

مجله علمی ترویجی «پدافند غیرعامل»

سال یازدهم، شماره ۳، پاییز ۱۳۹۹، (پیاپی ۴۳): صص ۱-۱۴

علمی - ترویجی

راهبردهای نوین حفاظت از زیرساخت‌های حیاتی

سید محسن میریوسفی^۱، رضا غفارپور^{۲*}

تاریخ دریافت: ۱۳۹۸/۰۴/۲۰

تاریخ پذیرش: ۱۳۹۸/۱۱/۲۸

چکیده

امروزه زیرساخت‌های حیاتی در برابر حوادث طبیعی، حملات عمدی فیزیکی یا سایبری و تجاوز کشورهای متخاصم بیش از قبل آسیب‌پذیر هستند. به علاوه، از آنجایی که بیشتر عملکردهای جامعه وابستگی شدیدی به عاملیت زیرساخت‌های حیاتی دارد، هر گونه اختلال در کارکرد یکی از زیرساخت‌ها می‌تواند منجر به ایجاد پیامدهای مخرب در سایر زیرساخت‌های وابسته و به تبع آن در کل جامعه گردد. از این رو، بحث حفاظت از زیرساخت‌های حیاتی به یکی از اولویت‌های تحقیقاتی قرن بیست و یک تبدیل شده است. در کشور ما، مستحکم‌سازی زیرساخت‌های حیاتی و کاهش احتمال حملات عمدی، آسیب‌پذیری‌ها و پیامدهای مخرب، تنها با رعایت الزامات پدافند غیرعامل محقق می‌گردد. حفاظت از زیرساخت‌های حیاتی در مقابله با انواع مختلف تهدیدات، به عنوان یکی از اهداف پدافند غیرعامل، با ایجاد و توسعه راهبردهای حفاظتی مناسب و کارا امکان‌پذیر است. در این مقاله، برخی شیوه‌ها و راهبردهای ملی حفاظت از زیرساخت‌های حیاتی بیان شده است. با ظهور و توسعه مفاهیم جدیدی همچون تاب‌آوری در این حوزه، سیاست‌ها، راهبردها و اقدامات مشترک طرح‌های ملی حفاظت از زیرساخت‌های حیاتی تحلیل گردیده است. در نهایت، برخی اهداف راهبردی بعلاوه مهمترین الزامات و چالش‌های پیش‌روی حوزه حفاظت از زیرساخت‌های حیاتی به منظور توسعه چارچوب‌ها و با دیدگاهی آینده پژوهانه مطرح شده است. بدین ترتیب، با استفاده از روش مطالعات تطبیقی، برخی الزامات اولیه در رابطه با راهبرد ملی حفاظت از زیرساخت‌های حیاتی استخراج و تحلیل شده است که می‌تواند گامی موثر در پیشبرد اهداف پدافند غیرعامل کشور محسوب گردد.

کلیدواژه‌ها: حفاظت از زیرساخت‌های حیاتی، زیرساخت‌های حیاتی، امنیت، تاب‌آوری، آسیب‌پذیری، پدافند غیرعامل

^۱ باشگاه پژوهشگران جوان و نخبگان، واحد اردبیل، دانشگاه آزاد اسلامی، اردبیل، ایران
^۲ استادیار دانشگاه جامع امام حسین (ع) - (rghaffarpour@ihu.ac.ir) - نویسنده مسئول

۱- مقدمه

اجرای الزامات پدافند غیرعامل در حوزه زیرساخت‌های حیاتی، می‌تواند در راستای کاهش اثرات و آسیب‌های ناشی از فجایع طبیعی و حوادث آب و هوایی نیز اثر بخش بوده و موجب تسهیل مدیریت بحران شود.

بنابراین، دو مسأله تغییر شکل و تشدید تهدیدات مربوط به حوزه زیرساخت‌های حیاتی، بررسی و بروزرسانی سیاست‌ها و راهبردهای اتخاذ شده در این حوزه را الزام آور ساخته است. در این راستا، بازنگری و اصلاح طرح‌ها و برنامه‌های حفاظت از زیرساخت‌های حیاتی، چند سالی است که در دستور کار کشورهای بسیاری قرار گرفته است. برنامه حفاظت از زیرساخت‌های حیاتی اتحادیه اروپا^۲ (EPCIP) و برنامه حفاظت از زیرساخت‌های ملی ایالات متحده^۳ (NIPP) از این جمله هستند.

در کشور ما نیز، تجربه وقوع حوادث در زیرساخت‌های مختلف نشان داده است که توجه انحصاری به بحث حفاظت بدون بهره‌مندی از مفاهیم پدافند غیرعامل، امری شکننده، پرهزینه و حتی غیرقابل جبران است. حفاظت کامل از سامانه‌ها و زیرساخت‌های حیاتی علاوه بر حفاظت فیزیکی و الزامات نظامی - امنیتی، با اجرای ضوابط و الزامات پدافند غیرعامل محقق می‌گردد. در بند اول سیاست‌های کلی نظام در خصوص پدافند غیرعامل مصوب مجمع تشخیص مصلحت نظام، مجموعه اقدامات غیرمسلحانه که موجب افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقاء پایداری ملی و تسهیل مدیریت بحران در مقابل تهدیدات و اقدامات نظامی دشمن می‌گردد، به عنوان مفهوم پدافند غیرعامل تعریف شده است. یکی از تفاسیری که از مسأله ارتقاء پایداری ملی بیان شده عبارتست از پایداری زیرساخت‌ها در برابر بحران‌های پیش رو به طوری که تمام دستگاه‌ها مقاومت نموده و حکومت بتواند تعادل خود را حفظ نماید [۴].

پایداری سازی زیرساخت‌ها و کاهش آسیب‌پذیری آن‌ها در برابر تهدیدات، از مهمترین اهداف پدافند غیرعامل است. تاب‌آوری^۴ به عنوان مفهومی جدید در حوزه پدافند غیرعامل، در پی دستیابی به این مهم است. از دیدگاه سامان‌های، یک سامانه در صورتی تاب‌آور است که با وجود تغییر شرایط در محیط عملکرد، هر چند این تغییر طولانی مدت باشد، ویژگی سازگار بودن^۵ سامانه، آن را در سطح قابل قبولی از پایداری عملکرد و ساختار قرار دهد و سامانه به کلی دچار خرابی نشود [۵]. از دیدگاه مهندسی

اقتصاد پایدار و توسعه جوامع، بدون برنامه‌ریزی راهبردی برای حفاظت و تأمین امنیت زیرساخت‌های حیاتی امکان‌پذیر نیست. زیرساخت‌های برق، گاز، آب و فاضلاب، نفت و پتروشیمی، ارتباطات و مخابرات، حمل و نقل، بانکداری و خدمات مالی، کشاورزی و تغذیه، سلامت و بهداشت عمومی و خدمات اضطراری از جمله زیرساخت‌های حیاتی هستند که نقش کلیدی در توسعه و پایداری جوامع امروز دارند. در سال‌های اخیر، به واسطه صدمات ناشی از تشدید حملات عامدانه، فجایع طبیعی و حوادث شدید آب و هوایی، مسأله حفاظت از زیرساخت‌های حیاتی^۱ (CIP) اهمیتی دوچندان یافته است [۱].

حملات عامدانه به تهدیدات فیزیکی و سایبری اطلاق می‌شود که از روی دشمنی و برای ایجاد اختلال در سامانه‌های زیرساختی انجام می‌گیرد. حملات نظامی، تروریستی، عملیات نفوذ و خرابکاری مهمترین تهدیدات حوزه زیرساخت‌های حیاتی هستند که می‌توانند به دو صورت فیزیکی و سایبری موجبات آسیب‌پذیری این سامانه‌ها را فراهم آورده و در نتیجه ساختار سیاسی و امنیتی کشورها را حتی در مقیاس‌های ملی با خسارات جبران‌ناپذیر مواجه سازند. از آنجا که تأسیسات و دارایی‌های زیرساختی نسبت به ساختارهای دولتی و نظامی، اهداف آسیب‌پذیرتر و در دسترس‌تری هستند، زیرساخت‌های حیاتی یکی از اهداف جذاب برای حملات عامدانه محسوب می‌شوند [۲]. از این رو، حفاظت از زیرساخت‌های حیاتی در برابر حملات عامدانه، بیشترین توجهات را بین متولیان زیرساخت‌ها و محققان این حوزه به خود اختصاص داده است.

با توجه به گرم شدن زمین و در نتیجه تغییرات آب و هوایی، وقوع فجایع طبیعی و حوادث شدید آب و هوایی در چند سال اخیر افزایش یافته است [۳]. این حوادث از آنجا که گستره جغرافیایی وسیعی را تحت تاثیر قرار می‌دهند، می‌توانند تجهیزات مختلفی از یک زیرساخت یا حتی چند زیرساخت مختلف را به طور هم‌زمان با اختلال و صدمات جدی مواجه ساخته و منجر به ایجاد پیامدهای مخرب در سایر زیرساخت‌های وابسته و به تبع آن ناامنی در کل جامعه گردد. باید توجه داشت، هر چند در کشور ما برنامه‌ریزی در جهت پیش‌بینی و کاهش آسیب‌پذیری‌های ناشی از تهدیدات طبیعی مانند سیل، طوفان و زلزله بر عهده سازمان مدیریت بحران است، اما در صورتی که این حوادث در مناطق یا شرایطی رخ دهد که احتمال بروز حملات نظامی یا مشکلات امنیتی را در پی داشته باشند، در حوزه اقدامات سازمان پدافند غیرعامل نیز تلقی می‌گردد. از این رو،

^۲ European Programme for Critical Infrastructure Protection

^۳ National Infrastructure Protection Plan

^۴ Resilience

^۵ Compatibility

^۱ Critical Infrastructure Protection

پیشگیری^۵ یا کاهش اثرات^۶ یک حادثه مخرب تعریف شده است. به عبارت دیگر، حفاظت از زیرساخت‌های حیاتی، مجموعه اقدامات و فعالیت‌های مقاوم‌سازی^۷ برای تضمین عاملیت و تداوم کارکرد زیرساخت‌ها را شامل می‌شود. نکته حائز اهمیت در این تعاریف این است که دیدگاه‌های اولیه در ارتباط با مفهوم حفاظت از زیرساخت‌های حیاتی، تنها مباحث پیشگیری و مقاوم‌سازی زیرساخت‌ها را طرح کرده است؛ اما با ظهور مفهوم تاب‌آوری در این حوزه، ویژگی‌های دیگری نظیر قابلیت انطباق، جذب، پاسخ و بازیابی سریع نیز برای امنیت زیرساخت‌ها در نظر گرفته شده است [۷]. در این بخش، لزوم تغییر نگرش نسبت به مفاهیم حفاظت و تاب‌آوری زیرساخت‌های حیاتی، با بیان خط سیر تحول و تکامل این دو مفهوم نشان داده شده است.

در مراحل اولیه بحث‌های حفاظت از زیرساخت‌های حیاتی، به ویژه در ایالات متحده آمریکا، به‌طور برجسته‌ای تمرکز روی تهدیدات مربوط به تروریسم معطوف شده است [۸]. این مورد حتی قبل از حادثه ۱۱ سپتامبر نیز قابل مشاهده است. برای مثال در گزارش نهاد ریاست جمهوری ایالات متحده^۸ در سال ۱۹۹۷ اظهار شده است که با وجود طراحی ضعیف زیرساخت‌های حیاتی کشور، احتمال اینکه حوادث و فجایع طبیعی زیرساخت‌های کشور را تهدید کند، بسیار بالاست؛ این درحالی است که تمرکز اصلی دولت بیشتر متوجه تلاش‌های دشمن برای آسیب رساندن، سوء استفاده یا خرابکاری در زیرساخت‌ها متمرکز بوده است [۹].

تاکیدات و توجهات روی حملات عمدی پس از حادثه یازدهم سپتامبر به شدت افزایش یافت. این مسأله که کشورهای غربی با یک دشمن باهوش و مصمم مواجه هستند که دائم به دنبال تحمیل بیشترین خسارت به زیرساخت‌هاست، دیدگاه غالب آن زمان بود. در نتیجه، این موضوع که تمرکز اصلی بایستی روی تجزیه و تحلیل بدترین حالت ممکن معطوف باشد، در ایالات متحده بسیار شایع شد [۱۰]. این رویکرد تا حد زیادی توسط اتحادیه اروپا نیز تقلید شد. حملات تروریستی بویژه بمب گذاری‌های ۲۰۰۴ مادرید و ۲۰۰۵ لندن، عامل اصلی پایه‌گذاری طرح اروپا برای حفاظت از زیرساخت‌های حیاتی (EPCIP) بودند [۱۱].

پس از طوفان کاترینا در سال ۲۰۰۵، احیای نسبی رویکردهای همه جانبه یعنی در نظرگیری همه‌ی خطرات و

زیرساخت، تاب‌آوری توانایی مشترک سامانه‌های توزیع وابسته به هم، برای مقاومت^۱ در برابر خطاهای احتمالی چندگانه، جذب^۲ آسیب‌های اولیه و بازگشت سریع^۳ به شرایط عملکرد نرمال تعریف شده است [۶].

در واقع آنچه تاب‌آوری بر آن تاکید دارد، توانایی سامانه برای پیش‌بینی و جذب اختلالات بالقوه، توسعه قابلیت انطباق^۴ سامانه برای سازگاری با تغییرات درونی یا بیرونی سامانه و پایه‌ریزی رفتارهای هدفمند برای سامانه یا زیرساخت در پاسخ به اختلالات و تهدیدات است [۷]. همانطور که مشاهده می‌گردد به منظور تأمین امنیت زیرساخت‌های حیاتی، جدای از شناخت مفاهیم پایه‌ای این حوزه نظیر تهدیدات، ریسک و آسیب‌پذیری‌ها، وابستگی زیرساخت‌ها و اولویت‌ها، توسعه و بکارگیری مفهوم تاب‌آوری در طرح‌ها و راهبردهای حفاظت از زیرساخت‌های حیاتی امری ضروری و حائز اهمیت است.

این مقاله با محوریت ارائه رویه‌های کلی در مسأله حفاظت از زیرساخت‌های حیاتی، برخی شیوه‌های تأمین امنیت آن‌ها در کشورهای مختلف را بصورت عام بحث نموده و راهبردها و مفاد کلی آن را تدوین کرده است. تاکید عمده این مطالعه، معطوف اصلی‌ترین و جدیدترین چالش‌های پیش روی حوزه حفاظت از سامانه‌های زیرساختی می‌باشد؛ که هدف آرمانی هدایت پژوهشگران و محققان کشور به سمت توسعه و بروزرسانی چارچوب‌ها، سیاست‌ها و راهبردهای موجود با استفاده از مباحث جدیدی همچون تاب‌آوری را دنبال می‌کند.

در این راستا، لزوم تغییر نگرش نسبت به مفاهیم حفاظت و تاب‌آوری زیرساخت‌های حیاتی به عنوان یکی از مهمترین اهداف این تحقیق، در بخش دوم مقاله بحث شده که تاکنون مطالعه‌ای در این خصوص در کشور ارائه نگردیده است. بخش سوم مقاله به بیان راهبردهای حفاظت از زیرساخت‌های حیاتی از منظر دستورالعمل‌ها، راهبردها و سیاست‌های راهبردی برخی کشورها پرداخته است. در بخش چهارم، الزامات اولیه در رابطه با راهبرد ملی حفاظت از زیرساخت‌های حیاتی، با شناسایی و تحلیل نقاط تمرکز، اولویت‌ها و چالش‌های راهبردی در این حوزه با رویکردی آینده پژوهانه ارائه شده است.

۲- لزوم تغییر نگرش نسبت به مفاهیم حفاظت و

تاب‌آوری زیرساخت‌های حیاتی

حفاظت از زیرساخت‌های حیاتی در ساده‌ترین حالت، توانایی

⁵ Prevention

⁶ Mitigation

⁷ Hardening or Withstanding

⁸ US Presidential Report

¹ Resist

² Absorbability

³ Rapid Recovery

⁴ Adaptability

نیز پیش‌تاز بود [۱۸]. در آخرین نسخه منتشرشده از برنامه حفاظت از زیرساخت‌های ملی [۱۹] در سال ۲۰۱۳، حفاظت از زیرساخت‌های حیاتی به عنوان عامل توانمندساز تاب‌آوری زیرساخت‌ها تعریف شده است. پس از آن، در تمامی رویکردهای ایالات متحده در ارتباط با امنیت زیرساخت‌های حیاتی، تاب‌آوری در کنار حفاظت به رسمیت شناخته شده و حتی بیشتر بر آن تاکید شده است [۱۷].

همان‌طور که در مورد مفهوم حفاظت از زیرساخت‌های حیاتی نیز اتفاق افتاد، اتحادیه اروپا نیز پس از تعویق چند ساله، همان‌طور که سیر ایالات متحده را دنبال کرد، کمیون تجدیدنظر برنامه حفاظت از زیرساخت‌های حیاتی اتحادیه اروپا اظهار کرد که مفهوم تاب‌آوری قبلاً هم در طرح‌های حفاظت از زیرساخت‌های حیاتی هرچند اندک نقش داشته است [۲۰]. با این وجود، تاب‌آوری به عنوان یک مفهوم جایگزین برای حفاظت، تا سال ۲۰۱۴ به طور جدی در موسسات کمیون اروپا مطرح نشد [۱۷].

در چند سال اخیر، مفهوم تاب‌آوری مکرراً در اسناد و برنامه‌های اتحادیه اروپا دیده می‌شود به طوری که بیشتر اصطلاح حفاظت و تاب‌آوری زیرساخت‌های حیاتی مورد استفاده قرار می‌گیرد. در اسناد جدید، این دو مفهوم عموماً در کنار هم آورده شده اما به صراحت در رابطه با مفهوم هر کدام، تفاوت‌ها و ارتباط آن‌ها بحث نشده است. همچنین در این اسناد تاکید شده که اتحادیه اروپا با تقویت اقدامات آمادگی، تعدیلی و واکنشی به دنبال ارائه ابزارهای مفید برای بهبود حفاظت و تاب‌آوری زیرساخت‌های حیاتی است [۱۷].

یکی دیگر از مصادیق تغییر نگرش نسبت به موضوع حفاظت از زیرساخت‌های حیاتی، توسط کمیته بین‌الملل کاهش فجایع سازمان ملل متحد [۲۱] ارائه شده است. این تعریف که به نوعی مفهوم مدرن مسأله حفاظت از زیرساخت‌های حیاتی تلقی می‌گردد؛ توانایی یک سامانه، اجتماع یا جامعه در معرض مخاطرات برای مقاومت، جذب، انطباق و بازیابی از آثار یک مخاطره به روشی سریع و موثر، من جمله از طریق حفظ و ترمیم ساختارها و عملکردهای بنیادی و اساسی را به‌عنوان تاب‌آوری زیرساخت‌های حیاتی تعریف کرده است. نکته قابل توجه در این تعریف این است که در سالهای اخیر و در سطوح ملی، تفاسیر بسیاری از موضوع تاب‌آوری در زیرساخت‌های حیاتی عنوان شده است که کمابیش از تعریف ارائه شده توسط این سازمان برای مفهوم به روز شده مسأله حفاظت از زیرساخت‌ها تبعیت می‌کند. نکته قابل توجه دیگر اینجاست که به کار بستن واژه مقاومت در این الگو، حاکی از شمول اقدامات حفاظتی در این چارچوب

تهدیدها در راهبردهای حفاظت از زیرساخت‌های حیاتی ایالات متحده بنا شد و تاکید تک بعدی ایالات متحده روی تروریسم را تا حدی تغییر داد. این درحالی بود که هنوز تروریسم به‌عنوان تهدید اصلی زیرساخت‌های حیاتی محسوب می‌شد [۱۲]. به‌علاوه، بعد از این طوفان بود که تغییر نگرش قابل توجهی از حوزه حفاظت از زیرساخت‌های حیاتی به سمت اطمینان از تاب‌آوری آن‌ها شکل گرفت [۱۳].

به طور مشابه، رویکرد اتحادیه اروپا نیز در ارتباط با حفاظت از زیرساخت‌های حیاتی، تعادل بین تروریسم و سایر مخاطرات تنظیم شد. در سال ۲۰۰۵ در طرح اروپا برای حفاظت از زیرساخت‌های حیاتی (EPCIP)، سه رویکرد در رابطه با تهدیدهای پیش روی زیرساخت‌ها مطرح شد. رویکرد توجه همه جانبه به انواع مخاطرات، رویکردی همه جانبه برای همه مخاطرات با تخصیص اولویت برای تهدید تروریسم، و رویکرد توجه همه جانبه به تهدیدات تروریستی. پس از بررسی‌های طولانی مدت، انتخاب کمیون مربوطه در سال ۲۰۰۶، رویکرد همه جانبه برای تهدیدات با اولویت تروریسم بود. در این رویکرد تهدید به‌عنوان هر نشانه، پیشامد یا حادثه‌ای تعریف شد که پتانسیل ایجاد اختلال یا تخریب زیرساخت‌های حیاتی یا مولفه‌ای از آن‌ها را دارد [۱۱،۱۴].

در این راستا و در بخشنامه نهایی شورای تصمیم‌گیری طرح، رویکردی همه جانبه اتخاذ و طی آن مقرر شد انواع تهدیدات انسان‌ساز، فنی و فجایع طبیعی در فرآیند حفاظت از زیرساخت‌های حیاتی در نظر گرفته شود؛ اما تهدید تروریسم دارای اولویت باشد. به علاوه، این دستورالعمل حفاظت را تمامی فعالیت‌هایی تعریف می‌کند که با هدف حصول اطمینان از عملکرد صحیح، پیوسته و یکپارچه‌ی زیرساخت‌های حیاتی، به منظور پیشگیری، تعدیل اثر و خنثی‌سازی یک تهدید، ریسک یا آسیب‌پذیری انجام می‌گیرد [۱۵].

در کنار این توجهات، زمانی که برنامه حفاظت از زیرساخت‌های حیاتی اتحادیه اروپا (EPCIP) در سال ۲۰۰۸ ارائه شد، مفهوم تاب‌آوری در اسناد آن دیده نشد؛ اما تصدیق شد که نمی‌توان از همه‌ی زیرساخت‌ها در برابر تمامی تهدیدات محافظت کرد. راه‌حل آن‌ها اولویت‌بندی اقدامات حفاظتی نسبت به هم‌دیگر و سپس تمرکز روی اهداف حفاظتی انتخابی اتخاذ گردید [۱۶]. همچنین، این دستورالعمل منجر به تحریک کشورهای عضو برای شناسایی زیرساخت‌های حیاتی خود و تبیین راهبردهای حفاظتی ملی شد [۱۷].

بدین ترتیب چند سالی طول کشید تا مفهوم تاب‌آوری در سطوح سیاستی کشورها دیده شود. ایالات متحده در این موضوع

بنابراین توجه انحصاری به بحث حفاظت، ممکن است دیدگاه کاذبی از ایمنی را بوجود آورد که می‌تواند فاجعه‌آمیز باشد. این تعبیر نیز ضرورت گذر از بحث‌های حفاظتی پیشین به سمت مفاهیم تاب‌آوری زیرساخت‌های حیاتی را بیش از پیش آشکار ساخته است. در ادامه و در راستای شناخت و استخراج اهداف و چالش‌های راهبردی در این حوزه، سیاست‌ها و راهبردهای امنیتی برخی کشورها با رویکردی کلی‌نگر بررسی شده است.

۳- راهبردهای حفاظت از زیرساخت‌های حیاتی

در چند سال گذشته، تجربه وقوع حوادث در زیرساخت‌های حیاتی موجب شده ملت‌های بیشتری مسئله تأمین امنیت زیرساخت‌های حیاتی را در اولویت اقدامات و برنامه‌های ملی خود قرار دهند. در این راستا، بهره‌گیری از دانش و تجربیات جهانی می‌تواند گامی موثر در ارتقای سطح دانش و تجربه برنامه‌ریزان و دست‌اندرکاران حوزه پدافند غیرعامل کشور محسوب گردد. در این بخش از مقاله، مجموعه انتخابی از سیاست‌ها و راهبردهای ملی در ارتباط با مباحث حفاظت و تاب‌آوری زیرساخت‌های حیاتی به صورت هدف‌دار و از منظر دستورالعمل‌ها و راهبردهای ملی کشورها، برای شناسایی نقاط تمرکز، اولویت‌ها و چالش‌های راهبردی در حوزه تأمین امنیت زیرساخت‌های حیاتی ارائه شده است.

۳-۱- برنامه حفاظت از زیرساخت‌های ملی ایالات

متحده (NIPP)

ایالات متحده آمریکا اولین کشوری است که توسعه و ایجاد طرح‌ها و ابتکارات حفاظت از زیرساخت‌های حیاتی را در دستورکار قرار داده است [۲۵]. نخستین راهبرد ایالات متحده در ارتباط با موضوع حفاظت از زیرساخت‌های حیاتی، در فرمان اجرایی شماره ۶۳ سیاست‌های راهبردی ریاست جمهوری [۲۶] در سال ۱۹۹۸ منتشر شده است. در این گزارش، زیرساخت‌های حیاتی شناسایی و تعاریف و الزامات اولیه حفاظت از آن‌ها مطرح شده است. همچنین لزوم بررسی آسیب‌پذیری زیرساخت‌ها با استفاده از روش‌های انعطاف‌پذیر و پویا که هم بخش‌های خصوصی و دولتی و هم امنیت داخلی و بین‌المللی را دربرگیرد، در این گزارش بیان شده است. طبق این راهبرد یکی از دلایل ضرورت ایجاد وزارت امنیت داخلی، حفظ امنیت زیرساخت‌های حیاتی عنوان شده است.

رویکرد بعدی ایالات متحده در سند شماره ۲۱ سیاست‌های راهبردی [۲۷] با هدف تقویت امنیت و تاب‌آوری زیرساخت‌های حیاتی در برابر تهدیدات فیزیکی و سایبری در سال ۲۰۱۳ ارائه شده است. طبق این سند، دولت باید با همکاری ایالات، مقامات

می‌باشد. بنابراین تاب‌آوری را می‌توان به عنوان یک مفهوم چتری تعبیر کرد که مباحث حفاظت از زیرساخت‌های حیاتی را نیز دربر می‌گیرد.

در حالت کلی، با وجود آنکه در اسناد ملی کشورها، راهبردهای مستقل با عنوان تاب‌آوری زیرساخت‌های حیاتی چندان به چشم نمی‌خورد؛ اما بررسی دقیق‌تر تعداد زیادی از اسناد ملی و گزارش‌های راهبردی نشان می‌دهد که تاب‌آوری به عنوان عنصر کلیدی در برنامه‌ها و راهبردهای نوین تأمین امنیت زیرساخت‌های حیاتی حضور دارد و این نشان‌دهنده تغییر دیدگاه‌ها از مباحث حفاظت به سمت مفاهیم تاب‌آوری است که در بخش بعدی مقاله به برخی از آن‌ها اشاره شده است.

در حوزه مقالات و مطالعات آکادمیک نیز، مفهوم تاب‌آوری از اواسط سال ۲۰۰۰ در سیاست‌های غیررسمی و تحقیقات علمی حوزه‌ی مدیریت بحران به یکباره ظهور و به سرعت شهرت گرفت؛ و طولی نکشید که تاب‌آوری با کنار زدن توجهات قبلی روی مباحث حفاظت، وارد حوزه‌های آکادمیک مطالعات زیرساخت‌های حیاتی شد [۲۲]. تمرکز مقالات و تحقیقات این حوزه بیشتر روی اقدامات پیشگیرانه و فعالیت‌های آمادگی قبل از وقوع بحران، پاسخ و واکنش مناسب در جریان بحران، و مهمتر از همه بازیابی پس از وقوع بحران، از دیدگاه زیرساخت‌های مختلف، تهدیدات مختلف و روش‌های ارزیابی و بهبود تاب‌آوری آن‌ها در مواجهه با این مخاطرات معطوف شده است.

بررسی مقالات و مطالعات تحقیقاتی سال‌های اخیر، بیانگر این حقیقت است که تأکیدات جهانی برای گذر از بحث حفاظت زیرساخت‌های حیاتی به سمت مفهوم تاب‌آوری آن‌ها شدت یافته است. پیشرفت‌های حال حاضر، منعکس‌کننده این امر است که به‌عنوان یک قاعده کلی در ارتباط با تهدیدات واقعی، حفاظت کامل هرگز نمی‌تواند تضمین شود و از طرفی دیگر، موکد این امر است که رسیدن به سطح مطلوب حفاظت مقرون به صرفه هم نیست [۲۳].

بدین لحاظ، در یکی از جالب‌ترین تعابیر مقالات این حوزه، بحث حفاظت و تاب‌آوری با تشبیه به چوب سخت و چوب انعطاف‌پذیر مقایسه شده است. از آنجا که حفاظت کامل هرگز امکان‌پذیر نیست و به تعبیری قوی‌ترین دیوارها در برابر حوادث تاب نمی‌آورند و فرو می‌ریزند، حفاظت در بالاترین سطح خود، مانند چوب سخت است؛ هرچند به راحتی خم نمی‌شود، اما در برابر فشارهای شدید به شدت شکننده است و معمولاً دیگر قابل تعمیر نیست. در مقابل چوب انعطاف‌پذیر و تاب‌آور، به راحتی خم می‌شود و همیشه شکل خود را حفظ کرده و به سختی می‌شکند [۲۴].

در دستور کار قرار داده است. زیرساخت‌های انرژی، فناوری اطلاعات و ارتباطات، حمل و نقل (جاده‌ای و ریلی و هوایی و دریایی)، تأمین آب و دفع فاضلاب، خدمات مالی، مواد غذایی، خدمات سلامت، مراکز آتش نشانی و امداد و نجات، خدمات اجتماعی و درمانی، نهادهای اجرایی، سرویس‌های اطلاعاتی امنیتی و دفاعی، به عنوان ده زیرساخت حیاتی این کشور و با عنوان کارکردهای حیاتی جامعه شناخته شده است [۲۸].

تحلیل آسیب‌پذیری زیرساخت‌های این کشور از سال‌های ۲۰۰۵ تا ۲۰۱۰ در دستور کار سازمان مدیریت شرایط اضطراری دانمارک (DEMA) قرار گرفت که یک سازمان دولتی تحت نظر وزارت دفاع این کشور است. در این راهبرد، آسیب‌پذیری مفهومی است که بیشتر روی آن تمرکز شده و به نوعی مفهوم مقابل تاب‌آوری معرفی شده است. در این چارچوب، توانایی کلی سامانه برای کارکرد و دستیابی به اهداف سامانه در مواجهه با تهدیدها به عنوان آسیب‌پذیری (و به نوعی معنای متضاد آن؛ تاب‌آوری) تعریف شده است. در تعریف دیگر این سازمان، یک سامانه زمانی آسیب‌پذیر است که فاقد ظرفیت لازم برای برنامه‌ریزی، پیشگیری، پاسخ یا بازیابی در مواجهه با یک تهدید مشخص باشد. بر اساس این راهبرد، ارزیابی آسیب‌پذیری با مقایسه تهدیدها در برابر ظرفیت‌های موجود و درجه مطلوب حفاظت انجام گرفته است. در حالت کلی این رویکرد بیانگر این مطلب است که مفهوم آسیب‌پذیری و تاب‌آوری دو روی یک سکه هستند که معانی یکسانی را به اشتراک می‌گذارند [۲۸-۳۰].

این سازمان گزارشات مربوط به آسیب‌پذیری زیرساخت‌ها را به طور منظم انتشار داده است. در اولین گزارش نمایه خطرپذیری ملی^۲ سازمان [۲۸] در سال ۲۰۱۳، حوادث متوجه زیرساخت‌های حیاتی شناسایی و بر اساس انسان‌ساخت یا طبیعی بودن و اهمیت هریک از مخاطرات برای زیرساخت‌های مختلف اولویت‌بندی شده است. در این تحلیل، آسیب‌پذیری تهدیدات انسان‌ساخت در دو دسته‌ی جداگانه حوادث و تهدیدات امنیتی بررسی شده است. این سازمان با توجه به تحلیل‌های آسیب‌پذیری، چند نوع حادثه را برای تحقیقات بیشتر انتخاب کرده که از آن جمله می‌توان به گردبادها، طوفان‌های سخت و خیزاب‌ها، باران‌های سنگین و رگبارهای ناگهانی، حوادث حمل و نقل، حوادث هسته‌ای و حملات سایبری و فیزیکی اشاره کرد. هدف این گزارش، ایجاد آمادگی لازم در جامعه و مستحکم‌سازی آن در برابر حوادث و فجایع عنوان شده است که به نوعی مفهوم تاب‌آوری اجتماعی را تداعی می‌کند.

گزارش سال ۲۰۱۵ این سازمان [۲۹]، روی سامانه مدیریت

محلی و صاحبان و متصدیان زیرساخت‌های حیاتی در بخش‌های خصوصی و دولتی، در وهله اول با شناسایی دارایی‌ها و سامانه‌هایی که زیرساخت‌های حیاتی ملی را تشکیل می‌دهند، ارزیابی آسیب‌پذیری زیرساخت‌ها و دارایی‌ها را با استفاده از یک روش مدیریت خطرپذیری در مواجهه با تهدیدات ملی به انجام رساند. برآورد خطرپذیری، شناسایی و اولویت‌بندی، مجموعه اقداماتی است که می‌تواند موجب کاهش خطرپذیری شود. همچنین این سیاست راهبردی، تدوین یک برنامه تحقیق و توسعه جدید در حوزه زیرساخت‌های حیاتی و لزوم بروزرسانی برنامه حفاظت از زیرساخت‌های ملی (NIPP) در بازه‌های زمانی هر چهار سال یکبار را در دستورکار قرار داده است. متن این سند، منعکس‌کننده افزایش توجهات به مفهوم تاب‌آوری و رویکردهای تحلیل چند مخاطره‌ای است.

در برنامه حفاظت از زیرساخت‌های حیاتی ملی (NIPP) [۱۹]، بخش‌های انرژی (برق، نفت، گاز)، ارتباطاتی و مخابراتی، آب و فاضلاب، خدمات اضطراری و اورژانسی، خدمات مالی، مواد غذایی و کشاورزی، خدمات دولتی، سلامت و بهداشت عمومی، فناوری اطلاعات، راکتورهای هسته‌ای، سامانه‌های حمل و نقل، مواد شیمیایی، تسهیلات تجاری، تولیدات حیاتی، سدها و صنایع دفاعی، به عنوان شانزده زیرساخت‌های حیاتی این کشور طبقه‌بندی و شناخته شده است. در این راهبرد، بخش‌ها و زیربخش‌های حیاتی به صورت اجتماع منطقی یک سری دارایی‌ها، سامانه‌ها یا شبکه‌ها تعریف شده که کارکردها و عملکردهای عمومی جامعه، حاکمیت و اقتصاد را میسر می‌سازند. همچنین، امنیت و تاب‌آوری بخش‌های انرژی و مخابراتی به واسطه اهمیت آن‌ها برای عملکرد سایر زیرساخت‌ها، بیشتر مورد تاکید قرار گرفته است. هدف از لزوم بروزرسانی برنامه حفاظت از زیرساخت‌های ملی، افزایش تمرکز و توجه روی وابستگی سایر بخش‌ها به زیرساخت‌های انرژی و ارتباطاتی و همچنین راه‌های کاهش ریسک‌های مربوطه، به علاوه توسعه سیاست‌ها و برنامه‌های حوزه امنیت سایبری زیرساخت‌های حیاتی عنوان شده است. بر اساس راهبرد کلی این سند، حفاظت از زیرساخت‌های حیاتی به عنوان عامل توانمندساز حوزه تاب‌آوری زیرساخت‌ها شناخته شده است. به‌علاوه در تمامی رویکردهای اخیر ایالات متحده در ارتباط با امنیت زیرساخت‌های حیاتی، تاب‌آوری در کنار حفاظت به رسمیت شناخته شده و حتی بیشتر بر آن تاکید شده است [۱۷].

۳-۲- سازمان مدیریت شرایط اضطراری دانمارک^۱ (DEMA)

دانمارک یکی از کشورهایی است که سامانه امنیت و ایمنی اجتماعی توسعه یافته، همراه با فعالیتهای تحقیقاتی مربوطه را

² National Risk Profile

¹ Danish Emergency Management Agency

اصطلاح زیرساخت‌های حیاتی اصلاً به کار بردن نشده و به جای آن عبارت خدمات مبتنی بر زیرساخت استفاده شده است. همچنین، از منظر راهبردهای ملی این کشور، حفاظت و بازگردانی سریع کارکردهای ضروری جامعه، دو عنصر کلیدی در تاب‌آوری اجتماعی عنوان شده است.

۳-۴- سازمان پیش‌بینی رویدادهای شهری سوئد^۴ (MSB)

بی شک سوئد یکی از اولین کشورهای است که دیدگاه‌های ایمنی و امنیت اجتماعی خود را بیشتر بر پایه تاب‌آوری و نه فقط حفاظت محض بنا کرده است [۳۳]. سازمان پیش‌بینی رویدادهای شهری سوئد (MSB) در سال ۲۰۱۱، راهبرد ملی حفاظت از زیرساخت‌های حیاتی و خدمات پراهمیت اجتماعی را به دستور دولت تهیه کرده است. در مقدمه این گزارش تصریح شده که هدف این راهبرد ملی، توسعه و ایجاد جامعه تاب‌آور است. ظرفیت جامعه برای مقاومت و همچنین بازیابی از اختلالات من جمله تعاریف این سازمان در ارتباط با تاب‌آوری است [۳۴].

گزارش سال ۲۰۱۳ سازمان [۳۵] با هدف ایجاد آمادگی برای حوادث آینده منتشر شده است. در این گزارش، چگونگی تاثیر تحولات احتمالی مختلف در آینده، بر روی مسئله امنیت اجتماعی تحلیل و ده چالش راهبردک در این حوزه شناسایی شده است. حفظ و تداوم عملکرد زیرساخت‌های حیاتی در مواجهه با حوادث و امنیت سایبری از جمله این چالش‌های راهبردک هستند. همچنین در این گزارش، تهدیدات، آسیب‌پذیری‌ها و مسائل پیش‌روی حوزه امنیت اجتماعی تحلیل و راهبردهای پیشنهادی به منظور مقابله با این چالش‌ها ارائه شده است.

گزارش بعدی این سازمان تحت عنوان اقدامات عملی برای حفاظت از زیرساخت‌های حیاتی و کارکردهای اساسی جامعه [۳۶]، با هدف تهیه پیش‌نیازهای لازم برای ایجاد یک برنامه عملی و بر پایه راهبرد، در راستای توسعه اقدامات حفاظتی ارائه شده است. تضمین امنیت سامان‌های زیرساخت‌ها و ایجاد جامعه تاب‌آور با ظرفیت‌های بهبود یافته در حوزه زیرساخت‌های حیاتی به منظور مقاومت و بازیابی از اختلالات شدید، به عنوان اولویت‌های برنامه کاری این سازمان تا سال ۲۰۲۰ تعیین شده است.

در این راهبرد، حفاظت از زیرساخت‌های حیاتی به اقدامات و فعالیت‌هایی اطلاق می‌شود که برای اطمینان از عاملیت و پیوستگی زیرساخت‌های حیاتی و در نتیجه کل جامعه مورد نیاز است؛ در حالی که تاب‌آوری، توانایی جامعه و زیرساخت‌های آن

بحران کشور متمرکز شده است. در این گزارش تصریح شده که هدف از این برنامه، اطمینان از ایجاد یک جامعه مستحکم و مقاوم از طریق توسعه و تقویت فعالیت‌های آمادگی، به منظور پیشگیری و پاسخ به حوادث و فجایع بزرگ است. اگرچه در آخرین گزارش این سازمان [۳۰] در سال ۲۰۱۸، باز صحبتی از تاب‌آوری نشده و تمرکز اصلی روی مفاهیم پیشگیری، آمادگی و پاسخ به حوادث است تا تاب‌آوری از دیدگاه بازیابی سریع؛ اما مدل تحلیل بر پایه کاربردی از یک چرخه مدیریت بحران نمونه با مراحل قبل، حین و پس از بحران است؛ به طوری که همه پارامترهای اساسی مفهوم تاب‌آوری در آن دیده می‌شود.

۳-۳- اداره حفاظت شهری نروژ^۱ (DSB)

در راهبردها و راهبردهای کلی این کشور در رابطه با زیرساخت‌های حیاتی، استفاده از مفاهیم تاب‌آوری کاملاً مشهود است. گزارش تحلیل خطرپذیری ملی^۲ [۳۱] توسط اداره حفاظت شهری نروژ (DSB) در سال ۲۰۱۴ ارائه و جوامع تاب‌آور به عنوان یک مفهوم جدید در حوزه حفاظت شهری معرفی شده است. در این گزارش عنوان شده که این مفهوم به طور فزاینده‌ای در حال گسترش است و به واسطه ارتباطات پیچیده و وابستگی‌های متقابل در زیرساخت‌های جامعه، حتی ممکن است موضوع تاب‌آوری در آینده از دیدگاه تقویت و تحکیم حفاظت شهری، اهمیت راهبردی بیشتری نیز پیدا کند.

گزارش سال ۲۰۱۷ این سازمان [۳۲] که با عنوان کارکردهای حیاتی در جامعه^۳ انتشار یافته است، به این موضوع پرداخته که کدام توانایی‌ها و قابلیت‌های عملکردی و کارکردی باید در همه شرایط و زمان‌ها در جامعه حفاظت شده و پایدار شوند. در این گزارش، عبارت کارکردهای حیاتی جامعه، تعریف و این کارکردها طبقه‌بندی و اولویت‌بندی شده است. طبق این راهبرد، کارکردهایی که جامعه نمی‌تواند در فقدان آن‌ها هفت روز یا کمتر با عوامل تهدیدکننده ایمنی و یا امنیت مردم مقابله کند، کارکردهای حیاتی جامعه محسوب می‌شوند. این کارکردها در سه دسته حاکمیت، امنیت ملی و عاملیت اجتماعی دسته‌بندی و تحلیل شده است. یکی از زیربخش‌های حوزه عاملیت اجتماعی، خدمات مبتنی بر زیرساخت بوده و شامل سامانه‌ها و دارایی‌هایی است که معمولاً با عنوان زیرساخت‌های حیاتی شناخته می‌شوند. طبق این راهبرد، خدمات اضطراری و تأسیسات ضروری همچون انرژی و آب از جمله حیاتی‌ترین حوزه‌های خدمات مبتنی بر زیرساخت هستند. جالب توجه است که در راهبردهای این کشور،

¹ The Norwegian Directorate for Civil Protection

² National Risk Analysis

³ Vital functions in society

⁴ The Swedish Civil Contingencies Agency

ارزیابی خطرپذیری ملی [۳۹] در سال ۲۰۱۶ منتشر شده است. در این گزارش، مجموعه نسبتاً جامعی از ارزیابی‌های ریسک به همراه ارزیابی ظرفیت‌ها ارائه شده است. مخاطرات در چهارگروه اصلی مخاطرات طبیعی^۴ (شامل ۱۰ مورد مخاطره)، حوادث عظیم و بزرگ^۵ (شامل ۴ مورد مخاطره)، اختلال در زیرساخت‌های فنی و سامانه‌های تغذیه^۶ (۷ مورد) و مخاطرات متخاصم و خرابکارانه^۷ (۴ مورد) دسته‌بندی شده است. دسته سوم منحصرأ به زیرساخت‌های حیاتی مربوط می‌شود که مخاطراتی همچون اختلال در تأمین انرژی، اختلال در ارتباطات الکترونیکی، اختلال در سامانه پرداخت، اختلال در تأمین مواد غذایی، اختلال در تأمین آب آشامیدنی، اختلال در سامانه حمل و نقل و اختلال در تأمین دارو در این حوزه بررسی شده است. همچنین، حملات سایبری و تروریسم نیز در دسته مخاطرات خرابکارانه و متخاصم به عنوان یکی از بزرگترین چالش‌های پیش‌روی حوزه زیرساخت‌های حیاتی معرفی و تحلیل شده است. شایان ذکر است، یکی دیگر از تأکیدات عمده این چارچوب، مقاوم‌سازی و تاب‌آوری زیرساخت‌های وابسته، به منظور جلوگیری از آثار آیشاری یا زنجیره‌ای^۸ شدید است. همچنین در این گزارش، تحلیل هر سناریوی خرابی برای حوادث ذکر شده، بر مبنای توانایی جامعه در پیشگیری و پاسخ به آن سناریو و تأثیرات بالقوه آن در حفاظت ملی سوئد انجام شده است. به علاوه، در تحلیل هر کدام از سناریوها، مباحثی نظیر احتمال وقوع، حساسیت و عدم قطعیت مربوط به آن سناریو بررسی و بحث شده است.

۳-۵- وزارت امنیت داخلی فنلاند^۹

برای اولین بار در کشور فنلاند، پروژه ارزیابی خطرپذیری ملی [۴۰] در اواخر سال ۲۰۱۶ توسط سازمان امنیت داخلی وزارت کشور منتشر شده است. ارزیابی خطرپذیری ملی امکان تشخیص حوادث پیش‌بینی نشده‌ای را فراهم می‌آورد که وقوع آن‌ها زندگی و سلامت مردم را به خطر انداخته، موجب خسارات و زیان‌های اقتصادی در سطوح ملی شده و آسیب‌های زیست محیطی و اجتماعی شدید را پدید می‌آورند. در این گزارش، بر مبنای ارزیابی ریسک برای این کشور به منظور تحلیل‌های دقیق‌تر انتخاب شدند. این مخاطرات در دو دسته کلی طبقه‌بندی شده است: حوادث گسترده با تأثیرگذاری شدید در کل جامعه^{۱۰}

برای پیشگیری، مقاومت، مدیریت و بازیابی از اختلالات تعریف شده است. از دیگر اهداف این راهبرد، حفاظت کامل از زیرساخت‌های خدماتی پراهمیت، توسعه روش‌های نوین در تحلیل ریسک و آسیب‌پذیری، و بهره‌مندی از دانش، ابتکار و آموزش برای فرهنگ‌سازی ایمنی و تاب‌آوری در تمامی سطوح جامعه می‌باشد. همچنین توسعه راهبردهای بر پایه مفهوم تاب‌آوری به منظور تقویت آمادگی در برابر حوادث، مهمترین هدف تحقیقاتی این سازمان در حوزه حفاظت از زیرساخت‌های حیاتی و خدمات پراهمیت شهری، برای سال‌های ۲۰۱۴ تا ۲۰۱۸ تعیین شده است.

در این راستا، گزارش‌های دیگری نیز از جانب این سازمان منتشر شدند که مأموریت اصلی آن‌ها، اعطای دانش و آگاهی در مورد نحوه به کارگیری مفهوم تاب‌آوری در بخش‌های مختلف جامعه بوده است. در این گزارشات تأکید شده که مفهوم تاب‌آوری در معرض توسعه بیشتر قرار دارد و سازمان توسعه این مفهوم را دنبال خواهد کرد [۳۷]. در کنار این توجهات، سازمان مذکور بودجه قابل توجهی را برای تاسیس مرکز تحقیقات حفاظت از زیرساخت‌های حیاتی^۱ (CenCIP) مستقر در دانشگاه لند^۲ اختصاص داده است. در حالی که تلاش‌ها برای جایگزینی مفهوم تاب‌آوری در برابر مباحث حفاظتی به سرانجام نرسید، اما با این وجود تحقیقات عملی زیادی در حوزه تاب‌آوری زیرساخت‌های حیاتی انجام گرفت [۳۳].

سازمان MSB که از سال ۲۰۱۱ پروژه ارزیابی خطرپذیری ملی^۳ خود را به سفارش دولت آغاز کرد، از بین بیش از ۲۰۰ حادثه شناسایی شده در تحلیل‌های خطرپذیری و آسیب‌پذیری سازمان، ۲۷ مورد بخصوص از حوادث سخت و خطرناک ملی را شناسایی و تحلیل کرده است. از جمله این ۲۷ رخداد، حوادثی همچون اختلال در تأمین سوخت، تأمین برق، تهیه مواد غذایی، ظغیان منابع آبی و سیل، آلودگی آب‌های آشامیدنی، موج‌های گرما، رانش زمین و طوفان‌ها را می‌توان نام برد. علاوه بر این، برای حوادث شدید منحصر به این کشور، یازده سناریو ایجاد و روی هفت مورد از آن‌ها تحلیل و ارزیابی‌های جامع انجام شده است؛ حوادثی که بیشترین ریسک کلی را با توجه به ترکیب احتمال و شدت موجب می‌شدند، بدین منظور انتخاب شده و در نتیجه این تحلیل‌ها، روش‌ها و فرآیندهای ارزیابی خطرپذیری ملی توسعه یافته است [۳۸].

در ادامه سری گزارشات این سازمان، نسخه به روز شده پروژه

⁴ Natural Hazards

⁵ Major Accidents

⁶ Disruption to technical infrastructure and supply systems

⁷ Antagonistic Hazards

⁸ Cascading Failures

⁹ Ministry of the Interior Finland

¹⁰ Wide-Ranging Events Affecting Society

¹ The Centre for Critical Infrastructure Protection Research

² Lund University

³ National Risk Assessment

در طرح تاب‌آوری زیرساخت‌های حیاتی [۴۲]، دولت استرالیا همانند ایالات متحده و برخی کشورهای اروپایی، هدف ایجاد یک رویکرد مشارکت دولتی-خصوصی را برای تاب‌آوری زیرساخت‌ها برگزیده است. همچنین در تمامی راهبردهای این کشور، امنیت سامانه‌های فناوری اطلاعات و ارتباطات مورد توجه ویژه‌ای قرار گرفته است. از آنجایی که بسیاری از زیرساخت‌های حیاتی بر پایه سامانه‌های سایبری بنا شده، این کشور به منظور افزایش امنیت سایبری، یک شبکه به اشتراک‌گذاری اطلاعات ایمن^۲ (TISN) ایجاد کرده و آن را اصلی‌ترین ساز و کارهای افزایش تاب‌آوری در زیرساخت‌ها عنوان کرده است. از جمله اهداف این راهبرد ایجاد رویکردی بین بخشی و شناسایی وابستگی‌های متقابل بین بخش‌های مختلف زیرساختی عنوان شده است.

در گزارش بعدی از راهبرد تاب‌آوری زیرساخت‌های حیاتی استرالیا [۴۳] در سال ۲۰۱۵، سیاست‌های این کشور در رابطه با تاب‌آوری زیرساخت‌ها بیان شده است. ایجاد یک بستر کارا برای همکاری بخش‌های دولتی و خصوصی با صاحبان و گردانندگان زیرساخت‌ها، توسعه و ارتقا پیکره دانش تاب‌آوری سازمانی و درک عمومی از تاب‌آوری سازمانی، مساعدت و همکاری با صاحبان و گردانندگان زیرساخت‌های حیاتی برای شناسایی و تحلیل وابستگی‌های متقابل بین بخشی، سیاست‌گذاری به‌روز و به موقع در مورد مباحث مربوط به تاب‌آوری زیرساخت‌های حیاتی، پیاده‌سازی راهبرد امنیت سایبری برای ایجاد محیطی با عملکردهای الکترونیکی ایمن و تاب‌آور، پشتیبانی از برنامه‌ها و طرح‌های تحقیقاتی مرتبط با تاب‌آوری زیرساخت‌های حیاتی، از جمله دیدگاه‌های راهبردی این راهبرد است. در حالت کلی، بر اساس راهبردهای این کشور می‌توان استدلال کرد که تاب‌آوری جامعه به عنوان رویکردی نوین در حفاظت از زیرساخت‌ها در برابر تمامی مخاطرات محسوب می‌شود.

۴- الزامات اولیه در راهبرد ملی حفاظت از زیرساخت‌های حیاتی

کشور ما با توجه به وسعت جغرافیایی و موقعیت ژئوپلیتیک در منطقه، در معرض انواع بحران‌های بالقوه محیطی مهم از سیل و زلزله، و بحران‌های انسان‌ساز مهم از جنگ و حملات تروریستی قرار دارد. آمارهای جهانی نشان می‌دهد ایران جزء ده کشور تحت تأثیر انواع بلایای طبیعی در دنیا است. از طرفی دیگر، تجربه حاصل از جنگ‌های اخیر در منطقه بخصوص جنگ آمریکا و

(شش مورد مخاطره) و حوادث شدید منطقه‌ای^۱ (پانزده مورد مخاطره).

هدف از این پروژه، ادغام و گردآوری تمامی خطرپذیری‌های مهم ملی و همچنین شدت آثار و احتمال وقوع آن‌ها عنوان شده است. حوزه تهدیدات سایبری، در دسته اول مخاطرات (حوادث گسترده با تاثیرگذاری شدید در کل جامعه) به عنوان یکی از مهمترین اولویت‌های پژوهشی این سازمان برای چند سال آینده تعریف شده است. در این راستا، با ایجاد تمایز بین حوزه‌های استفاده از فضای سایبری برای فلج سازی سامانه‌های حیاتی جامعه، مخاطرات مربوط به جرایم سایبری، و مخاطرات مربوط به امنیت داده‌ها در دیجیتال‌سازی، سیاست‌ها و چالش‌های مرتبط با هر بخش به تفصیل بیان شده است. همچنین در دسته حوادث شدید منطقه‌ای، حملات تروریستی و مخاطرات مربوط به فجایع طبیعی، اولویت اول سیاست‌های سازمان برای مقابله، برنامه‌ریزی‌های پیشگیرانه و اقدامات حفاظتی در نظر گرفته شده است [۴۰]. در حالت کلی می‌توان گفت رویکرد این راهبرد برای تأمین امنیت در بخش‌های مختلف، توسعه فعالیت‌های آمادگی بر مبنای ارزیابی خطرپذیری حوادث می‌باشد و مفاهیم تاب‌آوری هنوز در اسناد و سیاست‌های رسمی این کشور مشاهده نمی‌شود.

۳-۶- راهبرد تاب‌آوری زیرساخت‌های حیاتی استرالیا

استرالیا از جمله کشورهایی است که سیاست‌های امنیت زیرساختی پیچیده و پیشرفته‌ای را برای حفاظت از زیرساخت‌های حیاتی هم در برابر تهدیدات امنیتی معاصر و هم مخاطرات آینده، در دستور کار قرار داده است. اولین راهبرد استرالیا برای تأمین امنیت زیرساخت‌های این کشور، تحت عنوان راهبرد تاب‌آوری زیرساخت‌های حیاتی [۴۱] در سال ۲۰۱۰ منتشر شده است. در این راهبرد، تغییر نگرش نسبت به سمت مفهوم تاب‌آوری به عنوان رویکردی همه جانبه برای حفاظت در برابر تمامی خطرات، کاملاً مشهود است. به علاوه، توجه ویژه‌ای به بحث وابستگی زیرساخت‌ها و بخش‌ها به همدیگر شده است. هدف از تاب‌آوری زیرساخت‌ها در این گزارش عبارتست از برنامه‌ریزی هماهنگ بین بخش‌ها و شبکه‌ها، اقدامات واکنشی، اقدامات بازیابی انعطاف‌پذیر و بموقع و توسعه یک فرهنگ سازمانی که توانایی تأمین حداقل سطح خدمات را در طول مدت اختلالات، شرایط اضطراری و فجایع داشته و بتواند به سرعت به عملکرد کامل خود بازگردد.

^۲ TISN: Trusted Information Sharing Network

^۱ Serious Regional Events

مخاطرات در بسیاری از موارد می‌توانند ناشناخته یا نوظهور باشند، پس نمی‌توان برای تهدیدات ناشناخته اقدامات حفاظتی چندانی در نظر گرفت. ثانیاً، اقدامات حفاظتی به تنهایی نمی‌تواند موجب کاهش وقوع مخاطرات شود یا بازبایی سریع خدمات را تضمین کند. ثالثاً، در صورتی که با وجود اقدامات حفاظتی، به هر دلیلی تأمین خدمات مورد نیاز زیرساخت‌های حیاتی با اختلال و قطعی مواجه شود، صاحبان و متصدیان آن‌ها اصولاً ظرفیت محدودی برای بهره‌برداری مداوم از زیرساخت‌ها خواهند داشت و به اصطلاح در بلند مدت تاب اختلال و قطعی را نمی‌آورند.

بنابراین، پیشرفت‌های حال حاضر منعکس‌کننده این امر است که به عنوان یک قاعده کلی در ارتباط با تهدیدات واقعی، حفاظت کامل هرگز نمی‌تواند تضمین شود؛ و از طرفی دیگر، موکد این امر است که رسیدن به سطح مطلوب حفاظت مقرون به صرفه هم نیست. با توجه به تبعات مختلف خرابی و از کارافتادگی زیرساخت‌های حیاتی (حتی کوتاه مدت) در سطوح اجتماعی، اقتصادی و امنیتی کشورها، رویکردهای تاب‌آوری زیرساخت‌های حیاتی و در نتیجه تداوم کارکرد آن‌ها (با وجود اختلالات) بیش از پیش دنبال می‌شود. با بررسی و تحلیل این رویکردها با دیدگاهی آینده‌پژوهانه، الزامات اولیه یک راهبرد نوین حفاظت از زیرساخت‌های حیاتی به شرح زیر است:

مسئله اول در مطالعات و گزارشات ارائه شده، سناریوهای تهدید است. مرور اجمالی راهبردها، بیانگر این مطلب است که توجه بیشتر سازمان‌ها در ابتدای کار روی مخاطرات مربوط به حملات تروریستی در زیرساخت‌های حیاتی متمرکز شده است. اما امروزه این دیدگاه غالب ایجاد شده که میزان ریسک مخاطرات سایبری و حوادث شدید آب و هوایی در زیرساخت‌ها، کمتر از حملات تروریستی نیست. بنابراین یکی از الزامات اولیه در راهبردهای نوین حفاظت از زیرساخت‌های حیاتی، توجه به رویکردهای همه‌جانبه یا چند جانبه برای مخاطرات^۲ است.

مسئله بعدی، افزایش وابستگی‌های متقابل بین زیرساخت‌هاست. در عصر حاضر، زیرساخت‌های حیاتی برای عملکرد صحیح، سریع و موثر، به صورت پیچیده روی همدیگر اثر متقابل دارند. از این رو، حیاتی بودن یک زیرساخت تنها به دلیل تأثیرات مستقیم آن به واسطه وقوع تهدیدات یا هر نوع خرابی و قطع خدمات آن‌ها نیست؛ بلکه به دلیل تأثیر روی سایر زیرساخت‌هاست که به عنوان تأثیرات مرتبه دوم شناخته شده و اهمیت حیاتی بودن یک زیرساخت را مشخص می‌کند.

بنابراین، عواملی که امنیت زیرساخت‌های امروزی را به مخاطره می‌اندازند، منحصراً به تهدیدات خارجی محدود نمی‌شوند؛ احتمال وقوع اختلالات درونی ناشی از خرابی‌های

کشورهای عضو ناتو علیه عراق و سوریه و همچنین تجربه تلخ هشت سال دفاع مقدس موید این حقیقت است که زیرساخت‌های حیاتی در نسل نوین جنگ‌ها به مصابه خط مقدم و هدف‌های اولیه در جنگ‌های نسل گذشته هستند؛ در نتیجه، راهبرد انهدام و تخریب این زیرساخت‌ها چه به صورت فیزیکی و چه به صورت سایبری، بیشتر مورد توجه و تمرکز کشورهای مهاجم و گروه‌های تروریستی وابسته به آن‌ها قرار گرفته است.

مقابله با این دست از تهدیدات که که کمتر قابل پیش‌بینی بوده در عین حال، تأثیرات و خسارات شدیدی روی جامعه و زیرساخت‌های آن تحمیل می‌کنند و عموماً با عنوان حوادث با احتمال وقوع کم و تأثیرگذاری بالا^۱ شناخته می‌شوند؛ بسیار دشوار بوده و در عین حال امری ضروری است. تجربیات حوادث مختلف در کشور عزیزمان نشان داده که توجه انحصاری به بحث حفاظت بدون بهره‌مندی از مفاهیم پدافند غیرعامل، امری شکننده، پرهزینه و حتی غیرقابل جبران است. بنابراین، حفاظت کامل از سامانه‌ها و زیرساخت‌های حیاتی در برابر تهدیدات یادشده، علاوه بر حفاظت‌های فیزیکی و الزامات نظامی-امنیتی، با اجرای ضوابط و الزامات پدافند غیرعامل محقق می‌گردد.

در این راستا، پیش‌بینی تهدیدات ملی، تحلیل خطرپذیری زیرساخت‌های مختلف کشور در برابر آن‌ها، و اعمال برنامه‌ریزی‌های پیشگیرانه و هوشمندانه متولیان حوزه پدافند غیرعامل با استفاده از مفاهیم جدیدی همچون تاب‌آوری، گامی موثر در راستای حفاظت حداکثری از زیرساخت‌های حیاتی محسوب می‌گردد. این اقدامات و الزامات باید در مراحل مختلف بخصوص طراحی و بهره‌برداری زیرساخت‌های کشور مورد توجه قرار گرفته و دست‌یابی به زیرساخت‌هایی ایمن و پایدار را تضمین کنند. لازم به ذکر است الزامات پدافند غیرعامل در حوزه حفاظت از زیرساخت‌های حیاتی کشور در قالب یک راهبرد و راهبرد ملی، هنوز منتشر نشده اما در دستورکار سازمان پدافند غیرعامل کشور قرار گرفته است.

در این بخش از مقاله، با استفاده از مطالعات تطبیقی در حوزه راهبردهای ملی حفاظت از زیرساخت‌های حیاتی و شناسایی و تحلیل نقاط تمرکز، اولویت‌ها، اهداف و چالش‌های راهبردک در این حوزه، برخی الزامات اولیه به منظور ترسیم وضعیت مطلوب یک راهبرد ملی اثربخش و کارا استخراج و تحلیل گردیده است، که می‌تواند در توسعه و تدوین راهبرد ملی حفاظت از زیرساخت‌های حیاتی کشور مورد توجه قرار گیرد.

چشم‌انداز نامساعد، ناسازگار و درحال تغییر مخاطرات و تهدیدات متوجه زیرساخت‌های حیاتی موجب شده اقدامات پیش‌بینی، پیشگیری و آمادگی برای تعدیل اثر مخاطرات، با استفاده از الزامات حفاظتی پیشین امکان‌پذیر نباشد؛ چراکه اولاً،

^۲ All-Hazard or Multi-Hazard Approaches

^۱ High-Impact, Low-Probability

زیرساخت‌های حیاتی را شامل می‌شود. در این حوزه، هر چند که زیرمباحثی پدید آمده و حتی نهادینه شده است؛ اما هنوز مرز دقیق مباحث حفاظت و تاب‌آوری در سیاست‌ها، دستورالعمل‌ها و راهبردهای ملی مرتبط با زیرساخت‌های حیاتی تیره و تاریک است.

از دیدگاه برخی کشورهای اروپایی، رویکردهای بر پایه تاب‌آوری به عنوان یکی از سیاست‌های نوظهور در حوزه حفاظت از زیرساخت‌های حیاتی شناخته می‌شود. این درحالی است که برخی دیگر، تاب‌آوری را رویکردی نوین و همه جانبه و به عنوان جایگزین مباحث حفاظت از زیرساخت‌های حیاتی در نظر گرفتند. همچنین تاب‌آوری به عنوان مفهوم به‌روز شده مسأله حفاظت از زیرساخت‌های حیاتی نیز تعبیر شده است. از دیدگاه برخی راهبردها، تاب‌آوری فعالیت‌ها و آمادگی‌های لازم برای حفاظت از زیرساخت‌هاست؛ در حالی که راهبردهای دیگر، حفاظت را عامل توانمندساز تاب‌آوری زیرساخت‌ها تلقی می‌کنند.

بنابراین، تمامی شواهد حاکی از آن است که در سال‌های اخیر تاکیدات جهانی برای جایگزینی مفاهیم و الزامات بر پایه تاب‌آوری شدت یافته و بیشتر سیاست‌های ملی در حوزه زیرساخت‌های حیاتی، از مفهوم حفاظت به سمت تاب‌آوری آن‌ها سوق پیدا کرده است. باید توجه داشت اگرچه موضوع تاب‌آوری در سیاست‌ها و راهبردهای حفاظتی برخی کشورها به طور جداگانه مطرح نگردیده است، اما این مفهوم به طور تلویحی در اسناد رسمی آن‌ها پوشش داده شده است. استفاده از مفاهیمی چون استحکام، انطباق، انعطاف‌پذیری و بازگردانی سریع در اسناد و چشم‌اندازهای ملی در حوزه زیرساخت‌های حیاتی دیده می‌شود که المان‌های کلیدی در مفهوم تاب‌آوری هستند.

به‌عنوان یکی از مهمترین نتایج این پژوهش، با بررسی اسناد حوزه امنیت زیرساخت‌های حیاتی می‌توان استنباط کرد که دیدگاه‌های سنتی در رابطه با ایمنی و امنیت زیرساخت‌ها نیز از توسعه و پی‌ریزی سیاست‌های تاب‌آوری در آینده نزدیک پشتیبانی و حمایت کرده و بر این باورند که مناظرات ایمنی و امنیت در زیرساخت‌ها، بدون استفاده از مفهوم تاب‌آوری امکان‌پذیر نخواهد بود. از این رو بعد نیست در آینده‌ای نه چندان دور، مفاهیم تاب‌آوری زیرساخت‌های حیاتی (CIR) به تدریج جایگزین مفهوم اولیه حفاظت از زیرساخت‌های حیاتی (CIP) شود. بنابراین توجه به رویکردهای تاب‌آور-محور از اصول و الزامات اصلی راهبردهای نوین تلقی می‌گردد که باید در راهبرد ملی حفاظت از زیرساخت‌های حیاتی کشور نیز مد نظر قرار گیرد.

آبشاری یا زنجیره‌ای مربوط به همبندی یا وابستگی متقابل زیرساخت‌ها، چالش‌ها و مشکلات جدیدی را در این حوزه بوجود آورده است. از آنجا که وابستگی متقابل، یک ویژگی متداول برای سامانه‌های زیرساختی است، واضح است که توانایی شناسایی، مدل‌سازی و تحلیل ابعاد مختلف این وابستگی، از دیگر الزامات اولیه یک راهبرد ملی حفاظت از زیرساخت‌های حیاتی به‌روز و کارا محسوب می‌گردد.

از آنجا که وابستگی متقابل زیرساخت‌های حیاتی، معمولاً با ارتباطات سایبری و از طریق بستر فناوری اطلاعات و ارتباطات محقق می‌گردد، مسأله بعدی در این حوزه تهدیدات سایبری است. در دنیای امروز، مدیریت، کنترل و بهینه‌سازی اهداف و عملکردهای زیرساخت‌های حیاتی توسط حوزه سایبر انجام می‌گیرد؛ به عبارت دیگر، بخش سایبر است که تجهیزات و المان‌های فیزیکی را کنترل می‌کند. بنابراین از دیگر الزامات برای حالت مطلوب یک راهبرد نوین حفاظت از زیرساخت‌های حیاتی، در نظرگیری، مدل‌سازی و تحلیل زیرساخت‌های حیاتی به صورت سامانه‌های فیزیکی-سایبری وابسته به هم است.

بنابراین، نظر به اینکه فضای سایبری هیچگونه حد و مرزی ندارد و با کمترین هزینه و از هر نقطه جهان می‌توان هدف را مورد حمله قرار داد؛ تهدیدات سایبری را می‌توان یکی از بزرگترین چالش‌های پیش روی حوزه امنیت زیرساخت‌های حیاتی قلمداد کرد. به همین جهت، فرآیند طراحی سیاست‌های امنیت سایبری پایدار برای زیرساخت‌های حیاتی، در دستورکار بیشتر کشورهای جهان و همچنین سازمان پدافند غیرعامل کشور قرار گرفته است.

یکی دیگر از مهمترین مسائل و چالش‌ها در حوزه تأمین امنیت زیرساخت‌های حیاتی، تقابل میان رویکردهای بر پایه حفاظت و رویکردهای تاب‌آور-محور می‌باشد. حفاظت در حوزه زیرساخت‌های حیاتی به دنبال مستحکم‌سازی دارایی‌های حیاتی در برابر حملات یا تهدیدات احتمالی است. تعریف تاب‌آوری به عنوان یک مفهوم جایگزین برای حفاظت شاید گمراه‌کننده به نظر برسد؛ اما موضوعی است که در سیاست‌های اخیر برخی کشورها مطرح شده است.

رویکردهای بر پایه تاب‌آوری در حوزه زیرساخت‌های حیاتی علاوه بر اقدامات و الزامات پیشگیرانه، کاهش‌دهنده و فعالیت‌های آمادگی قبل از وقوع بحران، بر روی انطباق، پاسخ و واکنش مناسب در جریان بحران، و مهمتر از همه بازیابی پس از وقوع بحران نیز احاطه دارند. این اقدامات منحصر به شرایط بحران نیست و بروز هرگونه اختلال در خدمت‌رسانی و سرویس‌دهی

ایجاد یک بستر کارا برای همکاری بخش‌های دولتی و خصوصی با صاحبان و گردانندگان زیرساخت‌ها؛ از دیگر راهکارها و الزامات مطرح شده برای ایجاد جوامع تاب‌آور و عبور از وضعیت موجود به سمت وضعیت مطلوب هستند، که باید در راهبرد ملی حفاظت از زیرساخت‌های حیاتی کشور مد نظر قرار گیرند.

۵- نتیجه‌گیری

امروزه، نقش حیاتی زیرساخت‌ها در اقتصاد پایدار و توسعه جوامع از یک‌سو، تغییر شکل و تشدید تهدیدات مربوط به این حوزه از سوی دیگر، برنامه‌ریزی راهبردی برای حفاظت و تأمین امنیت زیرساخت‌های حیاتی را الزام‌آور ساخته است. این مهم با بررسی و روزرسانی مداوم سیاست‌ها و راهبردهای اتخاذ شده در این حوزه امکان‌پذیر است. از این رو، بازنگری و اصلاح طرح‌ها و برنامه‌های حفاظت از زیرساخت‌های حیاتی، چند سالی است که در دستورکار کشورهای بسیاری قرار گرفته است.

از آنجا که در کشور عزیزمان حفاظت از سامانه‌ها و زیرساخت‌های حیاتی علاوه بر حفاظت‌های فیزیکی و الزامات نظامی امنیتی، با اجرای ضوابط و الزامات پدافند غیرعامل محقق می‌گردد؛ این مقاله با بررسی و تحلیل راهبردهای اتخاذ شده در سطوح ملی، در راستای اهداف کمک به ایجاد درک بهتر تهدیدات و چالش‌های پیش روی سامانه‌های زیرساختی، لزوم تغییر نگرش نسبت به مفاهیم و راهبردهای نوین حفاظت از زیرساخت‌های حیاتی، بیان الزامات اولیه برای توسعه چارچوب‌ها و همچنین برنامه‌ریزی راهبردی تأمین امنیت زیرساخت‌های حیاتی تلاش کرده است.

در این راستا، پس از بیان لزوم تغییر نگرش نسبت به مفاهیم حفاظت و تاب‌آوری زیرساخت‌های حیاتی به عنوان یکی از مهمترین اهداف این تحقیق از، بخش‌هایی مطالعات تطبیقی در رابطه با راهبردهای ملی حفاظت از زیرساخت‌های حیاتی از منظر دستورالعمل‌ها، راهبردها و سیاست‌های راهبردی برخی کشورها به صورت هدفمند طرح شد. در نهایت، الزامات اولیه در رابطه با راهبرد ملی حفاظت از زیرساخت‌های حیاتی، با شناسایی و تحلیل نقاط تمرکز، اولویت‌ها و چالش‌های راهبردک در این حوزه با رویکردی آینده پژوهانه ارائه شد. امید است این پژوهش بتواند الهام بخش راهکارهایی نو متناسب با نیازهای کشور، و همگام با دیدگاه‌های بین‌المللی، در جهت افزایش توانمندی کشور در حوزه تأمین هر چه بهتر امنیت زیرساخت‌های حیاتی گامی هرچند اندک برداشته باشد.

اختصاص مطالعات بیشتر روی مدل‌سازی و تحلیل تاب‌آوری زیرساخت‌های حیاتی، با توجه خسارات و تبعات شدید حوادث با

باید توجه داشت که رویکردهای بر پایه تاب‌آوری، نه تنها روی زیرساخت‌های مجزا متمرکز هستند، بلکه روی مجموعه کارکردهای ضروری اجتماعی نیز توجه ویژه‌ای داشته و موضوع جوامع تاب‌آور به عنوان یکی از بحث‌های بین‌رشته‌ای جذاب و پرطرفدار حال حاضر در حوزه تحقیقات آکادمیک کشورهای پیشرفته، در معرض ظهور و توسعه بیشتر قرار گرفته است.

اما گذر از بحث‌های پیشین حفاظت از زیرساخت‌های حیاتی و وضعیت موجود، به سمت راهبردهای نوین حفاظتی و مفهوم فراگیر جوامع تاب‌آور (وضعیت مطلوب)، مستلزم ایجاد یک سری تغییرات کلیدی است. از آنجایی که نمی‌توان به طور قاطع مشخص کرد که کدام زیرساخت‌ها نقش حیاتی‌تری در پیشبرد اهداف هر اجتماع دارند، توسعه استانداردهای تاب‌آوری در همه زیرساخت‌ها موجب افزایش امنیت در کل جامعه خواهد شد. از طرفی دیگر، اگر زیرساخت‌ها اصولاً تاب‌آور ساخته شوند، از هزینه‌های زیاد حفاظت از آن‌ها نیز کاسته می‌شود. بنابراین، مفهوم تاب‌آوری باید به عنوان یک استاندارد همه‌جانبه در طراحی و مدیریت زیرساخت‌ها در نظر گرفته شود.

زیرساخت‌های حیاتی اصولاً برای بلندمدت ساخته می‌شوند، بدیهی است یک زیرساخت بی‌دوام و شکننده، حتی با وجود اقدامات کاهشی یا تعدیل اثر یا گزینه‌های پشتیبان و افزونگی، نمی‌تواند بلافاصله جایگزین یا بازسازی شود. از این رو، داشتن دیدگاه بلندمدت در مسأله امنیت زیرساخت‌های حیاتی با ایجاد و توسعه مدیریت ریسک در همه ساختارهای اجتماعی به منظور تاب‌آوری جوامع و عبور از وضعیت موجود، امری ضروری است. همچنین، از آنجایی که زیرساخت‌ها و تهدیدات متوجه آن‌ها به طور دائم در حال تغییر هستند، اتخاذ معیارها و شاخص‌های بهتر برای ارزیابی و طراحی آن‌ها در کوتاه‌مدت، ایجاد سامانه‌های تاب‌آور در طول دهه‌های بعد را در پی خواهد داشت. بعلاوه، چشم انداز روبه‌رشد تهدیدات سایبری در سطوح ملی نیز بیانگر این حقیقت است که باید با استفاده از رویکردهای جامع بر پایه مفهوم تاب‌آوری، تلاش‌های بیشتری برای ایجاد و توسعه راهبردهای نوین در حوزه امنیت سایبری کشور صورت گیرد.

لزوم چندمخاطره‌ای و چندجانبه بودن عملکردها و اقدامات تأمین امنیت زیرساخت‌ها؛ بکارگیری رویکردهای پیشگیرانه و مردم محور؛ لحاظ تاب‌آوری در عملکردهای مدیریتی تمامی بخش‌های دولتی و خصوصی با مشارکت و تعامل کل جامعه؛ لزوم تقویت انسجام در سیاست‌ها، اهداف، شاخص‌ها و سامانه‌های ارزیابی عملکرد؛ پیاده‌سازی راهبرد امنیت سایبری ایمن برای ایجاد جامعه‌ای با عملکردهای الکترونیکی تاب‌آور؛ تقسیم مسئولیت‌ها بین دولت، مقامات بخش‌های مختلف و ذینفعان؛ و

- International Critical Information Infrastructure Protection Policies, Zurich, Switzerland: ETH (Swiss Federal Institute of Technology), vol. 1, 2006.
- [9] The Report of the President's Commission on Critical Infrastructure Protection, "Critical Foundations: Protecting America's Infrastructures," Washington, DC, 1997.
- [10] G. M. Brown, M. Carlyle, J. Salmeron, and K. Wood, "Defending Critical Infrastructure," *Interfaces*, vol. 36, no. 6, pp. 530-544, 2006.
- [11] C. Pursiainen, "The Challenges for European Critical Infrastructure Protection," *J. Eur. Integr.*, vol. 31, no. 6, pp. 721-739, 2009.
- [12] P. W. Parfomak, "Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options," CRS Report for Congress, Congressional Research Service, Washington, DC, USA, 2007.
- [13] T. D. O'Rourke, "Critical Infrastructure, Interdependencies and Resilience," *Bridge-Washington-National Academy of Engineering*, vol. 37, no.1, pp. 22-29, 2007.
- [14] Commission of the European Communities, "Proposal for a Directive of the Council on Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve Their Protection," Brussels, 2006.
- [15] European Council, "On the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection," *Official Journal of the European Union*, Council Directive 2008/114/EC, Dec. 2008.
- [16] M. Lindström and S. Olsson, "The European Programme for Critical Infrastructure Protection," in *Crisis Management in the European Union: Cooperation in the Face of Emergencies*, S. Olsson, Ed., Heidelberg, Berlin: Springer, 2009.
- [17] C. Pursiainen and P. Gattinesi, "Towards Testing Critical Infrastructure Resilience," EUR—Scientific and Technical Research reports, European Commission, Joint Research Center, Luxembourg, Rep. EUR 26575 EN, Feb. 2014.
- [18] J. D. Moteff, "Critical infrastructure resilience: the evolution of policy and programs and issues for Congress," Washington DC, USA, CRS Report no. R42683, 2012. [Online]. Available: <https://cyberwar.nl/d/R42683.pdf>
- [19] Department of Homeland Security, "NIPP 2013: Partnering for Critical Infrastructure Security and Resilience," United States Department of Homeland Security (DHS), Washington, DC, USA, 2013. [Online]. Available: <https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience>
- [20] European Commission, "Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCIP)," Brussels, Belgium, Rep. SWD (2012) 190 final, 2012. [Online]. Available: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/pdf/policies/crisis_and_terrorism/epcip_sw_d_2012_190_final.pdf

احتمال وقوع کم و تاثیرگذاری بالا روی این زیرساخت‌ها و جامعه‌ی متأثر آن‌ها، امروز بیش از قبل ضروری است. نتیجه این امر، استفاده از راهکارهای نوین حفاظتی برای دستیابی به زیرساخت‌هایی امن با حداقل آسیب‌پذیری در برابر حوادث خواهد بود. بنابراین، از جمله مهمترین محورهای تحقیقاتی آینده‌پژوهانه در این حوزه، توسعه و ایجاد شاخص‌ها، معیارها و روش‌های مختلف مدل‌سازی و تحلیل تاب‌آوری زیرساخت‌های حیاتی کشور در برابر انواع مخاطرات و وابستگی‌های متقابل است. در این زمینه، مدل‌سازی و بهبود تاب‌آوری زیرساخت‌های انرژی و مخازنی، با توجه نقش اعانه‌دهنده و اساسی آن‌ها در پیشبرد اهداف سایر زیرساخت‌ها و همچنین با توجه به اینکه نسبت به ساختارهای دولتی و نظامی اهداف آسیب‌پذیرتر و در دسترس‌تری هستند، در برابر حوادث شدید آب و هوایی و حملات عمدی و تروریستی، از اساسی‌ترین اولویت‌های پژوهشی حال حاضر در کشور معرفی می‌شود. برآیند این مطالعات، توسعه الزامات و راهبردهای حفاظتی در حوزه پدافند غیرعامل و در نتیجه، تضمین امنیت زیرساخت‌های کشور عزیزمان در برابر انواع مخاطرات خواهد بود.

۶- مراجع

- [1] F. Petit, D. Verner, J. Phillips, and L. P. Lewis, "Critical Infrastructure Protection and Resilience Integrating Interdependencies," in *Security by Design*, A. J. Masys, Ed., Cham., Switzerland: Springer, 2018.
- [2] R. Ghaffarpour and S. Zamanian, "Determining the Importance of Implementing Passive Defense in 400 KV High Voltage Posts Using Multiple Attribute Decision-Making Methods," *Passive Defense Quarterly*, vol. 9, no. 1, pp. 1-8, 2018. (In Persian)
- [3] Y. Wang, C. Chen, J. Wang, and R. Baldick, "Research on Resilience of Power Systems Under Natural Disasters—A Review," *IEEE Trans. Power Systems*, vol. 31, no. 2, pp. 1604-1613, 2016.
- [۴] جلالی، غلامرضا، چهارگفتار در باب پدافند غیرعامل، قم، محدث، ۱۳۹۱.
- [5] B. Allenby and J. Fink, "Toward Inherently Secure and Resilient Societies," *Science*, vol. 309, pp. 1034-1036, 2005.
- [6] T. C. Sharkey, B. Cavdaroglu, H. Nguyen, J. Holman, J. E. Mitchell, and W. A. Wallace, "Interdependent Network Restoration: On the Value of Information-Sharing," *Eur. J. Oper. Res.*, vol. 244, pp. 309-321, 2015.
- [7] R. Francis and B. Bekera, "A Metric and Frameworks for Resilience Analysis of Engineered and Infrastructure Systems," *Reliab. Eng. Syst. Safe.*, vol. 121, pp. 90-103, 2014.
- [8] A. Wenger and V. Mauer, Eds., *International CIIP Handbook 2006: An Inventory of 20 National and 6*

- <https://www.divaortal.org/smash/get/diva2:700420/FULLTEXT01.pdf>
- [34] The Swedish Civil Contingencies Agency, "Annual Report 2011: Sweden's National Platform for Disaster Risk Reduction," MSB, Karlstad, Sweden, 2011. [Online]. Available: <https://www.msb.se/siteassets/dokument/publikationer/english-publications/annual-report-2011-swedens-national-platform-for-disaster-reduction.pdf>
- [35] The Swedish Civil Contingencies Agency, "Strategic challenges for societal security," MSB, Karlstad, Sweden, 2013. [Online]. Available: <https://www.msb.se/siteassets/dokument/publikationer/english-publications/strategic-challenges-for-societal-security.pdf>
- [36] The Swedish Civil Contingencies Agency, "Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure," MSB, Karlstad, Sweden, 2014. [Online]. Available: <https://www.msb.se/siteassets/dokument/publikationer/english-publications/action-plan-for-the-protection-of-vital-societal-functions--critical-infrastructure.pdf>
- [37] The Swedish Civil Contingencies Agency, "Making Cities Resilient in Sweden," MSB, Karlstad, Sweden, 2015. [Online]. Available: <https://www.msb.se/siteassets/dokument/publikationer/english-publications/resilient-cities-in-sweden-six-inspiring-examples-on-drr-action.pdf>
- [38] The Swedish Civil Contingencies Agency, "Swedish National Risk Assessment 2012," MSB, Karlstad, Sweden, 2013. [Online]. Available: <https://www.msb.se/RibData/Filer/pdf/26621.pdf>
- [39] The Swedish Civil Contingencies Agency, "A Summary of Risk Areas and Scenario Analyses 2012–2015," MSB, Karlstad, Sweden, 2016. [Online]. Available: <https://www.msb.se/siteassets/dokument/publikationer/english-publications/a-summary-of-risk-areas-and-scenario-analyses-20122015.pdf>
- [40] Ministry of The Interior Finland, "National Risk Assessment 2015," Ministry of the Interior Publication, Helsinki, Finland, 2016. [Online]. Available: <http://julkaisut.valtioneuvosto.fi/handle/10024/64973>
- [41] Australian Government, "Critical Infrastructure Resilience Strategy," Commonwealth of Australia, 2010. [Online]. Available: <https://www.tisn.gov.au/Documents/Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.pdf>
- [42] Australian Government, "Critical Infrastructure Resilience Strategy: Plan," Commonwealth of Australia, 2015. [Online]. Available: <https://cicentre.gov.au/document/P16S011>
- [43] Australian Government, "Critical Infrastructure Resilience Strategy: Policy Statement," Commonwealth of Australia, 2015. [Online]. Available: <https://cicentre.gov.au/document/P16S013>
- [21] United Nations General Assembly, "Report of the Open-Ended Intergovernmental Expert Working Group on Indicators and Terminology Relating to Disaster Risk Reduction," UNISDR, New York, NY, USA, 2016.
- [22] A. Boin and A. McConnell, "Preparing for critical infrastructure breakdowns: the limits of crisis management and the need of resilience," *J. Conting. Crisis Man.*, vol. 15, pp. 50–59, 2007.
- [23] E. Zio, "Challenges in the Vulnerability and Risk Analysis of Critical Infrastructures," *Reliab. Eng. Syst. Safe.*, vol. 152, pp. 137–150, 2016.
- [24] J. Landstedt and P. Holmström, "Electric Power Systems Blackouts and the Rescue Services: The Case of Finland," Emergency Services College of Finland and State Provincial Office of Western Finland, Finland, 2007.
- [25] N. Petrakos and P. Kotzanikolaou, "Methodologies and Strategies for Critical Infrastructure Protection," In *Critical Infrastructure Security and Resilience*, D. Gritzalis, M. Theocharidou, and G. Stergiopoulos, Eds., Cham, Switzerland: Springer, 2019.
- [26] White House, "Presidential Decision Directive 63: Protecting America's Critical Infrastructures," Washington, DC, USA, 1998. [Online]. Available: <http://www.fas.org/irp/offdocs/pdd-63.htm>
- [27] White House, "Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience," Washington, DC, USA, 2013. [Online]. Available: <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>
- [28] The Danish Emergency Management Agency, "National Risk Profile," DEMA, Denmark, 2013. [Online]. Available: [https://brs.dk/viden/publikationer/Documents/National_Risk_Profile_\(NRP\)_-_English-language_version.pdf](https://brs.dk/viden/publikationer/Documents/National_Risk_Profile_(NRP)_-_English-language_version.pdf)
- [29] The Danish Emergency Management Agency, "Crisis Management in Denmark," DEMA, Denmark, 2015. [Online]. Available: https://brs.dk/viden/publikationer/Documents/Crisis%20Management%20in%20Denmark_UK.pdf
- [30] The Danish Emergency Management Agency, "National Risk Profile for Denmark," DEMA, Denmark, 2018. [Online]. Available: <https://brs.dk/viden/publikationer/Documents/Danes%20perception%20of%20risk.pdf>
- [31] The Norwegian Directorate for Civil Protection, "National Risk Analysis 2014," DSB, Norway, 2014. [Online]. Available: https://www.dsb.no/globalassets/dokumenter/rapporter/nrb_2014_english.pdf
- [32] The Norwegian Directorate for Civil Protection, "Vital Functions in Society," DSB, Norway, 2017. [Online]. Available: https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-ii_english_version.pdf
- [33] C. Pursiainen, Ed., "Towards a Baltic Sea Region Strategy in Critical Infrastructure Protection," Nordic Centre for Spatial Development (Nordrgio), Stockholm, Sweden, Nordrgio Rep. 2007:5, 2007. [Online]. Available:

New Critical Infrastructure Protection Strategies

S. M. Miryousefi, R. Ghaffarpour*

Abstract

Nowadays, critical infrastructures are more vulnerable to natural events, malicious physical and cyber-based attacks or intrusions. Since most societal functions rely heavily on critical infrastructures' functionality, disturbances in any of them, can yield fatal consequences for interdependent infrastructures and subsequently, for the depending society. Therefore, critical infrastructure protection (CIP) has become an important research field in this century. In our country, to strengthen critical infrastructures and reduce the likelihood of willful attacks, possible vulnerabilities and negative consequences, it is imperative to consider the requirement of passive defense. Hence, critical infrastructure protection against any types of threats, as one of the goals of passive defense, would be achieved by developing and expanding appropriate strategies and guidelines. In this paper existing methodologies and national strategies for critical infrastructure protection is described. Resilience as a novel concept in common practices and strategies that have been applied in various countries to establish national protection plans, is investigated. In the concluding remarks, a set of strategic goals and also the most important challenges and requirements for developing critical infrastructure protection frameworks with a futuristic outlook are proposed. Thus, comparative research methodology is used to analyze the primary requirements of our national critical infrastructure protection strategy which could be counted as an effective step in achieving passive defense objectives.

Key Words: *Critical Infrastructure Protection, Critical Infrastructure, Security, Vulnerability, Resilience, Passive Defense*