تهران؛ پایتخت تجارت ایران

سپر دیجیتال ایران: معماری نوین تاب‌آوری سایبری برای رشد اقتصادی در عصر جنگ‌های ترکیبی

معاونت مطالعات اقتصادی و آینده پژوهی

اتاق بازرگانی، صنایع، معادن و کشاورزی تهران

سپر دیجیتال ایران: معماری نوین تاب‌آوری سایبری برای رشد اقتصادی در عصر جنگ‌های ترکیبی

مرداد ماه ۱۴۰۴

از طریق پست الکترونیکی زیر می‌توانید پیشنهادها و نظرات اصلاحی خود را به واحد مربوطه منعکس کنید:

Economic_research@tccim.ir

فهرست مطالب

خلاصه مدیریتی

ماهیت منازعه علیه جمهوری اسلامی ایران به شکلی برگشت‌ناپذیر تغییر کرده است. جنگ ۱۲روزه اخیر با رژیم صهیونیستی، صرفاً یک درگیری نظامی نبود، بلکه اعلام رسمی ورود به یک جنگ اقتصادی به ویژه در حوزه سایبری نیز بود. میدان اصلی نبرد از حوزه فیزیکی به حوزه سایبری–فیزیکی در حال گسترش است؛ جایی که حملات به زیرساخت‌های حیاتی با هدف فلج کردن اقتصاد و تضعیف انسجام اجتماعی طراحی می‌شوند. حملات پیچیده اخیر به بخش‌های صنعتی، بانکی و خدمات عمومی ایران، حوادثی مجزا نیستند، بلکه کارزاری مستمر از یک جنگ ترکیبی به شمار می‌روند.

این گزارش استدلال می‌کند که وضعیت دفاعی کنونی ایران، که ریشه در رویکردهای امنیتی سنتی و مبتنی بر حفاظت از محیط پیرامونی دارد، در برابر این تهدیدات مدرن به شکلی خطرناک ناکافی است. یک شکاف حیاتی میان راهبرد دشمن – که نقاط اتصال میان فناوری، اقتصاد و جامعه را هدف قرار می‌دهد – و پاسخ پراکنده کشور وجود دارد.

در پاسخ، این گزارش توسعه و پیاده‌سازی یک معماری ملی **تاب‌آوری سایبری** را پیشنهاد می‌کند. این صرفاً یک طرح دفاعی نیست، بلکه یک راهبرد جامع و ملی برای تقویت **بازدارندگی مبتنی بر انکار** است که بر یک تغییر پارادایم بنیادین استوار است: گذار از "جلوگیری از نفوذ" به "تضمین تاب‌آوری با فرض وقوع نفوذ". این معماری بر چهار رکن راهبردی بنا شده است: ۱) حکمرانی یکپارچه و بازدارندگی فعال، ۲) تداوم عملیات اقتصادی در شرایط نبرد، ۳) پدافند هوشمند در عمق، و ۴) بسیج سرمایه انسانی و اقتصادی.

این گزارش، سرمایه‌گذاری در تاب‌آوری سایبری را بازتعریف می‌کند. این یک هزینه از دست رفته نیست، بلکه یک سرمایه‌گذاری ملی با کاربری دوگانه است. با ساختن این "سِپر دیجیتال"، ایران می‌تواند به طور همزمان حاکمیت خود را در برابر تهاجم خارجی ایمن سازد و رشد یک صنعت فناوری و امنیت سایبری داخلی در کلاس جهانی را کاتالیز کند و بدین ترتیب، موتور جدیدی برای شکوفایی اقتصادی و یک مزیت راهبردی برای آینده خلق نماید.

این گزارش خواستار تشکیل فوری یک کارگروه مشترک میان دولت و بخش خصوصی، با مشارکت اتاق بازرگانی تهران، برای عملیاتی‌سازی پیشنهادهای این گزارش است.

مقدمه

نشـــســـت اخیر در اتاق بازرگانی تهران با عنوان "تاب‌آوری و مدیریت فناوری اطلاعات، و تهدیدات ســـایبری در شرایط جنگ و پساجنگ"، اجماع نظری میان کارشناسان بخش دولتی و خصوصی را برجسته ساخت: منازعه با رژیم صهیونیستی، به‌ویژه پس از جنگ ۱۲ روزه، وارد مرحله‌ای نوین و مستمر از جنگ ترکیبی شده است. این واقعیت در حملات هدفمند و مکرر به حیاتی‌ترین زیرساخت‌های اقتصادی و اجتماعی ایران تجلی یافته است.

این گزارش استدلال می‌کند که مدل‌های امنیتی سنتی، که بر ساختن یک دژ دیجیتال نفوذناپذیر (رویکرد "قلعه و خندق") متمرکز هستند، منسوخ شده‌اند. دشمن از پیش در داخل دیوارها حضور دارد و از آسیب‌پذیری‌های موجود در زنجیره تأمین نرم‌افزار، سیستم‌های صنعتی قدیمی و شبکه پیچیده خدمات دیجیتال درهم‌تنیده بهره‌برداری می‌کند. حملات به صنایع فولاد و سامانه توزیع سوخت کشور، گواه آشکار این واقعیت است.

برگزاری چنین نشـــســـتی در لتاق بازرگانی، به خودی خود نشـــان‌دهنده یک درک حیاتی و نوین در میان رهبران اقتصـادی کشـور اسـت: مرز میان ریسـک تجاری و ریسـک امنیت ملی از میان رفته اسـت. اتاق بازرگانی دیگر تنها متولی منافع کســـب‌وکارها نیســـت، بلکه به نقشـــی خطیر به عنوان یکی از مدافعان خط مقدم ثبات اقتصـــادی و تقویت‌کننده بازدارندگی ملی رانده شده است.

در پاســـخ به این شـــرایط، این گزارش پارادایم جدید**ـتاب‌آوری مبتنی بر طراحی** را معرفی می‌کند. با الهام از درس‌های حیاتی منازعات مدرن، بقای ملی دیگر به جلوگیری از هر حمله بسـتگی ندارد، بلکه به توانایی مقاومت در برابر حملات، محدودسازی آسیب‌ها و بازیابی سریع عملکردها و در عین حال حفظ کارکردهای حیاتی وابسته است. این جوهره **تاب‌آوری** است. این گزارش تغییر پارادایم از "امنیت مبتنی بر پیشگیری" به "تاب‌آوری مبتنی بر فرض وقوع نفوذ" را به عنوان سنگ بنای راهبرد آینده پیشنهاد می‌کند.

این یادداشت سیاستی، ابتدا به تشخیص آسیب‌پذیری‌های خاص زیرساخت‌های حیاتی ایران می‌پردازد، سپس یک معماری دقیق و چهار رکنی برای **تاب‌آوری ملی** ارائه می‌دهد و در نهایت، یک نقشه راه مشخص و عملیاتی برای اجرای مشـترک توسـط بخش دولتی و خصـوصـی ترسـیم می‌کند. این نقشـه راه نه به عنوان یک بار اضـافی، بلکه به عنوان یک فرصـت راهبردی برای تبدیل یک آسـیب‌پذیری حیاتی به منبعی از قدرت پایدار ملی و پویایی اقتصـادی قاب‌بندی شده است.

ارزیابی چشم‌انداز تهدید: آسیب‌پذیری‌های ایران در برابر نبردهای ترکیبی

دکترین دشمن: اخلال سایبری-فیزیکی

تحلیل حملات اخیر نشـان می‌دهد که راهبرد دشـمن از سـرقت اطلاعات فراتر رفته و بر ایجاد اخلال ملموس و فیزیکی برای فلج کردن صنایع کلیدی و کاشتن بذر نارضایتی عمومی متمرکز شده است. اهداف با دقت برای ایجاد حداکثر تأثیر اقتصـادی و روانی انتخاب می‌شـوند. این رویکرد، یک تحلیل دقیق از زنجیره ارزش اقتصـاد ایران را در پس خود دارد؛ مهاجمان نقاطی را هدف قرار می‌دهند که در آن سـیسـتم‌های دیجیتال، فیزیکی و اجتماعی به شـکننده‌ترین شـکل به یکدیگر متصـل‌اند و اخلال در آن‌ها بیشـترین تأثیر آبشـاری را به همراه دارد. انتخاب اهدافی چون سوخت (تأثیر بر حمل‌ونقل و زندگی روزمره) و فولاد (تأثیر بر ساخت‌وساز، صنعت و صادرات) تصادفی نیست، بلکه نشـان‌دهنده هدف‌گیری هوشـمندانه گلوگاه‌های اقتصـادی کشـور اسـت. این اختلال سـایبری – فیزیکی تازه نیست، در سالهای اخیر نیز رخ داده است. – **رخداد اول، حمله سایبری به صنایع فولاد در تیرماه ۱۴۰۱:** حمله به شـرکت‌های بزرگی چون فولاد مبارکه و فولاد خوزسـتان، قلب صـنعتی کشـور را نشـانه گرفت و به توقف عملیات تولید منجر شـد. این حمله از بدافزار پاک‌کننده‌ای (Wiper) به نام "Chaplin" (مرتبط با خانواده بدافزاری Meteor) اسـتفاده کرد که هدف آن نه جاسـوسـی، بلکه تخریب کامل داده‌ها و سـیسـتم‌ها بود. این امر، نیت آشـکار دشـمن برای توقف تولید و تحمیل خسـارت مسـتقیم اقتصـادی را به اثبات می‌رساند. و **– رخداد دوم، اختلال در سامانه توزیع سوخت به‌تاریخ آذرماه ۱۴۰۲:** این حمله که برای دومین بار رخ می‌داد، مسـتقیماً خدمات عمومی را برای ایجاد اخلال اجتماعی گسـترده و تضـعیف اعتماد عمومی به توانایی دولت در ارائه خدمات اسـاسـی هدف قرار داد. اسـتفاده از پیام‌های تحریک‌آمیز بر روی نمایشـگرهای جایگاه‌ها، مؤلفه‌ای آشـکار از جنگ روانی بود که با هدف تشدید تنش طراحی شده بود.

جنگ ۱۲ روزه و جبهه جدید مالی-دیجیتال

جنگ ۱۲ روزه اخیر، جبهه جدیدی از نبرد اقتصادی را گشود که در آن زیرساخت‌های مالی و اقتصاد دیجیتال کشور به اهداف اصلی تبدیل شدند.

- **حمله به زیرساخت بانکی (بانک سپه و پاسارگاد):** در جریان این جنگ، گروه هکری "گنجشک درنده" (Predatory Sparrow) که به رژیم صهیونیستی منتسب است، مسئولیت حملات گسترده به بانک‌های سـپه و پاسـارگاد را بر عهده گرفت. مهاجمان با بهره‌گیری از ضـعف‌های امنیتی در پورت‌های مدیریتی سـرورها (ILO)، کنترل زیرسـاخت‌ها را به دسـت گرفتند. در حالی که بانک سـپه با کمک سـایر بانک‌ها توانست خدمات حیاتی را حفظ کند، بانک پاسارگاد با اختلالات طولانی‌مدت مواجه شد که حتی پس از هفته‌ها به طور کامل برطرف نشد و منجر به حذف بخش "بانکداری مجازی" از وب‌سایت آن گردید. این

حملات که با هدف ایجاد اختلال در خدمات روزمره و تضـعیف اعتماد عمومی به نظام بانکی طراحی شـده بودند، ضعف‌های جدی در **تاب‌آوری** این بخش حیاتی را آشکار ساختند.

- **حمله‌به صـ رافی رمزارز (نوبیتکس):** همزمان، بزرگترین صـرافی رمزارز ایران، نوبیتکس، هدف حمله‌ای پیچیده قرار گرفت که منجر به سرقت مبلغی حدود ۵۰ میلیون دلار شد. این حمله که مسئولیت آن را نیز گروه "گنجشـک درنده" بر عهده گرفت، ماهیتی کاملاً سیاسـی و روانی داشـت؛ چرا که هکرها بخش بزرگی از دارایی‌های سرقتی را به آدرس‌های سفارشی با شعارهای ضدحکومتی منتقل کرده و عملاً آن‌ها را سوزاندند تا نشان دهند هدفشان نه سود مالی، بلکه ضربه زدن به اقتصاد دیجیتال و ایجاد بی‌اعتمادی است. علاوه بر سرقت، انتشار سورس کد و اطلاعات داخلی پلتفرم، آسیب‌پذیری‌های عمیق‌تری را در زنجیره تأمین نرم‌افزار و امنیت زیرساخت‌های اقتصاد دیجیتال کشور به نمایش گذاشت.

شناسایی ضعف‌های سیستماتیک

موفقیت این حملات، ریشـه در آسیب‌پذیری‌های ساختاری و تکرارشونده‌ای دارد که باید به صورت بنیادین برطرف شوند:

- **آسیب‌پذیری ۱: ضعف در جدلسازی شبکه و انزوای "فرضی":** ادعای مکرر مبنی بر "آفلاین" یا ایزوله بودن سیستم‌های حیاتی مانند سامانه سوخت، با موفقیت حملات به چالش کشیده شده است. این امر نشـان می‌دهد که مسیرهای دسترسـی پیش‌بینی‌نشـده یا ناامن وجود دارند و اصـول بنیادین امنیتی مانند جداسازی شبکه (Network Segmentation) و معماری اعتماد صفر به درستی پیاده‌سازی نشده‌اند. این ضـعف، ضـرورت پیاده‌سـازی فوری "مدل امنیتی مبتنی بر بی‌اعتمادی پیش‌فرض" (Zero Trust) را آشکار می‌سازد.
- **آسیب‌پذیری ۲: زنجیره تأمین نرم‌افزار آسیب‌پذیر:** مسیر نفوذ احتمالی در حمله به صنایع فولاد، بهره‌برداری از آسیب‌پذیری در نرم‌افزارهای کنترل صـنعتی (محصـول شـرکت ایریسـا) بوده اسـت. اسـتفاده از نسخه‌های قدیمی، به‌روزنشده یا حتی کرک‌شده نرم‌افزار در صنایع حیاتی، یک نقطه ضعف بزرگ در مدیریت زنجیره تأمین و یک دعوتنامه آشـکار برای مهاجمان اسـت. این نشـان‌دهنده وابسـتگی سـیسـتماتیک به نرم‌افزارهای شخص ثالث بدون ارزیابی امنیتی کافی است.
- **آسـیب‌پذیری ۳: شـکاف در همگرایی‌فناوری اطلاعات (IT) وفناوری عملیاتی (OT):** خطرناک‌ترین تهدیدها در نقطه تلاقی شـبکه‌های فناوری اطلاعات (IT) و فناوری عملیاتی (OT) قرار دارند. مهاجمان پس از نفوذ به محیط کمتر امن IT (مانند ایمیل‌های سـازمانی)، به سـمت محیط بسـیار حسـاس OT که فرآیندهای فیزیکی (مانند کوره‌های فولاد یا پمپ‌های بنزین) را کنترل می‌کند، حرکت می‌کنند. فقدان امنیت طراحی‌شده برای سیستم‌های OT، یک آسیب‌پذیری بزرگ ملی است و لزوم "توسعه زیرساخت‌های OT" و ایمن‌سازی آن‌ها را دوچندان می‌کند.

معماری ملی تاب‌آوری سایبری: یک نقشه راه برای اقدام مشترک

برای مقابله با این تهدیدات چندوجهی، کشور نیازمند یک معماری امنیت ملی منسجم و آینده‌نگر است. این بخش یک چارچوب راهبردی چهار رکنی را به عنوان هسته اصلی پیشنهادهای این گزارش معرفی می‌کند. این یک معماری کل‌نگر و یکپارچه است که در آن هر رکن، دیگری را تقویت می‌کند.

رکن اول: فرماندهی و کنترل یکپارچه؛ از حکمرانی تا بازدارندگی فعال

اصل بنیادین این رکن، اتخاذ رویکرد "کل جامعه" (Whole-of-Society) است که کارآمدی آن در دفاع سایبری اوکراین به اثبات رسید. دفاع سایبری ملی، وظیفه‌ای فراتر از توان یک نهاد دولتی است و نیازمند همکاری بی‌نقص و اعتمادساز میان تمامی ذی‌نفعان برای ایجاد بازدارندگی مؤثر است.

اقدامات کلیدی:

- **ایجاد کارگروه بحران سایبری دولتی-خصوصی:** این اقدام، پیشنهادهای مختلف برای تشکیل کمیته‌های مشترک را در یک نهاد قدرتمند و ادغام می‌کند. این کارگروه که با حضور نمایندگان وزارت ارتباطات، مرکز ملی فضای مجازی، مرکز افتا و نماینده‌ای تام‌الاختیار از اتاق بازرگانی تشکیل می‌شود، نه تنها به بحران‌ها واکنش نشان می‌دهد، بلکه به طور مستمر در زمینه اشتراک‌گذاری اطلاعات تهدید، برنامه‌ریزی مشترک و نظارت بر رزمایش‌های سایبری ملی فعالیت خواهد کرد.
- **راه‌اندازی سامانه ملی هشدار حملات سایبری:** پیاده‌سازی "سامانه ملی هشدار حملات سایبری" برای ارائه اطلاعات تهدید عملیاتی و بلادرنگ به کسب‌وکارها، یک گام حیاتی برای گذار از گزارش‌های طبقه‌بندی‌شده دولتی به یک سیستم اطلاع‌رسانی انبوه و مؤثر است.
- **تسهیل و چابک‌سازی مقررات:** برای تحقق "کاهش نهادهای نظارتی موازی" و" تسهیل مقررات‌گذاری"، باید یک محیط قانونی چابک ایجاد شود که سرمایه‌گذاری در امنیت را تشویق کند، نه آنکه نوآوری را با بوروکراسی خفه کند. این شامل ایجاد "پناهگاه‌های امن قانونی (Legal Safe Harbors)" برای شرکت‌هایی است که اطلاعات تهدید را به اشتراک می‌گذارند.

رکن دوم: بقای اقتصادی در میدان نبرد؛ تداوم کسب‌وکار و زیرساخت‌های توزیع‌شده

اصل بنیادین این رکن، تضمین بقای دیجیتال و اقتصادی از طریق حفظ کارکردهای حیاتی در حین و پس از حمله است. این امر مستلزم طراحی سیستم‌هایی است که برای بقا و تاب‌آوری ساخته شده‌اند.

اقدامات کلیدی:

• **الزام به تدوین و آزمون طرح‌های تداوم کسب‌وکار (BCP/DRP):** اجرای " الزام سازمان‌ها و بانک‌ها به داشتن نقشه پشتیبان اطلاعات و سناریوی بازگشت به شرایط عادی (DRP) " و " طرح‌های جامع‌تر تداوم کسب‌وکار (BCP) " باید به یک الزام قانونی برای بخش‌های حیاتی تبدیل شود.[1] اثربخشی این طرح‌ها باید از طریق " مانورهای عملیاتی پدافند غیرعامل " به صورت منظم راستی‌آزمایی گردد.

• **مهاجرت راهبردی به ابر (درس آموخته از اوکراین):** این یک پیشنهاد حیاتی است. تجربه اوکراین در انتقال پتابایت‌ها داده دولتی و بانکی به زیرساخت‌های ابری عمومی امن (مانند AWS) درست در آستانه تهاجم، از فروپاشی دولت و نظام مالی آن کشور جلوگیری کرد. این گزارش قویاً خواستار **بازنگری راهبردی در سیاست‌های بومی‌سازی داده** است تا امکان ذخیره‌سازی نسخه‌های پشتیبان رمزنگاری‌شده و توزیع‌شده بین‌المللی از **داده‌های غیرحساس** اما عملیاتی کشور فراهم شود. این راهبرد، نهایی‌ترین طرح بازیابی فاجعه در برابر تهدید حملات فیزیکی به مراکز داده داخلی است. بازار جهانی امنیت ابری که در سال ۲۰۲۵ ارزشی بالغ بر ۴۰ میلیارد دلار دارد، نشان‌دهنده بلوغ و اهمیت این فناوری است.

• **ایجاد مناطق ویژه اقتصاد دیجیتال: تبدیل پاشنه آشیل تمرکزگرایی به فرصت سرمایه‌گذاری:** تمرکز حدود ۹۰ درصد از ترافیک داده و خدمات محتوایی کشور در تهران، یک ریسک سیستماتیک عظیم ایجاد کرده است. این تمرکزگرایی، پایتخت را به یک نقطه شکست واحد (Single Point of Failure) در برابر حملات سایبری، بلایای طبیعی یا تهدیدات نظامی تبدیل می‌کند. راهکار تاب‌آورانه، حرکت به سمت توزیع‌شدگی زیرساخت با راهبری بخش خصوصی است. پیشنهاد می‌شود با الگوبرداری از تجارب موفق جهانی مانند "شنژن" در چین که به تنهایی ۴۶ درصد از FDI و ۶۰ درصد از صادرات چین را به خود اختصاص داده[3] و بیش از ۳۰ میلیون شغل ایجاد کرده است، "مناطق ویژه اقتصاد دیجیتال" در نقاط راهبردی کشور (مانند مناطق آزاد قشم و ماکو) ایجاد شود.[2] این مناطق با ارائه مشوق‌های مالیاتی جذاب (مانند کاهش مالیات شرکت‌ها از ۲۵ درصد به ۱۵ درصد در شنژن) و زیرساخت‌های پیشرفته (شامل مراکز داده توزیع‌شده، مزارع پردازش گرافیکی (GPU) و حمایت از زنجیره ارزش سیلیکون)، می‌توانند به قطبی برای جذب سرمایه‌گذاری داخلی و بین‌المللی تبدیل شوند.[4] این رویکرد نه تنها تاب‌آوری زیرساختی کشور را از طریق توزیع‌شدگی جغرافیایی افزایش می‌دهد، بلکه با کاهش هزینه‌های عملیاتی تا ۸۰ درصد در مقایسه با مدل‌های متمرکز، مزیت اقتصادی قابل توجهی برای بخش خصوصی ایجاد می‌کند.[5]

رکن سوم: پدافند در عمق؛ از اعتماد صفر تا شکار فعال تهدید

با پذیرش این فرض که دشمن از پیش در شبکه‌های ما حضور دارد، تمرکز دفاعی باید از ممانعت در مرزها به شناسایی، مهار و ریشه‌کن‌سازی تهدید در داخل شبکه معطوف شود تا بازدارندگی فعال شکل گیرد.

اقدامات کلیدی:

• **الزام ملی برای معماری اعتماد صفر (ZTA):** پیشنهاد "پیاده‌سازی Zero Trust Mode" باید از یک توصیه به یک الزام راهبردی ملی برای تمام نهادهای دولتی و زیرساخت‌های حیاتی ارتقا یابد. اصل بنیادین ZTA، یعنی "هرگز اعتماد نکن، همیشه راستی‌آزمایی کن"، به طور مستقیم با الگوی حرکت جانبی مهاجمان که در حملات به فولاد و سوخت مشاهده شد، مقابله می‌کند. با توجه به رشد بازار جهانی ZTA به بیش از ۲۵ میلیارد دلار در سال ۲۰۲۵، این رویکرد به یک استاندارد جهانی تبدیل شده است.

• **ایمن‌سازی مرز IT/OT:** باید یک برنامه ملی اختصاصی برای امنیت فناوری عملیاتی (OT) با ادغام پیشنهادهایی برای " توسعه زیرساخت‌های OT " ایجاد شود. این برنامه شامل الزام به جداسازی شبکه‌های IT و OT، ایجاد پایگاه داده ملی آسیب‌پذیری‌های نرم‌افزارهای صنعتی و ترویج اصول " امنیت در طراحی " (Secure-by-Design) برای سازندگان داخلی تجهیزات OT است.

• **تغییر پارادایم رزمایش‌ها؛ از پدافند غیرعامل به شکار فعال آسیب‌پذیری (باگ‌بانتی):** به جای رزمایش‌های نمایشی و سنتی، پیشنهاد می‌شود کشور به سمت برگزاری رویدادهای مستمر و آنلاین " باگ‌بانتی " (Bug Bounty) حرکت کند. در این مدل، از جامعه جهانی و داخلی هکرهای کلاه سفید دعوت می‌شود تا در ازای پاداش مالی، آسیب‌پذیری‌های زیرساخت‌های کشور را شناسایی و گزارش کنند. این رویکرد که بازار جهانی آن تا سال ۲۰۲۷ به بیش از ۵.۴ میلیارد دلار خواهد رسید، یک راهکار اثبات‌شده و بسیار مقرون‌به‌صرفه برای افزایش تاب‌آوری عملیاتی است. تجربه وزارت دفاع آمریکا (DoD) که از طریق این برنامه‌ها بیش از ۲۱۰۰ آسیب‌پذیری را کشف کرده، کارآمدی این مدل را نشان می‌دهد.

• **عصر نبرد الگوریتم‌ها: گسترش کاربرد هوش مصنوعی در دفاع و تهاجم سایبری:** میدان نبرد سایبری به طور فزاینده‌ای توسط هوش مصنوعی (AI) هدایت می‌شود. مهاجمان از هوش مصنوعی برای ساخت ایمیل‌های فیشینگ فوق‌پیشرفته (که در ۸۲.۶درصد حملات فیشینگ استفاده می‌شود)، تولید بدافزارهای هوشمند و شکستن رمزهای عبور (۵۱درصد از رمزهای عبور رایج در کمتر از یک دقیقه شکسته می‌شوند) استفاده می‌کنند.[6] در مقابل، دفاع نیز باید هوشمند شود. بازار جهانی هوش مصنوعی در امنیت سایبری از ۱۵ میلیارد دلار در سال ۲۰۲۵ به ۱۳۵ میلیارد دلار تا سال ۲۰۳۰ خواهد رسید.[7] ابزارهای دفاعی مبتنی بر هوش مصنوعی می‌توانند حجم عظیمی از داده‌ها را تحلیل کرده، تهدیدات را با دقت ۹۸درصد شناسایی و زمان پاسخ به حوادث را تا ۷۰درصد کاهش دهند. این گزارش بر لزوم سرمایه‌گذاری راهبردی در این حوزه و ایجاد بستری برای رشد شرکت‌های دانش‌بنیان داخلی متخصص در هوش مصنوعی و بلاکچین تأکید می‌کند تا کشور بتواند در این مسابقه تسلیحاتی الگوریتمی، هم در دفاع و هم در ایجاد بازدارندگی تهاجمی، پیشرو باشد.

رکن چهارم: تسلیح سرمایه انسانی و اقتصادی؛ از مهارت‌افزایی تا اقتصاد دانش‌بنیان سایبری

این رکن، نقطه اتصال امنیت ملی و توسعه اقتصادی، و جذب مشارکت بخش خصوصی است. هدف، تبدیل هزینه‌های امنیت سایبری به یک موتور محرک اقتصادی و تقویت بازدارندگی از طریق توانمندسازی داخلی است.

اقدامات کلیدی:

• **تأسیس صندوق ملی تاب‌آوری سایبری:** راه‌اندازی " صندوق ملی تاب‌آوری سایبری " با سرمایه‌گذاری مشترک دولت و بخش خصوصی، می‌تواند منابع مالی لازم برای اعطای وام‌های کم‌بهره جهت ارتقای امنیتی را فراهم کرده و به عنوان یک سازوکار " بیمه مدیریت امنیت سایبری " در برابر حوادث فاجعه‌بار عمل کند.

• **ایجاد مشوق‌های اقتصادی:** پیاده‌سازی " مشوق‌های مالیاتی و تسهیلات کم‌بهره " برای شرکت‌هایی که به سطوح معینی از تاب‌آوری سایبری (مانند پیاده‌سازی کامل ZTA) دست می‌یابند، انطباق با استانداردها را از یک هزینه به یک مزیت رقابتی تبدیل می‌کند.

• **جنگ بر سر استعدادها: حفظ و تعامل سازنده با سرمایه انسانی سایبری:** کشور با یک "جنگ فرسایشی" برای حفظ استعدادهای سایبری خود روبروست. رفتارهای نامناسب، از جمله نظام‌های پرداخت دستوری و محدودیت‌های سقف حقوق در بخش دولتی که با ارزش واقعی این متخصصان گران‌قیمت همخوانی ندارد، و همچنین محدودیت‌های غیرضروری برای سفرهای خارجی که آزادی‌های شخصی را خدشه‌دار می‌کند، به مهاجرت گسترده این سرمایه حیاتی منجر شده است. برای مقابله با این روند، باید از مدل‌های موفق جهانی الگوبرداری کرد. پیشنهاد می‌شود با الهام از برنامه "بورسیه برای خدمت" (Scholarship for Service) در آمریکا،[11] دولت با سرمایه‌گذاری در تحصیلات تکمیلی نخبگان، آن‌ها را به خدمت در بخش‌های حیاتی متعهد سازد.[9] همچنین، بازنگری فوری در نظام‌های جبران خدمات برای متخصصان کلیدی و ارائه بسته‌های رقابتی شامل حقوق، مزایا و فرصت‌های توسعه حرفه‌ای، و رفع موانع بوروکراتیک غیرامنیتی، برای حفظ این نیروها ضروری است.[10]

• **ایجاد خط لوله ملی استعدادهای سایبری با رویکرد آموزش ۴.۰:** برای رفع کمبود حیاتی نیروی انسانی، باید از مدل‌های سنتی فراتر رفته و یک برنامه ملی مهارت‌افزایی مبتنی بر " آموزش ۴.۰ " (Education 4.0) تدوین شود. این رویکرد به جای تمرکز بر دانش نظری، بر توسعه مهارت‌های عملی و کاربردی مانند حل مسئله پیچیده، تفکر انتقادی و خلاقیت با استفاده از فناوری‌های نوین (مانند هوش مصنوعی و یادگیری ماشین) برای ایجاد تجارب یادگیری شخصی‌سازی‌شده تأکید دارد. این برنامه شامل ایجاد " بانک اطلاعاتی متخصصان امنیت سایبری " برای بسیج سریع در بحران و راه‌اندازی بوت‌کمپ‌های فشرده برای تربیت نسل جدیدی از مدافعان سایبری است که برای نیازهای واقعی اقتصاد جنگی و صنعت ۴.۰ آماده شده‌اند.

سیاست‌های پیشنهادی و نقشه راه اجرایی

گذار از چشم‌انداز راهبردی به یک برنامه اقدام عملیاتی، نیازمند یک نقشه راه شفاف و مشخص است. این نقشه راه، یک دعوتنامه برای اقدام مشترک است؛ فراخوانی به بخش خصوصی تا با تکیه بر چابکی و نوآوری خود و با حمایت و همگامی دولت، سکان هدایت خصوصی‌سازی و توسعه اقتصاد دیجیتال امن کشور را به دست گیرد. این اقدامات، هزینه‌های دفاعی نیستند، بلکه سرمایه‌گذاری‌های مولدی هستند که آینده اقتصادی ایران را شکل خواهند داد. جدول زیر، پیشنهادهای سیاستی حاصل از هم‌اندیشی خبرگان را در چارچوب معماری چهار رکنی تاب‌آوری سایبری، دسته‌بندی و ارائه می‌کند. ماهیت زمانی موضوعات در سه دسته زمانی تقسیم بندی شده است، که به ترتیب به شرح ذیل می باشد: - کوتاه مدت (کمتر از ۳ ماه) — میان مدت (۳ الی ۶ ماه) — بلند مدت (بیشتر از ۶ ماه)

جدول ۱: اقدامات پیشنهادی برای تقویت تاب‌آوری سایبری ملی

ردیف	موضوع اصلی	عنوان اقدام	ماهیت زمانی	دستگاه‌ها/سازمان‌های مرتبط
۱	فرماندهی و کنترل یکپارچه	ایجاد کارگروه بحران سایبری دولتی-خصوصی برای هماهنگی، رصد و واکنش سریع	کوتاه مدت	اتاق بازرگانی، وزارت ارتباطات، مرکز ملی فضای مجازی، سازمان پدافند غیرعامل، مرکز افتا
۲	فرماندهی و کنترل یکپارچه	راه‌اندازی سامانه ملی هشدار و اشتراک‌گذاری اطلاعات تهدید برای اطلاع‌رسانی بلادرنگ به بنگاه‌ها	میان مدت	مرکز افتا، وزارت ارتباطات، اتاق بازرگانی، شرکت‌های بخش خصوصی
۳	فرماندهی و کنترل یکپارچه	بازنگری و تسهیل مقررات حوزه ICT با هدف کاهش نهادهای موازی و ایجاد پناهگاه امن قانونی برای اشتراک‌گذاری اطلاعات	میان مدت	مرکز ملی فضای مجازی، مجلس شورای اسلامی، وزارت ارتباطات، قوه قضائیه

ردیف	موضوع اصلی	عنوان اقدام	ماهیت زمانی	دستگاهها/سازمانهای مرتبط
۴	بقای اقتصادی در میدان نبرد	تدوین و الزام به اجرای طرحهای تداوم کسبوکار (BCP) و بازیابی فاجعه (DRP) در زیرساختهای حیاتی با برگزاری رزمایشهای منظم	میان مدت	سازمان پدافند غیرعامل، بانک مرکزی، وزارت نیرو، وزارت نفت، وزارت صمت، اتاق بازرگانی
۵	بقای اقتصادی در میدان نبرد	بازنگری در سیاستهای حاکمیت داده برای امکانسنجی پشتیبانگیری امن و رمزنگاریشده از دادههای حیاتی در زیرساختهای ابری توزیعشده	بلند مدت	مرکز ملی فضای مجازی، شورای عالی امنیت ملی، وزارت ارتباطات، نهادهای حاکمیتی
۶	بقای اقتصادی در میدان نبرد	ایجاد " مناطق ویژه اقتصاد دیجیتال " برای جذب سرمایهگذاری و توزیع زیرساختهای حیاتی (مراکز	میان مدت	دبیرخانه شورای عالی مناطق آزاد، معاونت علمی ریاست جمهوری، وزارت اقتصاد، اتاق بازرگانی

ردیف	موضوع اصلی	عنوان اقدام	ماهیت زمانی	دستگاه‌ها/سازمان‌های مرتبط
		داده، مزارع پردازش)		
۷	پدافند در عمق	تدوین استاندارد ملی و الزام به پیاده‌سازی معماری اعتماد صفر (Zero Trust) در کلیه دستگاه‌های دولتی و زیرساخت‌های حیاتی	میان مدت	سازمان فناوری اطلاعات، سازمان پدافند غیرعامل، مرکز افتا، کلیه وزارتخانه‌ها و سازمان‌ها
۸	پدافند در عمق	ایجاد برنامه ملی ایمن‌سازی فناوری عملیاتی (OT) شامل جداسازی شبکه‌های IT/OT و مدیریت آسیب‌پذیری زنجیره تأمین نرم‌افزار	میان مدت	وزارت صمت، وزارت نیرو، وزارت نفت، سازمان پدافند غیرعامل، شرکت‌های دانش‌بنیان
۹	پدافند در عمق	تدوین نقشه راه ملی توسعه و به‌کارگیری هوش مصنوعی در دفاع سایبری با حمایت	بلند مدت	معاونت علمی ریاست جمهوری، وزارت دفاع، وزارت ارتباطات، شرکت‌های دانش‌بنیان

ردیف	موضوع اصلی	عنوان اقدام	ماهیت زمانی	دستگاهها/سازمانهای مرتبط
		از شرکت‌های دانش‌بنیان		
۱۰	پدافند در عمق	راه‌اندازی برنامه‌های ملی و مستمر " شکار آسیب‌پذیری " (باگ‌بانتی) برای ارزیابی عملیاتی امنیت زیرساخت‌های حیاتی	کوتاه مدت	مرکز افتا، سازمان پدافند غیرعامل، اتاق بازرگانی، شرکت‌های دانش‌بنیان
۱۱	تسلیح سرمایه انسانی و اقتصادی	راه‌اندازی " صندوق ملی تاب‌آوری سایبری " جهت ارائه تسهیلات و پوشش بیمه‌ای برای ارتقای امنیت و جبران خسارت بخش خصوصی	کوتاه مدت	اتاق بازرگانی، وزارت اقتصاد، بیمه مرکزی، سازمان بورس و اوراق بهادار
۱۲	تسلیح سرمایه انسانی و اقتصادی	تعریف بسته‌های تشویقی (مالیاتی و تسهیلاتی) برای شرکت‌های پیشرو در	کوتاه مدت	وزارت اقتصاد، سازمان امور مالیاتی، بانک مرکزی، اتاق بازرگانی

ردیف	موضوع اصلی	عنوان اقدام	ماهیت زمانی	دستگاهها/سازمانهای مرتبط
		پیادهسازی استانداردهای تابآوری سایبری		
۱۳	تسلیح سرمایه انسانی و اقتصادی	بازنگری در نظام جبران خدمات و رفع موانع غیرمالی برای حفظ و جذب نخبگان امنیت سایبری در بخشهای دولتی و خصوصی	میان مدت	سازمان امور اداری و استخدامی، معاونت علمی ریاست جمهوری، وزارتخانهها، اتاق بازرگانی
۱۴	تسلیح سرمایه انسانی و اقتصادی	تدوین برنامه ملی مهارتافزایی سایبری مبتنی بر " آموزش ۴.۰ " با همکاری دانشگاهها و بخش خصوصی و ایجاد بانک اطلاعاتی متخصصان	کوتاه مدت	وزارت علوم، وزارت ارتباطات، معاونت علمی ریاست جمهوری، اتاق بازرگانی

جمعبندی: فرصت راهبردی در دل بحران

تشدید تهدیدات سایبری در چارچوب یک اقتصاد جنگی، یک چالش وجودی است که نمیتوان آن را نادیده گرفت. با این حال، این شرایط یک نقطه عطف تاریخی نیز به شمار میرود. این گزارش نشان داد که مسیر پیش رو، یک چشمانداز دوگانه را ترسیم میکند: ساختن "سپر دیجیتال" به طور همزمان هم یک اقدام برای تقویت بازدارندگی

ملی و هم یک کنش برای توسعه اقتصادی است. یک زیرساخت دیجیتال امن و تاب‌آور، پیش‌نیاز بنیادین برای مشارکت و رقابت‌پذیری ایران در اقتصاد جهانی قرن بیست و یکم است.

اتاق بازرگانی، صنایع، معادن و کشاورزی تهران در این چشم‌انداز، نه یک ذی‌نفع منفعل، بلکه رهبر و قهرمان اصلی نقش‌آفرینی بخش خصوصی در این مأموریت ملی است. این گزارش به پیشنهاد اتاق بازرگانی، به عنوان یک سند بنیادین برای ایجاد یک مشارکت قدرتمند و پایدار با دولت بوده، تا چشم‌انداز ایرانی دیجیتال، امن و شکوفا به واقعیت بپیوندد. در عصر جنگ‌های ترکیبی، قدرت اقتصادی و امنیت ملی، دو روی یک سکه‌اند.

منابع:

1. BCP (Business Continuity Plan) and DRP (Disaster Recovery Plan), IBM: https://www.ibm.com/think/topics/business-continuity-vs-disaster-recovery-plan
2. Special Economic Zones: How one city helped propel its country's economic development, https://www.weforum.org/stories/2022/02/special-economic-zones-how-one-city-helped-propel-its-country-s-economic-development/
3. Global Experiences with Special Economic Zones - With a Focus on China and Africa Douglas Zhihua Zeng - World Bank, https://www.worldbank.org/content/dam/Worldbank/Event/Africa/Investing%20in%20Africa%20Forum/2015/investing-in-africa-forum-global-experiences-with-special-economic-zones-with-a-focus-on-china-and-africa.pdf
4. Navigating Tech Growth in Special Economic Zones - TecEx, https://tecex.com/navigating-tech-growth-in-special-economic-zones/
5. Economics of Decentralized Cloud Storage, Part 1 - Impossible Cloud, https://www.impossiblecloud.com/blog/part-1-the-economics-of-decentralized-cloud-storage
6. AI Cyber Attack Statistics 2025: Phishing, Deepfakes & Cybercrime Trends - Tech Advisors, https://tech-adv.com/blog/ai-cyber-attack-statistics/
7. AI in Cybersecurity Strategic Market Roadmap: Analysis and Forecasts 2025-2033, https://www.datainsightsmarket.com/reports/ai-in-cybersecurity-1981659

8. AI in Cybersecurity: How AI is Changing Threat Defense - Syracuse University's iSchool, https://ischool.syracuse.edu/ai-in-cybersecurity/
9. CyberCorps®: Scholarship for Service, https://sfs.opm.gov/
10. Navigating the Cybersecurity Salary Landscape: A Comprehensive Guide to Negotiation, https://www.eccu.edu/blog/navigating-the-cybersecurity-salary-landscape-a-comprehensive-guide-to-negotiation/
11. 8 Effective Strategies for Attracting and Retaining Top Cybersecurity Talent, https://www.cybersecuritydistrict.com/8-effective-strategies-for-attracting-and-retaining-top-cybersecurity-talent/

واژه‌نامه

اصطلاحات راهبردی و مفهومی

- **تاب‌آوری سایبری** (Cyber Resilience): توانایی یک سیستم یا سازمان برای ادامه فعالیت‌های حیاتی خود با وجود وقوع یک حمله سایبری موفق.
- **جنگ‌های ترکیبی** (Hybrid Warfare): استفاده هماهنگ از ابزارهای نظامی، اقتصادی، اطلاعاتی و سایبری برای فلج کردن زیرساخت‌های حیاتی و تضعیف انسجام اجتماعی یک کشور.
- **سایبری-فیزیکی** (Cyber-Physical): اشاره به سیستم‌هایی دارد که در آن عملیات دیجیتال (سایبری) به طور مستقیم فرآیندهای جهان فیزیکی را کنترل کرده و تحت تأثیر قرار می‌دهد.
- **زیرساخت‌های حیاتی** (Critical Infrastructure): دارایی‌ها و سیستم‌های کلیدی که برای عملکرد اقتصاد و جامعه ضروری هستند، مانند انرژی، بانک و خدمات عمومی.
- **بازدارندگی مبتنی بر انکار** (Deterrence by Denial): راهبردی دفاعی که با افزایش چشمگیر استحکام و تاب‌آوری سیستم‌ها، موفقیت حمله را برای دشمن پرهزینه و غیرممکن می‌سازد.
- **سپر دیجیتال** (Digital Shield): یک معماری جامع ملی برای ایمن‌سازی زیرساخت‌های حیاتی کشور در برابر تهاجم سایبری و همچنین کاتالیزوری برای رشد اقتصاد دیجیتال.
- **کل جامعه** (Whole-of-Society): این اصطلاح که در سند به "کل جامعه" ترجمه شده است، به یک رویکرد راهبردی اشاره دارد که در آن تمام بخش‌های جامعه—شامل نهادهای دولتی، بخش خصوصی و شهروندان—به صورت یکپارچه و هماهنگ برای مقابله با یک بحران یا چالش ملی، مانند دفاع سایبری، همکاری می‌کنند.

- **رویکرد "قلعه و خندق" (Castle-and-Moat Approach):** یک مدل امنیتی سنتی و منسوخ که صرفاً بر ساختن یک محیط پیرامونی نفوذناپذیر برای جلوگیری از ورود مهاجمان متمرکز است.
- **تاب‌آوری مبتنی بر طراحی (Resilience by Design):** رویکردی که در آن، توانایی مقاومت و بازیابی سریع از حملات، از همان ابتدای طراحی در معماری سیستم‌ها لحاظ می‌شود.
- **همگرایی IT و OT (IT/OT Convergence):** نقطه تلاقی و اتصال شبکه‌های فناوری اطلاعات (IT) با شبکه‌های فناوری عملیاتی (OT) که فرآیندهای صنعتی و فیزیکی را کنترل می‌کنند.
- **نقطه شکست واحد (Single Point of Failure):** بخشی از یک سیستم که در صورت از کار افتادن، منجر به توقف کامل کل مجموعه شده و یک ریسک سیستماتیک بزرگ محسوب می‌شود.
- **پدافند غیرعامل (Civil Defense):** مجموعه اقدامات غیرنظامی برای کاهش آسیب‌پذیری زیرساخت‌ها و تضمین تداوم خدمات ضروری در شرایط بحران.

اصطلاحات فنی و عملیاتی

- **زنجیره تأمین نرم‌افزار (Software Supply Chain):** تمام مراحل، اجزا و فرآیندهای درگیر در ساخت و تحویل یک نرم‌افزار که می‌تواند خود هدف حمله قرار گیرد.
- **بدافزار پاک‌کننده (Wiper Malware):** نوعی نرم‌افزار مخرب که با هدف تخریب کامل و پاک کردن دائمی داده‌ها و از کار انداختن سیستم‌ها طراحی شده است.
- **معماری اعتماد صفر (Zero Trust Architecture - ZTA):** مدلی امنیتی که بر اصل "هرگز اعتماد نکن، همیشه راستی‌آزمایی کن" استوار است و هیچ کاربر یا دستگاهی را به طور پیش‌فرض معتبر نمی‌داند.
- **جداسازی شبکه (Network Segmentation):** تقسیم‌بندی یک شبکه بزرگ به بخش‌های کوچک و ایزوله برای محدود کردن حرکت مهاجم در صورت نفوذ به شبکه.
- **شکار فعال تهدید (Active Threat Hunting):** فرآیند جستجوی پیشگیرانه و مداوم در شبکه‌ها برای کشف مهاجمانی که از سیستم‌های دفاعی خودکار عبور کرده‌اند.
- **باگ‌بانتی (Bug Bounty):** برنامه‌ای که در آن به هکرهای قانونمند (کلاه سفید) برای کشف و گزارش آسیب‌پذیری‌های امنیتی پاداش مالی داده می‌شود.
- **طرح تداوم کسب‌وکار (BCP) و بازیابی فاجعه (DRP):** برنامه‌هایی مدون برای تضمین ادامه کارکردهای حیاتی یک سازمان (BCP) و بازیابی زیرساخت‌های فنی آن پس از یک حادثه مخرب (DRP).
- **حرکت‌جانبی (Lateral Movement):** تکنیکی که مهاجمان پس از نفوذ اولیه، برای حرکت در داخل شبکه و دسترسی به دارایی‌های باارزش‌تر از آن استفاده می‌کنند.
- **امنیت در طراحی (Secure-by-Design):** رویکردی مهندسی که در آن ملاحظات امنیتی از اولین مراحل فرآیند طراحی و ساخت یک محصول یا سیستم لحاظ می‌شود.

- **هوش مصنوعی در امنیت سایبری (AI in Cybersecurity):** استفاده از الگوریتم‌های هوشمند برای تحلیل حجم عظیم داده‌ها، شناسایی خودکار تهدیدات پیشرفته و کاهش زمان پاسخ به حملات.

اصطلاحات اقتصادی و نهادی

- **اقتصاد دیجیتال (Digital Economy):** آن بخش از فعالیت‌های اقتصادی که بر پایه فناوری‌های دیجیتال، داده‌ها و اینترنت برای ارائه کالا و خدمات شکل گرفته است.
- **مناطق ویژه اقتصاد دیجیتال (Special Digital Economic Zones):** مناطق جغرافیایی با زیرساخت‌های پیشرفته و مشوق‌های مالیاتی برای جذب سرمایه‌گذاری و توسعه شرکت‌های فناوری‌محور.
- **اقتصاد دانش‌بنیان (Knowledge-Based Economy):** نظامی اقتصادی که در آن، دانش و نوآوری به عنوان اصلی‌ترین محرک‌های رشد و خلق ثروت عمل می‌کنند.
- **سرمایه‌گذاری مستقیم خارجی (FDI):** این عبارت مخفف Foreign Direct Investment به معنای "سرمایه‌گذاری مستقیم خارجی" است. این اصطلاح به سرمایه‌گذاری اطلاق می‌شود که توسط یک شرکت یا فرد از یک کشور در منافع تجاری کشور دیگر انجام می‌شود.
- **آموزش ۴.۰ (Education 4.0):** رویکردی نوین در آموزش که بر توسعه مهارت‌های عملی مورد نیاز در انقلاب صنعتی چهارم (صنعت ۴.۰) تمرکز دارد.
- **پناهگاه امن‌قانونی (Legal Safe Harbor):** چارچوب‌های حقوقی که از شرکت‌ها در برابر مسئولیت قانونی، در صورت اشتراک‌گذاری اطلاعات تهدیدات سایبری با حسن نیت، محافظت می‌کند.
- **بورسیه برای خدمت (Scholarship for Service):** این اصطلاح که در متن سند "بورسیه برای خدمت" نامیده شده، به برنامه‌هایی اشاره دارد که در آن دولت یا سازمان‌ها، هزینه‌های تحصیلات عالی افراد نخبه را در رشته‌های تخصصی و حیاتی تقبل می‌کنند و در مقابل، آن افراد متعهد می‌شوند تا پس از پایان تحصیلات، برای مدت معینی در بخش‌های ضروری دولتی یا عمومی خدمت کنند.