راهبرد جرم‌انگاری مستقل حملات سایبری در حقوق کیفری ایران

حمید بهره‌مند* و هادی مرسی**

نوع مقاله: علمی	تاریخ دریافت: ۱۴۰۰/۰۱/۱۸	تاریخ پذیرش: ۱۴۰۰/۱۰/۲۹	شماره صفحه: ۳۲۴-۲۸۵

حمله سایبری اقدام مجرمانه سایبری است که می‌تواند تلفات و خساراتی علاوه بر انسان به سامانه‌های رایانه‌ای وارد کند. در حقوق کیفری ایران به‌ویژه قانون جرائم رایانه‌ای اصطلاح «حمله سایبری» استفاده نشده است، ازاین‌رو، در شرایط کنونی در قالب جرائم رایانه‌ای انجام می‌گیرد. پژوهش حاضر با لحاظ این امر که هدف اصلی قانون جرائم رایانه‌ای بیشتر ناظر بر حمایت از داده‌ها و سامانه‌های رایانه‌ای شهروندان بوده است و از حیث ماهیت جزء جرائم عادی، ملی و فاقد سازمان‌یافتگی است، مقابله با حمله سایبری را در قالب جرم رایانه‌ای در دستور کار خود قرار نداده است؛ زیرا هدف از جرم‌انگاری حمله سایبری حمایت از داده‌ها و سامانه‌های رایانه‌ای مرتبط با امنیت کشور است و با لحاظ این امر که حمله سایبری را اغلب یک کشور علیه کشور دیگر مرتکب می‌شود از ماهیت فراملی و سازمان‌یافته برخوردار بوده که موجب لطمه دیدن امنیت یک کشور می‌شود. ازاین‌رو، در این پژوهش با روش توصیفی. تحلیلی مفهوم حمله سایبری را از سه حیث ماهیت، هدف جرم‌انگاری و اوصاف موضوعی متفاوت از مفهوم جرائم رایانه‌ای می‌داند. همچنین از حیث نظری با تمسک به اصول جرم‌انگاری مانند اصل ضرر، مصلحت عمومی، ضرورت، تناسب جرم و مجازات و درنهایت لزوم توجه به راهبردها، رویکردها و همکاری بین‌المللی جرم‌انگاری مستقل به‌نظر می‌رسد لازم است در نظام حقوقی داخلی، علاوه بر جرائم رایانه‌ای فعلی، حملات سایبری به‌طور مستقل جرم‌انگاری و ضمانت اجراهای متناسبی با نوع و شدت حملات و خسارت‌های احتمالی یا واردشده اتخاذ شود.

کلیدواژه‌ها: جرم‌انگاری؛ فضای سایبر؛ حملات سایبری؛ جرائم سایبری؛ جرائم بین‌المللی

---

* استادیار دانشکده حقوق و علوم سیاسی، دانشگاه تهران (نویسنده مسئول)؛
Email: bahremand@ut.ac.ir

** دانشجوی دکتری حقوق جزا و جرم‌شناسی، دانشکده الهیات و معارف اسلامی، دانشگاه میبد؛
Email: stu.h.mersi@meybod.ac.ir

فصلنامه مجلس و راهبرد، سال بیست‌ونهم، شماره یکصدویازدهم، پاییز ۱۴۰۱

doi: 10.22034/MR.2022.4685.4565

مقدمه

در دنیای ارتباطات امروزی حمایت از داده‌ها و سامانه‌های رایانه‌ای یکی از اهداف اساسی حقوق کیفری در فضای سایبر است. داده‌ها و سامانه‌های رایانه‌ای از حیث میزان درجه اهمیت یکسان نیستند. برخی از آنها از درجه اهمیت بسیاری برخوردارند زیرا هرگونه آثار مخربی، امنیت کشور را تحت‌الشعاع قرار می‌دهد. با تصویب قانون جرائم رایانه‌ای در ۱۳۸۸/۰۳/۰۵ سیاست جنایی نظام حقوقی ایران در برابر اقدام‌های مجرمانه‌ای که علیه حقوق، داده‌ها و سامانه‌های رایانه‌ای عموم شهروندان در فضای سایبر ارتکاب می‌یابند و اقدام‌های مجرمانه‌ای که علیه داده‌ها و سامانه‌های رایانه‌ای مرتبط با امنیت کشور در فضای سایبر انجام می‌شود به‌نحو یکسان و در قالب جرائم رایانه‌ای پیش‌بینی شده است. مجموعه این اقدام‌های مجرمانه «حمله سایبری» نامیده شده و این‌گونه تعریف شده است: «حملات سایبری مجموعه اقدام‌هایی است که توسط یک دولت به‌منظور نفوذ یا ایجاد اخلال در سامانه‌های رایانه و یا شبکه رایانه‌ای، علیه دولت دیگر ارتکاب می‌یابد» (خلیل‌زاده، ۱۳۹۳: ۲۶).

گفتنی است با وجود وفاق اجتماعی در این موضوع که حمله سایبری برخلاف جرائم رایانه‌ای امنیت کشورها را تحت تأثیر قرار می‌دهد، اما این امر چنانکه باید، مورد توجه اسناد بین‌المللی و قوانین فعلی ایران قرار نگرفته است. به‌نظر می‌رسد علت چنین غفلتی دو امر است: اول آنکه تعریف واحد، جامع و مانعی از حمله سایبری ارائه نشده است که موجب شده دو مفهوم «حمله سایبری» و «جرم رایانه‌ای» از ماهیت واحد و یکسانی مفروض شود و دوم آنکه ضرورت اتخاذ یک سیاست جنایی افتراقی در قالب جرم‌انگاری مستقل «حمله سایبری» مورد غفلت واقع شود. ازاین‌رو، پرسشی که می‌توان مطرح کرد آن است که از چه جهت یا جهاتی «حمله سایبری» با «جرم رایانه‌ای» متفاوت است.

بدین‌منظور در قسمت اول (مفهوم‌شناسی حمله سایبری) این مطالعه به تحلیل و ارزیابی تعاریف ارائه شده از حمله سایبری پرداخته است و سپس در قسمت دوم (تعریف مختار از حملات سایبری) با ارائه تعریف جامع و مانع از حمله سایبری مرزهای تفکیک آن را با جرم رایانه‌ای از حیث ماهیت، هدف جرم‌انگاری و اوصاف موضوع تبیین می‌کند تا دلایل ضرورت جرم‌انگاری مستقل حمله سایبری مشخص شود. پرسش دیگری که قابلیت طرح دارد آن است که جرم‌انگاری حمله سایبری در سایه کدام اصل یا اصول و ضوابط ردای مشروعیت به تن می‌پوشد. بدین‌منظور در قسمت چهارم (اصول و مبانی جرم‌انگاری مستقل حمله سایبری) به تبیین این موضوع پرداخته است.

دوم آنکه برابر دانستن نتایج زیان‌بار ناشی از حمله سایبری با جرائم رایانه‌ای است. ازاین‌رو، پرسشی که مطرح می‌شود آن است که گستردگی دامنه نتایج زیان‌بار ناشی از حمله سایبری چقدر می‌تواند باشد. بدین‌منظور در قسمت ۳-۱ (مصادیق حمله سایبری در مفهوم مضیق) به تحلیل و ارزیابی مهم‌ترین حملات سایبری علیه جمهوری اسلامی ایران پرداخته شده است تا مشخص شود حمله سایبری گونه‌ای جدید از حملات تلقی می‌شود که نه‌تنها کاربران بلکه نیروهای نظامی می‌توانند با توسل به آن آسیب‌های جسمانی و خسارت‌های فیزیکی گسترده‌ای را با فضای سایبر ایجاد کنند و دامنه نتایج زیان‌بار ناشی از آن می‌تواند از تضعیف عملکرد شبکه‌های رایانه‌ای تا حملات شدید علیه ساختارهای زیربنایی ملی یک کشور در فضای سایبر در نوسان باشد.

برای اهمیت این امر می‌توان به حمله سایبری ناشی از بدافزار استاکس‌نت[1] اشاره کرد که یکی از مهم‌ترین حملات سایبری علیه ایران تلقی می‌شود. این بدافزار نخستین بار به‌صورت کاملاً تصادفی در تابستان ۲۰۱۰ کشف شد (شلدون، ۱۳۹۱: ۳۲۰). بدافزار

1. Stuxnet

استاکس‌نت با وارد کردن داده‌های مخرب به سامانه‌های کنترلی، عملکرد ابزارها و تجهیزاتی که سامانه‌های رایانه‌ای را هدایت می‌کردند، مختل می‌کرد تا موجب آسیب به سانتریفیوژهای موجود در نیروگاه هسته‌ای نطنز و به دنبال آن متوقف‌سازی غنی‌سازی اورانیوم در ایران شود. پس از آن، حملات سایبری دیگری ارتکاب یافتند از قبیل: دوکو[1] در آبان ۱۳۹۰ علیه تأسیسات صنعتی ایران، وایپر[2] در اردیبهشت ۱۳۹۱ علیه سامانه‌های رایانه‌ای و شبکه داخلی وزارت نفت ایران، فلیم[3] در خرداد ۱۳۹۱ علیه تجهیزات نفتی کشورهای خاورمیانه ازجمله ایران و حمله سایبری ارتکابی در تیر ۱۳۹۹ که اولین انفجار در تأسیسات هسته‌ای نطنز را موجب شد. اخیراً نیز در مورخ ۱۴۰۰/۱/۲۲ با حمله سایبری دیگری علیه شبکه برق تأسیسات غنی‌سازی نطنز موجب انفجار در آن مرکز شد.[4] ارتکاب حملات سایبری پی در پی از سال ۲۰۱۰ تا سال ۲۰۲۱ میلادی علیه ایران، نشانگر آن است که با توجه به موقعیت جمهوری اسلامی ایران در خاورمیانه، هیچ‌گاه از گزند حمله سایبری در امان نخواهد بود.

۱. مفهوم‌شناسی حمله سایبری

با توجه به اینکه نظرهای گوناگونی درباره مفهوم حمله سایبری وجود دارد و هریک از نظریه‌پردازان و کارشناسان از زاویه دید خود به آن پرداخته‌اند، در این قسمت تلاش شده

---

1. Duqu
2. Viper
3. Flame

۴. روزنامه رژیم صهیونیستی *جروزالم پست* روز یکشنبه نوشت: «براساس گزارش‌ها به‌نظر می‌رسد عامل آنچه حادثه خوانده شده، حمله سایبری باشد که احتمالاً اسرائیل انجام داده است. براساس گزارش‌های خارجی نطنز پیش از این هم هدف حمله‌های سایبری اسرائیل قرار گرفته بود، به‌گونه‌ای که در سال ۲۰۰۱ حمله به این تأسیسات، در عملیات مشترک با ایالات متحده، بیش از یک هزار سانتریفیوژ را نابود کرد» (خبرگزاری *تابناک*).

است با تجزیه و تحلیل تعاریف ارائه شده، تعریف جامع و مانعی از حمله سایبری ارائه شود.

۱-۱. حمله سایبری در مفهوم موسّع

برخی از نویسندگان، حمله سایبری را حمله‌ای دانسته‌اند که از یک سامانه رایانه‌ای به‌نحوی علیه سامانه رایانه‌ای یا شبکه رایانه‌ای یا وب‌سایت دیگر ارتکاب می‌یابد که محرمانگی، تمامیت و قابلیت دسترسی سامانه‌های رایانه‌ای و اطلاعات ذخیره شده در آن را به مخاطره می‌اندازد (Junaidu Bello and Mua'zu Abdullahi Saulawa, 2015: 3). براساس این تعریف، مهم‌ترین هدف جرم‌انگاری در زمینه حمله سایبری، حمایت از محرمانگی، صحت، تمامیت و قابلیت دسترسی سامانه‌های رایانه‌ای و به تبع آن داده‌های ذخیره شده در آنان در مقابل تجاوز و هجوم سایر سامانه‌های رایانه‌ای است. همچنین براساس تعریف مذکور وجود حداقل دو سامانه رایانه‌ای جهت شکل‌گیری مفهوم حمله سایبری لازم و ضروری است. به‌عبارت‌دیگر، می‌توان گفت مفهوم حمله سایبری تنها در فضای سایبری میان سامانه‌های رایانه‌ای با یکدیگر شکل می‌گیرد و در فضای سایبری میان کاربر با سامانه رایانه‌ای شکل نخواهد گرفت (برای مطالعه بیشتر نک: مرسی، ۱۳۹۷: ۲۵-۱۷).

برخی نویسندگان حمله سایبری را به این معنا می‌دانند: «ایجاد اخلال در صحت یا درستی داده‌ها که معمولاً از طریق اعمال کدهای مخرب و تغییر در منطق برنامه‌ها و کنترل داده‌ها صورت می‌گیرد و به خروجی‌های اشتباه توسط سامانه‌های رایانه‌ای منجر می‌شود» (جالینوسی، ابراهیمی و قنواتی، ۱۳۹۲: ۱۰). تعریف مذکور کانون توجه خود را بر نتایج ناشی از حمله سایبری متمرکز کرده است؛ درحالی‌که تعاریفی که کانون توجه خود را بر نتایج ناشی از حمله سایبری متمرکز می‌کنند از آن جهت دارای اشکال است که نمی‌توان میان مفهوم حمله سایبری با سایر مفاهیم مجرمانه مشابه قائل به تفکیک شد؛ زیرا در جرائمی

همچون دسترسی غیرمجاز، سرقت رایانه‌ای تخریب داده و غیره که با جرائم سایبری تحقق می‌پذیرد، نمی‌توان میان مفاهیم مشابه جرائم سایبری و جاسوسی سایبری با مفهوم حملات سایبری تمایزی قائل شد. برای مثال، عنوان مجرمانه «سرقت رایانه‌ای» که علیه محرمانگی تلقی می‌شود، از این قابلیت برخوردار است که علاوه بر حملات سایبری توسط جرائم سایبری هم ارتکاب می‌یابد.

در تعریف دیگری از حمله سایبری بیان شده است یک حمله سایبری شامل چهار حوزه از دست دادن تمامیت، از دست دادن قابلیت دسترسی، از دست دادن محرمانگی داده و اطلاعات و درنهایت تخریب فیزیکی سامانه‌های رایانه‌ای است (www.globalsecurity.org/military/library/policy/army). تعریف مذکور به‌گونه‌ای متفاوت کانون توجه خود را به روی نتایج ناشی از حملات سایبری معطوف کرده است.

همان‌طور که مشخص است تعاریف ارائه شده موسع هستند چراکه رفتار و موضوع را محدود نکرده و بر مرتکب و قصد خاصی نیز تأکیدی نشده است. این امر سبب می‌شود حمله سایبری، جرائم رایانه‌ای موضوع‌محور و وسیله‌محور را دربرگیرد[1] و نتوان میان آنها تفکیک قائل شد. درحالی‌که بدیهی است حمله سایبری اقسام جرائم وسیله‌محور از قبیل کلاهبرداری رایانه‌ای، نشر اکاذیب و هتک حیثیت افراد در فضای مجازی را دربرنمی‌گیرد؛ زیرا موضوع حمله سایبری همانند جرائم رایانه‌ای موضوع‌محور داده و سامانه رایانه‌ای است درحالی‌که موضوع جرائم رایانه‌ای وسیله‌محور داده و سامانه رایانه‌ای نیست بلکه آنها جرائم سنتی هستند که تنها وسیله ارتکاب سامانه رایانه‌ای است. ازاین‌رو، مفهوم

---

۱. در یک تقسیم می‌توان جرائم رایانه‌ای را به جرائم رایانه‌ای موضوع‌محور و جرائم سایبری وسیله‌محور دسته‌بندی کرد. جرائم رایانه‌ای موضوع‌محور جرائمی است که داده‌ها و سامانه‌های رایانه‌ای هدف یا موضوع جرم می‌باشند که «جرائم سایبری محض» نیز گفته می‌شود. در مقابل، جرائم رایانه‌ای وسیله‌محور، سامانه‌های رایانه‌ای وسیله ارتکاب جرم است (مرسی، ۱۳۹۷: ۴۰-۳۹).

موسع حمله سایبری معیاری برای تمییز مفهوم حمله سایبری از جرائم رایانه‌ای ارائه نمی‌دهد.

۲-۱. حمله سایبری در مفهوم مضیق

ریچارد ای.کلارک[1] در تعریف حملات سایبری بیان می‌دارد: «حملات سایبری مجموعه اقدام‌هایی است که یک دولت به‌منظور نفوذ یا ایجاد اخلال در سامانه‌های رایانه و یا شبکه رایانه‌ای، علیه دولت دیگر ارتکاب می‌یابد» (خلیل‌زاده، ۱۳۹۳: ۲۶). شایسته به‌نظر نمی‌رسد که ارتکاب حملات سایبری محدود به اقدام‌های مجرمانه‌ای در فضای سایبر شود که مرتکبی خاص مانند یک دولت علیه دولت دیگر انجام می‌دهد؛ زیرا در برخی از موارد نفوذگران[2] داخلی یک کشور می‌توانند در فضای سایبر عملیات مجرمانه‌ای را علیه سامانه‌های رایانه‌ای دولت خود مرتکب شوند که نتایج ناشی از آن در برخی موارد با عملیات مجرمانه‌ای که یک دولت علیه دولت دیگر در فضای سایبر مرتکب می‌شود تفاوت چندانی نخواهد داشت. همچنین باید در نظر داشت که ماهیت فضای سایبر این امکان را برای مهاجمان درون‌مرزی فراهم می‌سازد که آنان از همان بستری حمله کنند که مهاجمان برون‌مرزی از آن بستر برای حملات سایبری خود بهره می‌برند. ازطرفی باید یادآور شد دیگر نمی‌توان مفهوم امنیت ملی را همانند گذشته درخصوص مسائل نظامی و مرزهای داخلی و خارجی تعریف کرد، بلکه امروزه، خطر افت کیفیت زندگی شهروندان نیز نوعی تهدید علیه امنیت ملی محسوب می‌شود.

برخی دیگر حمله سایبری را مجموعه اقدام‌های مجرمانه‌ای دانسته‌اند که در جهت

---

1. Richard A. Clarke
2. Hacker

تضعیف عملکرد شبکه‌های رایانه‌ای برای اهداف امنیتی، سیاسی و ملی ارتکاب می‌یابد (Hathaway etal., 2012: 822-826)، تعریف مذکور متشکل از سه قسمت است: قسمت اول مجموعه رفتارهای مجرمانه‌ای است که در جهت جمع‌آوری اطلاعات، تعیین نقاط ضعف، نفوذ و درنهایت حمله انجام می‌گیرد. قسمت دوم تضعیف عملکرد شبکه‌های رایانه‌ای است، اولین عاملی که سبب تضییق مفهوم حملات سایبری می‌شود محدود کردن موضوع حملات سایبری به شبکه‌های رایانه‌ای است. شبکه‌های رایانه‌ای مجموعه‌ای از سامانه‌های رایانه‌ای خودمختار و متصل به یکدیگر هستند که توانایی تبادل اطلاعات با یکدیگر را دارند (خرم‌آبادی، ۱۳۹۱: ۱۹). منظور از تضعیف عملکرد شبکه‌های رایانه‌ای، ناکارایی سامانه‌های رایانه‌ای با اعمالی از قبیل اخلال در توزیع و سرویس خدمات،[1] ممانعت از دسترسی،[2] نفوذ به سامانه رایانه‌ای،[3] حذف وب‌سایت،[4] سوءاستفاده از مرورگرهای وب خصوصی و عمومی،[5] سوءاستفاده از پیام‌ها،[6] سرقت یا مالکیت غیرمجاز مالکیت معنوی (آی پی)[7] و غیره است که می‌توان آنان را به سه دسته کلی رفتارهای مجرمانه علیه محرمانگی، رفتارهای مجرمانه علیه صحت و رفتارهای مجرمانه علیه تمامیت شبکه‌های رایانه‌ای تقسیم کرد. قسمت سوم اهداف امنیتی، سیاسی و ملی است. توجه به اهداف مهاجمان سایبری عامل دیگری برای تضییق مفهوم حملات سایبری به‌شمار می‌رود. تعریف صریح و مشترکی از مفاهیمی همچون امنیت، امنیت عمومی، امنیت ملی صورت

1. Denial-of-service and Distributed Denial-of-service Attacks
2. Breach of Access
3. System Infiltration
4 Website Defacement
5. Private and Public Web Browser Exploits
6. Instant Messaging Abuse
7. Intellectual property (IP) Theft or Unauthorized Access

نگرفته است و هرکس از زاویه دید خود به تعریف آن پرداخته است که این امر از چندوجهی بودن مفهوم امنیت ناشی می‌شود؛ اما به‌طورکلی می‌توان وجوه و ابعاد مختلف امنیت را در محورهای سیاسی، اقتصادی، نظامی، فرهنگی و زیست‌محیطی دسته‌بندی کرد (ماندل، ۱۳۹۶: ۸۳-۷۱). برای مثال باری بوزان[1] امنیت را «رهایی از تهدید و توانایی دولت و جوامع برای حفظ هویت مستقل و یکپارچگی کارکردی در مقابل نیروی تغییردهنده» تعریف کرده است (Buzan, 1991: 432).

از دید آرنولد ولفرز[2] امنیت در مفهوم عینی به‌معنای فقدان تهدیدها نسبت به ارزش‌های اکتسابی تلقی می‌شود و در یک مفهوم ذهنی براساس دلهره و نگرانی از به مخاطره افتادن ارزش‌ها و توانمندی‌های لازم در کسب نتایج منصفانه ارزیابی می‌شود (چگینی‌زاده، ۱۳۷۹: ۶۷). ریچارد اولمن[3] در تعریف امنیت ملی بیان داشته است: «تهدید امنیت ملی اقدام یا سلسله رویدادهایی است که نخست، به شکلی مؤثر و در یک دوره زمانی کوتاه خطر افت کیفیت زندگی را برای ساکنان کشور پیش می‌آورد و دوم، با خطر جدی کاهش طیف خط‌مشی‌هایی که حکومت یا واحدهای غیرحکومتی خصوصی موجود در داخل کشور (اشخاص، گروه‌ها و شرکت‌ها) می‌توانند از میان آنان دست به انتخاب زنند، همراه است» (تریف و همکاران، ۱۳۸۴: ۴۹). مسلماً با این تعریف تصور ما از عوامل تهدیدزا دامنه بیشتری می‌یابد. برخی از نظریه‌پردازان، امنیت ملی را معادل با ارزش‌های حیاتی یک کشور می‌دانند (خلیلی‌پور رکن‌آبادی و نورعلی‌وند، ۱۳۹۱: ۱۷۵). بااین‌حال در مورد خصوصیات و ویژگی‌های امنیت ملی تحلیل‌گران به‌طور عمده بر سه ویژگی تحول‌پذیری، نسبی بودن و ذهنی بودن تأکید دارند.

---

1. Barry Buzan
2. Arnold Wolfers
3. Richard Ulman

برخی نیز در تعریف حمله سایبری علاوه بر آنکه مرتکب حمله سایبری را محدود به دولت می‌کنند، هدف آن را به زیرساخت‌های حیاتی یک کشور محدود می‌کنند به عبارتی: «اقدام‌هایی که دولت برای هدف قرار دادن زیرساخت‌های اساسی یک دولت دیگر ازجمله سیستم بانکی، انرژی و حمل‌ونقل عمومی که به شبکه رایانه‌ای متصل هستند صورت می‌پذیرد» (خلیل‌زاده، ۱۳۹۳: ۳۳).

همان‌طور که بیان شد، صحیح به‌نظر نمی‌رسد حملات سایبری را به مرتکب خاصی محدود کرد؛ بلکه شایسته است از اهداف مهاجمان سایبری به‌عنوان یک عامل مشدده مجازات در نظر گرفته شود یا تحت شرایطی به‌عنوان معیاری در جهت تغییر عنوان حملات سایبری به عناوینی همچون تروریسم سایبری و جنگ سایبری بهره گرفت. برای مثال، می‌توان گفت هرگاه یک حمله سایبری با هدف ایجاد رعب و وحشت میان مردم ارتکاب یابد آن حمله سایبری به‌عنوان تروریسم سایبری تغییر ماهیت یابد یا هرگاه اهداف مهاجمان سایبری از حملات خود مراکز نظامی یا منافع ملی یک کشور باشد، عنوان حمله سایبری به جنگ سایبری تغییر ماهیت یابد.

سازمان شانگهای،[1] تعریف دیگری از حملات سایبری ارائه کرده است. در این خصوص این سازمان حملات سایبری را «روشی روان‌شناسی ـ روان‌شناختی [برای] شستشوی مغزی جهت بی‌ثباتی جامعه و دولت و نیز وادار ساختن دولت برای تصمیم‌گیری در جهت منافع طرف مخالف یا دشمن تعریف کرده است»(Hathaway etal., 2012: 825) . علاوه بر این، سازمان مذکور انتشار اطلاعاتی را که به ضرر نظام‌های سیاسی، اجتماعی، اقتصادی، همچنین در زمینه‌های مذهبی، اخلاقی و فرهنگی سایر کشورها است از تهدیدهای اصلی علیه امنیت اطلاعات معرفی کرده است(Ibid.) . نظر برخی از نویسندگان این است

1. Shanghai

که سازمان شانگهای رویکرد موسع‌تری نسبت به حملات سایبری نشان داده است؛ با این استدلال که سازمان شانگهای حملات سایبری را جریان روان‌شناختی برای بی‌ثبات کردن جامعه و دولت در نظر گرفته است که موجب انتشار اطلاعات مضر در سامانه‌های رایانه‌ای اجتماعی، سیاسی، معنوی، فرهنگی و اخلاقی به‌منظور آسیب به امنیت اطلاعاتی می‌شود (خلیل‌زاده، ۱۳۹۳: ۲۷). درحالی‌که به‌نظر می‌رسد نظریه مذکور قابل خدشه است زیرا سازمان شانگهای با محدود کردن هدف و قصد در حملات سایبری که بی‌ثبات کردن جامعه و دولت است موجب تضییق مفهوم حملات سایبری شده است.

همان‌طور که مشخص است تعاریف ارائه شده مضیق هستند چراکه رفتار و موضوع را محدود کرده یا بر مرتکب و قصد خاصی تأکید داشته است. مضیق کردن موضوع حملات سایبری به داده‌ها و سامانه‌های رایانه‌ای موجب آن می‌شود که جرائم رایانه‌ای وسیله‌محور از شمول حملات سایبری خارج شوند و تنها جرائم رایانه‌ای موضوع‌محور از قبیل تخریب داده، اخلال در سامانه و ممانعت از دسترسی تحت شمول حملات سایبری قرار گیرند و مضیق کردن اهداف مرتکب به اهداف امنیتی موجب آن می‌شود که جرائم رایانه‌ای موضوع‌محور مطروحه در قانون جرائم رایانه‌ای از شمول مفهوم حملات سایبری نیز خارج شوند چراکه در تحقق آن جرائم اهداف امنیتی و به دنبال آن بر هم زدن امنیت کشور مطرح نیست. بنابراین باید توجه داشت از حیث عنصر مادی، رفتار فیزیکی حملات سایبری با جرائم رایانه‌ای موضوع‌محور همانند است اما از حیث ماهیت، اهداف جرم‌انگاری و اوصاف موضوع با یکدیگر متفاوتند که در ادامه در قسمت (تعریف مختار از حمله سایبری) به تبیین آنها پرداخته شده است.

۳-۱. مصادیق حملات سایبری در مفهوم مضیق

همان‌طور که بیان شد در عنصر مادی تنها از حیث رفتار فیزیکی حملات سایبری با جرائم رایانه‌ای موضوع‌محور همانند هستند. بنابراین رفتارهای فیزیکی در حملات سایبری همانند جرائم رایانه موضوع‌محور به سه دسته: ۱. رفتارهای ناقض محرمانگی؛ ۲. رفتارهای ناقض تمامیت و ۳. رفتارهای ناقض دسترس‌پذیری تقسیم‌بندی می‌شوند. ازطرف‌دیگر، قانونگذار در قوانین خود از عنوان حمله سایبری استفاده نکرده و این امر موجب آن شده است مقررات مستقیمی برای مقابله با حملات سایبری وجود نداشته باشد؛ بنابراین در وضعیت کنونی نظام حقوقی ایران فقط در قالب مصادیق ذیل می‌توان به تحلیل و مقابله کیفری با حملات سایبری پرداخت. باید در نظر داشت ممکن است مجازات‌های پیش‌بینی شده در قانون جرائم رایانه‌ای برای مرتکبان جرائم سایبری منصفانه و بازدارنده باشد اما برای مرتکبان حمله سایبری منصفانه و بازدارنده نیست؛ زیرا برای مثال شایسته نیست مرتکبان حمله سایبری علیه تأسیسات هسته‌ای ایران به همان مجازاتی محکوم شوند که یک کاربر عادی داده‌های متعلق به کاربر دیگر را حذف می‌کند و تأثیری در امنیت کشور ندارد. ازاین‌رو، گفتنی است مقنن هنگام جرم‌انگاری مستقل حملات سایبری مجازات‌های بازدارنده و متناسبی برای مرتکبان آن پیش‌بینی کند.

۱-۳-۱. سرقت رایانه‌ای

عنوان مجرمانه سرقت رایانه‌ای را می‌توان در نظام حقوقی ایران در ماده (۷۴۰) قانون مجازات اسلامی (تعزیرات) ملاحظه کرد.[۱] برخی از نویسندگان آن را مترادف با «هک» یا

---

۱. ماده (۷۴۰) قانون مجازات اسلامی مقرر می‌دارد: «هرکس به‌طور غیرمجاز داده‌های متعلق به دیگری را برباید، چنانچه عین داده‌ها در اختیار صاحب آن باشد، به جزای نقدی از یک میلیون (۱،۰۰۰،۰۰۰) ریال تا بیست میلیون (۲۰،۰۰۰،۰۰۰) ریال و در غیر این صورت به حبس از نودویک روز تا یک سال یا جزای نقدی از پنج میلیون (۵،۰۰۰،۰۰۰) ریال تا بیست میلیون (۲۰،۰۰۰،۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد».

«نفوذ غیرمجاز» در سامانه‌های رایانه در نظر گرفته‌اند (صبحی شیشوان، ۱۳۸۳: ۷۱-۶۱)، درحالی‌که به‌نظر می‌رسد مفاهیمی همچون «هک» یا «نفوذ غیرمجاز» ارتباط بیشتری با عنوان مجرمانه دسترسی غیرمجاز داشته باشد. برخی دیگر، سرقت رایانه‌ای را در مفهوم مضیق کپی غیرقانونی نرم‌افزارها تعریف کرده و در مفهوم موسع کپی غیرقانونی کالاها، نرم‌افزارها، اسناد، صوت‌ها و فیلم‌های دیجیتال تعریف کرده‌اند که در آن فرد با هر هدفی به‌صورت غیرقانونی و بدون اجازه دارنده به پشتیبان‌گیری اقدام می‌کند (مارکوم و هیگینز، ۱۳۹۷: ۱۳۵-۱۳۴). این نظر مطابق با ماده (۷۴۰) قانون مجازات اسلامی (تعزیرات) است و برمبنای آن حملات سایبری ارتکابی علیه جمهوری اسلامی مورد تحلیل و ارزیابی قرار گرفته است.

مفهوم دیگری که شایسته است مطرح شود، مفهوم سرقت هویتی است، در حقوق آمریکا تعریف شده است: «استفاده یا انتقال عامدانه و بدون مجوز قانونی اطلاعات دیگران با قصد ارتکاب جرم یا هر رفتار مجرمانه دیگری که ناقض قانون فدرال، ایالتی یا محلی باشد» (همان: ۹۸). ازاین‌رو، بعید به‌نظر نمی‌رسد که هدف از حمله سایبری سرقت هویت ملی یک کشور باشد که نتایجی از قبیل خسارت‌های مالی فراوان و بی‌اعتبارسازی یک کشور را به همراه داشته باشد.

در آبان ماه ۱۳۹۰ خبر از حمله بدافزاری به نام دوکو به تأسیسات صنعتی ایران بروز کرد (Wiles and Reyes, 2007). هدف از حمله سایبری دوکو جمع‌آوری و سرقت داده‌ها و اطلاعات بود؛ بدین‌معنا حمله سایبری دوکو تنها یک روتکیت،[1] سرقت اطلاعات بود (www.gerdab.ir/fa/news/8175) . طراحان بدافزار دوکو برای نفوذ به سامانه‌های رایانه‌ای

1. Rootkit

از یک اشکال ناشناخته‌ای که در مدیریت فونت[1]های موجود در هسته ویندوز وجود داشت به سامانه‌های رایانه‌ای موردنظر خود نفوذ کردند. سپس بدافزار به اجزای مختلف سامانه‌های رایانه‌ای نفوذ می‌کرد و با یک فایل متنی ورد[2] که از محصولات شرکت مایکروسافت[3] است، گسترش می‌یافت و سطح امنیت سامانه‌های رایانه‌ای را تحت تأثیر قرار می‌داد و به‌علت آنکه این بدافزار فایل‌هایی با پسوند دی کیو[4] می‌ساخت، متخصصان نام این بدافزار را دوکو نامیدند. بدافزار دوکو هنگامی که در سامانه‌های رایانه‌ای هدف قرار می‌گرفت عملکرد خود را در همان لحظه آغاز نمی‌کرد بلکه هنگامی‌که سامانه‌های رایانه‌ای برای مدت تقریباً ۱۰ دقیقه مورد استفاده قرار نمی‌گرفتند آغاز به فعالیت می‌کرد و به سرقت اطلاعات حساس صنعتی و دیگر سازمان‌ها می‌پرداخت.

درواقع طراحان دوکو به دنبال اطلاعاتی نظیر اسناد طراحی مورد استفاده در سامانه‌های کنترل، نظارتی و سرقت داده‌ها و اطلاعات سامانه‌های اسکادا[5] بودند تا احتمال شکست در زمان حمله به تأسیسات صنعتی و نیروگاه‌ها به‌اندازه چشمگیری کاهش یابد[6] (Ibid.).

---

1. Font
2. Word
3. Microsoft
4. DQ

۵. سامانه‌های اسکادا برای کنترل و نظارت بر فرایندهای مختلف (صنعتی، زیرساختی و تأسیساتی) به‌کار می‌رود. فرایندهای صنعتی شامل: تأسیسات تولیدی، تولید برق، پالایش نفت، استخراج معدن یا فعالیت‌های مشابه دیگر است که در محیط‌های شبیه به کارخانه رخ می‌دهند. فرایندهای زیرساختی حول سامانه‌های آب و فاضلاب، خطوط لوله انتقال نفت و گاز طبیعی، انتقال برق، سامانه‌های ارتباطی نظیر سامانه‌های تلفن همراه و کابل‌های ارتباط زمینی و دیگر سامانه‌های اداره‌کننده کالا و خدمات انجام می‌گیرند و معمولاً با نام خدمات عمومی رفاهی شناخته می‌شوند. فرایندهای تأسیساتی نیز فرایندهای مختلف گرمایشی، تهویه، با مصرف انرژی را تنظیم می‌کنند. سامانه‌های اسکادا تقریباً در همه اموری که با آن سروکار داریم به چشم می‌خورند(Andress and Winterfeld, 2011: 123) .

۶. در صورت پذیرش این امر که داده‌های سامانه‌های کنترلی مذکور با توجه به تبصره «۱» ماده (۷۳۱) قانون مجازات اسلامی (تعزیرات) سری محسوب می‌شوند ازآن‌جهت که در تبصره «۲» ماده پیش‌گفته نحوه تعیین و تشخیص داده‌های سری را موکول به تصویب آیین‌نامه اجرایی کرده است و تاکنون آیین‌نامه مذکور تصویب نشده است ماده (۷۳۱) قانون مجازات اسلامی (تعزیرات) قابلیت اجرا ندارد.

بدافزار پیچیده و پیشرفته فلیم[1] پس از استاکس‌نت و دوکو سومین بدافزار مهم رایانه‌ای بود که در مه ۲۰۱۲ علیه کشور ایران مورد استفاده قرار گرفت. در مورد عملکرد بدافزار فلیم کارشناسان بر این عقیده بودند که نه‌تنها اطلاعات را کپی و به سرور مقصد انتقال می‌داد بلکه توانایی تغییر در دستورات و اطلاعات موجود در سامانه‌های رایانه‌ای مورد نظر و همچنین توانایی فعال کردن میکروفن‌های سامانه‌های رایانه‌ای جهت ضبط کردن صداهای اطراف خود را داشت. دیگر توانایی‌های بدافزار فلیم که برای نخستین بار دیده شد، با استفاده از فناوری بلوتوث[2] برای انتشار خود به دیگر سامانه‌های رایانه‌ای بود که در فاصله کمی از سامانه رایانه‌ای آلوده قرار داشتند و به سرقت اطلاعات موجود در سامانه‌های رایانه‌ای اطراف نیز منجر می‌شد (مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر، ۱۳۹۱: ۳۳۳).

ازاین‌رو می‌توان به این نتیجه مهم دست یافت که یک مهاجم سایبری می‌تواند با سامانه رایانه‌ای خود علیه دیگر سامانه‌های رایانه‌ای، مرتکب رفتارهای مجرمانه‌ای شود به‌گونه‌ای که آنان را تحت کنترل خود درآورده و به‌عنوان ابزار و وسیله ارتکاب جرم علیه دیگر سامانه‌های رایانه‌ای استفاده کند بدون آنکه کاربران آنها مطلع شوند.

به‌عبارت‌دیگر عنوان حمله سایبری ازیک‌سو نسبت به سامانه‌های رایانه‌ای اولیه‌ای که مورد هدف او قرار می‌گیرند تحقق می‌یابد و ازسوی‌دیگر نسبت به سامانه‌های رایانه‌ای ثانویه‌ای که سامانه‌های رایانه‌ای اولیه مورد حمله قرار داده‌اند، قابل تحقق است.

پیرامون توانایی فعال کردن میکروفن سامانه‌های رایانه‌ای برای ضبط صداهای اطراف

---

1. Flame
2. Bluetooth

خـود بـا توجه به اینکه ضبط صداهای اطراف در فضای میان کاربر و سـامانه رایانه‌ای پدید می‌آید، شـاید در بادی امر عنوان مجرمانه شـنود غیرمجاز ناشـی از جرائم سـایبری مناسب به‌نظر رسـد؛ اما باید توجه داشـت صداهای اطراف داده‌های (صفر و یک) تلقی نمی‌شـوند تا عنوان مجرمانه شـنود غیرمجاز تحقق یابد بلکه ابتدا صداها را میکروفن دریافت و سـپس تبدیل به داده (صفر و یک) می‌کند؛ اما در مورد صداهایی که به‌صورت داده‌های دیجیتالی (صفر و یک) در سـامانه رایانه‌ای ذخیره و ارسـال می‌شـوند به‌نظر می‌رسـد عنوان مجرمانه سـرقت رایانه‌ای ناشـی از حملات سایبری قابل تحقق اسـت؛ زیرا ازیک‌سو صداهای ذخیره شـده به‌صـورت دیجیتالـی (صفـر و یـک) اسـت و ازسـوی‌دیگر در زیرفضـای سـایبری میان سامانه رایانه‌ای ذخیره و ارسال می‌شود.

درنهایـت نتیجـه‌ای کـه می‌تـوان گرفت هـدف از جرم‌انگاری در زمینه سـرقت ناشـی از حمـلات سـایبری نوعـی ماهیـت بازدارندگی دارد، زیـرا با جرم‌انـگاری آن سـبب جلوگیری از حملات سـایبری گسـترده با دامنـه نتایجی به‌مراتب زیان‌باری شـده که از سـرقت داده‌ها و اطلاعات قبلی به‌دست آمده‌اند.

۲-۳-۱. حملات سایبری ناقض تمامیت

درخصوص عناوین مجرمانه‌ای که با حملات سـایبری علیه تمامیت داده‌ها و سـامانه‌های رایانه‌ای در فضای سایبر تحقق می‌یابد و موجب آثار مخربی بر آنان می‌شود می‌توان به دو عنـوان مجرمانـه «تخریب داده» و «اخلال در سـامانه رایانه‌ای» دسـت یافت که در ادامه به آن پرداخته شده است.

۱-۲-۳-۱. تخریب داده

در حقـوق ایـران نیـز قانونگذار با تصویب مـاده (۷۳۶) قانون مجازات اسـلامی (تعزیرات) به

جرم‌انگاری عنوان مجرمانه تخریب داده‌های رایانه‌ای اقدام کرد تا خلأ پیش‌گفته در قوانین سنتی موجود را برطرف سازد.[۱]

۲-۲-۳-۱. اخلال در عملکرد سامانه رایانه‌ای

قانونگذار در ماده (۷۳۷) قانون مجازات اسلامی (تعزیرات) عنوان مجرمانه اخلال در سامانه‌های رایانه‌ای را پیش‌بینی کرد.[۲] استاکس‌نت نقطه‌عطفی در حملات سایبری ایجاد کرد و سبب شد نظرات افراد زیادی را درباره اینکه یک حمله سایبری تحت شرایط و ویژگی‌های خاص مصداق جنگ در فضای سایبر تلقی شود، به خود جلب کند (شلدون، ۱۳۹۱: ۳۲۰). همان‌طور که در مقدمه پژوهش ماهیت و نحوه عملکرد بدافزار استاکس‌نت بیان شد کدها و دستورالعمل‌های جدیدی را به سامانه‌های کنترلی وارد می‌کرد تا تعداد دور بر دقیقه سانتریفیوژها را تغییر دهد. تغییر دور بر دقیقه سانتریفیوژها مستلزم تغییر در دستورالعمل‌های از پیش تعریف شده سامانه‌های رایانه‌ای است؛ درنتیجه می‌توان حمله سایبری مذکور را مصداق بند «ب» ماده (۷۳۴) قانون مجازات اسلامی (تعزیرات) قرار داد اما ازآنجاکه حمله سایبری یادشده باعث تغییر عملکرد سامانه رایانه‌ای به‌عبارت‌دیگر باعث «مختل شدن» سامانه رایانه‌ای شده است به‌نظر می‌رسد در این حالت چون عمل خاص (تغییر داده) مشمول ماده خاص قانون است تنها همان عنوان خاص یعنی اخلال در عملکرد سامانه رایانه‌ای شود.

---

۱. ماده (۷۳۶) قانون مجازات اسلامی مقرر می‌دارد: «هرکس به‌طور غیرمجاز داده‌های دیگری را از سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده حذف یا تخریب یا مختل یا غیرقابل پردازش کند به حبس از شش ماه تا دو سال یا جزای نقدی از بیست‌وپنج میلیون (۲۵. ۰۰۰. ۰۰۰) ریال تا صد میلیون (۱۰۰. ۰۰۰. ۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد».

۲. ماده (۷۳۷) قانون مجازات اسلامی مقرر می‌دارد: «هرکس به‌طور غیرمجاز با اعمالی از قبیل وارد کردن، 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».

۳-۳-۱. ناقض قابلیت دسترسی

در حقوق ایران عنوان «ممانعت از دسترسی» با وضع ماده (۷۳۸) قانون مجازات اسلامی (تعزیرات) به‌طور مستقل و جدای از عنوان مجرمانه «تخریب داده» و «اخلال در سامانه رایانه‌ای» پیش‌بینی شده است.[۱] حملات سایبری علیه کشور استونی که در سال ۲۰۰۷ آغاز شد می‌تواند نمونه‌ای از حملات سایبری باشد که مصداق عنوان مجرمانه ممانعت از دسترسی تلقی شود؛ زیرا طبق نظر حملات توزیع‌یافته اختلال در سرویس‌دهی (دی داس)[۲] موجب شد سایت‌های قربانی از دسترس خارج شوند و توانایی ارائه خدمات نداشته باشند (Tikk, Kaska and Vihul, 2010: 20). سپس فعالیت نهادهای بزرگ مانند بانک‌ها، سازمان‌ها و غیره را تحت تأثیر قرار داد به‌گونه‌ای که مانع خدمات عمومی اینترنتی از قبیل: ارائه گزارش‌های مالیاتی، درخواست برای یارانه‌ها و مزایای دولتی و غیره شد که دولت برای رفاه حال شهروندان در نظر گرفته بود (Ibid.: 21).

درباره تحلیل ماهیت حقوقی حمله مذکور می‌توان اذعان داشت ازآنجاکه حملات (دی داس) به تخریب داده یا اخلال در سامانه رایانه‌ای منجر نمی‌شود بلکه به‌علت اضافه‌بار تنها موجب ممانعت از دسترسی به سایت‌ها می‌شود؛ می‌توان آن را مصداق عنوان مجرمانه «ممانعت از دسترسی» قرار داد(Ibid.: 20) .

---

۱. ماده (۷۳۸) قانون مجازات اسلامی مقرر می‌دارد: «هرکس به‌طور غیرمجاز با اعمالی از قبیل مخفی کردن داده‌ها، تغییر گذرواژه یا رمزنگاری داده‌ها مانع دسترسی اشخاص مجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی شود، به حبس از نودویک روز تا یک سال یا جزای نقدی از پنج میلیون (۵. ۰۰۰. ۰۰۰) ریال تا بیست میلیون (۲۰. ۰۰۰. ۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد».

2. DDOS

۲. تعریف مختار از حملات سایبری

حملات سایبری به اعمالی اطلاق می‌شود که برای اهداف امنیتی با سامانه‌های رایانه‌ای به قصد تضعیف تمام یا بخش اعظمی از سامانه‌های رایانه‌ای متعلق به یک گروه خاص اعم از سازمان‌ها، نهادها و غیره ارتکاب می‌یابد. بدین‌ترتیب مفهوم حمله سایبری هریک از اعمال مشروحه زیر است که برای اهداف امنیتی با سامانه‌های رایانه‌ای به قصد تضعیف تمام یا بخش اعظمی از سامانه‌های رایانه‌ای متعلق به یک‌گروه خاص ارتکاب می‌یابد:

۱. اخلال در سامانه‌های رایانه‌ای،

۲. تخریب داده‌های ذخیره شده در سامانه‌های رایانه‌ای،

۳. تغییر در داده‌های ذخیره شده موجود در سامانه‌های رایانه‌ای،

۴. ممانعت از دسترسی به سامانه‌های رایانه‌ای و داده‌های موجود ذخیره شده،

۵. رونوشت یا برش از داده‌های ذخیره شده موجود در سامانه‌های رایانه‌ای.

گروه خاص در تعریف مذکور از قبیل سازمان‌ها، نهادها و غیره است که حمله به داده‌ها و سامانه‌های رایانه‌ای متعلق به آنها امنیت کشور را به مخاطره می‌اندازد. لازم است قانونگذار به همراه جرم‌انگاری حمله سایبری فهرستی از مصادیق این گروه خاص را ارائه دهد.

مطابق با تعریف فوق می‌توان مصادیق عنصر مادی حملات سایبری را تحت عناوین جرائم علیه صحت، تمامیت و دسترس‌پذیری سامانه‌های رایانه‌ای و داده‌های ذخیره شده در آن قرار داد. همان‌گونه که در تعریف فوق معلوم است حمله سایبری مفهومی ناظر بر جرم خاص نیست بلکه شامل مجموعه‌ای از اعمال مجرمانه است که معمولاً در سطحی وسیع و گسترده تحقق می‌یابد.

در حقوق کیفری انجام عملی مادی که قانونگذار آن را جرم‌انگاری کرده برای احراز

مجرمیت کافی نیست، بلکه لازم است مجرم از نظر روانی نیز بر ارتکاب جرم قصد مجرمانه داشته باشد. براساس ماده (۱۴۴) قانون مجازات اسلامی[۱] که برای تحقق جرائم عمدی علم مرتکب به موضوع جرم را شرط دانسته است؛ باید مهاجم سایبری علم و آگاهی داشته باشد که رفتار مجرمانه‌اش درخصوص سامانه رایانه‌ای و به تبع آن داده‌های ذخیره شده در آن است. همچنین برای تحقق جرائم عمدی براساس ماده (۱۴۴) قانون مجازات اسلامی قصد ارتکاب جرم نیز شرط است.

پیرامون عنصر روانی حمله سایبری می‌توان بیان داشت که حمله سایبری عملیات مجرمانه سایبری است که اغلب با انگیزه برتری‌طلبی‌های گروهی به قصد تضعیف عملکرد تمام یا بخش اعظمی از شبکه‌های رایانه‌ای متعلق به یک گروه خاص صورت می‌گیرد. به‌عبارت‌دیگر سامانه‌های رایانه‌ای قربانی حملات سایبری، نه به‌عنوان یک سامانه رایانه‌ای بلکه عضوی از یک شبکه رایانه‌ای متعلق به یک گروه خاص، قربانی می‌شود. به‌عبارت‌دیگر، هدف مستقیم حمله سایبری سامانه‌های رایانه‌ای متعلق به یک گروه خاص است نه صرف سامانه رایانه‌ای. لذا چنین اعمالی معمولاً براثر یک حادثه یا قصور ساده ارتکاب نمی‌افتد بلکه به قصد تضعیف عملکرد تمام یا بخش اعظمی از شبکه‌های رایانه‌ای متعلق به یک گروه خاص انجام می‌پذیرد.

احراز قصد و نیت خاص حملات سایبری، یعنی قصد تضعیف تمام یا بخش اعظمی از سامانه‌های رایانه‌ای متعلق به یک گروه خاص امری دشوار است، زیرا قصد امری ذهنی و درونی است و تأکید بر لزوم اثبات آن باعث بلاکیفر ماندن بسیاری از مهاجمان سایبری

---

۱. ماده (۱۴۴) قانون مجازات اسلامی: «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 براساس قانون منوط به تحقق نتیجه است، قصد نتیجه یا علم به وقوع آن نیز باید محرز شود».

می‌شود. بنابراین می‌توان برای حل این مشکل، شرایط و اوضاع احوال پیرامون حملات سایبری یا قرائن و شواهد بیرونی قضیه که جنبه عینی دارند را مورد توجه قرار داد.

این اوضاع و احوال عوامل گوناگونی چون ماهیت کلی آن اعمال؛ ارتکاب آن در منطقه‌ای خاص، تکرار، استمرار و وسعت حملات سایبری و غیره شامل خواهد شد. به‌عبارت‌دیگر کیفیت وقایع ممکن است به‌گونه‌ای باشد که ثابت کند مهاجم می‌دانسته یا علم به وقوع داشته است. قصد خاص حملات سایبری از جهت اینکه وجه فارق آن از دیگر عملیات‌های مجرمانه سایبری و جرائم مندرج در نظام‌های ملی است، نیز اهمیت خاصی دارد. اگرچه اعمالی که از مصادیق حملات سایبری تلقی می‌شوند در عناوین خاص خود، چون تخریب داده، اخلال در سامانه رایانه‌ای و غیره، در قوانین سایر کشورها جرم شناخته شده‌اند اما هدف ارائه مفهوم جدید حمله سایبری به‌عنوان یکی از مهم‌ترین عملیات‌های مجرمانه سایبری حمایت از سامانه‌های رایانه‌ای موجود در شبکه‌های رایانه‌ای متعلق به یک گروه خاص است و این چیزی فراتر از حمایت از سامانه‌های رایانه‌ای فردی است. بنابراین اگر اعمال ارتکابی بدون توجه به تعلق سامانه یا سامانه‌های رایانه‌ای قربانی به گروهی خاص یا بدون قصد تضعیف عملکرد سامانه‌های رایانه‌ای موجود در شبکه‌های رایانه‌ای متعلق به یک گروه خاص انجام شود، مرتکب فقط به‌عنوان جرمی سایبری تحت تعقیب قرار می‌گیرد و نه حملات سایبری. برای مثال هدف حمله سایبری استاکس‌نت که علیه سامانه‌های رایانه‌ای مشغول به‌کار در نیروگاه هسته‌ای ایران در نطنز ارتکاب یافت، صرف سامانه رایانه‌ای نبود بلکه به این اعتبار بود که این سامانه‌های رایانه‌ای مشغول به‌کار در نیروگاه هسته‌ای بودند.

پرسشی که قابلیت طرح دارد آن است که هرگاه یک حمله سایبری علیه سامانه‌های رایانه‌ای به‌گونه‌ای ارتکاب یابد که علاوه بر نقض قوانین سایبری به نقض قوانین سنتی منجر شود، برای محکومیت مهاجمان سایبری احراز دو سوءنیت ضروری است؟ برای

مثال حمله استاکس‌نت که علیه تأسیسات نیروگاه هسته‌ای ایران ارتکاب یافت به‌گونه‌ای طراحی شده بود که بدافزار دستورالعمل‌های جدیدی را در پی ال سی‌ها[1] بارگذاری کند. پی ال سی‌ها وظیفه داشتند سرعت چرخش سانتریفیوژها را بین ۸۰ تا ۱۲۰ دور در دقیقه نگه دارند؛ اما بدافزار استاکس‌نت کدها و دستورالعمل‌های جدیدی را به آنها داد تا تعداد دور بر دقیقه سانتریفیوژها را تغییر دهد؛ در طول زمان، این بدافزار سبب می‌شد سرعت سانتریفیوژها به حدی بالا روند تا از کار بیفتند.

همچنین حمله سایبری اخیری که روز یکشنبه بیست‌ودوم فروردین ماه ۱۴۰۰ علیه شبکه برق تأسیسات غنی‌سازی نطنز ایران ارتکاب یافت، موجب انفجار در آن مرکز شد که ممکن بود به کشته شدن بسیاری از کارکنان آنجا منجر شود. آیا احراز قصد تخریب تأسیسات غنی‌سازی نطنز یا قصد کشته شدن کارکنان آنجا ضروری است؟ به‌نظر می‌رسد در این‌گونه موارد که با حمله سایبری یک نتیجه در فضای سایبر و یک نتیجه در فضای واقعی حاصل می‌شود، باید میان قصد نتیجه در فضای سایبر و قصد نتیجه در فضای فیزیکی تمایز قائل شد و درنتیجه آن، احراز دو سوءنیت مجزا لازم و ضروری باشد.

بنابراین در مثال‌های فوق برای محکومیت مهاجمان سایبری تحت عنوان مجرمانه اخلال در عملکرد سامانه‌های رایانه‌ای کنترلی لازم است تا قصد اولیه او که در فضای سایبر تحقق می‌یابد یعنی اخلال در عملکرد سامانه‌های رایانه‌ای کنترلی یا علم به وقوع آن احراز شود و قصد تبعی او در مورد نتیجه دوم که در فضای واقعی تحقق می‌یابد یعنی تخریب تأسیسات غنی‌سازی یا قصد کشته شدن کارکنان آنجا یا علم به وقوع آن با توجه به ذیل ماده (۱۴۴) قانون مجازات اسلامی احراز شود. به‌نظر می‌رسد در صورت احراز قصد اولیه و

---

۱. Programmable Logic Controller(PLC) در هر کارخانه، برای کنترل تجهیزات از سامانه‌های رایانه‌ای خاصی موسوم به پی ال سی استفاده می‌شود که درواقع نوعی کنترلگر قابل برنامه‌ریزی منطقی‌اند.

تبعی، رفتار ارتکابی مهاجم سایبری مشمول تبصره «۱» ماده (۱۳۴) قانون مجازات اسلامی قرار گیرد.[۱]

به‌طورکلی سوءنیت خاص اولیه همه حملات سایبری که در فضای مجازی تحقق می‌یابند شامل یک یا چند مورد از موارد قصد تخریب داده، اخلال در سامانه رایانه‌ای، ممانعت از دسترسی به سامانه رایانه‌ای و داده رایانه‌ای، تغییر، رونوشت و برش داده‌های رایانه‌ای و سوءنیت خاص تبعی همه حملات سایبری از بین بردن امنیت یک کشور است. این سوءنیت می‌تواند در قالب‌هایی از قبیل حمله به سامانه‌های متعلق به نیروگاه هسته‌ای یا سامانه‌های متعلق به مراکز ارائه خدمات ضروری عمومی از قبیل خدمات درمانی، آب، گاز، مخابرات، حمل‌ونقل و بانکداری تحقق یابد.

همان‌طور که مشخص است تعریف ارائه شده در این قسمت در زمره تعاریف مضیق حملات سایبری قرار می‌گیرد؛ زیرا از حیث موضوع و اهداف محدود شده است.

۳. تفاوت‌های میان حمله سایبری و جرائم رایانه‌ای موضوع‌محور

پس از شناخت مفهوم حمله سایبری و ارائه یک تعریف جامع و مانع از حمله سایبری مشخص شد که از هیچ حیثی با جرائم رایانه‌ای وسیله‌محور مشابهتی ندارد، تنها در عنصر مادی از حیث رفتار فیزیکی با جرائم رایانه‌ای موضوع‌محور مشابهت دارد و از سایر حیث‌ها

---

۱. ماده (۱۳۴) قانون مجازات اسلامی: «در جرائم موجب تعزیر هرگاه جرائم ارتکابی بیش از سه جرم نباشد دادگاه برای هریک از آن جرائم حداکثر مجازات مقرر را حکم می‌کند و هرگاه جرائم ارتکابی بیش از سه جرم باشد، مجازات هریک را بیش از حداکثر مجازات مقرر قانونی مشروط به اینکه از حداکثر به‌اضافه نصف آن تجاوز نکند، تعیین می‌نماید. در هریک از موارد فوق فقط مجازات اشد قابل اجرا است و اگر مجازات اشد به یکی از علل قانونی تقلیل یابد یا تبدیل یا غیرقابل اجرا شود، مجازات اشد بعدی اجرا می‌گردد.

در هر مورد که مجازات فاقد حداقل و حداکثر باشد، اگر جرائم ارتکابی بیش از سه جرم نباشد تا یک‌چهارم و اگر جرائم ارتکابی بیش از سه جرم باشد تا نصف مجازات مقرر قانونی به اصل آن اضافه می‌گردد.

تبصره «۱». درصورتی‌که از رفتار مجرمانه واحد، نتایج مجرمانه متعدد حاصل شود، طبق مقررات فوق عمل می‌شود».

متفاوت است. وجود این تفاوت‌ها ضرورت جرم‌انگاری مستقل حمله سایبری را می‌طلبد که در این قسمت به تبیین این تفاوت‌ها پرداخته شده است.

۱-۳. تفاوت در ماهیت

در یک تقسیم‌بندی می‌توان جرائم را در دو دسته قرار داد: دسته اول جرائمی که ارتکاب رفتار مجرمانه به همراه شرایط و عنصر معنوی محقق جرم است. رفتار مجرمانه این جرائم مستقل از یکدیگر است؛ اما دسته دوم جرائم، مانند نسل‌کشی، جرائم علیه بشریت، جرائم جنگی است که یک رفتار واحد، محقق جرم نیست بلکه این عناوین بر دسته‌ای از جرائم یا رفتارهای مجرمانه متفاوت بار می‌شود که خود این رفتارها نیز جرائم مستقلی هستند. برای مثال رفتار جرائم علیه بشریت شامل قتل، تجاوز جنسی، شکنجه، حبس غیرقانونی و غیره است؛ زمانی جرم علیه بشریت را تشکیل می‌دهد که همراه با حمله گسترده و یا سازمان‌یافته علیه یک جمعیت غیرنظامی ارتکاب یابد. درواقع رفتار این جرائم همان جرائم دسته اول است لیکن شرایط دیگری بر آنان اضافه شده و دسته‌ای از رفتارها را دربرمی‌گیرد. درصورتی‌که جرمی در دسته دوم قرار می‌گیرد نیاز به جرم‌انگاری مستقل داشته تا قانونگذار با پیش‌بینی شرایط اختصاصی، جرائم سنتی را به‌عنوان رفتار این جرائم پیش‌بینی و با آنان برخورد شدیدی کند. در غیر این صورت ناگزیر باید به عناوین مجرمانه‌ای که در دسته نخست وجود دارد دست یازید. برای مثال به‌دلیل عدم جرم‌انگاری نسل‌کشی در حقوق کیفری ایران درصورتی‌که فردی به قصد نابودی یک گروه قومی، ملی، مذهبی و نژادی مرتکب قتل شود تنها به‌عنوان قتل عمد قابل تعقیب است. ماهیت حملات سایبری از دسته دوم است. بدین معنا که رفتار آنها، جرائم دیگر است که در قانون جرائم رایانه‌ای پیش‌بینی شده‌اند ازاین‌رو با توجه به ارتکاب منسجم و

سازمان‌یافته آنها، گستردگی نتایج زیان‌بار ناشی از آنها و هدف ارتکاب آنها که بر هم زدن امنیت یک کشور است، ضروری است مقنن آن را به‌عنوان یک جرم مستقل پیش‌بینی کند. لیکن در صورت فقدان این پیش‌بینی، چنانچه در حقوق ایران چنین است، نهایتاً می‌توان به عناوین خردتر و جرائمی که در دسته نخست قرار دارند، یعنی مواد پیش‌بینی شده در قانون جرائم رایانه‌ای متوسل شد و بدان عناوین حمله‌کنندگان را کیفر کرد.

اغلب حملات سایبری را یک دولت علیه دولت دیگر انجام می‌دهد برخلاف جرائم رایانه‌ای موضوع‌محور ماهیت ملی ندارد بلکه یک ماهیت فراملی است. همچنین ازآنجاکه جنگ سایبری از بستر حمله سایبری تحقق می‌یابد نه جرم رایانه‌ای برخی نویسندگان عقیده دارند فقدان چنین تفکیکی (میان جرم رایانه‌ای و حمله سایبری) قطعاً دست مفسران و سیاستگذاران را در اعمال گسترده چارچوب قواعد جنگ در فضای سایبر را که از بستر و گذرگاه حمله سایبری عبور می‌کند باز می‌گذارد که مسلماً می‌تواند تبعات خطرناک و سوئی در گسترش جنگ و جنگ‌طلبی کشورها به همراه داشته باشد (اصلانی و رنجبریان، ۱۳۹۴: ۲۶۵). عدم دسته‌بندی میان این مفاهیم به نوعی لجام‌گسیختگی در تفسیر و طبعاً اعمال قواعد حقوق بین‌الملل بنا به مصلحت و مصالح ملی و نظامی منجر خواهد شد که در نوع خود. خواسته و ناخواسته. می‌تواند معادلات موجود در روابط بین‌المللی را به مخاطره بیندازد (همان: ۲۶۹). ازاین‌رو، برخی از نویسندگان مبحث حمله سایبری و مباحث مرتبط با آن را یعنی جنگ سایبری و تروریسم سایبری را در قلمرو و فضای حقوق بین‌الملل مورد تحلیل و ارزیابی قرار داده‌اند (همان: ۲۶۱).

۲-۳. تفاوت در هدف جرم‌انگاری

مفهوم حملات سایبری و جرائم رایانه‌ای موضوع‌محور دو هدف متفاوت در جرم‌انگاری

است. در جرائم رایانه‌ای موضوع‌محور هدف حمایت از داده‌ها و سامانه‌های رایانه‌ای است درحالی‌که هدف از جرم‌انگاری حملات سایبری حمایت از امنیت و اقتدار یک کشور در فضای مجازی است. ازاین‌رو در اغلب حملات، مرتکبان حملات خود را متوجه داده‌ها و سامانه‌های مرتبط با امنیت ملی می‌کنند. بنابر این هدفی که مقنن از جرم‌انگاری حمله سایبری دنبال می‌کند، امری فراتر از هدف مقنن از جرم‌انگاری جرائم رایانه‌ای است.

۳-۳. تفاوت در اوصاف موضوع

موضوع حمله سایبری همانند جرائم رایانه‌ای موضوع‌محور داده‌ها و سامانه‌های رایانه‌ای هستند اما بنابر تعریف ارائه شده از حمله سایبری، آن داده‌ها و سامانه‌های رایانه‌ای دارای اوصاف دیگری هستند که در ادامه به تبیین آنها پرداخته شده است.

۱-۳-۳. تعلق داده‌ها یا سامانه‌های رایانه‌ای به گروه خاص

ممکن است در بادی امر با لحاظ ماده (۷۳۹) قانون مجازات اسلامی به‌نظر رسد مقنن در قانون جرائم رایانه‌ای ازیک‌طرف به اهداف امنیتی و ازطرف‌دیگر، به تعلق سامانه‌های رایانه‌ای به یک گروه خاص توجه داشته است و این ماده ضرورت جرم‌انگاری مستقل حملات سایبری را ساقط می‌کند. در پاسخ باید گفت به‌رغم اینکه در اقدامی شایسته مقنن برای رفتارهای مجرمانه تخریب داده، اخلال در سامانه رایانه‌ای و ممانعت از دسترسی چنانچه علیه سامانه‌های رایانه‌ای ارائه‌دهنده خدمات ضروری عمومی ارتکاب یابند مجازات شدیدتری در نظر گرفته است،[۱] اما این

---

۱. ماده (۷۳۹) قانون مجازات اسلامی مقرر می‌دارد: «هرکس به قصد خطر انداختن امنیت، آسایش و امنیت عمومی اعمال مذکور در مواد (۸)، (۹) و (۱۰) این قانون را علیه سامانه‌های رایانه‌ای و مخابراتی که برای ارائه خدمات ضروری عمومی به‌کار می‌روند، از قبیل خدمات درمانی، آب، برق، گاز، مخابرات، حمل‌ونقل و بانکداری مرتکب شود، به حبس از سه تا ده سال محکوم خواهد شد».

امر، نیاز جرم‌انگاری مستقل حملات سایبری را مرتفع نمی‌سازد چراکه اولاً همان‌طور که قبلاً بیان شد از حیث ماهیت و اهداف، حملات سایبری با جرائم رایانه‌ای متفاوت هستند. ثانیاً، ممکن است سامانه‌های متعلق به یک سازمان یا نهادی جهت ارائه خدمات ضروری عمومی نباشد ولی اخلال در آن سامانه‌های رایانه‌ای امنیت کشور را به خطر بیاندازد مانند سامانه‌های متعلق به تأسیسات هسته‌ای. ثالثاً، رفتارهای فیزیکی ناشی از حملات سایبری علاوه بر موارد مذکور در ماده یادشده شامل سرقت رایانه‌ای نیز می‌شود. رابعاً، حملات سایبری برخلاف جرائم رایانه‌ای به‌نحو گسترده و سازمان‌یافته ارتکاب می‌یابند و درنهایت اینکه میزان مجازات پیش‌بینی شده در قانون یادشده ممکن است برای مرتکبان جرائم رایانه‌ای بازدارنده و منصفانه باشد اما برای مرتکبان حملات سایبری بازدارنده و منصفانه نخواهد بود.

۲-۳-۳. شبکه‌ای بودن داده‌ها و سامانه‌های رایانه‌ای

منظور از شبکه‌ای بودن داده‌ها و سامانه‌های رایانه‌ای آن است که داده‌ها و سامانه‌های رایانه‌ای در بستر شبکه رایانه‌ای قرار داشته باشند. شبکه‌های رایانه‌ای مجموعه‌ای از سامانه‌های رایانه‌ای خودمختار و متصل به یکدیگر هستند که توانایی تبادل اطلاعات با یکدیگر را داشته باشند (خرم‌آبادی، ۱۳۹۱: ۱۹). در تحقق جرائم رایانه‌ای موضوع‌محور لازم و ضروری نیست که داده‌ها و سامانه‌های رایانه‌ای در بستر شبکه رایانه‌ای قرار گرفته شده باشند. برای مثال هنگامی که کاربر داده‌های فردی را از یک کارت حافظه[1] حذف می‌کند در بستر شبکه رایانه‌ای مرتکب عنوان مجرمانه تخریب داده نشده است بلکه در بستری غیر از شبکه رایانه‌ای مرتکب عنوان مجرمانه تخریب داده شده است. اما رفتارهای فیزیکی در حملات سایبری از قبیل تخریب داده، اخلال در سامانه رایانه‌ای در بستر شبکه

1. Flash Memory

رایانـه‌ای ارتـکاب می‌یابند و همین بسـتر شـبکه‌ای بـودن و ماهیت سـازمان‌یافته بودن آن سـبب گستردگی نتایج زیان‌بار ناشی از حملات سـایبری نسبت به جرائم رایانه‌ای می‌شود؛ زیـرا هنگامی که مرتکبان حملات سـایبری به یک سـامانه رایانه‌ای نفـوذ کردند ازآنجاکه آن سـامانه یـا سـامانه‌های رایانه‌ای متعلق به یک شـبکه رایانه‌ای هسـتند، اخـلال در عملکرد آن سـامانه می‌توانـد در همـه سـامانه‌های رایانـه‌ای متصل به شـبکه اخلال به‌وجـود آورد و درنهایت تمام شبکه را از کار بیاندازد.

بسـتر شـبکه رایانـه‌ای بـرای حمـلات سـایبری امـکان فرامرزی بـودن ارتـکاب حملات سـایبری را بـرای مرتکبـان بـه ارمغـان مـی‌آورد؛ زیـرا آنـان از توانایی‌هـای لازم بـرای عبـور از محـدوده مرزهـای جغرافیایـی جهـت رسـیدن بـه اهـداف اصلـی خود برخـوردار می‌شـوند (عظیمی و خشنودی، ۱۳۹۵: ۱۶۴).

۴. اصول و مبانی جرم‌انگاری مستقل حمله سایبری

وقـوع حمله سـایبری در فضای سـایبر امری مسـلم و انکارناپذیر اسـت. آنچـه در این میان مهم اسـت نوع واکنش اتخاذ شـده ازسوی حکومت در قبال آن است. راهبرد شایسته برای مقابله با آن جرم‌انگاری مستقل در چارچوب حقوق کیفری است. ازآنجاکه شدیدترین شیوه برخورد حکومت با اعمال و رفتارهای افراد از رهگذر تصویب قوانین و مقررات کیفری نمایان می‌شـود و به این طریق بخشـی از گستره آزادی فردی به‌نفع اقدام‌های قهری دولت مضیق می‌شـود، بایـد معیارها و ضوابطی بـرای به‌کارگیری فرایند جرم‌انگاری موجود باشـد تا ضمن مشـروعیت یافتن اسـتفاده از ضمانـت اجرای کیفری ازسـوی حکومت از تعـرض غیرقانونی بـه آزادی‌هـای افراد جلوگیری به‌عمل آید. بـه موازات گزینش چنین رویکـردی درباره حمله سایبری پرسشی که مطرح می‌شود این است که جرم‌انگاری حمله سایبری و اعمال واکنش

کیفری درباره آن با کدام اصل یا اصول توجیه‌کننده جرم‌انگاری در تخصیص ضمانت اجرای کیفری برای رفتارهای مذکور مورد استفاده قرار می‌گیرد که در پاسخ می‌توان به اصل ضرر، مصلحت عمومی، ضرورت، تناسب جرم و مجازات و اصل لزوم توجه به راهبردها، رویکردها و همکاری بین‌المللی اشاره کرد.

۱-۴. اصل ضرر

این فلسفه که انسان تا جایی‌که به دیگری ضرر نمی‌رساند آزاد است، منجر به مداخله «حداقلی» حقوق کیفری در قلمرو آزادی‌های فردی در فضای سایبر می‌شود. بنا بر اصل مذکور، اگر بخواهیم اصل ضرر، موجبات دخالت بی‌اندازه دولت در فضای سایبر را در پی نداشته باشد باید برای شدت ضرر ملاکی داشته باشیم؛ زیرا هر نوع رفتار آدمی می‌تواند متضمن ضرر به دیگری باشد. ازاین‌رو سه مدل جرم‌انگاری اصل ضرر در فضای سایبر خطرآفرینی انتزاعی، خطرآفرینی واقعی و ضرر شدید قابل طرح است.[۱]

با توجه به جنبه سازمان‌یافته بودن و گستردگی نتایج زیان‌بار ناشی از حمله سایبری که امنیت کشور را تحت‌الشعاع قرار می‌دهد، از میان سه مدل یادشده حمله سایبری از مصادیق سومین مدل جرم‌انگاری اصل ضرر در فضای سایبر، یعنی مدل جرم‌انگاری ضررهای شدید است که هدف آن حمایت از ارزش‌ها و منافع ملی در فضای سایبر، در برابر

---

۱. نخستین مدل جرم‌انگاری اصل ضرر در جرائم سایبری مدل خطرآفرینی انتزاعی است که جرم‌های ناشی از آن به‌طور معمول، ضرر وارد را مستقیم مجازات نمی‌کنند. در این مدل نقض مقررات و قوانین اداری یا محدوده مجازی که در پروانه‌ها و مجوزهای اداری اجازه داده شده، جرم‌انگاری شده است. این مدل در ماده (۲۱) قانون جرائم رایانه‌ای پیش‌بینی شده است. دومین مدل جرم‌انگاری اصل ضرر در فضای سایبر، مدل خطرآفرینی واقعی است که برمبنای آن صرف تخلف از مقررات اداری و مجوزها و پروانه‌های صادر شده برای ارائه خدمات رایانه‌ای، کافی نیست، بلکه تهدید به آسیب کافی است. این مدل در ماده (۳) قانون جرائم رایانه‌ای پیش‌بینی شده است (برای مطالعه بیشتر نک: علمداری و فرجیها، ۱۳۹۶: ۱۷۳-۱۷۰).

صدمات شـدید اسـت که با روش‌های دیگر نمی‌توان از آن پیشـگیری کرد و چنان آثار بدی بر امنیت کشـور برجای می‌گذارد که چاره‌ای جز جرم‌انگاری آن نیسـت. آثار مخرب و ویرانگر حمله سایبری در مقدمه و قسمت مصادیق حملات سایبری به تفصیل تبیین شد.

۲-۴. اصل مصلحت عمومی

امـروزه اصـل رفـاه یا تأمین نظم، امنیت و آسـایش عمومـی، عمده‌ترین توجیـه و دلیل برای مداخلـه در حـوزه آزادی‌هـای افـراد از طریـق جرم‌انـگاری بسـیاری از رفتارهاسـت. بـر ایـن اساس، قانون کیفری ازیک‌سو به حمایت از جامعه علیه کسانی که نظم اجتماعی را مختل می‌کنند و ازدیگرسو به حمایت از ارزش‌های مورد پذیرش جامعه می‌پردازد. با توجه به اصل مصلحـت عمومی، قانونگذار می‌بایسـت با هر جرم‌انـگاری و تصمیم‌گیری پیرامون مصلحت عمومی منافع همه کسـانی که نمایندگی آنها را عهده‌دار اسـت در نظر گیرد (راسـخ، ۱۳۸۴: ۱۱۵). بنابر این نظریه، یک تصمیم عمومی در مواجه با فضای سـایبر که قرار اسـت بر زندگی همـگان اثرگـذار باشـد بایـد توافـق عمومی و در بسـتر عقل عمومـی صورت پذیـرد (صانعی، ۱۳۸۲: ۱۱۵). همان‌طـور کـه اشـاره شـد ارتکاب حملات سـایبری علاوه بر آنکه شـهروندان را از بهره‌منـدی از خدمـات ضـروری عمومـی از قبیل آب، بـرق و گاز محروم می‌سـازد، موجب لطمـه دیـدن امنیت کشـور نیز می‌شـود. ازاین‌رو، حفـظ منافع و مصلحـت عمومی ضرورت جرم‌انگاری حملات سایبری را می‌طلبد.

۳-۴. اصل ضرورت

مهم‌ترین بایسـته در زمینه جرم‌انگاری از یک عمل، ضرورت و ناگزیر بودن جرم شـمردن آن عمل است. به بیانی دیگر جرم شمردن یک فعل یا ترک فعل باید آخرین حربه برای نیل به

خواسته مقنن باشد. ازاین‌رو باید گفت استفاده از ضمانت اجراهای کیفری برای حمایت از ارزش‌ها و ایدئال‌ها آنگاه مجاز است که نتوان از سایر ضمانت اجراها بهره جست.

اصل ضرورت در جرم‌انگاری حمله سایبری جایگاه ویژه‌ای دارد و با اعمال این اصل به یک جرم‌انگاری حداقلی دست خواهیم یافت. «چه آنکه به اقتضای شرایط خاص حاکم بر فضای سایبر و امکانات ویژه آن، به‌راحتی می‌توان قبل از رسیدن کار به مرحله جرم‌انگاری، از وقوع بسیاری از جرائم پیشگیری کرد» (حاجی‌ده‌آبادی و سلیمی،۱۳۹۳: ۶۸-۶۶). اما ازآنجاکه حمله سایبری را غالباً یک دولت علیه دولت دیگر مرتکب می‌شود، مرتکبان آن از امکانات و ابزارهای پیشرفته‌ای برخوردارند که دولت برای آن فراهم می‌سازد. ازاین‌رو، صرف توسل به پیشگیری اجتماعی و وضعی برای مقابله با حملات سایبری مؤثر نخواهد بود. برای نمونه شاید نصب دیوار آتشین[1] یا آنتی ویروس[2] از حیث پیشگیری وضعی مانع تحقق جرائم رایانه‌ای شود اما استفاده از آنها به‌عنوان یک عامل مؤثر در پیشگیری وضعی از حملات سایبری چندان کارساز و مؤثر نخواهد بود.

۴-۴. اصل تناسب جرم و مجازات

«تئوری تناسب جرم و مجازات تحت تأثیر آموزه‌های مکاتب مختلف کیفری و جرم‌شناختی ازجمله مکتب کلاسیک، نئوکلاسیک، مکتب تحققی و مکتب دفاع اجتماعی همواره در حال تحول و تکامل بوده است» (حبیب‌زاده و رحیمی‌نژاد، ۱۳۸۷: ۱۱۶). اهمیت و ظهور این اصل را می‌توان در ماده (۵) اعلامیه جهانی حقوق بشر (۱۹۴۸)، ماده (۷) کنوانسیون بین‌المللی حقوق مدنی و سیاسی (۱۹۶۶) و مواد (۲ و ۴) کنوانسیون بین‌المللی منع شکنجه

1. Fire Wall
2. Anti Virus

و رفتارها و مجازات‌های ظالمانه غیرانسانی و وحشیانه (۱۹۴۸) مشاهده کرد (همان). میزان صدمه، فایده اجتماعی مجازات، نوع جرم ارتکابی، خصوصیات شخصی مجرم ازجمله مهم‌ترین معیارهای تناسب جرم و مجازات است (حاجی‌ده‌آبادی و سلیمی، ۱۳۹۳: ۷۱).

مجازات‌های پیش‌بینی شده در قانون جرائم رایانه‌ای ممکن است برای مرتکبان جرائم رایانه‌ای بازدارنده باشد اما برای مرتکبان حملات سایبری که به‌طور سازمان‌یافته امنیت کشور را هدف خود قرار می‌دهند، بازدارنده نیست. برای مثال محکوم کردن مرتکب حمله سایبری که موجب اخلال در عملکرد سامانه‌های رایانه‌ای متعلق به نیرگاه هسته‌ای شده است مطابق ماده (۷۳۷) قانون مجازات اسلامی به حبس تعزیری درجه شش چندان متناسب و بازدارنده نیست. ازاین‌رو، شایسته است مقنن با جرم‌انگاری مستقل حمله سایبری ضمانت اجرای کیفری بازدارنده و متناسبی تعیین کند.

ارتکاب حملات سایبری در بستر شبکه رایانه‌ای مستلزم آن است که مرتکب با سامانه خودش به سامانه‌های رایانه‌ای قربانی نفوذ کند، بدیهی است نفوذ از یک سامانه رایانه‌ای به سامانه رایانه‌ای دیگر مستلزم آن است که مرتکب از مهارت‌هایی در زمنیه علوم فناوری و اطلاعات برخوردار باشد (کوره‌پز و همکاران، ۱۳۹۳: ۱۲۵)، درحالی‌که مرتکبان جرائم سایبری لزوماً چنین شاخصه‌ای ندارند. به عقیده برخی نویسندگان، ارتکاب حملات سایبری رایانه‌ای مستلزم دانش و استفاده از نرم‌افزارهایی است که برای عموم کاربران فضای سایبر ناآشناست و کشف این حملات جز با بهره گرفتن از کارشناسان مجرب و متخصص ممکن نیست(Wiles and Reyes, 2007: 18) . ازاین‌رو، از حیث خصوصیات شخص مجرم با یک فرد متخصص در حوزه علوم فناوری و اطلاعات روبه‌رو هستیم.

۵-۴. اصل لزوم توجه به راهبردها، رویکردها و همکاری بین‌المللی

باید دانست برای مقابله کیفری کارآمد و مؤثر نسبت به حملات سایبری حتی با برخورداری از کارآمدترین و مؤثرترین قوانین داخلی، لازم است حقوق کیفری از ویژگی ملی بودن خود چشم‌پوشی کرده و با ماهیت حملات سایبری یعنی فراملی بودن خود را تطبیق دهد که این امر مستلزم تدوین قوانینی هماهنگ در سطح بین‌المللی در برابر حملات سایبری است. بنابراین امکان تصویب یک معاهده بین‌المللی، تأسیس نهادی بین‌المللی برای رسیدگی به حملات سایبری و متعاقب آن پیش‌بینی تدابیری همچون اعمال حق اولویت (تقدم) و حفظ امنیت کشورها از این‌گونه حملات، دور از ذهن نخواهد بود؛ زیرا تا زمانی که حملات سایبری را اغلب دولت‌ها یا با حمایت‌های آشکار و نهان یا با سکوت و رضایت تلویحی و داخل در قلمرو حاکمیت آنها صورت می‌گیرد، دل بستن به محاکمه مرتکبان حملات سایبری ازسوی دولتی که خود در آن نقش دارد، آرمانی دور از وقعیت است.

در صورتی که حملات سایبری به‌عنوان جرائم بین‌المللی تلقی شوند ممکن است نهاد بین‌المللی متولی امر رسیدگی به حملات سایبری شود که این امر «استفاده از حق اولویت محاکم ملی برای رسیدگی به جرائم بین‌المللی» را مطرح می‌کند؛ زیرا اعمال حق اولویت مستلزم آن است که جرائم مشمول صلاحیت نهادهای بین‌المللی در قوانین داخلی کشور گنجانده شود تا محاکم ملی بتوانند طبق قوانین متبوع خود به آن رسیدگی کنند. ممکن است برای اعمال حق اولویت توسط دولت‌ها دو امر مورد بررسی قرار گیرد: مورد اول، صلاحیت تقنینی و قضایی آن دولت است که براساس قوانین داخلی خود آن دولت بررسی می‌شود و مورد دیگر، استقلال و بی‌طرفی محکمه رسیدگی‌کننده آن است که مطابق معیارهای شناخته شده در حقوق بین‌الملل ارزیابی می‌شود. در این صورت محاکم ملی صلاحیت‌دار می‌توانند با اعمال حق تقدم مانع دخالت نهاد بین‌المللی متولی امر رسیدگی

به حملات سایبری در موضوع‌هایی شوند که ممکن است با حاکمیت و منافع ملی کشور متبوعشان ارتباط پیدا کند.

ازسوی‌دیگر، جرائم رایانه‌ای موضوع‌محور که در قوانین داخلی پیش‌بینی شده‌اند فقط به‌عنوان جرم عادی مطرح است نه جرائم بین‌المللی که به‌صورت برنامه‌ریزی شده، گسترده و سازمان‌یافته ارتکاب می‌یابند. در این صورت، با توجه به ماده (۱۰) اساسنامه دیوان بین‌المللی کیفری یوگسلاوی سابق و ماده (۹) اساسنامه دیوان بین‌المللی کیفری رواندا، رسیدگی محاکم ملی به یک جنایت بین‌المللی به‌عنوان جرمی عادی را از شمول قاعده منع محاکمه و مجازات مجدد خارج دانسته و به دیوان‌های موصوف اجازه رسیدگی به همان جرم را می‌دهد (اردبیلی، حبیب‌زاده و فخربناب، ۱۳۸۵: ۱۹-۱۸). چنین امری در اساسنامه رم وجود ندارد؛ زیرا طبق بند «۳» ماده (۲۰) اساسنامه، رسیدگی قبلی در دادگاه دیگر، چنانچه به‌طور واقعی و صادقانه انجام گرفته باشد مانع از رسیدگی دیوان بین‌المللی کیفری نسبت به همان موضوع خواهد شد. ازاین‌رو اتخاذ چنین رویکردی برای نهاد بین‌المللی متولی رسیدگی‌کننده به حملات سایبری بعید نیست، بدین‌معناکه رسیدگی به حملات سایبری با ماهیت بین‌المللی به‌عنوان جرمی عادی ازسوی محاکم ملی، نوعی عدم تمایل به رسیدگی صادقانه تلقی شود و راه برای اعمال صلاحیت نهاد بین‌المللی متولی این امر هموار گردد.

۵. جمع‌بندی و نتیجه‌گیری

«حمله سایبری» امروزه یکی از مهم‌ترین عملیات‌های مجرمانه سایبری به‌شمار می‌رود، زیرا امنیت کشور را تحت‌الشعاع خود قرار داده و بستری برای تحقق سایر عملیات‌های مجرمانه

سایبری از قبیل تروریسم سایبری و جنگ سایبری قلمداد می‌شود. ازاین‌رو، برای مقابله با حملات سایبری، ضروری است حقوق کیفری با مداخله به این حوزه، مرتکبان را به‌سزای اعمال خود برساند.

در حقوق کیفری ایران به‌ویژه در قانون جرائم رایانه‌ای سخنی از عنوان مجرمانه «حمله سایبری» گفته نشده است ازاین‌رو راهکارهای مقابله کیفری با حملات سایبری را در قوانین موجود به‌ویژه قانون جرائم رایانه‌ای می‌توان جستجو کرد. قوانین موجود از حیث عنصر مادی همه رفتارهای فیزیکی حملات سایبری را دربرمی‌گیرد اما از سایر حیث‌ها چنین نیست.

از حیث ماهیت باید اذعان داشت، اولاً رفتار مجرمانه در جرائم رایانه‌ای مانند تخریب داده، اخلال در سامانه رایانه‌ای یا ممانعت از دسترسی، مستقل از یکدیگر هستند. درحالی‌که 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 به‌طور مستقل در قانون جرائم رایانه‌ای پیش‌بینی شده است. بدین‌معناکه در حمله سایبری رفتارهای فیزیکی شامل تخریب داده، اخلال در سامانه رایانه‌ای، ممانعت از دسترسی و سرقت رایانه‌ای است؛ زمانی این رفتارها عنوان مجرمانه حمله سایبری را تشکیل می‌دهند که همراه با گستردگی یا سازمان‌یافتگی علیه امنیت کشور ارتکاب یابند. ثانیاً جرائم پیش‌بینی شده در قانون جرائم رایانه‌ای ماهیت ملی دارد درحالی‌که ماهیت حملات سایبری، فراملی است 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 جرم‌انگاری مستقل حمله سایبری حمایت و تضمین امنیت کشور در فضای سایبر است که چنین هدفی لزوماً در

جرائم رایانه‌ای صادق نیست. ازاین‌رو برخلاف جرائم رایانه‌ای، متضرر یک حمله سایبری حاکمیت است.

از حیث موضوع جرم نیز موضوع حملات سایبری بسیار مضیق‌تر از جرائم رایانه‌ای است چراکه موضوع جرم در حملات سایبری داده‌ها و سامانه‌هایی را دربرمی‌گیرد که آسیب به آنها موجب بر هم خوردن امنیت کشور می‌شود.

از حیث اصول نظری نیز می‌توان با تمسک به اصل ضرر، مصلحت عمومی، ضرورت، تناسب جرم و مجازات و لزوم توجه به راهبردها، رویکردها و همکاری بین‌المللی مداخله حقوق کیفری در این عرصه، جرم‌انگاری مستقل حملات سایبری را ضروری دانست. ازاین‌رو، پیشنهاد پژوهش حاضر با تکیه بر تفاوت مفهوم جرم حمله سایبری از جرم رایانه‌ای آن است که به شرح زیر عنوان مجرمانه حمله سایبری در قوانین موضوعه حقوق کیفری ایران پیش‌بینی شود و مجازات مرتکب در صورتی که مشمول یکی از حدود مقرر در کتاب دوم قانون مجازات اسلامی نباشد، حسب مورد یک یا دو درجه تشدید شود.

حمله سایبری عبارت است از ارتکاب هریک از اعمال زیر به قصد بر هم زدن امنیت کشور با سامانه‌های رایانه‌ای یا علیه آنها:

۱. اخلال در سامانه‌های رایانه‌ای که متعلق به یک گروه خاص باشد.

۲. تخریب داده‌های ذخیره شده در سامانه‌های رایانه‌ای که متعلق به یک گروه خاص باشد.

۳. تغییر در داده‌های ذخیره شده موجود در سامانه‌های رایانه‌ای که به یک گروه خاص تعلق داشته باشد.

۴. ممانعت از دسترسی به سامانه‌های رایانه‌ای و داده‌های موجود ذخیره شده در آنها که به یک گروه خاص متعلق باشد.

۵. رونوشت یا برش از داده‌های ذخیره شده موجود در سامانه‌های رایانه‌ای که متعلق به یک گروه خاص است.

البته باید گفت گروه خاص در تعریف مذکور عبارت است از سازمان‌ها، نهادها و مؤسسه‌هایی که حمله به داده‌ها و سامانه‌های رایانه‌ای متعلق به آنها امنیت کشور را به مخاطره می‌اندازد.

منابع و مآخذ

۱. اردبیلی، محمدعلی، محمدجعفر حبیب‌زاده و حسین فخربناب (۱۳۸۵). «نسل‌کشی و ضرورت جرم‌انگاری در حقوق کیفری»، فصلنامه *مدرس علوم انسانی*، دوره ۱۰، ش ۳.

۲. اصلانی، جبار و امیرحسین رنجبریان (۱۳۹۴). «بررسی تطبیقی و تحلیل تعریف حمله سایبری از منظر دکترین، رویه کشورها و سازمان‌های بین‌المللی در حقوق بین‌الملل»، فصلنامه *تحقیقات حقوقی*، ش ۷۱.

۳. تریف، تری و همکاران (۱۳۸۴). *مطالعات امنیتی نوین*، ترجمه علیرضا طیب و وحید بزرگی، چاپ اول، تهران، نشر پژوهشکده مطالعات راهبردی.

۴. جالینوسی، احمد، شهروز ابراهیمی و طیبه قنوانی (۱۳۹۲). «جایگاه فضای سایبر و تهدیدات سایبری در استراتژی امنیت ملی ایالات متحده آمریکا»، فصلنامه *دانش سیاسی و بین‌المللی*، سال دوم، ش ۵.

۵. چگینی‌زاده، غلامعلی (۱۳۷۹). «رویکردی نظری به مفهوم امنیت ملی در جهان سوم»، مجله *سیاست خارجی*، ش ۱.

۶. حاجی‌ده‌آبادی، احمد و احسان سلیمی (۱۳۹۳). «اصول جرم‌انگاری در فضای سایبر (با رویکردی انتقادی به قانون جرائم رایانه‌ای)»، فصلنامه *مجلس و راهبرد*، سال ۲۱، ش ۸۰.

۷. حبیب‌زاده، محمدجعفر و اسماعیل رحیمی‌نژاد (۱۳۸۷). «مجازات‌های نامتناسب مجازات‌های مغایر با کرامت انسانی»، فصلنامه *حقوق* دانشگاه تهران، دوره ۳۸، ش ۲.

۸. خبرگزاری *تابناک*: https://www.tabnak.ir/fa/news/1045466 (last visited on 9/5/2021)

۹. خرم‌آبادی، احمد (۱۳۹۱). *مسئولیت کیفری ارائه‌دهندگان خدمات اینترنتی*، چاپ اول، تهران، نشر دادیار.

۱۰. خلیل‌زاده، مونا (۱۳۹۳). *مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری*، چاپ اول، تهران، نشر مجد.

۱۱. خلیلی‌پور رکن‌آبادی، علی و یاسر نورعلی‌وند (۱۳۹۱). «تهدیدات سایبری و تأثیر آن بر امنیت ملی»، فصلنامه *مطالعات راهبردی*، ش ۵۶.

۱۲. راسخ، محمد (۱۳۸۴). *حق و مصلحت؛ مقالاتی در فلسفه حقوق و فلسفه ارزش*، جلد اول، چاپ دوم، تهران، نشر طرح نو.

۱۳. شلدون، بی.جان (۱۳۹۱). «استاکس‌نت و قدرت سایبری در جنگ»، *در امنیت و جنگ سایبری* (۲)، چاپ اول، تهران، نشر مؤسسه فرهنگی و مطالعات و تحقیقات بین‌المللی ابرار معاصر.

۱۴. صانعی، پرویز (۱۳۸۲). *رابطه حقوق با عوامل اجتماعی و روانی*، چاپ اول، تهران، نشر طرح نو.

۱۵. صبحی شیشوان، بهنام (۱۳۸۳). «شیوه‌های گوناگون سرقت رایانه‌ای»، ماهنامه *وکالت*، ش ۲۱ و ۲۲.

۱۶. عالی‌پور، حسن (۱۳۹۳). *حقوق کیفری فناوری اطلاعات*، چاپ سوم، تهران، انتشارات خرسندی.
۱۷. عبدالله‌خانی، علی (۱۳۸۳). *نظریه‌های امنیت مقدمه‌ای بر طرح‌ریزی دکترین امنیت ملی (۱)*، چاپ اول، تهران، نشر مؤسسه فرهنگی و مطالعات و تحقیقات بین‌المللی ابرار معاصر.
۱۸. عظیمی، فاطمه و هادی خشنودی (۱۳۹۵). «نقش تروریسم سایبری در تهدید علیه امنیت ایران و راه‌های پیشگیری از آن»، فصلنامه *مطالعات سیاسی*، سال نهم، ش ۳۴.
۱۹. علمداری، علی و محمد فرجیها (۱۳۹۶). «مطالعه تطبیقی مبانی جرم‌انگاری جرائم سایبر در نظام کیفری ایران و آلمان»، مجله *پژوهش‌های حقوق تطبیقی*، دوره ۲۱، ش ۴.
۲۰. *قانون مجازات اسلامی* (۱۳۹۶). ویرایش پنجم، چاپ دهم، تهران، نشر معاونت تدوین، تنقیح و انتشار قوانین و مقررات ریاست جمهوری.
۲۱. کوره‌پز، حسین‌محمد، سیدمحمود میرخلیلی، عبدالعلی توجهی و حمید بهره‌مند (۱۳۹۳). «نیم‌رخ جرم‌شناختی بزهکاران سایبری»، *پژوهش حقوق کیفری*، سال سوم، ش ۹.
۲۲. مارکوم، کترین دی و جرج ای. هیگینز (۱۳۹۷). *شبکه‌های اجتماعی به‌مثابه ابزار ارتکاب جرم*، ترجمه حمیدرضا دانش‌ناری و ابراهیم داودی دهاقانی، چاپ اول، تهران، نشر میزان.
۲۳. ماندل، رابرت (۱۳۹۶). *چهره متغیر امنیت ملی*، ترجمه پژوهشکده مطالعات راهبردی، چاپ چهارم، تهران، نشر پژوهشکده مطالعات راهبردی.
۲۴. مرسی، هادی (۱۳۹۷). «مقابله با حملات سایبری در حقوق کیفری ایران و اسناد بین‌المللی (با تأکید بر حملات سایبری علیه ایران)»، پایان‌نامه کارشناسی ارشد، تهران، دانشکده حقوق و علوم سیاسی دانشگاه تهران.
۲۵. مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر (۱۳۹۱). *امنیت و جنگ سایبری (۲) (ویژه سلاح‌ها، جنگجویان و حملات سایبری)*، چاپ اول، تهران.

26. Andress, Jason and Steve Winterfeld (2011). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, Amesterdam, Boston, Syngress/Elsevier.
27. Buzan, Barry (1991). "New Patterns of Global Security in the Twenty-First Century", *International Affairs* 67 (3).
28. Hathaway, O.A. etal. (2012). "The Law of Cyber-Attack," *California Law Review* 100 (4). https://www.scopus.com/inward/record.uri?eid=2-s2.0-84865318969&partnerID=40&md5=58759a152d788354c59cb6221e883cb4.
29. Junaidu Bello Marshall, E. and E. Mua'zu Abdullahi Saulawa (2015). "Cyber

Attacks: The Legal Response", *International Journal of International Law*, Vol. 1, Issue 2.
30. Tikk, Eneken, Kadri Kaska and Liis Vihul (2010). *International Cyber Incidents: Legal Considerations,* Cooperative Cyber Defence Centre of Excellence (CCDCOE). available at: https://ccdcoe.org/publications/books/legalconsiderations.pdf
31. Training, U.S. Army and Doctrine Command (2005). "Cyber Operations and Cyber Terrorism", In *DC Intelligence, Fort Leavenworth, KA, USA: US Army,* United States Congress (1984).
32. Wiles, Jack and Reyes Anthony (2007). "The Best Damn Cybercrime and Digital Forensics Book Period", http://www.irdiplomacy.ir/fa/news/1913134 (last visited on 7/10/2020).
33. www.gerdab.ir/fa/news/8175 (last visited on 7/10/2020)
34.www.globalsecurity.org/military/library/policy/army/other/tradoc-dcsint-hbk_1-02-2005.pdf