فصلنامه مطالعات حقوق
Journal of Legal Studies
شماره سی ام. بهار ۱۳۹۸، صص۱۴۸-۱۰۳ Vol 3. No 30. 2019, p 103-148
شماره شاپا (۲۵۳۸-۶۳۹۵) ISSN: (2538-6395)

بررسی تطبیقی تروریسم سایبری در قوانین جزایی کشورهای ایران و آمریکا

دکتر محسن برهانی[۱]. عاطفه حاج محمدی[۲]
۱. عضو هئیت علمی دانشگاه مفید. قم. ایران
۲. دانشجوی کارشناسی ارشد رشته حقوق جزا و جرم شناسی دانشگاه مفید. قم. ایران
hajmohammadi.atefeh@yahoomail.com

چکیده

یکی از موضوعات مهم سه دهه گذشته مسئله تهدید تروریسم بوده و روز به روز اهمیت آن در ادبیات حقوقی و روابط بین الملل بیشتر و بیشتر می‌شود. در این میان و اکنون تروریسم سایبری به عنوان اصلی‌ترین نوع تروریسم رایج در جهان به یکی از مهم‌ترین چالش‌های امنیتی تبدیل شده، به گونه‌ای که ساختار نظم جهانی ای را با خطر فروپاشی مواجه کرده است. مهم‌ترین هدف تروریسم به مخاطره افکندن امنیت است زیرا در نبود امنیت، کلیه امور جامعه دچار اخلال می‌گردد. تروریسم سایبری به یکی از چالش‌های عمدهٔ نظام‌های حقوقی به خصوص نظام‌های کیفری تبدیل شده است. بزه تروریسم، دیگر از رویکردهای سنتی خود رنگ باخته و به سوی فناوری‌های نوین روی آورده است. در میان اکثر نظام‌های حقوقی جهان، به جرم انگاری تروریسم سایبری صریح و اختصاصی پرداخته نشده‌است. ایران نیز از این قاعده مستثنی نبوده و نیاز به تدوین و اعمال قوانین صریح و واضحی جهت پیشگیری و مقابله با این مشکل حقوقی دارد. در این میان مهم ترین سوالی که مطرح می‌شود این است که آیا قوانین مطرح شده تا کنون از نظر حقوقی و کیفری قوانین جامع و کاملی بوده است؟ خلاءهای موجود در نظام کیفری ایران در مورد تروریسم سایبری چیست و چگونه باید در رفع آنها کوشید.

به نظر می‌رسد یکی از بهترین راه‌حل‌های ممکنه برای حصول اطمینان از صحت عملکرد ایران در نحوه قانون‌گذاری و امور اجرایی این قوانین، مقایسه قوانین ایران در حوزه تقنینی و کیفری با آمریکا که جزو کشورهای پیشرو در این زمینه می‌باشد است. این نوشتار به صورت توصیفی و تحلیلی به واکاوی و بررسی و مقایسه چگونگی عملکرد این دو کشور در زمینه قانون‌گذاری و اعمال آن می‌پردازد و سعی دارد برای آن راه‌حلی قابل اجرا و موثر پیدا کند، در پایان به این سر انجام می‌رسد که حوزه حقوقی کشور نیاز به بازبینی و نگارش قوانین جدید و کامل‌تری جهت پیشگیری و مقابله با تروریسم سایبری را داراست.

واژه‌های کلیدی: تروریسم سایبری، قانون گذاری، پیشگیری و مقابله با تروریسم سایبری

مقدمه

ویژگی‌های بی‌همتای فناوری‌های اطلاعات و ارتباطات، تحولات بنیادینی را در قلمرو حیات بشری پدید آورده است. نخستین ویژگی بی‌همتای فناوری‌های اطلاعات و ارتباطات، جهان‌گیری گسترش این فناوری‌هاست. این ویژگی باعث گردیده است فناوری‌های اطلاعات و ارتباطات نفوذ جهان گسترانه‌ای به دست آورند و در یک گستره جغرافیایی خاص و محدود نگنجند. به عبارت بهتر، فناوری‌های اطلاعات و ارتباطات تمامی مرزها را در می‌نوردند و از جهان مرز زدایی می‌کنند. این مرز زدایی و کمرنگ کردن مرزهای سنتی، زمینه تسهیل حرکت هر چه آزادانه‌تر کالا، سرمایه و افراد را فراهم می‌کند. دومین ویژگی مهم و چشمگیر فناوری‌های اطلاعات و ارتباطات، کنترل ناپذیری و لجام گسیختگی آن است. گسترش فناوری‌های اطلاعات و ارتباطات به گونه‌ای است که در بسیاری از موارد حتی عاملان گسترش و زمینه سازان آن نیز نمی‌توانند آن را در کنترل خود در آورند.[1] ویژگی سوم که پیوند تنگاتنگی با ویژگی دوم دارد و البته سایر ویژگی‌های فناوری‌های اطلاعات و ارتباطات را تحت الشعاع قرار می‌دهد، " قاعده گریزی" در این پدیده است. این ویژگی به علت ماهیت شبکه‌ای فناوری‌های اطلاعات و ارتباطات است که نوعی وضعیت غیر سلسله مراتبی و شبکه‌ای در عرصه‌ای که حضور می‌یابد، می‌آفریند. این وضعیت غیرسلسله مراتبی، محیط سنتی و پویش‌های امنیتی آن را که نظام‌مند است نه شبکه‌ای، تحت تأثیر قرار می‌دهد.[2] چهارمین ویژگی فناوری‌های اطلاعات و ارتباطات، که خصوصیتی بدیع و بدعت زا نیز به شمار می‌آید، ایجاد و گسترش جهان مجازی است. این ویژگی عصر امنیت را دو جهانی ساخته است: جهان واقعی و جهان مجازی. جهان واقعی همان عرصه سنتی امنیت است و جهان مجازی عرصه‌ای است که گسترش فناوری‌های اطلاعات و ارتباطات هر روز بر اهمیت و تأثیر گذاری آن می‌افزاید، به گونه‌ای که در حال حاضر رویدادهای جهان مجازی بر جهان واقعی سایه می‌افکند.

بهره‌گیری گروه‌های تروریستی از امکانات فضای مجازی، نوع جدیدی از تهدید را پدید می‌آورد که "سایبر تروریسم" نامیده می‌شود. سایبر تروریسم هر گونه اقدام تروریستی است که در آن از سیستم‌های اطلاعاتی و فناوری‌های دیجیتالی به عنوان ابزار حمله و آماج حمله استفاده می‌شود. این حملات باید به اعمال خشونت بر ضد اشخاص یا داریی‌ها بیانجامد، به گونه‌ای که ایجاد رعب و وحشت نماید.

در جهان کنونی و به علت پیشرفت بشری از جمله پیشرفت در فناوری و امنیت؛ اهتمام تمام دولت‌ها برای حفظ وصیانت از کشور و امنیت مردم خود می باشد. این امنیت و حفظ چه به صورت فیزیکی و چه به صورت حفظ اطلاعات محرمانه امنیتی، اقتصادی و مرزی می باشد. در این بین به علت افزایش روزافزون تکنولوژی‌های کامپیوتری و اینترنتی و افزایش عملکرد دولت‌ها به صورت الکترونیکی و به علت عدم

1- Cavelty, M. D. Cyber-Security and Threat Politics; US efforts to secure the information age. New York: Routlefge, p. 67 (2008)

2- Mesko, G. "Perceptions of Security: Local Safety Councils in Slovenia". In: U. Gori, & I. Paparela. Invisible Threats; Financial and Information Technology Crimes Against National Securi,y. Netherlands: IOS Press, p. 81 (2006)

وجود ابزارهای امنیتی لازم؛ دسترسی به اطلاعات (چه فردی و چه کشوری) به آسانی صورت گرفته و موجب ضررهای جبران ناپذیری برای مردم و دولت‌ها خواهد بود.

در این بین سیاست‌های جدیدی برای جنگ سرد و نابودی دولت‌ها از طرف برخی کشورها اتخاذ شده است که به براندازی دولت‌ها و جنگ از طریق فضای سایبر می‌پردازند. در اصطلاحات حقوقی به این گونه حملات "تروریسم سایبری" گفته می‌شود.

شاید مختصرترین و مناسب‌ترین تعریف از تروریسم سایبری این باشد که «تروریسم سایبری عبارت است از هر اقدام غیر قانونی برضد سیستم‌ها و اطلاعات با انگیزه‌های سیاسی».[1] این تعریف در پی نشان دادن اهمیت، اشخاص یا گروه‌هایی که به آن دست می‌زنند و نیز عواقب جرم نیست. تنها این معنا را به صورت کوتاه بیان می‌کند که تروریسم سایبری هر اقدام بر ضد سایبر بر پایه انگیزه سیاسی را گویند. در اینجا انگیزه، ماهیت این پدیده را نشان می دهد. اگر چه در یک رویکرد حقوقی محض تروریسم سایبری فقط شامل اقدامات سایبری ضد سیاست ها و داده‌ها و اطلاعات با انگیزه‌های سیاسی است.

درباره میزان خطرناکی این جرم، باید گفت که اگرچه هدف تروریست‌ها معمولا قتل سران سیاسی و براندازی حکومت است اما صدمه‌هایی که با حمله الکترونیکی به شبکه‌های رایانه‌ای وارد می‌آید ممکن است بسیار سهمگین باشد و اثرات آن تا مدتها باقی بماند. در واقع، تروریست‌ها صرف نظر از ماهیت و اهداف اقداماتشان، نتایج بسیار زیان بار و گاه جبران ناپذیری به جای می‌گذارند. معمولا آنها نقاط حساس و حیاتی جوامع را هدف قرار می‌دهند تا اساسی‌ترین ضربات را به دشمنان خود وارد کنند و بهترین بهره‌برداری را از وضعیت موجود به عمل آورند کـه بی تردید زیرساخت‌های حیاتی و زیربنایی از بهترین گزینه‌ها به شمار می‌آیند.

در درک عمومی برداشت کلی بر این است که تروریسم سایبری به معنای تهاجمات و تهدید به تهاجمات غیرقانونی به رایانه ها، شبکه‌ها و اطلاعات ذخیره شده در آنها می باشد که به منظور ارعاب یا وادارکردن یک دولت یا مردم آن صورت می‌گیرد. به علاوه برای آنکه یک تهاجم، تروریسم سایبری تلقی شود، باید منجر به اعمال خشونت علیه اشخاص یا اموال گردد یا حداقل آنقدر خسارات وارد آورد که منجر به وحشت گردد. تهاجماتی که باعث فوت، آسیب جسمی، انفجار، تصادف هواپیماها، آلودگی آب یا لطمه شدید اقتصادی میشوند، ازجمله این موارد هستند.

ایران در چند سال اخیر به شدت با این موضوع در ارتباط بوده است، در ایران هرچند قانون خاص برای این مشکل وجود ندارد اما سعی شده است در قانون جرائم رایانه ای و قوانین عمومی جزایی به این موضوع پرداخته شود. اما از انجا که هنوز سیستم تقنینی مسلم و شفاف درباره این معضل جامعه شکل نگرفته است و بدین صورت جلوگیری، مبارزه، انتخاب مجازات مناسب برای مرتکبان و اعمال سیاست های حقوقی در

1- Rod Stark : Cyber Terrorism, Rethinking New Technology, Department of Defense and – strategic Studies ,. p. 9 1999

برابر آن با مشکل مواجه خواهد شد. بنابراین می بایست به بررسی ابعاد این جرم و راهکارهای حقوقی- پیشگیری و مجازات این جرم در بین یک کشور مهم در این مسئله، "آمریکا"، که جزو یکی از کشورهای پیشرو در امر قانون گذاری است و ایران که به تازگی مورد حملاتی از این دست قرار گرفته است به صورت تطبیقی بپردازیم.

تعریف تروریسم سایبری

با پیدایش کامپیوتر، جرائم کامپیوتری نیز بوجود آمد. اصطلاح تروریسم سایبر برای اولین بار در سال ۱۹۹۶ با تلفیق واژه‌های تروریسم و فضای سایبر ایجاد گردید. به واقع پیشینه این پدیده به تاریخچه جرایم سایبر برمیگردد و آن نیز به زمانی که اینترنت وارد عرصه حیات انسانی شد. به دیگر کلام، پیشینه تروریسم سایبر، ریشه در سابقه جرایم سایبر دارد. از آنجا که این جرایم از زمان پدیداری اینترنت خلق شده‌اند، در نتیجه از قدمت چندانی برخوردار نیستند. وانگهی، نظر به اینکه تروریسم سایبر نیز خود به نوعی پدیده ای نوین و مصداقی تازه از جرایم سایبری است، پیشینه عملی چندانی ندارد.

تاریخچهٔ جرائم کامپیوتری را می‌توان به سه نسل طبقه بندی نمود:

نسل اول: جرایم رایانه‌ای که تا اواخر دههٔ ۱۹۸۰ می‌باشد شامل سرقت و کپی برداری از برنامه‌ها و جرائم علیه حریم خصوصی اشخاص، مانند سرقت از آثار و تحقیقات افراد بود.

نسل دوم: که تحت عنوان جرائم داده‌ها نامیده می‌شود تا اواخر دهه ۱۹۹۰ ادامه داشته است. در این دهه تمامی جرائم علیه تکنولوژی اطلاعاتی، ارتباطاتی، کامپیوتری، ماهواره‌ای و شبکه‌های بین‌المللی تحت عنوان جرائم علیه داده‌ها اطلاق می‌شود.

نسل سوم: که از اواسط دههٔ ۱۹۹۰ شروع می‌شود، جرائم کامپیوتری، تحت عنوان جرائم سایبری و جرائم در محیط سایبر معروف گردید.[۱]

امروزه سایبر تروریسم خطرناک تر از تروریسم سنتی است؛ پیوند و اتصال شبکه جهانی اینترنت به روشنی گویای این واقعیت است که ویرانگری و آسیب‌رسانی می‌تواند در یک لحظه سراسر جهان را فرا گیرد. سوء استفاده از فناوری‌های رایانه‌ای و اینترنتی می‌تواند امنیت ملی، آسایش عمومی و موجودیت یک جامعه را به مخاطره انداخته و تاثیرهای منفی بی‌شماری را بر زندگی افراد اجتماع تحمیل کند

بهره‌گیری از اینترنت و شبکه‌های رایانه‌ای و امکاناتی، با هدف نابود ساختن شبکه‌های زیربنایی یک جامعه مانند انرژی، حمل و نقل، فعالیت‌های دولتی و تاثیرگذاشتن بر یک دولت، شهروندان، گروه‌ها و مواردی از این قبیل که این شبکه ها پدید می آورند. فضای سایبری نیز از سوی برخی کارشناسان به عنوان تأثیر

۱- هافمن، بروس و پاراکینی، جان، بازنگری در تروریسم و مفهوم تروریسم بیولوژیکی، (۲۰۰۱) «مترجم: رحمان قهرمان پور، فصلنامه مطالعات دفاعی - امنیتی

فضا و جامعه‌ای که توسط رایانه ها، اطلاعات و ابزارهای الکترونیکی، شبکه های دیجیتالی و یا کاربران آن شکل می‌گیرد، تعریف شده است. تروریسم سایبری که حاصل تلاقی و همگرایی دو واژه ترور و سایبر شکل گرفته است در عنوان عبارت اولی خود ترس و واهمه راگوشزد میکند و سایبر هم که همان فضای مجازی است و براین اساس می‌توان گفت ایجاد هرنوع ترس و واهمه‌ای از طریق فضای مجازی را تروریسم سایبری می‌گویند. البته اگرچه سلاح‌های گرم و مهمات شیمیایی از جمله ابزارهای تروریسم در جهان واقع به شمارمی‌روند، رایانه‌ها نیز ابزاری برای تروریسم سایبر خواهند بود که درپی دسترسی و حمله به اهداف مشخصی از رایانه‌ها و سیستم‌های اطلاعاتی هستند. [۱]

در خصوص پدیدهٔ تروریسم به عنوان یک پدیدهٔ مجرمانه یک مانع بزرگ در این راه وجود دارد و آن این که اگر قرار است اقدامات تروریستی تحت شمول ضمانت اجراهای کیفری که بعضا سنگین و حتی جبران ناپذیر مانند اعدام قرار گیرند باید تعاریف مشخص و دقیقی از آن‌ها که عاری از هرگونه ابهام باشد در قوانین کیفری انعکاس یابد.

با این حال تمامی این مسائل زمانی به حد غایت مشکل می‌شوند که ضرورت ایجاب کند در فضایی به اجرا درآیند که به بسیاری از مبانی و شیوه‌های اجرایی معمول آنها پایبند نیست. قابلیت مجازی‌سازی، این امکان را فراهم آورده تا داده‌های الکترونیکی در قالب فرآیندهای الکترونیکی به جای اشخاص، ادارهٔ امور را در دست گیرند که نمونه بارز آن را در بانک داری الکترونیکی شاهد هستیم. همین مسئله به ظاهر ساده باعث شده تا مراجع کیفری مطالبات مالی الکترونیکی را بر عنوان مجرمانه کلاهبرداری منطبق ندانند و قانون گذاران را مجبور کنند قوانین جدیدی را به تصویب برسانند با این استدلال که عنصر فریب در آنها وجود ندارد و نسبت به سیستم ها و برنامه‌های رایانه‌ای صدق نمی‌کند.[۲]

عدم اجماع بر سر عناوین مجرمانه و به تبع آن جرم انگاری متحدالشکل برای مبارزه با جرایم سایبری به خوبی در اسناد بین‌المللی منطقه‌ای و بین‌الدولی‌ای که تا کنون تدوین و منتشر شده نیز مشهود اسهت. بارزترین آن کنوانسیون اروپایی جرایم سایبری ۲۰۰۱ است. با اینکه اکثریت اعضای این کنوانسیون را کشورهای عضو شورای اروپا تشکیل می‌دهند و آن ها نظام حقوقی مشابه دارند اما تنها نُه عنوان مجرمانه از دویست عنوان مجرمانه سایبری که تا کنون شناسایی شده در این سند منعکس شده و از میان نُه عنوان نیز تنها هرزه نگاری کودکان با حق شرط مواجه نشده است.[۳]

در ضمن میان حمله سایبری و تروریسم سایبری نیز تفاوت‌هایی وجود دارد. البته برخی تروریسم سایبری را به معنی حملات از پیش طراحی شده با انگیزه سیاسی می‌دانند که توسط گروه‌های تحت حمایت کشورها

۱- فیرحی، داود و ظهیری، صمد، رهیافت های موجود در تحلیل پدیده تروریسم، (۱۳۸۷)، فصلنامه سیاست، مجله دانشکده حقوق و علوم سیاسی، دوره۳۸، شماره۳ صفحه ۱۵۶

۲- عالی پور حسن، حقوق کیفری فناوری اطلاعات -۱۳۹۰ چاپ اول تهران انتشارات خرسندی صفحه ۲۳

۳- همان ص ۳۵

یا عوامل خرابکار، علیه سیستم‌های رایانه‌ای و اطلاعاتی، برنامه‌های رایانه‌ای و داده‌ها انجام می‌شود، به نحوی که منجر به خشونت علیه اهداف غیرنظامی شود. در تروریسم سایبری بر خلاف حملات سایبری، هدف نظامی مشخصی وجود ندارد و هدف، بیشتر تاثیرگذاری بر ساکنین یک شهر یا کشور است. لذا هدف حملات اصوالا غیرنظامیان هستند و ارتکاب آن نیز لزوماً به هدایت دولت نیست. در واقع تروریست‌های سایبری صرفاً بدنبال ایجاد ترس و آسیب‌رسانی در افراد جامعه هستند. اما رابطه‌ی منطقی میان حملات سایبری و جنگ سایبری را می‌توان عموم خصوص مطلق در نظر گرفت. یعنی تمام جنگ‌های سایبری شامل حملات سایبری هم می‌شوند حال بعضی حملات سایبری ممکن است به حد یک جنگ سایبری برسد یا نرسد. عبارت دیگر تنها حملات سایبری‌ای به آستانه جنگ سایبری می‌رسند که اثری معادل و هم تراز حملات نظامی داشته باشند و یا در بطن یک مخاصمه مسلحانه رخ دهند.[۱]

در واقع می‌توان گفت که حملات سایبری به گروه یا تعداد زیادی از اعمال ارتکابی از سوی هکرها اطلاق می‌شود که بعضاً با خشونت یا آثارشدید همراه است. البته حملات سایبری یا به عبارت دیگر حملات هکری می‌تواند رویکردهای مجرمانه متفاوتی داشته باشد. گاه این حملات مقدماتی است و برای کسب اطلاعات و داده‌ها جهت ارتکاب جرایم سایبری صورت می‌گیرد و گاه این حملات مستقیماً در چارچوب یک توصیف جزایی سایبری صورت می‌گیرد. به هر حال حملات هکری یا حملات سایبری عنوان عامی است که بر مصادیق متعدد اطلاق می‌شود و دسته‌ای از این مصادیق را تروریسم سایبری می‌نامند.

مرکز مطالعات راهبردی و بین المللی در گزارش خود در سال ۱۹۹۸ با عنوان «جرم سایبر، تروریسم سایبر، جنگ سایبر، به سوی یک شکست قطعی»، تعریفی نسبتاً عام برای تروریسم سایبر ارائه داده است. به موجب این تعریف، تروریسم سایبر عبارت است از «حملات از پیش مقرر با انگیزه سیاسی از سوی گروههای درون ملی یا عوامل زیرزمینی یا اشخاص علیه سیستم‌های اطلاعاتی و رایانه‌ای، برنامه‌های رایانه‌ای و داده‌هایی که منجر به خشونت علیه اهداف غیرنظامی می‌شوند».[۲] دیگران تروریسم سایبر را عملی مجرمانه دانسته‌اند که با استفاده از رایانه‌ها و ابزارهای مخابراتی که منجر به خشونت، خرابکاری و یا متلاشی ساختن سرویس‌ها می‌شود، به قصد ایجاد ترس از راه ایجاد سردرگمی و تردید درمیان جمعیتی معین با هدف تاثیرگذاری بر حکومت یا مردم (دولت یا ملت) برای انطباق با برنامه های خاص سیاسی، اجتماعی یا ایدئولوژی ارتکاب میابد.

در تعاریف آمده از تروریسم سایبری می‌توان به تعاریف ارائه شده از سوی آمریکا پرداخت اداره تحقیقات فدرال آمریکا (اف. بی. آی) تروریسم سایبری را اینگونه تعریف می‌نماید: «حمله‌های با انگیزه سیاسی و از پیش برنامه ریزی شده توسط گروه های خرد اجتماعی و یا آژانس های مخفی علیه اطلاعات، سیستم های کامپیوتری، برنامه های کامپیوتری و یا اطلاعاتی که به اعمال خشونت علیه اهداف نظامی منجر شود. مرکز

۱- ضیایی، یاسر و خلیل زاده مونا، مسئولیت بین المللی دولت ناشی از حمالت سایبری، ، مجله ی حقوقی شهردانش، شماره ۲۳ ص ۸۶

2- Colarik, Andrew M, Cyber Terrorism: political and Economic Implications, IDEA Group Publishing, 2006, P. 46

حمایت از زیرساخت های ملی آمریکا در تعریف تروریسم سایبری رویکرد متفاوتی را دنبال نموده است: «یک اقدام مجرمانه که به وسیله کامپیوتر یا ظرفیت‌های ارتباطات مخابراتی با هدف نفوذ در دولت و یا اشخاص، برای دستیابی به موافقت آنها، جهت برنامه‌های خاص سیاسی، اجتماعی و یا ایدئولوژیکی انجام شده و منجر به اعمال خشونت و یا خسارت و یا قطع سرویس‌های عمومی شود به نحوی که باعث ایجاد ترس از طریق ایجاد سردرگمی و بی‌ثباتی شود».

متاسفانه در توصیف رکن قانونی جرم تروریسم سایبری باید خاطر نشان کرد که هر چند در سالیان اخیر قانون جرایم رایانه‌ای مصوب ۱۳۸۸/۰۳/۰۵ به تصویب مجلس شورای اسلامی رسیده و قدری خلاءهای قانونی راکه در زمینه جرایمی که درباره رایانه واقع می‌شوند پر کرده است، اما قانون جامعی برای مبارزه با اعمال متنوع از این دست نمی باشد. یکی از مصادیق آن همین جرم سایبر تروریسم است که به ناچار و با کمی اغماض شاید برخی از مواد این قانون در این زمینه کارایی داشته باشند.

اما با نگاه به مهمترین کنوانسیون مقابله با تروریسم سایبری مشهور به «کنوانسیون بوداپست»، سایبر تروریسم را می‌توان این‌گونه تعریف کرد: «اقدامات برنامه ریزی شده و هدفمند با اغراض سیاسی و غیرشخصی که علیه رایانه‌ها و امکانات و برنامه های ذخیره شده در درون آن‌ها، از طریق شبکه جهانی صورت می‌گیرد و هدف از چنین اقدامی نابودی یا وارد کردن آسیب‌های جدی به آنهاست.»[1]

با توجه به تعاریف ذکر شده، تروریسم سایبری، با انگیزه سیاسی صورت می‌گیرد؛ با استفاده از رایانه به عنوان سلاح و ابزار یا به عنوان هدف و موضوع صورت می‌گیرد؛ از سوی گروه‌های درون ملی یا عوامل زیرزمین به قصد خشونت، تأثیرگذاری بر شاهدان و ناظران آن یا تغییر سیاست‌های دولت مربوطه صورت می‌گیرد. اما به این گذاره‌ها باید انگیزه‌های مالی و اقتصادی را نیز اضافه کرد تا تعریف تروریسم سایبری کامل شود.

حقوق ایالات متحده آمریکا

در این بخش در صددیم تا ضمن تجزیه تحلیل محدودیت ها و ظرفیت های نظام ایالات متحده آمریکا، دستاوردها و تجربه‌های حقوق جزایی و کیفری این کشور را بررسی کنیم. ابتدا قواعد و مقررات موجود در زمینه تروریسم سایبری در نظام ایالات متحده آمریکا مورد تجزیه تحلیل و مقایسه قرار خواهد گرفت. سپس اطلاعات مربوط به شیوه و سازوکارهای اجرایی مبارزه با تروریسم سایبری در این کشور از طریق بررسی آراء قضایی صادره در این زمینه و اسناد و مدارک منتشره از سوی وزارت کشور ایالات متحده آمریکا در این زمینه خواهیم پرداخت. هدف از این بررسی‌ها یافتن مجموعه از کاستی‌ها و توانمندی‌های قانونی این کشور در راستای مبارزه با این جرم بسیار مهم است.

1- Convention on Cybercrime Budapest, 23. XI. 2001

نظام قانونی آمریکا، بیشتر از غالب کشورهای جهان، دارای چند لایه است. یکی از دلایل آن مجزا بودن قوانین فدرال و ایالتی است. برای درک این مطلب، باید یاد آوری کنیم که ایالات متحده به عنوان یک کشور واحد بنیان‌گذاری نشد بلکه بنیاد آن بر ۱۳ مستعمره بود که هر کدام مدعی استقلال از پادشاهی بریتانیا شدند. بخش ۸۰۲ از قانون میهن پرستی ایالات متحده آمریکا[1] تعریف تروریسم برای پوشش "داخلی"، به عنوان بین المللی تروریسم مخالف گسترش داده است. یک شخص در تروریسم داخلی شرکت می کند، اگر اقدام "خطرناک برای زندگی بشر" انجام دهد که تخلف از قوانین جنایی یک ایالت یا ایالات متحده است، اگر یکی از اقدام‌های در نظر گرفته شده است:

(الف) ارعاب یا مجرم بودن یک غیرنظامی جمعیت؛

(ب) تاثیر گذاشتن بر سیاست یک دولت توسط ارعاب و اجبار؛

(پ) تأثیر بر رفتار دولت توسط تخریب، ترور یا آدم ربایی توده‌ای.

علاوه بر این، اعمال باید در درجه اول در قلمرو صلاحیت ارضی ایالات متحده صورت گیرد و اگر چنین نیست، ممکن است به عنوان تروریسم بین‌المللی محسوب شود.

بخش ۸۰۲ جرم جدیدی از تروریسم داخلی ایجاد نمی کند. با این حال، نوع رفتارهایی را که دولت می‌تواند هنگام بررسی "تروریسم" بررسی کند، گسترش می‌دهد. قانون میهن پرستی ایالات متحده آمریکا قدرت‌های دولتی را برای تحقیق در مورد تروریسم گسترش داد و برخی از این قدرت‌ها برای تروریسم داخلی قابل اجراست.

از زمان تصویب قانون میهن پرستی، دو قانون جدید دیگر به تصویب رسید که تروریسم داخلی را تضمین می کند. اطلاعات مالیات دهندگان[2] بخش ۶۱۰۳ (C) (3) (i) به وزیر خدمات درآمد اجازه می‌دهد که اطلاعات مالیات‌دهندگان را به سازمان مناسب اجرای قانون فدرال، مسئول تحقیق و یا پاسخ به حادثه تروریستی ارائه دهد. اگر مورد آزار و اذیت قرار گیرد، این مفاد می‌تواند توسط اجرای قانون برای دسترسی به اطلاعات مالیات دهندگان محرمانه معترضین سیاسی مورد استفاده قرار گیرد.

مقررات مواد زیستی و سموم[3] بخش ۲۶۲a و ۷ قوانین ایالات متحده. A. بخش ۸۴۰۱ تنظیم‌کننده عوامل بیولوژیکی و سموم است. اگر شخصی با یک سازمان درگیر در تروریسم داخلی یا بین المللی مشارکت داشته باشد، او مجاز به دسترسی به این عوامل مجاز نیست. طبق قانون، دادستان کل، افراد مربوط به "تروریسم" را به وزارت کشاورزی شناسایی می کند. هنگامی که شخص در لیست ذکر شده است، او نمی تواند به هیچ یک از عوامل یا سموم تنظیم شده دسترسی پیدا کند. این احتمالا بیشتر مردم را تحت تاثیر قرار نخواهد داد، اما ممکن است به شخص دیگری مانند دانشمند تاثیر بگذارد که ممکن است در کار خود به طور منظم از عوامل بیولوژیکی یا سموم استفاده کند.

1- Pub. L. No. 107-52
2- U. S. C. A26.
3- U. S. C. A42.

به طور خلاصه باید گفت قوانین مورد استناد ما در این پژوهش، کدهایی هستند که در سیستم قانون‌گذاری فدرال، شامل مجلس نمایندگان، مجلس سنا و رئیس جمهور، تصویب و اجرائی شده و جرم انگاری و مجازات برای جرائم مشخص شده را به صورت محدوده حداقلی و حداکثری معین کرده است به طوری که ایالات در تعیین مجازات نباید از این محدوده خارج شوند.

سیستم حفظ حریم خصوصی ایالات متحده، مسلما قدیمی‌ترین، قوی‌ترین و موثرترین در جهان است. سیستم "حفظ حریم خصوصی دولت" بیشتر به اجرای پس از اجرای حکومت و رسیدگی به دعوا خصوصی متکی است. در حال حاضر، مقررات امنیت سایبری شامل دستورالعمل‌های اجرایی و قوانین کنگره است که فناوری اطلاعات و سیستم‌های کامپیوتری را تضمین می کند.

در ایالات‌متحدهٔ‌آمریکا برای مقابله با تعرضات به این سه عامل مهم در عرصهٔ فناوری اطلاعات و تکنولوژی ارتباطات از سال‌ها پیش اقدامات مهمی در تدوین قوانین و اعمال مجازات بر متجاوزان صورت گرفته است. البته به همین نسبت نیز اصلاحات مهمی هم در بخش ماهوی و هم در شیوهٔ اجرای آنها انجام شده است.

سه قانون مهم فدرال امنیت سایبری وجود دارد:

ـ قانون انتقال قابلیت اطمینان و مسئولیت پذیری [۱]

ـ قانون مدرنیزاسیون خدمات مالی [۲]

ـ قانون امنیت ملی، شامل قانون مدیریت امنیت اطلاعات فدرال[۳]

اما این مقررات تنها مربوط به صنایع مرتبط با کامپیوتر نیست مانند ارائه‌دهندگان خدمات اینترنت [۴]و شرکت‌های نرم افزاری. علاوه بر این، زبان مبهم این مقررات، فرصت زیادی برای تفسیر دارد.

در تلاش‌های اخیر برای تقویت قوانین امنیتی سایبری، دولت فدرال چندین قانون امنیتی جدید را معرفی می‌کند و همچنین تغییرات قدیمی‌تر را برای یک اکوسیستم امنیت بهتر معرفی می‌کند. در زیر چند نفر از آنها هستند:

قانون به اشتراک‌گذاری اطلاعات امنیت سایبری [۵]: هدف آن بهبود امنیت سایبر در ایالات‌متحده از طریق به اشتراک‌گذاری گسترده اطلاعات در مورد تهدیدات امنیتی سایبری است. این قانون اجازه اشتراک‌گذاری اطلاعات ترافیک اینترنت بین دولت ایالات متحده و شرکت های فناوری و تولید می‌دهد. این لایحه در تاریخ ۱۰ ژوئیه ۲۰۱۴ در مجلس سنای ایالات متحده معرفی شد و در تاریخ ۲۷ اکتوبر ۲۰۱۵ در مجلس سنا تصویب شد.

1- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
2- Gramm-Leach-Bliley Act or Financial Services Modernization Act of 1999
3- Federal Information Security Management Act of 2002 (FISMA)
4- ISPs
5- Cybersecurity Information Sharing Act (CISA)

قانون بهبود امنیت سایبری:[1] این قانون به تاریخ ۱۸ دسامبر ۲۰۱۴ به امضاء رسیده است. این یک مشارکت جاری و داوطلبانه دولتی و خصوصی برای بهبود امنیت سایبری و تقویت تحقیقات و توسعه در زمینه امنیت سایبری، توسعه نیروی کار و آموزش و پرورش و آگاهی و آمادگی عمومی است.

قانون صدور اطلاعیه مبادله اطلاعات مربوط به مبادله مالی:[2] این لایحه به یک مبادله بیمه درمانی نیاز دارد که هر فردی را که اطلاعات شخصی آن به علت نقض امنیت هر سیستم نگهداری شده، توسط مبادله در اسرع وقت به دست بیاید.

قانون ملی پیشرفت در زمینه حفاظت از امنیت سایبری: این قانون، قانون امنیت ملی را در سال ۲۰۰۲ اصلاح میکند تا اجازه دهد وزارت امنیت داخلی[3] مرکز ملی امنیت و ارتباطات سایبری[4]شامل دولت، اشتراک اطلاعات و مراکز تجزیه و تحلیل و نهادهای خصوصی در میان نمایندگان غیر فدرال توانایی مبارزه با تروریسم سایبری را داشته باشند.[5]

تصویب اولین قانون در این زمینه به سال ۱۹۸۴ برمی‌گردد که کنگرهٔ آمریکا اقدام به تصویب قانونی آزمایشی جهت مقابله با جرایم ارتکابی در دنیای الکترونیک نمود. این قانون در سالهای ۱۹۹۴ و ۱۹۹۶ مورد بازنگری قرار گرفت و هم اکنون نیز قانون سال ۱۹۹۶ لازم الاجرا می باشد. این قانون در مادهٔ ۱۸ قانون ایالات متحده بخش ۱۰۳۰ آن گنجانیده شده است.

لازم به ذکر است که کلیهٔ مفاد این بخش در راستای حمایت از تعرضات مربوط به این سه عامل مهم یعنی: حفظ اطلاعات در برابر افشای غیرمجاز آنها، حفظ صحت اطلاعات در برابر تغییر یا آسیب به آنها، حفظ عملکرد مفید سیستم و در دسترس نگهداشتن اطلاعات، می باشد. اما همانطور که در تفاسیر قانونی مربوطه نیز مشخص شده قسمتA2 بیشترین وضوح را در حمایت از اولین عامل دارد و قسمتA5 نیز در مورد حمایت از عوامل دوم و سوم می باشد که در جای خود مورد بررسی قرار خواهد گرفت.

صنعت خدمات مالی هدف قابل توجهی از نظر تهدیدات امنیتی سایبری است. در طول چند سال گذشته، وزارت امور خارجه خدمات مالی آمریکا در تهدیدهای رو به رشدی که برای سیستم اطلاعات و مالی توسط دولت های دیگر، سازمان‌های تروریستی و بازیگران مستقل جنایی انجام گرفته است، نظارت دقیق داشته است.

با در نظر گرفتن جدی بودن مسئله و ریسک برای همه اشخاص تحت کنترل، برخی از استانداردهای حداقل تنظیم قانونی ضروری است، در حالی که بیش از حد قانونی نیست، به طوری که برنامه‌های امنیتی سایبری می‌توانند با خطرات مرتبط مطابقت داشته و با پیشرفت های تکنولوژیکی مواجه شوند.

1- Cybersecurity Improvement Act of 2014 -2017
2- ACT ON REAL NAME FINANCIAL TRANSACTIONS AND GUARANTEE OF SECRECY 2015
3- DHS
4- NCCIC
5- ISACA

بر این اساس، این مقررات طراحی شده است تا ترویج حفاظت از اطلاعات مشتری و نیز در سیستم‌های فناوری اطلاعات سازمان‌های نظارتی انجام شود. این مقررات مستلزم هر شرکت برای ارزیابی مشخصات ریسک خاص خود و طراحی برنامه‌ای است که خطرات آن را به طور جدی مورد بررسی قرار می‌دهد.

مبحث اول: قانون جرائم مربوط به کامپیوتر

حال به بررسی بخش ۱۰۳۰ از مادهٔ ۱۸ قانون ایالات متحده که دربارهٔ کلاهبرداری و جرایم مرتبط با آن نسبت به کامپیوتر می‌باشد، می‌پردازیم. بخش‌های متعدد این قسمت، قوانین کیفری علیه تروریسم را تقویت می‌کنند. این عنوان جرایم را برای تروریسم علیه حمل‌ونقل جرم افزوده است. همچنین به تروریسم داخلی می‌پردازد و آن را تعریف می کند که شامل "اقدامات خطرناک برای زندگی بشر که نقض قوانین جنایی ایالات متحده یا هر ایالتی است" که به نظر می رسد به منظور ارعاب و یا مجبور کردن یک جمعیت غیرنظامی است؛ برای تأثیرگذاری بر سیاست دولت با ارعاب یا اجبار؛ یا به وسیله تخریب، ترور، یا آدم ربایی، بر رفتار دولت تأثیر بگذارد؛ و در درجه اول در قلمرو صلاحیت ارضی ایالات متحده اتفاق می افتد. علاوه بر این، برخی از قوانین جنایی محدودیت ها را گسترش می دهد. جایی که اعمال برخی از جرایم تروریستی "منجر به ایجاد یک خطر قابل پیش بینی، مرگ و یا آسیب جدی جسمی به فرد دیگری شد"، محدودیت های قانونی حذف می شود. همچنین در نظر دارد جلوگیری از تروریسم سایبری را با افزایش مجازات های جرم و جنایت برای نقض قوانین تخفیف و تجاوز به کامپیوتر مورد هدف قرار دهد. این تعریف قانونی "کامپیوترهای محافظت شده" را اصلاح میکند به طوری که رایانه های موجود در خارج از ایالات متحده راهم شامل می‌شوند.

دولت ایالات متحده در حال تلاش برای معرفی قوانین سختگیرانه برای تجهیز سازمان‌ها برای حفاظت از اطلاعات از آخرین تهدیدات اینترنتی است. با این حال، "بروس شنییر" به درستی گفت که حملات سایبری موفق به سیستم‌های دولتی با وجود تلاش‌های دولت ادامه می‌یابد. این امر برای شرکت‌های خصوصی هم صادق است. توصیه می‌شود که سازمان‌ها در مورد امنیت برنامه‌ها و داده‌های خود اقدام کنند. جنایتکاران سایبری همیشه در حال حرکت هستند و در رویکرد خود برای حمله پیشرفت می کنند. به همین دلیل شرکت ها باید سیستم های خود را به طور منظم برای شناسایی آسیب پذیری ها و بلافاصله به نقاط ضعف برسانند.

این قسمت از پژوهش، چارچوب و سندها را با شروع کنگره ۱۱۷ آغاز می‌کند تا بیش از ۳۰ کنگره را که بخشی از آن هستند یا مربوط به آن هستند، اصلاح کنند. این شامل بحث در مورد مسائل مربوط به قانون‌گذاری و فعالیت در کنگره ۱۱۳ می‌شود.[۱]

مبحث دوم : قوانین امنیت سایبری

اسناد قانونی اخیر، از جمله بسیاری از لایحه ها معرفی شده در کنگره های اخیر، به طور عمده بر مسائل در چند حوزه گسترده، از جمله به شرح زیر:

"حفاظت از زیرساخت‌های بحرانی سازمان‌های خصوصی"، "به اشتراک‌گذاری اطلاعات امنیت اطلاعات در میان مراکز خصوصی و دولتی"، "وزارت امنیت داخلی مقامات برای حفاظت از سیستم‌های فدرال"، "اصلاح قانون مدیریت اطلاعات امنیت فدرال"، "نیروی کار سایبری"، و"تحقیق و توسعه"

"سایر موضوعات" شامل قانون جرایم سایبری، اعلان نقض حقوق بشر و امنیت سایبری مربوط به دفاع نیز در طرح‌های قانونی مورد توجه قرار گرفته اند. حداقل برخی از مراکز مطالعاتی که در این باره صورت می‌گیرد، تغییرات صریح را در قوانین جاری پیشنهاد کرده‌اند. با این حال، هیچ کدام از چنین اصلاحاتی تا پایان کنگره ی شانزدهم تصویب نشد.

در کنگره ۱۱۲ و ۱۱۳، چندین سندی که به طور خاص بر روی امنیت سایبری متمرکز شده بود، بررسی شد.

اسناد قانونی جامع در کنگره ۱۱۲ شامل:

قانون امنیت سایبری ۲۰۱۲ [۲] توصیه های یک کارگروه مجلس نمایندگان مجلس و یک سند توسط دولت اوباما. [۳]در مجلس سنا مورد بحث قرار گرفت اما دو مورد در رای گیری با شکست مواجه شد. در غیاب تصویب قانون امنیت سایبری در آن کنگره، کاخ سفید، با مقررات مربوط به حفاظت از اطلاعات جاسوسی، از جمله به اشتراک‌گذاری اطلاعات و توسعه استانداردها تصمیمات خود را به انجام رساند.

در کنگره‌ی سیزدهم، چندین سند و برخی از مسائل مطرح شده برای بهبود بخشی امنیت سایبری و توصیه‌هایی که توسط هیئت بررسی انجام شده است، مطرح شده است. چهار مورد در مجلس نمایندگان در کنگره ۱۱۲ را تصویب شد اما مجلس سنا آنها را مورد توجه قرار نداد. آنها دوباره مجددا به بررسی گذاشته شدند و مجددا به تصویب کنگره ۱۱۵ رسیدند.

۱- برای گردآوری گزارش CRS و سایر منابع در مورد امنیت سایبری، به گزارش CRS Report R42507، Cybersecurity: گزارش‌های معتبر و منابع، توسط موضوع، توسط ریتا تهان. برای گزارش‌های مرتبط با امنیت سایبری انتخاب شده در CRS، به بررسی مسائل مربوط به CRS قبل از کنگره مراجعه کنید.

2- FISMA
3- S. 3414
4- same

– قانون به اشتراک گذاری و حفاظت از اطلاعات سایبری[1]بر اشتراک و هماهنگی اطلاعات تمرکز دارد.
– قانون بهبود امنیت سایبری سال ۲۰۱۳ و قانون تحقیق و توسعه فناوری شبکه و فناوری آمریکا در سال ۲۰۱۳ در مورد فناوری های تحقیق و توسعه سایبری امنیتی فدرال و استانداردهای فنی است.
– قانون مدرنیزاسیون امنیت اطلاعات فدرال سال ۲۰۱۳ پرداخت.
همچنین تصویب مجلس سه طرح بود که به نقش وزارت امنیت داخلی در امنیت سایبری اشاره داشت: قانون پیشرفت تحقیق و توسعه زیربنای بحرانی، قانون امنیت ملی امنیت سایبری و قانون حفاظت از زیرساخت‌های بحرانی امنیت ملی و سال ۲۰۱۳. آنها شامل مقررات مربوط به نیروی کار، تحقیق و توسعه، به اشتراک گذاری اطلاعات و همکاری دولتی / خصوصی در حفاظت از اطلاعات محرمانه هستند.

سه کنوانسیون سمینار سنا در کنگره ۱۱۳:

• قانون استخدام و نگهداری نیروی کار سایبری[2]در سال ۲۰۱۴، پرونده مربوط به مسائل مربوط به نیروی کار، مجلس سنا را به عنوان اصلاحیه تصویب کرد.
• قانون حفاظت از امنیت ملی در سال ۲۰۱۴ مجوز مرکز به اشتراک گذاری اطلاعات را فراهم می‌کند.
• قانون مدرنیزاسیون امنیت اطلاعات فدرال ۲۰۱۴، به اصلاح قانون مدیریت اطلاعات امنیت فدرال می‌پردازد.
چهار لایحه، با اصلاح، در پایان کنگره‌ی ۱۱۳ برگزار شد: این پرونده‌ها به اصلاح قانون مدیریت اطلاعات امنیت فدرال و مسائل نیروی کار و فعالیت‌های به اشتراک گذاری اطلاعات اشاره دارد.
نقش فدرال در رسیدگی به امنیت سایبری پیچیده است. این شامل هر دو امنیت سیستم‌های فدرال و انجام نقش مناسب فدرال در حفاظت از سیستم‌های غیرفدرال می‌باشد. هیچ مقررات در چارچوب کلی وجود ندارد، اما بسیاری از مقررات اعمال شده در مورد جنبه‌های مختلف امنیت سایبری قرار دارند. برخی از مفاد قابل توجه در اعمال زیر است:
ـ دستگاه تقلبی دسترسی و کامپیوتر تقلب و سوء استفاده از قانون ۱۹۸۴ حملات مختلف بر روی سیستم‌های کامپیوتری فدرال و در آن استفاده شده توسط بانک ها و در تجارت بین ایالتی و خارجی را ممنوع کرده است.
ـ قانون حفظ حریم خصوصی ارتباطات الکترونیکی سال ۱۹۸۶ ممنوعیت استعفای الکترونیکی غیر مجاز را ممنوع کرده است.

1- H. R. 624

ـ قانون امنیت کامپیوتر سال ۱۹۸۷ زیر نظر مؤسسه ملی استاندارد و فناوری[1]مسئولیت توسعه استانداردهای امنیتی سیستم های کامپیوتری فدرال را، به جز سیستم‌های امنیت ملی [2]که برای دفاع استفاده می‌شود و ماموریت‌های اطلاعاتی، و مسئولیت وزیر بازرگانی برای صدور استانداردهای امنیتی را به عهده داشت.

ـ قانون کاهش حجم حسابداری در سال ۱۹۹۵ زیر نظر مسئول دفتر مدیریت و بودجه[3]برای توسعه سیاست‌های امنیت سایبری پرداخت.

ـ قانون کلینگر-کوهن سال ۱۹۹۶ مسئولین را برای اطمینان از کفایت آژانس‌های اطلاعاتی و سیاست های امنیتی، مقام مأموریت اطلاعات [4]را در سازمان‌ها ایجاد کرد و به وزیر بازرگانی مجوز داد تا استانداردهای امنیتی اعلام شده را اعمال کند.

ـ قانون امنیت ملی در سال ۲۰۰۲ [5]به وزارت امنیت داخلی [6] بعضی از مسئولیت های امنیتی سایبری را علاوه بر موارد ذکر شده توسط مسئولیت‌های عمومی خود برای امنیت داخلی و زیرساخت های حیاتی [7] اعمال کرده است.

ـ قانون تحقیق و توسعه سایبری که در سال ۲۰۰۲ نیز تصویب شد، مسئولیت های تحقیقاتی در زمینه امنیت سایبری برای بنیاد ملی علوم [8]را تأسیس کرد.

ـ قانون دولت الکترونیک در سال ۲۰۰۲ به عنوان وسیله قانونی اصلی برای هدایت مدیریت فناوری اطلاعات فدرال و ابتکارات برای ایجاد اطلاعات و خدمات آنلاین در اینترنت و شامل نیازهای مختلف امنیتی سایبری است.

ـ قانون مدیریت اطلاعات فدرال امنیت اطلاعات در سال ۲۰۰۲ [9] مسئولیت های سازمان امنیت سایبری را تقویت و تدوین کرد، یک مرکز حادثه مرکزی فدرال ایجاد کرد و به جای وزیر بازرگانی؛[10]مسئولیت صدور استانداردهای امنیت سایبری فدرال را به عهده داشت.

بیش از ۴۰ قانون دیگر که توسط خدمات تحقیقات کنگره[11]شناسایی شده‌اند نیز مقررات مربوط به امنیت سایبری دارند. اصلاحات به بسیاری از این قوانین پیشنهاد شده است. بسیاری از لایحه‌ها و قطعنامه‌های سایبری در سه کنگره اخیر، بیش از ۴۰ نفر در کنگره های ۱۱۳ و ۱۱۲ و بیش از ۶۰ مورد در کنگره ۱۱۱ مورد معرفی شده اند. تعدادی از لایحه‌ها اصلاح قوانین کنونی را پیشنهاد می‌دهند و چندین مورد بحث و

1- NIST

۲- این اصطلاح در U. S. C. 44 تعریف شده است. §۳۵۴۲(ب) (۲)

3- OMB
4- CIO
5- HSA
6- DHS
7- CI
8- NSF NIST
9- (FISMA)، NIST
10- OMB
11- CRS

گفتگو را با چهار لایحه که به طور خاص در امنیت سایبری در پایان کنگره ۱۱۳ انجام شده است، دریافت کرده‌اند.

به طور کلی، اسناد قانونی در مورد امنیت سایبری در کنگره‌های اخیر به طور عمده بر مسائل در ۱۰ حوزه گسترده تمرکز کرده است:

ـ حفاظت از امنیت داخلی و زیرساخت‌های حیاتی (به خصوص شبکه برق و صنایع شیمیایی)،

ـ به اشتراک گذاری اطلاعات و هماهنگی بین بخش ها،

ـ مسئولیت‌ها و اقتدار سازمان های فدرال،

ـ اصلاح قانون مدیریت اطلاعات امنیت فدرال،

ـ تحقیق و توسعه (تحقیق و توسعه)،

ـ نیروی کار سایبری،

ـ نقض داده‌ها منجر به سرقت یا قرار گرفتن در معرض اطلاعات شخصی مانند اطلاعات مالی،

ـ جرایم سایبری و مجازات،

ـ استراتژی امنیت ملی سیتی،

ـ تلاش‌های بین‌المللی

برای بسیاری از این موضوعات، حداقل برخی از اسناد مربوط به آنها، تغییراتی را در قوانین جاری پیشنهاد کرده‌اند. با وجود عدم تصویب قانون سایبر، در کنگره‌های قبلی، به نظر می رسد که اساسا قابل توجه بودن حمایت از قوانین مهم برای رسیدگی به بسیاری از مسائل شناسایی شده در مجلس، مجلس سنا و کاخ سفید، روش های مختلفی را برای چنین قوانینی در نظر گرفته اند.

اسناد قانونی در کنگره‌های اخیر، روش‌های متعددی را برای رسیدگی به مسائل امنیتی سایبری در نظر گرفته‌اند. بحث زیر رویکردهای مختلفی را از سندهای کنگره‌های ۱۱۲ تا ۱۱۷ ارائه می‌دهد که مسائل زیر را در بر می گیرد: "موضوعات انتخاب شده در قانون پیشنهادی"، "به اشتراک گذاری اطلاعات مربوط به امنیت اطلاعات"، وزارتخانه های امنیت ملی برای حفاظت از سیستم های فدرال"، "اصلاح"، "نیروی کار سایبری"، و "تحقیق و توسعه"، و نیز بعضی "موضوعات دیگر" - قانون جرم گذاری جرایم، اعلان نقض اطلاعات و امنیت سایبری مربوط به دفاع است.[۱]

نسخه فرعی کمیته ای از سند فدرال [۲] قانون امنیت ملی را اصلاح کرد تا به وزیر امنیت داخلی برای انجام ارزیابی مستمر خطر ابتلا امنیت داخلی و زیرساخت های حیاتی به ویروس‌های اطلاعاتی بپردازد تا سالانه در طرح حفاظت از زیرساخت‌های ملی مورد استفاده قرار گیرد. [۳]همچنین برای بررسی مقررات سایبری

۱- برای بحث در مورد مسائل حقوقی مرتبط با حفاظت از سیستم های فدرال، امنیت داخلی و زیرساخت های حیاتی، و به اشتراک گذاری اطلاعات، نگاه کنید به گزارش CRS R42409

2- HR 367439

۳- وزارت امنیت داخلی، "طرح حفاظت از زیرساخت های ملی"، ۱۹ نوامبر ۲۰۱۴،

برای امنیت داخلی و زیرساخت‌های حیاتی تحت پوشش (به عنوان تعیین شده توسط وزیر) و پر کردن هر شکاف با استفاده از مجموعه‌ای از استانداردهای به رسمیت شناخته شده اجماع، در صورت لزوم، و برای کار با بنیاد ملی علوم برای ایجاد چنین استانداردهای در صورت لزوم اطلاحات لازمه صورت گرفته است. این قانون، پیشروی نظارتی فراتر از استانداردهای جمع آوری شده را ممنوع کرده است.

نسخه کامل سند کمیته تحقیقاتی قانون امنیت ملی را به شیوه‌ای متفاوت از نسخه فرعی کمیته تغییر داده است. این امر به وزیر امور خارجه اجازه می‌دهد در ارزیابی ریسک و سایر فعالیت‌های محافظتی با توجه به خصوصی‌سازی امنیت داخلی و زیرساخت‌های حیاتی تنها بر اساس درخواست صاحبان و اپراتورها، مشارکت داشته باشد. این امر به وزیر دارایی نیاز دارد تا یک استراتژی امنیت سایبری را برای سیستم‌های امنیت داخلی و زیرساخت‌های حیاتی ایجاد کند و تصریح می‌کند که این لایحه نمی‌تواند مجوز بیشتری برای وزارت امورخارجه امریکا در اختیار نهادهای فدرال یا غیر فدرال قرار دهد.

سندهای بعدی مقررات خاصی برای حفاظت از مصونیت امنیت داخلی و زیرساخت های حیاتی نداشتن؛ شبیه به آنهایی که در اسناد مورد بحث قرار گرفته است. با این حال، این لایحه مجازات جبران خسارت برای کامپیوترهای امنیت داخلی و زیرساخت های حیاتی را فراهم خواهد کرد و مانند سندهای مورد بحث در بالا، آنها شامل مقررات به اشتراک گذاری اطلاعات است که می تواند در حفاظت از مصونیت امنیت داخلی و زیرساخت های حیاتی مفید باشد.

لایحه در کنگره ی ۱۱۳ در محدوده ی زمانی کمتر از کنگره ۱۱۲ در نظر گرفته شده است. سند فدرال فرآیندی را ایجاب می کند که توسط بنیاد ملی علوم به همان شکل ایجاد شده در فرمان اجرایی ۱۳۶۳۶ ایجاد شود. دیگر اسناد مسئولیت قانونی را به عهده خواهند داشت و مسئولیت مرکز ملی، ادغام سیبرد و ارتباطات (امنیت داخلی و زیرساخت های حیاتی) توسط وزارت امنیت داخلی در سال ۲۰۰۹ تحت اقتدار قانونی موجود برای ارائه و تسهیل اشتراک اطلاعات و رخداد واکنش در میان موسسات امنیت داخلی و زیرساخت های حیاتی دولتی و خصوصی خصوصی شده است. سند بعدی فدرال در دسامبر ۲۰۱۴ اعمال شد. سند بعدی نیز مسئولیت وزارت امنیت داخلی را برای هماهنگی در بخش های امنیت داخلی و زیرساخت‌های حیاتی در زمینه امنیت سایبری فعالیت ها، ارائه پاسخ حادثه ای برای کمک به نهادهای امنیت داخلی و زیرساخت های حیاتی و ترویج توسعه فناوری های امنیتی سایبری به عهده دارد.

موانع برای به اشتراک گذاشتن اطلاعات در مورد تهدیدات، حملات، آسیب پذیری ها و سایر جنبه های امنیت سایبری - هم درون بخش ها و هم در بخش های مختلف - به عنوان مانع مهمی در حفاظت موثر سیستم های اطلاعاتی، به ویژه در ارتباط با امنیت داخلی و زیرساخت های حیاتی، در نظر گرفته شده اند. مثال‌ها شامل موانع قانونی، نگرانی در مورد مسئولیت و سوء استفاده، حفاظت از اسرار تجاری و دیگر

اطلاعات کسب و کار اختصاصی و عوامل نهادی و فرهنگی است؛ برای مثال، رویکرد سنتی به امنیت تمایل دارد تا تاکید بر محرمانه بودن، که لزوما مانع از تبادل اطلاعات شود.

اسنادی برای کاهش یا حذف چنین موانعی، از جمله مقررات اسناد قانونی در دو کنگره اخیر، موجب نگرانی شده است، برخی از آنها با هدف حذف موانع موجود مواجه مشکلاتی هستند که در حال حاضر مانع از اشتراک می شوند. برای مثال شامل خطراتی برای حفظ حریم خصوصی فرد و حتی سخنرانی آزاد و حقوق دیگر میشوند، استفاده از اطلاعات برای اهداف غیر از امنیت سایبری، مانند اقدامات نظارتی دولتی غیررسمی، بهره برداری تجاری از اطلاعات شخصی، یا توافق ضد رقابت میان شرکت های تجاری که در حال حاضر قوانین فدرال را نقض می کنند.[۱]

اصلاح قانون مدیریت اطلاعات امنیت فدرال

قانون مدیریت امنیت اطلاعات فدرال در سال ۲۰۰۲ به تصویب رسید. این چارچوبی را که در چندین قانون قبلی تصویب شده بود، مرور کرد. قانون مدیریت اطلاعات امنیت فدرال در ابتدا تصویب شد برای تمرکز بر روی روش و گزارش به جای امنیت عملیاتی، تاکمبود معیارهای به طور کلی پذیرفته شده امنیت سایبری، تغییرات در تفسیر آژانس از ماموریت در عمل، تمرکز بیش از حد بر روی سیستم‌های اطلاعاتی فردی به عنوان مخالف به اطلاعات عمومی آژانس معماری و معیارهای کافی برای اجرای انطباق در سازمانها و در سراسر سازمان مورد بررسی قرارگیرد.

هفت سند قانونی در کنگره ۱۱۲ (گزارش نیروی کار، پنج لایحه فدرال،[۲] سند کاخ سفید) قانون مدیریت اطلاعات امنیت فدرال را تجدید نظر می کنند، در حالی که بسیاری از چارچوب کنونی را حفظ می کنند: همه باید شرایط لازم را برای برنامه های امنیتی اطلاعات آژانس، بررسی مستقل سالانه برنامه های امنیتی، و گزارش‌های مربوط به اثربخشی و کمبود برنامه‌ها داشته باشند.

تمامی الزامات مورد نیاز برای نظارت مستمر بر سیستم‌های آژانس، از جمله نظارت خودکار باید فراهم شده باشد.

همه مسئولان قبلی می توانند مسئولیت بنیاد ملی علوم را برای توسعه استانداردهای امنیت سایبری، از جمله استانداردهای اجباری، حفظ کنند. یکی از لوایح[۳] مسئولیت فعلی وزیر بازرگانی را برای صدور استانداردها حفظ کرده است، در حالیکه دیگر لوایح[۴] و سند کاخ سفید این مسئولیت را به وزیر بازرگانی منتقل کرده است.

۱- نگاه کنید به " قوانین ضد ترویج و بخش ۵ قانون کمیسیون تجارت فدرال "

2- HR 4257، S 2105، S. 2151، S. 3342، S 3414

3- H. R. 4257

4- S. 2105، S. 2151، S. 3342، S. 3414

لایحه دیگری [1]نیز مسئولیت فعلی وزیر بازرگانی را برای نظارت بر سیاست امنیت اطلاعات فدرال و ارزیابی برنامه های اطلاعاتی سازمان آژانس حفظ کرده است. دولایحه دیگر[2]و سند کاخ سفید، مقامات و توابع را برای سیاست امنیتی اطلاعات از وزیر بازرگانی به وزارت امنیت داخلی منتقل کرده اند. وزیر بازرگانی قبلا تعدادی از مقامات را به وزارت امنیت داخلی به صورت اداری اختصاص داده بود، [3]و گزارش کار گروه بیانگر حمایت از این رویکرد است. برعکس، دولایحه دیگر[4]این مسئولیت را به وزیر بازرگانی منتقل کرده است. با این حال، هیچ یک از این اسناد به دبیران بازرگانی یا مقامات امنیت داخلی اجازه نداد تا برنامه های امنیت اطلاعات آژانس را تصویب یا رد کنند. فقط یک لایحه[5]به صراحت قدرت فعلی وزیر بازرگانی را حفظ کرده بود تا از اقتدار مالی خود برای تحقق پاسخگویی استفاده کند.

دو سند دیگر [6]و سند کاخ سفید، مقامات امنیتی جدیدی را به وزیر امنیت داخلی ملحق کرده، که مسئولیت آنها از جمله تشخیص نفوذ، استفاده از اقدامات متقابل، دسترسی به ارتباطات و دیگر ترافیک سیستم در سازمان ها و همچنین قدرت جهت آژانس های مستقر در انجام اقدامات محافظتی و در صورت تهدید قریب الوقوع بدون مشاوره قبلی برای حفاظت از سیستم های آژانس اقدام کنند، می باشد. این سند[7] وزارت امنیت داخلی را با نقش بسیار محدودتری در اختیار داشت و نیاز به انجام تجزیه و تحلیل امنیتی مداوم با استفاده از اطلاعات ارائه شده توسط سازمانها داشت. اما لایحه دیگری[8]این مسئولیت را به جای وزیر بازرگانی می دهد.

فقط یک لایحه[9]می‌تواند ماموریت فعلی قانون مدیریت اطلاعات امنیت فدرال را که مسئولیت وزیر بازرگانی را برای تضمین عملیات یک مرکز حوادث فدرال به عهده دارد حفظ کند. با این حال، اما دو لایحه دیگر [10]و سند کاخ سفید هر کدام حاوی مقررات دیگری بود که مرکزهایی را در داخل وزارت امنیت داخلی تشکیل می دادند که برای گزارش حادثه، اشتراک اطلاعات و سایر فعالیت های امنیتی سایبری فراهم شده بود. در مقابل، لوایح دیگر [11]شامل مقرراتی برای تسهیل گزارش دهی به تعدادی از مراکز بود.

1- H. R. 4257
2- S. 2105، S. 3414
۳- نگاه کنید به جفری زینتز، وویک کندری، و هوارد اشمیت، "دستورالعمل گزارشگری مالی برای قانون مدیریت امنیت اطلاعات فدرال و مدیریت حفظ حریم خصوصی آژانس"، M-10-15، 21 آوریل ۲۰۱۰ : http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-15. pdf; Orszag and Schmidt, "Clarifying Cybersecurity Responsibilities. "
4- S. 2151، S. 3342
5- H. R. 4257
6- S. 3414، S. 2105
7- S. 2151
8- S. 3342
9- H. R. 4257
10- . S. 3414
11- S. 3342، S. 2151

مقررات لایحه فدرال[1] عمدتا مشابه آنهایی که در کنوانسیون ۱۱۲ ریاست جمهوری در لایحه های[2] نیاز به صدور گواهینامه سازمان از امنیت وب سایت هایی که اطلاعات قابل شناسایی شخصی را جمع آوری می کنند، هستند. مرکز اطلاعات شناسایی شخصی[3] همچنین یک بخش را به قانون مدیریت اطلاعات امنیت فدرال اضافه خواهد کرد که نیاز به وزیر بازرگانی برای ایجاد رویه هایی برای آژانس هایی که در صورت نقض اطلاعات مربوط به اطلاعات شناسایی شخصی، از جمله اعلان افراد تحت تعقیب و سایر اقدامات به صورت مناسب، پیگیری می شود. در لایحه دیگری[4] گزارش شده است که قانون، مدیریت اطلاعات امنیت فدرال را برای تأیید قانونی، قانونی برای وزارت امنیت داخلی برای نظارت بر امنیت سیستم عامل آژانس در نظر می گیرد که مطابق با مجوز چنین اختیاری است که توسط وزیر بازرگانی در سال ۲۰۱۰ اعلام شده است [5] حال، بر خلاف برخی از لوایح قبل از آن، این لایحه [6] نه به طور خاص نیاز به نظارت مستمر از اطلاعات سیستم، اما نیاز به سازمانی برای پیاده‌سازی دستورات عملیاتی از وزارت امنیت داخلی را تاکید دارد، [7] که می تواند شامل مسئولیت انتقال برای مرکز حادثه فدرال به وزارت امنیت داخلی، و نیاز به وزیر بازرگانی برای ایجاد روش‌هایی برای اطلاع رسانی و پاسخ‌های دیگر را به نقض اطلاعات شناسایی شخصی برطرف سازد. نسخه پذیرفته شده ازلایحه [8] شامل برخی از زبان سازش، از جمله در استفاده از نظارت مستمر و روشن کردن نقش وزیر بازرگانی، وزارت امنیت داخلی، و سازمان های فردی است.

اصلاحات پیشنهادی از مقررات کنونی

برای شناسایی قوانینی که ممکن است نامزد برای تجدیدنظر قرار گیرند، خدمات تحقیقات کنگره یک جستجوی گسترده، مشاوره با متخصصین مختلف و بررسی منابع مختلف از جمله اسناد قانونی در کنگره‌های اخیر انجام داد. این جستجو بیش از ۵۰ قوانین بالقوه مربوطه را بدست آورد که تجدیدنظرهای پیشنهادی برای اکثر آنها مشخص شده است. [9] برای هر یک از قوانینی که در زیر بحث شده است، این گزارش حاوی مطالبی است که شامل:

1- H. R. 1163
2- H. R. 4257.H. R. 3635
3- PII
4- S. 2521

۵- Orszag و Schmidt، "روشن ساختن مسئولیت امنیت سایبری"

6- S. 2 ،521

۷- برنامه فعلی در وزارت امنیت داخلی، "تشخیص و کاهش مداوم "(CDM)، 2014 ژوئن ۲۴ توصیف شده است
http://www.dhs.gov/cdm .

8- S. 2521

۹- ۲۷ مدرک وجود دارد، اما یکی از قوانین ضد تراست شامل چهار قانون مختلف است. هیچ یک از دو لیست به طور قطعی یا جامع نبوده است. به عنوان مثال، برخی از تحلیلگران ممکن است استدلال کنند که مجوز های مجود بیشتر باید شامل شود، یا به طور متناوب، برخی از مقررات که شامل می شوند، از اهمیت زیادی برخوردار نیستند.

ـ نامی است که در قانون اساسی شناخته شده است،

ـ شماره قانون عمومی، که همراه با استنادات مقررات در قانون اساسی و مربوط به استنادات قوانین ایالات متحده می باشد. [۱]

ـ شرح مختصری از ارتباط قانون امنیت سایبری؛ و

ـ بحث در مورد تجدید نظرها یا به روز رسانی های سندی پیشنهاد شده است.

مقررات مورد بحث تنها شامل مواردی هستند که خدمات تحقیقات کنگره اسناد خاصی را برای تجدید نظر در آنها از ناظران مختلف و در منابع عمومی درخواست کرده است. مقررات جدیدی از قوانین فدرال که به صراحت به عنوان اصلاح قوانین جاری نامگذاری شده مشخص نشده است.

توصیه هایی برای زبان قانونی در اطلاعیه نقض داده ها در سند کاخ سفید و گزارش کار گروه است. این دو اسناد و لایحه مربوط به این موضوع که در کنگره ۱۱۲ معرفی شدند، ۷۹ قانون اساسی را که مورد تجدید نظر قرار می‌گیرد، مشخص می‌کند. یکی از این لایحه ها [۲] ۱۸ مورد قانونی فصل ۴۷ (تقلب و اظهارات غلط) با اضافه کردن یک بخش جدید در انتها را مورد بررسی قرارداده است، اما این مقرره هیچ قانون اسمی را که در لایحه یا قوانین ایالات متحده مشخص نشده است تغییر نمی‌دهد. بنابراین در بحث زیر درج نشده است. با این حال، این لایحه همچنین ۱۸ مورد قوانین ایالات متحده را تجدید نظر کرده است. سند کاخ سفید[۳] که توسط «قانون دسترسی تقلب و رایانه ای برای سوء استفاده و نقض قوانین سال ۱۹۸۴» اضافه شده است، نیز مورد بحث قرار گرفته است.

لایحه با مقرراتی است که به وضوح مربوط به یک قانون نامیده می شود، اما این قانون را صریحا اصلاح نمی کند. یک مثال از ۱۱۱ کنگره سندی [۴]است که مقررات امنیت سایبری را که ممکن است به عنوان اصلاحیه های قانون امنیت ملی تفسیر شود، بیان کرده اما به آن اشاره نشده است. این مقررات در این پژوهش بحث نشده است، زیرا تأثیرات آنها بر اساس قوانین خاص با اطمینان مشخص نیست. رویکردی که در این پژوهش استفاده شده از تمرکز بر مقررات توسط نام های متداول آنها در بسیاری موارد مفید است، اما در برخی موارد، به خصوص در رابطه با قوانین ایالات متحده، محدودیت های قابل توجهی دارد.

بعضی از قوانین، مانند قانون ایالات متحده آمریکا[۵] ، ممکن است در بسیاری از عناوین و بخش ها طبقه بندی شوند، [۶]که می توانند تجزیه و تحلیل را به چالش بکشند. با این حال، عدم همبستگی بین قوانین اعلام شده و اصلاحیه پیشنهادی در کد ایالات متحده که در بالا شرح داده شده است، ممکن است در مواردی

۱- برای اطلاعات بیشتر در مورد فرم های استناد، کتابخانه قانون کنگره، "اساسنامه های فدرال"، فوریه ۲۸، ۲۰۱۴ را ببینید
http://www.loc.gov/law/help/statutes.php .

2- S. 1151
3- § 1030
4- H. R. 5590
5- Patriot 2001

۶- این قانون به ۱۵ عنوان طبقه بندی شده است.

منجر به شکاف قابل توجهی در پوشش مقررات مربوط به قانون مربوط به امنیت سایبری با رویکردی مانند این شود. بنابراین، تجزیه و تحلیل ارائه شده در اینجا نمی تواند کامل باشد.

۱-۲-۵-۲- گفتار پنجم : به روز رسانی های احتمالی مقررات مربوطه مهم

استفاده از نیروهای نظامی را در اجرای قانون های غیرنظامی در ایالات متحده محدود می کند، مگر اینکه در داخل تسهیلات دولت فدرال باشد.[1]

دادگاه ها تصریح کرده‌اند که نقض این قانون زمانی رخ می دهد که اجرای قانون های غیرنظامی "استفاده مستقیم از تحقیقات نظامی" را منجر شود، زمانی که استفاده از ارتش برای فعالیت های مقامات غیرنظامی باشد یا زمانی که نیروی نظامی مورد استفاده قرار می‌گیرد تا شهروندان را به ارتش سوق دهد به صورت اجباری بوده است.

بعضی از ناظران ادعا می کنند که این قانون مانع از همکاری ارتش در امنیت سایبری با سازمان های مدنی می شود که ممکن است از تخصص و قابلیت‌های نظامی ساکنان ارتش و وزارت دفاع پشتیبانی کند.[2] علاوه بر این ممکن است گاهی اوقات دشوار باشد که یک حمله سایبری جنایی از یک دفاع ملی جدا باشد، به خصوص اگر حمله به قسمتی از امنیت داخلی و زیرساخت های حیاتی مرتبط باشد.

بعضی‌ها پیشنهاد دادند که این قانون اصلاح شود تا زمانی که ارتش آمریکا بتواند در داخل کشور در مورد تهدیدات اینترنتی به چنین زیرساخت هایی، که اکثر آنها به صورت خصوصی هستند، دسترسی داشته باشد. دیگران معتقدند که اصلا نیازی به تجدیدنظر نیست، زیرا رئیس جمهور تحت قانون فعلی مجاز است تا نظامیان را برای حمایت از مقامات مدنی در صورت وقوع یک فاجعه داخلی هدایت کند.

یادداشت توافق نامه بین وزارت امنیت داخلی، وزارت دفاع امریکا و ایجاد نیروی مأموریت ملی سایبری فرماندهی سایبری ایالات متحده برای حفاظت از اطلاعات جاسوسی ممکن است احتمال این که ارتش نقش مهمی در پاسخ دادن به یک حمله سایبری عمده در شبکه های اطلاعاتی آمریکا داشته باشد، افزایش دهد. با این حال، برخی معتقدند که دفاع از سیستم های اطلاعاتی ایالات متحده تنها باید در اختیار سازمان‌های غیرنظامی نظیر وزارت امنیت داخلی و پلیس فدرال آمریکا باشد، زیرا دخالت نظامی باعث ایجاد نگرانی های حریم خصوصی غیرقابل قبول و نگرانی های آزادی های مدنی می شود.

6- Posse Comitatus Act of 1879 Ch. 263, 20 Stat. 152. 18 U. S. C. §1385

۱- به عنوان مثال، نگاه کنید به جفری ک. تومر، "دیدگاه استراتژیک امنیت داخلی: اصلاح قانون مجلس و نقش DOD در امنیت داخلی" (تک نوشته، دانشکده مطالعات پیشرفته نظامی، فرماندهی ارتش ایالات متحده و کالج ستاد عمومی، فورت لاینوروست، کانزاس، ۱۱ جولای ۲۰۰۲)
http://www. dtic. mil/cgibin/GetTRDoc?Location=U2&doc=GetTRDoc. pdf&AD=ADA403866

۳-۱-۲- مبحث سوم : قوانین ضد ترویج و بخش ۵ قانون کمیسیون تجارت فدرال[1]

۱-۳-۱-۲- گفتار اول: بخش ۵ قانون کمیسیون تجارت فدرال۲

هنگامی که در قانون آمده است، اصطلاح "قوانین ضد تراست" به طور کلی یعنی سه قانون ذکر شده در قوانین ایالات متحده [۴]که سه قانون اول ذکر شده در بالا است. همچنین اغلب در فهرست قوانین ضد تراست شامل بخش [۵] قانون کمیسیون تجارت فدرال است که منجر به معاملات غیرمنصفانه و گمراه کننده می‌شود. بخش [۵] گنجانده شده است، زیرا دادگاه ها دریافتند که رقابت ناعادلانه شامل حداقل فعالیت‌هایی می‌شود که اعمال شرمن یا کلیتون را نقض می کنند.[۵]

قوانین ضد ترویج و همچنین بخش ۵ قانون کمیسیون تجارت فدرال مجموعه‌ای از مقررات است که مانع ترکیب یا توافق که به طور نامحدود محروم از تجارت باشد می‌شود. هر زمان که رقبا در یک بازار خاص اطلاعات را به اشتراک بگذارند، نگرانی های ضد تراست ممکن است به علت خطر توافق بین رقبا افزایش یابد.

توافقنامههای به اشتراک گذاری اطلاعات بین شرکت‌های خصوصی ممکن است تحت تاثیر نظارت بر ضد آن باشد، زیرا اشتراک اطلاعات بین رقبا، فرصت‌هایی برای همکاری با هدف محدود کردن تجارت ایجاد کند. [۶]با این حال، توافقنامه‌های به اشتراک گذاشتن اطلاعات برای مبارزه با امنیت سایبری ممکن است با اصول ضد تروریستی مطابقت داشته باشد تا زمانی که اهداف آنها برای مبارزه با تهدیدات سایبری به جای مانع رقابت باشد. [۷]برخی از ناظران ممکن است استدلال کنند که برای توسعه توافقنامه های موثر و کارآمد در زمینه اطلاعات برای تهدیدات امنیتی سایبری، یک معافیت صریح از قوانین ضد تروریستی برای این موافقتنامه ضروری است. کنگره قبلا چنین معافیتی را پیشنهاد کرده است. به عنوان مثال، لایحه [۸] (کنگره ۱۰۷) یک معافیت بهره برداری از قوانین ضد تراست و بخش ۵ قانون کمیسیون تجارت فدرال را به افراد قانون‌گذار و اجرایی توافق‌های وارد شده صرفا به منظور "تسهیل اصلاح یا اجتناب از امنیت سایبری" مشکل مربوط به آن یا ارتباط یا افشای اطلاعات برای کمک به تصحیح یا جلوگیری از اثرات یک مسئله مربوط به امنیت سایبری است، قائل شده است. چنین معافیتی، بعد از تصویب کنگره، به شرکت

1- Sherman Antitrust Act Ch. 647, 26 Stat. 209. 15 U. S. C. §§1-7. Wilson Tariff Act Ch. 349, §73, 28 Stat. 570. 15 U. S. C. §§8-11. Clayton Act P. L. 63-212, 38 Stat. 730. 15 U. S. C. §§12-27.

2- FTC

3- Ch. 311, §5, 38 Stat. 719. 15 U. S. C. §45(a).

4- §12 (a) ،

5- United States v. American Airlines Inc. , 743 F. 2d 1114 (5th Cir. 1984); FTC v. Motion Picture Advertising Serv. Co. , 344 U. S. 392, 394-95 (1953); FTC v. Cement Institute, 333 U. S. 683, 694 (1948); Fashion Originators' Guild v. FTC, 312 U. S. 457, 463-64 (1941).

6- Federal Trade Commission and Department of Justice, Antitrust Guidelines for Collaborations among Competitors, April 2000, http://www. ftc. gov/os/2000/04/ftcdojguidelines. pdf.

7- Ibid.

8- HR 2435

کنندگان در بازار اجازه می‌دهد که در به اشتراک گذاشتن اطلاعات برای مبارزه با تهدیدات امنیتی سایبری بدون نگرانی در مورد پیروی از قوانین ضد تراست شرکت کنند.

گزارش کارگروهی، اظهار داشت که ممکن است معافیت ضد ترویج مورد نیاز باشد. یکی از لوایح [1]در کنگره‌ی ۱۱۳، به طور خاص قوانین مربوط به قوانین ضد قانون را ذکر نمی کند، اما"با وجود هرگونه قانون دیگر" اجازه می‌دهد اطلاعات مربوط به امنیت سایبری را در میان اشخاص حوزه ی خصوصی تقسیم کنند.[2] به طور صریح اطلاعات مربوط به تهدیدات امنیت سایبری از قوانین ضد کنترلی تبادل اطلاعات میان نهادهای خصوصی معاف می‌شود. دیگران می‌توانند ادعا کنند که قوانین ضدترویج در طبیعت انعطاف پذیر هستند، به ویژه به این دلیل که آنها به توافقنامه های به اشتراک گذاری اطلاعات مربوط می‌شوند و قوانین به طور انعطاف پذیر توسط ادارات قضایی مورد استفاده قرار می‌گیرند. این ویژگی انعطاف پذیر ممکن است نیاز به معافیت های معین از استفاده از قوانین را از بین ببرد، در حالی که سازمان های ضد تراست درگیر و آگاه از شرکت در توافق در مورد اشتراک اطلاعات هستند.[3]وزارت دادگستری درحال حاضر به شرکت‌هایی که مایل به ایجاد توافقنامه‌های اشتراکی در مورد مجازات و رقابت در رسیدن به اهداف ارائه شده در طرح‌های خود را برای همکاری با آژانس هستند توجه بسیاری دارد. [4]دستور العمل بازرگانی معمولا بیان می‌کند که وزارت دادگستری قصد ندارد قوانین ضدکنترلی را علیه همکاری سندی اعمال کند. وزارت دادگستری دستور العمل‌های کسب و کار را برای شرکت هایی که قصد اشتراک گذاری اطلاعات را برای مبارزه با تهدیدات امنیتی سایبری دارند، منتشر کرده است. وزارت دادگستری و کمیسیون تجارت فدرال راهنمایی های مشترک را ارائه کرده‌اند که "به طور صحیح اشتراک گذاری اطلاعات تهدید اینترنتی ضد ترویج را افزایش دهد"[5]

۲-۳-۱-۲- گفتار دوم : مؤسسه ملی استاندارد و فناوری قانون[6]

مقررات اصلی بیان مسئولیت های سازمانی مربوط به استانداردهای فنی را به عهده داشت. بعدها اصلاحات به طور کلی مفاد مربوطه را به طور خاص اضافه خواهد کرد.

موضوعات تحقیقاتی مرتبط، از جمله سیستم های کامپیوتری و مخابراتی، امنیت اطلاعات و سیستم های کنترل، شناسایی شده است.

1- HR 624
2- S 2588

۳- به کمیسیون تجارت فدرال و اداره عدالت، راهنمایی های ضد تراست نگاه کنید.

4- 28 C. F. R. §50. 6.

۵- وزارت دادگستری و کمیسیون تجارت فدرال، "بیانیه سیاست های ضدتروریسم در مورد به اشتراک گذاری اطلاعات مربوط به امنیت اطلاعات"، ۱۰ آوریل ۲۰۱۴

http://www.justice.gov/atr/public/guidelines/305027. pdf .

6- Ch. 872, 31 Stat. 1449. 15 U. S. C. §271 et seq

یک برنامه استاندارد کامپیوتری را در موسسه ملی استاندارد و فناوری(بنیاد ملی علوم) اجرا کردند.

علیرغم اقتدار فعلی بنیاد ملی علوم برای انجام تحقیق در مورد کامپیوترها و امنیت اطلاعات، نگرانی هایی مطرح شده است که آیا این فعالیت ها باید با در نظر گرفتن محیط تهدید در حال رشد برای امنیت سایبری افزایش یابد. در کنگره ۱۱۱، یک لایحه[1] که توسط مجلس تصویب شد، نیازمند تحقیقات داخلی در زمینه مدیریت هویت و امنیت سیستم های اطلاعاتی، شبکه ها و سیستم های کنترل صنعتی بود. لایحه های مشابه[2] مجلس را در کنگره ۱۱۲ و ۱۱۳[3]به تصویب رساندند.[4]

همیچنین در حقوق آمریکا نیز می‌توان با اشاره به بخش‌های ۲۳۳۲ تا قسمت I ۲۳۳۲ از زیر فصل B۱۱۳ تروریسم از فصل یکم با عنوان جرائم و آیین دادرسی کیفری دیده می شود که بسته به اوضاع و احوال و کیفیت جرم تروریستی ارتکابی طیف وسیعی از مجازات ها شامل جزای نقدی تا حبس ابد و اعدام در نظر گرفته است. این کدها در سیستم قانون‌گذاری فدرال شامل مجلس نمایندگان، مجلس سنا و رئیس جمهور، تصویب اجرایی و جرم انگاری و مجازات معین کرده است.

در آمریکا کنترل و نظارت بر همه جرائم سایبری بر عهده واحد جرائم سایبری است که به موجب بخش ۴۲۳ از قسمت H از زیر فصل ۷ ام از فصل یکم از عنوان ۶ امنیت داخلی تاسیس شده است.

بخش ۷۴۰۳ از فصل ۱۰۰ از عنوان ۱۵ اجازه دسترسی به زیرساخت ها و سیستم ها اعم از نرم افزار و سخت افزار و شبکه هارا به منظور تحقیقات، کشف و تعقیب جرائم سایبری داده است.

به موجب الحاقیه بخش ۵۰۹ از فصل ۳۱ از قسمت دوم از عنوان ۲۸ آیین دادرسی کیفری، دادستان کل آمریکا باید برای بررسی قانونی و رهگیری و تهیه و حفظ ادله در جرائم سایبری اقدام به تاسیس مکان آزمایشگاهی مناسب همراه با تعدادکافی تجهیزات و آموزش و پرسنل و دادستان، تحت نظارت خود نماید.

در قانون میهن پرستی آمریکا بخش به تروریسم سایبری اختصاص داده شده است که این بخش در قانون مرتبط بعدی یعنی قانون آزادی آمریکا نیز ابقا نگردیده است. بنابراین اینطور متصور است که عنصر قانونی برخورد با جرائم سایبری همان مشمول تعریف کلی بخش ۲۳۳۱ از فصل 113B از قسمت اول از عنوان ۱۸ جرائم آیین دادرسی کیفری باشد و مجازات آن نیز مجازات‌های مقرر در بخش ۲۳۳۲ از همین فصل و قسمت و عنوان برجسب نوع و شدت باشد.

در آخر باید به بررسی‌های کنگره در سال ۲۰۱۸ بپردازیم. در نیمه اول سال ۲۰۱۸، کنگره ایالات متحده مشغول طراحی قوانینی است که اهداف فروشندگان خدمات و محصولات خارجی را که خطر آلودگی به

1- H. R. 4061
2- H. R. 2096
3- H. R. 756

۴- همچنین نگاه کنید به " لایحه تحقیق و توسعه. H. R. 3696 "و S. 1353 سند (کنگره ۱۱۳) در قانون که فرایند ایجاب می کند که توسط بنیاد ملی علوم شبیه آنچه که در دستورالعمل ۱۳۶۳۶ ایجاد شده برای ایجاد استانداردهای و شیوه های توافق برای رسیدگی به امنیت سایبری امنیت داخلی و زیرساخت های حیاتی ایجاد کند. همچنین نگاه کنید به "اقدامات شعبه اجرایی" و "موضوعات انتخاب شده در قانون سندی".

آژانس های دولتی را به خطر می‌اندازد، تهدید می کند در همین حال، کمیسیون امنیت و بورس[1] راهنمای جدیدی را درباره سیاست‌ها و روش‌های سیسکو برای شرکت‌های ثبت شده منتشر کرده است. این کمیسیون امنیت و بورس دستورالعمل تفسیری در مورد افشای اطلاعات عمومی در مورد امنیت سایبری را در ۲۱ فوریه ۲۰۱۸ منتشر کرد. این راهنمایی به مسئولیت‌های هیئت مدیره مربوط می شود تا اطمینان حاصل شود که شرکت‌ها در برنامه‌ریزی و پاسخ به عملیات‌های اینترنتی، در حال برنامه ریزی هستند و ممکن نیست باعث آسیب مالی به سرمایه گذاران شود. طبق گفته کنگره، شرکت ها باید :بررسی مجدد فرآیند که هیئت مدیره شرکت استفاده می کند تا مسئولیت خود را برای نظارت بر ریسک امنیت سایبری بر عهده بگیرد؛ بررسی خط مشی‌ها و روش‌های شرکت مربوط به کنترل و روش‌های افشای اطلاعات، تجارت خودی و افشای اطلاعات انتخابی را به عهده بگیرید و در نظر بگیرید که آیا فاکتور ریسک امنیت سایبری و سایر اطلاعات افشا شده شرکت باید تجدید شود. کمیسیون امنیت و بورس همانطور که در مقررات امنیت سایبری در ایالت نیویورک برای بخش مالی فعالیت می کند، مسئولیت آن را در هیئت مدیره برای برنامه ریزی شرکت های ذکر شده برای پاسخگویی به نقض امنیت سایبری مطرح می کند. همانطور که پیشنهاد کنگره می گوید: "کمیسیون امنیت و بورس انتظار دارد شرکت ها در مورد خطرات و حوادث سایبری که برای سرمایه گذاران مهم هستند، افشاسازی کنند." کمیسیون امنیت و بورس می‌خواهد هیئت مدیره درک کند که شرکت امنیتی سایبری دیگر فقط یک بخش فناوری اطلاعات نیست.

بررسی نظام حقوقی ایران

به گزارش افتانا[2] تروریسم سایبری که این روزها وارد چهارمین دهه عمر خود شده، اکنون چنان گسترش یافته که از سال ۲۰۱۲ به عنوان سال جهنمی در این زمینه نام برده و اینگونه اظهار میشود که در این فضا افراد با داشتن یک میلیارد دلار و کمتر از پنجاه نفر نیروی متخصص قادر خواهند بود یک کشور را از کار بیندازند. این موضوع برروی کشور ما نیز بی‌تاثیر نبوده و طی این مدت ایران نیز در فضای سایبری مورد حملات مختلف قرار گرفته و تلاشهایی شده است تا بخش‌های مختلفی مانند نفت، صنعت، بانک و. . . از کار افتاده و یا دچار اختلال شوند. شمار حملات ریز و درشتی که در این زمینه صورت گرفته چنان وسیع بوده که وزیر ارتباطات زمانی شمار آنها را حتی تا ۱۴ هزار حمله ارزیابی کرده بود. در این میان در شرایطی که هنوز مدت زیادی از حملاتی مانند فلیم (شعله آتش) و مینی فلیم نمیگذرد این روزها در فضای رسانهای از حمله بدافزار جدیدی به نام ناریلام صحبت می‌شود.

1- SEC

۲- پایگاه خبری امنیت فناوری اطلاعات

استاکس نت و حمله به بخش صنعتی اواسط سال ۸۹ بود که رسانه‌های مختلف در سطح دنیا بحث حمله ویروس جاسوسی به نام استاکس نت خبر داده و بر این نکته تاکید کردند که این ویروس بخش صنعتی کشورها را مورد حمله قرار داده و برخی رایانه‌های ایران را هم تحت تاثیر قرار داده است. البته در همان دوره محسن حاتم [۱]با اشاره به اینکه هجوم ویروس استاکس نت به رایانه‌های ایرانی میتواند دارای دلایل اقتصادی یا سیاسی باشد، گفت: آلودگی به این ویروس از حدود هشت ماه پیش در ایران آغاز شده و مشخص نیست چرا رسانه های بیگانه هم اکنون این موضوع را مطرح می‌کنند. وی عمده مراکز مورد تهاجم این ویروس صنایع مربوط به بخش نفت و نیرو دانسته و از شناسایی IPهای آلوده و طراحی آنتی ویروس خبر داده بود. البته این بدافزار کشورهای متعددی مانند هند، اندونزی و پاکستان را هم مورد حمله قرار داده بود. گاوس و سیستم بانکی ویروس گاوس را می‌توان به عنوان یکی دیگر از حملات سایبری دانست که هدف اصلی آن کشورهای خاورمیانه بود. این ویروس که به عقیده بسیاری از کارشناسان جهان توسط همان طراحان استاکس نت طراحی شده بود قابلیت حمله به زیرساخت‌های اصلی کشورها را داشت. این بدافزار در ۱۰ آگوست سال ۲۰۱۲ تحت خانواده تروجان‌ها شناسایی و در اواسط سال ۲۰۱۱ به عنوان تروجان بانکی توسط مهاجمین مورد استفاده قرار گرفته و سیستم‌های هدف این بدافزار، سیستم‌های خانواده ویندوز ارزیابی شده بود. در واقع این تروجان به منظور دستیابی به اطلاعات سیستم‌های قربانی و سرقت اطلاعات اعتباری، پست الکترونیکی و شبکه های اجتماعی ایجاد شده بود و کارکرد آن به این شکل نبود که همه نوع اطلاعات قابل جمع‌آوری در آن ذخیره شود بلکه مشخصات سیستم استفاده شده و اطلاعات بانکی و اینترنتی مرورگر مورد علاقه این بدافزار بود. شعله آتش در تجهیزات نفتی اما در این مدت یکی از جدی ترین حملات سایبری حمل‌های بود که نسبت به تجهیزات نفتی کشورهای خاورمیانه صورت گرفت. این بدافزار که با نام فلیم[۲]به کشورهای مختلفی ارسال شده بود، پیچیدگی‌های متعددی داشت و علاوه بر جاسوسی، یک ویروس مخرب به شمار می‌رفت. در این زمینه پیش از گزارش شرکت سیمانتک تصور میشد که ویروس "فلیم" تنها یک ابزار جاسوسی و سرقت اطلاعات بوده است اما ویکرام تاکور، سخنگوی شرکت سیمانتک گفت که این شرکت یکی از بخش‌های ویروس "فلیم" را شناسایی کرده که میتواند فایل‌ها را از کامپیوترها نخست فلیم یا گاوس برای آلوده ساختن حداکثر تعداد ممکن قربانیان و جمع‌آوری حجم زیادی از اطلاعات مورد استفاده قرار می‌گیرند. پس از اینکه داده‌ها جمع‌آوری و بازبینی شدند، یک قربانی جالب توجه انتخاب شده و شناسایی می‌شود. سپس مینی فلیم برروی سیستم قربانی منتخب نصب می‌شود تا به نظارت عمیق تر و جاسوسی دقیق‌تر ادامه دهد. پاک کند و این بدان معنی است که ویروس "فلیم" می‌تواند به برخی از برنامه‌های مهم سیب وارد کرده و اجرای آنها را مختل کند و حتی می‌تواند به طور کلی سیستم عامل را از کار بیندازد. چند روز پس از انتشار اخبار مربوط به این

۱- معاون وقت وزیر صنایع

۲- شعله آتش

بدافزار، مرکز ماهر مدعی شد که برای نخستین بار در دنیا، ابزار پاکسازی بدافزار فلیم را تولید و به زودی از طریق سایت مرکز ماهر در اختیار کاربران قرار خواهد داد. شعله آتش از جمله بدافزارهای پیچیدهای محسوب می‌شد که از طریق ۴۳ آنتی ویروس مختلف، امکان شناسایی این بدافزار وجود نداشت. علاوه بر ایران در این حوزه، فلسطین، مجارستان، لبنان، استرالیا، سوریه، روسیه، هنگ کنگ و امارات از جمله کشورهایی بودند که مورد هدف این بدافزار قرار گرفتند.

اواخر تیرماه امسال بود که یک ویروس که بیش از هشت ماه از شروع فعالیت آن میگذشت، شناسایی شد و اینگونه اعلام شد. که حدود ۸۰۰ رایانه توسط این بدافزار آلوده شده است. خبر انتشار این ویروس اولین بار توسط کسپرسکی اعلام شد که ادعا می‌کرد که این تروجان بیش از ۸۰۰ کامپیوتر را آلوده کرده و بیش از هشت ماه از شروع فعالیت آن می‌گذرد و مشخص نیست چرا یک بدافزار ساده که از مدت‌ها قبل توسط شرکتهای معتبر آنتی ویروس شناسایی شده بود، در یک مقطع زمانی به طور گسترده تحت پوشش خبری قرار گرفته است ثبت اطلاعات صفحه کلید، عکس گرفتن از صفحه مانیتور در فواصل مشخص، عکس گرفتن در صورت استفاده از قبیل، و ایجاد درهای پشتی جهت نفوذ و دسترسی مهاجم، ضبط، ذخیره و ارسال فایلهای Gmail و یاskype ، facebook. صوتی از جمله کارکردهای این ویروس بود وزیر ارتباطات و فناوری اطلاعات درباره این بدافزارخطاب به کاربران گفته بود که از باز کردن ایمیل‌ها و فایل هایی که از. طریق کاربران ناشناخته برای آنها ارسال میشود خودداری کنند گویای آن بود که یک بدافزار ساده و کم هزینه بوده و در آن از هیچ بررسی های به عمل آمده بر روی نمونه های آسیب پذیری خاصی جهت انتشار و آسیب رسانی به سیستم ها استفاده نشده است. لذا بر خلاف ادعا های صورت گرفته مبنی و در نظر گرفتن آن به عنوان یک تهدید هدفمند سایبری در مقایسه این بدافزار با تهدیداتی نظیر فلیم دور از ذهن بنظر میرسد. مینی فلیم اوایل مهر ماه ۱۳۹۳ و در شرایطی که تنها چند ماه از انتشار بدافزارهایی مانند فلیم و گاوس می گذشت این بار بدافزاری با نام مینی فلیم جاسوسی خود را آغاز کرد. در ارتباط با این بدافزار اینگونه اعلام شده بود که مینی فلیم در واقع شکلی جدید از بدافزار فلیم است که توسط حکومتها پشتیبانی می‌شود و به طور خاص برای جاسوسی طراحی شده و جایی که کار فلیم تمام می شود این بدافزار آغاز به کار می‌کند. در توضیحات کسپرسکی درباره مینی فلیم آمده بود: نخست فلیم یا گاوس برای آلوده ساختن حداکثر تعداد ممکن قربانیان و جمع آوری حجم زیادی از اطلاعات مورد استفاده قرار میگیرند. پس از اینکه داده ها جمع آوری و بازبینی شدند، یک قربانی جالب توجه انتخاب شده و شناسایی میشود. سپس مینی فلیم برروی سیستم قربانی منتخب نصب میشود تا به نظارت عمیق تر و جاسوسی دقیق تر ادامه دهد. بنا بر اعلام مرکز ماهر، احتمالا توسعه دهندگان مینی فلیم کار خود را در سال ۲۰۰۷ آغاز کرده اند. نکته دیگر آن که گفته می شد نرخ آلودگی این بدافزار به خصوص در مقایسه با گاوس و فلیم پایین بوده و تنها ۵۰ تا ۶۰ کامپیوتر در سراسر جهان توسط این بدافزار آلوده شده اند. اما در این نوع حملات تمرکز برروی تعداد قربانیان نیست، بلکه بیشتر اهداف خاص مد نظر است. در اوئل سال ۹۰ از ورود

بدافزاری تازه با نام ناریلام صحبت میشود که البته مرکز ماهر در این باره بر این نکته تاکید دارد که این بدافزار در سال ۸۹ توسط مراکز و شرکت‌های فعال در حوزه امنیت فناوری اطلاعات کشور شناسایی و گزارش شده است. در اطلاعیه مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ایی آمده است: بررسی‌های اولیه تا این لحظه نشان میدهد بدافزار فوق الذکر بر خلاف اخبار منتشر شده تهدید جدی سایبری نبوده بلکه یک بدافزار محلی است که احتمالا به منظور آسیب زدن به کاربران محصولات نرم افزاری شرکت خاص ایجاد شده است. طراحی و پیاده سازی این بدافزار اثری از پیچیدگیهای یک حمله سایبری یا حتی بدافزارهای قدرتمند گروههای خرابکار سایبری را ندارد و بیشتر شبیه یک بدافزار آماتوری است. دامنه فعالیت این بدافزار و انتشار آن بسیار محدود بوده و تنها کاربران محصولات نرمافزاری سیستمهای مالی و حسابداری میتوانند نسبت به اسکن سیستم توسط آنتی ویروس بروز شده اقدام کنند. البته با این وجود برخی از فعالان فضای مجازی در این زمینه بر این نکته اذعان داشتند که فارغ از اینکه آیا می توان گونه جدید ویروس ناریلام را یک بدافزار "ضد ایرانی" با اهداف سیاسی در نظر گرفت که با هدف حمله به زیرساخت‌های اطلاعاتی کشور تولید و منتشر شده و یا برعکس بزرگنمایی این ویروس در رسانه‌ها را یک ترفند تجاری، تبلیغاتی یا رسانه‌ایی تلقی کرد، مدیران شبکه های سازمانی کشور باید حداکثر توجه و هشیاری را در رعایت جوانب حفاظتی و امنیتی در شبکه به خرج دهند تا احتمال نفوذ این بدافزار و یا آلودگیهای ویروسی مشابه را به حداقل برسانند.[1]

استاکس نت کنترل دستگاه‌ها را به دست می گرفت و هدف آن سانتریفوژهای هسته‌ای در کارخانه نطنز ایران بود. این ابزار طوری طراحی شده بود که بسیار سری باشد تا حکم اقدام جنگی را که معمولا آشکار است پیدا نکند به گزارش شبکه تلویزیونی سی ان ان، الکس گیبنی، سازنده فیلم «روزهای صفر» در گفتگو با این شبکه تاکید کرد، استاکس نت کار موساد و سیا بوده است. کریستین امانپور درباره موضوع هسته ای ایران و حمله چند سال پیش به این برنامه با استفاده از بدافزار استاکس نت گفت بدافزار به حدی قوی است که به روشنی می توان عنوان اسلحه سایبری را به آن اطلاق کرد. الکس گیبنی کارگردان آمریکایی فیلم مستندی درباره استاکس نت و جنگ سایبری با عنوان «روزهای صفر» ساخته است. در این باره می گوید. الکس گیبنی درباره استاکس نت گفت، ابتدا استاکس نت را کسی نمی شناخت تا اینکه کارشناسان امنیت سایبری درباره آن صحبت کردند و مطالبی نیز در نشریات درباره آن نوشته شد. دیوید سانگر نیز در نیویورک تایمز درباره آن مطلب نوشت. بعد از آن بود که ما نیز مطالعات عمیق تری را درباره استاکس نت شروع کردیم.

1- http://ui.ac.ir/herasat

مبحث اول: قانون مبارزه با حمایت مالی تروریسم

در سال ۱۳۸۲ برای اولین بار لایحه‌ای با عنوان مبارزه علیه تروریسم در دولت جمهوری اسلامی ایران تهیه و کارشناسی های متعددی در مورد آن صورت گرفت؛ اما به دلایل اینکه به اعتقاد برخی با وجود جرم انگاری جرایم شبه تروریستی همچون محاربه و افساد فی الارض نیازی به جرم انگاری تروریسم نداریم، این لایحه به تصویب نرسید ؛ اما از آغازین دهه ۹۰ موضوع تروریسم و ضرورت جرم انگاری آن به عنوان یک جنایت یا رفتار مجرمانه تعزیری مجدداً بر سر زبان ها افتاد و براساس شرایط خاص زمانه و متأثر از ضرورت دوران گذار از قطعنامه های تحریمی علیه جمهوری اسلامی ایران، بخش مبارزه علیه تأمین مالی تروریسم از کل موضوع مبارزه علیه تروریسم، مورد توجه سیاست جنایی تقنینی قرار گرفت و " قانون مبارزه با تأمین مالی تروریسم" در تاریخ ۹۴/۱۲/۲۲ تصویب و به تاریخ ۱۰ فروردین ۱۳۹۵ ابلاغ گردید. بدون شک صرف نظر از اینکه ایراد اساسی مبنی بر عدم جرم انگاری مستقل و کیفرگذاری دقیق جرایم و جنایات تروریستی به حال خود باقی است، تصویب قانون فوق با حواشی متعددی که در حوزه مبارزه با پولشویی ایراد می‌نماید، می‌تواند گویای عزم جمهوری اسلامی ایران در مبارزه با ریشه ها و زمینه‌های افعال تروریستی باشد. نظام حقوقی ایران در مواجهه با جهانی شدن حقوق کیفری، بیشترین همگرایی را در خصوص موضوعات مرتبط با ابعاد مختلف اقتصادی داشته؛ بر همین اساس تأمین مالی تروریسم همانند پولشویی با فشار و پیگیری نهادهای اقتصادی به موضوع حقوق کیفری ایران تبدیل شده است ؛ عوامل و نهادهای درگیر با مبارزه با تأمین مالی تروریسم بسیار گسترده و فراگیر می باشد که در این میان بانک مرکزی به عنوان مقام پولی کشورها در راستای ایفای وظایف خود به ویژه تنظیم حجم نقدینگی و کنترل نرخ تورم، ناگزیر از رویارویی با ابعاد گوناگون اقتصاد پنهان که تأمین مالی تروریسم از مصادیق آن است، می باشد.

در بررسی قانون، باید گفت که مهم‌ترین نکته‌ای که در متن قانون ذکر شده است، نه تعریف تامین مالی تروریسم، بلکه تعریف خود تروریسم است. در این قانون، برای نخستین بار تروریسم در نظام حقوقی ایران تعریف شده است. پیش از این در حقوق ایران، تروریسم تعریف نشده بود و اگر با کسی که تروریست بود برخورد قانونی می‌شد، بر اساس سایر عناوین مجرمانه نظیر محاربه، افساد فی‌الارض، کودتا و نظایر آن بود. در این قانون، از تروریسم تعریف نسبتاً پیچیده‌ای ارائه شده است که برگرفته از کنوانسیون سازمان ملل متحد برای مبارزه با تامین مالی تروریسم است.

تعریف ارائه‌شده در قانون مبارزه با تامین مالی تروریسم ایران در یک نکته با تعریف کنوانسیون بین‌المللی مبارزه با تامین مالی تروریسم تفاوت دارد. در حالی که در کنوانسیون بین‌المللی، قید شده است که مجنی‌علیه عملیات تروریستی کسی است که نظامی فعال در جریان مخاصمه مسلحانه نیست، در قانون

۱- رضوی فرد، بهزاد (۱۳۹۶)، سخن دبیر علمی همایش، چکیده مقالات همایش بین المللی ابعاد حقوقی – جرم شناختی تروریسم، تهران: انتشارات دانشگاه عالمه طباطبایی، چاپ اول صفحه ۵

تصویب‌شده در ایران، قید شده است که مجنی‌علیه عملیات تروریستی، کسی است که دارای مصونیت قانونی است. چرا چنین تفاوتی وجود دارد؟ به نظر می‌رسد یک اشتباه در ترجمه باعث تصویب قانون ایران به این شکل شده است. از منظر حقوقی، اگر شخصی، شخص دیگری را در جنگ بکشد، تروریست محسوب نمی‌شود و متخاصم یا رزمنده محسوب می‌شود و اگر دستگیر شود، نمی‌شود او را به عنوان تروریست بازداشت و محاکمه کرد. تصور کنید که دولت ایران، با یک دولت خارجی در حال جنگ است. رزمنده ایرانی اسیر می‌شود، دولت خارجی حق ندارد اسیر جنگی را به عنوان تروریست در دادگاه‌های خود محاکمه و مجازات محکوم کند و برعکس، ایران هم حق چنین کاری را با اسرای طرف مقابل ندارد.

بنابراین، اگر چه رزمنده ایرانی عمل خشونت‌باری (جنگ) را علیه دولت خارجی انجام می دهد و قصد او هم تاثیرگذاری بر سیاست و خط‌مشی دولت متخاصم است، اما این عمل را نمی توان تروریستی به حساب آورد؛ چون او با رزمندگان دولت مقابل جنگیده است نه با شهروندان عادی. در حقوق جنگ، این عبارت به این صورت گفته می‌شود، «رزمنده کسی است که می تواند بکشد و می تواند کشته شود». یعنی اگر بکشد، تروریست نیست و اگر کشته شود، قاتل او تروریست محسوب نمی‌شود. بنابراین، اعمال خشونت علیه دیگری انجام دهد، در صورتی عمل وی تروریستی محسوب خواهد شد که مجنی‌علیه، رزمنده نباشد. همچنین اگر حکم اعدام کسی صادر شده باشد و مأمور اجرای حکم، این حکم را اجرا کند، کسی که این حکم را اجرا کرده است، تروریست محسوب نخواهد شد ولو اینکه این عمل، خشونت‌بار است. بر این اساس، در برخی از اسناد بین‌المللی از عبارت innocent people استفاده شده است. این عبارت، به معنای شخصی است که رزمنده یا محکوم به اعدام نیست.

در ایران، این عبارت به اشخاص دارای مصونیت قانونی ترجمه شده است. حال آنکه شخص دارای مصونیت قانونی کسی است که از مصونیت دیپلماتیک یا پارلمانی برخوردار است و این ترجمه صحیح نیست. در حال حاضر، تفسیر این بند از ماده (۱) قانون به این صورت خواهد بود که اگر شخصی سفیر یک کشور خارجی در ایران را به قصد تاثیرگذاری بر خط‌مشی ایران بکشد، مرتکب عملیات تروریستی شده است اما اگر صدها نفر ایرانی را که مصونیت ندارند بکشد، نمی توان او را تروریست محسوب کرد. چنین رهیافتی نه با استانداردهای بین‌المللی و نه با عقل سلیم مطابقت دارند و به نظر می‌رسد در اولین فرصت باید نسبت به اصلاح این قسمت از قانون و رفع این ایراد اقدام کرد.

تعریف دوم، که از تروریسم شده است، عبارت است از ارتکاب برخی اعمال با قصد تاثیرگذاری بر خط‌مشی جمهوری اسلامی ایران یا سازمان‌های بین‌المللی دارای نمایندگی در قلمرو جمهوری اسلامی ایران. اعمالی همچون خرابکاری در اموال و تاسیسات عمومی دولتی و غیردولتی، ایراد خسارت شدید به محیط زیست از قبیل مسموم کردن آب‌ها و آتش زدن جنگل‌ها؛ تولید، تملک، اکتساب، حمل، نگهداری، توسعه یا انباشت غیرقانونی، سرقت، تحصیل متقلبانه و قاچاق سموم، عناصر و مواد هسته‌ای، شیمیایی،

میکروبی و زیست‌شناسی (بیولوژیک)؛ و تولید، تهیه خرید و فروش و استفاده غیرقانونی و قاچاق مواد منفجره، اسلحه و مهمات از این دست دانسته شده‌اند. در مورد این تعریف باید ذکر کرد که اعمال مذکور در این تعریف، اگر به قصد تاثیرگذاری بر سیاست یا خط‌مشی جمهوری اسلامی ایران یا سازمان‌های بین‌المللی دارای نمایندگی در خاک جمهوری اسلامی ایران انجام شوند اعمال تروریستی محسوب می‌شوند و اگر چنین قصدی در آنها وجود نداشته باشد اعمال تروریستی محسوب نخواهند شد.

تعریف سوم، شامل اعمالی می‌شود، که صرف نظر از قصد مرتکب و نتیجه حاصله اعمال تروریستی محسوب می‌شوند. این اعمال عبارتند از: اعمال خطرناک علیه ایمنی هواپیما یا هوانوردی، تصرف هواپیمای در حال پرواز و اعمال کنترل غیرقانونی بر آن، ارتکاب خشونت علیه مسافر یا مسافران و خدمه هواپیما یا اعمال خطرناک علیه اموال موجود در هواپیمای در حال پرواز؛ تولید، ولید، تملک، اکتساب، حمل، نگهداری، توسعه یا انباشت غیرقانونی، سرقت، تحصیل متقلبانه و قاچاق سموم، عناصر و مواد هسته‌ای به میزان غیرقابل توجیه برای اهداف درمانی، علمی و صلح آمیز، و سایر مواردی که در ماده (۱) به آنها اشاره شده است. پس تفاوت اعمال مذکور در تعریف دوم و اعمال مذکور در تعریف سوم این است که اعمال مذکور در تعریف دوم در صورتی تروریستی محسوب می‌شوند که مرتکب آنها قصد تاثیرگذاری بر خط‌مشی جمهوری اسلامی ایران یا سازمان‌های بین‌المللی دارای نمایندگی در قلمرو آن را داشته باشد و اعمال مشمول تعریف سوم، اعمالی هستند که قطع نظر از قصد مرتکب و نتیجه حاصله عمل تروریستی محسوب می‌شوند.

تعریف چهارم، آخرین تعریف، شامل اعمالی می‌شود که به موجب قوانین داخلی یا کنوانسیون‌های داخلی جرم تروریستی شناخته شده و دولت جمهوری اسلامی ایران نیز به آن کنوانسیون‌ها ملحق شده باشد. همان‌طور که گفته شد، در حال حاضر، هیچ قانون داخلی دیگری وجود ندارد که عملی را جرم تروریستی شناخته باشد و در مورد معاهدات بین‌المللی نیز باید گفت اکثر اعمالی که در تعاریف دوم و سوم برشمرده شده‌اند، اعمالی هستند که به موجب کنوانسیون‌های بین‌المللی جرم تروریستی شناخته شده‌اند و دولت جمهوری اسلامی ایران نیز به آنها ملحق شده است. بنابراین، اعمال مذکور هم بر اساس تعاریف دوم و سوم و هم بر اساس تعریف چهارم، تروریستی محسوب خواهند شد.

در ادامه این تعریف، نکته مهمی قید شده است که قانون مبارزه با تامین مالی تروریسم در ایران را از اسناد بین‌المللی و سایر قوانین موجود در این زمینه متمایز می‌کند. تبصره ۲ از ماده (۱) قانون مقرر می‌دارد اعمالی که افراد، ملت‌ها، گروه‌ها یا سازمان‌های آزادی بخش برای مقابله با اموری از قبیل سلطه، اشغال خارجی، استعمار و نژادپرستی انجام می‌دهند از مصادیق اقدامات تروریستی موضوع این قانون نیست. تعیین مصادیق و گروه‌های مشمول این تبصره بر عهده شورای عالی امنیت ملی است. بر این اساس، انگیزه در مفهوم تروریسم و تامین مالی آن مدخلیت دارد و اگر عملی انجام شود که مشمول تعریف تروریسم باشد اما با انگیزه‌های مذکور در این تبصره انجام شده باشد، عمل تروریستی تلقی نخواهد شد و تامین مالی آن نیز

تامین مالی تروریسم تلقی نمی‌شود. نکته جالبی که در اینجا جلب توجه می کند این است که شورای عالی امنیت ملی، مکلف شده است سازمان‌ها و گروه‌های آزادی بخش را فهرست و اعلام کند. این در حالی است که در کشورهای دیگر، معمولاً عکس این روند وجود دارد و نهادهای ذی‌صلاح، سازمان‌ها و نهادهای تروریستی را مشخص و اعلام نمی کنند و این رویکرد، صحیح‌تر به نظر می‌رسد؛ چرا که اصل بر تروریست نبودن است و اگر سازمان یا گروهی تروریستی محسوب می‌شود باید نام آن اعلام شود نه اینکه نام گروه‌ها و سازمان‌های غیرتروریستی اعلام شود.

ماده کم‌سابقه دیگری که در قانون مبارزه با تامین مالی تروریسم ایران وجود دارد ماده (۳)[۱] است. بر اساس این ماده، اگر کسی از جرائم موضوع این ماده باخبر باشد و آن جرائم را در اسرع وقت به مقامات اداری، انتظامی، امنیتی یا قضایی ذی‌صلاح اطلاع ندهد، خود آن شخص هم مجرم است و به مجازات تعزیری درجه هفت محکوم می‌شود. این ماده از آن جهت کم‌سابقه (و شاید بتوان گفت بی‌سابقه) است که برای عموم مردم و نه فقط برای ضابطان قضایی، وظیفه اطلاع‌رسانی در مورد جرائمی که سایرین قصد انجام آنها را دارند در نظر گرفته است. علی‌الاصول، کشف جرم وظیفه ضابطین و دستگاه قضایی است و نه عموم مردم و صرف سکوت در مورد جرمی که دیگری انجام داده است یا می‌خواهد انجام دهد را نمی توان جرم محسوب کرد. علاوه بر این، عبارت مبهم «در اسرع وقت» بسیار مشکل‌ساز خواهد بود. در اسرع وقت یعنی چقدر؛ یک ماه؟ یک هفته؟ یک روز؟ یک ساعت؟ چقدر زمان لازم است تا سکوت اشخاص در مورد جرائمی که از آنها اطلاع دارند و اطلاع ندادن این امر منجر به ارتکاب جرم شود؟ عبارت مبهم دیگری که در این ماده وجود دارد، عبارت مقامات ذی‌صلاح اداری، انتظامی، امنیتی، یا قضایی است.

این مقامات ذی‌صلاح چه کسانی هستند؟ آیا باید به همه آنها اطلاع داده شود یا اطلاع‌رسانی به یکی از آنها کفایت می کند؟ چگونه باید مقام ذی‌صلاح را از مقام غیر ذی‌صلاح تشخیص داد؟ آیا از عموم مردم می‌توان انتظار داشت که مقامات ذی‌صلاح را بشناسند و ترتیبات اطلاع‌رسانی را نیز بدانند؟ اگر شخصی بداند که کسی قصد انجام عملیات تروریستی را دارد و این امر را اطلاع بدهد، آیا باید مدارک و اسنادی هم ارائه کند یا خیر؟ اگر مشخص شد که این اسناد و مدارک نادرست و غیرقابل اتکا بوده‌اند، آیا از اطلاع‌دهنده حمایت قانونی خواهد شد یا خیر؟ پاسخ این موارد در قانون مشخص نشده است و به نظر می‌رسد این منطقی نباشد که از عموم مردم که آموزشی در مورد کشف جرم و اطلاع‌رسانی و آیین دادرسی و شناسایی نهادهای ذی‌صلاح ندیده‌اند انتظار اطلاع‌رسانی داشته باشیم و برای عدم اطلاع‌رسانی هم برای آنها مجازات تعیین کنیم. این امر، با رویکرد قانونگذار، در قانون آیین دادرسی کیفری، مصوب سال ۱۳۹۲ نیز منطبق است. در این قانون، در تبصره ماده ۴۵ مقرر شده است «در صورتی که جرائم موضوع بندهای (الف)، (ب)، (پ)، و (ت) ماده (۳۰۲) این قانون به صورت مشهود واقع شوند، در صورت عدم

۱- ماده ۳: کلیه اشخاص مطلع از جرائم موضوع این قانون موظفند مراتب را در اسرع وقت به مقامات اداری، انتظامی، امنیتی یا قضائی ذی صلاح اعلام کنند، در غیر این صورت به مجازات تعزیری درجه هفت محکوم می شوند.

حضور ضابطان دادگستری، تمامی شهروندان می توانند اقدامات لازم را برای جلوگیری از فرار مرتکب و حفظ صحنه جرم به عمل آورند». همان‌طور که ملاحظه می‌شود، در این تبصره نیز از عبارت «می توانند» استفاده شده است و برای کلیه شهروندان -که ضابط قضایی نیستند- تکلیف حقوقی در نظر گرفته نشده است.

پرسش دیگری که در مورد مجازات تامین مالی تروریسم ممکن است مطرح شود این است که اگر شخص حقوقی، مرتکب جرم تامین مالی تروریسم شود، به چه مجازاتی محکوم خواهد شد؟ در این رابطه، ماده ۴ قانون مبارزه با تامین مالی تروریسم مقرر می‌دارد، «در صورت ارتکاب جرائم موضوع این قانون توسط شخص حقوقی، طبق مقررات قانون مجازات اسلامی، مصوب ۱ /۲ /۱۳۹۲ اقدام می‌شود». مجازات شخص حقوقی در ماده (۲۰) قانون مجازات اسلامی قید شده است. در این ماده مقرر شده است «در صورتی که شخص حقوقی بر اساس ماده (۱۴۳) این قانون مسئول شناخته شود، با توجه به شدت جرم ارتکابی و نتایج زیان بار آن، به یک تا دو مورد از موارد زیر محکوم می‌شود. این امر مانع از مجازات شخص حقیقی نیست:

الف- انحلال شخص حقوقی؛

ب- مصادره کل اموال؛

پ- ممنوعیت از یک یا چند فعالیت شغلی یا اجتماعی به‌طور دائم یا حداکثر به مدت پنج سال؛

ث- ممنوعیت از دعوت عمومی برای افزایش سرمایه، به‌طور دائم یا حداکثر برای مدت پنج‌سال؛

ج- جزای نقدی؛

چ- انتشار حکم محکومیت به وسیله رسانه‌ها» بنابراین، طیف گسترده‌ای از مجازات‌ها در اختیار قاضی قرار دارند که می تواند بسته به شرایط و دفعات جرم، هر یک از آنها را در خصوص شخص حقوقی اعمال کند.

تکالیف بانک‌ها و موسسات مالی نکته مهم دیگر این است که تکالیف بانک‌ها و موسسات مالی بر اساس این قانون چیست؟ در پاسخ به این امر، ماده ۱۳ قانون مبارزه با تامین مالی تروریسم مقرر داشته است که «تمامی اشخاص و نهادها و دستگاه‌های مشمول قانون مبارزه با پولشویی (که شامل همه اشخاص حقوقی می‌شود) موظف‌اند به منظور پیشگیری از تامین مالی تروریسم اقدامات زیر را انجام دهند:

الف- شناسایی مراجعان هنگام ارائه تمام خدمات و انجام عملیات پولی و مالی از قبیل انجام هر گونه دریافت و پرداخت، حواله وجه، صدور و پرداخت چک، ارائه تسهیلات، صدور انواع کارت دریافت و پرداخت، صدور ضمانت نامه، خرید و فروش ارز و اوراق گواهی سپرده، اوراق مشارکت، قبول ضمانت و تعهد ضامنان شامل امضای سفته، برات و اعتبار اسنادی و خرید و فروش سهام؛

ب- نگهداری مدارک مربوط به سوابق معاملات و عملیات مالی اعم از فعال و غیرفعال و نیز مدارک مربوط به سوابق شناسایی مراجعان، حداقل به مدت پنج سال بعد از پایان عملیات».

در ماده ۱۴ قانون نیز مقرر شده است «کلیه اشخاص مشمول قانون مبارزه با پولشویی موظف‌اند گزارش عملیات مشکوک به تامین مالی تروریسم را به شورای عالی مبارزه با پولشویی ارسال کنند». با توجه به این دو ماده، ملاحظه می‌شود که تکالیفی که در این ماده برای بانک‌ها و موسسات مالی و سایر اشخاص حقوقی در نظر گرفته شده است، مشابه با تکالیفی است که قانون مبارزه با پولشویی در نظر گرفته است. در این رابطه، سه وظیفه کلیدی وجود دارد که عبارتند از: شناسایی مشتری [1]؛ ارسال گزارش عملیات مشکوک[2]؛ و نگهداری سوابق. بر این اساس، به نظر می‌رسد آیین‌نامه‌ها و دستورالعمل‌های مبارزه با تامین مالی تروریسم نیز چیزی شبیه به آیین‌نامه‌ها و دستورالعمل‌های قانون مبارزه با پولشویی باشند و حتی ممکن است با انجام اصلاحاتی در آیین‌نامه‌ها و دستورالعمل‌های مبارزه با پولشویی، آنها را در رابطه با تامین مالی تروریسم نیز اعمال کرد و بدین ترتیب، از تکرار احکام مربوط به این دو جرم پرهیز کرد.

مورد بررسی بعدی را نیز باید با این عنوان اعلام کرد که بررسی خط به خط این قانون نشان می دهد برخلاف توقعات کنونی از نظام حقوقی ایران نه تنها در هیچ کجای این قانون دولت ملزم به پذیرش توصیه‌های گروه ویژه اقدام مالی [3]نشده است، بلکه حتی یک کلمه درباره توصیه‌های گروه ویژه اقدام مالی وجود ندارد. البته گروه های حقوقی با انتشار نامه قائم مقام شورای نگهبان درباره عدم مغایرت قانون مبارزه با تامین مالی تروریسم با شرع و قانون اساسی، آن را موافقت شورای نگهبان با تعهد به گروه ویژه اقدام مالی خواندند.

تأمین مالی تروریسم همانند پولشویی با فشار و پیگیری نهادهای اقتصادی به موضوع حقوق کیفری ایران تبدیل شده است؛ شاید بتوان گفت در ایران سیاست جنایی اجرایی در خصوص پولشویی و تأمین مالی تروریسم بسیار پیشروتر از سیاسات جنایی تقنینی و قضایی است. این پیشرو بودن در حدی است که قانون مبارزه با پولشویی صحبتی از تأمین مالی تروریسم نمی‌کند. ولی آیین‌نامه‌ی پولشویی و تمامی دستورالعمل‌ها و بخشنامه‌های صادره در خصوص پولشویی به تأمین مالی تروریسم اشاره می‌کنند. سوالی که به ذهن متبادر می‌شود این است که چگونه بدون جرم انگاری مستقل تروریسم و عدم شمول برخی از اقدامات تروریستی در عناوین مجرمانه سنتی حقوق کیفری ایران، تامین مالی تروریسم را جرم انگاری می‌کنیم؟ چگونه لایحه تروریسم را که در تاریخ ۱۳۸۲/۹/۱۵ توسط دولت به مجلس تقدیم شد به بوته فراموشی می‌سپاریم ولی قانون مبارزه با تامین مالی تروریسم را تصویب می‌کنیم؟ به نظر می‌رسد مقابله با تأمین مالی تروریسم بخشی از تلاش جامع‌تری است که برای مقابله با تروریسم صورت می‌پذیرد. از این رو نیازمند تصویب قانون مقابله با تروریسم هستیم که تأمین مالی تروریسم نیز به عنوان یکی از شیوه‌های مهم مقابله با تروریسم در آن گنجانده شود.

1- KYC
2- STR
3- FATF

مبحث دوم: قانون جرائم رایانه‌ای

در حال حاضر موادی از قانون مجازات جرائم رایانه‌ای نظیر مواد ۱، ۳، ۴، ۸، ۹، ۱۰ و ۱۱ را می‌توان تا حدی در انطباق برخی از مصادیق سایبر تروریسم با این مواد قانونی راه‌گشا تلقی کرد.

ماده ۱: هرکس به طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای مخابراتی که به وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد.

در این ماده بررسی چند نکته حائز اهمیت است.

ـ اولا این دسته از جرایم شامل دسترسی غیرمجاز، شنود و دریافت بدون مجوز و جاسوسی رایانه ای است. دسترسی غیر مجاز که موضوع ماده ی یک قانون است، به مجازات مندرج در قانون محکوم می شود. این ماده جرم را بر اساس دو قید مستوجب مجازات دانسته است؛ اول اینکه دسترسی غیر مجاز باشد؛ دوم اینکه داده یا سیستم به وسیله‌ی تدابیر امنیتی حفاظت شده باشد. اگر حفاظت در حد کلمه ی عبور نیز باشد، مشمول این ماده است و در غیر این صورت، مشمول این ماده از قانون نمی شود[۱]

ـ ثانیا در بررسی رکن مادی این جرم باید گفت که رفتار فیزیکی در این جرم فعل دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی می باشد حال اینجا سوالی ممکن است پیش آید آن هم اینکه آیا این جرم با ترک فعل نیز محقق می شود؟در پاسخ باید بگوییم که خیر این جرم با ترک فعل محقق نمی شود.

ـ سومین نکته این است که در مورد مجازات۹۱ روز تا یک سال حبس یا جزای نقدی از پنج میلیون (۵. ۰۰۰. ۰۰۰) ریال تا بیست میلیون (۲۰. ۰۰۰. ۰۰۰) ریال یا هر دو مورد باید دید واقعا وضع مجازاتی این چنین برای اعمالی که دارای چنین اثرات و پیامدهای گاه جبران ناپذیر و گسترده دارند کافی است؟

چند نکته دیگر در خصوص این ماده وجود دارد برای مثال در خصوص واژه غیرمجاز در ماده سوالاتی مطرح می‌شود اول اینکه مرجع تشخیص مجاز یا غیر مجاز بودن کیست؟یعنی چه دسترسی هایی مجاز و چه دسترسی‌هایی غیر مجاز است. که به نظر باید روشن شود که در ماده روشن نیست.

ماده ۳: هر کس به طور غیرمجاز نسبت به داده‌های سری درحال انتقال یا ذخیره‌شده در سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده مرتکب اعمال زیر شود، به مجازات‌های مقرر محکوم خواهد شد: الف) دسترسی به داده‌های مذکور یا تحصیل آنها یا شنود محتوای سری در حال انتقال، به حبس از یک تا سه سال یا جزای نقدی از بیست میلیون (۲۰. ۰۰۰. ۰۰۰) ریال تا شصت میلیون (۶۰. ۰۰۰. ۰۰۰) ریال یا هر دو مجازات.

۱- بررسی قانون جرائم رایانه‌ای مصوب ۱۳۸۸/۳/۵، حمید خانزاده، انتشارات دادگستر، ۱۳۸۸، ص ۳

ب) در دسترس قراردادن داده‌های مذکور برای اشخاص فاقد صلاحیت، به حبس از دو تا ده سال.
ج) افشاء یا در دسترس قرار دادن داده‌های مذکور برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آنها، به حبس از پنج تا پانزده سال.

تبصره۱ـ داده‌های سری داده‌هایی است که افشای آنها به امنیت کشور یا منافع ملی لطمه می‌زند.

در مورد این ماده و نکات قابل ذکر آن باید به چند مورد اشاره کرد.

در ماده‌ی ۳ همان طور که ذکر شد، «دسترسی به داده‌های مذکور یا تحصیل آنها یا شنود محتوای سری در حال انتقال در دسترس قرار دادن داده‌های مذکور برای اشخاص فاقد صلاحیت، افشا یا در دسترس قرار دادن داده‌های مذکور برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آنها» را جرم کرده است.

ماده۸ ـ هرکس به طور غیرمجاز داده‌های دیگری را از سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده حذف یا تخریب یا مختل یا غیرقابل پردازش کند به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون (۱۰. ۰۰۰. ۰۰۰) ریال تا چهل میلیون (۴۰. ۰۰۰. ۰۰۰) ریال یا هر دو مجازات محکوم خواهدشد.

در این ماده در کنار نکات دیگری که قابل بررسی خواهد بود باید بیان کرد که، تفاوت بین جرم اخلال در داده‌ها و جعل در این است که جعل نیاز به سوءنیت خاص(قصد تقلب)دارد، اما تحقق جرم اخلال در داده‌ها نیاز به قصد تقلب ندارد.[1]

ماده۹ـ هر کس به طور غیرمجاز با اعمالی از قبیل واردکردن، انتقال دادن، پخش، حذف کردن، متوقف کردن، دستکاری یا تخریب داده‌ها یا امواج الکترومغناطیسی یا نوری، سامانه‌های رایانه‌ای یا مخابراتی دیگری را از کار بیندازد یا کارکرد آنها را مختل کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون (۱۰. ۰۰۰. ۰۰۰) ریال تا چهل میلیون (۴۰. ۰۰۰. ۰۰۰) ریال یا هر دو مجازات محکوم خواهدشد.

ماده۱۰ـ هرکس به طور غیرمجاز با اعمالی از قبیل مخفی کردن داده‌ها، تغییر گذر واژه یا رمزنگاری داده‌ها مانع دسترسی اشخاص مجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی شود، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون (۵. ۰۰۰. ۰۰۰) ریال تا بیست میلیون (۲۰. ۰۰۰. ۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.

ماده۱۱ـ 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.

۱- حیدری، حسن(۱۳۹۲). اعمال صلاحیت کیفری درمورد جرائم ارتکابی در فضای سایبری. پایان‌نامه حقوق جزا و جرم‌شناسی. دانشگاه آزاد اسلامی واحد مرکزی تهران

در خصوص مواد قانونی کیفری، در رابطه با پیشگیری از وقوع تروریسم سایبری و به تبع حمایت از بزه‌دیدگان آن، می‌توان به موادی از متن ماده‌های بالا اشاره نمود که شباهت خاصی به جرم‌انگاری تروریسم سایبری دارد.

یکی از مقررات مهم این قانون‌ها شناسایی دو نوع بزهکار است که که با تعیین کیفر در انتهای ماده، به بازدارندگی مرتکبان افعال مندرج در مادهٔ ۱۱، پرداخته است است.

بزه‌دیدگان مورد حمایت در این مقرره، سیستم‌های رایانه‌ای و مخابراتی هستند که برای ارائه خدمات ضروری عمومی به کار می‌روند. با توجه به این که در تروریسم سایبری تأسیسات مورد استفادهٔ عمومی مورد هجوم قرار می‌گیرند، اقدام شایسته‌ای توسط قانون‌گذار به شمار می‌رود. در این راستا قانون‌گذار با تعیین مجازات، به ارعاب بزهکاران بالقوه که قصد ارتکاب اعمال مندرج در این ماده را دارند و همچنین تکرار بزه توسط دسته‌ای دیگر از اعمال غیرمجازی که به طور معمول توسط تروریست‌های سایبری به منظور تخریب یا اختلال در داده‌ها و سیستم‌های رایانه‌ای و مخابراتی استفاده می‌شود، افعالی از قبیل مخفی کردن داده‌ها، تغییر گذرواژه یا رمزنگاری داده‌ها است که بدین وسیله، منجر به ممانعت از دسترسی اشخاص مجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی می‌شود، در این صورت قانون‌گذار با مجرمانه قلمداد نمودن اعمال فوق، برای مرتکب حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات تعیین کرده است که با غیر حصری شمردن اعمال مذکور، اقدام شایسته‌ای را در جهت محافظت از داده‌ها و سیستم‌های رایانه‌ای و همچنین با اعمال کیفر حبس یا جزای نقدی بازدارندگی را برای انواع بزهکاران شکل داده است. [1]قانون‌گذار در این سه ماده به صورت کامل و غیر حصری به شایع‌ترین اعمال ارتکابی که علیه تأسیسات حیاتی کشور انجام می‌شود پرداخته است که اقدام شایسته‌ای در خصوص جرم‌انگاری افعال مرتبط با تروریسم سایبری به شمار می‌رود.

هرچند که این قانون به صورت صریح و کامل به بررسی تروریسم سایبری و راه کار های پیشگیری و مبارزه با آن نپرداخته است اما به عنوان مرتبط‌ترین منبع در میان قوانین دیگر که به توضیح برخی اصطلاحات پرداخته و برای آنها راهکار ارائه داده است و می‌توان آن را به دید یک پیشرفت بزرگ نگاه کرد.

با بررسی‌های انجام شده در مراجع حقوقی و مربوط به تروریسم و در راستای پیشرفت کشور در مورد مبارزه با تروریسم، دادستان کل کشور با بیان اینکه خوشبختانه در جمهوری اسلامی ایران تمهیدات قانونی لازم در زمینه سایبر تروریسم و جرائم رایانه‌ای پیش بینی و اقدامات خوبی صورت گرفته، تشکیل کارگروه تعیین مصادیق محتوای مجرمانه به ریاست دادستان کل کشور که امکان رصد، کشف، شناسایی و برخورد با سایبر تروریسم و جرائم سابیری را فراهم ساخته است را از جمله مصادیق این تمهیدات عنوان کرد.

۱- زینب سادات موسوی، پایان-نامه حمایت از بزه‌دیدگان تروریسم سایبربدر حقوق کیفری، ۱۳۹۰ دانشگاه اصفهان، ص ۴۸

دادستان کل کشور با سند تشکیل دبیرخانه منطقه‌ای دائم مبارزه با تروریسم و تهیه ساختار مشترک قضایی، اطلاعاتی و انتظامی و ایجاد پژوهشگاه علمی با موضوع مبارزه با تروریسم به منظور تبادل تجارت، پیگیری از طریق ارگان‌های ذیربط برای ایجاد سیستم حمایتی در کشورهای عضو و به صورت ملی برای مساعدت به کشورهایی که بزرگترین آسیب را از تروریسم متحمل می‌شوند را نیز به عنوان سند دیگر مطرح کرد.[1]
همچنین می توان از توجه به اعمال شدت در مواد ۱۳۰، ۱۲۱، ۱۱۶، ۱۱۴، ۱۰۹، ۷۱، ۴۷ قانون مجازات اسلامی و نیز مواد ۳۰۳، ۲۹۰، ۲۳۷ قانون آیین دادرسی کیفری که به صورت‌های مختلف از جمله تعیین دادگاه های انقلاب به عنوان مرجع رسیدگی کننده و نیز افزایش مجازات‌ها و منع اعمال تخفیف در مراحل دادرسی دریافت که اهمیت این جزم در قانون‌گذاری ایران بع چه صورت می‌باشد.

نتیجه‌گیری

آنچه تلاش شد در این مختصر نوشتار تبیین و بر آن تأکید گردد، وضعیت کشورمان در برابر یک پدیدهٔ شوم و ناگزیر است؛ ناگزیر از آن جهت که نه امکان کنار گذاشتن فناوری اطلاعات و ارتباطات الکترونیکی و نه سرکوبی یک شبه تمامی گروه‌های تروریستی وجود دارد. بدتر اینکه روز به روز از دو جهت اینگونه تهدیدات جدی‌تر می‌شوند: از یک سو گروه‌های تروریستی از آمادگی بیشتری برای وارد آوردن لطمات سهمگین برخوردار می‌شوند و از سوی دیگر، دشمنان به بهانه و اتهام اینکه ما تنها یا بزرگترین کشور حامی تروریسم هستیم، خود را برای یک رویارویی تمام عیار و مقابله به مثل سایبری آماده می کنند.
با توجه به بررسی‌های صورت گرفته در قلمروهای جرائم سایبری در ایالات متحده آمریکا، می‌توان گفت تغییرات مراجع قانون گذاری این کشور در قوانین فدرال در طول ۲۰ سال گذشته قابل ملاحظه بوده و البته، همچنان در حال تکامل هستند. چالش‌های آژانس های دولتی و سازمان های مرتبط آنها در شناخت قوانینی که قابل اجرا هستند، درک قوانین قابل اجرا و سپس یافتن کمک‌های لازم برای اجرای الزامات دیکته شده تحت آن قوانین بوده است.
نظام حقوقی ایالات متحده در تمامی موارد به تجزیه و تحلیل و ایجاد راهکار های جدید و قوانین جدید برای پیشگیری، کشف، مجازات و حتی ایجاد راهکارهای حقوقی برای محافظت از حقوق بزه دیدگان جرائم سایبری پرداخته است. بررسی‌های سالانه، ایجاد سازمان‌های مرتبط، منصوب کردن افراد در پست های حقوقی برای بررسی و قانون گذاری بهتر در این زمینه نشانه های تلاش این نظام حقوقی برای ایجاد فضای کاملا قانونی و حقوقی برای رسیدگی به این جرائم می باشد.

1- The 14th Summit of the Shanghai Cooperation Organization (SCO) Chief Prosecutors in China

مطلب مهمی که در مورد نظام حقوق ایالات متحده می‌توان به آن اشاره کرد تلاش‌های مسئولین فدرال برای امنیت سایبری برای توسعه و اجرای سیاست های امنیت اطلاعات، اصول و دستورالعمل ها؛ و سایر توابع، از جمله ارزیابی های خطر و فعالیت های دیگر برای محافظت از سیستم‌های حقوقی است.

همانگونه که در بررسی‌ها نشان داده شد سه اصل مهم و اساسی در نظام حقوقی این کشور وجود دارد که رعایت آن در هر لایحه و هر سندی الزامی و غیرقابل تغییر است. این اصول شامل حمایت از قوانین اصلی و مهم برای رسیدگی به بسیاری از مسائل شناسایی شده و در وضع قوانین جدید، داشتن مسئولیت مربوط به امنیت سایبری در تمامی سیستم‌های سازمان‌های فدرال، و حمایت از بزه‌دیدگان، می‌باشد.

رویکردهای کلی نظام حقوقی ایالات متحده بر پایه بررسی‌های دوره‌ای و منظم می‌باشد به طوری که سالانه نتایج و مقررات جدید و به روزی به مقررات اصلی اضافه و آنهارا تکمیل می نماید. بدین صورت هم قوانین جامع و کامل و به روز هستند و هم در تمامی موارد کاربرد دارند. وضع مجازات های شدید برای عاملان و معاونان جرائم تروریسم سایبری، پیگیری دقیق از مرحله شناسایی تا مرحله مجازات، حمایت کامل از بزه دیدگان مهم‌ترین ویژگی های نظام حقوقی ایالات متحده در مورد جرائم تروریسم سایبری می باشد. به همین دلیل می توان گفت جرم تروریسم سایبری از منظر این نظام حقوقی جزء جرائم بسیار مهم می باشد و بررسی و قانون گذاری و رسیدگی به آن در دادگاه های مشخص شده در اولویت بوده و به صورت فوری به آن رسیدگی میشود. ایجاد گروه مخصوص حقوقی برای کشف و بررسی تروریسم سایبری، ایجاد گروه حقوق دانان جهت وضع قوانین جدید و به روز رسانی قوانین قدیمی، ایجاد دادگاه مخصوص رسیدگی به این قوانین در ایالات متحده خود نشانگر درست بودن ادعا بالا می باشد.

و اما در قسمت دوم بررسی‌ها، برداشت ها از قوانین ایران و نحوه قانون‌گذاری و رسیدگی به پرونده‌های جرم تروریسم سایبری ما را به این نتیجه رساند که برخلاف سیستم قوی حقوقی موجود در ایران، رسیدگی به این جرم در سطح پایینی قرار دارد.

تروریسم سایبری در سال‌های اخیر به یکی از چالش های اصلی دولت ها به خصوص کشورمان تبدیل شده است. از لحاظ قانون گذاری، نظام حقوقی فعلی ایران با داشتن تنها یک قانون صریح آنها نه در مورد جرم انگاری خود تروریسم بلکه برای مبارزه با تامین مالی آن هیچگونه جرم انگاری مشخصی در این باره ندارد. همچنین از بزه دیدگان نیز به جز استناد به قواعد عام، مقرراتی دربارهٔ جبران خسارت حمایت دیگری دیده نمیشود. بنابراین به منظور ممانعت از هرگونه ایراد خسارت بیشتر بر زیرساخت های اطلاعاتی کشور، لزوم اتخاذ تدابیر قانونی بیشتری احساس می شود.

بررسی ها نشان داد که باتوجه به عدم وجود یک تعریف مشخص برای این جرم و یا حتی عدم قانونگذاری خاصی برای این جرم، و تنها با استناد به یک قانون مختصر جهت رسیدگی به حمایت مالی از تروریسم؛ و عدم وجود دادگاه خاص یا ارگان خاص دولتی جهت رسیدگی به این جرم، باید گفت که این جرم در قانون جمهوری اسلامی ایران جایگاه خاص و مهمی را نداشته و درصد اهمیت به آن بالا نمی‌باشد. این

عدم توجه موجب شده تا در بسیاری از موارد با ضعف قوانین و عدم شمول آنها در موقع تعیین کیفر و مجازات مناسب در دادگاه‌ها مواجه شویم. بسیاری از این ضعف ها از عدم به روز رسانی قوانین نشاءت می گیرند.

خلاءهای موجود در نظام حقوقی ایران را می‌توان در چند دسته بیان کرد.

دسته اول: خلاء در گروه‌های بررسی‌کننده قوانین و قانون گذاران می‌باشد. بدین صورت که نظام حقوقی ما با عدم آموزش مناسب و تربیت حقوق‌دانان مطلع و آگاه از تمامیت جرم تروریسم سایبری مواجه است، این خلاء منجر به عدم قانون‌گذاری مناسب و نقصان داده های حقوقی در دادگاه‌ها می‌شود.

دسته دوم: عدم وجود دادگاه و مراجع رسیدگی منحصر به فرد برای این جرم می‌باشد. عدم حضور قضات آموزش دیده و مراجع رسیدگی‌کننده خاص برای این جرائم، رسیدگی به این جرائم را با مشکلات فراوانی از جمله عدم تناسب جرم و مجازات، عدم برگزاری به موقع دادگاه ها و گاه با توجه به عدم وجود قانون اختصاصی در تعریف این جرم، موجب عدم صدور رای درست می‌شود. این موارد سیستم حقوقی کشور را با مشکلات فراوان مواجه می‌سازد.

از مجموع مطالب ذکر شده می توان اینگونه برداشت کرد که قانون گذاران ایالات متحده آمریکا با توجه به حساس بودن موضوع تروریسم سایبری در دنیای کنونی با دقت بیشتری به بررسی و جرم انگاری می‌پردازد. ایجاد نهادهای مختلف، بررسی دوره‌ای قوانین و به روز رسانی آنها، مهمترین پیشگیری‌های حقوقی برای مبارزه با تروریسم سایبری در ایالات متحده آمریکا می باشد.

بدیهی است برای حل این معضل باید راهکارهای گوناگون اساسی و زیربنایی در حوزه‌های مختلف طرح‌ریزی شود. انچه در اینجا مورد تاکید قرار گرفته، بستر سازی حقوقی از منظر حوزه کیفری و جرم شناسی است. هرچند باید هر این زمینه به یک نکته اساسی توجه داشت و آن اینکه از انجا که کلیه راهکارهای مبارزه با تروریسم به طور اعم، و مبارزه با تروریسم سایبری به طور اخص، با یکدیگر ارتباط دارند و بر یکدیگر تاثیرگذارند، الزام است پیش از هر چیز راهبردهای مبارزه با تروریسم با توجه به مصابح داخلی و عنایت به شرایط بین‌المللی تدوین شیوه و زمینه اجرای گسترده آن فراهم گردد.

یافتن راه‌های پیشگیری حقوقی حملات سایبری به ایران و همچنین تلاش برای سهیم شدن در مدیریت اینترنت جهانی از طریق حضور در مجامع موثر و مرتبط، اقداماتی است که به رفع ضعف در حوزه قانون‌گذاری و اجرای قوانین داخلی کمک شایانی خواهد کرد.

فهرست منابع و مآخذ

ـ ابوالمعالی الحسینی، سید وحید؛ علیزاده طباطبایی، زهرا سادات. (۱۳۸۷)، حقوق امنیت اطلاعات شبکه. فصلنامه فقه و حقوق.

ـ اچ. کاریو، فردریک. (۱۳۸۷)، تروریسم دولتی و ایالت متحده آمریکا، محمودی فقیهی، رضا، تهران: نشر دفتر مطالعات بینالمللی مبارزه با تروریسم دانشگاه آزاد اسالمی، چاپ اول.

ـ افخم، راضیه. (۱۳۸۸)، تروریسم در حقوق ایران و اسناد بین‌المللی، پایان نامه کارشناسی ارشد، رشته حقوق جزا و جرمشناسی، دانشگاه آزاد اسالمی واحد تهران مرکز.

ـ الخنسا، می. (۱۳۹۰)، تروریسم صهیونیستی و مقابله با آن در حقوق بین الملل امروز، مجموعه مقالات کنفرانس بین‌المللی ائتلاف جهانی علیه تروریسم برای صلح عادلانه، تهران، نشر مجمع جهانی صلح اسالمی، چاپ اول.

ـ برنر، سوزان. (۱۳۸۲)، قانون نمونهٔ آئین پیجویی جرایم سایبر، جلالی فراهانی، امیرحسین، معاونت حقوقی و توسعهٔ قضایی قوهٔ قضائیه.

ـ بزرگمهری، مجید. (۱۳۹۰)، مبارزه با تروریسم در سازمان ملل متحد، تحلیلی از تعریف تروریسم و راه‌های مقابله با آن در کنوانسون های مصوب مجمع عمومی، مجله رهیافت‌شناسی بین المللی.

ـ پاکزاد، بتول. (۱۳۸۸)، تروریسم سایبری، رساله دکتری حقوق جزا و جرم‌شناسی. دانشکده حقوق دانشگاه شهید بهشتی.

ـ پورسعید، فرزاد. (۱۹۳۳)، تحول تروریسم در روابط بین‌الملل، فصلنامه مطالعات راهبرد، سال ۱۲، شماره چهارم، شماره مسلسل ۴.

ـ جانسون، استوارت و دیگران. (۱۳۸۴)، چالش‌های نوین، ابزارهای نوین برای تصمیم گیری دفاعی، زنگنه، جواد؛ غریب آبادی، کاظم، انتشارات ستاد مشترک سپاه پاسداران انقلاب اسلامی، چاپ اول، تهران.

ـ رئیسی، لیال؛ حیدرقلیزاده، جعفر. (۱۳۹۶) بررسی تروریسم دولتی آمریکا و تأثیر استراتژی آن کشور بر امنیت کشورهای حوزه خلیج فارس و خاورمیانه از منظر حقوق بین‌الملل، در: آمریکا و تروریسم، مجموعه مقاالت کنفرانس بینالمللی عملکرد دولت آمریکا در غرب آسیا از منظرحقوق بشردوستانه، زیر نظر دکتر سهراب صالحی، تهران، انتشارات پژواک عدالت، چاپ اول.

ـ شورای عالی امنیت فضای تبادل اطلاعات کشور، (۱۳۸۴)، متن و مشروح سند راهبرد ی امنیت فضای تبادل اطلاعات کشور.

ـ صفاری، علی. (بی تا)، مبانی نظری پیشگیری ار وقوع جرم، مجله تحقیقات حقوقی، شماره ۳۴-۳۳.

ضیایی، یاسر؛ خلیل زاده، مونا. (؟)، مسئولیت بین المللی دولت ناشی از حملات سایبری، مجلهی حقوقی شهردانش، شماره ۲۳.

ـ عالی پور، حسن. (۱۳۹۰)، حقوق کیفری فناوری اطلاعات، معاونت حقوقی و توسعه قضایی قوه قضاییه، کمیسیون سیاست جنایی، انتشارات خرسندی، چاپ اول، تهران.

ـ عالی پور، حسن. (۱۳۹۰)، حقوق کیفری فناوری اطلاعات، چاپ اول تهران: انتشارات خرسندی.

ـ موسسه توسعه حقوق فناوری اطلاعات برهان مشاوره حقوقی، (۱۳۹۴)، مفهوم شناسی جرایم رایانه‌ای، جرایم اینترنتی و جرایم سایبری.

ـ نجفی ابرندآبادی، علی حسین. (۱۳۸۰). تقریریات درس جرم شناسی، تهران: دوره دکتری دانشگاه تربیت مدرس.

ـ نجفی ابرندآبادی، علی‌حسین. (۱۳۸۳)، پیشگیری عادلانه از جرم، علوم جنایی، مجموعه مقالات در تجلیل از استاد آشوری، انتشارات سمت.

ـ نیازپور، امیرحسن. (۱۳۸۴)، پیشگیری از بزهکاری در قانون اساسی و لایحه پیشگیری از وقوع جرم، مجله حقوقی دادگستری، شماره ۴۵.

__ United Nations, International Review of Criminal Policy- United Nations Manual on the Prevention and Control of Computer-Related Crime, Nos. 43 and 44

__ United Nations, International Review of Criminal Policy- United Nations Manual on the Prevention and Control of Computer-Related Crime, Nos.

Cavelty, M. D. (2008), Cyber-Security and Threat Politics; US efforts to secure the information age. New York: Routlefge.

__ Mesko, G. (2006), "Perceptions of Security: Local Safety Councils in Slovenia". In: U. Gori, & I. Paparela. Invisible Threats; Financial and Information Technology Crimes Against National Securi,y. Netherlands: IOS Press.

__ Director of National Intelligeence. (2010), Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence. United State of America.

__ Director of National Intelligeence. (2010), Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence. United State of America.

__ Rod Stark. (1999), Cyber Terrorism, Rethinking New Technology, Department of Defense and – strategic Studies.

__ Ghislaine DOUCET. (1983), Le terrorisme et son contentieux, Orléans.

Diego Muro, Ethnicity and Violence (2010), The Case of Radical Basque Nationalism, New York: Routledge.

__ ISRAEL' S LESSONS FOR FIGHTING TERRORISTS AND THEIR IMPLICATIONS FOR THE UNITED STATE by DANIEL L. BYMAN

__ LIBERATION MOVEMENTS IN SOUTHERN AFRICA Nathan Shamyurira University of Dar-es-Salaam Tanzania The Eighth AnnualHANS WOLFF MEMORIAL LECTURE

__ Strobe Tallbott and Nayan chand ,eds. (2001), an age of terror America and the world after September 11, New York : basic books.

__ Peterson, M, J. the U. N. (2006), general assembly , great Britain : TJ international I. td , padstow, conrwall.

__ Greg Travalio and John Altenbrug. (2003), Terrorism, State Responbility and the Use of Military Force, Chicago Journal of International Law, Vol. 97.

__ Peterson M. J. (2004), using the general assembly ,in Jane Boulden and Thomas G. weiss eds. , Terrorism and the U. N. : befor and after September 11 (Bloomington : Indiana university press.).

(1991), Review and implementation of the Concluding Document of the Twelfth Special Session of the General Assembly, G. A. res. 51/46.

__ UN Ad Hoc. (1996). Committee on Terrorism, Deraft International Comprehensive Convention on International Terrorism, in Annexes to the Report of the Ad Hoc Committee Established by General Assembly Resolution.

The Ad Hoc. (1996), Committee was established in 1996 by UN General Assembly Resolution51/210.

__ Colarik, Andrew M. (2006), Cyber Terrorism: political and Economic Implications, IDEA Group Publishing.

Brenner and Goodman, "In Defense of Cyberterrorism: An Argument for Anticipating CyberAttacks,"

__ Akay, Haluk. (2011), Tackling Cyber Terrorism in a Globalized World.

Kowalski, Melanie. (2002), Cyber-Crime: Issues, Data, Sources, and Feasibility of Collecting PoliceReported Statistics, Canadian Centre for Justice Statistics, Minister of Industry.

Hildreth, Steven A. , (2001), Cyberwarfare, CRS Report for Congress.

__ William L. Tafoya,Ph. D. (2011), "Cyber Terror", FBI Law Enforcement Bulletin (FBI. gov).

__ Adams, Jo-Ann M. (1996) 'Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet', Computer and High Technology Law, 12: 403-434.

__ Aldesco, Albert I. (2002), 'The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime', Loyola of Los Angeles Entertainment Law Review, vol. 23: 81-123.

__ Ashworth, Andrew & Horder, Jeremy. (2013), Principles of Criminal Law (7th edition), Oxford: Oxford University Press.

Brenner, Susan W. 'U. S. (2004), Cybercrime Law: Defining Offences', Information Systems Frontiers, 115-132.

__ (2010), Computer Crime and Intellectual Property Section Criminal Division, Prosecuting Computer Crimes, published by Office of Legal Education Executive Office for United States Attorneys.

__ Darden, Brandon. (2010), 'Definitional Vagueness in the CFAA: Will Cyber-bullying Cause the Supreme Court to Intervene?' Southern Methodist University Science and Technology Law Review, vol. XIII : 329-358

Antolin-Jenkins, Vida M. (2005), "Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?", Naval Law Review, V. 51, p. 132-136

Brenner, Susan W. (2007), "Technological Change and The Evolution of Criminal Law: "At Light Speed": Attribution and Response To Cybercrime/Terrorism/ Warfare", Journal of Criminal Law & Criminology V. 97, p. 379475

Brickey, Jonalan. (2013), "Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace", http://www. ctc. usma. edu/posts/defining-cyberterrorism-capturing-a-broad-range-of-activities-in-cyberspace.

__ Charvat, Jpiag, "Cyber Terrorism: A New Dimension in Battlespace", http:// www. ccdcoe. org/publications/virtualbattlefield/05_CHARVAT_Cyber%20 Terrorism. pdf

__ Collin, Barry C. , "The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge", Remarks at the 11th Annual International Symposium on Criminal Justice Issues, http://afgen. com/terrorism1. html

"Cyber Crime", FBI, http://www. fbi. gov/about-us/investigate/cyber

__ Gordon, Sarah & Ford, Richard. (2006), "On the Definition and Classification of Cybercrime", J. Computer Virology, p. 13-20.

Krasavin, Serge, "What is cyber-terrorism?", http://www. crime-research. org/ library/Cyber-terrorism. htm

Pollitt, M. M. (1997), "Cyberterrorism: Fact or Fancy?", Proceedings of the 20 National Information Systems Security Conference, p. 285-289

"Prospective Analysis on Trends in Cybercrime from 2011 to 2020", French

__ National Gendarmerie (Agence Nationale de Sécurité des Systèmes d'Information (ANSSI), http://www. mcafee. com/hk/resources/white-papers/wptrends-in-cybercrime-2011-2020. pdf

__ (2010), U. S. Department Of Justıce, Computer Crime and Intellectual Property Section, Criminal Division, "Prosecutıng Computer Crımes", http:// www. justice. gov/criminal/cybercrime/ccmanual/ccmanual. pdf

__ White, Jonathan R. (2012), "Terrorism&Homeland Security", Cengage Lerarning, Wadsworth, California.

Weimann, G. , (2004), How Modern Terrorism Uses the Internet. http://www. usip. org/publications/www terrornet-how-modern-terrorism-uses-internet

__ Weimann, G. (2005), "Cyberterrorism: The Sum of All Fears?", Studies in Conflict & Terrorism, p. 129-149.

Zanini, M. & Edwards, S. J. A. (2001), "The Networking of Terror in the Information Age", In J. Arquilla & D. Ronfelt (Eds), Networks and Netwars, Santa Monica, CA: RAND Corporation, p. 29-60.

__ Yeh, Brian T. (2006), USA Patriot Act Additional Reauthorizing Amendment, CRS Report for Congress

__ Computer Security Institute. (2001), Financial Losses Due to Internet Intrusions, Trade Secret Theft and Other Cyber Crimes Soar. Retreived from http://www. prnewswire. com/newsreleases/financial-losses-due-to-internet-intrusions-trade-secret-theft-and-other-cyber-crimes-soar71628527. html

__ Kabay, M. E. (2000), Studies and Surveys of Computer Crime. Security Portal.

(2000), President's Working Group on Unlawful Conduct on the Internet. The Electronic Frontier: the Challenge of Unlawful Conduct Involving the use of dhe Internet 41.

Saul, B. (2008), Defining Terrorism to Protect Human Rights. Sydney Law School Legal Studies Research Paper No: 08-125.

__ Brazil, Salvador. (2010), Twellfth United Nation Congress on Crime Prevention and Criminal Justice. Comprehensive strategies for global challenges: crime prevention and criminal justice systems and their development in a changing world, A/CONF. 213/9. Retreived from http://www. un. org/en/conf/crimecongress2010

__ Swires, Peter. (2004), The System of Foreign Intelligence Surveillance Law, George Washington Law Review.

__ (1981), The Provisions of Executive Order 12333, United States Intelligence avtivities

__ Peter W. Wilson and others. (1998), Strategic Information Warfare Rising. New York: Rand Corporation.

Cyber War: The Next Threat to National Security and What to Do About It, 2010. with Robert K. Knake

__ Matt W. Ransom, Confederate General from North Carolina By Clayton Charles Marlow

Lang Beebe. Nicole, Srinivasan Rao. v. (2005), Using Situational Crime Prevention Theory to Explain the Effectiveness of Information Systems Security, Proceedings of the 2005 SoftWars Conference, Las Vegas.

http://www. cpa. org. au/guardian/2016/1744/02-editorial. html

laws

__ Draft Statute for an International Criminal Court with commentaries 1994

Draft comprehensive convention against international terrorism

Convention on Cybercrime Budapest, 23. XI. 2001

__ International Convention on Cyber Crime and Terrorism

U. S. Code › Title 18 › Part I › Chapter 113B › § 2331

18 U. S. Code § 1030 - Fraud and related activity in connection with computers

__ Fourth Amendment to the U. S. Constitution

__ White House Coordinator to Oversee Cyber Security

__ Health Insurance Portability and Accountability Act of 1996 (HIPAA)

__ Gramm-Leach-Bliley Act or Financial Services Modernization Act of 1999

__ Federal Information Security Management Act of 2002 (FISMA)

__ Cybersecurity Information Sharing Act (CISA)

__ Cybersecurity Improvement Act of 2014 -2017

__ ACT ON REAL NAME FINANCIAL TRANSACTIONS AND GUARANTEE OF SECRECY 2015

__ The Federal Rules of Civil Procedure

__ The 14th Summit of the Shanghai Cooperation Organization (SCO) Chief Prosecutors in China