

Policy Strategies for Enhancing the Security Resilience of Iran's Electricity Infrastructure Against Environmental Hazards and Technological Attacks

Mohammad Babaei¹, Seyed Ali Mosazadeh², Ebrahim Safari³

£

secondYear
Autumn and Winter1404

Research paper

:Date received
1404/05/01
:Date accepted
1404/05/29
Pages: 169-190

Abstract:

In the era of digital transformation and the Fourth Industrial Revolution, the

boundary between physical and cyber security has become blurred, and technological threats have become one of the main challenges to national security. Environmental systems and technological infrastructures are highly interdependent, and the combined environmental and digital risks have made countries' power grids strategic targets for cyber and destructive attacks. This research, with a "macro and strategic perspective" and with a special focus on the power infrastructure as the backbone of the country's social, economic, and defense sustainability, analyzes the policy of technological risks and presents a national model of technological resilience in Iran. The analysis framework includes three fundamental axes: the evolution of the concept of infrastructure security in light of new technologies, the recognition of technological governance gaps, and the design of a strategic model for reengineering energy policy and protecting electricity infrastructure. The findings show that technological resilience is not simply the product of technical development, but rather the combined result of policy, technology, and human resource management, and to overcome combined threats, Iran needs to establish national technological sovereignty. Based on this analysis, Iran's national doctrine of technological resilience is based on four fundamental principles: Focusing national strategic command and direction, intelligent risk analysis and early warning, protecting energy and critical infrastructure, and developing human capital and national technological literacy. This framework can be the basis for designing national policies and strategies to increase infrastructure resilience and national security.

Keywords: National resilience, environmental risks, national security, electricity infrastructure, artificial intelligence, technological policy

- 1 . PhD in National Security Threats, Imam Hadi (AS) Faculty, Imam Hussein (AS) University,
- 2 . Corresponding author: PhD in Political Geography, Imam Hadi (AS) Faculty, Imam Hussein (AS) Comprehensive University,
- 3 . PhD in English Language Teaching, Imam Hadi (AS) Faculty, Imam Hussein (AS) University,

استراتيجيات سياسية لتعزيز قدرة البنية التحتية للكهرباء في إيران على الصمود في وجه المخاطر البيئية والهجمات التكنولوجية

محمد بابائي^١، سيد علي موسى زاده^٢، ابراهيم سفري^٣

ملخص

في عصر التحول الرقمي والثورة الصناعية الرابعة، باتت الحدود بين الأمن المادي والأمن السيبراني غير واضحة، وأصبحت التهديدات التكنولوجية أحد أبرز التحديات التي تواجه الأمن القومي. وترتبط الأنظمة البيئية والبنية التحتية التكنولوجية ارتباطاً وثيقاً، وقد جعلت المخاطر البيئية والرقمية مجتمعةً شبكات الطاقة في الدول أهدافاً استراتيجية للهجمات السيبرانية والتدميرية. يحلل هذا البحث، من منظور استراتيجي شامل، مع التركيز بشكل خاص على البنية التحتية للطاقة باعتبارها الركيزة الأساسية للاستدامة الاجتماعية والاقتصادية والدفاعية للبلاد، سياسة المخاطر التكنولوجية، ويقدم نموذجاً وطنياً للمرونة التكنولوجية في إيران. يشمل إطار التحليل ثلاثة محاور أساسية: تطور مفهوم أمن البنية التحتية في ضوء التقنيات الحديثة، وتحديد الثغرات في الحوكمة التكنولوجية، وتصميم نموذج استراتيجي لإعادة هندسة سياسة الطاقة وحماية البنية التحتية للكهرباء. وتُظهر النتائج أن المرونة التكنولوجية ليست مجرد نتاج للتطور التقني، بل هي نتيجة مُجمعة للسياسات والتكنولوجيا وإدارة الموارد البشرية، وللتغلب على التهديدات المُجمعة، تحتاج إيران إلى ترسيخ سيادتها التكنولوجية الوطنية. وبناءً على هذا التحليل، تستند العقيدة الوطنية الإيرانية للمرونة التكنولوجية إلى أربعة مبادئ أساسية:

يركز هذا الإطار على القيادة والتوجيه الاستراتيجيين الوطنيين، والتحليل الذكي للمخاطر والإنذار المبكر، وحماية الطاقة والبنية التحتية الحيوية، وتنمية رأس المال البشري والمعرفة التكنولوجية الوطنية. ويمكن أن يشكل هذا الإطار أساساً لتصميم سياسات واستراتيجيات وطنية لتعزيز مرونة البنية التحتية والأمن القومي.

الكلمات المفتاحية: المرونة الوطنية، المخاطر البيئية، الأمن القومي، البنية التحتية

للكهرباء، الذكاء الاصطناعي، السياسة التكنولوجية

١. حاصل على درجة الدكتوراه في التهديدات الأمنية الوطنية، كلية الإمام الهادي (عليه السلام)، جامعة الإمام الحسين (عليه السلام).

٢. المؤلف المسؤول عن المراسلات: حاصل على درجة الدكتوراه في الجغرافيا السياسية، كلية الإمام الهادي (عليه السلام)، جامعة الإمام الحسين (عليه السلام) الشاملة.

٣. حاصل على درجة الدكتوراه في تدريس اللغة الإنجليزية، كلية الإمام الهادي (عليه السلام)، جامعة الإمام الحسين (عليه السلام).

راهبردهای سیاستی ارتقاء تاب‌آوری امنیتی زیر ساخت برق ایران در برابر مخاطرات محیطی و حملات فناوریانه

محمد بابایی^۱، سیدعلی موسی زاده^۲، ابراهیم صفری^۳

چکیده

در عصر تحول دیجیتال و انقلاب صنعتی چهارم، مرز میان امنیت فیزیکی و سایبری مبهم شده و تهدیدات فناوریانه به یکی از اصلی‌ترین چالش‌های امنیت ملی تبدیل شده‌اند. سیستم‌های زیست‌محیطی و زیرساخت‌های فناوریانه به شدت به یکدیگر وابسته هستند و مخاطرات ترکیبی محیطی و دیجیتالی، شبکه‌های برق کشورها را به اهداف استراتژیک برای حملات سایبری و مخرب تبدیل کرده است. این پژوهش با «نگرش کلان و راهبردی» و با تمرکز ویژه بر زیرساخت برق به عنوان ستون فقرات پایداری اجتماعی، اقتصادی و دفاعی کشور، به تحلیل سیاستی مخاطرات فناوریانه و ارائه الگوی ملی تاب‌آوری فناوریانه در ایران می‌پردازد. چارچوب تحلیل شامل سه محور بنیادین است: تحول مفهوم امنیت زیرساختی در پرتو فناوری‌های نوین، بازشناسی خلأهای حکمرانی فناوریانه و طراحی الگویی راهبردی برای بازمهندسی سیاست انرژی و حفاظت از زیرساخت برق. یافته‌ها نشان می‌دهد تاب‌آوری فناوریانه نه صرفاً محصول توسعه فنی، بلکه نتیجه تلفیقی از سیاست، فناوری و مدیریت منابع انسانی است و برای عبور از تهدیدات ترکیبی، ایران نیازمند استقرار حاکمیت فناوریانه ملی است. بر اساس این تحلیل، دکترین ملی تاب‌آوری فناوریانه ایران بر چهار اصل بنیادین استوار است: تمرکز فرماندهی و هدایت راهبردی ملی، تحلیل هوشمند مخاطرات و هشدار سریع، حفاظت از انرژی و زیرساخت‌های حیاتی و توسعه سرمایه انسانی و سواد فناوریانه ملی. این چارچوب می‌تواند مبنای طراحی سیاست‌ها و استراتژی‌های ملی برای افزایش تاب‌آوری زیرساخت‌ها و امنیت کشور باشد.

واژگان کلیدی: تاب‌آوری ملی، مخاطرات محیطی، امنیت ملی، زیرساخت برق، هوش مصنوعی،

سیاست فناوریانه

۴

سال دوم

پاییز و زمستان ۱۴۰۴

مقاله پژوهشی

تاریخ دریافت:

۱۴۰۴/۰۵/۰۱

تاریخ پذیرش:

۱۴۰۴/۰۵/۲۹

صص: ۱۶۹-۱۹۰

۱. دکتری تهدیدات امنیت ملی، دانشکده امام هادی^(ع)، دانشگاه جامع امام حسین^(ع)،

(dr.mohammadbabaee.1970@gmail.com)

۲. نویسنده مسئول: دکتری جغرافیای سیاسی، دانشکده امام هادی^(ع)، دانشگاه جامع امام حسین^(ع)،

(seyvedali3023@gmail.com)

۳. دکتری آموزش زبان انگلیسی، دانشکده امام هادی^(ع)، دانشگاه جامع امام حسین^(ع)،

(safariiabrahim1@gmail.com)

۱. مقدمه:

در جهان معاصر، فناوری دیگر تنها ابزار توسعه نیست، بلکه به عاملی مؤثر در شکل‌دهی نظم امنیتی نوین تبدیل شده است، به‌طوری که زیرساخت‌های حیاتی مانند شبکه‌های برق در برابر تهدیدات سایبری و ترکیبی آسیب‌پذیرتر از همیشه هستند. پژوهش‌ها نشان می‌دهند که با دیجیتالی شدن شبکه‌های الکتریکی و یکپارچه شدن اجزای فیزیکی و دیجیتال، پیامدهای آسیب‌پذیری‌ها گسترده‌تر شده‌اند و تهدیدات سایبر-فیزیکی می‌توانند عملکرد و پایداری این شبکه‌ها را به‌طور جدی مختل کنند، به‌ویژه زمانی که کنترل و ارتباطات دیجیتال نقش کلیدی در بهره‌برداری شبکه دارند. (Zibaeirad et al., 2024)

در چنین شرایطی، کشورهایی که فاقد نظام یکپارچه تاب‌آوری فناورانه باشند، در برابر بحران‌های ترکیبی محیطی و فناورانه به سرعت دچار فروپاشی سیستمی خواهند شد. جمهوری اسلامی ایران نیز به واسطه موقعیت ژئوپلیتیکی و ساختار زیرساختی خود، از جمله شبکه برق ملی، تأسیسات هسته‌ای، صنایع نظامی و هواپیمایی، بیش‌از هر زمان دیگر نیازمند راهبرد ملی تاب‌آوری فناورانه است. در دهه اخیر، هم‌زمان با افزایش وابستگی به فناوری‌های دیجیتال در بخش انرژی و دفاع، مخاطرات نوینی همچون تهدیدات ناشی از شناسایی و حمله توسط سامانه‌های سنسور از راه دور دشمن، تهدیدات ناشی از تهاجم هوایی، حملات سایبری هدفمند، تهدیدات ناشی از اقدامات تروریستی (بمب‌های گرافیتی و ...)، اختلال در سامانه‌های صنعتی ناشی از بکارگیری سلاح‌های الکترومغناطیس و تهدیدات هوش مصنوعی ظهور یافته‌اند که نمونه‌هایی از حملات تروریستی به شبکه‌های برق کشورهای مختلف در جدول زیر تشریح شده است:

نام کشور	تاریخ حمله	مکان حمله	نحوه و نتایج حمله
آمریکا	نیمه شب ۱۶ آوریل ۲۰۰۳	حمله تروریستی به پست انتقال شرکت Metcalf در نزدیکی Jose San	ابتدا مهاجمین کابل فیبر نوری AT & T را قطع کرده و سامانه ارتباطی را از کار انداختند و سپس با شلیک‌های متعدد به تجهیزات پست باعث از کار افتادن ۱۷ ترانسفورماتور از مجموع ۲۰ ترانسفورماتور آن پست انتقال گردیدند و حدود ۱۶ میلیون دلار صدمه وارد کردند. این حادثه منجر به از کار افتادن آن پست به مدت ۲۷ روز گردید.

راهبردهای سیاستی ارتقاء تاب‌آوری امنیتی زیر ساخت برق ایران در برابر مخاطرات محیطی و حملات فناورانه

عراق	ابتدای شروع حملات نیروهای داعش در سال ۲۰۱۴	حمله تروریست ها به سه دکل در دو خط انتقال برق پر قدرت بین دیالی و کرکوک	استفاده از بمب های دست ساز و آسیب رسانی به چهار خط انتقال برق، توقف نیروگاه های متعدد برق رسانی در عراق، خروج ۱۱۰۰ مگا وات برق از مدار
آلبانی	۳۱ دسامبر ۲۰۱۳	حمله تروریستی به دکل برق در منطقه Kurbini	استفاده از TNT و انهدام یکی از پایه های دکل
یمن	سپتامبر ۲۰۱۴	حمله تروریستی به خطوط انتقال برق کشور	خاموشی سراسری: ۲۳ میلیون نفر در یک روز بدون برق ماندند

(پالیزوان و دشتی، ۱۳۹۶: ص ۳)

علاوه بر موارد مندرج در جدول قبلی، حمله گروه BlackEnergy به شبکه برق اوکراین (۲۰۱۵)، حمله سایبری به زیر ساخت برق ونزوئلا (۲۰۱۹) و حملات نظامی روسیه به زیر ساخت های برق اوکراین (۲۰۲۴) نمونه های دیگری از ضربه به زیرساخت های برق کشورهاست که می توان به آنها اشاره نمود.

در ایران نیز طی سال های اخیر حملات سایبری متعددی به سامانه های کنترل توانیر صورت گرفت که با هشیاری دست اندرکاران توانیر خنثی سازی شد و مانع از قطع سراسری برق یا اختلال جدی در روند برق رسانی کشور گردید. بر اساس اظهارات رسمی شرکت توانیر؛ در جنگ تحمیلی ۱۲ روزه رژیم صهیونیستی علیه ایران در سال ۱۴۰۴، بیش از ۵۰ حادثه بزرگ برق رسانی در کشور (ناشی از حملات موشکی) شکل گرفت که حجم خسارات وارده به تأسیسات صنعت برق، حدود ۲۰۰۰ میلیارد تومان برآورد گردید (رجبی مشهدی، ۱۴۰۴). این رخدادها نشان دادند که زیرساخت کشور نه تنها ستون فقرات توسعه اقتصادی، بلکه محور پایداری امنیت ملی است. درعین حال مخاطرات محیطی مانند سیل، زلزله و خشکسالی نیز ساختار شبکه برق را تهدید می کند.

از سوی دیگر، در اسناد بالادستی کشور مانند «سند ملی امنیت سایبری» و «نقشه جامع علمی کشور» اگرچه به مقوله امنیت در حوزه های مختلف نظیر امنیت انسانی، زیرساخت ها، توسعه انسانی، اقتصاد، فرهنگ و ... اشاره شده، اما مفهوم تاب آوری فناورانه هنوز به صورت مستقل و عملیاتی مورد سیاست گذاری قرار نگرفته است (نصر اصفهانی و همکاران، ۱۴۰۳). این

خلاً باعث شده است که در مواجهه با بحران‌ها، تصمیم‌گیری‌ها بیشتر واکنشی باشند تا ساختاری و پیش‌دستانه.

در نتیجه پژوهش حاضر با هدف طراحی یک چارچوب نظری و سیاستی برای مدیریت هوشمند مخاطرات فناورانه در ایران و تدوین الگوی ملی تاب آوری فناورانه با تمرکز بر زیرساخت برق کشور انجام می‌شود.

۲. پیشینه پژوهش

مسعود کسرای نژاد (۱۳۹۴) در پژوهش خود با عنوان «مطالعه فنی، اقتصادی و زیست محیطی ساخت نیروگاه تولید هم زمان برق، حرارت و برودت (CCHP)» به ارزیابی احداث نیروگاه با ویژگی‌های یاد شده از منظر اقتصادی پرداخته و در پایان، ساخت نیروگاه تولید هم زمان در مقیاس ۵ مگاوات را تأیید و دارای توجیه پذیری مالی و اقتصادی عنوان کرده است.

نجفی روادانق و همکاران (۱۳۹۸) در مقاله «چارچوب طراحی شبکه‌های توزیع تاب آور در برابر حوادث طبیعی» عمده مطالعات خود را بر طراحی تاب آور بهینه شبکه توزیع برق استوار نموده و به منظور نیل به این هدف و مفهوم تاب آوری و عوامل مؤثر در ارتقای آن، استخراج اطلس جامع آسیب پذیری شبکه‌های توزیع و همچنین مدل سازی ریسک مبتنی بر حوادث طبیعی را مورد بحث و بررسی قرار داده اند.

جاسیوناس و همکاران (۲۰۲۱) در مقاله ای با عنوان «مروری بر تاب آوری سیستم انرژی» با ارائه یک نمای کلی از چشم انداز تهدید و بررسی دقیق تر از تهدیدات سایبری و آب و هوایی عنوان می نمایند: «اختلالات عمده» این پتانسیل را دارند که به درآمدهای سالیانه بخش های انرژی خسارت وارد کنند. این مقاله تصریح می کند که تاب آوری سیستم انرژی به نوع سیستم و نوع تهدید بستگی داشته و با تغییر سیستم ها؛ انواع تهدیدات مرتبط نیز تغییر می کنند.

نوروستا و همکاران (۱۴۰۱) در مقاله «شناسایی و اولویت بندی تهدیدات نیروگاه های برق حرارتی و ارائه راهکارهای پدافند غیر عامل» به شناسایی و اولویت بندی تهدیدات اثرگذار محیطی و به دست آوردن راهکارهای متناسب با اصول و مبانی پدافند غیر عامل پرداخته است.

یزدانی (۲۰۲۳) در مقاله « تجزیه و تحلیل و برنامه ریزی تاب آوری سیستم انرژی » عنوان می نماید که سناریوهای تاب آوری شامل نوسانات سوخت های فسیلی، نوسانات تقاضا و کمبود عرضه انرژی است. نتایج تحقیقات وی نشان می دهد که طیف گسترده ای از اثرات هزینه (علی الخصوص هزینه سرمایه گذاری سیستم انرژی) برای یک سیستم انرژی؛ بسته به نوع انتخاب سیستم و سناریوی تاب آوری است (صادقی و همکاران، ۱۴۰۲).

در جمع بندی پیشینه، می توان گفت: شکاف اصلی در نظام پژوهش و سیاست ایران، نبود مدل جامع حکمرانی داده محور برای مدیریت هم زمان مخاطرات محیطی و فناورانه است. لذا لازم است یک چارچوب مفهومی بومی سازی شده برای مرحله عملیاتی تدوین شود که با هویت اجتماعی- اسلامی ایران سازگار بوده و بر اصول حکمرانی مبتنی بر مقاومت تکیه داشته باشد.

۳. چارچوب مفهومی

مفهوم تاب آوری امنیتی در عصر فناوری های نوین اصطلاح « تاب آوری » برای اولین بار توسط هولینگ (Holling, 1973) در علم اکولوژی برای تبیین مفهوم توانایی یک سیستم برای جذب شوک ها، تغییرات و اختلالات در حالی که عملکرد سیستم باقی بماند، تعریف گردید. (Wang et al, 2015)

Spaans & Waterhout (2017) تاب آوری را در توانایی افراد، جوامع، مؤسسات، شرکت ها و سیستم ها در یک شهر برای زنده ماندن، سازگاری و رشد بدون در نظر گرفتن نوع استرس مزمن و شوک های حاد که در معرض آن قرار دارند، تعریف می نمایند.

جهانی شدن و تحولات سریع؛ از ویژگی های محیطی عصر کنونی است. در این شرایط، کشورها باید انعطاف پذیری و قدرت واکنش منطقی در محیط پرقابث را داشته باشند تا با شرایط موجود همسو و بقای خود را حفظ کنند (نجاری و همکاران، ۱۳۹۴).

بررسی ها نشان می دهد که در سطح ملی، تاب آوری امنیتی شامل سه رکن بنیادین است:

۱. شناخت تهدید فناورانه
۲. تطابق توان انطباق زیرساختی
۳. ظرفیت تصمیم سازی سریع و داده محور

مفهوم تاب آوری فناوریانه

تاب آوری فناوریانه (Technological Resilience) از تلاقی سه حوزه « مدیریت بحران»، « فناوری‌های نوین» و « امنیت ملی» پدید آمده‌است. همانطور که در بخش چارچوب مفهومی اشاره شد؛ این مفهوم به توانایی یک نظام ملی در حفظ تداوم و عملکرد حیاتی خود در برابر شوک‌های حاد اعم از تهدیدات فناوریانه، حملات سایبری، اختلالات داده‌ای یا فروپاشی شبکه‌های هوشمند که در معرض آن قرار دارند، اشاره دارد.

از دیدگاه نظریه‌پردازان حوزه امنیت، تاب آوری فناوریانه بخشی از « امنیت زیرساختی نسل بعدی یا نسل چهارم» است که نه تنها شامل تجهیزات فیزیکی، بلکه داده‌ها، الگوریتم‌ها و شبکه‌های یادگیرنده نیز می‌شود (Siddiqui et al. 2020). در این چارچوب، تاب آوری فناوریانه به معنای بازسازی سریع ظرفیت ملی در برابر اختلال فناوریانه تعریف می‌شود، نه صرفاً پیشگیری از آن.

از نظر فلسفه امنیتی جمهوری اسلامی ایران نیز، فناوری بخشی از هویت ملی و استقلال سیاسی است. چنان‌که رهبر معظم انقلاب تأکید کرده اند: « در مسئله هوش مصنوعی، بهره بردار بودن امتیاز محسوب نمی‌شود. این فناوری لایه‌های عمیقی دارد که باید بر آن لایه‌ها مسلط شد. آن لایه‌ها دست دیگران است. اگر شما نتوانید لایه‌های عمیق و متنوع این فناوری را هوش مصنوعی را تأمین کنید، فردا اینها یک ایستگاهی مثل آژانس اتمی درست می‌کنند برای هوش مصنوعی،... که اگر چنانچه به آن ایستگاه رسیدید، باید اجازه بگیرید که در فلان بخش از هوش مصنوعی استفاده کنید، در فلان بخش دیگر حق ندارید استفاده کنید!» (آیت الله خامنه‌ای، ۱۴۰۳) که این دقیقاً همان مفهوم استقلال فناوریانه و عدم وابستگی اراده‌ای است که در ادبیات امنیت فناوری مطرح می‌شود. بر این مبنا، تاب آوری فناوریانه در ایران مفهومی فراتر از پایداری صنعتی است، بلکه ابزار صیانت از استقلال ملی در برابر وابستگی فناوریانه جهانی است.

۴. رابطه تاب آوری فناوریانه با امنیت ملی

« امنیت» از نظر مفهومی به وضعیتی اطلاق می‌شود که نیروهای حفظ‌کننده وضع موجود؛ توان محافظت را از نیروهای شناخته شده بر هم زننده آن داشته باشند (پور ابراهیمی و

همکاران، ۱۴۰۳). امنیت ملی در قرن بیست و یکم؛ دیگر تنها به معنای حفاظت از مرزها و توان نظامی نیست؛ بلکه به حفظ «حاکمیت داده»، «حفظ تمامیت سایبری» و «حفاظت و کنترل زیرساخت‌های حیاتی» کشورها نیز وابسته است. لذا دولت‌ها و جوامع؛ مجموعه‌ای از ابزارها و سیستم‌ها (نظیر هوش مصنوعی) و استراتژی‌ها را بکار می‌گیرند تا بدون از دست دادن داده‌ها یا تأخیرهای عملیاتی در برابر اختلالات و مخاطراتی همچون بلایای طبیعی، حملات سایبری و سایر بحران‌ها، توانایی تاب‌آوری خود را افزایش دهند که به تعبیری می‌توان آن را تاب‌آوری فناورانه نامید (مقدسی، ۱۴۰۴). در این میان، زیرساخت برق کشور به عنوان ستون فقرات امنیت انرژی، یکی از حساس‌ترین و حیاتی‌ترین مؤلفه‌های امنیت ملی محسوب می‌شود. برخی از پژوهشگران و اندیشه‌ورزان حوزه امنیت معتقدند که در صورت نفوذ الگوریتم‌های مهاجم به شبکه SCADA برق و خاموشی سراسری؛ نه تنها عملکرد صنعتی مختل می‌شود، بلکه امنیت ملی در حوزه‌های نظامی، هسته‌ای و ...، با تهدید فروپاشی زنجیره‌ای روبرو می‌شوند. این دیدگاه مؤید آن است که امنیت فناورانه؛ بخش جدایی‌ناپذیر امنیت ملی است، نه ضمیمه‌ای از آن.

۵. فناوری‌های نوین به مثابه دوگانه تهدید-فرصت

پژوهش‌های اخیر نشان می‌دهد که فناوری‌های نوین به‌صورت دوگانه‌ای تهدید-فرصت در ساختار امنیتی کشور عمل می‌کنند: از یک‌سو با فراهم‌سازی ابزارهای پیش‌بینی، داده‌کاوی و ارائه تحلیل سریع، موجب تقویت تصمیم‌سازی امنیتی می‌شوند و از سوی دیگر با افزایش سطح اتصال و اتکای زیرساخت‌ها به شبکه‌های هوشمند، وابستگی فناورانه و در نتیجه تهدیدپذیری راهبردی را افزایش می‌دهند. به‌ویژه فناوری‌هایی مانند هوش مصنوعی، اینترنت اشیاء (IoT) و کلان‌داده‌ها (Big Data) در عین ایجاد تحول در مدیریت منابع و بحران‌ها، بستر نفوذپذیری سایبری و بی‌ثباتی زیست‌محیطی را گسترش داده‌اند.

از نمونه‌های بارز این وضعیت، حملات سایبری ۲۰۱۴ به شبکه برق اوکراین و ۲۰۲۱ به شبکه برق تگزاس بود که در اوکراین ۲۵۰ هزار نفر از مردم را بدون برق گذاشت و در تگزاس؛ هم‌زمان با موج سرما، به بحران گسترده انسانی منجر شد (برق‌نیوز، ۱۳۹۹). این رخداد، مرز میان تهدید فناورانه و بحران محیطی را از میان برداشت.

۶. جایگاه زیرساخت برق در نظریه تاب آوری

زیرساخت برق به عنوان نظامی با پیوستگی فضایی و فناورانه بالا، محور تمام فعالیت‌های صنعتی، دفاعی و هسته‌ای کشور هاست. از دیدگاه نظریه زیر ساخت‌های حیاتی (Critical Network Theory)، هر گونه اختلال در یکی از گره‌های کلیدی آن می‌تواند به فروپاشی کل سیستم منجر شود (Yang et al. 2024). در طرح جامع پدافند غیر عامل شبکه‌های توزیع برق در برابر تهدیدات تروریستی، تاب آوری زیرساخت برق تابع عوامل زیر است:

شناخت آسیب‌ها و تهدیدات

کاهش آسیب‌پذیری

هوشمندسازی شبکه (Smart Grid Integration)

بازدارندگی بهینه در برابر حملات

استقلال سخت‌افزاری (تجهیزات) و نرم‌افزاری از منابع خارجی

نظام هشدار زود هنگام (Early Warning System)

فرماندهی مدیریت منابع انسانی و شبکه؛ برای کنترل عملیات بحران

در ایران، عوامل پیش‌گفته هنوز به‌صورت یکپارچه و جامع در سامانه‌های توزیع برق پیاده‌سازی نشده‌اند. بسیاری از این سامانه‌ها به‌طور قابل توجهی به نرم‌افزارهای خارجی یا واسطه‌ای وابسته‌اند که این مسئله می‌تواند باعث افزایش سطح تهدیدات سایبری شود؛ به‌طوری‌که یک عامل مخرب می‌تواند بدون اجرای مستقیم حمله سایبری، از طریق نفوذ یا دست‌کاری پارامترهای یادگیری ماشین، عملکرد پیش‌بینی، کنترل و پایداری شبکه‌های توزیع را مختل کند که این نوع حملات در ادبیات پژوهشی به‌عنوان حملات خصمانه بر مدل‌های هوش مصنوعی (adversarial AI attacks) شناخته شده‌اند و نشان‌دهنده ضعف در تاب آوری و قابل اعتماد بودن الگوریتم‌های ML در سیستم‌های انرژی است (Zibaeirad et al., 2024).

علاوه بر تهدیدات نرم‌افزاری، شبکه‌های برق نیز در معرض حملات فیزیکی و ترکیبی سایبری-فیزیکی قرار دارند. در این سناریوها، حمله به یک بخش از شبکه توزیع می‌تواند اثر دومینویی ایجاد کرده و پیامدهای گسترده‌تری در کل زنجیره برق‌رسانی به دنبال داشته باشد،

همان‌طور که در مطالعات امنیت شبکه‌های هوشمند اشاره شده است، چنین تهدیداتی نیازمند توجه به راهکارهای تقویت تاب‌آوری سایبری- فیزیکی، کاهش آسیب‌پذیری‌های مبتنی بر ICT، و بکارگیری استراتژی‌های دفاع پیشرفته در سامانه‌های کنترل توزیع انرژی است.

در نتیجه تاب‌آوری فناورانه زیرساخت برق کشور به معنای تضمین پایداری سیاسی و نظامی ایران است. زیرا برق نه فقط انرژی صنعتی، بلکه محرک دفاع، کنترل پرتابگرهای هوافضا و کارکرد پشتیبانی از مراکز هسته‌ای را نیز تأمین می‌کند.

۷. سیاست‌های ملی و مدیریت کلان دولت‌ها در مواجهه با تهدیدات فناورانه

در سالهای اخیر، کشورهای پیشرو در صنعت، مطالعه بر روی شناسایی تهدیدات تروریستی و امنیت انرژی در حوزه الکتریسته را در دستور کار امنیت ملی خود قرار داده‌اند و بلوک‌های منطقه‌ای، مانند اتحادیه اروپا و یا سازمان‌های بین‌المللی مانند ناتو توجه بی‌سابقه‌ای به مسائل امنیت انرژی الکتریسته کرده‌اند. چه بسا که قطعی برق یک کشور در زمان جنگ می‌تواند اولین اولویت برای هدف قرار دادن امنیت آن کشور در تمام عرصه‌ها باشد و قطعی برق حتی برای یک مدت محدود، ممکن است پیامدهای جبران‌ناپذیری به دنبال داشته باشد. کشورها به این مهم رسیده‌اند که طرح‌های پدافند غیرعامل قبل از انجام مراحل تهاجم و در زمان صلح تهیه و اجرا می‌گردند.

امنیت اطلاعات در دنیای سایبر با افزایش قابل توجه تعداد سطوح حمله، یکی از دلایل اصلی نگرانی در دولت‌هاست (Rastogi et al, 2020). لذا در سطح کلان، کشورها به سوی «حاکمیت فناورانه ترکیبی» (Hybrid Tech Governance) حرکت کرده‌اند؛ یعنی مدیریت یکپارچه امنیت، فناوری و محیط. به طور مثال:

از سال ۲۰۱۷، با اجرای قانون امنیت سایبری و توسعه ساختارهای نهادی و سیاست‌های حکمرانی سایبری در سطح ملی، جمهوری خلق چین به طور نظام‌مند، زیر ساخت‌های حیاتی دیجیتال و سایبری را به عنوان بخش کلیدی امنیت ملی ارتقاء داده است. این تحولات چارچوبی برای تقویت تاب‌آوری سایبری در برابر تهدیدات فنی، داده‌ای و امنیتی فراهم کرده‌اند. اگر چه ادغام رسمی ساختارهای امنیت سایبری با امنیت زیست محیطی در یک نهاد ملی یکپارچه در اسناد رسمی منتشر نشده است. (Wagner, 2017)

بر پایه « Digital Decade Policy Programme 2030 » اتحادیه اروپا توسعه زیر ساخت های دیجیتال، امن و پایدار را به عنوان شرط لازم تحقق اهداف انرژی و محیط زیست در دهه ۲۰۳۰ تعریف کرده است. این برنامه، در چارچوب گذاری موازی دیجیتال و سبز (Twin Transition)، نشان می دهد که امنیت انرژی و حفاظت محیط زیست بدون ظرفیت های دیجیتال ایمن و پایدار نمی تواند محقق شود.

ایران نیز در « سند راهبردی جمهوری اسلامی ایران در فضای مجازی »، بر هم پوشانی مخاطرات محیطی با تهدیدات سایبری تأکید کرده است (شورای عالی فضای مجازی، ۱۴۰۱). لذا حفاظت از داده ها و زیر ساخت های برق کشورها در برابر مخاطرات محیطی، تهدیدات فناوری پایه و همچنین حملات سایبری؛ مستلزم معماری و طراحی امنیتی در سطوح ویژه و خاصی است که به نظر می رسد؛ هدف معماری امنیت، فراهم ساختن چارچوبی است که دولت ها بتوانند بر اساس آن؛ نیازمندی های امنیت را شناسایی و در مورد بهترین راه حل های پیاده سازی امنیت یکپارچه، تصمیم گیری نمایند.

۸. فناوری هوش مصنوعی و مدیریت ریسک های محیطی - امنیتی

هوش مصنوعی در مدیریت بحران ها و ارزیابی تهدیدات، نقش « پیش دستانه » دارد. سیستم های مبتنی بر Machine Learning با تحلیل پیوسته داده های اقلیمی، ترافیک انرژی و تهدیدات شبکه، قادرند مدل های پیش بینی ریسک را به صورت لحظه ای اصلاح کنند. در مقابل، بر اساس طبقه بندی جامع ریسک های هوش مصنوعی، AI می تواند در قالب استفاده های مخرب و حملات الگوریتمی (Adversarial AI) بصورت خودکار، به عاملی برای اختلال و بی ثبات سازی سیستم های پیچیده و زیرساخت های حیاتی تبدیل شود (Slattery et al., 2024).

مطالعات نوین در حوزه امنیت شبکه های هوشمند انرژی نشان می دهند که الگوریتم های یادگیری ماشین، به ویژه شبکه های مولد خصمانه (GAN)، می توانند برای تولید داده های جعلی به گونه ای به کار گرفته شوند که سامانه های پایش و تصمیم یار مبتنی بر هوش مصنوعی در شبکه های برق، وضعیت شبکه را به صورت ناپایدار یا ایمن تشخیص دهند. در این راستا، Efatinasab و همکاران (2024) نشان می دهند که حملات مبتنی بر GAN قادرند سامانه های

پیش بینی پایداری شبکه برق هوشمند را با تزریق داده های سنسوری ساختگی فریب دهند، به گونه ای که مدل های یادگیری ماشین علیرغم ناپایداری واقعی، خروجی های عادی و غیر هشداردهنده تولید می کنند. این یافته ها بیانگر آن است که هوش مصنوعی نه تنها ابزار دفاعی، بلکه بالقوه می تواند به ابزار تهاجمی برای بی ثبات سازی زیر ساخت های حیاتی انرژی تبدیل شود.

مطالعات تکمیلی در سال های ۲۰۲۴ و ۲۰۲۵ نیز با تمرکز بر حملات تزریق داده جعلی (False Data Injection Attacks) مبتنی بر یادگیری عمیق تأکید می کنند که وابستگی فزاینده زیر ساخت های برق به سامانه های هوشمند، سطح جدیدی از آسیب پذیری الگوریتمی ایجاد کرده است که می تواند در آینده نزدیک به حملات واقعی علیه نیروگاه ها و شبکه های انتقال برق منجر شود (Liu et al., 2025). از این منظر، تهدیدات الگوریتمی مبتنی بر هوش مصنوعی باید به عنوان بخشی از امنیت زیر ساختی نسل چهارم و در چارچوب مفهومی تاب آوری فناورانه مورد تحلیل قرار گیرند.

۹. ضرورت تدوین دکترین ملی تاب آوری فناورانه

دکترین ملی تاب آوری فناورانه مستلزم چهار محور بنیادین است:

پایش هوشمند تهدیدات ترکیبی (Hybrid Threats Monitoring)

یکپارچه سازی سیاست های محیطی و امنیتی در سطح شورای عالی امنیت ملی

ایجاد شبکه ملی آزمایشگاه های ارزیابی تهدیدات فناورانه

تربیت نخبگان داده محور در دستگاه های حاکمیتی

چنین دکترینی می تواند پایه ای برای بازتعریف قدرت ملی در عصر فناوری باشد.

۱۰. چارچوب نظری

چارچوب نظری این پژوهش بر پایه مفهوم « تاب آوری فناورانه در زیرساخت های حیاتی ملی » طراحی شده است. در این پژوهش، تاب آوری فناورانه به عنوان توانایی سیستم های ملی پیچیده برای پیش بینی، جذب، انطباق و بازیابی مؤثر از شوک ها و اختلالات دیجیتال، سایبری و فناورانه تعریف می شود. مطالعات اخیر در حوزه زیرساخت های حیاتی نشان می دهند که افزایش سطح پیچیدگی سیستم ها، وابستگی فزاینده به هوش مصنوعی و همگرایی سامانه های سایبری و

فیزیکی، الگوهای جدیدی از ریسک و آسیب‌پذیری را ایجاد کرده‌اند که با رویکردهای سنتی مدیریت بحران به‌طور کامل قابل کنترل نیستند (Islam et al., 2025). از این‌رو، چارچوب‌های نظری معاصر تأکید دارند که تحلیل تاب‌آوری زیرساخت‌های حیاتی باید به‌صورت هم‌زمان ابعاد فناورانه، امنیتی و حکمرانی را در بر گیرد.

بر این اساس، پژوهش حاضر با بهره‌گیری از ادبیات موجود و تلفیق آن با الزامات بومی زیرساخت‌های حیاتی، یک چارچوب مفهومی سه‌بعدی تحت عنوان «مدل سه‌بعدی تاب‌آوری فناورانه ملی» ارائه می‌دهد. فرض بنیادین این مدل آن است که سطح تاب‌آوری ملی حاصل تعامل پویا و وابستگی متقابل میان سه بعد فناورانه، امنیتی و حکمرانی است، به‌گونه‌ای که ضعف در هر یک از این ابعاد می‌تواند کارآمدی سایر ابعاد و در نتیجه تاب‌آوری کل سیستم را کاهش دهد.

بعد فناورانه (Technological Dimension): این بعد شامل سامانه‌های هوشمند داده‌محور و زیرساخت‌های دیجیتال مشتمل بر هوش مصنوعی، اینترنت اشیاء (IoT)، و سیستم‌های پیش‌بینی‌کننده است که عملکرد و خدمات حیاتی را تضمین می‌کنند.

بعد امنیتی (Security Dimension): ابعاد امنیتی به مجموعه‌ای از ظرفیت‌ها اشاره دارد که از پدافند سایبری، دفاع چندلایه، امنیت داده و اطلاعات، و مکانیزم‌های تشخیص تهدیدات ترکیبی (Hybrid Threats) تشکیل می‌شوند (Islam et al., 2025). در این بعد، توان دفاع سایبری، عملیاتی‌سازی سیستم‌های کشف و پاسخ خودکار، و هماهنگی میان سازمان‌ها و نهادهای امنیتی به‌عنوان مؤلفه‌های کلیدی تعریف می‌شوند که تاب‌آوری سیستم‌های ملی را در برابر حملات پیشرفته افزایش می‌دهند.

بعد حکمرانی (Governance Dimension): بعد حکمرانی به نظام سیاست‌گذاری، مدیریت ریسک داده‌محور، و هماهنگی بین‌بخشی اشاره دارد که زمینه اجرای اثربخش راهبردهای تاب‌آوری را فراهم می‌سازد (Marapu, 2025). این بعد همچنین شامل ساز و کارهای پاسخگویی، آموزش و فرهنگ تاب‌آوری سازمانی و هماهنگی بین نهادهای حکمرانی است تا تاب‌آوری به‌صورت سیستمی و نه جزیره‌ای تأمین شود.

در مجموع، مدل سه‌بعدی پیشنهادی نشان می‌دهد که تاب‌آوری فناورانه ملی نه حاصل یک عامل منفرد، بلکه نتیجه تعامل نظام‌مند و هم‌افزای ابعاد فناورانه، امنیتی و حکمرانی است؛

به گونه‌ای که حکمرانی داده‌محور و هماهنگ، شرط لازم برای بهره‌برداری ایمن از ظرفیت‌های فناوریانه و تقویت دفاع سایبری در زیرساخت‌های حیاتی محسوب می‌شود.

۱۰. روش‌شناسی تحقیق

این پژوهش از نوع کاربردی و سیاست‌محور است و از روش ترکیبی (Mixed-Method) استفاده می‌کند تا یافته‌ها از اعتبار بالایی نظری و عملی برخوردار باشند.

الف) روش کیفی: در بخش کیفی از تحلیل محتوای اسناد راهبردی ملی (سند امنیت ملی، سند پدافند غیرعامل، نقشه جامع علمی کشور) و مصاحبه‌ها و هم‌اندیشی‌های خبرگان حوزه‌های امنیتی، انرژی و فناوری استفاده شده است.

ب) روش تحلیل سیاستی: تحلیل سناریو برای ۵ وظیفه بحرانی انجام شده:

حمله سایبری به شبکه برق

اختلال در هوش مصنوعی و کنترل بار

تحریم تجهیزات سخت‌افزاری

فروپاشی داده در مراکز هسته‌ای، نظامی و حیاتی

قطع هم‌زمان برق و ارتباطات

این تحلیل مبتنی بر چارچوب حکمرانی و ریسک استخراج شده از سند راهبردی جمهوری اسلامی ایران در فضای مجازی (شورای عالی فضای مجازی جمهوری اسلامی ایران، ۱۴۰۱) مبتنی بر تجزیه و تحلیل سیاست‌ها و اقدامات کلان، الگوی راهبردی حفاظت سایبری از زیرساخت‌های اطلاعاتی حیاتی و اسناد ملی مربوط به امنیت فضای تولید و تبادل اطلاعات بوده است تا مؤلفه‌های سیاست‌پذیری، داده‌محوری و مدیریت ریسک به صورت سیستماتیک در سناریوها لحاظ گردد.

علاوه بر روش‌های یاد شده؛ از تجربیات حاصل از تحقیقات سایر کشورها و نیز تحقیقات صورت پذیرفته توسط محققان داخلی نیز استفاده شده است.

تحلیل مصداقی مخاطرات محیطی و فناورانه

امروز به سبب درهم تنیدگی فناوری‌های هوشمند، « زیرساخت‌های انرژی و فضای سایبری » به شکل بحران‌های ترکیبی در دنیا درآمده است. ایران نیز به عنوان کشوری با اقلیم متنوع و منابع آب و انرژی حساس، در سال‌های اخیر با افزایش میانگین دما، کاهش بارندگی و بار سنگین خشکسالی مواجه شده است که موجب تشدید تهدیدات زیست محیطی، کمبود منابع آبی و فشار بر شبکه‌های انرژی شده است (Talaie & Rezania, 2024). هم‌زمان، زیرساخت‌های برق و سامانه‌های هوشمند وابسته به فناوری دیجیتال و شبکه‌های ICS/SCADA نیازمند بررسی آسیب‌پذیری و مدل‌های تاب‌آوری در برابر تهدیدات اقلیمی و تکنولوژیک هستند، چرا که خطرات ناشی از تغییرات اقلیمی می‌تواند عملکرد این زیرساخت‌های حیاتی را مختل کند (Karagiannakis et al, 2025).

در این میان، مفهوم تاب‌آوری فناورانه به عنوان بخشی از دکترین امنیت ملی، اهمیت فزاینده‌ای یافته است.

مخاطرات محیطی نوین و وابستگی فناورانه زیرساخت‌ها:

در سال‌های اخیر، تغییرات آب و هوایی و گرم شدن کره زمین منجر به افزایش وقوع حوادث طبیعی شده است. تابستان‌های بسیار گرم و طولانی، زمستان‌های بسیار سرد همراه با یخبندان‌های شدید، سیلاب‌های ناگهانی و خسارت بار، طوفان‌های با سرعت بالا و مخرب، تندبادهای گسترده و فاجعه بار و ... همگی از رخدادهایی هستند که برای همگان آشنا بوده و در اقصای نقاط کره زمین مرتباً در حای وقوع می‌باشند. بسته به موقعیت جغرافیایی یک منطقه، وقوع برخی از این حوادث محتمل‌تر و برخی دیگر بعید است؛ اما، افزایش وقوع آنها بر اساس مستندات موجود، واقعیتی انکارناپذیر است.

در دهه گذشته، زیرساخت‌های حیاتی کشورها، به ویژه شبکه‌های برق، با سرعت بالایی دیجیتالی شده‌اند. بگونه‌ای که مرز میان مخاطرات طبیعی و تهدیدات فناورانه به تدریج کمرنگ شده است. افزایش دمای جهانی و نوسانات اقلیمی موجب تشدید بار مصرفی برق شده و در نتیجه وابستگی شبکه‌های توزیع به سامانه‌های هوشمند پیش‌بینی و تنظیم بار مبتنی بر SCADA، LOT و یادگیری ماشین افزایش یافته است (Kiasari et al, 2024).

در ایران نیز تغییرات اقلیمی، به ویژه در شمال و شرق کشور، فشار مضاعفی بر شبکه های انرژی و آب وارد کرده است. درحالی که توسعه زیرساخت‌های دیجیتال مدیریتی در برخی موارد بدون رعایت کامل استانداردهای امنیتی صورت گرفته است (Talaie & Rezanian, 2024) لذا کشور ما با انواع مخاطرات محیطی و فناورانه روبرو است که در مطالب بعدی به آنها پرداخته خواهد شد.

۱۱. بحران آب و فرونشست زمین

تحقیقات سنجش از دور و داده های میدانی نشان می دهند که کسری شدید منابع آب زیر زمینی در ایران با افزایش نرخ فرونشست زمین هم راستا بوده است. به طور مثال در دشت اصفهان - برخوار، میانگین فرونشست سالانه ۲۵ تا ۴۵ سانتی متر طی دوره ۲۰۱۵-۲۰۲۲ گزارش شده است که با افت قابل توجه سطح آب زیر زمینی همبستگی دارد (Ahmadi Beni et al, 2024). این پدیده نه تنها تهدیدی زیست محیطی بلکه تهدیدی برای زیرساخت‌های فناوری اطلاعات، فیبر نوری به خطوط انتقال برق است.

پژوهش « بررسی میزان آسیب پذیری و تاب آوری شهر اصفهان در برابر پدیده فرونشست زمین » نشان می دهد این پدیده در زمین ناشی از عوامل طبیعی و فعالیت های انسانی در نقاط مختلف دنیا و در طی سالهای اخیر در کشور به خصوص در اصفهان به علت برداشت بی رویه از آبهای زیرزمینی، خشکسالی و عوامل دیگر پدیدار و سبب آسیب های جدی به زمین های کشاورزی، ساختمان های مسکونی، جاده ها و دیگر سازندها و بروز خسارت های زیست محیطی، اقتصادی و اجتماعی شده است (شفيعی و شمسی، ۱۴۰۳: ۲۴) تحلیل آسیب پذیری و تاب آوری شهری ناشی از این فرونشست زمین در اصفهان به عنوان ابزاری در راستای پیشگیری از زایش فاجعه مورد توجه قرار گرفته است.

بحران آب نه تنها یک چالش زیست محیطی و منابع طبیعی است، بلکه به صورت غیرمستقیم، امنیت سایبری زیر ساخت های آب و سیستم های مرتبط را نیز تحت تأثیر قرار می دهد. با افزایش دیجیتال سازی در مدیریت منابع آب و کنترل فرایندهای توزیع و پالایش آب، زیر ساخت های آبی به مجموعه های سایبر- فیزیکی متصل به اینترنت و سیستم های کنترل صنعتی

تبدیل شده اند که بیش از گذشته در معرض حملات سایبری قرار می گیرند. لذا مسائل ناشی از کمبود منابع آب می تواند ریسک های امنیت سایبری را تشدید کند (Tuptuk et al., 2021).

تغییرات اقلیمی و موج های گرمایی:

تحلیل داده های دمای روزانه از ایستگاه های ملی نشان می دهد که فرکانس، شدت و موج های گرمایی در ایران به طور معنا داری افزایش یافته است، به گونه ای که الگوهای دمایی کشور از تغییرات اقلیمی اثر می پذیرند (Babaeian et al., 2025). همچنین داده ها و مدل های آب و هوایی ترکیبی نشان می دهند که بخش های گسترده ای از ایران (مناطق مرکزی و شرقی) با خطرات چندگانه اقلیمی از جمله گرماهای شدید و خشکی مواجه هستند که پیامدهای جدی برای منابع آب، کشاورزی و تولید انرژی دارد (Mousavi et al., 2025).

طوفان های گرد و غبار و تهدید زیرساخت انرژی:

پدیده گرد و غبار در ایران به عنوان یک مخاطره اقلیمی - محیطی برجسته شناخته می شود که منشأ آن علاوه بر بادهای فصلی و خشکسالی، در ترکیب عوامل طبیعی و انسانی مانند بیابان زایی و مدیریت نامناسب منابع خاک و آب نهفته است. تحلیل های سیستماتیک نشان داده اند که این پدیده در مناطق غربی و مرکزی ایران به طور مکرر و گسترده رخ می دهد و باعث افزایش غلظت ذرات معلق در جو، اختلال در فعالیت های کشاورزی، کاهش دید افقی و فشار بر سلامت جامعه می شود که خود می تواند به صورت غیر مستقیم بر زیر ساخت های فناوری و عملکرد تجهیزات حساس نظیر سامانه های حسگری و کنترل صنعتی نیز تأثیرگذار باشد (Abbasnia et al., 2023). به نظر می رسد ترکیب طوفان های گرد و غبار با خطاهای سایبری، بازتابی از بحران های محیطی - فناورانه ترکیبی است که باید در سیاست های ملی مدیریت بحران گنجانده شود.

تهدیدات محیطی ایران به ویژه بحران آب، تغییر اقلیم و گرد و غبار، دیگر صرفاً پدیده های طبیعی نیستند. بلکه به واسطه پیوندشان با سامانه های دیجیتال، بخشی از امنیت ملی فناورانه محسوب می شوند. لذا هرگونه بی توجهی به مدیریت داده های محیطی، مستقیماً می تواند باعث اختلال در زیرساخت های انرژی و حتی بحران های اجتماعی شود.

۱۲. مخاطرات فناورانه در ایران

در دهه اخیر، ساختار فناورانه کشور ایران به طور پیوسته از حالت ابتدایی و نیمه متصل به سمت یکپارچگی فناورانه کامل تر حرکت نموده، به نحوی که بکارگیری فناوری های دیجیتال در بخش دولت هوشمند، داده محوری، اینترنت اشیاء و خدمات الکترونیک، به پوشش گسترده تر اتصال فناوری در سطوح ملی منجر شده است و این روند، به ویژه در ایجاد خدمات یکپارچه دولت و ارتقای حکمرانی دیجیتال مشهود است (Fathi et al., 2025). اما ادغام گسترده فناوری های اطلاعاتی و عملیاتی در شبکه های هوشمند انرژی، از جمله اتصالات میان IoT، سامانه های کنترل صنعتی (ICS) و شبکه های ارتباطی، با افزایش سطح پیچیدگی و وابستگی دیجیتالی، مخاطرات امنیتی جدیدی ایجاد کرده است که می تواند به کاهش تاب آوری ساختاری انرژی منجر شود. آسیب پذیری های موجود در معماری ارتباطات و کنترل هوشمند، به ویژه زمانی که به روز رسانی های امنیتی؛ ناقص یا نامنظم هستند، سطح خطر حملات سایبری را افزایش می دهد. لازم به ذکر است یکی از مهمترین تهدیدات تاب آوری سیستم، اقدامات خرابکارانه و تروریستی است که می توان در دو بخش زیر آنها را دسته بندی نمود:

حملات فیزیکی و حملات سایبری

در صورت عدم توجه به تأمین امنیت شبکه و انجام اقدامات پیشگیرانه در برابر این قبیل حملات، احتمال بروز خطراتی با پیامدهایی به مراتب سنگین تر از حوادث طبیعی وجود دارد. دلیل این امر، عمدی بودن اقدامات خرابکارانه است که با هدفی از پیش تعیین شده، به منظور ایجاد بیشترین خسارت ممکن برنامه ریزی شده اند.

پیشرفت و افزایش نفوذ بستر مخابراتی و اینترنت در صنعت برق، در کنار مزایای بیشماری که دارد، سطح نفوذپذیری شبکه را بالا می برد. افزایش دسترسی ها، شبکه را در برابر حملات سایبری بسیار آسیب پذیر می نماید. از این رو توجه به سیستم های پایش و کنترل و حفاظت ناحیه گسترده و استفاده از پروتکل های امنیتی مناسب، راهکار مناسبی برای افزایش تاب آوری شبکه می باشد. استفاده از سیستم های بیسیم شبکه به منظور شناسایی هویت کارکنان قسمت های مختلف مانند پست یا نیروگاه نیز جزو اقدامات پیشگیرانه قرار می گیرد.

مطالعات اخیر نشان می دهند که با افزایش وابستگی زیر ساخت های صنعتی ایران، به ویژه در بخش های انرژی، نفت و گاز، به سامانه های کنترل صنعتی (ICS) و فناوری های متصل (Ilot)، این سیستم ها در معرض تهدیدات سایبری رو به گسترش قرار گرفته اند. این پژوهش ها ضمن شناسایی بردارهای حمله و ضعف های امنیتی، تأکید می کنند که آسیب پذیری های موجود می تواند منجر به اختلال در عملکرد و کاهش تاب آوری زیر ساخت های حیاتی کشور شود و نیازمند ارتقاء سازو کارهای دفاعی، اطلاعاتی و سیاست گذاری منطقه ای و ملی برای ارتقای مقاومت و تاب آوری سایبری هستند (Taleghani & Jaber eilzadeh Sola, 2025).

مصادیق واقعی عملیات سایبری:

الف) Stuxnet: که در سال ۲۰۱۰ کشف شد، یکی از پیشرفته ترین کرم های سایبری است که به طور خاص برای هدف قرار دادن و آسیب رساندن به سیستم های کنترل صنعتی (PLC/SCADA) طراحی شده بود، و در تحلیل های تاریخی امنیت سایبری به عنوان یکی از نخستین حملات واقعی با اثر مستقیم بر زیر ساخت های فیزیکی شناخته می شود. تمرکز این حمله بر تأسیسات غنی سازی اورانیوم ایران در نطنز در بیش از صد بوده و تحلیل ها نشان می دهند که Stuxnet در بیش از صد هزار سیستم منتشر شده است و بیش از ۶۰ درصد آلوده سازی مربوط به ایران بوده است که اهمیت آن را در زمینه امنیت سایبری و تهدیدات علیه زیر ساخت های حیاتی، برجسته می کند (Stuxnet, 2015). این حمله نشان داد که دشمنان قادرند از مسیر زنجیره تأمین فناوری خارجی، به لایه های فیزیکی نفوذ کنند.

ب) حمله به جایگاه های سوخت ایران: در سال های اخیر، زیرساخت های هوشمند توزیع سوخت ایران بارها هدف حملات سایبری قرار گرفته اند. در ۲۶ اکتبر ۲۰۲۱، حمله سایبری گسترده ای سیستم پرداخت الکترونیکی سوخت را در جایگاه های سراسر کشور مختل کرد و فرایند سوخت گیری با کارت اعتباری را متوقف ساخت و مجبور به استفاده از روش های آفلاین شدند (Iranian fuel cyberattack 2021). همچنین در دسامبر ۲۰۲۳ نیز اختلال وسیعی در شبکه توزیع سوخت رخ داد که بر اساس گزارش های شرکت ملی پخش فرآورده های نفتی ایران و رسانه های معتبر، حدود ۶۰ تا ۷۰ درصد جایگاه های سوخت را از سیستم هوشمند خارج کرد و

نمایانگر آسیب‌پذیری زیر ساخت‌های حیاتی کشور در برابر تهدیدات سایبری است (Associated press, 2023).

ج) حمله به سامانه‌های راه‌آهن (تیرماه ۱۴۰۰): حوادث سایبری ثبت‌شده در حوزه حمل‌ونقل ریلی ایران نشان می‌دهد که سامانه‌های اطلاع‌رسانی و پشتیبان عملیاتی این بخش در برابر حملات سایبری هدفمند آسیب‌پذیر هستند. در جولای ۲۰۲۱ (تیر ۱۴۰۰)، شبکه ریلی ایران با یک حمله سایبری مواجه شد که طی آن تابلوهای اطلاع‌رسانی ایستگاه‌های قطار پیام‌های جعلی درباره تأخیر یا لغو حرکت قطارها را نمایش دادند و اطلاعات نادرست به مسافران ارائه شد. این حادثه، بدون آن‌که به‌طور رسمی به‌عنوان تخریب فیزیکی یا نفوذ به هسته ایمنی سامانه‌های کنترل قطار گزارش شود، اهمیت تفکیک امنیتی، پایش مداوم و تقویت تاب‌آوری سایبری در سامانه‌های OT و ICS حوزه حمل‌ونقل ریلی را برجسته می‌سازد و در ادبیات جدید امنیت زیرساخت‌های حیاتی به‌عنوان یک نمونه واقعی از تهدیدات سایبری با پیامدهای عملیاتی مورد استناد قرار می‌گیرد (Associated Press, 2021).

۱۲. سیاست‌های کلان و خلأهای مدیریتی

الف) نبود هماهنگی نهادی

علاوه بر تعدد بازیگران نهادی در عرصه امنیت سایبری جمهوری اسلامی ایران، پژوهش‌های علمی نشان می‌دهند که فقدان یک ساختار هماهنگ و یکپارچه برای تبادل داده‌ها و هماهنگی میان سازمان‌های مسئول، از جمله شورای عالی فضای مجازی، مرکز ملی فضای مجازی، وزارت ارتباطات، پلیس سایبری، پدافند غیرعامل و دیگر نهادهای امنیتی، منجر به ناکارآمدی در واکنش به حملات سایبری و افزایش پیچیدگی در مدیریت رخدادها شده است (کریمی کلیمانی و همکاران، ۱۴۰۳: ۱۲۸-۱۳۵). اینگونه به نظر می‌رسد نهادهای متعدد و بعضاً موازی در حوزه سایبری فعالیت می‌کنند و نبود یک فرماندهی و راهبرد واحد، منجر به تصمیم‌های ناهماهنگ و واکنشی می‌شود (صفا، ۱۴۰۴).

ب) ضعف در سیاست‌گذاری یکپارچه تاب‌آوری

پژوهش‌های نوین در حوزه تاب‌آوری دیجیتال نشان می‌دهند که در بسیاری از کشورهای پیشرفته؛ سیاست‌های تاب‌آوری فناورانه در سطح ملی و چندسطحی با چارچوب‌های حکمرانی و

هماهنگی بین‌بخشی تدوین و اجرا می‌شود. در حالی که تمرکز تحلیل‌ها درباره کشورهای با منابع محدودتر (از جمله ایران)، بیشتر بر ظرفیت‌های سازمانی و توسعه تدریجی این سیاست‌ها در سطح بنگاه‌ها و نهادهای منفرد است (Collova & Lilyanova, 2024).

ج) عدم اتصال امنیت زیست‌محیطی و فناوریانه

تحلیل سیاستی نشان می‌دهد که تهدیدات اقلیمی - شامل خشکسالی، سیلاب، موج گرما و خطرات محیطی دیگر - به‌طور رسمی تهدیدات جدی امنیت ملی شناخته شده‌اند، اما نقش آنها در سیاست‌های ملی اغلب در کنار تهدیدات فناوری و سایبری قرار نمی‌گیرد و نیازمند ادغام کامل هستند (Council on Strategic Risks, 2025). تاب‌آوری سایبری به‌عنوان یک قابلیت چندبعدی در ادبیات علمی شناخته می‌شود که شامل «توان جذب اختلالات و شوک‌های سایبری»، «قابلیت بازسازی و انطباق پس از حمله»، و «توان تحول ساختاری در بلندمدت» است؛ این ابعاد به‌طور مستقیم با بهبود سطح بلوغ و عملکرد ملی در مواجهه با تهدیدهای سبیرنتیک مرتبط هستند (Araujo et al, 2024).

با توجه به موارد پیش گفته؛ تحلیل‌ها نشان می‌دهد که ایران امروز در قلب «گذر از حاکمیت فیزیکی به حاکمیت داده‌ای» ایستاده است. این گذار، هم فرصت و هم تهدید است. تهدید از آن جهت که اگر داده‌های ملی در زیرساخت‌های آسیب‌پذیر قرار گیرند، حاکمیت از درون تضعیف می‌شود. بحران‌های فناوریانه اخیر (سوخ، راه‌آهن و ...) تنها نمادهایی از نبرد نرم‌افزاری علیه تاب‌آوری ملی هستند. دشمنان به‌جای حمله مستقیم نظامی، زیرساخت داده را هدف گرفته‌اند. زیرا سقوط داده، سقوط قدرت تصمیم‌سازی است. در چنین وضعی هر حمله سایبری نه صرفاً تهدیدی دیجیتال، بلکه تجلی اراده دشمن برای فروپاشی مدیریت ملی از درون است. از همین رو «سیاست تاب‌آوری فناوریانه» باید از سطح فنی به سطح دکترینال ارتقاء یابد.

الگوی پیشنهادی راهبرد ملی تاب‌آوری فناوریانه ایران:

الف) ضرورت تدوین دکترین ملی تاب‌آوری فناوریانه

تحولات فناوری در سال‌های اخیر موجب شکل‌گیری پارادایمی نو در امنیت ملی کشورها شده است. پارادایمی که امنیت را نه صرفاً در مرزهای جغرافیایی، بلکه در مرزهای

راهبردهای سیاستی ارتقاء تاب‌آوری امنیتی زیر ساخت برق ایران در برابر مخاطرات محیطی و حملات فناورانه

داده‌ای زیر ساختی و فناورانه تعریف می‌کند. در چنین شرایطی، تاب‌آوری فناورانه به‌عنوان یکی از مؤلفه‌های قدرت ملی شناخته می‌شود و مستقیماً با تداوم حاکمیت ارتباط دارد. ایران بدلیل ویژگی‌های اقلیمی، ژئوپلیتیکی و فناورانه، بیش از بسیاری از کشورها نیازمند طراحی «دکترین جامع ملی تاب‌آوری فناورانه» است. دکترینی که بتواند از درهم‌تنیدگی تهدیدات اقلیمی، سایبری و زیرساختی عبور کرده و امنیت ملی را در برابر شوک‌های فناورانه پایدار نگه دارد.

(ب) الگوی پیشنهادی تاب‌آوری فناورانه ایران

بر اساس شواهد بین‌المللی از جمله چارچوب سیاستی OECD در امنیت دیجیتال (OECD, 2022) که بر راهبری راهبردی ملی، حفاظت از فعالیت‌ها و زیرساخت‌های حیاتی و توانمندسازی سرمایه انسانی تأکید دارد، و با بهره‌گیری از مفاهیم چارچوب‌های بلوغ و تاب‌آوری در امنیت سایبری، الگوی جامع تاب‌آوری فناورانه ایران می‌تواند حول چهار محور اصلی طراحی شود:

محور اصلی	راهبردها و مسیرها	نوآوری و مزیت عملیاتی
فرماندهی ملی یکپارچه و هدایت راهبردی تاب‌آوری فناورانه	ایجاد «شورای عالی تاب‌آوری فناورانه» ذیل شورای عالی امنیت ملی با حضور نمایندگان وزارت نیرو، دفاع، اطلاعات، ارتباطات و سازمان پدافند غیرعامل	هماهنگی کلان میان نهادهای حیاتی، کاهش زمان تصمیم‌گیری در بحران تا ۳۰٪
	تمرکز شورا بر «هماهنگی راهبردی تبادل اطلاعات فوری و مدیریت رخدادهای چند بعدی»	افزایش سرعت واکنش و هماهنگی عملیاتی بین بخش‌های مختلف
	فرماندهی متمرکز برای افزایش سرعت پاسخ به تهدیدات	افزایش سرعت پاسخ و کاهش خطای تصمیم‌گیری
	تدوین چارچوب تصمیم‌گیری سریع (Rapid Decision Framework)	کاهش زمان واکنش به بحران‌های فناورانه، بهبود کارایی تصمیمات
	ایجاد هم‌افزایی میان نیروهای نظامی، صنعتی و دانشگاهی	تبادل اطلاعات چندجانبه و هم‌افزایی منابع برای تاب‌آوری حداکثری
	توسعه شاخص‌های ملی ارزیابی تاب‌آوری فناورانه	امکان پایش و بهبود مستمر عملکرد تاب‌آوری
	برگزاری مانورهای ملی تاب‌آوری فناوری	شبیه‌سازی تهدیدات واقعی و تقویت آمادگی عملی

تجمیع داده‌ها و تحلیل بلادرنگ تهدیدات	طراحی پلتفرم داده‌های ملی تاب‌آوری	
کاهش خسارت و سرعت واکنش به تهدیدات	کشف، پیش‌بینی و هشدار به موقع نسبت به حملات سایبری و خرابی‌های زیرساختی	ایجاد شبکه ملی و هشدار سریع فناوریانه
پیش‌بینی دقیق تهدیدات و بهبود تصمیم‌گیری	طراحی بر پایه AI-driven Predictive Analysis و تحلیل داده‌های صنعتی و اقلیمی	
ایجاد تجربه عملی و هم‌افزایی دانشگاهی-صنعتی	پیاده‌سازی اولیه از طریق شبکه شتاب‌دهنده‌ها و آزمایشگاه‌ها	
اولویت‌بندی تهدیدات و ارسال هشدار سریع	سیستم هشدار ملی چندلایه‌ای (Multi-tier Alert System)	
تحلیل تهدیدات پیشرفته و جامع	5. ادغام داده‌های فضای سایبری و IoT صنعتی	
دسترسی فوری به وضعیت زیرساخت‌ها و رخدادها	توسعه سامانه پایش بلادرنگ (Real-time Monitoring Dashboard)	
اطمینان از رسیدن هشدارها بدون اختلال	طراحی کانال‌های امن ارتباطی بین نهادهای حیاتی	
بهبود دقت پیش‌بینی و کاهش تهدیدات غیرمنتظره	استفاده از مدل‌های یادگیری ماشینی برای تحلیل و پیش‌بینی حملات	
افزایش مقاومت شبکه‌های حیاتی و کاهش اختلالات	تمرکز بر پایداری زیرساخت‌های برق، گاز، پالایشگاه‌ها و حمل‌ونقل هوشمند	حفاظت از انرژی و زیرساخت‌های راهبردی
کاهش خاموشی‌ها و افزایش پایداری عملیاتی	برطرف نمودن اختلالات برق ناشی از خطاهای نرم‌افزاری	
امکان بازیابی خودکار و تقویت تاب‌آوری	طراحی سامانه‌ای با لایه دوم امنیت (dual security layer)	
تمرکز تخصصی و میان‌رشته‌ای برای حفاظت از انرژی	ایجاد مرکز ملی حفاظت انرژی سایبری	
پیش‌بینی و کاهش اختلالات قبل از وقوع	سامانه پیش‌بینی اختلالات زیرساختی	
تضمین تداوم فعالیت‌ها حتی در شرایط بحران	مکانیزم افزونگی عملیاتی (Operational Redundancy)	
کاهش آسیب‌پذیری سیستم‌های صنعتی	استانداردسازی پروتکل‌های امنیتی OT و SCADA	
بهبود سرعت بازگشت به حالت عملیاتی عادی	مرکز ملی بازیابی اضطراری انرژی و زیرساخت‌ها	

راهبردهای سیاستی ارتقاء تاب‌آوری امنیتی زیر ساخت برق ایران در برابر مخاطرات محیطی و حملات فناورانه

اجرای آزمون‌های تاب‌آوری زیرساختی سالانه	ارتقای آمادگی عملی و کاهش خسارت در بحران
بکارگیری و تربیت نیروی انسانی مقاوم	افزایش تاب‌آوری انسانی و مدیریتی کشور
ارائه آموزش‌های تخصصی در سطح مدیران و کارشناسان	ارتقای مهارت‌های تصمیم‌گیری در بحران
گنجانیدن برنامه‌های رسمی آموزش ملی برای دانش‌آموزان	ایجاد نسل آینده با سواد فناورانه بالا
طراحی مدرک ملی تخصصی تاب‌آوری فناورانه و امنیت سایبری	رسمیت‌بخشی به مهارت‌ها و استانداردسازی
توسعه پلتفرم آموزش آنلاین و شبیه‌سازی تهدیدات	یادگیری عملی و تعاملی برای همه کارکنان
ایجاد برنامه‌های رشد و نگهداشت استعدادهای فناورانه	حفظ و جذب نیروی متخصص در بخش دولتی و خصوصی
برگزاری کارگاه‌ها و مسابقات ملی هک و دفاع سایبری	تقویت مهارت عملی و رقابتی نیروی انسانی
راه‌اندازی مراکز نوآوری فناورانه با تمرکز بر آموزش	ترکیب آموزش و نوآوری برای تاب‌آوری بلندمدت

توسعه سرمایه انسانی و سواد فناورانه ملی

تحقیقات و بررسی‌های میدانی نشان می‌دهد که تاب‌آوری فناورانه در ایران باید بر اساس «مدل شبکه‌ای و هم‌افزا» طراحی شود. یعنی فرماندهی متمرکز در رأس قرار دارد، اما با تبادل داده چندسویه میان زیر نظام‌های عملیاتی. لذا تاب‌آوری فناورانه در ایران باید از سطح پروژه‌های جزئی به سطح دکترین ملی ارتقا یابد.

برابر یافته‌های تحقیق؛ دکترین پیشنهادی بر چهار اصل استوار است:

۱. تمرکز فرماندهی و هدایت راهبردی ملی
 ۲. تحلیل هوشمند مخاطرات و هشدار سریع
 ۳. خودکفایی فناورانه در حفاظت از انرژی و زیر ساخت‌های حیاتی
 ۴. توسعه سرمایه انسانی با سواد فناورانه ملی.
- این الگو اگر با حمایت مستقیم دولت و نهادهای امنیتی پیاده‌سازی شود، می‌تواند ظرف مدت زمانی کمتر از یک دهه، موجب افزایش قابل توجه ضریب پایداری زیرساخت‌های حیاتی

ایران شود. چنین مدلی نه تنها برای مقابله با تهدیدات سایبری بلکه برای مدیریت بحران‌های محیطی (مانند طوفان، گرد و غبار و فرونشست زمین) نیز کارآمد است. به بیان دیگر؛ دکترین تاب آوری فناورانه، حلقه اتصال میان محیط و فناوری است؛ پلی میان طبیعت و داده.

پیشنهادهای سیاستی و راهبردی ویژه برای دولت جمهوری اسلامی ایران در حوزه تاب آوری فناورانه و مدیریت مخاطرات زیرساخت برق کشور

در عصر فناوری‌های نوین و تهدیدات سایبری پیچیده، زیرساخت برق کشور به عنوان محور حیاتی امنیت ملی و انرژی استراتژیک، در معرض مخاطرات متعددی قرار دارد. قطع برق یا نفوذ سایبری به شبکه توزیع می‌تواند پیامدهای دومینویی بر تأسیسات هسته‌ای، نظامی، هواپیمایی، حمل و نقل و صنایع بزرگ کشور ایجاد کند.

با توجه به تحلیل بخش‌های پیشین؛ ضرورت تدوین یک بسته سیاستی و راهبردی ملی که تاب آوری فناورانه و امنیت زیرساخت‌های حیاتی را هم زمان تضمین کند، بیش از پیش روشن می‌شود. ارائه سیاست‌ها و راهبردهایی که بتوانند تاب آوری برق کشور و ارتباط آن با تأسیسات حساس ملی را ارتقاء دهند و یا فناوری‌های نوین، تهدیدات سایبری و محیطی را پیش بینی، مهار و مدیریت کنند.

محور نخست پیشنهادی: باز مهندسی حکمرانی فناورانه و ایجاد شورای عالی تاب آوری زیرساخت‌ها

۱. تشکیل «شورای عالی تاب آوری زیرساخت‌ها» زیر نظر شورای عالی امنیت ملی با عضویت نمایندگان وزارت نیرو، وزارت دفاع، سازمان پدافند غیرعامل، وزارت اطلاعات، سپاه پاسداران انقلاب اسلامی و سازمان انرژی اتمی

۲. ایجاد ساختار فرماندهی واحد و هماهنگی برای پیشگیری و پاسخ به تهدیدات سایبری، محیطی و ترکیبی

۳. تعریف سلسله مراتب تصمیم‌گیری مبتنی بر زمان واقعی با امکان اجرای فوری دستورات اضطراری

۴. استقرار «ستاد واکنش سریع ملی» برای مدیریت رخدادهای فناورانه و زیرساختی.

محور دوم پیشنهادی: سیاست انرژی هوشمند و امنیت سایبری زیرساخت

۱. استاندارد سازی و به‌روزرسانی سامانه‌های SCADA و ICS در تمامی نیروگاه‌ها و شبکه‌های توزیع برق
۲. پیاده‌سازی رمزنگاری مقاوم در برابر حملات کوانتومی در شبکه کنترل توانیر
۳. ایجاد سامانه ملی پیش‌بینی حملات سایبری باهوش مصنوعی و یادگیری ماشین
۴. توسعه شبکه برق مقاوم در برابر حملات EMP، حملات ترکیبی محیطی و سایبری
۵. طراحی و پیاده‌سازی سامانه‌های پشتیبان انرژی در مراکز حیاتی شامل تأسیسات هسته‌ای و نظامی

محور سوم پیشنهادی: حفاظت انرژی و زیرساخت‌های راهبردی

۱. تعیین سطوح حفاظتی انرژی (A تا D) براساس حساسیت و اهمیت مراکز
۲. توسعه سامانه‌های خود ایمن برای نیروگاه‌های حرارتی، آبی، هسته‌ای و خطوط انتقال برق
۳. اتصال حفاظت فیزیکی و سایبری در یک چارچوب یکپارچه
۴. استفاده از فناوری بلاک چین برای حفاظت زنجیره تأمین تجهیزات زیرساخت برق
۵. تدوین برنامه ملی بازیابی سریع و تداوم خدمات در شرایط بحران

محور چهارم پیشنهادی: سرمایه‌گذاری در هوش مصنوعی ملی برای پایش و پیش‌بینی

خطرات

۱. ایجاد مرکز ملی کاهش هوش مصنوعی زیرساخت انرژی با همکاری دانشگاه‌ها و پژوهشگاه‌ها
۲. تحلیل رفتار شبکه برق با یادگیری عمیق و الگوریتم‌های پیش‌بینی عملیات سایبری
۳. توسعه سامانه‌های پیش‌هشدار برای زیرساخت برق نیروگاه‌ها و مراکز حیاتی هسته‌ای و نظامی

۴. تلفیق داده‌های محیطی، انرژی و سایبری برای ایجاد مدل‌های پیش‌بینی مخاطرات ترکیبی

محور پنجم پیشنهادی: سیاست‌های پشتیبان فرهنگی، آموزشی و انسانی

۱. آموزش تخصصی نیروهای مهندسی برق و برق و فناوری اطلاعات در حوزه تاب آوری فناوریانه و امنیت سایبری
۲. اصلاح برنامه‌های درسی دانشگاه‌ها با تمرکز بر تاب آوری و امنیت زیرساخت‌های حیاتی
۳. توسعه دیپلماسی فناوریانه با کشورهای هم‌پیمان (روسیه، چین و هند) برای تبادل دانش و تکنولوژی
۴. ایجاد «مدرسه عالی امنیت انرژی» در وزارت علوم و پژوهشگاه‌ها
۵. ترویج فرهنگ امنیت داده‌ای در سازمان‌های دولتی و صنعتی

جمع‌بندی راهبردی

تاب‌آوری فناوریانه در امنیت زیرساخت‌های حیاتی برق، نه یک مؤلفه فنی محدود، بلکه حلقه راهبردی اتصال میان محیط زیست، انرژی و داده در معماری امنیت ملی قرن بیست‌ویکم محسوب می‌شود. در جهانی که تهدیدات سایبری، شوک‌های اقلیمی، اختلالات زنجیره تأمین و جنگ‌های ترکیبی به‌صورت هم‌زمان و هم‌افزا عمل می‌کنند، زیرساخت برق به‌عنوان «بستر مادر» سایر زیرساخت‌ها، به‌کانون آسیب‌پذیری یا قدرت ملی تبدیل شده است. بر این اساس، اجرای یک بسته سیاستی یکپارچه تاب‌آوری فناوریانه که به‌طور هم‌زمان ابعاد نهادی، فناوریانه و انسانی را پوشش دهد، می‌تواند تا افق ۱۴۱۰ پیامدهای راهبردی زیر را برای کشور به همراه داشته باشد:

۱. **افزایش جهشی ضریب تاب‌آوری ملی:** این بسته، با تقویت ظرفیت جذب شوک، انطباق سریع و تحول ساختاری در زیرساخت‌های حیاتی، قادر است ضریب تاب‌آوری کشور – به‌ویژه در مراکز حساس هسته‌ای، نظامی و راهبردی – را بیش از دو برابر ارتقا دهد و کشور را از وضعیت «واکنش‌محور» به وضعیت «پیش‌دستانه و مقاوم» منتقل کند.

۲. کاهش چشمگیر زمان واکنش به حملات سایبری و ترکیبی: با استقرار سامانه‌های هوشمند بایش، پاسخ خودکار، و فرماندهی یکپارچه سایبری- فیزیکی، زمان تشخیص، تصمیم‌گیری و واکنش به حملات سایبری می‌تواند به کمتر از ۴ ساعت کاهش یابد؛ امری که در معادلات جنگ سایبری، تفاوت میان اختلال موقت و فروپاشی سیستمی را رقم می‌زند.

۳. تضمین امنیت داده و تاب‌آوری زنجیره تأمین زیرساختی: این رویکرد، با بومی‌سازی فناوری‌های کلیدی، تنوع‌بخشی به تأمین‌کنندگان، و ایمن‌سازی داده‌های عملیاتی و راهبردی، امنیت داده‌ها و پایداری زنجیره تأمین تجهیزات حیاتی برق و فناوری‌های وابسته را تضمین می‌کند و وابستگی‌های شکننده را به مزیت‌های راهبردی تبدیل می‌سازد.

در این چارچوب، می‌توان با ضریب اطمینان بسیار بالایی بیان کرد که کلید موفقیت نه در یک ابزار خاص، بلکه در هم‌افزایی چهار مؤلفه بنیادین نهفته است:

- هماهنگی نهادی و حکمرانی یکپارچه
- بهره‌گیری از فناوری‌های پیشرفته و بومی‌پذیر
- حفاظت از انرژی و زیرساخت‌های راهبردی
- سرمایه انسانی تاب‌آور، آموزش‌دیده و یادگیرنده.

اهمیت این بسته سیاستی فراتر از مقابله با تهدیدات سایبری صرف است؛ چرا که همان زیرساخت‌ها و ساز و کارهای تاب‌آور، در مواجهه با بحران‌های محیطی، بلایای طبیعی، خشکسالی، موج‌های گرما و شوک‌های انرژی نیز کارآمد خواهند بود. از این منظر، تاب‌آوری فناورانه نه یک راه‌حل بخشی، بلکه سنگ‌بنای شکل‌گیری «دکترین ملی فناورانه و تاب‌آور» است؛ دکترینی که امنیت، توسعه پایدار و اقتدار ملی را در یک چارچوب منسجم و آینده‌نگر به هم پیوند می‌زند.

منابع:

۱. آقابیکگی، س. (۱۴۰۴)، "ایران کشوری با حوادث بالا/ وقوع ۱۵۰ زلزله در هفته"، سایت خبرگزاری جمهوری اسلامی ایران، شماره خبر: ۸۶۰۰۱۱۳۷ <https://irna.ir/xjVZTg>
۲. آیت الله خامنه ای، س.ع. (۱۴۰۳) "بیانات در نخستین دیدار هیئت دولت چهاردهم"، پایگاه اطلاع رسانی دفتر حفظ و نشر آثار حضرت آیت الله العظمی خامنه ای، <https://www.khammenei.ir>
۳. برق نیوز، (۱۳۹۹) "حمله سایبری به شبکه برق"، <https://barghnews.c۸۹۹۷۸۴۴۹>
۴. پالیزوان، م. دشتی، رضا. (۱۳۹۶) "مقاوم سازی زیر ساخت های شبکه برق با استفاده از روش های پدافند غیر عامل"، فصلنامه علمی-ترویجی پدافند غیرعامل، سال ۹، شماره ۴، صص ۵۷-۶۷
۵. پور ابراهیمی، ع. حمید زاده، م. طلوعی اشلقی، عباس. معتدل، م. (۱۴۰۳) "مفهوم سازی امنیت با رویکرد پایداری و تاب آوری سازمان"، تحقیقات کتابداری و اطلاع رسانی دانشگاهی، ۵۸ (۲)، ۸۷-۱۰۴ <http://doi.org/10.22059/jilib.2024.378155.1745>
۶. رجبی مشهدی، م. (۱۴۰۴) "خسارت ۲۰۰۰ میلیارد تومانی حملات اخیر رژیم صهیونیستی به تأسیسات صنعت برق"، سایت خبرگزاری توانیر، شماره خبر: ۱۳۲۷۸۶، News.tavanir.org.ir/x38jW
۷. رضایی، ش. بهزاد فر، م. ترکمن، م. (۱۴۰۴) "بررسی تحولات پژوهش های جهانی تاب آوری شهری و هم پیوندی آن با انرژی های تجدید پذیر و تغییر اقلیم: یک مطالعه علم سنجی (۲۰۰۰-۲۰۲۵)"، نشریه علمی پژوهشی اقتصادی و برنامه ریزی شهری، دوره ۷، شماره ۳، خرداد ۱۴۰۵
۸. شفیعی دارافشانی، ع و شمسی اژی، ع. (۱۴۰۳) "بررسی میزان آسیب پذیری و تاب آوری شهر اصفهان در برابر پدیده فرونشست زمین"، منظر، سال ۱۶ شماره ۶۹، ۳۷-۲۴.
۹. شورای عالی فضای مجازی جمهوری اسلامی ایران (۱۴۰۱)، سند راهبردی جمهوری اسلامی ایران در فضای مجازی (افق ۱۴۱۰)

۱۰. صادقی، ز. نجاتی، م. سنایی، س. (۱۴۰۲) "بررسی تاب‌آوری انرژی ایران و همسایگان منتخب: الگوی برنامه ریزی خطی داده ستانده چند منطقه ای"، اقتصاد و الگو سازی، سال ۱۴، شماره یک، صص ۱۸۶-۱۶۳.
۱۱. صفا، م. (۱۴۰۴) "حکمرانی سایبری در ایران- چالش‌ها و راهکارها"، سیویلیکا
۱۲. کریمی کلیمانی، م. محمودزاده، ا. تقی‌پور، ر. بوشهری، ع. (۱۴۰۳) "الگوی حکمرانی صنعت امنیت سایبری جمهوری اسلامی ایران"، فصلنامه نگرش مدیریت راهبردی، سال ۲، شماره ۳. صص ۱۵۲-۱۲۷
۱۳. کسرای نژاد، م. طائی، ح. حیدری، ک. (۱۳۹۴) "مطالعه فنی، اقتصادی و زیست محیطی ساخت نیروگاه تولید هم زمان برق، حرارت و برودت (CCHP)"، دانشگاه علامه طباطبائی، دانشکده علوم اقتصادی، پایان نامه کارشناسی ارشد
۱۴. مقدسی، م. (۱۴۰۴) "تاب‌آوری زیر ساخت چیست؟" پایگاه خبری روانشناسی و بهداشت روان (میگنا)، کد مطلب: ۶۷۶۶۴
۱۵. نجاری، ر. آذر، ع. جلیلیان، ح. (۱۳۹۴) "ارائه مدل هوشمندی سازمان: مورد مطالعه شرکت‌های تولیدی". مطالعات رفتار سازمانی، سال چهارم، شماره یک، ۲۴-۱
۱۶. نجفی روادانق، س. کریمی، م. حق‌فام، م. (۱۳۹۸) "چارچوب طراحی شبکه‌های توزیع تاب‌آور در برابر حوادث طبیعی"، مجله انجمن مهندسی برق و الکترونیک ایران، دوره ۱۸، شماره ۲، تابستان ۱۴۰۰، صص ۱۲۹-۱۱۹
۱۷. نصر اصفهانی، ع. لسان طوسی، ف. نجفی رستاقی، ح. برومند کاخکی، ا. (۱۴۰۳) "مقدمه ای بر ایران تاب‌آور"، مرکز پژوهش‌های مجلس شورای اسلامی، شماره مسلسل: ۲۰۱۷۶، کد موضوعی: ۳۵۰
۱۸. نو روستا، ح. رادان، ی. نکوئی، ع. اسکندری، م. (۱۴۰۱) "شناسایی و اولویت بندی تهدیدات نیروگاه‌های برق حرارتی و ارائه راهکارهای پدافند غیرعامل"، دو فصلنامه علمی پژوهشی مدیریت بحران، ویژه نامه پدافند، صص ۱۲-۱

[۱۹] Abbasnia, A., Boloori Arabani, A., Javan, M., & Zare, S. (2023). Assessment of Rural Vulnerability to Sand and Dust Storms in Iran. Atmosphere, 14(2), Article 281.

[۲۰] Ahmadi Beni, F., Entezari, M., Sadeghi, A., & Salehi, A. (2024). Quantifying land subsidence and its nexus with groundwater depletion in Isfahan-Borkhar plain: An integrated approach using radar interferometry and spatial bivariate relationships. *Remote Sensing Applications: Society and Environment*. <https://doi.org/10.1016/j.rsase.2024.101248>

[۲۱] Araujo, M. S. d., Machado, B. A. S., & Passos, F. U. (2024). Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance. *Applied Sciences*, 14(5), 2116. <https://doi.org/10.3390/app14052116>

[۲۲] Associated Press. (2021, July 10). Hackers disrupt Iran's rail service with fake delay messages. <https://apnews.com/article/middle-east-technology-iran-a1690f768777b25bc8a8fe6d94bf8669>

[۲۳] Babaeian, I., Khazanedari, L., Kouzegaran, S., & Malbusi, S. (2025). Observed heat wave assessment over Iran and its future projections through 2200 under SSP scenarios Reserch Institute for Meteorology and Atmospheric Science.

[۲۴] Collovà, C., & Lilyanova, V. (2024). Digital public services in the National Recovery and Resilience Plans. *European Parliamentary Research Service*

[۲۵] Council on Strategic Risks. (2025, January 13). Climate Security Policy Recommendations for the New Administration. Retrieved from <https://councilonstrategicrisks.org/2025/01/13/climate-security-policy-recommendations-for-the-new-administration>

[۲۶] Digital Decade - Policy Programme 2030. Commission Europea.eu Efatinasab, E., Brighente, A., Rampazzo, M., Azadi, N., & Conti, M. (2024). GAN-GRID: A novel generative attack on smart grid stability prediction. *arXiv preprint arXiv: 2405. 12076*.

[۲۷] Fathi, B., Rahimi, G., & Nejhad Haji Ali Irani, F. (2025). Quantitative analysis of factors affecting the realization of smart government in Iran with emphasis on the dimensions of digital governance. *Digital Transformation and Administration Innovation*, 3(1). 1-11.

[۲۸] Iranian fuel cyberattack. (2021). In Wikipedia. Retrieved [date], from https://en.Wikipedia.org/wiki/2021_Iranian_fuel_cyberattack.

[۲۹] Islam, S., Basheer, N., Papastergiou, S., Ciampi, M., & Silvestri, S. (2025). Intelligent dynamic cybersecurity risk management framework with explainability and

[۳۰] Jasiūnas, J., Lund, P. D., & Mikkola, J. (2021). Energy system resilience—A review. *Renewable and Sustainable Energy Reviews*, 150, 111476.

- [۳۱] Karagiannakis, G., Panteli, M., & Argyroudis, S. (2025). Fragility modeling of power grid infrastructure for addressing climate change risks and adaptation. arXiv:2504.20056. <https://arxiv.org/abs/2504.20056>.
- [۳۲] Kiasari, M., Ghaffari, M., & Aly, H. H. (2024). A comprehensive review of the current status of smart grid technologies for renewable energies integration and future trends: The role of machine learning and energy storage systems. *Energies*, 17(16), 4128. <https://doi.org/10.3390/en17164128>.
- [۳۳] Liu, Z., Liu, M., Wang, Q., & Tang, Y. (2025). GAN-based false data injection attacks against smart grid monitoring systems. *Engineering*
- [۳۴] Marapu, N. R. (2025). Building resilient national infrastructure: AI and NIST frameworks for smart cities and utilities. *International Journal of Emerging Research in Engineering and Technology*, V5I3P107. <https://doi.org/10.63282/3050-922X.IJERET-V5I3P107>
- [۳۵] Mousavi, S. F., et al. (2025). Near-term climate extremes in Iran based on compound hazards. *Scientific Reports*.
- [۳۶] OECD. (2022). OECD policy framework on digital security: Cybersecurity for prosperity (OECD Publishing). <https://doi.org/10.1787/a69df866-en>
- [۳۷] Rastogi, N., Dutta, S., J. Zaki, M., Gittens, A., & Aggarwal, C. (2020). MALOnt: An ontology for malware threat intelligence. arXiv:2006.11446v1 [cs.CR]. Association for Computing Machinery. <https://doi.org/10.48550/arXiv.2006.11446>.
- [۳۸] Siddiqui, F., Hagan, M., & Sezar, S. (2020). Establishing cyber resilience in embedded systems for securing next-generation critical infrastructure. 32nd IEEE International Systems-on-Chip Conference (SOCC). <http://doi.org/10.48850/arXiv.2004.02770>
- [۴۰] Slattery, P., et al. (2024). The AI Risk Repository: A comprehensive taxonomy of risks from artificial intelligence. arXiv:2408. 12622.
- [۴۱] Spaans, M & Waterhout, B (2017). Building up resilience in cities worldwide – Rotterdam as participant in the 100 Resilient cities Programm Citese, 61, 109-116. <https://doi.org/10.1016/j.cities.2016.05.011>
- [۴۲] Stuxnet(Second Edition). (2015). Science Direct
- [۴۳] Talaie, A., & Rezaei, S. (2024). Climate Change in Iran: Challenges and Solutions – A Short Communication. *Journal of Environmental Treatment Techniques*, 12(4), 19-29.

[۴۴] Taleghani, M., & Jaber eilzadeh Sola, M. R.(2025). Assessing cybersecurity Threates in sensitive industrial systems of Iran. Reserch gate. <https://zenodo.org/records/16795806> (open access)

[۴۵]

[۴۵] Tuptuk, N., Hazell, P., Watson, J., & Hailes, S. (2021). A systematic review of the state of cyber-security in water systems. *Water*, 13(1), 81. <https://doi.org/10.3390/w13010081>

[۴۶] Wagner, J. (2017). China's Cybersecuti Law: What You Need to Know. The diplomat.com.

[۴۷] Wang, L.- J., Guo, M., Sawada, K., Lin, J. (2015). Landslide susceptibility mapping in Mizunami City, Japan: A comparison between logistic regression, bivariate statistical analysis and multivariate

[۴۸] Yang, Z., Barroca, B., Mebarki, A., Laffrechine, K., Dolidon, H., & Lilas, L (2024). Critical infrastructure resilience : a guide for building indicatore systems based on a multi-criteria framework with a focus on implementable actions. *Natural Hazarda and Earth System Science*, 24, 3723-3753.

[۴۹] Zibaeirad, A., Koleini, F., Bi, S., Hou, T., & Wang, T. (2024). A comprehensive survey on the security of smart grid: Challenges, mitigations, and future research opportunities. *arXiv*. <https://arxiv.org/abs/2407.07966>

