امکان سنجی قتل از طریق فضای مجازی

چکیده:

قتل از طریق فضای مجازی، واقعیتی فنی–حقوقی است که شناخت آن و پی بردن به جایگاهش در نظام حقوقی داخلی و بین‌المللی، نیازمند انجام مطالعات میان رشته‌ای است. ولی از نگاه حقوقی، قتل از طریق فضای مجازی، به مجموعه اعمال مجرمانه‌ای گفته می‌شود که از جهت رکن روانی، هم‌چون قتل سنتی با انگیزه‌های شخصی مانند انتقام جویی یا انگیزه‌های مالی رخ می‌دهند و از لحاظ رکن مادی، تابع سه معیار متفاوت‌است. نخست، معیار هدف جرم و آن ناظر به اقداماتی است که علیه سامانه‌ها و زیرساخت‌های فضای مجازی صورت گرفته و از طریق ایجاد اختلال در آن‌ها منجر به قتل می‌گردد. دوم، با معیار وسیله ارتکاب جرم که طبق آن فضای مجازی هم‌چون وسیله ارتکاب جرم در اختیار مرتکب قرار می‌گیرد. سوم، معیار آثار بیرونی است که طبق آن قتل از طریق فضای مجازی به اقداماتی گفته می‌شود که در فضای بیرون منجر به قتل افراد می‌شود. علاوه بر بررسی ماهوی قتل از طریق فضای مجازی، اتخاذ تدابیری به‌منظور مقابله و پیشگیری از آن ضروری است که این امر نیازمند ابهام زدایی از قوانین و هم‌چنین اتخاذ تدابیر شکلی افتراقی است و از آن‌جا که اصلاح قوانین و اختصاص آئین دادرسی افتراقی به پدیده‌ای مجرمانه فرع بر وجود و فراگیر شدن آن در جامعه است،ابتدا باید نسبت به آن امکان سنجی صورت گرفته و واقعیت آن در جامعه حقوقی اثبات شود که دراین راستا مراجعه به اخبار و نظرات متخصصین در این عرصه و قوانین موجود علی‌رغم پراکندگی آن‌ها مؤثر خواهدبود.

واژگان کلیدی: قتل، فضای مجازی، جرم رایانه‌ای،تروریسم سایبری

مقدمه

حفظ جان و بقای حیات تمایلی مشترک میان حیوانات و انسان است و تلاش‌های روزمره موجودات نیز درهمین راستا می‌باشد. جوامع انسانی نیز باتوجه به تقسیم نقشی که میان اعضای آن‌ها وجود دارد همواره بر حفظ نظم و تمامیت اعضای خود کوشش نموده‌اند و همین مسأله از گذشته تاکنون زمینه ساز رشد و توسعه جوامع و تبدیل شدن آنان به شکل کنونی گردیده است.

مهم‌ترین چالشی که زندگی جمعی انسان‌هارا تهدید می‌نماید، درگیری‌ها و اقداماتی است که منجر به مرگ برخی افراد جامعه می‌شود و ازهمین رو، از گذشته تا کنون با مرتکبین این جرائم برخوردی شدید و بدون چشم پوشی صورت گرفته‌است. اهمیت جرم قتل به‌قدری زیاد است که در جوامع قدیمی اولین قانون‌گذاری‌ها در خصوص این جرم انجام گردیده و اکنون با گذشت هزاران سال هم‌چنان این جرم موضوع بحث محافل حقوقی و علمی است.[1]

درجهان کنونی و با رشد چشم‌گیر تکنولوژی و فضای مجازی در آن، گزارش‌ها و اخبار بسیاری درباره امکان وقوع قتل از طریق فضای مجازی به‌دست آمده است[2] و اگرچه پذیرش این‌که فضای مجازی با شکل و شمایل غیر واقعی خود بتواند در کشتن افراد کاربرد داشته باشد امری است مشکل، اما اهمیت جرم قتل باتوجه به‌موضوع آن، یعنی جان انسان به‌عنوان هسته تشکیل دهنده اجتماع، به‌گونه‌ای است که نباید نسبت به آن سهل انگاری صورت بگیرد مخصوصا اگر گزارش و هشداری نیز در این زمینه به دست رسیده باشد. بنابراین، قتل از طریق فضای مجازی هرچند ظاهری توأم با احتمالات و خیال داشته باشد، اما باتوجه به اهمیت بسیار زیادی که تأمین امنیت افراد جامعه دارد

---

[1]. برای مثال نگاه کنید به مواد ۱۹۶ به بعد مجمع القوانین حمورابی که در آن تعرض به جان شهروندان جرم بوده و با قصاص فرد خاطی مجازات می‌شد.

[2]. شرکت Animas، سازنده تجهیزات پزشکی به مشتریان پمپ انسولین ساخت این شرکت با نام OneTouch Ping در خصوص وجود ضعفی امنیتی که مهاجم را قادر به تغییر در مقدار انسولین تزریق شده به بیمار می کند هشدار داده است. به‌گزارش شرکت مهندسی شبکه گستر به‌نقل از سایت Computer World، این آسیب پذیری توسط یکی از محققان شرکت Rapid7 که خود یک بیمار دیابتی و از استفاده کنندگان این پمپ است شناسایی شده‌است. این ضعف امنیتی در نتیجه عدم رمزنگاری ارتباطات بی‌سیم بین پمپ انسولین و کنترل کننده قند خونی است که از راه دور مقدار انسولین تزریقی را تعیین می‌کند. فرد مهاجم می‌تواند ترافیک ارتباطی را رصد نموده و نتایج قند خون و مقدار انسولین را که بصورت متن ساده ردوبدل می‌شوند شنود کند. علاوه براین، مهاجم قادر است از سمت کنترل کننده، داده نادرستی را به پمپ ارسال کند. برای مثال، با اعلام قند بالا به پمپ فرد مهاجم می‌تواند سبب تزریق مقدار فراوانی انسولین به بیمار شود بنحوی که سبب افت شدید قند خون و بروز حالت شوک انسولین و درنهایت مرگ وی شود.

باید توسط جوامع حقوقی و اندیشمندان مورد بررسی قرار گیرد تا مشخص شود کـه چنـین جرمـی ازلحاظ حقوقی چه‌وضعیتی داشته و چگونه جایگاهی دارد.

بررسی حقوقی قتل از طریق فضای مجازی باتوجه به ابهاماتی کـه دربـاره آن مطـرح مـی‌شـود، متمایز از سایر پدیده‌های مجرمانه است. در سایر جرائم باتوجه به محقـق شـدن آن‌هـا در جامعـه و ضرورتی که از حیث مقابله با مرتکبان و پیشگیری از تکرار آن‌ها وجود دارد، مباحث حقوقی فراوانی پیرامون آن‌ها شکل گرفته‌است و در مباحثات جدید هدف ارائه نظریات دقیق‌تر و کاربردی‌تر اسـت. اما در جرم مذکور قبل از ورود به جنبه‌های حقوقی و کیفری بحث، باتوجه به ابهاماتی که راجـع بـه اصل وجود و قابلیت تحقق آن از طریق فضای مجازی مطرح است ضروری است در ابتدا بستر ایـن جرم یعنی فضای مجازی، از لحاظ قابلیت تحقق یا عدم قابلیت در وقوع چنین جرمی بررسی گردد.

اگرچه پژوهشگران در خلال مباحث حقوقی به جرائمی کـه از طریـق فضـای مجـازی ارتکـاب می‌یابد پرداخته‌اند لکن به موضوع مذکور یعنی قابلیت یا عدم قابلیـت ارتکـاب جـرم قتـل ازطریـق فضای مجازی و همچنین چگونگی ارتکاب و نحوه استفاده از این بستر در ارتکاب جـرم موصـوف پرداخته نشده است[۳] و همین مساله موجب اختلاف نظر میان حقوقدانان گردیـده اسـت. در نوشـتار پیش رو به فضای مجازی از دوجنبه نگریسته خواهدشد. نخست، باتوجه به ساختار فضای سـایبر و امکانات و خصوصیات آن که می‌تواند بستری برای ارتکاب جرم قتل باشد پرداخته خواهدشـد و در ادامه با مراجعه به دیدگاه کارشناسان و متخصصین عرصه سایبر و همچنین توجه به قوانین و مقرراتی که در برخی کشورها درخصوص ارتکاب این جرم تدوین گردیده است به بررسی قابلیـت یـا عـدم قابلیت فضای مجازی در رخ دادن بزه مذکور پرداخته خواهدشد که بدین منظور بهتراست میان ابعاد مختلف موضوع تفکیک به عمل آمده و ابتدا به بررسی درون ساختاری[٤] ومتعاقب آن به بررسی برون ساختاری[٥] پرداخته‌شود.

---

[۳]. علی اکبر ایزدی فرد، سید مجتبی حسین نژاد، «بررسی فقهی قتل ازطریق فضای مجازی»، مجله مطالعات فقه و حقوق اسلامی، ١٤، ١٣٩٥.

[٤]. قابلیت داشتن یا نداشتن ویژگی ها و ساختار فضای مجازی به عنوان بستر قتل

[٥]. بررسی اخبار،نظریه ها و کنفرانس های مربوط به قتل از طریق فضای مجازی

۱-امکان سنجی قتل ازطریق فضای مجازی با رویکرد فنی

فضای مجازی حاصل تعامل داده‌ها و اطلاعات بارگذاری شده افراد و سامانه‌ها و شبکه‌هایی است که با ترکیب نمودن اطلاعات به صورت کدگذاری شده به گسترش ارتباطات و دسترسی کاربران می پردازند[۶] و همین خصوصیات فضای مجازی است که آن را به سوژه‌ای جذاب برای بزه‌کاران تبدیل می‌نماید. هنگامی که از بررسی درون ساختاری سخن به میان می‌آید منظور واکاوی ویژگی‌ها و عناصر متشکله این مجموعه است به‌گونه‌ای که مبین خصوصیات و شرایط بارز آن باشد و در درک اینکه چگونه ممکن است فضای مجازی بستر ارتکاب جرم باشدکمک کند و در مقابل، منظور از بررسی برون ساختاری تحلیل فرضیه‌ها، تحقیقات به عمل آمده، اخبار و اقداماتی است که در ارتباط با قتل از طریق فضای مجازی بوده و حاوی مطالبی در نفی و اثبات آن باشد.

چنانچه از درون به محیط سایبر نگریسته شود معلوم می‌شود که محیط سایبر و ارتباطات در فضای مجازی بدون رایانه و سیستمی که به واسطه آن بتوان به این عرصه وارد شد امری غیرممکن است؛ از آن جا که بحث مورد نظر درمقام بررسی امکان یا عدم امکان وقوع قتل از طریق فضای مجازی است بنابر قاعده عقلی که بیان می‌کند ضرورت یک امر ضرورت مقدمه آن را می‌طلبد،[۷] ابتدا باید بررسی شود که رایانه به عنوان دریچه ورود به فضای مجازی چه ویژگی‌ها و کارکردهایی دارد و به دنبال آن استفاده از فضای مجازی چه آثار و تبعاتی دارد که می تواند آن را به بستری مناسب جهت ارتکاب قتل بدل نماید.

اصطلاح سیستم رایانه‌ای ترکیب دو واژه سیستم و رایانه است که اگرچه این دو غالبا باهم به کار برده می‌شوند اما هریک معنای مخصوص به خود را دارد؛ سیستم بسته به اینکه در چه شاخه و رشته‌ای به کار رود معناهای متفاوتی دارد ولی در ارتباط با جهان اطلاعات و داده‌ها به‌عنوان مجموعه‌ای از عناصر شناخته می‌شود که برای دست یابی به هدفی واحد به صورت هماهنگ کار می‌کنند. یک سیتم رایانه‌ای متشکل از دو بخش کلی سخت افزار و نرم افزار است و منظور از سخت افزار، قطعات، ریز پردازنده‌ها و سایر ادواتی هستند که کنارهم قرار گرفتن آن‌ها منجر به عملیات

---

[۶]. منصوره فروزان، آشنایی با رایانه(تهران:کتاب همراه،۱۳۸۳)،۳۷

[۷]. روح الله موسوی خمینی،؛مناهج الوصول الی علم الاصول(قم: موسسه تنظیم و نشر آثار امام خمینی،۱٤۱٥ه.ق)،۷٦

دریافت، پردازش و ارائه داده‌ها می‌گردد و منظور از نرم افزار نیز سیستم عامل و دستورالعمل کدنویسی شده‌ای است که نحوه تعامل اجزا را در راستای ایفای وظایف مشخص می‌کند.[۸] به طور خلاصه می‌توان هروسیله‌ای که داده‌ها و اطلاعات ورودی را به منظور دست یافتن به هدف و منظور خاصی تجزیه و تحلیل می‌کند رایانه نام نهاد[۹] و چنانچه از واژه سیستم رایانه‌ای استفاده شود یعنی هردو بخش سخت افزار و نرم افزار مورد اشاره قرار گرفته است.

همانطور که بیان شد، سیستم رایانه‌ای به عنوان دریچه ورود و پل ارتباط با فضای مجازی به کار می‌رود و خود فضای مجازی نیز همانگونه که از نام آن پیداست برپایه اموری غیر عینی و مجازی همچون داده‌ها و اطلاعات استوار شده است. بنابراین، بررسی استفاده‌ها وکارکردهای فضای مجازی و خطرات و تهدیدهای آن را می‌توان تحت دوعنوان کلی محوریت داده‌ها و اطلاعات به عنوان ویژگی فنی و محوریت هک و کرک به عنوان ویژگی امنیتی تفکیک نمود و سپس به بررسی هریک پرداخت.

۱-۱-محوریت داده و اطلاعات

از میان تکنولوژی‌ها و فن‌آوری‌های نوین ارائه شده توسط بشر، شبکه ی جهانی اینترنت یا به بیان دیگر فضای سایبری و خدمات مربوط به آن با رونق و استقبالی بی‌نظیر از طرف جهانیان مواجه گردیده است؛ دلیل این امر چیست؟ محیط آنلاین دارای چه ویژگی است که اینگونه انسان‌هارا به خود مشتاق و وابسته نموده است؟ در انواع و اقسام فعالیت‌ها از این بستر استفاده می‌شود به طوری که شاید اگر صدسال پیش به جهانیان گفته می‌شد که درآینده روزی خواهد آمد که ازطریق فضای مجازی قادر به تهیه غذا و سایر امور زندگی خود خواهند بود کسی آن را نمی‌پذیرفت اما امروزه استفاده از فضای مجازی به جنبه خاصی از زندگی انسان ها منحصر نیست و به جرأت می‌توان گفت زندگی انسان درهمه ابعاد آن با فضای مجازی عجین و حتی درمواردی به آن وابسته نیز شده است.

فضای مجازی دنیایی است سرشار از اطلاعات و داده‌ها و هرآن‌چه انسان با اقدامات خود به این

---

[۸].فرهاد قلی زاده نوری، مترجم، فرهنگ تشریحی اصطلاحات کامپیوتری مایکروسافت(تهران: هیأت مؤلفان و ویراستاران انتشارات مایکروسافت،۱۳۸۱)، ۷۱۷

[۹]. قانون تجارت الکترونیکی مصوب۱۳۸۲،ماده۲ بند"و"

عرصه وارد می‌کند یا از آن خارج می‌نماید نه بـه شـکل ملمـوس و عینـی بلکـه بصـورت داده‌هـای رمزگذاری شده می‌باشند؛ همین ویژگی فضای مجازی به سرعت و سهولت جابه‌جایی‌ها دراین محیط منجر گردیده و از طرف دیگر از طریق اتصالات مجازی که همچون یک شبکه فوق گسترده سرتاسر مناطق را پوشش می‌دهد به انسان ها کمک نموده تا بسیاری از امور را بدون استفاده از نیروی انسانی و با کمک سامانه ها و نرم افزارها به انجام برسانند. به طور مثال، درحـال حاضـر بسـیاری از مراکـز تجاری به‌جای استخدام حسابدار مالی و صرف هزینه‌های فراوان از برنامه های حسـابداری اسـتفاده می‌کنند، در مراکز پزشکی نیاز نیست تا نیروی انسانی به تزریق داروها و کنترل نمودن علائم حیـاتی بیمار بپردازد و از پمپ‌های تزریق دارو مانند پمـپ تزریـق انسـولین، پمـپ تزریـق خـون بیمـاران تالاسمی و پمپ‌های قابل کاشت دربدن[10] استفاده می‌شود. همچنین در حمل و نقل دریایی، هوایی و زمینی نیز از سامانه‌های هوشمند، همچون سیستم خودکار هدایت کشـتی، خلبـان خودکـار و رانـنـده اتومبیل خودکار[11] بهره برداری می‌شود. علاوه براین‌ها، به نمونه بارز اسـتفاده از فضـای مجـازی کـه استفاده از شبکه‌های اجتماعی است می‌توان اشاره کرد که برقراری ارتباط و دریافت و ارسال پیام را از گوشه و کنار جهان برای انسان فراهم نموده است و همه این‌ها به دلیل برتری و مزیت‌هایی است که استفاده از سامانه‌های رایانه‌ای و هوشمند نسبت به انجام امور توسط نیروی انسانی دارند. فارغ از این، انجام پاره‌ای امور به‌گونه‌ای است که یا دقت و ظرافت زیادی را می‌طلبد و یا از توان انسان که همواره درمعرض خطا و غفلت قراردارد فراتر است. بنابراین، جایگزینی نیروی انسانی بـا آن‌هـا بـه حکم عقل امری پسندیده است. مزیت‌ها و فواید فضای مجازی که سبب استقبال و گرایش انسان به استفاده از آن گردیده محدود به موارد مصرحه فوق نبوده و مـوارد مـذکور تنهـا بخـش کـوچکی از امتیازات استفاده از فضای مجازی در سازوکارهای زندگی بشر است. اما نکتـه‌ای کـه حـائز اهمیـت است آن است که آیا می‌توان تصور نمود فضای مجازی که بنیانش بر نقل و انتقال اطلاعات اسـتوار گردیده و تمام آثار و کارکردهای آن ناشی از نقل و انتقال همین داده‌ها است تحت شرایطی به‌صورت مستقیم منجر به مرگ افراد شود؟

---

[10].PCA pump, Infiosion pump, implant pump

[11].Auto pilot, Auto driving system, Auto sailor

در پاسخ به پرسش فوق باید به این نکته اشاره کرد که فرق میان قتل به شیوه سنتی و مرسوم با انواع سلاح سرد و گرم با قتل از طریق فضای مجازی در چیست؟ در قتل سنتی، مجرم با بکارگیری اعضای بدن و ابزار و وسایل جرم، بصورت فیزیکی و ملموس اقداماتی را انجام می‌دهد که منجر به مرگ افراد می‌شود و همین سلسله عوامل در قتل از طریق فضای مجازی هم به شکلی دیگر به‌وقوع می‌پیوندد. بدین صورت که یک فرد آشنا به محیط سایبر با ورود و تداخل در سازوکارهای آن در اطلاعاتی که درحال تبادل اند تغییراتی ایجاد نموده و منجر به مرگ بزه دیده می‌شود. اگر مرتکب قتل سنتی طی فرمانی که از مغز صادر می‌شود با به حرکت درآوردن دست و اعضای بدن از طریق ریختن سم در غذای دیگری مرتکب جرم می‌شود؛ در قتل از طریق فضای مجازی نیز اعمال تغییر در اطلاعات و داده‌ها به مثابه فرمان مغز و نتیجه نهایی مانند تزریق دوز بیشتری از دارویی مانند انسولین[۱۲] به مثابه ریختن سم بوده و منجر به مرگ بیمار می‌گردد. بنابراین، فضای مجازی و ماهیت مبتنی بر داده و اطلاعات آن نمی‌تواند مانعی در تصور ارتکاب قتل از طریق مزبور باشد و از لحاظ فنی و ساختاری می‌توان چنین واقعه‌ای را تصور نمود.

۱-۲-منبع باز[۱۳] بودن اطلاعات فضای مجازی

در بررسی خصوصیات فنی و ساختاری فضای مجازی که می‌تواند زمینه ساز روی آوردن مجرمین به ارتکاب قتل از این طریق باشد، یک ویژگی دیگر از محیط سایبری خودنمایی می‌کند و آن دسترسی و امکان اعمال تغییرات توسط سایر افراد در اطلاعات و سازوکارهای فضای مجازی

---

[۱۲]. پمپ انسولین تقریبا به اندازه یک تلفن هوشمند و یا کارت اعتباری است که در بیرون بدن قرار می‌گیرد و انسولین داخل مخزن آن از طریق یک لوله باریک (catheter) و با یک سوزن نازک (cannula) متصل به لایه چربی زیر پوست، تزریق می‌شود. در پمپ انسولین، میزان انسولین پایه معمولاً توسط پزشک تعیین می‌شود و این قابلیت وجود دارد که در پمپ چندین برنامه برای تزریق میزان انسولین پایه تنظیم شود، درنتیجه بسته به زمان‌های مختلف شبانه روز که میزان حساسیت بدن به انسولین، مصرف غذا و فعالیت بدنی متفاوت است، می‌توان با کمک پمپ مقادیر مختلفی از انسولین را تزریق نمود. بعضی از پمپ‌ها این قابلیت را دارند که در صورت کاهش قند، بدون اینکه به بیمار اعلام نمایند، خودبه‌خود تزریق انسولین پایه را به طور موقت قطع نمایند و با افزایش مجدد قند خون، تزریق انسولین پایه را دوباره شروع کنند. این قابلیت به ویژه برای والدین کودکان کوچک‌تر که خطر افت قند خون هنگام خواب در آنها بیشتر است، بسیار کاربرد دارد. همچنین پزشک معالج می‌تواند به کمک نرم افزار کامپیوتری داده‌های حاصل از پمپ را به صورت جدول و نمودار مشاهده نماید و تغییرات لازم را در میزان انسولین مصرفی برای بیمار اعمال نماید.

[13]. Open Source

است.

به‌طور کلی اطلاعات و نرم افزارهای قابل اجرا بر روی ابزار گوناگون مانند موبایل و سیستم‌های رایانه‌ای به صورت کد بسته ارائه میشوند. یعنی بجز فرد سازنده اطلاعات شخص دیگری به آن‌ها دسترسی نداشته و امکان اعمال تغییر در کدهای برنامه برای وی وجود ندارد. در مقابل یکسری نرم افزارها و اطلاعات بصورت اوپن سورس یا منبع باز و با امکان دسترسی همگان به کدهای برنامه ارائه میشوند و این امکان را به برنامه نویسان میدهند تا با تغییرات خاص نرم افزار را تغییر داده و امکانات دلخواه را به نرم افزار اضافه کنند، نرم افزار را به صورت دلخواه توسعه دهند و استفاده از آن را شخصی سازی نمایند.[۱۴] بسیاری از سامانه‌ها و نرم افزارهایی که در بخش‌های مختلف جامعه اعم از پزشکی، حمل و نقل و... استفاده می‌شوند باهدف دسترسی آسان کاربران و سهولت در استفاده بصورت کدباز ارائه می‌گردند و همین مسأله می‌تواند خطرساز شده و زمینه ساز ارتکاب جرائمی علیه بیماران و مصرف کنندگان خدمات و سامانه‌های متصل به اینترنت باشد. تا جایی که سازمان غذا و داروی آمریکا (FDA)[۱۵] به این مسئله مهم پرداخته است و در سال ۲۰۱۳ ارزیابی امنیت سایبری دستگاه پزشکی و به روزرسانی آن را به‌عنوان یک معیار برای تایید محصول اعلام کرده است. همچنین در سال ۲۰۱٤ موسسه ملی فناوری و استانداردهای آمریکا (NIST)[۱۶] چارچوبی برای بهبود امنیت سایبری زیرساختارهای اساسی مورد استفاده در حمل و نقل و... وضع کرد.[۱۷]

۲- امکان سنجی قتل از طریق فضای مجازی با رویکرد امنیتی

اگرچه در فواید بهره برداری از فضای مجازی جای هیچ شک وشبهه‌ای باقی نمی‌ماند، ولی درعین‌حال استفاده از فضای مجازی آکنده به تهدیدات وخطرات فراوان است و همانگونه که افراد عادی در انجام امور روزانه خود ازآن سود می‌برند به‌همان میزان بزهکاران نیز مشتاق به‌این عرصه‌اند و روزبه‌روز بر دامنه جرائم سایبری افزوده می‌گردد، زیرا همان طور که افراد جامعه به دلیل سهولت

---

[۱۴]. مسعود شفیعی، نرم افزار منبع باز و آزاد(تهران: پیام رسان،۱۳۸۵)، ۳۸

[15] . Food and Drug Administration

[16] . National Institute of Standards and Technology

[17] . Andrew, Ashowrth. Principles of Criminal Law, Chicago University, [5th ed.2006] p365.

انجام امور یا عدم نیاز به مداخله نیروی انسانی از امکانات و خدمات فضای مجازی بهره‌می‌برند. بزهکاران نیز می‌توانند با خیالی آسوده اقدامات مجرمانه را تنها با استفاده از داده‌های کدگذاری شده و سازمان یافته[۱۸] بدون آن که درحال ارتکاب جرم مشاهده یا دستگیر شوند انجام دهند. بنابراین، اگرچه در نگاه اول ارتکاب قتل از طریق فضای مجازی به‌عنوان فعلی مادی که موضوع آن نیز تمامیت جسمانی بزه دیده است امری ناممکن به‌نظر می‌رسد اما باتوجه به کاربردهایی که فضای مجازی برای مجرمان می‌تواند داشته باشد از یک طرف و ضعف‌های امنیتی آن از طرف دیگر، می‌توان آن را ابزار و وسیله‌ای مناسب برای ارتکاب جرم دانست. امروزه و باتوجه به شیوع استفاده از سامانه‌های رایانه‌ای در بخش‌های گسترده و گاها حیاتی، تهدید سایبری در مواردی ممکن است به منزله‌ی تهدید امنیت ملی باشد و از همین رو کارشناسان مسائل امنیتی علی‌رغم نیاز جامعه به گسترش استفاده از فضای مجازی و همگام شدن با پیشرفت‌های جهانی از وجود رایانه‌ها در هراسند. به زعم آن‌ها رایانه‌ای کردن امور بیش از آن‌که افزایش دهنده رفاه و امنیت ملی باشد به آسیب پذیری بیشتر جامعه منجر می‌شود. بنا به‌ادعای یکی از متخصصان امنیتی رایانه‌ها در همه امور زندگی‌ما، از شبکه‌های برق رسانی گرفته تا سیستم‌های توزیع مواد غذایی، دفاع ملی و تقریبا تمامی جنبه‌های اساسی نقش مهمی ایفا می‌کنند و کسی که با طرز کار این مجموعه آشنایی داشته باشد قادر است که آسیب‌های جدی به جامعه وارد کند و حتی کل اقتصاد مملکت را دچار بحران نماید. بنابراین، به منظور مقابله و پیشگیری باید سازوکارهای امنیتی دقیق درنظر گرفته شود و برای مقابله با خطرات احتمالی آماده بود.[۱۹]

۲-۱- ضعف امنیت فضای مجازی باتوجه به قابلیت هک و کرک

هنگامی که از فضای مجازی و امکانات و اطلاعات موجود درآن سخن گفته می‌شود بدیهی است که استفاده از این امکانات به‌صورت صحیح و مسالمت آمیز نمی‌تواند خطرساز و پایه ریز جرایم

---

[۱۸]. ادوارد والتس، عملیات و اصول جنگ اطلاعات، ترجمه معاونت پژوهش و تولید علم (تهران: موسسه آموزشی و تحقیقاتی صنایع دفاعی،۱۳۸٦)،٤.

[۱۹]. کریس هیبلزگری، جنگ پست مدرن سیاست نوین کیفری،ترجمه احمدرضاتقاء (تهران: معاونت تحقیق و پژوهش دانشکده فرماندهی و ستاد سپاه پاسداران، ۱۳۸۱)،٦٧.

سایبری همچون قتل از طریق فضای مجازی باشد؛ بلکه ایـن دسترسـی غیـر مجـاز بـه اطلاعـات و داده‌های فضای مجازی است که می‌تواند آن را به محیطی خطرساز و ناامن بدل نماید. هک و کرک[۲۰] به معنای نفوذ غیرمجاز به سیستم رایانه‌ای و داده‌های فضای مجازی دو عمل فنی رایج در این عرصه هستند که مقدمه ارتکاب جرائم سایبری به‌شمار می‌روند. درواقع اگر امروزه ازجرایم مجازی از جمله قتل از طریق فضای مجازی سخن به میان می‌آید براساس اعتقاد به همین دو عمل مذکور است.

هک، استفاده خلاقانه از یک سیستم است به گونه‌ای که کاربر(هکر) با اعمال تغییرات در سازوکار آن بتواند نحوه کار و پردازش اطلاعات آن سیستم را تغییر دهد و به طور خلاصـه بتوانـد بـه درون سیستم نفوذ کند.[۲۱] آن چه فضای مجازی را خطرناک می‌کند همین قابلیت نفـوذ بـه فضـای مجـازی باتوجه به ضعف امنیتی آن بوده که به‌دنبال آن رخنه اطلاعاتی، دست یابی به اطلاعات رمـز گـذاری شده، اعمال تغییرات در آن‌ها و به اصطلاح کرک[۲۲] نمودن آن‌ها حاصل می‌شود که توجه به این نقاط ضعف امنیتی، باعث می‌شود برای فضای مجازی قابلیت ایجـاد خطـر و تناسـب آن بـه‌عنـوان بسـتر ارتکاب جرم را قائل شد.

هنگامی که بشر فضای مجازی را به دلیل امتیازات و امکاناتی که در اختیارش قرار می‌دهد پذیرفته و به زندگی خویش وارد می‌کند، طبیعی است که باید برای حفظ امنیت این پدیده و مصون ماندن آن از تعرضات افراد شرور تدبیری بیاندیشد؛ اینکه جوامع بخش‌های بسیاری از امور و اطلاعات فراوانی را در بستر فضای مجازی قرار دهند اگرچه تسهیل امور را به دنبال دارد اما به همان میـزان انسـان را درمقابل خطرات آسیب پذیر می‌کند و این عقلانی به نظـر نمـی‌رسـد. بنـابراین، اسـتفاده از فضـای مجازی همواره این چالش را فراروی انسان قرار می‌دهد کـه آیـا دل سـپردن بـه ایـن تکنولـوژی و مشارکت دادن آن در جنبه های بیشتر زندگی از امنیت کافی برخوردارد اسـت؟ پاسـخ منفـی اسـت؛ تجربه و بررسی‌های محققان ثابت نموده که فضای مجازی از همان بدو پیدایش کـه شـکل سـاده و ابتدایی داشت تا به امروز که بسیار پیشرفته شده است در معرض نفوذ و دسترسی هکرها بوده اسـت

---

[20].Hack and Crack

[۲۱]. قلی زاده نوری، مترجم، فرهنگ تشریحی اصطلاحات کامپیوتری مایکروسافت،۳٤٥.

[۲۲].همان، ۱۸٦.

و ماهیت مبتنی بر اطلاعات فضای مجازی به گونه‌ای است که اطلاعات کاربران آن در معرض حمله‌های سایبری و هک قرار دارند و جالب این است که باتوجه به متنوع بودن فعالیت‌ها و اطلاعات فضای مجازی هکرها نیز به فراخور موضوع و هدفی که از حمله سایبری مدنظر دارند روش‌های گوناگونی را مورد استفاده قرار می‌دهند و با بررسی حمله‌های سایبری رخ داده تاکنون به این نتیجه می‌رسیم که فضای مجازی علی رغم همه مزایایی که دارد از لحاظ ایمنی محیطی ناامن و پرخطر است.

روش‌های عمده‌ای که هکرها از آن‌ها در تهاجم‌های سایبری خود استفاده می‌کنند عمدتا تحت عنوان یکی از دسته‌های ذیل قرار می‌گیرد:

۲-۱-۱- حمله جستجوی فراگیر[۲۳]

این روش قدیمی ترین روش هک است، درفضای مجازی به‌این علت که محتوای آن اطلاعات و داده‌ها هستند و شکل خارجی ندارند محافظت خارجی معنایی ندارد و معمولا از رمزگذاری داده‌ها و شبکه‌ها استفاده می‌شود؛ دراین روش، فرد هکر ترکیب‌های مختلف اعداد و حروفی که ممکن است رمز ورود باشند را نه به صورت دستی که فوق العاده زمان‌بر است بلکه از طریق برنامه نویسی انجام می‌دهد و با صرف زمانی اندک به شبکه و داده‌های حفاظت شده دسترسی پیدا می‌کند[۲۴]. به طور مثال، در یک بیمارستان استفاده از دستگاه‌های کنترل علائم حیاتی به متخصصان تعلق دارد و برای جلوگیری از دخالت سایرین برای آن‌ها رمز ورود درنظر گرفته می‌شود اما با استفاده از این روش امنیت دستگاه‌ها و بیماران تحت کنترل با خطر مواجه است.

۲-۱-۲- واسطه گذاری[۲۵]

در این روش هکر با جای گذاری یک برنامه در سیستم و شبکه مورد نظر که همچون یک واسطه عمل می‌کند از تمام اقدامات،اخبار،اطلاعات و هرآن‌چه در سیستم فرد سوژه می‌گذرد مطلع می‌شود و

---

[23]. Brute Forse

[۲۴]. واژه نامه و فرهنگ امنیت فضای تولید و تبادل اطلاعات (تهران: مؤسسه انتشارات علمی دانشگاه صنعتی شریف،۱۳۹٤)، ۲۱۳.

[25].MAN in The Middle (M.I.T.M.)

علاوه بردست یابی به اطلاعات امکان اعمال تغییر درآن هارا نیز دارد[۲۶]. به‌طور مثال هنگامی که فردی از طریق پست الکترونیکی نسخه درمان پزشکی خودرا دریافت می‌کند برنامه مورد نظر یک نسخه از آن را برای فرد هکر ارسال می‌کند و از وضعیت بیمار، داروهایی که باید استفاده کند و شرایط جسمی و روحی او مطلع می‌شود و این می تواند بسیار خطرناک باشد. زیرا با اعمال تغییر در نسخه بیمار می‌تواند وی را به سمت مصرف داروهایی که منجر به مرگ او می‌گردد سوق دهد یا با اطلاع از وضعیت روحی وخیم سوژه می‌تواند با ارسال پیامی وحشتناک موجبات حمله قلبی بیمار و مرگ او را فراهم آورد.

Comment [گل محمدی۱]: این قسمت حذف شود.

۲-۲-ضعف امنیت فضای مجازی باتوجه به قابلیت ربایش اطلاعات

ضعف‌های امنیتی فضای مجازی فقط به حمله‌های سایبری و در دست گرفتن کنترل سامانه‌ها و ارتباطات(هک و کرک) محدود نبوده، بلکه اطلاعات و داده‌ها در فضای مجازی فارغ از اینکه منبع باز یا بسته باشند قابل شنود و سرقت اند. فرد مجرم می‌تواند با نفوذ به یک شبکه سایبری اطلاعات در گردش آن را برباید و با سوء استفاده از آن‌ها یا ایجاد تغییر و تحریف در آن‌ها به اهداف مجرمانه خود دست یازد که این مسأله خود ناشی از ضعیف بودن ایمنی سامانه‌ها و سیستم‌های رایانه‌ای است وهمین نقاط ضعف امنیتی فضای سایبر است که موجب روی آوردن مجرمان به استفاده از آن‌ها در ارتکاب بزه گردیده.

۲-۲-۱- جاسوسی اطلاعات[۲۷]

شاید آن‌چه در افکار عمومی مترادف هک قرار گیرد همین روش باشد؛ عموم مردم هنگامی که از هک سیستم‌های رایانه‌ای سخن به میان می‌آید ذهنشان سمت ربوده شدن اطلاعات شخصی می‌رود و این همان چیزیست که در روش نفوذ سایبری به‌کار می‌رود. دراین روش تمامی کارها و پردازش‌های سیستم هک شده حتی فشردن یک دکمه کامپیوتر به‌صورت دوره‌ای بدون اطلاع مالک سیستم برای

---

[26]. Ashley, Kean. The history of the criminal liability of chidren, 53Ll. Q. REV. 364[1937].p45.

[27].Key Loggin

هکر ارسال می‌شود و ازین طریق می‌تواند به اطلاعات و رمزهای ورود دسترسی پیدا کند[۲۸]. فرقی که با روش دوم یعنی واسطه‌سازی دارد این است که برخلاف واسطه سازی هکر قادر به اعمال تغییرات مورد نظرش در داده‌های سوژه نمی‌باشد. فرد مجرم با توسل به این روش می‌تواند اطلاعات و داده‌هایی که در یک سامانه رایانه‌ای رد و بدل می‌شوند را بدست آورده و از آن‌ها استفاده مجرمانه نماید. بطور مثال، در دستگاه‌های کنترل حیات و سامانه‌های پزشکی معمولا برای جلوگیری از دسترسی سایر افراد و مراجعان به کنترل این سامانه‌ها برای آن‌ها رمزگذاری صورت می‌گیرد و از آن‌جا که سامانه‌های مزبور تحت شبکه‌ای از داده به‌صورت واحد عمل می‌کنند باتوجه به ضعف امنیتی که دارند بدست آوردن رمز آن‌ها و در دست گرفتن کنترل آن‌ها می‌تواند زمینه ساز خطر جانی برای بیماران باشد.

۲-۲-۲- نشست ربایی[۲۹]

در تمام وبسایت‌ها کوکی‌ها استفاده می‌شوند و کاربرد آن‌ها بدین نحو است که وبسایت‌ها با استفاده از این کوکی‌ها به شناسایی مخاطبان خود که قبلا به آن‌ها مراجعه نمودند و اعطای مجوزهای مناسب به آن‌ها می‌پردازند؛ به طور مثال هنگامی که در یک وبسایت نام کاربری و رمز ورود درج می‌شود، سایت مذکور با به خاطر سپردن کوکی فرد مذکور در مراجعات بعدی وی را مجاز به استفاده از امکانات و اطلاعات سایت می‌شناسد. در این روش هکر با سرقت نمودن کوکی‌های ذخیره شده در رایانه‌های افراد و با دزدیدن هویت آن‌ها خودرا به عنوان فرد موردنظر جا زده و به مجوزهای آن‌ها دسترسی پیدا کرده و راه برای سوء استفاده های بعدی وی هموار می‌گردد.[۳۰] مثلا در یک مرکز کنترل ترافیک و مدیریت چراغ‌های راهنمایی رانندگی، چنان‌چه فرد هکر بتواند با استفاده از کوکی‌های کاربر مربوطه خودرا به جای وی به سامانه موردنظر معرفی نموده و ورود نماید، ممکن است بتواند با دخل و تصرف در داده‌های سامانه موجب وقوع حادثه و خسارت به شهروندان گردد که بدیهی است اقدام وی در این مورد مطابق قوانین کیفری مصداق تسبیب در جنایت علیه افراد بوده

---

[28]. Michaiel, Bassiouni. International Terrorism and political crimes; Carls C Thomas publisher, 1975, p. XIV. P98.

[29].Cookei Stealing

[۳۰]. امید غفاری نیا، Session Hijacking، مجله عصر ارتباطات، ۳۸۲ (۱۳۸۹)، ۲۸.

و مستحق مجازات است.

۲-۲-۳- بدافزار[۳۱]

تروجان برگرفته از اسب تروآ اشاره به اسبی دارد که در انه اید، یکی از حماسه های یونان آمده است و در جریان جنگ تروآ برای نفوذ به دژ دفاعی مستحکم حریف از آن استفاده شد، نیروهای مهاجم در مجسمه اسب چوبی بزرگ پنهان شدند و مجسمه به عنوان هدیه صلح وارد قلعه تروآ شد و شبانه با بازنمودن درهای قلعه، زمینه تصرف آن را فراهم آوردند. تروجان‌ها برنامه‌هایی هستند که هنگام نصب یک برنامه به همراه‌آن وارد سیستم میزبان شده و با ایجاد یک در پشتی، دسترسی غیر مجاز به کامپیوتر مقصد را فراهم کرده و می‌توانند تمام داده‌های آن را به بیرون منتقل کنند.[۳۲] دسترسی به داده‌ها و انتقال آن‌ها به بیرون از سامانه میزبان این‌گونه حملات، باعث می‌شود تا فرد مجرم با بررسی داده‌ها و اعمال تغییرات در آن‌ها زمینه‌ی ارتکاب جرایم بعدی را فراهم آورد. به‌طور مثال در یک پمپ تزریق انسولین ممکن است باتوسل به این روش فرد مجرم به میزان داروی تزریقی به بدن بیمار دسترسی پیدا کرده و با اعمال تغییر در میزان آن سبب مرگ بیمار شود.

روش‌های مذکور رایج ترین و پرکاربرد ترین راه‌های نفوذ به شبکه‌ها و سیستم‌های رایانه‌ای است و منحصر به این موارد نیست؛ حال با درنظر گرفتن چنین وضعیتی که فضای مجازی از طرفی دارای حجم انبوهی از داده‌ها و اطلاعات حیاتی انسان‌ها بوده و به‌صورت مستقیم با جان انسان‌ها سروکار دارد و از طرف دیگر مورد هجمه‌های گوناگون افراد سودجو قرار می‌گیرد؛ آیا فضای مجازی از امنیت و حفاظت کافی برخوردار است؟ آیا استفاده از فضای مجازی در عرصه‌های مهم همچون برج مراقبت پرواز، کنترل هدایت کشتی‌ها، کنترل قطارهای واگن شهری و سایر زمینه‌هایی که جان انسان‌های زیادی را درمعرض سوء استفاده‌های افراد بدخواه قرار می‌دهد کار درستی است؟

بنابراین، در بررسی قابلیت داشتن یا نداشتن وقوع قتل از طریق فضای مجازی باتوجه به مطالب

---

[31].Malware

[32]. Carey, Peter; Media Law, Sweet & Maxwell, Second Edition, London, 1999. P75.

فوق، حداقل بخش اول این قضیه[۳۳] که عبارت از آسیب پذیری و ناامن بودن فضای مجازی یا به بیان دیگر قابلیت وقوع قتل است بالقوه به اثبات می‌رسد اما در خصوص اینکه آیا درعمل و در واقع نیز چنین قتلی تاکنون رخ داده است یا خیر به بررسی خارجی و کنکاش اخبار و نظریه‌ها و سایر مطالب مرتبط با بحث نیاز است.

۳-امکان سنجی قتل ازطریق فضای مجازی بارویکرد اجتماعی

فضای مجازی باتوجه به مزایا و خدماتی که به انسان ارائه می‌دهد روز به روز درعرصه‌های بیشتری از زندگی بشر نفوذ می‌کند، به‌گونه‌ای که امروزه استفاده از اینترنت به استفاده‌های شخصی محدود نمی‌شود و جامعه بشری به آن وابسته شده‌است. وابستگی زیرساخت‌های حیاتی کشور به استفاده از فناوری ارتباطات و اطلاعات، آسیب پذیری آن‌ها در مقابل تهدیدهای سایبری را افزایش داده و باتوجه به گستره استفاده از فضای مجازی که بخش های متنوع و گوناگون زندگی جامعه را دربرگرفته است تنوع جرائم قابل ارتکاب از طریق فضای مجازی نیز افزایش یافته و امروزه در عرصه‌های مختلف زندگی شاهد تخلفات و جرائمی هستیم که در بستر مجازی رخ می‌دهند و دیگر نمی‌توان جرائم سایبری را به طیف خاص و کوچکی محدود نمود.

همان‌طور که پیش‌تر نیز ذکر شد یکی از سوالات و پرسش‌های مهم در خصوص جرائم قابل ارتکاب از طریق فضای مجازی معطوف به جنایات علیه تمامیت جسمانی اشخاص بوده و نکته‌ای که بحث برانگیز می‌باشد ماهیت غیر جسمی و غیر مادی فضای مجازی است. اصل و شاکله فضای مجازی را اطلاعات و داده‌ها تشکیل می‌دهند و این پرسش که چگونه ممکن است با توسل به داده و اطلاعات سبب مرگ افراد گردید باتوجه به مساله فوق پرسشی بجاست. بدین منظور در این قسمت از نوشتار حاضر به بررسی دیدگاه کارشناسان عرصه‌های گوناگون و افرادی که به‌گونه‌ای با فضای سایبر و سامانه‌های آن در ارتباط بوده‌اند پرداخته خواهدشد تا معین شود که فارغ از مباحث امنیتی و فنی فضای مجازی، آیا قابلیت وقوع قتل از طریق آن نزد محققین و کارشناسان در سطح بین‌الملل

---

[۳۳]. به طور خلاصه می‌توان بحث را به صورت یک قضیه که دارای دو بخش است درنظر گرفت: ۱.عدم امنیت و قابلیت سوء استفاده از فضای مجازی علی رغم گسترش فوق العاده آن در زمینه های مختلف زندگی انسان. ۲.امکان استفاده بزهکاران از فضای مجازی در ارتکاب قتل.

پذیرفته شده‌است یا خیر.

۳-۱- دیدگاه کارشناسان

اگرچه اینترنت در دهه ۱۹۵۰ میلادی توسط وزارت دفاع آمریکا و به‌منظور تقویت ارتش ایجاد شد،[۳۴] اما به مرور زمان با نشان دادن کاربردهایی که داشت در عرصه های مختلف توسط بشر به کار گرفته شد به طوری که امروزه در تعریف اینترنت هدف نظامی آن در حاشیه قرار گرفته است.[۳۵] حدود هفتادسال از استفاده بشر از تکنولوژی در عرصه‌های مختلف می‌گذرد و جامعه بشری در استفاده از فضای مجازی به تجربه و دانش کافی جهت بررسی منافع و آسیب‌های فضای مجازی دست یافته است. برای بررسی خطرات و تهدیدهای احتمالی فضای مجازی بهتر است استفاده‌های مختلف و نظرات متخصصان آن‌ها را مورد تحلیل قرار داد.

۳-۱-۱- حمل ونقل: روز به روز استفاده از فن‌آوری و فضای مجازی در حمل و نقل اعم از هوایی،دریایی و زمینی شایع‌تر می‌شود و در بخش‌های گسترده‌تر از آن استفاده می‌گردد.

در نخستین روزهای رونق حمل ونقل هوایی، هواپیماها جهت حفظ ایمنی درطول پرواز، نیاز مبرمی به توجه و دقت خلبانان داشتند. بدیهی است که این موضوع در بردهای طولانی پرواز و ساعت های مداوم سفر خلبانان را دچار خستگی می‌کرد و به دنبال آن جان مسافران هم به خطر می‌افتاد. خستگی خلبان در پروازهای طولانی و خطراتی که ممکن بود به بار بیاورد و همچنین سرزدن خطاهای انسانی در کنترل هواپیما، متخصصان حوزه پرواز را برآن داشت تا با استفاده از تکنولوژی در سفرهای طولانی از حجم فعالیت خلبان بکاهند و هدایت هواپیما به سامانه‌های هوشمند پرواز خودکار سپرده شود. اهمیت سیستم پرواز خودکار به گونه‌ای است که امروزه هیچ هواپیمای مسافربری بدون خلبان خودکار پرواز نمی‌کند مگر هواپیماهای قدیمی و کوچک که کمتر از

---

[۳۴]. محمدطلوع عسگری و دیگران، اینترنت اشیا: شبکه‌های حسگر بی‌سیم(تهران: آریادانش،۱۳۹۸)، ۱۷.

[35]. Dorothy, Denning. Activism, Hactivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, in Network and Wars: the future of terror, crime and militancy, sponsored by Nautilus Institute, 1999. P92.

۲۰ سرنشین دارند. براساس مقررات بین المللی حمل و نقل هوایی، تمامی هواپیماهایی که بیش از۲۰ نفر ظرفیت دارند ملزم به نصب و استفاده از سیستم خلبان خودکار می‌باشند و قوانین داخلی نیز سازمان هواپیمایی کشور را ملزم به برقراری سازوکارهایی در راستای تأمین بی‌خطری پرواز نموده است.[۳۶] علاوه بر هواپیما در کشتی‌ها نیز به دلیل مشابه، به‌تدریج سعی بر کاربرد هرچه بیشتر هوش مصنوعی به‌جای نیروی انسانی است و به همین منظور از سامانه‌های هدایت خودکار کشتی استفاده می‌شود که براساس مسیری که روی نقشه‌ی مسیریابی برای آن تعیین می‌شود به صورت خودکار و با استفاده از داده‌های موقعیت یاب مکانی[۳۷] مسیر مورد نظر را طی می‌نماید. همچنین در اتومبیل‌های جدید از سیستم راننده خودکار استفاده می‌شود که با استفاده از دستوراتی که به رایانه خودرو داده شده است می‌تواند مسیر مورد نظر را دنبال نماید. اکنون با دانستن کاربرد تکنولوژی با کمک فضای مجازی در هدایت وسایل مذکور از طرفی و خصوصیاتی که پیشتر برای فضای مجازی مطرح‌شد مبنی بر هک پذیری و قابلیت نفوذ به سامانه‌ها و شبکه‌های فضای مجازی از طرف دیگر؛ نوبت به بررسی واقعیت های استفاده از فضای مجازی در امور مذکور می‌رسد.

در راستای اثبات قابلیت وقوع قتل از طریق فضای مجازی می‌توان به نظرات کارشناسان عرصه حمل و نقل اشاره نمود که به زعم آنان، هوشمند شدن اداره امور حمل و نقل علی‌رغم تمام کمک‌هایی که به انسان‌ها نموده بازهم نتوانسته ضعف ایمنی خودرا درمقابل تهاجمات سایبری بپوشاند و نحوه استفاده از این سامانه‌ها و کیفیت آن‌ها به‌گونه‌ای است که در بسیاری از حوزه‌ها نگرانی‌هایی وجود داشته و هشدارهایی نیز داده شده‌است که همین می‌تواند نشان دهنده امکان وقوع قتل از طریق فضای مجازی از منظر کارشناسان و خبرگان امر حمل و نقل باشد می‌باشد.[۳۸] به‌طور

---

[۳۶]. به موجب ماده۵ (اصلاحی ۱۳٦۷/۱/۲۵)قانون هواپیمایی کشوری مصوب ۱۳۲۸/٤/۲۸ سازمان می‌تواند از محل درآمدهای قانونی خود درقالب بودجه‌های مصوب و درصورت وجود کسری از محل درآمدهای عمومی کشور طبق مقررات استفاده نماید. وظایف عمده سازمان مزبور به قرار زیر می باشد:

الف- ایجاد،توسعه،بهره برداری و نگهداری فرودگاه‌ها و دستگاه‌های ناوبری و مخابراتی،رادیویی و تلگرافی و تلفنی که مخصوص تنظیم رفت و آمد هواپیماها و تأمین بی‌خطری پرواز لازم می‌باشد و به طورکلی هرنوع نظارت و مساعدتی که به منظور پیشرفت هواپیمایی کشوری و تأمین بی‌خطری پرواز لازم باشد.

ب-....

[37].G.P.S Global.Position.System

[۳۸]. مجتبی نیک رهی، محمدفاضل محمدی، تهدیدات سایبری و راه‌های مقابله با آن(تهران: نظری،۱۳۹۷)، ٤۹.

مثال، درجهت تایید امکان وقوع جرم قتل از طریق فضای مجازی می‌توان به گزارش‌های ذیل اشاره نمود.

شرکت ایدکو (توزیع کننده محصولات کسپرسکی در ایران) به عنوان شرکتی که درحوزه امنیت فضای مجازی فعالیت می‌نماید بیان نموده طبق بررسی‌های امنیتی صورت گرفته از قطارهای تندرو شهری، سیستم کنترل فرمان آن‌ها از میزان بالای آسیب پذیری این قطارها درمقابل تهاجمات سایبری حکایت دارند،[۳۹] به‌عنوان مثال نسخه مدرت اتوماسیون زیمنس که در این قطارها استفاده شده است توسط سیستم وینک آرت[۴۰] کنترل می‌شود که این سیستم با رایانه‌هایی که ویندوزهای ۳۲ بیتی دارند کار می‌کند و در پروژه مشهور حمله استاکس نت مورد هجوم هکرها قرار گرفت[۴۱] و از ضریب امنیتی پایینی برخوردار است و این ضعف امنیتی هکرهارا قادر می‌سازد تا با دردست گرفتن کنترل قطارهای واگن شهری جان عده زیادی را به خطر بیاندازند.

علاوه براین، سیستم راننده خودکار در خودروهای هوشمند نیز موضوعی است که چندین بار مورد توجه و هشدار کارشناسان امنیتی قرار گرفته است، بررسی‌ها و تحقیقات جدید صورت گرفته مبین ضعف شدید سخت افزار و نرم افزار خودروهای هوشمند هستند. دراین خودروها از رایانه استفاده شده است اما به دلیل سهل انگاری سازندگان و دست کم گرفتن تهدیدهای سایبری نسبت به امنیت آن‌ها اقدام جدی صورت نگرفته است و برهمین اساس خودروهای هوشمند قابل هک شدن می باشند و فرد هکر می تواند با در درست گرفتن کنترل رایانه خودرو ، عملا مدیریت خودرو را بدست آورده و از این طریق سرنشینان را به قتل برساند. برای اثبات این امر کافی است فرض شود که اتومبیلی که در جاده ای کوهستانی و پر پیچ وخم درحرکت است تحت تأثیر حمله سایبری از کنترل خارج شود یا با قطع شدن برق ، خودرو در لحظه‌ای حساس خاموش شود و به دره سقوط کند.

---

[۳۹]. محسن قربانعلی افجه، سیستم کنترل و مانیتورینگ قطار شهری(تهران: مینوفر،۱۳۹۵)، ۳۹.

[40].Winc Art

[41]. Seymour, Goodman. Cyberspace as a medium for terrorists, Technological Forecasting & Social Change, volume 74, 2007. P98.

درهواپیماها و کشتی‌ها نیز استفاده از سیستم هدایت خودکار می‌تواند زمینه مناسبی برای هجوم سایبری و از کنترل خارج کردن هواپیما و کشتی پدید آورد. نحوه کار سیستم های خودکار به این صورت است که در ابتدای مسیر اطلاعات مورد نیاز به سامانه داده می‌شود و سامانه براساس دستورهای ورودی مسیر را طی می نماید و ازباب احتیاط داده‌ها و اطلاعات مسیر نیز به یک سیستم رایانه ای ارسال می‌شود.[۴۲] همانگونه که قبلا ذکر شد ماهیت فضای مجازی به گونه‌ای است که علی‌رغم تنوع داده‌های موجود درآن هکرها قادراند به انواع و اقسام شبکه‌ها و سیستم‌ها نفوذ کنند. بنابراین، فرض وقوع قتل از طریق هک کردن سیستم هدایت خودکار هواپیما و کشتی دور از ذهن نیست و قابل تحقق است.

۳-۱-۲- خدمات پزشکی درمانی: علاوه بر حمل و نقل در امور پزشکی و درمانی نیز از تکنولوژی استفاده‌های فراوانی می‌شود؛ اگرچه درگذشته موضوع امنیت تجهیزات حوزه سلامت مغفول مانده بود اما اتفاقاتی که اخیرا رخ داده است توجه عمومی را به آسیب پذیری سیستم‌های مرتبط در حوزه پزشکی جلب کرده است. امروزه کاشتنی‌ها[۴۳] و تعداد بسیار زیادی از وسایل پزشکی نظیر دستگاه‌های کنترل حیات بیمار و پمپ‌های انسولین به صورت متصل درشبکه دیده می‌شوند و قادر هستند تا اطلاعات وضعیت حاضربیمار را انتقال داده و همچنین دستوراتی را برای انجام یک فعالیت همچون تزریق مقدار خاصی از دارو دریافت کنند.[۴۴] پیشرفت‌های شگرف در زمینه سلامت بیماران، بیش از هرچیز ناشی از پیشرفت های فناوری بوده ولیکن این نوع از پیش رفت‌ها مخاطراتی را نیز به دنبال داشته است. به عنوان مثال درسال۲۰۱۵ میلادی به دنبال بروز مشکل امنیتی در یکی از مدل های پمپ‌های انسولین تولیدی توسط شرکت جانسون اند جانسون[۴۵] این شرکت با ۱۱٤۰۰۰ بیمار در ایالات متحده و کانادا ارتباط برقرار کرد تا نسبت به خطرات سایبری موجود اطلاع رسانی کند زیرا آسیب پذیری‌هایی در سیستم کنترل دیده شده بود که در صورت هک شدن وسیله امکان

---

[۴۲]. فرامرز نصری و مجید فراست، ناوبری الکترونیکی(تهران، دانشگاه علوم دریایی امام خمینی ره»،۱۳۹۹)، ۸۳.

[43].Implent

[۴۴]. جکس ملیت، فرانسیس مورایس، ایمپلنت در یک نگاه، ترجمه و تحقیق محمدباقر باغبانی و شیرین شیدفر (تهران: شایان نمودار،۱۳۹٦)، ٦۳.

[45].Johnson and Johnson Company

استفاده از پمپ برای تزریق دوز مهلکی از انسولین به بیمار مهیا می‌شد.[٤٦] همچنین جـی رادکلیـف[٤٧] مشاور ارشد امنیتی و محقق در زمینه رایانه و امنیت شبکه کمپانی رپید، که خود بیمار دیـابتی اسـت گزارش داده که در صورت عدم پیش بینی سازوکار مناسبی برای حفظ امنیت داده‌ها از نظر فنی امکان دستیابی مخفیانه به اطلاعات و توقف تبادل اطلاعات و تغییر آن‌ها وجود دارد. به عقیده وی طراحان کاشتنی‌های پزشکی، امنیت سایبری محصولاتشـان را نادیـده گرفتـه‌انـد و تولیدکننـدگان تجهیـزات پزشکی هنوز در زمینه امنیت سایبری به بلوغ نرسیده اند. در واقع تمرکز سازندگان ایـن محصـولات معطوف بر کارایی پزشکی و موفقیت در نتایج علمی بوده است و ازهمین رو توان پردازشی متوسطی برای آن‌ها درنظر گرفته شده است و همین مانع از به‌کارگیری سیستم‌های محافظتی پیشرفته بر روی آن‌ها می‌باشد. علاوه براین شرکت امنیتی زینگ باکس[٤٨] با بررسی تهدیدات سایبری مراکز درمـانی و پزشکی ضعف امنیت سیستم‌های پزشکی را با بیان اینکه درسال ۲۰۱۷ مراکز پزشکی بیشتر از مراکـز مالی مورد هجوم سایبری قرار گرفته اند تایید نمود.

تهدیدات سایبری در امور پزشکی به‌طور کلی در دو زمینه کاشتنی‌های پزشـکی همچـون بـاتری قلب قابل کاشت دربدن و تجهیزات پزشکی مانند دستگاه‌های کنترل حیات و پمپ‌های تزریـق دارو قابل اعمال است. همانطور که در مطالب فوق ذکر شد در هردو دسته مذکور امکان حمله سـایبری و نفوذ به شبکه‌های مراکز پزشکی متصور است، ازهمین رو سازمان غذا و داروی آمریکا پس از وصول هشدارهای مراکز امنیتی در ارائه این محصولات محدودیت‌هایی از جمله امنیت سایبری دستگاه‌ها را درنظر گرفته است. سوزان شوارتز،[٤٩] مدیر دانشکده علوم و مشارکت‌های استراتژیک مرکز بهداشت و درمان سازمان غذا و داروی آمریکا می‌گوید اگر در دستگاه‌ها و ملزومات پزشکی استانداردهای امنیت سایبری برآورده نشود، آژانس ورود دستگاه‌های پزشکی به بازار را به تـأخیر انداختـه و حتـی آن را متوقف می‌کند؛ زیرا علی‌رغم کاربردهای مفید این دستگاه‌ها، استفاده از آن‌ها جان انسان‌ها را هـم در

---

46. Jim, wolf. First Terrorist Cyber-Attack Reported by U.S. Reuters, May5, 1998. P78.

47. Jay Radlklif

48. Zing Box

49. Susan Shwartz

خطر قرار می دهد و سازمان درنظر دارد تا امنیت وسایل پزشکی را در سراسر دنیا افزایش دهد.

٤- امکان سنجی قتل از طریق فضای مجازی با رویکرد حقوقی

واقعیت حقوقی هرپدیده به‌معنای طرح آن در نظام قانون‌گـذاری کشـور یـا دسـت کـم در رویـه قضایی است و گرنه صرف طرح موضوعی نزد حقوقدانان نمی‌تواند مؤید واقعیت آن پدیده از نگـاه حقوقی باشد. بنابراین، چنانچه در یک جامعه به رسمیت شناخته شدن جرمی مورد بحث باشد یکـی از راه‌های معتبر، بررسی قوانین و مقررات آن جامعه است. در بحث مورد نظر نیز از آن جا که هدف، بررسی امکان وقوع قتل از طریق فضای مجازی است با بررسی قوانین ایران و سایر کشورها می‌توان دریافت که دیدگاه نظام‌های حقوقی آن‌ها درقبال این نوع قتل چیست.

پیش از بررسی منابع حقوقی راجع به قتل از طریق فضای مجازی، ذکر این نکتـه لازم اسـت کـه امروزه سیاست جنایی در جرم انگاری از سه رویه پیروی می‌کند: جرم انگاری داخلی همزمان با جرم انگاری بین المللی، جرم انگاری ناشی از حقوق بین الملل و انتقال جرم انگاری از حقوق داخلی بـه حقوق بین المللی.[٥٠] فرایند جرم انگاری قتل از طریق فضای مجازی به عنوان یکی از زیرشاخه‌هـای تروریسم سایبری در اصل از سطح داخلی (به ویژه ایالات متحده آمریکا) به سطح بین المللی رفته و از سوی دیگر سطح منطقه‌ای اروپا نیز در گسترش مفهوم تروریسـم و قتـل سـایبری تـأثیر بسـزایی گذاشته است، زیرا کشورهای مذکور جزو کشورهای توسعه یافته به شمار رفته و طبیعـی اسـت کـه سطح فن‌آوری و وابستگی به آن در آن‌ها بیشـتر باشـد، از همـین رو بیشـتر از سـایر دولـت هـا بـا چالش‌های فضای مجازی مواجه بوده و در قانون گذاری در این عرصه پیشتاز به شمار می روند.

کشورها در جرم انگاری پیرامون قتل از طریق فضای مجازی از رویه‌ای واحد تبعیت نمی‌کننـد و تدابیر آن‌ها دراین خصوص را می‌توان به دو دسته کلی قانون گذاری عنوان محـور و قـانون گـذاری محتوی محور تقسیم نمود.از همین رو کشورها در جرم انگاری قتل از طریق فضای مجازی، بسته به

---

٥٠. علی حسین نجفی ابرندآبادی، «تقریرات درس تاریخ تحولات کیفری»، گروه حقوق جزا و جرم شناسی،دانشـکده حقـوق دانشـگاه شـهید بهشتی،تهران، ایران،٥٠٠،٢٨١٢.

نظام حقوقی که از آن تبعیت می کنند یکی از شیوه های مذکور را برگزیده اند، به ایـن صـورت کـه کشورهای دارای نظام حقوقی کامن‌لا غالبا تمایل به ذکر عنوان داشته و درمقابل، کشورهای پیرو نظام حقوقی رومی–ژرمنیک بیشتر تمایل به ذکر محتوای جرم مورد نظر دارند.

نخستین قانونی که تروریسم سایبری را به‌طور صریح مورد اشاره قرار مـی‌دهـد درسـال۲۰۰۱ در آمریکا به تصویب رسید؛ لایحه‌ای تحت عنوان«پیشگیری و تعقیـب تروریسـم سـایبری»[۵۱] در مـدت کوتاهی پس از حملات ۱۱ سپتامبر به مجلـس نماینـدگان آمریکـا داده شـد و تحـت عنـوان قـانون پاتریوت[۵۲] به تصویب رسید، قانون پاتریوت قانونی است که برای دست یابی به اهداف موردنظر بـه اصلاح قوانین سابق درموارد شکلی و افزایش اختیارات مجریان قانون می‌پردازد. دراین لایحه تحـت تأثیر حملات تروریستی ۱۱سپتامبر قانون گذاران آمریکا با درنظر گرفتن تهدیدهایی که تروریست‌ها می‌توانند با استفاده از فضای مجازی ایجاد نمایند اهتمـام خـودرا بـر تقویـت امنیـت ملـی سـایبری گذاشته‌اند. اظهارات جان آشکرافت[۵۳] دادستان کل، مقابل کمیته امور قضایی مجلس آمریکا کـه بیـان داشت: «درحال حاضر فن‌آوری از قوانین ما جلو زده است و این نقص قوانین ماسـت»[۵۴] از دغدغـه امنیت فضای مجازی نزد سیاست‌مداران آمریکایی حکایت دارد. سرانجام به منظور مبارزه با تروریسم سایبری، ماده ۸۱٤ قانون پاتریوت، قوانین مربوط به جرایم رایانه‌ای در مجموعه قوانین ایالات متحده آمریکا بخش ۱۰۳۰ (قانون جرایم سایبری) را اصلاح می‌نماید. به موجب ماده ۸۱٤ ایراد خسارت یا دسترسی غیر مجاز به رایانه حفاظت شده که موجب تغییر یا آسیب رساندن در آزمایشـات پزشـکی تشخیص بیماری‌ها، درمان یا نگهداری از یک یا چند شخص بشود یا منتهی به ایراد صدمه جسمی یا

---

[51]. Rick, suri. Cyber Crime, pentagon press, New Delhi, reprint 2003. P121.

[۵۲] .مجموعه قوانین USA PATRIOT ACT شامل نه عنوان مقرراتی زیر است:

۱.افزایش امنیت داخلی در برابر تروریسم ۲.روش‌های پیشرفته نظارتی ۳.قانون سرمایه گذاری ضد تروریستی و منع پول شویی در سطح بـین المللی ٤.محافظت از مرزها ۵.رفع موانع در تحقیق درباره تروریسم ٦.تأمین مأموران محافظتی برای قربانیـان حـوادث تروریسـتی ۷.اشـتراک گذاری گسترده اطلاعات در مبارزه با تروریسم ۸.تقویت حقوق جزا علیه تروریسم ۹.اطلاع رسانی بهینه در خصوص تهدیدات سایبری

[53]. John Ashcroft

[۵٤].جان آشکرافت به تأثیر فوق‌العاده فضای مجازی در افزایش سطح تروریسم معتقـد بـود، بـه عقیـده وی کنتـرل ترافیـک هـوایی بـه کمـک سیستم‌های رایانه‌ای ممکن است تحت تأثیر حملات سایبری هرج و مرج گسترده ای به بار آورده و جان بسیاری را به خطر بیاندازد. همچنین استفاده از سیستم‌های رایانه‌ای ممکن است زمینه حملات ویروسی و اختلال در زیرساخت‌های حیاتی همچون شبکه برق رسانی را به دنبـال بیاورد بنابراین به قانونی دقیق و مستحکم نیاز است که توانایی تضعیف و حذف زیرساخت‌های تروریستی را داشته باشد.

تهدید امنیت عمومی شود جرم انگاری شده و ضمانت اجرای متناسب درنظر گرفته شده‌است.

علاوه بر قوانین کیفری فوق الذکر برای پیشگیری از تهدیدات فضای مجازی، رئیس جمهور آمریکا راهبرد ملی ایمن سازی فضای مجازی را در سال ۲۰۰۳ به‌امضاء رساند. هدف‌های مقررشده در راهبرد ملی، حفاظت از زیرساخت‌های حیاتی آمریکا در مقابل حملات فضای مجازی، کاهش آسیب پذیری ملی در برابر حملات مجازی و تأسیس مرکز حفاظت اطلاعات در مقابله با تهدیدات فضای مجازی می‌باشد.[۵۵]

کشور دیگری که قتل از طریق فضای مجازی را تحت عنوان تروریسم سایبری به صراحت جرم انگاری نموده پاکستان است که در لایحه قانونی(فرمان حکومتی) رئیس جمهور تحت عنوان«پیشگیری از جرایم الکترونیکی»[۵۶] در سال ۲۰۰۸ انجام شده است. طبق ماده۱۷ این قانون که با اعمال اختیارات بند۱ ماده۸۹ قانون اساسی توسط رئیس جمهور به تصویب رسیده است[۵۷] هرشخص یا گروهی که اقدام تروریستی را با قصد مجرمانه و به وسیله رایانه یا شبکه رایانه‌ای انجام دهد و اقدام وی منجر به آسیب رساندن به تمامیت جسمانی افراد جامعه یا زیر ساخت های حیاتی کشور یا اختلال گسترده در اموری که جان مردم به صورت مستقیم با آن ها در ارتباط است گردد مجرم سایبری تلقی گردیده و در مواردی که اقدامات وی منجر به‌مرگ اشخاص گردد به مجازات مرگ یا حبس‌ابد محکوم می‌گردد.[۵۸]

در قانون‌گذاری محتوی‌محور، مقنن بنابر ملاحظاتی از قبیل تفسیر قانون یا چالش‌های مرتبط با عنوان، از به کار بردن عنوان مجرمانه اجتناب نموده و به جای آن ارکان و گونه‌های تشکیل دهنده آن عنوان را ذکر می‌کند. کشورهای متعددی از جمله فرانسه، بلژیک، آلمان و... با این شیوه اقدام به جرم انگاری محتوی قتل‌از طریق فضای‌مجازی تحت عناوین کلی جرم سایبری یا تروریسم نموده اند.

---

[55].Ozeren, Suleyman; Op.cit,2005.p.59

[56].Prevention Of The Electronic Crimes- Ordinance NO.IV of 2008,Published In The Gazette Of Pakistan, Extraordinery,Part-I,Dated The31st May,2008

[۵۷].ذکر این نکته لازم است که لوایحی که رئیس جمهور به ترتیب مقرر در اصل ۸۹ قانون اساسی پاکستان به تصویب برساند درحکم قانون است و از اعتبار قانونی برخوردارند.

[۵۸]. سیدابراهیم حسینی، شریعت و تقنین درکشورهای اسلامی ایران، عربستان و پاکستان (قم، مؤسسه آموزش و پژوهش امام خمینی«ره»، ۱۳۹۶)، ۳۹.

قانون مجازات فرانسه در بخش تروریسم درماده ۱-۴۲۱ تحت عنوان اعمال تروریستی، محتوای قتل از طریق فضای مجازی را جرم انگاری نموده است. طبق ماده ۱-۴۲۱ هنگامی‌که شخص یا گروهی عمدا با هدف آسیب رساندن به نظم و امنیت عمومی در ارتکاب جرایم زیر شرکت نمایند مرتکب رفتارهای تروریستی شده‌اند: الف-تعرض عمدی به حیات،تمامیت جسمانی اشخاص یا هواپیماربایی و آدم ربایی. ب-سرقت‌ها، اخاذی‌ها، تخریب‌ها، ویران سازی‌ها و انهدام‌ها و نیز جرایم مربوط به داده و انفورماتیک که به موجب کتاب سوم ازاین قانون تعریف شده اند،...[۵۹]

دربند۲ماده فوق جرایم مربوط به داده‌ها و فضای مجازی که در فصل سوم قانون آمده‌اند رفتار تروریستی به‌شمار رفته اند. این جرایم در مواد ۳۲۳-۱ تا ۳۲۳-۳ آمده اند و شامل جرایمی از قبیل دسترسی غیرمجاز(هک) به یک سیستم پردازشگر خودکار و ایجاد مانع یا اخلال در کارکرد آن و همچنین دستیابی متقلبانه به داده‌ها می‌شود. نکته حائز اهمیت آن است که موارد مذکور دراین ماده از جمله مواردی هستند که قتل از طریق فضای مجازی به وسیله آن ها رخ می‌دهد و به عبارت دیگر قانون گذاران فرانسوی اقدامات و رفتارهایی را که منجر به قتل به شیوه مذکور می شود را تحت یک عنوان کلی و گسترده همچون تروریسم آورده اند.

بررسی قوانین و مقررات ایران نشان دهنده‌ی پیروی مقنن از رویه محتوی محوری است. به طور مثال درقانون جرایم رایانه‌ای مصوب پنجم خرداد ماه ۱۳۸۸ اگرچه به قتل از طریق فضای مجازی به صورت مستقیم اشاره نشده است اما محتوای این جرم تحت عناوین کلی دیگر تا حدودی مورد اشاره قرار گرفته است. فصل دوم قانون مزبور با عنوان جرائم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی پیش بینی شده است که مبحث دوم آن درارتباط با تخریب و اختلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی است. در ذیل این مبحث و در ماده۱۱ آمده است: «هرکس به قصد به خطرانداختن 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 به‌کار می‌روند، از قبیل خدمات درمانی، آب، برق، گاز، مخابرات، حمل و نقل و بانک‌داری مرتکب شود، به

---

[۵۹].قانون مجازات فرانسه، ترجمه محمدرضاگودرزی و لیلا مقدادی، (تهران: معاونت حقوقی و توسعه قضاییه سلسبیل، ۱۳۸۶)، ۲۵۹.

حبس از سه تا ده سال محکوم خواهد شد.» این ماده قانونی اگرچه به وقوع قتل از طرق مـذکور در مواد ۸و۹و۱۰[۶۰] یعنی تخریب و اختلال در داده‌ها و سیستم‌های رایانه‌ای اشاره ننموده امـا بـا درنظـر گرفتن وصف مجرمانه برای رفتارهای فوق درمواردی که منجر به اخلال و سلب امنیت عمومی شود تلویحا بر واقعیت قانونی قتل از طریق فضای مجازی در ایران صحه گذاشته است، زیرا هنگامی کـه قانون گذار سلب امنیت و آسایش عمومی را مستوجب مجازات حـبس بدانـد تعـرض بـه حیـات و زندگی افراد جامعه را که جرمی مهم‌تر است به طریق اولی مستحق مجازات سنگین‌تر می‌داند.بنابراین اگرچه در قوانین و مقررات ایران به ارتکاب قتل از طریق فضای مجازی صراحتا اشاره نشـده لـیکن باتوجه به اصول و مبانی مذکور در قانون جرایم رایانه‌ای قتل از طریق فضای مجازی بنابرنظر قـانون گذار متصور و قابل تعقیب است.

نتیجه

قتل ازطریق فضای مجازی، پدیده‌ای انکار ناپـذیر وتأثیرگـذار در حـوزه سیاسـت جنـایی بیشـتر کشورهاست و از سوی دیگر تهدیدی جدی و نوین برای امنیت ملی کشورها و اعضای جامعه آن‌ها به‌شمار می‌رود. عمق این تهدید در ورای ارتباط گسترده و تنگاتنگ زیرساخت‌های حیاتی کشـورها با فضای مبادلات الکترونیکی یا همان فضای سـایبری نهفتـه‌اسـت و ایـن زیرسـاخت‌هـا درمعـرض شدیدترین و پیچیده‌ترین حملات قرار دارند؛ باتوجه به مطالبی که درنوشتار حاضر درخصوص قتـل از طریق فضای مجازی مطرح گردید، علاوه‌بر نتیجه کلی فوق مبنی بر قابلیـت وقـوع چنـین جرمـی به‌شیوه مذکور می‌توان به دستاوردهای زیر نیز اشاره کرد:

---

[۶۰].ق.ج.ر مصوب۱۳۸۸/۳/۵، ماده۸:هرکس به‌طور غیرمجاز داده‌های دیگری را از سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده حذف یـا تخریب یا مختل یا غیر قابل پردازش کند به حبس از شش ماه تا دوسال یا جزای نقدی از ده میلیون ریـال تـا چهـل میلیـون ریـال یـا هـردو مجازات محکوم خواهد شد. ماده۹:هرکس به‌طور غیرمجاز با اعمالی از قبیل واردکردن،انتقال دادن، پخش، حذف‌کردن،متوقف کردن،دستکاری یا تخریب داده‌ها یا امواج الکترومغناطیسی یا نوری،سامانه‌های رایانه‌ای یا مخابراتی دیگری را از کار بیاندازد یا کارکرد آن‌هـارا مختـل کند،بـه حبس از شش ماه تا دوسال یا جزای نقدی از ده میلیون ریال تا چهل میلیون ریال یا هردو مجازات محکوم خواهدشد. ماده۱۰:هرکس به‌طـور غیرمجاز با اعمالی از قبیل مخفی کردن داده‌ها،تغییر گذرواژه یا رمز نگاری داده‌ها مانع دسترسی اشـخاص مجـاز بـه داده‌هـا یـا سـامانه‌هـای رایانه‌ای یا مخابراتی شود، به حبس از نودویک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریـال یـا هـردو مجـازات محکوم خواهد شد.

نخست، باتوجه به شواهد و استدلال‌های عدیده درباره هستی داشتن قتل سایبری از نگاه فنی، امنیتی و حقوقی باید پذیرفت و باور کرد که پدیده‌ای به نام قتل از طریق فضای مجازی وجود دارد و باتوجه به کاربردهای اینترنت در اقدامات تروریستی و نمونه‌هایی از اقدامات و تهدیداتی که در گذشته رخ داده‌اند امروزه تردیدی در واقعیت و هستی تروریسم سایبری وجود ندارد. از ابتدای سال ۲۰۱۰ میلادی و باتوجه به اتفاقات گوناگونی که رخ داد، از جمله حمله سایبری به زیرساخت‌های حیاتی کشور استونی و حمله ویروسی استراکس نت به نیروگاه‌های هسته‌ای ایران و نمونه‌های متعدد دیگر، بحث امکان یا عدم امکان قتل از طریق فضای سایبری کم‌رنگ گردیده و اقدامات علمی و فنی هم‌چون برگزاری همایش‌ها، سمینارها، اصلاح زیرساخت‌ها و تصویب قوانین بازدارنده جایگزین تردیدها گردیده است.

دوم، قائل شدن به تفکیک بین دو عنوان قتل و قتل سایبری است و این جدایی تنها در این اندازه نیست که قتل از طریق فضای مجازی را شیوه‌ای از ارتکاب جرم قتل دانست، بلکه تفاوت‌های این دو در حوزه رکن مادی و به ویژه بستر و موضوع جرم است و درواقع شناخت ماهیت قتل سایبری نیاز به دست‌یابی به تعریفی جامع از این پدیده دارد. از آن‌جا که در اقدامات مجرمانه موردنظر، محیط سایبری گاه وسیله ارتکاب جرم و گاه خود هدف اعمال مجرمانه واقع می‌شود، می‌توان قتل از طریق فضای مجازی را بدین صورت تعریف نمود، جرمی است که درآن قصدمرتکب بر به قتل رساندن دیگران وابسته به فضای مجازی و اینترنت بوده که در آن کاربردی دوگانه دارد، گاه به‌صورت وسیله ارتکاب جرم و گاه به‌عنوان هدف اقدامات مجرمانه مورد استفاده قرار می‌گیرد و مراد از فضای مجازی در این تعریف معنای اعم آن، یعنی سامانه‌های رایانه‌ای، مخابراتی و دیجیتالی است.

سوم، پذیرش مفهومی یا محتوایی قتل سایبری درنظام عدالت کیفری ایران است. با بررسی قوانین و مقررات کیفری می‌توان به پذیرش پراکنده اعمال کشنده سایبری از دید تقنینی اشاره نمود. درجایی که فضای سایبری نقش وسیله برای اقدامات مجرمانه دارد، مانند قتل بیماران قلبی از طریق ارسال پیام شوک‌آور ، می‌توان به ماده٤ قانون جرائم رایانه‌ای اشاره نمود که استفاده از سامانه‌ها و ابزارهای رایانه‌ای به‌منظور دست‌یابی به داده‌های سری و شخصی را جرم انگاری نموده است. و درخصوص جرم انگاری هدف محور می‌توان پذیرفت که در ماده۱۱ قانون جرائم رایانه‌ای باعنوان «تخریب و

اختلال درداده‌ها یا سامانه‌های رایانه‌ای ومخابراتی»به برخی مصادیق برجسته قتل سایبری اشاره شده است که در آن‌ها فضای مجازی به‌عنوان هدف حملات مجرمین قرار گرفته و منتهی به مرگ شهروندان می‌گردد.

پیشنهاد

نخست، لزوم اتخاذ سیاست‌های پیشگیرانه متناسب با فضای مجازی است. زیرا باتوجه به اهمیت و تأثیرات مهمی که برخی موارد قتل از طریق فضای مجازی ممکن است به‌بار آورد، مانند اقدام مجرم بر ایجاد اختلال در سیستم ناوبری هواپیما یا سیستم‌های پزشکی مراکز درمانی، حجم آسیب‌ها و خسارات وارد شده به‌قدری سنگین است که بهتراست درنظام‌های حقوقی نسبت به این جرائم توجه بیشتری شده و سازوکارهای حفاظتی مناسب درنظرگرفته شود و بیش از کیفردهی بر پیشگیری از این جرائم اهتمام شود.

دوم، باتوجه به خصوصیات فنی فضای مجازی و نحوه ارتکاب جرائم در این بستر از جمله قتل، لزوم اتخاذ سیاست جنایی شکلی افتراقی در رسیدگی به این جرائم روشن می‌شود. انتشار ویروس، هک کردن سامانه، جاسوسی داده‌های سری و حملات منع از سرویس مهم‌ترین اقداماتی هستند که در جرم مذکور ممکن است از آن‌ها استفاده شود و بررسی آن‌ها نیاز به فرایندی اختصاصی و فنی دارد از این رو اکتفا نمودن به مقررات آئین دادرسی کیفری حاضر که برای رسیدگی به جرائم عادی و معمول مقرر گردیده شاید نتواند رسیدگی عادلانه، متناسب و سریعی که مدنظر قانون‌گذار در رسیدگی به جرائم می‌باشد را تأمین کند.

Comment [گل محمدی۲]: نحوه نگارش تغییر داده شود و به صورت پیشنهاد ارائه گردد.
در حال حاضر همان مطالب قبلی است که در قالب نتیجه گیری نوشته اید، اگر مطالعه کنید کاملا متوجه می شوید که نحوه نگارش در قالب ارائه پیشنهادات نیست.

فهرست منابع

الف- منابع فارسی

ایزدی فرد، علی اکبر و سید مجتبی حسین نژاد. «بررسی فقهی قتل ازطریق فضای مجازی». مجله مطالعات فقه و حقوق اسلامی ١٤ (١٣٩٥): ٧-٣٤.

باغبانی، محمدباقر و شیرین شیدفر، مترجم. ویرایش اول. تهران: شایان نمودار،١٣٩٦.

تقاء، احمدرضا. مترجم. جنگ پست مدرن سیاست نوین کیفری. تهران: معاونت تحقیق و پژوهش دانشکده فرماندهی و ستاد سپاه پاسداران، ١٣٨١.

حسینی، سیدابراهیم. شریعت و تقنین درکشورهای اسلامی ایران، عربستان و پاکستان. ویرایش سوم. قم: مؤسسه آموزش و پژوهش امام خمینی«ره»، ١٣٩٦.

شفیعی،مسعود. نرم افزار منبع باز و آزاد. ویرایش اول. تهران: پیام رسان،١٣٨٥.

عسگری، محمدطلوع، رضا قاسمی، مهدی حسینی مهدی و علی نجفی. اینترنت اشیا شبکه‌های حسگر بی‌سیم. ویرایش اول. تهران: آریادانش،١٣٩٨.

غفاری نیا، امید. نشست ربایی. مجله عصر ارتباطات. شماره٣٨٢. ١٣٨٩.

فروزان، منصوره. آشنایی با رایانه. ویرایش اول. تهران: کتاب همراه،١٣٨٣.

قربانعلی افجه، محسن. سیستم کنترل و مانیتورینگ قطار شهری. ویرایش دوم. تهران: مینوفر،١٣٩٥.

قلی زاده نوری، فرهاد، مترجم. فرهنگ تشریحی اصطلاحات کامپیوتری مایکروسافت. ویرایش سوم. تهران: هیأت مؤلفان و ویراستاران انتشارات مایکروسافت،١٣٨١.

گروه واژه گزینی انجمن رمز ایران، واژه نامه و فرهنگ امنیت فضای تولید و تبادل اطلاعات. تهران: مؤسسه انتشارات علمی دانشگاه صنعتی شریف،١٣٩٤.

گودرزی، محمد رضا و مقدادی لیلا، مترجم. قانون مجازات فرانسه. ویرایش اول. تهران: معاونت حقوقی و توسعه قضایی قوه قضاییه سلسبیل، ١٣٨٦.

معاونت پژوهش و تولید علم، مترجم. عملیات و اصول جنگ اطلاعات. ویرایش دوم.تهران: موسسه آموزشی و

تحقیقاتی صنایع دفاعی،۱۳۸٦.

موسوی خمینی ،روح الله. مناهج الوصول الی علم الاصول. ویرایش دوم. قم: موسسه تنظیم و نشر آثار امام خمینی،۱٤۱۵ه.ق.

نجفی ابرندآبادی، علی حسین. «تقریرات درس تاریخ تحولات کیفری». گروه حقوق جزا و جرم شناسی، دانشگاه شهید بهشتی،تهران، ایران.۱۳۷۸.

نصری، فرامرز و مجید فراست. ناوبری الکترونیکی. ویرایش دوم. تهران: دانشگاه علوم دریایی امام خمینی«ره»،۱۳۹۹.

نیک رهی، مجتبی و محمدفاضل محمدی. تهدیدات سایبری و راه‌های مقابله با آن. ویرایش سوم. تهران: نظری،۱۳۹۷.

ب- منابع لاتین

Ashworth, Andrew. Principles of Criminal Law, Chicago University, [5th ed.2006]

Kean, Ashley. The history of the criminal liability of chidren, 53Ll. Q. REV. 364[1937]

Bassiouni, M.Ch. International Terrorism and political crimes; Carls C Thomas publisher, 1975, p. XIV

Carey, Peter; Media Law, Sweet & Maxwell, Second Edition, London, 1999

Collin, Barry; The Future of Cyberterrorism , Crime and Justice International, March1997

Denning, Dorothy. Activism, Hactivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, in Network and Wars: the future of terror, crime and militancy, sponsored by Nautilus Institute, 1999

Goodman, Seymour. Cyberspace as a medium for terrorists, Technological Forecasting & Social Change, volume 74, 2007

Suri, Rick, Cyber Crime, pentagon press, New Delhi, reprint 2003

Wolf, Jim. First Terrorist Cyber-Attack Reported by U.S. Reuters, May5, 1998

Abstract

Cyber terrorism is one of the latest examples of real terrorism and an increasing threat to the international community, employed by individuals having access to this modern science and wants to apply it against third world countries through illegal employment of modern technologies and electronic and computer devices in virtual space. Therefore, putting aside the fact that it is the West which is mostly the main cause of cyber terrorism while claiming leading the fight against it, there are certain international documents designed and approved to prevent and contain all forms of terrorism, particularly cyber terrorism. Pathologically speaking, we can claim that these documents not only have not brought any success in fighting this emergent phenomenon, but have, also, deteriorated the situation by paving the way for its rise in national and international arena. Thus, the present article takes a close look at cyber terrorism and its related concepts and evaluates the international documents from the perspective of international criminal law., this article tries to review general concept of cyber terrorism as a criminal phenomenon and Strategies and shortcomings of the legal system to deal with it.This Research through interdisciplinary study and with constructivist approach, will explore the phenomenon of cyber-terrorism, and will respond to it, how mental frameworks actors in the international arena will be effective on creating cyber threats, and in resolving this security dilemma In the social process, actors identity and their perceptions in the prevention and legislation on the international arena, is effective.

Keywords: Cyber Terrorism, Murder, Criminal Law, Manslaughter