مجله سیاست دفاعی
سال نوزدهم، شماره ۷۶، پائیز ۱۳۹۰

بررسی احتمال آسیب‌پذیری رسانه ملی در مقابل تروریسم سایبری

تاریخ دریافت مقاله: ۱۳۹۰/۰۵/۱۷
تاریخ تأیید مقاله: ۱۳۹۰/۰۶/۲۲
صفحات مقاله: ۲۸۲ – ۲۶۷

عباس بشیری [۱]
محمدنبی آقاتقی [۲]
علی‌اکبر سردره [۳]
محمدرضا سردره [٤]

چکیده:

سایبر تروریسم به حمله‌های اطلاعاتی اطلاق می‌گردد که به طور خاص شبکه‌های اطلاعاتی سازمان‌های دولتی و یا رسانه‌ها را مورد حمله قرار می‌دهد و هدف‌های اصلی آن شامل جاسوسی، ایجاد آسیب‌های سیاسی، اجتماعی، فرهنگی و اقتصادی و یا حتی فیزیکی (ویروس stuxnet) می‌باشد. بر اساس تعریف ارائه شده می‌توان گفت که سایبر تروریسم و مقابله با آن از لحاظ امنیتی بسیار مهم بوده و مورد توجه سازمان‌های اطلاعاتی کشورهای مختلف دنیا می‌باشد. یکی از نقاط آسیب‌پذیر در مقابل این پدیده رسانه‌ها می‌باشند. رسانه‌ها نقش آگاهی‌دهنده و یا هشداردهنده در مواقع بحرانی را دارند و یا این‌که حتی در مواقع غیربحرانی دارای مسئولیت سنگینی در زمینه‌ی تطابق محتوی و مفهوم برنامه‌ها با دیدگاه‌های ایدئولوژیک مخاطبان هستند؛ بنابراین، کنترل بر فرستنده‌های رسانه‌ای یا سیستم‌های اتوماسیون داخلی آنها (به‌عنوان مثال، سیستم اتوماتیک رایانه‌ای برای تنظیم و پخش برنامه‌ها از رادیو و تلویزیون) می‌تواند عواقب خطرناکی را در ابعاد گوناگون سیاسی، فرهنگی و امنیتی در پی داشته باشد. این پژوهش نشان می‌دهد که در صورت عدم توجه به استفاده از شبکه‌های امن برای کنترل فرستنده‌ها در آینده، شبکه‌ی کنترل فرستنده‌های زمینی صدا و سیما پاشنه‌ی آشیل این رسانه در مقابل سایبر تروریسم خواهد بود.

* * * * *

۱- کارشناسی ارشد روابط بین‌الملل مدرس دانشگاه آزاد اسلامی، واحد رودبار.
۲- کارشناس ارشد روابط بین‌الملل و مدرس دانشکده شهید مطهری دانشگاه علمی کاربردی.
۳- کارشناس دانشگاه آزاد اسلامی، واحد رودبار.
٤- متخصص رایانه و نرم‌افزارهای کنترل فرستنده.

واژگان کلیدی

رسانه‌ی ملی، تروریسم سایبری، نرم‌افزارهای کنترل فرستنده و مدیریت پخش.

مقدمه

از سایبرتروریسم، با عنوان تروریسم جدید[1] در هزاره‌ی سوم یاد می‌شود. پیشرفت فناوری‌های ارتباطی و در رأس آنها اینترنت در کنار سپرده شدن بسیاری از امور به رایانه‌ها باعث شده است تا سرمایه‌های ملی شامل سرمایه‌های واقعی (مانند زیرساخت‌های اجتماعی، اقتصادی، انرژی و ...) و سرمایه‌های سایبری مانند اطلاعات امنیتی مورد تهدید دائمی تروریست‌ها باشند. موضوع سایبر تروریسم برای کشورمان که در حال حاضر مورد تهدید دائمی کشورهای بیگانه و گروه‌های اسلام‌ستیز می‌باشد، دارای اهمیت دو چندانی است. تاکنون تعاریف متعددی از سایبرتروریسم ارائه شده است؛ در حالی که، این عبارت دارای مرزهای مشترکی با جنگ الکترونیکی، هکتیویسم و جرم‌های رایانه‌ای است؛ اما به نظر می‌رسد که این پدیده در درون خود دارای ویژگی‌هایی است که آن را از سایر پدیده‌های مشابه متمایز می‌کند. سایبرتروریسم، عبارت است از، انجام اعمال خرابکارانه با استفاده از فناوری‌های نوین که در نهایت می‌تواند موجب خسارت‌های مالی، فیزیکی و یا اطلاعاتی، امنیتی گردد. یکی از ناحیه‌های آسیب‌پذیر در مقابل سایبرتروریسم زیرساخت‌های مخابراتی و ارتباطاتی است. این زیرساخت‌ها شامل انواع دریافت‌کننده‌های امواج از ماهواره‌ها، فرستنده‌های زمینی و سایر تأسیسات الکترونیکی مخابراتی دریافت و صدور امواج می‌باشند. این زیرساخت‌های مخابرات هم در صنعت رسانه و هم در شبکه‌ی مخابراتی مربوط به تلفن‌های همراه یا ثابت و شبکه‌های ارتباطی مربوط به اینترنت کاربرد دارد. تأثیرپذیر بودن زیرساخت‌های مخابراتی و الکترونیکی رسانه‌های رادیویی و تلویزیونی در مقابل سایبر تروریسم از یک‌سو و اهمیت سیاسی و امنیتی و ایدئولوژیکی برخی از این رسانه‌ها از سوی دیگر باعث می‌شود تا موضوع آمادگی دفاعی در مقابل حملات سایبری بر این رسانه‌ها اهمیت بیشتری پیدا کند.

1- new terrorism

این موضوع درباره رسانه‌ی ملی کشورمان دارای حساسیت بسیار بیشتری است، چنان‌که از نظر مقام معظم رهبری (مد ظله‌العالی) صدا و سیما در جمهوری اسلامی دارای اهمیت مضاعفی است به گونه‌ای که به صورت خلاصه می‌توان گفت که از نظر ایشان دو عامل انتشار سخنان ملت در نظام جمهوری اسلامی و همچنین مبارزه با تبلیغات خصمانه‌ی رسانه‌های بیگانه باعث اهمیت مضاعف رسانه‌ی ملی برای جمهوری اسلامی می‌گردد.

حال با توجه به اهمیت ذکر شده برای رسانه‌ی ملی و استفاده‌ی این رسانه از تجهیزات الکترونیکی و ارتباطی، احتمال آسیب‌پذیری زیرساخت‌های ارسال امواج رادیویی و تلویزیونی وجود دارد و حرکت به سوی استفاده از فرستنده‌هایی که قابلیت کنترل توسط اینترنت را دارند موجب افزایش نگرانی‌ها در این مورد می‌شود. با توجه به حساسیت موضوع در این مقاله به بررسی و نواحی آسیب‌پذیر رسانه‌ی ملی در مقابل پدیده‌ی شوم سایبرتروریسم می‌پردازیم.

تعریف سایبر تروریسم و سابقه‌ی آن در ایران

تاکنون تعریف مشخصی از سایبر تروریسم ارائه نشده است، اما محققان مختلف هر کدام از یک زاویه این پدیده را بررسی و تعاریف خود را ارئه کرده‌اند که در این قسمت تلاش می‌شود تا با مروری بر این تعاریف مرزهای این پدیده با سایر مفاهیم مشابه بازشناخته و تفکیک گردد. «باری کالین» در ۱۹۹۷ این واژه را وضع کرد. او سایبر تروریسم را چنین تعریف می‌کند: سوءاستفاده عمدی از یک سیستم، شبکه یا مولفه‌ی اطلاعاتی رایانه‌ای برای تحقق هدفی که مؤید یا تسهیل‌کننده مبارزه یا اقدام تروریستی است (Lewis, 2002).

«دنینگ»، سایبر تروریسم را چنین تعریف می‌کند؛ سایبر تروریسم مرز مشترک تروریسم با فضای مجازی است و اغلب به معنی حمله و تهدید به وسیله یا علیه کامپیوترها، شبکه‌ها و اطلاعات ذخیره‌شده برای ترساندن و اجبار و فشار بر یک حکومت و مردمش برای رسیدن به اهداف سیاسی و اجتماعی است. برای واجد شرایط شدن یک حمله به صورت سایبر تروریسم آن حمله باید دربرگیرنده‌ی خشونت علیه مردم یا دارایی آنها باشد یا حداقل به بازتولید وحشت و ترس منجر گردد (Denning, 2000).

این تعریف حملاتی که منجر به مرگ یا جراحت بدنی، انفجار، سقوط هواپیماها، آلودگی هوا یا کاهش قدرت اقتصادی یا سقوط اقتصادی می‌گردد را شامل می‌شود. می‌توان گفت که حمله به زیرساخت‌ها جلوه‌هایی از سایبرتروریسم هستند. حملاتی که سرویس‌ها و خدمات غیرضروری را مورد حمله قرار می‌دهند یا مایه‌ی آزار اندک شوند جزء این تعریف نمی‌شوند. در کشورهایی که کنترل نظارت بر عملکرد تأسیسات زیربنایی به وسیله‌ی برنامه‌های رایانه‌ای صورت می‌گیرد، احتمال آسیب‌پذیری این زیرساخت‌ها بیشتر خواهد بود (Gordon, 2008).

ارتش آمریکا سرمایه‌های ملی در معرض هجوم سایبر تروریسم را به دو دسته تقسیم می‌کند:

۱) سرمایه‌های سایبری (اطلاعاتی) شامل اطلاعات امنیتی و طبقه‌بندی شده‌ی ملی یا پایگاه‌های اینترنتی مربوط به سازمان‌ها و نهادهای دولتی.

۲) سرمایه‌های واقعی شامل تأسیسات نیروگاهی، تأسیسات حمل و نقل و تجهیزات ارتباطی و مخابراتی.

نکته‌ی بسیار مهم این است که امروزه سایبر تروریسم علاوه بر تهدید سرمایه‌های اطلاعاتی و سایبری دولت‌ها تهدیدی جدی برای سرمایه‌های واقعی نیز محسوب می‌گردند؛ به‌گونه‌ای که ایجاد خسارت‌های فیزیکی توسط تروریسم سایبری کاملاً محتمل است و بسیاری از کشورهای جهان با جدی گرفتن این تهدیدها در حال شناسایی و رفع نقاط ضعف خود با استفاده از دانش پدافند غیرعامل هستند (Frauenheim, 2002).

جمهوری اسلامی ایران با جایگاه خاص سیاسی خود دارای موقعیتی است که آن را در معرض تهدید و هجمه‌های منطقه‌ای و بین‌المللی قرار داده است. در سال‌های اخیر رویارویی با دشمنان وارد دوره‌ی جدیدی شده است که از آن به‌عنوان جنگ الکترونیک یاد می‌شود. ویروس stuxnet یکی از جلوه‌های این رویارویی می‌باشد که با هدف خرابکاری در تأسیسات هسته‌ای ایران طراحی شده بود. نتایج تجزیه و تحلیل‌های انجام شده از سوی آژانس جاسوسی و اطلاعات اروپا با طبقه‌بندی سری که به رؤیت هفته‌نامه‌ی آلمانی اشپیگل نیز رسید، نشان داد احتمالاً برای توسعه‌ی ویروس استاکس‌نت، یک برنامه‌نویس، دست کم سه سال با یک هزینه‌ی چند ده میلیونی به کارگیری شده است. در همین حال شرکت سایمنتک نیز به سهم خود معتقد

است، فقط انجام آزمون‌ها و تست‌های لازم در تأسیسات شبیه‌سازی شده (اتمی ایران) به پنج تا ده برنامه‌نویس به مدت شش ماه نیاز داشته‌اند».

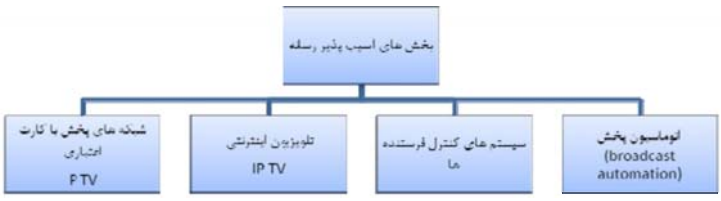
در واقع این اظهارات تنها بخشی از واقعیت نبرد تمام عیار غرب در حوزه‌ی فناوری و جنگ نرم علیه نظام اسلامی قلمداد می‌شود که از سوی دولت ایالات متحده امریکا و رژیم صهیونیستی در برابر دستاوردهای ملت ایران و فناوری‌های صلح‌آمیز هسته‌ای دانشمندان ایرانی طرح‌ریزی می‌شود. موضوعی که هم‌اکنون با شکست دشمن از بهره‌برداری خود از نتیجه‌ی فعال‌سازی ویروس استاکس‌نت در رویارویی با ایران اعتراف به شکست و ردپای سازمان جاسوسی هم‌چون موساد و شبکه‌های جاسوسی غرب را برملا می‌کند. حملات سایبری دشمن محدود به تأسیسات نیروگاهی نمی‌باشد، بلکه تأسیسات مخابراتی و ارتباطی ما نیز در معرض تهدید حمله‌ی سایبری دشمنان قرار دارد. در قسمت بعد به بررسی حمله‌ی سایبری به رسانه‌ی ملی و عواقب آن می‌پردازیم.

رسانه‌ی ملی و حمله‌ی سایبری، عواقب سیاسی و امنیتی حمله به رسانه‌ی ملی

همان‌گونه که ملاحظه می‌گردد، استکبار جهانی به دنبال ضربه زدن به ملت ایران و نظام جمهوری اسلامی است و در این راه از همه‌ی ابزارهای موجود استفاده می‌کند. به این ترتیب لزوم شناخت نقاط در معرض تهدید حمله‌ی سایبری دشمن و کسب آمادگی به‌منظور مقابله با این توطئه‌ها امری بسیار ضروری است. یکی از نواحی آسیب‌پذیر در مقابل سایبر تروریسم تأسیسات ارتباطی و مخابراتی مانند فرستنده‌های زمینی و ماهواره‌ای می‌باشند. وابستگی رسانه‌های کشورمان و به خصوص رسانه‌ی ملی به عملکرد این فرستنده‌ها و حرکت صدا و سیما به سوی استفاده از اینترنت برای برقراری ارتباط میان فرستنده‌ها لزوم تفکر در مورد خطرات احتمالی ناشی از حمله‌ی سایبری به رسانه‌ی ملی را روشن می‌نماید. بنابراین، توجه به احتمال وقوع حمله‌ی سایبری علیه رسانه‌ی ملی و بررسی نقاط آسیب‌پذیر این رسانه در مقابل حملات سایبری باید در دستور کار این سازمان و هم‌چنین مجامع تحقیقی پژوهشی کشور قرار گیرد. در این پژوهش تلاش گردیده تا با شناخت اولیه از وضعیت زیرساخت‌های

ارتباطی و فرستنده‌های مورد استفاده در صدا و سیما و زمینه‌ی توسعه و تجهیز فرستنده‌های رادیویی و تلویزیونی به شناخت و تشریح نقاط آسیب‌پذیر این رسانه در مقابل سایبر تروریسم پرداخته شود. به این منظور لازم است که در ابتدا به بررسی اولیه‌ی نحوه‌ی پخش و تجهیزات پخش مورد استفاده این سازمان پرداخته شود. در حال حاضر، پخش زمینی امواج متداول‌ترین شیوه‌ی پخش در ایران است. بنابراین، در ادامه به معرفی این شیوه و احتمال آسیب‌پذیری آن توسط حملات سایبری می‌پردازیم.

اما لازم است قبل از پرداختن به این بحث مروری اجمالی بر نواحی آسیب‌پذیر رسانه در مقابل سایبر تروریسم بپردازیم. نمودار شماره‌ی ۱ به صورت خلاصه نشان‌دهنده‌ی بخش‌هایی از رسانه است که در مقابل سایبر تروریسم آسیب‌پذیر هستند.



نمودار شماره‌ی ۱- بخش‌های آسیب‌پذیر رسانه در مقابل سایبر تروریسم

برنامه‌های اتوماسیون پخش نرم‌افزارهایی هستند که زمان‌بندی برنامه‌های پخش را به صورت خودکار انجام می‌دهند و بنابراین، نیاز به نیروی انسانی به‌منظور نظارت بر زمان‌بندی پخش برنامه‌ها را از بین می‌برند. هک شدن این نرم‌افزارها توسط هکرها موجب می‌شود تا اختیار زمان‌بندی پخش برنامه‌ها یا قطع و وصل نمودن شبکه به دست آنها بیفتد. با توجه به این‌که رسانه‌ی ملی در حال حاضر دارای تعداد نیروی انسانی بالا برای کنترل پخش برنامه‌ها بوده و استفاده از نرم‌افزارهای پخش خودکار در دستور کار آن قرار ندارد؛ بنابراین، می‌توان نتیجه گرفت که رسانه‌ی ملی از این لحاظ در مقابل هکرها مورد تهدید نمی‌باشد. علاوه بر این، همان‌گونه که در بخش بعدی ملاحظه می‌گردد با توجه به ضعف تجهیزات در زمینه‌ی خطوط DSL روش‌های نوظهور پخش مانند IP TV

جایگاه مهمی در رسانه‌ی ملی ندارند، هر چند که برنامه‌های توسعه‌ی آتی این سازمان در جهت ترویج این‌گونه پخش می‌باشد، اما با توجه به فاصله‌ی زمانی زیاد تا مجهز شدن تمام مناطق کشور به خطوط DSL به نظر می‌رسد که هم‌چنان روش پخش زمینی اصلی‌ترین روش پخش در رسانه‌ی ملی باقی بماند. زمینه‌ی آخر آسیب‌پذیری رسانه‌ها کانال‌های پخش با کارت اعتباری یا P TV می‌باشد که در این مورد باید گفت که هک شدن رمز عبور این شبکه‌ها بیشتر بر اساس منافع اقتصادی هکرها بوده و در نتیجه، به صورت اساسی نمی‌توان هک شدن آنها را با عواقب امنیتی و سیاسی ناشی از اختلال در پخش فرستنده‌ها یکی دانست، ضمن این‌که این سیستم پخش در کشور ما وجود ندارد و هنوز برنامه‌ای در مورد آن از طرف صدا و سیما مشخص نشده است. با توجه به نکات مطرح شده در این قسمت می‌توان نتیجه گرفت که در حال حاضر نگرانی‌ها در مورد حمله‌ی سایبری به رسانه‌ی ملی در حیطه‌ی فرستنده‌ها و نحوه‌ی کنترل آنها محدود می‌باشد. با توجه به این‌که صدا و سیما به دنبال استفاده از فرستنده‌هایی است که قابلیت کنترل از شبکه را دارند؛ بنابراین، به نظر می‌رسد که حمله‌ی سایبری به سیستم کنترل این فرستنده امری کاملاً محتمل بوده و لازم است که در مورد مقابله با آن تدابیر لازم اندیشیده شود اما قبل از تشریح نکات فنی در زمینه‌ی فرستنده‌ها؛ اشاره‌ای کوتاه به مهم‌ترین عواقب امنیتی و سیاسی اختلال در پخش برنامه‌های رسانه‌ی ملی می‌پردازیم که به شرح زیر می‌باشد:

۱) ازبین رفتن نقش آگاهی بخشی و آرامش بخشی رسانه در جامعه در هنگام مواجهه با بحران‌های سیاسی و امنیتی؛
۲) غلبه‌ی تبلیغاتی رسانه‌های بیگانه در صورت قطع برنامه‌های رسانه ملی هرچند به صورت بسیار کوتاه مدت؛
۳) شکست در جبهه‌ی جنگ الکترونیک در مقابل دشمان و عواقب سیاسی و امنیتی آن؛
٤) بی‌اعتمادی مردم به رسانه ملی و مسئولین آن؛
۵) بر هم خوردن نظم عمومی و آرامش روانی جامعه در نتیجه ایجاد حس بی‌ثباتی ناشی از ضربه‌پذیر بودن رسانه‌ی ملی؛

با توجه به موارد بالا می‌توان نتیجه گرفت که هرگونه اختلال هر چند کوتاه در رسانه‌ی ملی ضربه‌های جبران‌ناپذیر سیاسی و امنیتی بر ملت ایران و نظام مقدس جمهوری اسلامی وارد خواهد نمود؛ از این رو، لازم است که مسئولین با حساسیت بیشتری به این موضوع توجه نمایند. در ادامه به تشریح چگونگی آسیب‌پذیری صدا و سیما در مقابل سایبر تروریسم در زمینه‌ی کنترل فرستنده‌های زمینی می‌پردازیم.

اهمیت پخش زمینی[1]

یکی از روش‌های متداول پخش سیگنال‌های تلوزیونی و رادیویی، پخش زمینی است. پخش زمینی امواج بالاترین اولویت را در ایران داراست. دلیل این امر در دستور نبودن استفاده از «ماهواره»[2] به‌عنوان یکی دیگر از روش‌های ارسال و نیز عدم استفاده و توسعه‌ی پخش «کابلی»[3] است (Michael.N et al, 2010). البته استفاده از روش‌های نوین دیگری نظیر «IP TV» نیز در حال حاضر در دستور کار سازمان صدا وسیما وجود دارد که با توجه به نوظهور بودن آن و نیز عدم وجود زیرساخت‌های لازم جهت توسعه‌ی آن (تجهیز مراکز مخابراتی سراسر کشور برای راه‌اندازی خطوط DSL)،در حال حاضر رقیب جدی برای پخش زمینی محسوب نمی‌گردند و کماکان دریافت زمینی امواج، بالاترین ضریب نفوذ را نسبت به سایر روش‌های پخش داراست. از طرف دیگر نخستین روش سیگنال‌رسانی از مراکز رادیویی و تلوزیونی در دنیا از زمان پیدایش رادیو و پس از آن تلوزیون، پخش زمینی بوده است. به همین دلیل، ابزارهای مورد استفاده در این بخش طی سالیان متمادی گسترش و پیشرفت بسیار زیادی کرده‌اند و گیرنده‌های منطبق بر این روش پخش در کلاس‌های مختلف، در اقصی نقاط دنیا وجود دارند. ایران هم از این قاعده مستثنی نیست و در دور افتاده‌ترین نقطه‌ی کشور نیز فرستنده‌ها و به طبع آن گیرنده‌های پخش زمینی وجود دارند (Eric Micheletti, 2009).

1- terrestrial Broadcasting
2- satellite
3- Cable

ظریب نفوذ بسیار بالای این روش پخش و همچنین قدرت رسانه‌ای بی‌مانند شبکه‌های رادیویی و تلویزیونی به سبب دسترسی همگانی به آن، اهمیت این شیوه‌ی پخش را صد چندان می‌کند، چه این‌که رادیو و تلویزیون ملی یک کشور همیشه مهم‌ترین و مؤثرترین و البته در دسترس‌ترین پل ارتباطی بین حاکمیت و مردم آن کشور است.

جایگاه فرستنده‌های پخش زمینی[1]

جایگاه روش پخش زمینی برنامه‌های رادیویی و تلویزیونی سبب شده است، فرستنده‌های پخش زمینی به‌عنوان مهم‌ترین ابزار آن از درجه اهمیت بسیار زیادی برخوردار باشند. فرستنده‌های پخش زمینی وظیفه‌ی انتشار امواج (رساندن سیگنال به گیرنده) را بر عهده دارند و در مدت ٢٤ ساعت شبانه‌روز به صورت پیوسته در حال پخش برنامه هستند و به هیچ‌وجه نباید این عمل متوقف و یا دچار مشکل شود. در واقع، می‌توان گفت خروجی کار رسانه‌ی ملی توسط فرستنده‌ها پخش می‌شود، تا در نهایت برنامه‌هایی که با دقت فراوان و کیفیت فنی بسیار بالا (به خصوص از لحاظ صوت و تصویر) ساخته می‌شوند، با همان کیفیت به سمع و نظر مخاطبان بی‌شمارش برسد. ناگفته پیداست که کیفیت و قدرت خروجی فرستنده‌ها باید به‌طور مستمر در بهترین وضعیت ممکن باشند، چه کوچک‌ترین اختلال در کار فرستنده‌ها باعث بروز اختلال[2] در صدا و تصویر و یا پایین آمدن سطح سیگنال در منطقه‌ی تحت پوشش فرستنده و در نتیجه تضعیف سیگنال دریافتی گیرنده‌ها شود (Michael Erbschloe, 2008).

خاموش شدن فرستنده‌ی فعال (درحال پخش برنامه) یا به عبارت دیگر، قطع یک کانال رادیویی ویا تلویزیونی به هر علتی، بدترین اتفاقی است که می‌تواند رخ دهد. حتی درصورتی که فرستنده‌ی فعال نیاز به سرویسی یا تنظیم پیدا کند، فرستنده‌ی رزو کار پخش برنامه را تا زمان سرویس یا تنظیم فرستنده‌ی اصلی، بر عهده می‌گیرد. در صوتی که امکان جایگزینی فرستنده‌ی رزرو وجود نداشته باشد، خاموشی فرستنده‌ی فعال منوط به اخذ مجوز از مراجع

1- terrestrial broadcasting transmitter
2- Noise

ذی‌صلاح سازمان صدا و سیما است؛ ضمن این که، مجوز این کار برای زمانی داده می‌شود که زمان پخش برنامه‌های کانال به اتمام رسیده و یا کمترین مخاطب (معمولاً نیمه‌های شب)، مشغول دیدن یا شنیدن برنامه (کانال در حال پخش) هستند. بنابراین، رسیدگی و نظارت بر عملکرد فرستنده‌ها به جهت جلوگیری از وقوع قطعی و یا بروز اشکال در کار فرستنده‌ها، از مهم‌ترین و حساس‌ترین وظایف سازمان صدا و سیما است.

نکته‌ی قابل تأمل دیگر، ظهور روش پخش دیجیتال تلویزیونی زمینی (DVB-T) در برابر پخش آنالوگ قدیمی است. در این روش، یک فرستده‌ی تلوزیونی قادر به پخش چند شبکه‌ی تلویزیونی مختلف (روی یک فرکانس) است، بر خلاف پخش آنالوگ که به ازای هر شبکه تلویزیونی یک فرستنده‌ی اختصاص می‌یافت. برای مثال، در تهران شبکه‌های یک، دو، سه، چهار، پنج، خبر، آموزش و قرآن از طریق یک فرستنده به صورت دیجیتال پخش می‌شوند. پرواضح است که محافظت و رسیدگی بر صحت عملکرد این نوع فرستنده‌ها از چه درجه‌ی اهمیتی برخوردار است.

درآمدی بر ایستگاه فرستنده‌های پخش زمینی

فرستده‌های رادیو و تلوزیونی در مکانی موسوم به ایستگاه فرستنده[1] استقرار می‌یابند. به دلیل ماهیت و نحوه انتشار امواج، ایستگاه‌ها در مکان‌هایی ساخته می‌شوند که کمترین مانع بین آنتن فرستنده و گیرنده وجود داشته باشد. این امر سبب می‌شود مکان احداث ایستگاه‌ها در مرتفع‌ترین نقطه منطقه‌ی تحت پوشش (و البته بعضاً صعب‌العبور) واقع شود. ایستگاه‌ها بر اساس منطقه تحت پوشش (و به طبع آن میزان قدرت فرستنده‌هایش) به سه دسته ایستگاه‌های پر قدرت، میان قدرت و کم قدرت تقسیم می‌شوند.

- ایستگاه‌های پرقدرت شهرهای بزرگ و مناطق اطراف آن را پوشش می‌دهند و با توجه به تعدد فرستنده‌ها و قدرت بالای آنها، همیشه مهندسان و اپراتورهایی نظارت بر کارکرد فرستنده‌ها بر عهده دارند. در این نوع ایستگاه‌ها اتاق مانیتورینگ وجود

1- Transmitter station

دارد که به صورت ۲٤ ساعته خروجی فرستنده‌ها (توسط گیرنده‌های مخصوصی که در این واحد وجود دارد) چک می‌شود در صورت بروز مشکل احتمالی، به سرعت اشکال برطرف گردد.

- ایستگاه‌های میان قدرت وظیفه‌ی پوشش شهرهای کوچک را بر عهده دارند. امکانات و پرسنل این ایستگاه‌ها محدود بوده و مجهز به اتاق مانیتورینگ نیستند؛ اما همیشه حداقل یک اپراتور وضعیت فرستنده‌ها را زیر نظر دارد تا در صورت بروز اشکال، آن را برطرف و یا مسئولان امر را مطلع کند.
- ایستگاه‌های کم قدرت در مناطق دورافتاده و کم جمعیت به طور عمده روستایی برپا می‌شود. در این نوع ایستگاه‌ها اپراتوری وجود ندارد و در صورت بروز مشکل در فرستنده‌ها گزارشات مردمی، مسئولان امر را مطلع کرده و اکیپی از مناطق نزدیک برای رسیدگی به مشکل اعزام می‌گردد. علاوه بر آن بازدیدهای دوره‌ای از این ایستگاه‌ها در دستور کار مراکز صدا و سیما قرار دارد که البته صعب‌العبور بودن و دسترسی بسیار سخت به بعضی از این ایستگاه‌ها، نظارت دوره‌ای بر آن را مشکل‌تر می‌کند.

لزوم ایجاد یک شبکه‌ی ارتباطی بین ایستگاه‌ها و مراکز

ایجاد یک شبکه‌ی ارتباطی بین ایستگاه‌ها و مراکز می‌تواند نظارت و رسیدگی به وضعیت ایستگاه‌ها و به طبع آن فرستنده‌ها (حتی در دور افتاده‌ترین نقاط کشور) را ساده‌تر نماید. در این صورت امکان مانیتورینگ وکنترل فرستنده‌ها منوط به حضور اپراتورها در ایستگاه‌ها نیست و حتی از کیلومترها دورتر از ایستگاه، می‌توان از صحت عملکرد فرستنده‌ها اطمینان حاصل کرد و یا در صورت نیاز برخی از پارامترهای فرستنده‌ها را اصلاح کرد؛ ضمن این که، وجود یک شبکه‌ی کنترلی و نظارتی بین ایستگاه‌ها و مراکز امکان نظارت و کنترل مرکزی در تهران را نیز، به‌عنوان مرکز اصلی را در پی دارد، امری که مدیران سازمان صدا وسیما را بر آن داشته تا در جهت تحقق این امر گام بردارند.

استفاده از اینترنت برای ایجاد شبکه‌ی کنترل و نظارت

استفاده از شبکه‌ی اینترنت جهت نظارت و کنترل فرستنده‌ها از راه دور، روشی آسان را برای ایجاد یک شبکه‌ی متمرکز در برابر سازمان صدا وسیما قرار می‌دهد. در حال حاضر، اینترنت با توجه به توسعه و نفوذ آن در اقصی نقاط کشور، بهترین وسیله برای ایجاد شبکه‌های ارتباطی است. از این سو پیشرفت فناوری و هم عرض آن، ارتقای فناوری ساخت فرستنده‌ها، مجهز شدن آنها به ابزارهای اتصال از راه دور[1] مبتنی بر پروتکلTCP/IP را منجر شده است. وجود این قابلیت، امکان ایجاد ارتباط اینترنتی را با فرستنده‌ها ممکن می‌کند. بنابراین، همه ابزارهای لازم جهت شبکه کردن ایستگاه‌ها و در نهایت دسترسی به فرستنده‌های پخش زمینی از راه دور، مهیا است.

خطرات استفاده از شبکه‌ی اینترنت

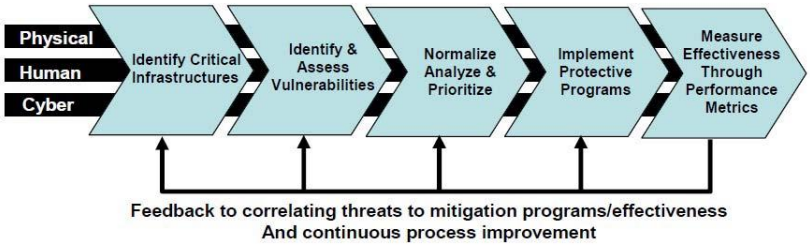
شبکه‌ی جهانی اینترنت از ابتدا برای داشتن بستری اطلاعاتی امن و محافظت شده، طراحی نشده است، بلکه قابلیت دسترس‌پذیری[2] و انعطاف‌پذیری[3] آن مورد توجه طراحان و توسعه‌دهندگان اینترنت بوده است. همین امر سبب شده تا همیشه از اینترنت به‌عنوان بستری پرخطر برای انتقال داده‌های مهم و حیاتی یاد شود. استفاده از ابزارها و نرم‌افزارهای امنیتی و البته پروتکل‌های امن مانند HTTPS[4] می‌تواند ضعف امنیتی اینترنت را پوشش دهد. اما خبرهایی که از هک شدن سایت‌ها و شبکه‌های اطلاعاتی ریز و درشت وحملات سایبری به بزرگ‌ترین سایت‌های اینترنتی و غول‌های این صنعت نظیر گوگل، مایکروسافت و حتی وب سایت‌های بسیار امنیتی مانند CIA، هر روزه شنیده می‌شود نشان می‌دهد همیشه راه جدیدی برای حمله‌ی سایبری هکرها حتی به امن‌ترین تأسیسات اینترنتی وجود دارد (Lepick et al, 2003).

1- Remote Connection
2- Availability
3- Resiliency
4- Secure HTTP

با توجه موارد ذکر شده در باب درجه اهمیت پخش زمینی و بستر اطلاعاتی ناامن اینترنت، به روشنی می‌توان دریافت که در صورت ایجاد شبکه‌ی نظارتی و کنترلی اینترنتی برای ایستگاه‌ها، که منجر به دسترسی و کنترل مستقیم فرستنده‌های پخش زمینی از طریق اینترنت گردد، چه خوراک خوبی برای حملات سایبری بر پیکره‌ی پخش زمینی رادیویی و تلویزیونی در کشورمان و حتی خاموشی فرستنده‌ها، در اختیار هکرها خواهد گذاشت. حتی استفاده از جدیدترین دستاورهای امنیتی به شیوه‌ی متداول در دنیای اینترنت نیز نمی‌تواند تضمین‌کننده‌ی عدم آسیب‌پذیری در حوزه‌ی مورد بحث باشد.

نتیجه‌گیری

فرایند مقابله با تروریسم به طور کلی شامل مراحل مختلفی از شناخت تأسیسات مورد تهدید تا راه‌های مقابله با حملات می‌باشد. نمودار شماره‌ی (۲) فرایند مقابله با تروریسم را به صورت کلی نشان می‌دهد. همان‌گونه که ملاحظه می‌گردد، راهبردهای کلی مقابله با تروریسم سایبری نیز در نخستین مرحله بر شناخت تأسیسات مورد تهدید می‌باشد که این پژوهش گامی اولیه در همین مرحله می‌باشد. از این رو، برنامه‌ریزی دقیق برای مقابله با حملات سایبری بر ضد رسانه‌ی ملی نیازمند مطالعات فنی در گام‌های بعدی است که پرداختن به آنها در این مقاله نمی‌گنجد. اما با توجه به بحث صورت گرفته در این مقاله تلاش می‌گردد تا ارائه‌ی پیشنهادات به صورت کلی صورت گیرد.



نمودار شماره‌ی ۲- فرایند مقابله تهدیدات تروریستی با منشاهای مختلف (Senta Monica, 2001)

به‌کارگیری شبکه‌ای ابداعی و انحصاری بومی مبتنی بر بستر اینترنت می‌تواند پیشنهاد خوبی برای حل مشکل امنیتی در حوزه‌ی ایستگاه‌های پخش زمینی باشد. به این ترتیب که در ایستگاه‌ها، فرستنده‌ها با همان روش متداول ومعمول با یکدیگر شبکه گردند و این شبکه از طریق یک شبکه با توپولوژی و پروتکل انحصاری (والبته رمزنگاری شده)که برای این منظور طراحی شده به شبکه‌ی جهانی اینترنت متصل گردد. این امر سبب شده تا اتصال مستقیم شبکه‌ی فرستنده‌ها به اینترنت از بین رفته و دسترسی به فرستنده‌ها از طریق پروتکل‌های مرسوم و عمومی اینترنت که در دسترس همگان است غیرممکن گردد.

منابع

فارسی

۱- جعفری، علی‌اصغر، (۱۳۸۸)، «***منشور رسانه***»، انتشارات سروش.

انگلیسی

2- richard a.clarke and robert knake , (Apr 20,2010), "***cyber war:the next threat to national security and what to do about it***".

3- Carlisle Barracks, (2000), "***Transnational Threats : Blending Law Enforcement and Military Strategies***".

4- Ron Rhodes,Aug 1, (2011), ***"Cyber Meltdown: Bible Prophecy and the Imminent Threat of Cyberterrorism***"

5- George V. Jacobson, (Apr 2009), "***Cybersecurity, Botnets, and Cyberterrorism***".

6- Robert T. Uda, (2009), "***Cybercrime, Cyberterrorism, and Cyberwarfare***", Oct 1

7- Jason Porterfield, (Jan 2011), "***Careers as a Cyberterrorism Expert***" (Careers in Computer Technology).

8- James A Lewis, Dec (2002), "***Assessing the Risks of Cyberterrorism, Cyber War and Other Cyber Threats***", Center for Strategic and International Studies.

9- Dorothy E. Denning , May 23, (2000), "***Cyberterrorism Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives***", Georgetown University.

10- Ed Frauenheim, (2002), "***Cyberterror and Other Prophecies***", December 12.

11- Michael N. Schmitt & Brian T. O'Donnell, editors (2010), "***Computer Network Attack and International Law***".

12- Eric Micheletti, (2009), "***Forces spéciales, Guerre contre le terrorisme***.

13- Michael Erbschloe, (2008), "***Information Warfare : How to Survive Cyber Attacks***".

14- Santa Monica, (2001), "***Networks and Netwars : The Future of Terror, Crime, and Militancy***".

15- O. Lepick, J.F. Daguzan, (2003), "***Le terrorisme non conventionnel***", 15 mars.

16- editors, Abraham D. Sofaer, "***Seymour E. Goodman. contributing authors: Mariano-Florentino Cuellar***" ... [et al.] Stanford, CA.

17- Based on a conference on international cooperation to combat cyber crime and terrorism, held at the Hoover Institution on December 6 and 7, 1999, Hoover Institution Press. 2001, The Transnational Dimension of Cyber Crime Terrorism.