نشریه علمی پدافند غیرعامل

سال دوازدهم، شماره ۴، زمستان ۱۴۰۰، (پیاپی ۴۸): صص ۷۹-۶۵

علمی- ترویجی

بررسی خاموشی‌های سراسری و ارائه راهکارهای مقابله با تهدیدات و آسیب‌پذیری‌های شبکه سراسری بارویکرد پدافند غیرعامل

محمد مهرابی[۱]، حسین ذکی دیزجی[۲*]، ستار قهرمانی[۳]، محمد لطف‌آبادی[۴]

تاریخ دریافت: ۱۳۹۹/۱۲/۰۹

تاریخ پذیرش: ۱۴۰۰/۰۳/۱۷

چکیده

پدافند غیرعامل به مجموعه اقدام‌های غیرمسلحانه‌ای که موجب افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقاء پایداری ملی و تسهیل مدیریت بحران در مقابل تهدیدها و اقدام‌های نظامی دشمن می‌شود، اطلاق می‌شود. شبکه سراسری برق نیز زیربنای بسیاری از زیرساخت‌های حیاتی کشور می‌باشد و هرگونه خلل در این زیربنا، سایر زیرساخت‌های کشور تحت تأثیر قرار می‌گیرند و باعث بروز مشکلات زیاد و تأثیرات قابل توجهی بر بخش‌های مختلف جامعه می‌شود و اداره کشور را با چالش‌های جدی مواجه می‌سازد. بنابراین این مقاله ابتدا به بررسی و تحلیل عوامل مؤثر در خاموشی‌های سراسری جهان می‌پردازد. سپس با توجه به عوامل خاموشی به شناسایی تهدیدات و آسیب‌پذیری‌های شبکه سراسری برق پرداخته و راهکارهای مناسب جهت کاهش آسیب‌پذیری‌ها و به دنبال آن بهبود پایداری شبکه سراسری برق ارائه می‌نماید. در انتها نیز برای پیاده‌سازی اصول پدافند غیرعامل در برابر خاموشی‌ها، راهکارهای ذکر شده متناسب با اصول اصلی پدافند غیرعامل ارائه شده تا راهبردها و راهکارهای پدافند غیرعامل در جهت مصون‌سازی شبکه سراسری برق تبیین گردد. نتیجه این اقدامات، تداوم فعالیت برق‌رسانی در جامعه بوده و موجب افزایش پایداری ملی در برابر تهدیدات و مخاطرات می‌گردد.

کلیدواژه‌ها: خاموشی سراسری، شبکه سراسری برق، پدافند غیرعامل، تهدیدات، آسیب‌پذیری

[۱] کارشناسی ارشد، دانشکده برق، دانشگاه علم و صنعت ایران، تهران

[۲] استادیار، دانشگاه جامع امام حسین(ع)، تهران- نویسنده مسئول (kpzaki@ihu.ac.ir)

[۳] کارشناسی ارشد، سازمان پدافند غیرعامل کشور، تهران

[۴] کارشناسی ارشد، سازمان پدافند غیرعامل کشور، تهران

۱- مقدمه

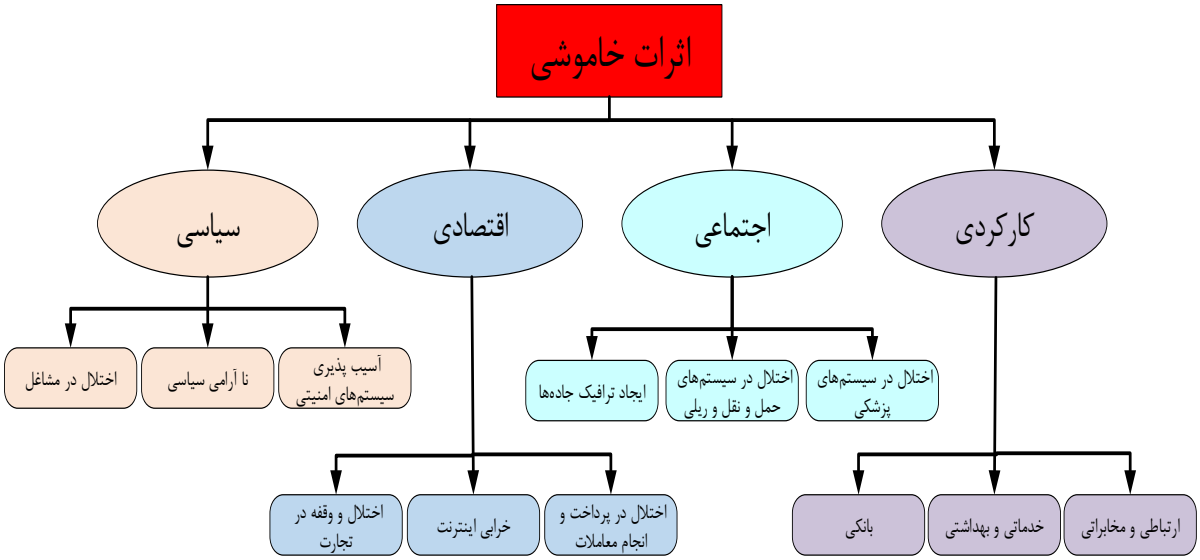
انرژی الکتریکی روز به روز در حال تبدیل شدن به یک عنصر کلیدی و مؤثر در زندگی بشر می‌باشد و تأمین توان با ضریب قابلیت اطمینان بالا یک ضرورت اساسی برای زندگی مدرن امروزی است. از این رو تقریباً تمام فعالیت‌های روزانه بشر وابسته به انرژی الکتریکی است و در صورت بروز هرگونه وقفه در این انرژی، فعالیت‌های روزانه مختل می‌شوند و تبعات زیان‌بار اجتماعی، سیاسی و اقتصادی را به دنبال دارد. در این حالت هرچه جامعه پیشرفته‌تر، وابستگی به انرژی الکتریکی بیشتر، درنتیجه وابستگی‌ها شدیدتر است. در شبکه برق، خطاها و عوامل خواسته یا ناخواسته‌ای وجود دارد که با رخ دادن آن‌ها بقیه عناصر شبکه تحت تأثیر قرار می‌گیرند. با ادامه یافتن این‌روند، پایداری شبکه به خطر افتاده و احتمال حرکت شبکه به سمت خاموشی سراسری افزایش می‌یابد [۱].

وقوع خاموشی سراسری، علاوه بر مشکلات فنی بسیاری که به وجود می‌آورد، صدمات اقتصادی، اجتماعی و سیاسی جبران‌ناپذیری در بر دارد. به‌عنوان‌مثال در تابستان سال ۲۰۰۳ خاموشی سراسری بخش وسیعی از آمریکا و کانادا را در برگرفت. این خاموشی باعث بی‌برقی بیش از ۵۰ میلیون نفر در ایالات‌متحده و کانادا شد. این خاموشی سراسری علاوه بر تأثیرات ظاهری که داشت، تأثیرات زیادی روی خدمات زیرساخت‌های مختلف مانند بانکی، خدماتی، ارتباطی و... برجای گذاشت. در این خاموشی سراسری نزدیک به 62GW از ۲۶۰ نیروگاه در کمتر از یک دقیقه از مدار خارج شد [۲]. در کشور ونزوئلا قطع برق در روز ۷ مارس ۲۰۱۹ در ساعت اوج مصرف در کاراکاس اتفاق افتاد و بعد از آن تقریباً تمام مناطق کشور بدون برق شدند. مقامات ونزوئلا توضیح دادند مخالفان در نیروگاه برق‌آبی "گوری" خرابکاری کردند. نیکلاس مادورو، رئیس‌جمهور وقت ونزوئلا، امپریالیسم آمریکا را متهم به خاموشی برق ونزوئلا کرد.

در کشور ایران نیز چند خاموشی تأثیرگذار در طی دهه‌های اخیر اتفاق افتاده است که ازجمله آن‌ها می‌توان به خاموشی‌های ۱۳۶۹/۵/۷، ۱۳۸۰/۲/۳۰ و ۱۳۸۲/۱/۱۲ در مرکز شهر اهواز و همچنین خاموشی در تاریخ ۱۳۹۵/۱۱/۸ در خوزستان اشاره کرد که به‌صورت سریالی تا ۱۳۹۵/۱۲/۶ ادامه داشت. وقوع این خاموشی‌ها در سیستم قدرت به خودی خود صورت نمی‌گیرد و ناشی از یکسری خطا در شبکه و یا تحمیل حوادث غیرقابل پیش بینی و ناگهانی به شبکه توسط گروه‌های متخاصم هستند. در سال ۱۳۸۰ وقوع یک خطای فنی در یکی از خطوط انتقال توان بین بخش شمالی با مرکزی کشور باعث خروج آن و به دنبال آن گسترش بی‌برقی در کل کشور به مدت ۹ ساعت گردید. در این شرایط انتقال توان از خطوط دیگر از بخش شمالی کشور با تولید بالاتر به بخش جنوبی از طریق خطوط در مدار امکان‌پذیر نبوده و بنابراین سایر خطوط اصلی بین مناطق به ترتیب خارج گردیدند. عملکرد اشتباه سیستم‌های حفاظتی، عدم عملکرد سریع اپراتورها از جمله دلایل اصلی گسترش بی‌برقی در کل کشور گردید. جالب این است که حادثه شروع‌کننده این خروج‌های غیرقابل کنترل تنها خروج یک خط انتقال ۴۰۰ kV بوده است [۳].

بررسی موضوع خاموشی سراسری از آن جهت بیشتر حائز اهمیت می‌گردد که قطع شدن شبکه برق می‌تواند یکی از اهداف اصلی در تهدیدات تروریستی- امنیتی، حمله های نظامی و یا اقدامات خرابکارانه باشد و به دنبال آن تبعات زیان‌بار اجتماعی، سیاسی و اقتصادی برای جامعه داشته باشد. به‌عنوان مثال عدم عملکرد صحیح ادوات حفاظتی ممکن است ناشی از حمله سایبری دشمن به شبکه سراسری و تحمیل اضافه‌بار به شبکه برق و یا ناشی از تحریک مردم به مصرف هم‌زمان توسط عوامل نفوذی دشمن باشد. بنابراین در این مقاله به بررسی علل خاموشی‌های مهم جهان و شناسایی تهدیدات و ارائه راهکارهایی متناسب با اصول پدافند غیرعامل پرداخته می‌شود. در ادامه ساختار مقاله به‌صورت زیر سازمان‌دهی شده است:

در بخش ۲ به بررسی عمده خاموشی‌های سراسری مهم جهان پرداخته شده است. سپس استخراج عوامل خاموشی به تفکیک سطوح مختلف، تهدیدات، آسیب‌پذیری‌ها و راهکارهای مقابله با آن‌ها در بخش ۳ آورده شده است. در بخش ۴ راهکارهای مقابله‌ای با رویکرد پدافند غیرعامل به تفکیک بخش‌های مختلف شبکه ارائه شده است. در نهایت در بخش ۵ نتیجه‌گیری از مقاله صورت گرفته است.



شکل (۱) اثرات خاموشی

۲- خاموشی‌های سراسری

۲-۱- صنعت برق و خاموشی‌های سراسری از منظر پدافند غیرعامل

اهمیت صنعت برق امروز بر هیچ‌کس پوشیده نیست. زندگی امروز بشر آن‌چنان با این صنعت پیوند دارد که همان‌طور که بیان شد نبود آن می‌تواند بر بخش‌های اجتماعی، سیاسی، اقتصادی و کارکردی جوامع اثرات سوء داشته باشد که در شکل (۱) قابل مشاهده می‌باشد [۴, ۵]. به هر دلیل قطع برق علاوه بر خسارت بر بخش‌های خانگی، صنعتی، تجاری و کشاورزی می‌تواند به‌عنوان یک تهدید فرا روی امنیت ملی به حساب آید. از سوی دیگر امروزه قطع برق به عنوان یک آماج با اهمیت از سوی گروه‌های تروریستی و دولت‌های متخاصم برای فلج کردن جوامع و کشورها استفاده می‌شود. لذا شناسایی تهدیدات و اتخاذ راهکارهای مناسب در برخورد با آن‌ها امری ضروری است.

بنابراین می‌توان اظهار داشت از آنجایی که شبکه برق زیرساخت زیرساخت‌های حیاتی کشور می‌باشد، لذا هرگونه خلل در این زیرساخت سایر زیرساخت‌های کشور تحت تأثیر قرار می‌گیرند که خود باعث بروز مشکلات عدیده‌ای در جامعه گردیده و می‌تواند بر بخش‌های مختلف آن تأثیرات قابل‌توجهی بگذارد و اداره کشور را با چالش‌های جدی مواجه سازد.

۲-۲- بررسی خاموشی‌های سراسری

تاکنون چندین خاموشی سراسری در جهان اتفاق افتاده است که مطالعه هر یک می‌تواند در ارائه راهکارهای پدافندی و جلوگیری از تکرار آن تجارب ارزشمندی را ارائه دهد. بدین منظور در جدول (۱) بزرگ‌ترین خاموشی‌های سراسری جهان به‌همراه علل هر یک از خاموشی‌ها تشریح شده است [۴, ۶].

در جدول (۱) شاخص‌های کلیدی ارزیابی خاموشی‌های سراسری یعنی مدت‌زمان هر خاموشی و تعداد افراد تحت تأثیر نیز ارائه شده است. بزرگی هر یک از خاموشی‌ها از دید شبکه، فعالان صنعت برق و مصرف‌کنندگان به کمک دو شاخص فوق قابل ارزیابی خواهد بود. برای مشخص شدن شدت خاموشی می‌توان هر خاموشی را متناسب با تعداد افراد تحت تأثیر نسبت به مدت‌زمان خاموشی سنجید. مسلماً خاموشی که دارای مدت‌زمان بیشتر و تعداد افراد تحت تأثیر بیشتر می‌باشد، شدت بالایی داشته است. همان گونه که از جدول (۱) مشاهده می‌شود، خاموشی ونزوئلا یکی از شدیدترین خاموشی‌ها برای یک کشور در طول تاریخ می‌باشد. همچنین خاموشی ۲۰۱۲ هند و ۲۰۰۳ آمریکا شمالی- کانادا به ترتیب دارای بیشترین افراد تحت تأثیر و بیشترین مدت‌زمان خاموشی می‌باشند.

۳- استخراج عوامل خاموشی، تهدیدات و آسیب‌پذیری‌های شبکه برق

۳-۱- بررسی علل خاموشی‌های سراسری به تفکیک عوامل مختلف

عوامل منجر به خاموشی را می‌توان به دو دسته عوامل طبیعی و عوامل غیرطبیعی تقسیم‌بندی نمود که عوامل غیرطبیعی خود به دو دسته عوامل غیرعمدی و عوامل عمدی تقسیم‌بندی می‌شوند. عوامل غیرعمدی شامل عوامل فنی، عوامل مدیریت شبکه و عوامل سیستمی که شامل سرمایه‌گذاری و بازار می‌باشند و عوامل عمدی شامل جنگ، حملات تروریستی و هکرها و دیگر گروه‌های غیر تروریستی می‌شوند[۴, ۷]. در ادامه به توضیح هر یک از این عوامل پرداخته می‌شود.

۳-۲- عوامل طبیعی

به مجموع عوامل غیر انسانی چون طوفان، سیل، رعدوبرق، آتش‌سوزی و ... اطلاق می‌شود که باعث ازکارافتادن دارایی‌های شبکه و یا تغییر شدید در بار و مصرف می‌شود. عوامل طبیعی نقش به سزایی در خاموشی‌ها داشته و به دنبال آن پیامدهای اقتصادی و اجتماعی مانند نارضایتی مردم و مصرف‌کننده‌ها و ایجاد هرج‌ومرج در جامعه را دارند (مانند خاموشی سال ۱۳۹۵ خوزستان). در شکل (۲) دسته‌بندی خاموشی‌های سراسری ناشی از عوامل طبیعی آورده شده است.

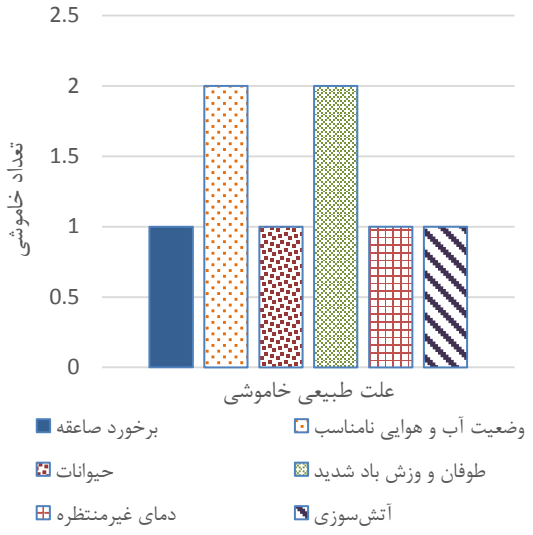
۳-۳- عوامل غیرطبیعی

این عوامل به دو گروه عوامل عمدی و غیرعمدی تقسیم‌بندی می‌شود. عوامل غیرعمدی شامل مسائل فنی، مدیریتی و سرمایه‌گذاری در شبکه سراسری می‌شود. این عوامل اگرچه در دسته‌بندی عوامل غیرعمدی لحاظ شده‌اند ولی ممکن است به وجود آمدن آن‌ها ناشی از تدابیر دشمن باشد. به عنوان مثال عدم عملکرد صحیح ادوات حفاظتی ممکن است ناشی از حمله سایبری دشمن به شبکه سراسری و همچنین تحمیل اضافه‌بار به شبکه سراسری ناشی از تحریک مردم به مصرف هم‌زمان توسط دشمن باشد؛ بنابراین عوامل غیرعمدی مؤثر در خاموشی‌های سراسری عبارت‌اند از [۷]:

جدول (۱): خاموشی‌های مهم سراسری

تاریخ و کشور خاموشی	مدت‌زمان خاموشی (ساعت)	تعداد افراد تحت تأثیر (میلیون)	علل خاموشی
۱۴ اوت ۲۰۰۳ آمریکا شمالی-کانادا	۱۶-۷۲ آمریکا تا ۱۹۲ ساعت در کانادا	۵۰	پشتیبانی توان راکتیو ناکافی، مشکلات هماهنگی و ارتباط، آگاهی وضعیت ناکافی
۲۳ سپتامبر سوئد-دانمارک	۵	۴	تریپ نیروگاه هسته‌ای
۱۲ جولای ۲۰۰۴ آتن	۵	۵	پشتیبانی توان راکتیو ناکافی، اقدامات اصلاحی نامناسب
۲۴ سپتامبر ۲۰۰۶ پاکستان	۶	۱۶۰	پشتیبانی توان راکتیو ناکافی، بهره‌برداری در نزدیکی محدوده پایداری، نقض معیار امنیتی N-1
۴ نوامبر ۲۰۰۶ اروپا	۲	۴۵	اقدامات اصلاحی نامناسب، آموزش ناکافی، مشکلات هماهنگی و ارتباط، بهره‌برداری در نزدیکی محدوده پایداری
۲۶ آوریل ۲۰۰۷ کلمبیا	۴/۵	۴۱/۱۶	مسائل حفاظتی، آموزش ناکافی، مسائل مربوط به طراحی سیستم، خطاهای تعمیر و نگهداری
۲۶ فوریه ۲۰۰۸ فلوریدا	۳	۳	آموزش ناکافی، مشکلات هماهنگی و ارتباط، خطاهای تعمیر و نگهداری
۸ سپتامبر ۲۰۱۱ مکزیک-آمریکا	۱۲	۲/۷	قطع خط انتقال
۴ فوریه ۲۰۱۱ برزیل	۱۶	۵۳	خطا روی خط انتقال و ایجاد نوسانات توان، مسائل حفاظتی،
۳۰ جولای ۲۰۱۲ هند	۱۵	۶۲۰	اضافه‌بار روی خط انتقال، پشتیبانی توان راکتیو ناکافی، اقدامات اصلاحی نامناسب، مشکلات هماهنگی و ارتباط، بهره‌برداری در نزدیکی محدوده پایداری
۲۲ می ۲۰۱۳ ویتنام	۱۰	۱۰	اپراتور جرثقیل (خطای انسانی)
۶ اوت ۲۰۱۳ فیلیپین	۱۲	۸	ناپایداری ولتاژ
۲۰۱۳ تایلند	۱۰	۸	تداخل صاعقه
۳۱ اکتبر ۲۰۱۳ سوریه	-	-	حمله تروریستی
۱ نوامبر ۲۰۱۴ بنگلادش	۲۴	۱۵۰	خروج ایستگاه HVDC
۲۶ ژانویه ۲۰۱۵ پاکستان	۲	۱۴۰	خطای فنی نیروگاه
۲۷ مارس ۲۰۱۵ هلند	۱/۵	۱	وضعیت آب‌وهوایی نامناسب
۳۱ مارس ۲۰۱۵ ترکیه	۴	۷۰	خرابی سیستم قدرت، مسائل حفاظتی، پشتیبانی توان راکتیو ناکافی، بهره‌برداری در نزدیکی محدوده پایداری، آگاهی وضعیت ناکافی، نقض معیار امنیتی N-1
۲۳ نوامبر ۲۰۱۵ اوکراین	۶	۲۳۰	حمله سایبری
۷ ژوئن ۲۰۱۶ کنیا	۴	۱۰	اتصال کوتاه ترانسفورماتور به علت یک حیوان

ادامه جدول (۱): خاموشی‌های مهم سراسری			
۲۸ سپتامبر ۲۰۱۶ استرالیا	۶/۱	۱/۷	صدمات طوفان به زیرساخت‌های سیستم انتقال و حوادث آبشار
۱ مارس ۲۰۱۷ آمریکا	۱۱	۲۱	خرابی‌های آبشاری در سیستم انتقال
۲۶ اوت ۲۰۱۷ اروگوئه	۴	۳/۴	خرابی‌های آبشاری در اثر وضعیت نامناسب آب‌وهوایی
۱۰ سپتامبر ۲۰۱۷ جنوب شرقی آمریکا	۵	۷/۶	رویدادهای آبشاری و خروج خط انتقال
۱۰ ژانویه ۲۰۱۸ سودان	۲۴	۴۱/۵	خرابی‌های آبشاری
۳ جولای ۲۰۱۸ آذربایجان	۸	۸	دمای غیرمنتظره بالا
۲۱ مارس ۲۰۱۸ برزیل	۱	۱۰	خرابی خط انتقال
۲۰ دسامبر ۲۰۱۸ کانادا	۴	۰/۴	سرعت باد شدید در حدود ۱۰۰ کیلومتر بر ساعت
مارس ۲۰۱۹ ونزوئلا	۱۶۸	کل کشور (۲۸)	آتش‌سوزی، عدم سرمایه‌گذاری کافی، عدم مدیریت شبکه



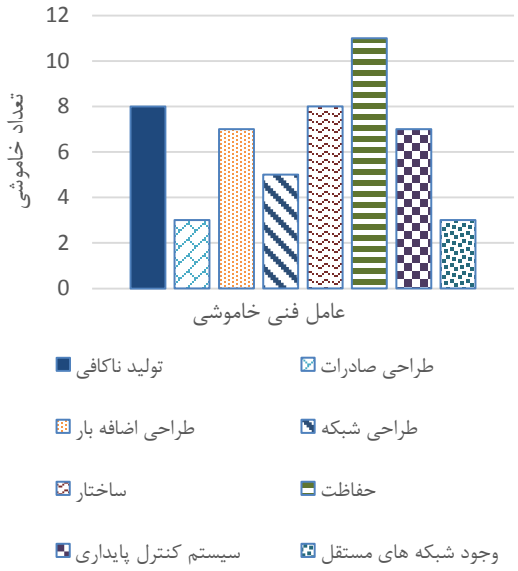
شکل (۲): دسته‌بندی خاموشی‌های سراسری ناشی از عوامل طبیعی [۷]

عوامل فنی: این عوامل به نحوه ایجاد اختلال و گسترش خطا در شبکه اشاره دارد و شامل علت‌های فنی اعم از هماهنگی‌های حفاظتی، اضافه‌بار، ساختار شبکه و ... می‌باشد. دسته‌بندی خاموشی‌های ناشی از مسائل فنی در شکل (۳) آورده شد است. همان‌گونه که مشاهده می‌شود مسائل فنی مربوط به سوءعملکرد ادوات حفاظتی نقش مؤثری در ایجاد خاموشی‌ها داشته‌اند.

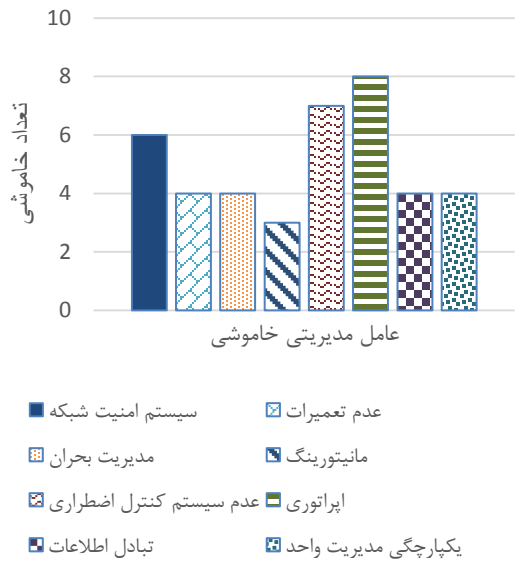
عوامل مدیریت شبکه: این عوامل شامل مدیریت شبکه در زمان وقوع حادثه و همچنین زیرساخت‌های سامانه جهت مواجهه با حادثه می‌شود. بدین ترتیب جریان صحیح و دقیق اطلاعات، اپراتوری صحیح و توازن تولید و مصرف ازجمله این عوامل هستند. دسته‌بندی خاموشی‌های ناشی از مسائل مدیریتی در شکل (۴) آورده شده است که آموزش ناکافی اپراتور جهت انجام اقدامات اصلاحی به موقع، بیشترین تأثیر در خاموشی‌ها را داشته است.

عوامل سرمایه‌گذاری و بازار تصمیم: این عوامل به مجموعه رویه‌های بازار برق و سرمایه‌گذاری مناسب و کافی اشاره دارد تا نقش آن‌ها را در خاموشی سراسری بیان نماید. دسته‌بندی خاموشی‌های ناشی از مسائل سرمایه‌گذاری و بازار تصمیم در شکل (۵) آورده شده است. همان‌گونه که مشاهده می‌شود عدم سرمایه‌گذاری کافی در شبکه سراسری بیشترین تأثیر را روی ایجاد خاموشی‌های سراسری گذاشته است.

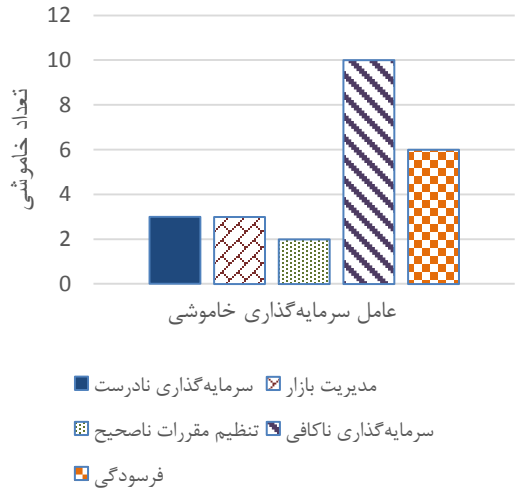
دسته دیگر عوامل غیرطبیعی مؤثر در خاموشی‌های سراسری عوامل عمدی می‌باشند. این عوامل همان‌گونه که از اسم آن‌ها مشخص است به‌صورت عمدی و خصمانه روی شبکه سراسری صورت می‌گیرند و اگر با اطلاعات و برنامه‌ریزی‌های قبلی صورت پذیرند، می‌توانند باعث ایجاد خاموشی سراسری گسترده‌ای شوند. سیستم‌های انتقال و توزیع به‌واسطه گستردگی فیزیکی و درنتیجه آسیب‌پذیری زیاد نسبت به سایر قسمت‌های شبکه، بیشتر مورد هدف حمله و اقدامات خصمانه قرار می‌گیرند. به‌طورکلی عوامل عمدی را می‌توان به سه دسته جنگ، حملات تروریستی و هکرها و دیگر افراد و گروه‌های غیر تروریستی تقسیم‌بندی نمود. شکل (۶) این موضوع را نشان می‌دهد.



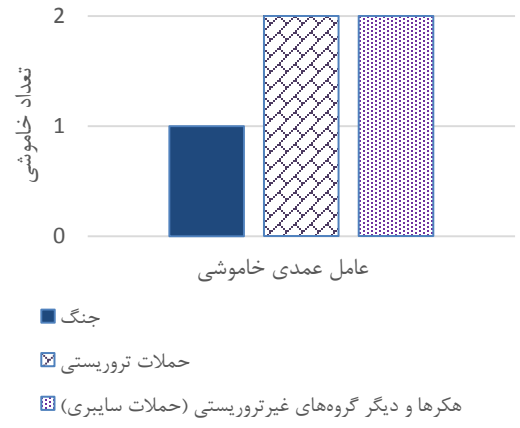
شکل (۳): دسته‌بندی خاموشی‌های سراسری ناشی از عوامل فنی [۷]



شکل (۴) دسته‌بندی خاموشی‌های ناشی از مدیریت شبکه [۷].



شکل (۵): دسته‌بندی خاموشی‌های ناشی از سرمایه‌گذاری و بازار تصمیم [۷].



شکل (۶): دسته‌بندی خاموشی‌های سراسری ناشی از عوامل عمدی [۷].

۳-۴- تهدیدات شبکه برق

تهدیدات متنوعی برای شبکه برق وجود دارد، ولی با توجه به عوامل مؤثر و تجربه جهانی در خاموشی‌های سراسری، تهدیدات کلیدی برای شبکه سراسری برق عبارت‌اند از [۷, ۸]:

۳-۴-۱- تهدیدات تروریستی - امنیتی

یکی از بزرگ‌ترین تهدیدات در زمان تهاجمات دشمن به‌ویژه از طریق حمله‌های هوایی از بین بردن دارایی‌های حساس اعم از نیروگاه‌ها، پست‌ها و خطوط انتقال می‌باشد. دارایی‌های حساس به دارایی‌هایی اطلاق می‌شود که دشمن با از کار انداختن و یا از بین بردن آن‌ها بتواند تأثیر بسیار زیادی در روند جنگ و از کار انداختن نیروهای متقابل و پیش رو بگذارد. با توجه به تحقیقات صورت گرفته در طی ۱۰ سال و از سال ۱۹۹۶ تا ۲۰۰۶، ۲۵۰۰ حمله توسط گروه‌های تروریستی به خطوط انتقال و دکل‌ها در بخش‌های مختلف جهان صورت گرفته است. پست‌های برق هدف بعدی حملات تروریست‌های بین‌المللی از نظر تکرار دفعات با بیشتر از ۵۲۸ حمله بوده است که این تعداد شامل پست‌ها و کلیدخانه‌های مجاور پست‌هاست که با موشک‌های نارنجک‌انداز، خمپاره‌اندازها، سلاح‌های کوچک و ... به‌طور واقعی و هدفمند مورد حمله قرارگرفته‌اند [۸, ۹].

مهم‌ترین راهکار در برابر این تهدیدات کاهش حساسیت و وابستگی خاموشی سراسری شبکه به یک دارایی خاص و یا به عبارتی کوچک‌سازی و ایجاد پراکندگی در فضای سرزمینی، ملی و استانی است. جهت این امر بهترین راه رعایت شرط N-1 و حتی N-2 در شبکه و همچنین استفاده از منابع تولیدات پراکنده می‌باشد. این راهکار باعث ایجاد امکان جزیره سازی شبکه در هنگام وقوع حادثه می‌شود. بدین ترتیب با از دست رفتن خطوط انتقال و نیروگاه‌های دیگر شبکه به‌طورکلی خاموش نمی‌شود و امکان تأمین حداقل بارهای مورد نیاز جهت استمرار بخشی به خدمات وجود دارد. بدین ترتیب راهکارهایی که می‌توان برای این نوع تهدیدات ارائه نمود، عبارت است از:

- ✓ اصلاح خط‌مشی مدیریت تولید به توسعه تولید در توزیع
- ✓ امکان جزیره سازی شبکه در هنگام وقوع حادثه (در صورتی که پس از جزیره سازی، در یک جزیره توازن تولید و تقاضا برقرار نبود می‌توان از راهکار حذف بار جهت برقراری توازن بین تولید و تقاضا بهره برد)
- ✓ کوچک‌سازی و ایجاد پراکندگی (استفاده از منابع تولید پراکنده)

۳-۴-۲- بمب‌ها و تهدیدات نوین

امروزه تهدیدات فرا روی شبکه‌های برق تنها به تهدیدات تروریستی، صدمات فیزیکی و کلاسیک محدود نمی‌شود. بلکه در تهدیدات نوین، استفاده از ویژگی‌های ذاتی الکتریسیته و همچنین آسیب‌پذیری‌های ذاتی شبکه برق مورد توجه قرار گرفته است. این ویژگی‌ها و خصوصیات منجر به طرح ایده برای بمب‌های جدید شده است تا با ایجاد اتصال کوتاه، اضافه ولتاژ و یا حتی ایجاد حرارت منجر به آسیب دیدن تجهیزات و یا از بین رفتن کارایی آن‌ها گردد. ازجمله مهم‌ترین این بمب‌ها می‌توان به بمب‌های الکترومغناطیسی، گرافیتی و لیزری اشاره نمود [۱۰, ۱۱].

بهترین راهکار در این بخش مقاوم‌سازی شبکه در برابر تهدیدات نوین چون شیلدینگ، ارتینگ، کوتینگ، کاهش حساسیت شبکه به یک دارایی خاص و ... است.

۳-۴-۳- تهدیدات سایبری

سیستم‌های نوین برق به‌شدت بر اتوماسیون، کنترل متمرکز تجهیزات و ارتباطات سریع تکیه دارند. حیاتی‌ترین سیستم‌ها، سیستم‌های نظارت کنترلی و گردآوری داده‌ها (SCADA) هستند که اندازه‌گیری‌های آنلاین از پست‌ها و گره‌های شبکه را جمع‌آوری می‌کنند و سیگنال‌های کنترلی را به تجهیزاتی همانند مدارشکن‌ها ارسال می‌نمایند. بسیاری از سیستم‌های کنترلی دیگر، نظیر سیستم‌های اتوماسیون و حفاظت پست‌ها هر یک می‌توانند تجهیزات محلی مشخصی را کنترل نمایند. دیگر سیستم‌های برخط کامپیوتری نظیر سیستم‌های مدیریت انرژی (که قابلیت اطمینان سیستم در قبال رخدادها را تحلیل می‌کند) یا سیستم‌های بازار (که خرید و فروش الکتریسیته را مدیریت می‌کند) تنها تأثیر غیرمستقیمی بر شبکه دارند؛ اما تمامی چنین دستگاه‌هایی به‌طور بالقوه در قبال حملات سایبری چه از طریق ارتباط اینترنتی و چه حضور فیزیکی آسیب‌پذیرند. هرگونه ارتباط از راه دور که حتی بخشی از آن خارج از کنترل بهره‌بردار سیستم باشد، به‌طور بالقوه مسیری ناامن به درون عملیات بهره‌برداری از سیستم و تهدیدی برای شبکه برق محسوب می‌شود.

هکرها در صورت دسترسی به سیستم SCADA می‌توانند برای قطع جریان برق، انتقال علائم خطا به اپراتورهای شبکه، مسدود کردن مسیر جریان اطلاعات مهم یا غیرفعال نمودن سیستم‌های حفاظتی اقدام کنند. اگرچه احتمال ایجاد خاموشی‌های گسترده توسط حملات سایبری کم است، اما چنین حملاتی در صورت هماهنگی صحیح می‌توانند صدمات ناشی از حملات فیزیکی را تشدید کنند. برای مثال قطعی‌های زنجیره‌ای زمانی بیشتر می‌شود که اپراتورها اطلاعات محل شروع خطا را دریافت نکنند یا ابزارهای حفاظتی از کار افتاده باشند. با توجه به مطالب بیان شده، انواع حملات سایبری که هدف آن‌ها عمدتاً مراکز کنترلی شبکه برق می‌باشد در جدول (۲) ارائه شده است.

جدول (۲): روش‌ها و انواع حملات سایبری [۱۲]

نوع حمله سایبری	توصیف حمله
انکار خدمات	در این روش دسترسی کاربران مجاز به سامانه و بالعکس از دست می‌رود در واقع حمله‌کننده از یک نقطه شروع به غوطه‌ور کردن کامپیوترهای هدف در پیام‌های مختلف و انسداد آمدوشد قانونی داده‌ها می‌نماید. این امر باعث می‌شود که هیچ سامانه‌ای نتواند از اینترنت استفاده و یا با سامانه‌های دیگر ارتباط برقرار کند.
انکار گسترده خدمات	در این روش به جای شروع حمله از یک منبع، هم‌زمان از تعداد زیادی سامانه توزیع‌شده اقدام به حمله می‌کنند. غالباً این کار با استفاده از کرم‌ها و تکثیر آن‌ها در رایانه‌های متعدد برای حمله به هدف صورت می‌گیرد.
ابزارهای سوءاستفاده	این ابزارها در دسترس عموم قرار دارد که می‌توانند با برخورداری از سطوح مهارتی مختلف، آسیب‌پذیری‌های موجود در شبکه‌ها را کشف و از آن طریق وارد شوند.
بمب منطقی	نوعی خرابکاری که در آن برنامه‌نویس کدی وارد برنامه می‌نماید که در صورت بروز اتفاقی خاص، برنامه خودبه‌خود یک فعالیت تخریبی را صورت می‌دهد.
اسنیفر	برنامه‌ای است که داده‌های مسیریابی شده را شنود نموده و با بررسی هر بسته در جریان داده‌ها به دنبال اطلاعات خاصی مانند کلمه‌های عبور می‌گردد.
اسب تروجان	برنامه‌ای رایانه‌ای که کلی خطرناک را مخفی می‌کند. معمولاً اسب تروجان دارای ظاهری مشابه برنامه‌های مفیدی است که کاربر تمایل به اجرای آن‌ها دارد.
ویروس	برنامه‌ای است که فایل‌های رایانه‌ای که معمولاً برنامه‌های اجرایی هستند را با وارد کردن نسخه‌ای از خود در آن فایل‌ها آلوده می‌سازد. با بارگذاری فایل‌های آلوده در حافظه، این نسخه‌ها اجرا و به ویروس امکان آلوده کردن سایر فایل‌ها را می‌دهد. بر خلاف کرم‌ها ویروس برای انتشار، نیازمند دخالت انسانی است.
کرم	برنامه‌ای رایانه‌ای مستقل که با نسخه‌برداری از خود از یک سامانه به سامانه‌ی شبکه تکثیر می‌شود. بر خلاف ویروس‌های رایانه‌ای، کرم‌ها نیازی به دخالت انسان برای انتشار ندارند.
جاسوس‌افزار	بدافزار نصب شده بدون اطلاع کاربر برای ردیابی و با ارسال داده‌ها به طرف سوم غیرمجاز به صورت پنهانی
شماره‌گیری مکرر	برنامه ساده‌ای که شماره تلفن‌های متوالی را شماره‌گیری می‌کند تا مودمی را پیدا کند
جنگ شبکه‌های بی‌سیم	روشی برای امکان ورود به شبکه‌های رایانه‌ای بی‌سیم با استفاده از یک لب تاپ، آنتن و کارت شبکه بی‌سیم که شامل گشت زنی در موقعیت‌های خاص برای دسترسی غیرمجاز می‌باشد
ارسال هرزنامه	ارسال نامه‌های پست الکترونیک تجاری ناخواسته که می‌تواند حاوی سازوکار تحویل نرم‌افزارهای مخرب و سایر تهدیدات سایبری باشد.
سرقت کلمه‌های عبور	با استفاده از هرزنامه افراد را فریب می‌دهد تا اطلاعات حساسی خود را افشا نمایند.
ساخت وب‌سایت جعلی	ایجاد یک وب‌سایت فریب برای تقلید از یک سایت واقعی و مشروع و معمولاً در مورد پست الکترونیک این عمل هنگامی رخ می‌دهد که آدرس فرستنده و دیگر بخش‌های مشخصات نامه الکترونیک تغییر داده می‌شود به‌طوری که گیرنده تصور می‌کند نامه از مبدأ معتبری ارسال شده است.
فریب	روشی که دزدان کلمه عبور برای فریب کاربران و متقاعد کردن آن‌ها از ارتباط با وب‌سایت معتبر بکار می‌برند.
بات نت	شبکه‌ای از سامانه‌های کنترل از راه دور آلوده که برای هماهنگی حملات، توزیع بدافزار و هرزنامه و پیام‌های سرقت اطلاعات، بکار برده می‌شود. بات‌ها معمولاً به صورت مخفیانه در سامانه هدف نصب می‌شوند و امکان کنترل از راه دور رایانه مورد هدف را به کاربر غیر مجاز می‌دهند تا اهداف خرابکارانه خود را محقق کنند. از بات نت‌ها به‌عنوان سربازان الکترونیکی نیز نام برده می‌شود.

بنابراین پس از پیاده‌سازی اتوماسیون و انجام پروژه‌های هوشمندسازی شبکه برق، کلیه شبکه به صورت دیجیتالی و کامپیوتری فرمان پذیر می‌شوند. بدین ترتیب با حملات سایبری اطلاعات شبکه قابل برداشت و تغییر خواهند بود و فرمان‌ها نیز می‌توانند به تناسب دلخواه گروه متخاصم تغییر کنند. راهکارهای مقابله با این تهدیدات، عبارت است از:

- ✓ ایجاد مقاوم‌سازی سایبری
- ✓ ایجاد شبکه مخابراتی مستقل جهت بهبود امنیت و پایداری سیستم‌های مخابراتی
- ✓ طراحی بهینه شارش اطلاعات شبکه با حفظ امنیت آن‌ها و دسترس‌پذیری آن‌ها برای واحدهای اجرایی و تصمیم گیر
- ✓ توسعه مانیتورینگ شبکه با ملاحظات دفاع سایبری
- ✓ مجهزسازی شبکه به سیستم اتوماسیون و هوشمندسازی جهت افزایش سرعت عمل در هنگام حادثه

۳-۴-۴- تهدیدات مردم محور

تحریک مصرف‌کنندگان به مصرف هم‌زمان ازجمله تهدیدات مردم محوری است که با تحریک مردم نسبت به افزایش ناگهانی مصرف برق شروع می‌شود و با ضعف‌های شبکه‌ای توسعه می‌یابد. معمولاً در طرح‌های شبکه اضافه‌بار تا حدودی لحاظ می‌شود. بنابراین شش روش مقابله با این تهدید وجود دارد[۱۳]:

- ✓ توسعه متوازن مراکز تولید
- ✓ کنترل بار و مدیریت تقاضای مصرف‌کنندگان به‌ویژه از طریق پارامترهای اقتصادی و قیمت شناور برق
- ✓ افزایش تعداد و ظرفیت خازن‌های نصب شده در شبکه توزیع جهت تأمین توان راکتیو در بخش توزیع و حداقل سازی توان راکتیو درخواستی از نیروگاه‌ها و شبکه انتقال توسط توزیع که موجب آزادسازی ظرفیت خطوط انتقال می‌شود
- ✓ توسعه متوازن نیروگاه‌ها با بار در مناطق جغرافیایی مختلف
- ✓ امکان سازی حذف بار
- ✓ استفاده از روش‌های حذف‌بار نوین در زمان وقوع خطا یا عیب

۳-۴-۵- نفوذ در منابع انسانی اپراتوری و مدیریت

کارمندان و پیمانکارانی که حق دسترسی به سیستم‌های برقی را دارند، در صورتی که بخواهند، می‌توانند آسیب‌های بزرگی به سیستم برق وارد کنند. ضمناً چنین کارکنانی قابلیت آسیب‌رسانی به دارایی‌های فیزیکی ترانسفورماتورها و تجهیزات پست برق را حتی مؤثرتر از حملات افراد خارج از سیستم دارند. همچنین خرابی بزرگ می‌تواند توسط اپراتور سیستم که عمداً اقداماتی را جهت قرار دادن سیستم در شرایط آسیب‌پذیر انجام می‌دهد، ایجاد کند. همچنین امکان دارد کارمندان ناراضی باعث ایجاد خطر گردند اما به‌طور معمول انتظار می‌رود به‌تنهایی دست به این کار بزنند. در مقابل یک یا چند کارمند که با عوامل خارجی در ارتباط هستند می‌توانند باعث تحمیل خسارات عمده و ایجاد اختلال و آسیب به‌مراتب بیشتری گردند. در حالی که آسیب مشابه نیز می‌تواند به‌طور مستقیم یا غیرمستقیم توسط پیمانکارانی که به تجهیزات دسترسی دارند انجام شود. یک نگرانی ظریف‌تر و شدیدتر وجود این احتمال است که پرسنل پیمانکار که در حال کار با بروز رسانی نرم‌افزارهای مهم هستند، امکان آسیب‌رسانی از طریق وارد کردن ویروس (به عنوان مثال ویروس تروجان) و یا سایر برنامه‌های کامپیوتری مخرب که می‌توانند بعداً فعال شوند را دارند و با این روش در آینده سبب اختلال در سیستم‌های کنترل گردند. به طور کلی این دسته از تهدیدات که عمدتاً به نفوذ دشمن به مراکز تصمیم گیر برمی‌گردد، دارای ابعاد گسترده و متنوعی است که می‌بایست برای هر یک راهکار جداگانه‌ای اتخاذ گردد. راهکارهای مقابله بانفوذ در بدنه اجرایی صنعت برق عبارت است از:

- ✓ مدیریت و فرماندهی واحد شبکه و همچنین برنامه‌ریزی و عملکرد هماهنگ بین مراکز برق منطقه‌ای
- ✓ تقویت اپراتورها برای بهبود توانایی آن‌ها در مقابله با اختلالات و تقویت نظارت بر آن‌ها

راهکارهای مقابله بانفوذ در بدنه مدیریت صنعت برق عبارت‌اند از:

- ✓ اجرای برنامه‌های قوی غربالگری چه برای افراد مشغول کار چه برای استخدام افراد جدید
- ✓ تنظیم مقررات در بخش‌های خصوصی صنعت برق جهت تضمین کیفیت عملکرد چون تولید مطمئن، تعمیرات مناسب و...
- ✓ توسعه خودکفایی در تولید کالا، ارائه خدمات و مشاوره
- ✓ ارتقاء نظارت بر بخش خصوصی

راهکارهای مقابله بانفوذ در بدنه وزارت نیرو و شرکت برق:

- ✓ واگذاری شبکه انتقال به بخش خصوصی
- ✓ استفاده از مردم یاری در نظارت بر شرکت‌های خدماتی و اصلاح قوانین (تدوین قوانینی چون حمایت از حقوق مصرف‌کننده جهت امکان سازی احقاق حق)

۳-۴-۶- تحریم

تحریم‌ها توانایی دولت‌ها را در کنترل و اداره امور به‌صورت اقتصادی کاهش می‌دهد که کشور مذکور را از لحاظ خرید کالا و خدمات از کشورهای دیگر با محدودیت مواجه می‌کند، درنتیجه سطح خدمات را نسبت به تقاضای جامعه کاهش می‌دهد. به‌منظور مقابله با این تهدید راهکارهای اساسی زیر وجود دارد:

- ✓ کنترل بار و مدیریت تقاضای مصرف‌کنندگان به‌ویژه از طریق پارامترهای اقتصادی و قیمت شناور برق
- ✓ توسعه خودکفایی در تولید کالا، ارائه خدمات و مشاوره
- ✓ پیاده‌سازی اقتصاد مقاومتی در صنعت برق
- ✓ اصلاح تنظیم مقررات جهت تشویق به سرمایه‌گذاری بخش تولید در توزیع
- ✓ پیاده‌سازی ارزیابی اقتصادی
- ✓ نظارت بر عملکرد اقتصادی شرکت‌های تابعه وزارت نیرو
- ✓ ایجاد تنوع در استفاده از نیروگاه‌های مختلف برق‌آبی، سیکل ترکیبی، بادی، خورشیدی، زمین‌گرمایی، هسته‌ای، لرزه‌ای
- ✓ ایجاد تنوع در منابع خرید خارجی تجهیزات و منحصربه‌فرد نبودن منبع تولید و فروش کالا، تجهیزات و ابزار مورد نیاز

۳-۵- آسیب‌پذیری شبکه برق و راهکارهای کاهش آن

در این قسمت به بررسی دارایی‌های اساسی شبکه برق به تفکیک بخش‌های مختلف و استخراج قسمت‌های آسیب‌پذیر آن در برابر تهدیدات متصور، پرداخته می‌شود [۸, ۱۲, ۱۴ و ۱۵]:

۳-۵-۱- مراکز تولید

تجهیزات و دارایی‌های اساسی مراکز تولید عبارت است از: توربین‌ها و ژنراتورها، ترانسفورماتور اصلی واحدهای نیروگاهی، تابلوها و سامانه‌های حفاظت، دکل‌های خط انتقال خروجی از نیروگاه، سامانه‌های سوخت‌رسانی و خنک‌کننده، ترانسفورماتور و سامانه مصرف داخلی نیروگاه و واحدهای شیمیایی.

مراکز تولید انرژی الکتریکی که حجم زیادی از توان مصرفی شبکه را به صورت متمرکز تولید کرده، به عنوان یکی از اهداف حملات تروریستی شناخته می‌شوند؛ زیرا در صورت 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، به طور طبیعی دارای تمهیداتی جهت مقابله با تهدیدات طبیعی یا غیرطبیعی هستند و از این رو، کمتر مورد حمله گروه‌های تروریستی قرار می‌گیرند. به طور کلی، مهم‌ترین قسمت‌های آسیب‌پذیر این مراکز به شرح زیر هستند:

- ✓ توربین و ژنراتور
- ✓ ترانسفورماتور اصلی نیروگاه
- ✓ سامانه سوخت‌رسانی
- ✓ سامانه خنک‌کننده
- ✓ سامانه برق‌رسانی داخلی
- ✓ واحدهای شیمیایی

۳-۵-۲- پست‌های انتقال و فوق توزیع

تجهیزات و دارایی‌های اساسی پست‌های فشارقوی شبکه برق عبارت است از: ترانسفورماتور قدرت، ترانسفورماتور مصرف داخلی پست، سوئیچرها شامل باسبارها، برقگیرها، سکسیونرها، مدارشکن‌ها و ترانس‌های ولتاژ و جریان، ساختمان حفاظت و کنترل، سیستم‌های مخابراتی و ارتباطی.

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 فشارقوی ملموس‌تر است. از جمله دلایلی که باعث افزایش حساسیت پست‌های برق‌رسانی می‌شود، می‌توان به وجود تجهیزات مهم و اساسی در این مراکز و همچنین مدت‌زمان زیادی که جهت جایگزینی آن‌ها لازم است، اشاره کرد. طبق یک توافق کلی میان برنامه ریزان امنیتی، کلیدی‌ترین پست‌های فشارقوی در زمره مطلوب‌ترین اهداف تروریستی در سامانه انتقال قدرت هستند. مهم‌ترین قسمت‌های آسیب‌پذیر این مراکز به شرح زیر می‌باشند:

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

۳-۵-۳- 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 بر این، تهدیدات

طبیعی مانند طوفان‌ها و یخ‌بندان‌ها نیز از عوامل طبیعی دردسرساز برای این بخش از شبکه برق محسوب می‌شوند. با این حال، در صورت بروز آسیب بر روی خطوط انتقال، می‌توانند سریعاً تعمیر شوند مگر اینکه یک حمله گسترده و هماهنگ شده انجام گرفته باشد. به طور کلی، مهم‌ترین قسمت‌های آسیب‌پذیر این مراکز به شرح زیر هستند:

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

همچنین عدم توسعه متوازن تولید با مصرف مورد نیاز در یک منطقه جغرافیایی مشخص، باعث ایجاد جذابیت مناطقی از کشور برای دولت‌های بیگانه و همسایه جهت نفوذ و ایجاد عیب می‌گردد. از طرفی نقاطی که تولید نسبت به مصرف بسیار کمتر است، برای تروریست‌ها جهت ایجاد خاموشی در آن مناطق و به احتمال بالا خاموشی سراسری به صورت دومینویی با تحمیل اضافه‌بار به کریدرها و خطوط انتقال اصلی، دارای جذابیت بالایی است. خاموشی‌های هند و ترکیه از جمله این خاموشی‌ها بود.

۳-۵-۴- 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 به طور مداوم برای نظارت بر عناصر شبکه برق 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 به نوعی مغز سامانه محسوب می‌شوند، منجر به ایجاد آسیب‌های اساسی و مخرب در شبکه می‌گردد. عمده آسیب‌پذیری این مراکز از جانب تهدیدات سایبری می‌باشد و لذا عمده تمرکز بر افزایش امنیت سایبری این مراکز است؛ زیرا معمولاً تا حد قابل قبولی از لحاظ فیزیکی، حفاظت لازم برای آن‌ها لحاظ شده است. به طور کلی تجهیزات آسیب‌پذیر مراکز کنترل به شرح زیر هستند:

- ✓ سامانه ارتباطی
- ✓ سامانه پایشی
- ✓ سامانه پردازشی

به طور نمونه برخی از مسیرهای تهدید و آسیب‌پذیری به مراکز کنترل و سامانه اسکادا در ذیل آورده شده است:

- ✓ ارتباطات اینترنتی و ارتباطات شبکه‌های تجاری (به‌عنوان نمونه می‌توان ارتباط سرور با شرکتی مثل بورس برق را مثال زد)
- ✓ به خطر افتادن با شبکه‌های خصوصی مجازی (VPNs)
- ✓ ارتباط بی‌سیمی غیرمطمئن کشف شده توسط کاربران لپ‌تاپ مهاجم
- ✓ راه‌های اتصال گروه پشتیبان به سامانه اسکادا به خصوص در مواقع برنامه‌ریزی، توسعه، تست و راه‌اندازی سامانه
- ✓ ارسال ایمیل‌های کاذب و آلوده یا هرزنامه به شبکه‌های کنترل (اسکادا)

۳-۵-۵- تجهیزات توزیع

این بخش از شبکه برق، توان را از ایستگاه انتقال خطوط و ایستگاه‌های فشار متوسط شبکه به تمام مشترکین پایین‌دست، انتقال می‌دهند. تعداد اجزای سامانه توزیع بیشتر و ظرفیت کمتری نسبت به اجزای سامانه انتقال دارند و قطعات یدکی به طور کلی در این بخش‌ها بیشتر است. ارزش، قیمت و همچنین حوزه تغذیه و میزان اثرگذاری هر یک از این دارایی‌ها بسیار کمتر از دارایی‌های انتقال است. هدف قرار دادن اجزای سامانه توزیع می‌تواند موجب بروز مشکلاتی در تأمین برق مشترکین گردد اما این مشکلات معمولاً امکان کنترل بیشتری نسبت به حملات بر روی سامانه‌های انتقال و یا مراکز تولید، دارند؛ مگر این که هدف آن‌ها قطع برق مراکز بحرانی و حساس در سامانه توزیع باشد. به طور کلی تجهیزات آسیب‌پذیر این بخش از شبکه برق به شرح زیر هستند:

- ✓ ترانسفورماتورهای توزیع
- ✓ دکل‌های برق و هادی‌های توزیع
- ✓ کنتورها و تجهیزات اندازه‌گیری
- ✓ تجهیزات الکتریک ی مشترکین

در جدول (۳) به‌طور خلاصه اقدامات جهت افزایش امنیت و کاهش آسیب‌پذیری شبکه سراسری برق در برابر تهدیدات متصور به تفکیک بخش‌های مختلف شبکه، قابل مشاهده می‌باشد. بر اساس جدول (۳) ویژگی‌های متعدد خطوط با عایق گازی (GIL) سبب می‌شود که دامنه کاربردهای آن در خطوط انتقال و توزیع افزایش یابد. به‌عنوان مثال می‌توان به موارد ذیل اشاره نمود:

- ✓ استفاده در مسیرهای بلند و صعب‌العبور
- ✓ امکان نصب در تونل مشترک تأسیسات شهری

- ✓ ارتباط میان پست‌های اصلی و فرعی شبکه
- ✓ حذف حریم‌ها و زیباسازی فضای شهری
- ✓ امکان نصب در نزدیکی خطوط راه‌آهن و فرودگاه‌ها
- ✓ ارتباطات درون نیروگاهی و ایستگاهی

۴- راهکار مقابله‌ای با رویکرد پدافند غیرعامل

پنج اصل و رکن اساسی پدافند غیرعامل شامل بازدارندگی، پایداری ملی، کاهش آسیب‌پذیری، تداوم کارکردهای ضروری و ذخیره‌سازی می‌باشد. در این بخش راهکارهای ارائه شده برای مقابله با تهدیدات و کاهش آسیب‌پذیری شبکه سراسری برق متناسب با اصول پدافند غیرعامل ارائه می‌گردد تا راهکارهای پدافند غیرعامل تبیین گردند. لذا راهکارهای اجرایی مصون‌سازی بخش‌های مختلف شبکه برق شامل بخش تولید انرژی، بخش انتقال، بخش توزیع، شبکه‌های ارتباطی و اطلاعات و بخش تجهیزات شبکه متناسب با اصول پدافند غیرعامل شامل بازدارندگی، پایداری، کاهش آسیب‌پذیری، تداوم کارکردهای ضروری و ذخیره‌سازی به ترتیب در جداول (۸- ۴) دسته‌بندی و ارائه شده است.

جدول (۳): اقدامات جهت افزایش امنیت فیزیکی و کاهش آسیب‌پذیری شبکه سراسری برق در برابر تهدیدات متصور

بخش شبکه	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 خنک‌کن • رعایت نکاتی در زمینه ساخت دودکش‌های نیروگاه • رعایت نکاتی در مورد واحدهای شیمیایی نیروگاه • رعایت نکاتی در زمینه سامانه‌های خنک‌کننده • 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 مکان‌یابی مناسب، اختفاء، پراکندگی و استحکامات در زمان احداث • مکان‌یابی مناسب و بررسی دسترس‌پذیری در زمان احداث • استفاده از سامانه‌های پایش گسترده (WAMS) در کنار سامانه‌های 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 GIS به جای AIS • افزایش مقاومت فیزیکی بدنه ترانسفورماتورها
افزایش امنیت خطوط انتقال	• رعایت اصول مربوط به مکان‌یابی مناسب، اختفاء، پراکندگی و استحکامات در زمان احداث • مکان‌یابی مناسب و بررسی دسترس‌پذیری در زمان احداث • در نظر گرفتن اقدامات حفاظتی اضافی در طراحی خطوط دور افتاده • استفاده از دوربین‌های مادون‌قرمز و حسگرهای ارزان قیمت جهت پایش فنی و فیزیکی • استفاده از دکل‌های خودنگهدار در مناطق حساس • استفاده از مقره‌های جدید کامپوزیت به جای مقره‌های سنتی سرامیکی و شیشه‌ای • افزایش استفاده از خطوط کابلی و زیرزمینی (GIL) به جای خطوط هوایی
افزایش امنیت شبکه توزیع	• افزایش استفاده از خطوط کابلی و زیرزمینی (GIL) به خطوط هوایی • افزایش استفاده از کابل‌های خودنگهدار در شبکه‌های فشار متوسط و فشار ضعیف • افزایش قابلیت اتوماسیون توزیع جهت برق‌رسانی مشترکین بحرانی • به کارگیری روش‌های حذف بار هوشمند • افزایش تولیدات پراکنده
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 و بومی‌سازی در ساخت تجهیزات شبکه (به‌ویژه سامانه‌های ارتباطی و پردازشی)

جدول (۴): راهکارهای پدافند غیرعامل در بخش تولید انرژی برق

بازدارندگی	• مکان‌یابی مناسب، کوچک‌سازی و پراکنده‌سازی مراکز تولید و نیروگاه‌ها: گسترش تولید برق از نیروگاه‌های تولید پراکنده، کوچک مقیاس و پربازده برق و تولید همزمان برق و حرارت که خود نیازمند اصلاح خط‌مشی مدیریت تولید به توسعه تولید در توزیع است. • متنوع سازی نیروگاه‌ها از طریق توسعه نیروگاه‌ها با سوخت‌های متنوع و یا تأمین سوخت از چند طریق مختلف، افزایش بهره‌برداری از منابع جدید توان اکتیو و راکتیو مانند انواع فن‌آوری‌های DG و خودروهای هیبریدی و همچنین تلاش برای افزایش سهم انرژی‌های تجدیدپذیر با اولویت انرژی‌های آبی به‌ویژه استفاده از برق تولید سدهای مرزی با در نظر گرفتن عدم قطعیت ناشی از مدیریت منابع آب • احداث نیروگاه جدید به جای توسعه نیروگاه • توسعه متوازن نیروگاه‌ها و توزیع و پراکندگی آن‌ها در مناطق جغرافیایی مختلف
پایداری	• افزایش سرعت نصب و توسعه تولید در شبکه برق • استقلال پایداری شبکه از تولید توسط نیروگاه‌های مرزها
کاهش آسیب‌پذیری	• مقاوم‌سازی ساختمانی و ساختاری • استفاده از تجهیزات امنیتی فیزیکی پیشرفته (دوربین‌ها، حسگرها، روشنایی پیشرفته) • ذخیره و تأمین سوخت مورد نیاز نیروگاه‌های سوختی از دو مسیر مجزاء
تداوم کارکردهای ضروری	• توسعه نیروگاه‌های تلمبه ذخیره‌ای و دیزل ژنراتورها • توسعه استفاده از باطری‌ها و UPSها • توسعه ذخیره‌سازی انرژی برق در محل بارهای حیاتی، حساس و مهم
ذخیره‌سازی	• مکان‌یابی مناسب ادوات داخلی نیروگاه • خاموش کردن نیروگاه در زمان ضربه و حمله

جدول (۵): راهکارهای پدافند غیرعامل در بخش انتقال

بازدارندگی	• اتصال و یکپارچگی شبکه انتقال ایران با کشورهای همسایه • یکسان‌سازی ضریب بهره‌برداری شبکه در همه جای سیستم
پایداری	• ایجاد شبکه انتقال یکپارچه منطقه‌ای بین ایران و کشورهای همسایه متحد • استفاده بیشتر از فناوری‌های الکترونیک قدرت ولتاژ بالا • استفاده بیشتر از اتصالات و لینک‌های DC
کاهش آسیب‌پذیری	• مطالعه مجدد شبکه برق و تنظیم مجدد رله‌های حفاظتی به‌صورت مستمر • هماهنگی مطمئن بین حفاظت شبکه و تولید • مدیریت بهینه بهره‌برداری از ادوات حفاظتی از جهت تعمیر و تنظیم آن‌ها • تعیین حداکثر و حداقل بارگذاری تجهیزات با توجه به قیود اقتصادی و امنیتی • اصلاح ساختار شبکه و همچنین اصلاح رویه طراحی و برنامه‌ریزی توسعه شبکه انتقال با ملاحظات عدم قطعیت بار و رشدهای ناگهانی در مطالعات شبکه لحاظ شود تا خطوط و پست‌ها اضافه‌بار نشوند • تعمیر و نگهداری منظم، ارزیابی و آزمایش نیروگاه‌ها و تجهیزات پست‌ها • مقاوم‌سازی ساختمانی و ساختاری دارایی‌های حیاتی، حساس و مهم
تداوم کارکردهای ضروری	• اصلاح ساختار شبکه و همچنین اصلاح رویه طراحی و برنامه‌ریزی توسعه شبکه انتقال به طوری که با از دست رفتن یکی از خطوط و یا پست‌ها شبکه پایدار باقی بماند
ذخیره‌سازی	• انباشت تجهیزات موردنیاز در زمان حادثه

جدول (۶): راهکارهای پدافند غیرعامل در بخش توزیع

بازدارندگی	• یکسان‌سازی ضریب بهره‌برداری شبکه در همه جای سیستم • نیروگاه‌ها با ظرفیت کم و تعداد زیاد • پست‌ها با ظرفیت کم و تعداد زیاد • مشابه‌سازی با مبلمان شهری، مسقف نمودن، احداث فیدرها و پست‌ها به صورت زیرزمینی و همچنین پست‌های کیوسکی
پایداری	• امکان‌سازی جزیره‌ای نمودن شبکه برق و تولید محلی
کاهش آسیب‌پذیری	• مطالعه مجدد شبکه برق و تنظیم مجدد رله‌های حفاظتی به صورت مستمر • مدیریت بهینه بهره‌برداری از ادوات حفاظتی از جهت تعمیر و تنظیم آن‌ها • تعیین حداکثر و حداقل بارگذاری تجهیزات با توجه به قیود اقتصادی و امنیتی • تعمیر و نگهداری منظم، ارزیابی و آزمایش خطوط و پست‌ها • مقاوم‌سازی ساختمانی و مقاوم‌سازی الکتریکی دارایی‌های شبکه اعم از خطوط و پست‌ها • مقاوم‌سازی در برابر تهدیدات نوین چون شیلدینگ، اصلاح ارتینگ و کوتینگ
تداوم کارکردهای ضروری	• توسعه نقاط مانور و کلیدزنی • توسعه تولیدات پراکنده • توسعه خودتامینی مشترکین و تولیدات اضطراری • هوشمندسازی شبکه با ملاحظات دفاع سایبری جهت پایش و تسریع انجام فعالیت‌ها • امکان دستی نمودن فعالیت‌های شبکه جهت اقدام در زمان شکست دفاع سایبری
ذخیره‌سازی	• انباشت تجهیزات موردنیاز در زمان حادثه • توسعه استفاده از ذخیره‌سازها • توسعه استفاده از خودروهای برقی

جدول (۷): راهکارهای پدافند غیرعامل در بخش شبکه ارتباطی و اطلاعات

بازدارندگی	• کنترل ورود و خروج اطلاعات و محدودیت دسترسی جهت کاهش نفوذپذیری آن‌ها • دخالت دادن ملاحظات پدافند غیرعامل در مکان‌یابی مراکز جمع‌آوری و تحلیل بازدارندگی اطلاعات شبکه و سیستم • احداث مراکز کنترل در منطقه‌ای حفاظت شده و جلوگیری از شفاف شدن مکان مراکز دیسپاچینگ
پایداری	• ایجاد مقاوم‌سازی و برقراری تمهیدات دفاع سایبری در سامانه‌های اتوماسیون و دیسپاچینگ، مدیریت خاموشی، صورتحساب مشترکین، بازار برق، حقوق و پرداخت، کنترل پروژه و نرم‌افزارهای برنامه‌ریزی فنی • طراحی بهینه شارش اطلاعات شبکه با حفظ امنیت آن‌ها و دسترس‌پذیری آن‌ها برای واحدهای اجرایی و تصمیم گیر
کاهش آسیب‌پذیری	• مقاوم‌سازی و حفاظت فیزیکی از شبکه مخابراتی برق در برابر تهدیدات سایبری و تروریستی • استفاده از رمزنگاری، قفل‌های سخت‌افزاری و نرم‌افزاری و ... جهت ارتقاء امنیت شبکه نرم‌افزارها در برابر تهدیدات سایبری و تروریستی • مقاوم‌سازی دیسپاچینگ‌ها و ایستگاه‌های اطلاعاتی از نظر سازه‌ای • ایجاد شبکه مخابراتی مستقل جهت بهبود امنیت و پایداری سیستم‌های مخابراتی • پیاده‌سازی ملاحظات دفاع سایبری در طرح نصب و بهره‌برداری دارایی‌ها (خطوط، پست‌ها و نیروگاه‌ها)
تداوم کارکردهای ضروری	• عدم پیاده‌سازی کنترل مستقیم بار به صورت هوشمند • عدم وابستگی کامل خدمات اضطراری به فضای تبادل اطلاعات مکانیزه و امکان دستی نمودن اجرای دستورات و تصمیمات
ذخیره‌سازی	• تهیه و ذخیره پشتیبان از اطلاعات مهم

جدول (۸): راهکارهای پدافند غیرعامل در بخش تجهیزات

بازدارندگی	• کاهش و یا حذف وابستگی به تولیدکنندگان خارجی و خودکفایی در تولید تجهیزات • تعدد و پراکندگی انبار تجهیزات
پایداری	• وجود سیستم‌های پایش کیفیت خرید تجهیزات
کاهش آسیب‌پذیری	• سرویس، تعمیر و آماده نگاه داشتن تجهیزات یدکی
تداوم کارکردهای ضروری	• امکان و سهولت انتقال تجهیزات از انبار • مکان‌یابی بهینه انبار • تعداد و پراکندگی انبار تجهیزات جهت دسترسی آسان
ذخیره‌سازی	• انبار کالاهای راهبردی موردنیاز در زمان بحران به ویژه ژنراتورهای موبایل و دیزل ژنراتورها

جدول (۹): تجمیع راهکارهای پدافند غیرعامل برای کل شبکه سراسری برق

بازدارندگی	• کوچک‌سازی و پراکنده‌سازی • ایجاد راهبرد اختفاء و استتار • یکسان‌سازی ضریب بهره‌برداری در شبکه • خودکفایی در شبکه
پایداری	• توسعه استفاده از لینک‌ها و اتصالات DC • ایجاد قابلیت جزیره‌سازی و تولید محلی در شبکه • مقاوم‌سازی سایبری • استفاده از سیستم‌های پایش پیشرفته و طراحی بهینه شارش اطلاعات شبکه و ایجاد محدودیت در دسترس‌پذیری آن‌ها
کاهش آسیب‌پذیری	• مقاوم‌سازی ساختاری • مقاوم‌سازی در برابر تهدیدات نوین • مطالعه و تنظیم مستمر رله‌های حفاظتی، مدیریت و هماهنگی بهینه آن‌ها • تعیین میزان حداقل و حداکثر بارگذاری تجهیزات شبکه • طراحی برنامه‌های تعمیر و نگهداری‌های منظم • پیاده‌سازی ملاحظات دفاع سایبری
تداوم کارکردهای ضروری	• توسعه تولیدات پراکنده • ذخیره‌سازی انرژی برق به ترتیب در محل بارهای حیاتی، حساس و مهم • اصلاح ساختار شبکه جهت برآوردن معیار امنیتی N-1 و حتی N-2 • توسعه نقاط مانور و کلیدزنی در شبکه • هوشمندسازی شبکه با ملاحظات دفاع سایبری
ذخیره‌سازی	• انباشت تجهیزات مورد نیاز در زمان حادثه و بحران • توسعه استفاده از ذخیره‌سازها و خودروهای برقی • تهیه فایل‌های پشتیبان از اطلاعات مهم شبکه

۵- نتیجه‌گیری

امروزه تمام فعالیت‌های روزانه بشر وابسته به انرژی الکتریکی است و در صورت بروز هرگونه وقفه در این انرژی، فعالیت‌های روزانه مختل می‌شوند و ضرر و آسیب‌های بیشمار اقتصادی، سیاسی، اجتماعی و کارکردی برای جوامع مختلف به دنبال دارد. متأسفانه در چند دهه اخیر با توجه به افزایش مصرف برق و به تبع آن افزایش میزان تولید و گسترش شبکه‌های برق‌رسانی مشکلاتی نیز با آن همراه شده که یکی از آن‌ها خاموشی سراسری سیستم قدرت است. تحلیل و بررسی اتفاقات رخ داده در این زمینه ما را برای جبران و جلوگیری از پیش آمدن حوادث مشابه آن یاری می‌کند. بنابراین در این مقاله با بررسی تعدادی از خاموشی‌های مهم جهان، عوامل مؤثر در این خاموشی‌ها مورد بررسی قرار گرفت و به دنبال آن تهدیدات پیش روی شبکه سراسری و قسمت‌های آسیب‌پذیر آن و ارائه اقدامات لازم ارائه گردید. در انتها جهت پیاده‌سازی اصول پدافند غیرعامل در برابر خاموشی‌ها، تناظر راهکارهای ارائه شده متناسب با اصول اصلی پدافند غیرعامل صورت گرفت تا راهبردها و راهکارهای پدافند

غیرعامل در جهت مصون‌سازی شبکه سراسری برق تبیین گردد. حال با توجه به راهکارهای پدافند غیرعامل ذکر شده در بخش ۴، اکنون می‌توان با ادغام و تلفیق این راهکارها، یک جدول واحـد از راهکارهای پدافند غیرعامل برای کل شبکه برق ارائه نمود که این راهکارها در جدول (۹) نشان داده شده است. نتیجه این اقدامات، تداوم کارکردها و فعالیت بـرق‌رسـانی در جامعـه شـده و موجـب افزایش پایداری ملی در برابر تهدیدات و مخاطرات می‌گردد.

۶- مراجع

[1] N. C. Chakraborty, A. Banerji, and S. Biswas, "Survey on major blackouts analysis and prevention methodologies," presented at the Michael Faraday IET International Summit, 2015 .

[2] S.-K. Joo, J.-C. Kim, and C.-C. Liu, "Empirical analysis of the impact of 2003 blackout on security values of US utilities and electrical equipment manufacturing firms," IEEE Trans Power Syst, vol. 22, no. 3, pp. 1012-1018, 2007.

[3] M. Sanaye-Pasand, "Scrutiny of the Iranian national grid," IEEE Power Energ Mag, vol. 5 , no. 1, pp. 31-39, 2006.

[4] H. Haes Alhelou, M. E. Hamedani-Golshan, T. C. Njenda, and P. Siano, "A survey on power system blackout and cascading events: Research motivations and challenges," Energies, vol. 12, no. 4, p. 682, 2019.

[5] M. Shuai, W. Chengzhi, Y. Shiwen, G. Hao, Y. Jufang, and H. Hui, "Review on economic loss assessment of power outages," Procedia Comput Sci, vol. 130, pp. 1158-1163, 2018.

[6] O. P. Veloza and F. Santamaria, "Analysis of major blackouts from 2003 to 2015: Classification of incidents and review of main causes," The Electricity Journal, vol. 29, no. 7, pp. 42-49, 2016.

[7] R. Dashti, Analysis of electricity blackouts in the world and passive defense solutions. Tehran, Passive Defense Organization, 2015.(in persian)

[8] N. R. Council, Terrorism and the electric power delivery system. National Academies Press, 2012.

[9] E. Lipton, "US report lists possibilities for terrorist attacks and likely toll," New York Times, vol. 16, 2005.

[10] W. Radasky, "High-altitude EMP (HEMP) Environments and Effects," NBC Report, pp. 24-29, 2002.

[11] R. Azadehdel, H. Monsef, and H. Dehghani, "Power System Modeling and Simulation of Power Systems with Passive Defense Approachagainst Electromagnetic Attacks," Passive Defense Quarterly, vol. 20, no. 5, pp. 29-40, 2014. (in persian)

[12] H. Skandary, Technical analysis of passive defense considerations in power plants and substations. Tehran, Bostan Hamid, 2014 .(in persian)

[13] P. J. Maliszewski and C. Perrings, "Factors in the resilience of electrical power distribution infrastructures," Appl Geogr, vol. 32, no. 2, pp. 668-679, 2012.

[14] N. R. Council, The resilience of the electric power delivery system in response to terrorism and natural disasters: summary of a workshop. National Academies Press, 2013.

[15] M. Palizvan and R. Dashti, "Enhancing Security of Power Transmission Systems Against Destructive Attacks in the Field of the Passive Defense " Passive Defense Quarterly, vol. 9, no. 3, pp. 11-19, 2018. (in persian)

An Enquiry into Blackouts and the Presentation of Solutions to Deal with Threats and Vulnerabilities of the Power Network Through the Passive Defense Approach

M. Mehrabi[1], H. Zakidizaji[2*], S. Ghahremani[3], M. Lotfabadi[4]

Abstract

The term of passive defense refers to a set of unarmed actions that increase deterrence, reduce vulnerability, guarantee the continual of essential activities, promote national stability and facilitate crisis management in the face of enemy threats and military actions. The electrical power grid is an infrastructure, vital for the country and any disruptions in the grid, affects other infrastructures of the country. In such circumstances, many problems emerge which have significant effects on different sections of society and cause serious challenges to the administration of the country. Hence in this article, first the factors affecting power blackouts around the world are analyzed, then regarding the causes of blackouts, the threats and vulnerabilities of the national power grid are identified and appropriate solutions are provided to reduce the vulnerabilities and to improve the stability of the national power grid. In order to implement the principles of passive defense against blackouts, these solutions are proposed with consideration of the main principles of passive defense. Finally, the strategies of passive defense required for enhancing the national power grid security are determined based on the proposed solutions. The result of these strategies is the continuity of electricity supply for the society and the proliferation of national resilience against threats and dangers.

Key Words: *Blackout, Power Grid, Passive Defense, Threats, Vulnerability*

* Imam Hossein Comprehensive University (kpzaki@ihu.ac.ir) -Writer-in-Charge