فصلنامه مطالعات جنگ
سال دوم، شماره پنجم، تابستان ۱۳۹۹
مقالهٔ ششم از صفحه ۱۲۵ تا ۱٤٦

تروریسم سایبری؛ تهدیدی علیه سیستم‌های کنترل صنعتی زیرساخت‌های کشورهای غرب آسیا

دکتر محمدحسن نامی[۱]، مصطفی طوقانیان[۲]

دریافت مقاله: ۹۹/۰۱/۲۹ پذیرش مقاله:۹۹/۰۴/۲۷

چکیده

منطقه غرب آسیا طی چند سال اخیر و به‌طور مشخص، بعد از حادثه ۱۱ سپتامبر ۲۰۰۱ با گسترش تروریسم و فراگیر شدن فضای تقابلی و جنگ نیابتی مواجه شده است. ورود فناوری اطلاعات در زیرساخت‌های حیاتی کشورهای مختلف اعم از آب، برق، نفت، گاز و ... ضمن کاهش هزینه‌ها و راحتی کنترل مصرف و پایش باعث ایجاد فضاهایی شده که به حفره‌های امنیتی مشهور شده است. اهمیت موضوع در این است که پیامدهای چنین چالشی برای کشورهایی نظیر کشورهای جنوب غرب آسیا که از بُعد فناوری در حوزه‌های صنعتی و زیرساختی وابسته به غرب می‌باشند (فاقد توانمندی‌های بومی در حوزه سیستم‌های کنترل صنعتی می‌باشند) و دارای اقتصادهای ملی تک‌محصولی و مبتنی بر صادرات نفت، گاز و محصولات پتروشیمی می‌باشند؛ فراگیر می‌باشد و در این ایام شاهد گسترش ورود جریان‌ها و رویکردهای تروریستی به حوزه حملات سایبری و توسعه تروریسم سایبری می‌باشیم. سوال اصلی در این بررسی این است که در صورت گسترش فضای جنگ نیابتی و روند به‌کارگیری تروریسم نیابتی توسط کشورهای منطقه به حوزه سایبری؛ کدام یک از زیرساخت‌های سایبری توسط تروریسم سایبری مورد تهاجم قرار خواهد گرفت؟ روش پژوهش در این بررسی توصیفی- تحلیلی و شیوه گردآوری اطلاعات کتابخانه‌ای می‌باشد. بر طبق نتایج به دست آمده مشخص گردید موضوع تسری دامنه جنگ‌های نیابتی حاکم بر منطقه جنوب غرب آسیا به حوزه تروریسم سایبری که توسط گروه‌های غیردولتی صورت می‌پذیرد، تهدیداتی را با آثار و پیامدهای متنوع و گسترده متوجه زیرساخت‌های اساسی دارای سیستم‌های کنترل صنعتی می‌نماید.

واژگان کلیدی: تروریسم سایبری، سیستم‌های کنترل صنعتی، تروریسم نیابتی، منطقه جنوب غرب آسیا.

۱. دکترای جغرافیایی سیاسی و دکترای مدیریت استراتژیک عضو هیئت‌علمی دانشگاه علوم و فنون فارابی
dr.mh.nami@gmail.com
۲. دانشجوی کارشناسی ارشد پدافند غیرعامل، گرایش امنیت ملی mtufanian@ yahoo.com

مقدمه

منطقه جنوب غرب آسیا و شمال آفریقا یکی از کانون‌های درگیر جنگ، تروریسم و ناپایداری سیاسی در دهه‌های اخیر جهان بوده است. یکی از مهم‌ترین ابعاد خسارات وارده؛ سرمایه‌های انسانی و زیرساختی کشورهای درگیر بوده است. اعمال تهدیدات تروریستی علیه توده‌های جمعیتی وجه ثابت تهدیدات تروریستی طی ادوار مختلف تاریخی بوده است لیکن به نظر می‌رسد تخریب زیرساخت‌ها به وجه جدیدی از تهدیدات تروریستی به‌منظور ایجاد چالش‌های فراگیر برای امنیت ملی کشورها تبدیل گردیده است.

زیرساخت‌ها نقشی تعیین‌کننده و حیاتی در عملکرد یک سیستم در زمانه‌ای عادی، حین بحران‌ها و همچنین اقتصاد و امنیت یک کشور ایفا می‌کنند و حفظ امنیت زیرساخت‌ها در برابر حملات و تهدیدات، جز اولویت‌های امنیتی هر کشور است.

از آنجایی که اقدامات خرابکارانه و جنگ‌ها علیه زیرساخت‌ها علاوه بر ایمنی کارکنان و ایمنی زیرساخت‌ها، مبانی امنیت ملی کشورها را تحت تأثیر خود قرار می‌دهد، اهمیت حفاظت از زیرساخت‌ها در سراسر دنیا به یکی از موضوعات محوری در تأمین امنیت اقتصادی و ملی کشورها تبدیل شده است.

زیاده خواهی قدرت‌های بزرگ در منطقه که با بهره‌گیری از جمود فکری برخی از فرقه‌های سیاسی و مذهبی اسلام‌گرا همراه شده، یکی از مهم‌ترین موضوعاتی است که افزون بر تشدید منازعات سیاسی، تنازعات مذهبی را نیز شدت داده است. در این راستا تداوم روند منازعات سیاسی – مذهبی بین کشورها به‌ویژه در موضوع گسترش نفوذ منطقه‌ای، به‌تدریج زمینه‌های لازم برای کنش گری گستره تر جریان‌های تروریستی در قالب حمایت کشورهای متعارض از آن‌ها را به همراه داشته است. در ادامه روند تحولات امنیتی منطقه اکنون این سوال مطرح می‌گردد که با توجه به گسترش وابستگی زیرساخت‌های اساسی کشورهای منطقه (به‌ویژه در حوزه انرژی) به سیستم‌های کنترل صنعتی از یک‌سو و امکان به‌کارگیری تروریست‌های سایبری توسط کشورهای متخاصم در منازعات منطقه‌ای غرب آسیا؛ ماهیت تهدیدات علیه زیرساخت‌های وابسته به سیستم‌های کنترل صنعتی به چه سمتی سوق خواهد یافت؟

در این پژوهش با استفاده از روش توصیفی- تحلیلی استنباط می‌گردد؛ رقابت کشورهای غرب آسیا برای سردمداری در منطقه و هزینه بالای هرگونه تقابل نظامی مستقیم از یک‌سو و وابستگی

فناورانه عمده این کشورها در حوزه زیرساختی و تجهیزاتی به قدرت‌های فرا منطقه‌ای از سوی دیگر؛ موجب گردید با چراغ سبز و وضعیت سکوت و همراهی منفعلانه‌ی قدرت‌های فرا منطقه‌ای، روند حمایت برخی از کشورهای منطقه از جریان‌های تروریستی و به‌کارگیری این جریان‌ها علیه دیگر رقبای منطقه‌ای خویش، گسترش یابد. گستردگی پیامدهای ناشی از خسارت‌های وارده به زیرساخت‌ها در برخی از کشورهای مبتلا به بحران‌های امنیتی – تروریستی و تأثیر منفی آن بر امنیت ملی و به‌ویژه رابطه حکومت با شهروندان به حدی بود که این امر به‌تدریج موجب مطرح گردیدن نوعی آسیب‌پذیری راهبردی دولت‌ها در حوزه زیرساختی و موضوع تداوم اداره کشور گردید. این امر نوعی جذابیت هدف برای کشورهای حامی جریان‌های تروریستی منطقه ایجاد نموده است که پیش‌بینی می‌گردد در طی یک رویکرد نیابتی به انجام اقدامات تروریستی و خرابکارانه علیه مراکز تأثیرگذار زیرساختی کشورهای دیگر روی آورند. این روند موجب پیدایش تهدید جدیدی علیه زیرساخت‌های کشورهای منطقه تحت عنوان "تروریسم نیابتی" خواهد بود که اجرا و پیگیری اهداف آن در بستر سایبری محتمل‌ترین شیوه بوده و در این میان موضوع سیستم‌های کنترل صنعتی غیربومی که در زیرساخت‌های اساسی کشورهای (عمدتاً متکی به صادرات انرژی) جنوب غرب آسیا می‌توانند به حفره‌های امنیت سایبری تلقی گردند، مساعدترین زمینه شکل‌گیری تهدید می‌باشند. این رویکرد همچنین مورد اقبال قدرت‌های فرا منطقه‌ای به‌عنوان اهرمی جهت کسب درآمدهای اقتصادی بیشتر از کشورهای منطقه (بازسازی و ارائه خدمات فنی زیرساختی) به‌موازات یا جایگزین درآمدهای ناشی از فروش تسلیحات خواهد بود. شایان ذکر است وجود اعتراضات مردمی متأثر از شرایط سیاسی- اقتصادی و گسل‌های موجود بین مردم و برخی از حاکمیت‌های منطقه به‌عنوان عامل مساعدی است که امکان تقرب جریان‌های تروریستی به سمت گروه‌های معترض و معاند داخلی به‌منظور دسترسی راحت‌تر و انجام اقدامات خرابکارانه و تروریستی در زیرساخت‌ها را تسهیل خواهد نمود.

همان‌گونه که ملاحظه می‌گردد این پژوهش تنها به بررسی ابعاد فنی و یا بررسی موضوع در بستر مطالعات منطقه‌ای و مباحث دفاعی نپرداخته و با طرح ابعاد مختلف موضوع تلاش دارد احتمال وقوع این تهدید نوپدید را به مسئولین در رده‌های کشوری و لشکری گوش زد نماید.

مبانی نظری

زیرساخت‌ها

زیرساخت‌ها سرمایه‌های ملّی هستند که معمولاً برای احداث و توسعه آن‌ها مبالغ سنگینی صرف شده و برای آنکه این هزینه‌ها بازده مناسب را در اقتصاد کشور نشان دهند، زیرساخت موردنظر باید بتواند باقابلیت اطمینان بالایی برای تولید کالا یا ارائه خدمت، در شرایط عادی و اضطراری در دسترس باشد؛ از سوی دیگر به دلیل پیوستگی، تعامل و وابستگی بین زیرساخت‌های مختلف، اختلال یا انحراف در عملکرد یکی می‌تواند منجر به ایجاد جریانی از انحراف‌ها یا شکست‌ها در سایر زیرساخت‌ها شده؛ درنهایت عوارض نامطلوب زیادی در اقتصاد، بهداشت، ایمنی یا امنیت کشور برجای گذارد.

کمیسیون حفاظت از زیرساخت‌های بحرانی آمریکا[1] زیرساخت را چنین تعریف می‌کند: شبکه‌ای از سیستم‌ها و فرآیندهای مستقل و ساخته دست بشر که به‌صورت مشارکتی و سینرژیک زیرساخت‌هایی که برای تولید و توزیع جریان پیوسته‌ای از کالاها و خدمات ضروری عمل می‌کنند. از نظر این کمسیون، کمبود ظرفیت یا تخریب آن‌ها بر امنیت اقتصادی و سیاسی تأثیر مخرب دارند و عبارت‌اند از: ارتباطات مخابراتی، سیستم‌های مربوط به نیروی برق، نفت و گاز طبیعی، خدمات بانکداری و مالی، حمل‌ونقل، سیستم‌های تأمین آب، خدمات دولتی و خدمات اضطراری (Rinaldi et al, 2001: 12).

مفاهیم سیستم‌های کنترل صنعتی

سیستم‌های کنترل صنعتی که وظیفه هدایت و کنترل فرآیندهای فیزیکی را عهده‌دار هستند متشکل از مجموعه‌ای از حسگرها عملگرها و واحدهای پردازش داده مانند کنترل‌کننده‌هایی باقابلیت برنامه‌ریزی هستند که شبکه‌های ارتباطی آن‌ها را به مراکز اصلی مرتبط می‌سازند سیستم‌های کنترل صنعتی در واقع شامل:

PLC: به معنای کنترل کننده‌های منطقی برنامه پذیر است که از قسمت ورودی خود اطلاعات فرایند را دریافت و آن‌ها را بر طبق برنامه‌هایی که در حافظه ذخیره شده پردازش کرده و نتیجه عملیات را از قسمت خروجی به‌صورت دستورها و فرامین کنترلی به گیرنده و اجرا کننده‌های

1. president's commission on critical infrastructure protection

فرمان ارسال می‌نماید درگذشته این کار را مدارها و رله‌های فرمان انجام می‌دادند آسیب‌پذیری‌های plcها از سال ۲۰۱۰ شروع شده است (ICS-ALERT:2011).

DCS: سامانه کنترل dcs متشکل از چندینplc و تجهیزات فیلم از جمله حسگرها و شیرها و غیره و می‌باشد که این تجهیزات از طریق شبکه‌های صنعتی باهم در ارتباط می‌باشند (ICS-ALERT:2011).

SCADA: نوع دیگری از سامانه‌های کنترل صنعتی است که نسبت بهdcs پا را فراتر گذاشته و در یک مقیاس بزرگ‌تر مورد استفاده قرار می‌گیرد در واقع این سامانه نه تنها بخش‌های کنترل و ارتباطات شبکه‌ای را در سطح کنترل و فیلم پوشش می‌دهد بلکه دارای سطوح کنترل و پایش فرآیندهای صنعتی از راه دور به مسافت چند کیلومتری و در برخی موارد چند صد کیلومتری می‌باشند (Developer Works Security Editors: 2015).

تجهیزات شبکه‌ای مانند مسیریاب‌ها و سوئیچ‌ها: علاوه بر موارد فوق مسیریاب‌ها و سوئیچ‌ها از جمله تجهیزاتی هستند که در صنعت کنترل بسیار از آن‌ها استفاده می‌شود که اخیراً گزارش‌های مبنی بر آسیب‌پذیر بودن این تجهیزات نیز گزارش‌شده است.

از آنجا که امروز سیستم‌های کنترل صنعتی به‌طور وسیع با سیستم‌های حوزه فناوری اطلاعات پیوستگی دارند تمامی آسیب‌هایی که تجهیزات ارتباطی را تهدید می‌کنند تهدیدی برای سیستم‌های کنترل صنعتی نیز محسوب می‌شود با توجه به پیشرفته‌ای روز افزون در سیستم‌های کنترل صنعتی و استفاده آن‌ها از نرم‌افزار و سخت‌افزارهای شبکه‌ای یکسان و دارای استاندارد واحد، دسترسی افراد غیرمجاز به لایه‌های درونی این سیستم‌ها امکان‌پذیر شده است به‌طور کل یک هکر که قصد هک کردن یک سیستم کنترل صنعتی را دارد با دو چالش بسیار مهم روبرو می‌شود:

- شناخت از سیستم نفوذ و دسترسی به آن
- در دست گرفتن کنترل کامل و یا قسمتی از فرآیند کنترلی برای ایجاد درخت آب و ضربه به سیستم

مفاهیم امنیت سایبری

برای امنیت سایبری مفهومی به غیر از فقدان ناامنی یا امنیت کامل در فضای مجازی را نمی‌توان بیان کرد اما در خصوص فضای سایبری و چیستی فضای سایبری متأسفانه تاکنون تعریفی کامل که شامل کلیات این فضا باشد ارائه نشده است از مجموع نظرات می‌توان چنین استنباط نمود که

شبکه‌ای متصل به هم از زیرساخت‌های فناوری اطلاعات اعم از اینترنت، شبکه‌های مخابراتی، شبکه‌های کامپیوتری، پردازشگرها و کنترل‌گرهای داخلی صنایع مهم را شامل می‌شود. در سند سیاست‌های فضای سایبری آمریکا در سال ۲۰۰۹ این فضا به‌عنوان زیرساخت جهانی و متصل به هم ارتباطات و اطلاعات دیجیتال که تقریباً زیربنای تمامی وجوه جوامع مدرن را تشکیل می‌دهد تعریف شده است به‌طور کلی از فضای سایبری به‌عنوان محیطی برای انتقال داده‌ها و اطلاعات یاد می‌شود و تنها شامل اینترنت نمی‌شود بلکه شامل تمام شبکه‌ها و سیستم‌های ارتباطی و اطلاعاتی می‌باشد امنیت سایبری باید شامل سه عنصر بنیادی به شرح زیر باشد:

- محرمانگی به این معنا که اگر داده‌هایی که در فضای سایبری در حال انتقال هستند توسط مهاجم این خوانده شوند و مهربان بودن آن نقش شود.
- یکپارچگی اگر در حین انتقال داده ها در فضای سایبری اطلاعات توسط مهاجرین دستگاهی شده و تغییر داده شوند.
- در دسترس بودن این نوع حملات با هدف خارج کردن منبع اطلاعاتی از سرویس به گونه‌ای که دیگر آن منبع قادر به ارائه سرویس به دیگران نبوده و نه توان تبادل اطلاعات درستی با کاربرانش داشته باشد انجام می‌شود.

مراکز دیسپاچینگ

گستردگی زیرساختی اعم از فرایند تولید و استحصال، انتقال و توزیع و نیز اهمیت دقت در کنترل میزان تولید و توزیع و مبادلات استفاده از سیستم دیسپاچینگ را بیش از پیش ضروری می‌کند با در اختیار داشتن چنین سیستم‌هایی می‌توان به آسانی و با سرعت و قابلیت اطمینان بالا همه عملیات لازم از قبیل نمایش و انتقال اطلاعات تشخیص مؤثر و ردیابی خطاهای به وجود آمده را بررسی و کنترل نمود. امروزه دیسپچینگ الزامی حیاتی برای نظارت بهتر و مدیریت کارآمد می‌باشد و دسترسی به اطلاعات دقیق سریع و کافی از همه بخش‌های تولید انتقال توزیع و مصرف و با بهره‌گیری از نرم‌افزارهای تحلیلی برای پردازش اطلاعات اتخاذ تصمیمات مدیریتی در سطوح مختلف را با دقت و سرعت بالا انجام‌پذیر خواهد کرد و نه تنها ابزاری مؤثر در مدیریت خدمات به وجود آمده در سیستم و اصلاح به‌موقع آن است بلکه با استفاده از آن می‌توان به برنامه‌ریزی بهینه در تولید کاهش تلفات شناسایی منابع هدر رفتگی و توازن در عرصه و تقاضا دست یافت.

قابلیت تهیه و نگهداری گزارش‌های دقیق و جامع عملکردی از سیستم و محاسبات دقیق مبادلات انجام شده از دیگر مزایای استفاده از اسکادا می‌باشد.

یک سامانه دیسپچینگ معمولاً بخش‌های اصلی زیر را شامل می‌شود:

- پایانه راه دور (RTU): وظیفه جمع‌آوری اطلاعات دیجیتال و آنالوگ از نقاط مختلف شبکه و ارسال آن به مرکز دیسپاچینگ را برعهده دارد
- مرکز دیسپاچینگ: یک سیستم چند لایه‌ای سلسله مراتبی باقابلیت تعریف میزان دسترسی‌ها است که وظیفه پردازش نمایش و بایگانی اطلاعات از پایانه‌های راه دور و ارسال فرم آن را در صورت نیاز به رابطه دارد علاوه بر مرکز دیسپچینگ اصلی مراکز دیگری از قبیل مراکز استانی مراکز عملیاتی مراکز میانی و غیره می‌توانند سلسله مراتبی باشند و عملیات فیلترینگ اطلاعات یا استفاده و تصمیم‌گیری در آن ساعت را فراهم کنند در بیشتر مراکز دیسپاچینگ مرکز دیگری (Hot Redundant) به‌صورت یدکی دائمی همه جوانب با مرکز اصلی باربری می‌کند و به‌طور موازی در محل جغرافیایی دیگری است که وظیفه پشتیبانی مرکز اصلی را بر عهده دارد و در صورت بروز مشکلات فنی و خروج از سیستم مرکز اصلی نقش جایگزین را ایفا می‌کند.
- کانال‌های مخابراتی یکی از اجزای مهم سیستم‌های دیسپاچینگ زیرساخت‌های مخابراتی برای برقراری ارتباط است که بدون چنین بسترهای امکان‌پذیر نیست و اتصال‌ها، RTUهیچ‌کدام از اجزای سیستم اعم از مراکز عملیاتی واحدهای بهره‌برداری و مرکز اصلی ممکن نخواهد بود.
- نرم‌افزارهای کاربردی برای شبیه‌سازی تحلیل شبکه محاسبات و پردازش داده پیش‌بینی پارامترهای شبکه و تقویت قدرت تصمیم‌گیری و گزارش‌گیری به نرم‌افزار کاربردی قوی نیاز است تا ضمن ارتباط با نرم‌افزار اسکادا موارد اضافی زیر را نیز به خوبی به انجام رساند:
  - ✓ محاسبه ذخایر در صورت قابل ذخیره بودن مورد کنترل
  - ✓ شبیه‌سازی لحظه‌ای پارامترهای خطوط نفت و گاز اعم از فشار دما ترکیبات سیال و غیره
  - ✓ بررسی موازنه
  - ✓ بهینه‌سازی عملیات ارسال و توزیع
  - ✓ تحلیل پارامترهای کیفی و شبیه‌سازی عملیاتی که قرار است در آینده انجام شود.

سیستم‌های کنترل صنعتی

بسیاری از اتفاق‌های ناشی از خرابی‌های غیرعمدی ممکن است عملکرد عادی سیستم‌های کنترل صنعتی را تحت تأثیر قرار دهند بااین‌حال بزرگ‌ترین تهدید برای سیستم‌های کنترل صنعتی خرابی‌های عمده هدف‌دار است که درگذشته به‌صورت حمله فیزیکی و اجزای سیستم کنترل صورت می‌پذیرفت و هدف آن‌ها مختل کردن عملکرد سیستم بود حملات سایبری تکامل طبیعی برای این نوع حمل‌ها می‌باشند که برای مهاجمان ارزان‌تر و کم‌خطرتر و تحت اثر فاصله نیستند. در عین حال تکرار و هماهنگی آن‌ها بسیار راحت‌تر است در بین حمله‌های سایبری که تا به حال به سیستم‌های کنترل صنعتی انجام شده است هیچ حمله‌ای به اندازه حمله استاکس‌نت نتوانسته است آشکار کننده اهمیت این نوع تهدیدات برای سیستم‌های کنترل و به تبع آن سیستم‌های صنعتی و زیرساخت‌های حیاتی باشد با مطالعه در خصوص امنیت سایبری می‌توان متوجه کمبود در این زمینه و نیاز هر چه بیشتر به تحقیقات در این زمینه پی برد وضعیت کنونی امنیت سایبری در سیستم‌های کنترل صنعتی ناامیدکننده و قابل قیاس با امنیت سایبری فناوری اطلاعات در ۱۵ سال پیش نیست از سوی دیگر به علت ماهیت متفاوت سیستم‌های کنترل صنعتی و فناوری اطلاعات راه‌حل‌های امنیتی فناوری اطلاعات کفایت نیازهای مربوط در سیستم‌های رل صنعتی را نمی‌دهد که در کل می‌توان گفت فناوری اطلاعات هدف مراقبت از داده ها هست ولی در سیستم‌های فوق هدف مراقبت از عملکرد عادی سیستم و جلوگیری از خرابی‌های احتمالی اندی در آن است به عبارت دیگر در سیستم‌های کنترل صنعتی هدف از امنیت سیستم حفظ عملکرد اجزا به‌طور صحیح می‌باشد به‌طوری که کل سیستم بتواند به خوبی ایمنی کامل وظایف محوله را انجام بدهند کارهای انجام شده در این حوزه به نظر کافی نبوده و نیاز به توجه بسیار زیادی را می‌طلبد از آنجا که کشور ایران از دیرباز در منطقه و جهان از موقعیت استراتژیکی برخوردار است همیشه مورد تهاجم دولت‌های گوناگون قرار داشته است با تغییر رویکردهای بشر به سمت به سمت فناوری‌های اطلاعات حرکت انسان به سوی فناوری نوین در فضای مجازی تغییر مسیر یافته است در ماهیت حملات نیز تغییرات الگوی نموده است به اعتقاد بسیاری از متخصصین امروزه جنگ سایبری از مهم‌ترین انواع تهدیدات به شمار می‌رود.

حملات صورت گرفته بر روی سیستم‌های کنترل صنعتی در سال‌های اخیر نشان از قابلیت نفوذ در این سیستم‌ها دارد در زیر به برخی از این حملات اشاره شده است:

- حمله به ترافیک ارتباطات هوایی در ماساچوست آمریکا ۱۹۹۱
- حمله به خطوط لوله بنزین واشینگتن آمریکا ۱۹۹۶
- حمله به سیستم‌های کنترل فاضلاب استرالیا ۲۰۰۰
- حمله به خطوط لوله گاز روسیه ۲۰۰۰
- حمله به سیستم سیگنال ارتباطی قطار ساحل شرقی آمریکا با ویروس so big
- به نیروگاه هسته‌ای اوهایو آمریکا با کرم slammer
- حمله به نیروگاه برق شمال شرقی آمریکا و کانادا ۲۰۰۵
- حمله به کارخانه‌های ماشین‌سازی کاترپیلار و هواپیماسازی بوئینگ با کرم ۲۰۰۸
- حمله به نیروگاه هسته‌ای و خاموشی آن در گرجستان ۲۰۰۹
- حمله به نیروگاه هسته‌ای بوشهر با کرم استاکس نت در ایران ۲۰۱۰

در بخش بعدی مقاله در نظر داریم پس از پرداختن به مفاهیم اولیه در خصوص سیستم‌های کنترل صنعتی و امنیت سایبری و مراکز دیسپاچینگ به موضوع آسیب‌پذیر بودن سیستم‌های کنترل صنعتی اشاره کنیم و بعد از بررسی روش‌های حمله سایبری به موضوع امن سازی فضای سایبری و روش‌های مقابله با حمله‌های مرسوم اشاره نموده درنهایت تهدیداتی را که احتمالاً برای مراکز دیسپاچینگ به‌عنوان حمله سایبری صورت می‌گیرد را بررسی و جمع‌بندی و روش‌های مقابله با آن‌ها نیز مورد مطالعه قرار خواهد گرفت

جنگ‌های نیابتی

این نوع جنگ، کشمکشی میان دو کشور است که هیچ یک از آن‌ها خود را به‌طور مستقیم دخیل نمی‌کند. در این جنگ، قدرت‌های مخالف، از یک نیروی ثالث (بازیگران دولتی یا غیردولتی خشونت طلب و سربازان مزدور) به‌عنوان دست نشانده استفاده می‌کنند. البته تلاش می‌شود گستره به کارگیری این گروه‌ها در اندازه‌ای باشد که جنگ تمام عیار منجر نشود. همچنین جنگ‌های نیابتی می‌توانند در کنار جنگ‌های تمام عیار رخ دهند. تقریباً غیرممکن است که یک جنگ کاملاً نیابتی باشد زیرا گروه‌هایی که برای کشور یا کشورهای خاص می‌جنگند، معمولاً منافع خود را پیش می‌برند که می‌تواند با منافع کشور حامی در تضاد باشد. به‌طور نمونه، جنگ‌های نیابتی طی جنگ سرد، منطبق‌ترین ویژگی‌ها را با معیارهای جنگ نیابتی داشتند زیرا به‌موازات ادامه جنگ سرد، این جنگ‌ها در هدایت کشمکش مسلحانه میان حداقل دو دشمن ضروری به نظر می‌رسیدند.

همچنین تشدید جنگ‌های داخلی و مداخله بازیگران دولتی و غیردولتی خارجی در حمایت از یکی از طرف‌ها می‌تواند به جنگ نیابتی تبدیل شود. عبارت جنگ نیابتی یا جنگ از طریق نایب طی دوره جنگ سرد مطرح شود (شیرازی، ۱۳۹٤).

در تبیین نظری جنگ نیابتی باید گفت که جنگ‌های نیابتی بر محور اتحاد بازیگران دولتی با یکدیگر یا حتی اتحاد آن‌ها با بازیگران غیردولتی استوار است؛ لذا باید به بررسی کلی مؤلفه‌های نظریه‌های اتحاد بپردازیم. نظریه‌های اتحاد مبتنی بر رهیافت‌های آرمان‌گرایی و واقع‌گرایی است. رهیافت آرمان‌گرایی نقش ایدئولوژی را در شکل‌گیری اتحادها بسیار مهم ارزیابی می‌کند. در مقابل، رهیافت واقع‌گرایی در بررسی اتحادها بر قدرت کشورها و تهدیدهای خارجی تمرکز دارد.

امروزه نظریه‌های اتحاد با دو گرایش کلی همچنان پویا هستند؛ گرایش نخست اینکه بسیاری از نظریه‌پردازان واقع‌گرا با تأکید بر مفروض‌های پیشین بر این باورند که نظریه‌های اتحاد همچنان به شکل سابق پاسخگو هستند. گرایش دوم نیز در کنار نظریه‌های پیشین اتحاد، بر طیف جدیدی از نظریه‌های ائتلاف موقت تأکید دارند و معتقدند تحولات ناشی از جهانی شدن موجب شده تا در کنار اتحادها به شکل سابق، ائتلاف‌های موقتی نیز شکل بگیرد. به هر حال نظریه‌های اتحاد جدید، بنیان نظریه‌های خود را همچنان بر اساس مفروض‌های واقع‌گرایانه قبلی بنا می‌کنند؛ در حالی که اتحادهای سنتی بیشتر با فاکتورهای نظامی شناخته می‌شوند و در دنیای جدید اهداف سیاسی–اقتصادی در کنار اهداف نظامی مطرح شده‌اند (قوام و ایمانی، ۱۳۹۱: ۳۸–۳۷).

پس از جنگ سرد برخی از اندیشه‌ورزان روابط بین‌الملل این نظریه را مطرح کردند که تحول تاریخی پس از جنگ سرد، بروز کشمکش و تعارض میان جوامع و حکومت‌ها را از بین برده است؛ به عبارت دیگر، با پایان رقابت‌ها و تعارض‌های ایدئولوژیک در جهان، حکومت‌ها و جوامع انسانی دوره‌ای پایدار از صلح لیبرالیستی را تجربه خواهند کرد. در نظر آن‌ها، پایان یافتن رقابت‌های ایدئولوژیک در سطح کلان و سیطره مطلق ایدئولوژی لیبرال سرمایه‌داری در قالب مفهوم جهانی شدن، با تولید هنجارها و ساختارهای مشترکی را در جوامع و حکومت‌های گوناگون در پی خواهد داشت و این مسئله سبب زیر سوال رفتن زیربنای فلسفی رقابت در جهان خواهد شد. در نقطه مقابل، عده‌ای دیگر از متفکران روابط بین‌الملل از جمله واقع‌گرایان و نوواقع‌گرایان با این نظریه مخالفت ورزیده، مفهوم رقابت را در عنصری بنیادین و پایدار در روابط بین حکومت‌ها و قدرت‌ها می‌دانند. نقطه کلیدی نظریه آن‌ها این است که چون در سطح روابط

بین‌الملل قدرت برتر و غایی برای حل تعارض میان حکومت‌ها وجود ندارد (والت، ٦٥:١٩٦٤)، از نگاه ژئوپلیتیک، رقابت نوعی ستیزه گروهی در سطح روابط بین‌الملل است که نیازمند وجود حکومت‌ها، قدرت‌ها و یا سازمان‌های شبیه حکومت است و بسته به شرایط تکامل تاریخی، طی زمان اشکال مختلفی به خود می‌گیرد (ازغدی، ۵۷:۱۳۸۸).

جنگ‌های نیابتی از پایان جنگ جهانی دوم و آغاز جنگ سرد معمول شده و جنبه تعیین‌کننده نبرد جهانی در نیمه دوم قرن بیستم به شمار می‌رفت. این نوع جنگ عمدتاً به دلیل هراس از کشمکش مستقیم امریکا و شوروی و جلوگیری از بروز هولوکاست هسته‌ای بود. این شرایط سبب شد جنگ‌های نیابتی به‌عنوان راهی ظاهراً ایمن‌تر در تداوم دشمنی‌ها به کار گرفته شوند. همچنین دلایل فوری‌تری برای ظهور جنگ نیابتی درصحنه جهانی وجود داشت. شوروی اغلب جنگ‌های نیابتی را به لحاظ اقتصادی کم هزینه‌تر از درگیری مستقیم می‌دید. به علاوه، گسترش رسانه‌ای تلویزیونی و تأثیر آن بر درک عمومی سبب شد مخالفت افکار عمومی امریکا با جنگ و ماجراجویی‌های برون مرزی افزایش یابد.

طی قرن بیستم کشورها به‌طور فزاینده‌ای به جای درگیری نظامی مستقیم، به‌منظور دستیابی به اهداف نظامی یا شبه نظامی خود از گروه‌های نیابتی استفاده کردند. لاومن استدلال می‌کند که به‌منظور درک جنگ‌های نیابتی باید واقع‌گرایی در بافت پارادیم معاصر در نظام بین‌الملل و نیز هزینه‌های بالای مداخله نظامی مستقیم را درک کرد (لاومن، ۲۰۰۲، ٣٦-٣٣).

تهدیدات تروریستی

واژه‌ی ترور[1] از ریشه لاتینی "Terrere"به معنای ترس و ترساندن گرفته شده است و تروریسم در لغت به معنای ترساندن، حکومت ارعاب و تهدید، ایجاد ترس و وحشت در مردم است. تهدیدات تروریستی شامل کلیه‌ی انواع تهدیداتی است که ایجاد احساس ناامنی در میان مردم و مسئولان می‌کند. تهدیدات تروریستی یا امنیتی، ممکن است به‌صورت عینی یا ذهنی تظاهر پیدا کند و منشأ داخلی یا خارجی داشته باشد (شولتز و دیگران، ٢٣٤:١٣٨٦).

بمب‌گذاری، پرتاب مواد منفجره و استفاده از هر نوع اسلحه‌ی گرم و سرد، ترور و آدم ربایی یا گروگان‌گیری، ایجاد رعب و ترس جمعی و واداشتن مردم به ترک محل کار، سکونت یا محل تحصیل و مانند آن از مصادیق تهدیدات تروریستی به شمار می‌رود. این نوع تهدیدات ممکن است

[1] Terror

متوجه جان و مال افراد و یا عوامل توسعه زندگی عادی و فضای آرام زیست و فعالیت بشود و از همین رو مانند تهدیدات نظامی اثرات مستقیم و غیرمستقیمی بر روند توسعه و برنامه‌های توسعه‌ی پایدار و آمایش کشور هدف می‌گذارد.

از جنگ نیابتی تا به‌کارگیری تروریسم

در نگاه نخست، پدیده جنگ نیابتی ممکن است با واقع‌گرایی آشتی‌ناپذیر باشد زیرا واقع‌گرایی به‌طور سنتی رویکردی کاملاً دولت‌محور در قبال نظام بین‌الملل دارد. مطابق نظریه‌های واقع‌گرایی، دولت‌ها مهم‌ترین بازیگران هستند. با وجود این، ارتباطات مدرن و فناوری‌های نظامی بی‌تردید توازن قدرت را به سوی بازیگران غیردولتی کشانده است. به دلیل اینکه دولت‌ها دریافته‌اند که نمی‌توانند بازیگران غیردولتی را نادیده بگیرند، به‌طور فزاینده‌ای آن‌ها را به‌عنوان ابزارهای منافع دولتی انتخاب کرده‌اند.

دولت‌ها به دلیل وجود رقابت‌های میان خود ترغیب می‌شوند از تروریسم به‌عنوان ابزاری برای ارتقای قدرت در نظام بین‌الملل استفاده کنند؛ بدون اینکه خطرات جنگ به‌عنوان سایر اشکال مداخله نظامی را تجربه کنند (کنراد، ۵۳۱:۲۰۱۱).

اگرچه حمایت دولتی از تروریسم احتمالاً مورد پسندترین روش دخیل شدن در جنگ‌های نیابتی است، اما این پدیده به‌طور چشمگیری به گسترش افراط گرایی اسلامی در دوره پس از جنگ سرد باز می‌گردد. طی جنگ سرد، امریکا و شوروی با ارائه شکل‌های مختلف کمک به طرف‌های رقیب مانند جنگ‌های اعراب و اسرائیل وارد جنگ‌های نیابتی شدند (بار، سیمون، تاو، ۲٦۳:۱۹۸٤).

تروریسم ابزاری برای گسترش نفوذ

اصولاً جنگ‌های نیابتی به‌منظور کسب و گسترش نفوذ در یک حوزه رقابتی مشترک صورت می‌گیرد.

منافع ایدئولوژیک، ژئوپلیتیک، ژئواستراتژیک و ژئواکونومیک می‌توانند بنیان‌های انگیزشی جنگ‌های نیابتی را شکل دهند. رقابت در سه حوزه ژئوپلیتیک، ژئوایدئولوژیک و ژئواکونومیک شکل می‌گیرد. در تمام این سه حوزه، جغرافیا بنیان رقابت را تشکیل می‌دهد که در آن‌ها بر سر سیاست ایدئولوژی و اقتصاد رقابت صورت می‌پذیرد. در این میان، بازیگران غیردولتی یا دولتی می‌توانند به‌عنوان نایب در این رقابت‌ها نقش آفرینی و شرایط را برای آغاز جنگ نیابتی فراهم کنند.

ژئوپلیتیک که به بررسی تصمیمات سیاسی بر محیط جغرافیایی می‌پردازد، عاملی محوری در روند جنگ‌های نیابتی است. ژئوایدئولوژی نیز به بررسی تأثیرگذاری ایدئولوژی (اعم از مذهبی و غیرمذهبی) بر محیط جغرافیایی و افزایش اهمیت راهبردی آن برای رقبا در محیط جغرافیایی می‌پردازد. در عین حال، ژئواکونومی به بررسی تأثیرگذاری اقتصاد (از جمله اقتصاد انرژی) بر محیط جغرافیایی و افزایش اهمیت راهبردی آن برای رقبا در آن محیط جغرافیایی می‌پردازد. به نظر می‌رسد حوزه ژئوایدئولوژیک جدی‌ترین و تهدیدآمیزترین حوزه رقابت باشد که می‌تواند رقابت را به سه حوزه دیگر نیز سرایت دهد. به‌ویژه آنکه رقابت در این حوزه می‌تواند به بنیادگرایی مذهبی و در نوع شدید آن به تروریسم مذهبی منجر شود.

تروریسم نیابتی

چنانچه طرف‌های متخاصم باانگیزه‌های خاص (به‌ویژه ژئوایدئولوژیک) تلاش کنند علاوه بر ژئوپلیتیک پیرامونی خود؛ دایره این کنش و رقابت را به حوزه سرزمینی حریف منتقل و بازی را با محوریت به‌کارگیری جریان‌های تروریستی پیش ببرند و موجبات ایجاد بحران امنیتی و فرسایش توان دفاعی، سیاسی، اقتصادی، اجتماعی و ایدئولوژیک کشور مقابل را فراهم آورند، این رویکرد را می‌توان تروریسم نیابتی نامید.

سایبر تروریسم

با اینکه اصطلاح سایبر تروریسم را به‌عنوان نوع جدید و متمایزی از تروریسم به کار می‌برند، اما صحیح‌تر آن است که آن را یک تاکتیک جدید تروریستی بدانیم. سایبر تروریسم همان‌گونه که از عنوان آن پیداست، نوعی تروریسم است که در آن از یک مؤلفه رایانه‌ای استفاده می‌شود؛ از این لحاظ، سایبر تروریسم اساساً مانند دیگر اشکال تروریسم است. با این همه سایبر تروریسم از این جهت که موجودیت آن وابستگی تامی را با رایانه دارد، با دیگر تاکتیک‌های تروریستی متفاوت است.

بری کالینز که گفته می‌شود، اصطلاح سایبر تروریسم را وی ابداع کرده است، آن را این‌گونه تعریف کرده است؛ سوء استفاده عمومی از یک سیستم، شبکه یا مؤلفه اطلاعاتی رایانه‌ای، برای تحقق هدفی که مؤید یا تسهیل کننده مبارزه یا اقدام تروریستی است.

راداستارک نیز ضمن توجه به بعد رایانه‌ای ونیز بعد متعارف سایبر تروریسم، در تعریف آن می‌گوید: سایبر تروریسم عبارت است از استفاده هدفمند یا تهدید به استفاده از جنگ رایانه‌ای، یا توسل به خشونت بر ضد اهداف رایانه‌ای، باانگیزه‌های سیاسی، اجتماعی، اقتصادی یا مذهبی از

سوی گروه‌های غیردولتی یا گروه‌های تحت هدایت و حمایت دولت، به‌منظور ایجاد ترس و نگرانی و وحشت در جمعیت موردنظر و آسیب رساندن به دارایی‌ها و اموال نظامی و غیرنظامی.

وی توضیح می‌دهد که آنچه ماهیت سایبر تروریسم را تعیین می‌کند، هدف موردنظر است؛ به عبارت دیگر، سایبر تروریسم هرگونه حمله‌ای را که بر ضد سیستم‌های اطلاعاتی انجام شود، در بر می‌گیرد و لازم نیست حتماً برای انجام آن از رایانه استفاده شود. به‌طور کلی ما ترجیح می‌دهیم، سایبر تروریسم را هرگونه عمل تروریستی بدانیم که در آن از سیستم‌های اطلاعاتی یا فناوری دیجیتالی «رایانه‌ها با شبکه‌های رایانه‌ای» چه به‌عنوان ابزار حمله و چه به‌عنوان آماج حمله استفاده می‌شود؛ در اینجا نیز با افزودن قیدهایی می‌توان سایبر تروریسم را در قالب‌های مشخص‌تری قرار داد. ممکن است سایبر تروریسم ملی، بین‌المللی، دولتی یا سیاسی باشد، اما در هر حال، هسته مرکزی آن‌که همان آمیختگی عمل تروریستی با رایانه‌ها است، یکی است.

گذشته از دو اصطلاح جنگ رایانه‌ای و جنگ شبکه‌ای که برای توصیف منازعه رایانه‌ای مورد استفاده قرار می‌گیرد، مفهوم دیگری تحت عنوان جنگ اطلاعاتی وجود دارد که تحلیل گران نظامی درباره آن به بحث پرداخته‌اند؛ تعاریفی که از این مفهوم ارائه شده است، از عبارت ساده غلبه اطلاعاتی در جنگ شروع و به تعاریف پیچیده‌تری چون» اقداماتی که با هدف کسب برتری اطلاعاتی از طریق تأثیرگذاری بر اطلاعات و فرایندهای اطلاعات پایه و سیستم‌های اطلاعاتی و شبکه‌های رایانمند حریف، هم‌زمان با افزایش توانمندی‌های اطلاعاتی خود صورت می‌گیرد (مطابق تعریف وزارت دفاع امریکا) و نیز حمله عمدی... و سیستماتیک بر ضد فعالیت‌های اطلاعاتی حیاتی [دشمن] به‌منظور بهره‌برداری، تغییر یا تحریف و تخریب اطلاعات یا جلوگیری از ارائه خدمات (مطابق تعریف وزارت دفاع بریتانیا) ختم می‌شود. مطابق این سناریو، سایبر تروریسم نوعی جنگ اطلاعاتی است که توسط گروه‌های فرو دولتی دارای انگیزه‌های سیاسی، همانند گروه ارتش جمهوری خواه ایرلند، انجام می‌شود.

سرانجام، چنان‌که تیموتی ال سانز، در کتاب شناسی جنگ در عصر اطلاعات می‌نویسد: واژه‌هایی چون جنگ رایانه‌ای، جنگ اطلاعاتی، جنگ اطلاعات پایه، سایبر تروریسم، جنگ شبکه‌ای، شورشیان رایانه‌ای، جنگجویان اطلاعاتی (دیجیتالی)، سیطره اطلاعاتی، دفاع در فضای اطلاعاتی و آشفتگی اطلاعاتی، تنها بخش کوچکی از اصطلاحات نوظهوری را تشکیل می‌دهد که نماینده ادبیاتی است که با مبحث گسترده جنگ در عصر اطلاعات سروکار دارد.

در اینجا لازم است به دو مؤلفه اصلی سایبر تروریسم نگاهی بیندازیم؛ این دو مؤلفه عبارت است از:

۱- استفاده تروریست‌ها از رایانه برای انجام فعالیت‌های غیر خشونت‌آمیزی که اگرچه با تروریسم فاصله دارند، ولی آن را تسهیل می‌نمایند.

۲- فعالیت‌های تروریستی که در آن‌ها فناوری رایانه، یکی از اجزای مشخص حمله تروریستی (خواه به‌عنوان سلاح مورد استفاده یا هدف مورد حمله) است.

تهدیدات تروریستی و مراکز آسیب‌پذیر زیرساختی

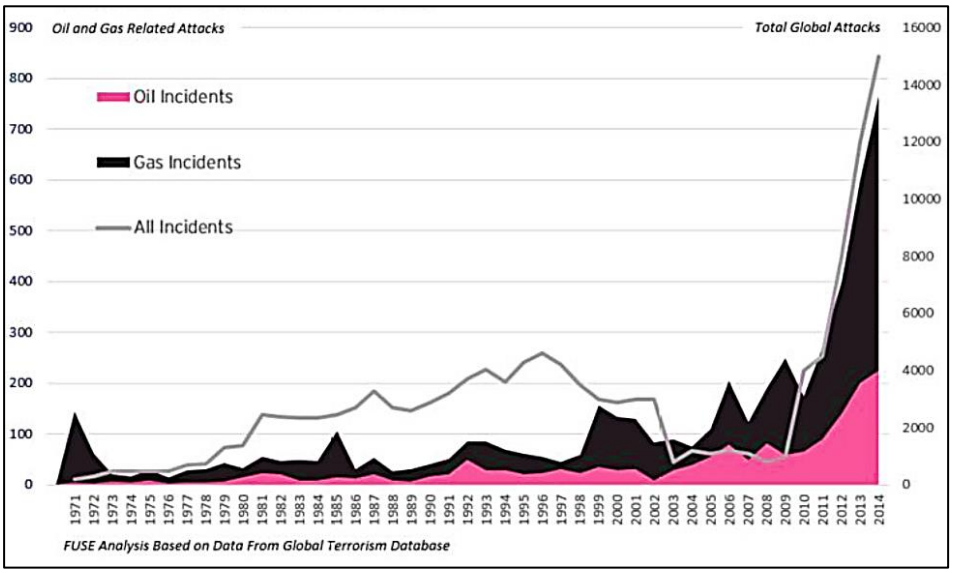
یکی از مباحث اساسی در تروریسم نوین عبارت است از عملیات تروریستی و خرابکارانه علیه مناطق و مراکز حساس، حیاتی و تأسیسات زیربنایی آسیب‌پذیر (طیب، ۱۳۹۲:۳۳).

این مراکز و تأسیسات که عمدتاً وابسته به سیستم‌های مرکزی تکنولوژی اطلاعاتی هستند، شامل مراکز جمعیتی، مراکز مخابراتی، تأسیسات تأمین انرژی، برق، آب، کارخانه‌های مواد غذایی، سیستم حمل و نقل و ... هستند. به همین خاطر تمرکز اقدامات تروریستی روی این نوع شبکه‌ها افزایش یافته است (افتخاری، ۱۳۸۱:۳۱۲).

مراکز علمی مختلفی در سراسر جهان به تعیین مصداق‌های زیرساخت‌ها و مراکز حیاتی و حساس پرداخته‌اند. ازجمله‌ی این مراکز کمیسیون ریاست جمهوری آمریکاست که برای حفاظت از زیرساخت‌های حیاتی با بررسی کارشناسانه‌ی این موضوع، ده هدف اساسی را در قالب زیرساخت‌های حیاتی و مراکز حساس تعیین کرده است. این زیرساخت‌ها و مراکز حیاتی و حساس عبارت‌اند از: زیرساخت‌های حمل و نقل، تولید و انباشت نفت و گاز، تأمین آب، خدمات اضطراری، مالی و بانکداری، نیروی برق، اطلاعات و ارتباطات، خدمات دولتی، زیرساخت‌های دفاعی و مردم. این زیرساخت‌ها خدمات لازم برای تأمین رفاه و زندگی مردم یک کشور را فراهم کرده، اموری از قبیل کنترل تأسیسات، هوا، فضای غیرنظامی تا هماهنگی خدمات امداد محلی و حفظ سیستم تجارت و بانکداری را شامل می‌شوند (مکنزی، ۱۳۸۲:۱۰۶).

القاعده و وابستگان آن، امکانات و کارکنان شرکت‌های نفتی در الجزایر، عراق، کویت، پاکستان، عربستان سعودی و یمن را مورد حمله قرار داده و میدان‌های نفتی متعددی را درگیر نمودند. (Report of the SG the threat posed by ISIL, 2016). گرچه بعضی از مؤلفان خاطرنشان می‌کنند که بخش انرژی تنها سهم کوچکی از حملات تروریستی را جذب می‌کند، اما روندها نشان می‌دهد

که علاقه تروریست‌ها به نفت و گاز افزایش چشمگیری یافته است (Brookings, 2016). (شکل ۱).



شکل ۱– حملات انجام شده علیه زیرساخت‌های نفت و گاز در جهان (CTED TRENDS REPORT, 2017)

مراکز پرجمعیت، کارخانه‌های مواد شیمیایی، تأسیسات انرژی، تأسیسات اتمی، صنایع غذایی، تأسیسات برق، منابع آب، از جمله اهداف مهم این گروه‌های تروریستی در حمله به مراکز حساس و حیاتی به شمار می‌روند (شاه حسینی، ۲۲:۱۳۸۸).

گزارش‌های متعدد نشان می‌دهد که در سال‌های اخیر مهم‌ترین علمیات تروریستی علیه تأسیسات زیربنایی شامل: عملیات علیه مراکز و تأسیسات راه آهن، ربودن هواپیما و کشتی، اتوبوس و ایستگاه‌های اتوبوس، تأسیسات انرژی و خطوط نفتی و فرودگاه بوده است (طیب، ۳۳:۱۳۸۲).

مطالب بالا نشان می‌دهد که اقدامات تروریستی علیه زیرساخت‌ها و مراکز حیاتی و حساس در سال‌های اخیر به یک موضوع وسوسه انگیز برای گروه‌های تروریستی تبدیل شده است. چه این‌که سازمان‌های تروریستی با انجام اقدامات تروریستی علیه مراکز حیاتی و حساس به دلیل وحشت عمومی که ایجاد می‌کند، به سرعت رسانه‌ای شده و در صدر اخبار جهان قرار می‌گیرند و ضمن مطرح کردن خود و مواضع‌شان در سطح رسانه‌ای می‌توانند از جذب حمایت‌های مالی و معنوی از جانب کشورهای رقیب و متخاصم کشور هدف برخوردار شوند.

تهدیدات سایبری در سیستم‌های کنترل صنعتی و اسکادا

با توجه به اطلاعات به دست آمده از پایگاه داده آسیب‌پذیری‌ها (OSVDB) مشخص است که ۸۵٪ آسیب‌پذیری‌های زیرساخت‌های کنترل صنعتی از سال ۲۰۱۱ به بعد کشف شده‌اند. یعنی درست بعد از کشف بدافزار استاکس نت. پایگاه داده (OSVDB) تا به اکنون مجموع ۱۰٦۹ را ثبت نموده است. با توجه به شکل زیر متوجه خواهیم شد که ۳۳٪ آسیب‌پذیری‌ها مبهم هستند و نصف بیشتر آن‌ها در پنج ساله اخیر شناسایی شده‌اند. اکنون زمان آن رسیده است که به اجرای برنامه‌های امنیتی در راستای امن‌سازی زیرساخت‌های کنترل صنعتی و اسکادا تحقق بخشیم و نگرشی عمیق به این مهم داشته باشیم. با توجه به مطالب عنوان شده، مشخص است که با نزدیک شدن مرز بین سیستم‌های کنترل صنعتی و فناوری اطلاعات، این سیستم‌ها آسیب‌پذیرتر خواهند شد. با نگاهی به شکل آماری زیر می‌توان پی به این مهم برد که بسیاری از حملات اتفاق افتاده در زیرساخت‌های صنعتی از جنس همان حملات زیرساخت‌های فناوری اطلاعات می‌باشد اما بنا به ماهیت این سیستم‌ها، تأثیر حملات سایبری بر روی این زیرساخت‌ها به مراتب هزینه بیشتری را برای کشور در بر دارد.

مخاطرات و تهدیدات امنیتی با گذشت زمان ابعاد گسترده و پیچیده‌تری پیدا می‌کند. از این رو امنیت اطلاعات به‌عنوان یک چرخه منظم در مهار و به حداقل رساندن این مخاطرات مورد توجه است. امروزه اتکا به تنها یک راه‌کار یا ابزار امنیتی به‌منظور تأمین امنیت و حریم شخصی اطلاعات سازمان‌ها کافی به نظر نمی‌رسد. بنا بر گزارش دیوان بازرسی ایالات متحده امریکا با وجود اینکه ۹۸٪ سازمان‌های دولتی از دیوارآتش استفاده می‌کنند، اما بیش از ٥٦٪ آن‌ها موارد دسترسی غیرمجاز به شبکه را گزارش داده‌اند. آموزش و ایجاد فرهنگ امنیت در سیستم‌های اسکادا و زیرساخت‌های کنترل صنعتی به‌منظور پوشش ضعف‌ها برای مقابله با تهدیدات نوین از جمله مواردی است که ضرورتی است. کشورهایی که ساز و کار مناسبی برای اطلاع رسانی، آموزش و تولید دانش امنیت دارند، آمادگی بهتری را در مقابله و کنترل تهدیدات سایبری از خود نشان می‌دهند.

زیرساخت‌های نیازمند سیستم‌های کنترل صنعتی و اسکادا

سیستم‌های کنترل صنعتی و اسکادا، بیشترین کاربرد را در سیستم‌هایی دارد که در گستره وسیعی پخش شده‌اند، کنترل و مانیتورینگ نسبتاً ساده‌ای دارند و نیازمند عملیات متناوب و غیرمتناوب

می‌باشند. گستردگی کاربرد ICS/SCADA در تأسیسات مختلف، بیانگر نیازمندی این صنایع به آن است؛ در مثال‌های زیر نمونه‌ای از تأسیسات گوناگون که ICS/SCADA برطرف کننده نیاز آن‌هاست، آورده شده‌اند:

- نیروگاه‌های برق، شبکه‌های انتقال و توزیع
- تأسیسات استخراج نفت خام و گاز و سایر سیالات
- خطوط انتقال و ایستگاه‌های توزیع مشتقات نفت و مواد شیمیایی و پتروشیمی
- سدها و آب‌بندها
- زیرساخت‌های آب و فاضلاب
- زیرساخت‌های حمل و نقل
- کارخانه‌ها و مراکز صنعتی مهم کشور، مانند صنایع خودرو، صنایع دفاعی و...
- زیرساخت‌های انرژی هسته‌ای و زباله‌های اتمی

پیامدهای گسترده؛ جاذبه اصلی برای تروریسم سایبری در حمله به سیستم‌های کنترل صنعتی

وابستگی گسترده طیف وسیعی از زیرساخت‌ها در منطقه جنوب غرب آسیا به سیستم‌های (اکثراً غیربومی) کنترل صنعتی به‌ویژه در حوزه انرژی (که اساسی‌ترین زیرساخت درآمدزای این کشورهای صادر کننده انرژی) باعث گردیده که این امر از یک‌سو دارای جذابیت خاصی در منظر تروریست‌های سایبری ایجاد نماید و از سوی دیگر در فضای تقابلی و جنگ نیابتی کنونی حاکم بر منطقه؛ می‌تواند مورد توجه سیاست مداران و استراتژیست‌های کشورهای متخاصم قرار گیرد که در چنین حالتی، به‌کارگیری و استخدام گروه‌های تروریستی سایبری امری بدیهی با کمترین بازخورد منفی برای کشور متخاصم خواهد بود.

نتیجه‌گیری

منطقه غرب آسیا طی چند سال اخیر و به‌طور مشخص، بعد از حادثه ۱۱ سپتامبر ۲۰۰۱ با چالش‌ها و ناامنی‌هایی مواجه شده است. بازیگر جدید عرصه سیاست بین‌الملل؛ جریان‌ها و گروه‌های تروریستی می‌باشند که نتایج آثار عملکردهای آن‌ها به‌طور گسترده در حافظه عمومی ملت‌ها و به‌ویژه مردم منطقه به جای مانده است. تداوم روند منازعات سیاسی – مذهبی بین کشورها به‌ویژه در موضوع گسترش نفوذ منطقه‌ای، به‌تدریج زمینه‌های لازم برای کنش گری گستره تر جریان‌های تروریستی در قالب حمایت کشورهای متعارض از آن‌ها را به همراه داشته است.

تروریسم نیابتی از جدی‌ترین تهدیدات منطقه می‌باشد که تصاویر تهدید و یا هراس‌آمیز از این نوع تروریسم در آینده چندان شفاف نیست. تحولات سیاسی منطقه در ابعاد مختلف موضوع تروریسم را بغرنج نموده و این وضع باعث شده که نتوان نظریه‌ای مطمئن در خصوص وجود تروریسم، انواع آن و میزان خطرات احتمالی تروریسم در آینده ارائه کرد.

ابهام‌های موجود، به نگرانی در خصوص تمایل کشورها در به‌کارگیری گروه‌های تروریستی به‌عنوان بازیگر نیابتی دامن زده است. روند جهانی شدن نیز فرصت‌های بی بدیلی برای تروریست‌ها فراهم کرده که امکان دست‌یابی به شیوه‌های ساخت و به‌کارگیری انواع سلاح و ایفای نقش تروریسم نیابتی و حفظ حیات خود با ایجاد ارتباط با دولت‌ها و کشورهای هم‌راستا (از منظر ژئوپلیتیک، ژئواکونومیک و به‌ویژه ژئوایدئولوژیک) چندان دور از دسترس نیست. یکی از مهم‌ترین نگرانی‌ها، در خصوص اهداف تروریسم نیابتی، تروریسم سایبری است که به نظر می‌رسد بر تخریب و نابودی تأسیسات زیربنایی و ایجاد چالش‌های فراگیر برای شهروندان به‌منظور بروز وضعیت‌های امنیتی و بحران آفرینی تمرکز دارد.

بسیاری از اتفاق‌های ناشی از خرابی‌های غیرعمدی ممکن است عملکرد عادی سیستم‌های کنترل صنعتی را تحت تأثیر قرار دهند بااین‌حال بزرگ‌ترین تهدید برای سیستم‌های کنترل صنعتی خرابی‌های عمده هدف‌دار است که درگذشته به‌صورت حمله فیزیکی و اجزای سیستم کنترل صورت می‌پذیرفت و هدف آن‌ها مختل کردن عملکرد سیستم بود حملات سایبری تکامل طبیعی برای این نوع حمل‌ها می‌باشند که برای مهاجمان ارزان‌تر و کم‌خطرتر و تحت اثر فاصله نیستند. در عین حال تکرار و هماهنگی آن‌ها بسیار راحت‌تر است. مراکز و تأسیسات اساسی عموماً وابسته به سیستم‌های کنترل صنعتی می‌باشد. این موضوع در ابتدا؛ ورود کشورهای متخاصم به‌عنوان بازیگران رسمی سیاست بین‌الملل را در پی داشت و نتایجی چون پروژه استاکس نت را موجب گردید اما با توجه به انتقال سریع این قابلیت به افراد و گروه‌ها؛ اکنون تروریست‌های سایبری علاوه بر تمرکز بر اجرای اهداف خود علیه کشورها و مراکز مدنظر خویش، در یک روند نیابتی در صدد پذیرش خرابکاری‌ها و اقدامات تروریستی از جانب سایر کشورها می‌باشند.

فضای جنگ نیابتی حاکم بر منطقه جنوب غرب آسیا امکان بروز این وضعیت‌ها را در این منطقه افزایش داده است. به‌ویژه آنکه مهم‌ترین زیرساخت‌های ملی این کشورها که شامل زیرساخت‌های

استحصال، تولید، انتقال و پالایش و صادرات محصولات حوزه انرژی، پتروشیمی و ... است به‌شدت به سیستم‌های کنترل صنعتی غیربومی وابسته است.

این روند همچنین مورد اقبال قدرت‌های فرا منطقه‌ای به‌عنوان اهرمی جهت کسب درآمدهای اقتصادی بیشتر از کشورهای منطقه خواهد بود. پیش‌بینی می‌گردد که بروز برخی اعتراضات مردمی متأثر از شرایط سیاسی– اقتصادی و گسل‌های موجود بین مردم و برخی از حاکمیت‌های منطقه به‌عنوان عامل مساعد، امکان تقرب جریان‌های تروریستی به سمت گروه‌های معترض و معاند داخلی و دسترسی راحت‌تر به اطلاعات سایبری و انجام اقدامات تروریستی سایبری در زیرساخت‌های دارای سیستم‌های کنترل صنعتی را تسهیل نماید که این امر لزوم انجام پژوهش‌های تکمیلی در این زمینه با هدف ترسیم سازی فضای احتمالی تقرب کشورهای متخاصم به گروه‌های تروریسم سایبری و اهداف احتمالی آن‌ها در سیستم‌های کنترل صنعتی فعال در حوزه‌های زیرساختی حیاتی، حساس و مهم را ضروری می‌نماید. این ضرورت موقعی بیشتر جلوه‌گر می‌شود که مسئولین جمهوری اسلامی ایران به‌موازات دنبال نمودن تأثیر تحریم‌ها بر صادرات انرژی، می‌بایست به سناریوی احتمالی ایجاد اختلال‌های گسترده در حوزه انرژی (اعم از صادرات و مصرف داخلی) از طریق تروریسم سایبری نیز دقت نظر داشته باشند.

فهرست منابع:

الف– منابع فارسی

- ازغندی، علیرضا؛ روشندل، جلیل (۱۳۹۱)، مسائل نظامی و استراتژیک معاصر، تهران: انتشارات سمت.
- افتخاری، اصغر (۱۳۸۱)، مراحل بنیادین اندیشه در مطالعات امنیتی، مطالعات امنیت ملی پس از جنگ سرد، پژوهشکده مطالعات راهبردی
- شاه حسینی، محمدحسن (۱۳۸۸)، بیوتروریسم از نظر طب رزمی، برگرفته از کتاب بیوتروریسم طیب، علیرضا (۱۳۸۲)، تروریسم، تهران؛ انتشارات غزال.
- شولتز، ریچارد و همکاران (۱۳۸۶)، رویکردهای جدید در مطالعات امنیتی، ترجمه‌ی سید محمدعلی تمقی نژاد، تهران، پژوهشکده مطالعات راهبردی.
- شیرازی، حبیب اله ابوالحسن (۱۳۹۴)، میزان سنجی تأثیر عنصر رقابت بر جنگ‌های نیابتی ایران و عربستان، فصلنامه پژوهش‌های سیاسی جهان اسلام، سال پنجم، شماره اول.
- قوام، سیدعبدالعلی؛ ایمانی، همت (۱۳۹۱)، نظریه رئالیستی اتحاد در روابط بین‌الملل، مجله رهیافت‌های سیاسی و بین‌المللی، شماره ۳۰
- کریمی، سحر (۱۳۹۴)، نحوه و چگونگی پیدایش و شکل‌گیری گروه‌های تروریستی بررسی موردی دولت اسلامی عراق و شام، ماهنامه پژوهش ملل ۱.
- مکنزی، کنت (۱۳۸۲)، جنگ نامتقارن، ترجمه‌ی: عبدالمجید حیدری، تهران، دانشکده فرماندهی و ستاد سپاه

ب– منابع انگلیسی

- Waltz, Kenneth Neal (1979).Theory of International Politics. Addison-Wesley Pub. Co.
- Loveman, Chris (2002). Assessing the Phenomenon of Proxy Intervention. Conflict and Security & Development, 2 (3), pp 29-48.
- Rinaldi, Steven M. James P. Peerenboom, and Terrence K. Kelly, (2001): Identifying, understanding, and analyzing critical infrastructure interdependencies, IEEE Control Systems, Volume 21, Issue 6, Pages 11-25. (doi: 10.1109/37.969131).
- Conrad, J. (2011). Interstate Rivalry and Terrorism: An Unprobed Link. Journal of Conflict Resolution.55 (4).
- Bar, Siman& Tov, Y. (1984). The strategy of War Proxy.Cooperation and Conflict.19 (4).

– CTED TRENDS REPORT (2017), physical protection of critical infrastructure against terrorist attacks, United Nations security council.
– Brookings Doha Center Analysis, (2016), "Risky Routes: Energy Transit in the Middle East" https://www.brookings.edu/wp-content/uploads/2016/07/en-energy-transitsecurity-mills-2.pdf.
– Report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat (2016), United Nations http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2016/92.