سردار مطیعی

معاون محترم انرژی سازمان پدافند غیرعامل کشور

دکتر شیخی

مشاور محترم سازمان پدافند غیرعامل کشور در حوزه سایبر

در ابتدا آقای مطیعی با عرض تبریك میلاد پیامبر اعظم (ص) و آرزوی قبولی طاعات سخنان، خود را با فرمایش مقام معظم رهبری شروع نمودند که "اگر چنانچه مدیران ارشد کشور اهمیت پدافند غیرعامل را درك نکنند و پدافند غیرعامل آنچنان که شاید و باید در کشور توسعه پیدا نکند و اعمل نشود، ما در معرض تهدیداتی قرار می گیریم که بعضی از آنها قابل جبران نیست" و سپس به تشریح مفهوم پدافند غیرعامل به عنوان مجموعه اقدامات غیرمسلحانه در برابر نیات دشمن پرداختند.

سپس ایشان با اشاره به چهار تهدید عمومی کشور(نظامی، تحریم، سایبری و تروریستی امنیتی) اولویت اعمال تهدید نظامی را بدلیل توان اقدام برتری جویانه کشور، پایین دانستند و شرایط خصوصی سازی در صنعت پتروشیمی را یکی از مهمترین دلایل کم تاثیر شدن اعمال تهدیدات تحریم ها در این صنعت برشمردند و بیانات خود را بر روی تهدیدات ریزپرنده ها، سایبری و تروریستی امنیتی متمرکز کردند.

وی لزوم عملیاتی شدن مصوبه ابلاغی شورای امنیت ملی (شماره ۲۸۹۷۱/م مورخ ۹۸/۶/۲۵) و دستورالعمل صادره برای مقابله با تهدید ریزپرنده ها را به عنوان تکالیف دستگاه ها، برای مقابله با تهدیدات در سطح زیر ۵۰۰۰ ft را ضروری دانسته و چهار اقدام ذیل را به عنوان حداقل انتظار از مدیران بیان داشتند.

الف) شناسایی نقاط حیاتی حساس

ب) آموزش عمومی برای مقابله با ریزپرنده ها

ج) آموزش تخصص اپراتوری در حد پتروشیمی

د) طراحی و تامین سامانه های مقابله با تهدیدات احتمالی

در ادامه ایشان ضمن اشاره به تهدیدات تروریستی امنیتی و توسعه یافتگی اشکال مختلف آن به برخی مصادیق اتفاق افتاده اخیر و خسارات وارده اشاره کردند و راهکارهای مقابله را در ارتقاء سطح امنیت پتروشیمی ها و ایجاد وحدت رویه و انسجام عمل در مقابله با تشدید مراقبت ها و پایش تهدیدات و آسیب پذیرها و کاهش آنها دانستند و بیان داشتند که تعیین نقش و وظایت نیروهای مسلح در همکاری با دستگاه های بین سازمان پدافند غیرعامل و وزارت نفت در دستور کار قرار گرفته است.

همچنین ایشان، سایر راهکارهای پدافند غیر عامل در سطح کلان را بقرار ذیل اعلام کردند.

الف) تدوین دستور العمل مقابله با نشست و انتشار مواد شیمیایی در مناطق.

ب) ایجاد بیمارستان برای مصدومین شیمیایی و زیرساخت های امداد و نجات و پاکسازی و رفع آلودگی.

ج) بررسی شعاع خط پیرامون شهرها و محیط زیست.

د) برگزاری رزمایش ها جهت ارتقاء و آمادگی.

و) تدوین طرح مقابله با شرایط اضطراری و تامین تجهیزات مقابله متناسب با تهدیدات و آسیب پذیری ها.

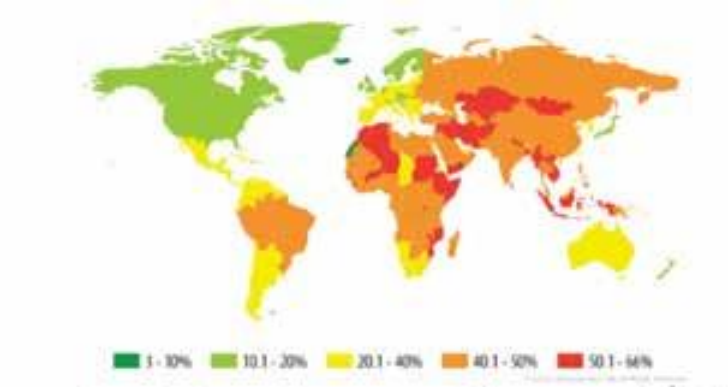
ه) تدوین طرح تخلیه اضطراری در مناطق پتروشیمی.

ز) تدوین دستور العمل بازگشت پذیری و بازیابی تاسیسات آسیب دیده در برابر تهدیدات.

در پایان نیز ایشان با تشریح مختصر تهدیدات سایبری در حوزه پتروشیمی به اهمیت ایجاد مرکز امداد سایبری (CERT) در مناطق متمرکز پتروشیمی ها درجنوب کشور به منظور رصد پایش و اقدام سریع برای کاهش تاثیر تهدیدات اشاره نمودند و ادامه بحث را به آقای شیخی سپردند.

آقای دکتر شیخی نیز آماری از وضعیت سایبری کشور و میزان حملات واقع شده براساس اطلاعات شرکت های بزرگ امنیتی مانند کاسپرسکی ، سایبربیت و کومودو ارائه دادند که گویای رتبه بالای تهدیدات سایبری در کشور به عنوان یکی از اهداف خارجی بود.

وی در ادامه به اجرای پروژه PRISM در ایالات متحده امریکا و توافق نامه فرماندهی سایبری ایالات متحده (NSA) با اغلب سایت های اینترنتی (مانند Face book ، Yahoo ، Google و . . .) که روزانه افراد بسیاری با آن مواجه هستند، اشاره نمودند که در حال جمع آوری اطلاعات، آنالیز و تحلیل مهندسی اجتماعی و شناسایی افراد، شرکت ها و اقدامات آنان می باشند.



جغرافیای آلودگی محلی مخرب در ۲۰۱۶ (رتبه بندی شده براساس درصد کاربران مورد هدف)

سپس با توجه به زیرساخت های نفوذ و در معرض بودن کشور برای حمله سایبری به معرفی راه های متداول نفوذ به شبکه های صنعتی واحدهای صنعتی پرداخته و بر لزوم افزایش حساسیت ها تاکید نموده و چالش های امنیت سایبری در صنعت پتروشیمی و پیشنهادات اجرایی خود برای کاهش آسیب پذیری های موجود را بقرار اعلام نمودند.

چالش های مربوط به امنیت سایبری در صنایع پتروشیمی کشور

۱- درك ضعیف کارکنان و مدیران صنایع حیاتی از تهدیدات سایبری و بروز نبودن دانش کارشناسان در حوزه امنیت سایبری صنعتی

۲- تردد پیمانکاران به صنایع و انتقال فایل به صنعت بدون رعایت ملاحظات امنیت سایبری، اعطای دسترسی از راه دور به پیمانکاران داخلی و خارجی و عدم دقت کافی برای جدا بودن زیرساخت های حساس صنعتی از اینترنت

۳- کمبود ابزارهای رصد برای کشف فعالیت بدافزارها در صورت ورود آلودگی به صنایع و عدم وجود گروه های پاسخ و امداد سایبری در صورت بروز رخداد و حمله سایبری

۴- عدم وجود متولی در حوزه امنیت سایبری صنعتی در داخل صنعت[۱]

۵- ضعف در بکارگیری فناوری های بومی امنیت سایبری صنعتی

۱- هم اکنون بخش IT صرفا بر روی اتوماسیون اداری فعال است و نظارتی بر مباحث امنیت سایبری بخش ابزار دقیق یا بخش بهره برداری ندارد

پیشنهادات اجرایی به منظور کاهش آسیب پذیری های سایبری:

۱- بکارگیری سامانه های ویروس یاب مرکب (Multi-AV) که در داخل کشور تولید می شوند و می توان آنها را به منظور ارزیابی فایل ها به شبکه اضافه نمود.

۲- بکارگیری سامانه های بومی لاك گیری در شبکه صنعتی پتروشیمی ها

۳- برگزاری دوره های آموزشی منظم در سطوح مختلف حوزه امنیت سایبری

۴- تربیت تیم ارزیاب صنعتی در واحدهای پتروشیمی و انجام ارزیابی های دوره ای توسط خود پتروشیمی

۵- ایجاد گروه های واکنش به رخداد سایبری (Cert) در پتروشیمی ها

همچنین ایشان در پایان ارائه خود، با انجام آزمایش شبیه سازی شده، اثبات کردند که برخی ویروس ها می توانند با ورود به سیستم ها بدون آنکه از خود رد باقی بگذارند ، کار خرابکاری خود را انجام دهند.