سایبر تروریسم:
شکل نوینی از ترور علیه منافع ملی

عنایت الله یزدانی *
فرزانه مرادی **
طیبه قنواتی ***

چکیده

تروریسم پدیده‌ی جدیدی نیست، بلکه از جمله پدیده‌هایی است که همزاد با بشر بوده و با به کارگیری خشونت علیه اشخاص، دولت‌ها و گروه‌ها برای پیشبرد زورمدارانه اهداف سیاسی یا عمومی به یکی از تهدیدات مهم بین‌المللی تبدیل شده است. در جهان معاصر، این پدیده به سبب پیوند با فناوری‌های نوین اطلاعاتی و ارتباطاتی، به یک گرفتاری راهبردی تبدیل شده و توانسته است گروه‌های کوچک، اما با ساختارهای پیچیده را به بازیگران برجسته در پهنه بین‌المللی تبدیل نماید. سایبر تروریسم[1] با هدف از کار

---

* دانشیار روابط بین‌الملل، گروه علوم سیاسی دانشگاه اصفهان (yazden2006@yahoo.com).
** کارشناس ارشد روابط بین‌الملل دانشگاه اصفهان.
*** کارشناس ارشد روابط بین‌الملل دانشگاه اصفهان.

تاریخ دریافت: ۱۳۹۱/۷/۹ **تاریخ پذیرش: ۱۳۹۲/۶/۶**
فصلنامهٔ پژوهش‌های روابط بین‌الملل، دورهٔ نخست، شمارهٔ سیزدهم، پاییز ۱۳۹۳، صص ۳۶-۹.

1. Cyberterrorism

انداختن عملیات زیرساخت‌های بحرانی یک کشور انجام می‌شوند که با توجه به رشد روز افزون تکنولوژی و ویژگی‌های منحصر بفرد فضای سایبر، تمامی دولت‌ها را با چالش‌های جدیدی روبه‌روکرده است. سؤال اصلی نوشتار این است که با توجه به در دسترس و منحصر بفرد بودن فضای سایبر، چگونه می‌توان بر تهدیدات سایبر تروریسم علیه منافع دولت‌ها فائق آمد؟ فرضیه نوشتار در پاسخ به سؤال اصلی این است که در عصر جدید با پیشرفت تکنولوژی و فناوری با تهدیدات جدیدی روبه‌رو شده‌ایم که دیگر نمی‌توان مانند گذشته امنیت ملی را تنها در محدوده مرزهای داخلی یک کشور نگاه کرد. امروزه مهاجمان تنها با در دست داشتن یک دستگاه رایانه، تهدیدی برای منافع یک کشور محسوب می‌شوند. چنین خطر نافذی، تمامی برداشت‌های رایج و سنتی از مفهوم امنیت ملی را زیر سوال برده است. مقاله به روش توصیفی- تحلیلی و با ابزار کتابخانه به رشته تحریر در آمده است.

واژه‌های کلیدی: *سایبر تروریسم، تروریسم، فضای سایبر، قدرت نرم، منافع ملی.*

مقدمه

امروزه با انقلاب اطلاعات و فناوری ارتباطات، که منجر به تغییرات بنیادی در حوزه‌های مختلف زندگی بشر گردیده، عصرحاضر به نام «عصراطلاعات» نام گرفته است، چرا که ماهیت علوم را اطلاعات تشکیل می‌دهد، عنصری که به دلیل اهمیت بسیار زیادش، عصرحاضر به آن نام شهرت یافته است. تا قبل از ظهور اینترنت، شاید واژه تروریسم، صرفا کشت و کشتار به وسیله بمب گذاری و اسلحه گرم و سایر سلاح‌ها و روش‌های خشونت بار را تداعی می‌کرد، اما امروزه با گسترش رسانه‌ها و وسایل ارتباطی، با نوع جدیدی از تروریسم روبه‌رو می‌شویم که با بهره‌گیری از ابزار برای تغییرنگرش، ایجاد بدبینی، موضع‌گیری‌های هیجانی، تغییرآداب و رسوم، تغییردرارزش‌ها وهنجارها، پشت پا زدن به میراث فرهنگی، کمرنگ نمودن معنویات، حمله به شخصیت‌ها و نظام‌های سیاسی، متمایل کردن دیگران به شیوه‌ها، روش‌ها، ارزش‌ها، هنجارها، دین و مکتب خود وغیره، ازاصول اساسی افراد گروه‌های نظام حکومتی تروریست می‌باشد

بر پایه فرهنگ علوم سیاسی آکسفورد، تروریسم اصطلاحی است که بر سر تعریف آن توافقی میان حکومت‌ها یا تحلیلگران دانشگاهی وجود ندارد، اما همچنان به شیوه‌های گوناگون و با برداشتی منفی برای بیان اقدامات خشونت‌آمیز «گروه‌های فرودولتی خودساخته» با انگیزه‌ها و اهداف سیاسی همراه با ایجاد ترس و وحشت بر ضد جان افراد به‌کار می‌رود (پیروزان، ۸۰: ۱۳۸۸). تروریسم از واژه«ترور» به معنای ترس و وحشت گرفته شده است و در عربی معاصر از لغت ارهاب برای معادل آن استفاده می‌شود (توکلی، ۱۲۶: ۱۳۸۶).

این پدیده مخرب در سطوح مختلفی رخ می‌دهد. ابتدا؛ در سطح فردی ترور،

اتفاقاتی که رخ می‌دهد بیشتر جنبه حسابرسی شخصی داشته و طرفین درگیر در آن دو یا چند نفر بیشتر نمی‌باشند.گاهی اوقات فقر فرهنگی- اجتماعی و همچنین فقر اقتصادی دلیل بارز اقدامات تروریستی در این سطح می‌باشد. سپس؛ در سطح ملی، طیف وسیعتری از افراد و گروه‌ها را در خود درگیر می‌سازد. در نهایت؛ در سطح بین‌المللی، حداقل بیش از سه کشور درگیر حادثه تروریستی هستند. در این سطح می‌توان از دو نوع ترور صحبت به میان آورد. یکی «تروریسم بین‌المللی دولتی»، و دوم «تروریسم بین‌المللی غیردولتی» که توسط اشخاص غیردولتی در سطح بین‌المللی انجام می‌پذیرد. در نوع اول، که تروریسم دولتی خارجی نیز نام دارد، ترور یکی از ابزارهای سیاست خارجی دولت‌های تندرو است. همچنان که هافمن اظهار داشته است: «دولت‌ها با به کارگیری پنهان نیروهای انسانی آماده به خدمت به عنوان جنگ افزارهای مکانیکی یا نیروهای غیر رزمنده، قادرند با صرف کمترین هزینه، موجودیت سیاسی هدف را تحت تأثیر و یا در معرض خطر جدی قرار دهند» (Shultz: 2008,2)

امروزه با انقلاب اطلاعات و فناوری ارتباطات، که منجر به تغییرات بنیادین در حوزه‌های مختلف زندگی بشر گردیده، عصر حاضر به نام «عصر اطلاعات» نام گرفته است، چرا که ماهیت علوم را اطلاعات تشکیل می‌دهد، عنصری که به دلیل اهمیت بسیار زیادش، عصر حاضر به آن نام شهرت یافته است. تا قبل از ظهور اینترنت، شاید واژه تروریسم، صرفاکشت وکشتار به وسیله بمب‌گذاری و اسلحه گرم و سایر سلاح‌ها و روش‌های خشونت بار را تداعی می‌کرد، اما امروزه با گسترش رسانه‌ها و وسایل ارتباطی، با نوع جدیدی از تروریسم روبه‌رو می‌شویم که با بهره‌گیری تام از ابزار برای تغییر نگرش، ایجاد بدبینی، موضع‌گیری‌های هیجانی، تغییر آداب و رسوم، تغییر در ارزش‌ها و هنجارها، پشت پازدن به میراث فرهنگی، کم رنگ نمودن معنویات، حمله به شخصیت‌ها و نظام‌های سیاسی، متمایل کردن دیگران به شیوه‌ها، روش‌ها، ارزش‌ها، هنجارها، دین و مکتب خود و غیره، از اصول اساس یا افرادگروه‌ها یا نظام حکومتی تروریست می‌باشد (دی آنجلیز، ۱۷: ۱۳۸۳). آژانس مدیریت فوق‌العاده فدرال[1]، تروریسم سایبری را این‌گونه تعریف می‌کند:

1. Federal Emergency Management Agency

«تهدید و حمله غیرقانونی علیه رایانه‌ها، شبکه‌ها و اطلاعات ذخیره شده در آن، زمانی که برای ترساندن و یا مجبور کردن یک حکومت یا مردم آن در پیشبرد اهداف سیاسی یا اجتماعی صورت می‌گیرد»، یکی از اهداف اصلی تروریسم سایبری و جنگ نرم بیگانگان، تغییر در طرز تلقی و آمادگی روانی وتقویت آیین ناهمنوایی جامعه هدف است (Botnets, 2008: 4).

۱. مبانی مفهومی- نظری: قدرت نرم و فضای سایبری[1]

اصطلاح قدرت نرم را جوزف نای اولین بار در کتابی تحت عنوان «ملزم به رهبری» که در سال ۱۹۹۰ منتشر گردید به کار گرفت. اما مراد وی از قدرت نرم چیست؟ قدرت نرم عبارت است از توانایی کسب مطلوب ازطریق «جاذبه» نه از طریق اجبار یا تطمیع. قدرت نرم توانایی شکل دهی، اثرگذاری و تعیین باورها و امیال دیگران است به نحوی که تضمین کننده‌ی اطاعت و فرمانبرداری آنان باشد (جمعی از نویسندگان، ۴۴: ۱۳۸۷).

در نگاه نای قدرت نرم از قدرت سخت به طور خاص قدرت اقتصادی و نظامی که به ترتیب مبتنی بر «مشوق‌ها» و تهدیدات هستند متمایز می‌گردد. بنابراین نای تقسیم‌بندی سه گانه‌ای از قدرت را پیشنهاد می‌کند: نظامی، اقتصادی و نرم. قدرت نظامی و اقتصادی هر دو ماهیتی سخت دارند و قدرت نرم از این حیث با آنها متفاوت است که مبتنی بر توانایی شکل دهی به ترجیحات دیگران می‌باشد. آن توانایی که تولید جذابیت می‌کند و منجر به فرمانبرداری می‌گردد (Lukes,2007: 90).

درسال ۱۹۹۰ نای قدرت سخت و نرم را همراه با دامنه‌ای از رفتار اجباری تا انتخابی از یکدیگر متمایزکرد؛ بالطبع در تعریف نای رفتار قدرت سخت بر پایه اجبار و پرداخت قرار داشت، درحالی که رفتار قدرت نرم بر اساس تدوین دستور کار، جذب یا ترغیب افراد استوار بود؛ حتی کشورهای بزرگی مانند آمریکا که منابع عظیمی از قدرت سخت و نرم در اختیار دارند، خود را در حال تقسیم عرصه با بازیگران جدید و مواجه شدن با مشکلات بیشتر در کنترل مرزهایشان در حوزه سایبر می‌بینند (نای، ۱۴۵: ۱۳۹۰).

1. CyberSpace

فضای سایبری از سوی برخی از کارشناسان به عنوان «تـأثیر فضـا و جامعـه‌ای که توسط یارانه‌ها، اطلاعات و ابزارهـای الکترونیکـی، شـبکه‌هـای دیجیتـالی و یـا کاربران آن شکل می‌گیرد» تعریف شده است (Lord and Sharp,2011: 10).

پسوند سایبر که خود این واژه از واژه کاربرد از «طریـق کـامپیوتر» اخـذ شـده است: سایبرنتیک عبارت است از تئوری ارتباطات و کنترل منظم بازخوردهـایی کـه ارتباط و کنترل موجودات زنده وماشین‌های دسـت سـاز بشـر را بررسـی مـی‌کنـد. سایبرنتیک را طلیعه‌دار تفکر پیچیده در پرسش و جست‌وجو از سامانه‌های فعال بـا کاربرد مفاهیم بازخوری و کنترلی نیز می‌دانند. تک واژه «سایبری» حتی امـروزه بـه نظر می‌رسد که دیگر هیچ پیوند مستقیمی با ریشه‌های خود نداشته باشد و بیشتر به نوعی تفکر نظام مند متصـل اسـت. مفهـوم «سـامانه‌هـا» قطعـا در بسـتر تهدیـدات سایبری، مفهـومی اصـلی و مرکـزی اسـت و دارای پیامـدهای رویـه‌ای وتئـوریکی متعددی برای چگونگی برخورد و بررسی موضوع است (دان کاولتی، ۲۶: ۱۳۸۹).

اگر چه فضای سایبر جای فضـای جغرافیـایی را نخواهـد گرفـت و حاکمیـت دولت را منسوخ نخواهد کرد، اما بی‌تردید شاهد پراکندگی قدرت در فضای سـایبر خواهیم بود و همین اعمال قدرت در هـر یـک از ایـن ابعـاد را بـه شـدت پیچیـده خواهد کرد. بر این اساس باید گفت، اگرچه مفهوم قدرت چیـز جدیـدی درعرصـه سیاست داخلی و خارجی نیست؛ اما قدرت سایبری چرا و به همین دلیل اسـت کـه تعاریف متعددی برای فضای سایبر ارائه شده است (نای، ۱۸۱: ۱۳۹۰).

آنچه لازم به یادآوری است این است که در بحث حملات تروریستی می‌تـوان سایبر تروریسم را جلوه‌هـایی از قـدرت نـرم بـه شـمار آورد. زیـرا، تروریسـت‌هـا می‌توانند بدون استفاده از زور و حمله فیزیکی و تنهـا بـا اسـتفاده از فضـای سـایبر حملات مخرب با بعد وسیعتر و بازدهی بیشتر را در مدت زمان بسیار کوتاهی و بـا صرف کمترین هزینه ممکن به انجام رسانند. از این روی می‌توانیم چنـین اقـدامات تروریستی را در شمار حملات جنگ نرم محسوب نماییم.

۲. مفهوم شناسی تروریسم

تروریسم عبارت است از هرگونه کاربرد غیرقـانونی و سـازماندهی شـده‌ی زور یـا

خشونت بر ضد اشخاص و اموال به قصد ترساندن یا وادار کردن شهروندان با دولت‌ها به انجام کاری در راستای یک هدف سیاسی یا اجتماعی خاص (ناجی راد، ۱۳۸۷: ۱۹).

تروریسم مجموعه اعمال ابزار و فنونی است که به صورت منظم و سازمان یافته برای ایجاد احساس ترس دسته جمعی که خشونت و کشتار بی حساب موجد آن است، به کاربرده می‌شود. تروریسم نه فقط با استفاده از وسایلی که می‌تواند زندگی و امنیت افراد را مورد سوءاستفاده قرار دهند، صورت می‌یابد بلکه از طریق تخریب خشونت‌آمیز خدمات عمومی و یا تجهیزات زیربنایی متعلق به جمع نیزاعمال می‌شود. هدف از اعمال تروریسم از هم پاشیدن ساخت اجتماعی و سیاسی که با ایجاد اغتشاش درنظم عمومی، انجام حملاتی علیه افراد یا گروه‌ها و دستیازی به اعمالی چون تلافی و انتقام، انجام می‌شود. در مواردی نیز یاغی‌ها و تبهکاران از تروریسم در جهت ایجاد هراسی که در تحقق اهدافشان مفید می‌نماید، سود بر می‌گیرند (آلن، ۱۹۹۶: ۴۲۶). آلکس اشمید معتقد است: «تروریسم شیوه اقدامات تکراری به منظور ایجاد دلهره و رعب و وحشت است که به دلایل سلیقه‌ورزی، جنایی و یا سیاسی توسط گروه‌های مختلف به کار گرفته می‌شود.»

۲-۱. ریشه‌های تروریسم

تروریسم پدیده‌ای بسیار متنوع و پیچیده است و نمی‌توان علل و ریشه‌های آن را در یک حوزه‌ی بخصوص مورد توجه قرار داد. لذا دستیابی به ریشه‌های تروریسم مستلزم توجه به حوزه‌های روانی، سیاسی، اقتصادی، مذهبی و فرهنگی است. در سراسر جهان شرایط سیاسی و اجتماعی بسیار متنوع و گوناگونی به پیدایش گروه های تروریست منجر شده است. تروریست‌های امروزی اعتقاد عمیقی به عادلانه بودن آرمان خود دارند.

ریشه روانی: نمی‌توان ادعا کرد که تروریست‌ها به لحاظ عاطفی افرادی عادی یا غیر عادی هستند اما معمولا گروه‌های تروریستی افرادی را بر می‌گزینند که از لحاظ عاطفی پایدار نیستند. معمولا آنها دارای انگیزه‌های متفاوتی برای ارتکاب چنین اقداماتی هستند؛ انگیزه‌هایی مانند انتقام، شهرت و یا کسب قدرت. بر همین

اساس انگیزهای فردی تحت تأثیر منافع شخصی یـا گروهـی و ایـدئولوژیک کـاملا متفاوت هستند و نمی‌توان آنها را به شکل کلی بیان داشت (Post,2005: 7-8).

ریشه‌هـای سیاسـی: تروریسـم پدیـده‌ای یکپارچـه نیسـت بلکـه هـم از نظـر ایدئولوژیک و هم سازمان و اهداف متفاوت مـی‌باشـد. بعنـوان مثـال، جنـبش‌هـای اجتماعی یا احزاب سیاسی که از حمایت مردمی برخوردارنـد از تروریسـم اسـتفاده می‌کنند.گاهی نیز تروریسم برای چنین گروه‌هایی تبدیل به هویت می‌شود و کارکرد استراتژی گونه خود را از دست می‌دهد، البته در شـرایطی خـاص. مـثلا وقتـی کـه امکان دستیابی به قدرت توسط حاکمیت از بین رفته، تروریسم می‌تواند مشـروعیت یابد و اهداف و حتی روش‌های آن مورد حمایت مردم قرار گیـرد (Crenshaw,2005: 13).

ریشه‌های اقتصادی: اگر چه فقر به تنهایی نمی‌تواند دلیل اصلی تروریسم باشـد اما تغییرات اقتصادی شرایطی را به وجود می‌آورد که برای بروز بی ثبـاتی و ظهـور جنبش‌های مختلف خصوصا حرکت‌های شبه نظامی و ایدئولوژیک افراطی مناسـب هستند (Gurr,2005: 19). اشخاصی که چنین اعمالی را انجام می‌دهند از حیـث سـن، نژاد و سابقه فرهنگی متفاوتند. بسیاری از آن‌ها را جوانان کم سن و سال جهان سوم تشکیل می‌دهند که شرایط سیاسی و اقتصادی دشوار جوامعشان به ایجاد مـوجی از تروریست‌های احتمالی در آن کشورها منتهی شده است.

ریشه‌های دینی و مذهبی: مـذهب بـه خـودی خـود بـه نـدرت باعـث اعمـال تروریستی بوده و ترور بیشتر وابسته به موقعیت بوده اسـت. از طرفـی نیـز مـذهب می‌تواند به فرهنگ خشونت کمک کند. یعنی با وجود آنکه نمـی‌توانـد تنهـا عامـل تروریسم باشد اما می‌تواند به بدتر شدن اوضاع کمک کند. مذهب به خاطر تکیه بـر موضوعاتی همچون مفهوم حقیقت، واقعیت‌های مطلق و اعمال خـوب، در تعریـف مفهوم خشونت می‌تواند به گسترش رویکردهای تروریسـتی کمـک کنـد. بنـابراین تروریسم صرفا مربوط به یک مذهب نمی‌شود (Juergensmeyer,2005: 27).

۳. سایبر تروریسم

۳-۱. تروریسم و اینترنت: تاریخچه فشرده

تا مدت‌ها رابطه تروریسم و اینترنت تا اندازه زیادی بصورت هراس از به اصطلاح امکان «تروریسم مجازی» بود. مارک پالیت در ۱۹۹۸، تروریسم مجازی را چنین تعریف کرد: «حمله‌هایی از پیش برنامه‌ریزی شده و با انگیزه سیاسی بر اطلاعات، سیستم‌های رایانه‌ای و داده‌ها که به خشونت ورزی گروه‌های فروملی یا عاملان مخفی بر ضد آماج‌های غیرنظامی منجر شوند» (طیب، ۱۳۴: ۱۳۹۰).

درتی دنینگ[1] تروریسم سایبر را این گونه تعریف کرده است: «حمله» یا «تهدید به حمله» به رایانه‌ها، شبکه‌ها و اطلاعات ذخیره شده در آنها که به طور غیرقانونی و به منظور ارعاب یا اجبار یک دولت یا مردم آن به پیشبرد اهداف اجتماعی و سیاسی انجام می‌گیرد. تعریفی که پیش نویس معاهده استنفورد[2] ارائه داده است اندکی با تعریف بالا تفاوت دارد: تروریسم سایبر به معنای استفاده یا تهدید به استفاده عامدانه از خشونت، اخلالگری و مداخله در سیستم‌های سایبر است که بدون مجوز قانونی صورت می‌گیرد، چه بسا به کشته یا زخمی شدن یک یا چند نفر می‌انجامد، خسارت‌های عظیمی بر املاک و ساختمان‌ها به بار می‌آورد، باعث نابسمانی مدنی[3] می‌شود یا زیان اقتصادی جدی وارد می‌سازد (هالپین، ۳۸۱: ۱۳۸۹).

پیدایش سایبر تروریسم را می‌توان با بررسی چگونگی دسترسی گروه‌های تروریست به فناوری رایانه‌ای و نحوه استفاده از آن را به تحلیل گذاشت. به همین ترتیب، حمله سایبری در معنای عام و کلی خود، حمله به شبکه‌های رایانه‌ای، ارتباطی و مخابراتی با هدف تخریب یا سرقت داده‌ها و اطلاعات معنا می‌شود. به نظر می‌رسد یکی از اولین حمله‌ها با استفاده از فضای سایبری، اواسط دهه ۷۰ میلادی، در دوران جنگ سرد بین ایالات متحده آمریکا و شوروی سابق رخ داد. اما در اغلب مستندات، مورد «گوزوو» به عنوان اولین جنگ سایبری بیان شده است.

1. Dorothy Dening
2. Stanford Draft Treaty
3. Civil Disorder

گسترش استفاده از این فضای مجازی که از دهه ۱۹۹۰ شدت گرفته است، امکان رسیدن تروریست‌ها به اهدافشان را بیشتر کرده است. حضور میلیون‌ها کاربر در دنیای مجازی، همراه با شرکت‌ها، کارخانجات و صنایع عمده بسیار، که در بسیاری از موارد از قابلیت آسیب پذیری بالایی نیز برخوردار است، خطر سوءاستفاده از فضای مجازی را بیشتر کرده و جذابیت آن را نیز افزایش داده است (کدخدایی و ساعد، ۱۳۹۰: ۷۳-۷۲).

سایبر تروریسم از همگرایی فضای سایبر و تروریسم پدید آمده است. در سایبر تروریسم، استفاده تروریست‌ها از فناوری رایانه یکی از اجزای مشخصه حمله تروریستی است. فناوری اطلاعات، دستیابی به قدرت‌هایی که از پیش از این در دست سازمان‌های بزرگ بود را برای گروه‌های کوچک و افراد نیز امکان‌پذیر ساخته است. از طرفی دیگر، سایبر تروریسم مقوله‌ی گسترده‌ای است که تروریسم اطلاعاتی، حمله‌های معنایی و جنگ شبیه سازی شده را در بر می‌گیرد. سایبر تروریسم به مقدار بسیار کم قابل کنترل است و از آنجا که خیلی تخیلی به نظر می رسد، فقط مقداری اندک با جنگ اطلاعاتی به عنوان یک کل، متفاوت است (آلبرتس و پاپ، ۱۳۸۵: ۱۱۹). آنچه ما به عنوان حمله سایبری می‌شناسیم، در واقع هدایت عملیات نظامی بر اساس قوانین حاکم بر اطلاعات است. هدف از این نوع حمله، تخریب سیستم‌های اطلاعاتی و ارتباطاتی می‌باشد؛ تلاش این حمله در جهت شناسایی اموری است که دشمن به شدت از آن محافظت می‌کند؛ این نوع حملات حرکتی در جهت تغییردهی «توازن اطلاعات و دانش» به نفع یک طرف است، بخصوص اگر توازن نیروها برقرار نباشد (قاسمی، ۱۳۸۸: ۳۲). استفاده از اطلاعات به صورتی که سرمایه و نیروی کار کمتری صرف شود. این نوع از حملات در برگیرنده فناوری‌های گوناگون به ویژه برای فرماندهی و کنترل، جمع آوری داده‌ها، و جاسوسی، پردازش و توزیع، هوشمند ساختن سیستم‌های تسلیحاتی، قفل کردن، سیستم‌ها را دچار اضافه بار اطلاعاتی کردن و نفوذ به داخل مدارها و خطوط اطلاعاتی و ارتباطی است (ناجی راد، ۱۳۸۴: ۲۲۳).

تروریسم مجازی در دهه ۱۹۹۰، بیشتر، مورد توجه دولت فدرال ایالات متحده قرار گرفت. یکی از مایه‌های خاص نگرانی این بود که دشمنان ایالات متحده که از

شکست دادن نیروهای آن کشور در میدان نبرد متعارف ناتوان بودند برای وارد کردن خساراتی به یگانه ابرقدرت باقی مانده روش‌های دیگری در پیش گیرند. بنابراین، حوادث ۱۱ سپتامبر ۲۰۰۱ به بسیاری از مقام‌های دولتی ایالات متحده تکان مضاعفی وارد کرد، این حملات نه بخودی خود هراس انگیز بود بلکه استفاده از روش‌های متعارف در این حملات، کاملا غیرمنتظره بود. اما حملات ۱۱ سپتامبر ۲۰۰۱، به هیچ وجه هراس از حملات مجازی را کاهش نداد بلکه از دید بسیاری فقط کمک کرد تهدیدهای مجازی باورپذیرتر شوند. به ویژه، در هفته‌ها و ماه‌های پس از ۱۱ سپتامبر ۲۰۰۱، احتمال حمله تروریستی مجازی به عنوان دنباله آن حملات، در سطح گسترده در ایالات متحده مورد اشاره قرار گرفت و در سطح بین‌المللی نیز مطرح شد (طیب، ۱۳۵: ۱۳۹۰). به دلیل آنکه فضای سایبری یک مأمن مناسب برای این تروریست‌ها است، دولت آمریکا نگران تهدیدهای پیشرفته‌تر احتمالی در آینده است. اف بی آی اخیرا آن دسته از افرادی را مورد بازجویی قرار داده که وابسته به القاعده بوده و تمایل داشته‌اند زیرساخت‌های حیاتی آمریکا را مورد حمله سایبری قرار دهند. دولت آمریکا باید بداند گروه‌های تروریستی می‌توانند در آینده به ابزارهای سایبری دسترسی پیدا کنند(Lord and Sharp, 2011: 19 .)

ظرف اندکی بیش از چهار هفته در ماه‌های آوریل و مه ۲۰۰۴، ابومصعب زرقاوی که زمانی رهبر «القاعده عراق» بود و اکنون دیگر زنده نیست «با استفاده حساب شده از آمیزه‌ای از خشونت افراطی و تبلیغاتی در سطح جهان به اوج شهرت و بدنامی دست یافت». او در اوایل آوریل ۲۰۰۴، یک پیام صوتی ضبط شده ۳۰ دقیقه‌ای روی اینترنت قرار داد که در آن توضیح داده بود که کیست و چرا می‌جنگد و جزئیات حملاتی را که خودش و گروهش مسئولیت آنها را به عهده گرفته بودند بازگو کرده بود. در مه ۲۰۰۴ زرقاوی یک گام پیش‌تر رفت و برای بیشترین بهره برداری از نیرویی که اینترنت از لحاظ چند برابر کردن قدرت وی داشت نوار ویدئویی گردن زدن یکی از گروگان‌های آمریکایی را روی اینترنت قرار داد. هدف از این تصاویر ویدئویی ایجاد تصوراتی بود که توجه متحدان و دشمنان زرقاوی را به یک اندازه جلب کند. از این لحاظ زرقاوی به موفقیتی بی چون و چرا دست یافت؛ این اقدام خطر چندانی برای زرقاوی نداشت ولی «دست‌کم به اندازه

بمبی که ۱۰۰ نفر از مردم را در نجف کشت، برنامه‌های ایالات متحده را متزلزل کرد و او را در سراسر جهان به قهرمان جهاد مبدل کرد» (طیب، ۱۳۶: ۱۳۹۰).

اگرچه هنوز شواهد محکمی در دست نیست که سازمان‌های تروریستی همانند القاعده بتوانند حملات گسترده نظامی را طراحی نمایند، اما این گروه‌ها از فضای سایبر برای انتشار پیام‌ها، آموزش و سربازگیری، بیشترین استفاده را می‌کنند. فضای اینترنت این امکان را برای گروه‌های تروریستی فراهم می‌کند که تکنیک‌های خود را با یکدیگر به اشتراک گذاشته، پیام‌های خود را اشاعه داده، سربازگیری نموده و به آموزش آنها بپردازند. آنچه موفقیت این گروه‌ها را در فضای سایبر تسریع می‌نماید، ارزان و در دسترس بودن این تکنولوژی‌ها است (Meyers, Powers, & Faissol, 2009: 25).

با توجه به آنچه گفته شد می‌توان نتیجه گرفت که، سایبرتروریسم[1] علاوه برآنکه فضای جدیدی برای تروریست‌های جدید ایجاد می‌کند که به واسطه هزینه پایین و غیر قابل شناسایی بودن آن می‌تواند جایگزین حمایت دولتی شود و این تروریست‌های مستقل می‌توانند برای تأمین نیازهای خود از قبیل اعتبارات مالی، آموزش یا پناهگاه امن به این فضا مراجعه کنند، قادر است حیات مجازی کشور هدف را نیز تهدید یا تخریب نماید. سایبر تروریسم این اقدام را از طریق آن چیزی انجام می‌دهد که به «سلاح‌های تخریب جمعی»[2] معروف شده است. این سلاح‌ها اعم از تکنیک‌های خردکننده جدید همچون پف کننده‌ها، بمب‌های منطقی، ویروس‌های جهش یابنده و اسب‌های تروا، این امکان را فراهم کرده‌اند که با فشار یک دکمه، خسارتی بیش از یک بمب به شبکه‌های مالی، بانکی، انرژی، مخابراتی، پزشکی و ترابری کشورهای پیشرفته‌ای همچون ایالات متحده که براساس فناوری رایانه‌ای سامان یافته‌اند، وارد کرد (فلمینگ، استول۱۳۳: ۱۳۸۴).

۴. فضای مجازی و تروریست‌ها

فضای مجازی، ویژگی‌ها و امکاناتی را دارد که آن را برای تروریست‌ها جذاب می‌کند. برخی از مهم‌ترین ویژگی‌های فضای مجازی که توجه تروریست‌ها، چه از

1. Cyberterrorism
2. Weapon of mass Distribution

جانب بازیگران دولتی و چه غیردولتی را به خود جلب کرده و موجب شده‌اند تا کنش‌گران دولتی و غیردولتی، خط‌مشی‌های خود را تغییر دهند و از دنیای فیزیکی به فضای مجازی روی آورند، عبارتند از:

بدون مرز بودن فضای مجازی: ماهیت فرامرزی فضای مجازی موجب می‌گردد تا کنش‌گران عرصه سیاست فارغ از موانع و مرزهای موجود در دنیای فیزیکی، مقاصد و اهداف خود را پیگیری کنند. بر همین اساس، فضای مجازی، محیط مطلوبی را برای اقدامات تروریستی فراهم می‌کند. این وضعیت زمانی شدت می‌یابد که جوامع به طور فزاینده‌ای به سمت به کارگیری فناوری‌های اطلاعات و ارتباطات در بخش‌های مختلف حرکت کند(Lord and Sharp, 2011: 24 .)

کاهش هزینه‌های جرم: فضای مجازی هزینه جرائم ارتکابی را برای تروریست‌ها از لحاظ نتایج اقدامات و احتمال دستگیری و مجازات به نحو قابل ملاحظه‌ای کاهش داده است. با توجه به اهمیت مسئله جرم برای تروریست‌ها، ماهیت فرامرزی فضای مجازی فرصت بسیار مغتنمی برای اقدامات تروریست‌ها در گستره جهانی است؛ چرا که با وجود دست‌یابی به اهداف مخرب پیش‌بینی شده، امکان به دام افتادن آن‌ها به حداقل ممکن می‌رسد. آن‌ها به راحتی می‌توانند از هر گوشه جهان مرتکب اقدامات زیان‌بار تروریستی در فضای مجازی شوند، بی آن که مجریان قانون کشور یا کشورهای آسیب دیده بتوانند آنها را شناسایی کنند (Lord and Sharp, 2011: 25) .

امکان وارد آوردن خسارت مالی، بدون رساندن آسیب‌های جسمی: اکثر اقدامات تروریستی در دنیای فیزیکی با آسیب‌دیدگی جسمانی افراد همراه است که این خود، سازوکاری چندانی با هدف جلب افکار عمومی و هم نواسازی آنها با اهداف تروریستی ندارد؛ زیرا اصولاً آسیب‌های جانی، به ویژه اگر با مرگ همراه باشد، حساسیت و واکنش‌های زیادی را علیه تروریست‌ها بر می‌انگیزند. بدین سان، اگر تروریست‌ها بتوانند بدون جریحه‌دار کردن احساسات مردم، لطمات مالی بسیاری به کشورها وارد آورند، به موفقیت بزرگی دست یافته‌اند. بدیهی است با وجود انواع اطلاعات ارزشمند مالی و دولتی در فضای مجازی و وابستگی فزاینده زیرساخت‌های حیاتی به فناوری‌های اطلاعات، فرصت بی‌نظیری برای اقدامات

تروریستی بدون تحریک افکار عمومی فراهم می‌شود (کدخدایی و ساعد، ۱۳۹۰: ۸۶-۸۴).

انجام بهینه‌ی فعالیت‌های پولی و بانکی: یکی از حوزه‌هایی که تقریباً به طور کامل تحت تأثیر فضای مجازی قرار می‌گیرند و روند توسعه و تکامل الکترونیکی شدن آن هم چنان ادامه دارد، پول و بانکداری الکترونیکی است که شرایط را برای سوءاستفاده از خدمات پولی و بانکی فراهم کرده است. برای مثال، گروه‌های جنایت‌کار سازمان یافته و تروریست‌ها که نیازمند مبادلات مالی‌اند و در عین حال با محدودیت‌های مالی بسیاری مواجه است؛ مجبورند درآمدهای مالی خود را تطهیر کنند تا بتوانند از آنها استفاده کنند. همچنین امکان جذب کمک‌های مالی از سوی هواداران و حامیان نیز بسیار آسان شده است و امکان ارسال کمک‌های نقدی از هر جای دنیا در کم‌ترین زمان ممکن فراهم گردیده است (کدخدایی و ساعد، ۱۳۹۰: ۸۶-۸۴). گروه‌های تروریستی با استفاده از کامپیوتر و اینترنت، در پی گسترش فعالیت‌های خود هستند. با استفاده از اینترنت و وب‌سایت‌ها بسیاری برای استخدام و افزایش بودجه فعالیت‌هایشان و برای اهداف آموزش جهادی استفاده می‌کنند. چند تن از مجرمان اخیراً محکوم شده‌اند، که از مهارت‌های خود برای جرائم اینترنتی و بدست‌آوردن اطلاعات کارت‌های اعتباری به سرقت رفته برای تأمین منابع مالی فعالیت‌های تروریستی‌شان استفاده کرده‌اند. امکان دارد که جنایت‌کاران و گروه‌های تروریستی تلاش کنند راه‌هایی برای همکاری با یکدیگر و نوع جدیدی از تهدید را بوجود آورند، که در آن افراط گرایان به ابزارهای قدرتمند برای جرائم اینترنتی و سرقت اطلاعات شخصی و یا منحل‌کردن سیستم‌های کامپیوتری، دسترسی پیدا کنند (Nagre & Warade.2008: 8).

۵. حملات سایبر تروریسم

همانگونه که گفته شد، حملات سایبر تروریسم، نوعی حمله است که در آن یک مؤلفه رایانه‌ای وجود دارد که سیستم‌های هدف را غیرقابل استفاده نموده، کارایی آنها را کم کرده و با تزریق اطلاعات غلط، دقت تصمیم‌گیری کاربران را کاهش داده و حتی منجر به سرقت اطلاعات می‌شوند (مرادی، ۱۳۸۷: ۵۷). این حمله یک اقدام

خصمانه با استفاده از کامپیوترها، اطلاعات الکترونیکی و یا شبکه‌های دیجیتالی که هدفش دستکاری، دزدی، اختلال و بی ارزش کردن سیستم‌های حساس، سرمایه‌ها و اطلاعات است. (Lord and Sharp, 2011: 10) در این حمله از فناوری رایانه‌ای می‌توان برای تهدید یا حمله کردن به منابع رایانه‌ای قربانی بهره گرفت. حملات سایبری تفاوت عمده‌ای که با دیگر اشکال معمول حمله دارند، این است که توسط عوامل نامعلوم انجام می‌پذیرد و ردیابی و یافتن محل اختفای آنان بسیار دشوار است. از طرفی نیز حملات سایبری بسیار ارزانتر از حملات معمولی است و در عین حال که فاقد آسیب پذیری‌ها و هزینه‌هایی هستند که اغلب متوجه شخص مهاجم می‌شود، در نهایت، ساختارهای شبکه‌ای گروه‌های مهاجم، آنها را در مقابل هر گونه اقدام تلافی جویانه ایمن ساخته و باعث افزایش توان خود ترمیمی آنها می‌شود (کاکاوند، ۱۳۸۲: ۱۵). حملات سایبری همانند سایر حملات پیچیده مستلزم توانمندی، مهارت و قصد و اراده است؛ با این حال، نیازی نیست که همه این ویژگی‌ها در آن واحد وجود داشته باشند. امروزه با توجه به اینکه می‌توان بدافزارها را از اینترنت دانلود کرد، دیگر نیازی نیست مهاجمین فضای سایبری همانند گذشته پول و زمان زیادی صرف کنند. مهمترین ابزار مورد استفاده در «زرادخانه» این مهاجمین سایت گوگل[1] است چرا که دسترسی به این توانمندی‌ها آن هم به صورت آنلاین[2] در این سایت نسبتا آسان است. مهاجرین سایبری می‌توانند به سهولت به مهارت و دانش لازم در این عرصه دست پیدا کنند. این شرایط درست برخلاف وضعیت دانشمندان تسلیحات هسته‌ای است که باید سال‌ها در دانشگاه درس بخوانند و اغلب نیز در سازمان‌های دولتی مشغول به کار می‌شوند.

۵-۱. حملات سایبری معروف

اما چند مثال از سایبرتروریسم برای ملموس شدن این تهدیدات؛ در سال ۲۰۰۰، یک کارمند ناراضی در تأسیسات آب استرالیا، با دستکاری سامانه کنترل رایانه این مرکز بیش از ۲۰۰ هزار گالن فاضلاب وارد رودخانه‌ها، پارک‌ها و هتل کرد. (Lord and Sharp, 2011: 24)

1. Google
2. OnLine

در ۹ می ۲۰۰۱، هکرهای چینی موفق بـه انهـدام ۱۰۰۰ وب سـایت آمریکـایی شدند، اما برای ادامه منازعه درخواست آتش بس کردند. اتحادیـه هکرهـای چینـی اعلام کرد با انهدام ۱۰۰۰ سایت آمریکایی، آنها به هدف خود رسیده‌اند و هر حملـه دیگری بعد از آن هیچ ارتباطی با آن ندارد. در مقابل هکرهای آمریکایی نیز با ارسال و گذاشتن پیام‌هایی مثل «ما از چین متنفر خواهیم بود و سایت‌هایش را مورد حمله قرار خواهیم داد» متقابلاً تلافی می‌کردند. بعد از یک جلسـه آن‌لایـن میـان اتحادیـه هکرها و اتحادیه شبکه قرمز مهمان چین، تصمیم گرفته شد که حملاتشان در تاریخ ۷ می، یعنی دومین سالگرد بمباران سفارت چین، متوقف شود. آنها تصـمیم گرفتنـد انهدام وب سایت‌های تجاری را به حداقل برسانند و به جای آن سایت‌های دولتـی را تخریب کنند. بنابر اظهارات شرکت کنندگان در این جلسه آن‌لایـن، هـدف آنهـا، جلب توجه مردم آمریکا برای نقد سیاست دولتمردانشان و درخواسـت صـلح میـان ملت‌ها بوده است. یک هکر گفت: «آمریکا می‌خواهد دنیا را به جنگ بکشاند» همـه مردم دنیا از صلح استقبال می‌کنند اما حکومت آمریکا می‌خواهد که همه را به جنگ بکشد. ما با این کار می‌خواهیم این پیام را به مردم آمریکا بفرستیم که ما همگی مثل هم هستیم اما آنها باید مانع از تخریب دنیا توسـط دولتشـان شـوند (کارازوجیـانی، ۱۳۸۸: ۱۶۶-۱۶۵).

در ماه مه سال ۲۰۰۷ گزارش شد کـه پارلمـان، وزارت‌خانـه هـا، بانـک‌هـا، و رسانه‌های کشور استونی از سوی روسیه مورد حمله قرار گرفته‌اند. در نخستین هفته از سال ۲۰۰۷ پنتاگون و برخی از کامپیوترهای فرانسوی، آلمـانی و انگلیسـی مـورد حمله هکرهای چینی قرار گرفتند. دولت چین هرگونه دست داشـتن دولـت درایـن حملات را رد کرد (عبداله خانی، ۱۳۸: ۱۳۸۶).

در سال ۲۰۰۹ محققان کانادایی شبکه گوست نت[1] را شناسـایی کـرد کـه ایـن شبکه به ۱۲۹۵ سیستم کامپیوتری در وزارتخانه‌ها، سفارت‌خانه‌ها و موسسأت چنـد ملیتی در کشورهای ایران، پاکستان، هند، کره جنوبی، آلمان و بسیاری دیگـر آسـیب رسانده و آنها را آلوده کرده بود. جالب اینجا بود که گوسـت نـت مـدیران خـود را قادر می‌ساخت تا از طریق دوربین‌های کامپیوتری و ابزارهای صوتی، کاربران مـورد

1. Ghost Net

هدف را تحت کنترل داشته باشند.. (Lord and Sharp, 2011: 17)

یک شبکه تبهکار بین‌المللی در فضای سایبری از بدافزاری به نام زئوس استفاده کرد تا از این طریق داده‌های پشتیبانی شرکت‌ها، شهرها و کلیساها را در کنترل خود بگیرد. پیش از آنکه اف‌بی‌آی و سایر نهادهای مجری قانون بتوانند در سال ۲۰۱۰ مانع عملیات این گروه شوند، گروه مذکور توانست ۷۰ میلیون دلار پول به سرقت ببرد و در نهایت اینکه تجارت تمام الکترونیک و البته سقوط سریع وال‌استریت در ماه می ۲۰۱۰ موجب بی‌ثباتی در این بازار شد و با ضرر یک تریلیون دلاری مواجه شد. همچنین برخی سهام نیز بیش از ۹۰ درصد ارزش خود را از دست دادند. هر چند این بی‌ثباتی غیرعامدانه بود و ارزش سهام و سهام نیز بازگردانده شد، اما این حادثه پیامدهای بالقوه حملات پیچیده سایبری بر ضد سامانه‌های مالی وابسته به تجارت الکترونیک را به خوبی نمایان کرد (Lord and Sharp, 2011: 24).

یکی از مهمترین حملات سایبری علیه اهداف کشورمان در سال ۲۰۱۰ رخ داد. در این حمله کرم «استاکس نت»[1] تلاش نمود اطلاعات سیستم‌های کنترل صنعتی را به سرقت برده و آنها را روی اینترنت قرار دهد. هدف از این حمله ایجاد فشار سیاسی بر ایران برای توقف طرح غنی سازی اورانیوم، نیروگاه‌های اتمی بوشهر و نطنز بود. حمله این کرم خطرناک نشان داد که ماهیت مبهم و ناشناخته سایبر تروریسم سبب می‌شود که اقدامات مقابله به مثل با مشاجره‌های سیاسی همراه شود و چه بسا هزینه‌های بسیار زیادی را برای دولت‌ها به وجود آورد (Lord and Sharp, 2011: 13).

اما شاید جالب‌ترین مثال به کرم رایانه‌ای نیمدا[2] مربوط می‌شود که به دلیل تأثیرگذاری مخرب بالای آن و هم‌چنین برخورداری از قابلیت‌های دیگر، مانند ویروس تروجان[3] به کرم چهار سر[4] معروف شده بود. این کرم رایانه‌ای یک هفته پس از واقعه یازده سپتامبر ۲۰۰۱، منتشر شد و خسارات زیادی به ویژه به

1. StuxNet
2. Nimda
3. Trojan Viruses
4. Four Headed Worm

سیستم‌های رایانه‌ای ایالات متحده، بریتانیا و هنگ‌کنگ وارد آورد (کدخدایی وساعد، ۱۳۹۰: ۹۳)

هک کردن سازمان سیا، اف بی آی، برای ارعاب یا اجبار مردم آمریکا مثال دیگر هک کردن پایگاه داده‌های بیمارستان و تغییر اطلاعات بیمار است که باعث مصرف نادرست دارو می‌شود. در ۲۰۰۳ طرح تجارت الکترونیک دلار اعلام کرد برای یک سال اگر اینترنت هک یا دستکاری شود در ۶.۵ بیلیون دلار معاملات جهانی اختلال بوجود می‌آید (Pladna,2007: 3).

هکران چینی به طور ناموفقی برای برپایی سرویس‌های نفی حمله[1] بر ضد سایت سی.ان. ان[2] در آوریل ۲۰۰۸ تلاش کردند، با هدف ساخت بد افزار[3] که کاربران عادی اینترنت را ناشیانه اما به طور بالقوه در حمله به کار بگیرند. برنامه‌ریزی برای حمله توسط یک متخصص نبرد اطلاعات آمریکایی در وبلاگش برملا شد و حجم ترافیک اینترنتی بر ضد سی.ان.ان از این روش بوجود آمد که آشکارا میان تحلیل کنندگان امنیت اینترنت به عنوان انکار سرویس‌های نفی حمله به ثبت رسانده شد (Krekel,2009: 38).

اگر چه سایبرتروریست مخرب‌تر از هکرها هستند اما هر دو تکیه اصلی کارشان بر روی نفوذ و آسیب به سیستم‌های رایانه‌ای است. در نتیجه بهترین دفاع در برابر این جریان سایبرتروریست و هکرها، بهبود امنیت رایانه است. دولت‌ها باید در پی گسترش مکانیسم‌های رسمی و غیررسمی برای همکاری‌های بین‌المللی برای ایجاد یک توافق‌نامه مشترک به منظور جلوگیری از این حملات مخرب باشند. از طرفی خود دولت‌ها باید خود را در برابر نسل بعدی فن‌آوری‌های اطلاعات مقاوم کنند. این مهم نیاز به سطح بی‌سابقه‌ای از همکاری بین موسسأت خصوصی و دولتی می‌باشد (Vatis,2002: 29-30).

همان‌طورکه مشاهده شد تهدیدات سایبری از ماهیتی متنوع، گسترده و منحصر بفرد برخوردارند. متنوع از این جهت که این تهدیدات تمام حوزه‌های زندگی بشر

1. DDos
2. CNN
3. Malware

را تحت تاثیر قرار داده‌اند، در نتیجه عدم امنیت در فضای سایبری بسیار بالاست، گستردگی از این جهت که نه تنها بازیگران دولتی بلکه شرکت‌های خصوصی، گروه‌ها و افراد را نیز درگیر خود کرده است و منحصر بفرد بودن نیز بدین سبب است که ماهیت این تهدیدات متمایز از تهدیدات سنتی و رایج گذشته است که البته این ویژگی بیشتر دولت‌ها و درک آنها از تهدید را تحت تاثیر قرار داده است. حال برای ملموس‌تر شدن تهدیدهای سایبرتروریستی به ارائه جدولی در این زمینه از تهدیدات و توصیفات آن به طور کامل می‌پردازیم.

جدول ۱. انواع تهدیدهای سایبر تروریستی (اقتباس از کتاب تروریسم و مقابله با آن، ۱۳۹۰: ۹۲)

تهدید	توصیف
گروه‌های جنایی	گروه‌های جنایی با هدف کسب پول به سیستم‌ها حمله می‌کنند
سرویس‌های اطلاعاتی خارجی	سرویس‌های اطلاعاتی خارجی که از ابزارهای سایبر برای جمع‌آوری اطلاعات و فعالیت‌های جاسوسی استفاده می‌کنند.
هکرها	هکرها گاهی اوقات با هدف ایجاد چالش یا به دست‌آوردن حقوق در اجتماع هکرها به شبکه نفوذ می‌کنند
جنگ اطلاعاتی	تعداد بسیاری از دولت‌ها برای توسعه دادن دکترین، برنامه‌ها و قابلیت جنگ اطلاعاتی تلاش می‌کنند تا از این طریق به توانایی اختلال در ارتباطات و زیرساخت‌های اقتصادی که از قدرت نظامی حمایت می‌کنند، دست یابند
تهدید داخلی	سازمان ناراضی داخلی، منبع اصلی جرائم رایانه‌ای هستند
نویسندگان ویروس	نویسندگان ویروس‌ها تهدیدهای جدی را برای شبکه‌های رایانه‌ای ایجاد می‌کنند

۶. تهدیدات سایبری و امنیت ملی

در علوم سیاسی قدرت و امنیت دو مفهوم کاملا وابسته به هم می‌باشند و به جرأت می‌توان گفت که شاید نتوان اندیشمندی را در این حوزه یافت که وابستگی این مفاهیم را به یکدیگر انکار کند. در طول سده‌های اخیر، تحول در مفهوم قدرت و منابع وابسته به آن، تغییر در مفهوم امنیت و تحولات وابسته به آن را بدنبال داشته است. در عصر جدید و بدنبال انقلابی که در اطلاعات رخ داده است، به نظر می‌رسد یکبار دیگر منابع قدرت در کشورها با دگرگونی عمیقی مواجه شده است که به تبع خود، مفهوم امنیت را نیز با تحولاتی مواجه نموده است (روزنا و دیگران، ۱۳۹۰: ۳۶۲).

توانایی استفاده از فضای سایبری یکی از مهم‌ترین منابع قدرت در قرن ۲۱ به حساب می‌آید. بازیگران دولتی و غیردولتی از این قدرت استفاده می‌کنند تا به

اهداف اجتماعی، ایدئولوژیکی، سیاسی، نظامی و مـالی خـود در فضـای سـایبری و دنیای واقعی دست یابند. افزایش سرعت فرایندها و ساختارهای پیشرفته، وابسـتگی بیشتر به اینترنت را به همراه داشته و باعث شده سـالانه میلیاردهـا دلار بـه اقتصـاد جهانی اضافه شود. تجارت اینترنتی در سـطح جهـان در سـال ۲۰۱۰ در حـدود ۱۰ تریلیون دلار بوده و تخمین زده می‌شود که این آمار در سال ۲۰۲۰ بـه ۲۴ تریلیـون دلار برسد. شرکت‌های اینترنتی تازه تأسیس، کـارآفرینی زیـادی در اقتصـاد جهـانی ایجاد کرده و در حالیکه کسب و کارهای قدیمی را به چالش می‌کشـد، محصـولات بهتر و جدیدتری به مشتریان ارائه می‌کند (Lord and Sharp, 2011: 22).

در دنیای امروز، بـزرگ‌تـرین قـدرت نیـز بعیـد اسـت بتوانـد، هماننـد سـایر حوزه‌های دریایی، زمینی و هوایی بر فضای مجازی نیـز تسـلط پیـدا کنـد. فضـای مجازی این نکته را نیز نشان می‌دهد که انتشار قدرت به این معنی نیست که برابری قدرت یا جایگزینی دولت‌ها به عنوان قدرتمندترین بازیگر در سیاست جهانی است. حتی کشورهای بزرگ و موثر که بـا منـابع عظیمـی از قـدرت سـخت و نـرم را در اختیار دارند مانند ایالات متحده، مشکل بیشتری در کنترل مرزهای خـود در حـوزه فضای مجازی دارند. فضای مجازی جـایگزین فضـای جغرافیـایی نخواهـد شـد و حاکمیت دولت را لغو نمی‌کند اما انتشار قدرت در فضای مجازی اعمـال قـدرت را پیچیده خواهد کرد. موانع ورود به فضای سایبری آن قدر کم هسـتند کـه بـازیگران غیردولتی و دولت‌های کوچک نیز می‌توانند با هزینه‌ای پایین نقش برجسـته‌ای ایفـا نمایند. برخلاف دریا، هوا و فضا حوزه سایبر در سه ویژگی با جنگ زمینی مشترک است. این ویژگی‌ها عبارتند از تعداد بازیگران، آسان بودن ورود و شانس اختفـا. بـا اینکه کشورهای معدودی نظیر آمریکا، انگلـیس، فرانسـه، روسـیه و چـین اسـتعداد بیشتری نسبت به دیگران دارند اما صحبت از تسلط در فضای سایبری بطوریکـه در مورد قدرت‌های دریایی و هوایی رایج است، بی معناست. حتی اگـر چنـین چیـزی هم وجود داشته باشد، وابستگی به سیستم‌های سـایبری پیچیـده بـرای پشـتیبانی از فعالیت‌های نظامی و اقتصادی، نقاط ضـعف جدیـدی را در کشـورهای بـزرگ بـه وجود می‌آورد که می‌توانند مورد بهره‌برداری بازیگران غیردولتی واقع شوند. اگرچـه فضای سایبر با گشودن فرصت‌های محـدود بـرای جهـش کشـورهای کوچـک بـا

استفاده از جنگ نامتقارن، ممکن است تغییراتی را در قدرت کشورها بوجود بیاورد، اما بازی را در انتقال قدرت تغییر نخواهد داد. از سوی دیگر، با اینکه دولت‌ها کماکان قویترین بازیگران هستند، اما حوزه سایبر احتمالا پراکندگی قدرت به سوی بازیگران غیردولتی را افزایش خواهد داد و این امر اهمیت شبکه‌ها به عنوان یک بعد کلیدی قدرت در قرن ۲۱ را نشان می‌دهد (Nye, 2010: 19-23).

بنابراین همان‌گونه که عنوان شد، در عصر جدید با توجه به توسعه فناوری اطلاعات و گسترش ارتباطات ناشی از آن، منابع قدرت دچار تحول و دگرگونی گسترده‌ای شده‌اند. دگرگونی منابع قدرت در عصر حاضر به دلیل ویژگیهای خاص خود، تعدد بازیگران را در عرصه قدرت بدنبال داشته و این تعدد بازیگران نیز به نوبه خود، عرصه کنترل و اعمال قدرت را بر دولت‌ها تنگ نموده است. از این رو، با چنین تحولی در مفهوم قدرت و با توجه به وابستگی پیش گفته میان مفاهیم قدرت و امنیت، به طور کاملا طبیعی، مفهوم امنیت نیز دچار تغییر و دگرگونی‌های عمیقی خواهد شد.

بر اساس نگرش سنتی، دولت‌ها به تضمین بقای خود و تأمین امنیت نظامی‌شان، اهمیت زیادی می‌دهند. در عین حال، باید توجه داشت که دولت‌ها امروزه ناچارند ابعاد جدیدی از امنیت را در نظر بگیرند. برای مثال، کانادایی‌ها امروزه نگران این نیستند که سربازان آمریکایی برای دومین بار (همانند سال ۱۸۱۳)، تورنتو را در آتش بسوزانند، بلکه از این نگرانند که رایانه‌ای در تگزاس، تورنتو را با مشکلی عمده روبه‌رو کند (نای، ۱۳۸۷: ۱۲۴). مفاهیم سنتی از جنگ بر اساس حمله و دفاع، توسط پیچیدگی‌های فضای مجازی به چالش کشیده شده‌اند و با سرعت تغییر پیدا می‌کنند و این تهدید به نوعی مفاهیم سنتی جنگ را تغییر داده است. تهدید سایبر نامتقارن است، از یک سو نیاز به سرمایه‌گذاری بزرگی برای استفاده یا حمله نیاز نیست. در مقابل، دفاع در برابر تهدید سایبر باید تمام جوانب را در نظر بگیرد که هزینه‌های آن امروزه در حال افزایش است (Tabansky, 2011: 88). مسئله دیگری که از تهدیدات سایبری بر می‌آید، ناشی از ابهامات قانونی آن است. بدین معنی که قانونی در زمینه فعالیت‌های خرابکارانه سایبری، به خصوص جنگ سایبری وجود ندارد. در قوانین جنگ به شیوه مرسوم و سنتی آن، توافق‌نامه‌ها و

تعهداتی همچون کنوانسیون ژنو و منشور سازمان ملل وجود دارد، که صراحتاً بیان می‌دارند که هیچ ملتی نمی‌تواند از زور علیه تمامیت ارضی یا استقلال سیاسی هر کشور دیگری استفاده کند. این در حالی است، که دشوار بتوان جنگ سایبری را در این چهارچوب تعریف نماییم (Markoff and Shanker, 2009).

بنابراین، چالش امنیت سایبری هم مهم و هم پیچیده است. دستیابی به ترتیبات مؤثر حکومت در این حوزه، به یک استراتژی جامع که شامل اقدامات هماهنگ بوسیله حکومت، بخش خصوصی و شهروندان نیاز دارد. جامعه جهانی نیز به صورت واضح، منافع مشترکی در حمایت امنیت سیستم‌های سایبری همکاری و اقدام فوری نیازمند است (Chertoff, 2008: 484). در راستای چنین اهمیتی بود که در ۲۹ می‌سال ۲۰۰۹، رئیس جمهور آمریکا اعلام کرد که فضای سایبری به عنوان یک دارایی مهم ملی است که ایالات متحده با تمام معنی از آن دفاع می‌کند (Lewis, 2011: 3).

از این رو، امنیت سایبری در ارتباط مستقیم با امنیت ملی یک کشور است. دیگر امروزه نمی‌توان امنیت ملی را منحصراً در ارتباط با مرزهای خارجی و حفاظت از جان شهروندان بوسیله نیروهای نظامی تعریف کرد. امروزه به لطف اینترنت و یک دستگاه رایانه، دشمن بدون اینکه متوجه حضور فیزیکی‌اش باشیم، تا خانه‌های ما رخنه کرده است. چنین خطر نافذی، تمامی برداشت‌های رایج و سنتی از مفهوم امنیت ملی را زیر سوال برده است.

نتیجه گیری

در سال‌های اخیر ماهیت تروریسم دچار دگرگونی شده است و با توجه به رشد روز افزون فناوری اطلاعات، از شکل سنتی خود به شکل جدید تغییر ماهیت داده است. در این شیوه‌های نوین، بجای استفاده از ابزارهای سخت‌افزاری، تروریست‌ها با استفاده از فضای سایبر دست به حمله می‌زنند و اهداف خود را با بیشترین ایمنی و کمترین هزینه عملی می‌نمایند. تروریست‌های سایبر برای پیشبرد مقاصد سیاسی خود، هر روز در حال ایجاد روش‌ها و ابزارهای هوشمندانه‌تر برای حمله به سیستم های رایانه‌ای و دولتی هستند. در چنین جایگاهی، امنیت ملی و جهانی در خطر می

باشد. دلیل وجود این خطر را می‌توان عدم وجود قوانین کافی حاکم بر اینترنت، وسعت مخاطبان بالقوه، ناشناس بودن ارتباط و سرعت جریان اطلاعات دانست. این موارد، ویژگی‌هایی هستند که برای مبارزه با تروریسم سایبر باید تحت بررسی و تحقیقات بیشتری قرار گیرند.

در حال حاضر سیاست‌های موجود در زمینه امنیت سایبری در مرزهای ملی محصور مانده‌اند و هیچ توافق بین‌المللی تأثیرگذاری در زمینه امنیت سایبری شکل نگرفته است. یکی از مهم‌ترین تهدیدات موجود در فضای مجازی حمله به زیرساخت‌های حیاتی یک کشور چه در بخش نظامی و چه غیرنظامی است. این زیرساخت‌ها در معرض تهدیدات چه از جهت درگیرهای نظامی و چه در حالتی فارغ از تهدیدات نظامی هستند. مشکل بزرگتر در این زمینه در مواردی است که فارغ از درگیرهای نظامی بین کشورها، این تهدیدات در دنیای فعلی جاری هستند، در این حالت غیرنظامی، مشکل دوچندان است زیرا نسبت دادن این حملات عملاً غیرممکن است. از سوی دیگر تهدیدات سایبری دارای ویژگی‌های افزون‌تری هستند که مشکل را دو چندان کرده است؛ زیرا این عوامل سبب شده است که فضای مجازی به میدان نبردی برای هکرها و گروه‌های تروریستی و غیره تبدیل شود و تروریست‌ها از پتانسیل موجود در فضای مجازی برای طرح‌ریزی و سایر اقدامات خود استفاده کنند.

اگر چه همکاری‌های ضدتروریستی میان کشورها بعد از ۱۱سپتامبر تقویت شده است و بسیاری از کشورها در این زمینه همکاری می‌کنند، اما امروزه تروریست‌ها از محیط نبرد جدیدی به لطف فضای مجازی برخوردار شده‌اند که به راحتی می‌توانند دانش فنی لازم برای ایجاد عملیات در این فضای مجازی را بدست آورند. امروز ما شاهد این هستیم که تروریست‌ها از این فضا به نحو احسن برای پیشبرد اهداف خود مورد استفاده قرار می‌دهند؛ این عوامل سبب شده است تا امروز بیش از هر زمان دیگری این تهدیدات جدی به نظر آید.

یکی از بهترین و صحیح‌ترین راهکارهای مقابله با سایبرتروریسم، بسترسازی حقوقی از طریق وضع قوانین و مقررات مورد نیاز است. اصلی‌ترین گام، تدوین و یک شکل نمودن قوانین جرایم رایانه‌ای و اینترنتی خواهد بود. در بیشتر کشورها

هنوز قوانین خاصی راجع به جرایم رایانه‌ای و اینترنتی تـدوین نشـده اسـت و ایـن موضوع یعنی وجود خلاءهای قانونی، نیروهای امنیتی رادر مقابله با جرایم رایانه‌ای و اینترنتی، سردرگم می‌کند و توانایی واکنش به موقع و مناسب ر ا از آنان می‌گیـرد. از طرف دیگر، جهت مدیریت حملات سایبر تروریسم بایستی انگیزه انجام حملات سایبری را شناسایی نمود. با شناسایی چنین انگیزه‌هایی می‌توان به هدف مورد نظـر دشمن پی برد و با دست یافتن به این مهم، در پی حفاظـت از ایـن اهـداف برآمـد. بنابراین اگر سایبر تروریسم به عنوان یک پدیده سیاسی- استراتژیک درک و شناخته شود، بسیاری از مشکلات برای مدیریت چنین بحران‌هایی حل می‌گردد.

می‌توان با تعریف واضح از استراتژی امنیت ملی کشورها، اهـداف، روش‌هـا و وسایل جدید در تلازم با این استراتژی را به وضوح تعریف نمود و افرادی برجسته را در پی رسیدن به این اهداف تربیت نمـود. از طرفـی نیـز بایسـتی سـطح آگـاهی عمومی را در بین آحاد مردم ارتقاء بخشید. از آنجا که سایبر تروریسـم دارای ابعـاد استراتژیک می‌باشد، بایستی سهم مهمی نیز برای انجـام پـژوهش و تحقیـق توسـط کارشناسان دفاعی و استراتژیک قائل شد.

در سطح داخلی نیز، بایستی با افزایش توانمندی‌های ملـی در صـدد مقابلـه بـا چنین حملاتی بر آمد. بایستی دست به مفهوم سـازی زد و بـا شناسـاندن خطـرات سایبر تروریسم در پی مقابله با این پدیده جدید برآمد. از طرفی نیز، آگاهی صـرف، کافی نیست بلکه باید افراد و مراکز پژوهشی را مجهز نمـود و بـا تهیـه سیسـتم‌هـا، سلاح‌ها و خط مشی‌ها برای مجهز کردن افراد، گروه‌ها یا سازمان‌ها در صدد مقابلـه با سایبر تروریسم بر آمد. بایستی دانش آموختگان بسیاری را جهت شناسایی، خنثی نمودن و حمله متقابل علیه اقدامات سایبر تروریسم تربیـت نمـود و سـطح کمـی و کیفی دانشگاه‌ها و مراکز تحقیقاتی را برای تربیت چنـین دانـش آموختگـانی ارتقـاء بخشید.

برای کمرنگ نمودن حملات سایبری بایستی دولت‌هـا همکـاری‌هـای لازم را انجام دهند. همکاری جهانی دولت‌ها برای مدیریت فضـای سـایبر بایـد مبتنـی بـر گفت‌وگو و مذاکره سیاسی باشد. زیرا اتخاذ راهکارهای نظامی تنها منجر به افزایش پراکندگی و تشتت در این فضا می‌گردد. بنـابراین بایسـتی اتخـاذ یـک چهـارچوب

سیاسی بین‌المللی برای مقابله با چالش‌های فضای سایبر، بـه یکـی از اولویـت‌هـای اصلی امنیت ملی کشورهای جهان محسوب شود. تنها همکاری بین‌المللی است کـه ما را قادر می‌سازد از جنایت‌های سایبری جلوگیری و از رشد سالم فضای سـایبری و اینترنت مطمئن شویم.

کتابنامه

منابع فارسی

آلبرتس، دیوید و پاپ، دانیل. (۱۳۸۵). *گزیده‌ای از عصر اطلاعات: الزامات امنیت ملی در عصر اطلاعات*، ترجمه علی علی آبادی و رضا نخجوانی، تهران، پژوهشکده مطالعات راهبردی.

بیرو، آلن. (۱۹۹۶).*فرهنگ علوم اجتماعی*، ترجمه دکتر باقر ساروخانی (۱۳۶۶)، تهران، انتشارات کیهان.

جمعی از نویسندگان. (۱۳۸۷). *بصیرت پاسداری*، تهران، اداره‌ی سیاسی نمایندگی ولی فقیه در سپاه.

دان کاولتی، میریام. (۱۳۸۹). *سیاست‌های تهدید و امنیت سایبری*، محبوبه بیات، تهران، مرکز آموزشی و پژوهشی شهید سپهبد صیاد شیرازی.

دی آنجلیز، جینا. (۱۳۸۳). *جرایم سایبر*، ترجمه سعید حافظی و عبدالصمد خرم آبادی، تهران، شورای عالی توسعه قضایی.

روزنا، جیمز و دیگران. (۱۳۹۰). *انقلاب اطلاعات، امنیت و فناوری‌های جدید*، مترجم علیرضا طیب، تهران، پژوهشکده مطالعات راهبردی.

عبداله خانی، علی. (۱۳۸۶). *جنگ نرم ۳: نبرد در عصر اطلاعات*، تهران، موسسه فرهنگی مطالعات و تحقیقات ابرار معاصر تهران.

فلمینگ، پیتر، استول، مایکل. (۱۳۸۴). «*سایبر تروریسم: پندارها و واقعیت‌ها*»، ترجمه اسماعیل بقایی هامانه و عباس باقرپور اردکانی، در مجموعه تروریسم، گردآوری علیرضا طیب، نشرنی.

قاسمی، فائزه. (۱۳۸۸). *بررسی نظریه‌های فمنیستی جنگ*، دانشکده علوم و اداری و اقتصاد، دانشگاه اصفهان.

کارازوجیانی، آتینا. (۱۳۸۸). *سیاست‌های منازعه سایبری*، مترجم محبوبه بیات، تهران، مرکز آموزشی و پژوهشی شهید صیاد شیرازی.

کدخدایی، عباسعلی و ساعد، نادر. (۱۳۹۰). «*تروریسم و مقابله با آن*»، مجمع جهانی صلح اسلامی.

ناجی راد، محمدعلی. (۱۳۸۴). *جهانی شدن تروریسم*، تهران، دفتر مطالعات سیاسی و بین‌المللی.

ـــــــــــــــ (۱۳۸۷). *جهانی شدن و تروریسم*، تهران، دفتر مطالعات سیاسی و بین‌المللی.

نای، جوزف. (۱۳۸۷). *رهبری و قدرت هوشمند*، ترجمه‌ی محمودرضا گلشن پژوه و الهام شوشتری زاده، تهران، مؤسسه‌ی ابرار معاصر تهران.
ـــــــــــــ (۱۳۹۰). *آینده‌ی قدرت*، ترجمه‌ی رضا مراد صحرایی، تهران، حروفیه.
هالپین، ادوارد و دیگران. (۱۳۸۹). *جنگ سایبر، جنگ اینترنتی و انقلاب در امور نظامی*، ترجمه روح الله آرانی، دفتر مطالعات سیاسی مرکز پژوهش‌های مجلس.

مقالات فارسی

پیروزان، علیرضا (۱۳۸۸)، «اتحادیه اروپایی و پدیده تروریسم»، تهران، وزارت اطلاعات، *فصلنامه اطلاعات سیاسی اقتصادی*، (۲۶۶-۲۶۵)، ص ۸۰.
توکلی، یعقوب (۱۳۸۶)، «واکاوی ترور و تروریسم»، تهران، حوزه هنری سازمان تبلیغات اسلامی، *ماهنامه سوره*، (۳۴)، ص ۱۲۶.
کاکاوند، عباس (۱۳۸۲) «حملات سایبری چالش جدید آمریکا»، *نشریه رسالت*، شماره ۱۳۸۲/۰۶/۰۴، ص ۱۵.
مرادی، مختار (۱۳۸۷) «مدیریت میدان نبرد: مقدمه‌های بر محیط شناسی نظامی و جنگ‌های اطلاعاتی»، *نشریه علوم اجتماعی*، (۱۰)، ص ۵۷.

منابع لاتین

Crenshaw, Martha, (2005). *"Political Explanations in Addressing the Causes of Terrorism"*, The Club de Madrid, Encyclopaedia Britannica, op. cit.
Chertoff, Michael (2008) , " *The Sybersecurity Challenge*", Regulation & Governance.
Congressional Research Service (*CRS)* (2008) , "*Botnets, Cybercrime and Cyber terrorism: Vulnerabilities and Policy Issues for Congress*", available at: www.crs.org, (accessed by July 23, 2011).
Gurr,Ted Robert, (2005). *"Economic Factors in Addressing the Causes of Terrorism"*, The Club de Madrid.
Juergensmeyer, Mark, (2005). *"Religion in Addressing the Causes of Terrorism"*, The Club de Madrid.
Post, Jerrold m, (2005). *"Psychology in Addressing the Causes of Terrorism"*, The Club de Madrid.
Krekel, Bryan, "*Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation Prepared for The US-China Economic and Security Review Commission*" October 9, 2009.
Lewis, james A. (2011) , " *Cyber Security Two Years Later*", Center for Strategic & International Studies (CSIS) , available at: http: //www.csis.org/publication/cybersecurity-two-years-later, (accessed by June 13, 2011).
Lord, Kristin M. & Sharp, Travis (2011) , "*America's Cyber future Security and Prosperity in the Information Age*", Center for a New American Security, Volume I.
Lukes Steven (2007) , "*Power and the Battle for Hearts and Minds: On the Bluntness of*

Soft Power", in Power in World Politics, London & New York: Routledge

Markoff, Jaud & Shanker, T. (2009) , "*Halted'03 Plan Illustrates U.S Fear of Cyberwar Risk*", The New York Times.

Meyers, C. A., Powers, S. S., & Faissol, D. M. (2009, October 08)."*Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidentsand Approaches*". Retrieved from Lawrence Livermore National Laboratory (LLNL): http: //www.osti.gov/bridge/servlets/purl/967712-BNpjlx/967712.pdf

Nagre, Dhanashree& Warade, Priyanka, (2008) "C*yber Terrorism Vulnerabilities and Policy Issues "Facts Behind The Myth*" http: //www.andrew.cmu.edu/user/dnagre/

Nye, Joseph s. (2010) , "*Cyber Power*", Belfer Center for Science and International Affairs

Brett Pladna, (2007) "*Cyber Terrorism and Information Security*" http: //www.infosecwriters.cominternational and public affairs New York

Shultz, (2008). *"Terrorism and the Modern World"*, Current Policy No. 629.

Tabansky ,Lior (May 2011) "*Basic Concepts in Cyber Warfare*" Military and Strategic Affairs/v 3/ n. 1

Vatis, Michael (2002) , *" Cyber Attacks: Protecting American's Security Against Digital Threats*", John F. Kennedy School of Government, Harvard UniversityCongressional Research Service (CRS) (2008) , "Botnets, "*Cybercrime and Cyber terrorism: Vulnerabilities and Policy Issues for Congress*", available at: www.crs.org, (accessed by July 23, 2011).