Scientific journal of Intelligence Horizons

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

Mohammad Babaei[1], Seyed Ali Mosazadeh[2], Ebrahim Safari[3]

۲
۲Year
Autumn 1404
Research paper
:Date received
۱٤۰٤/۰٥/۰۱
:Date accepted
۱٤۰٤/۰٥/۲۹
Pages: 169-19۰

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

۱. PhD in National Security Threats, Imam Hadi (AS) Faculty, Imam Hussein (AS) University,

۲. Corresponding author: PhD in Political Geography, Imam Hadi (AS) Faculty, Imam Hussein (AS) Comprehensive University,

۳. PhD in English Language Teaching, Imam Hadi (AS) Faculty, Imam Hussein (AS) University,

نشریه علمی آفاق اطلاعات

استراتیجیات سیاسیۀ لتعزیز قدرۀ البنیۀ التحتیۀ للکهرباء فی إیران علی الصمود فی وجه المخاطر البیئیۀ والهجمات التکنولوجیۀ

محمد بابائی[1] سید علی موسی‌زاده[2] ابراهیم سفری[3]

۷
السنۀ الثانیه
الخریف ۱٤۰٤
ورقۀ بحثیۀ
تاریخ الاستلام:
۱٤۰٤/۰۵/۰۱
تاریخ القبول:
۱٤۰٤/۰۵/۲۹
الصفحات: ۱۶۹-۱۹۰

ملخص

فی عصر التحول الرقمی والثورۀ الصناعیۀ الرابعۀ، باتت الحدود بین الأمن المادی والأمن السیبرانی غیر واضحۀ، وأصبحت التهدیدات التکنولوجیۀ أحد أبرز التحدیات التی تواجه الأمن القومی. وترتبط الأنظمۀ البیئیۀ والبنی التحتیۀ التکنولوجیۀ ارتباطًا وثیقًا، وقد جعلت المخاطر البیئیۀ والرقمیۀ مجتمعۀً شبکات الطاقۀ فی الدول أهدافًا استراتیجیۀ للهجمات السیبرانیۀ والتدمیریۀ. یحلل هذا البحث، من منظور استراتیجی شامل، مع التركیز بشکل خاص علی البنیۀ التحتیۀ للطاقۀ باعتبارها الرکیزۀ الأساسیۀ للاستدامۀ الاجتماعیۀ والاقتصادیۀ والدفاعیۀ للبلاد، سیاسۀ المخاطر التکنولوجیۀ، ویقدم نموذجًا وطنیًا للمرونۀ التکنولوجیۀ فی إیران. یشمل إطار التحلیل ثلاثۀ محاور أساسیۀ: تطور مفهوم أمن البنیۀ التحتیۀ فی ضوء التقنیات الحدیثۀ، وتحدید الثغرات فی الحوکمۀ التکنولوجیۀ، وتصمیم نموذج استراتیجی لإعادۀ هندسۀ سیاسۀ الطاقۀ وحمایۀ البنیۀ التحتیۀ للکهرباء. وتُظهر النتائج أن المرونۀ التکنولوجیۀ لیست مجرد نتاج للتطور التقنی، بل هی نتیجۀ مُجتمعۀ للسیاسات والتکنولوجیا وإدارۀ الموارد البشریۀ، وللتغلب علی التهدیدات المُجتمعۀ، تحتاج إیران إلی ترسیخ سیادتها التکنولوجیۀ الوطنیۀ. وبناءً علی هذا التحلیل، تستند العقیدۀ الوطنیۀ الإیرانیۀ للمرونۀ التکنولوجیۀ إلی أربعۀ مبادئ أساسیۀ:

یرکز هذا الإطار علی القیادۀ والتوجیه الاستراتیجیین الوطنیین، والتحلیل الذکی للمخاطر والإنذار المبکر، وحمایۀ الطاقۀ والبنیۀ التحتیۀ الحیویۀ، وتنمیۀ رأس المال البشری والمعرفۀ التکنولوجیۀ الوطنیۀ. ویمکن أن یشکل هذا الإطار أساسًا لتصمیم سیاسات واستراتیجیات وطنیۀ لتعزیز مرونۀ البنیۀ التحتیۀ والأمن القومی .

الکلمات المفتاحیۀ: المرونۀ الوطنیۀ، المخاطر البیئیۀ، الأمن القومی، البنیۀ التحتیۀ للکهرباء، الذکاء الاصطناعی، السیاسۀ التکنولوجیۀ

---

۱ . حاصل علی درجۀ الدکتوراه فی التهدیدات الأمنیۀ الوطنیۀ، کلیۀ الإمام الهادی (علیه السلام)، جامعۀ الإمام الحسین (علیه السلام).

۲ . المؤلف المسؤول عن المراسلات: حاصل علی درجۀ الدکتوراه فی الجغرافیا السیاسیۀ، کلیۀ الإمام الهادی (علیه السلام)، جامعۀ الإمام الحسین (علیه السلام) الشاملۀ.

۳ . حاصل علی درجۀ الدکتوراه فی تدریس اللغۀ الإنجلیزیۀ، کلیۀ الإمام الهادی (علیه السلام)، جامعۀ الإمام الحسین (علیه السلام).

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

محمدبابایی[1] سیدعلی موسی زاده[2] ابراهیم صفری[3]

چکیده

در عصر تحول دیجیتال و انقلاب صنعتی چهارم، مرز میان امنیت فیزیکی و سایبری مبهم شده و تهدیدات فناورانه به یکی از اصلی‌ترین چالش‌های امنیت ملی تبدیل شده‌اند. سیستم‌های زیست‌محیطی و زیرساخت‌های فناورانه به‌شدت به یکدیگر وابسته هستند و مخاطرات ترکیبی محیطی و دیجیتال، 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 فناورانه و ارائه الگوی ملی تاب‌آوری فناورانه در ایران می‌پردازد. چارچوب تحلیل شامل سه محور بنیادین است: تحول مفهوم امنیت زیرساختی در پرتو فناوری‌های نوین، بازشناسی خلأهای حکمرانی فناورانه و طراحی الگویی راهبردی برای بازمهندسی سیاست انرژی و حفاظت از زیرساخت برق. یافته‌ها نشان می‌دهد تاب‌آوری فناورانه 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 فناورانه ملی است. بر اساس این تحلیل، دکترین ملی تاب‌آوری فناورانه 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 فناورانه ملی. این چارچوب می‌تواند مبنای طراحی سیاست‌ها و استراتژی‌های ملی برای افزایش تاب‌آوری زیرساخت‌ها و امنیت کشور باشد.

۲۸
سال چهاردهم
پاییز و زمستان ۱۴۰۴
مقاله پژوهشی
تاریخ دریافت:
۱۴۰۴/۰۶/۰۳
تاریخ پذیرش:
۱۴۰۴/۰۶/۲۵
صص: ۴۱۰-۳۸۷

۱. دکتری تهدیدات امنیت ملی، دانشکده امام هادی(ع)، دانشگاه جامع امام حسین(ع)،
(dr.mohammadbabaei.1970@gmail.com)
۲. نویسنده مسئول: دکتری جغرافیای سیاسی، دانشکده امام هادی(ع)، دانشگاه جامع امام حسین(ع)،
(seyyedali3023@gmail.com)
۳. دکتری آموزش زبان انگلیسی، دانشکده امام هادی(ع)، دانشگاه جامع امام حسین(ع)،
(safariibrahim1@gmail.com)

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

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 تاب آوری 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 تاب آوری 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 سامانه سنجش از راه دور دشمن، تهدیدات ناشی از تهاجم هوایی، حملات سایبری هدفمند، تهدیدات ناشی از اقدامات تروریستی (بمب های گرافیتی و ...)، اختلال در سامانه‌های صنعتی ناشی از بکارگیری سلاح های الکترومغناطیس و تهدیدات هوش مصنوعی ظهور یافته‌اند که نمونه هایی از حملات تروریستی به شبکه های 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 شلیک های 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.
عراق	ابتدای شروع حملات نیروهای داعش در سال ۲۰۱۴	حمله تروریست ها به سه دکل در دو خط انتقال برق پرقدرت 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 منطقهKurbini	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 سامانه‌های 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. درعین‌حال مخاطرات محیطی مانند سیل، زلزله و خشکسالی نیز ساختار شبکه برق را تهدید می‌کند.

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 سیاست‌گذاری قرار نگرفته است (نصر اصفهانی و همکاران، ۱۴۰۳). این خلأ باعث شده‌است 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 کسرایی 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 ویژگی های 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 شبکه های 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 شبکه های 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.

نو روستا 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 غیرعامل پرداخته است.

یزدانیه (۲۰۲۳) در مقاله « تجزیه و تحلیل و برنامه ر یزی 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 جمع‌بندی 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 بومی‌سازی 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 « تـاب آوری » برای اولین بار توسـط هولینـگ (Holling, 1973) در علم اکولوژی برای تبیین مفهوم توانایی یک سیسـتم برای جذب شـوک ها، تغییرات و اختلالات در حالی که عملکرد سیسـتم باقی بماند، تعریف گردید. (Wang et al, 2015)

Spaans & Waterh out(2017) تاب آوری را در توانایی افراد، جوامع، مؤسسات، شرکت ها و سیستم ها در یک شهر برای زنده ماندن، سازگاری و رشد بدون درنظرگرفتن 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 پررقابت 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 تصمیم‌سازی سریع و داده محور

مفهوم تاب آوری فناورانه

تاب آوری فناورانه (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 شوک های حاد اعم از تهدیدات فناورانه، حملات سایبری، اختلالات داده‌ای یا فروپاشی شبکه‌های هوشمند که در معرض آن قرار دارند، اشاره دارد.

از دیدگاه نظریه‌پردازان حوزه امنیت، تاب آوری فناورانه بخشی از « امنیت زیرساختی نسل بعدی یا نسل چهارم » است که نه‌تنها شامل تجهیزات فیزیکی، بلکه داده‌ها، الگوریتم ها و شبکه‌های یادگیرنده نیز می‌شود (Siddiqui et al. 2020). در این چارچوب، تاب آوری فناورانه به معنای بازسازی سریع ظرفیت ملی در برابر اختلال فناورانه 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 نمی شود. این فناوری لایه های عمیقی دارد که باید بر آن لایه ها مسلط شد.

آن لایه ها دست دیگران است. اگر شما نتوانید لایه های عمیق و متنوع این فناوری را هوش مصنوعی را تأمین کنید، فردا اینها یک ایستگاهی مثل آژانس اتمی درست می کنند برای هوش مصنوعی،... که اگر چنانچه به آن ایستگاه رسیدید، باید اجازه بگیریدکه در فلان بخش از هوش مصنوعی استفاده کنید، در فلان بخش دیگر حق ندارید استفاده کنید! »(آیت الله خامنه ای ، ۱۴۰۳) که این دقیقاً همان مفهوم استقلال فناورانه و عدم وابستگی اراده ای است که در ادبیات امنیت فناوری مطرح می شود. بر این مبنا، تاب آوری فناورانه در ایران مفهومی فراتر از پایداری صنعتی است، بلکه ابزار صیانت از استقلال ملی در برابر وابستگی فناورانه جهانی است.

۴. رابطه تاب آوری فناورانه با امنیت ملی

« امنیت » از نظر مفهومی به وضعیتی اطلاق می شود که نیروهای حفظ کننده 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 دولت ها و جوامع؛ مجموعه ای از ابزارها و سیستم ها (نظیر هوش مصنوعی) و استراتژی ها را بکار می گیرند تا بدون از دست دادن داده ها یا تأخیرهای عملیاتی در برابر اختلالات و مخاطراتی همچون بلایای طبیعی، حملات سایبری و سایر بحران ها، توانایی تاب آوری خود را افزایش دهند که به تعبیری می توان آن را تاب آوری فناورانه نامید(مقدسی، ۱۴۰۴). دراین‌میان، زیرساخت برق کشور به عنوان ستون فقرات امنیت انرژی، یکی از حساس‌ترین و حیاتی‌ترین مؤلفه‌های امنیت ملی محسوب می‌شود. برخی از پژوهشگران و اندیشه ورزان 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 حوزه های نظامی، هسته ای و ...، با تهدید فروپاشی زنجیره‌ای روبرو می شوند. 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 می کنند: از یک‌سو با فراهم‌سازی ابزارهای پیش‌بینی، داده کاوی 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 تهدید پذیری راهبردی را افزایش می‌دهند. به‌ویژه فناوری‌هایی مانند هوش مصنوعی، اینترنت اشیاء (lot) و کلان داده‌ها (Big Data) در عین ایجاد تحول در مدیریت منابع و بحران‌ها، بستر نفوذپذیری سایبری و بی‌ثباتی زیست‌محیطی را گسترش داده اند.

از نمونه های 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(برق نیوز، 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 ساخت های 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 شبکه های توزیع برق در برابر تهدیدات تروریستی، تاب آوری زیرساخت برق تابع عوامل زیر است:

شناخت آسیب ها و تهدیدات

کاهش آسیب پذیری

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 تاب‌آوری و قابل اعتماد بودن الگوریتم‌های MLدر 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 برICT، و بکارگیری استراتژی‌های دفاع پیشرفته در سامانه‌های کنترل توزیع انرژی است.

درنتیجه تاب آوری فناورانه زیرساخت برق کشور به معنای تضمین پایداری سیاسی و نظامی ایران است. زیرا برق نه‌فقط انرژی صنعتی، بلکه محرک دفاع، کنترل پرتابگرهای هوافضا و کارکرد پشتیبانی از مراکز هسته‌ای را نیز تأمین می‌کند.

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

در سالهای اخیر، کشورهای پیشرو در صنعت، مطالعه بر روی شناسایی تهدیدات تروریستی و امنیت انرژی در حوزه الکتریسیته را در دستورکار امنیت ملی خود قرار داده اند و بلوک های منطقه ای، مانند اتحادیه اروپا و یا سازمان های بین المللی مانند ناتو توجه بی سابقه ای به مسائل امنیت انرژی الکتریسیته کرده اند. چه بسا که قطعی برق یک کشور در زمان جنگ می تواند اولین اولویت برای هدف قرار دادن امنیت آن کشور در تمام عرصه ها باشد و قطعی برق حتی برای یک مدت محدود، ممکن است پیامدهای جبران ناپذیری به دنبال داشته

باشد. کشورها به این مهم رسیده اند که طرح های پدافند غیرعامل قبل از انجام مراحل تهاجم و در زمان صلح تهیه و اجرا می گـردنـد.

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

از سال ۲۰۱۷ ، با اجرای قانون امنیت سایبری و توسعه ساختارهای نهادی و سیاست های حکمرانی سایبری در سطح ملی، جمهوری خلق چین به طور نظام مند، زیر ساخت های حیاتی دیجیتال و سایبری را به عنوان بخش کلیدی امنیت ملی ارتقاء داده است. این تحولات چارچوبی برای تقویت تاب آوری سایبری در برابر تهدیدات فنی، داده ای و امنیتی فراهم کرده اند. 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 هم‌پوشانی 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 فناورپایه 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 نماید.

۸. فناوری هوش مصنوعی و مدیریت ریسک‌های محیطی- امنیتی

هوش مصنوعی در مدیریت بحران‌ها و ارزیابی تهدیدات، نقش « پیش‌دستانه » دارد. سیستم‌های مبتنی بر Machine Learning با تحلیل پیوسته داده‌های اقلیمی، ترافیک انرژی و تهدیدات شبکه، قادرند مدل‌های پیش‌بینی ریسک را به‌صورت لحظه‌ای 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 زیرساخت‌های حیاتی تبدیل شود (Slattery et al., ۲۰۲۴).

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 (۲۰۲۴) 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)

یکپارچه‌سازی سیاست‌های محیطی و امنیتی در سطح شورای عالی امنیت ملی

ایجاد شبکه ملی آزمایشگاه‌های ارزیابی تهدیدات فناورانه

تربیت نخبگان داده محور در دستگاه‌های حاکمیتی

چنین دکترینی می‌تواند پایه‌ای برای بازتعریف قدرت ملی در عصر فناوری باشد.

۱۰ . چارچوب نظری

چارچوب نظری این پژوهش بر پایه مفهوم « تاب‌آوری فناورانه در زیرساخت‌های حیاتی ملی » طراحی شده است. در این پژوهش، تاب‌آوری فناورانه به‌عنوان توانایی سیستم‌های ملی پیچیده برای پیش‌بینی، جذب، انطباق و بازیابی مؤثر از شوک‌ها و اختلالات دیجیتال، سایبری و فناورانه تعریف می‌شود. مطالعات اخیر در حوزه زیرساخت‌های حیاتی نشان می‌دهند که افزایش سطح پیچیدگی سیستم‌ها، وابستگی فزاینده به هوش مصنوعی و همگرایی سامانه‌های 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 وکارهای 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؛ به‌گونه‌ای که حکمرانی داده‌محور و هماهنگ، شرط لازم برای بهره‌برداری ایمن از ظرفیت‌های فناورانه و تقویت دفاع سایبری در زیرساخت‌های حیاتی محسوب می‌شود .

۱۰. روش‌شناسی تحقیق

این پژوهش از نوع کاربردی و سیاست محور است و از روش ترکیبی (Mixed-Method) استفاده می‌کند تا یافته‌ها از اعتبار بالای 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 مصاحبه ها و هم اندیشی های خبرگان حوزه‌های امنیتی، انرژی و فناوری استفاده شده است.

ب) روش تحلیل سیاستی: تحلیل سناریو برای ۵ وظیفه بحرانی انجام‌شده:

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 سیاست ها و اقدامات کلان، الگوی راهبردی حفاظت سایبری از زیر ساخت های اطلاعاتی حیاتی و اسناد ملی مربوط به امنیت فضای تولید و تبادل اطلاعات بوده است تا مؤلفه های سیاست پذیری، داده محوری و مدیریت ریسک به صورت سیستماتیک در سناریوها لحاظ گردد.

علاوه بر روش های 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 درهم‌تنیدگی 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 سال های 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 شبکه های انرژی شده است (Talaie & Rezania, 2024). هم زمان، زیرساخت‌های برق و سامانه های هوشمند وابسته به فناوری دیجیتال و شبکه های ICS/SCADA نیازمند بررسی آسیب پذیری و مدل های تاب آوری در برابر تهدیدات اقلیمی و تکنولوژیک هستند، چرا که خطرات ناشی از تغییرات اقلیمی می تواند عملکرد این زیر ساخت های حیاتی را مختل کند(Karagiannakis et al, 2025)

دراین‌میان، مفهوم تاب آوری فناورانه به‌عنوان بخشی از دکترین امنیت ملی، اهمیت فزاینده‌ای یافته است.

مخاطرات محیطی نوین و وابستگی فناورانه زیرساخت‌ها:

در سال های اخیر، تغییرات آب و هوایی و گرم شدن کره زمین منجر به افزایش وقوع حوادث طبیعی شده است. تابستان های بسیار گرم و و طولانی، زمستان های بسیار سرد همراه با یخبندان های شدید، سیلاب های ناگهانی و خسارت بار، طوفان های با سرعت بالا و مخرب، تندبادهای گسترده و فاجعه بار و ...، همگی از رخدادهایی هستند که برای همگان آشنا بوده و در اقصی نقاط کره زمین مرتباً در حای وقوع می باشند. بسته به موقعیت جغرافیایی یک منطقه، وقوع برخی از این حوادث محتمل تر و برخی دیگر بعید است؛ اما، افزایش وقوع آنها بر اساس مستندات موجود، واقعیتی انکارناپذیر است.

در دهه گذشته، زیرساخت‌های حیاتی کشورها، به ویژه شبکه های برق، با سرعت بالایی دیجیتالی شده‌اند. بگونه ای 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. درحالی‌که توسعه زیرساخت‌های دیجیتال مدیریتی در برخی موارد بدون رعایت کامل استانداردهای امنیتی صورت گرفته است (Talaie & Rezania, 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, ۲۰۲۴). این پدیده نه‌تنها تهدیدی زیست‌محیطی 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 (شفیعی 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 اندکه 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., ۲۰۲۱).

تغییرات اقلیمی و موج‌های 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) .

طوفان‌های 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 طوفان‌های گرد و غبار با خطاهای سایبری، بازتابی از بحران‌های محیطی – فناورانه ترکیبی است که باید در سیاست‌های ملی مدیریت بحران گنجانده شود.

تهدیدات محیطی ایران به‌ویژه بحران آب، تغییر اقلیم و گرد وغبار، دیگر صرفاً پدیده‌های طبیعی نیستند. بلکه به واسطه پیوندشان با سامانه‌های دیجیتال، بخشی از امنیت ملی فناورانه محسوب می‌شوند. لذا هرگونه بی‌توجهی به مدیریت داده‌های محیطی، مستقیماً می‌تواند باعث اختلال در زیرساخت‌های انرژی و حتی بحران‌های 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

درصورت 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 (Iiot)، 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 سیستتم 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 لایه‌های فیزیکی نفوذ کنند.

ب) حمله به جایگاه‌های 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 آسیب پذیری زیر ساخت های 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 می رسد نهادهای متعدد و بعضاً موازی در حوزه سایبری فعالیت می کنند و نبود یک فرماندهی و راهبرد واحد، منجر به تصمیم های ناهماهنگ و واکنشی می شود(صفا، ۱۴۰۴)

ب) ضعف در سیاست‌گذاری یکپارچه تاب آوری

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 حالی‌که تمرکز تحلیل‌ها درباره کشورهایی با منابع محدودتر(از جمله ایران)، بیشتر بر ظرفیت‌های سازمانی و توسعه تدریجی این سیاست‌ها در سطح بنگاه‌ها و نهادهای منفرد است(Collovà & Lilyanova, ۲۰۲۴).

ج) عدم اتصال امنیت زیست‌محیطی و فناورانه

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 سیبرنتیک مرتبط هستند(Araujo et al, 2024).

با توجه به موارد پیش گفته؛ تحلیل ها نشان می دهد که ایران امروز در قلب « گذر از حاکمیت فیزیکی به حاکمیت داده ای » 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 فناورانه اخیر (سوخت، راه‌آهن و ...) تنها نمادهایی از نبرد نرم‌افزاری علیه تاب آوری ملی هستند. دشمنان به‌جای حمله مستقیم نظامی، زیرساخت داده را هدف گرفته اند. زیرا سقوط داده، سقوط قدرت تصمیم سازی است. در چنین وضعی هر حمله سایبری نه صرفاً تهدیدی دیجیتال، بلکه تجلی اراده دشمن برای فروپاشی مدیریت ملی از درون است. ازهمین‌رو « سیاست تاب آوری فناورانه » باید از سطح فنی به سطح دکترینال ارتقاء یابد.

الگوی پیشنهادی راهبرد ملی تاب آوری فناورانه ایران:

الف) ضرورت تدوین دکترین ملی تاب آوری فناورانه

تحولات فناوری در سال های اخیر موجب شکل‌گیری پارادایمی نو در امنیت ملی کشورها شده‌است. پارادایمی که امنیت را نه صرفاً در مرزهای جغرافیایی، بلکه در مرزهای داده‌ای زیر ساختی و فناورانه تعریف می‌کند. در چنین شرایطی، تاب آوری 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 تاب آوری 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 تاب آوری 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
	طراحی پلتفرم داده‌های ملی تاب‌آوری	تجمیع داده‌ها و تحلیل بلادرنگ تهدیدات
ایجاد شبکه ملی و هشدار سریع فناورانه	کشف، پیش‌بینی و هشدار به موقع نسبت به حملات سایبری و خرابی‌های زیرساختی	کاهش خسارت و سرعت واکنش به تهدیدات
	طراحی بر پایه AI-driven Predictive Analysisو تحلیل داده‌های صنعتی و اقلیمی	پیش‌بینی دقیق تهدیدات و بهبود تصمیم‌گیری
	پیاده‌سازی اولیه از طریق شبکه شتاب‌دهنده‌ها و آزمایشگاه‌ها	ایجاد تجربه عملی و هم‌افزایی دانشگاهی- صنعتی
	سیستم هشدار ملی چندلایه‌ای (Multi-tier Alert System)	اولویت‌بندی تهدیدات و ارسال هشدار سریع
	۱۵.ادغام داده‌های فضای سایبری و IoT صنعتی	تحلیل تهدیدات پیشرفته و جامع
	توسعه سامانه پایش بلادرنگ (Real-time Monitoring Dashboard)	دسترسی فوری به وضعیت زیرساخت‌ها و رخدادها
	طراحی کانال‌های امن ارتباطی بین نهادهای حیاتی	اطمینان از رسیدن هشدارها بدون اختلال

	استفاده از مدل‌های یادگیری ماشینی برای تحلیل و پیش‌بینی حملات	بهبود دقت پیش‌بینی و کاهش تهدیدات غیرمنتظره
حفاظت از انرژی و زیر ساخت های راهبردی	تمرکز بر پایداری زیرساخت‌های برق، گاز، پالایشگاه‌ها و حمل‌ونقل هوشمند	.افزایش مقاومت شبکه‌های حیاتی و کاهش اختلالات
	برطرف نمودن اختلالات برق ناشی از خطاهای نرم‌افزاری	کاهش خاموشی‌ها و افزایش پایداری عملیاتی
	طراحی سامانه‌ای با لایه دوم امنیت(dual security layer)	امکان بازیابی خودکار و تقویت تاب‌آوری
	ایجاد مرکز ملی حفاظت انرژی سایبری	تمرکز تخصصی و میان‌رشته‌ای برای حفاظت از انرژی
	سامانه پیش‌بینی اختلالات زیرساختی	پیش‌بینی و کاهش اختلالات قبل از وقوع
	مکانیزم افزونگی عملیاتی (Operational Redundancy)	تضمین تداوم فعالیت‌ها حتی در شرایط بحران
	استانداردسازی پروتکل‌های امنیتی SCADA وOT	کاهش آسیب‌پذیری سیستم‌های صنعتی
	مرکز ملی بازیابی اضطراری انرژی و زیرساخت‌ها	بهبود سرعت بازگشت به حالت عملیاتی عادی
	اجرای آزمون‌های تاب‌آوری زیرساختی سالانه	ارتقای آمادگی عملی و کاهش خسارت در بحران
توسعه سرمایه انسانی و سواد فناورانه ملی	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
	گنجاندن 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

تحقیقات و بررسی های میدانی نشان می دهد که تاب آوری فناورانه در ایران باید بر اساس « مدل شبکه‌ای و هم‌افزا » طراحی‌شود. یعنی فرماندهی متمرکز در رأس قرار دارد، اما با تبادل داده چندسویه میان زیر نظام های عملیاتی. لذا تاب آوری فناورانه در ایران باید از سطح پروژه‌های جزئی به سطح دکترین ملی ارتقا یابد.

برابر یافته های 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 ساخت های 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 نه‌تنها 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.

پیشنهادات 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 به‌عنوان 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، حمل‌ونقل 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 می شود. ارائه سیاست ها و راهبردهایی که بتوانند تاب آوری برق کشور و ارتباط آن با تأسیسات حساس ملی را ارتقاء دهند و یا فناوری های 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 هماهنگ 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 سایبریپ
۳. توسعه سامانه‌های پیش هشدار 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 فناورانه و امنیت سایبری
۲. اصلاح برنامه‌های درسی دانشگاه‌ها با تمرکز بر تاب آوری و امنیت زیرساخت‌های حیاتی
۳. توسعه دیپلماسی فناورانه 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 داده ای در سازمان‌های دولتی و صنعتی

جمع‌بندی راهبردی

تاب‌آوری فناورانه 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، به کانون آسیب‌پذیری یا قدرت ملی تبدیل شده است.

بر این اساس، اجرای یک بسته سیاستی یکپارچه تاب‌آوری فناورانه که به‌طور هم‌زمان ابعاد نهادی، فناورانه 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 پایش، 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 زیرساخت های 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 وکارهای 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؛ دکتریـنی که امنیت، توسعه پایدار و اقتدار ملی را در یک چارچوب منسجم و آینده‌نگر به هم پیوند می‌زند.

منابع:

۱. آقابیگی، 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.20۲۴.۳۷۸۱۵۵.۱۷۴۵

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 اقتصاد و برنامه ریزی شهری، دوره ۷، شماره ۳، خرداد ۱۴۰۵

۸. شفیعی دارافشانی، ع و شمسی اژیه، 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 تاب آوری 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- چالش ها 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. کسرایی 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 طباطبایی، دانشکده علوم اقتصادی، پایان نامه کارشناسی ارشد

۱۴. مقدسی، م. (۱۴۰۴) "تاب آوری 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 شرکت های تولیدی". مطالعات رفتار سازمانی، سال چهارم، شماره یک، ۲۴-۱

۱۶. نجفی روادانق، س. کریمی، م. حقی فام، م. (۱۳۹۸) "چارچوب طراحی شبکه های توزیع تاب آور 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 تاب آور"، مرکز پژوهش های 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 نیروگاه های 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 Send 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 relatioships. 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, l., 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.

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

[۲٥] 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

[۲٦] 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 modrling 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

[۳٤] 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

[۳٥] 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.

[۳۹] Siddiqui, F., Hagan, M., & Sezar, S. (2020). Estabilishing cyber resillence 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

[٤٠] Slattery, P., et al. (2024). The Al Risk Repository: A comprehensive taxonomy of risks from artificial intelligence. arXiv:2408. 12622.

[٤١] Spaans, M & Waterhout, B (2017). Building up resilience in cities worldwide – Rotterdam as participant in the 100 Resilient cities Programm Citiese, 61, 109-116. https:// doi.org/10.1016/j.cities.2016.05.011

[٤٢] Stuxnet(Second Edition). (2015). Science Direct

[٤٣] Talaie, A., & Rezania, S. (2024). Climate Change in Iran: Challenges and Solutions – A Short Communication. Journal of Environmental Treatment Techniques, 12(4), 19-29.

[٤٤] 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)

[٤٥]

[٤٥] 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

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

[٤٧] 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

[٤٨]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.