«مردم سالاری» بررسی می کند

آسیب‌پذیری سایبری ایران

سجاد عابدی

پدافند غیرعامل به معنای کاهش آسیب‌پذیری در هنگام بحران، بدون استفاده از اقدامات نظامی و صرفا با بهره‌گیری از فعالیت‌های غیرنظامی، فنی و مدیریتی است. اما در کشور ما بیشتر به عنوان یک سپر در راستای ناکارآمدی مدیریتی در حوزه دفاعی است.

تنها هفت سال پس از دستور برای مقابله با تهدیدات سایبری، یک بدافزار زنگ خطر را در ایران به صدا درآورد. استاکس‌نت (Stuxnet) بدافزار ساخت دولت‌های آمریکا و اسرائیل در سال ۱۳۸۹ تاسیسات هسته‌ای ایران از جمله نیروگاه بوشهر را هدف قرار داد. وبسایت خبری «یاهو نیوز» در گزارشی مفصل بعدها افشا کرد هدف از این عملیات که «بازی‌های المپیک» نامگذاری شده بود، تخریب برنامه اتمی ایران نبود؛ مهاجمان در تلاش بودند با این حمله در برنامه هسته‌ای کشور وقفه بیندازند تا فرصت لازم برای تلاش‌های دیپلماتیک ایجاد شود.

ادوارد اسنودن، کارمند سابق سازمان اطلاعات مرکزی آمریکا که اسناد زیادی را در رابطه با فعالیت‌های اطلاعاتی آمریکا افشا کرده است، در مصاحبه‌ای با اشپیگل گفته بود این بدافزار با همکاری مشترک آژانس امنیت ملی ایالات متحده آمریکا و اسرائیل ساخته شده است.

کارشناسان آژانس بین‌المللی انرژی اتمی اما در آن زمان گزارش دادند شمار قابل اعتنایی از سانتریفیوژهای تاسیسات نطنز آلوده و معیوب شده و در نتیجه غنی‌سازی اورانیوم را با اختلال مواجه کرده است. گمان می‌رفت این ویروس نخستین‌بار، دستی وارد سیستم‌های کامپیوتری ایران شده باشد. چند ماه بعد از کشف استاکس‌نت یک وبسایت اسرائیلی گفت که ایران ممکن است چندین کارگر نطنز را دستگیر و اعدام کرده باشد با این گمان که به آلوده کردن دستگاه‌ها به استاکس نت کمک کرده باشند.

مسئولان کشور بعدها اعلام کردند این ویروس در نهایت نتوانست ضربه سهمگینی به ساختارهای اتمی ایران وارد کند. اما گزارش‌ها تایید می‌کرد که دست‌کم سی هزار کامپیوتر و هزار سانتریفیوژ آلوده شدند. با این حال پیچیدگی و گستردگی این حمله به حدی بود که زنگ خطر را برای مقامات ایرانی به صدا در آورد و بنابر گزارش‌ها، ایران سرمایه‌گذاری زیادی در زمینه حملات سایبری کرد.

با توجه به توضیحات فوق، مصوبات شورای عالی فضای مجازی درخصوص شبکه ملی اطلاعات، بر لزوم ایجاد شبکه‌ای امن تاکید دارد. به طوری که در الزامات مربوط به ایجاد این شبکه، بر تحقق شبکه‌ای کاملاً مستقل و حفاظت شده نسبت به دیگر شبکه‌ها (از جمله اینترنت) با قابلیت عرضه انواع خدمات امن، اعم از رمزنگاری و امضای دیجیتالی به تمامی کاربران و نیز شبکه‌ای با قابلیت برقراری ارتباطات امن و پایدار میان دستگاه‌ها و مراکز حیاتی کشور، تاکید شده است.

در اصول حاکم بر شبکه ملی اطلاعات نیز موضوع سالم‌سازی و امنیت مورد توجه قرار گرفته است و حتی در حوزه خدمات این شبکه نیز خدمات سالم‌سازی و امنیت مورد نیاز زیرساخت فضای مجازی کشور و پشتیبانی از سالم‌سازی و امنیت لایه‌های بالایی خدمات کاربردی و محتوا که شامل خدمات زیرساخت سالم‌سازی و امنیت و خدمات مدیریت و عملیات امنیت می‌شود، الزام شده است.

وضعیت ایران در امنیت سایبری ضعیف است

با وجود تعاریف مشخصی که برای امنیت سایبری در شبکه ملی اطلاعات تکلیف شده است و با وجود مبلغ ۱۹ هزار میلیارد تومان که گفته می‌شود برای زیرساختهای این شبکه هزینه شده، اما وضعیت مقابله با تهدیدات سایبری، حفاظت از اطلاعات و مدیریت مخاطرات و صیانت از حریم خصوصی افراد هنوز تضمین و مشخص نیست.

برای مثال نشت اطلاعات و افشای پایگاه اطلاعات هویتی کاربران بسیاری از سازمان‌ها، اپراتورها، شرکت‌های دولتی و خصوصی در فضای مجازی طی ماه‌های اخیر از موضوعات خبرساز بوده و به دلیل نبود قوانین مشخص و راهکارهای امنیتی، بسیاری از این اطلاعات در فضای مجازی خرید و فروش می‌شوند.

کارشناسان معتقدند که نبود نظام حاکمیت سایبری در کشور، اتفاقاتی از نوع نشت اطلاعات و سرقت داده‌ها را رقم می‌زند. البته برخی نیز معتقدند که تهدیدات سایبری در حد و اندازه‌های مختلف از جمله به نشت پایگاه‌های اطلاعاتی، سرقت داده و یا تهدیداتی از نوع نفوذ به حریم خصوصی افراد در فضای مجازی در همه جای دنیا اتفاق می‌افتد و تنها مختص ایران نیست، اما با این وجود گزارش‌ها نشان می‌دهد که جایگاه جهانی ایران در این حوزه قابل دفاع نیست.

براساس گزارشی که مرکز پژوهش‌های مجلس منتشر کرده است، وضعیت ایران در مقایسه با سایر کشورهای جهان در زمینه حفظ حریم خصوصی کاربران در فضای مجازی، «بسیار ضعیف» ارزیابی شده است.

در این راستا این سوال مطرح می‌شود که آیا ضعف ساختارهای امنیتی کشور در فضای سایبری به ضعف زیرساخت‌های شبکه ملی اطلاعات باز می‌گردد؟ و چرا با وجود اینکه مسئولان بر تحقق ۸۰ درصدی شبکه ملی اطلاعات تاکید دارند، این تکلیف شبکه ملی اطلاعات به درستی کارساز نیست. سوال دیگر این است که مصوبه شورای عالی فضای مجازی درخصوص امنیت و حریم خصوصی چطور اجرایی شده است و سالم سازی و امنیت به عنوان اصول حاکم بر طراحی شبکه ملی اطلاعات در چه وضعیتی قرار دارد؟ این سوال نیز مطرح می‌شود که با وجود کارآمد بودن شبکه ملی اطلاعات، مشکل نشت اطلاعات از کجا است و مسئولیت افشای اطلاعات پایگاه‌های داده را چه نهادی برعهده می‌گیرد.

جای خالی یک مرکز فرماندهی امنیت سایبری

مطابق با آنچه که در «نظام ملی پیشگیری و مقابله با حوادث فضای مجازی»، در شورای عالی فضای مجازی به تصویب رسیده، مسئولیت هر دستگاهی در مقابله با حوادث فضای مجازی مشخص است. برای مثال طبق این مصوبه، حوادثی که در حوزه عمومی به وقوع می‌پیوندد، توسط نیروی انتظامی مورد رسیدگی قرار خواهد گرفت و حوادثی که در سازمان‌ها رخ می‌دهد از طریق وزارت ارتباطات و فناوری اطلاعات باید رسیدگی شود. مسئولیت جمع‌آوری ادله دیجیتال در جرایم عمومی فضای مجازی نیز به عهده نیروی انتظامی و مسئولیت جمع آوری ادله دیجیتال تخلفات اداری در سازمان‌ها به عهده سازمان حراست کل کشور است.

در این مصوبه همه دستگاه‌ها موظفند که با حوادث فضای مجازی دستگاه مربوط به خود مقابله کنند و به نوعی ناگزیر به حفاظت از پایگاه‌های داده خود هستند. اما به نظر می‌رسد این قانون پاسخگوی همه نیازها نیست و جای یک مرکز فرماندهی و تصمیم‌گیری برای امنیت در حوزه حاکمیت سایبری خالی است؛ به نحوی که ناامنی پایگاه داده بسیاری از سازمان‌ها و عدم پاسخگویی به ضرر و زیان‌های ناشی از نشت این اطلاعات طی ماه‌های اخیر، شاهد روشنی بر این ادعا است.

سردار باقری، معاون فناوری اطلاعات سازمان پدافند غیرعامل در مراسم صدور گواهی امنیتی محصولات بومی حوزه فناوری اطلاعات گفت که با وجود اینکه تفکیک کار در حوزه امنیت سایبری در سازمان فناوری اطلاعات، مرکز افتای ریاست جمهوری و پدافند سایبری صورت گرفته اما وضعیت امنیت در دستگاه‌ها و نهادهای حاکمیتی مناسب نیست.

وی همچنین ادامه داد: اگر شبکه ملی اطلاعات به معنای کامل راه بیفتد و شاهد داشتن سیستم عامل بومی، مرورگر بومی و جست‌وجوگر بومی و مواردی از این دست باشیم، آسیب پذیری سایبری حتماً کمتر خواهد شد.

پیش از این نیز ابوالحسن فیروزآبادی، دبیر اسبق شورای عالی فضای مجازی گفته بود که ما نظارت بسیار دقیق و نزدیکی در این بخش داریم و در مواردی که مطرح شد نیز نظارت داشتیم. البته مقداری فضاسازی و بزرگنمایی در رابطه با افشای اطلاعات هویتی بانکی و تلگرامی صورت گرفت. اما به هر ترتیب همه موارد رسیدگی شد و برخی موارد نیز توسط ضابطان قضائی مورد دستگیری و تعقیب قرار گرفتند.

آنچه بیش از هر چیز دیگر برای تأمین امنیت ملی کشور لازم به‌نظر می‌رسد توجهِ ویژه به شناسایی و احصای تهدیدات امنیت ملی کشور و تلاش درجهت مقابله با این تهدیدات است

وی اظهارداشت: با آمدن بیماری کرونا و اقبال عمومی مردم برای استفاده از فضای مجازی، مشخص شد که نرم‌افزارها و سامانه‌هایمان آن درجه از امنیت را شاید نداشته باشند که بتوانند پاسخگوی حضور این جمعیت در فضای مجازی باشند. لذا متأسفانه شاهد هستیم که بعضاً رخنه‌ها و آسیب پذیری‌های امنیتی در سامانه‌ها و بانک‌های اطلاعاتی وجود دارد. اما اینکه فکر کنید اینها رها شده و رسیدگی نمی‌شود، این طور نیست. ما تلاش می‌کنیم با تقسیم کاری که در کشور صورت گرفته، این موضوع تحت کنترل و رسیدگی قرار گیرد.

رفع خلأ امنیت سایبری با تحقق واقعی شبکه ملی اطلاعات

محمدحسن انتظاری، عضو حقیقی شورای عالی فضای مجازی نیز در این رابطه گفته است که رفع خلأ امنیت سایبری در کشور با تحقق کامل شبکه ملی اطلاعات صورت می‌گیرد.

شبکه ملی اطلاعات با این هدف قرار است ایجاد شود که امنیت اطلاعات در کشور، استقلال، اعمال حاکمیت سایبری و مدیریت آن در اختیار خودمان باشد؛ این اصل اساسی ایجاد شبکه ملی اطلاعات است. این موارد هم در تعریف شبکه ملی اطلاعات و در الزامات اولیه آن در سال ۹۲ به تصویب رسیده است.

وی ادامه می‌دهد که تا زمانی که شبکه ملی اطلاعات در کشور تحقق پیدا نکرده باشد با مسائلی مانند نشت اطلاعات روبرو هستیم و مساله اصلی در حال حاضر باید پرداختن به ایجاد و تحقق شبکه ملی اطلاعات باشد. چرا که یکی از ویژگی‌های اصلی این شبکه، حفاظت و مدیریت اطلاعات و امنیت است.

انتظاری خاطرنشان کرد: در شبکه ملی اطلاعات موضوع امن بودن در لایه‌های مختلف تعریف شده است و تبادل اطلاعات در فضای امن و اعمال سیاست‌های حاکمیت سایبری در این فضا در اهداف تحقق شبکه ملی اطلاعات مدنظر است. تا زمانی‌که شبکه ملی اطلاعات به معنای واقعی ایجاد نشود، ما همچنان شاهد اینگونه خطرات و آسیب پذیری‌ها خواهیم بود.

وی می‌افزاید: بخشی از موضوعات مربوط به امنیت سایبری به وظایف دستگاه‌ها باز می‌گردد که هریک باید وظایف خود را انجام دهند و وظیفه دیگر مربوط به محدوده حاکمیت است. به این معنی که حاکمیت باید نسبت به ایجاد شبکه ملی اطلاعات که یکی از ویژگی‌های اصلی آن امنیت اطلاعات و حفظ داده است، اهتمام جدی به خرج دهد و با ایجاد این شبکه، آسیب‌پذیری‌ها را به حداقل برساند.

امنیت محتوا در پیام‌رسان‌های بومی تضمین می‌شود

بررسی‌ها نشان می‌دهد که به دلیل نبود سازوکارهای مشخص فعالیت در شبکه‌های اجتماعی، بخشی از تهدیدات امنیتی در فضای مجازی که مربوط به نقض حریم خصوصی کاربران می‌شود، در این شبکه‌ها اتفاق می‌افتد. این درحالیست که در تمامی کشورهای پیشرفته دنیا، شبکه‌های مجازی ملزم به تبعیت از قوانین فضای مجازی آن کشورها برای صیانت از حریم خصوصی کاربران هستند و در صورت نقض آنها با جریمه‌های سنگینی مواجه می‌شوند. اما در ایران مشخص نبودن مصادیق گردآوری، استفاده، نگهداری، افشا و مسئولیت‌های متولیان داده‌های شخصی از جمله شبکه‌های اجتماعی داخلی و خارجی، حفاظت از حریم خصوصی کاربران در فضای مجازی را با سوالات جدی مواجه ساخته و برای بسیاری از مصادیق نقض حریم خصوصی در فضای مجازی هنوز قانونی مصوب نشده است.

لزوم برقراری تناسب میان عمل و پاسخ و ضرورت تاثیرگذاری پاسخ، خود چالش دیگری را مطرح می‌کند مبنی بر آنکه بایستی به توانمندی‌ای دست یافت که تاثیرگذاری پاسخ و تکرار آن به کرات در صورت نیاز را تضمین کند

محمدحسن انتظاری، عضو حقیقی شورای عالی فضای مجازی در این زمینه نیز می‌گوید: به همین دلیل تاکید بر استفاده از پیام‌رسان‌های داخلی می‌شود. چرا که اطلاعات شخصی کاربران که توسط پیام‌رسان‌های خارجی جمع آوری می‌شود در داخل کشور نیست و هیچ امنیتی هم برای آن وجود ندارد. موارد متعددی که از نشت اطلاعات در تلگرام اتفاق می‌افتد، گواه این موضوع است. اما استفاده از شبکه‌های اجتماعی داخلی با توجه به قوانین و مقرراتی که برای آنها متصور است، می‌تواند تا حدی تضمین‌کننده صیانت از حریم خصوصی افراد و حفاظت از اطلاعات باشد.انتظاری تاکید می‌کند که این موضوع با توجه به اینکه یکی از ضروریات در سند تبیین الزامات شبکه ملی اطلاعات بوده است، باید در سند کلان شبکه ملی نیز دنبال شود. وی ادامه می‌دهد: تضمین امنیت در لایه محتوا و خدمات محتوایی شبکه ملی اطلاعات در کمیته‌های تخصصی در مرکز ملی فضای مجازی بررسی شده است اما هنوز به صحن شورای عالی فضای مجازی برای تصویب نیامده است.

تضمین کند

این عضو شورای عالی فضای مجازی خاطر نشان می‌کند: برای تحقق این مهم، بخش‌های محتوایی کشور (اعم از سازمان تبلیغات اسلامی، وزارت ارشاد، سازمان صدا و سیما) گزارشاتی را به کمیسیون تخصصی مرکز ملی فضای مجازی، ارائه دادند ولی این گزارش هنوز به جمع بندی نهایی نرسیده است.

دستگاه‌ها در مورد حفاظت اطلاعات گزارش دهند

انتظاری در بخش دیگری از سخنانش می‌افزاید: در رابطه با حفاظت از داده‌ها، شورای عالی فضای مجازی مصوبه‌ای تحت عنوان «نظام پیشگیری و مقابله با حوادث سایبری» داشته که در آن، یک تقسیم کار ملی برای مدیریت کلان داده در کشور صورت گرفته و توسط مرکز ملی فضای مجازی نظارت می‌شود. در این سند، برای هر دستگاه تکالیفی دیده شده و هم اکنون این دستگاه‌ها باید به شورای عالی فضای مجازی گزارش دهند که برای پیاده‌سازی این مصوبه، چه اقداماتی انجام داده و چه برنامه‌ای تدوین کرده‌اند.

وی تصریح کرد: تا زمانیکه فعالیت هر یک از دستگاه‌های مسئول، مشخص نشود، نمی‌توان گفت که نظام پیشگیری حوادث فضای مجازی در چه بخش‌هایی با خلأ مواجه است.

انتظاری خاطرنشان کرد: نحوه برخورد دستگاه‌های مرتبط با مصوبه شورای عالی فضای مجازی در درجه اهمیت قرار دارد و آنها باید در این زمینه به صورت فعال، برنامه خود برای پیاده‌سازی وظایف‌شان را ارائه کنند.

وی می‌گوید: بررسی‌ها نشان می‌دهد که برخی دستگاه‌ها که مسئولیت به عهده‌شان است مسئولیت پذیرفته‌اند اما بعضی‌ها به صورت برنامه‌ریزی شده به این مصوبه نگاه نکردند و وظایف جاری خود را پیش می‌برند. عضو شورای عالی فضای مجازی گفت: باید از دستگاه‌هایی که در آنها درز اطلاعات اتفاق افتاده، گزارش دقیق خواست و این مسئولان باید پاسخگو باشند. در هر دستگاهی حفاظت از اطلاعات در درجه نخست اهمیت قرار دارد و مسئولیت حفاظت از اطلاعات به عهده همان دستگاه است و ساده‌انگاری مساله، صحیح نیست.

خدمات و زیرساخت‌های امنیتی باید ارزیابی امنیتی شوند

وی ادامه داد: پیشنهاد این است که برای حل مشکل حفاظت از داده در کوتاه مدت، نگاه‌مان به سمت امن‌سازی خدمات و زیرساخت‌های مبتنی بر ارزیابی امنیتی باشد.

انتظاری می‌گوید: موضوع این است که داده‌های ما در فضای سایبر اصولاً به اپلیکیشن‌های موبایل و خدمات تحت وب مربوط می‌شود و این کاربردها در یک بستر ارتباطی میزبانی شده و از یک زیرساخت ارتباطی بهره‌برداری می‌کنند. بنابراین اگر بخواهیم از این داده‌ها صیانت کنیم و دغدغه مان حریم خصوصی است، یکی از راه‌های مؤثر و مواجهه کارآمد با این مشکلات، می‌تواند ارزیابی امنیتی مستمر این برنامه‌های کاربردی و زیرساخت‌های ارتباطی باشد.

وی می‌افزاید: در این راستا باید با شناسایی آسیب‌پذیری‌ها در این حوزه، مانند نشت اطلاعات و نقض سیاست‌های امنیتی در حوزه حریم خصوصی، نسبت به امن سازی در این حوزه اقدام کنیم. با این رویکرد، پژوهشکده امنیت سال‌ها است که فعالیت می‌کند و ذیل نظر مرکز راهبردی افتا و مشارکت معاونت امنیت سازمان فناوری اطلاعات، به عنوان یکی از آزمایشگاه‌های مرجع امنیت در سطح کشور فعالیت دارد که نه‌تنها در حوزه شبکه، اپلیکیشن و زیرساخت، بلکه در حوزه سیستم‌های کنترل صنعتی نیز تست‌های ارزیابی امنیتی انجام می‌دهد.

این عضو شورای عالی فضای مجازی خاطر نشان کرد: آزمایشگاه تست محصولات و سالم‌سازی، آزمایشگاه تست و صیانت از زیرساخت‌های شبکه و آزمایشگاه تست اپلیکیشن به صورت کنسول و یا وب سرویس، از جمله آزمایشگاه‌های تحت نظر پژوهشکده امنیت هستند و اخیراً نیز مجوز اولین آزمایشگاه تست سامانه‌های کنترل صنعتی را دریافت کرده‌ایم. پژوهشکده امنیت در زمینه این محصولات به فعالیت می‌پردازد و آزمایشگاه آن، متولی ارزیابی بخشی از محصولات صنعتی پرکاربرد در زیرساخت‌های حیاتی کشور محسوب می‌شود.

وی اظهار داشت: تست و تائید محصولات خارجی قبل از بکارگیری آنها در سطح زیرساخت‌های حیاتی کشور بسیار حیاتی است. به عنوان مثال، بروز تهدیدات سایبری مانند «استاکس نت» و «فلیم» روی زیرساخت‌های اطلاعاتی و صنعتی کشور نشان داد که فایروال‌های خارجی این حملات را شناسایی نکردند. این مقام عضو شورای عالی فضای مجازی تصریح می‌کند: مشخص است که اغلب حملاتی که به زیرساخت‌های حیاتی و حساس انجام می‌شود، اساساً از نوع حملات سازمان یافته است و حاکمیت‌ها و دولت‌ها پشت آن قرار دارند و یا از سوی نهادهای تبهکاری انجام می‌شود که تزریق مالی آنها از طریق دولت‌های متخاصم صورت می‌گیرد. بنابراین ارزیابی امنیتی تمامی محصولات خارجی و داخلی باید در اولویت امر متولیان زیرساخت‌های حیاتی و حساس کشور قرار گیرد.

وی می‌افزاید: در این زمینه بهترین فضا برای تشخیص قابلیت عملکرد و راندمان سیستم، فضای آزمایشگاهی است که در یک محیط شبیه‌سازی شده، کاربرد مطمئن و امن محصولات و خدمات، مورد ارزیابی قرار می‌گیرد. انتظاری خاطرنشان کرد: اما آنچه که مشخص است این است که با وجود بلوغ در حوزه توسعه‌دهندگان اپلیکیشن‌ها، اما متدولوژی توسعه امن اپلیکیشن در کشور مورد استفاده قرار نمی‌گیرد؛ با وجودی که باید به این اصل توجه داشت که هرچه اطلاعات حیاتی‌تر باشند، حفاظت از داده و صیانت آنها برای ما مهم‌تر است و ضریب حساسیت الزامات امنیتی راجع به داده‌های سامانه‌های حساس و حیاتی باید سختگیرانه‌تر باشد اما با وجود تلاش‌های مرکز راهبردی افتا، مرکز مطالعات امنیت سایبری و شورای عالی فضای مجازی و غیره، همچنان نگاه ما نگاه سیستمی و پیشگیرانه نیست و منفعلانه است. هنوز نگاه می‌کنیم و زمانی که اتفاقی رخ داد، شروع به رفع و رجوع و رسیدگی به آن می‌کنیم و این نگاه منفعل است. بنابراین باید سعی شود تا قبل از بروز مشکل و مبتنی‌بر ارزیابی مخاطرات، نسبت به پیگیری اقدامات امنیتی لازم عمل شود.

وی اظهار داشت: نکته این است که شبکه ملی اطلاعات فقط زیرساخت اطلاعاتی و ارتباطی نیست. آنچه که در اختیار وزارت ارتباطات است، این دو لایه است. اما همانطور که در این سوال نیز عنوان شد، امنیت لایه خدمات و محتوا در لایه‌ای جدا از امنیت لایه زیرساخت‌های ارتباطی باید تأمین شود.

انتظاری تصریح کرد: برای مثال در لایه محتوا، رایج‌ترین تهدیدات «فیک نیوز» و «نقض صحت» است و اینها ربطی به سازوکار امنیتی حوزه ارتباطات ندارد. در لایه خدمات نیز ما در فضای سایبری قانون مشخصی نداریم و تکالیف آن نیز به عهده وزارت ارتباطات نیست.

وی می‌افزاید: من به عنوان یک کارشناس و پژوهشگر ارشد امنیتی، معتقدم که شبکه ملی اطلاعات از نظر زیرساخت ارتباطی و اطلاعاتی کارکرد خود را حفظ کرده و پایداری داشته و در سرویس دهی عرضه کنندگان خدمات، وابستگی به منابع بیرونی را کم کرده و برمبنای آن شاهد خدمات پایدار بوده ایم؛ ما یک بخشی از این لایه را مربوط به استقرار امنیت می‌دانیم و از نظر من به عنوان کسی که در حوزه امنیت کار می‌کند، وزارت ارتباطات در این حوزه خوب کار کرده است.

عضو شورای عالی فضای مجازی خاطرنشان کرد: باید توجه داشت که مسائل امنیتی لایه محتوا و خدمات، اساساً خارج از کنترل ما است و امنیت شبکه ملی اطلاعات را باید در قالب یک اکوسیستم تعریف کرد. تمامی وظایف این اکوسیستم به دوش وزارت ارتباطات نیست و این وزارتخانه تنها در حوزه امنیت زیرساخت‌های اطلاعاتی و ارتباطی مکلف است. این تکلیف مربوط به داده‌هایی می‌شود که در دیتاسنتر وجود دارد و باید حداکثر الزامات امنیتی را تأمین کند. اما در حوزه خدمات و محتوا با مسائلی روبرو هستیم که اینها باید در جای خود حل و فصل شوند و همه موارد را نمی‌توان با یک راه حل واحد مدیریت کرد.وی می‌گوید: در این اکوسیستم سازمان صدا و سیما، رسانه‌ها، بانک‌ها، نیروهای مسلح، پدافند غیرعامل و... باید حضور داشته باشند و باید ملاحظات امنیتی در لایه خدمات و محتوا پیش‌بینی و اجرایی شود.

انتظاری تصریح می‌کند: شاید یکی از جدی‌ترین مشکلات امنیتی به ویژه در حوزه CDN که با آن روبرو هستیم، بحث هرزنامه باشد. ما شاهد انتشار انواع و اقسام هرزنامه‌ها هستیم اما سوال اینجاست که آیا این مسئله تنها با حضور و نقش آفرینی وزارت ارتباطات و فناوری اطلاعات حل می‌شود، پاسخ خیر است زیرا مدیریت این فضا بر عهده ما نیست.

وی گفت: مشکل دیگری که با آن مواجه هستیم این است که نهادهای بالاسری در حوزه امنیت سایبری متعدد هستند. برای مثال مرکز ملی فضای مجازی سیاستگذار این حوزه است و مرکز مدیریت راهبردی افتای ریاست جمهوری نقش مرجع راهبردی را برعهده دارد اما سطح تعامل میان دستگاه‌های مختلف برای نیازهای امنیتی کم است. با این وجود و به دلیل اینکه ما در کشور دچار سیستم بروکراسی هستیم، یک مصوبه حدود یک سال طول می‌کشد تا توسط واحدهای مربوطه به اجرا برسد.

وی ادامه داد: این درحالی است که اینگونه تهدیدات در فضای سایبر مرتباً در حال تغییر است و فناوری‌های جدید با اشکال جدید وارد این فضا می‌شوند، بنابراین در این چرخه، نیازمند تسریع چرخه تصمیم‌گیری، تدوین آئین‌نامه‌ها و مصوبات نهادهای بالادستی و نیز تقویت شبکه‌سازی و ارتقای سطح تعامل‌پذیری بین کلیه دستگاه‌ها هستیم. بحث بعدی نیز این است که اگر قصدمان این است که می‌خواهیم موفق به صیانت از حریم خصوصی افراد و حفاظت از داده‌ها شویم، باید سطح اشراف و کنترل‌مان را در فضای مجازی ارتقا دهیم و این یک گلوگاه است.

انتظاری تصریح کرد: درخصوص کاربردی شدن پیوست پدافندی شبکه ملی اطلاعات نیز باید گفت که این سند در سطح سیاستگذاری است و با عملیاتی شدن آن شاهد تحقق الزامات پایه در سطح زیرساخت‌های حیاتی کشور در حوزه پدافند سایبری خواهیم بود. اجرا، ممیزی و پیگیری سند پدافندی شبکه ملی اطلاعات نیازمند استفاده از ظرفیت‌های سازمان پدافند غیرعامل است تا با تعامل این سازمان، در خصوص اجرای الزامات این سند نیز تقسیم کار مربوط به آن صورت گیرد.

باید توجه داشت امروزه اینترنت نقش بسزایی درارتباطات جهانی ایفا می‌کند و به طور فزاینده‌ای با زندگی مردم جهان عجین شده است. باوجوداین اینترنت دولت‌ها را در مقابل چالش‌های جدید امنیتی قرارداده است. گسترش حملات سایبری فرامرزی، امنیت سایبری را به یکی از نگرانی‌های عمده جهانی درقرن بیست ویکم تبدیل کرده است. تامین امنیت و مبارزه با تروریسم یکی از وظایف اصلی دولت‌ها می‌باشد که این مهم در فضای مجازی با توجه به ماهیت فضای سایبری به عنوان بستر اصلی اطلاعات کشور و احتمال هرگونه حمله و جنگ سایبری که باعث تهدید امنیت ملی کشورها می‌شود موجب گردیده تهدیدات سایبری ازتهدیدات سنتی متمایز گشته و اهمیت فراوانی به خود گیرد. حملات سایبری، پدیده‌ای نوظهور در میان جنگ افزارهای مدرن محسوب می‌شود که این حملات صلح و امنیت جهانی را تهدید می‌کند. در سال ۲۰۱۰ نیز برنامه هسته‌ای جمهوری اسلامی ایران مورد حمله بدافزار ((استاکس نت)) قرار گرفت.

گرچه استاکس نت از طریق اینترنت در جهان منتشر شد، اما آثار مخرب آن محدود به سیستم‌های کنترلی خاصی بود که در ایران مورد هدف قرارگرفته بود. بررسی اجمالی مفهوم و انواع حملات سایبری و نوع ارتباط آن با امنیت ملی می‌توان به درک درستی از میزان و اهمیت حملات سایبری به عنوان یک تهدید بزرگ علیه امنیت ملی کشورمان پی برد. بررسی مسئولیت دولت‌ها درخصوص حملات سایبری و عدم وجود قواع آمره بین‌المللی، اهمیت نیاز به تدوین قواعد جدید و منطبق با اصول بین‌الملل و منشور سازمان ملل متحد وقواعد حقوق بشر را گوشزد می‌نماید.

جمهوری اسلامی ایران، به‌عنوان کشوری با موقعیت راهبردی، در دنیای معاصر همواره در معرض انبوهی از تهدیدات در سطوح فروملی، ملی و فراملی است. آنچه بیش از هر چیز دیگر برای تأمین امنیت ملی کشور لازم به‌نظر می‌رسد توجهِ ویژه به شناسایی و احصای تهدیدات امنیت ملی کشور و تلاش درجهت مقابله با این تهدیدات است و باتوجه به محدودیت زمان و منابع مالی و انسانی برای مقابله با این تهدیدات، اولویت‌بندی دقیق تهدیدات اهمیت دارد.

لزوم برقراری تناسب میان عمل و پاسخ و ضرورت تاثیرگذاری پاسخ، خود چالش دیگری را مطرح می‌کند مبنی بر آنکه بایستی به توانمندی‌ای دست یافت که تاثیرگذاری پاسخ و تکرار آن به کرات در صورت نیاز را تضمین کند. برخی از کارشناسان معتقدند که دفاع سایبری، بر خلاف تدابیر مقابله‌جویانه (فیزیکی) که رقیب را به طور قطعی خنثی می‌کند، می‌تواند فعالیت‌های رقیب را مختل کرده یا موقتا وی را خلع سلاح سازد؛ اما هیچ یک از راهکارهای سایبری نمی‌تواند منجر به خنثی سازی قطعی تهدید شوند.