شرایط اقتصادی در حال تغییر است

محسن رضایی، معاون اقتصادی رئیس جمهور در حاشیه اولین نشست مشترک با اعضای کمیسیون اقتصادی مجلس اظهار کرد: «در دولت برنامه‌ریزی‌هایی صورت گرفته تا صرفا به مسائل روزمره که بسیار مهم هم هستند، اکتفا نکنیم. این مسائل باید جدی برخورد شود، اما مسائل بنیادین و درازمدت هم اهمیت دارد.» وی عنوان کرد: «نکته اساسی‌ای که ما دنبال می‌کنیم، ابتدا ایجاد یکپارچگی میان مجلس، دولت، قوه قضاییه، بخش خصوصی و همه مردم است. همان‌طور که با یکپارچگی در انقلاب و دفاع مقدس پیروز شدیم، امروز برای حل مشکلات اقتصادی کشور و پیشرفت در مسائل اقتصادی نیاز به یکپارچگی داریم.» معاون اقتصادی رئیس جمهور تصریح کرد: «اول باید از دولت و مجلس این یکپارچگی را آغاز کنیم و بعد هم میان دولت و بخش خصوصی، همچنین دولت و همه آحاد جامعه آن را ادامه دهیم. حتی ایرانیان عزیز که در خارج هستند هم امروز دعوت می‌شوند تا سرمایه‌های فکری و مالی خود را وارد ایران کنند.»

سامانه سوخت هوشمند و پمپ‌بنزین‌های کشور روز ۴ آبان به دلیل حمله سایبری از دسترس خارج شد

عکس: میزان

بررسی ابعاد حقوقی حملات سایبری علیه کشورمان و امکان شکایت به نهادهای بین‌المللی

حق ایران برای حمله متقابل سایبری

مریم عاقلی

سیاسی

جنگ هکرها و نبرد هیبریدی این روزها دیگر به هیچ‌عنوان فقط در سطح دولت‌ها نیست و عملا قربانیان خود را در کف خیابان‌ها و از بین مردم می‌گیرد، شاید عینی‌ترین مصداق این نزاع اطلاعاتی-سایبری علیه کشورمان ۴ آبان باشد که با یک حمله گسترده هکری به شبکه هوشمند سوخت‌رسانی اتفاق افتاد و جایگاه‌های بنزین را در سالگرد حوادث آبان ۹۸ از پای درآورد و مردم را تحت‌فشار گذاشت. اگر در دهه ۸۰ هکرها با عظیم‌ترین و مخرب‌ترین حمله سایبری از ابتدای پیدایش این حوزه تاکنون یعنی استاکس‌نت، صنعت هسته‌ای ایران را نشانه گرفتند در سال‌های اخیر حملات سایبری به شبکه راه‌آهن، شبکه پلیس راهور و جایگاه سوخت، رسما زمین جنگ را تغییرداده و داده‌کاوی در این زمینه ما را به اطلاعات جالبی می‌رساند. اطلاعات موجود نشان می‌دهد از دوسال گذشته تاکنون حجم حملات سایبری به شکل فزاینده‌ای زیاده‌شده که این موضوع قطعا ناشی از نوع و بافت دشمنانی است که ایران دارد. این افزایش به گونه‌ای بوده که بدون اغراق ایران را جزو رکورددار این حملات کرده یعنی هم از جهت گستره و تکرار این اتفاق و هم از جهت عمق حملات سایبری، کشورمان یکی از قربانیان اصلی این نوع جنگ مدرن است.

شاید بتوانیم این حملات را در سه سطح دسته‌بندی کنیم؛ برخی از این حملات هکری به‌صورت فردی توسط اشخاص صورت می‌گیرد که این مدل از حملات و هک‌شدن ضریبی از اهمیت ندارد. در سطح دوم ما با جریانات و گروه‌هایی در داخل و خارج از کشور مواجه هستیم که برخی تهدیدات سایبری را علیه زیرساخت‌های فناوری کشورمان انجام می‌دهند اما در سطح سوم ما با یک جنگ تمام‌عیار سایبری مواجه هستیم که یک دولت رسمی مانند آمریکا یا رژیم صهیونیستی پشت آن قرار می‌گیرد و یکی از بارزترین و به‌روزترین حملات سطح سوم مثل همین ماجرای هک‌شدن شبکه هوشمند سوخت‌رسانی کشور بود که دامنه و دربرگیری وسیعی داشت و به همین دلیل دولت با تصمیم درست و به‌موقع، اطلاع‌رسانی دقیق و شفاف درباره ابعاد و سطح تخریب در این زمینه ارائه کرد.

نکته حساس در این ماجرا تشکیل سازمان پدافند غیرعامل با هدف مقابله با همین تهدیدات بوده که این روزها صحبت از کم‌اثرشدن اقدامات آن از همیشه جدی‌تر است درحالی که پدافند غیرعامل به معنای کاهش آسیب‌پذیری هنگام بحران بدون استفاده از اقدامات نظامی و صرفا با بهره‌گیری از فعالیت‌های فنی و مدیریتی است اما درست در ایام سالروز تشکیل آن کشور دچار یک حمله وسیع سایبری شد و جایگاه‌های بنزین کشور زیر ضرب قرار گرفت. تهدیداتی که باوجود برنامه‌ریزی و طراحی‌های خاص پدافند در برابر تهدیدات سایبری زنگ خطر را برای دولت به صدا درآورد و لزوم تقویت زیرساخت شبکه‌ها و امنیت سایبری را بیشتر از همیشه پررنگ کرد؛ چراکه قطعا حمله سایبری اخیر آخرین‌بار نبوده و بازهم ادامه خواهد داشت.

> حملات سایبری از نگاه دشمن مکمل تحریم‌هاست و در کنار تحریم سیستم اقتصادی هک کردن سیستم خدماتی و اطلاعاتی رضایت عمومی را مورد هدف قرار می‌دهد

تایید حمله سایبری توسط آمریکا و اسرائیل

هرچند به گفته سردار جلالی رئیس سازمان پدافند وقتی ما دو حادثه بندر شهید رجایی و راه آهن را تحلیل کردیم متوجه شدیم از نظر مدل حمله کاملا شباهت داشتند و از نظر ما طراحان و عوامل این حمله قطعا دشمنان ما یعنی آمریکا و رژیم صهیونیستی هستند. وقتی کسی می خواهد در لایه سخت افزار به شما حمله کند باید به لایه سیستم نهادینه‌شده در آن مجموعه نفوذ اطلاعاتی داشته باشد بنابراین کشورهایی که دارنده یا سازنده همان سیستم هستند یا افرادی هستند که بتوانند بعدا آن را به صورت فیزیکی ساخته و در سیستم گذاشته باشند. در این گزارش تلاش داریم تبیین کنیم که چرا حملات سایبری از نگاه دشمن به نوعی مکمل تحریم‌هاست و در کنار بخش‌هایی از سیستم اقتصادی که با تحریم زیر فشار قرار گرفته، با هک‌کردن سیستم خدماتی، امنیتی و اطلاعاتی هم تلاش می‌کند تا رضایت عمومی را مورد هدف قرار دهد و عملا با فلج‌کردن زیرساخت‌ها و اختلال در کارکرد آن اثر تحریم‌ها را تصاعدی بالا ببرد.

جنگ پلاس سایبری

اگر تا همین یکی دو دهه قبل اوج بحران‌سازی علیه کشورمان، شکل دادن به حلقه‌ها و تجمعات ضدامنیتی و هدایت افکار سیاسی در انتخابات یا جنگ اقتصادی و اطلاعاتی بود، اما این مدل جنگ‌های اصطلاحا نرم، سر و شکل جدیدی گرفته است. مراکز مطالعات استراتژیک در غرب از نوع جدیدی از جنگ به نام جنگ‌های هیبریدی یا ترکیبی نام می‌برند که نیروهای ایرانی را ملزم کرده تا با ابتکار عمل و تغییرات تاکتیکی در عرصه نبردهای نظامی و دیپلماتیک به دفاع هیبریدی روی بیاورند. کنفرانس امنیتی مونیخ در سال ۲۰۱۵، هشت ابزار اصلی دولت‌ها برای نبرد هیبریدی را دیپلماسی، جنگ اطلاعاتی و پروپاگاندا، حمایت از نابسامانی‌ها و شورش‌های محلی، نیروهای نامنظم و چریکی، نیروهای ویژه، نیروهای کلاسیک نظامی، جنگ اقتصادی و نهایتا حمله‌های سایبری عنوان کرد. درواقع ابزار جنگ ترکیبی یا هیبریدی از تحریم اقتصادی، جنگ سایبری، ترور، حمله نظامی، عملیات روانی توسط رسانه‌ها و فریب رهبران و نهادهای تصمیم‌ساز را شامل می‌شود.

پس می‌بینیم که ما با یک مجموعه کامل از آخرین متد عملیاتی مدرن مواجه هستیم که هم فردی همچون شهید فخری‌زاده را با جاسوسی سایبری ترور می‌کند و به شهادت می‌رساند و هم پروژه نفوذ را در سطح تصمیم‌گیران اصلی حوزه اقتصادی که داستان آن را در بلوای ارزی سال ۹۷ و محکومیت رئیس سابق بانک مرکزی دیدیم، پیش می‌برد، برای کشورمان هزینه می‌سازد و سازوکار تحریم اقتصادی چرخ‌های این جنگ را می‌چرخاند.

البته چون موضوع اصلی بحث ما جنگ سایبری است، خوب است این موضوع را به شکل دقیق‌تر بدانیم که حمله سایبری یکی از لایه‌های عملیات اطلاعاتی است؛ یعنی دشمن بعد از هدایت و مدیریت ادراکی رهبران کشور هدف، در وهله دوم سراغ زیرساخت اطلاعاتی آن کشور می‌آید؛ در این لایه که اغلب از آن به عنوان لایه ارتباطی با فضای سایبر نام می‌برند، حملات نرم‌افزارهای مخرب و هکرها به زیرساخت‌هایی مانند شبکه اینترنتی و داخلی سازمان‌ها، سامانه‌های پشتیبانی و مولدهای برق صورت می‌گیرد و لایه سوم هم در بستر فیزیکی شامل رایانه‌ها، سامانه‌های مخابراتی، تاسیسات و تجهیزات اتفاق می‌افتد که شاید بتوان ردپای آن را در خرابکاری تأسیسات هسته‌ای نطنز دنبال کرد.

سابقه حملات سایبری علیه ایران

در حالی که کارشناسان فضای مجازی بارها بر موضوع امنیت داده و تقویت زیرساخت‌های ارتباطی کشور تأکید کرده بودند، اما جمهوری اسلامی عملا یکی از دانشمندان برجسته هسته‌ای و دفاعی خود را به دلیل ضعف در این حوزه از دست داد، کما این‌که روزنامه نیویورک‌تایمز شهریورماه همین امسال جزئیاتی درباره عملیات ترور شهید فخری‌زاده توسط موساد را منتشر کرد که نشان می‌داد سلاح خودکار و کنترل از راه دور به‌کار رفته در این عملیات، با فناوری هوش مصنوعی ارتقایافته، صورت گرفته است.

نمونه دیگر ماجرای استاکس‌نت بود، بدافزاری ساخت آمریکا و اسرائیل که در سال ۱۳۸۹ تاسیسات هسته‌ای کشورمان ازجمله نیروگاه بوشهر را هدف قرار داد و ادوارد اسنودن، کارمند سابق سازمان سیا که اسناد زیادی را در رابطه با فعالیت‌های اطلاعاتی آمریکا افشا کرده بود، چندی بعد اعلام کرد این بدافزار با همکاری مشترک سازمان امنیت ملی آمریکا و اسرائیل ساخته شده، اتفاقی که هرچند نتوانست ضربه‌ای سهمگین به ساختار و شاکله هسته‌ای کشورمان وارد کند، اما پروژه غنی‌سازی اورانیوم را تا مدتی دچار اختلال کرد. این اتفاق از بزرگ‌ترین حملات سایبری علیه یک کشور هدف بود.

در سال ۱۳۹۱ هم دو بدافزار دیگر که در آن زمان یکی از پیچیده‌ترین برنامه‌های جاسوسی سایبری معرفی شدند، سیستم‌های نفتی و هسته‌ای کشورمان را مورد تهاجم قرار داد و در همان ایام وزارت نفت با تایید این موضوع، هدف این حمله را دزدی و تخریب اطلاعات عنوان کرد و حتی گفتند این ویروس، مادربرد رایانه‌ها را سوزانده و برای پاک کردن اطلاعات اقدام کرده است.

حمله با نسل جدید استاکس‌نت در سال ۱۳۹۷ هم مصداق دیگری از این جنگ سایبری است. سردار جلالی، رئیس سازمان پدافند غیرعامل گفت این حملات سایبری با استفاده از نسل جدید ویروس استاکس‌نت به چند بخش صورت گرفته و آذری جهرمی، وزیر وقت ارتباطات، هدف این حمله را صدمه زدن به زیرساخت‌های ارتباطی کشور اعلام کرد و از پیگیری آن در مجامع بین‌المللی خبر داد. این حملات سایبری سال ۱۳۹۷ با بخشی از تحریم‌های سنگین آمریکا علیه کشورمان همراه شد.

نمونه دیگر آن که همین اواخر اتفاق افتاد حمله سایبری به بندر شهید رجایی بود تا جایی که روزنامه واشنگتن‌پست آمریکا رسما این حمله را در اردیبهشت سال گذشته کار اسرائیل دانست. البته سال ۱۳۹۹ برای ایران از نظر حملات سایبری پرفشار بود؛ دو انفجار در تاسیسات هسته‌ای نطنز یکی در تیرماه پارسال و دومی در فروردین همین سال جاری و آتش‌سوزی در برخی نیروگاه‌های کشور هم به چنین خرابکاری‌هایی نسبت داده شد.

اتفاق دیگر در این جنگ سایبری هم هک شدن دوربین‌های اوین بود که مرداد امسال گروهی به نام عدالت علی با هک دوربین‌های مداربسته زندان اوین، تصاویری از برخورد خشن و غیرقانونی مسؤولان زندان با زندانیان منتشر کرد. این اتفاق گرچه توجهات را به نوع رفتار سیستم قضایی معطوف کرد و حتی موجب عذرخواهی مسؤولان زندان و وعده اصلاح این فرآیند به دلیل انتقادات اجتماعی بود، اما نفس وقوع این حمله هکری بار دیگر سطح آسیب‌پذیری بالای شبکه آی‌تی در برخی نهادهای مهم حکومتی را گوشزد کرد.

ناعادلانه بودن نظم نوین جهانی

اما در این جنگ نوین و مدرن که گستره و عمق زیادی هم دارد چه باید کرد؟ یکی از پاسخ‌های اصلی به این سوال، لزوم تقویت سیستم پدافند عامل و ارتقای امنیت سایبر است، چراکه خلا در این قضیه بدون رتوش خود را در ماجرای بنزین نشان داد، بنابراین باید با فاصله گرفتن از شعار و آمارسازی، این حوزه را جدی گرفت. اما اقدام مهم دیگری که می‌تواند دست ایران را در مواجهه با این حملات متعدد سایبری پر کند، بدون شک پیگیری حقوقی این موضوع در نهادهای بین‌المللی است. اساسا وقتی پمپ‌بنزین‌های کشور به عنوان یکی از حلقه‌های اصلی سیستم حمل‌ونقل روزمره مورد تهاجم گسترده قرار می‌گیرد و اتفاقا ایران هم می‌داند این موضوع از کجا ناشی شده چرا نباید آن را در سطح بین‌المللی و به صورت قضایی و حقوقی مورد پیگیری قرار داد؟

البته شاید بتوان گفت دلایلی مثل مشخص نبودن منشا دقیق این حمله یا سخت بودن اثبات چنین اتهامی در دادگاه بین‌المللی عامل عملی نشدن این راه‌حل تاکنون بوده است. به این نکته، این موضوع را هم اضافه کنید که عملا هیچ کنوانسیونی در سطح بین‌الملل برای پیگیری چنین شکایاتی وجود ندارد و دولت ایالات متحده آمریکا مانند حق وتو می‌خواهد این موضوع را هم در انحصار کشور خود نگه دارد. با وجود این نمی‌توان دست روی دست گذاشت و هیچ کار موثر جهانی نکرد. بدون شک پیگیری این فقره از حملات سایبری توسط دولت‌های مستقل نیازمند عملیاتی پیچیده و چند لایه است.

با تمام این اوصاف، یک گزاره برای ما قطعی است؛ ناعادلانه بودن نظم نوین جهانی. در واقع این موضوع مهم‌ترین درکی است که می‌توانیم از این معادله داشته باشیم، چون وقتی در چنین چشم‌اندازی در کنار گستره خطرناک جنگ‌های سایبری و اطلاعاتی با خلا وجود کنوانسیون‌های حقوقی برای رسیدگی قضایی در سطح بین‌الملل هم مواجه می‌شویم، مطمئن خواهیم شد این نظم نوین صرفا حقوق کشورهای غربی و آمریکای شمالی را مورد توجه قرار می‌دهد. از این رو در چنین مکانیسم ناعادلانه‌ای ما هیچ راهی جز ارتقای حقیقی و غیرشعاری سیستم‌های امنیتی، نظارتی، فنی و زیرساختی کشورمان نخواهیم داشت و راه‌های دیگر صرفا بیراهه است.

لزوم تشکیل مرجع بین‌المللی برای جرایم سایبری

طی دو سال گذشته حملات سایبری زیادی علیه سامانه‌های سیاسی، امنیتی و خدمات عمومی کشور صورت گرفته و خبرها حاکی از آن است که عمده این تجاوزات سایبری، به‌واسطه اقدامات کشورهای خارجی است. سوال اینجا است که جمهوری اسلامی ایران چگونه می‌تواند به‌خاطر این حملات سایبری، از حق و حقوق خود در مجامع بین‌الملل دفاع کند. دکتر علی زندی، استاد حقوق دانشگاه در همین ارتباط به روزنامه جام‌جم گفت: «این حملات در قانون ما در قالب تروریسم سایبری مطرح می‌شود. یعنی هر فرد یا نهادی باعث اختلال در سامانه‌های رایانه‌ای شود و خدمات عمومی مثل آب، برق، گاز، مخابرات، بانک‌ها و... را از کار بیندازد، به استناد ماده ۱۱ قانون جرایم رایانه‌ای کار و همچنین قانون مجازات اسلامی سال ۱۳۷۵، کار مجرمانه‌ای را مرتکب شده است.»

این استاد حقوق دانشگاه درباره این‌که جمهوری اسلامی ایران در صورت به‌دست آوردن مستنداتی مبنی بر دخالت یک کشور خارجی در حملات سایبری علیه منافع کشورمان، چگونه می‌تواند از طریق مجامع حقوقی بین‌المللی طرح شکایت و از حقوق ملت ایران دفاع کند، خاطرنشان کرد: «این مساله تابع قواعد حقوق بین‌المللی کیفری است. در این حوزه ما یک دیوان بین‌المللی کیفری (آی‌سی‌سی) داریم که مربوط به یک‌سری جرایم خاص مثل نسل‌کشی، جنایات جنگی و... است. سایبر گاهی موضوع ارتکاب جرم است و گاهی وسیله ارتکاب جرم. اگر موضوع سایبر به مصادیقی مثل نسل‌کشی یا جنایات جنگی مربوط باشد، دیوان بین‌المللی کیفری ممکن است به آن ورود کند و البته مشکلاتی هم در این زمینه وجود دارد. اگر موضوع مطالبه خسارت مدنی از عملکرد دولت‌ها مطرح باشد، این مساله را می‌توان از طریق دیوان لاهه پیگیری کرد. باز هم در این حوزه با این مساله مواجهیم که دولت‌ها از باب کیفری مصونیت دارند و از منظری حقوقی نهادی وجود ندارد تا با طرح شکایت از آن، بتوان دولتی را محاکمه کرد. ما البته کنوانسیونی با عنوان جرایم سایبر داریم که مربوط به سال ۲۰۰۱ است و از سال ۲۰۰۴ اجرایی شده، اما عمدتا مقررات آن توصیه‌ای است و ضمانت اجرایی ندارد.»

وی با اشاره به مشکلاتی که بر سر راه پیگیری حقوقی ایران برای شکایت از حملات سایبری وجود دارد، تصریح کرد: «واقعیت آن است همچنان باید در این زمینه منتظر بود تا دولت‌ها متحد شوند تا صلاحیت دیوان کیفری بین‌المللی را گسترده‌تر کنند یا این‌که مرجع بین‌المللی برای جرایم رایانه‌ای بنیان نهند.»

وی با اشاره به این‌که این هك سامانه‌های سوخت، هشداری برای ارتش سایبری ما بود تاکید کرد: «امروز جنگ در دنیا صرفا محدود به جنگ نظامی نیست، بلکه در فضای سایبر هم رخ می‌دهد و باید زمینه پیشگیری و مراقبت جدی از سامانه‌های رایانه‌ای در داخل کشور صورت بگیرد و مسؤولان به تقویت زیرساخت‌ها و بهینه‌سازی در عرصه نرم‌افزار بپردازند. باید جلوی نفوذ در این عرصه را از همان ابتدا گرفت، چون ضربه و زیانی که از این حوزه وارد می‌شود، قابل قیاس با تلفات و صدمات فیزیکی نیست. نفوذکنندگان در فضای سایبر، ناشناس و گمنامند. در این فضا احساس امنیت می‌کنند و به طور معمول دستگیری عوامل مرتکب این جرم، سخت‌تر صورت می‌گیرد. بنابراین برای برخورد با آنها باید مجهزتر بود.»

یادداشت شفاهی

حق مشروع اقدام متقابل

الهام امین‌زاده

کارشناس حقوق بین‌الملل

جمهوری اسلامی ایران طی سال‌های گذشته در معرض حملات سایبری زیادی قرار داشته است و طبعا اثبات این‌که این تجاوزات رایانه‌ای از طرف چه کسانی، نهادی یا کشوری صورت گرفته به عهده مراجع قضایی و امنیتی است. البته برخی از کشورهایی که علیه ایران اقدام به تجاوزات سایبری کردند ابایی از اعلام آن ندارند. در چند مورد مقامات رژیم صهیونیستی اعلام کردند نسبت به ایران اقدامات ایذایی انجام دادند و از این پس هم به این روند ادامه خواهند داد. این ادعاها به نوعی اعتراف به حملات سایبری علیه ایران از سوی رژیم صهیونیستی محسوب می‌شود و این دخالت، منافع مردم را دچار اختلال کرده است. طبعا به لحاظ حقوقی باید جمهوری اسلامی ایران در مجامع بین‌المللی نسبت به این عمل اعتراض کند. اولین اقدام بازدارنده که ایران در حوزه بین‌الملل می‌تواند انجام دهد اقدام متقابل علیه تروریست‌ها و متجاوزان سایبری است. به این معنا که حملات و فعالیت‌های سایبری که از منظر بین‌المللی قابل پذیرش نیست، اقدام متقابل علیه آن مجاز شناخته می‌شود. مستندات قانونی هم در این زمینه وجود دارد. طرح مسؤولیت بین‌المللی دولت‌ها در سال ۲۰۰۱، اقدام متقابل را برای کشورها به رسمیت شناخته است البته در چنین مواردی موضوعات حقوق بشری هم باید مورد لحاظ قرار گیرد. یعنی اگر یک مرکز نظامی یا علمی که در آن کشور تجاوزگر وجود دارد می‌تواند مورد اقدام و حمله سایبری متقابل قرار گیرد. بخشی از تلاش‌های ایران برای احقاق حقوق خود هم به سازمان‌ها و مجامع بین‌المللی بر می‌گردد با این توضیح که به طور معمول این سازمان و نهادهای بین‌المللی به نوع تحت تاثیر سیاست‌های دوگانه قرار دارند و در مقابل کشورهای قدرتمند هم به صورت مرعوبانه‌ای رفتار می‌کنند. بنابراین چندان امیدی به این مجامع نیست اما برای ثبت در اسناد بین‌المللی جمهوری اسلامی حتما باید این اقدامات را در مجمع عمومی سازمان ملل متحد و شورای حقوق بشر سازمان ملل و در شورای امنیت به عنوان شکایت اعلام کند. به‌ویژه این‌که ایران می‌تواند در شورای حقوق بشر سازمان ملل اعلام کند این حملات سایبری موجب اخلال در آسایش مردم شده و حمل و نقل عمومی را مورد هدف قرار داده است. بنابراین همه این اقدامات در نقض اعلامیه جهانی حقوق بشر است و ایران باید درخواست محکومیت اقدامات کشورهای متجاوز سایبری را ارائه دهد. البته این نکته را نباید از نظر دور داشت که علاوه بر اقدام متقابل علیه متجاوزان سایبری و همچنین ثبت شکایت از کشورهایی که در حوزه تروریسم سایبری عمل می‌کنند رویکرد موثرتری را می‌تواند در پیش بگیرد. در حال حاضر مهم‌ترین اقدام برای پیشگیری از تجاوزات و تروریسم سایبری، تقویت زیرساخت‌های داخلی در حوزه نرم‌افزار و فضای سایبری است.

«ماتوانستیم» به فرهنگ جدید تبدیل شده است

امیرسرتیپ علیرضا صباحی‌فرد، فرمانده نیروی پدافند هوایی ارتش در ارتباط برخط با فرماندهان مناطق و گروه‌های پدافندی با اشاره به ذکاوت، هوشیاری و موفقیت چشمگیر پدافند هوایی ارتش در به‌کارگیری عملیاتی انواع سامانه‌های راداری و موشکی در رزمایشات اخیر این نیرو بیان کرد: امروز پدافند هوایی ارتش با خودباوری و تکیه بر دانش و توان بومی به مرحله‌ای از بالندگی و صلابت رسیده است که در منطقه و جهان حرف‌های بسیاری برای گفتن دارد.

امیر سرتیپ صباحی‌فرد با تاکید بر این‌که در رزمایشات اخیر نیروی پدافند تنها گوشه‌ای از توانمندی موشکی این نیرو مورد ارزیابی عملیاتی قرار گرفت، افزود: پدافند هوایی ارتش با وجود اعمال تحریم‌های ظالمانه و ناجوانمردانه علیه کشورمان توانسته است در تمامی زمینه‌های راداری، موشکی، پهپادی و سایبری رشد بسیار چشمگیر و قابل‌قبولی داشته باشد.