مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

عصر فضای مجازی
سی و سوم

تروریسم سایبری ..... و ویژگی های آن

Cyber terrorism and its characteristics

عصر فضای مجازی

گزارش شماره ۳۳
اردیبهشت ۱۳۹۹

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

تروریسم سایبری و ویژگی‌های آن

**محتوای انتشار یافته در این اثر
الزاماً بیانگر دیدگاه مرکز ملی فضای مجازی نیست**

تهیه شده در پژوهشگاه فضای مجازی
(گروه مطالعات بنیادین)

تهیه کننده: رامین ولی‌زاده میدانی (دانشجوی دکتری جامعه‌شناسی سیاسی دانشگاه امام صادق (ع))
ناظر علمی: دکتر حسین مطلبی کربکندی

نشانی: تهران، میدان آرژانتین، خیابان بیهقی، نبش خیابان ۱۶غربی، پلاک ۲۰
تلفن: ۸۶۱۵۱۰۶۱-۰۲۱
کد پستی: ۱۵۱۵۶۷۴۳۱۱

فهرست

سخن نخست

سخن نخست

فضای مجازی با شتاب شگرف و رو به تزایدی که در حال بسط و گسترش است تمام ساحات اجتماعی، اقتصادی، سیاسی و فرهنگی زندگی بشر را درنوردیده و هر روز بخش بزرگی از زندگی واقعی را در خود فرو برده و حیات متفاوت و جدیدی به آن می‌دهد. لذا به نظر می‌رسد دو نگاه کلان به فضای مجازی وجود دارد: نگاه اول که بالاخص در ابتدای رشد و تکوین فضای مجازی مسلط شده بود، آن را همچون ابزاری کنار سایر ابزارهای بشری تصویر می‌کرد که تنها طریقیت داشت. اما نگاه دوم، در نتیجه رشد تحولات خیره‌کننده فضای مجازی و سایه گستری آن در حوزه‌ها و شئون بشر در یک دهه اخیر آن را چون سکویی می‌داند که بسیار فراتر از شأن ابزاری حیات انسان‌ها را سامان جدیدی داده و ادعای تمدن نوینی را دارد. رویکردی که از قضا از چشمان بصیر رهبر انقلاب نیز دور نمانده و انتظاری تمدنی از فضای مجازی در ایران را مطالبه داشته‌اند.

در همین راستا گزارش‌های عصرفضای مجازی تلاش می‌کند تا فهم سازمان‌ها و دستگاه‌های مرتبط با حوزه فضای مجازی را ارتقاء بخشیده و آن‌ها را برای مواجهه فعال و خردمندانه با تحولات این عرصه مهیا سازد.

سید ابوالحسن فیروزآبادی
دبیر شورای عالی و رئیس مرکز ملی فضای مجازی

چکیده

چکیده

گسترش فضای سایبری در سال‌های اخیر، امری مشهود است و این فضا متعلقات خاص خود را به همراه دارد. تروریسم سایبری، یکی از مفاهیم مورد توجه در این عرصه به شمار می‌آید. این پدیده، نشان‌دهنده حضور و استفاده عناصر تروریستی از فضای سایبری است که اقدامات تروریستی در آن کم‌هزینه‌تر محسوب می‌شود. با این حال، تروریسم سایبری با نوعی از پیچیدگی همراه است که تشخیص آن ممکن است به راحتی امکان‌پذیر نباشد. پژوهش حاضر، به دنبال شناخت چیستی تروریسم سایبری است. بر این اساس، سوال اصلی این نوشتار عبارت است از اینکه مفهوم، ویژگی‌ها و راهبردهای مقابله با تروریسم سایبری چیست؟ از آن‌جایی که بازیگران مختلفی در تروریسم سایبری تاثیرگذار هستند، شناخت این فضا، گام نخست برای مقابله با آن محسوب می‌شود. گستردگی عاملان، ردیابی دشوار، دشواری اثبات وقوع جرم، آسیب‌زایی گسترده، عدم محدودیت مکانی و زمانی، هزینه‌های ارزان، بهره‌برداری از شبکه‌های اجتماعی و تصویرسازی از

جملـه ویژگی‌هـای تروریسـم سـایبری اسـت. این پژوهـش بـا روش توصیفی – تحلیلـی و بـا اسـتفاده از منابـع کتابخانـه‌ای بـه دنبـال پاسـخ بـه سـوال طرح‌شـده اسـت. نتایـج پژوهـش حاضـر می‌توانـد در تصمیم‌سـازی‌ها و سیاسـت‌گذاری‌های فضـای سـایبری مثمرثمـر واقـع شـود.

واژگان کلیـــدی: فضـای سـایبری، تروریسـم، تروریسـم سـایبری، سیاسـتگذاری، اقدامـات تروریسـتی.

مقدمه

مقدمه

فضای سایبری، همچون فضای فیزیکی، فضایی واقعی محسوب می‌شود که بسیاری از امور روزانه شهروندان در آن انجام می‌گیرد. با رشد روزافزون فضای سایبری، بر پیچیدگی‌های آن نیز افزوده می‌گردد و در کنار فرصت‌های متعددی که این فضا برای بشر به ارمغان می‌آورد، تهدیدهای آن نیز به مرور شناسایی می‌شود.. شناخت و فهم صحیح این تهدیدات، نخستین گام برای مقابله با آن‌ها محسوب می‌شود. تروریسم سایبری یکی از این تهدیدات است که پژوهش حاضر به دنبال فهم چیستی آن است. کنترل و تحدید فضای سایبری آن‌چنان که در فضای ملموس انجام می‌گیرد، مقدور نیست؛ لایه‌های پوشیده‌ای در این فضا وجود دارد که مرزها را درنوردیده است. این گستردگی بر ارزش‌های حاکم در این فضا نیز تاثیر می‌گذارد.

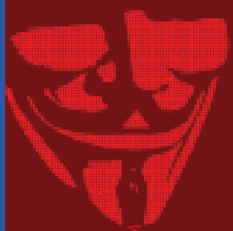
آنچه به‌عنوان آزادی گردش اطلاعات در فضای سایبری مشهور شده است، تحدیدپذیری این فضا را دشوار می‌سازد؛ لذا ممکن است

امنیت سایبری تحت‌تاثیر چنین مساله‌ای قرار گیرد. به عنوان نمونه، تروریسم سایبری در چنین فضایی قدرت مانور بیشتری پیدا می‌کند و مقابله با آن، به آسانی فضای فیزیکی نیست. این موضوع نشان می‌دهد که شناخت مقتضیات این پدیده، گام بسیار مهمی در مسیر مقابله با آن محسوب می‌شود. پژوهش حاضر تلاش می‌کند با پاسخ به این پرسش اصلی که مفهوم، ویژگی-ها و انواع تروریسم سایبری چیست، ماهیت پدیده مذکور را روشن سازد و به شرح راهبردهای مقابله با آن بپردازد. این نوشتار با بهره‌مندی از منابع کتابخانه‌ای و با روش توصیفی – تحلیلی سوال پژوهش را پاسخ می‌دهد.

سازمان‌دهی پژهش حاضر، به این صورت است که پس از بیان مقدمه، چارچوب مفهومی ذکر خواهد شد که برای ترسیم دایره معنایی تروریسم سایبری ضروری و مفید است. سپس ویژگی‌های این پدیده مورد بررسی قرار خواهد گرفت. پس از آن نیز راهبردهایی برای مقابله با این پدیده، بیان خواهد شد.

بخش اول

چارچوب مفهومی



CYBER TERRORISM

بخش اول

چارچوب مفهومی

در این بخش از پژوهش، به بررسی چارچوب مفهومی تروریسم سایبری می‌پردازیم تا دایره معنایی آن مشخص شود. از آن‌جایی که تروریسم سایبری از دو مفهوم تشکیل شده است، تبیین این دو مفهوم، به روشن شدن چارچوب مفهومی تروریسم سایبری کمک می‌کند. بر این اساس، ابتدا مفهوم تروریسم مورد بررسی قرار می‌گیرد و سپس مفهوم سایبر توضیح داده می‌شود.

۱-۱. تروریسم

مفهوم تروریسم، از مفاهیم پیچیده‌ای است که ترسیم دایره معنایی آن نیازمند توجه به متغیرهای مختلفی می‌باشد. به عبارت دیگر، مفهوم تروریسم هم در معنا و هم در مصداق، به صورت واحد تعریف نشده است. علاوه بر این، برخی محدودیت‌ها نیز بر این پیچیدگی می‌افزاید. به عنوان نمونه، ممکن است بازیگران مختلف بین‌المللی بر اساس ارزش‌های خاص خود، گروهی را در زمره

تروریست‌ها قرار دهند که از نگاه دیگران تروریست نباشد. بنابراین، در بسیاری از موارد، قالب‌های ارزشی، بر این تعریف تاثیرگذار هستند. بنابراین، برخی بر این باور هستند که پیچیدگی مذکور در این مفهوم باعث می‌شود که تعریف واحدی از آن ارائه نشود.[1]

تروریسم را در یک تعریف، به معنای استفاده از روش‌های خشونت‌آمیز علیه افراد، بازیگران سیاسی یا گروه‌های فروملی دانسته‌اند که به منظور تحقق یافتن اغراض مختلف از جمله اهداف سیاسی به کار گرفته می‌شود. در یک تعریف رایج دیگر، تروریسم عبارت است از بهره‌برداری از ابزار خشونت‌آمیز، برای به وجود آوردن ترس یا تهدید. سه متغیر در این تعریف مورد توجه واقع شده است؛ اولا روشی که در این پدیده استفاده می‌شود، دربردارنده خشونت است. ثانیا هدف از آن بازیگران سیاسی و بدنه اجتماعی محسوب می‌شود. ثالثا قصد تروریسم ایجاد هراس و تهدید به منظور اهداف سیاسی و اجتماعی است.[2]

برایان جنکیز از کارشناسان تروریسم، از این پدیده به عنوان یک تئاتر نام برده است. چرایی کاربرد چنین تعبیری عبارت است از اینکه تروریسم نیز همانند تئاتر طی یک طراحی پیشینی به اجرا درمی‌آید و نحوه اجرا نیز به صورتی است که توجه بسیاری از مخاطبان را به خود جلب کند. مخاطبانی که در مقابل چنین تئاتری قرار گرفته‌اند، از ضررهای جبران‌ناپذیر این مساله هراس دارند[3]؛ این در حالی است که مجریان تروریسم برای رسیدن به اغراض خود دست به هر اقدامی می‌زنند. آن‌ها حتی در این

1.Council of Europe, The threat of cybercrime, Situation report, 2015, p: 171.
2.Oliverio and Lauderdale, terrorism as deviance or social control, 2016, p: 157.
3.Aaviksoo, Cyber-attacks against Estonia Raised Awareness of Cyber threats, 2010, p: 37.

مسیر از جان خود نیز می‌گذرند؛ لذا این موضوع، پدیده‌ای پیچیده و چندلایه است که به سادگی قابل مهار نیست.[1] بنابراین، علیرغم وجود تعاریف متعدد برای پدیده تروریسم، هراس‌افکنی، بهره‌برداری از خشونت و مقاصد سیاسی از جمله عناصر مشترک در این تعاریف به‌شمار می‌روند.[2] بر این اساس، می‌توان گفت که عناصر مذکور، ارکان اساسی این پدیده را شکل می‌دهند. ایجاد ترس در اقدامات تروریستی، به عنوان مهم‌ترین رکن تروریسم شناخته می‌شود؛ لذا برخی تعاریف، تروریسم را مشخصاً به معنای وحشت‌آفرینی دانسته‌اند. در حقیقت، امنیت به عنوان موضوع و هدف تروریسم محسوب می‌شود.[3] بر این اساس، مجریان اقدامات تروریستی ایجاد هراس و وحشت را در دستور کار خود قرار می‌دهند. در بسیاری از موارد، چنین اقداماتی در وهله نخست، اشخاص و دارایی‌های آن‌ها را مورد هدف قرار می‌دهند؛ اما هدف غایی آن‌ها مواجهه با امنیت ملی است. بهره‌برداری از خشونت در اقدامات تروریستی، یکی دیگر از ارکان مهم آن محسوب می‌شود. این مفهوم، امری نسبی است که بسته به شرایط مکانی و زمانی، معنای متفاوتی دارد. خشونتی که در اینجا مورد بحث است، لزوما حالت فیزیکی ندارد؛ بلکه خشونت در معنای روانی نیز در قالب تروریسم قرار می‌گیرد.[4] اقداماتی که در این حوزه انجام می‌گیرد، به دنبال این است که با روش‌های فیزیکی و روانی هراس‌افکنی کنند[5] البته باید گفت آنچه به عنوان اقدامات خشونت‌آمیز در تروریسم مد نظر است، به خودی

1.Bogdanosky, Cyber Terrorism– Global Security Threat, International Scientific Defence, 2013, p: 92-91.
2.Merari, Terrorism as a Strategy of Insurgency, 2013, p: 102.
3.Brenner & Marc, In Defense of Cyberterrorism: An Argument for Anticipating Cyber Attacks, 2012, p: 17.
4. Oots, Bargaining with Terrorist: Organizational Consideration, Terrorism, 2015, p: 158-145.
5.Brito and Tate, Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy, 2011, p: 26.

خود نمی-تواند حامل اهداف این پدیده باشد، بلکه نتیجه‌ای که در پی استفاده از این اقدامات به دست می‌آید، مهم ارزیابی می‌شود. ایجاد هراس نتیجه حاصل از بهره‌برداری خشونت محسوب می‌شود.[1] علاوه بر آنچه گفته شد، ابزارهایی نیز که برای ایجاد خشونت مورد استفاده قرار می‌گیرند، بسته به هدف، ممکن است متفاوت باشند. به عنوان نمونه، اقدامات تروریستی در حوزه سایبری، از شبکه‌های اطلاعاتی و سیستم‌های آن استفاده می‌کنند.

سومین عنصر مهم در اقدامات تروریستی، اغراض سیاسی است که هدف مجریان این اقدامات، در این قالب تعریف می‌شود.[2] تروریسم، پدیده‌ای برای اجرایی ساختن اهداف سیاسی است و لذا برخی از تعاریف بر این نکته تاکید دارند که آن دسته از اقداماتی که حامل غرض سیاسی نیست، نمی‌تواند به عنوان اقدامی تروریستی ارزیابی شود.[3] اهداف سیاسی، خود دایره گسترده‌ای را شکل می‌دهد و اغراض عقیدتی و قومی را نیز شامل شود؛ بنابراین شناخت اهداف این اقدامات، گام اصلی برای مقابله با آن محسوب می‌شود. شناخت و مقابله با اهداف چنین اقداماتی، می‌تواند بهترین راهکار برای برخورد با آن به شمار آید؛ چرا که تروریسم را از لحاظ نرم‌افزاری با یک خلأ مواجه می‌سازد و مجریان آن نمی‌توانند قدرت مانور چندانی داشته باشند.

۱-۲. فضای سایبری

همچون تعاریف تروریسم، تعریف‌های ارائه شده از فضای سایبری

1.Capaldo, providing a Self-Defense against large scale attacks by irregular forces: The Israeli- Hezbollah conflict, 2017, p: 34.
2.Clay, Information Warfare and Cyberwar: Capabilities and Related Policy Issues, 2013, p: 79.
3.Ruby, The Deffinition of Terrorism, In Analyses of Social Issues and Public Policy, 2014, p: 14-9.

نیـز معانـی مختلفـی از ایـن مفهـوم را به دسـت می‌دهنـد. دسـته اول از این تعاریـف، فضـای سـایبری را غیرواقعـی تلقـی می‌کننـد و بـر این باور هسـتند کـه ایـن فضـا در عـرض دنیـای واقعـی قـرار دارد. [1] دومیـن دسـته از تعریف‌هـا، ایـن فضـا را محلـی بـرای انتقـال اطلاعـات دانسـته‌اند. [2] دسـته‌ای دیگـر از تعاریـف نیـز بـا دریچـه سـخت‌افزاری بـه فضـای سـایبری می‌نگرنـد و ایـن فضـا را متشـکل از اتصـال تعـداد بسـیاری از سیسـتم‌ها می‌داننـد. [3]

یکـی از تعریف‌هـا بـر اسـاس فرهنـگ لغـت «ماریـام وبسـتر» اشـاره می‌کند کـه فضـای سـایبر دنیـای آنلایـن از شـبکه‌های کامپیوتـری اسـت. [4] تعریـف دیگـر کـه از سـوی وزارت دفـاع آمریـکا ارائـه شـده اسـت، اشـاره می‌کنـد کـه فضـای مجـازی قلمرویـی جهانـی در فضـای اطلاعـات اسـت کـه ایـن محیـط شـبکه‌ای متصـل بـه هـم از زیرسـاخت‌ها را تشـکیل داده اسـت. [5] ایـن فضـا دربردارنـده شـبکه‌های ارتباطـات، سـامانه‌ها، کنترل‌کننده‌هـا و پردازشـگرها اسـت.

تعریـف دیگـر از فضـای سـایبری کـه از سـوی وینگفیلـد ارائـه شـده اسـت، بیـان مـی‌دارد کـه ایـن فضـا یـک محیـط فیزیکـی محسـوب نمی‌شـود، بلکـه فضایـی اسـت کـه از آن تحـت عنـوان «شـبکه فراگیـر جهانـی» یـاد می‌شـود. [6] همچنیـن یـک تعریـف دیگـر در ایـن زمینـه اشـاره می‌کنـد کـه فضـای سـایبر دربردارنـده تعامـلات افـراد بـه وسـیله سیسـتم‌هایی اسـت کـه از راه دور بـا یکدیگـر ارتبـاط دارند. [7] فـارغ از عبارتـی کـه در تعریـف فضـای سـایبری می‌تـوان اسـتفاده کـرد، مهـم ایـن اسـت کـه بـر خـلاف

1.Collin, The Future of Cyberterrorism: Where the Physical and Virtual Worlds Converge, 2017, p: 21.
2.Cornish, on cyber Warfare, A Chatham House Report, 2010, p: 8.
3.Hansen, Genetic programming for prevention of cyberterrorism through dynamic and evolving intrusion detection, 2016, p: 61.
4.https://www.merriam-webster.com/dictionary/cyberspace
5.Defense Department Cyber Efforts, 2017, p: 13.
6.Wingfield, The Law of Information Conflict: National Security Law in Cyberspace, 2016, p: 10.
7.Schaap, Cyber Warfare Operations: Development and Use under International law, 2014, p: 20.

دیدگاه-هایی که فضای سایبری را غیرواقعی تلقی می‌کنند و بر این باور هستند که این فضا در عرض دنیای واقعی قرار دارد؛ پیامدهای واقعی این فضا بر زندگی افراد بیانگر آن است که فضای سایبری نیز همچون فضای فیزیکی، فضایی واقعی محسوب می‌شود.

۱-۳. تروریسم سایبری

اصطلاح تروریسم سایبری که نخستین بار توسط کالین باری[1] مورد استفاده قرار گرفته است، از در کنار هم قرار گرفتن دو واژه تروریسم و فضای سایبری ایجاد شده است.[2] بر اساس تعاریف ذکر شده برای تروریسم و فضای سایبری، تروریسم سایبری به پدیده‌ای گفته می‌شود که از بستر اینترنت برای اهداف تروریستی استفاده می‌کند.

چنانچه پیشتر شرح داده شد، واژه تروریسم در «تروریسم سایبری» حامل نوعی از ترس و هراس است و تروریسم سایبری با بهره‌برداری از فضای سایبری به چنین هراسی دامن می‌زند.

بنابراین، تروریسم سایبری را می‌توان هرگونه اقدام خشونت آمیز در فضای سایبری تعریف کرد که به منظور ایجاد هراس و با اغراض سیاسی، انجام می‌شود.

تروریسم سایبری، با استفاده از فضای اینترنت و شبکه‌های رایانه‌ای، مقاصد مختلفی را مورد توجه قرار می‌دهد. به‌عنوان نمونه، شبکه‌های زیربنایی بازیگران هدف از جمله انرژی، راه‌های ارتباطی و تاسیسات دولتی، در دایره اهداف تروریسم سایبری قرار می‌گیرند.

1.Collin Barry
2.Walker, cyber terrorism. legal principle and law in the united kingdom, 2016, p: 31.

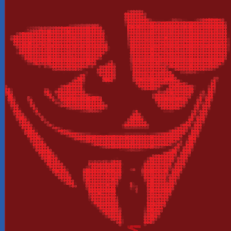
بسیاری از حملاتی که در قالب تروریسم سایبری انجام می‌گیرد، آن دسته از اقداماتی هستند که هکرها به آن دست می‌زنند. این رفتارها با تبعات زیان‌بار همراه است.[1] رویکردهای مجرمانه در این دسته از حملات متفاوت هستند: ممکن است این حملات، مقدمه‌ای برای به دست آوردن داده‌هایی برای جرایم دیگر باشد[2]؛ دسته دیگری از این اقدامات، حملاتی هستند که مستقیماً در حکم جرایم سایبری به شمار می‌روند.

این حملات از طریق افرادی انجام می‌گیرد که از آن‌ها تحت عنوان معترضان سایبری نام می‌برند.[3] پاره‌ای از این اقدامات تروریستی، به وسیله ایمیل‌های آلوده انجام می‌گیرد. در حال حاضر و با توجه به پیچیدگی ویروس‌هایی که در حملات سایبری مورد استفاده قرار می‌گیرند، رایانه‌ها آسیب‌پذیرتر شده‌اند و اکثر سیستم‌های مورد استفاده کنونی، درصدی از آسیب‌پذیری را دارند. همین آسیب‌پذیری موجب شده است که حملات تروریستی افزایش چشمگیری داشته باشند.

1.Annamarie, terrorism as deviance or social control, 2016, p: 76-75.
2.Podgar, Cyber crime: transnational or international, 2014, p: 83-82.
3.Seddon, Cyber terrorism, 2017, p: 38-37.

بخش دوم

ویژگی های تروریسم سایبری



CYBER TERRORISM

بخش دوم

ویژگی‌های تروریسم سایبری

پس از ارائه تعاریف تروریسم سایبری، در این بخش، ویژگی‌های این نوع از تروریسم شرح داده می‌شود. تروریسم سایبری در جوامع کنونی شیوع یافته است و چنانچه در مقدمه نیز ذکر شد، تروریسم در فضای سایبری از قدرت مانور بیشتری برخوردار است و مقابله با آن، به آسانی مقابله با تروریسم در فضای فیزیکی نیست؛ لذا شناخت ویژگی‌های آن ضروری به نظر می‌رسد.

۲-۱. گستردگی عاملان

ماهیت تروریسم سایبری به‌گونه‌ای است که بازیگران مختلفی دست به این اقدام می‌زنند. این عاملان دربرگیرنده افراد و گروه‌های دولتی و خصوصی هستند.[1] این گستردگی عاملان، خود از سهولت دسترسی به رایانه و اینترنت ناشی می‌شود. به عبارت دیگر، از آن‌جایی که ابزار استفاده شده در حملات سایبری شامل رایانه‌ها و خطوط اینترنتی هستند؛ انجام این نوع از تروریسم صعوبت چندانی ندارد.

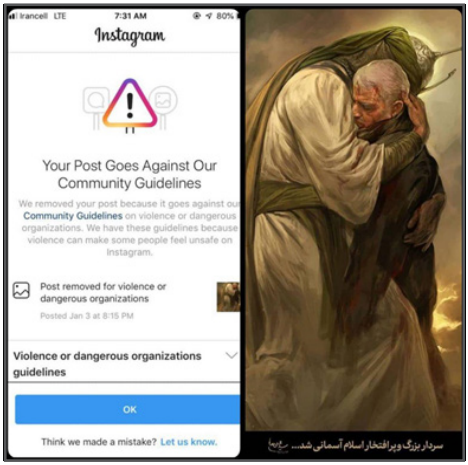
1.Starr, Towards an Evolving Theory of Cyber power, 2015, p: 13-12.

همچنین با توجه به اینکه بیشتر فعالیت‌های شخصی و سازمانی در اکثر کشورهای دنیا به وسیله سیستم‌های رایانه‌ای متصل به اینترنت انجام می‌گیرد؛ لذا کاربران این سیستم‌ها در معرض این نوع از تروریسم قرار دارند. علی‌رغم گستردگی این نوع از تروریسم، اشخاص و سازمان‌ها شناخت کافی از چنین حملاتی ندارند و بنابراین، به راحتی در معرض حملات سایبری قرار می‌گیرند. این در حالی است که افزایش اطلاعات در این زمینه می‌تواند مانعی برای حملات و تروریسم سایبری باشد.

عاملان اقدامات تروریستی در بستر سایبر، صرفاً در داخل یک کشور نیستند، بلکه در بیشتر موارد، این عاملان خارجی هستند که به اهداف خود در یک کشور دیگر حمله می‌کنند. با توجه به اینکه شناخت عاملان این اقدامات به سادگی امکان‌پذیر نیست، تروریسم سایبری در حال حاضر از سوی کشورهای متخاصم مورد بهره‌برداری قرار می‌گیرد.[1] از آن‌جایی که جنگ‌های سخت در فضای فیزیکی، هزینه‌ها و تبعات بسیاری به همراه دارد، اکنون بسیاری از بازیگران سیاسی که به دنبال هدف قرار دادن دیگر بازیگران هستند، از تروریسم سایبری استفاده می‌کنند. بر این اساس می‌توان گفت که بازیگران دولتی، نقش مهمی در پیشبرد تروریسم سایبری دارند.[2] چنانچه چنین حمایت‌هایی انجام نگیرد، می‌توان انتظار داشت که درصد قابل توجهی از اقدامات تروریستی در فضای سایبر کاهش پیدا کند؛ اما افزایش چنین اقداماتی موید این نکته است که بازیگران

1.Tosini, Sociology of Terrorism and Counterterrorism: A Social Science Understanding of Terrorist Threat, 2018, p: 50-49.
2.Walker, cyber terrorism. legal principle and law in the united kingdom, 2016, p: 24.

دولتی متخاصم از این رفتارها حمایت می‌کنند. در حقیقت، چنین اقداماتی در بسیاری از اوقات به سفارش این بازیگران صورت می‌گیرد و می‌توان ادعا کرد که کشورهایی که به دنبال حمله به اهداف خود هستند، با صرف هزینه‌هایی اقدام به سفارش این قبیل اقدامات تروریستی می‌کنند. به عنوان نمونه ایالات متحده آمریکا برای دستیابی به اهداف خود از تروریسم سایبری بهره‌برداری می‌کند؛ به‌گونه‌ای که برخی از شبکه‌های اجتماعی در فضای سایبری در راستای منافع واشنگتن حرکت می‌کنند. اقدام اینستاگرام در انسداد صفحات مربوط به سردار سلیمانی در مسیر تروریسم سایبری قابل تفسیر است. همچنین حذف دامنه بین‌المللی خبرگزاری فارس توسط آمریکا گام گذاشتن در تروریسم سایبری محسوب می‌شود. همه این نمونه‌ها نشان می‌دهد که بازیگران دولتی نقش ویژه‌ای در این نوع از تروریسم دارند.



تصویر ۱: حذف پست‌های مربوط به شهادت سردار سلیمانی توسط اینستاگرام

گروه‌های فروملی نیز در مساله تروریسم سایبری جایگاه مهمی دارند؛ چراکه این گروه‌ها در اکثر اوقات برای رساندن پیام‌های خود و یا گرفتن امتیازهایی از دولت‌ها اقدام به این کار می‌کنند.[1] آن‌ها با توجه به ناشناس ماندن عاملان در این فضا، به راحتی می‌توانند قدرت مانور داشته باشند؛ لذا فضای سایبر را مجرای مناسبی برای انتقال پیام‌های خود می‌دانند. بر این اساس، در برخی از اوقات مشاهده می‌شود که گروه‌های فروملی اقدام به هک یا نفوذ در نهادهای دولتی می‌کنند. اقلیت‌ها و گروه‌هایی که به دنبال اهداف خاصی هستند نیز از این فضا برای پیشبرد مقاصد خود استفاده می‌کنند.

1.Gina, Cyber Crimes, 2010, p: 75.

۲-۲. ردیابی دشوار

تروریسم سایبری در بیشتر اوقات به راحتی قابل ردیابی نیست و بنابراین، عاملان این نوع از تروریسم، حاشیه امن بیشتری را احساس می‌کنند. بر این اساس، عامل مذکور بر گستردگی این اقدامات نیز تاثیرگذار است.[1] گمنام ماندن عاملان حملات سایبری یکی از نکات کلیدی است که در تروریسم سایبری مورد توجه و استفاده است. این حملات نه تنها به آسانی مورد شناسایی قرار نمی‌گیرند، بلکه مقابله با آن‌ها نیز به سادگی ممکن نیست. در بسیاری از اقدامات تروریستی که در فضای سایبری انجام می‌گیرد، عاملان روش‌های پیچیده‌ای را برای نفوذ به اهداف خود به کار گرفته‌اند.[2] این موضوع نشان می‌دهد که آن‌ها از اطلاعات و آگاهی‌های گسترده‌ای در این زمینه برخوردار هستند؛ لذا برخورد با این عاملان و اقدامات نیز نیازمند داشتن سطحی همتراز از دانش فناوری خواهد بود؛ در غیر این صورت، پاسخ مناسبی منتقل نخواهد شد. این امر، موید این نکته است که کشورهایی که دارای سطح بالایی از دانش فناوری‌های سایبری هستند، به راحتی مورد هدف عاملان تروریستی قرار نمی‌گیرند.[3] همچنین این کشورها، در اکثر اوقات می‌توانند از این فناوری همچون سلاحی در مقابل رقبا و دشمنان خود استفاده کنند. نکته مهم دیگر در این زمینه، عبارت است از اینکه زمانی که تروریسم سایبری با حمایت کشورهایی با فناوری سایبری درخور انجام می‌گیرد، پاسخ به این حملات به سادگی ممکن نخواهد بود.

1.Charney, Rethinking the Cyber Threat A Framework and Path Forward, 2017, p: 56.
2.Lord, America's Cyber future Security and Prosperity inthe Information Age, 2014, p: 50-49.
3.Rodriguez, Cyber terrorism, 2016, p: 20-19.

ایـن موضـوع نشـان می‌دهـد کـه بـرای واکسـینه شـدن در مقابـل تروریسـم سـایبری، چـاره‌ای به‌جـز افزایـش دانـش فناورانـه در ایـن حـوزه وجـود نـدارد؛ در غیـر ایـن صـورت، امـکان مواجهـه بـا چنیـن حملاتـی در هـر لحظـه، وجـود دارد و ایـن امـر، تاثیـرات جبران‌ناپذیـری در پـی خواهـد داشـت. بنابرایـن بهتریـن شـیوه پاسـخ بـه تروریسـم سـایبری، قدرتمنـد شـدن در ایـن حـوزه اسـت. پیشـرفت روزافـزون دانـش سـایبری باعـث شـده اسـت کـه اقدامـات تروریسـتی در ایـن فضـا بـا روش‌هـای نویـن انجـام گیـرد. بـر ایـن اسـاس فنـاوری و دانـش تخصصـی در ایـن زمینـه، روزبـه‌روز بیشـتر مـورد توجـه قـرار می‌گیـرد. مقابلـه بـا تروریسـم سـایبری نیازمنـد برخـورداری از تخصص‌هـای لازم در ایـن حـوزه اسـت.

۲-۳. دشواری اثبات وقوع جرم

اقدامـات تروریسـتی در چارچـوب تروریسـم سـایبری، نه‌تنهـا قابلیـت ردیابـی سـختی دارنـد، بلکـه پـس از شناسـایی نیـز اثبـات جـرم بـه آسـانی امکان‌پذیـر نیسـت.[1] لزومـا همـه کشـورهای دنیـا قوانیـن لازم در ایـن زمینـه را بـه تصویـب نرسـانده‌اند و یـا قوانیـن موجـود بـا توجـه بـه پویایـی فضـای مجـازی، قابلیـت جواب‌گویـی بـه نیازهـای موجـود را نـدارد؛ لـذا عامـلان تروریسـم سـایبری از ایـن حیـث نیـز به سـهولت بیشـتری اقـدام به خرابـکاری در فضـای سـایبر می‌کننـد. حتـی اگر قوانین سـایبری پاسـخ‌گوی جرایـم ایـن حـوزه باشـد، در برخـی از اوقـات غیـر قانونـی بـودن اقدامـات در حـوزه سـایبری چنـدان قابـل تشـخیص نیسـت[2]؛ چراکـه مولفه‌هـای

1.Errol P, Democracy, Human Rights and the New Information Technologies in the 21st Century-The Law and Justice of Proportionality and Consensual Alliances, 2013, p: 363.
2.Noel, The regulation of cyberspace and the loss of national sovereignty, 2014, p: 102-101.

لازم بـرای اثبـات جـرم در فضـای سـایبری بـه سـادگی ممکـن نیسـت. ایـن نـکات مویـد ایـن واقعیـت اسـت کـه مقابلـه بـا تروریسـم سـایبری، نیازمنـد بررسـی‌های دقیـق حقوقـی در ایـن زمینـه اسـت تا زوایـای مختلـف اقدامات در ایـن حـوزه مشـخص شـود. ایـن امـر بسـتر لازم بـرای جلوگیـری از بـروز اقدامـات غیـر قانونـی در فضـای سـایبر را فراهـم خواهـد سـاخت. حتـی بـه نظـر می‌رسـد بـه مطالعـات میان‌رشـته‌ای در ایـن زمینـه نیـاز اسـت تـا ابعـاد فنـی و حقوقـی اقدامـات، بـا دقـت لازم مـورد تحلیـل قـرار گیـرد.[1] مطالعـات حقـوق سـایبر، می‌توانـد خلأهـای موجـود را شناسـایی کنـد و پاسـخ‌های درخـوری بـرای آن بیابـد. از آن‌جایـی کـه بازیگـران متخاصـم از فضـای سـایبر بـرای رسـیدن بـه اهـداف غیـر مشـروع خـود اسـتفاده می‌کننـد، حقـوق سـایبر می‌توانـد چنیـن رفتارهایـی را در مراجـع قانونـی رسـیدگی کنـد. همچنیـن پرداختـن بـه چنیـن مطالعاتـی، زمینـه افزایـش آگاهی‌هـای عمومـی را در حـوزه حقـوق سـایبری گسـترش خواهـد داد. ممکـن اسـت برخـی از افـراد بـدون آگاهـی از حقـوق فضـای سـایبر دسـت بـه اقدامـات غیـر قانونـی بزننـد کـه افزایـش اطلاعـات در ایـن حـوزه، بـرای جلوگیـری از چنیـن اقدامـات ناآگاهانـه‌ای مثمـر ثمـر خواهـد بـود.

۲-۴.آسیب‌زایی گسترده

در حـال حاضـر، زندگـی اقتصـادی و اجتماعـی مـردم وابسـتگی‌های زیـادی بـه فضـای سـایبری دارد. تـا جایـی کـه حتـی ایـن فضـا بـر حیـات سیاسـی و فرهنگـی مردمـان نیـز تاثیرگـذار اسـت. حـال بـا توجـه بـه حضـور پررنگ

1.Henry, Cyberspace Self-Government: Town Hall Democracy or Rediscovered Royalism?, 2016, p: 423.

فضای سایبر در زندگی شهروندان، اختلال در این فضا می‌تواند تبعات مخرب گسترده‌ای به همراه داشته باشد. جهت‌دهی‌های رسانه‌ای و جنگ‌های روانی که علیه بازیگران هدف در فضای سایبر روی می‌دهد، آسیب‌های بلندمدتی بر جای می‌گذارد. از آن‌جایی که انسان‌ها با تصویری که از حقیقت دارند، نسبت به موضوعات و مسائل مختلف واکنش نشان می‌دهند، تصویرسازی ایجابی یا سلبی از حقایق در ذهنیت مخاطبان تاثیر می‌گذارد[1]. در حقیقت یک جنگ حاد بین حقایق و تصاویر وجود دارد و آنجا که تصاویر ارائه شده از حقیقت به جای حقایق واقعی القا می‌شوند، ذهن مخاطبان با سوالات و ابهامات زیادی مواجه می‌شود.[2] فضای سایبر نیز در این بازی رسانه‌ای نقش فوق‌العاده‌ای بر عهده دارد. با توجه به اینکه شبکه‌های اجتماعی به صورت قارچی رشد کرده‌اند، این شبکه‌ها می‌توانند حقایق مد نظر را در قالب تصاویر به عنوان حقیقت واقعی ارائه و القا کنند. این موضوع در ذهنیت جوامع امروز تاثیرات زیادی بر جای گذاشته است. مخاطبان این فضا در اکثر اوقات به دنبال اثبات یا رد تصاویر ارائه شده نیستند و آن را به عنوان واقعیت می‌پذیرند. گستره تروریسم سایبری بر میزان آسیب‌زایی آن تاثیرگذار است و تروریسم سایبری با اقدامات پیچیده خود، تلاش می‌کند از گستره فضای سایبر نهایت بهره‌برداری را داشته باشد. عاملان تروریسم سایبری با اقدامات خود به دنبال تخریب یا گرفتن امتیازاتی از بازیگر هدف هستند.

با توجه به آنچه گفته شد، آسیب‌های حاصل از حملات سایبری

1.Dorothy, Cyberterrorism, 2015, p: 37.
2.Gabriel, Cyberterrorism: how real is threat?, 2014, p: 29.

درخـور توجـه ویـژه اسـت. بـه عنـوان نمونـه، می‌تـوان بـه از بیـن رفتـن داده‌هـا و اطلاعـات سیسـتم‌ها بـه دنبـال حمـلات سـایبری اشـاره کـرد کـه تاثیـرات تخریبـی گسـترده‌ای در پـی خواهـد داشـت. در بسـیاری از مـوارد، اقدامـات تروریسـتی در قالـب فضـای سـایبر، از داده‌هـای بازیگـران هـدف، بهره‌بـرداری می‌کننـد[1] ؛ به‌گونـه‌ای کـه هـک و نفـوذ بـه اطلاعـات اهـداف مـورد نظـر، گام نخسـت بـرای انجـام اقدامـات بعـدی در ایـن حـوزه بـه شـمار می‌آیـد. هکرهـا بـا نفـوذ بـا رایانه‌هـای شـخصی و سـازمانی اقـدام بـه دزدی اطلاعـات می‌کننـد و بهره‌برداری‌هـای پسـینی از ایـن داده‌هـا، موجـب افزایـش آگاهی‌هـای آن‌هـا از بازیگـر هـدف می‌شـود. همچنیـن ایجـاد اختـلال در سیسـتم‌های هـدف، بـا دسـتیابی بـه داده‌هـای آن امکان‌پذیـر می‌شـود. ایـن نـوع از اقدامـات می‌تواننـد آسـیب‌های حـادی را بـرای اهـداف خـود ایجـاد کننـد. ایـن اقدامـات در حالـی انجـام می‌گیـرد کـه هـدف مـورد هجـوم، ممکن اسـت امـکان پاسـخ‌گویی سـریع بـه مهاجم را نداشـته باشـد[2]؛ چراکـه در اکثـر اوقـات، شناسـایی عامـلان نیازمنـد دانش پیچیـده در ایـن زمینـه اسـت. توانایـی تاثیرگذاری بـر مهاجمان نیـز نیازمند برخـورداری از سـطح مطلـوب از دانـش فنـی در حـوزه سـایبری اسـت. اختلالاتـی کـه بـه دنبـال اقدامـات تروریسـتی در بسـتر سـایبر انجـام می‌گیـرد، همچنیـن می‌توانـد مشـکلات امنیتـی بـرای بازیگـر هـدف در پـی داشـته باشـد. بـه عنوان نمونـه نفوذ در شـبکه‌های بـرق و آب، زندگـی روزانه شـهروندان کشـور هـدف را بـا اخـلال مواجـه سـازد و چنانچه ایـن اختلالات تـداوم چنـدروزه داشـته باشـد، بـه اعتراضـات و آشـوب‌هایی مبدل‌شـود.[3]

1.james, Assessing the risk of cyberterrorism, cyber war and other cyber threats, 2013, p: 49.
2.Robert, the strategic logic of suicide terrorism, 2013, p. 343.
3.oates, owen and Gibson, the internet and politics; citizens, voters and activists, 2016, p: 64.

این نمونه موید نکته مذکور است که آسیب‌های تروریسم سایبری، ممکن است در دایره بسیار گسترده‌ای رخ دهد و به یک مسئله حاد امنیتی تبدیل شود. امروزه، کشورهای مختلف برای دور ماندن از چنین تهاجماتی تلاش می‌کنند تا اطلاعات فنی و سایبری خود را افزایش دهند. ایجاد پدافند سایبری از جمله اقداماتی است که در این زمینه انجام می‌گیرد. با این حال به نظر می‌رسد با توجه به گستردگی اقدامات تروریستی در این فضا شایسته است آگاهی‌های عمومی نیز در این باره افزایش یابد. ممکن است زیرساخت‌های سازمانی کشورها از این اقدامات مصون بماند؛ اما اشخاص مشغول در این سازمان‌ها، مورد حمله سایبری قرار گیرند. چنانچه رایانه‌های شخصی افراد تاثیرگذار سازمان‌های دولتی، مورد حمله سایبری قرار گیرد، ممکن است برخی از اطلاعات نهادها نیز به بیرون درز کند. بنابراین افزایش اطلاعات عمومی در این حوزه، بسیار ضروری است. نمونه‌ای که در میزان آسیب‌زایی تروریسم سایبری می‌توان بیان کرد، ادعای یکی از مقامات رسمی سیا است که به اعتقاد او تروریست‌ها در این فضا با صرف یک میلیارد دلار هزینه و استخدام بیست هکر حرفه‌ای می‌توانند زیرساخت‌های آمریکا را مختل سازند.[1] بر این اساس می‌توان گفت که حجم تخریبی در تروریسم سایبری بیش از اندازه‌ای است که انتظار می‌رود. این نکته را نیز باید اشاره کرد که نقاطی در اقدامات تروریستی در فضای سایبر مورد هدف قرار می‌گیرند که درصد تخریبی بیشتری داشته باشند. بنابراین زیرساخت‌های حیاتی

1.Schiller, Who Knows: information in the age of the fortune 2017 ,500, p: 25.

کشورها از جمله مهم‌ترین اهداف تروریست‌ها در این فضا هستند.

۲-۵. عدم محدودیت مکانی و زمانی

تروریسم سایبری مختص به جغرافیای مکانی و زمانی خاصی نیست؛ لذا عاملان آن در هر جغرافیایی می-توانند دست به عملیات بزنند. اهداف مورد نظر در اقدامات، صرفا در محدوده کشورها قرار ندارند؛ بلکه بسیاری از حملات سایبری در حال حاضر علیه کشورهای دیگر انجام می‌گیرد. گسترش فضای مجازی میدان عملیاتی جدیدی را برای عاملان تروریسم سایبری به وجود آورده است. این فضا بستری برای این نوع از تروریسم ایجاد کرده است که محدودیت‌های جهان بیرونی را ندارد[1] و عاملان آن اهداف خود را به سادگی دنبال می‌کنند. از آن‌جایی که دولت‌ها به دنبال کاهش هزینه‌های اداره کشور هستند، بیش از پیش به فضای سایبری روی آورده‌اند؛ اما رجوع به این فضا، لزوما با لوازم مورد نیاز آن، همراه نبوده است. بر این اساس، تروریسم سایبری نیز از این بستر بهره‌برداری می‌کند. دولت‌ها تنها حاضران در فضای سایبری نیستند، بلکه شرکت‌های خصوصی و اشخاص حقیقی نیز بنا به دلایلی از جمله کاهش هزینه‌ها در فضای سایبر، به این فضا علاقه‌مندتر شده‌اند. همه این زمینه‌ها دست به دست هم می‌دهد که عاملان تروریسم سایبری اهداف مورد نظر خود را در این فضا در تیررس خود بیابند.

سازمان‌های تروریستی از جمله عاملانی هستند که در فضای سایبر

1.William, terrorism Data Base: A comparison of Missions, Methods, and systems, 2013, p: 79-78.

دست به خرابکاری می‌زنند. این سازمان‌ها با توجه به آنچه بیان شد محدودیت زمانی و مکانی ندارند؛ لذا به راحتی می‌توانند مقاصد خود را مورد هدف قرار دهند.[1] این سازمان‌ها معمولا برای بسیج و جذب نیرو نیز از این فضا بهره‌برداری می‌کنند. به عنوان نمونه، گروه تروریستی داعش از فضای سایبری برای جذب نیرو و تبلیغ خود به صورت گسترده استفاده کرده است. همچنین گروه‌های تروریستی از فناوری‌های هوشمند و فضای سایبری برای به دست آوردن اطلاعات لازم جنگی بهره‌برداری می‌کنند. چنین فضایی برای تسهیل در اقدامات تروریستی آن‌ها بسیار موثر است. از آن‌جایی که به اعتقاد باری گوردن بوزان[2] (استاد روابط بین‌الملل دانشگاه اقتصاد لندن و نظریه‌پرداز نظریه مجموعه امنیتی منطقه‌ای) امنیت در نبود تهدید تعریف می‌شود؛ لذا تهدیدات حوزه سایبری نیز امنیت را مختل می‌سازد. حال، گستردگی اقدامات تروریستی در بستر سایبر موجب می‌شود که امنیت یک کشور و به عبارت دیگر امنیت ملی آن تحت‌الشعاع قرار گیرد.[3] با توجه به اینکه دایره این اقدامات محدود به مکان و زمان خاصی نیست؛ لذا چنین رفتارهایی امنیت ملی را به صورت پنهان مورد هدف قرار می-دهند. پیشرفت‌ها در حوزه فناوری ارتباطات، بستر لازم را برای جهانی شدن فراهم ساخته است. جهانی شدن ابعاد مختلفی را تحت تاثیر قرار می‌دهد. حوزه‌های مختلف سیاسی، اقتصادی، اجتماعی و فرهنگی، به دنبال جهانی شدن دچار تغییر و تحول می‌شوند. به عبارت دیگر،

1.CCDCOE, International cyber incidents: legal considerations, 2012, p: 45.
2.Barry Gordon Buzan
3.Dinstein, War, Aggression and self-defense, 2015, p: 24.

در نتیجه تغییرات گسترده در فناوری ارتباطات، محیط بین‌المللی نیز متحول شده است.[1] به عنوان نمونه، زمانی که تجارت الکترونیکی در اقتصاد ظهور یافت، تغییر شگرفی در محیط اقتصادی به وجود آورد. چنین تغییرات و عواملی در ایجاد جهانی شدن و تداوم آن نقش دارند[2]؛ به‌گونه‌ای که عنصر زمان و مکان، معنای پیشین خود را از دست داده است. گرچه ممکن است چنین فضایی در ابتدا مثبت ارزیابی شود؛ اما بسیاری از واحدهای سیاسی، تغییرات گسترده در این مقیاس را نمی‌پذیرند؛ چراکه این موضوع ارزش‌های مختص به خود را به همراه دارد.[3] باید توجه داشت که ارزش‌های جهانی‌شده و ارزش‌های ملی لزوما بر یکدیگر منطبق نیستند. تروریسم سایبری، در فضای جهانی‌شده ایجاد شده است و در این فضا به پیش می‌رود.[4]

۲-۶. هزینه‌های ارزان

در حال حاضر، رجوع به فضای سایبری با توجه به کاهش هزینه‌ها در این فضا، برای کاربران جذاب‌تر شده است؛ لذا طی سال‌های اخیر، بسیاری از فعالیت‌هایی که با صرف هزینه‌های هنگفت انجام می‌شد، اکنون در این فضا، با کمترین هزینه انجام می‌گیرد. با استفاده از بستر فضای مجازی، افراد در بسیاری از موارد برای انجام امور خود نیازی به مراجعات حضوری و صرف هزینه‌های مرتبط ندارند؛ لذا بسیاری از اقدامات مورد نیاز خود را در این فضا به انجام می‌رسانند. گرچه این امر راحتی بسیاری را برای زندگی کنونی ایجاد کرده است؛

1.Denning, Activism, Hacktivism and Cyberterrorism: the Internet as a Tool for Influencing Foreign Policy, 2013, p: 60-59.
2.Flemming, Myths and Realities of Cyberterrorism, 2014, p: 63.
3.Oots, Bargaining with Terrorist: Organizational Consideration, 2015, p: 19.
4.Rowe, and S.A, the Intelligent Information Systems: Meeting the Challenge in the Knowledge Era, 2012, p: 42.

اما اغلب افراد از آسیب‌های موجود در این فضا اطلاع چندانی ندارند.
افراد حقیقی، تنها کاربران فضای سایبری نیستند، بلکه اشخاص حقوقی به صورت گسترده‌تری در این فضا حضور دارند. دولت‌ها نیز در حال حاضر برای انجام بهتر امور خود و کاهش هزینه‌ها تلاش می‌کنند بسیاری از اقداماتی که در گذشته در فضای واقعی و به صورت سنتی انجام می‌گرفت، از طریق فضای سایبری به انجام برسانند.[1] بنابراین دولت‌ها نیز در معرض تروریسم سایبری قرار دارند. حتی این مساله برای دولت‌ها و نهادهای حاکمیتی بسیار مهم‌تر از اشخاص حقیقی است؛ چراکه میزان اطلاعات و داده‌هایی که در سایت‌های سازمان‌های دولتی وجود دارند، به مراتب از داده‌های رایانه‌های شخصی بیشتر و پراهمیت-تر است. علاوه بر آن برخی از دولت‌های متخاصم برای ضربه زدن به بازیگران هدف خود از فضای سایبری بهره‌برداری می‌کنند. حتی می‌توان گفت که درصد قابل توجهی از اقدامات تروریستی که در چارچوب تروریسم سایبری انجام می‌گیرد، با اطلاع و حمایت دولت‌های متخاصم شکل گرفته است.[2] در چنین فضایی و با در دسترس بودن این اهداف با طیف‌های گسترده (از دولت تا اشخاص حقیقی)، آنچه این فضا را برای انجام اقدامات تروریستی جذاب‌تر می‌کند، هزینه‌های پایین انجام این اقدامات در مقابل اقدامات در فضای فیزیکی است. انجام اقدامات تروریستی در فضای فیزیکی معمولا مستلزم فراهم آوری تجهیزات و امکاناتی است که هزینه‌های تامین مالی آن قابل توجه است. در

1.Sharp, cyber warfare and the use of force, 2013, p: 53.
2.Wingfield, the Law of Information Conflict: National Security Law in Cyberspace, 2016, p: 86.

مقابل بسیاری از حملات سایبری از رایانه‌هایی صورت می‌پذیرد که در بسیاری از خانه‌های معمولی در زندگی امروز یافت می‌شوند.
این موضوع باعث شده است که دولت‌ها بیش از پیش برای حفاظت از داده‌ها و اطلاعات موجود در فضای سایبری همت گمارند. اطلاع از تروریسم سایبری و اتخاذ پاسخ‌های مناسب در قبال این اقدامات تروریستی در فضای سایبری، گام نخست برای حفاظت بیشتر و بهتر از داده‌ها است.

۲-۷. استفاده گسترده از عنصر تصویرسازی

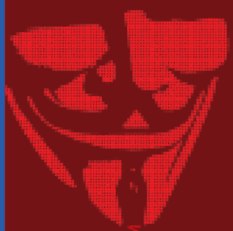
در فضای مجازی واقعیت‌های فیزیکی جای خود را به تصاویر داده‌اند و آنچه بازیگران از خود و مخاطبان خود به یاد دارند، پاره‌ای از تصاویر است که در برخی از اوقات از واقعیت‌ها منفک شده است. هر بازیگری تعریفی از خود در ذهن دارد که بر اساس همین ذهنیت با تصویری از بازیگر مقابل روبه‌رو می‌شود.[1] تصویری که بازیگر از خود به همراه دارد و تصویری که از مخاطب در ذهن تداعی می‌کند، ممکن است در عالم فیزیکی کاملا نادرست باشند. تروریسم سایبری از این ویژگی برای مشروع ساختن اقدامات خود بهره‌برداری می‌کند. به عنوان نمونه یک گروه تروریستی همچون داعش رسانه‌ای عظیم برای خود راه می‌اندازد و از این طریق سعی در وارونه جلوه دادن حقایق و ارائه تصاویر کاذب دارد. کشورهایی چون آمریکا در راستای همین ویژگی از تروریسم سایبری بدون اینکه مخاطبان به واقعیت‌ها پی ببرند، بهره‌برداری

1.Schaap,CyberWarfareOperations:DevelopmentandUseunderInternationallaw,2014,p:20.

می‌کنند. دنیای امروز در فضای رسانه‌ای دنیای جنگ تصویرها است و غلبه بازیگران با غلبه تصاویر به وجود می‌آید.

بخش سوم

تروریسم سایبری در بستر سکوهای ارتباطاتی



CYBER TERRORISM

بخش سوم

تروریسم سایبری در بستر سکوهای ارتباطاتی

پلتفرم یا سکو فرصت‌هایی برای مشاهده بهتر را فراهم می‌سازند.
جذابیت موجود در فضای سکوها باعث شده است که اقبال به آن‌ها افزایش یابد؛ اما همین بستر در برخی از اوقات به فضایی برای تروریسم سایبری تبدیل می‌شود. معروف‌ترین پلتفرم‌هایی که در نقاط مختلف دنیا مورد استفاده قرار گرفته‌اند، شامل اینستاگرام، لینکدین، فیس‌بوک، اوبر و آمازون هستند. شواهدی وجود دارد که نشان می‌دهد که این پلتفرم‌ها مورد سوءاستفاده برخی از بازیگران بین‌المللی قرار گرفته است.
قدرت‌های فرامنطقه‌ای در حال حاضر برای مشروعیت‌بخشی به اقدامات خود از شبکه‌های اجتماعی استفاده می‌کنند که این موضوع باعث قرابت اقدامات این قدرت‌ها به تروریسم سایبری می‌شود.[1] ازآن‌جایی که شبکه‌های اجتماعی پوشش جذابی در نگاه مخاطبان دارد، وقوع تروریسم سایبری در این فضا چندان ملموس نیست. همین ویژگی باعث شده است که قدرت‌های

1.Lord, America's Cyber future Security and Prosperity inthe Information Age, 2014, p: 50-49.

بزرگ از این فضا در راستای منافع خود بهره-برداری کنند.

تروریسم سایبری به صورت گسترده از شبکه‌های اجتماعی برای پیشبرد اهداف خود بهره‌برداری می-کند؛ به‌گونه‌ای که این شبکه‌ها بستر مناسبی برای چنین تروریسمی فراهم ساخته‌اند.[1] اینستاگرام[2] یکی از شبکه‌های محبوب اجتماعی است که امکان هم‌رسانی ویدئو و عکس را فراهم می‌سازد. دفتر مرکزی شرکت اینستاگرام در شهر سان فرانسیسکو از شهرهای ایالت کالیفرنیا در ایالات متحده آمریکا قرار دارد و واشنگتن از این شبکه در راستای منافع خود بهره‌برداری می‌کند. اقدام این شبکه در محدود سازی اخبار و تصاویر مربوط به شهادت سردار سلیمانی در راستای تروریسم سایبری قابل تفسیر است. آمریکا برای تامین منافع خود از پلتفرم‌هایی چون اینستاگرام و فیسبوک بهره‌برداری می‌کند و پی بردن به شواهد این واقعیت چندان دشوار نیست. اولا اشخاصی چون مارنی لِون که مدیر اجرایی اینستاگرام هستند، با آژانس اطلاعات مرکزی آمریکا[3] «سیا» مرتبط هستند[4] ؛ لذا می‌توان ادعا کرد که این پلتفرم‌ها بستری جدید برای جاسوسی و موجه جلوه دادن چهره ایالات متحده آمریکا به شمار می‌آیند. ثانیا عملکرد این شبکه‌ها نیز در راستای منافع آمریکا قرار دارد. زمانی که صفحات مربوط به سردار سلیمانی به عنوان چهره مبارزه با تروریسم از اینستاگرام حذف می‌شود، این اقدام به این معنا است که پلتفرم‌هایی چون اینستاگرام نیز در مسیر اقدامات واشنگتن گام برمی‌دارند. همان طور که

1.Denning, Activism, Hacktivism and Cyberterrorism: the Internet as a Tool for Influencing Foreign Policy, 2013, p: 60-59.
2.Instagram
3.Central Intelligence Agency
4.https://twitter.com/h0d3r_fa/status/1118144867090227200?lang=fa

آمریکا سردار سلیمانی را سدی در برابر اقدامات تجاوزکارانه خود می‌دانست، پلتفرم‌های آمریکایی نیز انتشار تصاویر و ویدئوهای مربوط به ایشان را برخلاف سیاست‌های خود می‌دانند.

تروریسم سایبری در بستر اینستاگرام محدود به بازیگران دولتی نیست، بلکه گروه‌های تروریستی نیز از این فضا برای ترویج اندیشه‌های خود بهره‌برداری می‌کنند. بر اساس تحلیل داده‌های شرکت «دیتا گوست» بیش از پنجاه هزار حساب کاربری در اینستاگرام در سال ۲۰۱۷ مربوط به گروه تروریستی داعش بود. [1] فیسبوک[2] نیز به عنوان یکی دیگر از شبکه‌های اجتماعی همراستا با سیاستهای دولت مریکا، دفتر مرکزی آن در شهر منلو پارک ایالت کالیفرنیا در ایالات متحده آمریکا قرار دارد. این شبکه اجتماعی در حال حاضر بیش از دو میلیارد کاربر فعال دارد که این میزان از کاربران آن را به بزرگ‌ترین شبکه اجتماعی در دنیا تبدیل کرده است. مسدود سازی صفحات مربوط به حزب الله لبنان و تلویزیون المنار را می‌توان نمونه‌ای از اقدامات تروریستی این سکوی ارتباطی به شمار آورد.

در حال حاضر دو سکوی بزرگ اینستاگرام و واتس‌اپ نیز در مالکیت فیس‌بوک قرار دارند. مارک زاکربرگ[3] رئیس هییت مدیره و مدیراجرایی فیسبوک است. جستجو در سوابق این فرد نشان می‌دهد که لابی‌های صهیونیستی و سرویس‌های جاسوسی حمایت‌های گسترده‌ای از وی به عمل آورده‌اند.

1.https://farsi.euronews.com/22/09/2017/jihadists-flee-to-instagram-after-purge-on-facebook
2.Facebook
3.Mark Elliot Zuckerberg

نمونه‌هایی از ارتباطات زاکربرگ با رژیم صهیونیستی نشان می‌دهد که او تحت حمایت‌های این رژیم قرار دارد. بنیامین نتانیاهو، نخست‌وزیر رژیم صهیونیستی درباره وی گفته است که او از وفادارترین افراد به آرمان‌های رژیم اسرائیل محسوب می‌شود.

Facebook founder Mark Zuckerberg, with Israeli Prime Minister Benjamin Netanyahu.

دیدار زاکربرگ و نتانیاهو

مایکل وینسنت هِیدن، رئیس پیشین سیا در موضع‌گیری خود در قبال فیسبوک اظهار کرده است که این پلتفرم خطرناک‌تر از سازمان‌های جاسوسی محسوب می‌شود. او بر این عقیده است که زوکربرگ نفوذ گسترده‌ای بر حریم خصوصی دارد. حجم ارتباطات مالک اینستاگرام و فیسبوک با دولت آمریکا نیز به اندازه‌ای است که باراک اوباما در جشن تولد مارک زوکربرگ حضور یافته بود.

این امر در تاریخ آمریکا رویدادی بی‌سابقه تلقی شده است. زوکربرگ فارغ‌التحصیل دانشگاه هاروارد است و زمانی که در این دانشگاه تحصیل می‌کرد، به انجمن Eta Psi پیوست. حضور وی در لیست افراد فرقه شیطان‌پرستی AEPi نیز جالب توجه است.

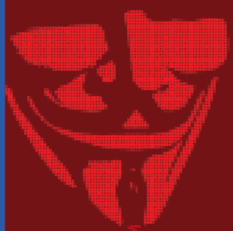
Jack Stahl	Epsilon	President of Revlon; former president of Coca-Cola	
Steve Stone	Phi Deuteron	Cy Young Winner 1980; Baltimore Orioles, Chicago White Sox TV color analyst	[1]
David Suissa	Honorary	Writer; President of *The Jewish Journal of Greater Los Angeles*	[29]
Yosef Tarshish (Joe Tarsh)	Upsilon Kappa Zeta	President of the Union of Jewish Students of the UK & Ireland 2013-14; Chair of the World Union of Jewish Students 2016-17	
John E. Wallace, Jr.	Rho Deuteron	New Jersey Supreme Court Justice, appointed May 20, 2003	
Sanford I. Weill	Beta	Co-chairman of Citigroup	[1]
Josh Weinstein	Pi Tau	Founder of YouAreTV, an interactive video platform[30]	[6]
Matt Weitzman	Sigma Pi	Co-creator and Co-Executive Producer of *American Dad!*	[1]
Adam Wexler	Omicron	Creator of GoRankem[31] and Insightpool[32]	[1]
Gene Wilder	Iota Upsilon	Actor, producer, and director	[1]
Walter Winchell	Lambda Deuteron	Gossip columnist, radio personality	[1]
Scott Wolf	Kappa Deuteron	Actor	[1]
Michael Yormark	Delta Deuteron	President of Roc Nation Sports	[1]
H. Albert Young	Rho Deuteron	Former Delaware Attorney General	[1]
Sam Zell	Omega Deuteron	Real estate entrepreneur; co-founder and chairman of Equity International; owner of the Tribune Company	[1]
Mark Zuckerberg	Eta Psi	Founder of Facebook	[33]
Danny Sprung	Delta	Masters, Recreation Sport & Tourism	[1]
Zach Tyler Eisen	Sigma Deuteron	Actor and voice actor; voice of Aang on *Avatar: The Last Airbender*	[34]
Vin Diesel	Hunter College	Actor '	[35]

• Italics indicate a deceased member. Deceased AEPis are said to enter the "Chapter Eternal."

خلاصه اینکه مستندات مذکور به خوبی نشان می‌دهد که مالک اینستاگرام، فیسبوک و واتس‌آپ رابطه گسترده‌ای با آمریکا و رژیم صهیونیستی دارد؛ لذا چندان عجیب نیست که سیاست‌گذاری‌های سکوهای مذکور نیز منطبق با خواست دولت‌های مذکور انجام می‌پذیرد.

بخش چهارم

راهبردهای پیشنهادی



CYBER TERRORISM

بخش چهارم

راهبردهای پیشنهادی

با توجه به مشخص شدن دایره معنایی تروریسم سایبری و ویژگی‌های آن، می‌توان راهبردهایی در این زمینه، مختص به کشورمان ارائه داد. از آن‌جایی که این مفهوم در کشورمان چندان مورد تحلیل قرار نگرفته است؛ لذا پژوهش حاضر تلاش داشت نقصان موجود در این زمینه را جبران کند. راهبردهای پیشنهادی به شرح زیر است:

- از آن‌جایی که منبع اقدامات تروریسم سایبری صرفا در محیط داخلی نیست؛ لذا ضروری است که بازیگران بین‌المللی در راستای مبارزه با این پدیده با یکدیگر همکاری کنند. هماهنگی نیروهای امنیتی کشورهای مختلف در این خصوص، از جمله راهبردهای پیشنهادی است.
- مقابله با حملات سایبری و تروریسم در این فضا، با پیچیدگی همراه است؛ بنابراین نیروهای داخلی لازم است به صورت هم‌افزا و هماهنگ، و تحت نظارت شورای عالی فضای مجازی (به عنوان عالی‌ترین سطح تصمیم‌گیری فضای مجازی در کشور) اقدام کنند.
- از آن‌جایی که دولت‌ها بیش از پیش به دنبال الکترونیکی کردن خدمات

در حوزه‌های مختلف اقتصادی و اجتماعی هستند؛ لذا نیاز است چالش‌های موجود در حوزه تروریسم سایبری قبل از هر اقدامی در این حوزه‌ها مورد توجه قرار گیرد.

- انقلاب اطلاعاتی باعث پیشرفت سریع و فزاینده در حوزه سایبری شده است؛ اما آگاهی لازم برای بهره‌برداری از این فضا با میزان استفاده‌ای که از آن انجام می‌گیرد، لزوما متناسب نیست. بر این اساس نیاز است که آگاهی‌های عمومی از تهدیدات موجود افزایش یابد.
- رسیدگی به اقدامات غیر قانونی در فضای سایبری، نیازمند تشریح دقیق قوانین در این حوزه است. ضعف قوانین در حوزه سایبری موجب افزایش جرایم در این حوزه شده است. لازم است قوانین در این حوزه به روز باشند.
- پرداختن به مطالعات حقوق سایبری در قالب مطالعات میان‌رشته‌ای یکی از راهکارهای لازم برای کاهش زمینه‌های اقدامات غیر قانونی در حوزه سایبر محسوب می‌شود.
- یکی از راه‌های مناسب برای پیگیری برخی اقدامات تروریستی در فضای سایبر، رجوع به مراجع قانونی بین المللی است. لازمه این کار نیز فعال‌تر شدن در این مراجع است.
- به‌کارگیری ظرفیت‌های آموزشی کشور برای تربیت متخصصان در حوزه سایبری و آشنایی آن‌ها با به‌روزترین اقدامات تروریستی در بستر سایبری از نیازها و اولویت‌های کشورمان است.
- شایسته است مصون‌سازی رایانه‌ها و سیستم‌های هوشمند نهادها و

اشـخاص مهـم در اولویـت قـرار گیـرد. سـپس ایـن موضـوع در سـطح گسـترده‌ای نیازمنـد پیگیـری اسـت.

منابع

[1]Annamarie, Oliverio &Pat, Lauderdale (2016), «terrorism as deviance or social control», Sage Publication, London, Thousand Oaks and New Delhi.
[2]Aaviksoo, Jaac (2010), "Cyber-attacks against Estonia Raised Awareness of Cyber threats", Defenses against Terrorism Review, Vol.3, No 2.
[3]Bogdanosky, Mitko (2013), "Cyber Terrorism– Global Security Threat, International Scientific Defence", Security And Peace Journal, NO. 13)24).
[4]Brenner, Susan & Marc Goodman (2012), "In Defense of Cyberterrorism: An Argument for Anticipating Cyber Attacks", Journal of Law, Technology and Policy.
[5]Capaldo, Giuliani ziccardi (2017), "providing a Self-Defense against large scale attacks by irregular forces: The Israeli- Hezbollah conflict", Harvard international law journal, vol. 48.
[6]CCDCOE (2012), International cyber incidents: legal considerations.
[7]Charney, Scott (2017); "Rethinking the Cyber Threat A Framework and Path Forward",Microsoft Corp. • One Microsoft Way • Redmond, WA 6399-98052 • USA.
[8]Clay, Wilson (2013), "Information Warfare and Cyberwar: Capabilities and Related Policy Issues", CRS Report RL31787.
[9]Collin, Barry (1997). The Future of Cyberterrorism: Where the Physical and Virtual Worlds Converge, 11th Annual International Symposium on Criminal Justice Issues.

[10]Cornish, Paul and et seq (2010), "on cyber Warfare, A Chatham House Report".

[11]Council of Europe (2015), The threat of cybercrime, Situation report, Council of Europe Publishing, p: 171.

[12]Defense Department Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities, (2017).

[13]Denning, Dorothy (2013), Activism, Hacktivism and Cyberterrorism: the Internet as a Tool for Influencing Foreign Policy, In: Aquila and Ronfeldt, Networks and Net wars: the Future of Terror, Crime, and Militancy, Santa Monica, RAND Corporation.

[14]Dinstein, Yoram (2015), War, Aggression and self-defense, Cambridge University press, 4th ed.

[15]Dorothy, Denning (2015), Cyberterrorism, united states: Georgetown university.

[16]Errol P. Mendes (2013), Democracy, Human Rights and the New Information Technologies in the 21st Century-The Law and Justice of Proportionality and Consensual Alliances, National Journal of Constitutional Law, no. 10.

[17]Flemming, Peter (2014). Myths and Realities of Cyberterrorism, Office of International Programs and the Center for Education and Research in Information Assurance and Security, Purdue University.

[18]Gabriel, Weimann (2004), Cyberterrorism: how real is threat? United states: institute of peace.

[19]Gina. De, Angelis (2010), Cyber Crimes, Chelsea House Publisher.

[20]Hansen, James and et seq (2016), Genetic programming for prevention of cyberterrorism through dynamic and evolving intrusion detection, Decision Support System, Vol.43.

[21]Henry H, Perritt, JR (2016), Cyberspace Self-Government: Town Hall Democracy or Rediscovered Royalism?, Berkeley Technology Law Journal, vol. 12.

[22]james, lewis (2013), Assessing the risk of cyberterrorism, cyber war and other cyber threats, center for strategic and international studies.

[23]Lord, Kristin M. & Sharp, Travis (2014), "America's Cyber future Security and Prosperity inthe Information Age", Center for a New American Security, VolumeI.12

[24]Merari, A (2013), Terrorism as a Strategy of Insurgency, Terrorism and Political Violence, Volume5, No. 4.

[25]Noel, Cox (2014), "The regulation of cyberspace and the loss of national sovereignty", Auckland University of Technology, Auckland.

[26]Oots, Kent (2015), Bargaining with Terrorist: Organizational Consideration, Terrorism, vol.13.

[27]Podgar, Ellen S, (2014), «Cyber crime: transnational or international», Wayne Law Review, vol. 50.

[28]Robert A, pape (2013), the strategic logic of suicide terrorism, American political science review, vol. 19, No. 3.

[29]Rodriguez, Carlos A. (2016), "Cyber terrorism", Inter-American Defense College as aprerequisite for the Diploma approved.

[30]Rowe, A.J and S.A Davis (2012), the Intelligent Information Systems: Meeting the Challenge in the Knowledge Era, Greenwood Publishing Group.

[31]Ruby, C.L. (2014), The Deffinition of Terrorism, In Analyses of Social Issues and Public Policy, 2002, pp.14-9.

[32]Sarah oates, Diana owen and Rachel K. Gibson (2016), the internet and politics; citizens, voters and activists, Routledge.

[33]Schaap, A.J, (2014). "Cyber Warfare Operations: Development and Use under International law", Air Force law review, vol 64.

[34]Schiller, Herbert (2017), Who Knows: information in the age of the fortune 500, Norwood.

[35]Seddon, Embar (2017), «Cyber terrorism», Edited Alan Oday, Ash gate Publishing company.

[36]Sharp, Walter gray (2013), cyber warfare and the use of force, Aegin research corporation.

[37]Starr, Stuart H. (2015), "Towards an Evolving Theory of Cyber power", National DefenseUniversity, Center for Technology and National Security Policy.

[38]Tosini, Domenico (2017), Sociology of Terrorism and Counterterrorism: A Social Science Understanding of Terrorist Threat, Journal Compilation, Blackwell Publishing, Ltd.

[39]Walker, Cliver (2016), «cyber terrorism. legal principle and law in the united kingdom», pen state law rev.110.no3.

[40]William Warner, Fowler (2013), terrorism Data Base: A comparison of Missions, Methods, and systems, California, RAND.

[41]Wingfield, Thomas (2016), the Law of Information Conflict: National Security Law in Cyberspace.

[42]https://www.merriam-webster.com/dictionary/cyberspace

[43]https://twitter.com/h0d3r_fa/status/1118144867090227200?lang=fa

[44]https://farsi.euronews.com/22/09/2017/jihadists-flee-to-instagram-after-purge-on-facebook

[45]https://www.forbes.com/profile mark-zuckerberg/6#f84479f3e06

[46]https://ahtribune.com/world/americas/academic-freedom/-1816 facebook-mark-zuckerberg-hall.html

[47]https://qz.com/300707/the-failure-of-silicon-valleys-say-anything-immigration-push/

[48]https://www.aepi.org/about/about-aepi/notable-alumni3-/ http://gawker.com/5634124/facebook-ceos-secret-frat-name-has-been-revealed

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

csri.majazi.ir

حـوزه فضـای مجـازی بـه انـدازه انقـلاب اسـلامی اهمیـت دارد. ایـن فضـا مثـل یـک رودخانـه پـر از آب و خروشـان اسـت کـه مـی آیـد و دائمـاً هـم بـر آب آن افـزوده و خروشـان تـر مـی شـود. اگـر مـا بـر ایـن رودخانـه تدبیـر کنیـم و برنامـه داشـته باشـیم، زه‌کشـی کنیـم و هدایـت کنیـم ایـن رودخانـه را تـا بـه سـد بریـزد، می‌شـود فرصـت. اگـر رهایـش کنیـم و برنامـه‌ای بـرای آن نداشـته باشـیم می‌شـود یـک تهدید.

csri.majazi.ir