تاریخ دریافت: ۱۴۰۱/۱۰/۱۰
تاریخ پذیرش:۱۴۰۱/۱۱/۰۴
مقاله پژوهشی

پژوهشنامه علوم دفاعی
شماره ۹، بهار ۱۴۰۲
ص ص ۲۷ تا ۷۰

مقابله با حملات سایبری علیه داده‌ها و سامانه‌های رایانه‌ای نظامی در حقوق کیفری ایران و کنوانسیون بوداپست

علینقی لزگی[۱]، محمد زرنگ[۲]، هادی مرسی[۳]

چکیده

افزایش حملات سایبری و جایگاه ویژه جمهوری اسلامی ایران در خاورمیانه ایجاب می‌کند که داده‌ها و سامانه‌های رایانه‌ای نظامی در برابر حملات سایبری قابل ارتکاب در فضای سایبر از آن سوی مرزها توسط دشمنان و بیگانگان مورد حمایت کیفری قرار گیرند. هدف پژوهش حاضر تحلیل و ارزیابی راهبردهای مقابله کیفری در قبال حملات سایبری علیه تمامیت داده‌ها و سامانه‌های رایانه‌ای نظامی است. تحقیق حاضر، یک تحقیق کیفی است که از نظر هدف، کاربردی و از حیث ابزار تحقیق، اسنادی و کتابخانه‌ای است و اطلاعات گردآوری شده شامل قوانین و مقررات کیفری مورد مطالعه و همچنین کنوانسیون جرائم سایبری بوده است که به روش توصیفی– تحلیلی مورد تجزیه و تحلیل قرار گرفته‌اند. علی‌رغم اینکه حملات سایبری علیه داده‌ها و سامانه‌های نظامی امنیت کشور را به مخاطره می‌اندازند، اما این امر مورد توجه اسناد بین‌المللی و قوانین فعلی ایران قرار نگرفته است. لذا مشخص نمی‌باشد، در صورت تحقق یک حمله سایبری به کدام عنوان یا عناوین مجرمانه می‌توان تمسک جست. یافته‌های تحقیق حاکی از آن است که، حملات سایبری علیه تمامیت داده‌ها و سامانه‌های رایانه‌ای نظامی ارتکاب می‌یابند و منجر به صدمه زدن، پاک کردن، خراب کردن، تغییر دادن یا توقف آن‌ها می‌شوند، در سطح بین‌المللی مصداق بندهای (۱) و (۲) ماده ۴ و ماده ۵ کنوانسیون بوداپست و گزارش توجیهی پیرامون آن قرار می‌گیرد و در سطح ملی مصداق مواد ۷۳۶ و ۷۳۷ قانون مجازات اسلامی-تعزیرات قرار می‌گیرند و می‌توان در قالب دو جرم رایانه‌ای اخلال در داده و سامانه رایانه‌ای به مقابله کیفری با آن‌ها پرداخت.

کلمات کلیدی: فضای سایبر، حمله سایبری، داده‌های نظامی، سامانه‌های نظامی، جرائم رایانه‌ای

---

[۱] استادیار گروه الهیات و معارف دانشگاه افسری امام علی(ع). تهران. ایران. ایمیل: a.lezgi@yahoo.com
[۲] مربی و عضو هیئت علمی گروه حقوق دانشگاه افسری امام علی(ع). تهران. ایران.
[۳] دانشجوی دکتری حقوق جزا و جرم شناسی دانشگاه میبد. یزد. ایران.

مقدمه

فضای سایبر، فضایی حقیقی و واقعی است و مجازی نیست[۱] هر چند که به شکل مادی و ملموس احساس شدنی نیست (زندی،۱۳۹۳، ص۱۶۰؛یکرنگی و دیگران،۱۴۰۰، ص۵۶۴). برخی از نویسندگان فضای سایبر را شامل تمام شبکه‌های رایانه‌ای موجود در دنیا و هر آنچه به این شبکه‌ها متصل است یا آنان را کنترل می‌کند، دانسته‌اند (Clarke,2010, p6). برخی دیگر فضای سایبر را فقط ناظر به همه منابع اطلاعاتی قابل‌دسترس در َشبکه‌های رایانه‌ای دانسته‌اند (www.library.arizona.edu/rio/glossary.html). وزارت دفاع ایالات متحده فضای سایبر را این‌گونه تعریف نموده است: «دامنه‌ای جهانی در فضای اطلاعات که متشکل از شبکه‌ها و سامانه‌های مستقل فناوری اطلاعات از قبیل اینترنت، شبکه‌های مخابراتی، سامانه‌های رایانه‌ای و پردازنده و کنترل‌هایی تعبیه شده است»(Joint Chiefs of Staff,2011,p141). در تعریف فضای سایبر گفته شده است: فضای سایبر فضایی است که داده‌های رایانه‌ای در آن به صورت صفر و یک ایجاد، ذخیره، جا به جا، دستخوش تغییرات و حذف می‌شوند(مرسی،۱۳۹۷، ص۲۳).

علاوه بر مزایا و محاسن پیشرفت تکنولوژی و فناوری، فرصت‌های جدید و ابزارهای نوینی در اختیار مجرمین و مهاجمین سایبری قرار داده است تا با کمترین هزینه و با راحت‌ترین شیوه‌ها، امکان ارتکاب حملات سایبری و وارد آمدن صدمات شدید بر داده‌ها و سامانه‌های رایانه‌ای نظامی را تسهیل کند. در حال حاضر فراهم کردن یک ارتش سنتی پر هزینه بوده به طوری که یک جت جنگنده بیش از یکصد میلیون دلار قیمت دارد. علاوه بر آن باید هزینه ناوها، تانک‌ها، ماهواره‌های جاسوسی و افراد مسلح را نیز در نظر گرفت. در مقایسه مبلغی بین یک تا ده میلیون دلار برای تأمین هزینه‌های تیمی متشکل از ده تا بیست نفوذگر برای یک

---

۱. برخی نویسندگان فضای سایبر را محیطی مجازی دانسته و آن را این‌گونه تعریف نموده‌اند:«محیطی مجازی و غیرملموس که در فضای شبکه‌های بین‌المللی (که از طریق اینترنت به هم متصل می‌شوند» ر.ک به: باستانی، برومند، جرائم کامپیوتری و اینترنتی جلوی نوین از بزهکاری، تهران، چاپ اول، نشر بهنامی،۱۳۸۳ به نقل از: کیهانلو، فاطمه و وحید رضادوست، حملات سایبری به‌مثابه توسل به‌زور در سیاق منشور ملل متحد، فصلنامه تحقیقات حقوقی، شماره ۶۹، سال ۱۳۹۳، ص ۹۵.

جنگ اطلاعاتی- سایبری کافی است. این تیم را با همین مبلغ می‌توان به آخرین مدل‌های رایانه‌ای مجهز کرد (سلمانی‌زاده، ۴:۱۳۸۰).

با تصویب قانون جرائم رایانه‌ای در ۱۳۸۸/۰۳/۰۵ سیاست جنایی نظام حقوقی ایران در برابر اقدام‌های مجرمانه‌ای که علیه داده‌ها و سامانه‌های رایانه‌ای حقوق، داده‌ها و سامانه‌های رایانه‌ای عموم شهروندان در فضای سایبر ارتکاب می‌یابد و اقدام‌های مجرمانه‌ای که علیه داده‌ها و سامانه‌های رایانه‌ای مرتبط با امنیت کشور در فضای سایبر انجام می‌شوند به نحو یکسان و در قالب جرائم رایانه‌ای پیش‌بینی شده است. مجموعه این اقدامات مجرمانه «حمله سایبری» نامیده شده و این‌گونه تعریف شده است:«حمله سایبری، مجموعه اقدام‌هایی است که توسط یک دولت به منظور نفوذ یا ایجاد اخلال در سامانه‌های رایانه‌ای و یا شبکه رایانه‌ای، علیه دولت دیگر ارتکاب می‌یابد» (خلیل‌زاده،۲۶:۱۳۹۳).

حملات سایبری گونه جدید و نوینی از تهدیدات سایبری است که ممکن است علیه تمامیت داده‌ها و سامانه‌های رایانه‌ای نظامی ارتکاب‌یابند و زیرساخت‌های حیاتی نظامی یک کشور را تحت الشعاع قرار دهند و امنیت کشور را به مخاطره اندازند. موقعیت و جایگاه خاص جمهوری اسلامی ایران در خاورمیانه سبب شده است در ده‌های اخیر بارها توسط دشمنان و بیگانگان مورد حمله سایبری قرار گیرد که می‌توان به حمله سایبری استاکس‌نت[۱] در سال ۱۳۸۹، حمله سایبری دوکو[۲] در سال ۱۳۹۰، حمله سایبری فلیم[۳] در سال۱۳۹۱ علیه نیروگاه‌های هسته‌ای ایران، حملات سایبری علیه سازمان بنادر و کشتیرانی سال ۱۳۹۹، زندان اوین ۱۴۰۰، شرکت هواپیمایی ماهان۱۴۰۰، صدا و سیما ۱۴۰۰ و سازمان فرهنگ و ارتباطات اسلامی ۱۴۰۱ اشاره کرد:

(https://www.tasnimnews.com/fa/news/1401/06/20/2772788/).

---

۱. Stuxnet

۲. Duqu

۳. Flame

در راستای حمایت از تمامیت داده‌ها و سامانه‌های رایانه‌ای در سطح بین‌المللی کنوانسیون بوداپست و گزارش توجیهی آن برپایه نشست‌هایی در نوامبر ۲۰۰۱ از سوی کمیته وزیران شورای اروپا پذیرفته شد.[1] و در راستای حمایت از تمامیت داده‌ها و سامانه‌های رایانه‌ای در سطح ملی قانون‌گذار ایران، قانون جرائم رایانه‌ای را در تاریخ ۳/۵/ ۱۳۸۸ با ۵۶ ماده و ۲۵ تبصره، تصویب کرد. به جهت آن‌که در آن زمان حملات سایبری روند رو به رشد خود را طی نکرده بودند و اثراتی که بر امنیت کشور می‌توانستند بگذارند، چندان ملموس نبود، این امر موجب شد در کنوانسیون بوداپست و قانون جرائم رایانه‌ای ایران عنوان مجرمانه «حمله سایبری» استفاده نشود. لیکن مشخص نمی‌باشد در صورت تحقق حمله سایبری علیه داده‌ها و سامانه‌های رایانه‌ای نظامی به کدام مواد قانونی پیش‌بینی شده در قانون جرائم رایانه‌ای می‌توان تمسک جست.

ضرورت این پژوهش در وهله اول تبیین مفهوم و ماهیت «حمله سایبری» است تا مشخص شود در پرتوی چه مواد قانونی می‌توان به مقابله کیفری با آن پرداخت و در وهله دوم تحلیل و ارزیابی مواد قانونی پیش‌بینی شده در قانون جرائم رایانه‌ای است که می‌توان با تمسک به آن‌ها به مقابله کیفری با حملات سایبری علیه داده‌ها و سامانه‌های رایانه‌ای نظامی پرداخت. لذا سؤال اصلی پژوهش حاضر این است که؛ راهبردهای مقابله کیفری در قبال حملات سایبری علیه تمامیت داده‌ها و سامانه‌های رایانه‌ای نظامی در پرتوی حقوق کیفری ایران و کنوانسیون بوداپست کدام است؟

پیشینه و مبانی نظری پژوهش

پیشینه پژوهش

مرتبط با موضوع این پژوهش، پژوهش‌های مناسبی انجام گرفته است، که در جدول (۱) به اختصار به چند نمونه از این پژوهش‌ها اشاره شده است.

---

۱ ر.ک به: جلالی فراهانی، امیرحسین(۱۳۹۵)، کنوانسیون جرائم سایبر و پروتکل الحاقی آن، تهران، چاپ دوم، نشر خرسندی.

جدول ۱. پیشینهٔ تحقیق

ردیف	پژوهشگر	موضوع پژوهش	یافته‌های پژوهش
۱	محمد یکرنگی، هادی مرسی و مهسا علیزاده	امکان‌سنجی استناد به دفاع مشروع به عنوان مانع مسئولیت کیفری	در این مقاله به تحلیل و ارزیابی امکان تمسک به دفاع مشروع در پرتوی ماده ۱۵۶ قانون مجازات اسلامی پرداخته شده است.
۲	هیتر هریسن، ترجمه حکیمی ها، سعید و هومان شاهرخ	کتاب جنگ سایبری و حقوق جنگ	در این کتاب به بررسی و تحلیل حملات سایبری پرداخته شده است که مصداقی از توسل به زور و حقوق بشردوستانه بین-المللی هستند.
۳	مونا، خلیل زاده	کتاب مسؤولیت بین‌المللی دولت‌ها در قبال حملات سایبری	در این کتاب به بررسی حقوق و قواعد حاکم بر فضای سایبر و همچنین به مسئولیت بین‌المللی دولت‌ها و نحوه انتساب و جبران خسارت در قبال حملات سایبری پرداخته شده است.
۴	حسن عالی‌پور	کتاب حقوق کیفری فناوری اطلاعات	از آنجایی که در حقوق کیفری ایران عنوان مجرمانه حمله سایبری اتخاذ نشده است، در این کتاب سخنی از راهبردهای کیفری مقابله با آن مطرح نشده است
۵	غلامرضا، محمدنسل	حقوق جزای اختصاصی جرائم رایانه ای در ایران	از آنجایی که در حقوق کیفری ایران عنوان مجرمانه حمله سایبری اتخاذ نشده است، در این کتاب سخنی از راهبردهای کیفری مقابله با آن مطرح نشده است

به طور کلی، مرتبط با موضوع پژوهش پیش‌رو، تحقیقات و آثار بسیاری از لحاظ کمی و کیفی به رشته تحریر در آمده است که به چند مورد از این آثار اشاره شد. اما وجه افتراق این پژوهش با دیگر پژوهش‌ها در این است که این پژوهش به تحلیل راهبردهای مقابله کیفری با

حملات سایبری علیه داده‌ها و سامانه‌های رایانه‌ای نظامی پرداخته ، موضوعی که در پژوهش-های صورت گرفته به آن اشاره نشده است.

مبانی نظری پژوهش

مفهوم حمله سایبری

پیرامون مفهوم حمله سایبری باید اذعان داشت تعریف واحد و مشترکی وجود ندارد، به نحوی که هر یک از کارشناسان و صاحب نظران از منظر دید خود به بیان مفهوم حمله سایبری پرداخته‌اند. از آنجایی‌که در برخی از آنان چهار عنصر مرتکب، موضوع، قصد یا رفتار موضوعیت داشته و در برخی دیگر موضعیت نداشته است، پژوهش حاضر آن‌ها را در دو مفهوم موسع و مضیق تبیین می‌کند.

حمله سایبری در مفهوم موسع

تعاریف ارائه شده در این قسمت از آن جهت موسع در نظر گرفته شده‌اند که رفتار و موضوع را محدود نکرده و بر مرتکب و قصد خاصی نیز تأکیدی نشده است. برخی از نویسندگان حملات سایبری را حمله‌ای می‌دانند که توسط یک سامانه رایانه‌ای علیه یک سامانه رایانه‌ای یا یک شبکه رایانه‌ای یا یک وب‌سایت به‌نحوی ارتکاب می‌یابد و محرمانگی، تمامیت و قابلیت دسترسی سامانه‌های رایانه‌ای و اطلاعات ذخیره‌شده در آن را به مخاطره می‌اندازد(Junaidu, 2015:3). بر اساس این تعریف، مهم‌ترین هدف جرم انگاری پیرامون حملات سایبری حمایت از محرمانگی، صحت، تمامیت و قابلیت دسترسی سامانه‌های رایانه‌ای و به تبع آن داده‌های ذخیره‌شده در آنان در مقابل تجاوز و هجوم سایر سامانه‌های رایانه‌ای می باشد. همچنین براساس تعریف مذکور وجود حداقل دو سامانه رایانه‌ای جهت شکل‌گیری مفهوم حمله سایبری لازم و ضروری می‌باشد. به عبارت دیگر، بر اساس تعریف مذکور می‌توان گفت مفهوم حمله سایبری تنها در زیرفضای سایبری میان سامانه‌های رایانه‌ای با یکدیگر شکل می‌گیرد و در زیرفضای سایبری میان کاربر با سامانه رایانه‌ای شکل نخواهد گرفت.

برخی از نویسندگان حمله سایبری را به معنای «ایجاد اخلال در صحت یا درستی داده‌ها که در اغلب موارد از طریق اعمال کدهای مخرب و تغییر در منطق برنامه‌ها و کنترل داده‌ها صورت می‌گیرد و منجر به خروجی‌های اشتباه توسط سامانه‌های رایانه‌ای می‌گردد، دانسته‌اند(جالینوسی، ابراهیمی و قنوانی،۱۳۹۵:۱۰). همچنین در تعریف دیگری یک حمله سایبری شامل چهار حوزه‌ی از دست دادن تمامیت، از دست دادن قابلیت دسترسی، از دست دادن محرمانگی داده و اطلاعات و در نهایت تخریب فیزیکی سامانه‌های رایانه‌ای است(Army, U.S,2005:1-3). و نیز شورای پژوهش ملی ایالات‌متحده آمریکا حملات سایبری را به‌عنوان «مجموعه اقداماتی عمدی جهت تغییر[۱]، اختلال، فریب[۲]، تخریب[۳] یا از بین بردن سامانه‌های رایانه‌ای، شبکه‌های رایانه‌ای، اطلاعات و داده‌های ذخیره‌شده یا در حال انتقال سامانه‌های رایانه‌ای یا شبکه‌های رایانه‌ای» تعریف نموده است(Oona, 2012:826). تعریف ارائه شده را از آن جهت که مرتکب جرم را محدود ننموده و یا بر قصد خاصی تأکید نکرده است می توان در زمره‌ی مفاهیم موسع ارائه‌شده از حملات سایبری قرار داد.

حمله سایبری در مفهوم مضیق

تعاریفی که در این قسمت به بیان آن‌ها پرداخته شده است از آن جهت مضیق در نظر گرفته شده‌اند که رفتار و موضوع را محدود کرده و یا بر مرتکب و قصد خاصی نیز تاکید داشته است.

ریچارد ای.کلارک[۴] در تعریف حملات سایبری بیان می دارد: حملات سایبری مجموعه اقداماتی می‌باشند که توسط یک دولت به منظور نفوذ یا ایجاد اخلال در سامانه‌های رایانه و یا شبکه‌ی رایانه‌ای، علیه دولت دیگر ارتکاب می‌یابد(خلیل‌زاده،۱۳۹۳:۲۶). شایسته به نظر

---

۱. degrade

۲. deceive

۳. destory

۴. A.Clarke,richard

نمی‌رسد که ارتکاب حملات سایبری محدود به اقداماتی گردد که توسط مرتکبی خاص مانند یک دولت علیه دولت دیگر ارتکاب می‌یابد؛ زیرا در برخی از موارد هکر[۱]های داخلی یک کشور می‌توانند در فضای سایبر عملیات مجرمانه‌ای را علیه سامانه‌های رایانه‌ای دولت خود مرتکب شوند که نتایج ناشی از آن در برخی از موارد با عملیات مجرمانه‌ای که توسط یک دولت علیه دولت دیگر در فضای سایبر ارتکاب می یابد تفاوت چندانی نخواهد داشت.

برخی دیگر حمله سایبری را مجموعه اقدامات مجرمانه‌ای دانسته‌اند که در جهت تضعیف عملکرد شبکه‌های رایانه‌ای برای اهداف امنیتی، سیاسی و ملی ارتکاب می‌یابد(Oona, 2012:822-826). برخی نیز در تعریف حمله سایبری علاوه بر آنکه مرتکب حمله سایبری را محدود به دولت می‌نمایند، هدف آن را نیز محدود به زیرساخت‌های حیاتی یک کشور می‌نمایند و این‌گونه حملات سایبری را تعریف می‌نمایند: «اقداماتی که از سوی دولت برای هدف قرار دادن زیرساخت‌های اساسی یک دولت دیگر ازجمله سیستم بانکی، انرژی و حمل نقل عمومی که به شبکه رایانه‌ای متصل هستند صورت می‌پذیرد.»(خلیل‌زاده،۱۳۹۳:۳۳)

سازمان شانگهای[۲]، تعریف دیگری از حملات سایبری ارائه نموده است. در این خصوص این سازمان حملات سایبری را به‌عنوان «روشی روانشناسی ـــ روان‌شناختی [برای] شستشوی مغزی جهت بی‌ثباتی جامعه و دولت و نیز وادار ساختن دولت برای تصمیم‌گیری در جهت منافع طرف مخالف یا دشمن تعریف نموده است.»(Oona, 2012:865). علاوه بر این، سازمان مذکور انتشار اطلاعاتی را که به ضرر نظام‌های سیاسی، اجتماعی، اقتصادی، هم‌چنین در زمینه‌های مذهبی، اخلاقی و فرهنگی سایر کشورها می‌باشد به‌عنوان یکی از تهدیدات اصلی علیه امنیت اطلاعات معرفی نموده است(Oona, 2012:865).

---

۱. Hacker

۲ shanghai

نظریه مختار در زمینه مفهوم سایبری

همان‌طور که مشـــخص گردید مهم‌ترین چالش در تعریف حمله ســـایبری فقدان معیار یا معیارهایی جهت تمییز آن با ســایر مفاهیم مجرمانه مشــابه از قبیل جرائم سایبری، تروریسم سایبری و غیره می‌باشد. بدین منظور در بند حاضر تلاش شده است با مبنا قرار دادن تعریفی که از حملات سایبری در مفهوم موسع بیان شد[1] و اعمال تغییراتی در آن، بتوان به شناختی کامل از مفهوم حملات ســایبری دســت یافت. بدین منظور لازم اســت عنصر مادی و معنوی حمله سایبری را تعیین و مورد بررسی و ارزیابی قرار داد.

الف: عنصر مادی حمله سایبری

رفتار فیزیکی مرتکب، شرایط و اوضاع و احوال تحقق رفتار مجرمانه و نتیجه رفتار مجرمانه (در صورت وجود) پیکره‌یِ «حمله سایبری» را به عنوان یک رفتار مجرمانه سایبری سبب می‌شوند.

در خصوص رفتار فیزیکی باید خاطرنشان کرد، حمله سایبری شامل مجموعه‌ای از جرائم «اخلال داده رایانه» و «اخلال سامانه رایانه‌ای» است. بنابر این از حیث رفتار فیزیکی شامل مجموعه رفتارهای پیش‌بینی شده برای تحقق جرم «اخلال داده رایانه‌ای» و «اخلال سامانه رایانه‌ای» است. مطابق ماده ۷۳۶ ق.م.ا، رفتارهای فیزیکی عبارتند از «حذف کردن»، «تخریب کردن»، «مختل کردن» و «غیر قابل پردازش کردن». عقیده پژوهش حاضر بر این است که رفتار فیزیکی در جرم «اخلال داده رایانه‌ای» هر رفتار مجرمانه در فضای سایبر است که منجر به اخلال یا غیر قابل پردازش شدن داده‌های رایانه‌ای شوند. مطابق ماده ۷۳۷ ق.م.ا رفتارهای فیزیکی عبارتند از «وارد کردن داده یا امواج الکترومغناطیسی یا نوری»، «انتقال دادن داده یا امواج الکترومغناطیسی یا نوری»، «پخش کردن داده یا امواج الکترومغناطیسی یا نوری»، «حذف کردن داده یا امواج الکترومغناطیسی یا نوری»، «متوقف کردن داده یا امواج

---

[1]. حملات ســایبری مجموعه اقدامات مجرمانه‌ای می باشــند که توسط یک سامانه رایانه‌ای علیه یک سامانه رایانه‌ای یا یک شــبکه رایانه‌ای شــخصــی یا یک وب‌ســایت به‌نحوی ارتکاب می یابد که محرمانگی، تمامیت، قابلیت دســترســی و همچنین اطلاعات ذخیره‌شده در سامانه رایانه ای را به مخاطره می‌اندازد.

الکترومغناطیسی یا نوری»، «دستکاری داده یا امواج الکترومغناطیسی یا نوری»، «تخریب داده یا امواج الکترومغناطیسی یا نوری». عقیده پژوهش حاضر بر این است که رفتار فیزیکی در جرم «اخلال سامانه رایانه‌ای» هر رفتار مجرمانه در فضای سایبر است که منجر به از کار انداختن یا مختل کردن سامانه‌های رایانه‌ای شوند.

در خصوص شرایط و اوضاع احوال تحقق جرم باید خاطرنشان کرد که موضوع جرم به ترتیب «داده رایانه‌ای» و «سامانه رایانه‌ای» است. موضوع جرم به وصف تعلق به یک گروه خاص که در پژوهش حاضر منظور از گروه خاص نهاد نظامی است و شبکه‌ای بودن داده‌ها و سامانه‌های رایانه‌ای موصوف شده است. لازم است که رفتارهای مجرمانه سایبری علیه داده‌ها و سامانه‌های نظامی (غیر قانونی) انجام شود. بنابر این در صورتی که شخص مرتکب به موجب قانون یا دستورات مقام قضایی یا اجازه از طرف افراد و مقامات مسئول و مجاز مافوق داده‌ای را حذف یا سامانه رایانه‌ای را از کار بیاندازد، عمل وی فاقد وصف جزایی است. در برخی موارد ارتش سایبری در مقام دفع تجاوز سایبری علیه داده‌ها و سامانه‌های رایانه‌ای می‌تواند با تمسک به دفاع مشروع با حمله سایبری اقدام به دفع تجاوز کنند و رفتار آنان غیر مجاز تلقی نمی‌شود. پیرامون مکان ارتکاب جرم باید گفت که فضای سایبر به عنوان مکان ارتکاب جرم « حمله سایبری» است؛ زیرا حمله سایبری خود مجموعه‌ای از جرم اخلال داده رایانه‌ای و اخلال سامانه رایانه‌ای نظامی است و چون آنان در فضای سایبر تحقق می‌یافتند، به تبع آنان، حملات سایبری نیز در فضای سایبر تحقق می‌یابند.

در مورد شخصیت مرتکب و وسیله ارتکاب جرم باید گفت که توصیف کلی مهاجمان سایبری و سلاح‌هایی که آنان در حملات خویش مورد استفاده قرار می‌دهند بسیار دشوار است؛ زیرا زمان زیادی از شکل‌گیری این عرصه نمی‌گذرد؛ اما می‌توان گفت اغلب افرادی که مهاجمان سایبری را تشکیل می‌دهند، هکرها[1] می‌باشند. هکرها معتقدند که با تجزیه و تحلیل داده‌ها و سامانه‌های رایانه‌ای و آشنایی با نحوه عملکرد آنان و به‌کارگیری دانش فناوری و اطلاعات در ساخت برنامه‌ها و نرم‌افزارهای جدید رایانه‌ای می‌توان درس‌های جالبی را در مورد داده ها و

---

[1]. Hackers

سامانه‌ای رایانه‌ای فراگرفت(بتز و استیون،۱۱:۱۳۹۱)، تا اقدامات مجرمانه‌ای علیه تمامیت داده‌ها و سامانه‌های رایانه‌ای از جمله داده‌ها و سامانه‌های رایانه‌ای نظامی در فضای سایبر به منصه‌ی ظهور برسانند.

اغلب هکرها با انگیزه‌های گوناگونی همچون اجتماعی، ایدئولوژیکی، سیاسی، نظامی، مالی و غیره دست به اقدامات مجرمانه می‌زنند؛ اما باید دانست که اغلب آنان از حوزه‌های امنیت و فناوری اطلاعات و سایر علوم رایانه‌ای وارد عرصه حملات سایبری می‌شوند و این یکی دیگر از مهم‌ترین دلایل تفکیک حملات سایبری از جرائم سایبری به اعتبار شخصیت مرتکب می-تواند تلقی شود. به‌عبارت‌دیگر، در اغلب حملات سایبری با متخصصانی در امور فناوری و اطلاعات و علوم رایانه‌ای یا افرادی مواجه‌ایم که از حداقل مهارت‌هایی در زمینه‌های یادشده برخودار می‌باشند، درحالی‌که مرتکبان جرائم سایبری الزاماً دارای چنین شاخصه‌ای نمی‌باشند.

جدول ۲. مهم‌ترین شخصیت‌های مرتکب حملات سایبری به اعتیار مهارت

ردیف	شخصیت مرتکب به اعتبار مهارت	تعاریف و ویژگی‌ها
۱	بچه اسکریپتی	بچه اسکریپتی در توصیف افرادی به کار می‌رود که هیچ مهارت خاصی برای حمله به سامانه‌های رایانه‌ای ندارند بلکه آنان عموماً برای انجام حملات خود از اسکریپت[۱]ها و ابزارهایی استفاده می‌کنند که دیگران نوشته‌اند و تنها مهارت آنان، بکار بردن این ابزارها است. بااین‌حال، این‌گونه مهاجمان اغلب در کار خود موفق‌اند، زیرا کاهش امنیت در برخی سامانه‌های رایانه‌ای و تعداد زیاد سامانه‌های متصل به اینترنت مسیر ارتکاب حمله را برای آنان هموار ساخته است(Andress,2011:11).
۲	بدافزار نویسان[۲]	بدافزار نویسان اصولاً مهاجمانی با مهارت‌های خاص تلقی می‌گردند، به‌ویژه آن‌هایی که نسخه اولیه‌ی بدافزار را

۱. Script.

۲. Malware Authors.

		می‌نویسند؛ زیرا آنان از مهارت ویژه‌ای در برنامه‌نویسی و هم‌چنین از دانشی در زمینه‌ی شناخت سیستم‌عامل[۱] و سامانه‌های رایانه برخوردار می‌باشند، در نتیجه آنان از این توانایی برخوردار می‌باشند که بدافزاری را تولید کرده و در شبکه جهانی اینترنت انتشار دهند(Andress,2011:195).
۳	هکرهای کلاه‌سیاه[۲]	از هکرهای کلاه‌سیاه به‌عنوان افراد شرور دنیای هکرها یاد می‌شود؛ زیرا برای آنان حکومت قانون ارزشی ندارد و اهمیت نمی‌دهند که در چه داده‌ها و سامانه‌های رایانه‌ای اخلال ایجاد کنند و یا چه آثارهای نامطلوبی از اقدامات خود باقی بر جای خواهند گذاشت. مهم‌ترین شاخصه‌ی هکرهای کلاه‌سیاه این است که از مهارت‌های بسیار بالایی در حملات و بهره‌برداری از سامانه‌ها و شبکه‌های رایانه‌ای هدف برخوردار می‌باشند به‌گونه‌ای که مهارت آنان در حملات سایبری و بهره‌برداری از سامانه‌های رایانه‌ای به‌مراتب از بچه اسکریپتی‌های متوسط بالاتر می‌باشد.
۴	هکرهای کلاه خاکستری[۳]	هکرهای کلاه خاکستری مابین هکرهای کلاه‌سفید[۴] و کلاه‌سیاه قرار دارند؛ زیرا آنان از یک‌سو، به‌سوی دیگر درحرکت‌اند(Andress,2011:196)، بدین معنا از آن‌جهت که کدهای ورود به سامانه‌های رایانه‌ای حفاظت‌شده را به دست آورده و به داخل آنان نفوذ می‌کند و به بسیاری از اطلاعات درون سامانه‌های رایانه‌ای دسترسی می‌یابند، همانند هکرهای سیاه تلقی می‌گردند و از سوی دیگر، بدان جهت که سبب تخریب داده‌ها یا اخلال در عملکرد سامانه‌های رایانه‌ای نمی‌گردند و همچنین ممکن است با کشف یک مشکل در

۱. Operaing-System

۲. Black-hats hacker

۳. Gray Hat Hacker

۴. White Hat Hacker

	سامانه‌های رایانه‌ای نظامی آن را به نهادهای مربوطه گزارش دهند تا برطرف سازند یا پیشنهاد همکاری برای حل این مشکل را به نهادهای نظامی می‌دهند، اقدامات آنان همانند هکرهای کلاه‌سفید تلقی می‌گردد. البته از این امر نباید غافل بود که در برخی از موارد ممکن است هکرهای خاکستری اطلاعاتی را که به دست آورده‌اند و در اختیار عموم قرار دهند که این امر فرصت مغتنمی برای هکرهای کلاه‌سیاه فراهم می‌سازد؛ زیرا آنان از اطلاعات به‌دست‌آمده توسط هکرهای کلاه خاکستری جهت حملات سایبری خود علیه داده‌ها و سامانه‌های رایانه‌ای نظامی استفاده کنند.

جدول ۳. مهم‌ترین شخصیت‌های مرتکب حملات سایبری به اعتیار انگیزه

ردیف	شخصیت مرتکب حملات سایبری به اعتیار انگیزه	تعاریف و ویژگی‌ها
۱	هکرهای سیاسی[۱]	انگیزه هکرهای سیاسی از حملات سایبری آن است که بر دیدگاه‌های مربوط به مسئله خاصی تأثیر گذارند یا از مهارت‌های خود برای حمایت از دیدگاه‌های خاص استفاده نمایند. لازم به ذکر است هکرهای سیاسی مانند هکرهای کلاه‌سیاه این توانایی را دارند تا از طریق اقدامات مجرمانه‌ای مانند هک وب‌سایت، ارسال انبوهی هرزنامه‌های الکترونیکی، حملات اختلال در سرویس‌دهی (داس)[۲] یا حملات توزیع‌شده اختلال در سرویس‌دهی (دی داس) به اهداف سیاسی خود برسند(Andress,2011:197).
۲	هکرهای میهن پرست	هکرهای میهن‌پرست نیز مشابهت زیادی با هکرهای سیاسی دارد، به‌طوری‌که می‌توان هکرهای میهن‌پرست

[۱] .Hacktivists

[۲].DOS (denial-of-service)

را زیرمجموعه‌ای از هکرهای سیاسی تلقی کرد، اما وجه تمایز آنان با هکرهای سیاسی در آن است که انگیزه‌های هکرهای میهن‌پرست اغلب به همراه نوعی ملی‌گرایی می‌باشد. همچنین فعالیت‌های آنان ممکن است در مقایسه با هکرهای سیاسی تا حدودی ماهیت دقیق‌تر و هدفمندتری داشته باشد و بسیاری از ابزارها و روش‌های مورد استفاده آنان بسیار مشابه با ابزارها و روش‌هایی است که هکرهای سیاسی مورد استفاده قرار می‌دهند؛ نظیر هک وب‌سایت و حملات (دی داس)؛ آنان عموماً در حمایت از اقدام یک کشور خاص عمل می‌کنند، هرچند که این حمایت به‌هیچ‌وجه رسمی نمی‌باشد (Andress,2011:198).

در خصوص وسیله ارتکاب جرم باید خاطرنشان کرد که سلاح‌های سایبری که مهاجم سایبری از آن‌ها برای حملات خویش بهره می‌برند، بدافزار[1] نام دارند، در واقع بدافزارها به ویروس‌ها، کرم‌ها، تروجان‌ها و برنامه‌های دیگری که با نیت اعمال خرابکارانه ایجاد می‌شوند، گفته می‌شود. به‌عبارت‌دیگر بدافزارها ابزارهای بدنیتی می‌باشند که به‌صورت مخفیانه وارد سامانه‌های رایانه‌ای می‌شوند و اعمال مخرب خاص خود را بر روی داده‌های ذخیره‌شده در سامانه‌های رایانه‌ای مورد هدف خود انجام می‌دهند که ممکن است منجر به وقوع خساراتی گردند و به علت آنکه اغلب آنان منجر به تضعیف عملکرد سامانه‌های رایانه‌ای می‌گردند، به این نام مشهور می‌باشند(داوری دولت‌آبادی،۱۳۹۳:۶).

لازم به ذکر است اکثر بدافزارها بر پایه و علیه سیستم عامل ویندوز طراحی و نوشته می‌شوند که دلیل آن وجود آسیب‌پذیری‌ها و ضعف‌های بی‌شماری است که در این نوع از سیستم‌عامل‌ها وجود دارد و اغلب افراد عادی تمامی بدافزارهای مخرب را با نام ویروس می‌شناسند و از نظر

[1]. Malware

عملکرد تفاوتی میان آن‌ها قائل نمی‌شوند، درحالی‌که شمار متنوعی از بدافزارهای مخرب در دنیای فضای سایبر وجود دارد و هرکدام نسبت به دیگری عملکردی کاملاً متفاوت دارد.

بدافزارهای رایانه‌ای دارای یک ظهور، چرخه حیات و یک افول می‌باشند. منظور از چرخه حیات بدافزار حدِفاصل میان ظهور و افول آن است. بدین معنی که ظهور یک بدافزار هنگامی است که توسط برنامه نویسان ایجاد می‌گردد و افول آن زمانی است که به‌طور کامل از روی سامانه‌های رایانه‌ای آلوده، حذف گردند. در حالت کلی می‌توان مراحل چرخه حیات یک بدافزار را این‌گونه بیان کرد که در گام اول ایده خلق بدافزار جدید شکل می‌گیرد و این ایده زمانی شکل می‌گیرد که روش و ایده‌ی جدید حمله یا سوءاستفاده از سامانه‌های رایانه‌ای کشف یا پیشنهاد گردد و در جوامع هکرها انتشار یابد. این روش‌ها آن‌قدر به اشتراک گذاشته می‌شوند و توسعه می‌یابند تا در نهایت بدافزار توسعه‌یافته، توانایی لازم جهت استفاده‌ی مهاجمان سایبری را به دست می آورد. در گام دوم پیاده‌سازی بدافزار مطرح می‌گردد؛ از دیرباز برای پیاده‌سازی یک بدافزار داشتن دانشی حرفه‌ای در زمینه‌های برنامه‌نویسی رایانه‌ای به‌ویژه زبان‌های برنامه‌نویسی نزدیک به زبان ماشین و همچنین دانشی دقیق در زمینه‌ی نحوه‌ی عملکرد سامانه‌های رایانه‌ای بسیار ضروری بود؛ اما امروزه با پیشرفت‌هایی که در زمینه‌ی ابزارهایی که جهت تولید بدافزارها مورد استفاده قرار می‌گیرند و همچنین به مدد شبکه جهانی اینترنت، هرکسی با استفاده از ابزارهای موجود و داشتن دانش برنامه‌نویسی اولیه می‌تواند یک بدافزار ایجاد نماید. در گام سوم تکرار عملکرد بدافزار مطرح می‌گردد؛ بدین معنا که پس از اینکه بدافزار جدید پیاده‌سازی و منتشر شد پیش از انجام عملیات اصلی و خرابکارانه خود، نیازمند تکرار برای یافتن میزبان‌های جدید و بالقوه می‌باشد. در گام چهارم پس ازآنکه بدافزار توانست به‌صورت موفقیت‌آمیز به سامانه رایانه‌ای میزبان نفوذ یابد، عملیات خرابکارانه خود را آغاز می‌نماید. البته گاهی اوقات بدافزارها دارای یک شرط برای فعال شدن می‌باشند و زمانی که این شرط برقرار شد عملیات خرابکارانه آغاز خواهد شد. به‌عنوان مثال برخی از مهاجمان سایبری زمان آغاز عملیات بدافزار را بر اساس آنکه کاربر کار خاصی را بر روی سامانه انجام دهد و یا تاریخ رایانه میزبان به تاریخ یا ساعت خاصی برسد، تنظیم می‌نمایند. در گام پنجم

بدافزار توسط ضد بدافزارها شناسایی و سیر افول عمر آن نیز آغاز می‌گردد. لازم به ذکر است در بیشتر موارد این مرحله پیش از مرحله چهارم و حتی گاهی پیش از مرحله سوم رخ خواهد داد که در نهایت بدافزارها توسط ضد بدافزارها پاک‌سازی می‌گردد(داوری دولت-آبادی،۱۳۹۳:۷).

بنا بر آنچه بیان شد می‌توان گفت بدافزارها سلاح‌های سایبری می‌باشند که مهاجمان سایبری از آنان در جهت حملات خود مورد استفاده قرار می‌دهند که با توجه به رشد روزافزون دنیای فناوری اطلاعات و افزایش روزانه‌ی تعداد سلاح‌های سایبری، نباید از این امر غافل بود که مهاجمان سایبری در آینده‌ای نه‌چندان دور از سلاح‌های مدرن‌تر و پیشرفته‌تری در جهت حملات خود علیه داده‌ها و سامانه‌های رایانه‌ای نظامی استفاده خواهند کرد. در پایان به‌طور اجمال به معرفی مهم‌ترین بدافزارها پرداخته می‌شود.

جدول ۴. مهم‌ترین سلاح‌های سایبری قابل استفاده در حملات سایبری

ردیف	اقسام سلاح‌های سایبری	تعاریف، ویژگی‌ها و عملکرد
۱	ویروس‌ها[۱]	ویروس‌ها یکی از مهم‌ترین بدافزارهایی قلمداد می‌شوند که مهاجمان سایبری در حملات خود از آنان بهره می‌برند. «ویروس، یک نوع بدافزار است که وقتی اجرا می‌شود، تلاش می‌کند خودش را در یک کد اجرایی دیگر کپی کند. وقتی موفق به انجام این کار شد، کد جدید، آلوده می‌شود. کد آلوده، وقتی اجرا می‌شود، به‌نوبه‌ی خود کد دیگری را می‌تواند آلوده کند. این عمل تولیدمثل یا کپی‌سازی از خود بر روی یک کد اجرایی موجود، ویژگی کلیدی در تعریف یک ویروس است»(آیوک،۱۳۹۱:۲۳).

[۱] .Viruses

۲	کرم‌ها[۱]	کرم‌ها نمونه‌ای دیگری از بدافزارهای رایانه‌ای می‌باشند که در تعریف آن بیان شده است: کرم‌ها بدافزار ناخواسته‌ای می‌باشند که مخفیانه در سامانه‌های رایانه‌ای کار گذاشته می‌شوند و به مهاجم اجازه می‌دهد که از راه دور آن را کنترل نماید. به گفته مرکز آموزش تضمین اطلاعات ارتش آمریکا «کرم، برنامه‌ای مستقل است و نیازی به فایل میزبان برای تکثیر ندارد؛ بلکه به فعل و انفعال انسانی نیاز دارد که وقتی سامانه رایانه‌ای را روشن می‌کند، زمینه‌ی فعالیت کرم مهیا شود.»[۲] مهم‌ترین ویژگی مشترک کرم‌ها این است که خود همانندساز هستند و نیاز به کدهای اجرایی دیگری ندارند(آیوک،۱۳۹۱:۲۵).
۳	اسب تروآ[۳]	اسب تراوا بدافزاری دیگری می‌باشد که در تعریف آن بیان شده است: «برنامه‌ای است که به‌ظاهر، قصد انجام یک کار بی‌خطر و موجه را دارد، اما به‌طور مخفیانه کارهای اضافی مخربی را نیز انجام می‌دهد»(آیوک،۱۳۹۱:۲۱).
۴	جاسوس‌افزار[۴]	جاسوس افزار یکی دیگر از بدافزارهای رایانه‌ای است که مهاجمان در حملات سایبری علیه محرمانگی داده‌ها از آن‌ها استفاده می‌نماید. در تعریف جاسوس‌افزار بیان شده است: «نرم‌افزاری است که اطلاعات را از یک کامپیوتر جمع‌آوری

[۱] .worms

[۲] .Isaac R. Porche III,Sollinger,jerry,mckay shawn, A Cyber Worm That Knows no Bounderies, RAND,2011.p.21.

[۳] .Trojan Horse

[۴] .spyware

		می‌کند و آن را برای شخص دیگری ارسال می‌کند.» (آیوک،۱۳۹۱:۲۷).
۵	بمب منطقی[۱]	بمب منطقی از آن دسته بدافزارهایی می‌باشد که این امکان را برای مهاجم سایبری فراهم می‌سازد که بخش راه‌انداز در آن تعبیه نماید. در تعریف بمب منطقی بیان شده است: «یک بمب منطقی کدی است که حاوی دو بخش است، بخش اول تخریب‌گر و بخش دوم راه‌انداز که عبارت است از یک شرط منطقی که ارزیابی می‌شود و کنترل می‌کند که چه زمانی تخریب‌گر اجرا شود. شرط راه‌انداز، فقط بر اساس قوه ابتکار است و می‌تواند بر مبنای شرایط محلی یا موضعی، مثل تاریخ، کاربری که وارد سیستم شده است، یا نسخه سیستم‌عامل تنظیم‌شده باشد.» (آیوک،۱۳۹۱:۲۰).

در خصوص نتیجه مجرمانه باید خاطرنشان کرد که جرم موضوع ماده ۷۳۶ و ۷۳۷ قانون مجازات اسلامی از جرائم مقید به نتیجه است. نتیجه در اولی عبارت است از: ورود خسارت به داده رایانه‌ای و در دومی عبارت است از: از کار انداختن سامانه رایانه‌ای یا ایجاد اخلال در کارکرد آن. حال با توجه به این امر که حمله سایبری شامل جرائم پیش‌گفته می‌باشد که با تحقق شرایطی دیگر جرم جدیدی را پدید می‌آورد، بنابر این نتیجه این جرم عبارت است از ورود خسارت به شبکه‌ای از داده‌های رایانه‌ای و یا از کار انداختن شبکه‌ای از سامانه‌های رایانه‌ای یا ایجاد اخلال در کارکرد آن‌ها است.

[۱] .Logic Bomb

ب: عنصر معنوی حمله سایبری

در جرم «حمله سایبری» ابتدا لازم است مرتکب بداند متعلق رفتار وی شبکه‌ای از داده‌ها و سامانه‌های رایانه‌ای نظامی است (علم به موضوع و اوصاف آن) و نداشتن اجازه از سوی مقام ذی‌الصلاح (علم به شرایط) است. منظور از سوء نیت عام این است که شخص مرتکب، قصد رفتارهای حذف کردن یا اخلال یا ... نسبت به شبکه‌ای از داده‌ها و سامانه‌های رایانه‌ای نظامی داشته باشد. جرم مذکور یک جرم مقید است و نیاز به حصول نتایج ورود خسارت به شبکه‌ای از داده‌های رایانه‌ای، از کار انداختن شبکه‌ای از سامانه‌های رایانه‌ای یا ایجاد اخلال در کارکرد آن‌ها دارد.

دارد. مطابق ذیل ماده ۱۴۴ قانون مجازات اسلامی شخص نظامی باید قصد موارد پیش‌گفته یا علم به وقوع آن‌ها را داشته باشد.[۱]

پرسشی که در این قسمت قابل‌طرح می‌باشد این است که هرگاه یک حمله سایبری علیه سامانه‌های رایانه‌ای به‌گونه‌ای ارتکاب یابد که نتایج فیزیکی نیز در فضای واقعی به همراه داشته باشد، آیا برای محکومیت مهاجم سایبری در فضای واقعی احراز سوءنیت او لازم است؟ به‌عبارت‌دیگر هنگامی‌که یک حمله سایبری علاوه بر نقض قوانین سایبری منجر به نقض قوانین سنتی گردد برای محکومیت مهاجمان سایبری احراز دو سوءنیت خاص ضروری می‌باشد؟ به‌عنوان مثال تصور نمایید یک حمله سایبری علیه سامانه‌های کنترلی، آفندی یا پدافندی نظامی به نحوی ارتکاب یابد که باعث انفجار در محیط اطراف شود و بسیاری از افراد جان خود را از دست بدهند و باعث تخریب استحکامات و بناهای موجود در مجاور محل شود. حال سؤال آن است احراز قصد قتل و تخریب مهاجمین نیز ضروری می‌باشد؟ به نظر می‌رسد در این‌گونه موارد که توسط یک حمله سایبری یک نتیجه در فضای سایبر و یک نتیجه در فضای واقعی حاصل می‌گردد. لازم است میان قصد نتیجه در فضای سایبر و قصد نتیجه در

---

[۱]. ماده ۱۴۴ ق.م.ا مقرر می‌دارد: «در تحقق جرائم عمدی علاوه بر علم مرتکب به موضوع جرم، باید قصد او در ارتکاب رفتار مجرمانه احراز گردد. در جرائمی که وقوع آن‌ها بر اساس قانون منوط به تحقق نتیجه است، قصد نتیجه یا علم به وقوع آن نیز باید محرز شود».

فضای فیزیکی تمایز قائل شد و در نتیجه آن، احراز دو سوءنیت مجزا لازم و ضروری باشد. بنابراین در مثال فوق برای محکومیت مهاجمان سایبری تحت عنوان مجرمانه‌ی اخلال در عملکرد سامانه‌های رایانه‌ای کنترلی لازم است قصد اولیه او که در فضای سایبر تحقق می یابد یعنی اخلال در عملکرد سامانه‌های رایانه‌ای کنترلی، پدافندی یا آفندی نظامی یا علم به وقوع آن احراز گردد و قصد تبعی او در مورد نتیجه دوم که در فضای واقعی تحقق می یابد یعنی به قتل رساندن جان افراد و تخریب استحاکامات و بناهای نظامی یا علم به وقوع آن با توجه به ذیل ماده ۱۴۴ ق.م.ا احراز گردد. به نظر می رسد در صورت احراز قصد اولیه و تبعی، رفتار ارتکابی مهاجمین سایبری مشمول ماده ۱۳۴ ق.م.ا قرار می‌گیرد.[1] به‌طورکلی نتیجه می‌شود

---

[1]. ماده ۱۳۴ ق.م.ا (اصلاحی سال ۱۳۹۹) مقرر می‌دارد:« در تعدد جرائم تعزیری، تعیین و اجرای مجازات به شرح زیر است:

الف- هرگاه جرائم ارتکابی مختلف نباشد، فقط یک مجازات تعیین می‌شود و در این صورت، دادگاه می‌تواند مطابق ضوابط مقرر در این ماده که برای تعدّد جرائم مختلف ذکرشده، مجازات را تشدید کند.

ب- در مورد جرائم مختلف، هرگاه جرائم ارتکابی بیش از سه جرم نباشد، حداقل مجازات هر یک از آن جرائم بیشتر از میانگین حداقل و حداکثر مجازات مقرر قانونی است.

پ- چنانچه جرائم ارتکابی مختلف، بیش از سه جرم باشد، مجازات هر یک، حداکثر مجازات قانونی آن جرم است. در این صورت دادگاه می‌تواند مجازات هر یک را بیشتر از حداکثر مجازات مقرر قانونی تا یک‌چهارم آن تعیین کند.

ت- در تعدّد جرائم درجه هفت و درجه هشت با یکدیگر، حسب مورد مطابق مقررات این ماده اقدام می‌شود و جمع جرائم درجه هفت و درجه هشت با درجه شش و بالاتر سبب تشدید مجازات جرائم اخیر نمی‌شود. در جمع این جرائم با جرائم درجه شش و بالاتر، به طور جداگانه برای جرائم درجه هفت و درجه هشت مطابق این ماده تعیین مجازات می‌شود و در هر صورت مجازات اشد قابل اجراء است.

ث- در هر یک از بندهای فوق، فقط مجازات اَشد مندرج در دادنامه قابل اجراء است و اگر مجازات اَشد به یکی از علل قانونی تقلیل یابد یا تبدیل شود یا به موجبی از قبیل گذشت شاکی خصوصی، نسخ مجازات قانونی یا مرور زمان غیرقابل‌اجراء گردد، مجازات اَشد بعدی اجراء می‌شود و در این صورت میزان مجازات اجراءشده قبلی در اجرای مجازات اَشد بعدی محاسبه می‌شود. آزادی مشروط، تعلیق اجرای مجازات و عفو در حکم اجراء است.

ج- در هر مورد که مجازات قانونی فاقد حداقل یا ثابت باشد، اگر جرائم ارتکابی بیش از سه جرم نباشد دادگاه می تواند تا یک ششم و اگر بیش از سه جرم باشد تا یک چهارم به اصل آن اضافه کند.

چ- در صورتی که در جرائم تعزیری، از رفتار مجرمانه واحد، نتایج مجرمانه متعدد حاصل شود، مرتکب به مجازات جرم اَشد محکوم می‌شود.

ح- هرگاه در قانون برای جرمی یکی از مصادیق مجازات‌های مندرج در مواد (۲۳) یا (۲۶) این قانون به‌عنوان مجازات اصلی مقرر شده باشد، آن مجازات در هر صورت اجراء می‌شود، حتی اگر مربوط به مجازات غیراَشد باشد. همچنین اگر

که سوءنیت خاص اولیه تمامی حملات تمامیت شبکه‌ای از سامانه‌های رایانه‌ای و داده‌های ذخیره‌شده در آن می‌باشد.

نکته دیگری که ذیل مباحث رکن معنوی حملات سایبری لازم است بررسی شود انگیزه‌ی مهاجم سایبری است. در تعریف انگیزه به طور عام بیان شده است که انگیزه کوشش درونی و میل نهانی است که انسان را به‌سوی عملی خاص رهنمون می‌شود لذا منظور از انگیزه در حقوق کیفری به طور خاص، هدف نهایی‌ای است که مرتکب به دنبال دستیابی به آن است و تفاوت آن با سوءنیت خاص آن است که انگیزه به تعدد افراد متعدد است درحالی‌که سوءنیت خاص در تمامی افراد یکسان است(الهام و برهانی،۱۳۹۴:۱۸۹). ضروری نمی‌باشد انگیزۀ مهاجمان سایبری را معطوف به انگیزه‌های سیاسی، امنیتی یا ملی نماییم؛ اما می‌توان گفت در برخی موارد انگیزه مهاجم سایبری می‌تواند سبب تغییر عنوان مجرمانه حمله سایبری به سایر عناوین مجرمانه سایبری گردد.

پس از واکاوی عناصر مادی و معنوی « حمله سایبری» علیه داده‌ها و سامانه‌های رایانه‌ای نظامی و با الهام از ماده ۷۳۶ ق.م.ا و ۷۳۷ قانون مجازات اسلامی می‌توان آن را بدین نحو در نظر گرفت:

«هر کس که به طور غیر مجاز در فضای سایبر مرتکب هـر یـک از اعمال زیر علیه شبکه‌ای از داده‌ها و سامانه‌های رایانه‌ای نظامی شود، در صورتی که مجازات وی مشمول یکی از حدود مقرر در کتاب دوم قانون مجازات اسلامی نباشد، حسب مورد با افزایش یک یا دو درجه به مجازات‌های پیش‌بینی شده در قانون مجازات جرائم نیروهای مسلح محکوم می‌شود:

۱ .اخلال در شبکه‌ای از داده‌ها یا سامانه‌های رایانه‌ای نظامی

مجازات اَشد وفق ماده (۲۵) این قانون، فاقد آثار تبعی و مجازات خفیف‌تر دارای آثار تبعی باشد، علاوه بر مجازات اصلی اَشد ، مجازات تبعی مزبور نیز اجراء میشود

خ- در تعدّد جرم در صورت وجود جهات تخفیف مجازات برای هر یک از جرائم، مطابق مواد (۳۷) و (۳۸) این قانون اقدام می‌شود.

د- در صورتی که مجموع جرائم ارتکابی در قانون عنوان مجرمانه خاصی داشته باشد، مقررات تعدّد جرم اِعمال نمی‌شود و مرتکب به مجازات مقرر در قانون محکوم می‌شود».

۲ .تخریب داده‌های ذخیره‌شده در شبکه‌ای از سامانه‌های رایانه‌ای نظامی. تبصره- گروه خاص در تعریف مذکور عبارت است از سازمان‌ها، نهادها، موسسات و ... است».

تعامل مفهوم حمله سایبری با جرم سایبری

حال برای پی بردن به این امر که در قالب کدام عناوین مجرمانه در کنوانسیون بوداپست و قانون جرائم رایانه‌ای می‌توان به مقابله کیفری با حملات سایبری پرداخت، باید گفت در یک تقسیم می‌توان جرائم سایبری را به دو دسته‌ی جرائم سایبری موضوع-محور و جرائم سایبری وسیله-محور تقسیم‌بندی نمود. جرائم سایبری موضوع-محور جرائمی سایبری می‌باشند که در آن داده‌ها و سامانه‌های رایانه‌ای هدف یا موضوع جرم می‌باشند به آنان «جرائم سایبری محض» نیز گفته می‌شود. از آن‌جا که در حملات سایبری هدف حمایت از تمامیت داده‌ها و سامانه‌های رایانه‌ای می‌باشد و در جرائم سایبری محض نیز موضوع جرم داده‌ها و سامانه‌های رایانه‌ای و هدف حمایت از آنان می‌باشد، می‌توان «حملات سایبری» را بر اساس «جرائم سایبری» محض این‌گونه تعریف نمود: حملات سایبری، جرائم سایبری محضی می‌باشند که در زیرفضای سایبری میان سامانه‌های رایانه‌ای با یکدیگر ارتکاب می‌یابند.[۱] در مقابل، جرائم سایبری وسیله محور، جرائم سایبری می‌باشند که در آن سامانه‌های رایانه‌ای وسیله‌ی ارتکاب جرم می‌باشند؛ مانند کلاهبرداری رایانه‌ای، نشر اکاذیب از طریق سامانه‌های رایانه‌ای.[۲]

رفتارهای مجرمانه در جرائم رایانه ای موضوع – محور همانند حملات سایبری مجموعه‌ای از اقدامات مجرمانه‌ای در فضای سایبر است که علیه تمامیت داده‌ها و سامانه‌های رایانه‌ای ارتکاب می‌یابد مانند رفتار مرتکب در تخریب داده ناشی از جرائم سایبری (ارتکاب تخریب رایانه‌ای در زیرفضای سایبری میان کاربر با سامانه رایانه‌ای) حذف یا تغییر است و در تخریب

---

[۱] کنوانسیون بوداپست و قانون‌گذار ایران بر اساس آنکه عملیات مجرمانه سایبری در زیرفضای سایبری میان کاربر با سامانه رایانه‌ای ارتکاب یابند یا در زیرفضای سایبری میان سامانه رایانه‌ای؛ تفکیکی قائل نشده و برای تمامی آنان از عنوان واحد جرائم سایبری استفاده نموده‌اند. درحالی‌که نوشتار حاضر بر این عقیده می باشد که جرائم سایبری بر خلاف حملات سایبری در زیر فضای سایبری میان کاربر با سامانه رایانه ای ارتکاب می یابد.

[۲]. ماده ۷۴۵ ق.م.ا (تعزیرات)

داده رایانه‌ای ناشی از حملات سایبری (ارتکاب تخریب در زیرفضای سایبری میان سامانه‌های رایانه‌ای با یکدیگر) نیز رفتار حذف یا تغییر در داده‌ها است.

در خصوص شرایط و اوضاع و احوال میان جرائم سایبری موضوع-محور با حملات سایبری محل امعان نظر است که موضوع جرم در حملات سایبری مانند جرائم سایبری موضوع- محور داده‌ها و سامانه‌های رایانه‌ای می‌باشند؛ اما وسیله‌ی ارتکاب در حملات سایبری لزوماً سامانه رایانه‌ای می‌باشد، درحالی‌که در جرائم سایبری موضوع-محور چنین الزامی وجود ندارد مانند اثرات مخرب ناشی از انتشار امواج الکترومغناطیسی بر روی داده‌ها و سامانه‌های رایانه‌ای؛ زیرا امواج الکترومغناطیسی لزوماً توسط سامانه‌های رایانه‌ای تولید نمی‌گردند، بلکه ممکن است توسط ابزارهای الکترونیکی تولید گردند که نتوان آنان را از آن‌جهت که توانایی دریافت ورودی و پردازش خودکار داده و تولید خروجی را ندارند، مصداق سامانه رایانه‌ای تلقی نمود. به‌عنوان نمونه می‌توان به انتشار امواج حاصل از تخلیه بارهای الکترونیکی ابرها که توسط صاعقه انجام می‌گیرد، اشاره نمود، چرا که ممکن است منجر به تخریب محتوای بسته‌های اطلاعاتی در حال انتقال گردد، یا پالس‌های الکترونیکی که توسط ابزارهای الکترونیکی تولید می‌گردد مانند ارسال پارازیت‌ها که توانایی تخریب داده‌ها را دارند همچنین باید توجه داشت که نحوه‌ی اثرگذاری امواج الکترومغناطیسی با نحوه‌ی اثرگذاری سامانه‌های رایانه‌ای که در جهت اقدامات مجرمانه بکار گرفته می‌شوند کاملاً متفاوت می‌باشند؛ زیرا اثرگذاری مخرب امواج الکترومغناطیسی بر روی جنس داده‌های رایانه‌ای متشکل از بارهای مغناطیسی و جریان‌های الکتریکی، می‌باشد. برای مثال با انتشار امواج مغناطیسی نمی‌توان مرتکب عناوین مجرمانه ای مانند «دسترسی غیرمجاز» به سامانه رایانه‌ای یا «سرقت رایانه‌ای» شد.

دیگری بودن سامانه رایانه‌ای یا همان شرط وجود حداقل دو سامانه رایانه‌ای در حملات سایبری لازم و ضروری می‌باشد، درحالی‌که در جرائم سایبری موضوع- محور وجود حداقل دو سامانه رایانه‌ای لازم و ضروری نمی‌باشد. به‌عبارت دیگر در جرائم سایبری موضوع- محور کاربر توسط یک سامانه رایانه‌ای اقدامات مجرمانه‌ای را علیه همان سامانه رایانه‌ای مرتکب می شود. به‌عنوان شاهد مثال؛ شخص (الف) سامانه رایانه‌ای شخص (ب) را در اختیار دارد و داده‌های

متعلق به شخص (ب) را حذف می‌نماید، در این صورت می‌توان گفت که کاربر توسط یک سامانه رایانه‌ای مرتکب جرم تخریب داده علیه داده‌های ذخیره شده در همان سامانه رایانه‌ای شده است.

مکان و فضای ارتکاب جرائم سایبری موضوع-محور همانند حملات سایبری نیز فضای سایبر است با این تفاوت که حملات سایبری تنها در زیرفضای سایبری میان سامانه‌های رایانه‌ای با یکدیگر ارتکاب می‌یابند؛ اما جرائم سایبری محض در زیرفضای سایبری میان کاربر با سامانه رایانه‌ای تحقق می‌یابند.

در نهایت از آنجایی‌که نتایج رفتارهای مجرمانه ارتکابی در جرائم سایبری محض محدود به نقض تمامیت داده‌های رایانه‌ای و سامانه‌های رایانه‌ای است ، نتایج مجرمانه در جرائم سایبری محض نیز معادل با حملات سایبری می‌باشند.

ویژگی‌های حمله سایبری و گستردگی آثار آن

الف- کم‌رنگ شدن نقش جغرافیا

یکی از ویژگی‌های بستر حملات سایبری به شمار می‌آید. این امر بر کسی پوشیده نیست شبکه جهانی اینترنت[۱]، به عنوان وسیع‌ترین بستر حملات سایبری، تأثیر به‌سزایی در کم‌رنگ شدن نقش جغرافیا داشته و این امکان را برای مهاجمان سایبری فراهم نموده است که از توانایی‌های لازم برای عبور از محدوده‌ی مرزهای جغرافیایی خود جهت رسیدن به اهداف اصلی خود برخوردار گردند(عظیمی و خشنودی،۱۳۹۵، ۱۶۴). این امر موجب شده است نهادهای دولتی به‌صورت غیررسمی از حملات سایبری ارتکاب یافته‌ی از آن سوی مرزها حمایت نمایند و موجب حملات سایبری منسجم‌تر و هدفمندتری شوند تا نتایج بسیار زیان‌باری را سبب گردند.

---

[۱] . Internet

ب- صرف زمان کوتاه و هزینه کم

صرف زمان کوتاه و هزینه کم یکی دیگر از امکاناتی می باشد که بستر حملات سایبری برای مهاجمان سایبری فراهم می‌آورد تا در مدت زمانی کوتاه و با کم‌ترین هزینه بیشترین خسارت را وارد آورند. در برخی از موارد که مهاجمان سایبری برای ارتکاب حملات خود نیاز به چندین هزار سامانه‌ی رایانه‌ای دارند، آنان از این توانایی برخوردار می باشند که بدون تهیه‌ی چندین هزار سامانه رایانه ای تنها با ایجاد یک بدافزار و انتشار آن در شبکه ی جهانی اینترنت سبب گردند که سامانه‌های رایانه‌ای متصل به شبکه جهانی اینترنت را تحت فرمان و کنترل خود درآورده و از آنان جهت حملات خود استفاده نمایند. نمونه‌ی بارز آن حملات سایبری«دی داس»[۱] می باشند.

ج- ناشناس ماندن مرتکب

بستر حملات سایبری از لحاظ ساختاری به‌گونه‌ای نامتمرکز می‌باشد، این ماهیت ساختاری، توجه بسیاری از مهاجمان سایبری را به‌سوی خود جلب نموده است؛ زیرا این توانایی و قابلیت را به آنان داده است، بدون آن‌که اثر یا نامی از خود باقی بر جای گذارند حملات سایبری خود را متوجه اهداف خود نمایند(Lord, K.M., & Sharp,2011, pp.20.28) .

د- تأثیرگذاری شگرف

تاثیرگذاری شگرف یکی دیگر از ویژگی‌های بستر حملات سایبری می‌باشد. ماهیت خاص فضای سایبر سبب اتکای روزافزون کاربران، شرکت‌ها، نهادهای دولتی و غیره به فضای سایبر شده است. این اتکا و وابستگی تا جایی پیش رفته است که اکثر منابع کاربران، سازمان‌ها و

---

[۱] . DDOS (distributed denial-of-service)

ر.ک به دسترر، جورج و امی آلیز و الکس هرواتین، حملات اختلال در سرویس دهی (دی داس): پیشگیری، تشخیص نفوذ و کاهش تاثیرات، ترجمه مؤسسه فرهنگی و مطالعات و تحقیقات بین المللی ابرار معاصر امنیت و جنگ سایبری۲ ، تهران،۱۳۹۱.

غیره در فضای سایبر قرار گرفته است. وجود منابع اطلاعاتی کاربران، سازمان‌ها و شرکت‌ها در فضای سایبر و همچنین زیرساخت‌ها و منابع حیاتی یک کشور در این فضا نظر مهاجمان سایبری را به سوی خود معطوف کرده است تا اعمال مجرمانه خود را علیه منابع اطلاعاتی که در فضای سایبر قرار دارند به منصه‌ی ظهور برسانند و بر دامنه‌ی خسارات ناشی از رفتارهای مجرمانه‌ی خویش بیافزایند (Lord, K.M., & Sharp,2011, pp. 20-28). همچنین موجب آشکار شدن نقاط ضعف زیرساخت های حیاتی یک کشور در فضای سایبر گردند(حسن بیگی، ۱۳۸۴، ۳).

روش‌شناسی تحقیق

تحقیق حاضر یک تحقیق کیفی است که از نظر هدف؛ کاربردی از حیث ابزار تحقیق، اسنادی و کتابخانه‌ای، از حیث روش تجزیه و تحلیل، توصیفی- تحلیلی و از حیث رویکرد مطالعه، از نوع تطبیقی بوده و مبتنی بر استنتاج مؤلفان از منابع و متون است. اطلاعات گردآوری شده شامل قوانین و مقررات از جمله قانون مجازات اسلامی و قانون مجازات جرائم نیروهای مسلح و همچنین کنوانسیون جرائم سایبری اتحادیه اروپا در خصوص جرائم سایبری علیه تمامیت داده‌ها و سامانه‌های رایانه‌ای نظامی بوده است.

یافته‌های تحقیق

از آنجایی که در اسناد بین‌المللی و قوانین فعلی ایران حمله سایبری جرم انگاری نشده است، با توجه به مقایسه‌ای که میان مفهوم حمله سایبری و جرم رایانه‌ای محض انجام شد در شرایط فعلی برای مقابله‌ی کیفری نسبت به حملات سایبری علیه داده‌ها و سامانه‌های رایانه‌ای نظامی لازم است جرائم رایانه‌ای محض را براساس فضا و مکان ارتکاب جرم به دو دسته تقسیم نموده و عنوان حمله سایبری بر جرایم رایانه‌ای محضی که در زیرفضای سایبری میان سامانه-های رایانه‌ای با یکدیگر ارتکاب می‌یابند، حمل نمود. در این‌صورت در پرتوی کنوانسیون بوداپست و قانون جرائم رایانه‌ای می‌توان در قالب اخلال در داده‌های رایانه‌ای نظامی و اخلال

در سامانه‌های رایانه‌ای نظامی به مقابله کیفری با حملات سایبری علیه داده‌ها و سامانه‌های رایانه‌ای نظامی پراخت.

۴-۱-مقابله کیفری با حملات سایبری علیه تمامیت داده‌های رایانه‌ای نظامی

در حقوق کیفری تخریب سنتی به معنای «وارد ساختن لطمه عمدی بر تمامیت فیزیکی شیء یا مال متعلق به دیگری» می‌باشد(گلدوزیان، ۳۹۴:۱۳۸۳)؛ اما از آنجایی‌که موضوع جرم تخریب سنتی مال فیزیکی و واقعی بود و تخریب اموال غیرملموس، مانند داده‌های رایانه‌ای را دربرنمی‌گرفت، موجب تصویب کنوانسیون بوداپست و قانون جرائم رایانه‌ای در این زمینه شد تا خلأ موجود برطرف گردد. در این راستا بند ۶۰ گزارش توجیهی کنوانسیون بوداپست مقرر می‌دارد: «هدف از وضع این ماده [مختل کردن داده[۱]] حمایت از داده‌ها و برنامه‌های رایانه‌ای همانند اشیاء مادی[۲] در برابر آسیب‌های عمدی است. منافع قانونی حمایت‌شده در اینجا تمامیت[۳] و اجرا یا کاربری مناسب از داده‌های ذخیره‌شده و برنامه‌های رایانه‌ای است». در جهت نیل به این هدف در بند ۱ ماده ۴ کنوانسیون بوداپست مقررشده است: «هر یک از اعضاء باید به‌گونه‌ای اقدام به وضع قوانین و سایر تدابیر کنند که در صورت لزوم بر اساس حقوق داخلی خود، صدمه زدن، پاک کردن، خراب کردن، تغییر دادن یا توقف کردن داده‌های رایانه‌ای را که به‌طور عمدی و بدون حق انجام می‌شود، جرم‌انگاری کنند». بند ۶۱ گزارش توجیهی در تبیین اصطلاحات «آسیب رساندن»[۴]، «تخریب»[۵]، «حذف»[۶]، «متوقف کردن»[۷] و «تغییر»[۸] مقرر می‌دارد: «آسیب رساندن» و «تخریب» به‌عنوان اعمال هم‌پوشاننده‌ای هستند که به‌طور خاص به تغییر منفی تمامیت یا محتوای اطلاعات داده‌ها و برنامه‌ها اشاره دارند.

---

۱ Data Interference

۲ Corporeal Objects

۳ Integrity

۴ Damaging

۵ Detoriorating

۶ Deletion

۷ Suppression

۸ Alteration

«حذف» داده‌ها معادل از بین بردن یک شیء مادی است. این عمل آن‌ها را از بین می‌برد تا قابل‌فهم نباشند. «متوقف کردن» داده‌های رایانه‌ای به معنای هر فعلی است که از دسترس‌پذیری داده‌ها برای شخصی که به رایانه یا حامل داده‌ای که داده‌ها بر روی آن ذخیره‌شده و به آن‌ها دسترسی دارد، جلوگیری می‌کند یا پایان می‌بخشد. «تغییر» به معنی دست‌کاری داده‌های موجود است. بنابراین واردکردن کدهای مغرضانه، مانند ویروس‌ها[۱] اسب‌های تروا[۲] مشمول این بند می‌شود، زیرا به تغییر داده‌ها منجر می‌گردد»(جلالی فراهانی،۱۳۹۵:۳۱). همچنین مطابق با بند (۱) ماده ۴ کنوانسیون بوداپست لازم است اعمال مجرمانه «بدون حق» ارتکاب یابند تا مصداق عنوان مجرمانه تخریب داده قرار گیرند. در این راستا در بند ۶۲ گزارش توجیهی مقررشده است: «فعالیت‌های معمول ذاتی معماری شبکه‌ها یا اقدامات تجاری یا عملیاتی معمول، مانند آزمون حفاظت امنیتی سامانه رایانه‌ای مجاز شمرده توسط مالک یا متصدی یا پیکربندی[۳] دوبارهٔ سیستم‌عامل به هنگامی‌که متصدی نرم‌افزار جدیدی دریافت می‌کند (نرم‌افزاری که دسترسی به اینترنت را فراهم می‌کند و برنامه‌های مشابه نصب‌شده پیشین را از کار می‌اندازد)، همگی به‌حق بوده و درنتیجه طبق این ماده جرم محسوب نمی‌شوند. تغییر داده ترافیک به‌منظور تسهیل ارتباطات ناشناس مانندکارکرد سامانه‌های باز ارسال نامه[۴] ناشناس یا تغییر داده‌ها با هدف حفاظت از ارتباطات (رمزگذاری)[۵] اساساً باید در راستای حمایت مشروع از حریم خصوصی مدنظر قرار گیرند و در نتیجه به‌حق تلقی شود. با این‌حال، ممکن است کشورهای عضو بخواهند برخی سوءاستفاده‌های مربوط به ارتباطات ناشناس را جرم‌انگاری کنند، همانند تغییر اطلاعات سر صفحهٔ بسته[۶] جهت پنهان کردن هویت مرتکب جرم»(جلالی فراهانی،۱۳۹۵ :۳۲-۳۱). همچنین مطابق بند (۱) ماده ۴

---

[۱] Viruses

[۲] Trojan Horses

[۳] Configuration

[۴] Remailer

[۵] Encryption

[۶] Header

کنوانسیون بوداپست هریک از اعمال مذکور از قبیل «آسیب رساندن»، «تخریب»، حذف و غیره باید به‌طور «عمدی» ارتکاب یابند که در بند ۶۳ گزارش توجیهی نیز بدان اشاره شده است. [۱]

بند (۲) ماده ۴ کنوانسیون بوداپست مقرر می‌دارد: «اعضاء می‌توانند حق جرم‌انگاری افعال مندرج در بند یک را درجایی که صدمه شدیدی وارد می‌شود اعمال کنند»(جلالی فراهانی،۱۳۹۵ :۳۲-۳۱). که در جهت اعمال شرط «صدمه شدید» توسط هر یک از دول اعضاء بند ۶۴ گزارش توجیهی مقرر می‌دارد: «در بند (۲) به اعضا اجازه داده‌شده است نسبت به این جرم حق شرط قائل شوند و مقرر کنند این رفتار به صدمه شدید منجر شود. تفسیر آنچه «صدمه شدید» را تشکیل می‌دهد به قانون‌گذار ملی واگذارشده است. چنانچه اعضا می‌خواهند از این حق بهره‌برداری کنند باید تفسیر خود را به دبیر کل شورای اروپا ارائه دهند.»

مطابق با بندهای (۱) و (۲) ماده ۴ کنوانسیون بوداپست و گزارش توجیهی پیرامون آن می‌توان گفت از آنجاکه حملات سایبری «عمدی» و« بدون حق» ارتکاب می‌یابند و قابلیت آن را دارند که منجر به صدمه زدن، پاک کردن، خراب کردن، تغییر دادن یا توقف کردن داده‌های رایانه‌ای گردند، می‌توان در صورت تحقق هریک از نتایج ذکرشده آن را مصداق ماده ۴ کنوانسیون بوداپست تلقی نمود.

در حقوق ایران نیز قانون‌گذار ایران با تصویب ماده ۷۳۶ ق.م.ا (تعزیرات) که مقرر می‌دارد: «هر کس به‌طور غیرمجاز داده‌های دیگری را از سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده حذف یا تخریب[۲]یا مختل[۳] یا غیرقابل‌پردازش کند به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون (۰۰۰. ۰۰۰. ۱۰) ریال تا چهل میلیون (۰۰۰. ۰۰۰. ۴۰) ریال یا

---

۱. بند ۶۳: «مجرم باید عمداً مرتکب جرم شده باشد» ر.ک: جلالی فراهانی، امیرحسین(۱۳۹۵)، کنوانسیون جرائم سایبر و پروتکل الحاقی آن، تهران، چاپ دوم، نشر خرسندی.

۲. تخریب؛ از میان بردن قسمتی یا تمام یک‌چیز. ر.ک به: عالی پور، حسن(۱۳۹۳)، حقوق کیفری فناوری اطلاعات، تهران، چاپ سوم، انتشارات خرسندی.

۳. اخلال؛ پدید آوردن آشفتگی و ناتوانی در کارکرد یک‌چیز است. ر.ک به: همان.

هر دو مجازات محکوم خواهد شد.» اقدام به جرم انگاری عنوان مجرمانه تخریب داده‌های رایانه‌ای نمود تا خلأ پیش‌گفته در قوانین سنتی موجود را برطرف سازد.

برای آنکه مشخص گردد یک حمله سایبری تحت چه شرایطی مصداق عنوان تخریب داده به‌ویژه ماده ۷۳۶ ق.م.ا (تعزیرات) قرار می‌گیرد. لازم است عنصر مادی حملات سایبری با عنصر مادی ماده مذکور تعیین و با یکدیگر مقایسه شوند.

رفتار فیزیکی- در ماده ۷۳۶ ق.م.ا مقنن از رفتارهای فیزیکی «حذف کردن»، «تخریب کردن»، «مختل کردن» و «غیر قابل پردازش کردن» استفاده کرده است که روی هم رفته، در زیر دو رفتار «تخریب» و «اخلال» گرد هم می‌آیند؛ زیرا حذف داده، همان تخریب است خواه کلی باشد و خواه جزئی و غیر قابل پردازش کردن نیز گونه‌ای از اخلال است. شایان ذکر است دو رفتار «حذف کردن» و «تخریب کردن»، نسبت به خود داده ارتکاب می‌یابد و دو رفتار «مختل کردن» و «غیر قابل پردازش کردن» نسبت به کار کرد و توانایی داده رخ می-دهد(عالی‌پور،۱۳۹۳:۲۲۰). حذف داده به معنای برداشتن جزئی و کلی داده از جایگاه خویش است، هر چند با بازیابی بتوان به آن داده دست یافت. اختلال در داده به معنای ایجاد آشفتگی و نابسامانی در داده‌ها است(بابایی،۱۳۹۸:۱۱۱). بدین معنا که بخشی از داده رایانه‌ای پردازش نمی‌شود. غیرقابل پذیرش کردن داده، برخی آن را به معنای از کار انداختن داده یا سلب کارایی و کارکرد آن تعریف کرده‌اند(عالی‌پور،۱۳۹۳:۲۲۰) و برخی دیگر انجام تغییراتی دانسته‌اند که علی الرغم وجود داده‌ها، آن‌ها را در سامانه رایانه‌ای غیر قابل پردازش می-سازد(محمدنسل، ۱۳۹۵:۸۴).

برخی معتقدند که اختلال یا غیر قابل پردازش کردن را نمی‌توان به عنوان رفتار مجرمانه به حساب آورد، بلکه به عنوان نتیجه‌ای است که از برخی رفتارها همانند تخریب جزئی داده‌ها ممکن است پدید آید(بابایی، ۱۳۹۸:۱۱). به نظر می‌رسد دو رفتار «حذف کردن» و «تخریب کردن» ناظر بر موجودیت خودِ داده و محتوای درون است. مانند حذف یک سند الکترونیکی یا ناخوانا کردن بخشی از سند الکترونیکی به شرط آن‌که مصداق جرم جعل رایانه‌ای قرار نگیرد. در واقع در دو مثال قبل داده‌ها پردازش می‌شوند، ولی تخریب شده‌اند. اما «مختل

شدن» یا «غیر قابل پردازش شدن» داده ناظر بر مرحله‌ی پردازش یا عملکرد داده است و نتایج حاصل از هر رفتاری در فضای سایبر هستند. در این صورت «مختل شدن» به معنای عدم پردازش بخشی از داده است و «غیر قابل پردازش شدن» به معنای عدم پردازش تمام داده است.

در خصوص شرایط و اوضاع و احوال ماده مذکور ابتدا باید بیان داشت موضوع جرم، داده است که باید موصوف به تعلق نهادهای نظامی باشد. خواه مالیت داشته باشد، خواه نداشته باشد، خواه استنادپذیر باشد و خواه نباشد.[1] که مطابق بند (ج) ماده ۷۵۴ قانون مجازات اسلامی زمانی‌که داده‌های متعلق به دولت یا نهادها و مراکز ارائه دهنده خدمات باشد مرتکب بیش از دو سوم حداکثر یک یا دو مجازات مقرر در ماده ۷۳۶ ق.م.ا محکوم خواهد شد.

وسیلهٔ ارتکاب جرم تخریب داده می‌تواند از طریق سامانه‌های رایانه‌ای به‌صورت نرم‌افزاری (مانند فرمان حذف داده‌ها) یا داده‌ها توسط انتشار امواج حذف و غیرقابل‌پردازش گردند که به‌اصطلاح «پارازیت» نامیده می‌شود و یا به‌وسیلهٔ برنامه‌های نرم‌افزاری مثل ویروس، کرم رایانه‌ای باشد تا برنامه‌ها و داده‌ها غیر پردازش گردند(عزیزی،۱۱۸:۱۳۹۴). در مورد حملات سایبری باید توجه داشت تنها حالتی را شامل می‌گردند که عمل تخریب یا غیرقابل‌پردازش داده‌ها توسط یک سامانه رایانه‌ای علیه داده‌های ذخیره‌شده در دیگر سامانهٔ رایانه‌ای ارتکاب یابد؛ بنابراین هرگاه تخریب یا غیرقابل‌پردازش کردن داده‌ها توسط انتشار امواج الکترومغناطیسی ناشی از وسایل و ابزارهایی صورت گیرد که عنوان سامانه رایانه‌ای بر آنان صدق نمی‌کند از شمول عنوان حمله سایبری خارج بوده ؛ اما همان‌طور که بیان شد با وجودآنکه انتشار امواج الکترومغناطیسی لزوماً توسط سامانه‌های رایانه‌ای ارتکاب نمی‌یابند؛ اما از آنجا که از برخی ویژگی‌های حملات سایبری از قبیل کم‌رنگ بودن نقش جغرافیا، عدم شناسایی مرتکبان، تأثیرگذاری شگرف و غیره برخوردار می‌باشند شایسته است انتشار امواج

---

[1] رفتارهای مذکور باید نسبت به داده‌های معتبر که از لحاظ قانونی ارزشمند هستند، صورت پذیرد. ر.ک به: فضلی، مهدی(۱۳۸۴)، تخریب و اختلال در داده‌ها و سامانه‌های رایانه‌ای» مجموعه مقالات همایش بررسی جنبه‌های حقوقی فناوری و اطلاعات، تهران، انتشارات سلسبیل، ۱۳۸۴.

الکترومغناطیسی توسط وسایل و ابزارهای الکترونیکی فارغ از آنکه عنوان سامانه رایانه‌ای بر آنان صدق می‌نماید یا صدق نمی‌نماید، در حکم حملات سایبری قرار گیرد.

مکان و فضای تخریب داده ناشی از حملات سایبری نیز مانند تخریب داده ناشی از جرائم سایبری در فضای سایبر است و تنها تفاوت میان تخریب داده ناشی از جرائم سایبری با تخریب داده ناشی از حملات سایبری در آن است که تخریب داده ناشی از جرائم سایبری در زیرفضای سایبری میان کاربر با سامانه رایانه‌ای رخ می‌دهد درحالی‌که تخریب داده ناشی از حملات سایبری در زیرفضای سایبری میان سامانه‌های رایانه‌ای با یکدیگر ارتکاب می‌یابد. در نهایت با توجه به ماده مذکور لازم است حملات سایبری منجر به یکی از نتایج حذف، تخریب، اخلال غیرقابل‌پردازش کردن داده‌ها گردند تا مصداق عنوان مجرمانه تخریب داده قرار گیرند.[1]

نکته‌ای که با توجه به‌عنوان جعل رایانه‌ای و تخریب داده‌ها می‌توان بیان داشت آن است که هرگاه یک حمله سایبری محتوای داده‌های رایانه‌ای را به‌گونه‌ای تغییر دهد که آن داده توسط سامانه رایانه‌ای قابل‌پردازش باشد، اما سامانه رایانه‌ای عملکرد نادرستی از خود بروز دهد، مصداق عنوان مجرمانه جعل رایانه‌ای یعنی بند (ب) ماده۷۳۴ ق.م.ا و ماده ۷۳۷ ق.م.ا قرار خواهد گرفت و هرگاه تغییر داده به‌گونه‌ای باشد که توسط سامانه رایانه‌ای قابلیت پردازش نداشته باشد، حملهٔ ارتکابی مصداق عنوان مجرمانه تخریب داده‌ها قرار خواهد گرفت که در مورد اخیر به نظر می‌رسد چون عمل خاص مشمول ماده خاص قانون است تنها همان عنوان خاص یعنی تخریب داده اعمال می گردد.

در خصوص نتیجه مجرمانه باید گفت، جرم موضوع ماده ۷۳۶ از جرائم مقید به نتیجه است اما برخی، نتیجه آن را ورود ضرر می‌دانند با این تصور که این رفتارها اگر منتهی به ضرر فرد نشود، جرم، محقق نخواهد شد. بنابر این اگر داده‌ها پس از حذف، قابل بازیابی باشند چون ضرری به دارنده وارد نشده لذا به لحاظ عدم تحقق نتیجه ، جرمی هم محقق نشده است(فضلی،

---

[1] دو اصطلاح «تخریب و اخلال» شامل دو اصطلاح واژه‌های «حذف و غیرقابل‌پردازش کردن» می‌شود؛ خواه کلی خواه جزئی باشد و غیرقابل‌پردازش کردن نیز گونه‌ای از اخلال می‌باشد. ر.ک به: عالی پور، حسن(۱۳۹۳)، حقوق کیفری فناوری اطلاعات، تهران، چاپ سوم، انتشارات خرسندی.

۱۶۹:۱۳۸۴). در مقابل عده‌ای عقیده دارند، نتیجه در این جرم از بین رفتن (کلی یا جزئی) یا غیر قابل استفاده شدن داده است. ضمن اینکه موضوع جرم در اینجا به جهت حمایت از تمامیت داده می‌باشد نه ورود ضرر، تمامیت داده نیز با رفتار ابتدایی مرتکب از بین رفته است(بابایی،۱۱۵:۱۳۹۸).

در تخریب سنتی برخی حقوقدانان ورود خسارت به خود مال را ضروری دانسته‌اند، به نظر می‌رسد چنین امری در تخریب سایبری نیز صادق است. بدین معنا که در دو رفتار «حذف کردن» و «تخریب کردن» که ناظر بر موجودیت داده رایانه‌ای و محتوای درون آن است، ورود خسارت به داده ضروری است. برای مثال چنانچه یک مرتکب فونت یک سند رایانه‌ای را از (B Nazanin) به «B Zar» تغییر دهد، چون خسارتی به موجودیت سند وارد نشده است، نمی‌توان حکم به تخریب داده رایانه‌ای داد. هر رفتاری در فضای سایبر علیه داده‌های رایانه‌ای ارتکاب یابد که باعث غیر قابل پردازش (کلی یا جزئی) آن نشود، نمی‌توان حکم به تخریب داد. بنابر این چنانچه مرتکب با استفاده از برنامه‌های فشرده ساز مانند «Winrar» حجم یک فایل را کاهش دهد تا سرعت پردازش آن افزایش یابد، چون خسارتی بر داده رایانه‌ای وارد نشده تا در پردازش آن خللی ایجاد شود، نمی‌توان حکم به تخریب داده رایانه‌ای داد.

مقابله کیفری با حملات سایبری علیه تمامیت سامانه‌های رایانه‌ای نظامی

در راستای حمایت از تمامیت سامانه‌های رایانه‌ای عنوان مجرمانه «اخلال در سامانه‌های رایانه‌ای» در کنوانسیون بوداپست و قانون جرائم رایانه‌ای موردتوجه قرار گرفت و جرم انگاری شد. اخلال در سامانه‌های رایانه‌ای به معنای پدید آوردن عمدی آشفتگی و ناتوانی در کارکرد درست و متعارف سامانه است و از شیوه‌هایی می‌باشد که امروزه مجرمان در فضای سایبر از آن با اهداف مختلفی بهره می‌گیرند، به‌عنوان مثال شخصی با وارد نمودن ویروس به سامانه رایانه‌ای دیگری موجب می‌شود که سامانه رایانه‌ای او خودبه‌خود روشن یا خاموش شود و یا موجب اخلال در عملکرد سامانه رایانه‌ای او گردد(فضلی،۱۷۲:۱۳۸۹). به نظر برخی این عنوان جای پایی در حقوق کیفری سنتی دارد. بدین معنا که در مواردی که سامانهٔ رایانه‌ای متعلق

به شخص حقیقی یا شخص حقوقی خصوصی است می‌توان آن را برابر با جرم از کار انداختن مال دیگری می‌باشد و درجایی که سامانه رایانه‌ای متعلق به دولت است می‌توان آن را برابر با خرابکاری در تأسیسات مورداستفاده همگانی موضوع ماده ۶۸۷ [۱] قانون مجازات اسلامی دانست(عالی‌پور،۱۳۹۲:۲۲۱).

کنوانسیون بوداپست عنوان مجرمانه «مختل کردن سامانه رایانه‌ای» را در ماده ۵ پیش‌بینی نموده و مقرر داشته است:«هر یک از اعضاء باید به‌گونه‌ای اقدام به وضع قوانین و سایر تدابیر کنند که در صورت لزوم بر اساس حقوق داخلی خود، ایجاد اشکال جدی عمدی و بدون حق در کارکرد سیستم رایانه‌ای را در اثر واردکردن، انتقال دادن، صدمه زدن، پاک کردن، خراب کردن، تغییر دادن یا متوقف کردن داده‌های رایانه‌ای جرم‌انگاری کنند.»

بند ۶۵ گزارش توجیهی در تبیین هدف جرم انگاری اخلال در سامانه رایانه‌ای که در توصیه نامۀ شماره ۹(۸۹)، از این جرم به «خرابکاری رایانه‌ای»[۲] تعبیر شده است، مقرر داشته است: « هدف از وضع این مقرره، جرم‌انگاری مختل کردن عمدی استفاده قانونی از سامانه‌های رایانه‌ای است که شامل تجهیزات مخابراتی به‌وسیله داده‌های رایانه‌ای یا تأثیرگذاری بر آن‌ها می‌شود. منافع قانونی موردحمایت، مشمول متصدیان و کاربران سامانه‌های رایانه‌ای یا مخابراتی می‌شود تا بتوانند به‌طور شایسته فعالیت کنند. این متن به شکل خنثی تنظیم‌شده تا تمامی انواع کارکردها را تحت حمایت قرار دهد.»(جلالی‌فراهانی،۱۳۹۴:۳۲) منظور از اصطلاح «مختل کردن»[۳] در ماده مذکور با توجه به بند ۶۶ گزارش توجیهی «به اعمالی اطلاق می‌گردد که در کارکرد مناسب سیستم رایانه‌ای مداخله می‌کنند. این کار با واردکردن، انتقال دادن، آسیب رساندن، حذف کردن، تغییر دادن یا متوقف کردن داده‌های رایانه‌ای انجام

---

[۱]. ماده ۶۸۷ق.م.ا (تعزیرات):«هر کس در وسایل و تأسیسات مورد استفاده عمومی از قبیل شبکه‌های آب و فاضلاب و... مرتکب تخریب یا ایجاد حریق یا از کار انداختن یا هر نوع خرابکاری شود بدون آنکه منظور او اخلال در نظم و امنیت عمومی باشد به حبس از سه تا ده سال محکوم خواهد شد.»

[۲] Computer Sabotage

[۳] Hindering

می‌شود.» از آنجاکه رفتار مجرمانه «تغییر دادن» داده‌های رایانه‌ای یکی از رفتارهای مجرمانه تمثیلی می‌باشد که در بند ۶۶ گزارش توجیهی به آن اشاره شده است.

رفتار مجرمانه در عنوان مجرمانهٔ «اخلال در سامانه رایانه‌ای » همانند تخریب داده‌های رایانه‌ای لازم است «بدون حق» و «عمدی» ارتکاب یابد. بدین منظور در بند ۶۸ گزارش توجیهی مقرر شده است: «فعالیت‌های معمول ذاتی طراحی شبکه‌ها یا اقدامات تجاری یا اجرایی معمول به‌حق هستند؛ مانند آزمایش امنیت سیستم رایانه‌ای یا حفاظت از آن‌که توسط مالک یا متصدی مجاز شمرده‌شده یا پیکربندی دوبارهٔ سیستم‌عامل به هنگامی‌که متصدی سیستم نرم‌افزار جدیدی را نصب می‌کند و برنامه‌های مشابه نصب شدهٔ پیشین را از کار می‌اندازد. ازاین‌رو، این اعمال طبق این ماده جرم نیستند، حتی اگر موجب اختلال شدید شوند»(جلالی‌فراهانی،۳۳:۱۳۹۳) و در بند ۷۰ گزارش توجیهی مقرر شده است: «این جرم باید «عمداً» ارتکاب یابد، یعنی مجرم قصد مختل کردن شدید را داشته باشد».

در بند ۶۷ گزارش توجیهی آمده است: «مختل کردن باید «شدید» باشد تا باعث اعمال ضمانت اجرای کیفری شود. هر عضو معیارهای «شدید بودن» این عمل را برای خود تعیین خواهد کرد. برای مثال، می‌تواند حداقل آسیب وارده به سیستم را معیار قرارداد. تدوین‌کنندگان، ارسال داده‌ها به سیستم خاص، به روش، اندازه یا تناوبی که اثر مخرب جدی بر توانایی دارند یا متصدی در استفاده از سیستم یا برقراری ارتباط با سایر دستگاه‌ها داشته باشد، معیار «شدید بودن» قرار داده‌اند (مانند استفاده از برنامه‌هایی که «حملات مانع خدمات»[۱] را ایجاد می‌کنند، کدهای زیان‌بار، نظیر ویروس‌هایی که از عملیات سیستم جلوگیری کرده یا سرعت آن را به نحو چشم‌گیری کاهش می‌دهند یا برنامه‌هایی که مقادیر زیادی رایانامه را برای گیرنده می‌فرستند تا کارکردهای ارتباطی سیستم را متوقف کنند)»(جلالی‌فراهانی،۳۳:۱۳۹۳). در نهایت گزارش توجیهی در موردی که ارسال رایانامهٔ ناخواسته[۲] با اهداف تجاری یا غیر آن، به ویژه اگر حجم زیادی داشته باشد یا به تناوب انجام

[۱] Denial Service Attacks (DoS)

[۲] Spamming

شود، ممکن است برای گیرنده مزاحمت ایجاد کند آیا می‌توان آن را مصداق عنوان «مختل کردن شدید سامانه رایانه‌ای» تلقی نمود یا خیر؟ در بند ۶۹ مقرر می‌دارد: «از نظر تدوین‌کنندگان، این عمل فقط زمانی جرم‌انگاری شود که عمداً ارتکاب یابد و ارتباطات به‌طور جدی مختل شود. با این‌حال اعضا می‌توانند در قوانین داخلی خود رویکرد متفاوتی را نسبت به مختل شدن اتخاذ کنند. برای مثال، پیش‌بینی چنین رفتارهایی را به‌عنوان تخلف اداری یا به نحو دیگری مشمول ضمانت اجرا بدانند. این متن تعیین میزان مختل شدن سیستم، به‌طور جزئی یا کلی، موقت یا دائم را به اعضا واگذار کرده تا کمیتهٔ آسیب وارده، اعمال ضمانت اجراهای اداری یا کیفری را بر اساس قانون داخلی توجیه کند.»

از آنجاکه حملات سایبری «عمدی» و «بدون حق» ارتکاب می‌یابند لازم است یک حمله سایبری منجر به مختل شدن عملکرد سامانه‌های رایانه‌ای گردد تا حمله سایبری ارتکاب یافته مصداق ماده ۵ کنوانسیون بوداپست قرار گیرد.

با توجه به آنکه تمامی رفتارهای تمثیلی ذکرشده در ماده ۵ کنوانسیون لازم است در فضای سایبر ارتکاب یابند، شایسته بود ماده ۵ بدین گونه تنظیم می‌شد: مختل کردن سامانه رایانه‌ای عبارت است از« ایجاد اشکال جدی، عمدی و بدون حق در فضای سایبر که کارکرد سامانه رایانه‌ای را مختل سازد و از ذکر یکایک رفتارهای تمثیلی خودداری می‌نمود».

در حقوق ایران نیز قانون‌گذار در ماده ۷۳۷ ق.م.ا (تعزیرات) که مقرر می‌دارد: «هر کس به‌طور غیرمجاز با اعمالی از قبیل واردکردن، انتقال دادن، پخش، حذف کردن، متوقف کردن، دست‌کاری یا تخریب داده‌ها یا امواج الکترومغناطیسی یا نوری، سامانه‌های رایانه‌ای یا مخابراتی دیگری را از کار بیندازد یا کارکرد آن‌ها را مختل کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون (۱۰ .۰۰۰ .۰۰۰) ریال تا چهل میلیون (۴۰ .۰۰۰ .۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.» عنوان مجرمانه اخلال در سامانه‌های رایانه‌ای را پیش‌بینی نموده است. برای آنکه مشخص گردد یک حمله سایبری تحت چه شرایطی مصداق عنوان اخلال در سامانه رایانه‌ای به‌ویژه ماده ۷۳۷ ق.م.ا (تعزیرات) قرار می‌گیرد. لازم است عنصر مادی حملات سایبری با عنصر مادی ماده مذکور تعیین و با یکدیگر مقایسه گردند.

با توجه به ماده ۷۳۷ ق.م.ا (تعزیرات) می‌توان رفتارهای مرتکب را به دو دسته تقسیم نمود ۱- اعمالی از قبیل واردکردن، انتقال دادن، پخش، حذف کردن، متوقف کردن، دست‌کاری یا تخریب داده‌ها، ۲- اعمالی از قبیل واردکردن، انتقال دادن، پخش، حذف کردن، متوقف کردن، دست‌کاری یا تخریب امواج الکترومغناطیسی یا نوری.

۱- داده‌های دستهٔ اول را با توجه به عملکرد آنان می‌توان به دو دستهٔ داده‌های سامانه‌ای و داده‌های کاربردی تقسیم نمود.[۱] داده‌های سامانه‌ای آن دسته از داده‌هایی می‌باشند که مرتبط با عملکرد سامانه‌های رایانه‌ای است؛ مانند سیستم‌عامل، در مقابل داده‌های کاربردی آن دسته از داده‌هایی می‌باشند که باعث آن می‌گردند کاربران امور معینی را به انجام برسانند مانند واژه‌پردازها. به نظر می‌رسد منظور از اصطلاح داده در ماده ۷۳۷ ق.م.ا (تعزیرات) داده‌های سامانه‌ای باشد و منظور از اصطلاح «داده» در ماده ۷۳۶ ق.م.ا (تعزیرات) داده‌های کاربردی باشد؛ زیرا قانون‌گذار با وضع ماده ۷۳۶ ق.م.ا (تعزیرات) حمایت خود را از داده‌ها اعلام نموده است و لزومی به تکرار آن در ماده ۷۳۷ ق.م.ا (تعزیرات) نداشت و از آنجاکه قانون‌گذار در ماده ۷۳۷ ق.م.ا (تعزیرات) درصدد حمایت از سامانه‌های رایانه‌ای برآمده است لازم است عبارت داده در ماده مذکور را حمل بر داده‌های سامانه‌ای گردد؛ بنابراین می‌توان به این نتیجه دست‌یافت در صورت ارتکاب جرم تخریب داده‌ها هرگاه موضوع تخریب داده‌های سامانه‌ای باشد، رفتار ارتکابی مصداق ماده ۷۳۷ ق.م.ا (تعزیرات) قرار خواهد گرفت و هرگاه موضوع تخریب، داده‌های کاربردی باشد، رفتار ارتکابی مصداق ماده ۷۳۶ ق.م.ا (تعزیرات) قرار خواهد گرفت. در نتیجه ازآنجایی‌که موضوع تخریب داده‌ها در ماده ۷۳۶ ق.م.ا (تعزیرات) و ماده ۷۳۷ ق.م.ا (تعزیرات) متفاوت می‌باشد، می‌توان گفت میان این دو عنوان مجرمانه همپوشانی وجود نخواهد داشت و رفتارهای مجرمانه منجر به تخریب داده‌ها با رفتارهای مجرمانه منجر به اخلال در سامانه‌های رایانه‌ای شامل مقررات تعدد جرم قرار نمی گیرند.

---

[۱] ر.ک به: پرسمن، راجر اس، مهندسی نرم‌افزار، ترجمه عین‌الله جعفرنژادقمی و ابراهیم عامل محرابی، تهران، چاپ هشتم، نشر دانش نگار،۱۳۹۳.

۲- دسته دوم شامل رفتارهای مجرمانهٔ تمثیلی است که توسط امواج الکترومغناطیسی یا نوری ارتکاب می‌یابند. سامانه‌های رایانه‌ای وسایلی الکترونیکی‌اند که از عناصر مغناطیسی و مدارهای الکترونیکی، ساخته شده‌اند؛ بنابراین انتشار امواج الکترومغناطیسی این قابلیت را دارا می‌باشند که بر عناصر مغناطیسی و مدارهای الکترونیکی اثر مخرب ایجاد نمایند.

سؤالی که مطرح می‌گردد آن است که امواج الکترومغناطیسی چگونه منجر به اخلال در سامانه‌های رایانه‌ای می‌گردند؟ برای پاسخگویی به سؤال مذکور دو حالت قابل‌تصور است: حالت اول امواج الکترومغناطیسی بر داده‌های متشکل از صفر و یک‌های موجود در عناصر مغناطیسی یا مدارهای الکترونیکی تأثیر می‌گذارند، در این صورت با توجه به تعریف ارائه‌شده از فضای سایبر در نوشتار حاضر[1] رفتار ارتکابی در فضای سایبر رخ داده و در دسته اول قرار می‌گیرد. حالت دوم امواج الکترومغناطیسی بدون تأثیرگذاری بر داده‌های موجود در عناصر مغناطیسی و مدارهای الکترونیکی بر شدت جریان‌های الکتریکی و مغناطیسی عبوری آنان تاثیر گذاشته و باعث اخلال در عملکرد آنان گردیده و به دنبال آن عملکرد سامانه رایانه‌ای مختل یا از کار می‌افتد. همچنین ممکن است انتشار امواج الکترومغناطیسی فارغ از اثر گذاری بر روی داده های رایانه‌ای سبب اتصال در قطعات الکترونیکی تشکیل دهنده ی مدارهای الکتریکی گردیده و متعاقب آن عملکرد سامانه رایانه‌ای مختل یا از کار بیفتد. در این حالت به نظر می‌رسد رفتار ارتکابی مصداق تخریب سنتی قرار گیرد، همچنان که هرگاه تغییر ناگهانی در ولتاژ برق باعث صدمه به مدارهای الکترونیکی در سامانه‌های رایانه‌ای گردد و به دنبال آن عملکرد سامانه رایانه‌ای از کار بیفتد مصداق تخریب سنتی قرار خواهد گرفت.

در مورد شرایط و اوضاع و احوال ماده مذکور ابتدا باید بیان داشت موضوع جرم «سامانه‌های رایانه‌ای» است؛ بنابراین لازم است حملات سایبری علیه داده‌های سامانه‌ای به‌گونه‌ای ارتکاب یابند که منجر به اخلال در سامانه‌های رایانه‌ای گردد تا مصداق ماده مذکور قرار گیرند. لازم به ذکر است هرگاه یک حمله سایبری علیه داده‌های در حال انتقال به‌گونه‌ای ارتکاب یابد که

---

[1]. فضای سایبر، فضایی است که داده‌ها در آن تبدیل به صفر و یک گردیده؛ بنابراین جنس داده‌ها و فضای سایبر دیجیتال (صفر و یک) می‌باشد.

آن داده‌ها پس از ورود به سامانه رایانه‌ای منجر به اخلال در عملکرد سامانه‌های رایانه‌ای گردد مصداق ماده مذکور قرار خواهد گرفت؛ زیرا آنچه در ماده پیش‌گفته ضرورت دارد نتیجه آن، یعنی اخلال در عملکرد سامانه‌های رایانه‌ای یا از کار انداختن آنان در فضای سایبر می‌باشد. با وجودآنکه وسیله ارتکاب در ماده فوق به‌صورت مطلق بیان شده است اما حملات سایبری تنها موردی را دربر می‌گیرند که اخلال در سامانه رایانه‌ای توسط یک سامانه رایانه‌ای دیگر ارتکاب یابد.

مکان ارتکاب اخلال در عملکرد سامانه رایانه ای ناشی از حملات سایبری همانند اخلال در عملکرد سامانه رایانه ای ناشی از جرائم سایبری فضای سایبر می باشد و تنها تفاوت میان اخلال در عملکرد سامانه‌رایانه‌ای ناشی از جرائم سایبری با اخلال در عملکرد سامانه رایانه‌ای ناشی از حملات سایبری در آن است که اخلال در عملکرد سامانه رایانه‌ای ناشی از جرائم سایبری در زیرفضای سایبری میان کاربر با سامانه رایانه ای رخ می دهد، در حالی که اخلال در عملکرد سامانه رایانه‌ای ناشی از حملات سایبری لزوماً در زیرفضای سایبری میان سامانه های رایانه ای با یکدیگر ارتکاب می یابد.

از آن جایی که حملات سایبری به طور غیرمجاز علیه دیگر سامانه های رایانه ای ارتکاب می یابند وجود قید »غیرمجاز« نیز خللی در شمولیت حملات سایبری بر ماده مذکور وارد نمی سازد. در نهایت لازم است یک حمله سایبری منتج به «از کار انداختن» یا «مختل کردن» در عملکرد سامانه رایانه ای گردد تا مصداق عنوان اخلال در سامانه رایانه‌ای قرار گیرد.

نتیجه‌گیری

حمله سایبری امروزه به عنوان یکی از مهم‌ترین تهدیدات سایبری علیه داده‌ها و سامانه‌های رایانه‌ای نظامی به‌شمار می‌روند، چراکه هرگونه اخلال در آن‌ها امنیت کشور را به مخاطره انداخته و بستری برای تحقق سایر عملیات‌های مجرمانه سایبری از قبیل تروریسم سایبری، جاسوسی سایبری و جنگ سایبری قلمداد می‌شود. این امر مهم مورد غفلت قانون‌گذار قرار

گرفته است و با بررسی کنوانسیون بوداپست و حقوق کیفری ایران پیرامون مقابله کیفری با عملیات‌های مجرمانه سایبری مشخص شد که تصویب‌کنندگان کنوانسیون بوداپست و قانون جرائم رایانه‌ای از عنوان مجرمانه حمله سایبری در تدوین قوانین خود بهره نبرده‌اند. اما با این وجود با تحلیل مفهوم و ماهیت حمله سایبری مشخص شدکه مشابه با نتایج ناشی از جرائم رایانه‌ای محض است که علیه تمامیت داده‌ها و سامانه‌های رایانه‌ای ارتکاب می‌یابند. این دسته از جرائم در کنوانسیون بوداپست و حقوق کیفری ایران مورد تقنین قرار گرفته است و در نتیجه می‌توان در قالب جرائم سایبری محض قابل ارتکاب علیه تمامیت داده‌ها و سامانه‌های رایانه‌ای نظامی یعنی اخلال داده رایانه‌ای و سامانه رایانه‌ای که در زیرفضا سایبری میان‌سامانه‌های رایانه‌ای با یکدیگر تحقق می‌یابند به مقابله‌ی کیفری با حملات سایبری پرداخت. بدین نحو که هرگاه موضوع حمله سایبری داده‌های رایانه‌های نظامی باشد، در سطح بین‌المللی رفتار مرتکب مصداق بندهای (۱) و (۲) ماده ۴ کنوانسیون بوداپست و گزارش توجیهی پیرامون آن و در سطح ملی مصداق ماده ۷۳۶ قانون مجازات اسلامی قرار می‌گیرد و هرگاه موضوع حمله سایبری سامانه‌های رایانه‌ای نظامی باشد، در سطح بین‌المللی رفتار مرتکب مصداق ماده ۵کنوانسیون بوداپست و در سطح داخلی مصداق ماده ۷۳۷ قانون مجازات اسلامی قرار می‌گیرد.

پیشنهادات

با وجود آن‌که قوانین موجود از حیث عنصر مادی تمامی رفتارهای فیزیکی حملات سایبری علیه داده‌ها و سامانه‌های رایانه‌ای نظامی را در بر می‌گیرد و می‌توان در قالب جرائم رایانه‌ای محض علیه تمامیت داده‌ها و سامانه‌های رایانه‌ای به مقابله کیفری با آن پرداخت ولی از حیث ماهیت باید اذعان داشت، اولاً رفتار مجرمانه در جرائم رایانه‌ای مانند تخریب داده، اخلال در سامانه رایانه‌ای مستقل از یکدیگر می‌باشند. در حالی‌که در حمله سایبری یک رفتار واحد، محقق جرم نیست. بلکه عنوان مجرمانه حمله سایبری بر دسته‌ای از رفتارهای مجرمانه متفاوت بار می‌شود که خود این رفتارهای مجرمانه به طور مستقل در قانون جرائم رایانه‌ای پیش‌بینی

شده‌اند. بدین‌معنا که، در حمله سایبری رفتارهای فیزیکی شامل تخریب داده و اخلال در سامانه رایانه‌ای است؛ زمانی این رفتارها عنوان مجرمانه حمله سایبری را تشکیل می‌دهند که همراه با گستردگی و یا سازمان یافتگی علیه امنیت کشور ارتکاب یابند. دوماً جرائم پیش‌بینی شده در قانون جرائم رایانه‌ای از ماهیت ملی برخودار هسنند، در حالی که ماهیت حملات سایبری، فراملی می‌باشد و شایسته نیست در قالب یک جرم عادی به مقابله کیفری با یک جرم فراملی پرداخت.

از حیث اهداف جرم‌انگاری باید اذعان داشت، هدف از جرم انگاری مستقل حمله سایبری حمایت و تضمین امنیت کشور در فضای سایبر است که چنین هدفی لزوماً در جرائم رایانه‌ای صادق نیست. از حیث موضوع جرم نیز، موضوع حملات سایبری بسیار مضیق‌تر از جرائم رایانه‌ای است. چراکه موضوع جرم در حملات سایبری داده‌ها و سامانه‌های رایانه‌ای از قبیل داده‌ها و سامانه‌های رایانه‌ای نظامی را در برمی‌گیرد که هرگونه اخلال در آن‌ها موجب بر هم خوردن امنیت کشور می‌شود. در نهایت مجازات‌های پییش بینی شده در قانون جرائم رایانه‌ای ممکن است برای مرتکبین جرائم سایبری بازدارنده باشد اما برای مهاجم دشمن و بیگانه که از آن سوی مرزها حملات سایبری خویش را به طور سازمان یافته متوجه داده‌ها و سامانه‌های رایانه‌ای نظامی می‌کند و امنیت کشور را به مخاطره می‌اندازد، بازدارنده و منصفانه نیست. ازاین رو، شایسته است مقنن با جرم‌انگاری مستقل حمله سایبری علیه داده‌ها وسامانه‌های رایانه‌ای نظامی درصدد مقابله کیفری با حملات سایبری مکرری بر آید که کشور جمهوری اسلامی ایران از گزند آن‌ها در امان نیست.

منابع

آیوک، جان(۱۳۹۱)، ویروس‌ها و بدافزارهای کامپیوتری، ترجمه بشری راد، بابک و آرش حبیبی لشکری، تهران، چاپ اول، انتشارات ناقوس.

بابایی، جواد (۱۳۹۸)، جرائم رایانه‌ای و آیین دادرسی حاکم بر آن، چاپ چهارم، تهران: نشر مرکز مطبوعات و انتشارات قوه قضاییه.

بتز، دیوید و تام استیون(۱۳۹۱)، تبارشناسی جنگ سایبری، ترجمه موسسه فرهنگی و مطالعات و تحقیقات بین‌المللی ابرار معاصر (امنیت و جنگ سایبری ۱)، تهران، چاپ اول، نشر موسسه فرهنگی و مطالعات و تحقیقات بین‌المللی ابرار معاصر.

الهام، غلامحسین و محسن برهانی(۱۳۹۴)، درآمدی بر حقوق جزای عمومی (جلد اول) جرم و مجرم، تهران، نشر میزان، چاپ اول.

پرسمن، راجر اس(۱۳۹۳) ، مهندسی نرم‌افزار، ترجمه عین‌الله جعفرنژادقمی و ابراهیم عامل محرابی، تهران، چاپ هشتم، نشر دانش نگار.

خلیل زاده، مونا (۱۳۹۳)، مسؤولیت بین‌المللی دولت‌ها در قبال حملات سایبری، تهران، چاپ اول، نشر مجد.

جالینوسی، احمد، شهروز ابراهیمی و طیبه قنوانی(۱۳۹۵)، جایگاه فضای سایبر و تهدیده‌های سایبری در استراترژی امنیت ملی ابالات متحده آمریکا، فصلنامه دانش سیاسی و بین الملل، سال دوم، شماره ۵.

جلالی فراهانی، امیرحسین(۱۳۹۵)، کنوانسیون جرائم سایبر و پروتکل الحاقی آن، تهران، چاپ دوم، نشر خرسندی.

حسن‌بیگی، ابراهیم(۱۳۸۴)، حقوق و امنیت در فضای سایبر، چاپ اول، تهران: نشر مؤسسه فرهنگی مطالعات و تحقیقات بین المللی ابرار معاصر.

دسترر، جورج و امی آلیز و الکس هرواتین(۱۳۹۱)، حملات اختلال در سرویس دهی (دی داس): پیشگیری، تشخیص نفوذ و کاهش تاثیرات، ترجمه مؤسسه فرهنگی و مطالعات و تحقیقات بین المللی ابرار معاصر امنیت و جنگ سایبری ۲، تهران، چاپ نخست، نشر مؤسسه فرهنگی و مطالعات و تحقیقات بین المللی ابرار معاصر.

سلمانی زاده، محمود(۱۳۸۰)، جنگ اطلاعات و امنیت، خبرنامه انفورماتیک، سازمان برنامه‌وبودجه کشور، شماره ۸۰.

زندی، محمدرضا(۱۳۹۳)، تحقیقات مقدماتی در جرائم سایبری، تهران: انتشارات جنگل، جاودانه، چاپ دوم.

عالی‌پور، حسن(۱۳۹۳)، حقوق کیفری فناوری اطلاعات، تهران، چاپ سوم، انتشارات خرسندی.

عزیزی، امیرمهدی(۱۳۹۴)، حقوق کیفری جرائم رایانه‌ای، تهران، چاپ دوم، نشرمجد.

عظیمی، فاطمه؛ خشنودی، هادی(۱۳۹۵)، «نقش تروریسم سایبری در تهدید علیه امنیت ایران و راه‌های پیشگیری از آن»، فصلنامه مطالعات سیاسی، سال نهم، شماره ۳۴.

داوری دولت‌آبادی، مجید(۱۳۹۳)، بدافزارها و راه‌کارهای مقابله، تهران، چاپ اول، نشر پندار پارس.

فضلی، مهدی(۱۳۸۴)، تخریب و اختلال در داده‌ها و سامانه‌های رایانه‌ای» مجموعه مفالات همایش بررسی جنبه‌های حقوقی فناوری و اطلاعات، تهران، چاپ اول، انتشارات سلسبیل، ۱۳۸۴.

فضلی،مهدی(۱۳۸۹)،مسولیت کیفری در فضای سایبر ،تهران،چاپ اول، نشر خرسندی.

گلدوزیان، ایرج(۱۳۸۳)، محشای قانون مجازات اسلامی، تهران، چاپ چهارم، نشرمجد.

محمدنسل، غلامرضا(۱۳۹۵)، حقوق جزای اختصاصی جرائم رایانه ای در ایران، تهران، چاپ دوم، تهران، نشر میزان.

مرسی، هادی(۱۳۹۷)، مقابله با حملات سایبری در حقوق کیفری ایران و اسناد بین‌المللی (با تأکید بر حملات سایبری علیه ایران)، پایان نامه برای دریافت درجه کارشناسی ارشد، تهران: دانشکده حقوق و علوم سیاسی دانشگاه تهران.

یکرنگی، محمد و هادی مرسی و مهسا علیزاده(۱۴۰۰)، «امکانسنجی استناد به دفاع مشروع به عنوان مانع مسئولیت کیفری در مقابل حملات سایبری»، مجله مطالعات حقوق کیفری و جرم شناسی، دوره ۵۱، شماره ۲، ۵۸۳-۵۶۱.

Army, U.S(2005), Cyber Operations and Cyber Terrorism" In U. Army, U.S. Army Trainin. Available at: https://www.globalsecurity.org/military/library/policy/army/other/tradoc-dcsint-hbk_1-02-2005.pdf

Andress, Jason & Steve Winterfeld, cyber warfare: Techniques, Tactics and Tools for Security Practitioners, Amesterdam, Boston:Syngress/ Elsevier,2011,p.11

Junaidu Bello Marshall, E., & Mua'zu Abdullahi Saulawa, E. Cyber- attacks: The legal response, International Journal of International Law, Vol.1, Issue.2, 2015.

Lord, K.M., & Sharp, T(2011), America's Cyber future Security and Prosperity in the Information Age, Center for a New American Security, center for a new American Security, Vol.1, No.2.

Oona A. H., Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel(2012). The Law of Cyber-Attack, California Law Review, Vol. 100, No. 4.

https://www.tasnimnews.com/fa/news/1401/06/20/2772788/

A.Clarke,Richard,K.Knanke,Robert,Cyber War:The Next Thread to National Security and What to Do about it,Manhattan,New York,Ecco,2010.

www.library.arizona.edu/rio/glossary.html

Joint Chiefs of Staff, Joint Publication 1-02, Dep't of Def. Dict. of Military and Assoc'd Terms,2001,p.141 available at: http://www.dtic.mil/doctrine/jel/newoubs/jp102.pdf