یادداشت

عاشورا؛ فراتر از یک آیین

ادامه از صفحه اول

از همکاری در هیئت‌های محلی تا مشارکت در برگزاری آیین‌های عزاداری و خدمت‌رسانی به عزاداران. در روزهای عزاداری محرم، اشکال متنوعی از کار جمعی و مشارکت داوطلبانه شکل می‌گیرد؛ همکاری‌هایی که حتی از مرزهای طبقاتی و اجتماعی نیز عبور می‌کند. این تجربه‌ها در واقع نوعی تمرین اجتماعی برای همبستگی، تعاون و کار مشترک است؛ تمرینی که به مرور زمان به بخشی از ذخیره فرهنگی جامعه ایرانی تبدیل شده است. در عین حال، بسیاری از مفاهیم دینی و اخلاقی نیز در همین بستر اجتماعی و آیینی به نسل‌های مختلف منتقل می‌شوند. از این منظر، محرم تنها حافظ یک خاطره تاریخی نیست، بلکه بستری برای تداوم آموزش‌های دینی و اخلاقی در جامعه نیز به شمار می‌رود.

محرم و خاطره حرکت اجتماعی

برای برخی نسل‌ها، به‌ویژه نسل‌های دهه‌های ۳۰، ۴۰ و ۵۰، محرم تنها یک آیین مذهبی نبود. در آن سال‌ها، این ایام گاه به بستری برای طرح نگاه‌های متفاوت به دین، بازخوانی مسئولیت اجتماعی مؤمنان، نقد نظم موجود و بازنمایی آرمان رهایی از سلطه و استعمار تبدیل شد. محرم در چنین روایت‌هایی، صرفا یادآور سوگ نبود؛ بلکه الهام‌بخش حرکت، بیداری و مسئولیت‌پذیری اجتماعی نیز به شمار می‌آمد.

این تجربه تاریخی نشان می‌دهد که عاشورا در حافظه اجتماعی ایرانیان، همواره ظرفیت‌هایی فراتر از یک روایت آیینی داشته است؛ ظرفیت‌هایی که از دل آموزه‌های دینی آن سرچشمه گرفته و در عرصه اجتماعی نیز بازتاب یافته‌اند.

درس‌های اخلاقی کمتر روایت‌شده

در کنار این ابعاد اجتماعی و تاریخی، عاشورا سرشار از آموزه‌های اخلاقی و انسانی نیز هست؛ آموزه‌هایی که شاید کمتر مورد توجه قرار گرفته‌اند. عاشورا تنها روایت یک تقابل سیاسی نیست، بلکه مجموعه‌ای از درس‌های اخلاقی درباره وفاداری، ادب، مسئولیت، گذشت، ایثار و کرامت انسانی است. از داستان مسلم بن عقیل و خانه هانی تا ادب و منش امام حسین (ع) در مواجهه با دشمنان، از رفتار حضرت عباس (ع) تا تدبیرهای امام سجاد (ع) در ادامه مسیر، همه و همه حامل پیام‌هایی عمیق درباره اخلاق انسانی‌اند. همچنین سیره امام حسین (ع) در دعوت به حق، پایبندی به عهد، پرهیز از آغازگری در خشونت و اهتمام به هدایت انسان‌ها، ابعاد دیگری از این میراث اخلاقی را آشکار می‌سازد. با این حال، به نظر می‌رسد این وجه اخلاقی عاشورا کمتر در روایت‌های عمومی و مجالس عزاداری بازتاب یافته و کمتر مجال یافته است تا به عنوان «اخلاق عاشورا» مورد توجه قرار گیرد.

عاشورا و درس سیاست

نهضت عاشورا در عین حال حامل آموزه‌هایی برای فهم سیاست نیز هست. اما پیش از آنکه یک کنش سیاسی باشد، تلاشی برای پاسداری از حقیقت دین، اصلاح امت و جلوگیری از استحاله ارزش‌های اسلامی بود. همین خاستگاه دینی و اخلاقی است که به این نهضت، ابعاد اجتماعی و سیاسی ماندگار بخشیده است. مفاهیمی چون عدالت‌خواهی، ایستادگی در برابر انحراف، مسئولیت‌پذیری در برابر سرنوشت جامعه و ضرورت حفظ پیوند میان اخلاق و قدرت، از جمله مفاهیمی است که می‌توان از دل این واقعه تاریخی استخراج کرد و درباره آنها اندیشید. با این حال، یکی از آسیب‌های سال‌های اخیر، استفاده ابزاری از عاشورا در مجادلات سیاسی روزمره است. گاه با قرائت‌ها و روایت‌های دلخواه از این واقعه، صحنه تقابل امام حسین (ع) و شمر به نزاع‌های سیاسی امروز پیوند زده می‌شود تا گروهی حذف و گروهی دیگر تثبیت شود. چنین رویکردی، در نهایت چیزی جز تقلیل یک نهضت دینی، تاریخی و اخلاقی به ابزاری برای جدال‌های روزمره نیست.

از هیئت‌های معنامحور تا هیئت‌های ستاره‌محور

تحولات آیین‌های عزاداری نیز در این میان قابل توجه است. در دوره‌هایی، مراسم محرم بیشتر حول محور وعظ، سخنرانی، تبیین معارف دینی و انتقال معنا شکل می‌گرفت. اما در سال‌های اخیر، در برخی موارد شاهد تغییراتی بوده‌ایم؛ از هیئت‌های معنامحور به هیئت‌هایی که گاه بیش از هر چیز بر چهره‌ها، جلوه‌های رسانه‌ای یا نوحه‌های سیاسی تکیه دارند. بی‌تردید شور و احساس، بخشی جدایی‌ناپذیر از فرهنگ عاشورایی است؛ اما اگر این شور از معرفت، فهم تاریخی و تأمل اخلاقی و دینی فاصله بگیرد، بخشی از ظرفیت تربیتی و فرهنگی عاشورا نیز کم‌رنگ خواهد شد. شاید یکی از نیازهای امروز، بازگشت دوباره به پیوند میان شور و شعور، احساس و معرفت و نیز توجه بیشتر به پیام‌های دینی، اخلاقی و انسانی عاشورا باشد.

سخن پایانی

عاشورا را نمی‌توان تنها در قالب یک مناسک مذهبی، یک خاطره تاریخی یا یک نماد سیاسی فهم کرد. عاشورا در عین حال روایتی از ایمان، اصلاح، اخلاق، مسئولیت و کرامت انسانی است. ماندگاری آن نیز از همین جامعیت سرچشمه می‌گیرد؛ از اینکه توانسته است در طول قرن‌ها، هم الهام‌بخش دینداری باشد، هم منبعی برای تأمل اخلاقی و هم پشتوانه‌ای برای همبستگی اجتماعی. از این منظر، محرم همچنان فرصتی برای بازاندیشی در نسبت ما با دین، اخلاق، جامعه و تاریخ است؛ فرصتی که هر نسل می‌تواند از دریچه نیازها و مسائل زمانه خود، بار دیگر به آن بازگردد و معنای تازه‌ای از آن بیابد.

دیپلماسی نفتی ایران در هند؛ فرصت بریکس برای بازگشت مقتدرانه به بازار جهانی نفت

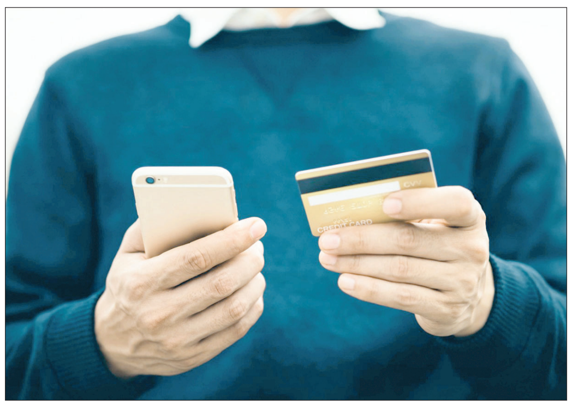
ادامه از صفحه اول

وزیر نفت همچنین با اشاره به آثار منفی تحریم‌ها و محدودیت‌های تجاری بر بازار جهانی انرژی، بر مسئولیت مشترک اعضای بریکس در حفظ ثبات بازار و تضمین امنیت عرضه و تقاضا تأکید و پیشنهاد «مشارکت امنیت انرژی بریکس» را مطرح کرد. این پیشنهاد، در صورت پیگیری، می‌تواند به ایجاد سازوکارهای مشترک برای تبادل اطلاعات بازار، توسعه سرمایه‌گذاری‌های انرژی، حفاظت از زیرساخت‌های حیاتی و افزایش تاب‌آوری زنجیره تأمین در میان اعضا منجر شود؛ اقدامی که هم به سود تولیدکنندگان و هم به سود مصرف‌کنندگان خواهد بود. واقعیت آن است که بهره‌گیری از این فرصت نیازمند صنعت نفتی آماده، توانمند و برخوردار از ظرفیت‌های فنی، مهندسی و مدیریتی است؛ ظرفیتی که صنعت نفت ایران با وجود سال‌ها تحریم و فشار خارجی، آن را حفظ کرده و در بسیاری از حوزه‌ها ارتقا داده است. این توان داخلی، پشتوانه اصلی دیپلماسی نفتی کشور برای حضور مؤثر در فضای جدید همکاری‌های بین‌المللی خواهد بود.

در نهایت، اجلاس انرژی بریکس در هند را می‌توان آغاز مرحله‌ای تازه در دیپلماسی نفتی جمهوری اسلامی ایران دانست؛ مرحله‌ای که در آن، رایزنی‌های دوجانبه با قدرت‌های بزرگ تولیدکننده و مصرف‌کننده انرژی، در کنار بهره‌گیری از ظرفیت‌های نهادمند بریکس، به ابزارهایی مکمل برای تقویت جایگاه ایران در بازار جهانی نفت تبدیل می‌شوند. در این چارچوب، دیپلماسی نفتی ایران می‌تواند به‌عنوان یکی از مهم‌ترین اضلاع دیپلماسی کلان جمهوری اسلامی ایران در عصر پساجنگ، نقشی تعیین‌کننده در توسعه همکاری‌های اقتصادی، ارتقای جایگاه بین‌المللی کشور و تأمین پایدار منافع ملی در نظم نوین انرژی جهان ایفا کند.

«شرق» در گزارشی علت افزایش حملات سایبری به سیستم بانکی کشور را بررسی می‌کند:

چرخه بی‌پایان هک بانکی



سونیتا سراب‌پور: ازکارافتادن کارت بانکی و سرویس‌های اینترنتی برخی بانک‌ها حداقل از دو سال گذشته به یک روتین طبیعی برای شهروندان تبدیل شده است. هکر یا گروهی از هکرها که آخر هم مشخص نمی‌شود از کجا آمده‌اند، سیستم بانکی کشور را هدف حملات سایبری قرار می‌دهند و مسئولان بانکی و رگولاتور بازار هم فقط از مردم می‌خواهند صبوری کرده و اخبار را از مراجع رسمی دنبال کنند. در نهایت هم بعد از چند روز و حتی چند هفته، بدون توضیح روشن درباره علت حادثه، میزان خسارت، نقاط آسیب‌پذیر و حتی یک عذرخواهی رسمی بابت نقض حقوق مشتریان مشکل برطرف می‌شود. از خرداد ۱۴۰۴ که حمله سایبری به بانک سپه و سپس پاسارگاد بخشی از خدمات بانکی کشور را مختل کرد تا خرداد ۱۴۰۵ که بانک‌های ملی، صادرات، تجارت و توسعه صادرات بار دیگر هدف حملات سایبری قرار گرفتند، یک پرسش بی‌پاسخ مانده است؛ چرا شبکه بانکی ایران هر چند ماه یک بار از کار می‌افتد اما هیچ‌گاه گزارشی شفاف درباره علت حمله، میزان خسارت و مسئولیت نهادهای متولی منتشر نمی‌شود؟ در این میان تنها چیزی که تکرار می‌شود صف مقابل شعب بانک‌ها، کارت‌های بانکی از کار افتاده و درخواست همیشگی مسئولان از مردم برای «صبوری» است.

داستانی که پیوسته تکرار می‌شود

اختلال و حملات سایبری به سیستم بانکی کشور اتفاق جدیدی نیست، اما آنچه در هفته‌های اخیر رخ داده از منظر نوع اتفاق و اطلاع‌رسانی از موارد عجیب است. هنوز مشخص نیست این حملات از داخل است یا خارج از کشور، هیچ گروه هکری مسئولیت انجام این حملات را نپذیرفته و هنوز مشخص نیست چرا در حالی که مقامات دولتی و بانک‌ها خبر از حل مشکل می‌دهند، اما هفته‌هاست که مردم برای خرید نان مشکل دارند، نمی‌توانند کرایه تاکسی‌شان را پرداخت کنند و انتقال یا دریافت وجه نیز همچنان با مشکل مواجه است. اواسط خرداد ۱۴۰۵ بود که خبر آمد شبکه بانکی کشور مورد حمله قرار گرفته و همین امر باعث شده زیرساخت‌های بانک‌های ملی، صادرات، توسعه صادرات و تجارت از کار بیفتد. خودپردازها، اینترنت‌بانک، موبایل‌بانک و بخشی از تراکنش‌های بانکی برای ساعت‌ها و در برخی موارد روزها از دسترس خارج شدند. شورای هماهنگی بانک‌ها و شرکت خدمات انفورماتیک که زیرساخت این بانک‌ها را تأمین می‌کند وقوع حملات سایبری را تأیید کردند اما مانند دفعات قبل تأکید داشتند که اطلاعات مشتریان در امنیت کامل قرار دارد. هنوز خدمات این چهار بانک به چرخه عادی ارائه خدمات باز نگشته بود که دوم تیر و پیش از شروع تعطیلات، خبر رسید که اختلالی گسترده در سطح شبکه بانکی کشور رخ داده و خدمات مبتنی بر کارت با مشکل جدی مواجه شده است. در این اتفاق هم بانک‌های ملی، صادرات و تجارت بیشتر از همه با اختلال روبه‌رو شدند. همان زمان شرکت ملی خدمات انفورماتیک در اطلاعیه‌ای در کنار درخواست صبوری از مردم توضیح داد: «این اختلال‌ها با هدف جلوگیری از دسترسی غیرمجاز و حفاظت از امنیت اطلاعات و دارایی‌های مشتریان، توسط شرکت خدمات انفورماتیک اعمال شده بود». در گام بعدی هم فرماندهی سایبری کشور اعلام کرد اختلال در خدمات کارت‌محور بانک‌های ملی، صادرات و تجارت در پی یک حمله سایبری هدفمند رخ داده است.

ساعت‌هاست که شرکت خدمات انفورماتیک اعلام کرده مشکل برطرف شده و خدمات این بانک‌ها برگشته‌اند اما بسیاری از کاربران در شبکه‌های اجتماعی اعلام می‌کنند که در هنگام خرید یا انتقال وجه با مشکل مواجه هستند. این نخستین بار نیست که شبکه بانکی ایران در برابر حملات سایبری آسیب‌پذیر نشان می‌داد. یک سال قبل و در میانه جنگ ۱۲ روزه ایران و اسرائیل، بانک سپه هدف حمله‌ای قرار گرفت که اختلال گسترده‌ای در خدمات غیرحضوری آن ایجاد کرد. ساعاتی بعد گروه هکری «گنجشک درنده» مسئولیت حمله را بر عهده گرفت و مدعی شد بخشی از زیرساخت‌های بانک را از بین برده است. تنها یک روز بعد نام بانک پاسارگاد نیز به فهرست قربانیان اضافه شد. دولت وقوع حمله به هر دو بانک را تأیید کرد و گفت آسیبی به اطلاعات مردم وارد نشده است؛ هرچند بازگشت کامل خدمات در برخی بخش‌ها روزها و حتی هفته‌ها زمان برد.

وقتی ارتباطی با دنیا نیست

اما اگر فقط رخدادهای دو سال اخیر در حوزه بانکی را کنار هم قرار دهیم، تصویری نگران‌کننده شکل می‌گیرد؛ تصویری از زیرساختی که هر بار با نامی تازه و روایتی متفاوت دچار اختلال می‌شود اما هیچ‌گاه گزارش فنی شفافی درباره علت اختلال و ازکارافتادن سرویس‌های بانکی منتشر نمی‌شود. نه مشخص است مهاجمان از چه مسیرهایی وارد شده‌اند، نه معلوم می‌شود چه آسیب‌هایی به سامانه‌ها وارد شده و نه نهادی مسئولیت مستقیم خسارت‌های واردشده به مشتریان را بر عهده می‌گیرد. در بسیاری از کشورهای جهان، پس از وقوع حمله سایبری به زیرساخت‌های مالی، بانک‌ها موظف‌اند جزئیاتی از حادثه، دامنه نفوذ، مدت اختلال، تعداد کاربران آسیب‌دیده و اقدامات اصلاحی را منتشر کنند. اما در ایران اغلب اطلاع‌رسانی‌ها به چند جمله کوتاه محدود می‌شود؛ جملاتی که معمولا با این عبارت آغاز می‌شوند: «خدمات هدفمند سایبری به زیرساخت‌ها صورت گرفته و اقدامات لازم در حال انجام است یا انجام شده است». به باور کارشناسان همین فقدان شفافیت باعث شده است هر حمله سایبری، علاوه بر خسارت عملیاتی، هزینه‌ای پنهان نیز به‌همراه داشته باشد: فرسایش اعتماد عمومی. اعتمادی که مهم‌ترین سرمایه هر نظام بانکی است و ازدست‌رفتن آن می‌تواند بسیار پرهزینه‌تر از چند ساعت یا چند روز اختلال در سرویس‌ها باشد. نیما امیرشکاری، فعال حوزه بانکداری الکترونیکی و کارشناس اقتصاد دیجیتال، در گفت‌وگو با «شرق» اعلام می‌کند که مسئله اصلی از نگاه او نه این حمله‌های اخیر، بلکه ریشه‌های تکرار چنین حملاتی است. او می‌گوید اگر بخواهد علت تکرار مدام حملات سایبری به زیرساخت‌های بانکی کشور را در یک عبارت خلاصه کند، «ضعف ارتباط با دنیا» است.

امیرشکاری معتقد است سیستم‌های زیرساختی برخی از بانک‌های کشور بسیار قدیمی و در مواردی ازکارافتاده شده‌اند: «بخش قابل توجهی از زیرساخت‌های بانکی ایران به حدود سه دهه قبل بازمی‌گردد. سامانه‌هایی که نه‌تنها در داخل کشور توسعه داده نشده‌اند، بلکه سال‌ها پیش از شرکت‌های خارجی خریداری شده و در طول زمان عمدتا فقط ظرفیت سخت‌افزاری آنها افزایش یافته است. تعداد پردازنده‌ها بیشتر شده، فضای ذخیره‌سازی افزایش یافته و تجهیزات جدیدی به آنها اضافه شده است، اما مغز نرم‌افزاری این سامانه‌ها همان چیزی است که سال‌ها قبل طراحی شده بود». به باور او سامانه‌ای که سال‌ها به‌روزرسانی نشود، وصله‌های امنیتی را دریافت نکند و تغییرات لازم روی آن اعمال نشود، به مرور به هدفی قابل پیش‌بینی برای مهاجمان سایبری تبدیل می‌شود: «زمانی که مهاجم بداند یک سامانه سال‌هاست تغییر نکرده، احتمال موفقیت حمله افزایش پیدا می‌کند». او با اشاره به تفاوت نوع کار بانک‌های ایرانی با بانک‌های خارجی می‌گوید: «تفاوت اصلی میان بانک‌های ایرانی و بانک‌های فعال در شبکه مالی جهانی دقیقا همین‌جاست. بانک‌های دنیا به‌طور مستمر مجبور به تطبیق با استانداردهای جدید هستند؛ از شیوه‌های اعتبارسنجی تا مدل‌های اعطای تسهیلات، امنیت اطلاعات و الزامات فنی. اگر بانکی خود را با این استانداردها هماهنگ نکند، به‌تدریج از رقابت حذف می‌شود. اما در ایران چنین فشاری وجود ندارد. بانک‌ها عمدتا در یک محیط بسته فعالیت می‌کنند و تنها الزام جدی آنها بخشنامه‌های داخلی ناکارآمد است. نتیجه نیز روشن است؛ نوسازی به یک انتخاب تبدیل می‌شود، نه یک ضرورت». امیرشکاری تأکید می‌کند که مشکل آسیب‌پذیری زیرساخت‌های بانکی کشور فقط نبود زیرساخت‌های به‌روز نیست: «مشکل فقط تجهیزات نیست. حتی بهترین تجهیزات دنیا نیز بدون پیکربندی صحیح و دانش فنی کافی امنیت لازم را نخواهند داشت. یکی از چالش‌های جدی ما این است که در بسیاری از موارد، تجهیزات خریداری می‌شوند اما دانش لازم برای تنظیمات پیشرفته امنیتی، سازگاری با محیط عملیاتی و مقاوم‌سازی آنها به اندازه کافی وجود ندارد».

او ادامه می‌دهد: «این کمبود دانش زمانی بیشتر خود را نشان می‌دهد که حادثه‌ای رخ می‌دهد. در روزهای ابتدایی حمله اخیر، پیشنهاد استفاده از مشاوران خارجی برای کمک به عارضه‌یابی و رفع مشکل مطرح شد. اما در عمل موانع متعددی وجود داشت؛ از محدودیت‌های سفر و شرایط جنگی تا حساسیت‌های امنیتی درباره حضور متخصصان خارجی یا حتی ارائه دسترسی از راه دور برای بررسی سامانه‌ها. نتیجه این می‌شود که بسیاری از ظرفیت‌هایی که می‌توانند به حل سریع‌تر بحران کمک کنند، عملا قابل استفاده نیستند». امیرشکاری اعلام می‌کند که شاید مهم‌ترین مسئله، فراتر از فناوری و تجهیزات، به شیوه حکمرانی بازگردد. آن‌طور که او می‌گوید، در سال‌های اخیر توازن میان نگاه نظارتی و توسعه به تدریج به هم خورده است: «در هر کشوری میان این دو مفهوم نوعی تعادل برقرار می‌شود. نه توسعه بدون امنیت امکان‌پذیر است و نه امنیت بدون توسعه پایدار می‌ماند. اما زمانی که کفه امنیت بیش از حد سنگین شود، تصمیم‌گیری‌های تخصصی نیز تحت تأثیر قرار می‌گیرند. امروز بسیاری از مدیران ترجیح می‌دهند به سامانه‌ای که در حال کار است، دست نزنند. نه به این دلیل که تغییر لازم نیست، بلکه به این دلیل که هزینه تصمیم‌گیری و ریسک تغییر بیش از حد بالا رفته است. مدیری که بخواهد یک تحول جدی ایجاد کند، ممکن است با انواع تفسیرها، سوءظن‌ها و فشارها مواجه شود. بنابراین راه کم‌هزینه‌تر این است که هیچ تغییری انجام نشود».

مدیرانی که تمایل به اطلاع‌رسانی ندارند

در حالی که روایت رسمی درباره اختلال اخیر بانک‌ها همچنان در ابهام قرار دارد، یک نکته بیش از هر چیز خودنمایی می‌کند؛ اینکه نظام بانکی ایران با وجود تجربه مکرر حملات سایبری، هنوز نتوانسته میان سرمایه‌گذاری روی تجهیزات، توسعه دانش تخصصی و پاسخ‌گویی عمومی تعادل برقرار کند. سعید سوزنگر، کارشناس امنیت، معتقد است ریشه بخش مهمی از این آسیب‌پذیری نه در کمبود فناوری، بلکه در ضعف امنیتی، بی‌توجهی به سرمایه انسانی و نبود سازوکارهای الزام‌آور برای پاسخ‌گویی نهفته است. سوزنگر در پاسخ به این پرسش که چرا سیستم بانکی کشور تا این اندازه مورد حمله قرار می‌گیرد، به «شرق» می‌گوید که در این زمینه چند دلیل عمده وجود دارد: «نخست اینکه به دلیل تحریم‌ها، امکان استفاده از بسیاری از ابزارهای به‌روز و استانداردهای جهانی امنیت سایبری را نداریم. دوم اینکه محدودیت‌های اینترنتی و فیلترینگ باعث شده بخشی از پروتکل‌ها و سازوکارهای امنیتی به شکل مطلوب مورد استفاده قرار نگیرند. عامل سوم نیز به ساختار اداری کشور بازمی‌گردد؛ ساختاری که در آن شرایط لازم برای استفاده حداکثری از دانش متخصصان امنیت در سازمان‌ها و بانک‌ها فراهم نشده است». او ادامه می‌دهد: «مشکل دقیقا از همین نقطه آغاز می‌شود. بسیاری از سازمان‌ها حاضرند هزینه‌های سنگین برای خرید تجهیزات و سخت‌افزارهای گران‌قیمت پرداخت کنند، اما حاضر نیستند همان میزان سرمایه‌گذاری را برای نیروی انسانی انجام دهند. نتیجه چنین رویکردی کاملا مشخص است؛ تجهیزات پیشرفته در اختیار داریم، اما دانش استفاده حداکثری از آنها یا دانش بهره‌برداری صحیح از ظرفیت‌هایشان را نداریم. حتی در مواردی که این دانش وجود دارد نیز انگیزه کافی برای استفاده از آن فراهم نشده است». به باور او در چنین شرایطی طبیعی است که متخصصان به همان سطح حداقلی از بهره‌برداری بسنده کنند. سوزنگر یکی دیگر از مشکلات در این زمینه را ضعف در اطلاع‌رسانی عمومی می‌دانند و اینکه نه نهاد ناظر بانکی و نه بانک خود را ملزم به پاسخ‌گویی در زمان اختلالات به دلیل حمله سایبری نمی‌دانند. او با اشاره به نبود اسناد بالادستی مؤثر برای صیانت از حقوق کاربران، می‌گوید: «در شرایط فعلی، بانک‌ها و کسب‌وکارها در بسیاری از موارد الزام جدی برای پاسخ‌گویی عمومی ندارند. همین مسئله باعث شده حملات سایبری به تدریج به پدیده‌ای عادی تبدیل شوند. البته در همه جای دنیا هک اتفاق می‌افتد، اما تفاوت در نحوه مواجهه با آن است. در بسیاری از کشورها، زمانی که یک سازمان دچار حادثه امنیتی می‌شود، موظف است به‌صورت مستمر و شفاف ذی‌نفعان و مشتریان خود را در جریان قرار دهد». این کارشناس امنیتی معتقد است تجربه حملات سایبری اخیر به بانک‌ها نشان می‌دهد اساسا در سیستم بانکی کشور، مدیران نیازی به پاسخ‌گویی نمی‌بینند و تمایلی به پذیرش مسئولیت یا اطلاع‌رسانی شفاف ندارند. او توضیح می‌دهد: «این در حالی است که وقتی سازمانی بابت نشت اطلاعات یا ضعف امنیتی با جریمه، مسئولیت حقوقی یا هزینه‌های مشخص مواجه نشود، انگیزه چندانی برای سرمایه‌گذاری بیشتر در حوزه امنیت نخواهد داشت. وقتی هزینه بی‌توجهی به امنیت پایین باشد، طبیعی است که اصلاح سیاست‌ها، افزایش بودجه امنیتی یا به‌روزرسانی فرایندهای آموزشی نیز در اولویت قرار نگیرد».

آیا اتصال به اینترنت باعث حملات سایبری می‌شود؟

با وجود اعلام بانک مرکزی و شرکت خدمات انفورماتیک مبنی بر حل مشکل ارائه خدمات به دنبال حمله یا حملات سایبری، اما طبق بررسی‌های میدانی و گزارش کاربران، این اختلال‌ها همچنان پابرجاست. پیگیری «شرق» از بانک مرکزی و شرکت خدمات انفورماتیک برای دریافت توضیحاتی در مورد این حمله تا لحظه انتشار این گزارش به نتیجه‌ای نرسیده است. این دو نهاد اعلام می‌کنند همچنان کارشناسان امنیتی و پلیس فتا در حال بررسی ابعاد موضوع هستند. در این بین، برخی با سرزنش اتصال اینترنت، اعلام می‌کنند که اگر اینترنت وصل نشده بود، این اتفاق نمی‌افتاد. برای نمونه امیر سیاح، معاون اقتصادی و تنظیم مقررات مرکز ملی فضای مجازی، در توییتی انتقادی در شبکه ایکس (توییتر سابق) نوشت: «یک ماه پیش، متخصصان امنیت سایبری هشدار می‌دادند زیر حملات شدید هستیم اینترنت بین‌الملل را باز نکنید، با روش‌های بی‌خطری می‌توان نیاز عموم به اینترنت بین‌الملل را تأمین کرد. وزیر ارتباطات به جای توجه، به نصیحت‌کننده‌ها توهین کرد. حالا که مردم گرفتار شده‌اند، کجاست بیاید جواب مردم را بدهد؟». در مقابل این نظر از سوی یک مقام فعال در حوزه فناوری، بهزاد اکبری، معاون وزیر ارتباطات و مدیرعامل شرکت ارتباطات زیرساخت، در توییتی این موضوع را فاقد پشتوانه فنی و غیرکارشناسی دانست. اکبری در توییت خود تأکید کرده بود: «سامانه‌های Core Banking این بانک‌ها و شرکت ارائه‌کننده خدمات به آنها اصلا به اینترنت عمومی متصل نیستند و سایر سامانه‌هایشان نیز «ایران‌اکسس» هستند».

اما شاید سؤال اصلی این باشد که آیا قطع اینترنت می‌تواند به افزایش حملات سایبری و کاهش امنیت سیستم‌ها کمک کند؟ سعید سوزنگر در پاسخ به این پرسش نظر نسبتا مثبتی دارد. او توضیح می‌دهد: «پاسخ این پرسش هم بله است و هم خیر. از یک سو، محدودیت‌های اینترنتی می‌تواند فرصت به‌روزرسانی بسیاری از سامانه‌ها را از بین ببرد و همین مسئله یکی از عوامل افزایش آسیب‌پذیری باشد. از سوی دیگر، برخی سناریوهای فنی دیگر نیز ممکن است مطرح باشند که بدون اطلاعات دقیق نمی‌توان درباره آنها با قطعیت اظهارنظر کرد». به باور او، اینکه صرف اتصال به اینترنت عامل اصلی حادثه بوده، از منظر فنی توضیح قابل قبولی نیست و نمی‌توان علت اصلی چنین حملاتی را بدون بررسی دقیق توضیح داد. او تأکید می‌کند که امنیت سایبری تنها با خرید تجهیزات حاصل نمی‌شود: «امنیت محصول ترکیبی از دانش، آموزش، نیروی انسانی متخصص، شفافیت، پاسخ‌گویی و سرمایه‌گذاری مستمر است. تا زمانی که این اجزا در کنار هم قرار نگیرند، تکرار چنین حوادثی چندان دور از انتظار نخواهد بود». بانکداری دیجیتال در سال‌های اخیر از یک ابزار کمکی، به ستون‌فقرات اقتصاد روزمره مردم تبدیل شده است؛ از خریدهای خرد تا جابه‌جایی‌های کلان، از دریافت حقوق تا پرداخت قبوض، همه چیز به زیرساخت‌هایی گره خورده که انتظار می‌رود در شرایط عادی و بحران، حداقل سطحی از پایداری را حفظ کنند. بااین‌حال، هر بار که شبکه بانکی از دسترس خارج می‌شود، مسئله فقط توقف چند سرویس نیست، بلکه زیرساختی حیاتی از کار می‌افتد که عملا روی زندگی روزمره میلیون‌ها نفر سایه انداخته است. مسئله زمانی پیچیده‌تر می‌شود که این اختلال‌ها نه به‌عنوان رخدادهای استثنائی، بلکه به‌عنوان اتفاقاتی تکرارشونده دیده می‌شوند؛ بدون گزارش‌های فنی شفاف، بدون اعلام دقیق دامنه آسیب و بدون پاسخ روشن درباره اینکه چه چیزی دقیقا از کار افتاده است و چرا؟ در چنین شرایطی، هر بحران جدیدی تنها ادامه همان چرخه قدیمی است: قطع سرویس‌ها، سردرگمی کاربران، اطلاعیه‌های کوتاه و کلی و بازگشت تدریجی خدمات بدون توضیحی درباره آنچه واقعا رخ داده است. به باور کارشناسان، تا زمانی که سازوکار شفاف گزارش‌دهی حین بحران و پس از بحران شکل نگیرد، مسئولیت‌ها دقیق تعریف نشود و پاسخ‌گویی جایگزین روایت‌های کلی و تکراری نشود، احتمال تکرار این اتفاق‌ها همچنان بالاست؛ اتفاق‌هایی آشنا که در آن کارت‌ها کار نمی‌کنند، کاربران نمی‌توانند از خدمات استفاده کنند و در نهایت تنها جمله‌ای که باقی می‌ماند همان عبارت تکراری است: «مشکل در حال پیگیری است، صبور باشید».

رخدادهای سایبری در سیستم بانکی که از سال ۱۴۰۰ تا تیر ۱۴۰۵ رخ داده است

تاریخ	بانک/موسسه	رخداد	وضعیت
بهمن ۱۴۰۰	ملی	نشت اطلاعات مشتریان	تکذیب بانک
بهمن ۱۴۰۱	سامانه‌های شتاب و شاپرک	اختلال شبکه و انجام نشدن تراکنش‌ها	حمله سایبری تکذیب شد
مرداد ۱۴۰۳	چند بانک و مؤسسه مالی	رسانه‌های خارجی از یک حمله سایبری گسترده به شبکه بانکی و مالی ایران خبر دادند. گزارش‌ها از اختلال در برخی خدمات بانکی و پرداخت سخن می‌گفتند اما جزئیات رسمی منتشر نشد	تأیید نشد
۲۷ خرداد ۱۴۰۴	بانک سپه	حمله سایبری گسترده به سامانه‌ها توسط گروه گنجشک پرنده	تأیید شد
۲۸ خرداد ۱۴۰۴	بانک پاسارگاد	سخنگوی دولت اعلام کرد دو بانک سپه و پاسارگاد هدف حمله سایبری قرار گرفته‌اند اما به اطلاعات مشتریان آسیبی وارد نشده است	تأیید شد
۲۴ خرداد	بانک ملی ایران، بانک صادرات ایران، بانک تجارت و بانک توسعه صادرات ایران	شورای هماهنگی بانک‌ها از حمله سایبری به زیرساخت ارتباطی مشترک چند بانک خبر داد. طبق اعلام رسمی داده‌های مشتریان آسیب ندید اما برخی خدمات مختل شد.	تأیید شد
۲تیر	بانک ملی، صادرات و تجارت	شرکت خدمات انفورماتیک اعلام کرد حمله سایبری باعث اختلال در سرویس‌های مبتنی بر کارت این بانک‌ها شده و خدماتی مانند خودپرداز، کارت‌خوان و موبایل‌بانک موقتاً متوقف شده‌اند.	تأیید شد

کتابخانه

وقتی ماشین‌ها درباره آینده تصمیم می‌گیرند

اگرچه ظهور هوش مصنوعی در سال‌های نخست بیشتر با شگفتی و هیجان همراه بود، اما خیلی زود روی دیگر این فناوری نیز خود را نشان داد؛ رویی که پرسش‌های جدی درباره آینده انسان، قدرت، امنیت و حتی ماهیت آگاهی مطرح می‌کند. کتاب «عصر هوش مصنوعی و آینده بشریت» تلاشی است برای ترسیم تصویری جامع از جهانی که به‌سرعت در حال تغییر است؛ جهانی که در آن فرصت‌ها و تهدیدهای هوش مصنوعی به‌طور هم‌زمان در برابر بشر قرار گرفته‌اند. نویسندگان کتاب معتقدند همان‌گونه که رنسانس، عصر روشنگری و انقلاب صنعتی مسیر تاریخ بشر را دگرگون کردند، اکنون نیز در آستانه ورود به دوره‌ای تازه قرار داریم؛ دوره‌ای که آن را «عصر هوش مصنوعی» می‌نامند. به باور آنها، این تحول به معنای پایان عصرهای پیشین نیست، بلکه آغاز مرحله‌ای جدید در تکامل تمدن انسانی است؛ مرحله‌ای که در آن ماشین‌ها نه‌تنها ابزار انجام کارها، بلکه بخشی از فرایند تصمیم‌گیری و تولید دانش خواهند بود. کتاب نشان می‌دهد که هوش مصنوعی می‌تواند تقریبا همه ابعاد زندگی انسان را تحت تأثیر قرار دهد؛ از آموزش، پژوهش و تجارت تا روابط اجتماعی، نظام‌های سیاسی، امنیت ملی، جنگ و دیپلماسی. در نگاه نخست، چنین تحولی می‌تواند نویدبخش افزایش رفاه، بهره‌وری و حل بسیاری از مشکلات پیچیده بشری باشد. با این حال، نویسندگان هشدار می‌دهند که سرعت پیشرفت این فناوری از سرعت درک ما از پیامدهای آن بیشتر است و همین مسئله می‌تواند به چالشی بزرگ برای جوامع تبدیل شود. بخش مهمی از کتاب به مخاطرات و پیامدهای ناخواسته هوش مصنوعی اختصاص دارد؛ از گسترش اطلاعات نادرست و تولید انبوه محتوای جعلی در زمان انتخابات و بحران‌های سیاسی تا جمع‌آوری گسترده داده‌های شخصی، تحلیل و پیش‌بینی رفتار شهروندان، نظارت نامحسوس دولت‌ها بر افراد و توسعه سامانه‌های تسلیحاتی خودکار. موضوعاتی که امروز دیگر صرفا فرضیه‌های علمی - تخیلی نیستند و نمونه‌هایی از آنها در نقاط مختلف جهان قابل مشاهده است. نویسندگان در ادامه پرسشی بنیادین را مطرح می‌کنند: آیا انسان همچنان تنها موجود دارای توانایی تصمیم‌گیری پیچیده، قضاوت اخلاقی و شکل‌دهی به آینده خواهد بود؟ یا اینکه با توسعه سامانه‌های هوشمند، بخشی از این جایگاه تاریخی به فناوری واگذار می‌شود؟ آنها پاسخ قطعی به این پرسش نمی‌دهند، اما تأکید می‌کنند که ندانسته‌های ما درباره هوش مصنوعی همچنان بیش از دانسته‌هایمان است؛ واقعیتی که دولت‌ها، سیاست‌گذاران، پژوهشگران و شهروندان را ناگزیر می‌کند با دقت بیشتری به آینده این فناوری بنگرند. «عصر هوش مصنوعی و آینده بشریت» حاصل همکاری سه چهره شناخته‌شده است: Henry Kissinger، دیپلمات و نظریه‌پرداز روابط بین‌الملل؛ Eric Schmidt، مدیرعامل پیشین گوگل؛ و Daniel Huttenlocher، پژوهشگر علوم رایانه. این کتاب در سال ۲۰۲۱ منتشر شد و تلاش می‌کند از منظر سیاست، فناوری و فلسفه به یکی از مهم‌ترین تحولات قرن بیست‌ویکم بپردازد. کتاب در هفت فصل تنظیم شده است: «کجا هستیم و چگونه به اینجا رسیدیم»، «فناوری و اندیشه بشر»، «شبکه جهانی پلتفرم‌ها»، «امنیت و نظم جهانی»، «از ماشین تورینگ تا اکنون و فراتر از اکنون»، «هوش مصنوعی و هویت انسانی» و «هوش مصنوعی و آینده». مجموعه‌ای از مباحث که خواننده را با فرصت‌ها، چالش‌ها و پرسش‌های بنیادین عصر هوش مصنوعی آشنا می‌کند.