دورهٔ ۵۱، شمارهٔ ۲، پاییز و زمستان ۱۴۰۰
صفحات ۵۶۱ تا ۵۸۳ (مقالهٔ پژوهشی)
DOI:10.22059/JQCLCS.2021.306582.1587

امکان‌سنجی استناد به دفاع مشروع به‌عنوان مانع مسئولیت کیفری در مقابل حملهٔ سایبری

محمد یکرنگی*
استادیار گروه حقوق جزا و جرم‌شناسی، دانشکده حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران
هادی مرسی
دانشجوی دکترای حقوق جزا و جرم‌شناسی، دانشکده الهیات و معارف اسلامی، دانشگاه میبد، یزد، ایران
مهسا علیزاده
دانشجوی دکترای گروه حقوق، دانشکده حقوق، دانشگاه تربیت مدرس، تهران، ایران
(تاریخ دریافت: ۱۳۹۹/۵/۱- تاریخ تصویب: ۱۴۰۰/۱۲/۲۲)

چکیده
دفاع مشروع به‌عنوان یکی از موانع مسئولیت کیفری در حقوق ایران با دیدگاه جرائم سنتی تبیین شده است. با این حال، افزایش حملات سایبری در فضای مجازی و توسعهٔ فناوری برای مقابله با این حملات پیش از مداخلهٔ دولت و وجود آسیب‌های جبران‌ناپذیر، این پرسش را پیش می‌آورد که آیا می‌توان در برابر حملهٔ سایبری به‌عنوان بزه کیفری، به دفاع مشروع به‌عنوان یک عامل مانع مسئولیت در حقوق کیفری (فارغ از ضوابط دفاع مشروع در حقوق بین‌الملل) استناد کرد. پژوهش حاضر به‌صورت توصیفی-تحلیلی درصدد است با بررسی امکان‌سنجی تسری ضوابط حاکم بر دفاع مشروع سنتی به حملات سایبری و تحلیل مبنای دفاع مشروع در فضای مجازی در نهایت به تجزیه‌وتحلیل وضعیت حقوقی دفاع مشروع، با الهام از شرایط تعیین‌شده در مادهٔ ۱۵۶ ق.م.ا از منظر قانونی بپردازد. این تحقیق در نهایت نتیجه‌گیری می‌کند که امکان توسعهٔ دفاعیاتی مانند دفاع مشروع به جرائم سایبری وجود دارد و مبانی سنتی دفاع مشروع برای توجیه این نوع دفاع در جرائم سایبری کفایت می‌کند. همچنین حق دفاع مشروع در مقابل حملهٔ سایبری می‌تواند به‌عنوان یکی از حقوق کاربران (شهروندان سایبری) در فضای سایبر قلمداد شود تا آنان بتوانند با توسل به آن درصدد حمایت از داده‌ها و سامانه‌های رایانه‌ای متعلق به خود یا دیگری برآیند.

واژگان کلیدی
حملات سایبری، دفاع مشروع، فضای سایبر، مهاجم سایبری، مدافع سایبری.

* yekrangi@ut.ac.ir
ORCID iDs: https://orcid.org/0000-0001-6831-6835

مقدمه

حملات سایبری امروزه جزء جداناپذیر از فعالیت کسانی شده است که در فضای مجازی زیست می‌کنند. پیش از دو دهه قبل، کمتر کسی گمان می‌کرد که زندگی بشر در میان دو دنیا تقسیم شود. به‌گونه‌ای که در ابتدای ورود رایانه به زندگی انسان در نیمهٔ دوم سدهٔ بیستم، تنها بخش‌های خاصی از جامعه تحت تأثیر آن قرار گرفت، ولی در سال‌های اخیر رایانه از ساخته‌های بسیار مهم و منحصربه‌فرد بشری تلقی می‌شود که همهٔ ابعاد زندگی شهروندان را دگرگون ساخته و آثار گسترده‌ای در تمامی امور اقتصادی، اجتماعی، فرهنگی، سیاسی و غیره از خود باقی بر جای گذاشته است، به‌گونه‌ای که عصر حاضر را عصر «فناوری و اطلاعات» می‌نامند. با این حال، ظهور و بروز هر پدیده‌ای در عالم واقع می‌تواند همراه با احکام و ابعاد حقوقی باشد که از این نظر، فضای سایبر و بسترهای آن قابل تأمل است.

حفظ حریم و امنیت داده‌ها و سامانه‌های رایانه‌ای یکی از مسائل حاصل از گسترش فناوری اطلاعات و مستلزم آن است رویکردهای جدیدی به‌منظور حمایت از آنان اتخاذ کند. این رویکردها در دو حوزه است؛ اول رویکردهایی که با مداخله دولت صورت می‌گیرد. با این حال، همواره دولت نمی‌تواند در تمامی لحظات و ساحت‌های حیات شهروندان حضور داشته باشد. به همین روی، رویکرد دوم نیز در مقابله با جرائم توسط دولت‌ها پذیرفته شده است که در صورت عدم حضور دولت و ضرورت، شهروندان خود بتوانند به مقابله با رفتار مجرمانه که آنها را تهدید می‌کند، اقدام کنند و به‌عبارتی، از خود دفاعی مشروع کنند. با پذیرش حق دفاع برای شهروندان سایبری، قانونگذار می‌تواند در جهت تکمیل و اثرگذاری رویکردهای پیشین خود گام مؤثری در راستای حمایت از داده‌ها و سامانه‌های رایانه‌ای بردارد. این امر نسبت به حملات سایبری که به‌دلیل آنی بودن، امکان توسل به قوای دولتی بسیار کم است، اهمیتی مضاعف یافته است و همچنین می‌تواند از گسترش دامنهٔ نتایج زیانبار ناشی از آن بکاهد.

برای اهمیت این امر تصور کنید هر گاه موضوع حملات سایبری داده و سامانه‌های رایانه‌ای نهادهای دولتی، کشاورزی، مواد غذایی، آب، بهداشت عمومی، خدمات اورژانس، پایگاه‌های صنعتی، مخابرات، انرژی، حمل‌ونقل، بانکداری و امور مالی، تولید مواد دارویی یا به‌طور کلی زیرساخت‌های حیاتی کشوری در فضای سایبر باشد یا اگر موضوع حملات سایبری سامانه‌های کنترلی باشد که برای خدمات ضروری به‌کار می‌رود و سبب قطع برق سراسری یا مسموم کردن منابع غذایی می‌شود، چه آثار زیانباری بر جامعه با شخص تحمیل خواهد شد (سلمانی‌زاده، ۱۳۸۰: ۲۰). با به رسمیت شناختن حق دفاع در برابر حملات سایبری افراد می‌توانند با اقدامات به‌موقع خود و پیش از آنکه نتایج زیانبار ناشی از حملات سایبری به دیگر سامانه‌های رایانه‌ای گسترش

یابد یا فضای سنتی را تحت‌الشعاع قرار دهد، در برابر آن واکنش نشان دهند و آن را دفع کنند. ازاین‌رو بحث از پذیرش دفاع مشروع در برابر بزه حملات سایبری امری نه نظری، بلکه مهم و مبتلابه خواهد بود که بررسی آن با توجه به گسترش روزافزون حملات سایبری ضروری است.

با این حال، در خصوص دفاع مشروع در فضای سایبر به‌عنوان یکی از موانع مسئولیت کیفری، حقوق ایران مقررهٔ خاصی در خود ندارد و تنها مادهٔ ۱۵۶ ق.م.ا که با دیدگاه جرائم سنتی تدوین شده، به‌عنوان مستند دفاع مشروع، در حقوق ایران پذیرفته شده است. از طرفی، ویژگی‌های خاص حملات سایبری، مانند سرعت در بروز انتشار، سرایت و گستردگی نتایج زیانبار ناشی از آن و عدم مواجههٔ حضوری[1] میان مدافع و مهاجم در این فضا سبب می‌شود که تطبیق دفاع مشروع به معنای سنتی با آنچه در فضای سایبر مدنظر است، با ابهاماتی همراه شود. از طرف دیگر، می‌توان گفت ماهیت حملهٔ فعلی یا قریب‌الوقوع، ضرورت دفاع و رعایت مراحل دفاع از مواردی است که قابل تطبیق با فضای مجازی نیز است و می‌توان از مقررهٔ مادهٔ ۱۵۶ ق.م.ا برای دفاع مشروع سایبری هم بهره برد. به همین سبب تحقیق حاضر از مبنا آغاز کرده و در بند ابتدایی به تدقیق در موضوع امکان اعمال ضوابط دفاع مشروع سنتی به حملات سایبری می‌پردازد. در این بند به این بحث پرداخته می‌شود که آیا می‌توان مقرره‌ای را که با دیدگاه جرائم غیررایانه‌ای نگارش شده است، تسری داد و به‌عنوان دفاعی برای حملهٔ سایبری از آن بهره برد. بند دوم، به مبانی دفاع مشروع سایبری می‌پردازد و در پی پاسخگویی به این پرسش است که آیا می‌توان مبانی دفاع مشروع سنتی را برای توجیه دفاع مشروع در برابر حملات سایبری به‌کار برد. در این دو بند، تحقیق مبنایی است. در نهایت بند سوم با رویکرد توصیفی تحلیلی به ارزیابی ضوابط دفاع مشروع مقرر در مادهٔ ۱۵۶ ق.م.ا می‌پردازد و آن را با شرایط حملات سایبری تحلیل می‌کند و به مواردی مانند آنکه خطر یا تجاوزی که بتواند سامانهٔ رایانه‌ای دیگری را تهدید کند چگونه است و اساساً چگونه رخ می‌دهد؟ قریب‌الوقوع یا بالفعل بودن خطر در فضای سایبر چگونه تحقق‌پذیر است؟ در صورت تحقق فعلی یا قریب‌الوقوع خطر اساساً موضوعات مورد حمایت در دفاع مشروع در مقابل حملات سایبری چیست؟ آیا تنها مال و عرض شامل موضوعات مورد حمایت در این نوع خاص دفاع مشروع می‌شود یا آنکه حملات سایبری می‌تواند نفس یا آزادی تن را هم هدف قرار دهد مورد تحلیل قرار می‌گیرد.

---

۱. عدم مواجههٔ حضوری در حملات سایبری نشأت‌گرفته از ویژگی‌های بستر و مکان ارتکاب آن است، زیرا کمرنگ بودن نقش جغرافیا به‌عنوان یکی از ویژگی‌های فضای سایبر این امکان را برای مهاجمان سایبری فراهم کرده است که آنان از توانایی‌های لازم برای عبور از محدودهٔ مرزهای جغرافیایی خود برای رسیدن به اهداف اصلی خود برخوردار شوند. ر.ک: عظیمی و خشنودی، ۱۳۹۵: ۱۶۴.

۱. امکان اعمال ضوابط دفاع مشروع سنتی بر دفاع مشروع سایبری

فضای مجازی به عنوان فضایی جدای از دنیایی که در آن هر چیز قابل لمس است، درصورتی‌که دیدگاه شکاکیت هیومی به‌دلیل تجربه‌ناپذیر بودن این فضا کنار گذارده شود، امروزه به رسمیت شناخته شده است. بنابراین، حقوق نیز مانند سایر رشته‌ها و حتی اشخاص با دو دنیا مواجه است. به‌طور سنتی، حقوق ضوابط خود را بر پایهٔ دنیای واقعی بنا نهاده و با فرض واقعی بودن مرتکب جرم و فضای ارتکاب جرم مبادرت به وضع قانون کرده است، لیکن اکنون با روی کار آمدن فضای مجازی این پرسش مطرح است که آیا مقنن ضرورت دارد نسبت به هر امری که در فضای مجازی رخ می‌دهد، به‌طور مستقل مبادرت به وضع مقررات کند یا می‌توان مقررات حاکم بر فضای غیرمجازی را بر آن فضا حاکم دانست. پاسخ به این پرسش بی‌گمان به شناخت دقیق این فضا و وقایع رخ‌داده در آن نیاز دارد، لیکن می‌توان با تقسیم این فضا و مقایسهٔ آن با فضای واقعی به این پرسش، پاسخی نه فلسفی، بلکه واقع‌گرایانه داد. در فضای واقعی جرم با وجود بزهکار، آماج و فضای ارتکاب محقق می‌شود و همین سه جزء در فضای مجازی نیز وجود دارد؛ لیکن اشتراک و تمایزات آن حائز اهمیت است. در هر دو فضا مرتکب بی‌شک یک شخص انسانی است و این وجه اشتراک است و فضای ارتکابی وجه ممیزهٔ این دو است. لیکن نسبت به عنصر سیبل و آماج، دو امر متصور است؛ گاه سیبل جرم سامانه و داده است و گاه سامانه و داده وسیلهٔ ارتکاب است. در حوزهٔ دوم چون فضای مجازی و سامانه و داده وسیله محسوب می‌شود، اعمال قواعد حاکم بر فضای واقعی بر آن بلامانع است، لیکن در حوزهٔ نخست قاعدتاً جعل ضوابط خاص اجتناب‌ناپذیر است، مگر آنکه بتوان با مقایسهٔ این دو، به این نتیجه رسید که اعمال ضوابط عام بر این فضا ممکن است و بدین‌وسیله از توسعهٔ حقوق کیفری ممانعت به‌عمل آورد.

هنگامی‌که از دفاعیات بحث می‌شود، به‌طور مشخص بزهکار و بزه‌دیدهٔ انسانی در دو سوی آن قرار می‌گیرد. ازاین‌رو تحلیل در خصوص اینکه حکم دفاعیات مانند دفاع مشروع که برای جرائم سنتی وضع شده، با توجه به سیاق عبارات قانون، برای جرائم رایانه‌ای قابل اعمال است، ضروری است. به‌نظر می‌رسد به سه دلیل می‌توان معتقد بود که با توجه به الفاظ قانون، دفاع مشروع در مورد جرائم رایانه‌ای نیز اعمال‌شدنی است. دلیل نخست از منظر هرمنوتیکی است. هرمنوتیک را طبق تعریف «هنر تفسیر متن» بیان کرده‌اند (بخشی، ۱۳۹۵: ۲۲). از نظر نحلهٔ فکری سه گرایش تفسیر متن‌محور، مؤلفمحور و مفسرمحور در هرمنوتیک وجود دارد. فارغ از اختلاف این سه نحله، دو گرایش اصلی هرمنوتیک خاص و عام نیز قابل بحث است. در هرمنوتیک خاص نظر بر آن است که هر دانش، ضوابط خاص خود را برای تفسیر دارد و این همان گرایشی است که متن حاضر

پیرو آن است، زیرا نمی‌توان همان‌گونه‌که یک تابلوی نقاشی یا فیلم سینمایی[۱] تفسیر می‌شود، یک متن حقوقی را تفسیر کرد و حتی میان متون نیز تفاوت وجود دارد (اشمیث، ۱۳۹۵: ۲۲). درحالی‌که تفسیر متون مقدس مانند قرآن و سنت، گرایش به سمت احراز نظر مؤلف دارد، متون حقوقی بنابر هدف خود، بدانسبب وضع شده‌اند که به هدفی مانند رعایت حقوق شخص یا اشخاص یا نظم اجتماعی نائل شوند. ازاین‌رو تفسیر متن حقوقی در راستای این هدف صورت می‌گیرد. در این زمینه نمی‌توان به نظر مؤلف تأکید ورزید، زیرا ممکن است در زمان وضع قانون چنین پدیده‌ای از اساس وجود نداشته و به همین سبب در ذهن مؤلف (مقنن) نیز این موضوع اساساً نبوده است، ولیکن اکنون متن قابلیت آن را دارا باشد که چنین مواردی را در راستای هدف کلی حقوق در برگیرد. ازاین‌رو مانعی برای ورود آن نیست، چنانکه مصادیق «بیماری‌های مقاربتی»، «دستگاه‌های مخابراتی» و »وزارتخانه» در طول زمان تغییر کرده است؛ لیکن هیچ مفسری وزارتخانه‌ای را که در سال‌های اخیر ایجاد شده است، از شمول قوانین سابق بر آن به‌دلیل احراز نظر مقنن در زمان جعل قانون، خارج نمی‌داند. در خصوص دفاع مشروع نیز اگرچه در زمان تصویب، نظر مقنن بی‌گمان بر فضای سایبر نبوده، لیکن به‌نظر می‌رسد در این خصوص واژگان به‌کاررفته در دفاع مشروع مانند حمله، دفاع، مشروع مواردی است که قابل انطباق با فضای سایبری نیز است و به همین سبب آن را در مورد فضای سایبر می‌توان اعمال کرد و در واقع، مصداق آن را منحصر به فضای واقعی ندانست و با ظهور مصادیق جدید در شمول ماده دانست.

دلیل دوم، نحله‌های تفسیری در حقوق است. به‌طور سنتی، دو نحلهٔ تفسیری در حقوق وجود دارد که یکی بر زبان متعارف[۲] در تفسیر متون اصرار می‌کند و دیگری بر تعریف تخصصی واژگان حقوقی[۳] در جایی که تعریف تخصصی از واژه‌ای به‌عمل نیامده است، تنها تفسیر آن است که عرف از واژگان چه درمی‌یابد. در دفاع مشروع با هر دو رویکرد مواجهیم؛ از یک طرف، واژگانی مانند ضرورت را در معنای نبود راهی غیر از ارتکاب جرم تعریف کرده است (بند الف مادهٔ ۱۵۶ق.م.ا) و از طرفی واژگانی مانند دفاع و حمله تعریف شده است. ازاین‌رو این واژگان با مراجعه به عرف تفسیر می‌شوند. با مراجعه به عرف حمله را می‌توان هرگونه تجاوز من غیرحق دانست. در این مورد عرف بین کسی که با میله‌ای درصدد کوبیدن به یک باک اتومبیل است تا آن را منفجر کند و کسی که با دستکاری در رایانهٔ اتومبیل درصدد انفجار آن است، تفاوت معنادار قائل نمی‌شود. به همین سبب با مراجعه به تعریف عرفی واژگان به‌کاررفته در دفاع مشروع این واژگان قابل تأویل به فضای مجازی نیز است.

---

۱. در هرمنوتیک معنای عامی از متن وجود دارد و هر چیز قابل تفسیر می تواند موضوع آن قرار گیرد (بخشی، ۱۳۹۵: ۳۶-۳۵).

2. Common sense approach

3. Analytical approach

دلیل سوم را می‌توان با رویکرد تحلیل زبانی تفسیر کرد. طبق نظر «گفتار-کنش» جی ال آستین[1] تحلیل یک گزاره با این پرسش آغاز می‌شود: «اگر کسی این را بگوید چه عملی انجام می‌دهد و این سخن در چه شرایطی عملاً به‌کار گرفته می‌شود؟ وی بر این عقیده بود اگر هیچ شرایط قابل تصوری نباشد که در آن، گزاره را بتوان به‌کار گرفت، گزارهٔ مزبور هیچ معنایی ندارد» (مگی، ۱۳۹۷: ۲۰۷). این رویکرد خود سبب ایجاد تفسیر کاربردی، در حقوق شد. طبق این تفسیر باید به متن مفهومی را داد که امکان می‌دهد وظیفه‌ای را که برایش مقرر شده راست، انجام دهد (تروپه، ۱۳۹۰: ۱۳۴). در پرتو این تحلیل زبانی می‌توان گفت واژگان دفاع مشروع با توجه به تفسیر کاربردی به مفسر این اجازه را می‌دهد که این دفاع هرچند با نگرش سنتی تدوین شده است، نسبت به فضای سایبر اعمال شود.

۲. امکان توجیه دفاع مشروع نسبت به حملات سایبری با معیارهای سنتی

استمرار مشروعیت یک حکومت، در بعد تقنینی، مستلزم آن است که بتواند عملکرد خود را توجیه کند. به‌عبارتی، دولت باید قادر باشد، توجیه مناسبی برای هر مقررهٔ قانونی داشته باشد. بنابراین، هنگامی‌که از دفاع مشروع بحث می‌شود، این قاعده بر آن نیز قابل اعمال است. به همین سبب، به‌طور سنتی توجیهات متفاوتی برای دفاع مشروع براساس گرایش‌های متفاوتی فکری بیان شده است. برای مثال، حقوق طبیعی‌گرایانی مانند آگوئیناس، دفاع مشروع را حق طبیعی فرد دانسته‌اند. هگل، حمله را نفی حق و دفاع را نفی این اجبار دانسته و آن را توجیه کرده است (هگل، ۱۳۷۸: ۱۲۶). لاک و پیروان قرارداد اجتماعی معتقدند افراد حق برخورد با یکدیگر را در زمانی‌که به آنها صدمه‌ای وارد آید، طی قرارداد اجتماعی به دولت منتقل کرده‌اند و دولت موظف به دفاع از شهروندان شده است (لاک، ۱۳۸۷: ۱۷۸)، لیکن در موارد فوری که دولت حاضر نیست مانند دفاع مشروع حق اولیه به فرد بازگردد، وی می‌تواند از خویشتن دفاع کند. اگر هریک از این مبانی پذیرفته شود، می‌توان دفاع مشروع را توجیه‌شدنی دانست. لیکن پرسش اساسی در این بند آن است که این مبانی با توجه به حملهٔ فیزیکی و دنیای واقعی، بیان شده‌اند، آیا می‌توان از آنها برای توجیه حق دفاع مشروع در فضای سایبر بهره برد.

برای پاسخ توجه به موضوع دفاع مشروع ضروری می‌نماید. دو رویکرد می‌توان در خصوص موضوع دفاع مشروع در حملات سایبری اتخاذ کرد؛ رویکرد اول آن است که کانون توجه، بر نتایج ناشی از حملات سایبری در فضای سایبری متمرکز شود، در این صورت با توجه به آنکه موضوع حملات سایبری سامانه‌های رایانه‌ای و داده‌های ذخیره‌شده در درون آن است، حملات

1. H. R. Austin

سایبری تنها دو عنوان «مال» و «عِرض» را مورد تعرض قرار می‌دهند، زیرا از یک سو، برای تعریف مال[۱] لازم است از عرف استمداد جست و عرف به‌تدریج بر معنای مال افزوده و امروزه با توجه به گسترش روزافزون نقش فضای مجازی و گسترش کاربران آن، سامانه‌های رایانه‌ای و داده‌های ذخیره‌شده در درون آن مال محسوب می‌شوند. همچنین باید در نظر داشت داده‌های رایانه‌ای به لحاظ دارا بودن ارزش اقتصادی، منفعت مشروع، برآوردن نیاز و پرداخت پول در برابر آن بی‌تردید مال محسوب می‌شوند و تعرض به آنان بدون شک موجب تعرض یا در معرض تلف قرار گرفتن مال دیگری می‌شود و از سوی دیگر، از آنجا که آبرو و حیثیت لازمهٔ حیات اجتماعی افراد است و در صورت تعرض به آن باید اهرم و توانایی برای دفع آن از سوی قانونگذار در اختیار شهروندان قرار گیرد، لازم است علاوه‌بر مال، عرض[۲] را هم به‌عنوان موضوعی که ممکن است توسط حملات سایبری مورد تعرض قرار گیرد، در نظر گرفت، چراکه ممکن است یک حملهٔ سایبری به سرقت داده‌ها و اطلاعات شخصی و خانوادگی ذخیره‌شده در سامانه‌های رایانه‌ای کاربران منجر شودورویکرد دوم آن است که علاوه‌بر نتایج ناشی از حملات سایبری در فضای سایبر، نتایج ناشی از حملات سایبری در فضای سنتی را نیز مورد توجه قرار داد. در این صورت موضوع حملات سایبری علاوه‌بر دو عنوان «مال» و«عرض» دو عنوان دیگر یعنی «نفس» و «آزادی تن» را هم در برمی‌گیرد، زیرا از یک سو ممکن است حملات سایبری علیه سامانه‌های رایانه‌ای کنترلی (پی ال سی)[۳]، صنعتی، خدماتی یا نظامی به‌نحوی ارتکاب یابد که اخلال در عملکرد آنان به انفجار در آن مکان منجر شود و جان بسیاری از افراد حاضر در مکان را بستاند. همچنین ممکن است اخلال در عملکرد سامانه‌های رایانه‌ای کنترلی سبب شود ابزارهایی که تحت آن در حال کارند، از عملکرد متعارف خود خارج شده و جان افرادی را که با آن ابزار مشغول به کار هستند، به مخاطره اندازد. از سوی دیگر، این امکان وجود دارد که عملکرد درهای خروجی یک مکان وابسته به سامانه‌های رایانه‌ای کنترلی باشد که این امر در صورت وقوع حملات سایبری به آن سامانه‌های رایانه‌ای به اخلال در عملکرد آنان و متعاقب آن بسته شدن تمامی درهای خروجی منجر شود و مانع از خروج افراد شده و آنان مدتی در آن مکان حبس شوند. به‌نظر می‌رسد علاوه‌بر نتایج ناشی از حملات سایبری که در فضای سایبر ارتکاب می‌یابند، ضروری است از نتایج و آثار زیانباری که ممکن

---

۱. «آنچه در ملک کسی باشد و آنچه ارزش مبادله داشته باشد، دارایی، خواسته و ...». ر.ک: فرهنگ فارسی معین، ج ۳: ۳۰۷۸.

۲. عرض در لغت به معنای آبرو، اعتبار و حیثیت آورده شده است و معنای متفاوت از ناموس دارد و نبایست این دو واژه را مترداف انگاشت. در به‌کارگیری الفاظ اصل بر تأسیس است و نه توصیف، بنابراین منظور از عرض مفهومی گسترده‌تر است و هر ارزشی را که مرتبط با حیثیت و آبروی افراد باشد، شامل می‌شود. ر.ک: الهام و برهانی، ۱۳۹۵، ج ۱: ۱۶۵.

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

است توسط حملات سایبری در فضای سنتی علیه «نفس» و «آزادی تن» افراد ارتکاب یابد، غافل نبود و در نتیجه با اتخاذ رویکرد دوم، تمسک به دفاع مشروع را در مقابل حملات سایبری از منظر قانونی توجیه‌پذیر دانست. بر این اساس، از آنجا که موضوع حملهٔ هریک از ارزش‌های چهارگانهٔ نفس، مال، عرض یا ناموس است، می‌توان آن را به مصداق دفاع مشروع سنتی توجیه کرد، زیرا توجیهات سنتی دفاع مشروع، اعم از آنکه حق نفی حمله، دفاع به‌عنوان حق طبیعی، زوال حق مهاجم پس از حمله، قرارداد اجتماعی، نظم اجتماعی یا این موارد باشد، همگی بر اصل وجود حق دفاع برای شخص حقیقی مدافع تمرکز دارند و نه فضایی که در آن این حمله روی می‌دهد. به‌عبارتی، شناخت این حق در هریک از این توجیهات منوط به وجود فضای واقعی نشده است، بلکه منوط به خدشه به حق یک شخص در مواردی شده است که دسترسی به نیروهای دولتی وجود ندارد. بنابراین، می‌توان هریک از مبانی را که در خصوص دفاع مشروع سنتی وجود دارد، در این مورد اعمال کرد.

۳. تحلیل شرایط دفاع مشروع سنتی بر دفاع مشروع در برابر حملات سایبری

پس از تحلیل و بررسی امکان توسل به دفاع مشروع در مقابل حملات سایبری از منظر مبنایی و قانونی، در این قسمت با توجه به مادهٔ ۱۵۶ قانون مجازات اسلامی ۱۳۹۲ در پنج بند، به تحلیل مفهوم حملهٔ سایبری و تطبیق آن با حملهٔ غیرسایبری مذکور در دفاع مشروع، مهاجم در حملات سایبری، شرایط تجاوز و خطر در مقابل حملات سایبری، مدافع در حملات سایبری و شرایط دفاع در مقابل حملات سایبری می‌پردازیم. دفاع مشروع در حملات سایبری به معنای آن است که چنانچه کاربری از طریق سامانهٔ رایانه‌ای تمامیت سامانهٔ رایانه‌ای دیگری را مورد تعرض قرار داد و به اصطلاح به آن حملهٔ سایبری کرد، کاربر مقابل، از لحاظ قانونی حق دفاع از خود را دارد و اگر مرتکب رفتار مجرمانه شود، در صورت تحقق شرایط لازم، عمل وی فاقد عنوان مجرمانه و مسئولیت کیفری است.

۴. مفهوم حمله سایبری و تطبیق آن با حملهٔ غیرسایبری مذکور در دفاع مشروع

در راستای مفهوم حملهٔ سایبری باید گفت بیش از یک دهه است که تحلیلگران دربارهٔ پیامدهای بالقوهٔ حملات سایبری گمانه‌زنی‌هایی داشته‌اند، به‌گونه‌ای که اغلب نوشته‌ها در تعریف حملهٔ سایبری، همگی بر وارد کردن ضربهٔ اقتصادی یا فیزیکی گسترده بر اثر حملات سایبری تأکید دارند، اما بدیهی است تا زمانی‌که دولت‌ها تعریف واحدی از حملات سایبری به رسمیت نشناسند، علاوه‌بر آنکه کارشناسان و تحلیلگران نخواهند توانست خط‌مشی‌ها و توصیه‌های سیاسی و قانونی

هماهنگی را در خصوص حملات ارائه دهند، دیگر اقدامات چندجانبهٔ دولت‌ها برای مقابله با تهدیدهای رو به رشد ناشی از حملات سایبری بسیار دشوار خواهد بود.

مهم‌ترین چالش در تعریف حملهٔ سایبری فقدان معیار یا معیارهایی به‌منظور تمییز آن با سایر مفاهیم مجرمانه مشابه مانند جرائم سایبری، تروریسم سایبری و ... است. برای مثال در خصوص تعریف حملات سایبری بیان شده است: حملات سایبری، اقداماتی است که از یک سامانهٔ رایانه‌ای علیه یک سامانه‌ای رایانه‌ای یا یک شبکهٔ رایانه‌ای یا یک وب‌سایت به‌نحوی ارتکاب می‌یابد که محرمانگی، تمامیت و قابلیت دسترسی سامانهٔ رایانه‌ای و اطلاعات ذخیره‌شده در آن را به مخاطره می‌اندازد (Marshall & Saulawa, 2015: 3). «حملات سایبری مجموعه اقداماتی می‌باشند که توسط یک دولت به‌منظور نفوذ یا ایجاد اخلال در سامانه‌های رایانه‌ای یا شبکهٔ رایانه‌ای، علیه دولت دیگر ارتکاب می‌یابد» (خلیل‌زاده، ۱۳۹۳: ۲۶). حملات سایبری به معنای «ایجاد اخلال در صحت یا درستی داده‌ها که معمولاً از طریق اعمال کد مخرب و تغییر در منطق برنامه‌ها و کنترل داده‌ها صورت می‌گیرد و به خروجی اشتباه توسط سامانه‌های رایانه‌ای منجر می‌گردد» (جالینوسی و همکاران، ۱۳۹۲: ۱۰). یک حمله سایبری شامل چهار حوزه‌ی از دست دادن تمامیت، از دست دادن قابلیت دسترسی، از دست دادن محرمانگی داده و اطلاعات و در نهایت تخریب فیزیکی سامانه‌های رایانه‌ای است (Training & Command, 2005: 1-3). در نقد تعاریف مذکور می‌توان گفت از آنجا که که تنها کانون توجه خود را بر نتایج ناشی از حملات سایبری متمرکز می‌کنند، چنین امری سبب می‌شود مرز میان حملات سایبری با جرائم رایانه‌ای به‌ویژه جرائم رایانه‌ای موضوع محور مشخص نباشد. سازمان همکاری شانگهای به‌عنوان یک نهاد بین‌المللی حملات سایبری این‌گونه تعریف کرده است: «روشی روان‌شناسی ـ روان‌شناختی [برای] شست‌وشوی مغزی جهت بی‌ثباتی جامعه و دولت و نیز وادار ساختن دولت برای تصمیم‌گیری در جهت منافع طرف مخالف یا دشمن» (Hathaway *et al.*, 2012: 865). علاوه‌بر این، سازمان مذکور انتشار اطلاعاتی را که به ضرر نظام‌های سیاسی، اجتماعی، اقتصادی، همچنین در زمینه‌های مذهبی، اخلاقی و فرهنگی سایر کشورهاست، به‌عنوان یکی از تهدیدات اصلی علیه امنیت اطلاعات معرفی کرده است (Hathaway *et al.*, 2012: 825). در نقد این تعریف نیز می‌توان گفت کماکان مرز میان حملات سایبری با سایر عملیات مجرمانه مانند جاسوسی رایانه‌ای که عنوان مجرمانه‌ای در جهت جلوگیری از انتشارات اطلاعات محرمانه است و همچنین تروریسم سایبری مشخص نیست.

شایسته آن است عنوان مجرمانهٔ حملهٔ سایبری در زمرهٔ عناوین مجرمانه‌ای همچون نسل‌کشی، جرائم علیه بشریت، جرائم جنگی قرار گیرد که در آنان یک رفتار واحد، محقق جرم نیست، بلکه این عناوین بر دسته‌ای از جرائم با رفتارهای مجرمانهٔ متفاوت با شرایط اختصاصی حمل می‌شوند.

بنابراین نسبت به حملات سایبری به یک جرم‌انگاری مستقل نیاز است تا قانونگذار با پیش‌بینی شرایط اختصاصی، جرائم سایبری موضوع- محوری که در زیر فضای سایبری میان سامانه‌های رایانه‌ای با یکدیگر ارتکاب می‌یابند، به‌عنوان رفتار حملات سایبری پیش‌بینی کرده و با آنان برخورد شدیدتری کند. بدین‌منظور می‌توان گفت حملات سایبری به اعمالی اطلاق می‌شود که به‌وسیلهٔ سامانهٔ رایانه‌ای به قصد تضعیف تمام یا بخشی اعظمی از سامانه‌های رایانه‌ای متعلق به یک گروه خاص اعم از کاربران اینترنتی، سازمان‌ها، نهادها و غیره ارتکاب می‌یابد (مرسی، ۱۳۹۷: ۱۲۴-۱۲۲). بنابراین یک حملهٔ سایبری شامل هریک از اعمال مشروحهٔ زیر است که به قصد تضعیف تمام یا بخش اعظمی از سامانه‌های رایانه‌ای متعلق به یک گروه خاص از حیث همین عناوین ارتکاب یابد:

۱. اخلال در سامانه‌های رایانه‌ای؛

۲. تخریب داده‌های ذخیره‌شده در سامانه‌های رایانه‌ای؛

۳. تغییر در داده‌های ذخیره‌شده در سامانه‌های رایانه‌ای؛

۴. ممانعت از دسترسی به سامانه‌های رایانه‌ای و داده‌های ذخیره‌شده در آنها؛

۵. رونوشت یا برش (cut) از داده‌های ذخیره‌شده در سامانه‌های رایانه‌ای که متعلق به یک گروه خاصاند. گروه خاص در تعریف مذکور اعم از کاربران اینترنتی، سازمان‌ها، نهادها و ... است (مرسی، ۱۳۹۷: ۱۲۴-۱۲۲).

مطابق با تعریف مذکور از حملات سایبری می‌توان مصادیق عنصر مادی حملات سایبری را تحت عناوین جرائم علیه محرمانگی، صحت، تمامیت و دسترس‌پذیری سامانه‌های رایانه‌ای و داده‌های ذخیره‌شده در درون آن قرار داد. همان‌گونه که در تعریف مذکور معلوم است، حملهٔ سایبری مفهومی ناظر بر جرم خاص نیست، بلکه شامل مجموعه‌ای از اعمال مجرمانه است که معمولاً در سطحی وسیع و گسترده به قصد تضعیف عملکرد تمام یا بخش اعظمی از شبکه‌های رایانه‌ای متعلق به یک گروه خاص انجام می‌پذیرد.

در خصوص عنصر معنوی حملات سایبری می‌توان گفت که حملهٔ سایبری عملیات مجرمانهٔ سایبری است که به قصد تضعیف عملکرد تمام یا بخش اعظمی از شبکه‌های رایانه‌ای متعلق به یک گروه خاص صورت می‌گیرد. بنابراین هدف مستقیم در حملات سایبری سامانه‌های رایانه‌ای متعلق به یک گروه خاص است نه صرف سامانهٔ رایانه‌ای. چنین امری وجه تمایز مفهوم حملات سایبری با جرائم رایانه‌ای به‌ویژه جرائم رایانه‌ای موضوعمحور می‌شود. بنابراین اعمالی که جزء مصادیق حملات سایبری تلقی می‌شوند، در عناوین خاص خود، چون سرقت رایانه‌ای، تخریب داده، اخلال در سامانه‌های رایانه‌ای و ... در قوانین سایر کشورها جرم شناخته شده‌اند، اما باید در

نظر داشت هدف از جرم‌انگاری حملات سایبری به‌عنوان یکی از مهم‌ترین عملیات مجرمانهٔ سایبری حمایت از سامانه‌های رایانه‌های فردی نیست. ازاین‌رو اگر اعمال ارتکابی بدون توجه به تعلق سامانه یا سامانه‌های رایانه‌ای قربانی به گروه خاص یا بدون قصد تضعیف عملکرد سامانه رایانه‌ای موجود در شبکه‌های رایانه‌ای متعلق به یک گروه خاص انجام گیرد، مرتکب فقط به‌عنوان جرمی عادی تحت تعقیب قرار می‌گیرد (مرسی، ۱۳۹۷: ۱۲۴-۱۲۲). بهدلیل تداخل مصادیق حملات سایبری در جرائم رایانه‌ای، مقاله به بررسی امکان دفاع مشروع به همین عناوین خرد پرداخته است که در صورت وقوع یک حمله، در شرایط فعلی بتوان در برابر آن دفاع کرد.

۵. مهاجم در حملات سایبری

توصیف کلی مهاجمان سایبری امری بسیار دشوار است، زیرا زمان زیادی از شکل‌گیری این عرصه نمی‌گذرد، اما می‌توان گفت اغلب افرادی که مهاجمان سایبری را تشکیل می‌دهند، هکرها هستند. هکرها با تجزیه‌وتحلیل داده‌ها و سامانه‌های رایانه‌ای و آشنایی با نحوهٔ عملکرد آنان و به‌کارگیری دانش فناوری و اطلاعات در ساخت برنامه‌ها و نرم‌افزارهای جدید رایانه‌ای اقداماتی علیه محرمانگی، صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای در فضای سایبر به منصهٔ ظهور می‌رسانند.

قانونگذار ایران در مادهٔ ۱۵۶ قانون مجازات اسلامی ۱۳۹۲ و مواد دیگر مرتبط با دفاع مشروع، به‌طور خاص مشخص نکرده است که مهاجم در دفاع مشروع باید دارای چه ماهیتی باشد. با این حال در برابر این سکوت قانونی، تفسیرهایی را که می‌توان ارائه کرد، از سه تفسیر خارج نیستند.

تفسیر اول، با توجه به عبارت «در برابر هرگونه تجاوز یا خطر فعلی یا قریب‌الوقوع» در مادهٔ ۱۵۶ ق.م.ا و همچنین با توجه به آنکه عبارت «هر گونه تجاوز» عام محسوب می‌شود و در عام شمولیت نسبت به همهٔ مصادیق است، این نظر را مطرح می‌کند که تجاوز یا خطر می‌تواند از سوی هر نوع مهاجم با هر ماهیتی ایجاد شود و منحصر در ماهیت خاصی نیست. به‌طور مثال مهاجم می‌تواند انسان، حیوان یا هر عامل غیرانسانی یا طبیعی باشد.

تفسیر دوم، با توجه به سیاق عبارت نگارش‌شده در مادهٔ ۱۵۷ ق.م.ا مبنی بر «مقاومت در برابر قوای انتظامی و دیگر ضابطان دادگستری» به‌عنوان نوعِ خاصی از دفاع، شاید چنین به ذهن متبادر شود که مهاجم در دفاع مشروع همواره یک عامل انسانی است.

تفسیر سوم. با توجه به برخی از مواد دیگر قانونی می‌توان قائل بر این نظر بود که مهاجم علاوه‌بر آنکه می‌تواند انسان باشد، حیوان را نیز شامل می‌شود. با استناد به مادهٔ ۳۳۰ قانون مدنی که بیان می‌دارد: «اگر کسی حیوان متعلق به غیر را بدون اذن صاحب آن بکشد باید تفاوت قیمت

زنده و کشته آن را بدهد ولیکن اگر برای دفاع از نفس بکشد یا ناقص کند ضامن نیست»، می‌توان گفت که مهاجم علاوه‌بر انسان، حیوان را نیز شامل می‌شود. با توجه بر این نظر، فقط به‌دلیل وجود نص قانونی «انسان» و «حیوان» داخل در شمول مهاجم قرار می‌گیرد و سایر عوامل برای مثال عوامل طبیعی و آسمانی از تعریف مهاجم خارج می‌شود، زیرا باید به حدود نص اکتفا و بسنده کرد و در صورت فقدان نص، موضوع را از شمول تعریف خارج دانست. همچنین باید در نظر داشت عوامل موجههٔ جرم نیز به‌دلیل آنکه استثنا هستند و عنصر قانونی جرم را زایل می‌کنند، باید تفسیر مضیق شوند.

در حملات سایبری با توجه به آنکه هکرها توان حمله از طریق یک سامانهٔ رایانه‌ای به دیگر سامانهٔ رایانه‌ای را دارند، باید اذعان داشت مهاجم در موضوع دفاع مشروع در مقابل حملات سایبری تنها می‌تواند انسان باشد و فروض دیگر مهاجم اگرچه به لحاظ مبنایی در دفاع مشروع سنتی امکان‌پذیر است، به‌دلیل عدم امکان تحقق در حملات سایبری خروج تخصصی از موضوع دارد. بنابراین در حملات سایبری، مهاجم تنها ماهیت انسانی دارد. همچنین باید در نظر داشت است از آنجا که حملات سایبری در بستر فضای سایبر و از فواصل دور ارتکاب می‌یابند، این امر سبب عدم مواجههٔ حضوری میان مهاجم و مدافع به آن معنا که در دفاع مشروع سنتی موردنظر است، می‌شود. علاوه‌بر آن از آنجا که فضای سایبر به‌عنوان بستر حملات سایبری از لحاظ ساختاری به‌گونه‌ای نامتمرکز است، این توانایی و قابلیت را برای مهاجمان سایبری فراهم کرده است، بدون آنکه اثر یا نامی از خود باقی بر جای گذارند حملات سایبری خود را متوجه اهداف خود کنند (Lord & Sharp, 2011: 20-28). در نتیجه اساساً مدافع، علم و آگاهی دربارهٔ ویژگی‌های مهاجم ندارد و اطلاعی ندارد که آیا مهاجم مجنون است یا عاقل؛ کبیر است یا صغیر؟ بنابراین، تفکیکی که در دفاع مشروع سنتی بین حملهٔ صغیر و مجنون و اشخاص بالغ و مختار بیان شده است، در حملات سایبری شایان توجه نیست، زیرا مواجههٔ حضوری در این حملات وجود ندارد.

امروزه فضای سایبر این امکان را برای سازمان‌ها، نهادها، شرکت‌ها و مؤسسات فراهم کرده است که آنان برای تأثیرگذاری در عملکرد یکدیگر، دسترسی به اسناد و اطلاعاتی ذخیره‌شده یکدیگر در فضای سایبر و افشای آنان، آشکار کردن ضعف‌های امنیتی یکدیگر در فضای سایبر و متعاقب آنان بی‌اعتمادی شهروندان به شرکت‌ها و مؤسسات و همچنین گاهی برای حذف رقبای خود از بازار تجارت متوسل به حملات سایبری شوند. سؤالی که ممکن است مطرح شود آن است آیا اشخاص حقوقی در فضای سایبر می‌توانند مهاجم واقع شوند یا خیر؟ به نظر پاسخ منفی است. همواره رفتارهایی مانند حمله، توسط شخص حقیقی ارتکاب می‌یابد و شخص حقوقی تنها با شرایطی می‌تواند مسئولیت یابد. بنابراین، در دفاع مشروع شخص حقوقی هیچ‌گاه نمی‌توانند

مهاجم باشد، لیکن درصورتی‌که نمایندهٔ قانونی (شخص حقیقی) در راستای منافع و به نام آن شخص طبق مادهٔ ۷۴۷ قانون مجازات اسلامی اقدام کند، شخص حقوقی مسئولیت می‌یابد و درصورتی‌که در مقام دفاع صدمه‌ای به شخص حقوقی وارد شود، مانند آنکه به سامانه‌های این شرکت در نتیجهٔ دفاع صدمه وارد شود، این خسارت قابل مطالبه نیست.

۶. شرایط تجاوز و خطر در مقابل حملات سایبری

شرط ابتدایی و بدوی برای تحقق دفاع مشروع، آن است که تجاوز یا خطر فعلی یا قریب‌الوقوع باشد. نادیده‌گیری این شرط موجب می‌شود، دفاع مشروع موضوعیت نداشته و اساساً قابل تحقق ناشد.

از آنجا که حملات سایبری علیه سامانه‌های رایانه‌ای و داده‌های ذخیره‌شده در آن ارتکاب می‌یابد، تشخیص خطر فعلی یا قریب‌الوقوع امری تخصصی و فنی است که لازم است با جلب نظر کارشناسان فنی موارد خطر فعلی و قریب‌الوقوع در حملات سایبری تعیین و به‌صورت احصاشده بیان شوند. برای مثال به‌نظر می‌رسد صرف نفوذ به سامانهٔ رایانه‌ای می‌تواند به‌عنوان یکی از مصادیق خطر فعلی یا قریب‌الوقوع در فضای سایبر مطرح شود، زیرا یک حملهٔ سایبری از چندین مرحلهٔ جمع‌آوری اطلاعات، تعیین نقاط ضعف، نفوذ و در نهایت حمله تشکیل می‌شود. چراکه هر عملیاتی، چه فیزیکی و چه سایبری لازم است ابتدا با چشمانی کاملاً باز انجام گیرد، زیرا اجرای حملات سایبری بدون اطلاعات و آگاهی کافی از هدف، مانند بمباران مکانی است که از مسکونی یا نظامی بودن آن مطلع نیستیم و بدون اطلاعات و آگاهی کافی از هدف فقط نیروها و منابع خود را از دست می‌دهیم و احتمال ردیابی و شناسایی خود را برای دشمن افزایش خواهیم داد. پس از آنکه اطلاعات مهاجم دربارهٔ ماهیت سایبری هدف خود کامل شد، مرحلهٔ تعیین نقاط ضعف آغاز می‌شود. این مرحله از کار به‌واقع ساده‌ترین مرحلهٔ حملهٔ سایبری است، زیرا دانستن مشخصات هدف، تعیین عیوب سخت‌افزاری و نرم‌افزاری چندان دشوار نبوده و فقط زمان لازم است. پس از تعیین ضعف‌ها و با در نظر گرفتن اطلاعات به‌دست‌آمده و با آگاهی از سازوکارهای ردیابی، حملات سایبری در جهت نفوذ به هدف پیش می‌رود. پس از تحقق مرحلهٔ نفوذ تنها کافی است تیک‌تاک عقربه‌های ساعت را دنبال کرد تا اقداماتی مانند اخلال، تخریب و ... علیه تمامیت داده‌ها و سامانه‌های رایانه‌ای آغاز شود، بنابراین می‌توان مرحلهٔ نفوذ را به‌عنوان خطر قریب‌الوقوع و بالفعل در برابر حملات سایبری در نظر گرفت.[۱]

---

۱. شایان ذکر است در اسناد بین‌المللی مطابق مادهٔ ۲ کنوانسیون بوداپست «هریک از اعضا باید به‌گونه‌ای اقدام بـه وضـع قـوانین و سایر تدابیر کنند که در صورت لزوم براساس حقوق داخلی خود، دسترسی عمدی بدون حق بـه تمـام یـا بخـشی از یـک سیـستم

پرسشی که ممکن است در این قسمت مطرح شود آن است که وجود خطر یا تجاوز در عالم خارج ملاک است یا در ذهن مهاجم؟ پاسخ به این پرسش بازگشت به این امر دارد که در حقیقت دفاع از چه زمانی آغاز می‌شود؟ آیا آغاز دفاع مربوط به زمانی است که مدافع باور دارد مورد حمله قرار گرفته یا زمانی ملاک است که حمله به‌صورت عینی رخ داده باشد؟

حقوقدانان میان این صور مختلف تفکیک قائل شده‌اند، بدین‌نحو که هنگامی‌که خطر و تجاوز در عالم واقع وجود دارد، دفاع مشروع، دفاع واقعی تلقی می‌شود، در مقابل زمانی‌که مدافع به‌طور معقول باور دارد که مورد حمله قرار گرفته است، درحالی‌که در عالم واقع چنین نیست و مدافع از نیروی دفاعی علیه کسی استفاده می‌کند که در حقیقت مهاجم نیست، در اصطلاح دفاع مشروع «ظاهری» نامیده می‌شود (Fletcher, 1985: 972).

به‌عبارت دیگر می‌توان گفت «هر گاه مدافع در ذهن و نظر خود تجاوز یا خطری را فعلی یا قریب‌الوقوع فرض نماید به‌نحوی که ذهنیت او با قرائن معقول و عقلایی همراه باشد، اقدام به ارتکاب رفتار مجرمانه‌ای نماید که در عالم واقع خطر، تجاوز و مهاجمی وجود نداشته است، مرتکب دفاع مشروع ظاهری شده است» (محمودی‌جانکی و صادقی، ۱۳۹۴: ۱۵۷). البته باید در نظر داشت هر گاه ملاک و شاخصهٔ تعیین، ذهنیت مدافع مدنظر قرار گیرد، لازم است میان دو وضعیت قائل به تفکیک شد. وضعیت اول آن است که ذهنیت مرتکب همراه با قرائن معقول باشد، وضعیت دوم آن است که وضعیت ذهنی مرتکب فاقد قرائن معقول باشد. با تفکیک مذکور شایسته است اقدام مدافع در وضعیت اول مورد حمایت قانون‌گذار قرار گیرد.[1]

در حملات سایبری نیز این احتمال وجود دارد که اعتقاد و باور صادقانهٔ ذهنی مرتکب بر وقوع یک حملهٔ سایبری باشد، درحالی‌که در عالم واقع اساساً چنین حمله‌ای وجود خارجی نداشته

رایانه‌ای را جرم‌انگاری کنند. اعضا می‌توانند مقرر دارند این جرم با نقض تدابیر امنیتی و به قصد تحصیل داده‌های رایانه‌ای یا سایر مقاصد ناروا یا نسبت به سیستم رایانه‌ای که با سیستم رایانه‌ای دیگری ارتباط دارد، محقق می‌شود». برای مطالعهٔ ترجمهٔ متن کنوانسیون و گزارش توجیهی آن ر.ک: جلالی فراهانی، ۱۳۹۵. در حقوق کیفری ایران مطابق مادهٔ ۷۲۹ قانون مجازات اسلامی (تعزیرات) «هر کس به‌طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به‌وسیلهٔ تدابیر امنیتی حفاظت‌شده است دسترسی یابد، به حبس از نودویک روز تا یک سال یا جزای نقدی از بیست میلیون (۲۰،۰۰۰،۰۰۰) ریال تا هشتاد میلیون (۸۰،۰۰۰،۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد». صرف دسترسی غیرمجاز در شرایطی جرم‌انگاری شده است.

۱. شایان ذکر است پذیرفتن دفاع مشروع ظاهری در این حالت نیز اختلاف نظرهایی به‌همراه دارد. به عقیدهٔ برخی حقوقدانان عینی‌گرا، اشتباه نمی‌تواند خطا بودن رفتار را تغییر دهد و آن را موجه سازد، در نهایت بتواند در میزان سرزنش‌پذیری فرد نقش داشته باشد و عامل رافع مسولیت محسوب شود، اما جزء علل موجههٔ قانونی نمی‌تواند شمرده شود. ر.ک:

Byrd, B. Sharon, Wrongdoing and Attribution: Implications beyond the JustificationExcuse Distinction, The Wayne Law Review, Vol. 33, No. 4, 1987, pp:1321_1322.

به عقیدهٔ برخی دیگر نیز مجازات عمل مجرمانهٔ دیگری بر اثر اشتباه هیچ‌گاه منفعت همگانی را تأمین نمی‌کند. معقول بودن قصد دفاع و اینکه اجتناب از آن موقعیت برای وی یا هر انسان دیگری ممکن نبوده است، موجب می‌شود تا مسولیت کیفری بر او بار نشود. ر.ک:.Fletcher1984: 17-18

باشد. همان‌طورکه بیان شد، صرف نفوذ به سامانهٔ رایانه‌ای به تعرضی علیه تمامیت و دسترس‌پذیری سامانه رایانه‌ای منجر نخواهد شد، لیکن می‌تواند مقدمه و منشأ سایر رفتارهای مجرمانه‌ای مخرب مانند تخریب داده، اخلال در عملکرد در سامانهٔ رایانه‌ای و ... باشد. نفوذ در سامانهٔ رایانه‌ای به‌ویژه در حملات سایبری که مهاجم سایبری سامانهٔ رایانه‌ای قربانی خود را در اختیار ندارد و لازم است برای اعمال هرگونه رفتار مخربی ابتدا به سامانهٔ رایانه‌ای قربانی نفوذ یابد، جزء لاینفک و قریب‌الوقوع برای حملات سایبری تلقی می‌شود. بنابراین، به‌نظر می‌رسد اقداماتی را که مدافع علیه سامانه‌های رایانه‌ای، هکرهای کلاه‌خاکستری[1]، هکرهای کلاه‌سفید[2] انجام می‌دهد، بتوان در قالب دفاع مشروع ظاهری توجیه‌پذیر دانست، زیرا اقدامات هکرهای کلاه خاکستری از آن حیث که کدهای ورود به سامانه‌های رایانه‌ای حفاظت‌شده را به‌دست می‌آورند و به داخل آنان نفوذ می‌کنند، همانند هکرهای سیاه تلقی می‌شوند و این امر سبب می‌شود که مدافع به باور و اعتقاد ذهنی صادقانه‌ای برسد که سامانهٔ رایانه‌ای مورد هجوم و تجاوز قرار گرفته است، این امر با توجه به آنکه در فضای سایبر میان مدافع و مهاجم مواجههٔ غیرحضوری است، دوچندان می‌شود و از آنجا که اقدامات هکرهای کلاه خاکستری همچنین کلاه سفید سبب تخریب داده‌ها یا اخلال در عملکرد سامانه‌های رایانه‌ای نمی‌شود، بلکه ممکن است با کشف یک مشکل در سامانه‌های رایانه‌ای آن را به مدیران مربوطه گزارش دهند تا برطرف سازند یا پیشنهاد همکاری برای حل این مشکل را به مدیران سامانه‌های رایانه‌ای دهند، اقدامات آنان همانند مصداق حملهٔ سایبری تلقی نمی‌شود که این مسئله سبب می‌شود باور و اعتقاد صادقانهٔ ذهنی مدافع با عالم خارج تطابق نداشته باشد. با توجه به مواجههٔ غیرحضوری میان مدافع و مهاجم شایسته است پذیرش دفاع مشروع ظاهری را با توجه به ذهنیت مدافع در برابر حملات سایبری قابل تحقق دانست.

یکی دیگر از شرایط تحقق دفاع مشروع آن است که تجاوز یا خطر غیرقانونی باشد. این ویژگی در عنوان تجاوز یا خطر به‌نوعی مستتر و قابل فهم است، زیرا زمانی‌که امری قانونی و در جهت اعمال حق ارتکاب یابد، شایسته نیست اصطلاح خطر و تجاوز را بر آن بار کرد. بنابراین زمانی‌که سامانه‌های رایانه‌ای مطابق با حکم قانون مورد حملهٔ سایبری قرار می‌گیرند، شرط خطر و تجاوز که شرط اصلی و ابتدایی استناد به دفاع مشروع است، مفقود است و نمی‌توان مرتکب دفاع در مقابل اقدامات قانونی شد. با این حال، از آنجا که حملات سایبری در بستر فضای سایبر ارتکاب می‌یابند و این امر سبب عدم مواجههٔ حضوری میان مهاجم و مدافع برخلاف دفاع مشروع سنتی می‌شود، در نتیجه اساساً مدافع علم و آگاهی نسبت به ویژگی‌های مهاجم ندارد، در نتیجه اطلاعی ندارد که مهاجم یک مقام ذی‌صلاح است که با حکم قانون و با رعایت شرایط تحقیقات

1. Gray Hat Hacker
2. White Hat Hacker

مقدماتی در جهت کشف جرم، نسبت به سامانهٔ رایانه و داده‌های ذخیره‌شده در آن به سامانهٔ رایانه‌ای نفوذ کرده است. به‌عبارت دیگر، می‌توان گفت در قوانین کیفری لازم است اقدامات مدافع در قالب دفاع مشروع توجیه شود، مگر آنکه قرینه‌ای وجود داشته باشد که مدافع با علم و آگاهی از ویژگی‌های مهاجم اقدام به دفاع کرده است. این امر در تبصرهٔ مادهٔ ۱۵۶ که بیان کرده مدافع تنها وظیفهٔ اثبات اصل دفاع را دارد و اثبات فقدان شرایط را بر عهدهٔ مهاجم گذارده است، تقویت می‌شود. برای مثال موردی که مقامات ذی‌صلاح با اطلاع قبلی به کاربر مبنی بر اینکه لازم است سامانهٔ رایانه‌ای او از راه دور تحت کنترل قرار گیرد، در این میان هر گاه کاربر برای رهایی از این کنترل اقدامات مجرمانه‌ای علیه سامانه‌های رایانه‌ای که وظیفهٔ آنان کنترل سامانهٔ رایانه‌ای او بوده است، مرتکب شود، اقدامات او از موضوع دفاع مشروع خارج است و نمی‌تواند در برابر این‌گونه اقدامات کنترلی که توسط مقامات ذی‌صلاح انجام می‌گیرد، متوسل به دفاع برای دفع تجاوز و خطر شود، زیرا دفع تجاوز یا خطر از حیث مبانی تنها زمانی مشروع است که حقوق فردی او به ناحق و غیرقانونی مورد تعرض قرار گرفته باشد.

فرع دیگری که لازم است در این قسمت بیان شود، آن است که هر گاه قوای انتظامی و دیگر ضابطان دادگستری از حدود وظیفهٔ خود خارج شوند و حسب ادله و قرائن موجود خوف آن باشد که عملیات سایبری آنان موجب تعرض به عرض یا مال افراد می‌شود، با توجه به مادهٔ ۱۵۷ ق.م.ا که مقرر می‌دارد: «مقاومت در برابر قوای انتظامی و دیگر ضابطان دادگستری در مواقعی که مشغول انجام وظیفهٔ خود باشند، دفاع محسوب نمی‌شود، لکن هر گاه قوای مزبور از حدود وظیفهٔ خود خارج شوند و حسب ادله و قرائن موجود خوف آن باشد که عملیات آنان موجب قتل، جرح، تعرض به عرض یا ناموس یا مال گردد...»، دفاع سایبری جایز است. بنابراین موردی مانند آنکه مقامات ذی‌صلاح با اطلاع قبلی به کاربر مبنی بر اینکه لازم است سامانهٔ رایانه‌ای او از راه دور برای مدتی تحت کنترل قرار گیرد، در این میان مقامات ذی‌صلاح علاوه‌بر کنترل سامانهٔ رایانه‌ای، داده‌های شخصی و خانوادگی ذخیره‌شده در آن را بربایند، تخریب کنند یا مانع دسترسی کاربر به داده‌هایی شوند که به موجب مادهٔ ۶۷۳ قانون آیین دادرسی کیفری مصوب ۱۳۹۲/۳/۴ (با اصلاحات مصوب۱۳۹۴/۳/۲۴) دستور تفتیش و توقیف آنان صادر نشده است[1]، به‌نظر می‌رسد این امکان برای کاربر فراهم است که اقدام به دفع تجاوز کند، زیرا در این حالت به‌دلیل آنکه اعمال و رفتار مقامات ذی‌صلاح از حدود مجوز قانونی تجاوز کرده است، شایسته به‌نظر نمی‌رسد اقدامات

---

۱. مادهٔ ۶۷۳ ـ (الحاقی ۱۳۹۳/۰۷/۰۸): «دستور تفتیش و توقیف باید شامل اطلاعاتی از جمله اجرای دستور در محل یا خارج از آن، مشخصات مکان و محدوده تفتیش و توقیف ، نوع و میزان داده‌های موردنظر، نوع و تعداد سخت‌افزارها و نرم‌افزارها، نحوهٔ دستیابی به داده‌های رمزنگاری یا حذف شده و زمان تقریبی انجام تفتیش و توقیف باشد که به اجرای صحیح آن کمک می‌کند».

آنان را مورد حمایت قانونی قرار داد، بلکه لازم است دفاع در برابر اقدامات آنان را تابع عمومات دانست و آن را جایز شمرد.

وجود قرائن معقول یا خوف عقلایی در دفاع مشروع اعم از دفاع تام یا دفاع ظاهری یکی دیگر از شرایط تحقق دفاع مشروع است، زیرا بدون وجود مستند بودن دفاع به شواهد معقول نمی‌توان بر این باور بود که رفتار مدافع اگرچه ظاهراً مجرمانه قلمداد می‌شود، سزاوار برخورد به مانند یک مجرم واقعی نیست. بنابراین آنچه به رفتار ارتکابی مدافع، مشروعیت می‌بخشد، تحقق حالت روانی خاصی است که مدافع را به‌سوی صیانت از حقوق خود در مقابل تهاجم و تعرض صورت‌گرفته سوق می‌دهد و تنها زمانی این باور در فرد شکل می‌گیرد که شواهد و قرائن ملموسی در عالم واقع مبنی وجود خطر و تجاوز از سوی وی احساس شود. به‌عبارت دیگر، خوف عقلانی در مدافع، شرط ایجابی قرار گرفتن فرد «در مقام دفاع» است. این امر در بند «ب» مادهٔ ۱۵۶ ق.م.ا [1] نیز مورد تأیید و تصدیق قانونگذار به‌عنوان شرط لازم برای تحقق دفاع مشروع ذکر شده است.

شرط وجود قرائن معقول یا خوف عقلایی مدافع در حملات سایبری مستلزم آن است که مدافع متوجه تغییرات غیرعادی در عملکرد سامانهٔ رایانه‌ای خود شود. به‌عبارت دیگر، لازم است سامانهٔ رایانه‌ای از عملکرد متعارف خود خارج شود. مواردی همچون پیام‌های غیرمعمول از طرف آنتی‌ویروس (Antivirus)، تغییراتی در مرورگر (Browser) اینترنتی یا حرکت‌های عجیب ماوس (Mouse)، روشن و خاموش شدن چراغ وب‌کم (Webcam) و ... می‌تواند دلالت بر یک حملهٔ سایبری داشته باشد. البته باید در نظر داشت که گاهی تغییر در عملکرد متعارف سامانهٔ رایانه‌ای ممکن است ناشی از عیوب سخت‌افزاری یا نرم‌افزاری سامانهٔ رایانه‌ای باشد که در این‌صورت ابتدا لازم است مدافع از غیرمعیوب‌بودن سخت‌افزارها و نرم‌افزاری‌های سامانه‌ی رایانه‌ای خود اطمینان حاصل نماید.

آخرین شرط آن است که خطر یا تجاوز به‌سبب اقدام آگاهانه مدافع نباشد. این شرط در مادهٔ ۶۱ قانون مجازات اسلامی ۱۳۷۰ پیش‌بینی نشده بود، اما در مادهٔ ۱۵۶ قانون مجازات اسلامی ۱۳۹۲ به‌صراحت در بند «پ» بیان شده است.[2] با عنایت به شرط مذکور، مواردی مانند آنکه مهاجم سایبری علیه دیگر سامانه‌های رایانه‌ای مرتکب حملهٔ سایبری شود و در مقابل دیگر کاربران

---

۱. بند «ب» مادهٔ ۱۵۶ ق.م.ا مقرر می‌دارد: «دفاع مستند به قرائن معقول یا خوف عقلایی باشد».

۲. بند «پ» مادهٔ ۱۵۶ ق.م.ا مصوب ۱۹۳۲ مقرر می‌دارد: «خطر و تجاوز به‌سبب اقدام آگاهانه یا تجاوز خود فرد و دفاع دیگری صورت نگرفته باشد.»

سامانه‌های رایانه‌ای در مقام دفاع به سامانهٔ رایانه‌ای او حمله کنند، مهاجم سایبری نمی‌تواند با تمسک به دفاع مشروع حملات دیگری انجام دهد.

مورد دیگر حالتی است که کاربران آگاهانه خود را در معرض خطر حملهٔ سایبری قرار می‌دهند. مانند موردی که آنتی‌ویروس‌ها پیش از باز کردن ایمیل‌ها یا لینک‌ها به کاربر هشدار و اخطار می‌دهند و کاربر بدون توجه به آن هشدارها و اخطارها، ایمیل‌ها یا لینک‌هایی که ممکن است حاوی بدافزار باشند، باز کند. در این موارد به‌نظر می‌رسد به‌دلیل رفتار آگاهانهٔ کاربر، این عمل مشمول قاعدهٔ اقدام شده و نمی‌تواند به دفاع مشروع متمسک شود.

۷. مدافع در حملات سایبری

امری که در خصوص ماهیت مهاجم بررسی شد، قابل طرح در خصوص مدافع نیز است. قانونگذار با عبارت نخست مادهٔ ۱۵۶ق.م.ا به این پرسش و ابهام پاسخ داده است و تنها «فرد» را در قالب مدافع به رسمیت شناخته است. سؤالی که می‌توان مطرح کرد آن است که هر گاه سامانه‌های رایانه‌ای متعلق به اشخاص حقوق از طریق حملات سایبری مورد تعرض قرار گیرد، در این صورت ممکن است «مال» و «عرض» شخص حقوقی مورد خطر و تجاوز قرار گیرد، همچنین ممکن است «نفس» و «آزادی تن» کارکنانی که در نهادها، شرکت‌ها و غیره مشغول به‌کارند، مورد تجاوز قرار گیرد، در این صورت آیا اشخاص حقوقی می‌توانند به دفاع مشروع متوسل شوند؟ در یک رویکرد، با توسل به تفسیر لفظی می‌توان گفت با توجه به سیاق مادهٔ ۱۵۶ ق.م.ا پاسخ به این پرسش منفی است. همان‌گونه‌که به‌دلیل اصطلاح «فرد» به‌کاررفته در برخی مواد قانونی، حقوقدانان امکان اعمال مجازات‌های تکمیلی، نهاد تعویق و تعلیق اجرای مجازات را در مورد شخص حقوقی منتفی دانسته‌اند (شریفی، ۱۳۹۴: ۳۳۸-۳۳۷). باید امکان توسل به دفاع مشروع برای اشخاص حقوقی را نیز منتفی دانست.

لیکن، در رویکرد دوم و صحیح‌تر، می‌توان معتقد بود، دفاع نیز مانند حمله، یک رفتار انسانی است و رفتار تنها از شخص حقیقی می‌تواند سرزند. بنابراین، این امر که در ماده از لفظ «فرد» بهره برده است، نه برای خروج شخص حقوقی از ماده، بلکه برای تأکید بر آن است که تنها شخص حقیقی می‌تواند دفاع کند. بنابراین تفسیر، اگر نمایندهٔ قانونی شخص حقیقی در راستای منافع و به نام شخص حقیقی در مقام دفاع در برابر حملهٔ سایبری مرتکب جرم سایبری شد، از آنجا که شخص حقیقی خود دارای عوامل موجهه است و نمی‌تواند مورد تعقیب قرار گیرد، شخص حقوقی نیز از این حیث فاقد مسئولیت است.

۸. شرایط دفاع در مقابل حملات سایبری

نخستین شرطی که قانونگذار در بند «الف» مادهٔ ۱۵۶ ق.م.ا مورد توجه قرار داده است، ضرورت در رفتار مدافع است. ضرورت رفتار بستگی تام به ماهیت و جنس خطر و تجاوز دارد و بدون در نظر گرفتن خطر و تجاوز نمی‌توان این شرط را تفسیر کرد. همچنین باید در نظر داشت که ضرورت امری نسبی است و باید در بستر عرف تفسیر شود و معیار تشخیص و تعیین ضرورت یا عدم ضرورت رفتاری، تنها عرف می‌تواند باشد. تجاوز و خطر باید به‌گونه‌ای باشد که امکان دفع آن از طریقی غیر از دفاع ممکن نباشد و مدافع هیچ‌گونه راهی غیر از دفاع در مقابل او نداشته باشد. در خصوص در مقام دفاع بودن به‌نظر می‌رسد شرط ضرورت به‌صورت غیرمستقیم به دو موضوع «رعایت مراحل دفاع» و «در مقام دفاع بودن» مرتبط است.[۱]

تحقق شرط مذکور در حملات سایبری موجب می‌شود که ابتدا مدافع سایبری تمام تلاش خود را با توسل به تمامی ظرفیت‌ها و امکانات فنی جهت دفع حمله سایبری بدون آنکه به سامانهٔ رایانه‌ای مهاجم نفوذ کند، انجام دهد و درصورتی‌که اطمینان حاصل کرد که چاره‌ای جز نفوذ به سامانه‌ی رایانه‌ای مهاجم نیست، می‌تواند در مقام دفاع مشروع به سامانهٔ رایانه‌ای مهاجم هجوم آورد. برای مثال گاهی اقداماتی مانند خاموش کردن سامانه رایانه‌ای، قطع ارتباط سامانهٔ رایانه‌ای با شبکهٔ جهانی اینترنت یا نصب یک ضدِ بدافزار جهت شناسایی و از کار انداختن عملکرد آن و همچنین پاکسازی سامانهٔ رایانه‌ای از هرگونه بدافزار، سبب دفع حملهٔ سایبری شود که در این صورت نفوذ به سامانهٔ رایانه‌ای مهاجم در مقام دفاع مشروع توجیه‌شدنی نیست.

در برخی موارد ممکن است برای مدافع چاره‌ای جز حمله به سامانهٔ رایانه‌ای مهاجم نباشد. برای مثال ممکن است خاموش کردن سامانهٔ رایانه‌ای به تغییر در عملکرد سایر سامانه‌های رایانه‌ای موجود در یک شبکهٔ رایانه‌ای منجر شود که این امر ممکن است خسارات جبران‌ناپذیری را به‌همراه داشته باشد. همچنین ممکن است استفاده از ضدِ بدافزارها به‌منظور شناسایی و از کار انداختن بدافزار بدون فوت وقت عملاً امکان‌پذیر نباشد و دیگر شرایط را می‌توان در نظر گرفت

---

۱. شرط تناسب مبنای فقهی و شرعی نیز دارد. در آیهٔ ۱۹۴ سورهٔ بقره آمده است: «فمن اعتدی علیکم فاعتدوا علیه بمثل ما اعتـدی علیکم» (هر کس به شما ستم و تجاوزی بنماید، مانند خودش با وی رفتار کنید). این آیه به اهمیت و لزوم رعایـت تناسـب اشـاره دارد. تجاوز و حمله سبب نمی‌شود که شدیدتر از رفتار ارتکابی با مرتکب رفتار شود و تنها تا همان حدود و و اندازهٔ تعدی، دفـاع مشروعیت دارد. در ادامه آیهٔ شریفه می‌فرماید: «و اتقوا الله و اعلموا ان الله مع المتقین» (از خداوند بترسید. خداونـد بـا پرهیزکـاران است). از عبارت اخیر این‌گونه استنباط می شود که خداوند تبارک و تعالی در مقام نهی از اقدام متقابل بـیش از مثـل اسـت. ر.ک: عبدالتواب، ۱۹۸۳، ج ۱: ۲۴۹.

که شرط ضرورت را برای مدافع سایبری فراهم سازد، زیرا همان‌طورکه بیان شد، ضرورت رفتار بستگی تام با ماهیت و جنس خطر و تجاوز دارد.

علاوه‌بر مورد مذکور تحقق شرط ضرورت در حملات سایبری موجب می‌شود که مانند آنچه در فضای سنتی در دفاع مشروع بحث می‌شود، تحت این عنوان که آیا فرار در دفاع مشروع جایز است یا خیر، که البته در فضای سنتی نیز همان‌طورکه طبیعت دفاع با تغییر شرایط می‌تواند تغییر کند، احکام فرار هم دگرگون است (چگینی و همکاران، ۱۳۹۶: ۶۳۷)، در فضای سایبر نیز مطرح شود. بنابراین زمانی‌که با خاموش کردن سامانهٔ رایانه‌ای امکان دفع تجاوز محقق شود، می‌توان به‌دلیل شرط ضرورت امکان توسل به دفاع را منتفی دانست. حملات مدافع تنها در صورتی مجاز محسوب می‌شود که امکان دفع خطر به طریقی غیر از حمله امکان‌پذیر نباشد و چارچوب دفع خطر توجیه‌پذیر باشد. بنابراین، در صورت تحقق سایر شرایط هر گاه مدافع با اخلال در عملکرد سامانهٔ رایانه‌ای مهاجم توانست خطر را از سامانهٔ رایانه‌ای خود دفع کند، دیگر نمی‌تواند مرتکب اعمالی مانند سرقت داده‌های ذخیره‌شده در سامانهٔ رایانه‌ای مهاجم یا تخریب سایر داده‌های ذخیره‌شده در سامانهٔ رایانه‌ای او که برای دفع خطر ضروری نیست، شود.

شرط دیگری که قانونگذار در بند «ت» مادهٔ ۱۵۶ ق.م.ا برای تحقق دفاع مشروع لازم دانسته است، آن است که «توسل به قوای دولتی بدون فوت وقت عملاً ممکن نباشد یا مداخلهٔ آنان در دفع تجاوز و خطر مؤثر واقع نشود». این شرط، فوریت داشتن دفاع را به ذهن متبادر می‌نماید که در آن لازم است خطر و تجاوز به‌گونه‌ای باشد که مدافع علاوه‌بر اینکه چاره‌ای جز دفاع ندارد، امکان توسل به دیگر نهادها به‌منظور دفع تجاوز برای میسر نباشد، در این صورت لازم است فوراً واکنشی از خود بروز دهد.

در حملات سایبری شرط فوریت داشتن با وضوح بیشتری نمایان می‌شود، زیرا اصل سرعت در فضای سایبر به‌عنوان بستر حملات سایبری ملموس‌تر و پراهمیت‌تر است. با توجه به آنکه روند گسترش و سرایت نتایج زیانبار ناشی از حملات سایبری بسیار زیاد است و فوت وقت هنگام بروز حملات سایبری سبب آن می‌شود که بسیاری از منابع اطلاعاتی ذخیره‌شده در فضای سایبر سالم بودن یا صحت خود را از دست بدهند و همچنین ممکن است خسارات جبران‌پذیری علیه زیرساخت‌های حیاتی یک کشور در فضای سایبر وارد شود، در خصوص دفاع مشروع در برابر حملات سایبری باید گفت که در اغلب موارد امکان توسل به قوای دولتی بدون فوت وقت عملاً امکان‌پذیر نیست و حتی در صورت وجود این امکان مداخلهٔ آنان در دفع خطر و تجاوز به‌طور شایسته مؤثر واقع نمی‌شود، بلکه آنان با اقدامات خود می‌توانند مانع از گسترش و سرایت نتایج زیانبار ناشی از حملات سایبری شوند.

نتیجه

قوانین کیفری موقعیت و جایگاه رفیع در میان قوانین دارد و عهده‌دار صیانت از نفس، عرض، مال و آزادی افراد و نیز امنیت و آسایش جامعه است. با توجه به اهمیت و جایگاه قوانین کیفری نیاز است که قانونگذاری و قانون‌نگاری به‌گونه‌ای باشد که قانون پاسخگوی نیازهای روز جامعه باشد. با توجه به آنکه امروز عدم استفاده از فضای سایبر چه در سطح فردی و چه در سطوح کلان کشوری امری غیرممکن به‌نظر می‌رسد، ضرورت بررسی و کاوش در زمینهٔ فضای سایبر دوچندان است. این فضای پیشرفته و پیچیده که هر روز نیز بر گستردگی و پیچیدگی آن افزوده می‌شود، با آسیب‌های جدی امنیتی و حفاظتی همراه است که امکان مبدل شدن آسیب‌ها به تهدید بسیار زیاد دارد.

با توجه به ویژگی‌های جرائم سایبری امروزه سه رویکرد بر این جرائم می‌تواند حاکم باشد: نخست، آنکه این جرائم مانند جرائم سنتی بوده و همان ضوابط بر این رفتارهای مجرمانه این فضا حاکم است؛ دوم، این جرائم ویژگی‌های خاص خود را دارد و بنابر فضای متفاوت و ماهیت غیر از جرائم سنتی، نیازمند حقوق کیفری افتراقی خود است؛ در نهایت، رویکردی که بر تحمیل حقوق کیفری سنتی به‌عنوان اصل پای می‌فشارد، مگر با توجه به ماهیت این جرائم، جعل مقررات افتراقی ضروری نماید؛ رویکرد سوم، راهبردی مقرون به صلاح و مختار این مقاله است. بر این اساس، مقالهٔ حاضر درصدد بررسی آن بود که آیا می‌توان با توجه به مبانی و ضوابط حاکم بر دفاع مشروع سنتی آن را در دفاع در برابر حملات سایبری مورد استناد قرار داد.

از منظر مبنایی زمانی‌که یک سامانهٔ رایانه‌ای توسط مهاجمان سایبری که از حداقل مهارت‌هایی در زمینهٔ علوم فناوری و اطلاعات برخوردار است، مورد تهدید و حمله قرار می‌گیرد، بر مبنای حق طبیعی دفاع و به‌منظور برقراری نظم اجتماعی امکان استناد به دفاع مشروع برای سامانهٔ تهدیدشده وجود دارد؛ زیرا فضای سایبر با ویژگی‌هایی همچون کمرنگ شدن نقش جغرافیا، صرف زمان کوتاه و هزینهٔ کم، اتصال گستردهٔ افراد به شبکهٔ جهانی اینترنت، تأثیرگذاری شگرف و غیره موجب افزایش مهاجمان سایبری در این فضا شده است تا آنان اقدامات مجرمانهٔ خود را در این فضا به منصهٔ ظهور برسانند و از آنجا که حملات آنان در کسری از ثانیه اتفاق می‌افتد و فرصت توسل به قوای دولتی را برای شهروندان سایبری سلب می‌کند، بر مبنای حق طبیعی دفاع و همچنین برقراری نظم در فضای سایبر توسل به دفاع مشروع از جانب آنان در فضای سایبر قابل پذیرش است.

از منظر قانونی تحقق عنوان دفاع مشروع به‌عنوان یکی از موانع مسئولیت کیفری، تابع شرایط و ضوابطی است که اگر این شرایط و ضوابط با در نظر گرفتن ماهیت و چگونگی حملات سایبری و بستر آن یعنی فضای سایبر محقق شود، می‌توان ادعا کرد که عمل ارتکابی جرم نیست و عنوان

دفاع مشروع بر آن صادق است. با بررسی به‌عملآمده این نتیجه حاصل شد که این شرایط در خصوص شخص حمله‌کننده و مدافع و شروط دفاع مشروع، قابل تسری به دفاع در برابر حملات سایبری است. در خصوص موضوعات مورد حمایت در دفاع مشروع (نفس، مال، عرض و آزادی تن) و تعرض به آن از طریق حملهٔ سایبری، از یک سو می‌توان تنها نتایج ناشی از آن را در فضای سایبر را مدنظر قرار داد که در این صورت می‌توان «مال» و «عِرض» را مشمول دفاع مشروع دانست، از سوی دیگر، نتایج ناشی از حملات سایبری در فضای سنتی را نیز مدنظر قرار داد که در این صورت می‌توان قائل بر آن شد که حملات سایبری علاوه‌بر مال و عرض، «نفس» و «آزادی تن» افراد را نیز مورد تعرض قرار دهد. از سوی دیگر، تمامی شرایط حمله از جمله فعلیت و من غیرحق بودن و همچنین ضرورت دفاع و عدم امکان توسل به قوای دولتی در حملات سایبری وجود داشته و ازاین‌رو می‌توان در صورت وقوع حملهٔ سایبری درصورتی‌که با روش‌هایی غیر از ارتکاب جرم مانند قطع ارتباطات اینترانت یا اینترنت یا خاموش کردن سامانه امکان دفع یا رفع حمله میسر نشد، با ارتکاب جرم نسبت به دفاع از خود اقدام کرد. بنابراین، با توجه به فقدان عنوان خاص دفاع مشروع در فضای سایبر و مشترک بودن موضوع دفاع مشروع در فضای سنتی و فضای سایبر (جان، مال، عرض و آزادی تن) می‌توان دفاع مشروع در مقابل حملات سایبری را تابع عمومات دفاع مشروع به معنای سنتی قرار داد و براساس شرایط و ضوابط تعیین‌شده در خصوص آن و انطباق آن شرایط با فضای سایبر و حملات سایبری دفاع مشروع در برابر حملات سایبری را با توجه به مواد قانونی ۱۵۶ و ۱۵۷ ق.م.ا توجیه‌پذیر دانست.

منابع

الف) فارسی

۱. اشمیث، لارنس کی (۱۳۹۵). *درآمدی بر فهم هرمنوتیک*، ترجمهٔ بهنام خداپناه، چ اول، تهران: ققنوس.

۲. الهام، غلامحسین؛ برهانی، محسن (۱۳۹۵). *درآمدی بر جزای عمومی (جرم و مجرم)*، ج۱، تهران: میزان.

۳. بخشی، علی (۱۳۹۵). *هرمنوتیک*، چ نخست، قم: اشراق.

۴. تروپه، میشل (۱۳۹۰). *فلسفهٔ حقوق*، ترجمهٔ مرتضی کلانتریان، چ دوم، تهران: آگه.

۵. جالینوسی، احمد؛ ابراهیمی، شهروز؛ قنوانی، طیبه (۱۳۹۲). «جایگاه فضای سایبر و تهدیدهای سایبری در استراتژی امنیت ملی ایالات متحدهٔ آمریکا»، *فصلنامهٔ دانش سیاسی و بین‌الملل*، ش ۵، بهار، ص ۲۰-۱.

۶. جلالی فراهانی، امیرحسین (۱۳۹۵). *کنوانسیون جرائم سایبر و پروتکل الحاقی آن*، چ دوم، تهران: خرسندی.

۷. چگینی، مهدی؛ قیاسی، جلال‌الدین؛ خزایی، میثم (۱۳۹۶). «بررسی تطبیقی امکان فرار در دفاع مشروع در حقوق کیفری ایران، فرانسه و مصر»، *فصلنامهٔ علوم اجتماعی*، ویژه‌نامهٔ پیشگیری از جرم و حقوق، ش ۳۹، زمستان، ص ۶۴۵-۶۳۱.

۸. خلیل‌زاده، مونا (۱۳۹۳). *مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری*، چ اول، تهران: مجد.

۹. سلمانی‌زاده، محمود (۱۳۸۰). «جنگ اطلاعات و امنیت»، خبرنامهٔ انفورماتیک، *سازمان برنامه و بودجهٔ کشور*، ش ۸۰، بهار.
۱۰.شریفی، محسن (۱۳۹۴). *مسئولیت کیفری اشخاص حقوقی در حقوق ایران و انگلستان*، چ اول، تهران: میزان.
۱۱.عبدالتواب، محمد (۱۹۸۳م). *الدفاع الشرعی فی فقه الاسلامی*، ج ۱، قاهره: نشر عالم الکتب.
۱۲.عظیمی، فاطمه؛ خشنودی، هادی (۱۳۹۵). «نقش تروریسم سایبری در تهدید علیه امنیت ایران و راه‌های پیشگیری از آن»، *فصلنامهٔ مطالعات سیاسی*، ش ۳۴، زمستان، ص ۲۱۲-۱۹۹.
۱۳.لاک، جان (۱۳۸۸). *رساله‌ای در باب حکومت*، ترجمهٔ حمید عضدانلو، چ دوم، تهران: نشر نی.
۱۴.محمدی، ابوالحسن (۱۳۹۲). *مبانی استنباط حقوق اسلامی (اصول فقه)*، چ پنجاه‌ودوم، تهران: انتشارات دانشگاه تهران.
۱۵.محمودی جانکی، فیروز؛ صادقی، آزاده (۱۳۹۴). «دفاع مشروع ظاهری»، *آموزه‌های حقوق کیفری*، ش ۱۰، پاییز و زمستان، ص ۱۹۴-۱۵۵.
۱۶.مرسی، هادی (۱۳۹۷). *مقابله با حملات سایبری در حقوق کیفری ایران و اسناد بین‌المللی (با تأکید بر حملات سایبری علیه ایران)*، پایان‌نامهٔ کارشناسی ارشد، دانشکده حقوق و علوم سیاسی، دانشگاه تهران.
۱۷.معین، محمد، *فرهنگ فارسی معین*، ج ۳، تهران: امیرکبیر.
۱۸.مگی، برایان (۱۳۹۷). *داستان فلسفه*، ترجمهٔ مانی صالحی علامه، چ چهارم، تهران: اختران.
۱۹.هگل، گئورگ؛ فریدریش، ویلهلم (۱۳۷۸). *عناصر فلسفهٔ حق یا خلاصه‌ای از حقوق طبیعی و علم سیاست*، ترجمهٔ مهبد ایرانی‌طلب، چ ششم، تهران: قطره.

ب) انگلیسی

20. Byrd, B. S. (1987). "Wrongdoing and Attribution: Implications Beyond the Justification-Excuse Distinction", ***Wayne L. Rev.***, *33*.
21. Fletcher, G. P. (1984). "Rights and excuses", ***Criminal Justice Ethics***, Vol.3, No.2, pp.17-27.
22. Fletcher, G. P. (1985). "The right and the reasonable", ***Harvard Law Review***, pp.949-982.
23. Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). "The law of cyber-attack", ***California Law Review***, pp.817-885.
24. Lord, K. M., & Sharp, T. (Eds.). (2011). ***America's Cyber Future: Security and Prosperity in the Information Age***, Vol. 1, Washington, DC: Center for a New American Security.
25. Marshall, J.B & Saulawa M.A(2015). Cyber- attacks: The legal response, International Journal of International Law, 1(2).
26. Training, U. A., & Command, D. (2005, August). ***Cyber Operations and Cyber Terrorism***. In DC Intelligence. Fort Leavenworth, KA, USA: US Army. United States Congress (1984).
27. ***Definition of terrorism***, United States Code Congressional and Administrative News, 98th Congress, Second Session, Oct, Vol. 19.