راهبرد مقابله با حملات سایبری علیه سامانه‌های رایانه‌ای ارائه‌دهنده خدمات ضروری در قانون مجازات اسلامی مصوب ۱۳۹۲

هادی مرسی* و نفیسه متولی‌زاده نایینی**

نوع مقاله: پژوهشی	تاریخ دریافت: ۱۴۰۰/۰۴/۲۶	تاریخ پذیرش: ۱۴۰۰/۱۰/۲۹	شماره صفحه: ۵۵-۲۹

حملات سایبری که علیه سامانه‌های رایانه‌ای ارائه‌دهنده خدمات ضروری ارتکاب می‌یابند، مصداق ماده (۷۳۹) قانون مجازات اسلامی (ماده (۱۱) قانون جرائم رایانه‌ای) قرار می‌گیرند. براساس ماده یاد شده مرتکب آن صرفاً به مجازات تعزیری حبس ۳ تا ۱۰ سال محکوم می‌شود؛ درحالی‌که وقوع حملات سایبری علیه سامانه‌های رایانه‌ای ارائه‌دهنده خدمات ضروری از قبیل خدمات درمانی، آب، برق، گاز، مخابرات، حمل‌ونقل و ... موجب به خطر انداختن امنیت، آسایش و امنیت عمومی می‌شود. بنابراین صرف اکتفای مقنن به تعیین مجازات تعزیری و عدم تعیین مجازات حدی برای آن قابل نقد است. به این منظور، پژوهش حاضر به صورت کتابخانه‌ای و با روش توصیفی - تحلیلی درصدد است تا با بررسی مبانی فقهی و شرایط قانونی دو عنوان حدی «محاربه» و «افسادفی‌الارض»، امکان تسری ماده (۲۷۹) قانون مجازات اسلامی (محاربه) و ماده (۲۸۶) قانون مجازات اسلامی (افسادفی‌الارض) نسبت به حملات سایبری علیه سامانه‌های رایانه‌ای موضوع ماده (۷۳۹) قانون مجازات اسلامی را مورد تحلیل و ارزیابی قرار دهد تا مشخص کند با کدام‌یک از دو عنوان حدی ذکر شده در قانون مجازات اسلامی می‌توان مرتکب آن را مجازات کرد. در نهایت مقاله حاضر نتیجه‌گیری می‌کند سلاح‌های غیرمادی و غیرملموس سایبری را به آنچه که مشهور فقها و قانونگذار از واژه سلاح اراده کرده‌اند نمی‌توان تسری داد، در نتیجه عنوان حدی «محاربه» بر این‌گونه حملات سابیری قابل تسری نیست، بلکه عنوان حدی «افسادفی‌الارض» با لحاظ شرایط مقرر در قانون مجازات اسلامی قابل تسری خواهد بود.

کلیدواژه‌ها: جرائم سایبری؛ خدمات ضروری؛ حملات سایبری؛ محاربه؛ افسادفی‌الارض

---

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

** استادیار گروه حقوق، دانشگاه میبد (نویسنده مسئول)؛
Email: motavallizade@meybod.ac.ir

فصلنامه مجلس و راهبرد، سال سی‌ام، شماره یکصدوسیزدهم، بهار ۱۴۰۲
doi: 10.22034/MR-2107-4724

مقدمه

قانونگـذار ایران در تاریخ ۱۳۸۸/۳/۵ با تصویب قانون جرائم رایانه‌ای به مقابله کیفری با جرائم سـایبری پرداخت اما در آن زمان حملات سایبری روند رو به رشد خود را طـی نکرده بودند و تفاوت میان مفهوم آن با مفهوم جرائم رایانه‌ای چندان ملموس و قابل درک نبود و این عوامل باعث شـده بود قانونگذار از مقابله کیفری با این رفتار شنیع مجرمانه سایبری غافل بماند و در قالب جرائم رایانه‌ای به مقابله با آن بپردازد. درحالی‌که امروزه مشخص شده است از حیث ماهیت، حملات سایبری از جرائـم رایانـه‌ای متفاوت اسـت زیرا حملات سـایبری دارای ماهیـت فراملی، سـازمان‌یافته بوده و میان دولت‌ها بـا یکدیگر تحقق می‌یابـد، درحالی‌که چنین امری در جرائم سـایبری صادق نیست. همچنین هدف از پیش‌بینی مواد مقرر در قانون جرائم رایانه‌ای حمایت از داده‌ها و سـامانه‌های رایانه‌ای شـهروندان اسـت درحالی‌که هدف در عنوان مجرمانه حمله سایبری حمایت از داده‌ها و سامانه‌های رایانه‌ای اسـت که هرگونه اخلال در آنها موجب لطمه دیدن نظم عمومی در سطح وسـیع شـده و امنیت یک کشـور را به مخاطره می‌اندازد. بـرای نمونه می‌توان به حمله سـایبری استاکس‌نت[1] در سال ۱۳۸۹ علیه نیروگاه هسته‌ای و حمله سایبری دوکو[2] در سـال ۱۳۹۰و حمله سـایبری فلیم[3] در سال ۱۳۹۱ اشـاره کرد و حمله‌ای که اخیراً مورخ ۱۴۰۰/۱/۲۲ علیه شـبکه برق تأسیسـات غنی‌سازی نطنز در ایران ارتـکاب یافت که موجب انفجار در آن مرکز شـد که ممکن بود صدها نفر جان خود را از دست بدهند.

عدم تفکیک دو عنوان مجرمانه «حمله سـایبری» و «جرائم سـایبری» موجب

1. Stuxnet
2. Duqu
3. Flame

شـده اسـت مجازات قابل اعمال برای مرتکبان حملات سایبری علیه سامانه‌های رایانه‌ای که برای ارائه خدمات ضروری عمومی از قبیل خدمات درمانی، آب، برق، گاز، مخابرات، حمل‌ونقل و بانکداری به کار می‌روند، با توجه به ماده (۷۳۹) قانون مجازات اسـلامی میزان حبس تعزیری ۳ تا ۱۰ سـال باشـد. ایـن میزان مجازات ممکن اسـت برای جرائم سـایبری که از چنان گسـتردگی آثار زیان‌بـار برخوردار نیسـت، قابل توجیه باشد اما این میزان مجازات برای حملات سایبری که اغلب از آن طرف مرزها و توسط دولت‌های متخاصم و به نحو سازمان‌یافته تحقق می‌یابند که علاوه‌بر اخلال در فضای سـایبر موجب اخلال و رعب و وحشت در فضای واقعی نیز می‌شـوند و زندگی بسـیاری از شـهروندان، اقتصاد و امنیت یک کشور را تحت تأثیر خود قرار می‌دهد، چندان قابل توجیه نباشـد. برای مثال تصور کنید تداخل در سـامانه‌های ناوبری هوایی که باعث سـقوط هواپیما شـده و جان صدها انسان را می‌گیـرد، چه آثـار نامطلوبی از خود باقی خواهد گذاشـت. از نمونه آثار مخرب حملات سـایبری می‌توان به حملات ارتکابی علیه کشـور اسـتونی اشـاره کرد که بسـیاری از بخش‌های تجاری و صنعتی آن کشـور را تحت تأثیر قـرار داد و انجام فعالیت‌های روزمره بسـیاری از کاربران را مختل کـرد، به‌گونه‌ای که مانع خدمات عمومی اینترنتـی از قبیل ارائه گزارش‌های مالیاتی، درخواسـت بـرای یارانه‌ها، مزایای دولتی و ... شـد که توسـط دولت برای رفاه حال شهروندان در نظر گرفته شده بود (Eneken, Kardri and Liis, 2010: 10).

ضرورت این پژوهش ازآن‌رو نمایان می‌شود که مشخص نمی‌باشد برای مقابله با حملات سایبری علیه سامانه‌های رایانه‌ای ارائه‌دهنده خدمات ضروری (داده‌ها و سامانه‌های رایانه‌ای موضوع ماده (۷۳۹) قانون مجازات اسلامی) آیا باید همانند یـک جرم عادی رایانـه‌ای برخورد کرد و میـزان مجازات تعزیری ۳ تا ۱۰ سـال را

در نظـر گرفت یا می‌توان به عناوین حدی از قبیل «محاربه» یا «افسـادفی‌الارض» تمسک جست؟ در صورت تمسک به عناوین حدی برای مقابله با حملات سایبری به کدام‌یک از دو عنوان حدی یعنی «محاربه» یا «افسادفی‌الارض» پیش‌بینی شده در قانون مجازات اسـلامی می‌توان تمسک جست و شـرایط تحقق هر یک از آنان چیسـت؟ ازاین‌رو پژوهش حاضر ابتـدا به بیان مفهوم حمله سـایبری و ویژگی‌ها و گسـتردگی آثار مخـرب آن می‌پردازد تا وجـه تمایز آن از مفهـوم جرم رایانه‌ای مشـخص شـده و سـپس با توجه به مبانی فقهـی و قانونی دو عنـوان «محاربه» و «افسـادفی‌الارض» قابلیـت اعمال هـر یک از آنان را نسـبت بـه این‌گونه حملات سایبری مورد ارزیابی قرار می‌دهد.

۱. مفهوم حملات سایبری، ویژگی‌ها و گستردگی آثار آن

بـرای آنکه بتوان به رویکردهـای مقابله با حملات سـایبری در قانون مجازات اسـلامی دست یافت، لازم است مفهوم حمله سـایبری، ویژگی‌ها و گستردگی آثار آن تبیین شود.

۱-۱. مفهوم حمله سایبری

در مـورد مفهـوم حمله سـایبری تعریف واحد و مشـترکی وجود نـدارد، بلکه هـر یک از کارشناسـان و صاحب‌نظران از دید خود به بیان مفهوم حمله سـایبری پرداخته‌اند. به عنوان مثال در تعریف حمله سـایبری گفته شـده است: «حملات سـایبری مجموعه اقداماتی هسـتند که توسـط یک دولت به منظور نفوذ یا ایجاد اخـلال در سـامانه‌های رایانه‌ای و یا شـبکه رایانـه‌ای، علیه دولـت دیگر ارتکاب می‌یابـد» (خلیل‌زاده، ۱۳۹۳: ۲۶). حملات سـایبری به معنـای «ایجاد اخلال در صحت یا درستی داده‌هاست که معمولاً از طریق اعمال کد مخرب و تغییر در منطق

برنامه‌ها و کنترل داده‌ها انجام می‌شود و به خروجی اشتباه توسط سامانه‌های رایانه‌ای منجر می‌شود» (جالینوسی، ابراهیمی و قنواتی، ۱۳۹۲: ۱۰). یک حمله سایبری شامل چهار حوزه 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, 2005: 1-3).

هر یک از تعاریف ذکر دارای اشکالات و ایراداتی است که بررسی آنها از موضوع پژوهش حاضر خارج است. بنابراین پژوهش حاضر این تعریف را از حمله سایبری اختیار کرده است که« حملات سایبری به اعمالی اطلاق می‌شود که به وسیله سامانه‌هایرایانه ای به قصد تضعیف تمام یا بخشی اعظمی از سامانه‌های رایانه‌ای متعلق به یک گروه خاص اعم از کاربران اینترنتی، سازمان‌ها، نهادهاو... ارتکاب می‌یابد» (مرسی، ۱۳۹۷: ۱۲۲). از این رو حمله سایبری هر یک از اعمال شرح داده زیر است که به قصد تضعیف تمام یا بخش اعظمی از سامانه‌های رایانه‌ای متعلقبه یک گروه خاص از حیث همین عناوین ارتکاب می‌یابد:

- اخلال در سامانه‌های رایانه‌ای که متعلق به یک گروه خاص است.
- تخریب داده‌های ذخیره شده موجود در سامانه‌های رایانه‌ای که متعلق به یک گروه خاص است.
- تغییر داده‌های ذخیره شده موجود در سامانه‌های رایانه‌ای که متعلق به یک گروه خاص است.
- ممانعت از دسترسی به سامانه‌های رایانه‌ای و داده‌های موجود ذخیره شده در آنها که متعلق به یک گروه خاص است.
- رونوشت یا برش از داده‌های ذخیره شده موجود در یک سامانه‌هاس رایانه‌ای که متعلق به یک گروه خاص است. منظور از گروه خاص در تعریف مذکور اعم

ازکاربران اینترنتی، سازمان‌ها، نهادها و... است (همان: ۱۲۳-۱۲۲).

مطابـق این تعریـف مصادیق عنصر مـادی حملات سـایبری را می‌توان تحت خناویـن جرائم علیـه صحت، تمامیت و دسـترس‌پذیری سـامانه‌های رایانه‌ای و داده‌های ذخیره شده در درون آن قرار داد.

عنصر روانی در حمله سـایبری عبارت اسـت از قصد تضعیـف عملکرد تمام یا بخش اعظمی از شـبکه‌های رایانه‌ای متعلق به یـک گروه خاص. به‌عبارت‌دیگر سـامانه‌های رایانه‌ای قربانی حملات سـایبری، نه به عنوان یک سـامانه رایانه‌ای بلکـه به عنـوان عضوی از یک شـبکه‌یرایانه‌ای متعلق به یک گـروه خاص، قربانی می‌شـوند (همان: ۱۲۴-۱۲۳). از سـوی دیگر باید در نظر داشت احراز قصد و نیت خاص حملات سـایبری، یعنی قصد تضعیف تمام یا بخش اعظمی از سـامانه‌های رایانه‌ای متعلق به‌گروه خاص امری دشـوار اسـت، زیرا قصد امری ذهنی و درونی اسـت و تأکید برلزوم اثبات آن باعث بلاکیفر ماندن بسـیاری از مهاجمان سایبری می‌شـود. 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 قـرارداد. این اوضاع و احوال عوامل گوناگونی چون ماهیت کلی آن اعمال؛ ارتکاب آن در منطقه‌ای خاص، تکرار، اسـتمرار و وسعت حملات سـایبری و... را شامل خواهد شـد. به‌عبارت‌دیگر کیفیت وقایع ممکن است به‌گونه‌ای باشد که اثبات کند مهاجم می‌دانسته یا علم به وقوع داشته است.

۲-۱. ویژگی‌های حملات سایبری و گستردگی آثار آن

کم‌رنگ شـدن نقش جغرافیا یکی از ویژگی‌های بستر حملات سایبری به شمار می‌آید. این امر بر کسـی پوشـیده نیسـت که شـبکه جهانی اینترنـت،[1] به عنوان

1. Internet

وسیع‌ترین بستر حملات سایبری، تأثیر بسزایی در کم‌رنگ شدن نقش جغرافیا داشته و این امکان را برای مهاجمان سایبری فراهم کرده است که از توانایی‌های لازم برای عبور از محدوده مرزهای جغرافیایی خود جهت رسیدن به اهداف اصلی خود برخوردار شوند (عظیمی و خشنودی، ۱۳۹۵: ۱۶۴). این امر موجب شده است نهادهای دولتی به صورت غیررسمی از حملات سایبری ارتکاب‌یافته از آن سوی مرزها حمایت کنند و موجب حملات سایبری منسجم‌تر و هدفمندتری شوند تا نتایج بسیار زیانباری را سبب شوند، درحالی‌که در جرائم رایانه‌ای چنین امری صادق نیست.

صرف زمان کوتاه و هزینه کم یکی دیگر از امکاناتی است که بستر حملات سایبری برای مهاجمان سایبری فراهم می‌آورد تا در مدت زمان کوتاه با کمترین هزینه بیشترین خسارت را وارد آورند. به عنوان مثال در برخی از موارد که مهاجمان سایبری برای ارتکاب حملات خود نیاز به چندین هزار سامانه رایانه‌ای دارند، آنان از این توانایی برخوردارند که بدون تهیه چندین هزار سامانه رایانه‌ای فقط با ایجاد یک بد افزار و انتشار آن در شبکه جهانی اینترنت سبب شوند که سامانه‌های رایانه‌ای متصل به شبکه جهانی اینترنت را تحت فرمان و کنترل خود درآورده و از آنان برای حملات خود استفاده کنند که نمونه بارز آن حملات سایبری «دی داس»[1] است.

1. Distributed Denial of Service (DDOS)

حملات اختلال در سرویس‌دهی (دی داس) از جمله تهدیدات اصلی علیه تجارت الکترونیک محسوب می‌شود و به همین علت است که معمولاً مورد توجه گسترده رسانه‌ها قرار می‌گیرند. این نوع حملات عمدتاً از طریق ارائه درخواست‌های ساختگی برای دریافت اطلاعات به وبسایت‌ها انجام می‌شود تا دسترسی کاربران مجاز به خدمت‌های مختلف را مسدود کند (دسترر، جورج، امی آلیز و الکس هرواتین، «حملات اختلال در سرویس‌دهی (دی داس): پیشگیری، تشخیص نفوذ و کاهش تأثیرات»، امنیت و جنگ سایبری ۲، ترجمه مؤسسه فرهنگی و مطالعات و تحقیقات بین‌المللی ابرار معاصر، چاپ نخست، تهران، ۱۳۹۱، ص ۱۲۷. به‌عبارت‌دیگر مهاجم با ارسال درخواست‌های بسیار به یک سرور یا رایانه، باعث استفاده بیش از حد از منابع آن مانند پردازنده سرور، بانک

بستر حملات سایبری از لحاظ ساختاری به‌گونه‌ای نامتمرکز است، این ماهیت ساختاری توجه بسیاری از مهاجمان سایبری را به‌سوی خود جلب کرده است؛ زیرا این توانایی و قابلیت را به آنان داده است تا بدون آنکه اثر یا نامی از خود باقی برجای گذارند حملات سایبری خود را متوجه اهداف خود کنند (Lord and Sharp, 2011: 20-28).

تأثیرگذاری شگرف یکی دیگر از ویژگی‌های بستر حملات سایبری است. ماهیت خاص فضای سایبر سبب اتکای روزافزون کاربران، شرکت‌ها، نهادهای دولتی و ... به فضای سایبر شده است. این اتکا و وابستگی تا جایی پیش رفته است که اکثر منابع کاربران، سازمان‌ها و ... 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 منصه ظهور برسانند و بر دامنه خسارات ناشی از رفتارهای مجرمانه خویش بیافزایند (Ibid.). همچنین موجب آشکار شدن نقاط ضعف زیرساخت‌های حیاتی یک کشور دز فضای سایبر شوند (حسن‌بیگی، ۱۳۸۴: ۳).

۲. مقابله با حملات سایبری علیه سامانه‌های رایانه‌ای ارائه‌دهنده خدمات ضروری در قالب محاربه یا افسادفی‌الارض

براساس مفهوم حملات سایبری و ویژگی‌های آن، به نظر می‌رسد در مواردی که حملات علیه سامانه‌های رایانه‌ای ارائه‌دهنده خدمات ضروری ارتکاب می‌یابند، بتوان در قالب دو عنوان فقهی «محاربه» و «افسادفی‌الارض» در فقه

اطلاعاتی، پهنای باند و ... می‌شود، به‌نحوی‌که به دلیل حجم بالای پردازش سرور دچار وقفه، اختلال و یا حتی قطعی کامل می‌شود.

و حقوق اسلامی قرار داد. بنابراین باید توجه داشت که امکان تحقق محاربه یا افسادفی‌الارض در فضای سایبر متفرع بر آن است که موضوع آیه ۳۳ سوره مائده چیست؟ زیرا اکثریت قریب به اتفاق فقهای شیعه در آیه شریفه، افسادفی‌الارض را به محاربه معطوف می‌کنند در نتیجه معتقدند که آیه شریفه در مقام بیان تنها یک جرم است و افسادفی‌الارض عنوان مستقلی از محاربه نیست (هاشمی شاهرودی، ۱۳۷۶: ۲۰۰-۱۴۳؛ برهانی، ۱۳۹۴: ۳۴-۲۲). برخی معتقدند قانونگذار ایران در برخی از قوانین مصوب پس از انقلاب، برای اَعمالی مجازات اعدام تعیین کرده است که در آنها سلاح کشیدن مشاهده نمی‌شود مانند ماده (۲۳) قانون جرائم نیروهای مسلح مصوب سال ۱۳۸۲، ضمن اینکه مجازات اعدام پیش‌بینی شده در قوانین مورد اشاره جز از باب افسادفی‌الارض قابل توجیه نیست، چون با هیچ‌یک از حدود دیگر سنخیت ندارد و نمی‌توان آن را تعزیر (که لاجرم باید دون‌الحد باشد) تلقی کرد (میرمحمدصادقی، ۱۳۹۳: ۶۰)، زیرا این قاعده «التعزیر دون‌الحد» در کیفرگذاری تعزیرات مانع رسیدن به میزان مجازات‌های تعزیری به حد اعدام می‌شود (منتظری، ۱۳۶۷: ۵۴۴-۵۳۱؛ موسوی گلپایگانی، ۱۴۱۲: ۳۰۰-۲۹۷؛ موسوی اردبیلی، ۱۴۲۷: ۳۷۰-۳۶۵). در مقابل تعداد بسیار معدودی از فقها حد افسادفی‌الارض را از حد محارب مستقل دانسته‌اند (مؤمن، ۱۴۱۵: ۴۰۰).

بنابراین برخی متون فقهی و نیز برخی قوانین به تبع قرآن کریم این دو عنوان را در کنار هم ذکر کرده‌اند، به‌گونه‌ای که موهم این معناست که این دو، یک جرم به شمار می‌روند. در مقابل برخی از فقیهان ضمن بحث از جرائمی نظیر به آتش کشیدن منازل، تکرار قتل بردگان و غیرمسلمانان و ... متعرض عنوان افساد شده و مرتکبان اعمال مزبور را به عنوان مفسد فی‌الارض مستحق مجازات قتل یا قطع دانسته‌اند.

اکنون دو حالت قابل تصور است: حالت اول آنکه آیه شریفه در مقام بیان دو

عنوان مجرمانه است، حالت دوم آیه شریفه در مقام بیان یک عنوان مجرمانه است اما آن عنوان، عنوان افسادفی‌الارض است و عنوان محاربه از باب ذکر خاص قبل از عام در آیه آورده شده است. قانونگذار ایران در سال ۱۳۹۲ با تصویب قانون مجازات اسلامی به صراحت جرم افسادفی‌الارض را از محاربه تفکیک کرده و ماده (۲۸۶) و تبصره آن را به جرم افسادفی‌الارض تخصیص داد و مجازات اعدام را برای مرتکبان این جرم تعیین کرد. ازاین‌رو مبحث حاضر در دو قسمت به بررسی امکان تحقق عنوان فقهی «محاربه» و امکان تحقق عنوان فقهی «افسادفی‌الارض» در حملات سایبری علیه سامانه‌های ارائه‌دهنده خدمات ضروری عمومی می‌پردازد.

۱-۲. امکان تحقق عنوان مجرمانه محاربه در حملات سایبری علیه سامانه‌های رایانه‌ای ارائه‌دهنده خدمات ضروری

در این قسمت به امکان‌سنجی تحقق عنوان فقهی «محاربه» در صورت وقوع یک حمله سایبری علیه سامانه‌های رایانه‌ای ارائه‌دهنده خدمات ضروری عمومی پرداخته شده است. ازاین‌رو ابتدا به تبیین مفهوم محاربه و سلاح پرداخته شده است تا مشخص شود آیا سلاح‌های سایبری وجود قید «سلاح» را در عنوان فقهی «محاربه» دربرمی‌گیرند؟ سپس به بررسی شرایط لازم برای تحقق عنوان «محاربه» در این‌گونه حملات سایبری پرداخته شده است.

۱-۱-۲. مفهوم محاربه

ریشه واژه محاربه «حرب» است که متضاد کلمه «سلم» به معنی صلح است. محاربه و حرابه مصدر باب مفاعله و مشتق از حرب است که با فتح را به معنای سلب و با سکون را به معنای جنگیدن و نزاع است. در *لسان‌العرب* آمده: «غارت مال انسان و ترک آن شخص به‌گونه‌ای که هیچ چیزی برایش نماند» (ابن‌منظور، ۱۴۰۸: ۳۰۳).

۲-۱-۲. شرایط تحقق عنوان محاربه در حملات سایبری

ماده (۲۷۹) ق.م.ا سال ۱۳۹۲، ماده مبنایی جرم محاربه است. این ماده مقرر می‌دارد: «محاربه عبارت از کشیدن سلاح به قصد جان، مال یا ناموس مردم یا ارعاب آنهاست، به‌نحوی‌که موجب ناامنی در محیط شود ...». این تعریف متخذ از منابع فقهی است. محقق حلی در تعریفی گفته است: «محارب کسی است که سلاح می‌کشد» (محقق حلی، ۱۴۰۸: ۱۶۷). به‌این‌ترتیب علاوه‌بر وجود سوءنیت عام، یعنی عمد در کشیدن سلاح (تجرید سلاح)، سوءنیت خاص، یعنی قصد تعرض به جان، مال یا ناموس مردم، برای تحقق این جرم ضرورت دارد (میرمحمدصادقی، ۱۳۹۳: ۴۸). بر این اساس برای آنکه یک حمله سایبری تحت عنوان محاربه قرار گیرد، لازم است به قصد تعرض به جان، مال یا ناموس مردم ارتکاب یابد.

۱-۲-۱-۲. سلب امنیت در محیط

همچنین با توجه به ماده (۲۷۹) قانون مجازات اسلامی از اطلاق واژه (محیط) می‌توان گفت که این محیط اعم از سنتی (واقعی) و سایبری است و باید در نظر داشت نتایج زیان‌بار ناشی از حملات سایبری فقط بر امنیت فضای سایبر مؤثر نخواهد بود، بلکه امنیت فضای فیزیکی را نیز را به مخاطره می‌اندازد. ازاین‌رو قانونگذار در ماده (۷۳۹) قانون مجازات اسلامی مقرر می‌دارد: «هرکس به قصد به 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 شوند، به حبس از ۳ تا ۱۰ سال محکوم خواهد شد». شایسته بود مقنن قید «درصورتی‌که عمل ارتکابی مصداق محاربه نباشد مرتکب به حبس از ۳ تا ۱۰ سال محکوم خواهد شد» را به آن می‌افزود. ممکن

است این پرسش مطرح شود که در چه شرایطی ممکن است عمل ارتکابی مصداق محاربه نباشد؟ در پاسخ باید گفت با توجه به عدم تفکیک عنوان مجرمانه «حملات سایبری» از «جرائم سایبری»، فقط با تمسک به ماده (۷۳۹) قانون مجازات اسلامی می‌توان مرتکبین رفتارهای مجرمانه علیه سامانه‌های رایانه‌ای ارائه‌دهنده خدمات ضروری را مجازات کرد و ازآنجاکه این‌گونه رفتارهای مجرمانه می‌توانند ناشی از حملات سایبری یا جرائم سایبری باشند، در فرضی که رفتار مجرمانه ناشی از جرائم سایبری باشد و ارتکاب جرائم سایبری مستلزم استفاده از بدافزارها به عنوان سلاح نیستند، بنابراین امکان تحقق محاربه در اغلب موارد برای جرائم سایبری میسر نیست.

نکته دیگر وجود قید «مردم» در ماده (۲۷۹) ق.م.ا است که دلالت بر آن دارد برای صدق عنوان محاربه باید نوعی «عمومیت» در جرم وجود داشته باشد. ازاین‌رو در ادامه ماده (۲۷۹) آمده است: «هرکس با انگیزه شخصی به سوی یک یا چند شخص سلاح بکشد و عمل او جنبه عمومی نداشته باشد ... محارب محسوب نمی‌شود». ازآنجاکه موضوع جرم در ماده (۷۳۹) قانون مجازات اسلامی سامانه‌های رایانه‌ای هستند که برای ارائه خدمات ضروری عمومی است، قید «عمومی» در ماده موجب می‌شود وجود انگیزه شخصی را منتفی دانست. به‌عبارت‌دیگر انتفای انگیزه شخصی مرتکب ناشی از ماهیت سامانه‌های رایانه‌ای موضوع ماده (۷۳۹) قانون مجازات اسلامی، یعنی کاربرد همگانی و عمومی بودن آنان است.

نکته دیگری که از متن ماده (۲۷۹) استنباط می‌شود، مقید بودن جرم محاربه به سلب امنیت است. با توجه به ماهیت سامانه‌های رایانه‌ای موضوع ماده (۷۳۹) قانون مجازات اسلامی و کاربرد آنان که ارائه خدمات ضروری عمومی است، هرگونه اخلال در عملکرد آنان موجب سلب امنیت می‌شود. این امر از یک‌سو از قید «ارائه

خدمات ضروری عمومی» و از سوی دیگر از مثال‌هایی که مقنن از سامانه‌های رایانه‌ای ارائه‌دهنده خدمات ضروری عمومی ارائه کرده است، قابل استنباط است.[۱] با آنکه مثال‌های ذکر شده جنبه تمثیلی دارند اما ماهیت تمامی آنان بیانگر عمومی بودن و مرتبط بودن با نیازهای ضروری شهروندان جامعه است. نمونه دیگر سامانه‌های ارائه‌دهنده خدمات ضروری عمومی، سامانه‌های نظارت بر دسترسی و کنترل داده‌ها (اسکادا)[۲] است.

۲-۲-۱-۲. کشیدن سلاح

در میان فقها درباره وجود یا عدم وجود قید «سلاح» در تحقق محاربه دو قول وجود دارد: قول اول که مشهور فقها قائل به آن هستند شرط بودن قید سلاح است به‌طوری‌که حتی برخی از آنان تشهیر سلاح را نیز شرط دانسته‌اند (مفید، ۱۴۱۰: ۸۰۴؛ طوسی، ۱۴۰۰: ۷۲۰؛ همان، ۱۴۰۷: ۴۵۸). قول دوم که در مقابل قول اول است و اقل فقها را شامل می‌شود از جمله علامه حلی در *قواعد الاحکام* (حلی، ۱۴۱۳: ۵۶۸) و فرزندش فخرالمحققین در *ایضاح الفوائد* (حلی، ۱۳۸۷: ۵۴۳) و تعدادی از فقهای معاصر همچون آیت‌الله موسوی اردبیلی قائل به این امر هستند

---

۱. ماده (۷۳۹) قانون مجازات اسلامی در این زمینه مقرر می‌دارد: «هرکس به قصد به خطر انداختن امنیت، آسایش و امنیت عمومی ...، از قبیل خدمات درمانی، آب، برق، گاز، مخابرات، حمل‌ونقل و بانکداری مرتکب شود، به ...».

۲. سامانه‌های اسکادا برای کنترل و نظارت بر فرایندهای مختلف (صنعتی، زیرساختی، تأسیساتی) به کار می‌روند. 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، یا مصرف انرژی را تنظیم می‌کنند. سامانه‌های اسکادا تقریباً در همه اموری که با آن سروکار داریم به چشم می‌خورند. ر.ک:

Andress,Jason and Steve Winterfeld,*Cyber Warfare:Techniques,Tactics and Tools for Security Practitioners*, Amesterdam, Boston, Syngress/Elsevier, 2011,123.

که در صدق محاربه نیازی به تشـهیر سلاح و یا حمل سلاح نیست، بلکه آنچه که به عنوان مناط و ملاک در نظر گرفته می‌شود، صرف ایجاد ناامنی عمومی و برهم زدن اجتماعـی مردم و ایجاد ترس و رعب در دل آنهاسـت (موسـوی اردبیلی، ۱۴۲۷: ۵۱۵-۵۱۴). حال منشـأ این ناامنی از راهی که می‌خواهد باشد مثل اینکه شخصی بخواهد با شـکاندن و تخریب سـدهای آب و روانه کردن سیلاب به منازل و مزارع، جان و مال آنها را به خطر بیندازد (ایزدی‌فر و حسین‌نژاد، ۱۳۹۵: ۳۲).

بنابراین براساس قول دوم که اقل فقها را شامل می‌شود و قائل به این امر هستند کـه ایجاد ناامنی عمومی و برهم زدن اجتماع مردم موضوعیت داشـته و منشـأ این ناامنی‌ها موضوعیت ندارد دیگر نیازی به اثبات قید سلاح در حملات سایبری نبوده و کافی است تنها شرط ایجاد ناامنی توسط حملات سایبری تبیین شود. اما قانونگذار ایران در قانون مجازات اسـلامی مصوب ۱۳۹۲ به تبعیت از نظر مشهور فقها در ماده (۲۷۹) ق.م.ا مقرر داشته است: «محاربه عبارت از کشیدن سلاح به قصد جان، مال یا ناموس مردم یا ارعاب آنهاست، به‌نحوی‌که موجب ناامنی در محیط شود ...».

در مورد معنای «سـلاح» سـه قول در میان فقها وجود دارد: قول اول با اشاره به خبر جابر از امام محمد باقر(ع): «کسـی که در شهر با سلاح تهدید کند دستش قطع می‌شـود و اگر با این ابزار کسی را بزند کشـته می‌شود» (عاملی، ۱۴۰۱: ۵۲۸)، سلاح را محدود به سـلاح آهنین مثل شمشیر، نیزه، قمه، خنجر و چاقو کرده‌اند و وسایلی چون چوب و سـنگ و تازیانه را از شـمول آن خارج دانسـته‌اند (میرمحمدصادقی، ۱۳۹۳: ۵۰). در *تحریرالوسیله* نیز چنین آمده است: «اگر کسی بدون سلاح به دیگری حمله کند برای اینکه مال او را بسـتاند یا او را بکشد دفاع جایز است، بلکه در حالت دوم واجب است حتی اگر به قتل مهاجم بیانجامد. ولی حکم محارب در مورد چنین کسـی ثابت نیست. اگر کسی با تازیانه و عصا و سـنگ مردم را بترساند، ثبوت حکم

محارب در مورد او مشکل است، بلکه عدم ثبوت آن در صورت نخست [تازیانه و عصا] به واقع نزدیک‌تر است» (موسوی خمینی، ۱۳۹۳: ۴۹۲). قول دوم استفاده از سنگ، چوب، عصا، تازیانه و امثال آنها که عرف به صورت مجازی آنها را سلاح می‌داند را برای تحقق عنوان محاربه کافی دانسته‌اند (طباطبایی، ۱۴۱۸: ۱۴۹؛ مقدس اردبیلی، ۱۴۰۳: ۲۸۷؛ فاضل هندی، ۱۴۱۶: ۶۸۴). مستند این نظر روایت سکونی از امام صادق (ع) از قول پدرشان از امام علی (ع) است (میرمحمدصادقی، ۱۳۹۳: ۵۰). قول سوم، مطلق اخذ بالقوه و به‌کار بردن زور و قهر و غلبه حتی با استفاده از توان و قدرت بدنی، کافی می‌دانند (حلی، ۱۴۱۳: ۵۶۸). پیرامون تجرید سلاح نیز گروهی از فقها همچون صاحب جواهر حمل سلاح را در صدق محاربه کافی و مشروط به تشهیر سلاح ندانسته‌اند (نجفی، ۱۴۰۴: ۵۶۴).

همان‌طور که مشخص است هر سه قول قید سلاح را در تعریف محاربه شرط دانسته اما با تفصیل در جزئیات آن با یکدیگر اختلاف نظر دارند. برخی حقوقدانان معتقدند با پذیرش قول دوم یا سوم که در مورد سلاح موسع است، می‌توان اعمالی چون شکستن سد و سرازیر کردن آب به سوی خانه‌های مردم، پاشیدن فلفل یا اسید بر روی آنها و پخش کردن مواد آلوده و مسموم در هوا را از مصادیق محاربه دانست (میرمحمدصادقی، ۱۳۹۳: ۵۰). بنابراین با پذیرش نظرهای موسع پیرامون مفهوم سلاح می‌توان قائل به این امر شد که سلاح سایبری قابلیت انطباق با قید سلاح که شرط اساسی محاربه تلقی می‌شود را داراست و می‌توان حملات سایبری را در صورت تحقق سایر شرایط مصداق محاربه دانست. نکته مهم این است که عملکرد سلاح‌های سایبری اگرچه به مراتب خطرناک‌تر از چوب، سنگ و مثال‌های دیگری است که فقها ذکر کرده‌اند؛ اما رویکرد مشهور فقهی و حقوقی، ناظر بر سلاح‌های ملموس و مادی است.

قانونگذار ایران در ماده (۵) «قانون مجازات قاچاق اسلحه و مهمات و دارندگان سلاح و مهمات غیرمجاز» مصوب سال ۱۳۹۰ به سلاح‌هایی مانند سلاح سرد جنگی، سلاح گرم سبک غیرخودکار، سلاح گرم سبک خودکار و سلاح گرم نیمه‌سنگین و سنگین اشاره کرده است و در ماده (۲) همان قانون مقرر داشته است: «مقصود از سلاح و مهمات در این قانون انواع سلاح‌های گرم و سرد جنگی و شکاری، اعم از گلوله‌زنی و غیرگلوله‌زنی و مهمات مربوط به آنهاست». در تبصره این ماده آمده است: «اسلحه لیزری و آن دسته شبه‌سلاح‌هایی که به دلیل مشابهت و کاربرد، قابلیت جایگزینی سلاح را دارند از حیث احکام مندرج در این قانون، حسب مورد تابع احکام سلاح گرم قرار می‌گیرند و سلاح‌های آموزشی و بی‌هوش‌کننده تابع احکام سلاح شکاری هستند». برخی حقوقدانان معتقدند که مهمترین ضابطه در تعریف سلاح آن چیزی است که برای نزاع و جنگیدن ساخته شده است یا به کار می‌رود و معنای آن از لحاظ زمان و مکان متغیر است (همان: ۵۲). همچنین گفته می‌شود متون حقوقی برای آن وضع شده‌اند که به اهدافی مانند رعایت حقوق اشخاص و یا نظم اجتماعی نائل شوند. بنابراین لازم است تفسیر متن حقوقی در راستای این هدف انجام شود. ازاین‌رو نمی‌توان تنها به نظر مقنن تأکید ورزید؛ زیرا در زمان وضع قانون جرائم رایانه‌ای پدیده حملات سایبری از چنین رشدی برخوردار نبودند، اما امروزه با توجه به رشد روزافزون آنها ماده (۷۳۹) قانون مجازات اسلامی قابلیت آن را دارد که در راستای هدف کلی حقوق قرار گیرد. در خصوص سلاح نیز اگرچه در زمان تصویب، نظر مقنن بی‌گمان بر حملات سایبری نبوده اما اکنون به نظر می‌رسد ازآنجاکه حملات سایبری گونه‌ای جدید از مبارزات را رقم زده‌اند، دیگر نتوان اصطلاح سلاح را محدود به موارد سنتی آن دانست. اما در پاسخ باید گفت تسری مفهوم سلاح به سلاح‌های غیرملموس و غیرمادی

مانند بدافزارها چندان شایسته به نظر نمی‌رسد و نمی‌توان چنین مفهوم موسعی از سلاح ارائه داد، به ویژه آنکه آموزه‌های فقهی و شرعی چنین توسعه دامنه جرم‌انگاری در جرائم حدی را برنمی‌تابد. اما باید توجه داشت مقنن به عنوان یک جرم مانع، تولیدکنندگان، منتشرکنندگان و توزیع‌کنندگان بدافزارها را به حال خویش رها نکرده است بلکه در قبال بدافزارها[1] که امروزه به عنوان یک ابزار در جهت حملات سایبری استفاده می‌شوند، در بند «الف» ماده (۲۵) «قانون جرائم رایانه‌ای»[2] به جرم‌انگاری فرایند تولید، انتشار یا توزیع و در دسترس قرار دادن آن اهتمام ورزیده است (یکرنگی و مرسی، ۱۳۹۹: ۳۲۳).

۳. مفهوم افسادفی‌الارض و امکان تحقق آن در حملات سایبری علیه سامانه‌های رایانه‌ای ارائه‌دهنده خدمات ضروری

همان‌طور که بیان شد نمی‌توان سلاح سایبری را به آنچه که مشهور فقها و قانونگذار از واژه «سلاح» اراده کرده‌اند سرایت و توسعه داد و نمی‌توان با عنوان حدی محاربه به مقابله با حملات سایبری پرداخت. بنابراین در این قسمت به قابلیت اعمال عنوان فقهی «افسادفی‌الارض» در خصوص حملات سایبری علیه سامانه‌های رایانه‌ای ارائه‌دهنده خدمات ضروری خواهیم پرداخت.

۱-۳. مفهوم افساد فی‌الارض

از نظر لغوی افساد از باب افعال از «فسد» به معنای فساد کردن و برپا کردن

---

۱. نرم‌افزارهای مخربی هستند که به صورت مخفیانه وارد سامانه‌های رایانه‌ای می‌شوند و اعمال مخرب خاص خود را بر روی داده‌های ذخیره شده در سامانه‌های رایانه‌ای مورد هدف قرار می‌دهند. این امر به وقوع خساراتی منجر می‌شود و چون اغلب آنان به تضعیف عملکرد سامانه‌های رایانه‌ای منجر می‌شوند، به این نام مشهورند (داوری دولت‌آبادی، ۱۳۹۳: ۶).

۲. بند «الف» ماده (۲۵) قانون جرائم رایانه‌ای مقرر می‌دارد: «تولید یا انتشار یا توزیع و در دسترس قرار دادن یا معامله داده‌ها یا نرم‌افزارها یا هر نوع ابزار الکترونیکی که صرفاً به منظور ارتکاب جرائم رایانه‌ای به کار می‌رود».

فتنه اســت (معین، ۱۳۸۴: ۹۲۶) و از ریشه فساد اســت (فراهیدی، ۱۴۰۹: ۲۳۱؛ حمیــری، ۱۴۲۰: ۵۱۸۳) و به معنای گرفتن مال بــه صورت ظالمانه (فیروزآبادی، ۱۴۲۴: ۲۷۷) قحط و خشــکی (طریحی، ۱۳۷۵: ۱۲۱) نیز آمده اســت. این واژه در معنای خروج از چیزی از حالت اعتدال نیز به‌کار می‌رود. چنانکه راغب در *مفردات راغب* آورده است: «کسی که در شهر با سلاح تهدید کند دستش قطع می‌شود و اگر با این ابزار کســی را بزند کشــته می‌شود» (راغب، ۱۴۱۲: ۶۳۶) بر این اساس برخی با توجه به معنای لغوی فســاد معتقدند که می‌توان قتل، ظلم، کفر، جنگ، تضییع حقوق دیگران و اخلال در احکام الهی، قوانین و مقررات اســلامی را که همگی ضد اصلاح‌اند، از مصادیق افساد برشمرد (بای، ۱۳۹۵: ۳۰).

دربــاره مفهوم «فی‌الارض» برخی قائل بر دو احتمال هســتند. احتمال اول آن است که محل حلول فساد و ظرف ارتکاب این گناه کره خاکی است. احتمال دوم آن اســت که قید «فی‌الارض» کنایه از گستردگی عمل مرتکب و گویای برپاکردن فساد در منطقه یا ناحیه‌ای از زمین اســت (همان: ۳۲). بر این اســاس گفته شده است: «افســادفی‌الارض در اصطلاح هر نوع عملی است که جامعه را از حالت تعادل خارج کند و منشــأ فساد گسترده در محیطی شــود؛ هرچند بدون توسل به اسلحه باشد. بدیهی است که در این اندیشه حیات اجتماعی، اخلاقی، اقتصادی و فرهنگی و ... متعادل متصور شــده است که افساد این حالت را دچار آشفتگی و اختلال می‌کند» (برهانی و احمدزاده، ۱۳۹۷: ۲۱۲).

ایجاد آشفتگی و اختلال تنها محدود به فضای سنتی نیست، بلکه امروزه فضای ســایبر یا به اصطلاح «فضای مجازی» امکانات و تســهیلاتی را برای افراد جامعه به ارمغان آورده اســت که این امر اکثر افراد جامعه را به ســوی خودکشانده و خود را در کنار فضای ســنتی قرار داده است. برای مثال اگر یک حمله سایبری باعث قطع

برق سراسری شـود، چه آثار نامطلوبی در جامعه از خود باقی خواهد گذاشت. اگر با توجه به معنای لغوی فسـاد بتوان مواردی همچون ظلم، تضییع حقوق دیگران و اخلال در قوانین و مقررات اسـلامی را از مصادیق افسـاد برشمرد در این صورت تفاوتی نمی‌کند که این مصادیق در فضای سنتی تحقق یابند یا در فضای سایبر که امروزه تمامی افراد جامعه بخشی از زندگی خود را در آن می‌گذارند.

۲-۳. شرایط تحقق عنوان افسادفی‌الارض در حملات سایبری

قانونگذار در ماده (۲۸۶) قانون مجازات اسـلامی بـدون ارائه تعریف مجزایی از رفتار مجرمانه افسـادفی‌الارض مقرر داشته است: «هرکس به‌طور گسترده مرتکب جنایات علیه تمامیت جسمانی افراد، جرائم علیه امنیت داخلی یا خارجی کشور، نشـر اکاذیب، اخلال در نظام اقتصادی کشـور، احراق و تخریب، پخش مواد سمی و میکروبـی خطرناک یا دایر کردن مراکز فسـاد و فحشـا یا معاونت در آنها شـود، به‌گونه‌ای که موجب اخلال شـدید در نظم عمومی کشـور، ناامنی یا ورود خسارت عمده به تمامیت جسمانی افراد یا اموال عمومی و خصوصی، یا سبب اشاعه فحشا در حد وسیع شود مفسد فی‌الارض محسوب و به اعدام محکوم می‌شود».

بـا توجه به منطوق ماده (۲۸۶) قانون مجازات اسـلامی، مقنن در رابطه با رکن مادی، بیش از هر چیز به گستردگی اقدامات مرتکب و وسعت نتایج زیان‌بار حاصل از آن توجه داشـته است و اوصاف مذکور نقش اساسـی و محوری در ساختار جرم افساد فی‌الارض ایفا می‌کنند (رهبرپور و نورمحمدی، ۱۳۹۷: ۲۱۱).

حملات سـایبری نیز طیف وسـیعی از شـبکه‌های رایانه‌ای را تحت تأثیر قرار می‌دهد، در نتیجه وسـیع و گسـترده بودن جرائم ارتکابی مذکـور در ماده (۲۸۶) قانون مجازات اسـلامی که در حقیقت مربوط به رکن مادی جرم افسـاد فی‌الارض است در ذات حملات سایبری نهفته است.

با توجه به مفهوم حمله سایبری و سامانه‌های رایانه‌ای ذکر شده در ماده (۷۳۹) قانون مجازات اسلامی (تعزیرات) و هشت دسته عمده جرائم یاد شده در ماده (۲۸۶) قانون مجازات اسلامی بدیهی است فقط ۶ مورد آن یعنی «جنایات علیه تمامیت جسمانی افراد»، «جرائم علیه امنیت داخلی یا خارجی کشور»، «اخلال در نظام اقتصادی کشور»، «احراق»، «تخریب» و «پخش مواد سمی و میکروبی و خطرناک» توسط حملات سایبری قابل تحقق هستند[1] و دو مورد دیگر یعنی «نشر اکاذیب» و «دایر کردن مرکز فساد و فحشا» از شمول مفهوم حملات سایبری خارج هستند. علت آن است که در یک تقسیم‌بندی جرائم رایانه‌ای به دو دسته وسیله‌محور و موضوع‌محور تقسیم می‌شوند. جرائم رایانه‌ای وسیله‌محور جرائمی هستند که در آن سامانه رایانه‌ای وسیله ارتکاب است؛ مانند نشر اکاذیب یا ایجاد مرکز فساد و فحشا از طریق سامانه رایانه‌ای. درحالی‌که در جرائم رایانه‌ای موضوع‌محور (محض)، سامانه رایانه‌ای موضوع جرم هستند که با توجه به مفهوم اتخاذ شده از حمله سایبری در پژوهش حاضر، حملات سایبری زیرمجموعه‌ای از جرائم رایانه‌ای موضوع‌محور قرار می‌گیرند.

۴. جمع‌بندی و نتیجه‌گیری

قانونگذار ایران در ماده (۷۳۹) قانون مجازات اسلامی (ماده (۱۱) قانون جرائم رایانه‌ای) به جرم‌انگاری رفتارهای مجرمانه‌ای که علیه سامانه‌های ارائه‌دهنده خدمات ضروری عمومی ارتکاب می‌یابند، پرداخته است و برای مرتکب آن صرفاً

۱. برای مثال حمله سایبری به سامانه‌های رایانه‌ای کنترلی گازرسانی ممکن است به انفجار در خط لوله‌های گازرسانی منجر شده و باعث احراق، تخریب و از دست دادن جان چندین شهروند شود یا حمله به سامانه‌های رایانه‌ای کنترلی بانکداری به اخلال در نظام پولی و بانکی یک کشور منجر شود. همچنین حمله به سامانه‌های رایانه‌ای کنترلی حمل‌ونقل مواد سمی و میکروبی منجر به انتشار آنان در فضای واقعی شود.

مجازات تعزیری حبس ۳ تا ۱۰ سال پیش‌بینی کرده است، درحالی‌که ماهیت و کاربردهای سامانه‌های رایانه‌ای موضوع ماده (۷۳۹) قانون مجازات اسلامی موجب می‌شود هرگاه آنها موضوع حملات سایبری قرار گیرند در حد وسیع و گسترده‌ای نظم، امنیت و آسایش عمومی در فضای سایبر و واقعی (فیزیکی) را برهم زنند.

ممکن است به نظر آید سلب امنیت در محیط توسط حملات سایبری ایجاد می‌شود و گزینش عنوان حدی «محاربه» برای مجازات مرتکبین آن مناسب به نظر آید، اما ازآنجاکه مفهوم سلاح مدنظر مشهور فقها و حقوق ایران ناظر بر سلاح‌های ملموس و مادی است و نمی‌توان آن را به سلاح‌های سایبری غیرمادی و غیرملموس تسری داد، در نتیجه با فقدان یکی از ارکان و شرایط عنوان حدی «محاربه» یعنی سلاح کشیدن تمسک به عنوان حدی «محاربه» صحیح نیست.

با توجه به منطوق ماده (۲۸۶) قانون مجازات اسلامی قانونگذار در رابطه با رکن مادی بیش از هر چیز به گستردگی اقدامات مرتکب و وسعت نتایج زیان‌بار حاصله توجه داشته است، به‌نحوی‌که اوصاف مذکور نقش اساسی و محوری در ساختار جرم افسادفی‌الارض ایفا می‌کنند. در این صورت همان‌طورکه گفته شد به دلیل آنکه یک حمله سایبری گروه یا شبکه‌ای از سامانه‌های رایانه‌ای را تحت تأثیر قرار می‌دهد، این امر موجب گستردگی و وسعت نتایج زیان‌بار ناشی از حملات سایبری می‌شود، در نتیجه شرط وسیع و گسترده بودن جرائم ارتکابی مذکور در ماده (۲۸۶) ق.م.ا که در حقیقت مربوط به رکن مادی جرم افسادفی‌الارض است توسط حملات سایبری تحقق می‌یابند. همچنین با توجه به ذکر عناصر مادی حمله سایبری و هشت دسته عمده جرائم ذکر شده در ماده (۲۸۶) ق.م.ا فقط ۶ مورد آن یعنی «جنایات علیه تمامیت جسمانی افراد»، «جرائم علیه امنیت داخلی یا خارجی کشور»، «اخلال در نظام اقتصادی کشور»، «احراق»، «تخریب»، «پخش

مواد سمی و میکروبی و خطرناک» توسط حملات سایبری قابل تحقق هستند.

پیرامون عنصر معنوی نیز باید بیان داشت، احراز قصد و نیت خاص حملات سایبری در جهت افسادفی‌الارض، یعنی اخلال گسترده در نظم عمومی، ایجاد ناامنی، ایراد خسارت عمومی و یا اشاعه فساد یا فحشا در حد وسیع و یا علم به مؤثر بودن اقدامات امری دشوار است، زیرا قصد امری ذهنی و درونی است و تأکید بر لزوم اثبات آن باعث بلاکیفر ماندن بسیاری از مهاجمان سایبری 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 ... را شامل خواهد شد. با بررسی و تحلیل عناصر مادی و معنوی افسادفی‌الارض و تطبیق آن با حملات سایبری ارتکابی علیه سامانه‌های رایانه‌ای موضوع ماده (۷۳۹) قانون مجازات اسلامی، شایسته است یک تبصره به ماده (۷۳۹) قانون مجازات اسلامی (ماده (۱۱) قانون جرائم رایانه‌ای) اضافه شود: «هرکس به قصد به خطر انداختن امنیت، آسایش و امنیت عمومی اعمال مذکور در مواد (۸، ۹ و ۱۰) این قانون را توسط حمله سایبری 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 شوند، چنانچه حمله ارتکابی مصداق عنوان افسادفی‌الارض نباشد، به حبس از ۳ تا ۱۰ سال محکوم خواهد شد». همان‌طور که از تعریف پیشنهاد شده قابل استنباط است شرط تحقق عنوان حدی «افسادفی‌الارض» آن است که در وهله اول رفتار ارتکابی از ماهیت حمله سایبری برخوردار باشد نه ماهیت جرم رایانه‌ای چراکه حملات سایبری دارای ماهیت گسترده و سازمان‌یافته هستند. در وهله دوم موضوع حمله

سایبری سامانه‌ها و داده‌های رایانه‌ای مطرح است که باید در راستای ارائه خدمات ضروری عمومی مشغول به فعالیت باشند. ازاین‌رو هر سامانه یا داده رایانه‌ای را نمی‌توان موضوع این تبصره در نظر گرفت و در نهایت لزوم قصد به خطر انداختن امنیت، آسایش و امنیت عمومی ضروری است.

بنابراین با توجه به ویژگی‌ها و آثار و نتایج گسترده و زیان‌بار حملات سایبری علیه سامانه‌های رایانه‌ای ارائه‌دهنده خدمات ضروری، جهت پیشگیری از جرم و بازدارنده بودن مجازات‌ها و مقابله مناسب با این حملات همان‌طور که ذکر شد نیاز به اصلاح قانون در این زمینه وجود دارد و رعایت اصل تناسب جرم و مجازات چنین اقتضایی را دارد و صرفاً برای واکنش در مقابل این حملات سایبری نمی‌توان به حبس تعزیری در قبال مرتکب حمله سایبری اکتفا کرد.

منابع و مآخذ

۱. ابن‌منظور، محمدبن مکرم (۱۴۰۸). *لسان‌العرب*، جلد اول، چاپ اول، بیروت، نشر داراالاحیاء التراث العربیه.

۲. ایزدی‌فر، علی‌اکبر و مجتبی حسین‌نژاد (۱۳۹۵). «بررسی فقهی افسادفی‌الارض»، مجله *پژوهش‌های فقه و حقوق اسلامی*، دوره ۱۲، ش ۱۴.

۳. بای، حسینعلی (۱۳۹۵). «افسادفی‌الارض، مفسدفی‌الارض کیست؟»، مجله *حقوق اسلامی*، دوره ۳، ش ۲۹.

۴. برهانی، محسن (۱۳۹۴). «افسادفی‌الارض، ابهام مفهومی، مفاسد عملی (تحلیل حقوقی ماده (۲۸۶) قانون مجازات اسلامی)»، مجله *مطالعات حقوق کیفری و جرم‌شناسی*، دوره ۲، ش ۲و۳.

۵. برهانی، محسن و رسول احمدزاده (۱۳۹۷). «معیارهای ناظر بر شناسایی مفسدفی‌الارض با تأکید بر جرائم مواد مخدر»، مجله *مطالعات حقوق کیفری و جرم‌شناسی*، دوره ۴۸، ش ۲.

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

۷. حائری، سیدکاظم (۱۳۸۶). «انواع تعزیرات و ضوابط آن»، فصلنامه تخصصی *فقه اهل بیت*، سال سیزدهم، ش ۵۱.

۸. حر عاملی (۱۴۰۱). *وسایل‌الشیعه*، جلد هجدهم، باب دوم از ابواب حدالمحارب، چاپ پنجم، تهران، نشر مکتبه الاسلامیه.

۹. جسن بیگی، ابراهیم(۱۳۸۴).حقوق و امنیت در فضای سایبر، چاپ اول، تهران، مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر.

۱۰. حلی، حسن‌بن‌یوسف (۱۴۱۳). *قواعدالاحکام*، جلد سوم، چاپ اول، قم، دفتر انتشارات اسلامی قم.

۱۱. حلـی، محمدبن‌حسن‌بن‌یوسـف (۱۳۸۷). *ایضاح‌الفوائد*، جلد چهارم، چاپ اول، قم، نشـر مؤسسه اسماعیلیان.

۱۲. حمیـری، نشوان‌بن‌سـعید (۱۴۲۰). *شـمس‌العلوم*، جلد هشـتم، چاپ اول، بیروت، نشـر دارالفکر.

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

۱۴. داوری دولت‌آبادی، مجید (۱۳۹۳). *بدافزارها و راهکارهای مقابله*، چاپ اول، تهران، نشـر پندارپارس.

۱۵. راغـب، حسـین‌بن‌محمد (۱۴۱۲). *المفـردات فی غریب القرآن*، چاپ اول، دمشـق، نشـر دارالقلم.

۱۶. رحمتی، محمد (۱۳۷۵). *کتاب الحدود و التعزیرات*، جلد دوم، چاپ اول، قم، نشر مؤلف.

۱۷. رهبرپـور، محمدرضـا و حسـین نورمحمـدی (۱۳۹۷). «چالش‌های حقوقـی - قضایی جرم افسادفی‌الارض در قانون مجازات اسلامی ۱۳۹۲»، *پژوهش حقوق کیفری*، سال ششم، ش ۲۲.

۱۸. طباطبایی، سـیدعلی (۱۴۱۸). *ریاض‌المسـائل*، جلد شـانزدهم، چاپ اول، قم، مؤسسـه آل‌البیت علیهم‌السلام لاحیاءالتراث.

۱۹. طریحی، فخرالدین (۱۳۷۵). *مجمع‌البحرین*، جلدسوم، چاپ‌سوم، تهران، نشرمکتبه‌المرتضویه.

۲۰. طوسی، ابوجعفر محمدبن‌حسن (۱۴۰۰). *النهایه*، چاپ دوم، بیروت، نشر دارالکتب العربی.

۲۱. --- (۱۴۰۷). *الخلاف*، جلد پنجم، چاپ اول، قم، دفتر انتشارات اسلامی.

۲۲. 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.

۲۳. فاضل‌هندی، محمدبن‌حسن (۱۴۱۶). *کشف‌اللثام*، جلددهم، چاپ‌اول، قم، دفترانتشارات‌اسلامی.

۲۴. فراهیدی، عبدالرحمن خلیل‌بن‌احمد (۱۴۰۹). *کتاب‌العین*، جلد هفتم، چاپ دوم، قم، نشر مؤسسه دارالهجره.

۲۵. فیروزآبادی، محمدبن‌یعقوب (۱۴۲۴). *القاموس‌المحیط*، چاپ اول، تهران، نشر دارالفکر.

۲۶. محقق‌حلی، ابوالقاسم (۱۴۰۸). *شرائع‌الاسلام*، جلد چهارم، چاپ دوم، قم، نشر مؤسسه اسماعیلیان.

۲۷. 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.

۲۸. معین، محمد (۱۳۸۴). *فرهنگ معین*، تهران، چاپ دوم، نشر راه ارشد.

۲۹. مفید، محمدبن‌محمدبن‌نعمان (۱۴۱۰). *المقنعه*، چاپ دوم، قم، مؤسسه نشر اسلامی.

۳۰. مقدس اردبیلی، احمدبن‌محمد (۱۴۰۳). *مجمع‌الفائده*، جلد سیزدهم، چاپ اول، قم، دفتر انتشارات اسلامی.

۳۱. منتظری، حسینعلی (۱۳۶۷). *مبانی فقهی حکومت اسلام*، ترجمه محمود صلواتی، جلد سوم، چاپ اول، تهران، مؤسسه کیهان.

۳۲. موسوی اردبیلی، سیدعبدالکریم (۱۴۲۷). *فقه‌الحدود و التعزیرات*، جلد اول، چاپ اول، قم، دارالعلم.

۳۳. --- (۱۴۲۷). *فقه‌الحدود و التعزیرات*، جلد سوم، چاپ دوم، قم، مؤسسه نشر الجامعه المفید.

۳۴. موسوی‌الخمینی، سیدروح‌الله (۱۳۹۳). *تحریرالوسیله*، جلد دوم، چاپ سیزدهم، قم، نشر دارالعلم.

۳۵. موسوی گلپایگانی، سیدمحمدرضا (۱۴۱۲). *الدرالمنضود فی الاحکام الحدود*، جلد دوم، چاپ اول، قم، دارالقرآن الکریم.

۳۶. مؤمن، محمد (۱۴۱۵). *کلمات سدیده فی مسائل جدیده*، چاپ اول، قم، مکتبه امیرالمؤمنین (دارالعلم مفید).

۳۷. میرمحمدصادقی، حسین (۱۳۹۳). *جرائم علیه امنیت و آسایش عمومی*، چاپ بیست‌وپنج، تهران، نشر میزان.

۳۸. نجفی الجواهری، محمدحسن (۱۴۰۴). *جواهر الکلام فی شرح شرائع الإسلام*، جلد ۴۱، چاپ هفتم، نشر، دار إحیاء التراث العربی.

۳۹. هاشمی شاهرودی، سیدمحمود (۱۳۷۶). «محارب کیست و محاربه چیست؟ (بحثی در شناخت موضوع محاربه)»، مجله *فقه اهل بیت (ع)*، ش ۱۱ و ۱۲.

۴۰. یکرنگی، محمد و هادی مرسی (۱۳۹۹). «تحلیل جرم‌انگاری تولید و پخش نرم‌افزار و ابزار الکترونیکی صرفاً مجرمانه در سیاست کیفری ایران در پرتو اسناد فرامرزی»، فصلنامه *دیدگاه حقوق قضایی*، دوره ۲۵، ش ۹۲.

41. Andress, Jason and Steve Winterfeld (2011). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, Amesterdam, Boston, Syngress/Elsevier.

42. Army, U. (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.

43. Eneken, T., K. Kardri and V. Liis (2010). "International Cyber Incidents: Legal Considerations, Cooperatative Cyber Defence Center of Excellence", Tallinn, Estonia, CCDCOE, Available at: https://ccdcoe.org/publications/books/legalconsiderations.pdf.

44. Kimburg, A. and H. Tirmaa-Klaar (2011). "Cybersecurity and Cyberpower: Consept, Condition and Capabilities for Cooperaion for Action Within the EU", European Parliament, Avalaible at: http://www.europarl.europa.eu/RegData/etudes/STUD/2011/433828/EXPOSEDE_ET(2011) 433828_EN.pdf.

45. Lord, K.M. and T. Sharp (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.