

# 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؛ در حالی که وقوع حملات سایبری علیه سامانه‌های رایانه‌ای ارائه‌دهنده خدمات ضروری از قبیل خدمات درمانی، آب، برق، گاز، مخابرات، حمل و نقل 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 در صدد است تا با بررسی مبانی فقهی و شرایط قانونی دو عنوان حدی «محاربه» و «افساد فی الارض»، امکان تسری ماده (۲۷۹) قانون مجازات اسلامی (محاربه) و ماده (۲۸۶) قانون مجازات اسلامی (افساد فی الارض) نسبت به حملات سایبری علیه سامانه‌های رایانه‌ای موضوع ماده (۷۳۹) قانون مجازات اسلامی را مورد تحلیل و ارزیابی قرار دهد تا مشخص کند با کدام یک 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 غیر ملموس سایبری را به آنچه که مشهور فقها و قانونگذاران از واژه سلاح اراده کرده‌اند نمی‌توان تسری داد، در نتیجه عنوان حدی «محاربه» برای این گونه حملات سایبری قابل تسری نیست، بلکه عنوان حدی «افساد فی الارض» با لحاظ شرایط مقرر در قانون مجازات اسلامی قابل تسری خواهد بود.

**کلیدواژه‌ها:** جرائم سایبری؛ خدمات ضروری؛ حملات سایبری؛ محاربه؛ افساد فی الارض

\* 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 یکصد و سی‌و‌سیزدهم، بهار ۱۴۰۲

doi: 10.22034/MR-2107-4724

### مقدمه

قانونگذار ایران در تاریخ ۱۳۸۸/۳/۵ با تصویب قانون جرائم رایانه‌ای به مقابله کیفی با جرائم سایبری پرداخت اما در آن زمان حملات سایبری روند رو به رشد خود را طی نکرده بودند و تفاوت میان مفهوم آن با مفهوم جرائم رایانه‌ای چندان ملموس و قابل درک نبود و این عوامل باعث شده بود قانونگذار از مقابله کیفی با این رفتار شنیع مجرمانه سایبری غافل بماند و در قالب جرائم رایانه‌ای به مقابله با آن بپردازد. در حالی که امروزه مشخص شده است از حیث ماهیت، حملات سایبری از جرائم رایانه‌ای متفاوت است زیرا حملات سایبری دارای ماهیت فراملی، سازمان یافته بوده و میان دولت‌ها با یکدیگر تحقق می‌یابد، در حالی که چنین امری در جرائم سایبری صادق نیست. همچنین هدف از پیش‌بینی مواد مقرر در قانون جرائم رایانه‌ای حمایت از داده‌ها و سامانه‌های رایانه‌ای شهروندان است در حالی که هدف در عنوان مجرمانه حمله سایبری حمایت از داده‌ها و سامانه‌های رایانه‌ای است که هرگونه اختلال در آنها موجب لطمه دیدن نظم عمومی در سطح وسیع شده و امنیت یک کشور را به مخاطره می‌اندازد. برای نمونه می‌توان به حمله سایبری استاکس نت<sup>۱</sup> در سال ۱۳۸۹ علیه نیروگاه هسته‌ای و حمله سایبری دوکو<sup>۲</sup> در سال ۱۳۹۰ و حمله سایبری فلیم<sup>۳</sup> در سال ۱۳۹۱ اشاره کرد و حمله‌ای که اخیراً مورخ ۱۴۰۰/۱/۲۲ علیه شبکه برق تأسیسات غنی‌سازی نطنز در ایران ارتکاب یافت که موجب انفجار در آن مرکز شد که ممکن بود صدها نفر جان خود را از دست بدهند.

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

---

1. Stuxnet  
2. Duqu  
3. Flame

شده است 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 اسلامی میزان حبس تعزیری ۳ تا ۱۰ سال باشد. این میزان مجازات ممکن است برای جرائم سایبری که از چنان گستردگی آثار زیان‌بار برخوردار نیست، 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 علاوه بر اخلال در فضای سایبر موجب اخلال و رعب و وحشت در فضای واقعی نیز می‌شوند و زندگی بسیاری از شهروندان، اقتصاد و امنیت یک کشور را تحت تأثیر خود قرار می‌دهد، چندان قابل توجیه نباشد. برای مثال تصور کنید تداخل در سامانه‌های ناوبری هوایی که باعث سقوط هواپیما شده و جان صدها انسان را می‌گیرد، چه آثار نامطلوبی از خود باقی خواهد گذاشت. از نمونه آثار مخرب حملات سایبری می‌توان به حملات ارتكابی علیه کشور استونی اشاره کرد که بسیاری از بخش‌های تجاری و صنعتی آن کشور را تحت تأثیر قرار داد و انجام فعالیت‌های روزمره بسیاری از کاربران را مختل کرد، به‌گونه‌ای که مانع خدمات عمومی اینترنتی از قبیل ارائه گزارش‌های مالیاتی، درخواست برای یارانه‌ها، مزایای دولتی و ... شد که توسط دولت برای رفاه حال شهروندان در نظر گرفته شده بود (Eneken, Kardri and Liis, 2010: 10).

ضرورت این پژوهش از آن رو 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 یک جرم عادی رایانه‌ای برخورد کرد و میزان مجازات تعزیری ۳ تا ۱۰ سال را

در نظر گرفت یا می‌توان به عناوین حدی از قبیل «محرابه» یا «افساد فی الارض» تمسک جست؟ در صورت تمسک به عناوین حدی برای مقابله با حملات سایبری به کدام یک از دو عنوان حدی یعنی «محرابه» یا «افساد فی الارض» پیش‌بینی شده در قانون مجازات اسلامی می‌توان تمسک جست و شرایط تحقق هر یک از آنان چیست؟ از این رو پژوهش حاضر ابتدا به بیان مفهوم حمله سایبری و ویژگی‌ها و گستردگی آثار مخرب آن می‌پردازد تا وجه تمایز آن از مفهوم جرم رایانه‌ای مشخص شده و سپس با توجه به مبانی فقهی و قانونی دو عنوان «محرابه» و «افساد فی الارض» قابلیت اعمال هر یک از آنان را نسبت به این‌گونه حملات سایبری مورد ارزیابی قرار می‌دهد.

### ۱. مفهوم حملات سایبری، ویژگی‌ها و گستردگی آثار آن

برای آنکه بتوان به رویکردهای مقابله با حملات سایبری در قانون مجازات اسلامی دست یافت، لازم است مفهوم حمله سایبری، ویژگی‌ها و گستردگی آثار آن تبیین شود.

#### ۱-۱. مفهوم حمله سایبری

در مورد مفهوم حمله سایبری تعریف واحد و مشترکی وجود ندارد، بلکه هر یک از کارشناسان و صاحب‌نظران از دید خود به بیان مفهوم حمله سایبری پرداخته‌اند. به عنوان مثال در تعریف حمله سایبری گفته شده است: «حملات سایبری مجموعه اقداماتی هستند که توسط یک دولت به منظور نفوذ یا ایجاد اختلال در سامانه‌های رایانه‌ای و یا شبکه رایانه‌ای، علیه دولت دیگر ارتکاب می‌یابد» (خلیل‌زاده، ۱۳۹۳: ۲۶). حملات سایبری به معنای «ایجاد اختلال 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 سامانه‌های رایانه‌ای به قصد تضعیف تمام یا بخشی اعظمی از سامانه‌های رایانه‌ای متعلق به یک گروه خاص اعم از کاربران اینترنتی، سازمان‌ها، نهادها و... 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 متعلق به 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.
- رو نوشت یا برش از داده‌های ذخیره شده موجود در یک سامانه‌ها س رایانه‌ای که متعلق به یک گروه خاص است. منظور از گروه خاص در تعریف مذکور اعم

از کاربران اینترنتی، سازمان‌ها، نهادها و... است (همان: ۱۲۳-۱۲۲). مطابق این تعریف مصادیق عنصر مادی حملات سایبری را می‌توان تحت عناوین جرائم عیله صحت، تمامیت و دسترس‌پذیری سامانه‌های رایانه‌ای و داده‌های ذخیره شده در درون آن قرار داد.

عنصر روانی در حمله سایبری عبارت است از قصد تضعیف عملکرد تمام یا بخش اعظمی از شبکه‌های رایانه‌ای متعلق به یک گروه خاص. به عبارت دیگر سامانه‌های رایانه‌ای قربانی حملات سایبری، نه به عنوان یک سامانه رایانه‌ای بلکه به عنوان عضوی از یک شبکه رایانه‌ای متعلق به یک گروه خاص، قربانی می‌شوند (همان: ۱۲۴-۱۲۳). از سوی دیگر باید در نظر داشت احراز قصد و نیت خاص حملات سایبری، یعنی قصد تضعیف تمام یا بخش اعظمی از سامانه‌های رایانه‌ای متعلق به 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 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. به عبارت دیگر کیفیت وقایع ممکن است به گونه‌ای باشد که اثبات کند مهاجم می‌دانسته یا علم به وقوع داشته است.

## ۱-۲. ویژگی‌های حملات سایبری و گستردگی آثار آن

کم‌رنگ شدن نقش جغرافیا یکی از ویژگی‌های بستر حملات سایبری به شمار می‌آید. این امر بر کسی پوشیده نیست که شبکه جهانی اینترنت،<sup>۱</sup> 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 ارتکاب یافته از آن سوی مرزها حمایت کنند و موجب حملات سایبری منسجم‌تر و هدفمندتری شوند تا نتایج بسیار زیانباری را سبب شوند، در حالی که 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»<sup>۱</sup> 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 خدمات‌های مختلف را مسدود کند (دستر، 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. به عبارت دیگر 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 به گونه‌ای نامتمرکز است، این ماهیت ساختاری توجه بسیاری از مهاجمان سایبری را به سوی خود جلب کرده است؛ زیرا این توانایی و قابلیت را به آنان داده است تا بدون آنکه اثر یا نامی از خود باقی بگذارند 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 منصفه 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 (حسن بیگی، ۱۳۸۴: ۳).

## ۲. مقابله با حملات سایبری علیه سامانه‌های رایانه‌ای ارائه‌دهنده خدمات ضروری در قالب محاربه یا افساد فی الارض

بر اساس 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 «افساد فی الارض» در فقه



و حقوق اسلامی قرار داد. بنابراین باید توجه داشت که امکان تحقق محاربه یا افساد فی الارض در فضای سایبر متفرع بر آن است که موضوع آیه ۳۳ سوره مائده چیست؟ زیرا اکثریت قریب به اتفاق فقهای شیعه در آیه شریفه، افساد فی الارض را به محاربه معطوف می‌کنند در نتیجه معتقدند که آیه شریفه در مقام بیان تنها یک جرم است و افساد فی الارض عنوان مستقلی از محاربه نیست (هاشمی شاهرودی، ۱۳۷۶: ۲۰۰-۱۴۳؛ برهانی، ۱۳۹۴: ۲۲-۳۴). برخی معتقدند قانونگذار ایران در برخی از قوانین مصوب پس از انقلاب، برای اعمال 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 افساد فی الارض قابل توجیه نیست، چون با هیچ‌یک از حدود دیگر سنخیت ندارد و نمی‌توان آن را تعزیر (که لاجرم باید دون الحد باشد) تلقی کرد (میرمحمد صادقی، ۱۳۹۳: ۶۰)، زیرا این قاعده «التعزیر دون الحد» 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: ۳۶۵-۳۷۰). در مقابل تعداد بسیار معدودی از فقها حد افساد فی الارض 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 فی الارض 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 افساد فی الارض 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 افساد فی الارض را از محاربه تفکیک کرده و ماده (۲۸۶) و تبصره آن را به جرم افساد فی الارض تخصیص داد و مجازات اعدام را برای مرتکبان این جرم تعیین کرد. از این رو مبحث حاضر در دو قسمت به بررسی امکان تحقق عنوان فقهی «محاربه» و امکان تحقق عنوان فقهی «افساد فی الارض» 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 امکان سنجی تحقق عنوان فقهی «محاربه» در صورت وقوع یک حمله سایبری علیه سامانه‌های رایانه‌ای ارائه‌دهنده خدمات ضروری عمومی پرداخته شده است. از این رو ابتدا به تبیین مفهوم محاربه و سلاح پرداخته شده است تا مشخص شود آیا سلاح‌های سایبری وجود قید «سلاح» را در عنوان فقهی «محاربه» در بر می‌گیرند؟ سپس به بررسی شرایط لازم برای تحقق عنوان «محاربه» در این گونه 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 حربه 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 لسان العرب آمده: «غارت مال انسان و ترک آن شخص به گونه‌ای که هیچ چیزی برایش نماند» (ابن منظور، 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 ارباب آنهاست، به نحوی که 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). به این ترتیب علاوه بر وجود سوءنیت عام، یعنی عمد در کشیدن سلاح (تجريد 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.

### ۲-۱-۲-۱. 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. از این رو 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 به کار می‌روند، از قبیل خدمات درمانی، آب، برق، گاز، مخابرات، حمل و نقل و بانکداری مرتکب شوند، به حبس از ۳ تا ۱۰ سال محکوم خواهد شد». شایسته بود مقنن قید «در صورتی که عمل ارتكابی 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 ارتكابی 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 از آنجاکه 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. از این‌رو 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». از آنجاکه 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. به عبارت دیگر 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 یک‌سواز 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.<sup>۱</sup> 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)<sup>۲</sup> 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 به طوری که 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*, Amsterdam, Boston, Syngress/Elsevier, 2011, 123.

که در صدق محاربه نیازی به تشهیر 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 اجتماعی مردم و ایجاد ترس و رعب در دل آنهاست (موسوی اردبیلی، ۱۴۲۷: ۵۱۴-۵۱۵). حال منشأ این ناامنی از راهی که می‌خواهد باشد مثل اینکه شخصی بخواهد با شکناندن و تخریب سدهای آب و روانه کردن سیلاب به منازل و مزارع، جان و مال آنها را به خطر بیندازد (ایزدی فر و حسین نژاد، ۱۳۹۵: ۳۲).

بنابراین براساس قول دوم که اقل فقها را شامل می‌شود و قائل به این امر هستند که ایجاد ناامنی عمومی و برهم زدن اجتماع مردم موضوعیت داشته و منشأ 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 اسلامی 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 ارباب آنهاست، به نحوی که موجب ناامنی در محیط شود...».

در مورد معنای «سلاح» سه قول در میان فقها وجود دارد: قول اول با اشاره به خبر جابر از امام محمد باقر (ع): «کسی که در شهر با سلاح تهدید کند دستش قطع می‌شود و اگر با این ابزار کسی را بزند کشته می‌شود» (عاملی، ۱۴۰۱: ۵۲۸)، سلاح را محدود به سلاح آهنین مثل شمشیر، نیزه، قمه، خنجر و چاقو کرده‌اند و وسایلی چون چوب و سنگ و تازیانه را از شمول آن خارج دانسته‌اند (میرمحمدصادقی، ۱۳۹۳: ۵۰). در تحریرالوسیله نیز چنین آمده است: «اگر کسی بدون سلاح به دیگری حمله کند برای اینکه مال او را بستاند 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 کسی ثابت نیست. اگر کسی با تازیانه و عصا و سنگ 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 به کار 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 امثال‌های 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 غیر خودکار، 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. از این رو 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 از آنجاکه 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 غیر ملموس 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 بر نمی‌تابد. اما باید توجه داشت مقنن به عنوان یک جرم‌مانع، تولیدکنندگان، منتشرکنندگان و توزیع‌کنندگان بدافزارها را به حال خویش رها نکرده است بلکه در قبال بدافزارها که امروزه به عنوان یک ابزار در جهت حملات سایبری استفاده می‌شوند، در بند «الف» ماده (۲۵) «قانون جرائم رایانه‌ای»<sup>۲</sup> به جرم‌انگاری فرایند تولید، انتشار یا توزیع و در دسترس قرار دادن آن اهتمام ورزیده است (یکرنگی و مرسی، ۱۳۹۹: ۳۲۳).

### ۳. مفهوم افساد فی الارض 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 «افساد فی الارض» در خصوص حملات سایبری علیه سامانه‌های رایانه‌ای ارائه‌دهنده خدمات ضروری خواهیم پرداخت.

#### ۳-۱. مفهوم افساد فی الارض

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

درباره مفهوم «فی الارض» برخی قائل بر دو احتمال هستند. احتمال اول آن است که محل حلول فساد و ظرف ارتکاب این گناه کره خاکی است. احتمال دوم آن است که قید «فی الارض» کنایه از گستردگی عمل مرتکب و گویای برپا کردن فساد در منطقه یا ناحیه‌ای از زمین است (همان: ۳۲). بر این اساس گفته شده است: «افساد فی الارض در اصطلاح هر نوع عملی است که جامعه را از حالت تعادل خارج کند و منشأ فساد گسترده در محیطی شود؛ هر چند بدون توسل به اسلحه باشد. بدیهی است که در این اندیشه حیات اجتماعی، اخلاقی، اقتصادی و فرهنگی و ... متعادل متصور شده 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 سایبر یا به اصطلاح «فضای مجازی» امکانات و تسهیلاتی را برای افراد جامعه به ارمغان آورده است که این امر اکثر افراد جامعه را به سوی خود کشانده و خود را در کنار فضای سنتی قرار داده است. برای مثال اگر یک حمله سایبری باعث قطع

برق سراسری شود، چه آثار نامطلوبی در جامعه از خود باقی خواهد گذاشت. اگر با توجه به معنای لغوی فساد بتوان مواردی همچون ظلم، تضییع حقوق دیگران و اخلال در قوانین و مقررات اسلامی را از مصادیق افساد 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 افساد فی الارض در حملات سایبری

قانونگذار در ماده (۲۸۶) قانون مجازات اسلامی بدون ارائه تعریف مجزایی از رفتار مجرمانه افساد فی الارض مقرر داشته است: «هرکس به طور گسترده مرتکب جنایات علیه تمامیت جسمانی افراد، جرائم علیه امنیت داخلی یا خارجی کشور، نشر اکاذیب، اخلال در نظام اقتصادی کشور، احراق و تخریب، پخش مواد سمی و میکروبی خطرناک یا دایر کردن مراکز فساد و فحشا یا معاونت در آنها شود، به گونه‌ای که موجب اخلال شدید در نظم عمومی کشور، ناامنی یا ورود خسارت عمده به تمامیت جسمانی افراد یا اموال عمومی و خصوصی، یا سبب اشاعه فحشا در حد وسیع شود مفسد فی الارض محسوب و به اعدام محکوم می‌شود».

با توجه به منطوق ماده (۲۸۶) قانون مجازات اسلامی، مقنن در رابطه با رکن مادی، بیش از هر چیز به گستردگی اقدامات مرتکب و وسعت نتایج زیان بار حاصل از آن توجه داشته است و اوصاف مذکور نقش اساسی و محوری در ساختار جرم افساد فی الارض ایفا می‌کنند (رهبرپور و نورمحمدی، ۱۳۹۷: ۲۱۱).

حملات سایبری نیز طیف وسیعی از شبکه‌های رایانه‌ای را تحت تأثیر قرار می‌دهد، در نتیجه وسیع و گسترده بودن جرائم ارتكابی مذکور در ماده (۲۸۶) قانون مجازات اسلامی که در حقیقت مربوط به رکن مادی جرم افساد فی الارض 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<sup>۱</sup> 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. در حالی که 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 حمل و نقل مواد سمی و میکروبی منجر به انتشار آنان در فضای واقعی شود.

مجازات تعزیری حبس ۳ تا ۱۰ سال پیش‌بینی کرده است، در حالی که 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 «محرابه» برای مجازات مرتکبین آن مناسب به نظر آید، اما از آنجاکه 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 «محرابه» یعنی سلاح کشیدن تمسک به عنوان حدی «محرابه» 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، به نحوی که اوصاف مذکور نقش اساسی و محوری در ساختار جرم افساد فی الارض ایفا می‌کنند. در این صورت همان‌طور که 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 ارتكابی مذکور در ماده (۲۸۶) ق.م.ا.ک در حقیقت مربوط به رکن مادی جرم افساد فی الارض 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 افساد فی الارض، 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 افساد فی الارض و تطبیق آن با حملات سایبری ارتكابی 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 به کار می‌روند، از قبیل خدمات درمانی، آب، برق، گاز، مخابرات، حمل و نقل و بانکداری مرتکب شوند، چنانچه حمله ارتكابی مصداق عنوان افساد فی الارض نباشد، به حبس از ۳ تا ۱۰ سال محکوم خواهد شد». همان‌طور که از تعریف پیشنهاد شده قابل استنباط است شرط تحقق عنوان حدی «افساد فی الارض» آن است که در وهله اول رفتار ارتكابی از ماهیت حمله سایبری برخوردار باشد نه ماهیت جرم رایانه‌ای چرا که حملات سایبری دارای ماهیت گسترده و سازمان یافته 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. از این رو 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 مأخذ

۱. ابن منظور، محمد بن مكرم (۱۴۰۸). *لسان العرب*، جلد اول، چاپ اول، بيروت، نشر دارالاحياء التراث العربيه.
۲. ایزدی فر، علی اکبر و مجتبی حسین نژاد (۱۳۹۵). «بررسی فقهی افساد فی الارض»، مجله پژوهش های فقه و حقوق اسلامی، دوره ۱۲، ش ۱۴.
۳. بای، حسینعلی (۱۳۹۵). «افساد فی الارض، مفسد فی الارض کیست؟»، مجله حقوق اسلامی، دوره ۳، ش ۲۹.
۴. برهانی، محسن (۱۳۹۴). «افساد فی الارض، ابهام مفهومی، مفسد عملی (تحلیل حقوقی ماده (۲۸۶) قانون مجازات اسلامی)»، مجله مطالعات حقوق کیفری و جرم شناسی، دوره ۲، ش ۳ و ۲.
۵. برهانی، محسن و رسول احمدزاده (۱۳۹۷). «معیارهای ناطر بر شناسایی مفسد فی الارض با تأکید بر جرائم مواد مخدر»، مجله مطالعات حقوق کیفری و جرم شناسی، 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 بین الملل، سال دوم، ش ۵.
۷. حائری، سید کاظم (۱۳۸۶). «انواع تعزیرات و ضوابط آن»، فصلنامه تخصصی فقه اهل بیت، سال سیزدهم، ش ۵۱.
۸. حر عاملی (۱۴۰۱). *وسائل الشیعه*، جلد هجدهم، باب دوم از ابواب حدالمحارب، چاپ پنجم، تهران، نشر مکتبه الاسلامیه.
۹. جسین بیگی، ابراهیم (۱۳۸۴). *حقوق و امنیت در فضای سایبر*، چاپ اول، تهران، مؤسسه فرهنگی مطالعات و تحقیقات بین المللی ابرار معاصر.
۱۰. حلی، حسن بن یوسف (۱۴۱۳). *قواعد الاحکام*، جلد سوم، چاپ اول، قم، دفتر انتشارات اسلامی قم.



۱۱. حلی، محمدبن حسن بن یوسف (۱۳۸۷). *ایضاح الفوائد*، جلد چهارم، چاپ اول، قم، نشر مؤسسه اسماعیلیان.
۱۲. حمیری، نشوان بن سعید (۱۴۲۰). *شمس العلوم*، جلد هشتم، چاپ اول، بیروت، نشر دارالفکر.
۱۳. خلیل زاده، مونا (۱۳۹۳). *مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری*، چاپ اول تهران، نشر مجد.
۱۴. داوری دولت‌آبادی، مجید (۱۳۹۳). *بدا فزارها و راهکارهای مقابله*، چاپ اول، تهران، نشر پندارپارس.
۱۵. راغب، حسین بن محمد (۱۴۱۲). *المفردات فی غریب القرآن*، چاپ اول، دمشق، نشر دارالقلم.
۱۶. رحمتی، محمد (۱۳۷۵). *کتاب الحدود و التعزیرات*، جلد دوم، چاپ اول، قم، نشر مؤلف.
۱۷. رهبرپور، محمدرضا و حسین نورمحمدی (۱۳۹۷). «چالش‌های حقوقی - قضایی جرم افساد فی الارض در قانون مجازات اسلامی ۱۳۹۲»، پژوهش حقوق کیفری، سال ششم، ش ۲۲.
۱۸. طباطبایی، سیدعلی (۱۴۱۸). *ریاض المسائل*، جلد شانزدهم، چاپ اول، قم، مؤسسه آل‌البیت علیهم‌السلام لاحیاء التراث.
۱۹. طریحی، فخرالدین (۱۳۷۵). *مجمع‌البحرین*، جلد سوم، چاپ سوم، تهران، نشر مکتبه‌المرتضویه.
۲۰. طوسی، ابوجعفر محمدبن حسن (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، محمدبن حسن (۱۴۱۶). *کشف‌اللثام*، جلد دهم، چاپ اول، قم، دفتر انتشارات اسلامی.

۲۴. فراهیدی، عبدالرحمن خلیل بن احمد (۱۴۰۹). کتاب العین، جلد هفتم، چاپ دوم، قم، نشر مؤسسه دارالهجره.
۲۵. فیروزآبادی، محمد بن یعقوب (۱۴۲۴). القاموس المحيط، چاپ اول، تهران، نشر دارالفکر.
۲۶. محقق حلی، ابوالقاسم (۱۴۰۸). شرائع الاسلام، 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، محمد بن محمد بن نعمان (۱۴۱۰). المقنعه، چاپ دوم، قم، مؤسسه نشر اسلامی.
۳۰. مقدس اردبیلی، احمد بن محمد (۱۴۰۳). مجمع الفوائد، 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، سید عبدالکریم (۱۴۲۷). فقه الحدود و التعزیرات، جلد اول، چاپ اول، قم، دارالعلم.
۳۳. --- (۱۴۲۷). فقه الحدود و التعزیرات، جلد سوم، چاپ دوم، قم، مؤسسه نشر الجامعه المفید.
۳۴. موسوی خمینی، سید روح‌الله (۱۳۹۳). تحریر الوسیله، جلد دوم، چاپ سیزدهم، قم، نشر دارالعلم.
۳۵. موسوی گلپایگانی، سید محمد رضا (۱۴۱۲). الدر المنضود فی الاحکام الحدود، جلد دوم، چاپ اول، قم، دارالقرآن الکریم.
۳۶. مؤمن، محمد (۱۴۱۵). کلمات سدیدة فی مسائل جدیدة، چاپ اول، قم، مکتبه امیر المؤمنین (دارالعلم مفید).

راهبرد مقابله با حملات سایبری علیه سامانه‌های رایانه‌ای ارائه‌دهنده ... \_\_\_\_\_ ۵۵

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

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

۳۹. هاشمی شاهرودی، سید محمود (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*, Amsterdam, 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](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](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.