تروریسم سایبری

تاریخ دریافت: ۱۳۸۵/۶/۱ تاریخ تأیید: ۱۳۸۵/۷/۱۰

امیرحسین جلالی فراهانی*

چکیده

*یکی از تهدیدات امنیتی که همواره ملتها و دولتها را آزار داده، **اقدامات تروریستی** است که عمدتاً با پیامدهای بسیار زیانباری همراه هستند. بدیهی است «**زیرساختهای حیاتی**» از بهترین اهداف محسوب می‌شوند که با توجه به الکترونیکی شدن آنها، نه تنها ارتکاب اقدامات تروریستی آسان‌تر شده، بلکه لطمات وارد شده بسیار سهمگین هستند. البته ماهیت «**چند رسانه‌ای**» فضای سایبر، به تروریستها امکان بهره‌برداریهای سوء دیگری را هم داده است. این نوشته بر آن است که با تبیین اجمالی مفهوم عام **تروریسم سایبر** به عنوان یک **پدیدهٔ مجرمانه**، راهکارهای حقوقی مقابله با آن و وضعیت کشورمان را بررسی نماید.*

واژگان کلیدی: *تروریسم، فضای سایبر، پیش‌گیری، مجازات.*

* کارشناس ارشد حقوق کیفری و جرم‌شناسی، پژوهشگر در حقوق کیفری سایبری (jalalyfarahany1979@gmail.com).

مقدمه

همان‌طور که می‌دانیم، ماهیت علوم را اطلاعات تشکیل می‌دهد؛ عنصری که به دلیل اهمیت فوق‌العاده‌اش، عصر حاضر به آن نام گرفته است (جینا دی آنجلیز، ۱۳۸۳: ۱۷). به همین ترتیب، رشد هر حوزهٔ علمی بـه فـرآوری و پـردازش (Process) صـحیح، دقیـق و هرچـه سـریع‌تـر اطلاعاتش وابسته است. لذا آنچه نیمهٔ دوم قـرن بیـستم را از دوره‌هـای پیـشین متمـایز کـرده، دستیابی بشر به یک پردازشگر بسیار سریع و در عین حال مطمئن به نام رایانهٔ الکترونیکی است که سوئیچ اولین نمونه آن با نام ENIAC (Electronic Numerical Integrator And Computer) در سال ۱۹٤٦ چرخانیده شد (Casey, 2001: 32).

اما عامل مهمی که توانست در ایـن پیـشرفت پرشـتاب، بـه رایانـهٔ الکترونیکـی کمـک شایسته‌ای کند و قابلیتهای آن را به شکل مؤثرتر و کارآمدتر در معرض بهره‌برداری فراگیـر قرار دهـد، ارتباطـات الکترونیکـی (Electronic Communication) اسـت. پـیش از ایـن، بهره‌برداری از سیستمهای رایانه‌ای به همان محل استقرارشان محدود می‌شد و همین مسئله به طور چشمگیری از کارآیی‌شان کاسته بود. اما ارتباطـات الکترونیکـی امکـان دسـترس و بهره‌برداری دوردست از سیستمهای رایانه‌ای را فراهم کرده است، تا آنجـا کـه شـبکه‌هـای رایانه‌ای بزرگ بسیاری در سراسـر جهـان راه‌انـدازی شـده‌انـد و اکنـون بـدون هـیچ‌گونـه محدودیت زمانی و مکانی و با کیفیت مطلوب، به ارائهٔ انواع خدمات رایانه‌ای مـی‌پردازنـد (دزیانی، ۱۳۸٤: ٤٤).

بارزترین ویژگی فضای سایبر، دسترس‌پذیر سـاختن سـریع و بـا حـداقل هزینـهٔ کلیـهٔ اطلاعات آن‌لاین (Online) است که بـسیاری از نمونـه‌هـای آن را در وب‌سـایتهای شـبکهٔ جهانی اینترنت شاهد هستیم. این دسترس‌پذیری بـرای همگـان فـراهم آمـده و هـیچ‌گونـه تبعیضی اعمال نشده است. جالب‌تر اینکه اگر صاحبان منابع اطلاعات، رأساً یـا بـه واسـطهٔ دیگران، به ویژه متصدیان شبکه‌های اطلاع‌رسانی رایانه‌ای (Network Provider)، با اجرای تمهیدات گوناگون سخت‌افزاری و نرم‌افزاری، سعی در تحدید این میـزان دسـترس‌پـذیری داشته باشند، توفیق چندانی نمی‌یابنـد. زیـرا ایـن فـضا بـه همـان راحتـی انـواع ابزارهـای خنثی‌کننده را در اختیار همگان قرار داده است. به عبارت دیگر، تقریباً چیزی به نام تحدیـد دسترس به اطلاعات در فضای سایبر معنا ندارد (جلالی فراهانی، ۱۳۸٤: ۳۱).

با وجود این شرایط، به نظر می‌رسد در متزلزل شدن برخی مفاهیم حساس و اساسی، به ویژه امنیت (Security)، تردیدی باقی نمانده باشد. امنیت، همانند فضای سایبر، آن‌قدر انعطاف‌پذیر است که در هر سطح و کیفیتی معنا و کاربرد خود را حفظ می‌کند؛ از حوزه‌های کلان مانند امنیت بین‌المللی، منطقه‌ای و ملی تا امنیت یک بنگاه کوچک یا موضوع ویژه. صرف‌نظر از تعاریف گوناگون آن، می‌توان کارکرد اصلی‌اش را رفع هرگونه تهدید (Threat) دانست.

اما آن دسته از تهدیدکنندگانی که در این نوشتار مورد توجه قرار گرفته‌اند، تروریستها هستند که صرف‌نظراز ماهیت و اهداف اقداماتشان، نتایج بسیار زیانبار و گاه جبران‌ناپذیری به جای می‌گذارند. معمولاً آنها نقاط حساس و حیاتی جوامع را هدف قرار می‌دهند تا اساسی‌ترین ضربات را به دشمنان خود وارد کنند و بهترین بهره‌برداری را از وضعیت موجود به عمل آورند که بی‌تردید زیرساختهای حیاتی و زیربنایی از بهترین گزینه‌ها به شمار می‌آیند (Hinde, 2001: 568). البته سهولت و کم‌هزینه بودن ارتکاب این اقدامات نیز از اهمیت قابل توجهی برخوردار است، لذا این گروهها همواره به پیشرفته‌ترین ابزارها برای رسیدن به اهداف شوم خود مجهز هستند.

یکی از بهترین این ابزارها که به نظر می‌رسد تمامی ویژگیهای مورد نیاز تروریستها را در خود جمع کرده، فضای سایبر است. این نوشتار در پی تبیین واقعیات تروریسم سایبری در مفهوم موسع و راهکارهای حقوقی مقابله با آن است. در این زمینه، فصل اول به مفهوم و ماهیت تروریسم سایبری اختصاص دارد. در فصل دوم، راهکارهای حقوقی مقابله با آن که بی‌تردید به دلیل ماهیت مجرمانه‌اش مبتنی بر ضمانت اجراهای کیفری و همچنین تدابیر پیشگیرانه است تبیین می‌گردد. سپس در فصل سوم، وضعیت حقوقی کشورمان در برابر این تهدیدات بررسی می‌شود و در نهایت، نتیجه‌گیری به عمل خواهد آمد.

فصل اول. مفهوم و ماهیت تروریسم سایبری

در این فصل، به اجمال مفهوم مرکب تروریسم سایبری (Cyber Terrorism) تبیین می‌گردد. به این منظور، ابتدا به طور مجزا عناصر تشکیل‌دهندهٔ آن، یعنی تروریسم و فضای سایبر و سپس حاصل ترکیب آنها مورد بررسی قرار می‌گیرد.

گفتار اول: مفهوم و ماهیت تروریسم

با اینکه پیشینهٔ اقدامات تروریستی به اندازهٔ عمر بشر طولانی است، اما نه تنها هیچ‌گاه در بارهٔ آن اتفاق نظر وجود نداشته، بلکه معانی بعضاً متعارضی نیز به آن نسبت داده شده است. عده‌ای آن را تاکتیک و دیگران استراتژی دانسته‌اند. برخی آن را جنایت و گناهی نابخشودنی و گروهی وظیفه‌ای الهی و واکنش موجه به ظلم و ستم برشمرده‌اند. در هر حال، قدر مسلّم این است که تروریسم ابزاری برای رسیدن به هدف است. شاید بهترین تعبیر را برایان جنکینز (Brian Jenkins)، کارشناس تروریسم، ارائه داده باشد. وی در سال ۱۹۷٤، در کوتاه‌ترین و در عین حال رساترین عبارت، تروریسم را یک تئاتر معرفی کرد (U.S. Army TRADOC, 2004: 21)؛ زیرا همانند آن از پیش طراحی می‌شود و برای جلب نظر خیل عظیم مخاطبان ارتکاب می‌یابد. به نظر می‌رسد اکنون این تعبیر به دلیل ظهور و افزایش روزافزون انواع رسانه‌های ارتباط جمعی چاپی و الکترونیکی و همچنین جدی شدن مسائل راجع به این پدیده، به ویژه از ابتدای هزارهٔ جدید میلادی، بهتر قابل درک باشد.

اما دغدغهٔ اصلی تمامی مخاطبان این تئاتر وحشتناک، خسارات سنگین و بعضاً جبران‌ناپذیر مالی و جانی‌اش است؛ آن هم از جانب کسانی که به خوبی برای این نقش‌آفرینی خود را آماده کرده‌اند و حتی حاضرند برای رسیدن به هدفشان، از ارزشمندترین سرمایه‌شان، یعنی جانشان، بگذرند. لذا ایستادگی در برابر آنها یا به حداقل رساندن خساراتشان، بدون برنامه‌ریزی اصولی و راهبردی نه تنها نتیجه‌بخش نیست که ممکن است منجر به تشدید این‌گونه اقدامات نیز بشود.

به این ترتیب، پیش از هر چیز باید اقدامات تروریستی و عوامل آن به طور صحیح شناسایی شوند. این مسئله مستلزم شناسایی ابعاد گوناگون آن است. برای مثال، سازمان ملل متحد، به عنوان بزرگ‌ترین مرجع بین‌المللی، از سال ۱۹٦۳ تا کنون، در بارهٔ تروریسم و اقدامات تروریستی سیزده سند بین‌المللی به تصویب رسانده است و جالب اینکه تنها در سه سند صراحتاً به عنوان تروریسم اشاره شده و در بقیه تنها مصادیق اقدامات تروریستی برشمرده شده است. این سه سند عبارت‌اند از: کنوانسیون بین‌المللی برای جلوگیری از بمب‌گذاری تروریستی (International Convention for the Suppression of Terrorist Bombing) (۱۹۹۷)، کنوانسیون بین‌المللی برای جلوگیری از تأمین مالی تروریسم (۱۹۹۹)

(International Convention for the Suppression of the Financing of Terrorism)، و کنوانسیون بین‌المللی برای جلوگیری از اقدامات تروریستی هسته‌ای (۲۰۰۵) (International Convention For The Suppression of Acts of Nuclear Terrorism) (حکیمی‌ها، ۱۳۸۵: ۳۵٦). البته این سازمان در سال ۱۹۹۲ در یک تعریف غیررسمی که با استقبال گستردهٔ دانشگاهیان نیز مواجه شد، چنین مقرر داشته است:

> یک شیوهٔ مشتاقانه ـ رغبت‌انگیز در ارتکاب خشونت مکرر توسط افراد، گروهها یا دولتها به صورت (نیمه)محرمانه در جهت نگرش فکری خاص، مجرمانه یا سیاسی. در اینجا قربانیان اصلی خشونت، در مقایسه با آدم‌کشی، آماج اصلی محسوب نمی‌شوند (U.S. Army TRADOC,2004: 1-3).

به طور کلی، عناصر مشترک تشکیل‌دهندهٔ تروریسم عبارت‌اند از:

۱. سیاسی؛ ۲. روان‌شناختی؛ ۳. خشونت‌آمیز؛ ٤. پویا؛ ۵. مدبرانه؛ ٦. رسانه‌ای بودن.

۱. سیاسی: یک اقدام تروریستی، اقدامی سیاسی نیز محسوب می‌شود یا به منظور تأثیرگذاری سیاسی ارتکاب می‌یابد. کلوزویتز (Clausewitz) به خوبی در این باره اظهار داشته: *«جنگ دنبالهٔ سیاست با ابزاری دیگر است.»*

۲. روان‌شناختی: نتایج پیش‌بینی شدهٔ اقدامات تروریستی، تأثیر روان‌شناختی به دنبال دارد. تروریستها مخاطبان و نه قربانیان واقعی‌شان را هدف قرار می‌دهند. ممکن است مخاطب این اقدامات، همهٔ مردم، بخش خاصی از جامعه (مانند اقلیتهای قومی) یا نخبگان تصمیم‌ساز در جامعهٔ سیاسی، اجتماعی یا نظامی باشند.

۳. خشونت‌آمیز: هدف از قهر و غلبه و تخریب، تاثیرگذاری است. حتی اگر نتایج یا خسارات به بار آمده نتیجهٔ عملیات تروریستها نباشد، تهدید یا خشونت بالقوه ایجاد شده تأثیر خود را خواهد گذاشت.

٤. پویا: گروههای تروریستی به تغییر و تحول و تحرکات سیاسی نیازمندند. اما از آنجا که دیدگاههای انتقادی شدیدی دارند، همواره سرسختانه‌ترین مواضع را اتخاذ می‌کنند.

۵. مدبرانه: تروریسم یک اقدام از پیش طراحی شده و هدفمند برای تحقق اهداف مشخص است، به طور منطقی به کار گرفته می‌شود و از تاکتیکهای گزینشی خاصی برخوردار است و به هیچ وجه نمی‌توان آن را تصادفی دانست. برخورداری از امکانات و

پشتیبانیهای مستمر قدرتمند، این امکان را به تروریستها می‌دهد تا یک برنامه‌ریزی حتی طولانی‌مدت برای خود داشته باشند.

٦. رسانه‌ای بودن: تروریستها در جهت اهدافی که دنبال می‌کنند، عمداً به نحوی مرتکب اقدامات تروریستی می‌شوند یا تهدید به ارتکاب آنها می‌کنند که سریعاً در میان جامعهٔ مورد نظرشان انعکاس خبری داشته باشد و تأثیر دلخواهشان را بر مخاطبان بگذارد. مهم نیست چه کسی قربانی می‌شود یا چه میزان خسارات وارد می‌آید، بلکه میزان تأثیرپذیری مخاطبان از آنها حائز اهمیت است. لذا رسانه‌ها ابزار قدرتمند و مؤثری برای تروریستها محسوب می‌شوند (U.S. Army TRADOC,2004:1-4).

گفتار دوم: مطلوبیتهای فضای سایبر برای تروریستها

همان‌طور که در مقدمه اشاره شد، فضای سایبر دنیای بی‌کرانی از امکانات و قابلیتهای بی‌شمار است که بدون محدودیت در دسترس همگان قرار دارد و هرکس با هر انگیزه و هدفی می‌تواند از این موهبت بهره‌برداری کند. بی‌تردید تروریستها هم خود را از این قاعده مستثنا نمی‌دانند. آنها همانند هر مجرم عاقل دیگری این حق را برای خود قائل می‌شوند که از امکانات بی‌شمار این فضا در جهت تحقق اهدافشان بهره‌برداری کنند. البته محرز است که هر طیف از مجرمان با توجه به اهدافی که دنبال می‌کنند و انگیزه‌هایی که دارند، از ویژگیهای خاص این فضا بهره‌برداری می‌کنند که در صورت شناسایی آنها، بهتر می‌توان سیاستها و تصمیمات پیشگیرانه و تدافعی را اتخاذ کرد. در ادامه به آن دسته از ویژگیهای فضای سایبر که توجه تروریستها را به خود جلب کرده و باعث شده آنها خط مشیهای خود را تغییر دهند و از دنیای فیزیکی به فضای سایبر روآورند، به اجمال اشاره خواهد شد.

۱. بدون مرز بودن فضای سایبر: ماهیت فرامرزی فضای سایبر، آن هم به گونه‌ای که هیچ یک از موانع و مرزهای موجود در دنیای فیزیکی در آن ملاحظه نگردد، یک ویژگی اساسی محسوب می‌شود و مزایای بی‌شماری از آن نشأت می‌گیرد.

۲. کاهش هزینهٔ جرم: فضای سایبر هزینهٔ جرم را به طور قابل ملاحظه‌ای کاهش داده است. به هنگام محاسبهٔ هزینهٔ جرم دو مؤلفه مورد توجه قرار می‌گیرد: ۱. نتیجه‌ای که عاید

می‌شود؛ و ۲. احتمال دستگیری و مجازات.* مسئلهٔ هزینهٔ جرم برای تروریستها اهمیت بسیار و حتی حیاتی دارد. زیرا جرائمی که مرتکب می‌شوند، مجازاتهای بسیار سنگینی دارند و عملاً امکان رهایی از آنها وجود ندارد. لذا ماهیت فرامرزی فضای سایبر فرصت بسیار مغتنمی برای آنهاست که با وجود دستیابی به اهداف مخرب پیش‌بینی شده، امکان به دام افتادن آنها به حداقل ممکن می‌رسد. آنها به راحتی می‌توانند از هر گوشهٔ جهان مرتکب اقدامات زیانبار تروریستی در فضای سایبر شوند، بی‌آنکه مجریان قانون کشور یا کشورهای آسیب‌دیده بتوانند آنها را شناسایی کنند. حتی در صورت شناسایی نیز مشکلات اجرایی بسیاری جهت دستگیری و مجازات آنها وجود دارد (برنر، ۱۳۸۲: ٥٤).

۳. امکان وارد آوردن خسارات مالی، بدون آسیبهای جسمی: اکثر اقدامات تروریستی در دنیای فیزیکی، با آسیب‌دیدگی افراد همراه است که این خود چندان با هدف جلب افکار عمومی و همنواسازی آنها با اهداف تروریستی سازگاری ندارد. زیرا اصولاً آسیبهای جانی، به ویژه اگر با مرگ همراه باشد، حساسیتها و واکنشهای زیادی را برمی‌انگیزد که به نفع عوامل آن نیست. لذا اگر تروریستها بتوانند بدون جریحه‌دار کردن احساسات مردم، لطمات مالی بسیاری به دولتمردان وارد آورند، به موفقیت بزرگی دست یافته‌اند. بدیهی است با وجود انواع اطلاعات ارزشمند مالی و دولتی در فضای سایبر، این فرصت بی‌نظیر برای تروریستها فراهم شده است (وارن، ۱۳۸۲: ۲۱).

٤. تأمین راحت امکانات و عوامل مورد نیاز برای اقدامات تروریستی: ماهیت اقدامات تروریستی فیزیکی به گونه‌ای است که برای ارتکاب آنها باید به ابزارهایی متوسل شد که تأمین آنها با مشکلات زیادی همراه است، مانند انواع مواد منفجره. همچنین به دلیل خطرناک بودن این اقدامات و احتمال بالای دستگیری و مجازات، کمتر کسی حاضر می‌شود آن را به انجام برساند. اما فضای سایبر تمامی ابزارهای مورد نیاز برای انواع اقدامات تروریستی سایبری را به صورت روزآمد در اختیار همگان قرار داده و البته نحوهٔ به‌کارگیری آنها تا حدی ساده شده که با کمترین مهارت و تجربه می‌توان از آنها استفاده

* موضوعات راجع به هزینهٔ جرم از سوی دانشمندانی نظریه‌پردازی شده که دیدگاههای اقتصادی داشتند و از پیشگامان آنها می‌توان به ژرمی بنتام اشاره کرد که مبدع نظریات **فایده‌گرایی واکنش اجتماعی** بود. ر.ک: (نجفی ابرندآبادی، ۱۳۷۷: ۳۱)

کرد. هرچند به دلیل پایین بودن هزینهٔ ارتکاب این‌گونه اقدامات و امکان تأمین آن از سوی گروههای تروریستی، متخصصان بسیاری حاضرند مرتکب انواع اقدامات مخـرب سـایبری شوند (Denning, 1999: 239).

۵. انعکاس جهانی موفقیت، مکتوم ماندن شکستها: شاید فناوری اطلاعـات و ارتباطـات الکترونیکی تنها ابزاری باشد که جهانیان همگی به صورت مشترک از آن استفاده مـی‌کننـد. لذا هرگونه اختلال در آن به خوبی انعکاس جهانی دارد و به راحتی اعتبـار یـک کـشور یـا مجموعهٔ خاصی در فضای سایبر لکه‌دار می‌شود. به همین دلیل، از آنجا کـه تروریـستها بـه دنبال انعکاس جهانی اقداماتشان هستند، این فضا می‌تواند بهترین گزینه باشد. با این حـال، تا عملی در این فضا مشاهده یا آثار و نتـایج آن لمـس نگـردد، کـسی از وقـوع آن آگـاهی نمی‌یابد، لذا چنانچه این‌گونه اقدامات با شکست مواجه شود و به نتیجهٔ مورد نظـر نرسـد، عملاً به میزان قدرت و اعتبار تروریستها لطمه‌ای وارد نمی‌شـود. هـر لحظـه ممکـن اسـت چندین اقدام تروریستی در این فضا ارتکاب یابد، ولی معدودی از آنها به ثمر می‌نشینند.

٦. امکان هماهنگی لحظه‌ای در سراسر جهان با ضریب اطمینان بـالا: یکـی از ابزارهـای مورد نیاز و حیاتی تروریستها، وسایل ارتباطی پیشرفته است تا بتوانند در کوتاه‌ترین زمان و با کمترین مشکل از وضعیت یکدیگر آگاه شوند. فضای سایبر این امکان را برای آنها فراهم آورده و آنها می‌توانند با بهره‌گیری از انواع ابزارهـای ارتباطـات الکترونیکـی، ماننـد پـست الکترونیکی، محیطهای گپ (Chat) و... به شکل مکتوب، صوتی و ویدیویی و بـه صـورت زنده با یکدیگر ارتباط داشته باشند. البته مزیت برجستهٔ این ابزارها که امکـان بـه‌کـارگیری بهینه را برای گروههای تروریـستی فـراهم مـی‌آورد، امکـان رمزنگـاری (Cryptography) محتوای ارتباطات الکترونیکی با ابزارهـای بـسیار پیـشرفته اسـت کـه احتمـال رمزگـشایی (Decryption) آنها را بسیار ضعیف می‌گرداند. به این ترتیب، آنها می‌توانند بدون دغدغه از دستیابی مجریان قانون به محتـوای نـامفهوم ارتباطاتـشان، بـه راحتـی بـه همـاهنگی امـور بپردازند. همچنین شیوه‌های نوین استگانوگرافی (Steganography) بـه تروریـستها امکـان می‌دهد در لوای پیامهای مشروع و نامشکوک، اطلاعات راجع به اقدامات تروریستی‌شان را مبادله کنند (Hancock, 2001: 555).

۷. امکان جذب حامیان از سراسـر جهـان: همـان‌طـور کـه در گفتـار قبـل اشـاره شـد،

تروریسم مجموعهٔ اقدامات هدفمند مستمری است که تا رسیدن بـه هـدف نهـایی، کـه در بسیاری موارد دست‌نیافتنی است، ادامه دارند. لذا جلب حمایت جامعهٔ مخاطبان موردنظر و حتی عضوگیری از میان آنها، از جملـه اقـدامات حیـاتی گروههـای تروریـستی محـسوب می‌شود. حال با توجـه بـه اینکـه فـضای سـایبر امکانـات رسـانه‌ای بـسیار گـسترده‌تـر بـا تأثیرگذاری بسیار بیشتر را با هزینهٔ بسیار ناچیز نسبت به امکانات رسانه‌ای دنیـای فیزیکـی در اختیار همگان قرار داده است، تروریـستها نیـز بـا بهـره‌گیـری از آنهـا و سـاخت انـواع برنامه‌های تبلیغاتی چندرسانه‌ای (Multimedia) به جلب حامی و جذب نیـرو مـی‌پردازنـد (Desouza, 2003: 387).

۸. انجام بهینهٔ فعالیتهای پولی و بانکی: یکی از حوزه‌هایی که تقریباً به طور کامل تحـت تأثیر فضای سایبر قرار گرفته و روند توسعه و تکامل الکترونیکی شـدن آن همچنـان ادامـه دارد، پول و بانکداری الکترونیکی است. با این حال، امکان سوء استفاده از خدمات پولی و بانکی نیز افزایش چشمگیری یافته است. برای مثال، گروههـای جنایتکـار سـازمان‌یافتـه و تروریستها که نیازمند مبادلات مالی زیادی هستند و در عین حال با محدودیتهای مالی بـسیاری مواجه و همواره تحت نظرند، مجبورند عایداتشان را تطهیر (Money Laundering) کننـد تـا بتوانند از آنها استفاده کنند. در اینجا پول و بانکداری الکترونیکی کمک بسیار بزرگی به آنها محسوب می‌شوند، به گونه‌ای که اکنون پول‌شویی فیزیکی رو به زوال و پول‌شویی سایبری (Cyber Laundering) در حال ظهور است (جلالی فراهانی، ۱۳۸٤: ۱۰۹). همچنین امکـان جذب کمکهای مالی از سوی هواداران و حامیان نیز بسیار آسان شده و امکان ارسال کمکهـای نقدی از هر جای دنیا در کمترین زمان ممکن فراهم آمده است (Walker, 2006: 638).

گفتار سوم: تروریسم سایبر در مفهوم موسع

پیش از وارد شدن به اصل بحث، یادآور می‌شود تاریخچهٔ اقدامات تروریستی گواه ایـن مسئله است که تروریستها تقریباً از همان ابتدا به سیستمهای رایانه‌ای به عنوان یـک هـدف ارزشمند توجه داشته‌اند. البته این مسئله در مورد کلیهٔ فناوریهای سـطح بـالا (High-tech) صدق می‌کند که نمونهٔ بارز آن فناوری اطلاعات و ارتباطـات الکترونیکـی بـوده و هـست. برای مثـال، بریگـاد سـرخ، طـی دهـهٔ ۱۹۷۰، در ایتالیـا یـازده واحـد از تأسیـسات اصـلی پردازشگرهای ارتباطاتی را تخریب کرد. میزان خسارات وارد شده، پانصد هزار دلار برآورد

شد. این گروه طی بیانیه‌ای استفادهٔ روزافزون از رایانه‌ها را بخشی از توطئهٔ بیشینه کردن نظارتهای اجتماعی برشمرد. به نظر این گروه، رایانه‌ها به مثابهٔ ابزاری جهت درگیریهای طبقاتی به کار می‌رفتند و از این رو لازم بود به این شبکه‌های نظارتی تعرض شود تا از بین بروند (وارن، همان: ٦).

با این حال، همان‌طور که ملاحظه می‌شود، تمامی این اقدامات تروریستی و همچنین اهدافی که ویران می‌شوند یا آسیب می‌بینند، همگی در دنیای فیزیکی قرار دارند و به کلی از بحث این نوشتار که به بررسی اقدامات تروریستی در فضای سایبر می‌پردازد، خارج‌اند. در ادامه، مباحث در دو قسمت مطرح می‌شود. ابتدا مفهوم تروریسم سایبری صرف و سپس بهره‌برداری‌های جانبی تروریستها تجزیه و تحلیل می‌گردد.

۱. تروریسم علیه فضای سایبر

همان‌طور که از این عنوان پیداست، تروریستها کارزار خود را از دنیای فیزیکی به فضای سایبر انتقال داده‌اند که بدیهی است به دلیل قرار گرفتن در یک دنیای دیگر با شرایط و امکانات خاص و منحصر به فرد، سلاحها و اهداف نیز ماهیت و کارکرد متمایزی از دنیای فیزیکی پیدا می‌کنند. یکی از بهترین تعابیر برای این کارزار سایبری که معادل مفهوم مضیق تروریسم سایبری می‌باشد، جنگ اطلاعات (Information Warfare) است: «مبارزه در جهت نظارت و کنترل بر فعالیتهای اطلاعاتی». حتی به عقیدهٔ برخی صاحب‌نظران، از جمله پروفسور دوروثی دنینگ (Dorothy Denning)، اگر جنگ اطلاعات جلوهٔ تهاجمی به خود بگیرد، چنانچه در قابلیت استفاده (Usability) و تمامیت (Integrity) اطلاعات یکی از طرفین خللی وارد شود، طرف دیگر برندهٔ این جنگ خواهد بود (وارن، همان: ۷).

این مسئله تا حدی جدی تلقی شده که کشورهای پیشرو در این عرصه، در حال تربیت سربازان سایبری (Cyber Soldier) مجهز به انواع سلاحهای الکترونیکی هستند تا برای تهاجم یا دفاع از آمادگی لازم برخوردار باشند (جانسون و دیگران، ١٣٨٤: ٢٥٣). اما با توجه به اینکه قرار است در این نوشتار تنها مسائل حقوقی این حوزه مورد بررسی قرار گیرد، این ابعاد به مجال دیگری موکول می‌گردد.

همچنین از آنجا که بحث تروریسم سایبری به دلیل نوظهور بودن فضای سایبر جدید

است و همانند تروریسم سالها موضوع تحقیق و مطالعه نبوده است، نمی‌توان انتظار داشت به آن اندازه تعاریف و تحلیلهای گوناگون موجود باشد. با این حال، برخی صاحب‌نظران مانند پروفسور دنینگ این تعریف را ارائه داده‌اند:

> تروریسم سایبری از همگرایی تروریسم و فضای سایبر به وجود آمده است. درک عمومی بر این است که به معنای تهاجمات و تهدید به تهاجمات غیرقانونی به رایانه‌ها، شبکه‌ها و اطلاعات ذخیره شده در آنها می‌باشد که به منظور ارعاب یا وادار کردن یک دولت یا مردم آن برای پیشبرد اهداف سیاسی یا اجتماعی صورت می‌گیرد. به علاوه، برای اینکه یک تهاجم تروریسم سایبری تلقی شود، باید منجر به اِعمال خشونت علیه اشخاص یا اموال گردد یا حداقل آن‌قدر خسارات وارد آورد که منجر به وحشت گردد. تهاجماتی که باعث فوت، آسیب جسمی، انفجار، تصادم هواپیماها، آلودگی آب یا لطمهٔ شدید اقتصادی می‌شوند، از جملهٔ این موارد هستند. تهاجمات شدید علیه زیرساختهای حیاتی می‌تواند اقدامات تروریستی سایبری تلقی شود که البته به میزان آثار آنها بستگی دارد. تهاجماتی که خدمات غیرضروری را قطع یا نهایتاً مزاحمت هزینه‌بری را ایجاد می‌کنند، تحت شمول این تعریف قرار نمی‌گیرند (Walker, 2006: 633).

همان‌طور که از این تعاریف برمی‌آید، تروریسم سایبری صرف، به اقدامات خشونت‌آمیز سایبری از سوی گروهی با ویژگیهای خاص اطلاق می‌شود که به اهداف مشخصی تعرض می‌کنند و ملاحظه گردید، تعمداً اقدامات تهاجمی با آثار جزئی از شمول آنها خارج شده‌اند. اقدامات تروریستی سایبری باید در حدی باشند که بتوان معادل جنگ اطلاعات را برای آنها به کار برد. جنگ اطلاعات یک اقدام تروریستی است که برای ایجاد اختلال یا آسیب‌رسانی یا قطع جدی ارتباطات طرح‌ریزی می‌شود. ممکن است لازم باشد سیستمهای رایانه‌ای، برای تهدید زندگی افراد، به طور مستقیم مورد تعرض قرار گیرند، مانند ایجاد اختلال در سیستمهای کنترل ترافیک هواپیما یا سوابق بیمارستان. اما اگر قرار است دیگر اقدامات مجرمانهٔ سایبری مانند نشر انواع ویروسهای رایانه‌ای، تهاجمات مانع خدمات (Denial of Service Attacks)، ارسال انواع بمبهای الکترونیکی از طریق پست الکترونیکی و بسیاری تعرضات الکترونیکی دیگر تحت شمول این تعریف قرار گیرد، لازم است دیگر مؤلفه‌های تشکیل دهندهٔ مفهوم تروریسم سایبری نیز جمع باشد. پیش از هر چیز باید هویت عامل این اقدامات مشخص گردد. ممکن است یک هکر (Hacker) عادی

که هرگز در جهت اهداف تروریستی مرتکب این اعمال نـشده شناسـایی گـردد. همچنـین اهدافی که به آنها تهاجم شده و میزان خـسارات وارد شـده نیـز از معیارهـای اصـلی ایـن تعریف هستند و باید مورد توجه قرار گیرند. برخی رخدادهای اخیر عبارت‌اند از:

در سال ۱۹۹۷، معترضان اسپانیایی با ارسال هزاران نامهٔ الکترونیکی به مؤسسهٔ ارتباطـات جهـانی (Institute for Global Communication)، باعث اشباع سیستم ارائه‌دهندهٔ خدمات اینترنتی مورد نظر و بسته شدن دیگر ترافیکها شدند. هدف از این کار، جلوگیری از میزبانی (Hosting) این مؤسسه از وب‌سایب Euskal Herria Journal وابسته به جنبش استقلال باسک بود.

در سال ۱۹۹۸، شورشیان تامیل با ارسال تعداد زیادی پیام الکترونیکی به سفارتخانه‌های سری‌لانکا، باعث اشباع آنها و از کار افتادنشان شـدند. در جریـان جنـگ کـوزوو در سـال ۱۹۹۹، حامیان صربستان وب‌سایتهای ناتو و دولت امریکا را مورد حمـلات مـانع خـدمات قرار دادند و خساراتی را به آنها وارد آوردند (Walker, 2006: 635).

اما شاید جالب‌ترین مثال به کرم رایانه‌ای نیمدا (Nimda) مربوط می‌شـود کـه بـه دلیـل تأثیرگذاری مخرب بالای آن و همچنـین برخـورداری از قابلیتهـای دیگـر، ماننـد ویـروس تروجان (Trojan Viruses)، به کرم چهارسر (Four Headed Worm) معـروف بـود. البتـه معروفیت این کرم رایانه‌ای بیشتر به زمان انتشار آن مربوط می‌شود کـه درسـت یـک هفتـه پس از واقعهٔ یازدهم سپتامبر ۲۰۰۱ منتشر شد و خسارات زیادی را به ویژه بـه سیـستمهای رایانه‌ای ایالات متحده، بریتانیا و هنگ‌کنگ وارد آورد. با این حـال، دادسـتان کـل امریکـا، جان اشکرافت (John Ashcroft) اظهار داشت دلیلی مبنی بر ارتباط این کـرم بـا حمـلات یازدهم سپتامبر در دست نیست (Hinde, 2001: 570).

۲. فضای سایبر در خدمت تروریسم

در گفتار دوم، با انواع مطلوبیتهای منحصر به فرد فضای سایبر که توجه تروریستها را به خود جلب کرده آشنایی اجمالی صورت گرفت. آنچه باعث شده این فضا تا این حد بـرای تروریستها کارآیی داشته باشد، به ماهیت اقداماتشان برمـی‌گـردد. در گفتـار اول، بـه تعبیـر برایان جنکینز از تروریسم و اینکه یک تئاتر است اشاره شد. هدف از این تعبیر این بود که تأکید شود بزرگ‌نمایی و انعکاس گـستردهٔ اقـدامات تروریـستی همپایـه و حتـی بیـشتر از ارتکابشان ارزش و اهمیت دارد. به عبارت دیگر، چنانچه مخاطبان یـک اقـدام تروریـستی،

پیام اصلی تروریستها را با همان میزان تأثیرگذاری مورد نظرشان دریافت نکنند، زحماتشان هدر خواهد رفت.

با توجه به اهمیت این موضوع، اکثر گروههای تروریستی به بهره‌برداریهای جانبی از فضای سایبر نیز روآورده‌اند و حتی بیش از آنکه به آن آسیب برسانند، جهت ارائهٔ نمایشی مؤثر از اقداماتشان، به نحو بهینه از آن بهره‌برداری می‌کنند. به طور کلی، چهار شاخهٔ اصلی از فضای سایبر که به خدمت تروریستها درآمده‌اند عبارت‌اند از: ۱. ارتباطات؛ ۲. پشتیبانی پرسنلی و لجستیکی؛ ۳. جمع‌آوری اطلاعات؛ و ٤. تبلیغات.

۱. ارتباطات: فضای سایبر از ابعاد مختلف، حوزهٔ ارتباطات را متحول کرده است. علاوه بر سرعت فوق‌العادهٔ مبادلهٔ انواع پیامهای ارتباطی الکترونیکی، ابزارهای پیشرفته‌ای در این فضا وجود دارد که نه تنها از افشای محتوای آنها جلوگیری می‌کند (برنامه‌های رمزنگاری) که امکان ردیابی مبدأ ارتباطات را نیز با مشکلات جدی مواجه می‌سازد. هم‌اکنون بعضی ابزارهای ناشناس‌کنندهٔ (Anonymizer) پیشرفته هستند که با تحریف آدرسهای IP، ارتباطات الکترونیکی و مسیر حرکتشان، تقریباً شناسایی مبدأ را غیرممکن می‌سازند (Thornburgh, 2004: 66).

در این زمینه، به نمونه‌های بسیاری می‌توان اشاره کرد. از جمله مهم‌ترین آنها که با واقعهٔ یازدهم سپتامبر ۲۰۰۱ نیز مرتبط است، ارتباطات الکترونیکی مبادله شده میان اعضای القاعده به ویژه زکریا موسوی است که FBI از این طریق وی را تحت تعقیب قرار داد (Walker, 2006: 636).

۲. پشتیبانی پرسنلی و لجستیکی: به این مزیت بارز در گفتار قبل اشاره شد. جلب حامیان و از آن مهم‌تر عضوگیری برای اقدامات تروریستی و همچنین تأمین مالی این اقدامات از جمله مهم‌ترین موارد قابل ذکر هستند. جالب توجه اینکه بعضی رهبران گروهها با بهره‌گیری از ارتباطات زندهٔ الکترونیکی، به تشویق افراد برای الحاق به آنها استفاده می‌کنند. برای مثال، شیخ عمر بکری محمد، رئیس سازمان المهاجرون، از محیطهای گپ اینترنتی برای جلب پشتیبانی سازمان خود و دیگر گروههای جهادی استفاده می‌کند (Walker, 2006: 638).

۳. جمع‌آوری اطلاعات: از آنجا که کمتر موضوعی از زندگی بشر باقی مانده که در

فضای سایبر بروز نیافته باشد، این فضا به یک منبع غنی از اطلاعـات بـرای طراحـی انـواع اقدامات تروریستی تبدیل شده است. راجع به هر موضوع، اطلاعات نسبتاً دقیقی را می‌توان به دست آورد؛ از امکانات دفاعی محل مورد نظر گرفته تا نـشانی و شـماره‌هـای شناسـایی افراد. اخیراً موتور جستجوی گوگل با ارائهٔ خدمات Google Earth تصاویر بسیار واضحی را از هر نقطهٔ این کرهٔ خاکی ارائه می‌دهد که بدیهی است می‌تـوان از آنهـا بـرای هرگونـه تحرکات تروریستی بهره‌برداری کرد. مثال جالب توجهی که می‌توان در این زمینه بیان کرد، راجع به محمد نعیم نورخان معروف به ابوطلحـه اسـت کـه در ژولای ۲۰۰٤ در پاکـستان دستگیر شد و محتوای کامپیوترش نشان می‌داد برای حمله به اهدافی مانند مؤسسات مـالی در لندن، نیویورک و نیوجرسی طرحهایی آماده شده بود (Walker, 2006: 639).

٤. تبلیغات (Propaganda): گزینه‌ای که بیش از همه مـی‌توانـد اهـداف تئـاتر تـرور را محقق گرداند، تبلیغات است. با اینکه دیگر گزینه‌ها، یعنی برقـراری ارتباطـات هماهنـگ و گسترده در سراسر جهان، جلب انواع کمکها و حمایتهای افراد از سراسر جهان و همچنـین گردآوری منسجم و از پیش طراحی شدهٔ اطلاعات، به نحو چشمگیری می‌تواند به انعکاس هرچه بهتر اهداف و اقدامات تروریستها کمک کند، اما جان‌مایهٔ اصلی این نمایش تبلیغـات است. به عبارت دیگر، انعکاس اقدامات تروریستها و حتی اطلاع‌رسانی به مخاطبـان راجـع به اهداف متعالی ترسیم شده، عمدتاً از این طریق امکان‌پذیر است. در این‌گونـه وب‌سـایتها همه نوع اطلاعات یافت می‌شود. از تبلیغ مرگ (Propaganda of the Deed) گرفته، یعنـی قتلهای انجام شده، به ویژه سر بریدن (Decapitation) افراد، تا تبیین اهداف و رویکردها و اقداماتی که در این زمینه انجام شده است.

فصل دوم. راهکارهای حقوقی مقابله با تروریسم سایبری

بی‌تردید معضل به واقع جهانی تروریسم که تقریباً تمامی دولتهـا و ملتهـا را بـه جنـگ طلبیده و همواره لطمات بالقوه و بالفعل گونـاگونی را بـه آنهـا وارد آورده، مـستلزم اتخـاذ تدابیر جدی است تا عـلاوه بـر مقابلـهٔ مـؤثر بـا سیاسـت‌گـذاران، برنامـه‌ریـزان و عوامـل تروریستی، از وارد آمدن لطمات جانی و مالی بسیار جلوگیری گردد.

یکی از منطقی‌ترین و صحیح‌ترین راهکارهای مقابله با تروریـسم کـه حتـی مـی‌توانـد

زیربنای شایسته‌ای برای دیگر راهکارها نیز باشد، بسترسازی حقوقی از طریق وضع قوانین و مقررات مورد نیاز است. با توجه به اینکه ماهیت اقدامات تروریستی مجرمانه است و در واقع قانون‌نویسان و قانونگذاران با یک پدیدهٔ مجرمانه مواجه‌اند، لذا بسترسازی حقوقی بر پایهٔ قوانین کیفری صورت می‌گیرد. همان‌طور که ملاحظه شد، قانونگذاری کیفری راجع به تروریسم، سابقه‌ای نسبتاً طولانی دارد. اما از آنجا که نتایج و عواقب این‌گونه اقدامات بسیار زیانبار و وحشتناک است، مراجع ذی‌صلاح تقریباً از همان ابتدا به دنبال پیشگیری از وقوع آنها بوده‌اند. زیرا با توجه به اهدافی که تروریستها دنبال می‌کنند، در خصوص بسیاری از آنها به هیچ وجه انواع ضمانت اجراهای سنگین کیفری، حتی اعدام، تأثیرگذار نیست و حتی می‌تواند موجب تشجیع و تحریک همراهانشان گردد. لذا با توجه به شرایط خاص حاکم بر این پدیدهٔ مجرمانه، اولین گزینهٔ کاملاً عاقلانه و منطقی، اتخاذ تدابیر پیشگیرانه از وقوع تروریسم است؛ هر چند اهمیت این مسئله نباید جایگاه ضمانت اجراهای کیفری را تحت‌الشعاع قرار دهد.

بر این اساس، در این فصل دو راهکار اساسی مقابله با تروریسم به عنوان پدیدهٔ مجرمانه مورد بررسی قرار می‌گیرد. ابتدا قانون‌گذاری و کلیهٔ مسائل راجع به آن و سپس راهکارهای پیشگیری از وقوع آن تشریح می‌گردند.

گفتار اول: قانونگذاری کیفری راجع به تروریسم سایبری

مقابلهٔ کیفری با پدیدهٔ مجرمانه تروریسم، فرایندی است که از دو رکن اصلی تشکیل شده است: ۱. حقوق جزای ماهوی (جرم‌انگاری)؛ و ۲. حقوق جزای شکلی (آیین دادرسی کیفری). در ادامه به بررسی هر یک از این ارکان می‌پردازیم.

۱. حقوق جزای ماهوی تروریسم سایبری

در خصوص پدیدهٔ تروریسم به عنوان یک پدیدهٔ مجرمانه، یک مانع بزرگ در این راه وجود دارد و آن اینکه اگر قرار است اقدامات تروریستی تحت شمول ضمانت اجراهای کیفری بعضاً سنگین و حتی جبران‌ناپذیری مانند اعدام قرار گیرند، باید تعاریف مشخص و دقیقی از آنها که عاری از هرگونه ابهام باشد، در قوانین کیفری انعکاس یابد.

با این حال، تمامی این مسائل زمانی به حد غایت مشکل می‌شوند که ضرورت ایجاب

کند در فضایی به اجرا درآیند که به بسیاری از مبانی و شیوه‌های اجرایی معمول آنها پایبند نیست. پیش از این در خصوص ویژگیهای منحصر به فرد فضای سایبر توضیحاتی داده شد. برای مثال قابلیت **مجازی‌سازی** (Virtualization) این امکان را فراهم آورده تا داده‌های الکترونیکی در قالب فرایندهای الکترونیکی، به جای اشخاص ادارهٔ امور را در دست گیرند که نمونهٔ بارز آن را در بانکداری الکترونیکی شاهد هستیم. همین مسئلهٔ به ظاهر ساده باعث شده تا مراجع کیفری تقلبات مالی الکترونیکی را بر عنوان مجرمانهٔ **کلاهبرداری** منطبق ندانند و قانونگذاران را مجبور کنند قوانین جدیدی را به تصویب برسانند، با این استدلال که عنصر **فریب** در آنها وجود ندارد و نسبت به سیستمها و برنامه‌های رایانه‌ای صدق نمی‌کند (عالی‌پور، ۱۳۸۳: ۲۱۰).

همچنین فرامرزی بودن فضای سایبر، صرف‌نظر از مسائل دشواری که در حوزهٔ آیین دادرسی کیفری به وجود آورده و در قسمت بعد به آن اشاره خواهد شد، قانونگذاران کیفری را نیز با چالشهایی جدی مواجه کرده است. طبق اصول اساسی کیفری، اصل بر اجرای قوانین جزایی در قلمرو سرزمینی کشورهاست، مگر موارد استثنایی که به آن تصریح شده باشد (مادهٔ ۳ قانون مجازات اسلامی، مصوب ۱۳۷۰). حال چگونه می‌توان این قوانین را در مورد جرائمی قابل اجرا دانست که به قلمرو سرزمینی محدود نیستند. علاوه بر این، زمانی دشواری چاره‌جویی راجع به این‌گونه مباحث محرز می‌گردد که ملاحظات اجتماعی، سیاسی، فرهنگی و اقتصادی کشورها برای جرم‌انگاری پدیده‌های خاص سایبری نیز مورد توجه قرار گیرد. برای مثال، طی سالهای اخیر، یکی از معضلاتی که کشورهای بهره‌بردار از فضای سایبر با آن دست و پنجه نرم می‌کنند و حتی حوزه‌های کلان سیاست‌گذاری فناوری اطلاعات و ارتباطات الکترونیکی را تحت‌الشعاع خود قرار داده (کاشیان، ۱۳۸٤: ۵۸)، **پیامهای ناخواستهٔ الکترونیکی** (Unsolicited Electronic Message) یا همان **اسپم** (SPAM) است. اما تا کنون تنها چهار کشور اقدام به جرم‌انگاری این معضل کرده‌اند (OECD, 2005: 36). این عدم اجماع بر سر عناوین مجرمانه و به تبع آن جرم‌انگاری متحدالشکل برای مبارزه با جرائم سایبری، به خوبی در اسناد بین‌المللی، منطقه‌ای و بین‌الدولی‌ای که تا کنون تدوین و منتشر شده نیز مشهود است. بارزترین آن، کنوانسیون اروپایی جرائم سایبر (European Convention on Cybercrime, 2001) است. با اینکه

اکثریت اعضای این کنوانسیون را کشورهای عضو شورای اروپا تشکیل می‌دهند و آنها نظام حقوقی مشابهی دارند، اما تنها نُه عنوان مجرمانه از بیش از دویست عنوان مجرمانهٔ سایبری که تا کنون شناسایی شده، در این سند منعکس شده و از میان این نُه عنوان نیز تنها **هرزه‌نگاری کودکان** (Child Pornography) با **حق شرط** (Reservation) مواجه نشده است (عالی‌پور، ۱۳۸۵: ۱۶).

به این ترتیب، به نظر می‌رسد تکلیف عناوین مجرمانهٔ بسیار خاص و در عین حال حساسی مانند تروریسم سایبری روشن شده باشد. البته برخی کشورها سعی کرده‌اند به نحوی این حوزه را فتح باب کنند. برای مثال، در بخش اول قانون تروریسم بریتانیا، مصوب ۲۰۰۰ (United Kingdom Terrorism Act; 2000) چنین آمده است:

۱. در این قانون، تروریسم به معنای ارتکاب یا تهدید به ارتکاب اعمالی است که: الف. تحت شمول بند ۲ قرار گیرند؛ ب. ارتکاب یا تهدید به ارتکاب به منظور تأثیرگذاری بر دولت یا ارعاب مردم یا بخشی از آنها باشد؛ و پ. ارتکاب یا تهدید به ارتکاب به منظور پیشبرد اهداف سیاسی، مذهبی یا ایدئولوژیکی باشد. ۲. اعمالی که تحت شمول این بند قرار می‌گیرند، عبارت‌اند از: ... ث. اقداماتی که برای ایجاد اختلال یا قطع جدی یک سیستم الکترونیکی ارتکاب می‌یابند (Walker, 2006: 629).

در پایان، شایان ذکر است با وجود اینکه کشورها هنوز به طور گسترده به تروریسم سایبری در مفهوم خاص آن در قوانین جزایی نپرداخته‌اند، اما ماهیت این اقدام که همانا تخریب یا آسیب‌رسانی به داده‌ها و سیستمهای رایانه‌ای است، از جمله مصادیق اولیهٔ جرائم رایانه‌ای به شمار می‌روند که اغلب راجع به آن قوانین کیفری را به تصویب رسانده‌اند و به نظر می‌رسد با لحاظ کیفیات مشدده، فعلاً می‌تواند پاسخگوی نیازهای تقنینی باشد، ولی در آیندهٔ نزدیک با روند رو به رشد حملات تروریستی سایبری در سراسر جهان عملاً نیاز به قوانین خاص بروز خواهد یافت. در مورد جرائمی که به تمامیت داده‌ها و کارکرد سیستمهای رایانه‌ای لطمه وارد می‌آورند، کنوانسیون جرائم سایبر چنین اشعار می‌دارد:

مادّهٔ ٤. ایجاد اختلال در داده‌ها: ۱. هر یک از اعضا باید به گونه‌ای اقدام به وضع قوانین و دیگر تدابیر کنند که در صورت لزوم بر اساس حقوق داخلی خود، هر نوع صدمه زدن، پاک کردن، خراب کردن، تغییر یا قطع داده‌های رایانه‌ای را که به طور عمدی و بدون حق انجام می‌شود جرم‌انگاری کنند. ۲. اعضا می‌توانند حق جرم‌انگاری افعال مندرج در بند یک

را در جایی که صدمهٔ شدیدی وارد شده اعمال کنند. **مادّهٔ ۵. ایجاد اختلال در سیستمها:** هر یک از اعضا باید به گونه‌ای اقدام به وضع قوانین و دیگر تدابیر کنند که در صورت لزوم بر اساس حقوق داخلی خود، هر نوع ایجاد اشکال جدی عمدی و بدون حق را که در عملکرد سیستم رایانه‌ای در اثر وارد کردن، انتقال، صدمه زدن، پاک کردن، خراب کردن، تغییر یا متوقف کردن داده‌های رایانه‌ای به وجود می‌آید جرم‌انگاری کنند (گروه کارشناسان، ۱۳۸٤: ۱۷).

۲. حقوق جزای شکلی (آیین دادرسی کیفری)

اولین مسئله‌ای که به هنگام طرح مباحث کیفری باید در مورد آن تعیین تکلیف کرد، تعیین مرجع ذی‌صلاح قضایی است. در این زمینه، اولین قاعده‌ای که مورد توجه قرار می‌گیرد، صلاحیت دادگاه محل وقوع جرم (Location of Act) است (August, 2002: 536). رعایت این قاعده، در بسیاری موارد منجر به رعایت اصل سرزمینی کشورها در امور کیفری (Territoriality Nexus) نیز می‌شود. در مواردی هم که جرائمی حالت فرامرزی پیدا می‌کنند، قواعدی نسبتاً مورد اتفاق میان کشورها وضع شده تا در اعمال صلاحیت کیفری فرامرزی (Extraterritorial Jurisdiction) مشکل خاصی به وجود نیاید (European Committee on Crime Problems,1990: 9). اما در فضای سایبر، اولین و بدیهی‌ترین مسئله این است که چیزی به نام محل وقوع جرم معنا ندارد. در جرمی مانند نشر ویروس یا تصاویر مستهجن کودکان، هر سیستم رایانه‌ای در سراسر جهان می‌تواند محل وقوع جرم تلقی گردد. بالطبع هنگامی که نمی‌توان به این قاعدهٔ بدیهی تمسک کرد، مشکلات پیش روی دیگر قواعد محرز خواهد بود.

پس از صلاحیت کیفری، نوبت به فرایند اجرایی محاکم به همراه مجریان قانون برای تعیین تکلیف پرونده‌های مفتوح می‌رسد که عموماً از آن به عنوان **کشف علمی جرائم** یاد می‌شود و همان‌طور که شاهد هستیم، در اثر پیشرفت علوم در حوزه‌های مختلف، این شاخه از **علوم جنایی** نیز با تحولات شگرفی مواجه شده است. اما مسئله‌ای که فضای سایبر به طور خاص برای این شاخه به وجود آورده، به ماهیت کاملاً فنی آن مربوط می‌شود. مسلماً برای شناسایی عوامل جرمی که در فضای سایبر ارتکاب می‌یابد و به تبع اثبات جرم، باید وارد این فضا شد. لذا میزان قابلیت فنی مجریان قانون در شناسایی و

ردیابی آثار مجرمانهٔ الکترونیکی و کشف هویت مجرمان سایبری اهمیتی حیاتی دارد (Casey, 2001: 16). مهم‌ترین ثمرهٔ عملی این مسئله در **استنادپذیری ادلهٔ الکترونیکی** (Admissibility of Digital Evidence) ظاهر می‌شود.

با توجه به آسیب‌پذیری بالای داده‌های الکترونیکی، برای اینکه بتوان نزد محاکم به آنها به عنوان ادلهٔ محکمه‌پسند استناد کرد، مجریان قانون باید ضوابط پیچیده‌ای را رعایت کنند. البته وجود حساسیتهای خاص در مورد برخی حوزه‌های سایبری نیز مجریان قانون را با مشکلات بسیاری مواجه ساخته است. نمونهٔ بارز آن جمع‌آوری داده‌های شخصی و شنود ارتباطات الکترونیکی است که دغدغه‌های حقوق بشری بسیاری را برانگیخته است و به همین دلیل، در اسناد مربوط به این مسئله توجه ویژه‌ای شده است. برای مثال در مادهٔ ۱۵ کنوانسیون جرائم سایبر، از کشورهای عضو خواسته شده اقدامات این حوزه را با رعایت اسناد و قوانین حقوق بشری انجام دهند (گروه کارشناسان،۱۳۸٤: ۲۲).

همچنین برخلاف تصور عموم، فرامرزی بودن این فضا نه تنها کمکی به توسعهٔ ارتکاب عمل مجریان قانون نمی‌کند، بلکه در بسیاری موارد مجبورند برای جمع‌آوری داده‌های به سرعت فناپذیر رایانه‌ای از سیستمهای رایانه‌ای واقع در دیگر کشورها، تشریفات زمان‌بری را رعایت کنند که به هیچ‌وجه با شرایط حاکم بر این فضا سازگار نیستند. به دلیل وجود این‌گونهٔ مسائل حیاتی، در تمامی اسناد بین‌المللی و منطقه‌ای که تا به حال راجع به جرائم سایبر تدوین و منتشر شده، به مجریان قانون توجه ویژه‌ای شده است. نمونهٔ بارز آن کنوانسیون جرائم سایبر است که بیش از دوسوم مقررات آن به این حوزه اختصاص یافته است (Council of Europe, 2001: 21).

با توجه به این مسائل، به نظر می‌رسد اهمیت و جایگاه همکاری بین‌المللی برای مقابلهٔ کیفری با جرائم سایبر محرز شده باشد. تاکنون تلاشهای بسیاری برای همسو کردن کشورها صورت گرفته که باز هم نمونهٔ بارز آن کنوانسیون جرائم سایبر است. این سند، علاوه بر اینکه بخش مهمی از مقررات خود را به این حوزه اختصاص داده است، در پیشگفتار خود به صراحت اعلام می‌دارد:

... با اعتقاد به نیاز مبرم به یک سیاست جنایی مشترک به عنوان یک اولویت برای حمایت از جامعه در برابر جرائم سایبر، با اقداماتی از قبیل تصویب قوانین مناسب و

گسترش همکاریهای بین‌المللی و با آگاهی از دگرگونیهای اساسی‌ای که در اثر دیجیتالی شدن، همگرایی و ادامهٔ جهانی شدن شبکه‌های رایانه‌ای به وجود آمده است... (گروه کارشناسان، ۱۳۸٤: ١٤).

گفتار دوم: پیشگیری از وقوع تروریسم سایبری

برای اینکه اقدامات پیشگیرانه به طور سنجیده و صحیح به اجرا درآیند، لازم است سه رکن اصلی این پدیدهٔ مجرمانه بر اساس رهیافتهای جرم‌شناختی مطالعه و بررسی و مطابق نتایج به دست آمده، راهکارهای پیشگیرانهٔ مورد نیاز تدوین و اجرا گردند. این سه رکن عبارت‌اند از: ۱. تروریستهای سایبری؛ ۲. قربانیان اقدامات تروریستی سایبری؛ و ۳. فضای سایبر به عنوان بستر ارتکاب اقدامات تروریستی.

اما از میان الگوهای مختلف پیشگیری که به ویژه طی نیم قرن اخیر مورد نظریه‌پردازی و آزمون قرار گرفته‌اند، پیشگیری وضعی (Situational Prevention) و اجتماعی (Social Prevention)، به عنوان یکی از جامع‌ترین راهکارهای موفقیت‌آمیز پیشگیری از جرم مورد توجه قرار گرفته است (نجفی ابرندآبادی، ۱۳۸۰: ۷٤۸). کما اینکه برای پیشگیری از جرائم مهمی نظیر **جنایات سازمان‌یافتهٔ فراملی و فساد** اتخاذ و به ترتیب در **کنوانسیون‌های پالرمو (۲۰۰۰)** (United States Convention Against Corruption) **و مریدای (۲۰۰۳) سازمان ملل متحد** (United States Convention Against Transnational Organized Crime) بر آنها تأکید ویژه‌ای شده است (UNODC, 2004: 24).

به طور خلاصه، در پیشگیری اجتماعی، هدف، از بین بردن **انگیزهٔ مجرمانه** (Criminal Motivation) است و به همین دلیل، به آن پیشگیری بزهکارمحور (Criminal-based Prevention) گفته می‌شود. در اینجا راهکارهای اجتماعی، مانند رفع بیکاری و فقر که زمینه‌ساز شکل‌گیری انگیزه‌های مجرمانهٔ مالی و حتی قتل می‌شوند و همچنین راهکارهای تربیتی و آموزشی(Developmental-based Crime Prevention) برای کودکان، به عنوان آسیب‌پذیرترین گروه سنی، هم از لحاظ بزهکاری و هم از لحاظ بزهدیدگی، در دستور کار قرار می‌گیرند (نیازپور، ۱۳۸۲: ۱۳۸).

اما در پیشگیری وضعی، هدف، صیانت از بزهدیدگی بالقوه از طریق سلب فرصت (Opportunity) و یا ابزار (Tool) ارتکاب جرم است (Shinder, 2002: 353). بسیاری از

تدابیر امنیتی که در ساختمانها، اتومبیلها و نظایر آن به اجرا درمی‌آید یا اینکه از خرید و فروش انواع سلاحهای گرم و سرد جلوگیری می‌شود، در واقع پیشگیری وضعی از وقوع جرائم تبعی دنبال می‌گردد.

با توجه به این توضیحات اجمالی، به نظر می‌رسد نحوهٔ پیاده‌سازی تدابیر پیشگیرانهٔ اجتماعی و وضعی در فضای سایبر روشن شده باشد. اگر واقعیات و شرایط خاص حاکم بر این فضا به خوبی به کاربران آن، که عمدتاً قشر جوان و نوجوان جامعه هستند، منعکس شود، از شکل‌گیری و تحقق بسیاری از انگیزه‌های مجرمانه و در عین حال بزهدیدگی آنها پیشگیری خواهد شد. هم‌اکنون این مسئله تا حدی مورد توجه قرار گرفته که مباحث تخصصی تحت عنوان اخلاق سایبری (Cyber Ethics) از سوی صاحب‌نظران و سیاست‌گذاران این حوزه مطرح شده است (جلالی فراهانی، ۱۳۸۵: ٦٥).

با این حال، از آنجا که این فضا ماهیتی فنی دارد، دست‌اندرکاران بیشتر به دنبال اجرای تدابیر پیشگیرانهٔ وضعی فنی هستند که از نمونه‌های بارز آن می‌توان به انواع فیلترها (Filters) و تدابیر نظارتی (Monitoring Measures) اشاره کرد که البته ناکارآییهای این‌گونه ابزارها بر همگان محرز شده، اما به‌کارگیری آنها اجتناب‌ناپذیر است (جلالی فراهانی، ۱۳۸٤: ۱۳۳).

اما در خصوص کارآیی این تدابیر در مورد اقدامات تروریستی سایبری، روشن است که تدابیر پیشگیرانهٔ اجتماعی ماهیت تروریسم را هدف قرار می‌دهند و در این جهت می‌توانند از فضای سایبر به عنوان یک ابزار اطلاع‌رسانی و تبلیغاتی نیز استفاده کنند و البته تأکید ویژه‌ای بر این اقدامات در فضای سایبر داشته باشند. تدابیر پیشگیرانهٔ وضعی نیز عمدتاً بدون توجه به هویت مجرمان به کار می‌روند. برای مثال، هدف، پیشگیری از آلوده نشدن سیستمها به انواع ویروسها یا محتواهای مستهجن است و تفاوتی نمی‌کند مرتکب آن چه کسی است. البته برای برخی سیستمها که در زیرساختهای حیاتی مستقر هستند و عمدتاً مجرمانی نظیر تروریستها قصد تعرض به آنها را دارند، می‌بایست برنامه‌ریزیهای ویژه‌ای صورت گیرد. همچنین برای اینکه از دسترس کاربران به محتواهای ارسالی از سوی تروریستها جلوگیری شود، مانند انواع پیامهای تحریک‌کننده و مخل آسایش عمومی، می‌بایست فهرستهای سیاه یا سفید (Black & White Lists) فیلترها به نحوی تنظیم شود که تمامی حوزه‌های مربوط را شناسایی و دسترس‌ناپذیر کنند.

فصل سوم. وضعیت حقوقی ایران در برابر تروریسم سایبری

با توجه به وضعیت کنونی کشورمان، نه می‌توان فناوری اطلاعات و ارتباطات الکترونیکی را کنار گذاشت و به یک جامعهٔ عاری از آن تبدیل شد و نه امکان ریشه‌کنی هرگونه اقدام تروریستی علیه کشور وجود دارد. در نتیجه تنها گزینه‌ای که باقی می‌ماند، چاره‌جویی در خصوص رفع یا کاستن از تهدیدات یا عواقب اقدامات تروریستی سایبری در مفهوم موسع آن است که در ادامه اقدامات قانونی و مقرراتی در دو گروه مصوب و در شرف تصویب در دو حوزهٔ تروریسم و امنیت فضای سایبر بررسی خواهد شد.

گفتار اول: قوانین و مقررات مصوب یا در شرف تصویب در بارهٔ تروریسم

شایان ذکر است قانونگذار ما با این مفهوم بیگانه نیست و با اینکه تاکنون قانون خاصی به تصویب نرسانده، اما می‌توان در لابه‌لای بعضی قوانین کیفری موجود نمونه‌هایی را ملاحظه کرد که نمونهٔ بارز آن مادّهٔ ٦٨٧ قانون مجازات اسلامی مصوب ١٣٧٠ است. هرچند این مقررهٔ قانونی عام است و تنها اقدامات تروریستی را دربرنمی‌گیرد. لذا نمی‌تواند مبنای مناسبی برای مقابلهٔ جدی و اختصاصی با معضل تروریسم باشد. به همین دلیل، در سال ١٣٨٢ لایحه‌ای با عنوان «لایحهٔ مبارزه با تروریسم» در دولت هشتم تنظیم و به مجلس شورای اسلامی ارائه گردید که تا کنون به دلایل نامعلومی مسکوت مانده است.

همچنین کشورمان به عنوان یکی از اعضای سازمان ملل متحد، تا کنون به پنج سند از اسناد مصوب این سازمان راجع به تروریسم پیوسته و مطابق آنها تعهداتی را پذیرفته است، ولی هنوز هیچ یک از آنها جنبهٔ قانونی نیافته‌اند. البته چهار سند راجع به تروریسم هوایی است. سازمان کنفرانس اسلامی نیز در مورد تروریسم در سال ١٩٩٩ کنوانسیون مبارزه با تروریسم بین‌المللی را به تصویب رسانده است (حکیمی‌ها، ١٣٨٥: ٤٢١).

گفتار دوم: قوانین و مقررات مصوب یا در شرف تصویب راجع به امنیت فضای سایبر

همان‌طور که ملاحظه شد، تروریسم، امنیت فضای سایبر یا به عبارت بهتر امنیت اطلاعات الکترونیکی و زیرساختهای سخت‌افزاری و نرم‌افزاری این فضا را هدف قرار داده است. لذا باید قوانین و مقررات این حوزه در جهت ساماندهی امنیت آن و رفع هرگونه

تهدید از آن باشد. در این زمینه به سه سند قانونی با ماهیتهای متفاوت اشاره می‌گردد:

۱. قانون برنامهٔ چهارم توسعهٔ اقتصادی، اجتماعی و فرهنگی کشور، مصوب ۱۳۸۳: در این قانون بر حفظ امنیت زیرساختهای حیاتی و همچنین تأمین امنیت فضای تبادل اطلاعات تأکید ویژه‌ای شده است. در این میان، مادهٔ ٤٤ به شکل دقیقی به موضوع این نوشتار پرداخته و سوای اینکه به شکل هوشمندانه میان تأمین زیرساخت فناوری اطلاعات و ارتباطات الکترونیکی، یعنی مراکز دادهٔ اینترنتی و امنیت فضای تبادل اطلاعات (نام معادل فضای سایبر) رابطه برقرار کرده، راهکارهای اجرایی اصولی و اساسی آن را نیز پیش‌بینی کرده که عبارت است از سند **افتا** (امنیت فضایی تبادل اطلاعات) که در ذیل خواهد آمد. این مادّه اشعار می‌دارد:

> دولت موظف است به منظور استقرار جامعهٔ اطلاعاتی و تضمین دسترس گسترده، امن و ارزان شهروندان به اطلاعات مورد نیاز اقدامهای ذیل را به عمل آورد: ... ج. تهیه و تصویب سند راهبردی برقراری امنیت در فضای تولید و تبادل اطلاعات کشور در محیطهای رایانه‌ای حداکثر تا پایان سال اول برنامهٔ چهارم.

۲. سند راهبردی امنیت فضای تبادل اطلاعات، مصوب ۱۳۸٤: همان‌طور که در بند ج مادّهٔ ٤٤ قانون برنامه چهارم توسعه ملاحظه شد، دولت مکلف شده بود تا پایان سال اول برنامه، سند راهبردی برقراری امنیت در فضای تولید و تبادل اطلاعات کشور در محیطهای رایانه‌ای را تهیه کند و به تصویب برساند. ماحصل اقدامات صورت گرفته در شورای عالی امنیت فضای تبادل اطلاعات کشور به ریاست معاون اول رئیس جمهور، در خردادماه ۱۳۸٤ در قالب این سند و اسناد تابعهٔ آن، به ویژه سند مشروح، منتشر گردید. در این سند که بر پایهٔ سیاست‌گذاریهای کلان کشور تدوین شده است، چشم‌انداز، خط مشیهای کلان، اهداف کلان، راهبردها و اقدامات به تفصیل مورد توجه قرار گرفته است. در حوزهٔ اهداف کلان، مؤلفهٔ چهارم به حفظ زیرساختهای حیاتی کشور در مقابل حملات الکترونیکی اختصاص یافته است که در همین عرصه راهبرد اول امن‌سازی زیرساختهای حیاتی کشور در قبال حملات الکترونیکی در نظر گرفته شده است (شورای عالی امنیت فضای تبادل اطلاعات کشور، ۱۳۸٤: ۳).

۳. مصوبهٔ شورای عالی انقلاب فرهنگی در خصوص مقررات و ضوابط شبکه‌های اطلاع‌رسانی رایانه‌ای، مصوب ۱۳۸۰: پیرو دستور مقام معظم رهبری، این شورا در آن سال به تدوین و تصویب این مصوبه پرداخت. این سند برخلاف اسناد فوق، راجع به امنیت فضای سایبر نیست، بلکه می‌توان از آن مفاد راجع به تئاتر ترور را بهره‌برداری کرد و اصولاً

ماهیتی پیشگیرانه دارد. با وجود آشفتگی عجیبی که بر این سند حاکم است، بـه ترتیـب در مواد ٦ و ٧ آیین‌نامهٔ واحدهای ارائه‌کنندهٔ خدمات اطـلاع‌رسـانی و اینترنـت، رسـا (ISP) و آیین‌نامهٔ دفاتر خدمات حضوری اینترنت (Coffee Net) چنین آمده است:

... مادّهٔ ٦. تولید و عرضه موارد زیـر توسـط رسـاها (ISP) و کـاربران ممنـوع مـی‌باشـد: ٦ـ١. نشر مطالب الحادی و مخالف موازین اسلام؛ ٦ـ٢. اهانت به دین اسـلام و مقدسـات آن؛ ٦ـ٣. ضدیت با قانون اساسی و هرگونه مطلبی که استقلال و تمامیت ارضـی کـشور را خدشه‌دار کند؛ ٦ـ٤. اهانت به رهبری و مراجع مسلّم تقلید؛ ٦ـ٥. تحریف یا تحقیـر مقدسـات دینی، احکام مسلّم اسلام، ارزشهای انقلاب اسلامی و مبانی تفکر سیاسی امـام خمینـی؛ ٦ـ٦. اخلال در وحدت و وفاق ملی؛ ٦ـ٧. القـای بـدبینی و ناامیـدی در مـردم نـسبت بـه مشروعیت و کارآمدی نظام اسلامی؛ ٦ـ ٨. اشاعه و تبلیـغ گروههـا و احـزاب غیرقـانونی؛ ٦ـ٩. انتشار اسناد و اطلاعات طبقه‌بندی شده دولتی و امور مربوط به مسائل امنیتی، نظامی و عفت عمومی؛ و.... مادّهٔ ٧ـ تولید و عرضهٔ موارد زیر توسط شبکه‌های انتقـال اطلاعـات رایانه‌ای ممنوع می‌باشد: .... ٧ـ١١. ترویج ترور، خشونت و آموزش ساخت مواد تخریبـی از قبیل مواد محترقه و یا منفجره.

اما در میان قوانین در شرف تصویب راجع به این حـوزه، مـی‌تـوان بـه **لایحـهٔ جـرائم رایانه‌ای** اشاره کرد که از سوی قوهٔ قضاییه تهیـه شـده و در مجلـس شـورای اسـلامی در شرف تصویب نهایی است. شایان ذکر است، به هنگام تـدوین مـواد پیـشنهادی راجـع بـه جرائم رایانه‌ای در قوهٔ قضاییه، برخی کارشناسان پیشنهادهایی راجع به اختصاص یک مـادّه به تروریسم سایبری مطرح کردند که با توجیه مبتلابه نبودن در دستور کـار قـرار نگرفـت. با این حال، بخش دوم لایحه با عنوان جرائم و مجازاتها، مواد مناسـبی راجـع بـه **تخریـب و ایجاد اختلال در داده‌ها و سیستمهای رایانه‌ای و ممانعت از دستیابی** پیش‌بینی کرده است.

همچنین با عنایت به ضرورت تدوین مقررات شکلی خاص بـرای ایـن حـوزه، بخـش سوم با عنوان آیین دادرسی، مباحث راجع به الف) صلاحیت کیفری؛ ب) جمـع‌آوری ادلـهٔ الکترونیکی که خود مشتمل بر ١. نگهداری داده‌های ترافیک و اطلاعات کاربران، ٢. حفـظ فوری داده‌های رایانه‌ای ذخیره شده، ٣. ارائهٔ داده، ٤. تفتیش و توقیف داده‌ها و سیـستمهای رایانه‌ای و مخابراتی و ٥. شنود محتوای ارتباطات رایانـه‌ای اسـت؛ پ) اسـتنادپذیری ادلـهٔ الکترونیکی؛ ت) آیین‌نامه‌های مربوط؛ و ث) همکاریهای بین‌المللی را دربرگرفته است.

نتیجه‌گیری و پیشنهادها

آنچه تلاش شد در این مختصر نوشتار تبیین و بر آن تأکید گردد، وضعیت کشورمان در برابر یک پدیدهٔ شوم و ناگزیر است؛ ناگزیر از آن جهت که نه امکان کنار گذاشتن فناوری اطلاعات و ارتباطات الکترونیکی و نه سرکوبی یک‌شبهٔ تمامی گروههای تروریستی وجود دارد. بدتر اینکه روز به روز از دو جهت این‌گونه تهدیدات جدی‌تر می‌شوند: از یک سو گروههای تروریستی از آمادگی بیشتری برای وارد آوردن لطمات سهمگین برخوردار می‌شوند و از سوی دیگر، دشمنان به بهانه و اتهام اینکه ما تنها یا بزرگ‌ترین کشور حامی تروریسم هستیم، خود را برای یک رویارویی تمام عیار و مقابله به مثل سایبری آماده می‌کنند. لذا از اینکه تحت چنین شرایطی تا به حال به آن آماده‌باش سایبری (Cyber Vigilance) لازم دست نیافته‌ایم، خسارات بسیاری را متحمل شده و فرصتهای بسیاری را هم از دست داده‌ایم.

بدیهی است برای حل این معضل باید راهکارهای گوناگون اساسی و زیربنایی در حوزه‌های مختلف طرح‌ریزی شود. آنچه در اینجا مورد تأکید قرار گرفته، بسترسازی حقوقی از منظر حقوق کیفری و جرم‌شناسی است. هرچند باید در این زمینه به یک نکتهٔ اساسی توجه داشت و آن اینکه از آنجا که کلیهٔ راهکارهای مبارزه با تروریسم به طور اعم، و مبارزه با تروریسم سایبری به طور اخص، با یکدیگر ارتباط دارند و بر یکدیگر تأثیرگذارند، لازم است پیش از هر چیز راهبردهای کلان مبارزه با تروریسم با توجه به مصالح و مقتضیات داخلی و عنایت به شرایط بین‌المللی تدوین شود و زمینهٔ اجرای گستردهٔ آن فراهم گردد تا تحقق این‌گونه اقدامات بنیادین میسر گردد.

ضرورت سیاست‌گذاری کلان در این حوزه، زمانی عینیت بیشتری می‌یابد که دریابیم تروریسم از آن ماهیت محدود چند دههٔ پیش خود خارج شده و با به خدمت گرفتن فناوریهای نوین گوناگون، نظیر فضای سایبر، انرژی هسته‌ای، مواد بیولوژیکی و شیمیایی و مانند آن، حوزه‌های بین رشته‌ای را با چالش جدی مواجه ساخته است. عدم توجه به این مسئلهٔ بسیار مهم باعث می‌شود قوانین و مقرراتی که به طور مجزا در هر یک از این حوزه‌ها به تصویب می‌رسند، برای مثال قوانین و مقررات راجع به امنیت فضای سایبر از یک سو و قوانین و مقررات مبارزه با تروریسم از سوی دیگر، نتوانند آن رابطهٔ لازم و بایستهٔ را با یکدیگر برقرار کنند و عملاً نتیجهٔ مورد انتظار محقق نگردد.

منابع

الف. فارسی

۱. برنر، سوزان، *قانون نمونهٔ آئین پی‌جویی جرایم سایبر*، ترجمهٔ امیرحسین جلالی فراهانی، معاونت حقوقی و توسعهٔ قضایی قوهٔ قضائیه، ۱۳۸۲.

۲. جانسون، استوارت، ای و دیگران، *چالشهای نوین، ابزارهای نوین برای تصمیم‌گیری دفاعی*، ترجمهٔ محمدجواد زنگنه و کاظم غریب‌آبادی، ستاد مشترک سپاه پاسداران انقلاب اسلامی (معاونت عملیات)، چاپ اول، ۱۳۸٤.

۳. جلالی فراهانی، امیرحسین، *امکان‌سنجی قاعده‌مندسازی فیلترینگ (به عنوان یک اقدام پیشگیرانه از جرایم رایانه‌ای)*، مرکز تحقیقات، مطالعات و سنجش برنامه‌ای ادارهٔ کل مطالعات رسانه و ارتباطات صدا و سیما، شمارهٔ ۱۳۱، ۱۳۸٤.

٤. جلالی فراهانی، امیرحسین، «پول‌شویی الکترونیکی»، فصلنامهٔ تخصصی فقه و حقوق، شمارهٔ ٤، ۱۳۸٤.

۵. جلالی فراهانی، امیرحسین، «پیش‌گیری وضعی از جرائم سایبر در پرتو موازین حقوق بشر»، *فصلنامهٔ تخصصی فقه و حقوق*، شمارهٔ ٦، ۱۳۸٤.

٦. جلالی فراهانی، امیرحسین، پیشگیری *اجتماعی از جرایم سایبری: راهکاری اصولی برای نهادینه‌سازی اخلاق سایبری*، مرکز تحقیقات مخابرات، دومین مقالهٔ برگزیده همایش اخلاق و فناوری اطلاعات، آذرماه ۱۳۸۵.

۷. جینا دی آنجلیز، *جرایم سایبر*، ترجمهٔ سعید حافظی و عبدالصمد خرم‌آبادی، دبیرخانهٔ شورای عالی اطلاع‌رسانی، ۱۳۸۳.

۸. حکیمی‌ها، سعید، *تروریسم در حقوق ایران و اسناد بین‌المللی*، پایان‌نامهٔ دورهٔ دکتری حقوق کیفری و جرم‌شناسی، دانشکدهٔ علوم انسانی دانشگاه تربیت مدرس، به راهنمایی دکتر محمدجعفر حبیب‌زاده، سال تحصیلی ۸۵-۱۳۸٤.
۹. دزیانی، محمدحسن، *جزوهٔ آموزشی حقوق سایبر و جرایم سایبری*، جلد اول، ۱۳۸٤.
۱۰. شورای عالی امنیت فضای تبادل اطلاعات کشور، *متن و مشروح سند راهبردی امنیت فضای تبادل اطلاعات کشور*، خردادماه ۱۳۸٤.
۱۱. عالی‌پور، حسن و جلالی فراهانی، امیرحسین، *قانون جرایم رایانه‌ای «خلاءها و ضرورت‌ها»*، مرکز پژوهشهای مجلس شورای اسلامی، شمارهٔ ۷۸۸٤، ۱۳۸۵.
۱۲. عالی‌پور، حسن، «کلاهبرداری رایانه‌ای»، *مجلهٔ پژوهشهای حقوقی*؛ مؤسسهٔ مطالعات و پژوهش‌های حقوقی شهر دانش، شمارهٔ ٦، ۱۳۸۳.
۱۳. کاشیان، علیرضا و شریفی، احمد و جلالی فراهانی، امیرحسین، *راهبری اینترنت (مشارکت فراگیر)*، دبیرخانهٔ شورای عالی اطلاع‌رسانی، ۱۳۸٤.
۱٤. گروه کارشناسان؛ *کنوانسیون جرایم سایبر و گزارش توجیهی آن*، مرکز پژوهشهای مجلس شورای اسلامی، شمارهٔ ۷٦٤٦، بهمن‌ماه ۱۳۸٤.
۱۵. نجفی‌ابرندآبادی، علی‌حسین و هاشم‌بیگی، حمید، *دانشنامهٔ جرم‌شناسی*، انتشارات دانشگاه شهید بهشتی، ۱۳۷۷.
۱٦. نجفی ابرندآبادی، علی‌حسین، *تقریرات درس جرم‌شناسی*، تنظیمی محمدعلی بابایی، دورهٔ دکتری دانشگاه تربیت مدرس، نیم‌سال نخست ۸۰-۱۳۷۹.
۱۷. نیازپور، امیرحسن، «*پیش‌گیری از بزهکاری در قانون اساسی و لایحه پیشگیری از وقوع جرم*»، *مجلهٔ حقوقی دادگستری*؛ شمارهٔ ٤۵، ۱۳۸۲
۱۸. وارن، ماتئو و هاجینسون، ویلیام، «*تروریسم شبکه‌ای*»، ترجمهٔ غلامرضا رفعت‌نژاد، پژوهشکدهٔ مطالعات راهبردی، شمارهٔ ۵۱۲، ۱۳۸۲.

ب. لاتین

19. August Ray; International Cyber-Jurisdiction: A Comparative Analysis; *American Business Law Journal;* 2002.
20. Casey, Eoghan; *Digital Evidence and Computer Crime;* Academic Press; 2001.

21. Council of Europe; Explanatory Report to the Convention on Cyber Crime; (ETS no.185); 2001.
22. Desouza, Kevin c. & Tobin Hensgen; Semiotic Emergent Framework to Address the Reality of Cyber-terrorism; *Technological Forecasting & Social Change;* 70 (2003).
23. E. Denning, Dorothy; Activism, Hacktivism, and Cyber-terrorism: The Internet as a Tool For Influencing Foreign Policy; Nautilus Institute; fall 1999.
24. European Committee on Crime Problems (Council of Europe); Extraterritorial Criminal Jurisdiction; Strasbourg; 1990
25. Hancock, Bill; Cyber-tracking, Cyber-terrorism; *Computers and Security*; Volume 20; Number 7; 2001.
26. Hancock, Bill; Cyber-tracking, Cyber-terrorism; *Computers and Security*; Volume 20; Number 7; 2001.
27. Hinde, Stephen; Incalculable Potential for Damage by Cyber Terrorism: *Computers And Security;* vol. 20; Number 7; 2001.
28. OECD; DSTI/CP/ICCP/SPAM (2005)10/FINAL.
29. Shinder, Debra Littlejohn; Scene of the Cyber Crime, *Computer Forensics Hand Book;* Syngress Publication; 2002.
30. Thornburgh, Dick & S. Lin Herbert, Editors; Youth, Pornography and the Internet; National Academy Press; 2004.
31. United Nations Office on Drugs and Crime; the Global Program against Corruption; UN Anti-Corruption Toolkit; Third Edition; Vienna; September 2004.
32. U.S. Army TRADOC; A Military Guide to Terrorism in the Twenty-first Century; 2004.
33. Walker, Clive; Cyber-terrorism: Legal Principle and Law in the United Kingdom; Penn State Law Rev.; 110, no 3 wint 2006.