یادداشت

در سال پرچالش آموزشی جنگی

آیا شهریه مدارس قابل مطالبه است؟

حمیدرضا آقابابائیان، وکیل پایه‌یک دادگستری: سال تحصیلی جاری، سالی است که در تاریخ نظام آموزشی ایران با بحران‌های بی‌سابقه شناخته می‌شود. تلاقی بحران‌های محیطی (آلودگی هوا)، اقلیمی (سرمای زودهنگام) و از همه مهم‌تر، بحران‌های امنیتی و نظامی ناشی از تنش‌های منطقه‌ای، تقویم آموزشی کشور را با تعطیلی‌های پیاپی مواجه کرده است. در این میان، مدارس غیردولتی و مراکز آموزشی با چالش بزرگی مواجه شده‌اند؛ از یک سو آموزش حضوری ماه‌ها متوقف شده و جای خود را به آموزش مجازی داده است و از سوی دیگر، خانواده‌ها همچنان با مطالبه شهریه کامل مواجه هستند. این تضاد میان «توقف خدمات» و «تداوم دریافت هزینه‌ها»، یک چالش حقوقی و اقتصادی جدی ایجاد کرده که نیازمند تبیین دقیق براساسقوانین جاری کشور است.

تحلیل بر پایه قانون مدنی؛ شکست اصل معاوضه

رابطه میان مدرسه و ولی دانش‌آموز، در نگاه حقوقی یک «قرارداد معاوضه» است؛ به این معنا که «آموزش» عوض «شهریه» است. وقتی یکی از این دو طرف از کارکرد خود باز می‌ایستد، قرارداد دچار اختلال می‌شود.

۱- استناد به «امر قهری» (Force Majeure): طبق ماده ۲۲۴ قانون مدنی، اگر اجرای تعهد به دلیل حادثه‌ای خارج از اراده طرفین (مانند جنگ یا بلایای طبیعی) غیرممکن شود، متعهد از اجرای تعهد آزاد است. در زمان جنگ یا تعطیلی‌های اجباری، مدرسه «توانایی اجرای تعهد» خود را از دست داده است. از آنجا که در حقوق، «هیچ عوضی در برابر عوضی وجود ندارد»، مطالبه شهریه برای زمانی که خدماتی ارائه نشده، فاقد وجاهت قانونی است. همچنین ماده ۲۲۵ قانون مدنی تصریح دارد که اگر عدم اجرای تعهد ناشی از حادثه‌ای باشد که طرفین در آن تقصیری ندارند، متعهد نمی‌تواند خسارتی (یا در اینجا شهریه‌ای) مطالبه کند.

۲- مفهوم «استحاله قرارداد»: وقتی ماهیت خدمت تغییر می‌کند (مثلا از حضوری به مجازی)، قرارداد از نظر عملیاتی دچار استحاله می‌شود. در این حالت، قرارداد اولیه از نظر اعتبار اجرائی برای مطالبه مبلغ کامل، از بین می‌رود. همچنین باید اصل «عدم جواز ثروت بدون کار» را مدنظر داشت؛ هیچ نهادی نمی‌تواند بدون ارائه خدمات واقعی، ثروتی را از دیگری تحصیل کند.

نگاهی به الگوی قانون کار؛ تعلیق در برابر مطالبه

اگرچه رابطه مدرسه و دانش‌آموز مستقیم تحت قانون کار نیست، اما قواعد این قانون، الگوی مناسبی برای تحلیل «رابطه خدمات‌دهنده و خدمات‌گیرنده» در شرایط اضطراری است. طبق قواعد مستخلص از مواد ۱۵ و ۳۰ قانون کار، اگر فعالیت یک واحد اقتصادی به دلیل حوادث غیرقابل پیش‌بینی (مانند جنگ) متوقف شود، رابطه قراردادی به حالت «تعلیق» درمی‌آید. در دوران تعلیق، حقوق و تکالیف طرفین (پرداخت دستمزد یا شهریه) متوقف می‌شود تا زمانی که شرایط برای فعالیت عادی فراهم شود.

رویه قضائی و نظریات مشورتی؛ از کرونا تا امروز

نظریات مشورتی اداره حقوقی قوه قضائیه در موارد مشابه (مانند دوران پاندمی کرونا) بسیار روشن است. قوه قضائیه تأکید دارد که اگر اجرای تعهد به دلیل شرایط خارجی دچار استحاله شود، طرفین نمی‌توانند به‌صورت یک‌جانبه براساس قرارداد اولیه، تعهدات خود را مطالبه کنند. رویه محاکم در دوران کرونا نیز نشان داد که اگر آموزش از حالت «حضوری» به «مجازی» تغییر یابد، شهریه نباید ثابت بماند؛ زیرا «هزینه تولید خدمت» و «ماهیت خدمت» تغییر کرده است. بنابراین، مطالبه شهریه کامل در زمان تعطیلی یا تغییر ماهیت خدمت، برخلاف رویه قضائی است.

نتیجه‌گیری و پیشنهاد راهکار: پیشگیری از بحران قضائی

با استناد به مواد ۲۲۴ و ۲۲۵ قانون مدنی و با توجه به رویه قضائی در مواجهه با فورس‌ماژور می‌توان نتیجه گرفت:

۱. شهریه آموزشی: در صورت تعطیلی مطلق، مدرسه حق دریافت شهریه را ندارد. در صورت آموزش مجازی، تنها حق دریافت «شهریه تعدیل‌شده» (متناسب با کاهش هزینه‌های عملیاتی و تغییر ماهیت خدمت) را دارد.

۲. سرویس مدارس: از آنجا که موضوع قرارداد (حمل‌ونقل) اصلا انجام نشده، مطالبه هزینه آن کلا فاقد وجاهت قانونی است.

در نهایت، شایسته است دولت نیز با معافیت مهدها و مدارس از مالیات و عوارض و پرداخت وام‌های بلندمدت کم‌بهره مدارس و مهدها را یاری کند. وزارت آموزش و پرورش با همکاری سازمان تعزیرات و قوه قضائیه، با تدوین بخش‌نامه‌ای جهت «کسر شهریه و هزینه‌های سرویس در دوران تعطیلی»، از بروز بحران بزرگ جلوگیری کند. مدارس نیز از طریق «اعاده مبالغ شهریه» یا «تهاتر با شهریه سال آینده» نسبت به برگرداندن شهریه‌های مازاد اقدام کنند. اتخاذ این تصمیم، نه‌تنها عدالت را میان خانواده‌ها و مدارس برقرار می‌کند، بلکه از سرازیرشدن سیل عظیم پرونده‌های حقوقی مدارس غیرانتفاعی و مهدی‌ها به محاکم دادگستری و ایجاد گره در سیستم قضائی پیشگیری خواهد کرد.

معاون وزیر ارتباطات به‌تازگی گفته اینترنت به خاطر حملات سایبری قطع شده است

اینترنت در سایه امنیت سایبری

سونیتا سراب‌پور: بیش از ۴۰ روز و هزار ساعت از قطع اینترنت در ایران می‌گذرد. حالا دیگر قطع اینترنت به اعدادی تبدیل شده‌اند که کش می‌آیند و فقط به شماره‌های‌شان اضافه می‌شود. هفته گذشته سخنگوی دولت مانند بیش از یک سال گذشته اعلام کرد: «دولت پیگیر دسترسی آزاد به اینترنت است، اما شرایط جنگی است». در این ۴۴ روز گذشته از قطعی اینترنت یکی از دلایل اصلی این تصمیم، به صورت غیرمستقیم جلوگیری از ارسال عکس و ویدئو از مکان‌های مورد حمله دشمنان و به خطر افتادن امنیت بیشتر مکان‌ها و افراد اعلام شده است؛ اما به‌تازگی مشخص شده این تصمیم دلیل دیگری هم دارد. براساس روایت معاون سیاست‌گذاری وزارت ارتباطات که شب بیست‌ویکم فروردین‌ماه به صداوسیما رفته بود، گویا دلیل اصلی قطعی اینترنت جلوگیری از «حملات سایبری» است. احسان چیت‌ساز با حضور در یک برنامه تلویزیونی گفته است: «بخشی از محدودیت در ارتباطات بین‌الملل، ناشی از نگرانی درباره حملات سایبری بود که درعین‌حال، به حفظ پایداری ارتباطات داخلی کمک کرد». به‌جز این اظهارنظر، هفدهم فروردین هم چیت‌ساز در یک اظهارنظر دیگر اعلام کرده بود: «با اتصال مجدد به ارتباطات بین‌المللی، شبکه کشور در معرض حجم بالایی از حملات سایبری قرار می‌گیرد و لازم است برنامه‌ای دقیق برای صیانت از داده‌های حساس کشور طراحی و اجرا شود». این اظهارات یک مقام رسمی در وزارت ارتباطات روی آنتن زنده تلویزیونی در حالی مطرح می‌شود که در بیش از یک دهه گذشته مقامات مختلف ایران از وزیران ارتباطات گرفته تا رئیس سازمان پدافند غیرعامل و نمایندگان مجلس و... بارها از تقویت و توسعه توان دفاع سایبری کشور، توسعه شبکه ملی اطلاعات و کارکرد مثبت سامانه‌هایی بومی مانند «دژفا» به‌عنوان سپر امنیتی فضای مجازی سخن گفته‌اند. اگرچه کارشناسان در گفت‌وگو با «شرق» قطع اینترنت به بهانه برقراری امنیت سایبری را رد می‌کنند و با ارائه داده‌های قابل اتکا تأکید می‌کنند که قطع اینترنت امنیت سایبری را بیشتر به خطر می‌اندازد، اما سؤال اصلی این است که اگر اینترنت برای برقراری امنیت سایبری قطع شده است، چطور برخی مسئولان به دنبال ارائه اینترنت پرو سازمانی و شخصی از طریق اپراتورهای ارتباطی کشور هستند؟

سامانه و طرح‌هایی که فقط نام‌شان مانده

تیرماه سال ۱۳۹۸ بود که برخی رسانه‌های آمریکایی اعلام کردند حملات سایبری علیه ایران از سوی آمریکا انجام شده و توانسته‌اند سیستم‌های کامپیوتری کنترل حملات موشکی و راکتی سپاه پاسداران را با موفقیت از کار بیندازند. همان زمان این خبر از سوی جمهوری اسلامی تکذیب شد و محمدجواد آذری‌جهرمی، وزیر ارتباطات دولت دوازدهم، در توییتی ضمن تأیید این حملات گفته بود که سامانه «دژفا» جلوی این حملات ایستاده؛ سامانه‌ای که چند ماه قبل یعنی ۲۷ اردیبهشت ۱۳۹۸ هم‌زمان با روز جهانی ارتباطات به شکل عمومی از آن رونمایی شد. آن زمان اعلام شده بود «دژفا» یک طرح امنیتی جامع از انواع سامانه‌های امنیتی است که بخش عظیمی از تهدیدات موجود در شبکه‌ها به‌ویژه شبکه ملی اطلاعات را شناسایی و با آن مقابله می‌کند. در آن زمان تأکید شده بود که این سامانه‌ها صرفا برای شناسایی و مقابله با تهدیدات شبکه ملی اطلاعات نیست و می‌تواند تهدیدات زیرساخت‌ها، محیط وب، غیر وب (تجهیزات)، تلفن همراه، تجهیزات حوزه صنعت و دیگر موارد را شناسایی کرده و با آنها مقابله کند. در مراسم رونمایی از «دژفا» جهرمی از ۳۰ برابر شدن توان دفاع سایبری کشور به کمک این سامانه خبر داده بود.

به‌جز این اظهارنظر، تاکنون خبرهای مختلفی از مقامات گوناگون وزارت ارتباطات از دولت‌های نهم تاکنون در مورد تقویت ساختار دفاع سایبری کشور شنیده شده است. از سامانه‌های بومی گوناگونی برای مقابله با حملات DDoS و تهدیدات زیرساختی رونمایی شده یا برخی مقامات سازمان پدافند غیرعامل گفته‌اند ایران در زمره قدرت‌های سایبری منطقه است و در برخی اظهارات، حتی از ایران به‌عنوان «یکی از قدرت‌های برتر سایبری جهان» یاد شده است. آنچه از این ادبیات در این سال‌ها برمی‌آید، این است که این زیرساخت‌ها قرار بود نقش «سپر چندلایه دفاع سایبری» را ایفا کنند؛ سپری که بتواند از زیرساخت‌های حیاتی در برابر حملات گسترده محافظت کند. حالا سؤال این است که چرا این سامانه‌ها و طرح‌های گوناگونی که برای دفاع از امنیت سایبری کشور با بودجه‌های میلیاردی توسعه داده شده‌اند، حالا نمی‌تواند با حملات سایبری مقابله کند تا اینترنت قطع نشود و به دنبال آن خسارت میلیاردی به مردم و کسب‌وکارها وارد نشود. برای دریافت جواب این سؤال بارها با وزارت ارتباطات تماس گرفتیم، اما تا لحظه نگارش این گزارش هیچ‌کدام از مسئولان این وزارتخانه پاسخ‌گو نبودند.

حملات سایبری که هر ثانیه بیشتر می‌شود

هنوز آمار رسمی از میزان حملات سایبری پس از جنگ ایران، اسرائیل و آمریکا که حالا در مرحله آتش‌بس قرار دارد، منتشر نشده، اما نهم دی‌ماه ۱۴۰۴ درست چند روز قبل از اینکه اینترنت در دی ۱۴۰۴ برای ۲۰ روز قطع شود، بهزاد اکبری، مدیرعامل شرکت ارتباطات زیرساخت، در توییتی خبر داد که توانسته‌اند یکی از بزرگ‌ترین حملات سایبری به زیرساخت‌های کشور را خنثی کنند. او در این توییت نوشت: «یکی از ۱۲ حمله بزرگ DDoS جهان را که بیش از ۷۲۰ میلیون بسته در ثانیه بود، خنثی کردیم». پیش‌تر از این اتفاق شرکت ارتباطات زیرساخت در گزارشی که مرداد گذشته منتشر کرد، خبر داد که در فصل

بهار ۱۴۰۴، میانگین حملات روزانه دوهزارو ۳۱۳ حمله بوده است. طبق این گزارش درگاه برخط خدمات عمومی و دولتی بیشترین مقاصد برای حمله سایبری بوده‌اند. مبدأ اصلی این حملات از ۱۰ کشور بوده که در رأس آنها مجارستان، آلمان و اسپانیا قرار داشتند. در نسخه دیگر همین گزارش در پاییز ۱۴۰۳ نیز نشان می‌داد که در این مدت میانگین حملات روزانه به زیرساخت‌های کشور ۶۳۵ مورد بوده، میانگین حجم حملات ۳۶.۴ گیگابایت بر ثانیه گزارش شده و مجموع حملات مقابله‌شده نیز ۵۷هزارو ۲۱۸ مورد بوده است. چهار دقیقه و ۳۷ ثانیه میانگین مدت‌زمانی است که برای این حمله‌ها اعلام شده است. طولانی‌ترین حمله انجام‌شده در پاییز امسال چهار روز و ۹ ساعت و ۵۰ دقیقه بوده است. با این وضعیت و آمارها شاید بیراه نباشد که معاون وزیر ارتباطات بگوید اینترنت به خاطر جلوگیری از حملات سایبری قطع شده است.

به دنبال یک پاسخ‌گو

فعالان صنفی و بخش خصوصی که سال‌ها در حوزه امنیت سایبری فعالیت می‌کنند، در مواجهه با این سؤال که آیا با وجود برنامه‌ها، قوانین، طرح‌ها، سامانه‌های مختلف، اختصاص بودجه‌های کلان و... با هدف توسعه امنیت سایبری کشور، باید برای جلوگیری از حملات سایبری اینترنت کشور قطع شود، پاسخی ندارند. آنها بر این باورند که مشکل کشور در بخش امنیت سایبری مدیریت غیراستاندارد است. یک فعال صنفی که تمایلی به اعلام نامش ندارد، در گفت‌وگو با «شرق» از «تناقض در سیاست‌گذاری سایبری»، انتقاد می‌کند؛ تناقضی که به گفته او، از یک سو به محدودسازی سراسری دسترسی انجامیده و از سوی دیگر، مسیرهای دسترسی به خرید فیلترشکن‌های میلیونی را همچنان باز گذاشته است. به گفته این فعال صنفی، تصور اینکه بتوان با راهکارهای ساده یا اقدامات مقطعی از بروز تهدیدات سایبری جلوگیری کرد، نگاهی ساده‌انگارانه است: «در حوزه سایبری، وجود آسیب‌پذیری یک امر قطعی است. حتی ممکن است در همین لحظه، نقاط ضعفی وجود داشته باشد که هنوز شناسایی نشده‌اند. اتفاقا نگرانی اصلی هم همین بخش‌های پنهان و ناشناخته است که ممکن است در شرایط بحرانی خود را نشان دهند». با این حال، او تأکید می‌کند آنچه امروز بیش از خود تهدیدات، محل نقد است، «نحوه مدیریت شرایط» است: «وقتی از استاندارد صحبت می‌کنیم، منظور استانداردهای مدیریت امنیت اطلاعات است؛ یعنی مدیریت بحران به‌گونه‌ای که کمترین آسیب وارد شود. در چنین شرایطی، حداقل انتظار بخش خصوصی این است که سطح مشخصی از دسترسی داشته باشد تا بتواند به‌روزرسانی انجام دهد، پشتیبانی ارائه کند و آسیب‌پذیری‌ها را شناسایی و برطرف کند. راه‌حل، قطع کامل دسترسی نیست». این فعال صنفی در ادامه به یکی از مهم‌ترین تناقض‌های موجود اشاره می‌کند: «از یک سو گفته می‌شود اینترنت به دلیل مسائل امنیتی محدود شده، اما از سوی دیگر، دسترسی از طریق برخی وی‌پی‌ان‌های پولی که رقم‌شان به میلیون‌ها تومان می‌رسد همچنان برقرار است. از سوی دیگر مسئولان از راه‌اندازی اینترنت پرو صحبت می‌کنند که به کسب‌وکارها و برخی افراد با دسترسی ویژه داده شود. اگر موضوع امنیت است، این تفاوت در دسترسی چگونه توجیه می‌شود؟ آیا تهدیدات سایبری با پرداخت هزینه برطرف می‌شوند؟». این فعال حوزه فناوری اطلاعات همچنین به محدودیت‌های فنی ایجادشده برای فعالان این حوزه اشاره می‌کند و می‌گوید: «در شرایط فعلی، بسیاری از اقدامات ضروری مانند به‌روزرسانی سیستم‌ها، اعمال پچ‌های امنیتی و بررسی آسیب‌پذیری‌ها با محدودیت مواجه شده است. این در حالی است که چنین اقداماتی، حداقل‌های مدیریت امنیت محسوب می‌شوند. پرسش اینجاست که چرا این دسترسی‌ها فراهم نمی‌شود؟». به گفته او، در بسیاری از کشورها ابزارهایی مانند «کلید قطع» (Kill Switch) وجود دارد، اما استفاده از آنها معمولا موقت، مدیریت‌شده و متناسب با سطح دسترسی گروه‌های مختلف است: «این‌طور نیست که دسترسی برای همه و به‌صورت طولانی‌مدت قطع شود، بلکه سیاست‌ها به‌گونه‌ای تنظیم می‌شوند که هم امنیت حفظ شود و هم خدمات حیاتی مختل نشود». این فعال صنفی با اشاره به ساختار تصمیم‌گیری در این حوزه، اعلام می‌کند: «بسیاری از تصمیمات در سطحی اتخاذ می‌شود که عملا امکان گفت‌وگوی مستقیم یا حتی اظهارنظر رسمی درباره آن برای فعالان این حوزه وجود ندارد. حتی افرادی که در بدنه فعالیت می‌کنند نیز در مواردی با این شرایط هم‌نظر هستند، اما سطح تصمیم‌گیری در جای دیگری است».

قطع اینترنت به امنیت سایبری کمک می‌کند؟

در حالی که گروهی در بدنه تصمیم‌گیر، دسترسی مردم و کسب‌وکارها را به اینترنت قطع کرده‌اند تا آن‌طور که می‌گویند امنیت در بخش سایبری حفظ شود، اما برخی مدیران و کارشناسان معتقدند قطع اینترنت نه‌تنها به ایجاد امنیت در فضای سایبری کمک نمی‌کند، بلکه شرایط را پیچیده‌تر خواهد کرد. محمدرضا مستمع، مدیرعامل شرکت شرکت راسپینا نت پارس، در گفت‌وگو با «شرق» تأکید می‌کند قطع اینترنت لزوما به جلوگیری از حملات سایبری کمک نمی‌کند. او با اشاره به نمونه‌های از سازمان‌ها و بانک‌هایی که در دوران قطع اینترنت هک شده‌اند، می‌گوید: «بانک سپه سال گذشته حداقل چهار بار هک شده است. یک بار در بهار ۱۴۰۳، یک بار در جنگ ۱۲روزه و یک بار هم در جنگ فعلی. در مقابل، این بانک هیچ‌وقت نه به مشتری خود و نه به نهاد ناظر پاسخ‌گو نبوده که علت هک چه بوده است. همین عدم پاسخ‌گویی باعث می‌شود سیستم توسعه امنیت سایبری کشور به‌درستی صورت نگیرد». آن‌طور که او می‌گوید در شرایط فعلی فقط یک نهاد تصمیم می‌گیرد و حتی بخش‌هایی که در این زمینه فعال شده‌اند تا به برقراری امنیت سایبری کمک کنند، ازجمله مرکز افتا از تصمیم‌گیری و اتفاقات باخبر نیستند. او در پاسخ به این سؤال که چرا با وجود بارها هشدار که قطع اینترنت راه‌حل مناسبی برای جلوگیری از اتفاقات نیست، دلیل این شرایط را نبود دانش تخصصی در سطح تصمیم‌گیری می‌داند و تصریح می‌کند: «واقع‌بینانه اگر نگاه کنیم، این تصمیم‌ها ناشی از کمبود دانش در این حوزه است. قبلا هم‌زمان شاهد رشد کسب‌وکارهایی بودیم و قطع کامل اینترنت، جز در موارد خاص مانند حوادث آبان ۹۸، اتفاق نیفتاد و این افراد سعی داشتند با تلاش و گفت‌وگو مستمر جلوی محدودیت‌ها را بگیرند». از سوی دیگر او در پاسخ به این پرسش که چرا اینترنت برای برقراری امنیت سایبری قطع می‌شود، اما از سوی دیگر صحبت از ارائه اینترنت پرو (اینترنت بدون فیلتر) می‌شود، این‌گونه توضیح می‌دهد: «این رویکرد نشان‌دهنده اولویت‌بندی نادرست است. مشخص است مشکل اینترنت نیست. در عمل، به نظر می‌رسد اولویت به فعالیت‌های خاص داده می‌شود، در حالی که کسب‌وکارهایی که بر بستر اینترنت شکل گرفته‌اند و می‌توانند ارزش‌آفرینی کنند، از دسترسی به اینترنت هنوز محروم هستند. به نظر می‌رسد تصمیم بر این است فعلا در این بازه عده‌ای که تأیید می‌شوند اینترنت داشته باشند». آن‌طور که او می‌گوید، با وجود این ادعا مبنی بر ارائه اینترنت بدون فیلتر به کسب‌وکارها، هنوز کسب‌وکارهای عضو سازمان نظام صنفی رایانه‌ای به اینترنت دسترسی ندارند و مشخص نیست واقعا اینترنت پرو قرار است به چه کسانی ارائه شود.

وقتی فقط اینترنت ما قطع می‌شود

اینترنت در حالی در ایران به دلایلی ازجمله جلوگیری از حملات سایبری ۴۴ روز قطع شده که کشورهای همسایه درگیر در جنگ ایران با اسرائیل و آمریکا یا اوکراینی که از سال ۲۰۲۲ با روسیه در جنگ است، اینترنت‌شان را حتی برای یک روز قطع نکردند. بررسی تجربه کشورهایی که در شرایط جنگ یا بحران امنیتی قرار دارند، الگوی متفاوتی از مدیریت اینترنت را نشان می‌دهد:

اوکراین: ● از سال ۲۰۲۲ درگیر جنگ با روسیه است. ● اینترنت سراسری هرگز قطع نشده. ● از استارلینک، کلاد و همکاری با شرکت‌های فناوری جهانی استفاده بهره برده. ● تمرکز بر «تاب‌آوری سایبری» به‌جای قطع ارتباطات بوده است

لبنان: ● با وجود حملات و تنش‌های امنیتی. ● قطع سراسری اینترنت گزارش نشده.

در مقابل این الگوها، در ایران در دوره‌های مختلف و به‌ویژه در بحران اخیر: ● اینترنت به‌صورت گسترده محدود یا قطع شده. ● ارتباطات بین‌الملل با اختلال جدی مواجه شده. ● و هم‌زمان، محدودیت‌های گزینشی نیز اعمال شده است.

این در حالی است که برخی گزارش‌ها نشان می‌دهد بخشی از کاهش حملات سایبری در دوره‌های خاص، ناشی از کاهش سطح اتصال به اینترنت جهانی بوده است.

شکاف روایت و واقعیت

آنچه از کنار هم قرار گرفتن اظهارات رسمی، داده‌های حملات و تجربه فعالان حوزه فناوری اطلاعات به دست می‌آید، یک شکاف روشن است: از یک سو، روایت رسمی بر «قدرت سایبری، دژفا و تاب‌آوری شبکه ملی اطلاعات» تأکید دارد و از سوی دیگر، در مواجهه با بحران، همچنان «قطع یا محدودسازی اینترنت» به‌عنوان ابزار اصلی مدیریت به کار گرفته می‌شود. مسئله اصلی در وضعیت فعلی اینترنت ایران، صرفا میزان حملات سایبری یا شدت تهدیدات نیست، بلکه نحوه مواجهه با این تهدیدات است. در حالی‌که جهان به سمت افزایش تاب‌آوری، همکاری بین‌المللی و حفظ اتصال در شرایط بحران حرکت کرده، تجربه ایران نشان می‌دهد هنوز «قطع ارتباط» یکی از اصلی‌ترین ابزارهای مدیریت بحران سایبری باقی مانده است. این شکاف میان «ادعای قدرت سایبری» و «وابستگی به محدودسازی ارتباطات»، نقطه‌ای است که به گفته فعالان این حوزه، اگر بازتعریف نشود، هر بحران جدید فقط آن را عمیق‌تر خواهد کرد.

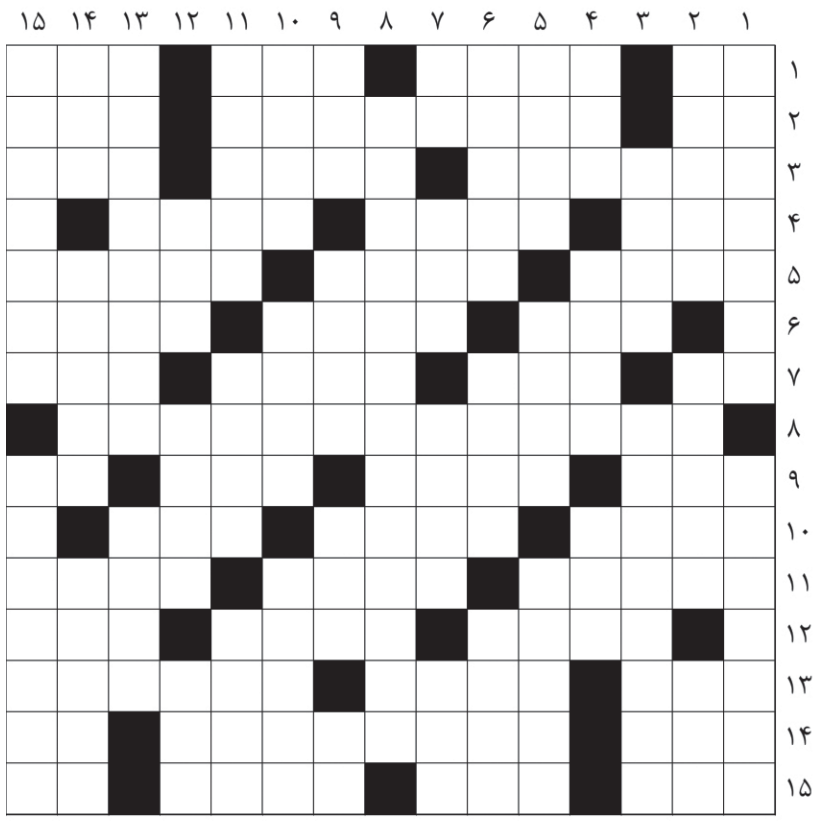
جدول ۵۲۹۱ طراح: بیژن گورانی

افقی:

۱- ستون بدن- از صفات خدا به معنی بسیار مهربان- شیشه آزمایشگاهی- مهره‌ای در شطرنج ۲- صدمه- معادل فارسی اختصار- نیم‌سال تحصیلی ۳- همگانی، عمومی- همراه پشتک- آموختنی لقمان حکیم ۴- بسیار گرم و سوزان- حساب و شمار- سنگواره ۵- خوراکی با تخم‌مرغ و گوجه‌فرنگی- ماهی تن- شادابی ۶- خریدوفروش- سالاد معروف ایتالیایی- ویتنام قدیم ۷- دریا- شهر بی‌قانون- تاوان‌گرفتن- خالی ۸- تابلوی نقاشی ونسان ون گوگ با موضوع بهار ۹- خلاف میل- خدای مصریان قدیم- خوشگذرانی- ضمیری عربی ۱۰- حضورداشتن- لگد- یاری‌دهنده ۱۱- رشته‌هایی از پوست گیاه- بخش جذاب خبر- معراج مؤمن است ۱۲- سهل- شیوه و روش- پاکیزه ۱۳- سوره مورچه- نویسنده فرانسوی کتاب قرارداد اجتماعی- تلاش‌کردن ۱۴- دایه- محصول کشاورزی سرشار از نشاسته- ضمیر غایب ۱۵- گوسفند قربانی- زاپاس- مثل این- تلخ

عمودی:

۱- حفاظت- سارق، دزد ۲- بزرگداشت- سرگرم- یاری و کمک ۳- بیشتر، اکثر- اثر معروف دانته، شاعر و نویسنده ایتالیایی ۴- سینمای سوخته آبادان- پرنده‌ای لذیذگوشت- آخرین سوره ۵- از القاب حضرت فاطمه(س)- عارفان- زبان رسمی ایرانیان ۶- بی‌همتا- افترا- مژده ۷- ابر و باد و... و خورشید و فلک درکارند- از قبایل قدیمی عرب- ویژگی‌های شخصیتی و فرهنگی فرد- کم‌وزن ۸- هر روزتان نوروز . ... ۹- پرچم- پیشرفته- جامه‌صاف‌کن- قسمتی از دست ۱۰- شریف‌تر- چهارم- یار ویس ۱۱- میانگین- روزه‌دار- سبز تیره ۱۲- چین‌وچروک پوست- خصم- اشاره به نزدیک ۱۳- از تیم‌های سری آ فوتبال ایتالیا- هم‌داستان کلیله ۱۴- گرم نیست- ترس و بیم- دست به کاری زدن ۱۵- نوعی جنگ‌افزار بسیار مرگبار که در هیروشیما و ناکازاکی به کار گرفته شد- بازاریاب

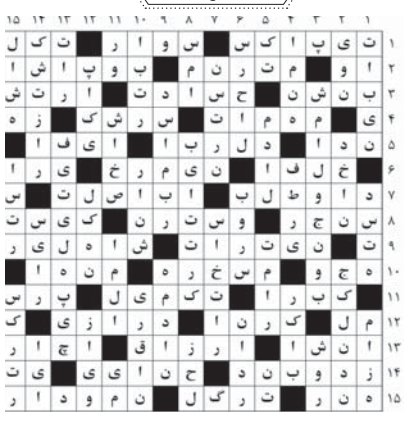


حل سودوکو ۴۲۸۶

۱	۵	۶	۲	۳	۴	۸	۷	۹
۹	۴	۸	۵	۱	۷	۳	۶	۲
۷	۳	۲	۶	۹	۸	۴	۵	۱
۳	۷	۵	۱	۴	۲	۶	۹	۸
۴	۲	۱	۸	۶	۹	۵	۳	۷
۸	۶	۹	۳	۷	۵	۱	۲	۴
۲	۱	۴	۹	۵	۳	۷	۸	۶
۵	۹	۷	۴	۸	۶	۲	۱	۳
۶	۸	۳	۷	۲	۱	۹	۴	۵

۹	۵	۱	۸	۲	۶	۴	۳	۷
۶	۸	۲	۳	۴	۷	۵	۱	۹
۳	۷	۴	۱	۵	۹	۶	۲	۸
۲	۶	۸	۴	۷	۵	۱	۹	۳
۱	۴	۵	۹	۳	۸	۲	۷	۶
۷	۳	۹	۲	۶	۱	۸	۴	۵
۴	۹	۳	۵	۸	۲	۷	۶	۱
۵	۲	۶	۷	۱	۳	۹	۸	۴
۸	۱	۷	۶	۹	۴	۳	۵	۲

حل جدول ۵۲۹۰



سودوکو سخت ۴۲۸۷

زمان پیشنهادی: ۴۰ دقیقه

قانون‌های حل جدول سودوکو

۱- در هر سطر و ستون باید اعداد یک تا ۹ نوشته شود. بدیهی است که هیچ عددی نباید تکرار شود.

۲- در هر مربع ۳×۳ اعداد یک تا ۹ باید نوشته شود و در نتیجه هیچ عددی نباید تکرار شود.

۱			۳					
	۲			۶	۴	۵	۷	
	۷	۵						۴
			۸			۲		
۹				۱				۶
		۲			۵			
۴						۳	۸	
	۵	۳	۹	۸			۴	
				۵				۲

سودوکو ساده ۴۲۸۷

زمان پیشنهادی: ۲۰ دقیقه

سودوکو

سودوکو Sudoku یک واژه ترکیبی ژاپنی به معنای عددهای بی‌تکرار است و امروزه به جدولی از اعداد گفته می‌شود که به عنوان یک سرگرمی رایج در نشریات کشورهای مختلف به چاپ می‌رسد.

		۹					۸	۶
	۷	۸	۵			۳		
۱				۴		۲		۵
		۴	۷		۲		۳	
۳	۹		۸		۵		۴	۱
	۶		۳		۴	۹		
۷		۱		۵				۳
		۵			۳	۱	۲	
۶	۸					۵		