فصلنامه مطالعات جنگ
سال دوم، شماره هفتم، زمستان ۱۳۹۹
مقالهٔ سوم از صفحه ٦٨ تا ٨٣

تهدیدات تروریسم سایبری و واکاوی تحرکات گروه تروریستی داعش در فضای سایبر

خداداد هلیلی*[۱]، محمدرضا سلطانپور[۲]

دریافت مقاله: ۹۹/۰۶/۲۲ پذیرش مقاله:۹۹/۱۰/۰۴

چکیده

گروه تروریستی داعش، از جمله فرقه‌هایی است که با مجهز شدن به فناوری‌های پیشرفته سایبری، اقدام به پیشبرد اهداف، تبلیغ ایدئولوژی، جذب مخاطبان و انجام عملیات تروریستی نموده است. تروریسم سایبری، چهره جدید تروریسم است که بدون آنکه خطرات سایر اقسام تروریسم را برای اقدام کنندگان آن داشته باشد می‌تواند اهداف مورد نظر را برآورده سازد. بسیاری از تحرکات این گروه در فضای سایبر، مصداق عینی تروریسم سایبری است. این گروه در ماه‌های اخیر با ازدست‌دادن سرزمین جغرافیایی خود، متحمل شکست‌های جدی شده است؛ اما در اندیشه راه‌اندازی خلافت سایبری است. برخی معتقدند، این گروه در آینده تبدیل به یک سازمان مجازی خواهد شد که با از دست دادن منابع مالی و نفتی خود، برای کسب درآمد و انجام عملیات تروریست هکرها را برای و سرقت پول و اعتبار از افراد و بانک‌ها به کار خواهد گرفت. هدف اصلی این مقاله، بررسی تهدیدات تروریسم سایبری و تجزیه و تحلیل تحرکات داعش در فضای سایبر است. بدین منظور پس از بررسی مفاهیم تروریسم سایبری، حملات سایبری و تسلیحات سایبری، به بررسی اقدامات داعش در فضای سایبر و واکاوی دلایل فاش نمودن عملیات سایبری ایالات‌متحده از منظر راهبردی می‌پردازیم. نتایج این تحقیق نشان می‌دهد، همانند جنگ‌های سنتی، جنگ سایبری ایالات‌متحده علیه این گروه تروریستی، به خاطر منزوی بودن این حکومت خود خوانده در سطح جهان، بهترین فرصت برای نمایش توانمندی‌های سایبری آمریکا و عاملی بازدارنده برای کشورهایی است که با آمریکا مناقشات سایبری دارند.

واژگان کلیدی: تسلیحات سایبری، حملات سایبری، تروریسم سایبری، داعش

۱. عضو هیئت علمی دانشگاه شهید ستاری (نویسنده مسئول) halili@chmail.ir
۲. عضو هیئت علمی دانشگاه شهید ستاری m_r_soltanpour@yahoo.com

مقدمه

در شکل سنتی، تروریسم معمولاً در قالب قتل سران سیاسی، گروگان‌گیری یا حمله به تجهیزات دولتی و عمومی انجام می‌شود. مفهوم تروریسم به معنای به‌کارگیری حساب شده خشونت غیرقانونی برای ایجاد ترس، با قصد مرعوب و مجبور کردن دولت یا جامعه در رسیدن به اهدافی است که عموماً سیاسی، مذهبی یا ایدئولوژیکی هستند. تروریسم استفاده غیرقانونی زور و خشونت علیه افراد یا اموال یا مرعوب و مجبور کردن دولت، جمعیت غیرنظامی یا هر بخش از آن‌ها با هدف پیش برد اهداف سیاسی یا اجتماعی است.

انجام عملیات تروریستی به شکل‌های مختلف مورد استفاده گروه‌های ناراضی و مخالف دولت قرار می‌گیرد. این گروه‌ها با ایجاد رعب و وحشت در تلاش برای دستیابی به اهداف و آرمان‌های خود هستند. امروزه تروریست‌ها با به‌کارگیری آخرین فناوری‌ها به شکل سازمان‌یافته‌تر و حرفه‌ای‌تر عمل می‌کنند. این مسئله تروریسم را به‌عنوان یکی از جدی‌ترین چالش‌ها و دغدغه‌های دولت‌ها تبدیل نموده است.

فضای سایبر موجب تسهیل و اشاعه عملیات تروریستی شده است. از دیدگاه دنینگ[1]، تروریسم سایبری[2] و تهدید به حملات غیر قانونی در فضای سایبر است که به قصد ترساندن یا مجبورکردن دولت‌ها برای پیشبرد اهداف سیاسی یا اجتماعی صورت می‌گیرد؛ بنابراین حملات سایبری اگر بتواند منجر به مرگ، صدمه بدنی، انفجار، سقوط هواپیما، آلودگی آب یا خسارات متعدد اقتصادی شود و زیرساخت‌های حیاتی را مختل کند می‌تواند یک حلمه تروریستی محسوب شود و حملاتی که خدمات عمومی غیرحیاتی را مختل می‌کند را نمی‌توان حملات سایبری تروریستی در نظر گرفت؛ به عبارت دیگر، تروریسم سایبری عبارت است از حملات عمدی با انگیزه سیاسی علیه اطلاعات، سامانه‌های فناوری اطلاعات و ارتباطات که بتواند به خشونت علیه اهداف غیرنظامی منجر شود (نمامیان، ۱۳۹۰).

---

1. Denning
2. Cyber terrorism

تروریسم سایبری، چهره جدید تروریسم است که بدون آنکه خطرات سایر اقسام تروریسم را برای اقدام کنندگان آن داشته باشد می‌تواند اهداف مورد نظر را برآورده سازد. تروریسم سایبری با هدف نابود ساختن زیرساخت‌های حیاتی مانند انرژی، حمل‌ونقل، خدمات اورژانس، تأمین آب، بانکداری، خدمات دولتی، شبکه توزیع برق و شبکه ارتباطات راه دور انجام می‌شود. بسیاری از این اقدامات موجب ایجاد ترس و واهمه می‌شود؛ بنابراین می‌توان آن‌ها را در زمره اقدامات تروریستی محسوب کرد چرا که همان اثرات سلاح‌های نظامی را به همراه دارد (جواهری، ۱۳۹٤).

اقدامات داعش در فضای سایبر مصداق بارزی از انجام عملیات تروریستی است. این گروه از بستر فضای سایبر و به‌ویژه شبکه‌های اجتماعی برای انجام اقدامات غیر قانونی خود استفاده می‌کند. داعش یکی از شاخه‌های گروه تروریستی القاعده است که به صورت غیررسمی از آن جدا شده و فعالیت مستقل خود را آغاز کرد. این گروه، پس از اعلام موجودیت در سال ۲۰۰٦ و تصرف مناطقی از عراق و سوریه، حکومت خود را اعلام و آن را تحت عنوان دولت اسلامی عراق و سوریه (ISIS) نام‌گذاری کرد. در بسیاری از منابع و کشورها، این گروه، با نام دولت اسلامی عراق و شام (ISIL) شناخته می‌شود که در آن حرف L به شام (Levant) که یک نام قدیمی برای سوریه، لبنان، اسرائیل و اردن است؛ اشاره دارد.

داعش، همیشه نشان داده است که خواهان استفاده از مدرن‌ترین تجهیزات برای مبارزه، چه در دنیای واقعی و چه در دنیای مجازی، با جهان است. داعش در دوره‌ای ظهور کرد که بازار استفاده از شبکه و رسانه‌های تعاملی و اجتماعی بسیار داغ و نوظهور بوده و هست. به‌منظور پیشبرد اهداف خود برای تبلیغ ایدئولوژی و جذب مخاطبان از رسانه‌های جمعی مختلفی استفاده می‌کند. این گروه در سال ۲۰۰٦ موسسه الفرقان، در سال ۲۰۱۳ موسسه الاعتصام و در ۲۰۱٤ مرکز الحیات را راه‌اندازی کرد که تولیدات خود را به زبان‌های انگلیسی، آلمانی، روسی و فرانسوی برای مخاطبان غربی منتشر می‌کنند. تأسیس شبکه رادیویی البیان و ایجاد حساب‌های کاربری در شبکه‌های اجتماعی توییتر و فیس‌بوک برای انتشار اخبار، تصاویر و فیلم‌های مرتبط با این گروه به ۲۳ زبان مختلف از جمله اقدامات این گروه در فضای سایبر است. توئیتر یکی از مهم‌ترین ابزارهای داعش

است. این گروه توئیت‌های خود را ابتدا به زبان انگلیسی و سپس در سطحی اندک و ناچیز به زبان عربی ارسال می‌کند.

داعش از ابزارهای نوین ارتباطی، نظیر تالارهای گفتگو، انتشار متون نوشتاری، دیداری و صوتی الکترونیکی و شبکه‌های اجتماعی در راستای ارتباطات فردی، تبلیغات، جذب و آموزش نیرو، جمع‌آوری اطلاعات و برنامه‌ریزی، تأمین مالی، شبکه‌سازی و تفرقه‌افکنی میان شیعه و سنی استفاده می‌نماید.

برخی معتقدند، این گروه با از دست‌دادن منابع مالی خود که از فروش نفت و مالیات تأمین می‌شد، در آینده ممکن است به جرایم سایبری متوسل شده و از هکرها برای سرقت پول و اعتبار از بانک‌ها برای کسب درآمد استفاده کند. به گفته کارشناسان امنیتی، داعش در آینده تبدیل به یک سازمان مجازی خواهد شد که تنها در فضای اینترنت موجودیت دارد و هیچ‌گونه زیرساخت و دفتری ندارند[1]. این گروه تروریستی پس از شکست‌های جدی خود، اقدام به راه‌اندازی خلافت سایبری نموده است.

وزارت دفاع آمریکا در سال ۲۰۱۵ از حملات سایبری برای مختل نمودن خطوط ارتباطی و سامانه‌های فرماندهی و کنترل داعش استفاده نموده است. انجام این عملیات، ابزاری مؤثر برای شکست داعش است، زیرا مانع از آن می‌شود که این گروه بتواند نیروهای خود را به درستی سازماندهی کند. هرچند اقدام وزارت دفاع آمریکا در علنی نمودن جزئیات عملیات سایبری خود، در ظاهر تعجب برانگیز است، اما در پس آن انگیزه‌ها و دلایلی راهبردی دیده می‌شود. در این مقاله، واکاوی اقدامات تروریستی داعش در فضای سایبر و تجزیه و تحلیل عملیات سایبری ایالات‌متحده علیه این گروه تروریستی مورد توجه قرار گرفته است.

تسلیحات و حملات سایبری

[1] econews.com

سلاح سایبری[1]، یک سامانه سایبری است که برای وارد نمودن خسارت (تخریب) به ساختار یا عملیات سامانه‌های سایبری دیگر، طراحی و تولید می‌شود. این سامانه‌ها شامل شبکه بات‌ها، بمب‌های منطقی، ابزارهای بهره‌برداری از آسیب‌پذیری، انواع بدافزارها و سامانه‌های تولید ترافیک، حملات ممانعت از سرویس و ممانعت از سرویس توزیع شده می‌باشند که برای انجام تهاجم‌های سایبری، مورد استفاده قرار می‌گیرند (سند راهبردی پدافند سایبری کشور). سلاح‌های سایبری به دو دسته اصلی سلاح‌های رها شده در شبکه و سلاح‌های سایبری برخوردار از کنترل آتش انسانی طبقه‌بندی می‌شوند. در تعریفی دیگر، سلاح سایبری به حملات پیچیده کامپیوتر به کامپیوتر گفته می‌شود که از طریق شناسایی و بهره‌برداری آسیب‌پذیری در یک بخش از نرم‌افزار مورد استفاده توسط طرف مقابل موجب ایجاد اختلال و نابودی یک سامانه فناوری اطلاعات یا یک شبکه می‌شود (Herr, 2014).

شبکه جهانی اینترنت شامل مجموعه‌ای از شبکه‌های کامپیوتری متصل به هم در سراسر جهان است که سنگ‌بنای ایجاد فضای سایبر محسوب می‌شود. حملات سایبری با استفاده از انتشار یک کد کامپیوتری تحت عنوان سلاح سایبری در شبکه جهانی اینترنت، موجب اختلال و تخریب در عملکرد شبکه‌های متصل و زیرساخت‌های حیاتی در فضای سایبر می‌شوند.

سلاح سایبری یک سلاح ناشناس و دقیق، بدون نیاز به حضور سرباز (هکر) است. این سلاح وابسته به شناسایی و بهره‌برداری از آسیب‌پذیری‌های فناوری اطلاعات است اما تنها زمانی می‌تواند کارآمد و مؤثر باشد که مخفی و محرمانه باشد و در صورت افشاشدن، کارایی خود را از دست می‌دهد.

به خاطر محدودیت خسارت فیزیکی و مرگ و میر، سلاح‌های سایبری از پتانسیل خشونت‌آمیزی برخوردار نیستند. هرچند پتانسیل ایجاد خشونت‌های عینی را نیز دارند. مثلاً بمباران یا حملات هواپیماهای بدون سرنشین که دسترسی غیرنظامیان به آب، برق، پول و یا مراقبت‌های بهداشتی را تحت تأثیر قرار می‌دهد؛ می‌تواند به‌وسیله سلاح‌های سایبری جایگزین شود.

[1] Cyber weapons

توسعه سلاح‌های سایبری بسیار دشوار و پرهزینه است و این مسئله بستگی به میزان کنترل و دسترسی طرف مقابل (دشمن) بر زیرساخت‌های فناوری اطلاعات، بستگی دارد. این سلاح با تخریب و اختلال در شبکه‌های کامپیوتری در فضای سایبر، اثرات ثانویه‌ای در ابعاد اقتصادی، سیاسی، اجتماعی را به همراه دارد و می‌تواند خرابی‌های گسترده‌ای در زیرساخت‌های حیاتی مانند آب، برق، انرژی، شبکه بانکی و ...ایجاد کند (Krepinevich, 2012). جذابیت این سلاح‌ها، عمدتاً به خاطر توانایی آن‌ها در ایجاد عدم اطمینان نسبت به اعتبار و کارایی سامانه‌های مبتنی بر اطلاعات از جمله سامانه فرماندهی و کنترل نظامی است که در آن، محرمانگی و امنیت اطلاعات امری حیاتی است.

سلاح سایبری سلاحی غیرقابل پیش‌بینی است که هنوز هم در مناقشات حقوقی بین‌المللی در زمینه جنگ سایبری با چالش‌های زیادی همراه است؛ بنابراین جامعه بین‌المللی نیازمند رویکردی فراملی برای ایجاد امنیت سایبری در میان تمامی کشورهاست تا گروه‌های تروریستی از جمله داعش از قابلیت‌های این سلاح برای حملات سایبری و هدایت حملات تروریستی استفاده نکنند.

امروزه در مباحث نظامی، اصطلاحاتی مانند زرادخانه سایبری، حملات سایبری و جنگ سایبری مورد توجه نظریه‌پردازان قرار گرفته است. منظور از حمله سایبری[1]، استفاده از تسلیحات سایبری به‌منظور صدمه زدن به اهداف مشخص است. حمله سایبری با توجه به نوع سلاح سایبری مورد استفاده تعریف می‌شود نه طبیعت هدف؛ بنابراین یک حمله سایبری می‌تواند از یک جنگ‌افزار سایبری علیه یک دارایی غیر سایبری یا علیه یک دارایی سایبری استفاده کند اما حمله سایبری به استفاده از یک جنگ‌افزار غیر سایبری علیه یک دارایی سایبری یا غیر سایبری اطلاق نمی‌شود. در صورت تشدید حملات سایبری میان کشورها و استفاده از این حملات توسط یک کشور علیه زیرساخت‌های کشور به صورت علنی و رسمی جنگ سایبری[2] اتفاق می‌افتد (Rauscher &Yaschenko, 2011).

---

1. Cyber attack
2. Cyber war

اقدامات داعش در فضای سایبر

فضای سایبر، به خاطر از بین بردن محدودیت‌های مکانی و زمانی، در رواج شکل جدیدی از تروریسم تأثیر زیادی داشته است. گروه تروریستی داعش علی‌رغم مخالفت ذاتی خود با فضای سایبر، از ابزارهای آن به طور گسترده‌ای در راستای دستیابی به اهداف تروریستی خود استفاده کرده است. برخی از مهم‌ترین اقدامات داعش در فضای سایبر عبارتند از:

- **موسسه الفرقان**: تولید سی‌دی و دی‌وی‌دی، پوستر، کتابچه، تولیدات تبلیغاتی اینترنتی و بیانیه‌های رسمی گروه، رسانه‌ای برای نشان دادن قدرت نظامی داعش و بازنشر پیام‌های رهبران داعش (عراقچی و جوزانی، ۱۳۹٦).
- **ایجاد موسسه الحیات**: تمرکز بر مخاطبان غربی و انتشار کلیپ‌های ویدئویی به همراه زیرنویس به ۱۰ زبان زنده دنیا و پخش آن در شبکه‌های اجتماعی مانند توییتر، فیس‌بوک، اینستاگرام و گوگل پلاس و انتشار نشریه دابق (Dabogh) به عربی و انگلیسی (Siboni, 2015) و (Schori, 2015).
- **ایجاد موسسه الاعتصام**: تمرکز بر فعالیت‌های تشریفاتی و مذهبی
- ایجاد تالارهای گفتگو (chat room) و انجمن‌های وب (web forum)، مانند المنبر و اعلام الجهادی
- ساخت و انتشار فیلم‌های ویدیویی باکیفیت بالا و بازی‌های رایانه‌ای (مانند شمشیرهای بران)
- تولید نرم‌افزارهایی مانند فجر البشایر (طلوع سحر) برای گوشی‌های هوشمند
- ایجاد شبکه اجتماعی مانند خلافت بوک (Mahzam, 2015).

داعش با استفاده از فناوری‌های پیشرفته صوتی و تصویری بیشترین بهره‌برداری و تأثیرگذاری را از فضای سایبر برای تحقق اهداف خود و همراهی افکار عمومی برده است. ماهیت حضور داعش در فضای سایبر را می‌توان به سه دسته تقسیم‌بندی کرد: ۱) ادامه حیات و یارگیری و استخدام اعضای جدید، ۲) ایجاد ترس و وحشت از جنایات انجام شده خود، ۳) تلاش برای استفاده از فضای سایبری به‌عنوان اهداف تهاجمی و حملات سایبری. داعش در تلاش برای استفاده از دامنه‌های

سایبری به‌منظور مختل کردن خدمات و آسیب‌رساندن به اطلاعات حساس است[1]. این گروه تروریستی، علاوه بر استفاده از فناوری‌های رسانه‌ای و فیلم‌سازی برای جذب افکار عمومی و تشویق افراد برای پیوستن به خود از طریق شبکه‌های اجتماعی، با جذب هکرهای حرفه‌ای به وب‌سایت‌های سازمان‌های دولتی و شرکت‌های زیرساختی حمله می‌کند. نمونه‌هایی از این حملات سایبری عبارتند از:

- هک کردن حساب‌های توییتری و یوتیوب ستاد فرماندهی مرکزی ایالات‌متحده آمریکا (CENTCOM)
- هک کردن حساب توییتری نیوزویک
- هک کردن سایت کارکنان نظامی ایالات‌متحده و دستیابی به سرورهای اطلاعات ارتش ایالات‌متحده
- هک کردن کانال‌های تلویزیونی فرانسه و قرار دادن کارت‌های اعتباری خویشاوندان سربازان فرانسوری که با داعش مبارزه می‌کردند و تهدید آن‌ها

داعش از ابزارهای ارتباطی و بسترهای چند رسانه‌ای به‌عنوان عاملی تسهیل کننده و کاتالیزور برای اثرگذاری بر مخاطب و جلب توجه و جذب نیرو و ایجاد شبکه‌ای از سلول‌های تروریستی در جهت تشکیل آنچه خلافت اسلامی می‌نامد، استفاده می‌کند. شبکه‌های اجتماعی به طور ناخواسته ابزاری برای قدرت سایبری داعش شده‌اند. در شکل (۱) برخی از مهم‌ترین اقدامات داعش در فضای سایبر نشان داده شده است (Griffin, 2014).

عملیات سایبری ایالات‌متحده علیه داعش

ایالات‌متحده از سال ۲۰۰۹ به سرمایه‌گذاری وسیعی برای راه‌اندازی یک نیروی سایبری تحت عنوان فرماندهی سایبری ارتش آمریکا (ARCYBER) اقدام نموده است. هزینه‌های عملیات سایبری پنتاگون در سال ۲۰۱۵ بیش از ۵ میلیارد دلار برآورد شده است. در حال حاضر بیش از ۶۰۰۰ نفر در زمینه توسعه و قابلیت‌های سایبری در آمریکا مشارکت دارند. با توجه به این

[1] www.irdiplomacy.ir

سرمایه‌گذاری عظیم، استفاده از تسلیحات نوین سایبری ساخته شده توسط ارتش سایبری آمریکا، در صحنه عملی، از اولویت‌های دولت اوباما و ترامپ بوده و از اوایل شکل‌گیری داعش شایعه استفاده از این سلاح‌ها، توسط آمریکا نیز مطرح شده است (Sanger, 2016).

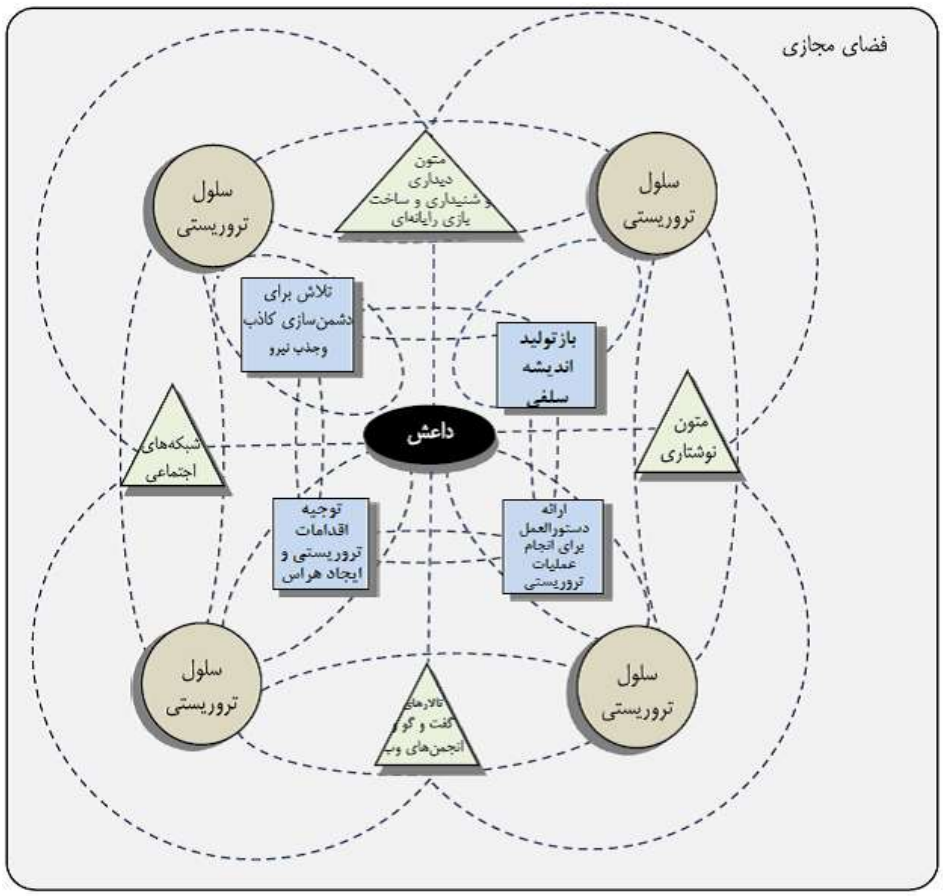
از اوایل سال ۲۰۱٦، مقامات وزارت دفاع آمریکا، استفاده از توانمندی‌های سایبری تهاجمی در سوریه و عراق و انفجار بمب‌های سایبری در مبارزه با داعش را به صورت علنی اعلام نموده‌اند. عملیات اعلام‌شده سایبری ارتش آمریکا علیه داعش در فضای سایبر شامل جمع‌آوری اطلاعات، تغییر پیام‌های داعش، ایجاد وب‌سایت‌های جعلی، اختلال در ارتباط داعش و مهار این گروه برای جذب و گسترش تبلیغات است که برای این منظور از سلاح‌های سایبری استفاده کرده است. اهداف مورد نظر ایالات‌متحده از این عملیات سایبری، از کار انداختن ساختار فرماندهی و کنترل، ایجاد مزاحمت و اختلاف در انتشار تبلیغات سایبری گروه داعش و ممانعت از انتقال الکترونیکی و مبادلات تجارت الکترونیکی این گروه اعلام شده است (Hennigan, 2016). اعلان بی پرده و افشای استفاده از سلاح‌های تهاجمی سایبری، توسط پنتاگون به دلایل زیر دور از انتظار به نظر می‌رسد (Jeppe & Jens, 2017).

۱. تأثیر عملیات سایبری، اغلب مبتنی بر ویژگی محرمانگی سلاح‌های سایبری متکی است چرا که با لو رفتن اطلاعات این تسلیحات و عمومی شدن آن‌ها، دشمن از آسیب‌پذیری شبکه خودآگاه شده و به سرعت نسبت به رفع آن اقدام می‌کند. این مسئله موجب می‌شود استفاده مجدد از این تسلیحات و بهره‌برداری از آسیب‌پذیری شبکه دشمن بی‌اثر شود.

۲. اعلان تهاجم سایبری و تخریب و اختلال در زیرساخت‌های فناوری اطلاعات داعش، از سوی ارتش آمریکا، بهانه‌ای برای توجیه ناکامی راهبران داعش در جذب جنگجویان خارجی فراهم می‌کند و آن‌ها می‌توانند فرماندهی سایبری ایالات‌متحده را مقصر ناکامی‌های خود در جذب نیرو و اداره دولت خود معرفی کنند.

۳. از آنجا که انجام عملیات مؤثر و امن در سایه عدم افشای اطلاعات آن انجام می‌شود، عملیات سایبری نیز از این قاعده مستثنی نیست؛ بنابراین فرهنگ رازداری بخشی از ذات سازمان‌های

اطلاعاتی است و تهاجمات سایبری نیز از جنس سرویس‌های جاسوسی است. لذا، دلیل توصیف ماموریت‌های سایبری آمریکا علیه داعش محرمانگی آن را از بین می‌برد.



شکل ۱: تحرکات داعش در فضای سایبر (Griffin, 2014)

تجزیه و تحلیل دلایل علنی نمودن عملیات سایبری علیه داعش

ایالات‌متحده در خلال جنگ با داعش، مکرراً از عملیات سایبری استفاده کرده است. از منظر راهبردی استفاده از تسلیحات سایبری توسط کشورها، محرمانه و مخفیانه انجام می‌شود. چرا که فاش نمودن علنی آن به مثابه اعلان جنگ سایبری است. پنتاگون عملیات سایبری خود علیه سامانه‌های فرماندهی و کنترل داعش را به صورت علنی اظهار نموده است. شواهد تجربی قوی در

زمینه دلایل افشای عملیات سایبری آمریکا موجود نیست، اما با توجه به اظهارات مقامات دولتی و نظامی آمریکایی مهم‌ترین دلایلی که موجب فاش نمودن این عملیات بوده است؛ بررسی می‌شود.

۱) مشروعیت بخشیدن به سرمایه‌گذاری‌های کلان در فرماندهی سایبری برای مخاطبان داخلی

ایجاد فرماندهی سایبری آمریکا نیاز به سرمایه‌گذاری وسیعی داشت که در خلال سال‌های ۲۰۰۹ تا ۲۰۱۶ از ۲۷ میلیارد دلار به حدود ۵۹ میلیارد دلار افزایش یافته است (Healey & Hughes, 2015). در سال ۲۰۱۷ وزارت دفاع بودجه‌ای در حدود ۷ میلیارد دلار برای امنیت سایبری پیش‌بینی کرده است. این سرمایه‌گذاری هنگفت نیاز به ارائه دلایل قانع‌کننده برای مالیات‌دهندگان آمریکایی دارد. انتقادات داخلی به ناکارآمدی مبارزه اوباما با داعش می‌تواند با دلایلی مانند ایجاد اختلال در توانایی داعش در استفاده از قلمرو سایبر توسط تهاجمات سایبری توجیه شود. حملات سایبری و هک کردن فرماندهی نیروهای مرکزی ایالات‌متحده (سنتکام) توسط داعش هرچند نشان از قدرت سایبری این گروه دارد؛ اما بعید به نظر می‌رسد که این گروه تروریستی ظرفیت فنی لازم برای ردیابی حملات سایبری فرماندهی سایبری و دفاع در برابر سلاح‌های سایبری آمریکا را داشته باشد (Nakashima, 2016).

۲) تضعیف اعتماد دشمن به زیرساخت فناوری اطلاعات و سامانه‌های فرماندهی و کنترل خود

در ادبیات جنگ سایبری، همانند جنگ‌های سنتی، بازدارندگی یک از موضوعات راهبردی است (Libicki, 2009). تسلیحات سایبری امروزه به‌عنوان یکی از عوامل مهم بازدارندگی درآمده است؛ به طوری که می‌تواند نقشی همانند زرادخانه‌های هسته‌ای داشته باشد. هر چند در سطح جهانی، خسارات ناشی از حملات سایبری به اندازه سلاح‌های هسته‌ای تجربه نشده است با این حال، مخفی نگه‌داشتن میزان تأثیر این تسلیحات همواره رعایت شده است؛ بنابراین اقدام آمریکا در فاش ساختن عملیات سایبری بر روی سامانه‌های فرماندهی و کنترل داعش می‌تواند به دلیل ارعاب و پیش‌دستی آمریکا برای بازیگران دولتی و غیردولتی در فضای سایبر و تهدید به اقدامات تلافی جویانه باشد.

ایالات‌متحده با ظهور سلاح‌های سایبری در راهبردهای خود حمله سایبری را حمله نظامی تلقی کرده و تهدید به اقدام متقابل نظامی نموده است.

علاوه بر بازداشتن مهاجمان از اقدام عملی برای حملات سایبری به زیرساخت‌های دیجیتالی ایالات‌متحده، اعلان توانایی‌های آمریکا در ایجاد اختلال در سامانه‌های نظامی داعش، می‌تواند میزان کنترل و نظارت بر شبکه‌های ارتباطی نظامی از جمله فرماندهی و کنترل را نشان دهد. این کار موجب از بین رفتن اعتماد به استفاده از فناوری‌های سایبری و افزایش شک و تردید در امکان طرح‌ریزی عملیات سایبری را به وجود می‌آورد. نتیجه این کار، تغییر رفتار از حالت تهاجمی به حالت انفعالی خواهد بود؛ که می‌تواند موجب کاهش ارتباطات و توانایی واکنش سریع در میدان جنگ را به همراه داشته باشد.

طبق گزارش‌های ارائه شده، از فعالیت‌های داعش در فضای سایبر، این گروه تروریستی از یک سامانه نظامی توسعه یافته و نوین فرماندهی و کنترل برخوردار است و توانایی‌های بالقوه در استفاده از فناوری‌های مختلف رمزنگاری و پشتیبانی از زیرساخت‌های خود را دارد. وابستگی سامانه فرماندهی و کنترل داعش به فناوری اطلاعات و ارتباطات آن در برابر حملات سایبری آسیب‌پذیر می‌کند؛ بنابراین اعلان آشکار حملات سایبری، اعتماد آن‌ها به این سامانه و استفاده از آن در طرح‌ریزی عملیات را کاهش می‌دهد. اقداماتی مانند قطع ارتباطات و تغییر در اطلاعات و پیام‌های ارسال شده از فرماندهان داعش باعث بدگمانی و ایجاد شک و تردید و کاهش روحیه آن‌ها می‌شود.

۳) نشان دادن قدرت سایبری خود به کشورهایی که با آمریکا مناقشات سایبری دارند

وابستگی زیرساخت‌های حیاتی ایالات‌متحده به فضای سایبر همواره آن را در معرض حملات سایبری قرار داده است. به‌عنوان مثال گروه هکری Shadow Broker در اوت ۲۰۱۶ فروش اطلاعات سرقتی خود از NSA را به مبلغ ۱ میلیون بیت‌کوین (حدود ۵۶۸ میلیون دلار) به حراج گذاشت. هرچند این حراج با شکست مواجه شد و این گروه با دسته‌بندی کوچک‌تر از اطلاعات آن‌ها را با مبالغ پایین‌تر در وب سایت‌های زیرزمینی به فروش رساند. هک‌کردن آژانس امنیت ملی

(NSA) آمریکا که نماد قدرت این کشور محسوب می‌شود. نشان از آسیب‌پذیری این کشور در حملات سایبری دارد. چیزی که با استفاده از حملات نظامی در فضای واقعی به شدت دشوار است.

نشان دادن اراده و توانایی انجام حملات سایبری بر علیه داعش یک راهبرد نظامی برای آمریکاست که از طریق آن سیگنال‌هایی برای سایر دولت‌های مخالف و گروه‌های غیردولتی ارسال می‌شود (DOD, 2017). این مسئله علاوه بر بازدارندگی یک تصویر بین‌المللی از میزان تأثیر و کارآمدی توانایی‌های سایبری آمریکا را نشان می‌دهد.

٤) تلاش برای همکاری جهانی برای تدوین، قوانین جنگ‌های سایبری و هنجارهای حقوقی سایبر

یکی از مباحث مهم در روابط بین‌الملل تعیین هنجارها و قوانین سایبری و حقوق بین‌الملل است. توافق‌نامه‌های بین‌الملل در حوزه فضای سایبری و ممانعت از وقوع جنگ‌های سایبری همواره ذهن اندیشمندان را به خود معطوف داشته است. در راهبردهای ناتو نمونه‌ای از این توافقات در حوزه سایبر دیده می‌شود. این اقدامات پس از اولین جنگ سایبری در تالین استونی شکل گرفت.

مقامات وزارت دفاع آمریکا یکی از دلایل حملات سایبری به داعش را زمینه‌سازی برای تدوین حقوق بین‌الملل سایبری و اقدامی برای شکل‌دهی به قوانین و هنجارهای بین‌المللی برای مقابله با تروریست سایبری و تحت عناوینی مانند حقوق بشر عنوان می‌کنند.

اخلاقی جلوه دادن این حملات با توجه به خساراتی که به شبکه‌های غیرنظامی وارد می‌شود، کار را برای ایالات‌متحده دشوار می‌کند. این کشور با تغییر پارادایم از قدرت سخت به قدرت نرم سعی در کسب وجهه بین‌المللی دارد؛ اما پیچیدگی‌های سلاح‌های سایبری غیرخشونت‌آمیز بودن آن‌ها را نمی‌تواند تأیید کند. روشن شدن منشأ حملات سایبری از طریق کشور آمریکا و اختلال در سانتریفیوژهای کشور ایران با سلاح سایبری استاکس نت با قوانین و هنجارهای بین‌المللی ناسازگار است و تلاش‌های این کشور در زمینه اعمال نفوذ در مجامع سایبر بین‌المللی برای جبران کاهش قدرت نرم این کشور انجام می‌شود. در صورتی که خشونت‌بار بودن سلاح‌های سایبری و

صدمه به غیرنظامیان در افکار عمومی مشخص شود. مقابله با ترویج این تسلیحات و نحوه برخورد با آن‌ها و ایجاد قوانینی بین‌المللی بشردوستانه برای آن‌ها ضروری به نظر می‌رسد.

تلاش آمریکا برای متوقف ساختن تبلیغات سایبری و اختلال در پرداخت‌های الکترونیکی و مبادلات مالی در فضای سایبر هرچند از تمایز و تناسب کافی در سطح بین‌الملل برخوردار نیست اما این کشور به خاطر جاه طلبی خود در فضای سایبر در تلاش برای همراه کردن افکار عمومی و توجیه عملیات سایبری خود با کنوانسیون‌های حقوق بین‌الملل است. از طرفی بهانه این کار را حملات سایبری داعش به زیرساخت‌های خود اعلام می‌کند.

به خاطر ویژگی‌های خاص حملات سایبری از جمله ناشناس ماندن مبدأ حملات و غافلگیری آن‌ها و نامشخص بودن اثبات عمدی یا سهوی بودن این حملات، اقدامات آمریکا در اعلام علنی حملات سایبری تلاش برای همراهی جامعه بین‌المللی برای دستیابی به فرهنگ‌سازی، تبیین هنجارها و اعمال قانون بر روی مهاجمان سایبری است.

نتیجه‌گیری

تسلیحات سایبری همانند سایر تسلیحات نظامی در یک رژه نظامی به نمایش گذاشته نمی‌شوند بلکه جلوه آن‌ها از طریق نمایش پیامدهای حمله به اهداف مورد نظر و ایجاد بازدارندگی و باور در به خطر انداختن اهداف راهبردی دشمن، امکان‌پذیر است.

از آنجا که در سطح بین‌الملل هیچ کشوری داعش را به رسمیت نمی‌شناسد و رسماً از آن پشتیبانی نمی‌کند، عملیات سایبری علیه داعش بهترین فرصت برای فرماندهی سایبری آمریکا در نمایش قدرت سایبری این کشور و نشان دادن توانایی انجام حملات سایبری تهاجمی و قدرت بازدارندگی و اعلان آن به کشورهایی مانند روسیه و چین بود که انگیزه کافی برای انجام حملات نظامی سایبری علیه آمریکا را دارند.

در این مقاله دلایل و انگیزه‌های ایالات‌متحده در عملیات سایبری بر روی سامانه‌های فرماندهی و کنترل داعش مورد بررسی قرار گرفته است. این دلایل عبارتند از:۱) ارائه دلایل قانع کننده برای مخاطبان داخلی در مورد سرمایه‌گذاری در حوزه فرماندهی سایبری و نشان دادن قابلیت‌های

تهاجمی و عملیاتی این فرماندهی در صحنه نبرد با اختلال در سامانه‌های فرماندهی و کنترل داعش، ۲) کاهش و تضعیف اعتماد داعش به سامانه‌های فرماندهی و کنترل مبتنی بر زیرساخت‌های فناوری اطلاعات و ایجاد راهبرد بازدارندگی از طریق شک و تردید ۳) نشان دادن قدرت سایبری ایالات‌متحده و ارعاب سایر کشورهایی که به طور غیرمستقیم با آمریکا مناقشات سایبری دارند ٤) تلاش برای همراه نمودن دولت‌های متحد برای تدوین هنجارها، قوانین و مقررات مربوط به جنگ‌های سایبری و حقوق سایبری در سطح بین‌الملل و همچنین تعیین اولویت‌های استفاده از سلاح سایبری در سطح بین‌الملل. در شکل (۲) این موارد نشان داده شده است.

شکل ۲: دلایل علنی نمودن عملیات سایبری آمریکا علیه داعش

فهرست منابع:

الف– منابع فارسی

- جواهری، مهدی (۱۳۹۴)، بررسی تروریسم از نظر گونه شناسی (مورد مطالعه تروریسم سایبری در بحث فناوری هسته‌ای در ایران، فصلنامه مطالعات بین‌المللی پلیس، سال ششم، شماره ۲۴، صص ۳۱-۶۴.
- عراقچی، سیدعباس، جوزانی، شاهین (۱۳۹۶)، بهره‌برداری داعش از فضای مجازی، فصلنامه روابط خارجی، سال نهم، شماره اول صص ۱۴۱-۱۷۵.
- نمامیان، پیمان (۱۳۹۰)، تروریسم سایبری از منظر حقوق بین‌الملل کیفری، مجموعه مقالات کنفرانس بین‌المللی ائتلاف جهانی علیه تروریسم برای صلح عادلانه، تهران.

ب – منابع انگلیسی

- OD DSB. (2017). "Task force on cyber deterrence". Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistic.
- Griffin, A. (2014). "Khelafa Book: ISIS Support Create Own Social Neetwork but Site Quickly Buckles"
- Healey, J. & Hughes, B. (2015) "Risk nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures, Atlantic Council".
- Hennigan, W. J. (2016). "Pentagon wages cyberwar against Islamic State" Los Angeles Times., February 29.
- Jeppe T. J. Jens R. (2017). "Cyber-bombing ISIS: why disclose what is better kept secret?" , JT Jacobsen, J Ringsmose - Global Affairs.
- Krepinevich, A. (2012) "Cyber warfare: A nuclear option?" Washington, DC: Center for Strategy and Budgetary Assessment.
- Libicki, M. C. (2009). "Cyberdeterrence and cyberwar". Santa Monica, CA: RAND
- Mahzam, R. (2015). "The Electronic Digitization of ISIS: Building a Multi- Media Legacy ", Rajaratnam School of International Studies
- Nakashima, E., & Ryan, M. (2016). "U.S. military has launched a new digital war against the Islamic State" Washington Post. , July 15
- Rauscher K.F. and Yaschenko V. (2011). Bilateral on Cybersecurity Critical Terminology Foundations, EastWest Institute and the Information Security Institute of Moscow State University
- Sanger, D. U.S. (2016). "cyber-attacks target ISIS in a new line of combat" New York Times. April 26.
- Schori L. Ch. (2015). "Cyber Jihad: Understanding and Countering Islamic State Propaganda", Geneva Center for Security Policy.
- Siboni, G., Cohen, D. and Koren, T. (2015). "The Islamic States Strategy in Cyberspace, Military and Strategic Affairs", Vol. 7, No.1.