اینترنت؛ ابزار سیاست

پاره نخست: تروریسم مجازی؛ تهدیدی برای آینده

نویسنده: مهدی عباسی
دانشجوی کارشناسی ارشد علوم سیاسی

هر چه به خطر نزدیک تر می شویم، به همان اندازه راه‌های نیروی منجی می درخشند
مارتین هایدگر

چکیده

در نخستین پاره از این مقاله نشان داده خواهد شد که اگرچه تروریسم مجازی خطری است که در آینده عملی خواهد شد اما هم آینده چندان دور نیست و هم با وجود شبکه اکنون عراق ها و زیاده گویی هایی درباره ابعاد این خطر می شود اما تروریسم مجازی واقعیتی است که در انتظار ایستاده نشسته است. به گونه‌ای که هم اکنون نیز دهشت افکنان می توانند به راحتی پشت یک رایانه متصل به شبکه به ویژه شبکهٔ اینترنت بنشینند و زیان‌های گسترده‌ای را بر جوامع بشری، به ویژه جوامع پیشرفته، تحمیل کنند در حین وضعیتی تروریست ها دیگر نیازی به بمب یا مواد منفجره نخواهند داشت بلکه می توانند به راحتی و با یک صفحه کلید، مودم، کیس، نمایشگر و یک خط تلفن اغلب این اقدامات را انجام دادن کلید اینتر، بنیادهای اقتصادی جوامع را از کار بیاندازند. این خطری است که شاید اکنون شواهد اندکی دارد اما گسترش آن در آینده، به دلایلی که گفته خواهد شد، پیش بینی پذیر است.

واژه‌های کلیدی: اینترنت، تروریسم مجازی، ساختارهای زیربنایی، سیاست، شبکه‌های رایانه‌ای.

چه چیزهایی جامعهٔ اطلاعاتی را تهدید می کنند؟

امروزه، اگر متون مربوط به فناوری اطلاعات و ارتباطات را بررسی کنیم، انبوهی از واژه‌های نوپدید را خواهیم یافت که گرچه همه‌روزه حجم آنها افزایش می یابد اما گاه کمتر تعریف درست و مشخصی از آنها می شود.

مثلاً برای اشاره به تروریسم جدیدی که به‌واسطهٔ پیشرفت و همه گیری فراوانیت ملی کشورها را تهدید می کند، شمار زیادی از واژه‌ها مانند جنگ اطلاعاتی (info war)، جنگ شبکه‌ای (net war)، حملهٔ مجازی (cyber harrasment/cyber attack)، جنگ مجازی (virtual war)، تروریسم دیجیتالی (digital terrorism)، جنگ رایانه‌ای (computer warfare)، تروریسم مجازی (پرکاربردترین آنها) و... به کار می روند. دلیل اصلی بروز چنین وضعیتی این است که بسیاری از بحث ها و اظهارنظرها دربارهٔ این نوع تروریسم به جای آنکه در فضایی علمی انجام شود، در رسانه‌های عمومی و در میان افکار عمومی رواج دارد. در این رسانه‌ها نیز بیش از علم و منطق، احساس حکمرانی می کند. شاید یک دلیل عمدهٔ نبود تعریف دقیق و قابل اعتنا از پدیدهٔ تروریسم

مجازی، کاربرد این واژه در سطوح غیرعلمی باشد. (ویمن Weimann) و از قضا یکی از مهم‌ترین مشکلاتی که افکار عمومی و به‌ویژه کاربران خانگی دربارهٔ تروریسم مجازی دارند، نبود تعریفی مشخص از خود این واژه است. اگر از ۱۰ نفر پرسیده شود که منظور از تروریسم مجازی چیست، شاید به ده پاسخ متفاوت برسیم. با این حال در تمامی این تعریف‌ها، ویژگی مشترکی به چشم می‌خورد: رایانه به طور جدی هدف و ابزار حملات تروریستی گروه‌های فروملی علیه دولت‌ها و گاه دولت‌ها علیه یکدیگر شده است (گوردون Gordon). این واژه‌ها یادآور نبردهای شرارت‌آمیزی هستند که علیه زیربنای حیاتی یک ملت و با استفاده از رایانه و شبکه‌های رایانه‌ای شکل می‌گیرند. این گونه حملات، مشکلات پیچیده‌ای را پدید می‌آورند که به حوزه‌های مختلف امنیتی و سیاسی نیز سرایت می‌کند.

باوجود این ابهامات، برای یافتن معنا و تعریفی روشن و آشکار از تروریسم مجازی تلاش‌های بسیاری شده است. شاید در میان تمامی تعریف‌های موجود از این پدیده، بتوان ویژگی‌های مشترکی را یافت که آدمی را قادر به دستیابی به یک برداشت منسجم و مشخص از پدیدهٔ تروریسم مجازی می‌سازد. تروریسم مجازی، محل برخورد و نقطهٔ کانونی تروریسم و فضای مجازی است. بر این اساس می‌توان به طور کلی تروریسم مجازی را چنین تعریف کرد:

«بهره‌گیری از اینترنت و شبکه‌های رایانه‌ای و امکاناتی که این شبکه‌ها پدید می‌آورند با هدف نابود ساختن ساختارهای زیربنایی یک جامعه مانند انرژی، حمل و نقل، فعالیت‌های دولتی و تأثیر گذاشتن بر یک دولت، شهروندان، گروه‌ها و ...»

. یک استاد علوم رایانه‌ای نیز در تعریف تروریسم مجازی می‌نویسد: تروریسم مجازی نقطهٔ کانونی تروریسم از یک سو، و فضای مجازی از سوی دیگر است. این واژه ناظر بر مجموعه‌ای از حمله‌ها و تهدیدها علیه رایانه‌ها، شبکه‌ها و اندوخته‌های اطلاعاتی است که دولت‌ها را مجبور به بازنگری برنامه‌ها و اهداف می‌سازد. به‌علاوه تروریسم مجازی باید منجر به خشونت علیه افراد و دارایی‌ها شود یا دست‌کم ایجاد آسیب و ترس کند. تروریسم مجازی زیربناها و شالوده‌های حیاتی را به خطر می‌افکند و خدمات حیاتی را مختل می‌کند. (Weimann)

در آغاز دههٔ ۱۹۹۰ کاربرد اینترنت رشد سریعی یافت، بحث‌ها بر سر «جامعهٔ اطلاعاتی» و ظهور آن بالا گرفت و مطالعاتی دربارهٔ خطراتی پنهانی که به واسطهٔ وابستگی بسیار زیاد به شبکه و فاوا، امریکا را تهدید می‌کرد، انجام شد. مفهوم تروریسم مجازی نیز از همین دوران ریشه می‌گیرد. آکادمی ملی علوم در امریکا، در دههٔ ۱۹۹۰، گزارش خود را دربارهٔ امنیت رایانه‌ای با این عبارات آغاز کرد:

ما در خطر هستیم. امریکا به گونهٔ فزاینده‌ای به رایانه‌ها وابسته است. فردا، دهشت‌افکنان ممکن است بتوانند به جای بمب تنها با یک صفحه کلید به ما زیان وارد آورند. در این هنگام، واژهٔ «پرل هاربر» (Pearl Harbour) الکترونیک در زمینهٔ تهدید ناشی از حمله‌ای رایانه‌ای به امریکا وضع شد. بر اساس سیاست‌های دولت امریکا، به وحشت از تروریسم مجازی دامن زده شد. به همین دلیل نیروهای روان‌شناختی، سیاسی و اقتصادی گوناگون با هدف افزایش ترس از تروریسم مجازی به کار گرفته شدند. از یک دیدگاه روان‌شناختی دو وحشت بزرگ دوران مدرن در واژهٔ «تروریسم مجازی» در هم آمیخته است: وحشت از بخت و تصادف و تعدی خشونت‌آمیز، و وحشت از فناوری رایانه‌ای (توماس Thomas).

با این حال تفاوتی آشکار و جدی میان تروریسم مجازی و سایر خرابکاری‌های رایانه‌ای و اینترنتی وجود دارد. در واقع میان، آسیب زدن به شبکه‌های اطلاعاتی و رایانه‌ای از یک سو و آسیب زدن به زیربناهای حیاتی یک ملت با بهره‌گیری از رایانه و شبکه‌های اطلاعاتی از سوی دیگر، تفاوت وجود دارد. به دیگر بیان، تنها اقداماتی را می‌توان در چارچوب تروریسم مجازی دسته‌بندی کرد که نه به شبکه‌های رایانه‌ای بلکه به تأسیسات و خدمات عمومی در یک کشور با استفاده از شبکه‌های رایانه‌ای صدمه بزنند. چنین است که به اعتقاد عده‌ای از پژوهشگران، شرط اینکه اقدامی تروریسم مجازی نامیده شود این است که آن کنش به خشونت علیه اهداف غیرنظامی بیانجامد و به‌وسیلهٔ گروه‌های فروملی یا عوامل پنهانی صورت بگیرد. اما عده‌ای از صاحب‌نظران اختلال در شبکهٔ اینترنت و سامانهٔ رایانه‌های دولتی را نیز یکی از جلوه‌های تروریسم مجازی می‌دانند. بر این اساس تروریسم مجازی شامل موارد زیر می‌شود:

◇ تخریب ساختارهای اطلاعاتی

◇ ایجاد اختلال کنترل شده و از راه دور در فاوا به‌ویژه اینترنت، شبکه‌های رایانه‌ای دولتی، سامانه‌های رایانه‌ای شهری مانند شبکه‌های مالی بانک‌ها، رسانه‌های جمعی و حتی استفاده از شبکه‌های رایانه‌ای برای ایجاد اختلال در مسیر کار چراغ‌های راهنمایی و رانندگی و سامانهٔ کنترل هواپیماها و فرودگاه‌ها و ... (ویمن).

بر اساس این تعریف‌ها، برخی از اقدامات و برنامه‌ها را می‌توان در قالب تروریسم مجازی دسته‌بندی کرد:

تروریست‌های مجازی قصد دارند از راه دور بر سیستم‌های کنترل کارخانه‌های تولید مواد غذایی و تولید دارو دست یابند و با دست‌کاری فرمول افزودنی‌ها و مواد به کار رفته در آنها به شمار زیادی از مردم صدمه بزنند.

تروریست‌های مجازی در پی آن هستند که بتوانند از راه دور و بدون حضور فیزیکی شهرهای موردنظر خود را بمباران کنند. آنها به دنبال تخریب سامانه‌های بانکی و معاملات بین‌المللی هستند.

آنها می‌خواهند که به سیستم‌های کنترل ترافیک شهری حمله کنند و حتی موجب تصادف هواپیماها با یکدیگر

شوند (کولین Collin).

در این راه تروریست‌ها گاه با طراحی برنامه‌ها و نرم‌افزارهای رایانه‌ای ویژه اقدام به ایجاد اختلال در سامانه‌های خدمات عمومی می‌کنند. آنها نرم‌افزارهای ویژه‌ای طراحی می‌کنند که حتی گاه از سوی مسئولان دولتی در نهادها و سازمان‌های عمومی استفاده می‌شود. مثلاً پلیس ژاپن در مارس ۲۰۰۰ اعلام کرد که اعضای فرقهٔ آئوم در ژاپن که یک بار در سال ۱۹۹۵ دست به عملیات تروریستی در متروی توکیو زده و موجب مرگ ۲۰ نفر و زخمی شدن ۶۰۰ نفر شده بودند نرم‌افزاری ویژه طراحی کرده‌اند که وسایل نقلیه و خودروهای پلیس را ردیابی می‌کند. آنها با استفاده از این نرم‌افزار مشخصات و اطلاعات طبقه‌بندی شدهٔ ۱۱۵ وسیلهٔ نقلیهٔ پلیس را منتشر ساختند. به‌علاوه تهیه‌کنندگان این نرم‌افزار، نرم‌افزارهای دیگری را نیز برای اختلال در چندین کارخانه و نهاد دولتی ژاپن طراحی کرده بودند.

آسیب‌پذیری جدید

چرا به تروریسم مجازی در حکم تهدیدی جدی برای آیندهٔ بشری توجه می‌شود؟ چه شرایطی برای حال و آیندهٔ جامعهٔ بشری پیش‌بینی می‌شود که تروریسم مجازی به‌مثابه خطری در برابر جوامع به‌شمار می‌آید؟

اکنون اصلی‌ترین ویژگی جوامع بشری آمیختگی کنش‌های سیاسی، اجتماعی و اقتصادی این جوامع با فاوا است. این آمیختگی به‌راحتی به وابستگی جوامع به این فاوا انجامیده است. همین وابستگی است که به نقطه ضعف جدی برای جوامع تبدیل شده است.

در واقع، تروریسم مجازی به این دلیل اعتبار یافته است که ملت‌ها و ساختارهای حیاتی آنها هر روز، بیش از پیش، به شبکه‌های رایانه‌ای وابسته می‌شوند. این امر بر آسیب‌پذیری آنها می‌افزاید و آسیب‌های جدیدی را نیز بر آنها تحمیل می‌کند. بدین ترتیب جوامع، «پاشنه آشیل‌ها» و «چشم اسفندیارهای» الکترونیک یافته‌اند.

در بسیاری از آثاری که به تروریسم مجازی پرداخته‌اند، گمان می‌رود که آسیب‌پذیری شبکه‌های رایانه‌ای موجب آسیب‌پذیری زیربناهای حیاتی یک ملت می‌شود و این آسیب‌پذیری امنیت ملی را به خطر می‌اندازد. پس تا زمانی که زیربناهای حیاتی یک کشور بیش از پیش به فاوا وابسته باشند، به همان اندازه آسیب‌پذیرتر خواهند شد. برای سنجش میزان این آسیب‌پذیری باید میزان وابستگی زیربناهای ملی را به شبکه‌های رایانه‌ای سنجید.

در سال ۲۰۰۳ جمعی از نویسندگان و روزنامه‌نگارانی که در سراسر دنیا دربارهٔ علوم رایانه‌ای مطلب می‌نوشتند، کتابی را منتشر کردند و در آن مدعی شدند که هدف اصلی تروریسم مجازی آسیب زدن به صنایع انرژی است. این مسئله به‌ویژه در مورد امریکا کاملاً درست است. یکی از نویسندگان این کتاب استدلال می‌کند که بخش صنایع انرژی در امریکا نخستین مهره‌ای است که می‌تواند در حملات تروریست‌های مجازی علیه امریکا استفاده شود. در این کتاب همچنین نشان داده شده است که خسارات ناشی از تروریسم مجازی تا چه اندازه ممکن است گسترده‌تر از حملات فیزیکی باشد.

عده‌ای دیگر معتقدند که شبکهٔ آب‌رسانی امریکا بسیار مستعد است که به هدف اصلی تروریسم مجازی تبدیل شود. در امریکا ۵۴ هزار و ۶۴ سامانهٔ مستقل آب‌رسانی وجود دارد. از این میان سه هزار و ۷۹۶ سامانه به ۸۱ درصد جمعیت امریکا و ۳۵۳ سیستم دیگر به بقیهٔ جمعیت، خدمات آب‌رسانی ارائه می‌دهند. با این حال گفته می‌شود که ناهمگونی فناوری شبکه که در این سیستم‌ها به کار رفته است، فعالیت تروریست‌های مجازی را دشوار و پیچیده می‌سازد (لوییس Lewis). تروریسم مجازی، آسان و کم‌هزینه است. در مجموع پنج مؤلفه موجب می‌شود که تروریست‌ها از شیوه‌های مجازی برای دستیابی به اهداف خویش بهره بگیرند:

۱. ارزان بودن این روش‌ها نسبت به روش‌های سنتی تروریسم: تروریست در روش مجازی تنها به یک رایانه و ارتباط با اینترنت و شبکه نیاز دارد و نیازی به صرف هزینه‌های کلان برای خرید اسلحه نیست.

۲. ابهام و بی‌نام و نشانی: روش مجازی هویت تروریست‌ها را پنهان نگاه می‌دارد. تروریست‌ها از اسامی مستعار استفاده می‌کنند و شناسایی هویت واقعی آنها برای نهادهای امنیتی بسیار مشکل است.

۳. تنوع و فراوانی اهداف: تروریست‌ها می‌توانند رایانه‌ها، شبکه‌های رایانه‌ای، افراد، امکانات عمومی، خطوط هوایی و ... را با استفاده از همین روش تهدید کنند.

۴. عملکرد قابل کنترل از راه دور: تروریسم مجازی از راه دور قابل کنترل است بنابراین نیازی به حضور فیزیکی تروریست نیست. بر این اساس خطر مرگ، سرمایه‌گذاری روانی و ... کاهش می‌یابد.

۵. گسترهٔ وسیع تأثیرگذاری: هنگامی که ویروس I Love You منتشر شد، آشکار گشت که تروریسم مجازی این توان را دارد که نسبت به روش‌های سنتی تروریسم، بر شمار بیشتری از افراد تأثیر بگذارد.

بنابراین امکان گسترش تروریسم در آینده کاملاً فراهم است اما عده‌ای از نویسندگان فقدان شواهد و نمونه‌هایی از این جریان را در دورهٔ فعلی، گواهی می‌گیرند بر اینکه دربارهٔ وجود خطر تروریسم مجازی اغراق شده است. تروریسم مجازی پدیده‌ای جدید است و چیزهای نو ممکن است در آغاز وحشتناک‌تر یا دلخواهانه‌تر از آنچه که

در واقع هستند، به نظر آیند. حتی اگر این اغراق را در دورهٔ کنونی بپذیریم، نمی توانیم منکر آن شویم که با گذشت زمان و دستیابی تروریست ها به امکانات جدیدتر و فناوری های به روزتر، این نوع تروریسم نیز گسترش بیشتری خواهد یافت. از سوی دیگر حملات ۱۱ سپتامبر نشان داد که بسیاری از نهادها و خدمات دولتی تا چه اندازه در برابر تروریسم آسیب پذیر هستند. اما این نقطهٔ قوت اساسی وجود دارد که جوامع پیشرفته زیربناهای حیاتی پیشرفته ای نیز دارند. آنها مبتنی بر بازار مولد هستند و ویژگی خودترمیم کنندگی دارند. تنها این امر می تواند از آسیب پذیری جوامع در برابر تروریسم مجازی بکاهد.

اکنون مبارزه با تروریسم مجازی نه تنها موضوعی سیاسی است بلکه به امری اقتصادی نیز تبدیل شده است. به گونه ای که در شرکت های رایانه ای شاخه های صنعتی و مطالعاتی برای مبارزه با تروریسم مجازی ایجاد شده است. بسیاری از شرکت ها به سرعت می کوشند نرم افزارها و سخت افزارهای ویژه ای تولید کنند که بتوانند ضریب ایمنی شبکه های رایانه ای و نیز رایانه های شخصی را بالا ببرند. بسیاری از کاربران خانگی نیز تلاش کرده اند برای سیستم های رایانه ای خود ابزارها و نرم افزارهای دفاعی مناسبی تهیه کنند. در واقع، به اعتقاد پاره ای از پژوهشگران، تروریسم مجازی کاربران خانگی را نیز هدف قرار خواهد داد (گوردون).

بنابراین در آینده ای نه چندان دور خواهیم دید که رایانه ها می توانند نقشی جدی و برجسته را نه تنها در حملات مجازی بلکه در هر گونه حملهٔ تروریستی و دیگر کنش های سیاسی که در بخش های دیگر بررسی خواهد شد ایفا کنند. نسل آیندهٔ تروریست ها در فضای مجازی و دیجیتالی فعالیت خواهند کرد. با این حال در این میانه نباید اسیر احساساتی شد که گردانندگان شرکت های رایانه ای با مقالات و تبلیغات خویش به خوانندگان و کاربران خانگی القامی کنند. آنها بیش از اندازه دربارهٔ خطر تروریسم مجازی به ویژه برای کاربران خانگی اغراق می کنند. در واقع، به میان آوردن کاربران خانگی در چارچوب اهداف تروریسم مجازی، تأثیر تبلیغات این دسته از مدیران و کارشناسان وابسته به شرکت های رایانه ای است که می کوشند کاربران خانگی را به خرید برنامه های ویروس کش و دیگر برنامه های حفاظتی خویش تشویق کنند.

آیا اقدامات القاعده نمونهٔ تروریسم مجازی است؟

پس از رخدادهای ۱۱ سپتامبر، در دنیا گفتمانی امنیتی حول محور تروریسم و مبارزهٔ با آن، سازمان یافت و در این راستا نیز خطر تروریسم مجازی برجسته شد. بحث و گفت وگو بر سر امنیت ملی، به ویژه در فضای مجازی، بسیاری از سیاستمداران را جذب خود ساخت. یک باره کاربرد واژهٔ تروریسم مجازی افزایش یافت و در رسانه ها دربارهٔ اقدامات تروریست ها و بودجه های کلان دفاعی سخن به میان آمد.

پس از حوادث ۱۱ سپتامبر، دولت فدرال امریکا برای بازسازی زیربنای امنیتی ۴/۵ میلیون دلار خرج کرد. پلیس فدرال امریکا بیش از یک هزار مأمور ویژهٔ تحقیق را در زمینهٔ تروریسم مجازی و امور مجازی، اینترنتی و شبکه ای به خدمت گرفت. مهم تر از همه اینکه در پی این رخدادها ادارهٔ امنیت فضای مجازی در کاخ سفید تأسیس شد (ویمن). اما آیا رخدادهای ۱۱ سپتامبر و اقدامات تروریستی القاعده را می توان به مثابه نشانه ای از تروریسم مجازی پنداشت؟ بسیاری از پژوهشگران معتقد هستند که اقدامات گروه القاعده، در چارچوب تروریسم مجازی دسته بندی می شود. اما در واقع القاعده و بهره گیری آن از اینترنت و رایانه، نه نشانهٔ تروریسم مجازی بلکه نشان دهندهٔ خطر بدید آمدن این گونه تروریسم در آینده است.

هنگامی که نیروهای امریکایی، رایانه ها، نوت بوک ها و لپ تاپ های القاعده را در افغانستان بررسی کردند، از دیدن اینکه القاعده اعضایی در اختیار دارد که از نظر علمی و فنی در زمینهٔ علوم رایانه ای بسیار حرفه ای و زبردست هستند، شگفت زده شدند. در میان نرم افزارهایی که در رایانه های القاعده بود ساختارها و مدل الکترونیک یک سد و اطلاعاتی دربارهٔ رایانه ای کردن شبکهٔ آب رسانی، هواپیماهای اتمی (atomic airplane) و استادیوم های ورزشی امریکا و اروپا دیده می شد. این شواهد هر چند هرگز نشان نمی داد که القاعده در پی طراحی یک عملیات تروریستی مجازی است اما بیانگر خطر وجود چنین عملیاتی در آینده بود (لوییس).

اعضای القاعده از اینترنت و شبکه های رایانه ای برای برقراری ارتباط با یکدیگر و طراحی حملات تروریستی فیزیکی استفاده می کردند. بی تردید می توان گفت که القاعده عاشق اینترنت است. شواهدی جدی نشان می دهند که تروریست ها در برنامه ریزی عملیات ۱۱ سپتامبر از اینترنت بهره برده اند. در افغانستان دوران طالبان استفاده از رایانه ممنوع بود. بر اساس گزارش ها، القاعده اطلاعات خود دربارهٔ هدف هایش را از راه اینترنت گرد می آورد و از همان راه نیز رمزگذاری می کرد. در ۱۶ سپتامبر ۲۰۰۲، گزارش ها نشان می دهند که سلول های القاعده در امریکا برای ارتباط با سلول های این گروه در مناطق دیگر، از تلفن اینترنتی بهره برده اند. این رویدادها نشان می دهند که اینترنت به یک ابزار «جنگ مجازی» برای تروریست ها بدل شده است. اینترنت این امکان را به تروریست ها می دهد که گمنام بمانند و در عین گمنامی منابع خویش را اداره و کنترل کنند.

از ۱۱ سپتامبر به بعد، منابع امریکایی وب سایت ها اینترنتی زیر را که با القاعده در ارتباط بودند بازبینی کردند:

◇ alneda.com که مقامات امریکایی ادعامی کنند که این سایت اطلاعات رمزدارشده‌ای که اعضای القاعده راهماهنگ می سازد، اخبار بین المللی دربارهٔ القاعده و مقالات، فتاوا و کتاب هایی رانیز منتشر می کند.
◇ assam.com که گمان می رود به القاعده وابسته باشد. این سایت در نقش بلندگوی جهاد در افغانستان، چچن و فلسطین عمل می کند.
◇ almuhajiroun.com یکی از سایت‌های القاعده است که بر هواداری از ترور پرویز مشرف رئیس جمهور پاکستان تأکید می ورزد.
◇ Vhj.Vhj.com که در پی آموزش چگونگی حملات رایانه‌ای به بینندگان خود است.
◇ aloswa.org که بخش هایی از سخنان بن لادن رانقل می کند، اصولی از شریعت که به تروریسم مشروعیت می بخشند رابه نمایش می گذارد و از القاعده حمایت می کند.
◇ drasat.com که به وسیلهٔ مرکز مطالعات وپژوهش های اسلامی (که برخی مدارک نشان می دهند که این مرکز، مرکزی تقلبی و غیرواقعی است) ایجاد شده است و گزارش گردیده است که بسیار قابل اعتمادتر از انبوه سایت هایی است که اخبار القاعده رامنتشر می سازند.
◇ jehad.net, alsaha.com, islammemo.com اعلامیه های القاعده رادر وب سایت های خود منتشر می سازند.
◇ mwhoob.net و aljehad.online پیام های سیاسی و مذهبی رامنتشر می سازند و سیاست امریکا و رهبران عرب، به‌ویژه عربستان، رامحکوم می کنند (توماس).

پس از حملات ۱۱ سپتامبر، القاعده برای استفاده از اندیشه و همکاری مسلمانان در سراسر جهان از اینترنت بهره برد. عده‌ای از رهبران مسلمان حملات القاعده راریاکاری می دانند. القاعده به طور رسمی دو سایت النداء و دراسات رااداره می کرد و در آنها از مشروع و قانونی بودن حملات ۱۱ سپتامبر سخن می راند. القاعده بر آن است که اسلام هیچ ارزش بنیادین مشترکی با غرب ندارد و مسلمان ها موظف هستند که اسلام را با بهره گیری از شمشیر گسترش دهند. بنابراین دیده می شود که اینترنت برای القاعده بیشتر ابزاری تبلیغی و ارتباطی است تا ابزاری برای تروریسم و جنگ مجازی.

اینترنت در راه سیاست

هنگامی که اینترنت برای نخستین بار پدیدار شد به آن به منزلهٔ ابزاری برای یکپارچه سازی فرهنگ ها و محیطی برای ارتباط بازرگانان، مصرف کنندگان و دولت ها با یکدیگر توجه شد. اینترنت مجال بی همتایی رابرای پدید آوردن «دهکدهٔ جهانی» به‌وجود آورده است. امروزه اینترنت همچنان پدید آمدن دهکدهٔ جهانی را نوید می دهد اما در همان حال، از برخی جنبه ها به تهدیدی دیجیتال و نبردگاهی مجازی تبدیل شده است. کاربرد اینترنت از سوی القاعده و نبرد مجازی تایوان و چین، اسراییل و فلسطین، پاکستان و هند، و چین و امریکا نمونه هایی از این تهدید هستند. در ماجرای جنگ در کوزوو نیز اینترنت به‌مثابه نبردگاهی مجازی میان نیروهای ائتلاف ناتو و عناصر صرب به‌کار می رفت.

همچنین در سال های گذشته بارها و بارها به شبکه های رایانه‌ای به‌وسیلهٔ هکرها و تروریست ها حمله شده است. حملاتی که آشکارا اهداف سیاسی داشته اند. مثلاً در سال ۱۹۹۸ شورشی های اسپانیایی به مرکزی دولتی با ایمیل های دروغین حمله کردند. در همین سال شورشی های تامیل سفارت خانه‌های سریلانکا را با هزار ایمیل در روز و به مدت دو هفته مختل ساختند. در سال ۱۹۹۹ نیز به رایانه های ناتو در جریان جنگ کوزوو به‌وسیلهٔ ایمیل ها و پیام‌های هرز حمله شد. همچنین ویروس های رایانه‌ای از برخی از کشورهای اروپای شرقی به این رایانه ها حمله کردند (دنینگ Denning).

بنابراین بی تردید در آیندهٔ بسیار نزدیک خواهیم دید که تروریسم مجازی، کنش ها و خشونت های سیاسی با استفاده از روش های ویژهٔ الکترونیک و در فضای دیجیتالی انجام می شوند.

در بخش های دیگر مقاله تأثیرات فاوا بر کنش های سیاسی کنشگران، با مطالعهٔ پدیده های هکتیویسم و سانسور، بیشتر بررسی خواهد شد.

منابع

1.Collin, Barry C. "The future of cyberterrorism", Institute for Security and Intelligence /afgen.com/ terrorism1.html.
2.Denning, Dorothy E. (2000), "Cyberterrorism", United States: Georgetown University.www.cs.georgetown,edu.
3.Gordon. Sarah (2003), "Cyberteroorism and the home user" ,Symantec Security Response. www.security response .symantec .com.
4.Green, jashua (2002), "the myth of cyberterrorism". washington monthly, November 2002.
5.Lewis, James A.(2003), "Assessing the risk of cyberterrorism, cyber war and other cyber threats" Center for strategic and International Studies/ www.golbalcontinuity.com/article/ articleview/413/1/45.
6.Thoenas, Timothy L. (2003), "Alqaeda and the internet: the danger of cynberplanning", parameters, Spring2003,112-123
7.Weimann, Gabriel (2004), "cyberterrorism: how real is threat? United States: Institute of Peace. www.usip.org /pubs / specialreports /sr119.html.