



سیدابراهیم رئیسی در جلسه ستادملی مقابله با کرونا ضمن اشاره به رفع برخی محدودیت‌های کرونایی در کشور گفت؛ اولویت اصلی، حفظ و صیانت از سلامت دانش‌آموزان، دانشجویان، کارگران و آحاد مردم است و حتما باید بازگشایی‌ها همراه با رعایت شیوه‌نامه‌های بهداشتی و جایگزینی روش‌های هوشمند باشد.

پیگیری رعایت شیوه‌نامه‌های بهداشتی در حوزه حمل‌ونقل هوایی وزمینی

رئییسی با انتقاد از سست شدن رعایت شیوه‌نامه‌های بهداشتی در حمل‌ونقل زمینی و هوایی گفت؛ نباید با پایین‌آمدن آمارو شاخص‌های ابتلا به کرونا، رعایت دستورالعمل‌های بهداشتی دچار سستی شود.رئیس قوه‌مجریه با تأکید بر به‌روزرسانی شیوه‌نامه‌های پیشگیری از کرونا گفت؛ باید وزارت بهداشت و

پذیرفته‌اند. قابل ذکر است که متأسفانه این نادیده گرفتن، تبعات منفی را برای کشور به دنبال داشت.

❖جلسه‌ای که اخیرا با آقای رئیس جمهور داشتید نتیجه‌ای برای تسهیل شرایط داشت؟

در شورای عالی فضای‌مجازی در خدمت ایشان بودم و صحبت‌هایی داشتیم که رویکرد ایشان مثبت بود ولی واقعیت امر این است که مراحل قانونی مسیر مشخصی دارد و به نتیجه رسیدن این موارد زمان بر است.

❖به موضوع جنگ‌سایبری اشاره کردید که از نوین‌ترین جنگ‌های معاصر است. درخصوص تدابیر وراهبردهای سازمان‌پدافندغیرعامل‌به‌منظورکاهش آسیب‌های این حوزه بفرمایید.

۱۰سال پیش یعنی‌سال۱۳۹۰ باحکم‌مرحومفیروزآبادی، رئیس ستادکل قبلی قرارگاه پدافند سایبری کشور را ساماندهی و راهبردها و برنامه‌هایی را در این حوزه پیش بینی و آنها را به‌روزرسانی کردیم البته تحولات فضای‌سایبری بسیار سریع و نیازمند برنامه است. درعرصه‌ملی‌نیزبرنامه‌دفاع‌سایبری‌رابرای‌نخستین‌بار برای دستگاه‌های مختلف تهیه‌کرده و در قالب آن رویکردها، چارچوب‌ها و فرآیندهای مرتبط با این نوع دفاع را به تصویب کمیته عالی پدافند غیرعامل رساندیم تا به همه دستگاه‌های کشور ابلاغ شود.

جنگ سایبری توسعه زیادی در دنیا پیدا کرده و در دانشگاه‌های عالی دفاعی کشورهای مختلف تدریس می‌شود؛دانشگاه‌های‌آمریکاازجمله‌این‌مراکز هستند که مقوله جنگ در شبکه‌های اجتماعی با متون جدی و قابل استناد در آنجا ارائه می‌شود.

درادبیات‌راهبردی‌بین‌اروپا و آمریکانیز موضوع‌اعمال‌فشاربه‌دولت‌هااز طریق‌تسلط‌حاکمیت‌برشبکه‌های اجتماعی یک موضوع جدی است. مکرون چندبار به تسلط اینترنت کالیفرنایی اعتراض‌کرده و خواستار ساماندهی اینترنت اروپایی‌شده تا مطابق سازوکار و چارچوب آنها باشد. این امر نشانگر این است که به ابعاداین جنگ واقف هستندوارهاکراهای مقابله باآن را در دستورکار دارند.امروزه در صحنه جنگ سایبری با شش مدل جدی آن مواجهیم که برای هریک نیازمندی راه‌حل پدافندی خاص آن هستیم؛ جنگ سایبری زیرساختی، جنگ سایبری نظامی، جنگ شبکه‌های اجتماعی، جنگ سایبری در حوزه مالی – پولی – ارزی، جنگ سایبری در حوزه‌شهره‌وشومندو جنگ سایبری هیبریدی‌انواع جنگ‌های سایبری راتشکیل می‌دهند. بخش کوچکی از ابزارهای جنگ سایبری در حوزه‌نظامی درجنگ‌فره‌باغ‌قابل مشاهده‌بودکه‌پهادهای خارجی در اختیار دولت آذربایجان قرار داشت و جنگ رزمی در فضای سایبر طراحی، هدایت، کنترل و اداره می‌شد و به‌این‌ترتیب پهاد اول عهده‌دار شناسایی، دیگری مسؤول صدور فرمان و پهاد سوم هم شلیک را عهده‌دار بود.

امروزه شاهدوجودهواپیماهای بدون‌سرنشین‌از راه دور هستیم و جنگ نظامی سایبری بسیار ملموس است‌واگرخداى ناکرده‌درگیر جنگ‌نظامی‌باشکوره‌های هم‌تراز با بالاتلار از خودمان باشیم حتماًبخش عمده‌ای از آن سایبری خواهد بود لذا باید به‌طور جدی در این عرصه کار کنیم.جنگ سایبری که در شبکه‌های اجتماعی هست نیز ازجمله مدل‌های رایج در جنگ است عرصه است و شبکه‌های اجتماعی به‌عنوان بستر سازماندهی، جهت‌دهی افکار عمومی و هدایت آنها به سمت اغتشاشات، آشوب‌ها و درگیری‌ها ایفای نقش می‌کنند و پلتفرم‌ها نقش اساسی را در این نوع جنگ‌ها عهده‌دار هستند.

طبیعتاً گام اولی که ما باید برای مقابله با این جنگ‌ها برداریم این است که ضمن شناسایی تهدیدها به بررسی اجزا و استراتژی درون سیستم بپردازیم تا بتوانیم با اشراف بر این موارد نقطه آغاز، پایان و تلفیق مدل‌های شش‌گانه جنگ سایبری را کشف و راهکارهای مقابله با آنها را طراحی کنیم. مثلاً در جنگ شبکه اجتماعی باید بستر و نقش مردم در این شبکه و مدل‌انگزارى آنها بر افکارعمومی‌را مورد‌مطالعه قرار دهیم تا متوجه راهبری و هدایت آنها در این عرصه شویم. البته این شناخت بسیار سنگین است و ما توانسته‌ایم تا حد زیادی نسبت به آن آشنا شویم.

❖به نظر می‌رسد مامای که زیرساخت‌اپلیکیشن‌ها خارجی‌باشدوقوع‌این‌اتفاقات‌طبیعی‌است‌ومتأسفانه در همین مساله آبان ۹۸ که به آن اشاره کردید اپلیکیشن‌ها نیز یک‌سری فراخوان‌ها را منتشر می‌کردند.

نقش زیرساخت‌در فضای حکمرانی‌سایبربسیارمهم است و با وجود بحث و جدل‌های فراوان که در فضای مجازی‌صورت‌گرفت‌شاهداین‌بودیم‌که تلگرام‌طلاپی

موضوع دفاعی کشور در فضای سایبر تعیین تکلیف شود. همان‌طور که اشاره کردم بخش عمده این جنگ و دفاع مرتبط با زیرساخت‌های کشور است و اغلب اتفاقات در این حوزه رخ می‌دهد؛ لذا ضروری است که موضوع مرزبانی، نحوه کنترل و دفاع از مرزها، پاسخ به تهدیدها، آمادہ‌سازی و دفاع سایبری کشور در این قانون تعیین تکلیف و تعامل آن با سایر مولفه‌ها مشخص شود.

زمانی ما در خصوص جنگ با دشمن بیرونی صحبت می‌کنیم و گاهی نیز جنگ در محیط داخلی مد نظر است که موضوع آن از جنس امنیت است. در جنگ خارجی کسی به موضوع Privacy (حریم خصوصی) کار ندارد؛ زیرا دشمن آن‌ور خط و ما در داخل مرزها هستیم ولی در مقوله برقراری امنیت در حریم داخلی یکی از مسائل اساسی حریم خصوصی است که باید حدود و ثغور آن توسط قانون تعیین شود تا ببینیم حریم عمومی و خصوصی چگونه تلقی می‌شود.

یک‌شبه تعطیل و همه داده‌های مردم که در سیستم به ثبت رسیده بود دود شد و از بین رفت زیرا تسلط صاحب پلتفرم بر موضوع محتوا باعث شده بود تا حکمرانی در اختیارش باشد.

اعمال حکمرانی آمریکایی‌ها در اپ‌استور (App Store) و فروشگاه‌های نرم‌افزاری خودشان باعث محدودیت و محرومیت اپلیکیشن‌های ایرانی شده. مساله قابل‌توجه این است که این اعمال حاکمیت همواره جدی‌تر و سختگیرانه‌تر می‌شود. راهبرد عملیاتی در این زمینه را می‌توان به‌ساماندهی برنامه‌های اساسی و زیربنایی در این عرصه معطوف کرد به‌طوری‌که نظام حکمرانی سایبری کشور، شبکه ملی اطلاعات و مسؤولان درخصوص مساله اهمیت زیرساخت‌های مرتبط با شبکه اجتماعی و فضای مجازی به یک باور مشترک رسیدند زیرا اگر گروهی اصل موضوع را جدی تلقی نکرده و دچار بازی‌های سیاسی،

فراگتنی‌وکاروژنالیستی‌شوندازکارزیربنایی‌واساسی عقب‌مانده و درنهایت زمینه‌های آسیب‌رسانی به کشور فراهم می‌شود.

به نظر می‌رسد در دولت فعلی فهم خوبی نسبت به امهات مسائل وجود دارد‌البته‌هنوزتدبیریزودقیقی در این خصوص اتخاذ نشده ولی امیدواریم به سمت درک واحدی در این عرصه برسیم.

همه ما می‌دانیم کشور دراین حوزه نیازمندجمع‌بندی و تصویب قانون است تا بتوان فضای مجازی با این وسعت و اثرگذاری را هدایت کرد. این آنا‌رشیست بودن بهترین حمل برای خارجی‌هاست تا آزادانه در این خصوص فعالیت کنند. ما مشکلی با حضور و فعالیت رسمی توئیتر، فیس‌بوک و اینستاگرام نداریم اما این حضور نیازمند توافق و قانون است. در دولت قبل ازوزیرخواستیم برنامه‌ای برای تعامل باطرف‌های خارجی تدوین و باآنها به توافق برسد.این‌بی‌نمایندگی‌وبی‌مسئولیتی‌به‌نفع‌سامانه‌های خارجی‌است؛چراکه یک جمعیت بی‌متولی و بی‌قانون ۸۰میلیونی را در اختیار دارد و هر طور که مایل است با آنها رفتار می‌کند.

❖اخیرا یک‌سری اخبار در خصوص حک اطلاعات پلیس راهور، راه‌آهن، دوربین‌های زندان‌اوین (سرقت فایل‌های آرشویی) منتشر شد یا این‌که برخی اپراتورها اطلاعات مشترکان را به فروش گذاشته بودند. این مراکز با سازمان‌پدافند‌همکاری‌خاصی

نداشتند؟ این فیلم‌ها چگونه منتشر شد؟

وقتی حادثه اتفاق می‌افتد سه لایه در خصوص آن مسؤولیت دارند؛ نخست اپراتور اولیه که مسؤول برقراری امنیت هستند و دستورالعمل‌هایی را مبنی بر به‌روز کردن سیستم و کنترل دسترسی‌ها باید رعایت کنند. بنابراین هر سازمانی مسؤول حفاظت از خودش است. مسؤولیت بعدی متوجه برقرارکنندگان امنیت عمومی است که بخش آشکار آن توسط پلیس و بخش پنهان از سوی

دستگاه‌های امنیتی رسد و کنترل می‌شود.

بخش امنیتی زیرساخت طبق اساسنامه سازمان پدافند غیرعامل به ما محول شده است. منتها مرکز ملی فضای مجازی تقسیم‌بندی را بین ما و سایر بخش‌ها انجام داده. بنابراین در چارچوب مقوله برقراری امنیت یک تقسیم‌بندی کلانی صورت گرفته است.

مادامی که زیرساخت‌های داخلی کشور فاقد امنیت باشند مجموعه فعالیت‌های آنها با ضریبی از ناامنی مواجه خواهد شد. همه افراد مایل هستند در جایی سرمایه‌گذاری کنند که از امنیت آن مطمئن باشند مثل گاو صندوق موجود در منازل. بنابراین مسؤولیت اولیه حفظ ایمنی به عهده خودتان است و باید در این خصوص پیش‌بینی‌ها و تدابیر لازم را اتخاذ کنید.

بنابراین زمانی که درباره شبکه ملی اطلاعات صحبت می‌شود باید مدل حکمرانی بر دارایی‌های عمومی در مجموعه‌ای با عنوان قلمرو ملی سایبری تعریف و دنبال شود؛ یعنی اگر نمایندگان حاکمیت مصمم به

درمان با همکاری سایر دستگاه‌ها برای به‌روزرسانی این شیوه‌نامه‌ها اقدام کند. رئیس جمهور با تأکید بر ضرورت حمایت از واکسن‌های ایرانی گفت؛ دانشمندان و متخصصان کشورمان تلاش ارزشمندی در تولید واکسن داخلی داشتند که باید از آنها حمایت حقوقی و مالی شود.

حفاظت هستند باید در وهله اول بداندن قرار است از چه چیزی محافظت کنند.مادر این خصوص بادوستان دولت قبل دچاربرخی سوءتفاهم بودیم به تعبیری که فهم ما از این مساله با درک دوستان تفاوت داشت. ما در حوزه‌های مربوط به خودمان علاوه بر پیگیری و رصد، در خصوص کوتاهی‌های صورت‌گرفته هشدار داده و مسؤولان خاطی را به دستگاه قضایی ارجاع می‌دهیم.

❖با توجه به این‌که شما در همه دستگاه‌ها ووزارتخانه‌ها نماینده دارید چرا معضلات موجود زیاد و نظارت اندک است؟

حوزه فعالیت ما نظامی است و در این حوزه استقلال داریم و برای اقدامات‌مان از فرد یا نهادهی غیر از فرمانده کل قوا اجازه نمی‌گیریم و در قبال مسؤولیت‌هایمان به پاسخگو هستیم اما حوزه پدافند غیرعامل نظامی نبوده و کشوری است و طبیعتاً همکاری‌های دولت را می‌طلبد. در بسیاری از کشورهای دنیا نیز وضعیت به همین منوال است‌وپدافندغیرعامل‌اساساًجزئی

ازدولت‌هاست‌امادرکشورما به دلیل این‌که سیستم فرماندهی نظامی از دولت جداست فعالیت ما نیز بین دولت و بخش دفاع تعریف شده است؛ درواقع رویکردهای اساسی در سیاست‌های دفاعی را از بخش دفاع می‌گیریم و پیاده‌سازی و اعمال آنها را در بخش کشوری انجام می‌دهیم‌لذا همکاری‌دولت‌ها باسازمان پدافند غیرعامل به شدت نمی‌تواند موثر باشد.

❖سردار اگر موافق باشید در پایان به سیاست‌های سازمان پدافند غیرعامل در عرصه پدافند زیستی بفرمایید.

بحث پدافند زیستی بسیار مفصل و نیازمند فرصت است اما به‌طور خلاصه باید بگویم از سال ۱۳۸۹ که سیاست‌های کلی نظام در موضوع پدافند غیرعامل در دستورکار مجمع قرار گرفت یکی از بندهای سیاست‌ها این بود که این سازمان مسؤول تدوین طرح‌های جامع دفاعی در حوزه تهدیدات زیستی، شیمیایی و هسته‌ای باشد. ما سال ۹۶ مانوری در حوزه پدافند زیستی در فرودگاه امام خمینی(ره) انجام دادیم که حتی اسم آن هم مقابله با کرونا‌ویروس بود. فیلم، عکس و گزارش‌های مرتبط با آن موجود است. تصاویر آشنایی که قبل از کرونا هیچ فردی آنها را باور نمی‌کرد. هشدار رسمی به دو سال قبل از وقوع انتشار ویروس برمی‌گردد. همه این اقدامات به دلیل

مطالعات و جمع‌بندی‌های ما بود اما متأسفانه دولت هشدارهای ما را نادیده گرفت. همین مطالب را با نام‌های می‌توانستیم اقدامات خیلی خوبی در سازماندهی کنیم اما این کار را نکردند بعد‌هم که پیشینه‌دارقرطیبه را نپذیرفتند تا مانع توسعه بیماری شویم. دکتر روحانی نگاه خاصی به سازمان پدافند داشت و رفتارش در قبال ما متفاوت بود. که ما از ستاد کرونا حذف کرد اما ما کم‌اگان وظایف‌مان را در این حوزه انجام دادیم. ما زمانی ۱۴ دستور عملیات پیشگیرانه صادر و اعلام کردیم که ویروس در حال شیوع است و باین

راهکارهای می‌توان از گسترده شدن آن جلوگیری کرد‌اما دولت جدی نگرفت. همین مطالب را با نام‌های سردار باقری اطلاع دادم و ایشان مراتب را به نیروهای مسلح ابلاغ کرد و آنها اقدامات لازم جهت آمادگی را انجام دادند‌اما در بخش کشوری به دلیل فقدان نظریه دفاعی هیچ اتفاق سازنده‌ای نیفتاد.

❖پیش‌بینی سازمان پدافند غیرعامل برای ماجرای کرونا چیست؟

سرانجام کرونا بستگی به سبک برخورد خودمان دارد. درحال حاضر شاهد صحنه حسرت‌برانگیز حضور تماشاگران در استادیوم‌های فوتبال اروپا هستیم. پشت صحنه خلق این رویداد فعالیت شبانه‌روزی سیستم‌های پدافندی است که در وهله اول همه دو دوز واکسن‌شان را دریافت کرده‌اند و قبل از شرکت در استادیوم دو نوبت تست کرونا داده‌اند.

درحالی‌که در کشور ما برخی افراد پس از دریافت یک دوز واکسن، پیروی از پروتکل‌ها را فراموش می‌کنند و رعایت‌از شیوه‌نامه‌ها تا ۴۰ درصد کاهش می‌یابد. البته طبق یافته‌های جدید، واکسن نیز کامل کمک‌کننده نخواهد بود زیرا باید بعد از گذشت پنج تا شش ماه دوباره تجدید شود وگرنه زنجیره قطع نخواهد شد. دوا‌ه‌براین اگر قرار است اقتصادمان را از شر کرونا‌رها کنیم باید یک پدافند زیستی خاصی را در عرصه اقتصاد کلید بزنیم تا مشاغل مختلف در کنارشان یک افسر ایمنی داشته باشند‌که همگان را ملزم به رعایت ضوابط کرونا کند. پشت صحنه راحتی مردم انجام فعالیت‌های این چنینی است وگرنه همان‌طور که انتظار داریم علی‌رغم انجام واکسیناسیون وارد پیک ششم می‌شویم. ❖



سردار جلالی، رئیس سازمان پدافند غیرعامل در گفت‌وگو با جام جم:

روحانی اعتقادی به جنگ سایبری نداشت

❖ این روزها بیشتر از هر وقت دیگری اخبار رئیس سازمان پدافند روی بورس است. حمله ۴ آبان به سامانه هوشمند سوخت‌رسانی و درگیر شدن طیف گسترده‌ای از مردم در این حمله سایبری، سردار غلامرضا جلالی، رئیس سازمان پدافند غیرعامل کشور را به صدر اخبار آورد. درست روزی که او در نشست خبری به مناسبت هفته پدافند مشغول ارائه آمار از آخرین اقدامات و تمهیدات صورت گرفته در حوزه سایبر بود، ناگهان خبر هک شدن کارت‌های سوخت در سالروز وقایع بنزینی سال ۹۸ خبرساز شد. بعد از این اتفاقات سردار جلالی در شبکه یک از پشت‌پرده این حمله سایبری گفت و تأکید کرد؛ براساس تحلیل‌های اطلاعاتی حمله سایبری به سامانه‌های سوخت ازطریق یک کشور خارجی، آمریکایی‌ها و صهیونیست‌ها انجام شده و در عین حال این نکته را هم گوشزد کرد که سازمان تحت مدیریتش از نظر اطلاعات فنی در حال بررسی است.

ما برآی انجام گفت وگویی تفصیلی درباره حملات سایبری به مراکز هسته‌ای، چگونگی توسعه بستر نفوذ، زیرساخت اپلیکیشن‌های خارجی، چپستی جنگ هیبریدی در ابعاد نوین و نقش بازآرندگی و دفاعی پدافند در این زمینه سراغ سردار غلامرضا جلالی، رئیس سازمان پدافند غیرعامل کشور

رفتیم که مشروح مصاحبه او با جام جم در ادامه آمده است:



امین صبحی

دبیر سیاسی

❖بعد از حملات سایبری به مراکز هسته‌ای چه تمهیدات و برنامه‌هایی را درخصوص بحث حفاظت از نیروگاه‌ها و مراکز هسته‌ای در دستور کار قرار دادید؟

دشمن صهیونیستی با همکاری آمریکایی‌ها یک استراتژی تهدید ترکیبی را علیه زیرساخت‌های هسته‌ای ما در نظر گرفته که شامل مجموعه‌ای از تهدیدات امنیتی، تروریستی و خرابکاری مبتنی بر قابلیت‌ها و ظرفیت‌های دشمن نظیر فضای مجازی، فضای جاسوسی، نفوذ و سایر قابلیت‌های فناوریانه که می‌تواند در این مسیر استفاده کند، می‌شود.

آنها در مرحله نخست تلاش کردند خلا‌های موجود در این حوزه را کشف و علیه ما استفاده کنند. طبعاً ما نیز برای مقابله با این تهدیدها به شناسایی اجزا و فرآیندهای مختلف این عملیات پرداخته و گام‌هایی را به منظور شناسایی آسیب‌ها و ضعف‌های خود برداشتیم تا راهکارها و پیشنهادهاتی را به منظور مضمون سازی و امن‌سازی سیستم‌های خود اتخاذ کنیم تا از این موضع دوباره دچار آسیب نشویم.

تهدید نظامی علیه تأسیسات هسته‌ای از گذشته تاکنون مطرح بوده از همین رو ما نیز اقدامات پیشگیرانه متقابل خوبی را در این خصوص انجام داده ایم؛ احداث زیرساخت‌های هسته‌ای کشور در اعماق زمین از جمله این موارد است وایجاد امنیت نسبی از جمله فواید آن است.

در حال حاضر بخش عمده‌ای از مجموعه‌ها در فضای امن زیرزمینی هستند و با این اقدام تهدیدات نظامی علیه این تأسیسات به حداقل رسیده است. بعد از حمله استانتسک – که حکم هشدار برای دستگاه‌های امنیتی و دفاعی داشت – نیز تلاش‌های زیادی در حوزه سایبری و به منظور آنالیز این ویروس و اجزای آن صورت گرفته و اقداماتی در راستای امن‌سازی سامانه‌های هسته‌ای و سامانه‌های مشابه انجام شد تا حدی که به این مدل تهدید اشراف پیدا کردیم. واقعیت این است که درگیری بین تهدیدو دفاع همواره وجود دارد و ما این مسیر را تا رسیدن به نقطه اوج دنبال می‌کنیم.

❖در حوزه مربوط به تهدیدات جاسوسی و نفوذ چطور؟

متأسفانه به دلیل برخی اشکالاتی که در ساختار و وضعیت ما وجود داشت، مشکلاتی در این زمینه داشتیم که دلیل عمده آن نیز مربوط به حضور عناصر خارجی (بازرسان آژانس) در شبکه‌ها می‌شد که با فیلمبرداری‌های ثابت و تلاش‌هایی که انجام می‌دادند، امکان نفوذ برایشان فراهم بود. متأسفانه دولت قبل در برخورد با عناصر آژانس تا حد زیادی ساده اندیشی می‌کرد و به منظور همکاری‌های بهتر و بیشتر با آژانس، دسترسی آنها را سهیل می‌کرد و همین مساله