شناسایی چالش‌های استراتژیک نوظهور در تروریسم نوین (۲)

تلخیص و ترجمه: عسگر قهرمانپور

در یادداشت قبلی به بررسی روندها و مسیرهای جهانی تروریسم(۱) پرداختیم. در این بخش چالش‌های استراتژیک در حال ظهور در تروریسم دهۀ ۲۰۲۰ شناسایی و برررسی خواهد شد.

مقدمه

به رغم دو دهه عملیات ضد تروریستی تحت هدایت ایالات متحده، فشار تروریسم مذهبی که توسط القاعده و داعش رواج یافته است، شکست قطعی و نهایی آن دشوار شده است. پژوهشی در نوامبر ۲۰۱۸ چنین برآورد کرد که تعداد مبارزان جهادی امروز تقریباً چهار برابر ۱۱ سپتامبر ۲۰۰۱ شده است. این پژوهش که توسط مرکز مطالعات استراتژیک و بین‌المللی (CSIS) منتشر شد، برآورد می‌کند که هم اکنون تقریباً ۲۳۰،۰۰۰ مبارز جهادی فعال در نزدیک به ۷۰ کشور جهان وجود دارند. اگرچه گروه‌هایی مانند القاعده و داعش از آن روز تاکنون نتوانسته‌اند، عملیاتی شبیه ۱۱ سپتامبر انجام بدهند، اما به نظر می‌رسد ایدئولوژی منجر به پرواز شخصی با هواپیما، چونان تومور سرطان به دیگر جاهای بدن گسترش یافته است.

جنگ جهانی علیه تروریسم به زودی وارد دهۀ سوم خود می‌شود. اگر چه ایالات متحده و متحدانش برتری‌های تاکتیکی را در میدان نبرد نشان داده‌اند، اما در آن سو، گروه‌های تروریستی همچنان به جذب نیرو ادامه می‌دهند. عوامل مؤثر بسیاری در این امر دخیل هستند، اما یک نظریه برای توضیح اینکه چرا برخی از گروه‌های تروریستی جانی تازه پیدا کرده‌اند، این است که مقامات ضدتروریسم به بهای فدا کردن استراتژی‌های بلند مدت که آیندۀ تروریسم را هدف قرار می‌دهد، به موفقیت تاکتیکی خود تکیه می‌کنند. در همین حال، سازمان‌های تروریستی

خود را با تلاش‌های ضدتروریسم و توسعه اقدامات متقابل سازگار کرده‌اند. اگرچه تحقیقات گسترده‌ای در این زمینه لازم است، اما تنها با شناسایی و فهم چالش‌های استراتژیک نوظهور می‌توان مقامات ضدتروریسم را برای مبارزه با تروریسم در دهۀ ۲۰۲۰ آماده کرد.

تشکیل ائتلاف‌های بین‌المللی

دکتر تریشیا بیکن در کتاب خود *چرا گروه‌های تروریستی ائتلاف‌های بین‌المللی تشکیل می‌دهند*[1]، ادعا می‌کند که امروزه بزرگترین تهدیدهای تروریستی القاعده و دولت اسلامی (داعش) اتحادهایی هستند که آنها با سایر گروه‌های تروریستی تشکیل می‌دهند. دکتر بیکن، تحلیلگر سابق دفتر مبارزه با تروریسم وزارت امور خارجه ایالات متحده، نزدیک به ۱۴ سال است که در خصوص تشکیل شبکه‌های تروریستی تحقیق می‌کند. او خاطرنشان می‌کند که تشکیل اتحاد در میان گروه‌های تروریستی پیشرفت جدیدی نیست اما، شبکه‌های پیچیده اتحادی که القاعده و دولت اسلامی ایجاد کرده‌اند، از نظر تاریخی منحصر به فرد هستند و به سازمان‌های آنها امکان داده در برابر فشار طولانی مدت ضدتروریسم مقاومت کنند. دکتر بیکن همچنین تصریح کرد که اتحاد برای گروه‌های تروریستی مفید است زیرا این امر از سلامت سازمانی آنها حمایت می‌کند. شاید ارزشمندترین مزیت ائتلاف‌های تروریستی این باشد که این گروه‌ها می‌توانند بهترین شیوه‌ها و درس‌های آموخته شده را به اشتراک بگذارند. با همه این اوصاف، گروه‌های تروریستی ذاتاً مأموریت‌های رقیب دارند. از یک طرف، آن‌ها به دنبال ایجاد یک انقلاب خشونت‌آمیز برای دستیابی به تغییرات اجتماعی یا سیاسی هستند. از سوی دیگر، آن‌ها به دنبال بقا هستند.

اگرچه اتحاد برای دوام سازمان‌های تروریستی بسیار مهم است، اما ایالات متحده تاکنون نتوانسته اتحاد آنها را مختل کند – ولو این کار بیش از پانزده سال در اولویت سیاست آن بوده است. دکتر بیکن همچنین ادعا می‌کند که این روند در واقع نشان می‌دهد آنها از یک ضعف اساسی رنج می‌برند. وی در کتاب خود چنین می‌نویسد: «گروه‌های تروریستی زمانی به دنبال تشکیل اتحاد هستند که از نظر مهارت، دانش یا توانایی بسیج منابع و از نظر

1. Why Terrorist Groups Form International Alliances

سازمانی ضعیف باشند. آن‌ها این مشکلات را تجربه می‌کنند و نمی‌توانند به تنهایی آنها را حل کنند. لذا ائتلاف به جای اینکه نشانهٔ قدرت باشد، اساساً نشانهٔ ضعف است.»

شبکه القاعده. القاعده از جذب منابع ضدتروریسم توسط دولت اسلامی بهره قابل توجهی برده است. در حالی که ایالات متحده و سایر رهبران جهانی توجه خود را بیشتر به داعش معطوف کرده‌اند، فرماندهی مرکزی القاعده در پاکستان که اغلب به عنوان هستهٔ القاعده نامیده می‌شود، فعالیت‌های خود را در سراسر خاورمیانه و شمال آفریقا گسترش داده است. القاعده که در اثر قیام‌های سیاسی در بهار عربی تقویت شده است، شبکه‌ای از امتیازات را در کشورهایی ایجاد کرده است که با ناآرامی‌های داخلی و بی‌ثباتی اجتماعی روبرو هستند. در یمن و مناطقی از عربستان سعودی، القاعده گروه‌های شبه نظامی سنی را متحد کرده تا وابسته منطقه‌ای خود، القاعده شبه جزیره عربستان (AQAP) را توسعه دهد. القاعده در الجزایر، مالی، موریتانی و نیجر بسیاری از گروههای افراطی کوچک‌تر را جذب کرده تا وابسته منطقه‌ای خود، القاعده مغرب اسلامی (AQIM) را توسعه دهد. القاعده علاوه بر گسترش دامنه جغرافیایی فرماندهی عملیاتی خود، مشارکت‌های استراتژیک با سایر سازمان‌های تروریستی تشکیل داده است. در ازای آموزش و بودجه، تعدادی از سازمان‌های تروریستی داخلی، از جمله طالبان در افغانستان و الشباب در سومالی، وفاداری خود را به القاعده اعلام کرده‌اند. این امتیازات و اتحادها به القاعده امکان داده تا فعالیت‌های خود را در ۱۸ کشور دنیا در آفریقا، آسیا و خاورمیانه گسترش دهد، و به طور پیوسته نفوذ منطقه‌ای پایدارتری را افزایش دهد (شکل ۵ را ببینید).

شکل ۵. شبکه بین‌المللی القاعده

القاعده با تمرکززدایی شبکه‌ای به طور فزاینده‌ای مقاومت بیشتری پیدا کرده است. درک نادرست شیوهٔ عملکرد شبکه القاعده باعث سردرگمی استراتژی جهانی برای مبارزه با آن شده است. نخست، هیچ گروهی در قلب شبکه وجود ندارد. فرماندهی مرکزی القاعده همچنان خطوط استراتژیک شبکه را ترسیم می‌کند، اما دیگر دستورالعملی صادر نمی‌کند. دوم، اتصالات جانبی یا روابط بین گروه‌های القاعده ساختاری مشبک مانند ایجاد می‌کند که به شبکه قدرت می‌بخشد. سوم، گرچه بسیاری از وابستگان القاعده صرفاً در سطح محلی فعالیت می‌کنند، اما در اساس شبکه گسترده‌تر القاعده را تقویت می‌کنند. بنابراین، مقامات ضدتروریسم باید یک استراتژی جهانی و جامع برای مقابله با القاعده تهیه کنند.

موفقیت‌های تاکتیکی علیه القاعده نتوانسته است شبکهٔ کلی آن را تضعیف کند. بلکه، القاعده در سال ۲۰۲۱ گسترش بیشتری نسبت به ابتدای سال ۲۰۱۱ یا ۲۰۰۱ خواهد داشت. این سازمان در دو دههٔ گذشته پیشرفت کرده و یک شبکهٔ پیچیده، سازگار و مقاوم توسعه داده است که همچنان به رشد خود ادامه می‌دهد. قلب سازمان اکنون ساختار آن محسوب می‌شود که از ارتباطات متقابل با وابستگان القاعده و متحدانش تشکیل شده است. فقط با فهم چگونگی همکاری هر گروه در شبکه القاعده، سیاست‌گذاران می‌توانند یک استراتژی جامع برای شکست

دادن القاعده تهیه کنند. با این همه، ایالات متحده و متحدانش همچنان درگیر تعاملات تاکتیکی هستند که نوید پیروزی‌های میدان جنگ را می‌دهند، اما هیچ چشم‌انداز واقع‌بینانه برای پیروزی در جنگ بزرگتر وجود ندارد.

شبکه دولت اسلامی (داعش). پیش‌تر به فرایند شکل‌گیری داعش در عراق اشاره کردیم و در اینجا لازم نیست در این باره توضیح داده شود.

شکاف بین القاعده و داعش نشان داد که همه اتحادهای تروریستی برای همیشه دوام ندارند. همچنین آسیب‌پذیری‌های اصلی را در چارچوب ایجاد اتحاد نشان داد. نخست، این شکاف نشان داد که دشمنان مشترک و ایدئولوژی‌های مشترک، به تنهایی ائتلاف گروه‌های تروریستی را به طور دائمی پیوند نمی‌دهند. دوم، نشان داد که (دست کم برخی) رهبران سازمان‌های تروریستی آگاه هستند که چگونه برداشت عمومی بر اهداف سازمانی آنها تأثیر می‌گذارد و روابط شخصی میان رهبران می‌تواند بیش از منافع مشترک باشد. سوم، این نکته مهم است که در هر درگیری یا شورشی، گروه‌های رقیبی وجود خواهند داشت که برای همان منابع و افراد جدید رقابت می‌کنند. این امر مسلماً بین مجاهدین افغان در جریان حمله شوروی به افغانستان وجود داشت.

داعش در خاورمیانه، وابسته‌های منطقه‌ای ایجاد کرده است که از آنها به عنوان ولایت یا استان در عربستان سعودی و یمن یاد می‌کند. گروه‌هایی که از درگیری‌های فرقه‌ای در کشورهای متبوع خود بهره قابل توجهی برده‌اند. در شمال آفریقا، داعش پایگاه‌هایی را در الجزایر، مصر و لیبی تاسیس کرده که از جمله استان‌های با رشد سریع دولت اسلامی هستند. در خارج از خاورمیانه و آفریقا، داعش استانی در قفقاز، منطقه‌ای در اروپای شرقی و همچنین استان‌هایی در چندین کشور آسیای جنوبی مانند افغانستان، پاکستان و بنگلادش ایجاد کرده است. امروزه، داعش دارای شبکه‌ای از استان‌های فعال در حداقل ۱۳ کشور جهان و همچنین تعدادی سلول کوچک‌تر، اما در حال رشد است (شکل ۶ را ببینید).

شکل ۶. شبکه بین‌المللی داعش

علاوه بر این، داعش هنوز تهدیدی فعال در عراق و سوریه به شمار می‌آید. در مارس ۲۰۱۸، داعش کنترل آخرین قطعه سرزمینی را که قبلاً در عراق و سوریه در اختیار داشت از دست داد. اما، اشتباهات تلفات سرزمینی آنها نباید به عنوان یک شکست پایدار توصیف شود. داعش اکنون به یک سازمان مخفی فعال تبدیل شده و به عنوان یک شورشی در هر دو کشور عمل می‌کند. همچنین، هزاران شبه نظامی داعش به جای جنگیدن تا سر حد برای دفاع از اشغال سرزمین خود، به مناطق مرزی روستایی واقع در عراق و سوریه عقب‌نشینی کردند و در آنجا به جوامع همدل پناه بردند. در واقع، پنتاگون تخمین می‌زند که داعش بین ۲۰ تا ۳۰ هزار عضو دارد که تقریباً به طور مساوی بین عراق و سوریه تقسیم شده‌اند و از موقعیت خوبی برای تجدید سازمان و بازسازی سلطه خود برخوردار است. در دهۀ ۲۰۲۰ این احتمال وجود دارد که این افراد پناهنده یا خود داعش یا چیزی شبیه به آن را دوباره سازماندهی و از نو تشکیل دهند.

اگرچه این کشور در حال حاضر با شکست‌های ارضی در عراق و سوریه روبرو است، اما بی تردید، با اتکا به شبکه جهانی استان‌های خود، مسئولیت بیشتری را به عهده خواهد گرفت و برگ برندۀ خود را حفظ خواهد کرد. تازه

بیشتر نگران‌کننده این است که به نظر می‌رسد روند بازآفرینی، تهدیدات قوی‌تر نیز ایجاد می‌کند. مشابه تحول از القاعده عراق به داعش، «داعش شماره ۲» می‌تواند به عنوان تهدیدی خطرناک‌تر و پویاتر از آنچه در سال ۲۰۱۴ به طرز چشمگیری تحقق یافت، ظاهر شود.

پدیدهٔ جنگجویان خارجی

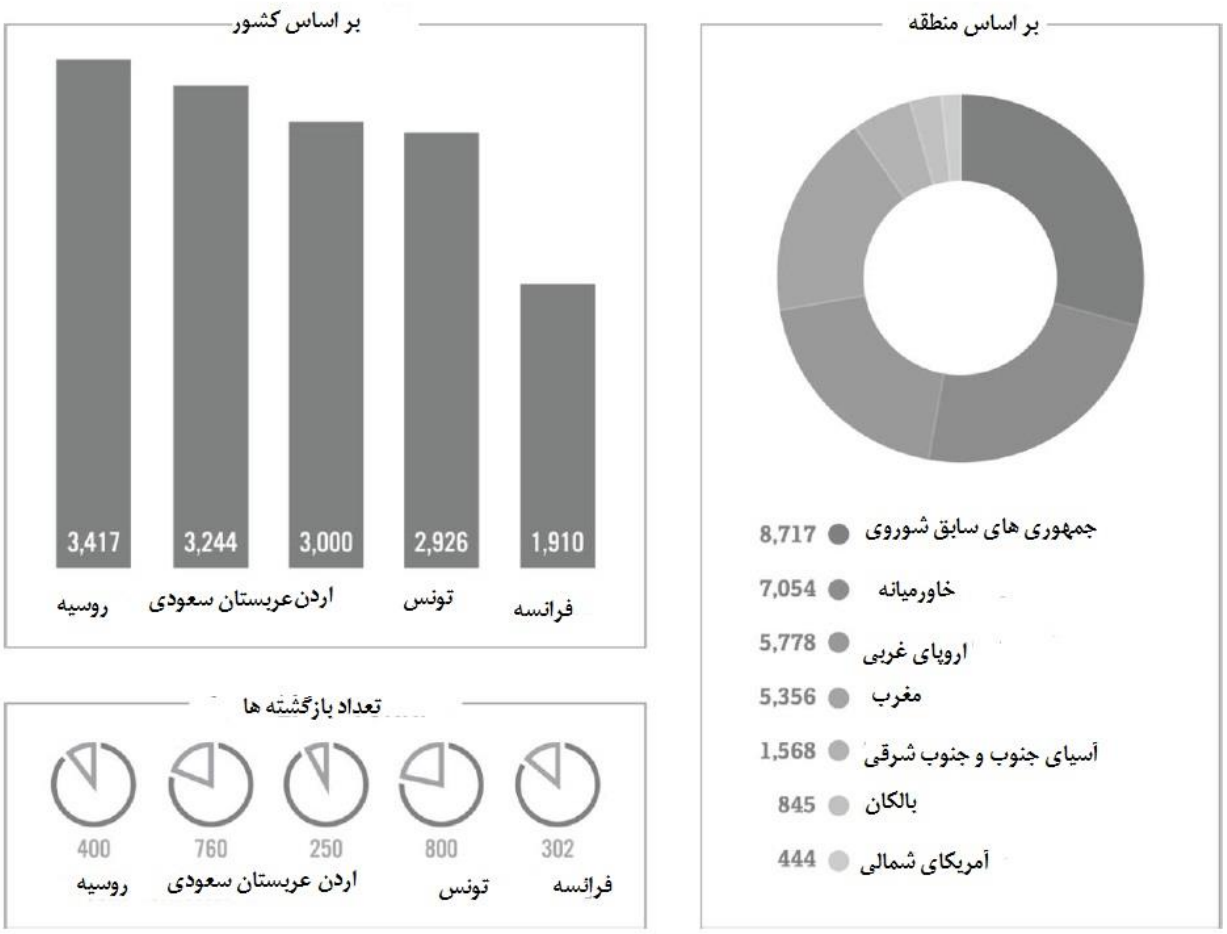
همانطور که دولت اسلامی سرزمینی را در عراق و سوریه تصرف کرد، هزاران تبعه خارجی را برای پیوستن به صفوف خود جذب کرد. اما، حال که تمام کنترل ارضی خود را از دست داده است، بسیاری از این اتباع خارجی یا به خانه خود بازگشته‌اند یا به مکان دیگری نقل مکان کرده‌اند. مطالعه‌ای که در سال ۲۰۱۷ توسط مرکز سوفان[2] انجام شد تخمین می‌زند که بیش از ۴۰،۰۰۰ تبعه خارجی از بیش از ۱۱۰ کشور جهان برای پیوستن به داعش به عراق و سوریه سفر کرده باشند. این افراد خانه‌های خود را ترک کرده و در برخی موارد خانواده‌های خود را برای جنگیدن برای بدیل ملی‌گرایی نقل مکان کرده‌اند. آن‌ها وقتی به داعش پیوستند، انتظار داشتند اشغال منطقه‌ای آن را گسترش دهند.

تحلیل بازگشت و جابجایی جنگجویان خارجی. پروپاگاندای حرفه‌ای و سواستفاده خوب دولت اسلامی از بی‌اعتمادی سیاسی به آنها امکان داد دامنهٔ جغرافیایی درخواست عضویت خود را فراتر از عراق و سوریه ببرند. در حقیقت، فقط ۳۰٪ از ۴۰،۰۰۰ جنگجوی خارجی با هویت از کشورهای خاورمیانه و شمال آفریقا مهاجرت کردند. ترکیب ۲۸۰۰۰ جنگجوی خارجی باقیمانده بسیار متنوع است. بیش از ۸۷۰۰ نفر از جنگجویان خارجی داعش از بومیان روسیه و جمهوری‌های سابق اتحاد جماهیر شوروی هستند که نشان‌دهندهٔ بیشترین تعداد جنگجویان خارجی با هویت از یک منطقه خاص است. بیش از ۵۷۵۰ جنگجوی خارجی برای جنگ در کنار داعش از کشورهای اروپای غربی سفر کرده‌اند، در حالی که ۱۵۰۰ نفر دیگر از جنوب شرقی آسیا مهاجرت کرده‌اند. نیمکره غربی نیز

2. The Soufan Center

از جذب داعش در امان نبود: ۴۴۴ فرد با هویت از آمریکای شمالی برای جنگیدن در کنار گروه تروریستی به عراق یا سوریه سفر کرده‌اند (شکل ۷ را ببینید)

شکل ۷. خاستگاه جنگجویان خارجی داعش



دلایل مختلفی وجود دارد که ممکن است جنگجویان‌های خارجی داعش تصمیم به بازگشت به کشورهای خود بگیرند. برخی ممکن است ناامید یا پشیمان شده باشند و بخواهند به زندگی قبلی خود بازگردند. برخی دیگر هنوز هم ممکن است بر اساس ایدئولوژی هدایت شوند اما تصمیم گرفتند از عراق و سوریه فرار کنند تا از مرگ قابل پیش‌بینی‌شان جلوگیری کنند. نگران‌کننده‌تر از همه، برخی چه بسا برای برنامه‌ریزی یا اجرای حمله به خانه فرستاده شده باشند، یا احساس کنند که می‌توانند کارهای بیشتری برای جنبش جهادی در داخل کشور انجام

دهند تا خارج. دیگر مبارزان خارجی ترجیح داده‌اند به جای بازگشت به وطن خود، به کشورهای جدید مهاجرت کنند. این وضعیت به ویژه در خاورمیانه و شمال آفریقا، جایی که کشورهایی با مرزهای اسفنجی پناهگاه امنی برای مهاجران افراطی فراهم می‌کنند، صدق می‌کند. مبارزان خارجی ممکن است ترجیح دهند که به یکی دیگر از استان‌های دولت اسلامی منتقل شوند، استان‌هایی که همچنان در سراسر جهان با قدرت و استخدام رشد می‌کنند.

چالش‌های قانونی برای بازگشت‌کنندگان. اگرچه جامعه بین‌المللی موافقت می‌کند که بازگشت‌کنندگان داعش تهدیدی جدی برای دهه‌های آینده به وجود می‌آورند، اما در مورد چگونگی مدیریت بهتر کسانی که بازگشته‌اند به توافق نرسیده است. اکثر کشورها چارچوب‌های قانونی برای پیگرد قانونی و حبس جنگجویان خارجی بازگردانده شده دارند، اما، آن‌ها به محض زندانی شدن، اغلب سعی در رادیکال کردن سایر زندانیان و ایجاد شبکه‌های استخدام در سیستم زندان می‌کنند. برخی از کشورها بر توسعهٔ برنامه‌های ادغام مجدد متمرکز شده‌اند، که طراحی و اجرای آنها بسیار دشوار است. برخی دیگر تصمیم گرفته‌اند با سلب تابعیت از شهروندی آنها، حق مسئولیت قانونی در قبال مبارزان خارجی بومی را انکار کنند که می‌تواند قوانین بین‌المللی را پیچیده کند.

سیاست ایالات متحده برای مدیریت جنگجویان خارجی که تابعیت ایالات متحده را دارند، بر نظام عدالت کیفری خود تکیه می‌کند، و در درجهٔ نخست جنگجویان خارجی را به خاطر حمایت مادی از یک سازمان تروریستی خارجی مشخص، متهم می‌کند. بر اساس گزارش مرکز سوفان، بیش از ۲۵۰ آمریکایی تلاش کردند به داعش بپیوندند که ۱۲۹ نفر از آنها با موفقیت به عراق و سوریه رسیدند.

ظهور تروریسم سایبری

سالهاست که گروه‌های تروریستی از اینترنت برای گسترش تبلیغات، استخدام عوامل و القا حملات گرگ‌های تنها[۳] استفاده می‌کنند. با این حال، آن‌ها اکنون افق‌های دیجیتالی خود را فراتر از شبکه‌های اجتماعی و پیام‌رسان صرف گسترش می‌دهند؛ آن‌ها به آرامی در حال توسعه توانایی‌های جنگ سایبری هستند تا با بازیگران دولتی رقابت کنند. گرچه گروه‌های تروریستی تاکنون نتوانسته‌اند دست به یک حمله مهم شبکه رایانه‌ای بزنند، اما فاصله بین آرزوها و توانایی‌های آنها به سرعت در حال نزدیک شدن است.

تروریسم سایبری. تروریسم سایبری معمولاً «حمله غیرقانونی یا تهدید به حمله علیه رایانه‌ها، شبکه‌ها و اطلاعات ذخیره شده در آن برای ارعاب یا زورگویی دولت یا مردم آن در پیشبرد اهداف سیاسی یا اجتماعی» تعریف می‌شود. بر خلاف مجرمان سایبری یا هکرها ، اهداف تروریست های سایبری وارد کردن خسارت شدیدتر و دائمی تری است که ممکن است شامل تلفات جانی یا آسیب اقتصادی شدید باشد. تروریست های سایبری به ویژه دشمنان پیچیده ای هستند. آنها نه تنها به دنبال بهره برداری از داده ها و اطلاعات ارزشمند هستند بلکه در تلاش برای برهم زدن نظم اجتماعی نیز به زیرساخت های مهم آسیب وارد می‌کنند. آنها از انتقام جویی نمی‌ترسند و در بسیاری از موارد با تضعیف وابستگی تکنولوژیکی به دنبال ایجاد بی‌ثباتی اساسی در جامعه هستند. به منظور تجزیه و تحلیل تهدید تروریسم سایبری، بررسی این خصوصیات تعریف و همچنین روش‌هایی که تروریست‌ها در گذشته استفاده می‌کردند و می‌توانند در آیندهٔ نزدیک استفاده کنند، مهم است.

انگیزه‌ها، گروه‌های تروریستی در آرزوی آسیب رساندن، ایجاد هرج و مرج و برهم زدن خدمات در کشورها و سازمان‌های مخالفشان هستند. آنها همچنین به طور فعال در حال توسعه قابلیت‌های تهاجمی جنگ سایبری مانند

۳. در تروریسم به حمله‌ای گفته می شود که به صورت انفرادی و بدون ارتباطات سازمانی انجام می شود. بهترین معادل برای این اصطلاح حمله انفرادی می‌باشد. گرگ تنها به شخصی گفته می‌شود که به تنهایی و بدون اینکه با گروهی ارتباط سازمانی داشته یا از آن کمکی دریافت کند در حمایت از آن گروه، جنبش یا عقیده دست به اعمال خشونت‌آمیز می‌زند. از آنجا که گرگ‌های تنها با گروه‌های تروریستی ارتباط مشخصی ندارند و به تنهایی دست به عملیات می‌زنند شناسایی آن‌ها برای نیروهای امنیتی دشوار است. در سال‌های اخیر گروه‌های القاعده و داعش طرفداران خود در کشورهای غربی را به انجام حملاتی به سبک گرگ‌های تنها تشویق کرده‌اند.

بدافزار یا جاسوس افزار برای آسیب رساندن به شبکه‌ها، ایجاد اختلال در فعالیت‌ها و هدایت منابع و جمع‌آوری اطلاعات، درآمدزایی و رشد نفوذ خود هستند.

روش‌ها. گروه‌های تروریستی نتوانسته‌اند به طور موثر در شبکه‌هایی که زیرساخت‌های امنیتی مهم را کنترل می‌کنند، نفوذ کنند. با این حال، آن‌ها در حال تمرین هستند. بر اساس گزارشی در سال ۲۰۱۵ که توسط پروژه تهدیدهای حیاتی موسسه آمریکن اینترپرایز منتشر می‌شود، هر سال، سازمان‌های نظامی و اطلاعاتی تعداد فزاینده‌ای از حملات تروریستی سایبری را ثبت می‌کنند که به طور معمول در یکی از سه دسته زیر قرار دارند:

* بد شکل کردن سیستم: مهاجم با سوء استفاده از تنظیمات نادرست یا آسیب‌پذیری، به وب سایت دسترسی پیدا می‌کند و محتوای اصلی آن را با تبلیغات یا ادعای معتبر جایگزین می‌کند. یک مهاجم با انگیزه همچنین ممکن است پرونده‌ها را از سرور حذف کند یا بدافزاری را بارگذاری کند.

* نفوذ در داده‌ها: مهاجم برای دسترسی و بارگیری اطلاعات محرمانه، به یک پایگاه داده امن نفوذ می‌کند. مهاجم ممکن است با یافتن نقص امنیتی در زیرساخت پایگاه داده یا به طور غیرمستقیم از طریق حملات مهندسی اجتماعی مانند فیشینگ، که از خطاهای انسانی سو استفاده می‌کنند، مستقیماً به سیستم هدف نفوذ کند.

* غیرقابل دسترس کردن سرویس[۴]: مهاجم وب سایت را با غرق کردن در بازدید، غیرقابل دسترس می‌کند. این حمله می‌تواند از طریق یک رایانه انجام شود، اما با رایانه‌های بیشتر اثربخشی آن افزایش می‌یابد، زیرا مدیریت سیستم‌های ترافیکی مخرب از طریق چندین آدرس IP برای سیستم‌های امنیت سایبری دشوارتر است.

علاوه بر این، همزمان گروه‌های تروریستی با تکثیر سلاح‌های سایبری و جذب افراد باهوش در فناوری، به تقویت زرادخانه‌های سایبری خود ادامه می‌دهند. این کار به افراد و سازمان‌ها امکان می‌دهد حملات پیچیده‌تری انجام دهند، مانند:

[4] . Denial of Service (DoS)

• باج افزارها[5]: مهاجم از سلاح‌های سایبری تبلیغاتی استفاده می‌کند که به صورت خودکار مقیاس بندی و تکثیر می‌شوند و به یک رشته کد اجازه می‌دهد تعداد بالایی از سیستم‌ها یا زیرساخت‌های شبکه را از بین ببرد. این حملات را می‌توان با فشار یک دکمه انجام داد و بسته به تنظیمات آنها، اغلب به راحتی غیرفعال می‌شوند. به مهاجم اجازه می‌دهد تا سیستم را تا زمان دریافت باج نگه دارد و سپس با دریافت باج آن را آزاد کند.

باج افزارها خصوصاً برای سازمان‌های تروریستی سودمند است زیرا می‌تواند روشی را هم برای بر هم زدن نظم اجتماعی و هم برای افزایش منابع مالی فراهم کند. با توجه به هزینه‌های انباشتی که باج افزار تولید می‌کند، به ویژه هنگامی که زیرساخت‌های حیاتی مانند بیمارستان‌ها یا مراکز حمل و نقل را مختل می‌کند، ممکن است شرکت‌ها و دولت‌ها مجبور شوند خواسته‌های سازمان‌های تروریستی را برآورده کنند.

ابزارها. روش‌های زیادی وجود دارد که گروه‌های تروریستی می‌توانند سلاح‌های سایبری را بدست آورند. انجمن‌ها و بازارهای وب تاریک، بدافزار و تخصص فنی را به طور گسترده در دسترس قرار می‌دهد. این اتاق‌های گفتگوی زیرزمینی همه چیز در اختیار گروه‌های تروریستی قرار می‌دهند: از بحث دربارهٔ حمله تا یادگیری نکات ناشناس و دانش عملیاتی، تا هر نوعی خدمات برای تروریست‌هایی که قصد حملات سایبری را دارند. افزون بر این، ویکی لیکس با انتشار اسناد طبقه‌بندی شده، ابزارهای هک فراوانی را در دسترس عموم قرار داده و آسیب‌پذیری‌های سایبری را که سازمان‌های تروریستی به خوبی می‌توانند از آن سوءاستفاده کنند، نشان داده است.

ظرفیت در حال رشد گروه‌های تروریستی. تعدادی از سازمان‌های تروریستی در حال تمرین مهارت‌های سایبری خود هستند و برخی از آنها قبلاً ابزارهایی را برای انجام حملات سایبری توهین آمیز نشان داده‌اند:

القاعده. در یک ویدئو ۲۰۱۲، القاعده اهداف خود را برای انجام «جهاد الکترونیکی» علیه ایالات متحده اعلام کرد، و آسیب‌پذیری شبکه‌های رایانه‌ای حیاتی آمریکا را با نقص در امنیت هواپیمایی قبل از حملات ۱۱ سپتامبر مقایسه

[5] . Ransomware

کرد. در این ویدئو، یک عامل القاعده «مجاهدین مخفی» را فرا می‌خواند، اصطلاحی که القاعده و سایر گروه‌های جهادی برای الهام بخشیدن به حملات تروریستی گرگ تنها، برای دست زدن به حملات سایبری به شبکه‌های دولت ایالات متحده و زیرساخت‌های مهم، از جمله برق توری به کار می‌برند.

حماس. در سال ۲۰۱۷، عوامل حماس موفق شدند تلفن‌های همراه ده‌ها سرباز اسرائیلی را هک کنند. حماس با ساختن پروفایل‌های جعلی در شبکه‌های اجتماعی که وانمود می‌کند زنان جوان هستند، ده‌ها سرباز اسرائیلی را ترغیب کرد تا یک برنامه همسریابی جعلی را در دستگاه‌های تلفن همراه خود بارگیری کنند، که در حقیقت ثابت شد وسیله‌ای برای نصب بدافزار است. این امر به حماس امکان می‌داد تا تماس‌ها، متن‌ها و نامه‌های الکترونیکی آنها را برای دستیابی به اطلاعات واحدهای نیروهای دفاعی اسرائیل (IDF)، تمرینات آموزشی و برنامه‌های عملیاتی کنترل کند. حماس در ژوئن ۲۰۱۸ با استفاده از برنامه‌ای که امتیازات جام جهانی را ردیابی می‌کرد، ترفند مشابهی را هدایت کرد که به زبان عبری در فیس بوک تبلیغ کردند. این برنامه مخرب پس از نصب، به حماس امکان ردیابی مکان‌های سربازان ارتش اسرائیل و استفاده از تلفن را به عنوان دستگاه شنود و دوربین فیلمبرداری می‌دهد.

حزب الله. وقتی ایران به توسعه قابلیت‌های جنگ سایبری خود ادامه می‌دهد، انتظار می‌رود حزب‌الله یکی از ذی نفعان اصلی آن باشد. شواهد فزاینده نشان می‌دهد که ایران به دنبال انجام حملات سایبری علیه ایالات متحده و اسرائیل بوده است.

دولت اسلامی. دولت اسلامی ظرفیت استقرار طیف گسترده‌ای از سلاح‌های سایبری تهاجمی را نشان داده است. این گروه تروریستی چندین کارزار مخرب به راه انداخته است که از طریق آنها سعی در کشف اطلاعات قابل شناسایی شخصی (PII) مربوط به پرسنل امنیتی یا نظامی، انتشار این اطلاعات و تشویق دیگران برای انجام حملات فیزیکی علیه این افراد داشته است. در سال ۲۰۱۵، یک هکر وابسته به داعش اطلاعات شخصی بیش از ۱۳۰۰ مقام ارتش و دولت ایالات متحده، از جمله نام، آدرس و سایر اطلاعات حساس را به عنوان «فهرست کشتار» برای الهام بخشیدن به حملات گرگ‌های تنها علیه این افراد و خانواده‌های آنها منتشر کرد.

چشم‌انداز یک ۱۱ سپتامبر سایبری. از آنجایی که جوامع مدرن به طور روزافزونی برای بهبود کارایی دولت و شرکت‌ها به فناوری وابسته شده‌اند، آسیب احتمالی یک حمله سایبری بزرگ به طور فزاینده‌ای مخرب شده است. امروزه، یک حمله سایبری بزرگ می‌تواند ثبات سیستم‌های پزشکی، غذایی و آب را به خطر بیندازد، حمل و نقل را مختل کند یا حتی بی‌ثبات کننده نیروگاه‌های هسته‌ای باشد. اخیراً، شورای مشاوره زیرساخت‌های ملی وزارت امنیت داخلی آمریکا (NIAC) هشدار داده است که «پیش از آنکه یک حمله سایبری در سطح ۱۱ سپتامبر علیه زیرساخت های مهم ایالات متحده انجام شود، یک فرصت محدود و زودگذر وجود دارد.» در این امر موضوع زمان مهم است؛ اما ابزارهای پاسخ همچنان نامشخص است، زیرا بسیاری از حساس‌ترین سیستم‌ها تحت کنترل بخش خصوصی و مستقل کار می‌کنند.

اگرچه سازمان‌های تروریستی صریحاً آرزوهای خود را برای انجام یک حمله سایبری بزرگ به سبک ۱۱ سپتامبر ابراز داشته‌اند، اما تاکنون قادر به انجام این کار نبوده‌اند. متخصصان ضدتروریسم و امنیت سایبری دهها پژوهش را حمایت مالی کرده‌اند، میزگردهای زیادی را برگزار کرده و مقالات بی‌شماری را در این زمینه نوشته‌اند.

نتیجه‌گیری

جنگ جهانی علیه تروریسم به زودی وارد دهۀ سوم خود خواهد شد. در حالی که ایالات متحده و متحدانش مزایای تاکتیکی را در میدان جنگ از خود نشان داده‌اند، در آن سو، تعداد مبارزان جهادی در ۱۱ سپتامبر ۲۰۰۱ تقریباً چهار برابر شده است. در طول هجده گذشته، جامعه ضدتروریسم درس‌های زیادی آموخته است، اما گروه‌های تروریستی نیز بیکار نمانده‌اند. آن‌ها نیز خود را با تاکتیک‌های معمول ضدتروریسم سازگار کرده و اقدامات متقابل خود را انجام می‌دهند. امروزه، سازمان‌های تروریستی در حال ایجاد ائتلاف‌های بین‌المللی هستند که گروه‌های آنها را قادر می‌سازد منابع خود را به اشتراک بگذارند و در مقابل فشار ضد تروریسم مقاومت کنند. جنگجوهای خارجی در سراسر جهان پراکنده شده‌اند و امکان تشکیل گروه‌های تروریستی جدید، تقویت گروه‌های موجود یا انجام حملات مرگبار خود را دارند. تروریست‌ها سلاح‌های سایبری تهاجمی را دنبال می‌کنند که قادر به تخریب

زیرساخت‌های حیاتی است. تنوع و شدت این تهدیدها فقط بر چالش‌هایی خواهد افزود که مقامات ضد تروریسم به زودی با آن روبرو خواهند شد. به منظور جلوگیری از قدرت یافتن تروریسم، به جای اینکه به سادگی به آن واکنش نشان دهیم، ایالات متحده باید تمرکز مجدد خود را بر روی موضوعاتی قرار دهد که ضد تروریسم را در سال‌های آینده بسنجد. بنابراین، با شناسایی و درک چالش‌های استراتژیک نوظهور، مانند تشکیل ائتلاف‌های بین‌المللی، پدیدهٔ جنگجوهای خارجی و ظهور تروریسم سایبری، مقامات ضد تروریسم آمادگی بهتری برای مبارزه با تروریسم در دههٔ ۲۰۲۰ خواهند داشت.