واکاوی جرم تروریسم سایبری از منظر حقوق و چالش‌های فرارو

محمد ابراهیم بشارتی،

دانش پژوه دکترای فقه وحقوق قضایی

چکیده

تازه‌ترین چهره خطرناک تروریسم که امروزه در اثر توسعه فناوری نوین در محیط مجازی یا همان فضای سایبر اتفاق می‌افتد، هرچند با تروریسم فیزیکی در ارتکاب اعمال مجرمانه متفاوت است، ولی از نگاه اهداف و انگیزه‌های مجریان هردو در یک رده جنایی قرار می‌گیرند. عمده تفاوت بین این دو رویکرد مجرمانه را در ابزارها و شیوه اجرای برنامه‌های عملیاتی، کم هزینه بودن، سهل الوصول بودن بزه‌دیدگان و مواردی از این دست می‌توان بازشناخت. پژوهش حاضر کوشید در یک بازه زمانی محدود با توجه به اهمیت موضوع، منابع در دسترس کتابخانه‌ای اعم از کتاب‌ها، مقالات علمی، گزارش‌های تحلیلی کارشناسان فنی و مصاحبه‌های علمی را به مطالعه بنشیند و ضمن توصیف ماهیت این پدیده مجرمانه، به نتایج قابل قبولی دست یابد. نتایجی که عمدتا حول دو محور دشواری شناخت ماهیت مجرمان در محیط مجازی و نیز فقدان قوانین کار آمد و پاسخ‌گو در حوزه‌های حقوق جزای شکلی و حقوق ماهوی جزائی متمرکز بود و می‌طلبد برای جبران این نقصیه قوانین جامع مطابق با استانداردهای امروزی تصویب گردد.

واژگان کلیدی:تروریسم، سایبر، چالش های حقوقی، قوانین شکلی، قوانین ماهوی.

مقدمه

از نگاه دکترین حقوق جزایی و جامعه شناسی جنایی هرچند تا دیروز، اعمال ارتکابی هرگاه علیه امنیت عمومی و یا حاکمیت یک کشور صورت می‌گرفت، جرم را در زمره جرائم علیه امنیت تعریف می‌کردند و جرائمی‌را که لطمات اصلی خودرا بر اعتماد عمومی بین افراد وارد می‌ساخت تحت عنوان جرائم علیه آسایش عمومی قرار می‌گرفت(سیدمحمود مجیدی، ۱۳۸۶ص ۳۴)، لیکن امروزه در هردو عرصه داخلی و بین المللی، با پدیده بسیار مخرب‌تری به نام تروریسم مواجهیم. تروریسم Terrorismمجموعه اعمال، ابزار و فنونی است‌که به صورت منظم و سازمان یافته برای ایجاد احساس ترس دسته جمعی‌که خشونت و کشتار بی‌حساب موجد آن است ،به کار برده می‌شود. تروریسم نه فقط با استفاده از وسایلی که می تواند زندگی و امنیت افراد را مورد سوء استفاده قرار دهند، صورت می یابد بلکه از طریق تخریب خشونت آمیز خدمات عمومی و یا تجهیزات زیر بنایی متعلق به جمع نیز اعمال می شود. هدف از اعمال تروریسم از هم پاشیدن ساخت اجتماعی و سیاسی است(معصومی، ۱۳۹۲). لذا است‌که برخی دیگر در تعریف معنای واقعی تروریسم، معتقداند؛ تررویسم صرفا خشونتی کورکورانه نیست، بلکه همان‌طور که از عنوان آن بر می‌آید، به القاکردن بدگمانی و دلواپسی و اضطراب گسترده و همه جانبه هم ارتباط دارد(داناپریست، ۱۳۹۲، ص ۲۳). پدیده‌ی بسیار خطرناکتری‌که در اثر پیدایش دانش نوین در عرصه فناوری اطلاعات و فراگیر شدن اندیشه‌ی دولت الکترونیک، به موازات راحت ترشدن انجام کارها، به سرعت رشد کرده و می‌رود تا تمام امنیت و آسایش را از زندگی عمومی و خصوصی جامعه و در رأس همه، دولت‌ها و مجموعه نهادهای امنیت آفرین عمومی به‌کلی برباید. سرعت نفوذ، قدرت تخریب و کم هزینه بودن ارتکاب این جرم، انگیزه بسیار بالایی را برای گروه‌ها و مجموعه اندیشه‌های هم‌سو جهت استفاده از آن به‌منظور ایجاد خسارت به جامعه‌ی هدف شکل داده تا آنجا که امروزه در بسیاری از کشورها، حتی برخی دولت‌ها نیز تمایل دارند برای وارد

کردن فشار بر رقیبان بین المللی و یا شرکت‌های تجاری و نهادهای رقیب از کاربردهای آن بهره بجویند. از همه مهم‌تر این‌که امروزه گروه‌های تروریستی و مجرمان سازمان یافته برای انجام اقدامات ویرانگر، بیش از هر وسیله دیگری به این سمت و سو کشیده شده اند و به‌طور سرسام آور از آن استفاه می‌نمایند. پدیده‌ی نوینی‌که جرم شناسان و جامعه شناسان جنایی به مدد اطلاعات بدست آمده از اندیشه وران حوزه فناوری اطلاعات از آن به ترورویسم سایبری Cyber Terrorism تعبیر می‌کنند .تروریسمی‌که صرفا در محیط و فضای سایبر به دنبال قربانیان خود می‌گردد. به لحاظ مفهومی فضایی سایبر، حوزه جهانی در محیط اطلاعاتی است‌که ماهیت متمایز و منحصر به فرد آن براساس استفاده از طیفی از الکترونیک‌ها و الکترو مغناطیس‌ها جهت ایجاد، ذخیره، تعدیل، تبادل و استفاده از اطلاعات از طریق شبکه‌های مرتبط به‌هم و وابسته به‌هم با استفاده از فن‌آوری‌های اطلاعاتی- ارتباطی شکل می‌گیرد(فرانکلین ۱۳۹۴، ص ۶۶).

پرواضح است‌که در محیط سایبر افراد با هویت‌های غیر واقعی و تن‌ها بر اساس تخیلات شخصی در محیط رسانه‌ای اینترنت حاضر می‌شوند و در هر قالب و عنوانی خودرا معرفی و با دیگران ارتباط برقرار می‌کنند. امروز در هر نقطه‌ای از دنیا با هر عنوان و شغلی و هر سلیقه‌ای می‌توانید در قالب یک شخصیت و حتی مراجع(رسمی و غیر رسمی) ظاهر شده و به عنوان مثال دوست‌یابی کنید و یا تبادل افکار نمایید و یا حتی به معاملات تجاری کلان دست بزنید. حضور پرنگ و بی‌شمار افراد مختلف و از قشرهای گوناگون جامعه در شبکه‌های بین المللی(اینترنت) باعث شده است انواع جرائم کامپیوتری وارد فرهنگ حقوق جزا شود(برومند باستانی، ۱۳۸۶، ص ۶۲) که از آن جمله ترورسیم سایبری[1] است.

به دیگر سخن، تروریسم سایبری در تعبیر ساده و در نگاه نخست، همان تروریسم است‌که در فضای سایبر رخ می‌دهد... جدید بودن تروریسم سایبری به اعتبار جدید بودن بستری است‌که در آن ارتکاب می‌یابد ولی متفاوت بودن آن با خود پدیده تروریسم به معنای تمایز

در برخی شرایط و اجزای رکن مادی جرم یا به تعبیر دقیق‌تر رفتار سرزنش پذیر است وگرنه چنان نیست‌که تروریسم در یک سرزمین گام نهاده و تروریسم سایبری در سر زمین دیگر. برعکس، تروریسم سایبری، چهره نوین خود تروریسم است؛ اما نه این‌که یکی از صور ساده آن باشد. بلکه این چهر نوین با ویژگی‌ها و شرایط منحصر به فردی همراه است. این نکته نشان می‌دهد که شناسایی تروریسم سایبری، پیش و بیش از هرچیز در گرو شناخت کلی خود تروریسم است(پیشین، همانجا، ص ۳۳ و ۳۴). چرا که با وجود نوظهور بودن، سایبر تروریسم به‌مراتب خطرناک‌تر از تروریسم کلاسیک و سنتی می‌باشد و تهدیدات آن برای امنیت ملی دولت‌ها و کشورها به خطری بالقوه تبدیل شده است(پورنقدی، ۱۳۹۲ص ۳۵) و به شناخت بیشتری نیاز دارد. شناختی‌که از هر جهت لازم و ضروری است. دولت ها امروزه به دنبال جرم انگاری و مبارزه حقوقی- کیفری علیه ستاد تروریسم سایبری اند. مبارزه منطقی و عادلانه با این پدیه نوین و در عین حال پیچیده، می‌طلبد که از هرلحاظ مورد نقادی و کنکاش علمی قرار گیرد تا با مشخص شدن ماهیت، قلمرو، کاربست‌ها و میزان ایجاد خسارتی‌که به‌بار می‌آورد، علاوه بر تدوین یک سیاست جنایی منسجم و کار آمد، روندهای ساندهی برخوردهای کیفری با مجرمان از حوزه قانونگذاری در بخش آئین دادرسی کیفری گرفته تا تعیین شاخص‌های اصلی مبین اصول کلی تحمیل مجازات به‌صورت منطقی و عدالت محور طراحی گردد.

به همین جهت، پژوهش حاضر در نظر دارد با توجه به ظرفیت محدود، ابتدا ماهیت این پدیده خطرناک بین المللی را واکاود و تا آنجا که در توان دارد، نیم نگاهی نیز به مشکلات حقوقی فرارو داشته باشد.

۱- تعریف

تروریسم سایبری نیز مانند دیگر جرائم و از جمله خود جرم تروریسم، تعریف واحد حقوقی که بتوان به عنوان تنها تعریف مرجع به آن نگریست، ندارد به همین جهت با مراجعه

به منابع مربوط، با تعاریف گوناگون مواجه می‌شویم که در ادامه به نمونه‌های از آن اشاره می‌گردد. مارک پولیت، مأمور ویژه‌ای اف بی آی تعریف کاربردی را به این شرح ارائه می‌کند: «تروریسم سایبری، حمله‌ای با قصد قبلی و با انگیزه سیاسی علیه اطلاعات، سامانه‌های رایانه‌ای و داده‌ها است‌که منجر به خشونت علیه هدف‌های غیر نظامی توسط گروه‌های فروملی یا سازمان‌های زیر زمینی می‌شود»(Pollitt Mrk, 1997, pp. 285-289.؛ به نقل از پاکزاد، ۱۳۹۰، ص ۸۸) و شاید مخصتر ترین و مناسب‌ترین تعریف معنوی از تروریسم سایبری این باشد که «تروریسم سایبری عبارت است از هر اقدام غیر قانونی بر ضد سیستم‌ها و اطلاعات با انگیزه‌های سیاسی»(پاکزاد، همان، ص ۸۹)

همچنانکه، «تروریسم سایبری از همگرایی تروریسم و فضای سایبر به وجود آمده است. درک عمومی براین است‌که به معنی تهاجمات و تهدید به تهاجمات غیر قانونی به رایانه‌ها، شبکه‌ها و اطلاعات ذخیره شده در آنها می‌باشد که به منظور ارعاب یا وادار کردن یک دولت یا مردم آن برای پیشبرد اهداف سیاسی یا اجتماعی صورت می‌گیرد. به علاوه، برای این‌که یک تهاجم، تروریسم سایبری تلقی شود، باید منجر به إعمال خشونت علیه اشخاص یا اموال گردد یا حد اقل آنقدر خسارت وارد آورد که منجر به وحشت گردد. تهاجماتی‌که باعث فوت، آسیب جسمی، انفجار، تصادم هواپیما، آلودگی آب یا لطمه شدید اقتصادی می‌شوند، از جمله این موارد هستند. تهاجمات شدید علیه زیرساخت‌های حیاتی می‌تواند اقدامات تروریستی سایبری تلقی شود، البته به میزان آثار آنها بستگی دارد. تهاجماتی‌که خدمات غیرضروری را قطع یا نهایتا مزاحمت هزینه‌بری را ایجاد می‌کنند، تحت شمول این تعریف قرار نمی‌گیرند»(جلالی فراهانی، ۱۳۸۹،ص ۱۷۸؛ همو، به نقل از بای ۱۳۹۳ص ۲۱۷).

به‌نظر می‌رسد این تعریف، کپی برداری شده از تعریفی است‌که توسط کارشناسان وزارت دفاع و امورخارجه آمریکا از تروریسم سایبری انجام داده اند و نویسنده محترم با اندک تغییرات در متن به‌کار رفته، از آن بهره گرفته باشد. از این رو لازم است متن کامل تعریف

تروریسم سایبری را از کتاب قدرت سیاسی و امنیت ملی به قلم کرامر فرانکلین و همکاران ایشان ذکر نماییم تا مشخص گردد که تفاوت و همسویی تعریف در چه اندازه قابل بازخوانی است. بر اساس این تعریف مقصود از ترورسیم در واقع:«حمله یا تهدید به حمله مبتنی بر رایانه به قصد ایجاد رعب یا اجبار دولت‌ها یا جوامع در پیگیری اهدافی‌که سیاسی، مذهبی یا ایدئولوژیکی هستند. حمله باید به اندازه کافی مخرب یا نفاق افکن باشد که ترس قابل مقایسه‌ای با آنچه که اقدامات فیزیکی تروریسم سبب می‌شوند ایجاد کنند. حملاتی که منجر به مرگ یا جراحت فیزیکی، قطع برق در منطقه وسیع، برخورد هواپیماها، آلودگی آب یا خسارت عمده اقتصادی می‌شوند از جمله این حملات به شمار می‌روند. حملاتی‌که خدمات غیر ضروری را مختل می‌کنند یا حملاتی‌که عمدتا یا نسبتا آزار دهنده هستند جزو تروریسم سایبری محسوب نمی‌شوند»(فرانکلین، ۱۳۹۴، ص ۵۵۹) نوع خاصی از حملات با هدف قرار دادن موارد مشخص است.

۲- ابزار به کار رفته در تروریسم سایبری

گروه‌های ترورسیم مستقر در فضای سایبر نیز مانند تروریست‌های فیزیکی برای پیشبرد اهداف خود از ابزار و وسایل مورد نیاز استفاده می‌کنند. با استفاده از برنامه‌های جعلی به نام ویروس، کرم، یا بمب‌های منطقی به منظور یران خسارت از طریق پاک کردن، صدمه زدن، مخدوش نمودن یا موقوف‌سازی داده‌ها یا برنامه‌های کامپیوتری انجام می‌گیرد(باستانی، برومند، ۱۳۸۶، ص ۵۴)[۲] برخی دیگر از کارشناسان فنی، هکرها[۳] را از ابزارهای حملات تروریستی در فضای سایبری می‌دانند و معتقد اند، حملات سایبری به گروه یا تعداد زیادی از اعمال ارتکابی از سوی هکرها اطلاق می‌شود که بعضا با خشونت یا آثار شدید همراه است(بی‌نا، ۱۳۹۵). ماهیت«چندرسانه‌ای» فضای سایبر به تروریست‌ها امکان بهره‌برداری‌های سوء دیگری را هم داده است. فشار یک دکمه کافی است تا انتشار بد افزارهای مخرب رایانه‌ای در عرض چندثانیه هزاران سیستم رایانه‌ای و مخابراتی در جهان‌را آلوده کند. به باور

خبرگان دانش نرم افزاری سیستم کامپیوتری، رایج‌ترین روش‌های این نوع تروریسم عبارتند از هک کردن، شیوع ویروس‌های رایانه‌ای، جاسوسی الکترونیک، دزدی هویت و تخریب یا دست‌کاری اطلاعات. تذکر این نکته لازم است که نرم‌افزارهای مخرب رایانه‌ای‌که تروریست‌های مستقر در محیط سایبر از آن‌ها برای پیش‌برد اهداف خود استفاده می‌کنند، به این چند نمونه‌ی مورد اشاره محدود نمی‌شود؛ بلکه متنوع اند و روز به روز در حال گسترش اند که از آن‌جمله می‌توان به ویروس‌ها، کرم‌ها، تروجان‌ها و اسپم‌ها اشاره کرد(بی‌نا، ۱۳۹۵).

در این میان کسانی نیز هستند که با ارائه اسناد و مدارک میدانی می‌خواهند اثبات کنند که ابزارهای مورد نیاز تروریسم سایبری و وسائلی‌که تا کنون از آن علیه کشورهای خاصی مانند ایران استفاده شده است، از تنوع بیشتری برخوردار است. به باور این دسته از تحلیل‌گران، آمریکا و رژیم صهیونیستی با انجام حمله‌های سایبری از تأسیسات هسته‌ای، (استاکس‌نت[۴]) تا ویروس شعله(Flame)[۵]، استارس(STARS)[۶]، دوکوپ(Ducu)[۷]، فلیم یا و اکوئیشن(Equation) انجام داده اند که همگی در راستای تروریسم سایبری علیه ایران تعریف می‌شود(عضو هیأت رئیسه کمیسیون امنیت ملی و سیاست خارجی مجلس، ۱۳۹۵).

۳- دشواری تشخیص هویت مجرم واقعی

نکته‌ای دیگر به ارتکاب عمل‌های مجرمانه‌ای مربوط می‌شود که فضای سایبر در اختیار مرتکبین جرایم سایبری قرار داده است، این امکان وجود دارد که مجرمین سایبری، البته آنهایی‌که از شیوه‌های نوین نفوذ غیر مجاز یا همان هک آگاهی کامل دارند، به‌راحتی از سیستم‌های رایانه‌ای دیگران برای ارتکاب جرایمشان استفاده کنند. در این‌صورت، ممکن است شخص حاضر در کشور دیگری به دلیل ارتکاب جرمی تحت تعقیب قرار گیرد که حتی روحش هم از آن بی خبر است. نمونه‌هایی از این‌دست بسیار است و اینجا هنر مجریان قانون را می‌طلبد که با بررسی دقیق دلایل و مدارک معتبر الکترونیکی و غیر الکترونیکی، صحت و سقم قضیه را روشن کنند. در همین راستا، مباحثی چون عذر عدم حضور در صحنه

جرم سایبری[۸] و تخصص در تطبیق آن با واقعیات به‌خوبی اهمیت خودرا نشان می‌دهد(جلالی فراهانی، ۱۳۸۹، ص ۸۵. برای این‌که حضور فیزیکی شخص در محل وقوع حادثه معنایی ندارد؛ مثلا برای سرقت از یک بانک، مدت مشخصی لازم است‌که سارق با حضور در محل دست به چنین عملی بزند، ولی ارتکاب جرم رایانه‌ای در مدتی کوتاه و بدون حضور در محل امکان‌پذیر است(حسینعلی بای و بابک‌پور قربانی، ۱۳۸۸، ص ۷۴). چرا که هرچند «مجازی بودن این فضا به معنای غیر واقعی بودن آن نیست زیرا در این فضا همان ویژگی هایی که در تعاملات دنیای واقعی انسانها وجود دارد، حاکم است(محمد مهدی انصاری، بی‌تا، ص ۴۱۷)، ولی«تشخیص تفاوت‌های موجود بین جرائم سایبری، تروریسم سایبری و جنگ سایبری اغلب دشوار است و معمولا ناظر را گمراه می‌کند. علل این امر فقط مسائل فنی نیست، اما واقعیت فیزیکی اینترنت می‌گوید که شناسایی مهاجم کار آسانی نیست. یکی از مشکلات اصلی مجزا کردن حمله‌های سایبری بر اساس عاملان آن‌ها به گروه‌های مجرم، تروریستی و نظامی این است‌که این هویت‌ها ممکن است سیال و مبهم باشند. حتی اگر بتوان مهاجمی را به‌طور فردی شناسایی کرد، این احتمال وجود دارد که مجرم سایبری در جنگ سایبری‌که تروریسم سایبری شناخته می‌شود نیز شرکت کنند؛ به همین ترتیب، در واقع جرم سایبری چه‌بسا گاه با جنگ سایبری اشتباه گرفته شود یا تروریست سایبری ممکن است تلاش کند با جعل هویت، خودرا در موقعیت سرباز سایبری جا بزند، که احتمالا تبعاتی جدی در پی خواهد داشت. ابهام در محیط سایبری واقعیتی است. مشکل تخصیص چنین دسته بندی‌های مشخصی به عاملان و سیاست‌های پیشنهادی مربوط به آن‌ها، چندین سال است‌که به چالشی اساسی تبدیل شده است(بی‌نا، امنیت و جنگ سایبری۱، ۱۳۹۱ص ۷۹)

علت این‌همه تأکید در ارتباط با دشوار بودن تشخیص هویت تروریست سایبری این است‌که ردیابی تروریست‌های سایبری نیز کار ساده‌ای نیست. آن‌ها می‌توانند با هویتی غیر واقعی در فضای مجازی وارد شوند و یا با هک کردن رایانه افراد دیگر از مسیر رایانه فرد

هک شده اهداف تروریستی خود را دنبال کنند. گستره فعالیت آن‌ها به وسعت تمامی مراکزی است‌که به نوعی به سیستم‌های رایانه‌ای مجهزند و به اینترنت متصل می‌شوند(گروه امنیت سایبری گرداب، ۱۳۹۵). در دیگر جرائم سایبری هرچند باور بر عمومی این است‌که معمولا این‌گونه مجرمان افراد باهوشی نیستند(خداقلی زاده، ۱۳۸۳ص ۳۲)، و لذا به باور بسیاری از کارشناسان« در حال حاضر تکنولوژی در اختیار مقام‌های قضایی آنقدر پیشرفته است که می‌توان به کمک یک نرم‌افزار، از داخل یک تلفن همراه خاموش با فشار یک دکمه تمامی اطلاعات داخل تلفن از قبیل شماره‌های تماس، عکس، فیلم و... را دریافت کرد»(کارشناس، ۱۳۸۰) هرچند در دیگر جرایم این‌گونه بتواند رد هویت مجرمان را زد، ولی در تروریسم سایبری‌که معمولا توسط گروه‌های تروریستی حتی با پشتوانه‌ای مالی و بهره‌گیری از دانش پیشرفته و تخصص برخی دولت‌ها انجام می‌پذیرد، بدلیل همکاری مستقیم برنامه نویسان و متخصصین فنی در حوزه رایانه‌ی، اغلب افراد باهوش و استعداد بالایی حضور دارند. کارپردازان نخبه‌ای‌که از یک‌سو با تمام حفره های امنیتی آشنایی کامل دارند و از سوی دیگر، علاوه بر انجام حملات موفقیت آمیز تروریستی، می‌توانند چنان با مهارت از صحنه‌ی ارتکاب جرم خارج شوند که تا حد ممکن هیچ‌گونه آثار و علامتی از خود برجای نگذارند.

بنابراین، اولین گام شناخت هویت واقعی تروریسم در فضای سایبری است و تا زمانی‌که هویت مجرم شناخته نشود، فرایند کشف و تحقیق جرم و همین‌طور تعقیب و مجازات مجرم نیز معنی ندارد.

۴– ضرورت‌های تقینی و مشکلات فرارو

امروزه به‌روشنی همه دریافته اند که «مضمون اطلاعات در کارکردی نرم‌افزارانه برای شکل‌دهی به افکار عمومی مورد استفاده قرار می‌گیرد و اعتماد عمومی، مشروعیت و جذابیت کلی را شکل می‌دهد»(حجت اله مرادی، ۱۳۸۹، ص ۶۹) و از سوی دیگر با این استدلال که« ظهور یک برنامه امنیتی جهانی در آینده‌ای نزدیک امکان پذیر نباشد»(همو، پیشین، ص

۷۷)، ناگزیر باشیم واکنش دولت‌ها را به‌صورت انحصار خشونت سیستمی در چارچوب امنیت ملی توجیه پذیر بدانیم، باید قبول نماییم که در همه کشورها، «حقوق کیفری با مشکلات قابل ملاحظه‌ای در برخورد با جرائم کامپیوتری مواجه است. در حال حاضر بدلیل گسترش تکنولوژی اطلاعاتی(IT[۹]) و اجزاء وابسته به آن در اکثر کشورهای دنیا، مشکلات ناشی از جرائم کامپیوتری گریبان‌گیر تمامی کشورهای جهان به‌طور کم و بیش گشته است و ضرورت دارد در حوزه تقنین کار بیشتری صورت‌گیرد. زمینه مشترک همه این مسائل مربوط به تکنولوژی کامپیوتر، از این واقعیت ناشی می‌شود که در حال حاضر همه قوانین کیفری غالبا اشیاء ملموس و قابل روئیت را مورد حمایت قرار می‌دهند و حمایت از اطلاعات و اشیاء نا ملموس و غیر فیزیکی مورد حمایت قانونی عملا تا اواسط قرن بیستم صورت نگرفته بود... در زمینهٔ آئین دادرسی و حقوق جزای بین الملل نیز جرایم کامپیوتری مسائل خاصی را مطرح نموده اند که نیاز به بررسی دارند. جایگزینی ادله غیر قابل رؤیت و غیر ملموس در عرصهٔ تکنولوژی کامپیوتری به‌جای موضوعات ملموس و قابل رؤیت، مأمورین قضائی را با مشکلات عدیده‌ای در زمینه تحقیق، تفتیش و جمع آوری ادلهٔ لازم جهت اثبات جرم مواجه نموده است و برای جامعه حقوقی این سؤال مطرح شده است که آیا اختیارات و مقررات موجود در آئین دادرسی کیفری برای حسن انجام تحقیقات مقدماتی و رسیدگی به (برومند باستانی، ص ۸۱) با چنین مشکل فراگیری که امروزه با آن مواجهیم برای مبارزه مؤثر با پدیده ویران‌گری به نام تروریسم سایبری کافی است؟ بدیهی است از نگاه ضرورت‌ها و بایسته‌های حقوقی، پاسخ کاملا منفی است و می‌طلبد دست‌گاه‌های قانونگذاری و نهادهای قضائی به این مسئله توجه ویژه‌ای از خود نشان دهند.

از طرفی نیز باتوجه به طبع فراملی بودن برخی از جرائم کامپیوتری به خصوص جرائم نسل جدید سبب گشته با افراد و کشورهای درگیر در قضیه افزایش یافته و همین موضوع موجب بروز تعارضات بین المللی چه از لحاظ صلاحیت رسیدگی دادگاه‌های صالح و چه

از نظر جمع‌آوری ادله گردد(همان، ص ۸۲). به همین جهت ضرورت دارد، مسئله مشکلات تقنینی را در دو حوزه قوانین شکلی و ماهوی و باتوجه به تأکید بر ضرورت‌های قانونگذاری کار آمد، به بررسی خواهیم گرفت.

٤-١ در حوزه قوانین شکلی(آئین دادرسی کیفری)

نخستین گام در ارتباط با حوزه قانون‌گذاری، توجه به قوانین شکلی است. این قوانین که به آئین دادرسی معروف است، تنها به روش رسیدگی به پرونده‌های کیفری و حقوقی می‌پردازد. در این مقطع آنچه مورد توجه می‌باشد، تدوین مجموعه قوانین و مقرراتی است‌که روش رسیدگی به پرونده‌های کیفری را پی می‌گیرد. روشی‌که از شروع به تحقیق در رابطه با جرم آغاز و در ایستگاه اجرای مجازات از حرکت می ایستد. چرا که آئین دادرسی کیفری، مجموعه اصول و مقرراتی است‌که برای کشف و تحقیق جرائم و تعقیب مجرمان و نحوه رسیدگی و صدور رأی و تجدیدنظر و اجرای احکام و تعیین وظایف و اختیارات مقامات قضائی وضع شده است(علی خالقی، ۱۳۸۸، ص۷). و چون طبق ماده ۲ (ق.آ.د.ک) مصوب ۱۳۹۲، دادرسی کیفری باید مستند به قانون باشد[۱۰] تا بتواند حقوق طرفین را تضمین کند، به این نتیجه می‌رسیم که در تروریسم سایبری به عنوان پدیده نوین مجرمانه، مشکلات اولیه در تحقیقات مقدماتی بروز می‌کند، چون عنصر مادی جرم کامپیوتری از طریق وارد کردن، محو، تغییر و ... داده، اطلاعات، برنامه‌ها و سیستم کامپیوتری، مخابراتی و ... تحقق می‌یابد. مقامات تعقیب و تحقیق دارای اختیاراتی هستند که در قوانین دادرسی کیفری، بدان اشاره شده و به هنگام بازجویی، بازرسی، معاینه محل، توقیف اشیاء مربوطه و .. بر چگونگی آن ها حکم‌فرما است؛ اما در جرایم رایانه‌ای با محیط‌های دیجتالی سروکار داریم و به تبع، خصایص این محیط‌ها بر قواعد مرسوم اثر می‌گذارد(حسینعلی بای، همان، ص ۷۶). هرچند به باور جرم‌شناسان در گروه‌های تروریستی(فزیکی)، در بسیاری مواقع افرادی‌که در رده‌های پائین، جرم را انجام می‌دهند، خود طعمه شده و حذف می‌شوند(فرید محسنی، ۱۳۹۴ص۱۷۲)،

لیکن در تروریسم سایبری بحث حذف و از بین رفتن مطرح نیست، و لذا تدوین مجموعه مقررات آئین دادرسی خاص خودرا می‌طلبد، تا بتواند به دادرسی عادلانه[11] جامه عمل بپوشاند.

بنابراین، باتوجه به توضیحاتی‌که گذشت، بدون تردید مشکلات تقنینی در ارائه مجموعه مقررات آئین دادرسی کیفری، کاری بس دشوار است و مشکلات خاص خودرا دارد. دشواری‌هایی‌که شناخت بستر کامل آن نیاز اساسی به رعایت اصول حاکم بر قواعد عمومی بین الملل و حفظ استقلال دولت‌ها در مواجه حقوقی با این پدیده در عرصه‌ی بین المللی دارد. وجود چنین مشکل هنگامی بیشتر بر جستگی خودرا به نمایش می‌گذارد که بخواهیم در حوزه حقوق داخلی نگارش مقررات آئین دادرسی کیفری را مطمح نظر قرار دهیم. موانعی‌که ارزیابی هریک از آن‌ها به نگارش کتابها و مقالات مفصل نیاز دارد. شاید بهمین جهت باشد که تاکنون در جمهوری اسلامی ایران، تنها قانون جرائم رایانه‌ای آنهم در ۱۱بهمن سال ۱۳۸۹، در هشت فصل و بیست و هشت ماده به تصویب مجلس شورای اسلامی رسیده و در این قانون نیز تنها به‌صورت کلی و نه مستقل، مجموعه‌ی جرایم اینترنتی را بدون توجه به اهمیت تروریسم سایبری‌که خود دنیای بزرگی از مباحث گسترده حقوق کیفری را در بر می‌گیرد، نگریسته شده است.

۴-۱-۱ تداخل صلاحیت‌ها و ضرورت تفکیک آن‌ها

اولین معضل در تدوین مقررات آئین دادرسی کیفری مربوط به تروریسیم سایبری، این است‌که گاه وظایف دو نهاد اجرائی و قضایی را به‌صورت متداخل و یا متعارض قرار می‌دهد و ضرورت دارد قانونگذاران، با دقت بیشتر به تفکیک آن‌ها بپردازد. با این توضیح که از یک‌سو نهاد قضائی به عنوان تنها نهاد متولی قانونی مبارزه با جرایم، متصدی کشف جرم، تعقیب مجرم و دیگر فرایند رسیدگی به امور کیفری است و از سوی دیگر در مساله تروریسم سایبری با توجه به اهمیت و خطر آفرینیی‌که دارد، به دخالت مستقیم نهاد اجرای کشور از

جمله نهاد ریاست جمهوری در ضلع دیگر پازل نیاز است. دلیل این تداخل کاری را باید در لابلای توجه خاص به مسئله امنیت اطلاعات و سیاست‌های مرتبط با آن به جست‌وجو بگریم. به باور کارشناسان امنیت اطلاعات به‌طورکلی، سیاست‌های امنیت اطلاعاتی، احکام، استانداردها و رهنمودهای مربوط به سیستم‌های اطلاعات باید تحت نظارت رئیس جمهور باشند و زیرنظر رؤسای سازمان‌هایی‌که مسئول نظام‌های امنیت ملی هستند، اجرا شوند(امنیت و جنگ سایبری۴، ۱۳۹۲ص۹۳). نظارت مستقیم و فنی نهاد ریاست جمهوری از جمله وزارت اطلاعات و فناوری اطلاعات بر سازمان‌های امنیت اطلاعات و امکاناتی‌که برای رصد و مبارزه با تروریسم در اختیار این نهاد اجرایی قرار می‌گیرد، هرگاه در قانون آئین دادرسی کیفری به خوبی تبیین نگردد، می‌تواند موجب سردرگمی و ایجاد ترافیک کاری بین دو قوه و گاه به کشمکش‌های سیاسی و حتی حقوقی منجر شود که پیامد بسیار زیانبار تر از رسیدگی به اصل جرائم تروریسم سایبری توسط نهاد قضائی دارد.

تا اینجا همه آنچه مورد اشاره قرار گرفت، به حقوق داخلی کشورها مربوط می‌شد، ولی نباید ندیده انگاشت که مسئله تداخل صلاحیت‌ها هم‌چنان‌که در حقوقی داخلی بازتاب ویژه دارد، صلاحیت بین المللی دولت‌ها را نیز دست‌خوش تغییرات بنیادین هم از نگاه اصل حاکمیت سرزمینی و هم از جهت تعارض آن با قواعد حاکم بر حقوق بین المللی می‌نماید که بایست در جای خود به‌طور مفصل به بحث گذاشته شود.

۴-۱-۲ فقدان تحلیل جامع کیفرشناسانه از تروریسم سایبری

جای هیچ‌گونه تردیدی باقی نیست‌که برای تدوین مربوط به آئین دادرسی کیفری در مبارزه با جرم تروریسم سایبری مانند دیگر جرایم، به یک تحلیل علمی و دقیق کیفرشناسانه نیاز است. امروزه مباحث جرم‌شناسی در دو حوزه کاربردی و نظری به دلیل مواجهه با جرائم سنتی و هرچند به ندرت تروریستی به معنای عام، نتایج ارزشمندی از پژوهش‌های علمی و میدانی در اختیار نهادهای قانون‌گذاری و سیاست‌ورزان جنایی قرار داده است، لیکن هنوز

در سنگر مبارزه با تروریسم سایبری‌که محصول توسعه دانش نوین اطلاعات رایانه‌ای می‌باشد، تحلیل روشن از وضعیت ارتکاب جرم، انگیزه مجرمان، شرایط اوضاع و احوال روانی و سیاسی یا اجتماعی بر فرایند ارتکاب جرم که بتواند راهکار مفیدی ارائه دهد وجود ندارد.

از آنجا که به باور جرم‌شناسان، یکی از علل و عوامل اصلی افزایش روحیه ستیزه جویی و قانون‌شکنی در جامعه افزایش هرج و مرج و بی‌نظمی حقوقی در جامعه است(غلام‌رضا محمدنسل، ۱۳۹۳ ص۱۸۴)، فقدان تحلیل جامعه کیفرشناسانه می‌تواند زمینه‌های خوبی برای این هرج و مرج در حوزه قانون‌گذاری شکلی را فراهم آورد. از همین رو است‌که در قوانین جدید و قدیم ایران بدلیل نامشخص بودن جایگاه تروریسم، جای خالی جرم‌انگاری تأمین نیروی انسانی(بتول پاکزاد، ۱۳۹۰، ص ۳۲۷) و یارگیری‌های لازم برای گسترش نیروهای فعال در حوزه تروریسم سایبری را شاهدیم.

بنابراین، تازمانی‌که دانشگاه‌ها و مراکز علمی، تحقیقات خودرا با محوریت کیفرشناسی نوین هم‌سو با موضوع تروریسم سایبری گسترش ندهند، طبیعی است نتایج قابل قبولی در این زمینه نخواهیم داشت و فقدان این عنصر کلیدی در سامانه نگاری مجموعه قوانین آئین دادرسی کیفری، از بزرگترین معضل در سیستم قانون نگاری می‌باشد. علاوه برآن موانع دیگری نیز وجود دارند که بدلیل پرهیز از پراکنده گویی، پرونده مباحث مربوط به این بخش را همین‌جا می بندیم و سراغ مشکلات موجود در حوزه قوانین ماهوی متمرکز می‌نماییم.

٤-۲- درحوزه قوانین ماهوی

به‌طور کلی، مقررات ماهوی مقرراتی است‌که برای ایجاد حق و مدیریت حقوق وضع شده است مانند دادگاه مدنی، لکن دادگاه کیفری به مواردی رسیدگی می‌نماید که در قوانین جرم تعریف شده باشد(رجبعلیان، ۱۳۹۶). به‌دیگرسخن، در مقررات ماهوی کیفری، همواره سخن از تبیین ماهیت اعمال مجرمانه، ارکان و شرایط مسئولیت کیفری، علل و عوامل رافع

مسئولیت، علل موجهه جرم، روش و منابع تفسیر حقوق کیفری، تعریف ادله اثبات دعوای کیفری خاص، و مجموعه اصول، قواعد و مقرراتی‌که ارتباط مستقیم با جرم انگاری و پاسخ کیفری عادلانه با رعایت قاعده تناسب جرم و مجازات به این بزه سایبری دارد می‌باشد. در تروریسم سایبری وضع مقرراتِ به‌روز و کار آمد که بتواند تا حد زیادی به تبیین ماهیت این عمل مجرمانه پوشش لازم را ارائه نماید، امروزه از اهمیت زیادی برخوردار است. چه این‌که این مجموعه مقررات، در حوزه حقوق جزای اختصاصی باشد و یا حقوق جزای عمومی. هم‌چنان‌که جای خالی آن در حقوق داخلی بسیاری از کشورها به روشنی احساس می‌شود، در حقوق بین الملل، کنوانسیون‌ها، معاهدات و آئین‌نامه‌های دیوان کیفری بین المللی نیز قابل لمس است.

در مقررات ماهوی باید مشخص گردد که آیا جرم تروریسم سایبری در ردیف کدام یک از جرائم قرار می‌گیرد و در کدام یکی از شاخه‌های حقوق جزا گنجانده شود. حقوق جزای عمومی و یا حقوق جزای اختصاصی. هرگاه حقوق جزای اختصاصی متکفل بحث از این عمل مجرمانه باشد، رابطه مستقیم آن بیشتر با امنیت و آسایش عمومی است یا با جرایم علیه تمامیت جسمانی افراد و همین‌طور با جرم علیه مالکیت و اموال ارتباط پیدا میکند. در صورتی‌که همه موارد پیش گرفته را در بر گیرد، کدام یکی را عنوان اولی و کدامین یکی دیگر را عنوان ثانوی بدانیم. وانگهی در صورتی‌که با حقوق جزای عمومی و روابط بین افراد و حاکمیت مرتبط باشد، قلمرو اصول مترقی حقوق جزا اعم از اصل برائت، اصل عطف به ماسبق نشدن مقررات کیفری و دیگر اصول مشابه را تا کجا می‌توان در نظر گرفت. از همه اینها که بگذریم، در حقوق جزای بین الملل نیز با توجه اهمیت امنیت بین المللی و خطرات ناشی از حملات تروریستی در محیط سایبر، چگونه می‌توان از ظرفیت‌های موجود در قواعد بین المللی اعم از جزای اختصاصی و جزای عمومی بهره گرفت. همه این‌ها مباحثی است‌که ضرورت تدوین مجموعه مقررات ماهوی را بیش از پیش مبرهن می‌کند. مراجعه به قوانین

موجود در ایران نشان می‌دهد که تا کنون توجه خاصی به تروریسم سایبری صورت نگرفته و آنچه تحت عنوان مقررات مربوط به جرائم اینترنتی تاکنون به تصویب رسیده، توان پاسخ‌گویی لازم در میدان مبارزه مقتدرانه کیفری با این عمل مجرمانه را ندارد و استفاده از اطلاقات یا ظهور و نصوص موجود در دیگر مقررات نظیر قانون مجازات اسلامی یا قوانین مربوط به جرائم نیروهای مسلح و حتی قانون مبارزه با جرایم اینترنتی نیز، از محمل حقوقی لازم برخوردار نیست. به همین منظور لازم است سیاست کیفری مشخصی در نظر گرفته شود. بر اساس این سیاست کیفری، دیگر مراحل مقررات ماهوی را لزوما باید پیمود.

۴-۲-۱- فقدان جرم انگاری بازدارنده و ضرورت تدوین آن

جرم انگاری اولین گام در تدوین سیاست کیفری ماهوی است. به باور پژوهش‌گران، جرم‌انگاری مهم‌ترین و آشکارترین دستاویز رویارویی با اعمال سرزنش پذیر و مخاطره آور است. جرم‌انگاری نه تنها با پشتوانه قدرت همراه است، به‌طور تبعی به کیفرانگاری نیز اشاره دارد و از این‌رو آنچه در جرم‌انگاری برجسته است، کیفر یا کیفرهایی است‌که در برابر رفتارهای سرزنش پذیر نهاده شده است(پاکزاد، ۱۳۹۰ ص۲۷۵). باتوجه به این‌که فضای سایبر علیرغم قرابت‌هایی‌که با رسانه‌های گروهی دیگر آن‌هم صرفا در بعد انتقال اطلاعات دارد، تفاوت‌های چند آن‌را از سایر رسانه‌ها جدا می‌سازد(فضلی، ۱۳۹۱ص۱۳۴)، و جرم‌انگاری اعمال بدون توجه به شیوه‌های صحیح آن، باعث متروک ماندن آن عمل از دیدگاه سیاست جنایی- قضائی می‌شود(ص ۶۷) در نظام حقوق داخلی ایران جرم‌انگاری مستقلی صورت نگرفته و تنها در ذیل جرائم رایانه‌ای بدون جایگاه مشخص، گنجانده شده است. کارکرد این عدم استقلال از همان نقطه آغازین پیداست که باشکست قطعی در میدان پیکار با شکل نو پیدای از یک جرم پیشرفته مواجه است.

با این حساب به نظر می‌رسد، جرم‌انگاری این عمل مجرمانه در قوانین داخلی از اهمیت خاصی برخوردار است. جرم انگاری نیز باید بگونه‌ای باشد که جنبه‌ی بازدارندگی آن

برجستگی خاصی را روی صفحه‌ی دید تروریست‌های سایبری به نمایش بگذارد. آنچنان این جرم‌انگاری از جذابیت و قدرت بازدارنگی برخوردار باشد که به محض مشاهده، بتواند در ارکان تصمیم‌گیری تروریسم سایبری تزلزل ایجاد کند. این هدف زمانی حاصل می‌شود که علاوه بر توجه به روش‌های صحیح اجرای مجازات‌ها، توجه به شخصیت مجرم، علل و عوامل روی آوری به ارتکاب جرم و مجموعه عناصر دخیل در شکل‌گیری این بزهکاری نوین، قویا مورد توجه قانون‌گذار قرار گیرد.

۴-۲-۲- فقدان عنصر تناسب میان جرم ترور سایبری و مجازات‌های موجود

مطالعه تاریخ حقوق کیفری به خوبی نشان میدهد که جرم انگاری هرچند سخت و با شدت صورت گیرد، در صورتی‌که بین عمل ارتکابی و وضع مجازاتها تناسب وجود نداشته باشد، هرگز کارکرد لازم را ندارد و نمی‌تواند موجب کاهش انگیزه در ارتکاب گرم گردد. کیفر انگاری که در قوانین مربوط به جرایم رایانه‌ای صورت گرفته، از نگاه یک تروریست سایبری به شوخی دستگاه قضایی با این مجرم فنی شباهت دارد تا تحمیل مجازات بازدارنده. زیرا این قوانین از همان ابتدا برای مبارزه با تروریسم سایبری طراحی نشده و صرفا تعیین کننده یکسری سیاست‌های کوچک کیفری است که جرایم کوچکتر در حوزه جرایم رایانه‌ها را پوشش می‌دهد نه فراتر از آن. جرایم مانند؛ شنود غیر مجاز، جاسوسی رایانه‌ای، جعل، سرقت و موارد مشابه.

نا گفته پیدا است وقتی یک تروریست سایبری، محیط مجازی را برای رسیدن به اهداف خود در نظر می‌گیرد، از نگاه تیپ شخصیتی با فرد عادی متفاوت است. او یک انسانِ دارای سطح علمی بالا و درک عالی از شرایط و اوضاع و احوال حاکم بر قوانین و اقتدار حکومت‌ها است. به یقین، هم از تخصص بیشتر برخوردار است و هم از نتیجه کاری که انجام می‌دهد گاه به مراتب از جاسوسی، شنود و دیگر جرایم رایانه‌ای به لحاظ اثرگزاری روی امنیت عمومی و آسایش شهروندان و حتی قلمرو حاکمیت دولت‌ها قوی تر است. تروریستی که با

نفوذ روی سیستم پالایشگاه‌ها و ایجاد اختلال، موجب انفجار در این دستگاه‌های عریض و طویل تولیدی آتش‌زا می‌شود، گاه یک شهر را به نابودی می کشاند، هواپیمای‌که در اثر حمله تروریسم سایبری ساقط می‌گردد تمامی سرنشیانش کشته می‌شود، نیروگاه اتمیِ‌که تروریست سایبری منفجر می‌کند، تمامی آثار حیات را از یک روی زمین و یا احد اقل کشور و شهر خاص نابود می‌کند. بنابراین، با چنین مجرمی نباید مانند یک جاسوس برخورد کرد. حبس و تبعید و مجازات نقدی فرد یا گروهی‌که شهر و گاه کشور را به نابودی مطلق می‌کشانند، نه با عدالت سازگاری دارد و نه جنبه بازدارندگی خاص(پیشگیری فردی) از شخص یا اشخاص مجرمین و همین‌طور بازدارندگی عام(پیشگیری عام) از دیگر مجرمین احتمالی می‌گردد. لذا مجازات‌هایی‌که برای این جرم در نظر گرفته می‌شود، می‌طلبد تا تناسب بیشتری با جرم ارتکابی داشته باشد.

امروزه تاکیدهای مکرر کیفرشناسان برای پایه استوار است‌که هدف کیفر تحمیلی به بزهکار، تنها برقراری تعادل اجتماعی، تنبیه خطای اخلاقیِ ارتکابی و مجازات مجرم به‌لحاظ عدم رعایت وظایف اجتماعی و ارضای افکار عمومیِ نگران و منزجر نیست. علاوه بر آن، لازم است‌که هر مجازات آن‌طور انتخاب و اجرا شود که برای دیگران عبرتی باشد و کارکرد پیشگیرانه‌ی سودمندی را نیز ایفا کند(بولُک، ۱۳۸۶ص۳۱). دست‌یابی به این هدف تنها در سایه رعایت تناسب بین جرم و مجازات امکان‌پذیر است.

۴-۲-۳- فقدان توجه لازم به شخصیت مجرم و علل و عوامل موثر بر ارتکاب جرم

واژه شخصیت که به مجموعه‌یِ پیچیده‌ای از صفاتِ عاطفی و رفتاری اشاره می‌کند که به موازاتِ حرکتِ فرد از وضعیتی به وضعیتی دیگر نسبتا ثابت باقی می‌ماند(جرج ولد، ۱۳۸۰ص۱۲۸)، از نگاه جرم‌شناسان و سردسته‌های مکاتب فکری در حوزه‌های حقوق جزاء، رواشناسی و جرم‌شناسی، همواره با تعریف‌های گوناگونی مواجه بوده است. ولی به نظر

می‌رسد بهترین تعریف این باشد که شخصیت را ساختمان زیستی- روانی فرد یا مجموع عومال داخلی و فردی به انضمام عوامل اجتماعی(حمیدرضا آدابی، ۱۳۹۳ ص ۱۸۷) بدانیم.

توجه به شخصیت مجرم و این‌که چه علل و عواملی باعث شده تا وی به سمت ارتکاب جرم در فضای سایبری روی آورد، از مهم‌ترین و کاربردی‌ترین سازوکار لازم در تدوین حقوق جزای ماهوی است. چرا که به باور جامعه شناسان کیفری و حقوق دانان هم‌سو با جرمشناسان، مجازات واکنش جامعه علیه عمل مجرمانه است. مجازات قادر است مجرم را در جامعه مطرود سازد و آزارش دهد. مجرم را اصلاح کرده و جلوی تکرار جرم را بگیرد(صادقی، ۱۳۸۹،ص ۱۰۱). مجازات زمانی از چنین اقتدار برخوردار خواهد بود که از همان ابتدا قانون‌گذار با دقت تمام، شخصیت مجرم و علل و عواملی را که این فرد نگون بخت را به وادی جرم سایبری کشانده مورد توجه جدی قرار دهد. ضرورت رعایت این موضوع، مانع از توجهی‌که باید قاضی رسیدگی کننده به پرونده و دادیار تحقیق باید داشته باشند نیست.

همچنانکه قبلا گذشت، در قانون مبارزه با جرایم رایانه‌ای جایگاه واقعی این اصل پرکاربرد خالی احساس می‌شود. دلیل این امر واضح است، زیرا به باور محققان؛ اخیرا تروریسم تبدیل به موضوع پر اهمیت در جرم‌شناسی شده است(سالی اس، ۱۳۹۲ص ۲۴) و تاکنون تحقیقات علمی جرم‌شناسانه قابل قبولی راجع به تروریسم سایبری که بخشی از تروریسم را تشکیل می‌دهد انجام نگرفته. این خلاء اساسی بهتر است با تدوین قانون جدید پر گردد. قانون جامعه و در بردارنده حد اکثری از فاکتورهای لازم و بایسته‌های تقنین در حوزه تدوین سایست جامع کیفری مبارزه با تروریسم سایبری. قانون ماهوی بدلیل اهمیت و جایگاه خاصی‌که در کاهش و کنترل جرم از طریق سزادهی به مجرمان دارد، می‌طلبد مطابق با استانداردهای روز به تصویب برسد. توجه جدی به مقوله شخصیت مجرم و عوامل موثر بر تکوین جرم، یکی از این استانداردهای مورد نیاز به شمار می‌رود.

نتیجه گیری

باتوجه به مباحث پیش گفته، پژوهش حاضر به دو نتیجه اصلی منجر گردید که در ادامه به آن‌ها اشاره می‌شود:

الف: در گام نخست، تعریف ماهیت جرم تروریسم سایبری بود که مشخص گردید با تروریسم در فضای خارجی تفاوت آشکاری دارد. برخلاف تروریسم فیزیکی، تروریسم سایبری هم از نگاه هزینه و هم از نگاه ابزار کار بسیار سهل الوصول برای رسیدن به اهداف تروریست‌ها است. ابزارهایی‌که گاه به مراتب خطرناکتر از انفجار هسته‌ای است و می‌تواند به نابودی کامل شهر و کشور منجر گردد.

ب: تروریسم سایبری به دلیل پیچیده‌گی‌هایی که از نگاه فنی دارد، گاه به دشواری در تشخیص هویت واقعی مجرمان منجر می‌گردد و این خودش برای رسیدگی به اتهام و مجازات مجرمان مشکلات فراوانی را ایجاد می‌کند. مشکلاتی‌که علاوه بر حقوق جزای شکلی و آئین دادرسی، در حقوق جزای ماهوی داخلی نیز به خوبی مشاهده می‌شود. مجموعه قوانین موجود اعم از قانون مجازات، قانون مبارزه با جرایم رایانه‌ای، هیچ‌کدام قادر به پاسخ‌گویی به نیاز فعلی مبارزه با تروریسم سایبری نیست. به همین جهت، ضرورت تدوین قوانین جامع که در برگیرنده بایسته‌های قانون‌گذاری کار آمد در مبارزه مقتدرانه با پدیده نو پیدای فراگیر و رو به رشد باشد، به‌خوبی مبرهن است. بدیهی است چنین قوانینی باید بگونه‌ای طراحی شود تا بتواند از ظرفیت دانش‌های نوین جرم‌شناسی، جامعه شناسی جنایی، روانشناسی جنایی، کیفر شناسی و دیگر یافته‌های حاصل از پژوهش‌های کاربردی همسو با دانش حقوق جزا، بهره جوید.

پی نوشت‌ها

۱-Cyber- terrorism

۲- توضیح:

۱-ویروس: عبارت است از یکسری کدهای برنامه که می‌توانند خودرا به برنامه‌های مجاز بچسپانند و به دیگر برنامه‌های کامپوتری منتقل شوند. ویروس می‌تواند با استفاده از یک قطعه مجاز نرم افزاری که به ویروس آلوده شده است و یا با استفاده از برنامه‌های آلوده به سیستم کامپیوتری واردشود.

۲- کرم: نیز به طریق ویروس ایجاد می‌شوند تا بانفوذ در برنامه‌ها در برنامه‌های داده‌پردازی مجاز، داده‌ها را تغییر دهد و یا تخریب و نابود سازد اما تفاوتی‌که کرم با ویروس دارد این است‌که کرم قدرت تکثیر خودش را ندارد... و لذا با استفاده از برنامهٔ تخریبی کرم بعنوان مثال، می‌توان به کامپوتر یک بانک دستور داد که وجوه موجود در بانک را به‌طور دائم به یک حساب غیر مجاز منتقل کند.

۳- بمب منطقی: که به آن بمب ساعتی نیز گفته می‌شود، روش دیگری است‌که به کمک آن می‌توان دست به سابوتاژ کامپوتری(اصلاح، موقوف‌سازی و یا پاک کردن غیر مجاز داده‌ها یا عملیات کامپیوتری به منظور مختل ساختن عملکرد عادی سیستم، آشکارا فعالیت مجرمانه به حساب می‌آیند) زد.(برومند باستانی، صص۵۵ و ۵۶ به نقل از؛ سازمان ملل«نشریهٔ سیاست جنائی»، ۴۴-۴۳- ۱۹۹۴، ترجمه دبیرخانه شورای عالی انفورماتیک- سازمان برنامه و بودجه کشور، جلد اول، مرداد ۱۳۷۶، ص ۳۲).

۳- هکر ها معمولا برنامه نویسان سیستم هستند که از بقیه برنامه نویسان باهوشتر بوده و سوراخهای حفاظتی را شناسایی می کنند تا این سوراخها شکافها را در جای دیگری پر کنند. یک هکر می تواند مدیریت یک شبکه رو برعهده داشته باشد و برای محافظت کردن شبکه خودش از دسترس دزدی های الکترونیکی باید دست به دزدیهای الکترونیکی غیر مجاز بزند.(راه‌خدازاده، مسعود، ۱۳۸۷/۷/۳۰)

۴- استاکس نت که بستر اجرایی آن سیستم عامل خانواده ویندوز است، از طریق حافظه‌های جانبی و یا ایمیل‌های آلوده از طریق تکنیک‌های روتکیت خاص و به صورت مخفیانه وارد سامانه قربانی شده و پس از ایجاد فایلی تقلبی با پسوند PIF/LINK، شروع به انتشار خود می‌کند. با این روش وارد تمامی حافظه‌های جانبی شده و با تزریق خود به اینترنت اکسپلورر از فایروال سامانه عبور می‌کند. این بدافزار به محض ورود به سامانه قربانی شروع به جمع آوری اطلاعات مربوط به کارگزارهای موجود در شبکه و نحوه پیکربندی آنها کرده و در نهایت تلاش می‌کند از طریق ارتباط راه دور به سایت‌هایی متصل شود که آدرس IP آن ها مکرراً در حال تغییر هستند. در نهایت، این تروجان با استفاده از آسیب پذیری ویندوز، یک در پشتی در سامانه ایجاد کرده و بدین طریق به مهاجم اجازه می‌دهد به صورت راه دور، کنترل سامانه را به دست گیرد.(بی‌نا، ۱۳۹۲، ص۲)

۵- ویروس Flame یک برنامه‌ی بسیار پیچیده و خرابکارانه است‌که در حال حاضر به‌صورت فعال و بعنوان یک سلاح سایبری برای هدف‌گذاری مراکز خاصی در کشورهای مختلف استفاده می‌شود.

بر اساس درخواست واحد مخابراتی بین المللی(ITU) از آزمایشگاه کسپرسکی برای بررسی این آلودگی ناشناخته، متخصصان کسپرسکی کشف کردند که این ویروس برای ارسال اطلاعات و جاسوسی سایبری ساخته شده است. این ویروس می تواند اطلاعات با ارزش را سرقت کند. این ویروس تنها اطلاعات مربوط به سیستم را سرقت نمی‌کند بلکه اطلاعات کامل در مورد سیستم های هدف گذاری شده، اطلاعات نمایش داده شده بر روی صفحات نمایش داده شده‌ی کامپیوتر و صدای محیط. پیچیدگی و عملکرد Flame بسیار متفاوت و پیچیده تر از هرگونه سلاح سایبری تا کنون است.

Flame پیچیده ترین و مخرب ترین سلاح سایبری تاکنون می‌باشد. این ویروس به‌صورتی طراحی شده است‌که تقریبا ردگیری آن غیر ممکن باشد. هر چند که بدافزار ها معمولا به گونه‌ای طراحی می‌شوند که کوچک و قابل مخفی شدن باشند، سایز ویروس Flame تا به‌حال ناشناخته باقی مانده است. Flame از تکنیک‌های بسیار پیچیده ای برای انتشار آلودگی در شبکه‌های کامپیوتری استفاده می‌کند که در گذشته تنها در یک سلاح سایبری از آن استفاده شده بود: استاکس نت. اگرچه به نظر میرسد ویروسFlame از مارس ۲۰۱۰ شروع به فعالیت کرده، اما هیچ نرم افزار امنیتی این مسئله را کشف نکرده است...تا اینکه آزمایشگاه کسپرسکی موفق به شناخت آن شد.(اخبار و مقالات امنیت اطلاعات، کاسپرسکی، ۱۳۹۱)

۶- ویروس استارس (به انگلیسی: Stars) یک ویروس رایانه‌ای است‌که در آوریل ۲۰۱۱ در ایران شناسایی شد. این ویروس که از خانواده استاکس‌نت دانسته می‌شود، خود را در میان پرونده‌های پی‌دی‌اف مخفی می‌کند(دانشنامه آزاد).

۷- تعریف مشخصی از این ویروس در منابع علمی و تخصصی انفورماتیک نیافتم.

۸- Cyber Alibi .

۹- Information Technology.

۱۰- منظور از مستند به قانون بودن دادرسی کیفری، اصل قانونی بودن رسیدگی و مستند به قانون بودن احکام دادگاه و سایر مراحل رسیدگی کیفری است(قانون‌یار، ۱۳۹۴، ص۷)

۱۱- دادرسی عادلانه و منصفانه عبارت است از این‌که، دعوای مطروحه میان طرفین دعوا در یک دادگاه صالح و مستقل و بی‌طرف، که مطابق با قانون تشکیل گردیده و در یک فضای آرام و شرایطی برابر توسط قضات متخصص و دانا به‌صورت علنی و با رعایت کلیه تضمینات شکلی و ماهوی مربوط به حقوق اصحاب دعوا مورد رسیدگی قرار گیرد(دیبا نژاد و شایسته، ۱۳۹۴ص۱۵)