فصلنامه علمی-ترویجی پدافند غیرعامل

سال نهم، شماره ٤، زمستان ۱۳۹۷، (پیاپی ٣٦): صص ۶۷-۵۷

مقاوم‌سازی زیرساخت‌های شبکه برق با استفاده از روش‌های پدافند غیرعامل

محمد پالیزوان*[۱]، رضا دشتی[۲]

تاریخ دریافت: ۱۳۹۶/۰۷/۱۹
تاریخ پذیرش: ۱۳۹۶/۱۱/۱۵

چکیده

امروزه سامانه‌های قدرت الکتریکی به‌عنوان یکی از اهداف راهبردی در جنگ‌های مدرن شناخته می‌شوند و خطرات گوناگونی آنها را تهدید می‌نماید که بایستی جهت مقابله با آنها تمهیداتی در نظر گرفته شود. با توجه به اهمیت سامانه قدرت در حفظ و تداوم فعالیت‌های جامعه، لازم است تا تدابیر امنیتی کافی برای کم‌اثر نمودن تهدیدات و کاهش آسیب‌پذیری‌ها اتخاذ گردد که در این زمینه، پدافند غیرعامل می‌تواند نقش مهمی در استمرار فعالیت چرخه تولید تا مصرف انرژی الکتریکی ایفا نماید. در این مقاله به تاثیر جایگاه پدافند غیرعامل در جهت افزایش امنیت سامانه‌های قدرت در مقابل خرابکاری‌ها و تهدیدات پرداخته شده است. بدین منظور، ابتدا به ارزیابی تهدیدات موثر و مخرب در شبکه‌های برق به همراه مروری بر برخی نمونه‌های عملیاتی در کشورهای مختلف پرداخته شده و سپس، نقاط آسیب‌پذیر بخش‌های اصلی سامانه قدرت اعم از مراکز تولید، پست‌های انتقال و فوق توزیع، خطوط انتقال، مراکز کنترل، و شبکه‌های توزیع، شناسایی و مطرح شده است. پس از آن، راهبردها و ایده‌های موثری در جهت کاش سطح آسیب‌پذیری هریک از این بخش‌ها ارائه گردیده که در مجموع به مقاوم سازی و افزایش امنیت شبکه تحت شرایط بحرانی و غیرطبیعی کمک خواهند کرد. این راه‌کارها بر اساس تجربیات سایر کشورها و تحقیقات انجام گرفته در حوزه پدافند غیرعامل ارائه شده و عمده تهدیدات سایبری و فیزیکی در شبکه‌های برق را می‌تواند پوشش دهد.

کلیدواژه‌ها: پدافند غیرعامل، سامانه‌های قدرت الکتریکی، مقاوم‌سازی، حملات مخرب

۱- دکتری هوافضا، معاونت انرژی سازمان پدافند غیرعامل کشور (palizvan_1363@yahoo.com)- نویسنده مسئول
۲- استادیار، دانشکده فناوری‌های نوین دانشگاه علم و صنعت ایران

۱- مقدمه

سامانه قدرت در حال تبدیل شدن به یک هدف محبوب به منظور حمله‌های مخرب به دلایل مختلف، از جمله اهداف نظامی و یا سیاسی که ناتوانی و یا تخریب آن اثرات منفی بر روی اقتصاد و امنیت ملی خواهد گذاشت، است. شبکه‌های قدرت را می‌توان به سه زیرلایه تقسیم نمود: لایه فیزیکی، لایه انسانی، و لایه اینترنتی. لایه فیزیکی اشاره به خواص ملموس مرتبط با برق، مانند نیروگاه‌های برق، خطوط انتقال و ترانسفورماتورها دارد. لایه انسانی اشاره به افرادی دارد که دسترسی به سامانه‌های قدرت داشته باشند؛ و لایه اینترنتی شامل اطلاعات سخت‌افزاری، نرم‌افزاری، داده‌ها، و شبکه‌های ارتباطی است که از عملکرد سامانه انرژی الکتریکی حمایت می‌کند. یک تهدید، زمانی مخرب است که از طریق سه لایه، مانند تخریب ترانسفورماتور در لایه فیزیکی، خسارات ناشی از عوامل مخرب (انسانی) در لایه تصمیم‌گیری انسان و حملات از طریق بدافزارها و هکرها در لایه‌های اینترنتی پیاده‌سازی شود. یک اقدام تهاجمی موفق در شبکه برق می‌تواند آثار ویرانگری بر امنیت ملی، اقتصاد و زندگی هر شهروند داشته باشد. با این‌حال، سامانه قدرت جنبه‌های مختلفی دارد که هیچ‌گاه نمی‌تواند در برابر یک حمله از پیش تعیین شده به‌طور کامل محافظت شود. نیروگاه برق به‌دلیل وسعت ساختمان و حجم تجهیزات و همچنین شبکه‌های انتقال و توزیع برق به دلیل در دسترس بودن، یکی از مهمترین اهداف کشورهای مهاجم در جنگ‌های نوین می‌باشند [۲-۱].

در مجموع، حوادثی که به‌طور بالقوه می‌توانند تهدیدی برای سامانه قدرت باشند، به دو دسته طبیعی و انسان‌ساز تقسیم می‌شوند. حوادث طبیعی می‌تواند در قالب سیل، طوفان، زلزله و آذرخش و حوادث انسان‌ساز نیز می‌تواند به‌صورت پدیده‌هایی نظیر جنگ، خرابکاری و حادثه صنعتی، به‌عنوان تهدیدات جدی برای عملکرد سامانه مذکور، مطرح شوند. حملات خصمانه‌ای که با دخالت عامل انسانی و با هدف ایجاد خسارات و تلفات رخ می‌دهد، در زمره حوادث انسان‌ساز (عمدی) قرار دارد. یعنی در شکل‌گیری این نوع حوادث، انگیزه، آگاهی و هدف نقش مهمی دارند. بنابراین، وجود مدیریت در سامانه قدرت در برابر وقوع این نوع حملات برای امنیت زیرساخت‌ها بسیار حیاتی خواهد بود؛ چراکه پیامدهای ناشی از این حملات از جنبه‌های مختلفی بر جامعه تحمیل می‌گردد [۳].

عمده تهدیدات موثر در صنعت برق به دو دسته کلی تقسیم می‌شوند که عبارتند از:

- تهدیدات ناشی از تهاجم سایبری
- تهدیدات ناشی از تهاجم فیزیکی

پدافند (دفاع) به دو صورت عامل (یعنی انجام عملیات تدافعی با جنگ افزار) و غیرعامل (یعنی انجام عملیات تدافعی بدون جنگ افزار) تعریف می‌گردد. به بیان ساده‌تر، پدافند غیرعامل به کلیه اقدامات یا تدابیری اطلاق می‌گردد که بدون استفاده از سلاح، موجب کاهش آسیب‌پذیری، تلفات، خسارات و افزایش پایداری شود. از نقطه نظر مدیریتی، اقدامات مورد نظر برای اجرای اصول پدافند غیرعامل، عمدتا قبل از حادثه انجام می‌شود؛ هرچند ممکن است برخی اقدامات آن، حین و پس از حادثه نیز صورت گیرد. بنابراین، با توجه به اهمیت سامانه قدرت در حفظ و تداوم فعالیت‌های جامعه، لازم است تا تدابیر امنیتی کافی برای کم‌اثر نمودن تهدیدات و کاهش آسیب‌پذیری‌ها اتخاذ گردد. در این حالت، پدافند غیرعامل می‌تواند نقش مهمی در استمرار فعالیت چرخه تولید تا مصرف انرژی الکتریکی ایفا نماید که در این مقاله به آن پرداخته خواهد شد.

با توجه به داده‌های به‌دست‌آمده از موسسه GTD، از ۱۵۲۵۴ حمله تروریستی که در سراسر جهان بین سال‌های (۱۹۹۸-۲۰۰۷) انجام گرفته است چیزی نزدیک به ۲۳۲ حمله تروریستی مربوط به زیرساخت‌های انرژی بوده که تقریبا حدود ۱/۵٪ تروریسم جهانی است [۲].

در این مقاله از تجربیات کسب شده از تحقیقات سایر کشورها و نیز تحقیقات انجام شده توسط محققان داخلی استفاده شده است. از جمله تحقیقات مهم و بین‌المللی انجام شده در این حوزه می‌توان به [۴-۱۰] اشاره کرد. از این‌رو، باید تمهیدات لازم برای مواجهه با تهدیدات مذکور اندیشیده شود، که در این مقاله با انجام بررسی‌های لازم، راه‌کارهای موثری در جهت افزایش قدرت دفاعی سامانه قدرت در بخش‌های مختلف (اعم از تولید، انتقال، توزیع و مراکز کنترل)، بیان خواهد شد.

۲- عمده تهدیدات موثر و مخرب در شبکه‌های برق

به‌طور کلی، شبکه برق به‌دلیل وسعت و حجم تجهیزات و همچنین به دلیل در دسترس بودن، یکی از مهمترین اهداف کشورهای مهاجم در جنگ‌های نوین می‌باشند. عمده تهدیدات موثر در این مراکز عبارتند از [۲]:

- تهدیدات ناشی از شناسایی توسط سامانه سنجش از راه دور دشمن
- تهدیدات ناشی از تهاجم هوایی (بمب، موشک)
- تهدیدات ناشی از اقدامات تروریستی
- تهدیدات ناشی از بمب‌های گرافیتی
- تهدیدات ناشی از تهاجم سایبری
- تهدیدات ناشی از سلاح‌های الکترومغناطیس

- تهدیدات ناشی از القای ولتاژ بالا

نیروهای مخرب و تروریستی دارای قابلیت‌های فنی و منابعی هستند که می‌خواهند تعداد زیادی از مردم را بکشند یا باعث ایجاد آسیب گسترده اجتماعی و اقتصادی در محل مورد تهاجم شوند. سامانه قدرت به دلیل اهمیت بالا و نقشی که در صنعت و زندگی روزمره مردم هر کشوری ایجاد می‌کند، به‌عنوان یکی از اهداف اولیه حملات تروریستی شناخته می‌شود. یک حمله پیچیده می‌تواند موجب خاموش شدن طولانی مدت در یک منطقه وسیع شود. در ادامه، برخی حملات تروریستی انجام گرفته در شبکه برق کشورهای مختلف در سال‌های اخیر تشریح می‌گردد [۱۱]:

آمریکا: در نیمه شب ۱۶ آوریل ۲۰۱۳، یک حمله تروریستی به پست انتقال شرکت Metcalf در نزدیکی San Jose انجام گرفت که در آن، ابتدا مهاجمین کابل فیبر نوری AT&T را قطع کرده و سامانه ارتباطی را از کار انداختند و سپس با شلیک‌های متعدد به تجهیزات پست باعث از کار افتادن ۱۷ ترانسفورماتور از مجموع ۲۰ ترانسفورماتور آن پست انتقال گردیدند و حدود ۱۶ میلیون دلار صدمه وارد کردند. این حادثه منجر به از کار افتادگی آن پست به مدت ۲۷ روز گردید. در کشور آمریکا، پس از حادثه ۱۱ سپتامبر ۲۰۰۱ بیشتر توجهات به تهدیدات سایبری متمرکز شده بود و با وقوع حادثه Metcalf، خطر حملات فیزیکی نیز بیش از پیش مورد توجه قرار گرفته است.

عراق: از ابتدای شروع حملات نیروهای داعش در سال ۲۰۱۴ در کشور عراق، حملات مختلفی توسط گروه‌های تروریستی به شبکه برق این کشور اعمال شده است. از جمله این حملات می‌توان به حمله تروریست‌ها به سه دکل در دو خط انتقال برق پرقدرت بین دیالی و کرکوک اشاره کرد که با انفجار این دکل‌ها با استفاده از بمب‌های دست‌ساز، چهار خط انتقال برق دچار آسیب شد و نیروگاه‌ها برق‌رسانی به مناطق واقع در این دو استان را متوقف کردند و ۱۱۰۰ مگاوات برق از مدار خارج گردید. همچنین یک خط انتقال نیروی پرقدرت بین منطقه المقدادیه و منطقه سد حمرین در دیالی، و خط دوم واقع در بین شهرهای هیت و حدیثه در انبار مورد حمله تروریست‌ها قرار گرفتند و در اثر آن شش دکل منفجر گردید و برق‌رسانی به شهرهایی که از سوی این دو خط تأمین می‌شدند قطع شده و موجب از دست رفتن ۸۰۰ مگاوات برق شده است.در مورد دیگر، تروریست‌ها یک خط ورودی برق به دیالی را با بمب‌های دست‌ساز مورد حمله قرار دادند و سه دکل را بین چهارراه الصفره و سد حمرین تخریب کردند که موجب از دست رفتن ۴۰۰ مگاوات برق شده است. علاوه براین، یک بمب دست‌ساز زیر یک دکل واقع در ناحیه اللطیفیه منفجر شد، که موجب کشته و زخمی شدن کارمندان وزارت برق این کشور و قطع ۴۰۰ مگاوات برق تأمینی برای بغداد، شده است. از جمله اقدامات گروه‌های تروریستی در این کشور می‌توان به انفجار دو برج شماره ۱۵۹ و ۱۶۰ خط انتقال برق فشار قوی جمهوری اسلامی ایران به عراق موسوم به خط 'مرصاد - دیاله' اشاره کرد، که منجر به خروج این خط از شبکه و خروج ۴۰۰ مگاوات برق از شبکه برق این کشور گردید.

آلبانی: در تاریخ ۳۱ دسامبر ۲۰۱۳ یک حمله تروریستی در کشور آلبانی انجام شد که منجر به آسیب دیدن سامانه برق‌رسانی این کشور از طریق انفجار یک دکل برق در منطقه Kurbini گردید. این دکل در خط انتقال ۴۰۰ کیلو ولت مرسوم به Tirana–Podgorica واقع شده که این انفجار باعث انهدام یکی از پایه‌های دکل شده است. این انفجار ناشی از به‌کارگیری TNT در این حمله بوده است.

یمن: در سپتامبر ۲۰۱۴ انجام یک حمله تروریستی بر خطوط انتقال کشور یمن، منجر به خاموشی سراسری در این کشور گردید و حدود ۲۳ میلیون نفر به مدت یک روز بدون برق بودند. این حادثه در اثر خروج تعدادی از خطوط انتقال برق این کشور توسط تروریست‌ها حاصل گردیده است.

مکزیک: در اکتبر ۲۰۱۳ یک گروه تروریستی در ایالت Michoacán کشور مکزیک، به ۹ پست برق حمله کرده و منجر به قطع برق بیش از ۴۰۰ هزار مشترک در آن منطقه شده است.

همچنین، در گذشته حملات فیزیکی متعددی در شبکه‌های برق سراسر جهان انجام شده که از جمله آنها می‌توان حملات تروریستی انجام گرفته در کشورهای شیلی، کلمبیا، آفریقای جنوبی، و السالوادور اشاره کرد که حملات صورت گرفته در عمده آنها، شامل قطع یا انفجار خطوط انتقال برق بوده است.

۳- قسمت‌های آسیب‌پذیر شبکه برق در برابر تهاجمات

با توجه به روش توصیفی- تحلیلی ارائه‌شده در [۱۲] جهت ارزیابی تهدیدات، آسیب‌پذیری‌ها و نیز تحلیل خطرپذیری زیرساخت‌های حیاتی، قسمت‌های اصلی آسیب‌پذیر در زیرساخت‌های سامانه برق، در برابر حملات مخرب، شامل موارد زیر می‌گردد [۱۰-۹]:

مراکز تولید: مراکز تولید انرژی الکتریکی که حجم زیادی از توان مصرفی شبکه را به‌صورت متمرکز تولید کرده، به‌عنوان یکی از اهداف حملات تروریستی شناخته می‌شوند؛ زیرا درصورت خروج یک ژنراتور بزرگ در شبکه، ظرفیت سامانه انرژی الکتریکی صدها مگاوات کاهش خواهد یافت. این مراکز به دلیل اهمیت بالایی که در شبکه دارند، به‌طور طبیعی دارای تمهیداتی جهت مقابله با تهدیدات طبیعی یا

مخرب هستند و از این‌رو، کمتر مورد حمله گروه‌های تروریستی قرار می‌گیرند. به‌طور کلی، مهمترین قسمت‌های آسیب‌پذیر این مراکز به شرح زیر هستند:

- توربین و ژنراتور
- سامانه سوخت‌رسانی
- سامانه خنک‌کننده
- سامانه برق‌رسانی داخلی
- واحدهای شیمیایی

پست‌های انتقال: پست‌های انتقال به دلیل اهمیت بالایی که در سامانه قدرت دارند، همواره در معرض آسیب‌رسانی از جانب گروه‌های مخرب هستند و این بحث در پست‌های فشار قوی ملموس‌تر است. از جمله دلایلی که باعث افزایش حساسیت پست‌های برق‌رسانی می‌شود، می‌توان به وجود تجهیزات مهم و اساسی در این مراکز و همچنین مدت زمان زیادی که جهت جایگزینی آنها لازم است، اشاره کرد. طبق یک توافق کلی میان برنامه‌ریزان امنیتی، کلیدی‌ترین پست‌های فشار قوی در زمره مطلوب‌ترین اهداف تروریستی در سامانه انتقال قدرت هستند. مهمترین قسمت‌های آسیب‌پذیر این مراکز به شرح زیر هستند:

- تجهیزات الکتریکی فشارقوی (اعم از ترانسفورماتورها، کلیدها، باس‌بارها)
- تجهیزات اندازه‌گیری
- سامانه ارتباطی
- سامانه کنترلی و حفاظتی

خطوط انتقال: خطوط انتقال انرژی الکتریکی از جمله راحت‌ترین و در دسترس‌ترین اهداف برای حملات تروریستی هستند و آمار نشان می‌دهد که این بخش از شبکه برق همواره در معرض بیشترین حملات تروریستی و مخرب بوده است. علاوه براین، تهدیدات طبیعی مانند طوفان‌ها و یخ‌بستگی‌ها نیز ازجمله عوامل طبیعی دردسرساز برای این بخش از سامانه قدرت محسوب می‌شوند. با این حال، در صورت بروز آسیب بر روی خطوط انتقال، می‌توانند سریعا تعمیر شوند مگر اینکه یک حمله گسترده و هماهنگ شده انجام گرفته باشد. به‌طور کلی، مهمترین قسمت‌های آسیب‌پذیر این مراکز به شرح زیر هستند:

- دکل‌های انتقال انرژی الکتریکی
- کابل‌های حامل انرژی الکتریکی
- مقره‌های عایقی

مراکز کنترل: سامانه‌های قدرت به شدت به مراکز کنترل خود وابسته هستند. کامپیوترها، تجهیزات سنجش از راه دور، فیبر، رادیو و خطوط اختصاصی تلفن، از جمله تجهیزات این مراکز هستند که به‌طور مداوم برای نظارت بر عناصر سامانه قدرت و انتقال اطلاعات حیاتی به مرکز کنترل، استفاده می‌شود. وظیفه این مراکز ایجاد هماهنگی در بهره‌برداری بهتر شبکه و حفظ قابلیت اطمینان آن است. از دست رفتن این مراکز که به‌نوعی مغز سامانه محسوب می‌شوند، منجر به ایجاد آسیب‌های اساسی و مخرب در شبکه می‌گردد. عمده تهدیدات این مراکز از جانب حملات سایبری می‌باشد و لذا عمده تمرکز بر افزایش امنیت سایبری این مراکز است؛ زیرا از لحاظ فیزیکی، حفاظت لازم برای آنها لحاظ شده است.

- سامانه ارتباطی
- سامانه پایشی
- سامانه پردازشی

تجهیزات توزیع: این تجهیزات قدرت را از ایستگاه انتقال خطوط و ایستگاه‌های فشار متوسط شبکه به تمام مشترکین پایین دست، انتقال می‌دهند. تعداد اجزای سامانه توزیع بیشتر و ظرفیت کمتری نسبت به اجزای سامانه انتقال دارند و قطعات یدکی به‌طور کلی در این بخش‌ها بیشتر است. هدف قرار دادن اجزای سامانه توزیع می‌تواند موجب بروز مشکلاتی در تامین برق مشترکین گردد اما این مشکلات معمولا امکان کنترل بیشتری نسبت به حملات بر روی سامانه‌های انتقال و یا ایستگاه‌های تولید، دارند؛ مگر این‌که هدف آنها قطع برق مراکز بحرانی و حساس در سامانه توزیع باشد.

- ترانسفورماتورهای توزیع
- دکل‌های برق و هادی‌های توزیع
- کنتورها و تجهیزات اندازه‌گیری
- تجهیزات الکتریکی مشترکین

۴- افزایش امنیت زیرساخت‌های سامانه قدرت از طریق پدافند غیرعامل

به‌طور کلی، اقدامات مورد نظر برای اجرای اصول پدافند غیرعامل، عمدتا قبل از حادثه انجام می‌شود؛ هرچند ممکن است برخی اقدامات آن، حین و پس از حادثه نیز صورت گیرد. بنابراین، با توجه به اهمیت سامانه قدرت در حفظ و تداوم فعالیت‌های جامعه لازم است تا تدابیر امنیتی کافی برای کم‌اثر نمودن تهدیدات و کاهش آسیب‌پذیری‌ها اتخاذ گردد. برخی اقدامات موثر برای بخش‌های مختلف شبکه در ادامه تشریح می‌گردد که عمده آنها از تحقیقات معتبر بین‌المللی استخراج گردیده است.

۴-۱- اعمال پدافند غیرعامل در حوزه تولید برق

در این بخش به بررسی اصول پدافند غیرعامل در رابطه با تولید انرژی الکتریکی پرداخته می‌شود. به‌کارگیری این اقدامات در کاهش تلفات انسانی و خسارات مالی مؤثر هستند. در ادامه برخی از مهم‌ترین این ملاحظات که باید در نیروگاه‌ها به منظور کاهش آسیب‌پذیری در شرایط تهاجم مورد توجه قرار گیرند، ارائه می‌شوند [۱، ۱۳و ۱۴].

- **مکان‌یابی مناسب:** مکان‌یابی مطلوب را می‌توان مهم‌ترین اقدام پدافند غیرعامل در کاهش آسیب‌پذیری مراکز حیاتی و حساس از جمله نیروگاه‌ها محسوب نمود، زیرا اگر در مرحله صفر طراحی پروژه، احداث و تأسیس مراکز حیاتی و حساس عوامل و معیارهای ذیربط دفاعی و امنیتی از قبیل حداکثر استفاده از عوامل طبیعی، آمایش سرزمینی، رعایت پراکندگی، پرهیز از انبوه و حجم‌سازی انبوه، مقاوم‌سازی اولیه و بسیاری از فرصت‌های موجود در دسترسی، رعایت، نظارت و کنترل گردد از بروز بسیاری از مشکلات بعدی که نوعاً پیچیده و هزینه بر هستند، جلوگیری به عمل خواهد آمد. در شناسایی محل احداث نیروگاه‌ها، علاوه بر مباحث فنی و اقتصادی، نکات مربوطه در زمینه بررسی پتانسیل حفاظت فیزیکی در برابر حملات تروریستی باید مورد توجه قرار گیرد که در این راستا از تجربیات متخصصان نظامی می‌توان استفاده کرد
- **رعایت اصل اختفاء:** هم‌رنگ بودن تجهیزات و ساختمان‌ها به رنگ محیط یکی از اقداماتی است که باعث اختفای تجهیزات می‌گردد. این هم‌رنگ‌سازی در سطوح سقف ساختمان‌های اداری، اتاق فرمان و مخازن سوخت انجام می‌گیرد. همچنین نشان ندادن نمای خارجی نیروگاه در رسانه‌ها به‌ویژه در ارتباط با محیط اطراف و جاده‌ها و کاشت درختان بلند در اطراف نیروگاه‌ها می‌تواند تا حدودی باعث اختفای نیروگاه شود.
- **رعایت اصل پراکندگی:** در طراحی و چیدمان اجزای نیروگاه‌ها باید اصلی پراکندگی را لحاظ نمود. بدین منظور تجهیزات حیاتی و پشتیبان آنها و همچنین موقعیت قرارگیری مخازن سوخت باید به گونه‌ای باشند که در اثر آتش سوزی یا موج ناشی از انفجار سایر تجهیزات و تاسیسات، حتی‌الامکان آسیب نبینند.

همچنین، با توجه به آنکه سهم عمده‌ای از انرژی الکتریکی در نیروگاه‌های کشور به‌صورت متمرکز تولید می‌گردد و این نیروگاه‌ها از لحاظ راهبردی بدون حفاظ در مقابل هرگونه حمله نظامی کشورهای مهاجم طراحی گردیده‌اند، با توسعه نیروگاه‌های تولید پراکنده می‌توان این موضوع را تا حدی مرتفع نمود. امروزه منابع تولید پراکنده به‌دلیل اثرات چشمگیری که در روند خصوصی‌سازی داشته و همچنین به‌دلیل مزایایی که در بهبود پارامترهای شبکه دارند، به‌طور گسترده در سطح جهان مورد بهره‌برداری قرار می‌گیرند. از دیدگاه پدافند غیرعامل، منابع انرژی‌های تجدیدپذیر، منابع راهبردی به‌حساب می‌روند، زیرا این منابع پایدار بوده و در صورت وقوع جنگ و یا تحریم‌های گوناگون، می‌توانند جایگزین مناسبی برای سوخت‌های فسیلی باشند. با استدلال به موارد فوق و لزوم در نظر گرفتن اصول و ملاحظات پدافند غیرعامل سرمایه‌گذاری در حوزه نیروگاه‌های تولید پراکنده اجتناب ناپذیر خواهد بود [۱۵].

- **ایجاد سازه‌های امن و مقاوم:** برای ایجاد این استحکامات در شرایط اضطراری از کیسه‌های شنی آماده استفاده می‌شود که در اطراف تجهیزات قرار می‌گیرد. در مورد تجهیزات بزرگ نیز از بشکه‌های پر از شن استفاده می‌شود. در اطراف ترانسفورماتورها دیوار بتنی محکم به نام دیوار آتش کشیده می‌شود. دیوار بتونی محافظ ترانسفورماتور قدرت اصلی در نیروگاه از سرایت آتش و موج انفجار از یک ترانسفورماتور آسیب‌دیده به ترانسفورماتورهای دیگر و دیگر تجهیزات مجاور آن جلوگیری می‌نماید.
- **نکاتی در زمینه احداث مخازن سوخت:** اغلب، مخازن سوخت را در ارتفاع بالاتری نسبت به نیروگاه قرار می‌دهند تا انتقال سوخت بدون نیاز به پمپ و توسط نیروی گرانش زمین انجام شود. این مساله هنگام آسیب دیدگی مخزن می‌تواند منجر به خروج سوخت و نشت آن به تجهیزات نیروگاه شود که موجب گسترش آتش‌سوزی‌های احتمالی و صدمه بیشتر به تجهیزات نیروگاه گردد. علاوه‌براین، اطراف مخازن سوخت می‌بایست دیوار بتونی کشیده شود تا در صورت انفجار این مخازن، مایع سوخت در سطح نیروگاه پخش نشود و باعث آتش سوزی بیشتر نگردد.
- **نکاتی در زمینه احداث ایستگاه‌های گاز:** ایستگاه‌های گاز در نیروگاه‌ها اغلب در فضای باز قرار دارند. این در حالی است که اصول پدافند غیرعامل لازم می‌دارد که در یک ساختمان بتونی مستحکم قرار بگیرند. ارتفاع این ساختمان نباید بلند باشد. در طراحی ایستگاه‌های گاز باید رعایت فاصله مناسب و دور از سایر تاسیسات حیاتی، پیش‌بینی تهویه مناسب، سامانه اطفای حریق و همچنین طراحی یک ایستگاه پشتیبان دیگر با رعایت حداکثر فاصله را مدنظر داشت.
- **نکاتی در زمینه ساخت برج‌های خنک کن:** با استفاده از هواکشی در برج‌های خنک‌کننده می‌توان تعداد و ارتفاع این برج‌ها را نسبت به برج‌های خنک‌کننده با مکش طبیعی کاهش

داد، با این وجود، همچنان ابعاد و شکل این برج‌ها قابل تشخیص خواهند بود. از سوی دیگر، با توجه به حیاتی بودن وجود برج‌های خنک‌کننده برای استمرار فعالیت نیروگاه، تعداد بیشتر آنها می‌تواند هنگام بروز آسیب موجبات ادامه فعالیت نیروگاه با ظرفیت کمتر را فراهم نماید. توده بخار برج‌هایی که با هواکش کار می‌کنند غلیظ‌تر از توده بخار مربوط به برج خنک‌کننده طبیعی است. برج‌های خنک‌کننده خشک، هیچ‌گونه توده بخار آب ندارند.

- **نکاتی در زمینه ساخت دودکش‌های نیروگاه:** با بررسی نیروگاه‌های موجود در کشور، ملاحظه می‌گردد که تعداد زیادی از این نیروگاه‌ها دارای دودکش تخلیه مشترک هستند. بدیهی است که اختلال در عملکرد هر یک از این دودکش‌ها، فرآیند تولید در واحدهای مرتبط را به مخاطره می‌اندازد. هرچند وجود این دودکش‌های مشترک ممکن است در کاهش هزینه‌های احداث یک نیروگاه مؤثر باشد اما به هرحال آسیب هر یک از آنها نیز می‌تواند متقابلاً از قابلیت اطمینان مجموعه نیروگاه بکاهد. در احداث دودکش‌های واحدهای مختلف یک نیروگاه باید اصل پراکندگی را رعایت نمود. دودکش‌های یک نیروگاه از جمله عناصری هستند که به‌راحتی از طریق عکس‌های ماهواره‌ای قابل تشخیص هستند و باید برای استتار یا اختفای آن اقدامات مناسبی صورت پذیرد.
- **نکاتی در مورد واحدهای شیمیایی نیروگاه:** برای جبران نشتی آب مقطر در سیکل بسته واحدهای بخاری، لازم است به میزان کافی آب تصفیه شده در دسترس باشد. به همین منظور در نیروگاه‌های بخاری از طریق واحدهای شیمیایی، با برهم‌کنش‌های شیمیایی آمونیاک و سود، آب تصفیه شده برای تزریق به سیکل بخار آماده می‌شود. در صورتی که این واحدها به‌خوبی محافظت نگردند، آسیب رسانی به آنها و انفجار تانک‌های سود و آمونیاک موجب آلودگی‌های زیست محیطی و گسترش آتش سوزی‌ها می‌شود. متاسفانه در اکثر نیروگاه‌های کشور این مخازن به نحو مطلوبی محافظت نمی‌شوند در حالی که به‌راحتی با ایجاد دیوارهای مسلح و سازه‌های امن می‌توان آسیب‌پذیری نیروگاه را از این ناحیه کاهش داد.
- **نکاتی در زمینه سامانه‌های خنک‌کننده:** در ژنراتورهای بزرگ برای خنک کردن سیم‌پیچ‌های استاتور از گاز هیدروژن استفاده می‌شود. به‌طور معمولی برای جبران نشتی‌های هیدروژن بر اثر تعمیر و راه‌اندازی مجدد واحدها، مخازن هیدروژن پشتیبان در محوطه نیروگاه وجود دارند. هیدروژن قابلیت انفجاری بالایی دارد و در صورت تماس مستقیم با هوا منجر به انفجار می‌گردد. متاسفانه علی‌رغم آسیب‌پذیری بالای مخازن نگهداری هیدروژن محافظت مناسب و مطلوبی از این مخازن صورت نمی‌گیرد و بیشتر این مخازن بدون پشتیبانی سازه‌های امن و محافظ در محوطه نیروگاه و بعضاً در مجاورت اجزای حیاتی نگهداری می‌شوند. در طراحی نیروگاه‌ها باید توجه ویژه‌ای به محافظت مخازن نگهداری هیدروژن مبذول شود.
- **سامانه‌های اعلام خطر و اطفای حریق کارآمد:** در صورت عدم مهار آتش سوزی‌های ناشی از حملات و گسترش این آتش‌سوزی‌ها به سایر بخش‌ها، به‌طور قطع اثر تخریبی و آسیب‌رسانی آنها چندین برابر می‌شود. وجود سامانه‌های اعلام خطر برای اطلاع‌رسانی به کارکنان نیروگاه به‌منظور ترک فعالیت و استقرار در پناهگاه‌های ایمن و همچنین استقرار سامانه‌های آتش‌نشان هوشمند و کارآمد در نقاط حساس و نقاطی که قابلیت اشتعال و انفجار بالایی دارند و تقویت سامانه‌های آتش‌نشان موجود، تأثیر زیادی بر کاهش خسارات و تلفات ناشی از انفجار و آتش سوزی دارد.
- **تجهیزات امنیتی فیزیکی پیشرفته:** مراکز تولید، پست‌ها، و همچنین مراکز کنترل در شبکه برق از اهمیت بالایی برخوردار هستند. برای این مراکز نیاز به توسعه تجهیزات امنیتی فیزیکی خاص مانند دوربین‌ها، حسگرها، دستگاه‌های تشخیص نفوذ، کنترل دسترسی، روشنایی پیشرفته، دیوارها و نرده‌های امنیتی محیطی، و نیز افزایش تعداد نیروهای انسانی حاضر در محل به‌همراه ارائه آموزش‌های لازم به آنها، وجود دارد، که همه این موارد منجر به کاهش آسیب‌پذیری و افزایش امنیت این اماکن (به‌خصوص در شب‌ها)، می‌گردد.

۴-۲- اعمال پدافند غیرعامل در حوزه پست‌های انتقال و فوق توزیع برق

در این بخش به بررسی اصول پدافند غیرعامل در رابطه با پست‌های انتقال و فوق توزیع پرداخته می‌شود. به‌طور کلی، در خصوص مقاوم‌سازی و افزایش امنیت پست‌های برق در برابر حملات تروریستی و مخرب، نکات زیر پیشنهاد می‌گردد که هرچه سطح ولتاژ پست افزایش یابد، رعایت آنها نیز حیاتی‌تر می‌شود (زیرا از لحاظ مباحث امنیت و پایداری در شبکه قدرت، اهمیت پست‌های فوق توزیع از پست‌های توزیع بیشتر است و همچنین اهمیت پست‌های انتقال از پست‌ها فوق توزیع نیز بیشتر می‌باشد). این نکات شامل موارد زیر می‌شوند [۱، ۹، ۱۱و ۱۵]:

- رعایت اصول مربوطه در زمینه‌های اختفاء، پراکندگی، و استحکامات در زمان احداث پست‌های برق که از اصول مهم پدافند غیرعامل محسوب می‌شوند.
- در شناسایی محل احداث پست‌های جدید، علاوه بر مباحث فنی

و اقتصادی، نکات مربوطه در زمینه بررسی پتانسیل حفاظت فیزیکی در برابر حملات تروریستی باید مورد توجه قرار گیرد که در این راستا از تجربیات متخصصان نظامی می‌توان استفاده کرد.

- انواع مراحل طراحی و مهندسی در جهت مقاوم‌سازی بخش‌های مختلف سامانه قدرت و کاهش آسیب‌پذیری اجزای کلیدی برای مقابله با تهاجم‌های فیزیکی باشد.
- پایش و کنترل موثر پست‌ها از طریق به‌کارگیری سامانه‌های پایش گسترده (WAMS) در کنار سامانه سنتی SCADA/EMS که این کار با نصب واحدهای اندازه‌گیری فازورهای سنکرون در پست‌های شبکه عملیاتی خواهد شد و نقش مهمی در بهبود بهره‌برداری شبکه و حفظ پایداری سامانه در شرایط بحرانی، ایفا خواهد کرد.
- مراکز تولید، پست‌ها، و همچنین مراکز کنترل در شبکه برق از اهمیت بالایی برخوردار هستند. برای این مراکز نیاز به توسعه تجهیزات امنیتی فیزیکی خاص مانند دوربین‌ها، حسگرها، دستگاه‌های تشخیص نفوذ، کنترل دسترسی، روشنایی پیشرفته، دیوارها و نرده‌های امنیتی محیطی، و نیز افزایش تعداد نیروهای انسانی حاضر در محل به‌همراه ارائه آموزش‌های لازم به آنها، وجود دارد، که همه این موارد منجر به کاهش آسیب‌پذیری و افزایش امنیت این اماکن (به‌خصوص در شب‌ها)، خواهد شد.
- استفاده از یک حصار مقاوم در اطراف پست به کمک دو صفحه مات که فضای بین آنها با شن و ماسه پر شده باشد و در مقابل نفوذ گلوله مقاومت کافی را داشته باشد.
- با توجه به اینکه مهم‌ترین تجهیز پست‌های برق ترانسفورماتورها هستند (از لحاظ فنی و اقتصادی)، لذا باید تهیه ترانسفورماتورها به شرکت سازنده تاکید شود که بدنه آنها مجهز به پوشش فلزی مقاوم در برابر گلوله باشد.
- بهبود نظارت الکترونیکی یکپارچه با استفاده از حسگرها و تجهیزات پایشی، و همچنین تجهیزات پردازش اطلاعات که قابلیت شناسایی و پاسخ‌دهی سریع در مقابل حملات همزمان به چند بخش مختلف را دارا هستند.
- استفاده از ابزارهای سامانه که می‌توانند محل حادثه راشناسایی و سامانه را کنترل نمایند و همچنین حوادث احتمالی را پیش-بینی نمایند.
- احداث و جایگزینی پست‌های داخلی (indoor) در مقابل پست‌های فضای باز باید افزایش یابد که پست‌های گازی (GIS) نمونه مناسبی از این پست‌ها هستند و در آن تجهیزات سوئیچگیر و ترانسفورماتورها با استفاده از عایق گازی (SF6) از یکدیگر جداسازی می‌شوند و این روش تاثیر بسیار مثبتی بر کوچک‌سازی فضای پست و اختفای آن می‌گذارد (بیشتر در پست‌های فوق توزیع و توزیع).

با توجه به هزینه سرمایه‌گذاری، بهره‌برداری و نگهداری بالا در این مراکز، مزایای عمده پست‌های GIS شامل فضای لازم بسیار کم (۱۰٪ فضای پست AIS)، عدم حساسیت به تأثیرات خارجی، سازگاری با محیط، و نیز ایمنی افراد و تجهیزات می‌شود.

۴-۳- اعمال پدافند غیرعامل در حوزه خطوط انتقال برق

در این قسمت به بررسی اعمال اصولی پدافند غیرعامل در رابطه با خطوط انتقال انرژی الکتریکی پرداخته می‌شود. در خصوص افزایش امنیت خطوط انتقال برق در برابر حملات تروریستی و مخرب، نکات زیر پیشنهاد می‌گردد (بدیهی است که در اینجا نیز هرچه سطح ولتاژ خط افزایش یابد، رعایت این موارد نیز حیاتی‌تر می‌شود) [۱، ۹، ۱۱، ۱۵]:

- رعایت اصول مربوطه در زمینه‌های اختفاء، پوشش و استحکامات که از اصول مهم پدافند غیرعامل محسوب می‌شوند.
- هنگام تعیین محل عبور یک خط انتقال برق علاوه بر مسائل فنی و اقتصادی، دسترسی آن جهت انجام حملات تروریستی نیز باید در نظر گرفته شود و مسیر مربوطه باید تا جایی که ممکن است از محل‌هایی عبور کند که در معرض دید عموم باشد.
- برای خطوطی که در مناطق دور افتاده و کم تردد احداث می‌شوند و کمتر قابل مشاهده عموم هستند، باید اقدامات حفاظتی اضافی در طراحی دکل‌ها در نظر گرفته شود و مقاومت بیشتری برای آنها در نظر گرفته شود.
- استفاده از دوربین‌های مادون قرمز، حسگرهای ارزان قیمت، و سامانه‌های ماهواره‌ای جهت ارائه اطلاعات از وضعیت الکتریکی و فیزیکی خط انتقال در زمان‌های مختلف که کمک زیادی به پایش امنیت خطوط توسط مراکز کنترل می‌نماید.
- استفاده بیشتر از دکل‌های جدید مرسوم به نوع خود-نگهدار (self-supporting tower) برای سامانه‌های انتقال انرژی الکتریکی و همچنین سامانه‌های ارتباطی که در برابر سقوط‌های متوالی دکل‌ها در شرایط حادثه، مقاوم هستند.
- توسعه استفاده استفاده از مقره‌های کامپوزیت جدید به جای مقره‌های سنتی سرامیکی و شیشه‌ای که مقره‌های جدید دارای مقاومت الکتریکی، حرارتی، و مکانیکی بیشتری نسبت به انواع مقره‌های طرح سنتی هستند.
- جایگزینی و احداث خطوط کابلی و زیرزمینی به جای خطوط هوایی قبلی باید افزایش یابد که خطوط با عایق گازی (GIL) نمونه مناسبی از این موارد هستند و در آن خطوط حامل انرژی

با استفاده از عایق گازی (SF6) از یکدیگر جداسازی می‌شوند و این روش تاثیر بسیار مثبتی بر کاهش فاصله بین خطوط و اختفای آن می‌گذارد (بیشتر در خطوط فشار متوسط و فشار ضعیف).

ویژگی‌های متعدد GIL سبب می‌شود که دامنه کاربردهای آن در خطوط انتقال افزایش یابد. به‌عنوان مثال می‌توان به مواردی مانند استفاده در مسیرهای بلند و صعب العبور، امکان نصب در تونل مشترک تاسیسات شهری، حذف حریم‌ها و زیباسازی فضای شهری، و نیز امکان نصب در نزدیکی خطوط راه آهن و فرودگاه‌ها اشاره نمود.

۴-۴- اعمال پدافند غیرعامل در حوزه مراکز کنترل برق

همان‌طور که ذکر شد، وظیفه این مراکز ایجاد هماهنگی در بهره‌برداری بهتر شبکه و حفظ قابلیت اطمینان آن است. از دست رفتن این مراکز که به‌نوعی مغز سامانه محسوب می‌شوند، منجر به ایجاد آسیب‌های اساسی و مخرب در شبکه می‌گردد. عمده تهدیدات این مراکز از جانب حملات سایبری می‌باشد و لذا عمده تمرکز بر افزایش امنیت سایبری این مراکز است. به‌طور کلی، در خصوص افزایش امنیت مراکز کنترل برق در برابر حملات تروریستی و مخرب، نکات زیر پیشنهاد می‌گردد [۱و ۱۱]:

- در شناسایی محل احداث مراکز کنترل جدید، علاوه بر مباحث فنی و اقتصادی، نکات مربوطه در زمینه بررسی پتانسیل حفاظت فیزیکی در برابر حملات تروریستی باید مورد توجه قرار گیرد که در این راستا از تجربیات متخصصان نظامی می‌توان استفاده کرد.
- مراکز کنترل در شبکه برق از اهمیت بالایی برخوردار هستند. برای این مراکز نیاز به توسعه تجهیزات امنیتی فیزیکی خاص مانند دوربین‌ها، حسگرها، دستگاه‌های تشخیص نفوذ، کنترل دسترسی، روشنایی پیشرفته، دیوارها و نرده‌های امنیتی محیطی، و نیز افزایش تعداد نیروهای انسانی حاضر در محل به‌همراه ارائه آموزش‌های لازم به آنها، وجود دارد، که همه این موارد جهت کاهش آسیب‌پذیری مراکز مختلف استفاده می‌شود.
- رشد کاربرد فناوری‌های ارتباطی در شبکه هوشمند امکان ایجاد بستر جدیدی از آسیب‌پذیری ناشی از نفوذ سایبری را فراهم می‌کند. برای جلوگیری از آسیب‌های ناشی از حملات سایبری، نیاز به تعریف ماموریت جدیدی با عنوان حفاظت از شبکه‌های هوشمند در برابر حملات سایبری می‌باشد.
- با توجه به این موضوع که این مراکز به‌نوعی مغز سامانه محسوب می‌شوند و از دست رفتن آنها باعث ایجاد آسیب‌های اساسی و مخرب در شبکه می‌گردد، لذا درنظر گرفتن مراکز پشتیبان برای این بخش از سامانه قدرت امری ضروری است تا در صورت بروز عیب یا حادثه در این مراکز، عملکرد سامانه مختل نشود و در این مواقع، مراکز پشتیبان به کنترل و مدیریت سامانه بپردازند.

۴-۵- اعمال پدافند غیرعامل در حوزه شبکه توزیع برق

انرژی برق دارای مصارف متنوعی است و نیازهای متعددی از جامعه را پاسخ می‌دهد. از جمله این مصارف می‌توان به مواردی همچون مصارف خانگی، تجاری، عمومی، صنعتی و کشاورزی اشاره نمود. با توجه به اهداف و مطالب بیان شده در زمینه پدافند غیرعامل، اهمیت شبکه‌های توزیع از نگاه پدافند غیرعامل به‌منظور حفظ تداوم انرژی برق بارهای حساس در مواقع بحران و عملکرد خرابکارانه گروه‌های متخاصم و تروریست، انکار ناپذیر می‌باشد. بدین منظور، با در نظر گرفتن اصول پدافند غیرعامل جهت تامین مطمئن انرژی برق بارهای حساس، باید تهدیدات و طرح‌های مربوطه ارائه گردد. جهت این امر می‌بایست پس از دشمن‌شناسی، تهدیدشناسی و آسیب‌شناسی، راهکارهای کاهش سطح آسیب در سه وجه مدیریت قبل از ضربه، مدیریت زمان ضربه و مدیریت بعد از ضربه بر اساس اصول پدافند غیرعامل مورد بررسی قرار گیرد. در خصوص افزایش امنیت شبکه‌های توزیع برق در برابر حملات تروریستی و مخرب، نکات زیر پیشنهاد می‌گردد [۱، ۹و ۱۶]:

- در حوزه به‌کارگیری پدافند غیرعامل در شبکه‌های توزیع، استفاده از کابل‌های زیرزمینی به‌جای خطوط هوایی می‌تواند علاوه بر تحقق اصول پدافند غیرعامل در این بخش‌ها، منجر به بهبود مسائل فنی و زیباسازی شهری نیز گردد.
- علاوه بر کابل‌های زیرزمینی، راهبرد استفاده از کابل‌های خود نگهدار در شبکه‌های فشار متوسط و فشار ضعیف نیز پیشنهاد می‌گردد. از نظر اجرایی و نگهداری، هزینه این سامانه بین سامانه هوایی با خطوط بدون عایق و سامانه کابل‌کشی زمینی می‌باشد. این سامانه در محل‌هایی که فضای لازم برای کابل‌کشی کم و یا گران می‌باشد، مناسب است. عوامل دیگری که باعث برتری این سامانه بر سامانه‌های هوایی می‌شود عبارتند از نصب و اجرای سریع و ساده، ایمنی و صورت ظاهری و کنترل زیست محیطی آن.
- افزایش قابلیت اتوماسیون توزیع جهت برق‌رسانی مشترکین بحرانی و حذف بار هوشمند، و همچنین افزایش نفوذ تولیدات پراکنده در این سامانه‌ها، به بهبود برق‌رسانی در شرایط اضطراری و کاهش آسیب‌پذیری شبکه، کمک شایانی می‌نماید.

به‌طور کلی، چکیده پیشنهادات جمع‌آوری شده جهت کاهش آسیب‌پذیری سامانه قدرت در مقابل تهدیدات و حملات مخرب

برحسب حوزه مربوطه، در قالب جدول (۱)، و چکیده راه‌کارهای ارائه‌شده برای افزایش امنیت فیزیکی سامانه قدرت برحسب بخش‌های مختلف، در قالب جدول (۲)، گردآوری شده است.

جدول (۱): چکیده پیشنهادات ارائه شده جهت کاهش آسیب‌پذیری سامانه قدرت در مقابل تهدیدات و حملات مخرب (برحسب حوزه آسیب‌پذیر)

حوزه مربوطه	اقدامات پیشنهادی جهت پیاده‌سازی	اقدامات پیشنهادی جهت تحقیق و توسعه
کاهش آسیب‌های فیزیکی در سامانه	- افزایش مقاومت فیزیکی پست‌های کلیدی و مراکز کنترل - افزایش نظارت فیزیکی - اضافه کردن دکل‌های انتقال مقاوم در برابر سقوط‌های متوالی دکل‌ها	- حسگرهای تشخیص نفوذ پیشرفته - توسعه راهبردهای افزایش ظرفیت سامانه - افزایش استفاده از منابع تولید پراکنده و ریزشبکه‌ها
کاهش آسیب‌های سایبری در سامانه	- حذف راه‌های ارتباطی غیرضروری با سامانه‌های خارجی - افزایش امنیت سایبری در تمام خطوط ارتباطی - توسعه بومی‌سازی در ساخت تجهیزات شبکه - انجام ارزیابی‌های قابلیت اطمینان در سامانه - وجود سامانه‌های پشتیبان برای مراکز کنترل	- بهبود امنیت سایبری برای حسگرها، مخابرات، و سامانه‌های کنترلی - سامانه‌های پایشی جهت کاهش خطاهای بهره-برداری
کاهش آسیب‌های پرسنلی ناشی از اپراتورها	- بهبود عملکرد کارمندان و پیمانکاران - گذراندن دوره‌های آموزشی مواجهه با بحران - بهبود برنامه‌ریزی و هماهنگی با بخش‌های دولتی	- شبیه‌سازهای آموزشی - گسترش حمایت از برنامه‌های آموزشی در حوزه مهندسی قدرت
افزایش مقاومت و امنیت جامع سامانه	- تغییر در اولویت‌ها و انگیزه‌های نهادی برای تضمین مدرن‌سازی مناسب سامانه انتقال - استفاده بیشتر از فناوری‌های الکترونیک قدرت ولتاژ بالا - استفاده بیشتر از اتصالات DC - گسترش مدیریت سمت بار و اتوماسیون توزیع	- سامانه‌های زیرزمینی ارزان قیمت - بهبود ارزیابی آسیب‌پذیری احتمالاتی - بهبود حسگرها، ارتباطات، تجزیه و تحلیل زمان واقعی و تصویرسازی سامانه - بهبود کنترل خودکار - بهبود توانایی جزیره‌سازی و خود ترمیمی - بهبود ذخیره‌سازی انرژی
افزایش سرعت بازیابی سامانه پس از حادثه	- برنامه‌ریزی گسترده برای قطعی‌های بسیار بزرگ - تعیین برخی از کارکنان به عنوان اولین پاسخ دهنده	- توسعه و ذخیره ترانسفورماتورهای بازیابی و سایر تجهیزات کلیدی - بهبود ابزار ارزیابی و برنامه‌ریزی
بهبود ارائه خدمات در شرایط بحرانی	- استفاده از سامانه‌هایی مانند چراغ عبور و مرور LED با باتری‌های شارژر - اتصال ژنراتور در محل بارهای بحرانی مانند پمپ‌ها تامین آب - برنامه‌ریزی‌های جامع برای حوادث احتمالی - کاهش وابستگی‌های متقابل بین زیرساخت‌های انرژی (آب، برق و گاز)	- معماری‌های توزیع شده وسیع - بهبود ذخیره‌سازی انرژی

جدول (۲): چکیده راه‌کارهای افزایش امنیت فیزیکی سامانه قدرت در مقابل حملات تهدیدات و حملات مخرب (برحسب بخش‌های سامانه قدرت)

قسمت‌های مربوطه	راه‌کارها
افزایش امنیت مراکز تولید	❖ رعایت اصول مربوط به مکان‌یابی مناسب، اختفاء، پراکندگی، و استحکامات در زمان احداث ❖ رعایت نکاتی در زمینه احداث مخازن سوخت ❖ رعایت نکاتی در زمینه احداث ایستگاه‌های گاز ❖ رعایت نکاتی در زمینه ساخت برج‌های خنک کن ❖ رعایت نکاتی در زمینه ساخت دودکش‌های نیروگاه ❖ رعایت نکاتی در مورد واحدهای شیمیایی نیروگاه ❖ رعایت نکاتی در زمینه سامانه‌های خنک کننده ❖ استفاده از سامانه‌های اعلام خطر و اطفای حریق کارآمد ❖ استفاده از تجهیزات امنیتی فیزیکی پیشرفته (دوربین‌ها، حسگرها، روشنایی پیشرفته) ❖ توسعه تولیدات پراکنده و منابع انرژی تجدیدپذیر (DG)
افزایش امنیت پست‌های انتقال و فوق توزیع	❖ رعایت اصول مربوط به اختفاء، پراکندگی، و استحکامات در احداث پست‌های برق ❖ مکان‌یابی مناسب و بررسی دسترس‌پذیری در زمان احداث ❖ استفاده از سامانه‌های پایش گسترده (WAMS) در کنار سامانه سنتی SCADA/EMS ❖ استفاده از تجهیزات امنیتی فیزیکی پیشرفته (دوربین‌ها، حسگرها، روشنایی پیشرفته) ❖ استفاده از یک حصار مقاوم و نرده‌های امنیتی در اطراف پست ❖ افزایش احداث و جایگزینی پست‌های داخلی (GIS) در مقابل پست‌های فضای باز ❖ استفاده از جعبه سیاه شبکه هوشمند در پست‌های انتقال (Smart Grid Black Box) ❖ افزایش مقاومت فیزیکی بدنه ترانسفورماتورها
افزایش امنیت خطوط انتقال	❖ رعایت اصول مربوطه در زمینه‌های اختفاء، پوشش و استحکامات در احداث خطوط انتقال ❖ مکان‌یابی مناسب و بررسی دسترس‌پذیری در زمان احداث ❖ در نظر گرفتن اقدامات حفاظتی اضافی در طراحی خطوط دور افتاده ❖ استفاده از دوربین‌های مادون قرمز و حسگرهای ارزان قیمت جهت پایش فنی و فیزیکی ❖ استفاده از دکل‌های خود-نگهدار در مناطق حساس ❖ استفاده از مقره‌های جدید کامپوزیت به جای مقره‌های سنتی سرامیکی و شیشه‌ای ❖ جایگزینی و احداث خطوط کابلی و زیرزمینی (GIL) به‌جای خطوط هوایی قبلی ❖ استفاده از جعبه سیاه شبکه هوشمند در خطوط انتقال (Smart Grid Black Box)
افزایش امنیت شبکه توزیع	❖ افزایش استفاده از کابل‌های زیرزمینی به‌جای خطوط هوایی در شبکه‌های توزیع ❖ افزایش استفاده از کابل‌های خود نگهدار در شبکه‌های فشار متوسط و فشار ضعیف ❖ افزایش قابلیت اتوماسیون توزیع جهت برق‌رسانی مشترکین بحرانی ❖ به‌کارگیری روش‌های حذف بار هوشمند در سامانه توزیع ❖ افزایش نفوذ تولیدات پراکنده در شبکه‌های توزیع
افزایش امنیت مراکز کنترل	❖ مکان‌یابی مناسب و بررسی دسترس‌پذیری در زمان احداث ❖ استفاده از تجهیزات امنیتی فیزیکی پیشرفته (دوربین‌ها، حسگرها، روشنایی پیشرفته) ❖ افزایش امنیت سامانه‌های ارتباطی و پردازشی در مقابل حملات سایبری ❖ در نظر گرفتن سامانه‌های پشتیبان برای مراکز کنترل ❖ توسعه بومی‌سازی در ساخت تجهیزات شبکه (به ویژه سامانه‌های ارتباطی و پردازشی)

۵- نتیجه‌گیری

در این مقاله به تاثیر جایگاه پدافند غیرعامل در جهت افزایش امنیت سامانه‌های قدرت در مقابل خرابکاری‌ها و تهدیدات پرداخته شده است. این ارزیابی به‌دلیل افزایش نگرانی‌ها نسبت به حملات خصمانه علیه زیرساخت‌های مختلف به ویژه سامانه قدرت انجام گرفته است. از اینرو، ابتدا به بررسی تهدیدات موثر شبکه‌های قدرت به همراه ارزیابی مهم‌ترین حملات صورت گرفته در این حوزه در کشورهای مختلف پرداخته شده و عواقب ناشی از وقوع آنها تشریح شده است. در ادامه، آسیب‌پذیری بخش‌های اصلی شبکه برق شامل مراکز تولید، پست‌های انتقال و فوق توزیع، خطوط انتقال، مراکز کنترل، و شبکه‌های توزیع، شناسایی و ارزیابی شده است. نهایتا، راهبردها و ایده‌های مربوطه در جهت کاش میزان آسیب‌پذیری هر یک از این مراکز معرفی گردیده که در مجموع، منجر به مقاوم‌سازی شبکه‌های برق می‌شوند. چکیده این راه‌کارها که بر اساس تجربیات سایر کشورها و تحقیقات صورت گرفته در حوزه پدافند غیرعامل به‌دست آمده، در دو جدول مجزا ارائه گردیده و اجرای آنها می‌تواند به افزایش پایداری و تاب‌آوری سامانه قدرت در مواجهه با شرایط بحرانی کمک نماید.

۶- منابع

۱. پالیزوان، محمد، بررسی کاهش آسیب‌پذیری شبکه‌های برق قدرت در مقابل حملات تروریستی، معاونت انرژی سازمان پدافند غیرعامل کشور، ۱۳۹۶.

۲. حق‌مرام، رضا، رحمانی، هادی، شناسایی تهدیدات تروریستی در یک شبکه برق و بهره‌گیری از منابع تجدیدپذیر به‌همراه خازن‌گذاری به‌منظور تقویت سطح پدافند غیرعامل، فصلنامه علمی-ترویجی پدافند غیرعامل، سال ششم، شماره ۲۱، صص ۸۶-۷۹، ۱۳۹۴.

۳. آزاده‌دل، رمضانعلی، منصف، حسن، دهقانی، حمید، مدل‌سازی و شبیه‌سازی سیستم قدرت با رویکرد پدافند غیرعامل در مقابل حملات الکترومغناطیسی، فصلنامه علمی- ترویجی پدافند غیرعامل، سال پنجم، شماره ۲۰، صص۴۰-۲۹، ۱۳۹۳.

4. E. Vugrin, A. Castillo, and C. Silva-Monroy, “Resilience Metrics for the Electric Power System: A Performance-Based Approach,” Sandia National Laboratories, Feb. 2017.

5. IET report for the Council of Science and Technology, “Modelling Requirements for GB Power System Resilience,” The Institution of Engineering and Technology, May 2015.

6. Stefan Hirschberg et al., “Health effects of technologies for power generation: Contributions from normal operation, severe accidents and terrorist threat,” Reliability Engineering and System Safety, vol. 145, pp. 373-387, 2015.

7. Electric Power Research Institute; “Electric Power System Resiliency: Challenges and Opportunities,” EPRI, Feb. 2016.

8. Y. Wang, C. Chen, J. Wang, and R. Baldick, “Research on Resilience of Power Systems under Natural Disasters-A Review,” IEEE Transactions on Power Systems, vol. 31, no. 2, pp. 1604-1613, Mar. 2016.

9. National Research Council, “Terrorism and the Electric Power Delivery System,” Washington DC: The National Academies Press, Nov. 2012.

10. National Research Council, “The Resilience of the Electric Power Delivery System in Response to Terrorism and Natural Disasters,” Summary of a Workshop, Washington DC: The National Academies Press, 2013.

11. A. Niglia et al., “The Protection of Critical Energy Infrastructure against Emerging Security Challenges,” IOS Press, 2015.

۱۲. مشهدی، حسن، امینی ورکی، سعید، تدوین و ارائه الگوی ارزیابی تهدیدات، آسیب‌پذیری و تحلیل خطرپذیری زیرساخت‌های حیاتی با تأکید بر پدافند غیرعامل، فصلنامه علمی پژوهشی مدیریت بحران، سال چهارم، شماره ۷، صص ۸۵-۶۹، ۱۳۹۴.

۱۳. مرکز مطالعات سیستم و انرژی، کاربرد پدافند غیرعامل در صنعت برق، شرکت مهندسین مشاور مونتکو، ۱۳۹۳.

۱۴. عسگری، محمد حسین، منصف، حسن، ابراهیم نژاد، محمد، ملاحظاتی در مورد طراحی نیروگاه‌های تولید برق کشور به منظور کاهش آسیب-پذیری آنها در شرایط، دومین کنفرانس نیروگاه‌های برق، ۱۳۸۸.

۱۵. گندمکار، مجید، دادفر، سجاد، عزتی، سیدمیثم، مبانی پدافند غیرعامل و مصادیق آن در صنعت برق با نگاه به مدیریت استراتژیک، چهاردهمین کنفرانس دانشجویی مهندسی برق ایران، ۱۳۹۰.

۱۶. دشتی، رضا، پدافند غیرعامل در سیستم‌های توزیع برق، دانشگاه مالک اشتر، ۱۳۹۰.

Reinforcing Power Network Infrastructures by Employing Passive Defense Applications

M. Palizvan*, R. Dashti

Abstract

Nowadays, electrical power systems which consist of generation, transmission, distribution, and control centers of electrical energy, are recognized as one of the strategic goals of modern warfare and threatened by various hazards, for which measures must be taken. Regarding the importance of power system in maintaining and sustaining communal activities, it is necessary to adopt adequate security measures to minimize threats and reduce vulnerabilities. In this context, passive defense can play an important role in the continuity of activities spanning from electric power generation up to consumption. In this paper, the influence of passive defense position upon increasing the security of power systems against sabotages and threats, has been addressed. To this end, first, the evaluation of destructive threats and related vulnerabilities in different parts of the network have been considered, then the effective strategies and ideas have been developed to decrease their vulnerability effects and increase the stability and security of network under critical and abnormal conditions. These strategies are based on the experiences of other countries and the research conducted in the field of passive defense, and can well cover most cyber and physical threats in the power grids.

Key Words: *Passive defense, electrical power systems, Reinforcement, destructive attacks*

* Passive Defense Organization of Iran (palizvan_1363@yahoo.com)- Writer-in-Charge