند ماده ۷۳۹، پدید آمدن اخلال در سامانه‌های رایانه ای و مخابراتی که خدمات ضروری ارایه می‌کنند را شرط نکرده، ولی برجستگی بزه به جهت پیامدها و نشانه هایی است که ممکن است از اخلال یا تخریب نمود یابد.

امروزه همه سامانه‌های دولتی و عمومی به رایانه ها و شبکه‌های رایانه ای مجهز هستند و خدمات ضروری نیز که بیشتر از سوی نهادی دولتی و عمومی ارایه می‌گردد، بر پایه رایانه و کنش‌های الکترونیکی عمل می‌کنند؛ از این رو اخلال در سامانه‌های رایانه ای و مخابراتی ارایه دهند خدمات ضروری مانند دستکاری در برنامه ها و داده‌های ثبت شده در بیمارستان ها، اخلال در برنامه فرود و برخاست هواپیماها یا اخلال در ناوبری هواپیما و کشتی ها و نیز راه آهن، اخلال در سامانه‌های آتش نشانی و اورژانس، اخلال در سامانه‌های توزیع برق، آب، گاز، تلفن و مانند آن همگی می‌تواند به پیآمدهای ناگواری همچون کشتار شهروندان، بی نظمی شهری و آشوب بیانجامد. برای نمونه می‌توان به قطع برق به طور گسترده در سال ۲۰۰۳ در آمریکا انگشت نهاد که به جهت دسترسی غیرمجاز به سامانه‌های نیروگاه‌های برق و اخلال در خدمات رسانی آنها، ۲۱ نیروگاه برق از کار افتادند و دیگر سازمان‌هاي مهم و حیاتی در ایالات متحده آمریکا، شامل پایگاه نیروی هوایی ادواردز و مرکز آزمایش بمب افکن‌هاي B-1 و B-2 نیز مختل شدند. این خرابی ها به واسطه کرم W32.Lovsan بوجود آمد. این اقدام منجر به قطع برق منطقه وسیعی از ایالات متحده آمریکا و شرق کانادا شد.[۱۰]

خدمات ضروری به طور نمونه‌ای بیان شده است و بسته به شرایط و جایگاه خدمات، ممکن است که برخی خدمات که در حالـت عـادی ضروری نباشند ولی در یک زمان ویژه، ضروری گردند؛ مانند زمـانی شهروندان به جهت تعطیلی بـه بانـک دسترسـی ندارنـد و نیـاز بـه عابربانک داشته باشند که چنین حـالتی، اخـلال در خـدمات دهـی

عابربانک ها می‌تواند موضوع ماده ۷۳۹ قرار بگیرد. بدین حال باید گفت که خدماتی ضروری است که نیاز به آن برای رفع هر گونه چالش و خطری روشن باشد و نتوان ارایه آن را به آینده واگذاشت؛ از این رو اخلال در سامانه ثبت نام دریافت رایانه یا دریافت سوخت و نیز اخلال در سامانه ثبت نام واحدهای آموزشی دانشگاه ها و همچنین اخلال در سامانه‌های خبررسانی مانند خبررسانی پلیسی و یا هواشناسی موضوع ماده ۷۳۹ قرار نمی گیرد.

بزه موضوع ماده ۷۳۹ باید به قصد خطر انداختن امنیت، آسایش و امنیت عمومی انجام شود که قصد غایی مرتکب است. در واقع باید گفت که رکن روانی بزه پیش بینی شده در ماده ۷۳۹، دارای سه عنصر است: نخست قصد رفتاری که مرتکب باید انجام یکی از رفتارهای پیش بینی در ماده‌های ۷۳۶، ۷۳۷ و ۷۳۸ را خواسته باشد. دوم قصد غایی که همانا قصد به خطر انداختن امنیت، آسایش و امنیت عمومی است. با این قصد باید گفت که ماده ۷۳۹ بخشی از تبصره ۱ ماده ۶۸۷ قانون مجازات اسلامی را که مقرر می‌کند، در صورتی که اعمال مذکور به منظور اخلال در نظم و امنیت جامعه و مقابله با حکومت اسلامی باشد مجازات محارب را خواهد داشت، نسخ کرده است. پس اگر اخلال رایانه‌ای به یکی از پیآمدهای پیش‌بینی شده در ماده ۶۸۷ بیانجامد و همراه با قصد اخلال در نظم و امنیت جامعه باشد، مرتکب دیگر محارب نخواهد بود و بر پایه ماده ۷۳۹ کیفر خواهد دید ولی نسبت به قصد مقابله با حکومت اسلامی که ماده ۷۳۹ درباره آن خاموش است، همچنان تبصره ۱ ماده ۶۸۷ به قوت خود مانده است. سوم آگاهی مرتکب که باید آگاه باشد که رفتار خود را بر روی سامانه‌هایی انجام می‌دهد که خدمات ضروری ارایه می‌دهند وگرنه رفتارش در زیر یکی از بزه‌های پیش‌بینی شده در مواد ۷۳۶، ۷۳۷ و ۷۳۸ بر حسب نوع رفتار جای می‌گیرد.

ج: شناخت راهکارهای پشتیبان ارزش: تدبیرهای حقوقی

تدبیرها و راهکارهای پشتیبانی از امنیت سایبری به عنوان ارزش، بدون شناخت چیستی و ویژگی‌های خود ارزش شدنی نیست. چنانکه پیش از این گفتیم فضای سایبر دو ویژگی برجسته دارد که سبب می‌شود تا شیوه برخورد با فضای سایبر و اندیشه برای تهدیدهای آن در راستای همین ویژگی برداشت شود. نخست اینکه فضای سایبر، فضای آزادی و خلوت ها است و دوم اینکه این فضا جهانی است. بنابراین باید این دو ویژگی را باور کرد . نه می‌توان از سرِ خودکامگی بر سر هر کاربر یا مشترک اینترنتی مامور گماشت و نه از سر نابخردی در پس برداشتن فضای جهانی و گماشتن فضای ملی به جای آن بود. در پی باور به این دو ویژگی است که می‌توان از امنیت فضای سایبر سخن گفت وگرنه با پشت پا زدن به این دو ویژگی، در اصل نه در پی امنیت سایبری که به دنبال حذف فضای سایبر هستیم.

از میان تدبیرهای گوناگون برای تامین امنیت، تدبیرهای حقوقی برجسته‌تر و منطقی‌تر است و از ریشه تدبیرهای مغایر یا این تدبیر، غیر قانونی‌اند و بنابراین دیگر تدبیرها باید نقش تکمیل-کننده برای تدبیرهای حقوقی داشته باشند. در یک نگاه کلی، تدبیرهای حقوقی می‌تواند در سه گام یا بستر کلان اعمال شوند که هر سه گام با هم پیوند تنگاتنگ و کمک‌کننده دارند. گام نخست، تدبیرهای داخلی است که در محدوده سرزمینی نمود می‌یابد. گام دوم، تدبیرهای دوجانبه و گام سوم تدبیرهای بین-المللی و جهانی است. هر سه گام خود بر تدبیرهای گوناگون پشیینی و پسینی دسته بندی می‌شوند:

۱-تدبیرهای یک جانبه یا داخلی

تدابیر داخلی یا یک‌جانبه به راهکارهای یک دولت پاسداری از فضای سایبر در برابر تهدیدها گفته می‌شود که نیرومندترین و مهمترین تدابیر برای رویارویی با تهدیدهای سایبری گفته می-شود. به راستی این تدبیرها چون با پشتوانه دولتی همراه است و می‌تواند چهره قهری داشته باشد، بیش از تدبیرهای دوجانبه و چندجانبه کارساز است. سخن از تدبیرهای داخلی یا درون سرزمینی بسیار است و تنها به طور کلی به آنها پرداخته می‌شود. تدبیرهای داخلی در قبال پدیده مجرمانه می‌تواند پنج حالت داشته باشد: تدبیرهای کیفری برای پیگرد و کیفر مرتکب، تدبیرهای تامینی برای دفع خطر بزه در آستانه انجام، تدبیرهای پیشگیرانه برای از میان برداشتن زمینه‌های بزه، تدبیرهای درمانی برای درمان و بازگردانی بزهکار و تدبیرهای ترمیمی برای جبران زیان‌های نمودیافته از بزه. در بزه‌های امنیتی که بزهکار با قصد یا انگیزه سیاسی و آگاهانه به سپهر بزهکاری وارد می‌شود، تدبیرهای درمانی چندان کارساز نیست. همچنانکه به جهت مطلق بودن

بیشتر بزه‌های امنیتی، تدبیرهای جبرانی نیز به برجستگی دیگر تدبیرها نیستند. از این رو به سه مورد دیگر اشاره می‌شود:

یکم: تدبیرهای کیفری: تدابیر کیفری به پیش‌بینی ضمانت اجراهای کیفری در رویارویی با پدیده مجرمانه سایبری گفته می‌شود. این تدابیر تنها نسبت به تهدیدهایی است که از سوی قانونگذار با کیفر رو به رو شده‌اند و هنگامی به اجرا در می‌آیند که رفتار مجرمانه، رخ داده باشد. تدبیرهای کیفری هرچند همه تهدیدها مانند جنگ را در بر نمی‌گیرد و نیز هرچند چهره پیشینی ندارد ولی برجسته ترین راهکار برای پاسخ به تهدیدهای مجرمانه مرزی و برگرداندن امنیت است. از این رو باید این تدبیرها جامع، سازگار با بزه و اجراشدنی باشند. تدبیرهای کیفری هم چهره ماهوی دارند که در پیکره بزه‌انگاری و پیش‌بینی کیفر و گزاره‌های آنها نمود می‌یابد(مانند قانون جرایم رایانه ای- بخش جرایم و مجازات‌ها) و هم چهره شکلی که در پیکره گردآوری ادله دیجیتال و پیگرد متهم در می‌آیند. (مانند بخش آیین دادرسی قانون جرایم رایانه‌ای). برای رویارویی کیفری با بزه‌های امنیتی سایبری، بایسته است تا مقرره‌های ماهوی و شکلی قانون جرایم رایانه‌ای هم گرامی داشته شود و هم آگاهانه و ریزبینانه اجرا شود. در کنار این قانون، به جهت برجستگی بزه‌های امنیتی سایبری، قانونگذار از وزارت اطلاعات نیز به عنوان ضابط دادگستری یاد کرده است، که می‌تواند نقش برجسته‌ای در پیگرد بزه‌های سایبری امنیتی داشته باشد. طبق ماده ۲۰۵ قانون برنامه پنجساله پنجم توسعه جمهوری اسلامی ایران (۱۳۹۴ ـ ۱۳۹۰)، وزارت اطلاعات موظف است با هدف دفاع از حاکمیت و منافع ملی و تقویت تعامل با جامعه اطلاعاتی و پیشگیری و مقابله با تهدیدات و تهاجم اطلاعاتی و امنیتی داخلی و خارجی به ویژه استکبار جهانی اقدامات زیر را انجام دهد:

الف ـ ارتقاء کمی و کیفی زیرساختهای اطلاعاتی با هدف تحکیم و تقویت امنیت پایدار و فراگیر

ب ـ پیشگیری و مقابله با فساد و اختلال در امنیت اقتصادی، جرائم سازمان‌یافته ضدامنیتی، اقدامات تروریستی و تهدیدات نرم امنیتی در مقام ضابط دادگستری. باید گفت که واژه " پیشگیری" در این بند با تعبیر " ضابط دادگستری" همخوانی نداشته و از ریشه زائد است، زیرا وظیفه بنیادین وزارت اطلاعات پیشگیری از بزه نیست، بلکه کشف یا رصد آن است، در حالی که پیشگیری ازبزه نیاز به برنامه‌های درازمدت و گوناگون دارد که هیچ پیوندی با وظیفه‌های وزارت اطلاعات ندارد، مگر اینکه واژه پیشگیری را در معنای جلوگیری از رخ دادن بزهی بدانیم که با اطلاعات به دست آمده، در آستانه وقوع است، نه نسبت به هر بزهی که در امکان رخ دادن آن در آینده باشد. به سخن دیگر در اینجا مفهوم پیشگیری بیشتر بر معنای اقدام تامینی گواهی می‌دهد تا مفهوم اصلی پیشگیری از وقوع بزه.

دوم: تدبیرهای تامینی: تدابیر تامینی به راهکارهایی گفته می‌شود که برای دفع حالت خطرناک و از میان برداشتن خطر پیش آمده به کار می‌آید. این تدبیرها برای برقراری امنیت در صحنه خطر است و از این رو به آن اقدام تامینی گفته می‌شود. اقدام تامینی هرچند برای شخص یا گروه دارایِ حالت خطرناک، پیشینه کیفری نمی‌آفریند ولی می‌تواند حقوق و آزادی‌های فردی را در تنگنا بگذارد. از این رو اقدام تامینی تنها باید برای از میان برداشتن خطر واقعی و رخ دادنی به کار آیند. پس اعمال اقدام تامینی در فضای سایبر برای پیشگیری از بزه در حال انجام باید با قرینه‌ای بخردانه و با هوشمندی اعمال گردد وگرنه فضای سایبر در اصل همانند خیابان یا پیرامون بازار یا پایانه مسافربری نیست تا بتوان تشخیص داد که چه کسی در آستانه بزهکاری است. با این حال نسبت به کسانی که پیشینه دوبار انجام بزه رایانه‌ای داشته‌اند و برای بار سوم یا بیشتر به بزه رایانه‌ای دست زنند، می‌توان از تدبیرهای تامینی بهره برد و همین رویکرد برای برخورد با بزه‌های امنیتی سایبری کارساز خواهد بود. بر پایه ماده۲۷ قانون جرایم رایانه ای، در صورت تکرار جرم برای بیش از دو بار دادگاه می‌تواند مرتکب را از خدمات الکترونیکی عمومی از قبیل اشتراک اینترنت، تلفن همراه، اخذ نام دامنهٔ مرتبه بالای کشوری و بانکداری الکترونیکی محروم کند:الف) چنانچه مجازات حبس آن جرم نودویک روز تا دو سال حبس باشد، محرومیت از یک ماه تا یک سال. ب) چنانچه مجازات حبس آن جرم دو تا پنج سال حبس باشد، محرومیت از یک تا سه سال. ج) چنانچه مجازات حبس آن جرم بیش از پنج سال حبس باشد، محرومیت از سه تا پنج سال

سوم: تدبیرهای پیشگیرانه: تدابیر پیشگیرانه به راهکارهای پیشگیری از رخ دادن تهدیدهای مجرمانه سایبری است. تدبیرهای کیفری برای پس از رخ دادن بزه و تدبیرهای تامینی برای آستانه بزه و تدبیرهای پیشگیرانه برای پیش از رخ دادن بزه

است. بنابراین تدبیرهای پیشگیرانه به طیف گسترده‌ای از تدبیرها گفته می‌شود که زمینه بزه سایبری را از میان بر می‌دارد. تدبیرهای پیشگیرانه هم پیشگیری اجتماعی و آموزش‌محور را در بر می‌گیرد و هم تدبیرهای وضعی و مکان محور(مانند پالایش یا بهره گیری از سامانه باروی آتشین و تدبیرهای همسان). به این دو دسته از تدبیرها باید پیشگیری زودرس را افزود؛ زیرا فضای سایبر بیش از همه برای نوجوانان گیراتر است و از این رو می‌توان با آموزش و کنترل نوجوانان و جوانان، پیشگیری زودرس برای رویارویی با بزه‌های سایبری امنیتی را به عمل آورد.

تدبیرهای پیشگیرانه در قانون ها نیز بازتاب یافته اند. پیش‌بینی کمیته تعیین مصادیق محتوای مجرمانه در قانون جرایم رایانه‌ای برای پالایش اینترنتی از یک سو و شرط پیش‌بینی تدبیرهای امنیتی و حفاظتی برای سامانه‌ها و داده‌های رایانه‌ای در ماده یک و چهار قانون جرایم رایانه‌ای از سوی دیگر، همگی برای پیشگیری از رخ دادن بزه سایبری است.

همچنین در قانون برنامه پنجم توسعه به برخی تدبیرهای پیشگیرانه پرداخته شده است. طبق ماده۱۹۶ قانون، ..دولت موظف است به منظور تقویت کمی و کیفی بسیج مستضعفان و حضور بیشتر نیروهای مردمی در صحنه‌های امنیت و دفاع از کشور، آرمانها و مبانی اندیشه انقلاب اسلامی و توسعه فرهنگ امر به معروف و نهی از منکر اقدامات و تسهیلات لازم را در طول برنامه به شرح زیر فراهم نماید... هـ ـ پشتیبانی و کمک به مقابله با جنگ نرم در حوزه‌های مختلف با اولویت حضور فزآینده در فضای مجازی و رایانه‌ای (سایبری) با رویکرد بومی. و نیز بر پایه ماده۲۳۱ به منظور ارتقاء سطح حفاظت از اطلاعات رایانه‌ای و امنیت فناوریها و اجرای سند امنیت فضای تبادل اطلاعات، اقدامات ذیل انجام خواهدگرفت: الف ـ کلیه دستگاههای اجرائی، نهادهای عمومی و شرکتهای غیردولتی دارای زیرساختهای حیاتی موظفند به منظور امن‌سازی زیرساختها و حفظ امنیت تبادل اطلاعات در مقابل حملات الکترونیک در چهارچوب سند امنیت فضای تبادل اطلاعات (افتا) تا پایان سال دوم برنامه امنیت فضای تبادل اطلاعات خود را ارتقاء بخشند. ب ـ کلیه دستگاههای اجرائی و اشخاص حقوقی ارائه‌دهنده خدمات عمومی موظفند از سال دوم برنامه نسبت به اجرای سامانه مدیریت اطلاعات اقدام نموده و نسبت به اجرای دستورالعملها و استانداردهای « افتا» از سال اول برنامه اقدام نمایند.

۲- تدبیرهای دوجانبه یا طرفینی

تدبیرهای دوجانبه به پیمان همکاری میان ایران و کشور دیگر در زمینه برنامه‌های گوناگون از جمله پیکار با بزه‌های سایبری و فرامرزی اشاره دارد. به جهت پیوند بزه‌های سایبری با بزه‌های فراملی مانند بزه‌های سازمان یافته و اقدام‌های تروریستی، بایسته است تا دولت ایران با برخی کشورها به ویژه کشورهای همسایه، پیمان نامه‌های دوجانبه برای همکاری‌های امنیتی و حقوقی پدید آورد تا در پیوندهای میان این کشورها با ایران، سیاست‌های همسانی برای رویارویی با بزه‌های سایبری گزینش شود. در برخی از این پیمان نامه‌های دوسویه به رویارویی با بزه‌های سایبری و نیز بزه‌های امنیتی مانند اقدام‌های تروریستی انگشت نهاده شده است. برای نمونه طبق ماده۱ قانون موافقتنامه همکاریهای امنیتی بین دولت جمهوری اسلامی ایران و دولت قطر مصوب ۱۳۸۹/۱۰/۱ زمینه‌های همکاری پیش بینی شده که در بند ۱۱ آن به جرایم رایانه‌ای و سایر جرایمی که با استفاده از وسایل مخابراتی صورت می‌گیرد، پرداخته شده است.

همچنین طبق بند ۱۰ ماده یک قانون موافقتنامه همکاری بین دولت جمهوری اسلامی ایران و دولت جمهوری ترکیه در زمینه مبارزه علیه قاچاق مواد مخدر، جرایم سازمان‌یافته و تروریسم مصوب ۱۳۹۰/۱/۳۱، مبارزه با جرایم رایانه‌ای و مخابراتی بر اساس قوانین و مقررات داخلی طرفها پیش بینی شده است که این خود پیوند تنگاتنگ بزه‌های سایبری با بزه‌های سازمان یافته و اقدام‌های تروریستی را می‌رساند. همچنین ماده یک موافقتنامه همکاری امنیتی بین دولت جمهوری اسلامی ایران و دولت جمهوری ایتالیا دولت جمهوری اسلامی ایران و دولت جمهوری ایتالیا مصوب ۱۳۸۲/۱۰/۲۳ به جرائم رایانه‌ای و سایر جرائمی که با استفاده از وسایل ارتباطی، صورت می‌گیرد. به جهت چهره جهانی بزه‌های سایبری امنیتی، باید دولت ایران برای رسیدن به امنیت سایبری، بر شمار این پیمان نامه‌های دوسویه بیفزاید.

۳- تدبیرهای چندجانبه یا بین المللی

تدبیرهای چندجانبه به اسناد جهانی یا بین‌المللی می‌پردازد که از خواست همسان بیشتر کشورها ناشی می‌شود. در سیاست‌های کلان کشور درباره اطلاع‌رسانی رایانه‌ای به « *اقدام مناسب برای دستیابی به میثاق‌ها و مقررات بین‌المللی و ایجاد اتحادیه‌های اطلاع‌رسانی با سایر کشورها به ویژه کشورهای اسلامی*» انگشت نهاده شده است. به راستی به جهت ماهیت جهانی و شبکه‌ای بزه-های سایبری، چاره‌ای مگر بودِ اراده جهانی برای پیکار با بزه‌های سایبری نمی‌ماند. هرچند در این زمینه تنها سند برجسته بین-المللی، کنوانسیون بوداپست درباره بزه‌های محیط سایبر است که آن هم چهره منطقه‌ای دارد، ولی بایسته است تا دولت ایران در برنامه‌های بین‌المللی به ویژه راهکارهای سازمان ملل یا اتحادیه-های منطقه‌ای برای پیکار با بزه‌های سایبری، شرکت کند. این همکاری به ویژه برای پیگرد متهمان به انجام بزه‌های سایبری، در هر جای جهان که باشند بسیار کارساز خواهد بود.

دستاورد

بزه‌های سایبری امنیتی به عنوان یکی از پدیده‌های تهدیدآمیز جدی برای امنیت سایبری و پیرو آن امنیت ملی به شمار می‌آید که حتی خطرناکی آنها از دیگر تهدیدها مانند جنگ نیز بیشتر است. پدیده‌های مجرمانه سایبری چون از سوی شهروندان باهوش یا از رهگذر باندها و سازمان‌های جنایی در می‌آید، هم به طور برنامه-ریزی شده و کلان رخ می‌دهند و هم در طول زمان دنباله دارند. از این رو امنیت سایبری با تهدیدی همیشگی رو به رو است.

انگاره بنیادین برای نیل به درون‌مایه سند چشم انداز ۱۴۰۴ و نیز عملی کردن سیاست‌های کلی نظام در زمینه امنیت سایبری، رویارویی بخردانه و اثرگذار با بزه‌های سایبری است. این رویارویی خود بر تدبیرهای چندی استوار است که با روی آوردن به ماهیت فضای سایبر باید همه ویژگی‌های آن در نظر باشد. به جهت چهره ترکیبی فضای سایبری، بایسته است تا تدبیرها هم چهره ملی داشته باشند، هم وجه دوجانبه و در پیکره تعامل با کشورهای همسایه و هم در پیروی از اراده بین المللی که در قالب برنامه‌های جهانی پیکارگر با بزه‌های سایبری نمود یافته است. این تدبیرهای سه سطحی، خود باز دارای برنامه و تدبیرهای خردتری هستند که می‌توانند قهرآمیز، تامینی و پیشگیرانه باشند. پس امنیت سایبری از نگاه حقوقی و قانونی، پیرو راهکاری سه سطحی با رویکرد سه برنامه‌ای(کیفری، تامینی و پیشگیرانه) است.

نکته بسیار برجسته برای امنیت سایبری، پاسداشتن حریم خصوصی شهروندان و آزادی آنها در فضای سایبر از یک سو و قانونگرایی در این فضا از سوی دیگر است. شکستن مرز قانون‌های کنونی خود عاملی برجسته برای ناامنی سایبری است. از این رو نیروی انتظامی باید بر پایه قانون به ضابطه گری دست زند و برنامه‌های مانند کنترل کاربران یا کافی نت‌ها، هیچ جایگاه قانونی نداشته و بلکه پشت پا زدن به اصول قانون اساسی است. در همین راستا با پیش‌بینی قانون جرایم رایانه‌ای و قانون برنامه پنجم توسعه، ضابط دادگستری در پیگرد بزه‌های سایبری، نیروی انتظامی(پلیس فتا) و در برخی موردها وزارت اطلاعات است و از این رو نهادهای که بر پایه قانون پیش‌بینی نشده‌اند مانند مرکز مبارزه با جرایم سازمان‌یافته فراملی سپاه پاسداران، در راستای قانون‌گرایی و جلوگیری از هم‌پوشانی اقدام‌های نهادهای مربوطه باید در دل نهاد نیروی انتظامی یا وزارت اطلاعات جای بگیرد.

منابع

الف- فارسی

۱-بوزان، باری؛ **مردم، دولت‌ها و هراس**، برگردان پژوهشکده مطالعات راهبردی، انتشارات پژوهشکده مطالعات راهبردی، چاپ اول، ۱۳۷۸، ص ۵۲

۲- جلالی، امیرحسین؛ **تروریسم سایبری**، فصلنامه تخصصی فقه و حقوق؛ شماره ۱۰؛ پاییز ۱۳۸۵، ص ۹۶

۳- فریدمن، لورنس؛ ، **مفهوم امنیت**، در مجموعه گزیده مقالات سیاسی- امنیتی، برگردان پژوهشکده مطالعات راهبردی، انتشارات پژوهشکده مطالعات راهبردی، چاپ دوم، ۱۳۷۸، ص ۳۱۹

۴- فلمینگ پیتر و استول مایکل؛ **سایبر تروریسم: پندارها و واقعیت‌ها**، برگردان اسماعیل بقایی هامانه و عباس باقر پور اردکانی، در مجموعه تروریسم، گردآوری و ویرایش علیرضا طیب، نشر نی، چاپ دوم، ۱۳۸۴، ص ۱۵۶

۵- کلهر، رضا؛ **جهاد مجازی: ماهیت و چالش‌ها**، فصلنامه مطالعات منطقه‌ای جهان اسلام، شماره ۳۲، سال هشتم، ۱۳۸۶، ص۳۱

۶- ماتئو وارن، ویلیام هاچینسون؛ **تروریسم شبکه‌ای**، برگردان غلامرضا رفعت نژاد، گزارش، انتشارات پژوهشکده مطالعات راهبردی، ، ۱۳۸۲ ، ص ۶

ب: انگلیسی

7-Ballard, James David and Hornik, Joseph G and Mckenzie, Douglas; **Technological facilitation of**

terrorism, , in Cyberterrorism, edited Alan Oday, Ashgate publishing company, 2004, p.44
8- Brenner, Susan W; **Cybercrime, cyberterrorism and cyberwarfare**, International review of penal law: cybercrime, AIDP, volume 77, 2006, p.457
9- Cohen, Fred; **Terrorism and cyberspace**, in Cyber terrorism, edited Alan Oday, Ashgate publishing company, 2004, p.150-151
10-Colarik, Andrew M; **Cyber terrorism**: political and economic implication, Idea Group Publication, 2006, p.51
11- Franks, Renae Angeroth; **The national security agency and its interference with private sector computer security**, Lowa law review, vol 72, 1986-1987, p. 1022
12- Gray sharp, Walter; **Balancing our civil liberties with our national security interests in cyberspace**, Texas review of law and politics, vol 4, 1999 - 2000, p.73
13-**International encyclopedia of laws**, volume 3: cyber law, edited by R. Blanpain, United Kingdom, written by Ian Lloyd, Kluwer law international, first published, 2004,up to date as of July 2006, p.487
14-Janczewski, Lech J and Colarik, Andrew M; **Managerial guide for handling cyberterrorism and information warfare,** Idea group publishing, 2005, pp.2 and 3
15- Jensen, Neil; **Technology and Intelligence**, journal of money laundering control, volume 8, no 3, 2005, p. 228
16-Lewis, Brian C; **Prevention of cybercrime admist international anarchy**, American criminal law review, vol 41, 2004, p.1355
17-Matusitz, Jonathan A; **Cyber terrorism: A postmodern view of networks of terror and how computer security experts and law enforcement officials fight them**, UMI dissertation services, University of Oklahoma, 2006,19 and 20
18- Nigel, Phair; **Cybercrime; the reality of the threat**, E-security Publishing, Canberra, 2007, p. 146
19- Ozeren, Suleyman; **Global response to cyberterrorism and cybercrime: A matrix for international cooperation and vulnerability assessment**, UMI dissertation services, university of north Texas, august 2005, p.28
20- Podesta, John D and Goyle, Raj: **Lost in cyberspace? Finding American liberties in a dangerous digital world**, Yale law and policy review, volume 23, 2005, p.517
21- Walker, Clive; **Cyber-Terrorism: legal principal and law in the United Kingdom**, Penn state law review, volume 110, 2005-2006, p.634

This page is intentionally left blank