تاریخ دریافت: ۹۱/۴/۴
تاریخ پذیرش: ۹۱/۴/۳۱

تروریسم دولتی در فضای مجازی و راهکارهای مقابله با آن

نوشتهٔ
احمدرضا شاه‌علی*
احسان موحدیان**

چکیده

با گسترش فناوری‌های ارتباطی و اطلاع‌رسانی، مفهوم و معنای بسیاری از پدیده‌های نام آشنای قدیمی به طور کامل یا نسبی تغییر کرده و تأثیرپذیری از تحولات پرشتاب عصر اینترنت باعث دگرگونی آن‌ها شده است.

تروریسم و یکی از شاخه‌های خطرناک آن یعنی تروریسم دولتی نیز از این تحولات تأثیرپذیرفته و پیدایش شبکه‌های اطلاع‌رسانی مانند اینترنت و شبکه‌های تلفن همراه به حامیان و سازمان دهندگان تروریسم دولتی امکان داده تا به شیوه‌های نوینی به اهداف خود جامه عمل بپوشانند.

در این مقاله ضمن بررسی معنا و مفهوم تروریسم دولتی در فضای مجازی، انواع و جنبه‌های مختلف این پدیده بررسی شده و راهکارهایی برای مقابله با آن ارائه می‌شود. همچنین راهکارهای مبارزه با تروریسم مجازی در ایران و اقدامات صورت گرفته در این زمینه بیان می‌شود. نویسندگان نشان داده‌اند تروریسم مجازی به علت ویژگی‌های خاص خود باعث شده تحقق اهداف حامیان تروریسم دولتی با هزینهٔ کمتر و سهولت و مخفی‌کاری بیشتر ممکن شود.

کلیدواژه: اینترنت، تروریسم، تروریسم دولتی، فضای مجازی، دولت، شبکه‌های رایانه‌ای.

مقدمه

نیاز انسان به برقراری ارتباط با همنوعان به منظور رفع نیازهای گوناگون مادی و معنوی به ابداع روش‌های گوناگون ارتباطی و اطلاع‌رسانی در طول تاریخ منجر شده، به‌گونه‌ای که طی دو دهه اخیر شاهد نفوذ دستاوردهای حاصل از فناوری اطلاعات و ارتباطات در جوامع مختلف به عنوان پیشرفته‌ترین فناوری ارتباطی موجود در جهان هستیم. امروزه پیشبرد بسیاری از امور عادی زندگی بدون استفاده از خدمات مبتنی بر این فناوری بسیار دشوار و در مواردی غیرممکن شده است و

* استادیار گروه معارف اسلامی دانشگاه علم و صنعت ایران shahali@iust.ac.ir
** دانجشوی دکتری روابط بین‌الملل دانشگاه علامه طباطبایی movahhedian@gmail.com

دولت‌های مختلف و همین‌طور شرکت‌های خصوصی از بستر اینترنت و وب برای ارائه خدمات گوناگون به مردم استفاده می‌کنند.

بنابراین اموری که قبلاً با صرف وقت و هزینه فراوان و پس از رفت‌وآمد مکرر به ادارات و سازمان‌های مختلف انجام می‌شدند، با مراجعه به چند وب‌گاه، پر کردن فرم‌های الکترونیک از قبل مشخص شده و ارسال آن‌ها با یک کلیک قابل انجام هستند.

مزایای ناشی از استفاده از اینترنت و خدمات اینترنتی به افزایش سریع تعداد کاربران آن در نقاط مختلف دنیا و از جمله ایران انجامیده است. بر اساس تازه‌ترین گزارش مرکز آمار ایران از مجموع ۲۰/۳ میلیون خانوار کشور در حدود ٤/۳ میلیون خانوار (۲۱/٤درصد) در محل سکونت به اینترنت دسترسی داشته‌اند. همچنین ۱۸/٤ میلیون نفر از جمعیت کشور در سال ۱۳۸۹ کاربر رایانه بوده‌اند.

از مجموع جمعیت کشور ۱۱ میلیون نفر کاربر اینترنت بوده‌اند و ضریب نفوذ اینترنت در کشور ۱٤/۷درصد است که نسبت به سال ۱۳۸۷ حدود ۳/٦درصد رشد نشان می‌دهد. از میان این افراد ٦/٤ میلیون نفر (۵۸/۱درصد) مرد و ٤/٤ میلیون نفر (٤۱/۹درصد) زن هستند. کاربران مرد و زن اینترنت به ترتیب ۱٦٦/٦ و ۱۲/۷درصد از کل جمعیت مردان و زنان را به خود اختصاص داده‌اند که‌این ارقام در مقایسه با سال ۱۳۸۷ به ترتیب ٤/۱ و ۳/۲درصد افزایش یافته است (خبرگزاری فارس، ۲۲ اسفند ۱۳۹۰).

ارائه خدمات عمومی به مردم با استفاده از اینترنت و دیگر انواع شبکه‌های الکترونیک مانند اینترانت که برای توصیف آن از واژه‌هایی همچون دولت الکترونیک و خدمات الکترونیک استفاده می‌شود، اگر چه باعث سهولت بسیاری از امور شده، اما فرایندهای مورد استفاده برای ارائه چنین خدماتی مشکلات متعددی را نیز برای جوامع بشری به وجود آورده که از جمله مهم‌ترین آن‌ها می‌توان به راحت‌تر شدن برنامه‌ریزی جهت انجام جرائم و تخلفات ریز و درشت و عملی کردن آن‌ها اشاره کرد.

با عنایت به اینکه حفظ امنیت شبکه‌های رایانه‌ای و محافظت از زیرساخت‌های مورد نیاز برای اداره شبکه اینترنت و ایمن‌سازی خدمات و اطلاعات ارزشمند موجود در آنکه اطلاعات حساس شخصی، تجاری و دولتی را شامل می‌شود، از اهمیت غیرقابل انکاری برخوردار است، ضروری است تا ضمن شناخت ابعاد مختلف پدیده نوظهور تروریسم مجازی (Cyber Terrorism) ، انواع و روش‌های مختلف اجرای این حملات و همین‌طور شیوه‌های مقابله با آن به طور تفصیلی مورد بررسی، تجزیه و تحلیل قرار بگیرد. با توجه به اینکه منابع و اطلاعات چندانی در مورد تروریسم مجازی مورد حمایت دولت‌ها به زبان فارسی وجود ندارد و کتب و مقالات موجود صرفاً تروریسم دولتی یا تروریسم مجازی را به طور جداگانه مورد بررسی قرار داده‌اند و کشورهای غربی و به خصوص آمریکا و رژیم صهیونیستی در دو سال اخیر از این روش جدید برای ضربه‌زدن به نظام جمهوری اسلامی‌استفاده کرده‌اند، مطالعه نظام‌مند پدیدهٔ تروریسم دولتی (State Terrorism) در فضای مجازی (Cyber Space) اهمیت فروانی می‌یابد.

در این مقاله که به بررسی مسئله تروریسم دولتی در فضای مجازی (State-Sponsored Cyber Terrorism) می‌پردازد، به‌این پرسش اساسی پاسخ داده شده که همه‌گیر شدن اینترنت و دسترسی آسان به فناوری‌های ارتباطی و اطلاع‌رسانی چه تأثیری بر تحقق اهداف تروریسم دولتی داشته است؟ برای پاسخ به‌این سؤال، یکی از پیامدهای فراگیرشدن اینترنت، یعنی شکل‌گیری مفهومی به نام تروریسم مجازی مورد بررسی قرار گرفته که ویژگی‌های خاص آن باعث شده تحقق اهداف حامیان تروریسم دولتی با هزینه کمتر و سهولت و مخفی‌کاری بیشتر ممکن شود.

همچنین نویسنده به سؤالات فرعی زیر پاسخ داده است: تعریف دو مفهوم تروریسم و تروریسم دولتی چیست، تعریف تروریسم مجازی و روش‌های مختلف اعمال آن از سوی دولت‌ها چه هستند، چه نمونه‌های عینی در این زمینه وجود دارد و در نهایت از چه روش‌ها و راهکارهایی برای مقابله با تروریسم مجازی دولتی در جهان و ایران استفاده شده است.

در این بررسی از روش توصیفی ـ تحلیلی در چارچوب تجزیه و تحلیل داده‌های اسنادی، محتوای اینترنتی و کتب و نشریات مرتبط استفاده شده است.

تعریف تروریسم و تروریسم دولتی

به نوشتهٔ دائرةالمعارف فرانسوی مشهور لاروس، تروریسم در لغت به‌معنای ترساندن، ایجاد ترس و وحشت در مردم و حکومت ارعاب و تهدید است. واژهٔ ترور (Terror) برگرفته از ریشه لاتین (Terreur) بوده که به‌معنای نظام یا رژیم وحشت است. کلید واژه ترور هم این گونه‌تعریف شده است: ایجاد هراس در تودهٔ مردم یا گروهی از مردم به منظور درهم شکستن مقاومتشان؛ برقراری نظام یا فرایند سیاسی بر پایهٔ این ترس، از طریق به‌کارگیری اقدامات حاد و خشونت‌بار (Larousse, 1964: 258).

در دانشنامه بریتانیکا (2004)، تروریسم "کاربرد نظام‌مند ارعاب یا خشونت پیش‌بینی ناپذیر بر ضد حکومت‌ها، مردمان یا افراد برای دستیابی به یک هدف سیاسی" دانسته شده است.
بر اساس ماده یک "کنوانسیون سازمان کنفرانس اسلامی برای مقابله با تروریسم" نیز تروریسم به هر اقدام خشونت‌آمیز یا تهدید به آن گفته می‌شود که صرف‌نظر از مقاصد مرتکبین آن به منظور ارعاب یا تهدید آنان صورت می‌گیرد و موجب به خطر افتادن جان یا امنیت آنان یا آسیب رساندن به محیط زیست یا به یکی از تأسیسات یا اموال خصوصی یا عمومی شود (علی بابایی، ۱۳۸٤: ۹٤ـ۱۸۸).

یکی از جامع‌ترین تعاریف دانشگاهی از مفهوم تروریسم که‌در منابع مختلف به طور مکرر بیان شده، تعریف آلکس پ.اشمید (Alex P.Schmid) است. اشمید که‌ازهمکاری بیش از پنجاه محقق و صاحب نظر به منظور پالایش و دقیق‌تر کردن تعریف خود بهره برده است، نتیجه می‌گیرد که:

تروریسم شیوه اقدامات تکراری به منظور ایجاد دلهره و رعب و وحشت است که بـه دلایـل سلیقه‌ورزی، جنایی و یا سیاسی توسط گروه‌های مختلف به کار گرفته می‌شود. البتـه تعریـف اشمیت به همین جا ختم نمی‌شود و در ادامه بـین نـوع اهـداف مـوردنظر، تـأثیر مـوردنظر، تصادفی یا انتخابی بودن عمل و...تفکیک قائل می‌شود (Schmid, 1993: 8).

با توجه به این تعاریف می‌توان تروریسم را به طور خلاصـه ایـن گونـه تعریـف کـرد: بـه کارگیری خشونت و استفاده از زور علیه اشخاص، دولت‌ها یا گروه‌ها برای دستیابی به اهـداف سیاسی یا اجتماعی.

تروریسم در دهه‌های اخیر تنوع بسیار زیادی پیدا کرده و دانشمندان علـوم اجتمـاعی انـواع مختلفی از آن را احصا و تعریف کرده‌اند که یکی از مهم‌ترین انواع آن که در این مقاله نیز مورد بحث قرار گرفته، تروریسم دولتی یا State terrorism است. در مورد تعریف تروریـسم دولتـی هم نظر یکسانی وجود ندارد و تعاریف مختلفی در این زمینه ارائه شده است. استفادهٔ فراگیر از این اصطلاح از اوایل دههٔ ۱۹۸۰ میلادی و از سـوی مـسئولان وزرات امـور خارجـه آمریکـا و سخنگویان کاخ سفید رواج پیدا کرد تا تروریسم صرفاً اقدامات خشونت‌آمیزی توصـیف شـود که توسط تعدادی از دولت‌های مغضوب از نظر آمریکا مانند لیبی، کره‌شمالی، ایران، سـوریه و شوروی سابق، سازماندهی، پشتیبانی و اجرا می‌شوند. منظـور ایـن مـسئولان دولتـی از کـاربرد اصطلاح تروریسم دولتی عبارت بـود از «اعمـال خـشونت برنامـه‌ریـزی شـده و دارای انگیـزه سیاسی به وسیله کارگزاران پنهان دولت بر ضد هدف‌های غیر رزمی» (دردریان، ۱۳۸۲: ۹۱).

در سال‌های بعد تعاریف آکادمیک متعددی از تروریسم دولتی ارائه شد. از جملـه دردریـان (1991: 251)، تروریسم دولتی را خشونت برنامه‌ریزی شده دانست که با انگیزه‌سیاسی و توسط کارگزاران غیررسمی دولت اعمال می‌شود.

یکی دیگر از تعاریف آکادمیک در این زمینه را جاناتان وایت ارائـه کـرده اسـت. از نظـر او تروریسم دولتی زمانی به وقوع می‌پیوندد که نظام‌های حـاکم، در عرصـهٔ روابـط بـین‌المللـی و خارج از تشریفات پذیرفته شده دیپلماتیک، اعمال خشونت کـرده یـا تهدیـد بـه اسـتفاده از آن می‌کنند. این خشونت برنامه‌ریزی شده با انگیزهٔ سیاسی، توسط کارگزاران پنهان دولت بـر ضـد هدف‌های غیررزمی اعمال می‌شود. وی علت حمایت دولت‌ها از تروریسم را تحقق آن دسته از اهداف سیاست خارجی می‌داند که از دیگر راه‌های سیاسی یا نظامی قابـل حـصول نیـستند. بـه اعتقاد وی گاه دولت‌ها برای به دست‌آوردن یـا تقویـت پایگـاه قـدرت و نفـوذ خـود در میـان جنبش‌های ایدئولوژیک از تروریسم حمایت می‌کنند. برخی دیگر از اقدامات تروریستی تحـت حمایت دولت برای فرونشاندن مخالفت‌های داخلی از رهگذر قتل مخالفان در خارج از کشور صورت می‌پذیرد. به کارگیری تروریسم دولتی مبین شیوه کم‌خطر و کـم‌خرجـی بـرای هـدایت سیاست خارجی است. تروریست‌های تحت حمایت دولت‌ها می‌توانند از مساعدت‌های دولت که به صورت سلاح یا مواد منفجره، ارتباطات، اسناد سفر و پناهگاه‌های امـن بـرای آمـوزش و عملیات در اختیارشان قرار می‌گیرد، بهره بجویند. ردیابی اقدامات آن‌ها اغلب دشوار اسـت، بـه

نحوی که دولت‌های دخیل در آن اقدامات می‌توانند احترام و مشروعیت خود را در جامعهٔ بین‌المللی حفظ کنند و در عین‌حال مخفیانه برای دستیابی به اهداف خود، تأمین منابع مالی مورد نیاز برای فعالیت‌های تروریستی را بر عهده بگیرند و این تروریست‌ها را مورد پشتیبانی مالی قرار دهند (White, 1991: 22-43).

در تعریفی دیگر، تروریسم دولتی اصطلاحاً برای توصیف دخالت دولت در امور داخلی یا خارجی دولتی دیگر به کار می‌رود که از طریق اجرای عملیات تروریستی یا مشارکت در آن، حمایت از عملیات نظامی برای زوال، تضعیف یا براندازی دولتی خاص یا کل دستگاه حاکمه یک کشور انجام می‌شود (Selden & Y.So, 2003: 4).

از جمله دیگر مصداق‌های تروریسم دولتی علاوه بر آنچه در بالا ذکر شد می‌توان به کمک‌های مادی و معنوی به گروه‌های مخالف و مشارکت در عملیاتی همچون بمب‌گذاری، مین‌گذاری بنادر و سواحل، آدم‌ربایی، هواپیما دزدی و ترور مقامات عالی مملکتی اشاره کرد (Aust, 2010: 265).

مهم‌ترین تفاوت میان تروریسم دولتی و غیردولتی در کارگزار انجام دهندهٔ آن است. در حالی که اقدامات تروریستی غیردولتی توسط افراد و گروه‌های مستقل بدون طرح ادعای وابستگی به احزاب سیاسی و دولت‌ها صورت می‌گیرد، اعمال تروریستی دولتی توسط یک یا چند دولت انجام می‌شود. این دولت‌ها یا خود به طور مستقیم اقدامات تروریستی مورد نظرشان را انجام می‌دهند، یا به طور غیرمستقیم و از طریق ارسال اسلحه و مهمات، امکانات پیشرفتهٔ نظامی و همچنین حمایت معنوی (سیاسی، تبلیغاتی و ...) از گروه‌های مخالف مقاصد خود را به پیش می‌برند یا در پایین‌ترین سطح پشتیبانی و حمایت صرفاً با وقوع اقدامات تروریستی موافقت کرده و به چنین کارهایی رضایت می‌دهند (Stohl & Lopez, 1988: 207-8).

کشورهای مختلف جهان با بهره‌گیری از این تعاریف و بر اساس منافع خود تلاش می‌کنند احزاب، گروه‌ها و دولت‌های مخالف با خود را در زمرهٔ تروریست‌ها قرار داده و در مقابل هر حزب، گروه و دولتی را که بر اساس منافع آن‌ها عمل کنند، از دایرهٔ شمول تروریسم خارج کنند. بر همین اساس است که دولت آمریکا نام کشورهایی همچون ایران را در فهرست کشورهای حامی تروریسم قرار داده و چنین استدلال می‌کند که جمهوری اسلامی با ارسال کمک‌های مادی و معنوی برای گروه‌هایی همچون حزب‌الله لبنان و حماس به طور غیرمستقیم در تروریسم دولتی سهیم است. اما نکته قابل تأملی که تناقض در سیاست‌ها و عملکرد کاخ سفید را آشکار می‌کند، آن است که کمک‌های رسمی آمریکا به گروه‌های مخالف ایران، از جمله گروهک منافقین و تصویب مکرر بودجه‌های خاص برای ایجاد نافرمانی و براندازی نظام سیاسی جمهوری اسلامی که به عنوان یک کشور مستقل در سازمان ملل متحد عضویت دارد، هرگز در زمره رفتارهای تروریستی محسوب نمی‌شود و ایالات متحده در قبال چنین اقداماتی پاسخگو نیست. این اقدامات دولت آمریکا که‌در دیگر کشورهای جهان هم روی داده، موجب

شده تا برخی اندیشمندان و فعالان سیاسی آمریکایی مانند نوام چامسکی ایالات متحده را بزرگ‌ترین حامی‌تروریسم دولتی بدانند (Barsamian, 2001).

تعریف تروریسم مجازی و تروریسم مجازی دولتی

تروریسم مجازی که با پیشرفت فناوری اطلاعات و ارتباطات شکل گرفت، متشکل از دو واژهٔ تروریسم و فضای مجازی است و تعاریف مختلفی که‌از آن ارائه شده نیز برگرفته از تعاریف واژه تروریسم است.

کالین باری اولین فردی بود که در دههٔ ۱۹۸۰ میلادی اصطلاح تروریسم مجازی را به کار برد و تعریفی برای آن ارائه کرد. بر اساس تعریف وی تروریسم مجازی به حمله یا حملاتی اطلاق می‌شود که با برنامه‌ریزی قبلی و با اغراض سیاسی، توسط گروه‌های ضددولتی خارجی یا مأموران مخفی خارجی، یا اشخاص حقیقی، علیه سامانه‌های اطلاعاتی و ارتباطی، سامانه‌های رایانه‌ای، برنامه‌های رایانه‌ای و داده‌ها انجام می‌شود که نتیجه عملی آن، وقوع اقدامات خشونت‌آمیز و هدف نهایی و از پیش تعیین شده آن، ایجاد ترس و ناامنی در میان مردم عادی است. بر اساس این تعریف، ابزار اجرای حملات تروریستی مجازی به جای سلاح‌های گرم، مواد منفجره و ارسال کمک‌های مادی و معنوی، رایانه‌ها و سخت‌افزارها و نرم‌افزارهای رایانه‌ای خواهند بود. (Barry, 1997: 15-18).

تعریف مشهور دیگری که توسط دوروتی دنینگ ارائه شده، به خوبی گویای ویژگی‌های تروریسم مجازی است:

> تروریسم مجازی عبارت است از تلاقی تروریسم و فضای مجازی:
> تروریسم مجازی عموماً به معنای حملات غیرقانونی بر ضد رایانه‌ها و شبکه‌های رایانه‌ای و اطلاعات ذخیره شده در آن‌هاست که هدف از آن ارعاب یا اجبار یک دولت یا اتباع آن به منظور پیشبرد اهداف سیاسی یا اجتماعی است. این حملات باید منجر به اعمال خشونت بر ضد اشخاص یا دارایی‌ها شود یا دست کم موجب وارد آمدن آن اندازه آسیب به آن‌ها شود که ایجاد ترس کند... حملات شدید به زیرساخت‌های مهم، بسته به آثاری که بر جا می‌گذارد، می‌تواند اقدامی سایبر تروریستی باشد؛ ولی نه حملاتی که ارائه خدمات غیر اساسی را مختل می‌سازد یا عمدتاً چیزی جز ایجاد سروصدای پر هزینه نباشد (Denning, 2001).

برخی صاحب‌نظران برای آنکه تعریفی جامع از تروریسم مجازی ارائه کرده باشند، آن را هرگونه حمله‌ای دانسته‌اند که در آن از سیستم‌های اطلاعاتی یا فناوری دیجیتالی (رایانه‌ها یا شبکه‌های رایانه‌ای) چه به عنوان ابزار حمله و چه به عنوان آماج حمله استفاده شود. به اعتقاد آنان اگر چه ممکن است تروریسم مجازی در سطح ملی، بین‌المللی، دولتی یا سیاسی صورت بگیرد، اما در هر حال هستهٔ مرکزی آن که آمیختگی عمل تروریستی با رایانه‌هاست، یکی است (فلیمینگ و استول، ۱۳۸۲: ۱۵٤).

در نهایت به نظر نگارنده، ترکیب تعاریف سه واژهٔ تروریسم، تروریسم دولتی و تروریسم مجازی، ما را به سوی تعریف کلید واژه تروریسم مجازی دولتی یا State-sponsored cyber terrorism رهنمون می‌سازد: «فعالیت‌های تروریستی که با حمایت مستقیم یا غیرمستقیم دولت‌ها و با استفاده از امکانات شبکه‌های رایانه‌ای و فناوری‌های نوین اطلاع‌رسانی بر ضد این شبکه‌ها یا زیرساخت‌های کلان اجرا شده و موجب ترس و ناامنی عمومی و اختلال و خسارات عمده می‌شود، تروریسم مجازی دولتی نامیده می‌شود.»

بر اساس تعاریفی که ارائه شد، می‌توان نتیجه گرفت تروریست‌های مجازی ضمن استفاده از رایانه‌ها و شبکه‌های رایانه‌ای برای ایجاد خرابکاری در خود این شبکه‌ها از آن‌ها برای حمله به دیگر تأسیسات و زیرساخت‌های حیاتی شامل تأسیسات آب و برق، انرژی، حمل و نقل، نهادهای تجاری و شرکت‌های فراملی، سازمان‌های بین‌المللی دولتی و غیردولتی، افراد و گروه‌های سیاسی دشمن، نیروهای امنیتی و دولت‌های ملی هم استفاده می‌کنند. برای مثال، با توجه به اینکه امروزه مدیریت و نظارت بر ارائه بسیاری از خدمات عمومی شامل حمل ونقل، انرژی، آب و برق و... از طریق اینترنت و شبکه‌های داده (Data Network) صورت می‌گیرد و تعداد کشورهایی که ساختارهای اقتصادی، اجتماعی و خدمات عمومی خود را بر بستر شبکه‌های رایانه‌ای و اینترنت استوار کرده‌اند روز به روز در حال افزایش است، تروریسم مجازی این هدف را هم شامل می‌شود.

بنابراین دست اندرکاران تروریسم مجازی برای پیشبرد اهداف خود می‌توانند با مختل کردن شبکه‌های رایانه‌ای و نرم افزارهای مورد استفاده برای مدیریت و کنترل شبکهٔ توزیع برق، باعث خاموشی‌های مکرر در نقاط مختلف یک شهر یا استان شوند. همچنین آن‌ها می‌توانند سامانه‌های مخابراتی را دچار مشکل کرده و کاری کنند که شهروندان در صورت وقوع حوادث غیرمترقبه مانند سیل، آتش‌سوزی، تصادف، طوفان و ... نتوانند با نهادهای مسئول مانند صلیب سرخ یا هلال احمر، آتش نشانی، پلیس، بیمارستان‌ها و پزشکی قانونی تماس بگیرند. همچنین با توجه به استفاده گسترده مردم در سراسر جهان از سامانه‌های حمل و نقل عمومی، فرودگاه‌ها، شبکه‌های ریلی درون و برون شهری و ...، ایجاد اختلال در سامانه‌های هدایت و ناوبری آن‌ها که عموماً از طریق رایانه‌ها و شبکه‌های رایانه‌ای مدیریت می‌شوند، از جمله دیگر اهداف مورد نظر تروریست‌های مجازی است. برای این کار فقط کافی است با نفوذ به این سامانه‌ها و دستکاری اطلاعات موجود در آن‌ها، اطلاعات مربوط به زمان حرکت و مسیر عبور قطارها، واگن‌های خطوط مترو یا هواپیماها را تغییر داد تا دو قطار یا دو هواپیما با هم برخورد کنند. همچنین می‌توان از طریق مختل کردن سامانه‌های انتقال و توزیع برق باعث قطع آن در زمان اوج استفاده مردم یا ایجاد نوسان در جریان الکتریسیته به منظور آسیب رساندن به تجهیزات گران قیمت مورد استفاده در این شبکه‌ها و همین‌طور وسایل برقی مورد استفاده مردم شد (Lewis, 2002).

در حالی که اختلال در رفت‌وآمد و دسترسی به‌خدمات روزمره و معطلی و سرگردانی شهروندان پیامدهای ساده تروریسم مجازی هستند، در صورت پیچیده‌تر شدن این حملات و گسترش دامنهٔ آن‌ها، بی‌اعتمادی به مسئولان محلی و ملی افزایش یافته و احساس ترس، ناامنی و بی‌پناهی به طور گسترده در مردم به‌وجود می‌آید. این وضعیت باعث کاهش مشروعیت و اقتدار سیاسی یک دولت و تزلزل آن خواهد شد و این امر هم به تضعیف حاکمیت ملی و جایگاه و موقعیت بین‌المللی یک کشور منجر می‌شود.

در حالی که هدف افراد یا گروه‌های تروریستی مجازی از این اقدامات، قدرت نمایی و سرقت اطلاعات حساس به منظور کسب سود شخصی و باجگیری‌های کلان است، دولت‌های حامی تروریسم مجازی به چالش کشیدن و زیرسؤال بردن اقتدار و حاکمیت دولت‌ها در سطوح ملی و بین‌المللی و همین‌طور سرقت اطلاعات محرمانه و مهم از شبکه‌های رایانه‌ای مورد استفاده در نهادهای حساس دولتی، شرکت‌های بزرگ خصوصی و حتی رایانه‌های شخصی مورد استفاده شهروندان عادی را مد نظر قرار می‌دهند تا پس از جمع‌آوری و تجزیه و تحلیل این داده‌ها از آن‌ها برای ارزیابی وضعیت و نقاط ضعف و قوت کشور مورد نظر در حوزه‌های سیاسی، اقتصادی، اجتماعی و نظامی بهره گرفته و بر اساس جمع‌بندی نهایی برنامه‌ریزی‌هایی را برای مقابله با آن کشور و تضعیف قدرت و جایگاه داخلی و بین‌المللی دولت حاکم بر آن به عمل آورند (Colarik, 2006 :14-28).

ویژگی‌های تروریسم مجازی و تروریسم مجازی دولتی

موارد زیر را، می‌توان در مجموع ویژگی‌های متمایزکننده تروریسم مجازی و تروریسم مجازی دولتی در مقایسه با تروریسم و تروریسم دولتی سنتی (از دیدگاه‌تروریست‌ها و حامیان آن‌ها) ذکر کرد:

۱. هدف قراردادن عدهٔ بیشتری از شهروندان

در حالی که با اجرای عملیات تروریستی به شیوهٔ سنّتی از طریق بمب‌گذاری، هواپیماربایی، گروگان‌گیری، قتل و ... عدهٔ محدودی دچار آسیب می‌شوند، با استفاده از شیوه‌های تروریستی مجازی می‌توان تمامی مردم یک شهر یا حتی یک یا چند کشور را دچار مشکل کرد و دامنه آسیب‌پذیری عمومی بسیار گسترده‌تر از قبل خواهد بود(Baldi ,Gelbstein & Kurbalija, 2003:18).

۲. عدم محدودیت جغرافیایی

با توجه به آنکه تروریست‌های سنّتی محدود به محل جغرافیایی استقرار خود هستند و ابزار مورد استفادهٔ آن‌ها نیز از قدرت تخریب از قبل مشخصی برخوردار است، آن‌ها قادر نخواهند بود به اندازه تروریست‌های مجازی خسارت و خرابی به بار آورند. تروریست‌های مجازی به جای استفاده از اسلحه و بمب و موشک با به کارگیری نرم افزارهای مخرب رایانه‌ای و حملات اینترنتی کل شبکه رایانه‌ای و رایانه‌های مورد استفاده برای مدیریت تأسیسات زیربنایی و همین‌طور رایانه‌های حاوی

اطلاعات حساس در شرکت‌های خصوصی، ادارات دولتی و منازل را آلوده می‌کنند و با توجه به ماهیت درهم تنیده شبکه‌های رایانه‌ای نرم‌افزارهای مخرب به سرعت از رایانه‌ای به رایانه دیگر منتقل شده و در یک پهنهٔ وسیع جغرافیایی که محدود به هیچ مرزی نیست، گسترش می‌یابند (Centre of Excellence Defence Against Terrorism, 2008: 36).

۳. سهولت پنهان کردن هویت

با توجه به آنکه تروریست‌های سنّتی برای انجام اقدامات خرابکارانه خود مجبور به حضور فیزیکی در اماکن مورد نظر و فعالیت‌های محسوس جسمانی هستند، شناسایی آن‌ها با دشواری کمتری صورت می‌پذیرد. اما تروریست‌های مجازی بدون نیاز به بمب و موشک و اسلحه معمولاً با استفاده از دانش و اطلاعات فنی خود و از طریق رایانه‌ها و با بهره‌گیری از فنون مهندسی دست به‌تخریب می‌زنند و برای همین می‌توانند به راحتی خود را یک کاربر عادی اینترنت معرفی کرده و بدون ایجاد حساسیت در میان شهروندان حملات خود را از طریق رایانه‌ها انجام دهند. همچنین باید توجه داشت که با پیشرفت فناوری اطلاعات و ارتباطات شیوه‌های مورد استفاده برای پنهان کردن هویت در فضای مجازی نیز افزایش چشمگیری یافته است. استفاده از سیستم‌های رایانه‌ای مختلف و همین‌طور نرم‌افزارهای واسط برای گمراه کردن پلیس و نیروهای امنیتی در کنار سرقت هویت دیگر کاربران اینترنت و شبکه‌های رایانه‌ای خصوصی ادارات و شرکت‌ها برای مقصر قلمداد کردن فرد یا افراد دیگر نمونه‌هایی از این روش‌هاست که شناسایی عامل یا عاملان اصلی اجرای حملات تروریستی مجازی را به شدت دشوار ساخته است (Centre of Excellence Defence Against Terrorism, 2008: 36).

۴. امکان همکاری بین‌المللی گسترده‌تر

تروریست‌های سنّتی به علت ضرورت همکاری با یکدیگر در فضای واقعی کم و بیش از یکدیگر شناخت دارند و حداقل عده‌ای از آن‌ها از ویژگی‌های شخصیتی، ظاهری و ... دیگر همکارانشان مطلع هستند. این شناخت نسبی موجب می‌شود تا در صورت دستگیری یک یا چند نفر از این تروریست‌ها بتوان از طریق آن‌ها، دیگر تروریست‌ها را شناسایی و برای دستگیری آن‌ها اقدام کرد. نگرانی از همین مسئله موجب می‌شود تروریست‌های سنّتی حتی در صورت تمایل به گسترش فعالیت و عضوگیری گسترده‌تر با مشکلات فراوانی مواجه بوده و نتوانند این کار را به سرعت و سهولت انجام دهند. اما تروریست‌های مجازی به علت نگرانی‌های کمتری که در این زمینه دارند به همکاری‌های گسترده بین‌المللی و عضوگیری از میان بهترین خبرگان و متخصصان علاقه دارند. این افراد بدون آنکه نیازمند به کسب اطلاع از هویت یکدیگر و حتی تماس و مکالمه حضوری باشند، به سادگی می‌توانند از طریق اینترنت و ابزاری مانند پست الکترونیکی، نرم‌افزارهای چت و گفت‌وگو، خدمات تلفن اینترنتی و ... به طور مستعار و ناشناس با یکدیگر در تماس بوده و برای انجام اقدامات خرابکارانه برنامه‌ریزی کنند. بنابراین دستگیری یک یا چند نفر از تروریست‌های مجازی هم کمک زیادی به شناسایی

هویت دیگر همدستان آنان نخواهد کرد و نیروهای امنیتی باید با صرف وقت و هزینه فراوان تلاش کنند از طریق مجاری ارتباطی الکترونیک این افراد به‌سرنخی برای دستگیریشان برسند (Council of Europe, 2007:15-16).

۵. گسترش دامنهٔ اقدامات تروریستی به زیرساخت‌ها و مؤسسات بانکی، مالی، اقتصادی و خدماتی

تروریست‌های سنّتی عمدتاً اهداف سیاسی یا اهدافی را هدف قرار می‌دهند که حمله به آن‌ها پیامدهای قابل توجه سیاسی به همراه داشته باشد. آن‌ها همچنین سعی می‌کنند نخبگان و نهادهای سیاسی را هدف حملات خود قرار داده یا با بمب‌گذاری، گروگان‌گیری و روش‌های مشابه این نخبگان را وادار به پذیرش خواسته‌های خود کنند. اما با توجه به توانمندی و امکانات وسیعی که در دسترس تروریست‌های مجازی قرار دارد، آن‌ها دامنهٔ فعالیت‌های خود را به اهداف سیاسی محدود نکرده و زیرساخت‌های عمومی مانند حمل و نقل، انرژی، شبکه‌های مالی و بانکی، سرویس‌های ارائه خدمات شهری وابسته به شهرداری‌ها، دولت‌ها و ... را هدف قرار می‌دهند. با توجه به تبعات گستردهٔ اختلال در این خدمات و شبکه‌ها که نارضایتی گسترده عمومی را به دنبال می‌آورد، تروریست‌های مجازی از اهرم‌های فشار قدرتمندی برای وادار کردن حاکمان سیاسی به پیروی از خواسته‌های‌شان برخوردار خواهند بود (Centre of Excellence Defence against Terrorism, 2008: 37).

۶. هزینه‌های کمتر

تروریست‌های سنّتی برای انجام فعالیت‌های تخریبی و خرابکاری در مقیاس جغرافیایی محدود نیازمند صرف هزینه‌های کلان برای خرید تسلیحات و انتقال آن‌ها، برنامه‌ریزی مخفیانه برای جابه‌جایی اسلحه و بمب، اختصاص بودجه برای آموزش نیروها و هماهنگ کردن آن‌ها و همین طور یافتن راه‌هایی برای اسکان و تخلیه سریع محل اجرای عملیات تروریستی هستند، اما تروریست‌های مجازی نیازمند صرف هیچ یک از این هزینه‌ها نیستند و فقط با استفاده از یک رایانه متصل به اینترنت می‌توانند خسارات گسترده‌ای به‌بار آورده و حمل‌ونقل عمومی، شبکه‌های انتقال آب و برق، خدمات الکترونیک، مالی و بانکی و ... را مختل کرده و اطلاعات حساس شرکت‌های خصوصی و سازمان‌های دولتی را به‌سرقت ببرند (Centre of Excellence Defence against Terrorism, 2008: 36).

روش‌های اجرای حملات تروریستی مجازی دولتی

امروزه برخی دولت‌ها با حمایت مستقیم و غیرمستقیم از تروریست‌های مجازی بر علیه دولت‌ها، احزاب و گروه‌های رقیب یا متخاصم که به هر علت امکان مقابله فیزیکی و نظامی با آن‌ها را ندارند، وارد عمل شده و تلاش می‌کنند اهداف از قبل تعریف شده خود را عملی کنند.

دولت‌ها برای اعمال تروریسم دولتی، به خشونت، ترور و سرکوب فیزیکی مردم، گروه‌ها و حاکمان دولت‌های دیگر متوسل می‌شوند و برای این کار از شیوه‌های مستقیم (استفاده از نیروهای رسمی حکومت مانند پلیس و ارتش) یا غیرمستقیم (بهره گرفتن از گروه‌های تروریستی و

شبه‌نظامی مورد حمایت خود) بهره می‌گیرند. اما شیوه‌های اعمال مستقیم یـا غیرمـستقیم تروریـسم مجازی دولتی متفاوت بوده و در قالب دسته‌بندی زیر بیانَ می‌شود:

۱. سرقت فیزیکی تجهیزات فنی

اگر چه در بسیاری از موارد تروریست‌های مجازی دولتی برای تحقق اهدافشان از دانش رایانـه‌ای خود و روش‌های مبتنی بر فناوری اطلاعات و ارتباطات استفاده می‌کنند، اما در مواردی نیـز بـرای دستیابی به اطلاعات مورد نظر یا ایجاد اختلال در شبکه‌های رایانـه‌ای بـه سـرقت فیزیکـی هـارد دیسک‌ها، حافظه‌های قابل حمل، رایانه‌های لپ‌تـاپ یـا دیگـر قطعـات حـساس سـخت‌افـزاری می‌پردازند. معمولاً این‌گونه اقدامات در شرایطی انجام می‌شوند که دولـت‌هـای حـامی تروریـسم مجازی برای دسترسی به اطلاعات مورد نظر یا انجام اقدامات خرابکارانه عجله زیادی دارند یا بـه علت پیچیدگی و امنیت بالای سیستم هدف توان نفوذ به آن را ندارند.

برآوردهای یک شرکت خصوصی ارائه‌دهندهٔ خدمات امنیتی در حوزهٔ فناوری اطلاعـات بـه نام مک‌آفی نشان می‌دهد که اگر هکرهـا و جانیـان آنلایـن بتواننـد اطلاعـات ذخیـره شـده در نوت‌بوک یا رایانه شخصی یک کارمند میان پایه در شرکتی مهم را سرقت کننـد، مـی‌تواننـد آن اطلاعات را به قیمت حداکثر ۶۰ هزار دلار به فروش برسانند. معمـولاً ایـن دسـتگاه‌هـا حـاوی اطلاعات ذی‌قیمتی در مورد قراردادهای تجاری و همین‌طور برنامه‌های آتی شرکت‌های مختلف هستند (خبرگزاری فارس، ۳۰ فروردین ۱۳۹۰).

به عنوان مثال می‌توان به سرقت یک لپ‌تاپ حاوی الگوریتم‌های مورد اسـتفاده در سیـستم فرماندهی و کنترل ایستگاه‌فضایی ISS آمریکا وابسته به ناسا در مارس سال ۲۰۱۱ اشاره‌کرد. در زمان انتشار گزارش این حادثه در فوریه سال ۲۰۱۲، ناسا ایـن اقـدام را بـه عوامـل و مـأموران کشورهای خارجی نسبت داد، هرچند هرگز هیچ دولتی به طور رسمی به این اقدام مـتهم نـشد. (pcmag.com, 2012).

۲. سوءاستفاده از آسیب‌پذیری و حفره‌های امنیتی نرم افزاری و سخت افزاری

شبکه‌های رایانه‌ای عمومی و خصوصی مورد استفاده اشخاص، نهادهای خصوصی و مؤسسات دولتی در همه جهان با استفاده از نرم افزارها و سخت‌افزارهای متنوعی اداره می‌شـوند کـه هـر یک توسط مؤسسه خاصی طراحی و عرضه شده‌اند. عموم این محصولات دارای نقاط ضعف و آسیب‌پذیری‌های فنی هستند که تروریست‌های مجازی دولتی با سوءاستفاده از آن‌ها می‌تواننـد به درون رایانه‌های شخصی متصل به اینترنت و دیگر شبکه‌ها نفوذ کرده و دست به خرابکـاری و سرقت اطلاعات بزنند. این افراد برای تسهیل اقدامات خرابکارانه خود معمولاً از برنامـه‌هـای مخربی به نام بدافزار استفاده می‌کنند.

بدافزار یا malware به ویروس (Virus)، کرم (Worm)، تروجان (Trojan) یا هر برنامه رایانه‌ای دیگری اطلاق می‌شود که با هدف انجام اعمال خرابکارانه طراحی شـده باشـد و بـدین منظـور بـه رایانه‌های شخصی و دیگر سیستم‌های الکترونیک نفوذ کند. تروجان برنامه‌ای ظاهراً بـی‌خطـر ولـی

شامل کدهای پنهانی است که برای سوءاستفاده یا صدمه‌زدن به رایانه‌ها طراحی می‌شود و معمولاً از طریق خدمات پست الکترونیک (email) برای کاربران ارسال می‌شود.

کرم برنامه‌ای نرم‌افزاری شامل کدهای مخرب است که به طور خودکار در شبکه‌های رایانه‌ای توزیع و منتشر می‌شود و به منظور حمله به وب‌گاه‌های اینترنتی و مصرف بیش از اندازهٔ پهنای باند (Bandwidth) شبکه‌های رایانه‌ای مورد استفاده قرار می‌گیرد. کرم‌ها برحسب برنامه‌ریزی انجام شده بدون مداخله یا پس از اجرا توسط کاربر، اقدامات خرابکارانه خود را انجام می‌دهند.

اما ویروس برنامه‌ای نرم‌افزاری است که کدهای آن با هدف تکثیر خودکار نوشته شده و تلاش می‌کند به سرعت از رایانه‌ای به رایانه‌های دیگر منتقل شود. ویروس‌ها معمولاً از طریق برنامه‌های دیگری میزبانی می‌شوند و پس از اجرای آن برنامه فعال شده و به نرم‌افزار، سخت‌افزار یا داده‌ها خسارت می‌زنند یا آن‌ها را آلوده می‌کنند (Carnaghi, 2004).

استفاده از یکی از انواع این بدافزارها از جمله ابزار مورد استفاده تروریست‌های مجازی دولتی است. برای نمونه می‌توان به حملهٔ کرم مخرب استاکس نت (Stuxnet) به تأسیسات غنی‌سازی اورانیوم در سایت هسته‌ای نطنز اشاره کرد. این کرم با سوءاستفاده از نقص امنیتی در سیستم عامل ویندوز مایکروسافت با آلوده‌کردن رایانه‌های کاربران صنعتی، فایل‌های خاصی را که مربوط به سیستم‌های کنترل و مدیریت اسکادا ساخت شرکت زیمنس بودند، به یک رایانه سرور خاص ارسال می‌کرد. به گفته یوراه مالکو رئیس لابراتوار شرکت امنیتی ESET در براتیسلاوای اسلواکی، این ویروس به محض ورود به فضای سیستم عامل ویندوز بررسی می‌کند که رایانه مورد نظر در قلمرو ایالات‌متحده قرار گرفته است یا خیر. در صورت منفی بودن این پرسش ویروس به صورت خودکار نرخ تکثیرش را کاهش می‌دهد که نشان می‌دهد طراحان ویروس علاقه‌مند نیستند این ویروس در سایر نقاط جهان نمود چندانی داشته باشد. شاید ما هم اکنون شاهد نسل جدیدی از تروریسم رایانه‌ای باشیم (*عصر ایران*، ١٦ مرداد ١٣٨٩ و Chien, 2010).

با گذشت زمان و بررسی دقیق‌تر استاکس نت توسط کارشناسان و متخصصان داخلی و خارجی، اطلاعات دقیق‌تری در مورد عوامل پشت پرده طراحی این کرم به دست آمد و روزنامه *نیویورک تایمز* با انتشار گزارشی در تاریخ ١٦ ژانویه ٢٠١١ اعلام کرد:

> رژیم صهیونیستی کرم استاکس نت را در مرکز اتمی دیمونا بر روی سانتریفیوژهای مشابه با نمونه‌های مورد استفاده در تأسیسات غنی‌سازی اورانیوم نطنز با موفقیت آزمایش کرده بود ... و از سوی دیگر شرکت آلمانی زیمنس هم در سال ٢٠٠٨ با همکاری متخصصان آمریکایی آسیب‌پذیری‌های سیستم کنترل صنعتی اسکادا را به طور دقیق شناسایی کرده بود... خاستگاه سیاسی این طرح به ماه‌های آخر دورهٔ ریاست جمهوری بوش در ژانویه سال ٢٠٠٩ باز می‌گردد. در آن زمان بوش مجوز اجرای یک برنامه سری برای تخریب سیستم‌های برقی و رایانه‌ای مرکز غنی‌سازی نطنز را صادر کرد. اوباما هم قبل از بر عهده گرفتن پست ریاست جمهوری از خلاصه این طرح مطلع شد و اجرای آن را سرعت بخشید. رژیم صهیونیست‌ها هم همین کار را کردند... آن‌ها معتقد بودند با اجرای این طرح برنامه‌های هسته‌ای ایران سه سال به تأخیر می‌افتد.

مجموعه شواهد و اسناد ارائه شده در این گزارش خبری ـ تحلیلی که بـا اظهـار نظرهـای مقامـات آمریکایی و رژیم صهیونیستی تکمیل شده، تردیدی در طراحی استاکس نت توسط ایالات متحـده و رژیم اشغالگر قدس باقی نگذاشته است. برای نمونه‌گری سامور (Gary Samore)، استراتژیست ارشد اوباما رئیس‌جمهور آمریکا در امور مقابله با سلاح‌های کشتار جمعی در واکنش به سـؤالی به اثرات استاکس نت بر توان هسته‌ای ایران بـا لبخنـد پاسـخ داده: «مـن خوشـحال هـستم کـه می‌شنوم آن‌ها برای استفاده از دستگاه‌های سانتریفیوژ دچار مشکل شده‌اند. آمریکا و متحـدانش هر کاری که از دستشان بر بیاید انجام می‌دهند تـا شـرایط را پیچیـده‌تـر و دشـوارتر کننـد.» در نهایت نویسندهٔ گزارش چنین نتیجه‌گیری کرده که طراحی و انتشار این کرم طرحی مـشترک از سوی آمریکا و رژیم صهیونیستی بوده و آلمان و بریتانیا هم به طور آگاهانه یا ناآگانه به اجـرای آن کمک کرده‌اند (New York Times, 15 January, 2011)

پیش‌بینی این گزارش در مورد ایجاد تأخیر سه ساله در پیشبرد برنامـهٔ هـسته‌ای ایـران محقـق نشد، زیرا رضا تقی‌پور وزیر ارتباطات و فناوری اطلاعات، در مصاحبه بـا خبرگـزاری مهـر در تاریخ ۱۰ آبان ماه ۱۳۸۹ از شناسایی و پاکسازی سیستم‌های آلوده به استاکس‌نت در کشور خبر داد و گفت: اکثر سازمان‌های اجرایی موفق شده‌اند با نرم‌افزارهایی که در اختیار دارند، پاکسازی سیستم‌های آلوده را به طور کامل انجام دهند و هم اکنون خطری از این بابت رایانه‌های ایرانـی را تهدید نمی‌کند. تقی‌پور بی‌احتیاطی و عدم اسکن حافظه‌های جانبی قبل از اتصال به رایانه‌هـا را عامل انتقال این کرم جاسوسی به سیـستم‌هـای صـنعتی ایـران دانـست و تـصریح کـرد ایـن حافظه‌های آلوده از خارج وارد کشور شده‌اند و منشأآلودگی از طریق شبکه‌های رایانه‌ای نبـوده است (خبرگزاری مهر، ۱۰ آبان ۱۳۸۹).

۳. فریب کاربران با استفاده از روش‌های مهندسی اجتماعی

از جمله دیگر روش‌هایی که تروریست‌های مجازی دولتی از آن بهره می‌گیرند، فریب‌دادن کـاربران به روش‌های مختلف و سوءاستفاده از غفلت و ناآگاهی آنان است. یکـی از متـداول‌تـرین روش‌هـا برای انجام این کار تکنیکی موسوم به فیشینگ است. در این روش، تروریست‌ها کپی کاملاً دقیقی از یک وب‌گاه یا خدمات تحت وب که به طور دائمی مورد استفاده کارمندان یک شرکت خصوصی یا مؤسسه دولتی قرار می‌گیرد را طراحی کرده و به شیوه‌های مختلف مانند ارسال پـست الکترونیکـی آنان را به بازدید از این وب‌گاه و درج اطلاعات شخصی خود در آن ترغیب می‌کنند. برای مثال بـه کاربر هشدار داده می‌شود که سرویس یا وب‌گاه مورد استفاده او در حال به روزرسانی اسـت و وی باید برای تداوم دسترسی به خدمات مورد نیازش، مجدداً اطلاعات شخصی خود را در وب‌گاهی که مشخص شده وارد کند. در این حالت تروریست‌های مجازی دولتی اطلاعات شخـصی کـاربر و از جمله کلمهٔ عبور او را به دست آورده و از این طریق دست به سرقت اطلاعـات و انجـام اقـدامات خرابکارانه می‌زنند (Jøsang, 2007: 4).

نمونهٔ عملی استفاده از این روش به آگوست سال ۲۰۱۱ برمی‌گردد. شرکت امنیتی مک‌آفی در تاریخ ۳ آگوست سال ۲۰۱۱ (مرداد ماه ۱۳۹۰) گزارشی منتشر کرد که بر اساس آن اطلاعات محرمانه۷۲ دولت، شرکت و سازمان مهم بین‌المللی بر روی اینترنت و وب‌گاه‌های رسمی آن‌ها از جمله سازمان ملل، اتحادیه کشورهای جنوب شرق آسیا (آسه‌آن)، کمیته بین‌المللی المپیک، آژانس بین‌المللی ضد دوپینگ، دوازده شرکت مقاطعه‌کار پنتاگون، یک مقاطعه‌کار وزارت دفاع بریتانیا، ده‌ها شرکت ساختمانی و فعال در حوزهٔ انرژی، فولاد، انرژی خورشیدی، فناوری، ارتباطات ماهواره‌ای، حسابداری و رسانه‌ای، چند اتحادیه فعال در زمینهٔ بیمه، شبکه‌های رایانه‌ای دولت‌های فدرال و محلی آمریکا وب‌گاه‌های وابسته به مغزهای متفکر آمریکا و اساتید دانشگاهی و برجسته‌این کشور، از سال ۲۰۰۶ تا زمان انتشار این گزارش به طور پیوسته سرقت شده‌اند. از میان این ۷۲ سازمان، ۴۹ مورد آمریکایی بوده یا مقر اصلی آن‌ها در آمریکا واقع بود. دولت‌های کانادا، هند، کره‌جنوبی، تایوان، آمریکا و ویتنام هم از جمله قربانیان حملات یاد شده اعلام شدند. در این گزارش احتمال استفاده تجاری از این اطلاعات رد شده و تصریح شده بود که روش مورد استفاده برای سرقت اطلاعات، فیشینگ بوده است. (Alperovitch, 2011).

به دنبال انتشار این خبر رسانه‌های غربی دولت چین را مظنون اصلی اجرای آن دانستند. ولی برخی منابع مستقل احتمال دخالت دولت‌های دیگر و به‌خصوص برخی کشورهای غربی را در این حملات را مطرح کردند. جیم لویس کارشناس برجستهٔ حوزهٔ امنیت سایبر در مرکز مطالعات استراتژیک و بین‌المللی در این مورد اظهار داشت:

> در حالی که چین متهم اصلی است، باید بدانیم که آمریکا و بریتانیا و روسیه هم به طور بالقوه توان انجام چنین حملاتی را دارند و به‌هر حال این کشورها هم برای جاسوسی از هم بسیار تلاش می‌کنند. نکتهٔ جالب این است که این حملات بی سروصدا در ۵ سال اخیر در جریان بوده ولی هکرها تا بدان حد مهارت و تخصص داشته‌اند که جلوی افشای این حملات و همین‌طور شناسایی دقیق خود را گرفته‌اند (خبرگزاری فارس، ۱۴ مرداد ۱۳۹۰).

علی‌رغم همهٔ فشارهای رسانه‌ای، دولت چین واکنشی نسبت به ادعاهای طرح شده نشان نداد، اما حدود یک ماه بعد در شهریور ماه ۱۳۹۰ که مطبوعات ژاپن، دولت چین را به حمله به رایانه‌های شرکت میتسوبیشی متهم کردند و مدعی شدند دولت پکن به دنبال سرقت اطلاعات مربوط به صنایع نظامی و دفاعی حساس ژاپن در زمینهٔ ساخت انواع زیردریایی و کشتی و موشک بوده، هانگ لی، سخنگوی وزارت امور خارجه چین این ادعا را رد کرد و گفت: «دولت چین با اقدامات هکری و هرگونه فعالیت‌های این‌چنینی مخالف است و معتقد است این ادعاهای بی‌اساس به توسعه همکاری‌های بین‌المللی در زمینهٔ تأمین امنیت سایبر آسیب وارد می‌کند.» (خبرگزاری رویترز، ۲۰ سپتامبر ۲۰۱۱)

تفاوت تروریست‌های مجازی دولتی و دیگر مجرمان اینترنتی

شاید تصور شود روش‌هایی که در بالا ذکر شد، توسط تروریست‌های مجازی و دیگر افرادی که در فضای مجازی دست به اقدامات تبهکارانه و خلافکاری می‌زنند هم، مورد استفاده قرار می‌گیرد و لذا اطلاق آن‌ها به تروریست‌های مجازی مورد حمایت دولت‌ها صحیح نیست. اما تروریست‌های مجازی دولتی از دو تفاوت عمده با دیگر مجرمان اینترنتی برخوردارند.

۱. این تروریست‌ها که انگیزه‌های سیاسی دارند و به طور مستقیم یا غیرمستقیم از دولتی دستور می‌گیرند، با هدف خرابکاری و سرقت اطلاعات به سامانه‌ها و شبکه‌های رایانه‌ای مختلف آسیب می‌زنند و لذا همهٔ مردم قربانیان آن‌ها محسوب می‌شوند. اما دیگر مجرمان اینترنتی که اصطلاحاً هکر (Hacker) نامیده می‌شوند، اهداف اقتصادی دارند، برای کسب سود مالی یا قدرت نمایی به سامانه‌ها و شبکه‌های از پیش تعیین شده حمله می‌کنند و فقط به قربانیان مورد نظرشان آسیب می‌زنند. بنابراین دامنه آسیب‌هایی که از طریق هکرها وارد می‌شود، محدودتر است.

۲. مجرمان فضای مجازی به علت رقابت شدیدی که با هم دارند، معمولاً دانش بالای خود را در اختیار دیگر هکرها یا گروه‌های هکری رقیب قرار نمی‌دهند و سعی می‌کنند قدرت فنی و علمی‌خود را حفظ کنند، اما تروریست‌های مجازی دولتی با توجه به انگیزه‌های سیاسی و ایدئولوژیکی که دارند تلاش می‌کنند تجربه‌ها و اطلاعات خود را در اختیار دیگران بگذارند و با سهیم کردن همفکرانشان در دانش خود، رسالتی را که تصور می‌کنند بر عهده دارند به سرانجام برسانند (Colarik, 2006: 52-3).

راهکارهای مقابله

با توجه به افزایش حملات تروریستی مجازی که مورد پشتیبانی دولت‌ها هستند و با عنایت به اتکای روزافزون مردم، دولت‌ها و شرکت‌های خصوصی به اینترنت و فناوری‌های پیشرفته ارتباطی برای پیشبرد امور مختلف شخصی و حرفه‌ای، باید راهکارهایی برای مقابله با این خطر نوظهور در نظر گرفته شود. این راهکارها را می‌توان به سه بخش کلی تقسیم کرد:

۱.آموزش‌های عمومی و تخصصی

ناآگاهی کاربران از شیوه‌های مورد استفاده تروریست‌های مجازی و تروریست‌های مجازی دولتی برای فریب و نفوذ به حساب‌های کاربری افراد، سرقت اطلاعات و وارد آوردن خسارت، باعث می‌شود این افراد راحت‌تر بتوانند اهداف خود را محقق کنند. به همین منظور باید هم مردم عادی و هم مقامات سیاسی و امنیتی و مدیران شرکت‌های بزرگ، آموزش‌های متناسب با شرایط خود را دریافت کنند. از یک‌سو باید شیوه‌های سوءاستفاده تروریست‌های مجازی آموزش داده شود و از سوی دیگر روش‌های ایمن‌سازی رایانه‌ها و شبکه‌های رایانه‌ای بر اساس نیاز هر کاربر به وی تعلیم داده شود (Khosrow-pour, 2004: 390).

۲. تدوین قوانین و استراتژی‌های مناسب و جامع

ارائه آموزش‌های عمومی و تخصصی در مورد تروریسم مجازی منجر به آن خواهد شد که شهروندان، فعالان عمده اقتصادی و مسئولان عالی‌رتبه سیاسی به ضرورت وضع قانون و تدوین استراتژی‌های امنیتی به منظور ارتقای امنیت کشور در فضای مجازی پی ببرند. در این مرحله باید سازوکارهای قضایی و حقوقی مناسبی برای مقابله با تروریسم مجازی به وجود آید و قوانین قدیمی متناسب با شرایط جدید به‌روز شوند تا از سوءاستفاده مجرمان از خلأهای قانونی و حقوقی جلوگیری شود و برخورد سریع و متناسب با تخلفات آن‌ها ممکن شود (Baldi et al, 2003: 73).

۳. ارتقای بنیه دفاعی

پس از ارائهٔ آموزش‌های لازم و وضع قوانین جدید، زمینه برای ایجاد سازمان‌های جدیدی که وظیفه مقابله با تروریسم مجازی دولتی را بر عهده بگیرند، به وجود خواهد آمد. این سازمان‌ها وظایفی همچون انجام فعالیت‌های علمی و تحقیقاتی و مقابلهٔ همه‌جانبه با حملات تروریست‌های مجازی را برعهده خواهند گرفت. از جمله دیگر روش‌های دفاعی، استفاده از فناوری‌های پیشرفته امنیتی برای سدکردن مسیر تهاجم تروریست‌های مجازی دولتی است. این فناوری‌ها عبارت‌اند از نرم‌افزارهای ضدویروس و فایروال‌ها و همین‌طور استفاده‌از راهکارهایی همچون تعیین سطوح دسترسی متفاوت برای افراد، بسته به نیاز آن‌ها در شبکه‌های رایانه‌ای عمومی و خصوصی در کنار به‌روزرسانی مرتب نرم‌افزارهای دائماً مورد استفاده مانند سیستم عامل ویندوز، نرم‌افزار اداری آفیس، مرورگرهای اینترنتی و ...(Ching, 2010: 43).

در این زمینه باید نکته‌ای را مد نظر قرار داد. نرم‌افزارهای خارجی اعم از نرم‌افزارهای تحت وب، اداری و حرفه‌ای مانند آفیس، مرورگرهای اینترنتی و حتی سیستم عامل ویندوز و همچنین نرم‌افزارهای امنیتی و ضدویروس که ساخت شرکت‌های مختلف اروپایی و آمریکایی هستند، اطلاعات مربوط به شیوه و تاریخچهٔ استفاده، مشخصات فنی رایانه‌ها و شبکه‌های رایانه‌ای مختلف را در صورت اتصال کاربر به اینترنت برای شرکت‌های سازنده خود ارسال می‌کنند تا از این اطلاعات برای شناسایی ویژگی‌ها و عادات کاربری خریداران و کاربران محصولات مختلف و برنامه‌ریزی برای بهینه‌سازی تولیدات بر اساس نیازها و شیوهٔ استفاده افراد استفاده شود. البته این اطلاعات ممکن است در اختیار دولت‌های متبوع این شرکت‌ها هم قرار بگیرد. برای مثال گوگل در سال ۲۰۰۹ اعلام کرد که از ٤٦٠١ درخواست دولت آمریکا برای افشای اطلاعات شخصی کاربران خدمات و نرم‌افزارهای مختلف خود با ۹٤درصد از آن‌ها موافقت کرده است. این شرکت در مهر ماه سال ۱۳۹۰ هم تمامی اطلاعات یکی از کاربران خود به‌نام Jacob Appelbaum را به درخواست دولت آمریکا در اختیار کاخ سفید قرار داد. این فرد یکی از همکاران داوطلب سایت ویکی‌لیکس(wikileaks.org)، افشاگر اسناد دولتی محرمانه آمریکا بود (خبرگزاری فارس، ۱۹ مهر ماه ۱۳۹۰).

با توجه به همکاری‌های امنیتی و اطلاعاتی گسترده دولت‌های غربی با شرکت‌های بزرگ فناوری همچون گوگل، استفاده از محصولات نرم‌افزاری و تولیدات رایانه‌ای غیربومی، راه‌حل مطمئنی برای تضمین امنیت کاربران و مقابله با تروریست‌های مجازی دولتی نیست. بنابراین ضروری است از ظرفیت‌های داخلی و توانمندی مهندسان و برنامه‌نویسان کشور به منظور طراحی برنامه‌های امنیتی و نرم‌افزارها و سیستم عامل‌های ایرانی که نیاز داخلی را برطرف کنند، استفاده شود.

مبارزه با تروریسم دولتی مجازی در ایران

پس از تصویب تشکیل شورای عالی امنیت فضای تبادل اطلاعات کشور (افتا) در سال ۱۳۸۲ توسط هیئت دولت وقت، اولین سند دولتی برای ایمن‌سازی فضای مجازی و تأمین امنیت فضای تبادل اطلاعات در سال ۱۳۸٤، توسط این شورا تدوین شد. پس از تصویب این سند با عنوان سند راهبردی امنیت فضای تبادل اطلاعات، ۲۰۰ میلیارد ریال اعتبار نیز توسط سازمان مدیریت و برنامه‌ریزی وقت به صورت متمرکز در اختیار شورای عالی افتا قرار گرفت تا طرح‌های امنیتی فناوری اطلاعات دستگاه‌های دولتی در اختیار آن‌ها قرار گیرد. همچنین به سازمان مدیریت و برنامه‌ریزی کشور اختیار داده شد تا در سال‌های بعد از پیش‌بینی اعتبار در بودجه طرح‌های فناوری اطلاعات سازمان‌ها و نهادهایی که فاقد بخش امنیت هستند، خودداری کند (رضایی، ۱۳۸۹ :۲۵).

قانون جرائم رایانه‌ای که‌کلیات آن در در ۲۷ آبان ۱۳۸۷ به تصویب مجلس شورای اسلامی رسید و در تاریخ ۷ تیر ۱۳۸۸ مورد تأیید شورای نگهبان قرار گرفت و سه روز بعد برای اجرا از سوی رئیس‌جمهور ابلاغ شد، مهم‌ترین قانونی است که در حال حاضر برای برخورد با انواع جرائم رایانه‌ای و از جمله اقدامات تروریستی مورد استناد قرار می‌گیرد (خبرآنلاین، ۲۲ تیر ماه ۱۳۸۸).

در این قانون که دارای ٥٦ ماده و ٢٦ تبصره است، به طور مستقیم از اصطلاح تروریسم مجازی یا تروریسم مجازی دولتی نامی به میان نیامده، اما قانون یاد شده از ظرفیت لازم برای مقابله با مرتکبین اقدامات تروریستی در فضای مجازی و مجازات آن‌ها برخوردار است، که در زیر به مواد مرتبط اشاره شده است.

۱. مبحث سوم از فصل اول قانون جرائم رایانه‌ای، طی مواد ۳ الی ۵، به جاسوسی رایانه‌ای اختصاص یافته و برای کسانی که به طور غیرمجاز به داده‌های سری، در حال انتقال یا ذخیره شده دسترسی پیدا کرده، یا آن‌ها را منتشر کنند، یا در اختیار دیگران قرار دهند، مجازات در نظر گرفته است.

۲. مبحث دوم از فصل دوم در مواد ۸ الی ۱۱، به "تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی" پرداخته است. به ویژه ماده۱۱، برای کسانی که با قصد به خطر انداختن امنیت و آسایش عمومی، علیه سامانه‌های رایانه‌ای و مخابراتی‌ای که برای ارائه خدمات عمومی‌مانند آب، برق، گاز، و خدمات بهداشتی و درمانی، حمل و نقل و بانکداری

به کار می‌روند مرتکب اقدام سوء شوند، سه تا ده سال حبس در نظر گرفته است. آنچه این ماده به آن اشاره کرده، دقیقاً با تعریف تروریسم مجازی همخوانی دارد.

۳. بند ب ماده ۲۵ "فروش یا انتشار یا در دسترس قرار دادن گذرواژه یا هر داده‌ای را که امکان دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی متعلق به دیگری را بدون رضایت او فراهم کند" جرم دانسته است. با توجه به اطلاق این ماده و نیز تصریح بند ج و د ماده ۲۶ همین قانون، چنانچه "داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی به دولت یا نهادها و مراکز ارائه‌دهندهٔ خدمات عمومی" متعلق باشند و یا "جرم به‌صورت سازمان یافته ارتکاب یافته باشد" مرتکب مشمول تشدید مجازات خواهد شد.

٤. بخش دوم قانون جرائم رایانه‌ای، که به آئین دادرسی اختصاص یافته، نیز امکان قانونی رسیدگی به جرائم مرتبط با تروریسم مجازی و صدور حکم مقتضی توسط مراجع ذیربط را فراهم کرده است. بند الف و ج ماده ۲۸، صلاحیت دادگاه‌های ایرانی را برای رسیدگی به جرائم اشخاص ایرانی یا غیرایرانی مرتکب جرایم موضوع این قانون، به رسمیت شناخته است (فیروزمنش، ۱۳۸۹: ۳۲).

پس از تصویب قانون جرائم رایانه‌ای در مجلس شورای اسلامی و لزوم تعیین ضابط قضایی برای این قانون، پلیس فضای تولید و تبادل اطلاعات (پلیس فتا) در سوم بهمن ماه سال ۱۳۸۹ به دستور فرمانده نیروی انتظامی جمهوری اسلامی ایران، سردار احمدی‌مقدم تشکیل شد (*همشهری*، سوم بهمن ۱۳۸۹). پلیس فتا در جهت ایجاد امنیت برای فعالیت‌های علمی، اقتصادی، اجتماعی در فضای مجازی، حفاظت از هویت دینی و ملی در این فضا و جلوگیری از تبدیل آن به بستر انجام فعالیت‌های غیرقانونی و ممانعت از تعرض به ارزش‌های جامعه در فضای مجازی فعالیت می‌کند (وب‌گاه پلیس فتا).

به دنبال افزایش تهدیدهای غرب بر ضد جمهوری اسلامی و همین‌طور تلاش این دولت‌ها برای استفاده از ظرفیت فضای مجازی و اینترنت به منظور اجرای برنامه‌ها و طرح‌های تروریستی و خرابکارانه بر ضد نظام، مراکز و نهادهای دیگری هم راه‌اندازی شدند که بر خلاف پلیس فتا به طور تخصصی و دقیق‌تر به مقابله با فعالیت‌های تروریستی مجازی که به طور مستقیم از سوی دولت‌های متخاصم اروپایی و آمریکایی برنامه‌ریزی شده بود، پرداختند. مرکز بررسی جرائم سازمان یافته، با هدف بررسی و پایش جرائم سازمان‌یافته در فضای مجازی اعم از فعالیت‌های تروریستی، جاسوسی، اقتصادی و اجتماعی، توسط سپاه پاسداران انقلاب اسلامی و با همکاری و هماهنگی سایر حوزه‌های اطلاعاتی و قضایی کشور، در سال ۱۳۸٦ تأسیس شد. این مرکز، با بهره‌گیری از توان علمی و اجرایی بیش از دو هزار متخصص فناوری اطلاعات و ارتباطات، به طور مرتب اینترنت را به منظور شناسایی تولیدکننده‌های محتواهای ضد اخلاقی و ضددینی رصد کرده، با همکاری مراجع ذی‌ربط، ضمن دستگیری مجرمین، وب‌گاه‌ها و وب‌نوشت‌های مستهجن را مسدود و آن‌ها بر روی وب‌گاهی با نام دامنه‌گرداب (www.gerdab.ir) منتقل می‌کند. در غرب، این اقدام سپاه علیه وب‌نوشت‌های

مستهجن از مصادیق تروریسم مجازی و فعالیتی انحصارطلبانه و مسدودکننده جریان مردم‌سالاری در ایران قلمداد شد (فیروزمنش، ۱۳۸۹: ۳٤).

اجرای "پروژه مرصاد" یکی از اقدامات مشخص این مرکز برای مبارزه با فعالیت‌های تروریستی از طریق فضای مجازی بوده که منجر به شناسایی شبکه "ایران پراکسی" شد، شبکه‌ای که با حمایت مالی مستقیم دولت ایالات متحده، نسبت به تخلیه بانک‌های اطلاعاتی کشور، نفوذ و خرابکاری در سایت‌های اینترنتی ایران و تولید فیلترشکن و ایجاد بستر ارتباط امن تلفنی و دیتا و ... برای دسترسی امن و غیرقابل ردیابی ایرانیان داخل کشور به سایت‌ها مختلف و مراکز سیاسی مورد نظر اقدام می‌کرد (سایت گرداب، ۲۳ اسفند ۱۳۸۸). این مرکز در اسفند ۱۳۸۸ هم از انهدام تعدادی از شبکه‌های سازمان یافته جنگ سایبری آمریکا و دستگیری ۳۰ نفر از عوامل آن خبر داد که تحت هدایت کاخ سفید درصدد جاسوسی از دانشمندان هسته‌ای ایران، جذب و سازمان‌دهی ایرانیان خارج از کشور، جریان‌سازی و جنگ روانی علیه نظام جمهوری اسلامی و مقدسات دینی، برگزاری تجمعات غیرقانونی و انتشار اخبار دروغ در اینترنت، انجام هک و نفوذ به سرورهای دولتی برای جاسوسی، برنامه‌ریزی برای اختلال در سیستم مدیریت شهری و شبکهٔ خدمات‌رسانی از جمله سامانه سوخت‌رسانی به منظور ایجاد نارضایتی مردمی و ... بودند (سایت گرداب، ۲٦ اسفند ۱۳۸۸).

با این توصیف، به نظر می‌رسد بر اساس قانون جرائم رایانه‌ای، خلأ قانونی خاصی برای رسیدگی به اقدامات تروریستی در فضای مجازی و مجازات تروریست‌های مجازی مورد حمایت دولت‌های خارجی و به خصوص آمریکا وجود ندارد.

نتیجه‌گیری

با عنایت به جوانی جمعیت ایران و سطح بالای تحصیلات بسیاری از شهروندان از یکسو و رشد سریع اقتصادی و اجتماعی کشور، استفاده از زیرساخت‌ها و سامانه‌های اطلاع‌رسانی و مهم‌ترین آن‌ها یعنی شبکه اینترنت در آینده روز به روز افزایش خواهد یافت.

از سوی دیگر، با توجه به رشد مداوم استفاده از اینترنت در کشور، وابستگی روزافزون به دستاوردهای فناوری اطلاعات و ارتباطات و ارائهٔ بسیاری از خدمات بخش دولتی و خصوصی بر این بستر، اختلال در دسترسی به اینترنت و دیگر شبکه‌های اطلاع‌رسانی، صدمات جدی به امنیت ملی، رفاه و آسایش عمومی مردم وارد کرده و حتی اقتدار نظام سیاسی را به چالش می‌کشد.

دولت‌های متخاصم و گروه‌های تروریستی وابسته به آن‌ها هم که به خوبی از این مسئله آگاهی دارند، با حداکثر توان فنی و علمی خود وارد نبرد با نظام اسلامی شده و با بهره‌گیری از شبکه‌های گسترده اطلاعاتی و دانش نیروهای متخصص در کنار صرف پول و امکانات متنوع سخت افزاری و نرم‌افزاری، در تلاش هستند اهداف خود را برآورده سازند.

این دولت‌ها برای رسیدن به اهداف خود از سه روش استفاده می‌کنند. روش اول سرقت فیزیکی هارددیسک‌ها، حافظه‌های قابل حمل، رایانه‌های لپ‌تاپ یا دیگر قطعات حساس

سخت افزاری است. سرقت یک لپ‌تاپ حاوی الگوریتم‌های مورد استفاده در سیستم فرماندهی و کنترل ایستگاه فضایی ISS آمریکا وابسته به ناسا در مارس سال ۲۰۱۱ نمونه عینی این مسئله محسوب می‌شود.

روش دوم طراحی کرم، ویروس یا تروجان برای سوءاستفاده از آسیب‌پذیری و حفره‌های امنیتی نرم‌افزاری و سخت‌افزاری مورد استفاده شرکت‌های خصوصی و نهادهای دولتی است که با انتشار کرم رایانه‌ای استاکس نت و تلاش ناکام آن برای آلوده‌کردن تأسیسات هسته‌ای ایران، توجه افکار عمومی به آن جلب شد.

در روش سوم هم با استفاده از تکنیک‌های مهندسی اجتماعی اعتماد مخاطب جلب شده و با شیوه‌هایی مانند فیشینگ برای تخلیه اطلاعاتی کاربر و سوءاستفاده از این اطلاعات برای سرقت حجم بالایی از داده‌های با ارزش اقدام می‌شود، چنانچه اطلاعات محرمانه۷۲ دولت، شرکت و سازمان مهم بین‌المللی جهان از سال ۲۰۰۶ تا ۲۰۱۱ به همین شیوه به سرقت رفت.

سهولت استفاده از روش‌های تروریستی در فضای مجازی و تنوع، مخفی‌بودن و کم هزینه بودن آن در مقایسه با روش‌های سنّتی بر علاقه حامیان تروریسم مجازی دولتی برای استفاده از این روش برای مقابله با جمهوری اسلامی افزوده است. در واقع رژیم صهیونیستی و آمریکا که به علت تبعات غیرقابل کنترل و هزینه‌های هنگفت حمله نظامی به تأسیسات هسته‌ای ایران قادر به چنین کاری نیستند، ترجیح دادند با مخفی کاری و صرف هزینه‌ای بسیار کمتر، یک کرم رایانه‌ای را برای تخریب سانتریفیوژهای مورد استفاده در نطنز طراحی کنند و به جای روش‌های تروریستی متداول و شناخته شده، به یکی از روش‌های تروریسم مجازی دولتی متوسل شوند. تداوم این حملات به شبکه‌های رایانه‌ای وزارت نفت و سپس وزارت علوم، تحقیقات و فناوری نشان می‌دهد که دشمن بر پیگیری این روش مبارزه اصرار دارد و فضای مجازی به خط مقدم نبرد ایران با آمریکا، رژیم صهیونیستی و دیگر هم‌پیمانان آن‌ها مبدل شده است.

ایمن‌سازی فضای مجازی در برابر حملات تروریست‌های مجازی دولتی امری دشوار، پیچیده و همراه با چالش‌های فراوان است، اما تحقق این هدف به سه روش ممکن خواهد شد. در ابتدا باید آموزش‌های تخصصی مختلف در مورد شیوه‌های سوءاستفاده تروریست‌های مجازی و روش‌های ایمن‌سازی رایانه‌ها و شبکه‌های رایانه‌ای در برابر حملات آنان، بر اساس نیازهای کاربران ارائه شود. سپس باید سازوکارهای قضایی و حقوقی مناسبی برای مقابله با تروریسم مجازی به وجود آید و قوانین قدیمی، متناسب با شرایط جدید به روز شوند تا از سوءاستفاده مجرمان از خلأهای قانونی و حقوقی جلوگیری شود. پس از طی شدن این دو مرحله، زمینه برای برداشتن گام نهایی و تأسیس سازمان‌های تخصصی که وظیفهٔ مقابله با تروریسم مجازی دولتی را بر عهده بگیرند، به وجود خواهد آمد.

دولت جمهوری اسلامی باید با عنایت به این نکات در جهت ارتقای آموزش‌های مرتبط با فناوری اطلاعات در سطح جامعه، ارائه طرح‌های قانونی مرتبط برای تصویب در مجلس شورای اسلامی، بومی‌سازی تجهیزات و امکانات نرم‌افزاری و سخت‌افزاری مورد استفاده در

حوزه فناوری اطلاعات و ارتباطات و تقویت نهادهایی همچون پلیس فتا تلاش کند تا کشور در این بخش هم مانند فناوری صلح‌آمیز هسته‌ای، به‌خود کفایی رسیده و قادر به رفع نیازمندی‌های خود در داخل باشد.

منابع

دردریان، جیمز (۱۳۸۲)، *گفتمان تروریستی: نشانه‌ها، دولت‌ها و نظام‌های خشونت سیاسی جهانی*، ترجمهٔ وحید بزرگی، تهران، نشر نی.

رضایی، مریم (۱۳۸۹) ، "افت و خیز افتا؛ درباره سند امنیت ملی در فضای تبادل اطلاعات"، ماهنامه *تحلیل گران عصر اطلاعات*، سال چهارم، شماره سی و هشتم، آذر ۱۳۸۹.

علی بابایی، غلامرضا (۱۳۸٤)، *فرهنگ سیاسی* آرش، تهران، نشر آشیان.

فلمینگ، پیتر و استول، مایکل (۱۳۸۲) ، *سایبر تروریسم: پندارها و واقعیت‌ها*، ترجمهٔ اسماعیل بقایی هامانه و عباس باقرپور اردکانی، تهران، نشر نی.

فیروزمنش، افشین (۱۳۸۹)، "پایان عصر معصومیت، تروریسم مجازی و مقابله با آن در ایران"، ماهنامه *تحلیل‌گران عصر اطلاعات*، سال چهارم، شماره سی و چهارم، تیرماه ۱۳۸۹.

Alperovitch, Dmitri (2011), " Revealed: Operation Shady RAT" (PDF: http://www.mcafee.Com/us/ resources/white-papers/wp-operation-shady-rat.pdf).

Aust, Anthony (2010), *Handbook of International Law* (2nd Ed.). Cambridge University Press. New York.

Baldi, Stefano & Gelbstein, Eduardo and Kurbalija, Jovan (2003), "Hacktivism, cyber-terrorism and cyber war: the activities of the uncivil society in cyberspace",Geneva, Diplo Foundation.

Barry, Collin (1997), "The Future of Cyber terrorism", Crime and Justice International Magazine, Vol.13, Issue 2, March 1997, from http://www.cjimagazine.com/archives/cji4c18.html?id = 415.

Barsamian, David (2001), "The United States is a Leading Terrorist State, An Interview with Noam Chomsky by David Barsamian ". Monthly Review, Volume 53, Issue 06 (November 2001), form www.monthlyreview.org/1101chomsky.htm.

Carnaghi, Bob (2004) Viruses, Worms, & Trojan Horses, July 31, 2004, from www. webpointmorpheus. com /technical/wpm_info-pdf/virus-worm-trojan. pdf .

Centre of Excellence Defence against Terrorism (2008), Responses to Cyber Terrorism (Nato Science for Peace and Security), Amsterdam, IOS Press.

Ching, Jacqueline (2010), *Cyberterrorism (Doomsday Scenarios, Separating Fact from Fiction)*, New York, Rosen Central.

Colarik, Andrew M. (2006), *Cyber terrorism: political and economic implications*, New York, Idea group publishing.

Chien, Eric, (2010), Stuxnet: A breakthrough, 16 November 2010, from http://www.symantec.com/ connect/blogs/stuxnet-breakthrough.

Council of Europe (2007), Cyberterrorism: The Use of the Internet for Terrorist Purposes (Terrorism and Law), France, Council of Europe Publishing.

Denning, Dorothy. E. (2001), "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," Nautilus Institute. from http://faculty.nps.edu/dedennin/ publications/ Activism-Hacktivism-Cyberterrorism.pdf , 8 June 2001.

Der Derian, James(1991), *The Terrorist Discourse*: *Signs*, States, and Systems of Global Political Violence ,World Security: Trends and Challenges at century's End, Edited by Michael T.Klare and Daniel C.Thomas, NewYork, St.Martin Press.

Jøsang, Audun et al. (2007), "Security Usability Principles for Vulnerability Analysis and Risk Assessment." (PDF: http://persons.unik.no/josang/papers/JAGAM2007-ACSAC.pdf Proceedings of the Annual Computer Security Applications Conference December 2007 (ACSAC'07). Retrieved 2012.

Khosow-pour, Mehdi (2004), *Innovations through Information Technology*, Pennsylvania, IGI Global.

Larousse, Pierre (1964), Grand Larousse encyclopédique en dix volumes, Paris Librairie Larousse, Vol. 10.

Lewis, James A (2002), "Assessing the risks of cyber terrorism, cyber war and other cyber threats", Center for strategic and international studies, from www.csis.org/files/media/csis/pubs/021101_risks_of_ cyberterror.pdf, December 2002.

Schmid, Alex P (1993), "The response problem as a definition problem", In: "Western response to terrorism", Alex Schmid and Ronald D.Crelinsten , London: Frank Cass & Co. Ltd.
Selden, Mark & Y.So, Alvin (2003),War and state terrorism: the United States, Japan, and the Asia-Pacific in the long Twentieth Century, Rowman & Littlefield Publishers.
Stohl, Michael & Lopez, George A (1988), *Terrible beyond Endurance*?: The Foreign Policy of State Terrorism. New York, Greenwood Press.
White, Jonathan Randall (1991), *Terrorism: An Introduction*, Pacific Grove CA: Brooks,Cole.

پایگاه‌های اینترنتی

پلیس فتا، بازیابی ۳۰ فروردین ۱۳۹۱ از: cyberpolice.ir/page/127
پی سی مگ، ۲۹ فوریه۲۰۱۲، بازیابی ۱۷ اردیبهشت ماه۱۳۹۱ از:
http://www.pcmag.com/article2/0,2817,2401020,00.asp
دانشنامهٔ بریتانیکا، بازیابی ۱ اردیبهشت ۱۳۹۱ از :
http://www.britannica.com/EBchecked/topic/588371/terrorism
خبرگزاری رویترز، ۲۰ سپتامبر ۲۰۱۱، بازیابی ۱۷ اردیبهشت ۱۳۹۱ از :
http://www.reuters.com/article/2011/09/20/mitsubishi-heavy-idUSL3E7KK1F320110920
خبرآنلاین، ۲۲ تیر ۱۳۸۸، بازیابی ۲۹ فروردین ۱۳۹۱ از : khabaronline.ir/detail/12548
خبرگزاری فارس، ۳۰ فروردین ماه۱۳۹۰، بازیابی ۲٤ فروردین ۱۳۹۱ از:
farsnews.com/newstext.php?nn=9001293328
خبرگزاری فارس، ١٤ مرداد ۱۳۹۰، بازیابی ۲۵ فروردین ۱۳۹۱ از :
farsnews.com/newstext.php?nn=9005120526
خبرگزاری فارس، ۱۹ مهر ۱۳۹۰، بازیابی ۲۵ فروردین ۱۳۹۱ از :
farsnews.com/newstext.php?nn=13900719000260
خبرگزاری فارس، ۲۲ اسفند ۱۳۹۰ ، بازیابی ۲٦ فروردین ۱۳۹۱ از :
farsnews.com/newstext.php?nn=13901221001265
خبرگزاری مهر، ۱۰ آبان ۱۳۸۹، بازیابی ۲٤ فروردین ۱۳۹۱ از :
mehrnews.com/fa/newsdetail.aspx?NewsID=1182559
سایت گرداب وابسته به مرکز بررسی جرائم سازمان یافته سپاه پاسداران انقلاب اسلامی، ۲۳ اسفند ۱۳۸۸، بازیابی ۲ اردیبهشت ۱۳۹۱ از : http://www.gerdab.ir/fa/mersad
سایت گرداب وابسته به مرکز بررسی جرائم سازمان یافته‌سپاه‌پاسداران انقلاب اسلامی، ۲٦ اسفند ۱۳۸۸، بازیابی ۲ اردیبهشت ۱۳۹۱ از :
http://www.gerdab.ir/fa/news/627/%D8%A7%D9%86%D9%87%D8%AF%D8%A7%D9%85-%D8%AA%D8%B9%D8%AF%D8%A7%D8%AF%DB%8C-%D8%A7%D8%B2-%D8%B4%D8%A8%D9%83%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%B3%D8%A7%D8%B2%D9%85%D8%A7%D9%86%E2%80%8C%D9%8A%D8%A7%D9%81%D8%AA%D9%87-%D8%AC%D9%86%DA%AF-%D8%B3%D8%A7%D9%8A%D8%A8%D8%B1%DB%8C-%D8%A2%D9%85%D8%B1%D9%8A%D9%83%D8%A7
عصر ایران، ١٦ مرداد ۱۳۸۹، بازیابی ١٦ فروردین ماه۱۳۹۱ از :
http://www.asriran.com/fa/news/129992/%D9%88%DB%8C%D8%B1%D9%88%D8%B3%DB%8C-%DA%A9%D9%87-%D8%B5%D9%86%D8%A7%DB%8C%D8%B9-%D8%A7%DB%8C%D8%B1%D8%A7%D9%86-%D8%B1%D8%A7-%D9%87%D8%AF%D9%81-%D9%82%D8%B1%D8%A7%D8%B1-%D8%AF%D8%A7%D8%AF%D9%87-%D8%A7%D8%B3%D8%AA
نیویورک تایمز، ١٦ ژانویه۲۰۱۱، بازیابی ٢٤ فروردین ۱۳۹۱ از:
nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=2
همشهری آنلاین، سوم بهمن ۱۳۸۹، بازیابی ۲۷ فروردین ۱۳۹۱ از:
hamshahrionline.ir/news-126496.aspx