

اینترنت؛ زیرساختی برای اقتصاد پس از دیجیتال



شده است. اعداد نیز این روایت را تقویت می‌کنند: اتصال روستاهای بالای ۲۰ خانوار به شبکه ملی اطلاعات ۹ درصد رشد کرده، سایت‌های نسل پنجم تلفن همراه ۲۴ درصد بیشتر شده‌اند، پوشش فیبر نوری ۳۷ درصد و اتصال مشترکان به فیبر ۱۵۰ درصد افزایش یافته است. کاربران واحد دولت هوشمند در کنار کاربران پیام رسان‌های بومی ۶۰ درصد رشد کرده‌اند؛ سرویس‌های مرکز تبادل اطلاعات ۵۱ درصد و تراکنش‌های آن ۹۲ درصد بیشتر شده‌اند. در حوزه فضایی نیز پرتاب‌های بومی ماهواره ۴۱ درصد و پرتاب‌های خارجی ۱۵۰ درصد رشد داشته و ایستگاه‌های سلماتس، چساران و چاپبار به پیشرفت ۹۸ درصدی رسیده‌اند. اینها نشانه‌های یک اقتصاد در حال حرکت‌اند؛ اما هنوز سند ورود به آینده نیستند.

آینده فناوری با دیجیتالی کردن گذشته ساخته نمی‌شود. اینکه فروشگاه سنتی به اپلیکیشن، صف اداری به پنجره واحد، یا تاکسی خیابانی به پلتفرم تبدیل شود، مهم

است؛ اما این ابتدای ماجراست. آزمون بزرگ‌تر جای دیگری است: آیا اینترنت ایران می‌تواند به زیرساخت کشف دارو، طراحی مواد، نو ساخت ماشین‌آلات هوشمند، مدیریت شبکه انرژی و افزایش بهره‌وری کشاورزی تبدیل شود؟ اگر پاسخ مثبت باشد، اقتصاد دیجیتال از «بازار آنلاین» فراتر می‌رود و به موتور فناوری‌های همگرا بدل می‌شود. اگر نه، کشور فقط ابزارهای تازه‌ای برای انجام کارهای قدیمی خواهد داشت؛ سریع‌تر، شیک‌تر، اما نه الزاماً آینده‌ساز. علی‌رغم مقاومت‌های تنظیم‌گران بخشی، دولت چهاردهم توانسته است با اجماع‌سازی با محوریت رئیس‌جمهوری مسیر اقتصاد دیجیتال را تا اندازه‌ای هموار کند. توسعه اتصال‌های فیبر نوری، تقویت خدمات برخط، تلاش برای افزایش کیفیت شبکه، بازنگری در سیاست مسدودسازی و قرار دادن اقتصاد دیجیتال در دستور کار دولت، همگی نشانه‌هایی از تغییرجهت‌اند. اما خطر آن است که موفقیت در رشد سهم اقتصاد دیجیتال، با موفقیت

به محتوا نیست. اینترنت همان زیرساختی است که داده، محاسبات، سرمایه، دانشگاه، صنعت و بازار را به یکدیگر متصل می‌کند. برای همین، کیفیت سیاست اینترنت باید نه با تعداد کاربران شبکه‌های اجتماعی بومی، بلکه با توان آن در پشتیبانی از علم و تولید سنجیده شود. پرسش درست این نیست که چند میلیون نفر خرید اینترنتی می‌کنند. باید پرسید یک پژوهشگر ایرانی با چه سرعت و اطمینانی به داده‌های علمی، مخازن کد، نرم‌افزارهای تخصصی، خدمات ابری و همکاران خارجی خود دسترسی دارد. یک شرکت دانش‌بنیان چه اندازه می‌تواند به بازارهای بین‌المللی، ابزارهای طراحی، خدمات امنیتی و زنجیره‌های ارزش جهانی متصل شود؟ یک بیمارستان، کارخانه یا مزرعه تا چه حد می‌تواند از هوش مصنوعی و تحلیل بلادرنگ داده استفاده کند؟

اقتصاد دیجیتال را می‌توان تا حدودی در داخل مرزهای ملی توسعه داد. اما فناوری‌های همگرا در انزوا رشد نمی‌کنند. دانش علمی فقط در مقاله‌ها ذخیره نمی‌شود. بخشی از آن دانشی ضمنی است که از همکاری، گفت‌وگو، مشاهده خطاها و کار مشترک به دست می‌آید. مهندس ماهر ممکن است بتواند یک دستگاه پیچیده را تنها با شنیدن صدای آن غیب‌یابی کند؛ دانشی که به‌سادگی در کتابچه راهنما نوشته نمی‌شود. پژوهشگر نیز از گفت‌وگو با همکاران خود چیزهایی می‌آموزد که در نسخه نهایی مقاله وجود ندارد؛ آزمایش‌هایی که شکست خورده‌اند، مسیرهایی که ارزش ادامه دادن ندارند و نشانه‌هایی که هنوز به نتیجه علمی قطعی تبدیل نشده‌اند. ایران از این نظر مزیتی بزرگ و تا اندازه‌ای استفاده‌نشده دارد: شبکه وسیع دانشمندان، مهندسان و کارآفرینان ایرانی در سراسر جهان. اینترنت پایلاد می‌تواند این پراکندگی جغرافیایی را به یک شبکه ملی دانش تبدیل کند. اینترنت محدود و نامطمئن، برعکس، حتی تخصصی آموزش مدل‌های هوش مصنوعی را کاهش می‌دهند؛ علم مواد، ساخت تراشه‌ها و باتری‌های بهتر را ممکن می‌کند؛ ماهواره‌ها داده موردنیاز کشاورزی دقیق، مدیریت آب و پایش محیط‌زیست را فراهم می‌کنند. مزیت اقتصادی دیگر در اختیار یک فناوری منفرد نیست. در فاصله میان فناوری‌ها شکل می‌گیرد. اینترنت در چنین اقتصادی صرفاً وسیله دسترسی

احتمال قطع دسترسی آن به بازار، نرم‌افزار، داده یا مشتری را محاسبه کند. نااطمینانی درباره اینترنت، نرخ بازده مورد انتظار را بالا می‌برد، دوره سرمایه‌گذاری را کوتاه می‌کند و منابع را به سمت فعالیت‌هایی می‌برد که کمتر نواورانه و زودبازده‌ترند. نتیجه، اقتصادی است که می‌تواند خدمات دیجیتال مصرف کند، اما در تولید فناوری‌های پیشرفته ناتوان می‌ماند. این وضعیت برای شرکت‌های دانش‌بنیان پرهزینه‌تر است. فاصله‌های خطرناک میان اثبات یک ایده در آزمایشگاه و تبدیل آن به محصول تجاری وجود دارد. شرکت جوان در این مرحله هنوز مشتریان کافی ندارد، هزینه تولیدش بالاست و سرمایه‌گذار نیز از آینده آن مطمئن نیست. در ایران، تحریم، نوسان ارز و دشواری تأمین مالی این فاصله را عمیق کرده‌اند. اینترنت ناپایدار، مانع دیگری به آن می‌افزاید.

اصلاح سیاست اینترنت همه این مشکلات را حل نمی‌کند، اما یکی از معدود اصلاحاتی است که می‌تواند هم‌زمان هزینه مبادله را کاهش دهد، بازار شرکت‌ها را بزرگ‌تر کند، همکاری علمی را آسان‌سازد و دسترسی به سرمایه و فناوری را بهبود بخشد. البته اینترنت باز به معنای اینترنت بی‌دفاع نیست. امنیت سایبری بر محرمانگی، صحت و دسترس‌پذیری استوار است. سیاستی که برای حفاظت از دو اصل اول، دسترس‌پذیری را قربانی کند، شبکه‌ای ظاهرآ امن اما از نظر اقتصادی کم‌فایده می‌سازد. افزون بر این، مسدودسازی گسترده کاربران را به فیلترشکن‌ها و نرم‌افزارهای ناشناخته سوق می‌دهد، به روزرسانی‌های امنیتی را دشوار می‌کند و امکان مدیریت تهدیدها را کاهش می‌دهد؛ سیاستی که امید می‌رود با تغییر رویه در شورای عالی فضای مجازی اصلاح شود. امنیت هوشمند باید مهاجم را هدف قرار دهد، نه اتصال را. از این‌رو، آزمون دولت چهاردهم فقط به رفع محدودیت یک یا چند پلتفرم محدود نمی‌شود. تغییر واقعی زمانی رخ می‌دهد که دسترسی به اینترنت از یک تصمیم اداری قابل تعلیق، به یک قاعده عمومی و قابل پیش‌بینی تبدیل شود. محدودیت‌های ضروری نیز باید هدفمند، مستند، مدت‌دار و قابل اعتراض باشند. تصمیم اضطراری بدون تاریخ پایان، به‌تدریج

به سیاست دائمی تبدیل می‌شود؛ همان‌گونه که امتیازهای موقت، اینترنت طبقه‌بندی را عادی می‌کنند. سیاستی که در سراسر دولت با آن مخالفت کردیم. توسعه فیبر نوری و نسل پنجم برای این تحول ضروری است، اما کافی نیست. ظرفیت بالای شبکه بدون دسترسی مؤثر به دانش، بازار و خدمات جهانی، مانند ساخت بندری پیشرفته و بستن مسیر آن به دریاست. شبکه ملی اطلاعات به عنوان یک ضرورت می‌تواند تاب‌آوری خدمات داخلی را افزایش دهد، ولی اگر به جای مکمل اینترنت جهانی به جانشین آن تبدیل شود، مزیت اقتصادی خود را نیز از دست خواهد داد.

برای رسیدن به اقتصاد فناوری‌های همگرا، سیاست اینترنت باید در کنار چند سیاست دیگر قرار گیرد: تأمین برق پایدار برای مراکز داده، دسترسی رقابتی دانشگاه‌ها و شرکت‌ها به توان محاسباتی، ایجاد زیرساخت‌های داده پژوهشی، حمایت بلندمدت از تحقیقات دانشگاهی، تقویت استانداردهای فنی، تسهیل همکاری با ایرانیان خارج از کشور و استفاده از خرید دولتی برای رساندن فناوری‌های نوپا به بازار. دولت همچنین باید سنجش موفقیت را تغییر دهد. تعداد مشترکان، میزان پوشش یا حجم ترافیک شاخص‌های مفیدی هستند، اما کیفیت یک زیست‌بوم نوآوری را نشان نمی‌دهند. شاخص‌های مهم‌تر عبارت‌اند از مدت و دامنه تحولات، دسترسی دانشگاه‌ها به منابع علمی، سهم صادرات دیجیتال، سرمایه‌گذاری خطرپذیر و تعداد شرکت‌هایی که از پژوهش به تولید رسیده‌اند.

دولت چهاردهم توانسته است سهم اقتصاد دیجیتال را افزایش دهد؛ اما این موفقیت باید نقطه آغاز باشد، نه خط پایان. ایران اکنون به سیاستی برای «اقتصاد پس از دیجیتال» نیاز دارد: اقتصادی که در آن اینترنت نه فقط محل معامله کالا و خدمات، بلکه بستر تولید علم و ترکیب فناوری‌ها باشد.

کشور را دهه آینده نه تنها بر سر داشتن بهترین الگوریتم، تراشه یا آزمایشگاه رقابت می‌کنند بلکه مزیت اصلی از آن کشوری خواهد بود که بتواند سریع‌تر از دیگران میان ایده، انسان، داده، سرمایه و بازار ارتباط

برقرار کند. برق‌گذاری ایران، پیش از آنکه به یک اختراع بزرگ وابسته باشد، به کیفیت همین اتصال بستگی دارد. خود را داشته باشد تا از وابستگی به کشورهای متخاصم جلوگیری شود و ریسک‌های مربوط به آن، به طرز چشمگیری کاهش یابد.

نقش دولت در نگهداشت متخصمان امنیت اطلاعات عباسی البته معتقد است که یکی از مهم‌ترین سرمایه‌های امنیت سایبری هر کشور، نیروی انسانی متخصص است، به گونه‌ای که حتی پیشرفته‌ترین تجهیزات امنیتی نیز بدون حضور کارشناسان نتوانند، آموزش دیده و به‌روز، نمی‌توانند امنیت پایدار ایجاد کنند.

این کارشناس ارشد امنیت اطلاعات البته تأکید می‌کند که حفظ متخصصان امنیت اطلاعات و فناوری اطلاعات، بخشی از راهبرد امنیتی ملی نیروهای متخصص به راحتی می‌توانند جذب شرکت‌های بزرگ در کشورهای دیگر شوند به همین دلیل هم باید برای حفظ این سرمایه انسانی تلاش کرد؛ سرمایه‌ای که در کنار ابزار و تجهیزات مورد نیاز، اینترنت پایدار و... ضامن تأمین امنیت سایبری زیرساخت‌ها هستند. عباسی البته برای نگهداشت این نیروی انسانی متخصص، پیشنهادهایی هم دارد و معتقد است دولت برای ماندگاری آنها باید مشوق‌های حرفه‌ای و اقتصادی مناسب ارائه دهد و با ایجاد امکان آموزش‌های مستمر و به‌روز در حوزه فناوری و امنیت و همچنین فراهم کردن امکان حضور آنها در دوره‌ها و استانداردهای بین‌المللی کمک کند مسیر رشد شغلی این متخصصان هموارتر شود.

امنیت ملی در عصر دیجیتال نیازمند زیرساخت ارتباطی قوی، متخصصان توانمند و فرآیندهای استاندارد مدیریت امنیت است. ایجاد مسیرهای ارتباطی غیررسمی و خارج از کنترل می‌تواند خود به یک ریسک امنیتی تبدیل شود. هدف باید ایجاد فضای دیجیتال امن و قابل مدیریت باشد.

بازگشایی اینترنت عملاً سطح امنیت سایبری زیرساخت‌ها را ارتقا بخشد و این مهم با تصمیم درست ستاد ویژه فضای مجازی محقق شد. به گفته او، با تصمیم برای بازگشایی اینترنت و برقراری مجدد اتصال آن پس از یک دوره محدودیت نسبتاً طولانی، در فضای امنیت سایبری شاهد دریافت اطلاعات Threat Intelligence، به روزرسانی IDS، IPS، EDR و فایروال‌ها، افزایش همکاری با مراکز امنیتی و افزایش توان شناسایی حملات بودیم که درنتیجه، آسیب‌پذیری سیستم‌ها کاهش یافت.

این کارشناس ارشد امنیت اطلاعات، یکی دیگر از بخش‌های مهم امنیت دیجیتال را که گاهی کمتر مورد توجه قرار می‌گیرد، سیستم‌های عامل دستگاه‌های مورد استفاده کاربران، سازمان‌ها و... می‌داند و می‌گوید: «امروزه تقریباً تمام فعالیت‌های دیجیتال کاربران و سازمان‌ها از طریق تلفن همراه، رایانه شخصی، سرور، تجهیزات صنعتی و تجهیزات هوشمند انجام می‌شود که همگی بر پایه سیستم‌های عامل مختلف از جمله اندروید، iOS، لینوکس و ویندوز فعالیت می‌کنند و البته امنیت آنها وابسته به دریافت مستمر به‌روزرسانی‌ها و اصلاح آسیب‌پذیری‌هاست.»

به گفته عباسی، قطع ارتباط پایدار علاوه بر باقی ماندن آسیب‌پذیری‌ها و عدم دریافت وصله‌های امنیتی، باعث می‌شود کاربران برای دریافت به‌روزرسانی‌های مورد نیاز خود، به منابع غیررسمی مراجعه کنند که به این ترتیب، احتمال استفاده از Firmware یا نرم‌افزارهای دستکاری‌شده افزایش می‌یابد. بنابراین اینترنت بخشی از زنجیره امنیت سیستم‌های عامل و تجهیزات دیجیتال است و حفظ این ارتباط، نقش مهمی در امنیت کاربران و سازمان‌ها دارد. او البته معتقد است ایران نیز باید مانند برخی کشورها سیستم عامل ملی

رئیس‌جمهوری برای حل مشکل، بهترین تصمیم را گرفت و با ابلاغ تشکیل ستاد ویژه ساماندهی و راهبری فضای مجازی کشور به ریاست معاون اول رئیس‌جمهور، مسیررفع محدودیت‌های اینترنتی را کوتاه‌تر کرد

پایدار زمانی ایجاد می‌شود که توان دفاعی افزایش یابد، نه اینکه ارتباطات فناوری حذف شود. آنچه مسلم است زیرساخت‌های فناوری برای عملکرد صحیح، نیازمند ارتباط مستمر با اکوسیستم جهانی فناوری و دریافت به‌روزرسانی‌ها، مدیریت تجهیزات، استفاده از سرویس‌های ابری و توسعه نرم‌افزارهای خود از طریق اینترنت پایدار هستند. «از نگاه عباسی، با دسترسی به اینترنت پایدار، عملاً دریافت پچ‌ها و وصله‌های امنیتی در کمترین زمان ممکن امکانپذیر و به این ترتیب سدی مناسب مقابل هکرها ایجاد می‌شود درحالی که در غیاب اینترنت بین‌الملل، دریافت این پچ‌ها امکان‌پذیر نیست و زیرساخت‌ها بسیار آسیب‌پذیر می‌شوند،

توسعه فناوری و بهره‌مندی جامعه از فرصت‌های دیجیتال ایفا کند.» در اعتقاد او، درک درست از موضوع ساماندهی واقعی فضای مجازی به معنای ایجاد یک محیط امن، پایدار و قابل مدیریت، گام اول در این تصمیم بود که به آن توجه جدی شد؛ محیطی که با مقابله با تهدیدات، امکان رشد علمی، اقتصادی و فناورانه کشور را نیز فراهم کند.

آسیب‌پذیری زیرساخت‌ها در غیاب اینترنت پایدار این کارشناس ارشد امنیت اطلاعات و اقتصاد دیجیتال می‌گوید: «باید به این موضوع توجه داشت که امنیت

نشان می‌دهد راهکار اصلی مقابله با این تهدیدات، قطع ارتباطات با اعمال محدودیت‌های دسترسی به اینترنت نیست، بلکه توسعه زیرساخت‌های دفاعی سایبری، ارتقای دانش امنیتی، آموزش نیروی انسانی و مدیریت هوشمند ریسک‌هایی است که می‌تواند به افزایش تاب‌آوری زیرساخت‌ها در شرایط بحرانی

همچون جنگ کمک کند.» عباسی در ادامه توضیح می‌دهد: «در این چارچوب، ستاد ویژه ساماندهی و راهبری فضای مجازی کشور توانست نقش مهمی در ایجاد هماهنگی میان دستگاه‌های مسئول سیاست‌های مدیریت ریسک‌های فضای دیجیتال و ایجاد تعادل میان امنیت،

کرد؛ مشکلاتی که حتی با ادله‌هایی همچون محافظت از زیرساخت‌ها در برابر حملات سایبری دشمن نیز از نگاه جامعه‌ای که اینترنت را همچون برق و آب لازم می‌داند، قابل قبول نبود.»

عباسی در ادامه می‌گوید: «بعد از جنگ ۴۰ روزه و اعلام آتش‌بس، مردم منتظر رفع محدودیت‌های اینترنتی بودند که این موضوع با مقاومت‌هایی مواجه شد. درست در این بزنگاه بود که رئیس‌جمهوری برای حل مشکل، بهترین تصمیم را گرفت و با ابلاغ تشکیل ستاد ویژه ساماندهی و راهبری فضای مجازی کشور به ریاست معاون اول رئیس‌جمهور، مسیر رفع محدودیت‌های اینترنتی را کوتاه‌تر کرد.» او معتقد است: «عملکرد صحیح و بجای این ستاد در بازگشایی اینترنت بین‌الملل، برخلاف تصور کسانی که مخالف باز شدن اینترنت بودند، عملاً به افزایش امنیت سایبری زیرساخت‌های حیاتی کشور کمک کرد، چراکه نبود اینترنت، خود مانع به‌روزرسانی‌های حیاتی دستگاه‌ها و آسیب‌پذیرتر شدن آنها می‌شد.»

توسعه زیرساخت‌های دفاعی سایبری جایگزین محدودیت‌های اینترنتی شود به اعتقاد این کارشناس ارشد امنیت اطلاعات و اقتصاد دیجیتال، فضای مجازی مانند هر زیرساخت حیاتی دیگری، با تهدیدات و مخاطرات مختلفی مواجه است. او ادامه می‌دهد: «درواقع حملات سایبری، بدافزارها، سرقت اطلاعات،

جاسوسی دیجیتال و سوءاستفاده از فناوری‌های نوین، چالش‌های جهانی هستند که تقریباً تمام کشورهای جهان با آن دست‌وپنجه نرم می‌کنند. اما تجربه جهانی

محبوبه ستارزاده گروه علم و فناوری

همزمان با تجاوز جنایتکارانه آمریکا به کشورمان، شاهد اعمال محدودیت‌هایی که هرچند مردم با روزهای جنگ با همراهی‌شان با دولت و حاکمیت، آن را پذیرفته بودند، اما با کمتر شدن تنش‌ها خواستار رفع محدودیت‌ها و بازگشت اینترنت بین‌الملل شدند؛ اینترنتی که برای بسیاری از مشاغل و کسب‌وکارها، آموزش عالی و تحقیق و... ضروری بود. مردم و به‌ویژه فعالان حوزه اقتصاد دیجیتال، برنامه‌نویسان و... ادامه‌دار شدن محدودیت‌ها را مشکل‌ساز می‌دانستند و معتقد بودند با وجود آتش‌بس، این روند باید زودتر تغییر کند. در این میان موضوعی که شاید کمتر مورد توجه قرار می‌گرفت، تهدید تضعیف امنیت سایبری زیرساخت‌های کشور در غیاب اینترنت بین‌الملل بود؛ موضوعی که کارشناسان حوزه امنیت اطلاعات و سایبری بر آن تأکید ویژه داشتند و دارند.

یک تصمیم درست در بزنگاه محمدرضا عباسی از کارشناسان ارشد امنیت اطلاعات و اقتصاد دیجیتال معتقد است در شرایطی که اینترنت در همه بخش‌های زندگی رسوخ کرده و به یکی از زیرساخت‌های حیاتی جوامع مدرن تبدیل شده، هرگونه اختلال یا قطع این فناوری می‌تواند تهدیدی جدی برای تداوم فعالیت‌های اقتصادی و اجتماعی، آموزش، اقتصاد دیجیتال و... باشد؛ تهدیدی که گاه بسیار خطرناک می‌شود.

او در توضیح این موضوع به «ایران» می‌گوید: «هرچند ایجاد محدودیت‌های اینترنتی در شرایطی همچون جنگ ۴۰ روزه و تجاوز آمریکا به کشورمان به عنوان تصمیم بالاترین مقام‌های امنیتی کشور قابل درک است، اما ادامه‌دار شدن قطع اینترنت بین‌الملل، مشکلات بسیاری در حوزه‌های مختلف ایجاد

بازگشایی اینترنت، زمینه‌ساز ارتقای تاب‌آوری زیرساخت‌ها



رئیس‌جمهوری برای حل مشکل، بهترین تصمیم را گرفت و با ابلاغ تشکیل ستاد ویژه ساماندهی و راهبری فضای مجازی کشور به ریاست معاون اول رئیس‌جمهور، مسیررفع محدودیت‌های اینترنتی را کوتاه‌تر کرد

پایدار زمانی ایجاد می‌شود که توان دفاعی افزایش یابد، نه اینکه ارتباطات فناوری حذف شود. آنچه مسلم است زیرساخت‌های فناوری برای عملکرد صحیح، نیازمند ارتباط مستمر با اکوسیستم جهانی فناوری و دریافت به‌روزرسانی‌ها، مدیریت تجهیزات، استفاده از سرویس‌های ابری و توسعه نرم‌افزارهای خود از طریق اینترنت پایدار هستند. «از نگاه عباسی، با دسترسی به اینترنت پایدار، عملاً دریافت پچ‌ها و وصله‌های امنیتی در کمترین زمان ممکن امکانپذیر و به این ترتیب سدی مناسب مقابل هکرها ایجاد می‌شود درحالی که در غیاب اینترنت بین‌الملل، دریافت این پچ‌ها امکان‌پذیر نیست و زیرساخت‌ها بسیار آسیب‌پذیر می‌شوند،

توسعه فناوری و بهره‌مندی جامعه از فرصت‌های دیجیتال ایفا کند.» در اعتقاد او، درک درست از موضوع ساماندهی واقعی فضای مجازی به معنای ایجاد یک محیط امن، پایدار و قابل مدیریت، گام اول در این تصمیم بود که به آن توجه جدی شد؛ محیطی که با مقابله با تهدیدات، امکان رشد علمی، اقتصادی و فناورانه کشور را نیز فراهم کند.

نشان می‌دهد راهکار اصلی مقابله با این تهدیدات، قطع ارتباطات با اعمال محدودیت‌های دسترسی به اینترنت نیست، بلکه توسعه زیرساخت‌های دفاعی سایبری، ارتقای دانش امنیتی، آموزش نیروی انسانی و مدیریت هوشمند ریسک‌هایی است که می‌تواند به افزایش تاب‌آوری زیرساخت‌ها در شرایط بحرانی

آسیب‌پذیری زیرساخت‌ها در غیاب اینترنت پایدار این کارشناس ارشد امنیت اطلاعات و اقتصاد دیجیتال می‌گوید: «باید به این موضوع توجه داشت که امنیت

نشان می‌دهد راهکار اصلی مقابله با این تهدیدات، قطع ارتباطات با اعمال محدودیت‌های دسترسی به اینترنت نیست، بلکه توسعه زیرساخت‌های دفاعی سایبری، ارتقای دانش امنیتی، آموزش نیروی انسانی و مدیریت هوشمند ریسک‌هایی است که می‌تواند به افزایش تاب‌آوری زیرساخت‌ها در شرایط بحرانی

کرد؛ مشکلاتی که حتی با ادله‌هایی همچون محافظت از زیرساخت‌ها در برابر حملات سایبری دشمن نیز از نگاه جامعه‌ای که اینترنت را همچون برق و آب لازم می‌داند، قابل قبول نبود.» عباسی در ادامه می‌گوید: «بعد از جنگ ۴۰ روزه و اعلام آتش‌بس، مردم منتظر رفع محدودیت‌های اینترنتی بودند که این موضوع با مقاومت‌هایی مواجه شد. درست در این بزنگاه بود که رئیس‌جمهوری برای حل مشکل، بهترین تصمیم را گرفت و با ابلاغ تشکیل ستاد ویژه ساماندهی و راهبری فضای مجازی کشور به ریاست معاون اول رئیس‌جمهور، مسیر رفع محدودیت‌های اینترنتی را کوتاه‌تر کرد.» او معتقد است: «عملکرد صحیح و بجای این ستاد در بازگشایی اینترنت بین‌الملل، برخلاف تصور کسانی که مخالف باز شدن اینترنت بودند، عملاً به افزایش امنیت سایبری زیرساخت‌های حیاتی کشور کمک کرد، چراکه نبود اینترنت، خود مانع به‌روزرسانی‌های حیاتی دستگاه‌ها و آسیب‌پذیرتر شدن آنها می‌شد.»

توسعه زیرساخت‌های دفاعی سایبری جایگزین محدودیت‌های اینترنتی شود به اعتقاد این کارشناس ارشد امنیت اطلاعات و اقتصاد دیجیتال، فضای مجازی مانند هر زیرساخت حیاتی دیگری، با تهدیدات و مخاطرات مختلفی مواجه است. او ادامه می‌دهد: «درواقع حملات سایبری، بدافزارها، سرقت اطلاعات،

جاسوسی دیجیتال و سوءاستفاده از فناوری‌های نوین، چالش‌های جهانی هستند که تقریباً تمام کشورهای جهان با آن دست‌وپنجه نرم می‌کنند. اما تجربه جهانی