تاریخ دریافت: ۱۳۹۵/۰۹/۲۵
تاریخ پذیرش: ۱۳۹۶/۰۲/۲۰

فصلنامهٔ مطالعات حفاظت و امنیت انتظامی
فصلنامهٔ علمی ـ ترویجی
سال دوازدهم، شمارهٔ چهل‌وسوم، تابستان ۱۳۹۶

بررسی نقش حفاظت فنّاوری اطلاعات و ارتباطات در جنگ‌های رایانه‌ای علیه ناجا با رویکرد پدافند غیرعامل

احمدرضا متین‌فر[۱]، وحید یادگاری[۲]، ناصر یسیلانی[۳]

از صفحهٔ ۱ تا صفحهٔ ۲۶

چکیده

زمینه و هدف: گستردگی مأموریت‌های سازمان نیروی انتظامی جمهوری اسلامی ایران، لزوم بهره‌گیری از سامانه‌ها و فنّاوری‌های نوین را همچون فنّاوری اطلاعات و ارتباطات، بسیار پررنگ کرده و خوشبختانه امروزه جایگاه این فنّاوری در تحقق مأموریت‌های ناجا بسیار مهم و اثرگذار است؛ از این‌رو، باید با پایش همیشگی وضعیت امنیتی و فنی فنّاوری اطلاعات سازمان، تهدیدها و آسیب‌ها را شناسایی و برای پایداری سامانه‌ها، آنها را رفع کرد؛ بنابراین در این تحقیق، وضعیت حفاظت فنّاوری اطلاعات و ارتباطات ناجا و سنجش آمادگی آن با رویکرد پدافند غیرعامل در مقابله با جنگ‌های رایانه‌ای علیه ناجا بررسی شده است. **هدف** اصلی تحقیق بررسی «نقش حفاظت فنّاوری اطلاعات و ارتباطات در جنگ رایانه‌ای علیه ناجا با رویکرد پدافند غیرعامل است».

روش‌شناسی: این تحقیق از نظر هدف و ماهیت کاربردی و از حیث روش جمع‌آوری پیمایشی است، حجم نمونه و آماری یکسان و از نوع «تمام‌شمار» است، جامعهٔ آماری شامل ۳۵ نفر از خبرگان این موضوع در فاوا ناجا و ساحفاناجا می‌باشد و نمونه به تعداد ۳۵ نفر شامل دامنهٔ افسران جزء و افسران ارشد و بالاتر است. در این پژوهش، پرسشنامهٔ محقق‌ساخته با ۵۰ پرسش بسته و طیف لیکرت تهیه شد و پس از توزیع بین دوازده خبره، پایایی و روایی آن با محاسبهٔ آلفای کرونباخ صورت گرفت. پس از آن، پرسشنامه به‌صورت تمام‌شمار هدفمند میان همهٔ افراد جامعهٔ نمونه توزیع و پس از گردآوری و تحلیل با نرم‌افزار spss مورد تحلیل قرار گرفته است.

یافته‌ها و نتیجه‌گیری: نتایج تحقیق نشان می‌دهد «وضعیت حفاظت فنّاوری اطلاعات در جنگ‌های رایانه‌ای علیه ناجا با رویکرد پدافند غیر عامل» با امتیاز ۱۶/۵۲ در حد خیلی خوب است و به الزام‌های پدافند غیرعامل فاوا در سطح ناجا، با وجود کمبودهایی، توجه شده است.

کلیدواژه‌ها: امکان‌سنجی، ساختار سازمانی، فرهنگ سازمانی، فنّاوری اطلاعات، مدیریت دانش.

---

۱. عضو هیئت علمی.
۲. عضو هیئت علمی.
۳. کارشناس ارشد پدافند غیرعامل، نویسنده مسئول (رایانامه: faslname.motaleat@chmail.ir)

مقدمه

در این تحقیق، ضمن طرح مسئله، اهمیت و ضرورت پرداختن به موضوع، مطرح و سپس فنّاوری اطلاعات و ارتباطات، نقش جنگ در گسترش فنّاوری اطلاعات و ارتباطات، استانداردهای مدیریت امنیت فنّاوری اطلاعات، نقش و اجزای فنّاوری اطلاعات و ارتباطات در ناجا و دستورکارهای موجود در زمینهٔ امنیت و پدافند غیرعامل فاوا تشریح و در پایان، به تحقیقات صورت‌پذیرفته و الگوی مفهومی تحقیق اشاره شده است. در ادامهٔ تحقیق، با توجه به نتایج پرسشنامهٔ خودساخته، وضعیت، تحلیل و پیشنهادهای کاربردی برای محققان و مدیران بیان شده است.

پیشینهٔ تحقیق:

در کتاب امنیت به روش پیشگیری الکترونیکی (حمید دوست‌محمدیان) با توجه به اهمیت فنّاوری اطلاعات در عصر حاضر و رشد سریع و در عین حال نامتوازن ساختار IT، به نقاط بالقوه آسیب‌پذیر و خطرناک آن اشاره و افزون بر آن، ضرورت توجه و پرداخت سریع و نیز نظام‌مند، معقول و هدفمند را یادآوری کرده است که سبب مصون‌سازی این بستر از تهدیدهای موجود و نیز حفظ امنیت ملی و حریم شخصی شهروندان در فضای جنگ و ستیزه‌جویی‌های بین‌المللی امروز می‌شوند و به این نتیجه رسیده است که اجرای پدافند غیرعامل در گسترهٔ فاوا کم‌هزینه‌ترین راه‌کار به‌شمار می‌رود. کتاب حاضر کوشیده است با بیان اصول پدافند غیرعاملی در پهنهٔ جنگ‌های نوین در دنیای امروز و نیز تأمین اصولی امنیت مبادلهٔ اطلاعات الکترونیکی در فضای مجازی و شبکه‌های رایانه‌ای به روش پیشگیری الکترونیکی، امکان ایجاد بستری امن در فضای مبادلهٔ الکترونیکی را تا اندازه‌ای مهیا کند تا در زمان‌های مخاطره‌آمیز (جنگ‌های الکترونیک) اطلاعات ضروری از دستبرد دور بماند.

در مقالهٔ «مبانی پدافند غیرعامل در حوزهٔ امنیت فنّاوری اطلاعات» (محسن آزادزاده و دیگران) آمده است: تأمین امنیت اطلاعات سازمان‌ها در محیط امروزی که از شبکه‌های به‌هم‌پیوسته تشکیل شده، کاری مشکل است و با ورود هر محصول الکترونیکی و هر ابزار نفوذ و جاسوسی، این کار سخت‌تر نیز می‌شود. همچنین با توجه به رشد روزافزون حمله‌ها

در شبکه‌های رایانه‌ای، تلاش برای مقاوم‌سازی آنها در برابر حمله‌ها و درنظر گرفتن مسائل مربوط به پدافند غیرعامل بسیار ضروری شمرده می‌شود. امروزه عوامل بسیاری امنیت شبکه‌ها را تهدید می‌کنند؛ از جمله حمله‌های گستردهٔ رخنه‌گرها (هکرها) که از نقاط آسیب‌پذیر سامانه‌ها برای رسیدن به هدف‌هایشان استفاده می‌کنند. با رخنه‌گری هر سرورِ میزبان، صدها یا شاید هزاران وب‌گاه، مورد نفوذ قرار می‌گیرند؛ بنابراین، باید از سرور و شبکهٔ خود حفاظت کرد و به مسائل پدافند غیرعامل با امکانات امنیتی توجه داشت. در این مقاله، پس از بررسی تهدیدهای داخلی و خارجی و حفاظت از سامانه‌ها، به ضرورت تأمین امنیت پرداخته می‌شود و مسائل مربوط به امنیت فنّاوری اطلاعات در عصر دیجیتال و مباحث مرتبط با رایانه‌های شخصی و اینترنت به میان می‌آید.

در پایان‌نامهٔ رضا نیک‌نفس با عنوان «بررسی شاخص‌های پدافند غیرعامل در فاوا ناجای استان همدان» زیرساخت‌های فناوری اطلاعات متناسب با استانداردهای سازمان پدافند غیرعامل بررسی شده و محقق چنین نتیجه‌گیری کرده است که با وجود متوسط بودن وضعیت، از آنجا که سامانه‌های فناوری اطلاعات در بستر شبکه‌ای محدود (اینترانت) قرار دارد، نمی‌توان تهدیدهای کلی را در مورد شبکهٔ ناجا به‌صورت جدی ارزیابی کرد.

در مقالهٔ «اصول و ملاحظه‌های پدافند غیرعامل در فضای سایبری» (جواد داوری و دیگران) سرمایه‌های فضای رایانه‌ای را مشتمل بر زیرساخت‌ها و سامانه‌ها و روش‌های ارزیابی دانسته‌اند. منظور از ارزیابی فنّاوری، فهرستی از فعالیت‌هاست که به‌طور تقریبی در هر ارزیابی کاربرد دارند. این مقاله، فنّاوری اطلاعات، اصول و ملاحظه‌های پدافند غیرعامل در فضای مجازی مورد استفاده در سطح سازمان‌ها طی سال‌های اخیر را ارزیابی می‌کند. تحقیق یاد شده سعی کرده است پیوند مناسبی بین ملاحظه‌های پدافند غیرعامل و مدیریت فنّاوری اطلاعات برقرار کند تا نتایج مطلوب‌تری از ارزیابی فنّاوری اطلاعات در فضای مجازی به‌دست آید.

در مقالهٔ «بررسی نقش فنّاوری اطلاعات در پدافند غیرعامل و مدیریت بحران و ارائهٔ الگویی جامع در مدیریت بحران» (پورکیانی و دیگران) بیان شده است: «پدافند غیرعامل،

در زمینهٔ فنّاوری اطلاعات و ارتباطات، به‌منظور امنیت، ایمنی و پایدارسازی زیرساخت‌های مهم کشور در مقابل تهدیدهای دشمن در زمینهٔ این فنّاوری شکل گرفته و یکی از مأموریت‌های مهم پاسداری از کشور، به‌ویژه حفاظت از زیرساخت‌های فنّاوری اطلاعات و ارتباطات، در مقابل حمله‌های احتمالی است» در این مقاله، ضمن توضیح اهمیت فنّاوری اطلاعات در پدافند غیرعامل و مدیریت بحران، به الگوی فراگیر مدیریت بحران، پیاده‌سازی آن، نمایش فیزیکی یک سامانه و رویدادهای مربوط به آن اشاره و طی فرایند الگوسازی، مؤلفه‌های اصلی سامانه، شناسایی و چگونگی ارتباط و اتصال آنها با یکدیگر و مؤلفه‌های این سامانه به‌صورت کامل و با تمامی جزئیات بحث شده است.

در مقالهٔ «فنّاوری‌های نوین در جنگ‌های آینده» (حسین سلامی) آمده است: «جنگ‌های نوین به‌محض آغاز، سرتاسر کشور یا کشورها را در بر خواهند گرفت؛ بنابراین در آینده، سامانه‌های فرماندهی و واپایش ارتباط و مخابرات، کسب اخبار، گردآوری و پردازش اخبار و تبادل سریع اطلاعات ماشینی و یکپارچه و منسجم، روزبه‌روز اهمیت بیشتری پیدا می‌کنند. در آینده، فقط سامانه‌های ابررایانه و ارتباط سریع، امن و از پیش تدوین شده، خواهند توانست در تصمیم‌های مؤثر آنی و انتقال لحظه‌ای دستورها در سطحی گسترده مؤثر باشند. برای گرفتن تصمیم‌های فرماندهی و مخابرهٔ آنها، به رایانه‌ها، ماهواره‌ها، تسهیلات گردآوری، پردازش و انتشار اطلاعات و شبکه‌های ارتباطات گسترده و یکپارچه نیاز است که انسجام نظام‌مند آنها بیشترین اهمیت را دارد».

در کتاب «مدیریت امنیت فنّاوری اطلاعات و ارتباط» (یوسفی و دیگران) به استانداردهای بین‌المللی حوزهٔ امنیت فاوا اشاره و شاخصه‌های ارزیابی آنها را بیان کرده و نتیجه گرفته‌اند امنیت باید در این شش محور بررسی و پیگیری شود:

- مستند هدف‌ها، راهبردها و سیاست‌های امنیتی فضای تبادل اطلاعات دستگاه؛
- مستند طرح تحلیل خطرهای امنیتی فضای تبادل اطلاعات دستگاه؛
- مستند طرح امنیت فضای تبادل اطلاعات دستگاه؛
- مستند طرح مقابله با حوادث امنیتی و ترمیم ایرادهای فضای تبادل اطلاعات دستگاه؛

- مستند برنامهٔ آگاه‌سازی امنیتی به کارکنان دستگاه؛
- مستند برنامهٔ آموزش امنیتی کارکنان تشکیلات تأمین امنیت فضای تبادل اطلاعات دستگاه.

در مقالهٔ «نقش رایانش ابری در پدافند سایبری سازمانی» (توقعی و دیگران) گفته‌اند: «امروزه تهدیدها در قالب شبکه‌های رایانه‌ای و مخابراتی رو به افزایش است و فضای مجازی به مکانی مناسب برای جنگ تبدیل شده است» جنگ مجازی به درگیری‌ها در فضای مجازی، با هدف‌های سیاسی و مذهبی، اشاره دارد و هدف از حملهٔ رایانه‌ای دستیابی به اطلاعات دیگر کشورها و ایجاد وقفه در تجارت است؛ به‌گونه‌ای که هزینه‌های اقتصادی را افزایش دهد. در رویکرد سنتی، سازمان‌ها امنیت را با بهره‌گیری از سازوکارها و سیاست‌های امنیتی گوناگون، برای سازمان خود فراهم می‌آوردند و دارایی خود را پشت دیوارهٔ آتش و سامانه‌های پیشگیری، از نفوذ در امان نگاه می‌داشتند. در این میان، رایانش ابری، با پیشرفت و گسترش روزافزون خود، کل صنعت فنّاوری اطلاعات و ارتباطات را دچار دگرگونی خواهد کرد؛ زیرا مهم‌ترین عامل در ایجاد امنیت به‌شمار می‌رود. اکنون این فنّاوری در حال تبدیل شدن به یکی از زیرساخت‌های اساسی اینترنتی است که بستر تغییر الگو به سمت قانونی شدن را فراهم می‌کند.

ابرها، خدمات متفاوتی عرضه می‌کند که یکپارچه می‌شوند و در چندین زمینه به‌کار می‌روند. در این مقاله، کاربرد رایانش ابری بررسی شده است؛ با این هدف که امنیت و ایمنی شبکه‌ها تضمین شود، زیرساخت‌ها و آسیب‌پذیری‌ها کاهش یابد و آستانهٔ تحمل در رویارویی با تهدیدها افزایش پیدا کند؛ تا اصول پدافند رایانه‌ای در پهنهٔ فنّاوری اطلاعات و ارتباطات رعایت و با ایجاد قابلیت به‌روزرسانی در سازمان‌ها با بهره‌گیری از فنّاوری‌های نوین، بر اجرای آنها نظارت شود.

بیان مسئله: با توجه به اهمیت فنّاوری اطلاعات در عصر حاضر و رشد سریع و در عین حال نامتوازن ساختار فنّاوری اطلاعات، این بستر به یکی از نقاط بالقوه آسیب‌پذیر و خطرناک در جهان بدل شده است که ضرورت توجه و پرداخت سریع و در عین حال نظام‌مند، معقول و هدفمند را می‌طلبد تا این بستر از تهدیدهای موجود در راستای حفظ

امنیت ملی و حریم شخصی شهروندان در فضای جنگ و مخاصمه‌های امروز بین‌المللی در امان بماند. در پاسخ به این ضرورت، پدافند غیرعامل در حوزهٔ فنّاوری اطلاعات و ارتباطات و جنگ رایانه‌ای به‌منظور امنیت و پایداری زیرساخت‌های مهم کشور در مقابل تهدیدهای دشمن از ناحیهٔ فنّاوری اطلاعات و ارتباطات شکل گرفته است. در جمهوری اسلامی ایران نیز همگام با پیشرفت‌های فنّاوری اطلاعات و ارتباطات، ارکان گوناگون کشور کوشیده‌اند از این ظرفیت بیشترین بهره را ببرند. برای نمونه، نیروی انتظامی در سال‌های اخیر به‌علت گسترهٔ فعالیت‌ها و مأموریت‌ها و همگام با فنّاوری‌های روز، توانسته است با استفادهٔ بیشینه از ظرفیت فنّاوری اطلاعات در راستای چابک‌سازی سازمان و بهبود فرایند کاری اقدام کند که این مهم خوشبختانه با طراحی بیش از دویست سامانه و زیرسامانه و راه‌اندازی شبکهٔ اینترانت ناجا در حال بهره‌برداری است. بدون شک این ظرفیت ایجاد شده، با توجه به اهمیت کاربردی آن، همواره هدف دشمنان داخلی و خارجی در حوزهٔ جنگ‌های رایانه‌ای و اطلاعاتی قرار می‌گیرد که سعی دارند با روش‌های گوناگون در آنها نفوذ کنند و بهرهٔ لازم را ببرند. از این‌رو، باید به مقولهٔ امنیت فنّاوری اطلاعات و استانداردهای پدافند غیرعامل توجه جدی داشت و ضمن هزینه‌کرد در این حوزه، به شاخص‌های آن با هدف حفظ و پایداری سامانه، دفع دسیسه‌ها و نیت پلید دشمن اهمیت داد.

اهمیت و ضرورت: با توجه به اهمیت این تحقیق، می‌توان گفت بسیار ضروری است که به پایش همیشگی مقولهٔ امنیت فنّاوری اطلاعات و ارتباطات و استانداردهای پدافند غیرعامل توجه شود و نتایج حاصل از انجام تحقیق، برای دفع راهکنش‌های دشمن در بهره‌گیری از شیوه‌های جنگ‌های رایانه‌ای علیه سامانه‌های فنّاوری اطلاعات ناجا به‌کار رود تا در برابر تهدیدها، پایداری ارتقاء یابد و از آسیب‌پذیری‌ها کاسته شود و به تداوم خدمات ضروری، بر بستر فنّاوری اطلاعات از سوی ناجا، در زمان بحران کمک کند. در صورت تحقق نیافتن و اجرا نشدن نتایج این پژوهش، شبکهٔ فاوا ناجا در مقابله با تهدیدها بسیار آسیب‌پذیر می‌شود و در جنگ‌های رایانه‌ای بیشترین زیان به مجموعه وارد خواهد شد.

هدف‌های تحقیق

هدف اصلی:

تعیین نقش حفاظت فنّاوری اطلاعات و ارتباطات در جنگ رایانه‌ای علیه ناجا با رویکرد پدافند غیرعامل.

هدف‌های فرعی

- تعیین انواع جنگ رایانه‌ای و روش‌های در نظر گرفته شده برای آن در ناجا؛
- تعیین وضعیت امنیت فنّاوری اطلاعات و ارتباطات در ناجا، با رویکرد پدافند غیرعامل؛
- تعیین وضعیت اجرای محورهای پدافند غیرعامل در گسترهٔ فنّاوری اطلاعات و ارتباطات ناجا.

سؤال‌های تحقیق

سؤال اصلی: نقش حفاظت فنّاوری اطلاعات و ارتباطات در جنگ رایانه‌ای علیه ناجا با رویکرد پدافند غیرعامل چیست؟

سؤال‌های فرعی

- انواع جنگ رایانه‌ای و روش‌های در نظر گرفته شدهٔ آن در ناجا کدام است؟
- وضعیت امنیت فنّاوری اطلاعات و ارتباطات در ناجا با رویکرد پدافند غیرعامل چگونه است؟
- وضعیت اجرای محورهای پدافند غیرعامل در حوزهٔ فنّاوری اطلاعات و ارتباطات چگونه است؟

فرضیه‌های تحقیق

- به‌نظر می‌رسد بین انواع جنگ رایانه‌ای و شیوه‌های در نظر گرفته شدهٔ آن در ناجا، ارتباطی وجود دارد؛
- بین وضعیت امنیت فنّاوری اطلاعات و ارتباطات در ناجا و پدافند غیرعامل، رابطه‌ای به چشم می‌خورد؛
- احتمال دارد بین وضعیت اجرای محورهای پدافند غیرعامل و حوزهٔ فنّاوری اطلاعات و ارتباطات، ارتباط وجود داشته باشد.

روش تحقیق: تحقیق حاضر، از نظر هدف «کاربردی» و از نظر روش «تحلیلی- توصیفی» است.

ادبیات تحقیق

فنّاوری اطلاعات و ارتباطات: این روزها جهان دانش، دستخوش دگرگونی‌ها و دستاوردهای بزرگی شده که بر همهٔ جنبه‌های زندگی بشر سایه انداخته است. در هیچ دوره‌ای از تاریخ، تغییر و پیشرفت‌های علمی شتابی این‌چنین فراگیر نداشته است. مهم‌ترین عامل این پدیدهٔ شگفت‌انگیز، دستیابی بشر به ابزاری کارامد به نام «فنّاوری اطلاعات و ارتباطات»[1] است. این فنّاوری، که به‌اختصار «فاوا» نیز نامیده می‌شود، قدرتی به انسان امروز می‌دهد که می‌تواند انواع اطلاعات را در قالب‌های گوناگون ذخیره و با سرعتی بی‌مانند پردازش کند و در دسترس همگان قرار دهد. بهره‌گیری از این فنّاوری، با ویژگی‌های بی‌مانندی که دارد، ساختارها و مأموریت‌های سازمانی را با دگرگونی‌های بنیادینی روبه‌رو می‌کند که هیچ سازمانی از آن بی‌بهره نمانده است؛ به‌گونه‌ای که همهٔ دولت‌ها و سازمان‌ها، با بهره‌گیری از این ظرفیت، سعی دارند وضعیت انجام شدن مأموریت‌ها را بهبود بخشند. در آغاز، لازم است بنیان‌ها و مبانی فنّاوری اطلاعات و ارتباطات را بشناسیم و با برخی از مفاهیم پایه‌ای و پرکاربرد این مبحث آشنا شویم. این فنّاوری از دو بخش درهم‌تنیدهٔ اطلاعات و ارتباطات برآمده است. برای آشنایی با پیشینهٔ فنّاوری اطلاعات و ارتباطات بهتر است هر یک از این دو بخش را جداگانه بررسی کنیم (دوست‌محمدیان، ۱۳۸۹: ۲۵).

فنّاوری اطلاعات و ارتباطات عبارتی کلی و دربرگیرندهٔ تمامی فنّاوری‌های پیشرفته و شیوهٔ ارتباط و انتقال داده‌ها در سامانه‌های ارتباطی است. این سامانه ممکن است شبکه‌ای مخابراتی، چندین رایانهٔ مرتبط با هم و متصل به شبکهٔ مخابراتی، اینترنت و همچنین برنامه‌های به‌کار رفته در آنها باشد. از کارکردهای مهم فنّاوری اطلاعات و ارتباطات می‌توان به «دولت الکترونیک» اشاره کرد. در واقع دولت الکترونیک وامدار فنّاوری اطلاعات و ارتباطات است. به‌کارگرفتن شبکهٔ اینترنت در سازمان‌های دولتی برای عرضهٔ خدمات و اطلاعات به مردم، شرکت‌ها و دیگر سازمان‌های دولتی یکی از تعریف‌های دولت الکترونیکی است. متخصصان و کارشناسان، دولت الکترونیکی را سازمانی مجازی

---

1. information & communication technology.

بدون ساختمان و دیوار توصیف می‌کنند که خدمات دولتی را بدون واسطه، به‌صورت ۲۴ساعته و طی هفت روز هفته در اختیار مشتریان قرار می‌دهد. به‌عبارتی دولت الکترونیکی به مجموعهٔ ارتباطات الکترونیکی میان دولت، شرکت‌ها و شهروندان و کارکنان دولت گفته می‌شود که از طریق شبکهٔ اینترنت شکل می‌گیرد (پورمراد، ۱۳۸۹: ۹۳).

اهمیت و ضرورت فنّاوری اطلاعات و ارتباطات: امروزه وضعیت فنّاوری اطلاعات و ارتباطات در کشورها، شاخصی برای برآورد توسعه‌یافتگی اقتصادی آنها به‌شمار می‌آید. گسترش سریع فنّاوری اطلاعات و ارتباطات در طول دو دهه، سبب بروز دگرگونی شگرفی در همهٔ نظام‌های اداری و مالی، حتی در شرکت‌های متوسط و کوچک شده و در بسیاری از موارد بنگاه‌های چندنفرهٔ تجاری را نیز دستخوش دگرگونی کرده است. دستاوردهای انقلاب فنّاوری اطلاعات و ارتباطات همراه با پیشرفت‌هایی در دیگر زمینه‌های دانش و فنّاوری، شکاف‌های تازه‌ای پدید آورده و به نابرابری‌های گذشته عمق بیشتری داده است. بخشی از جهان به دلیل‌های بسیاری توانسته است با ایجاد زیرساخت‌ها و بنیان‌ها و ظرفیت‌های لازم در زمینهٔ دانش و فنّاوری، پیشرفت پی‌درپی داشته باشد؛ آن‌گونه که بیشتر سهم بازارهای تولید و مصرفی فنّاوری پیشرفته را به خود اختصاص داده و دارای توانایی بالایی برای جذب این پیشرفت‌ها در حل مسائل و گسترش قابلیت‌ها و ظرفیت‌سازی شده است؛ در نتیجه، سریع‌تر و بهتر ثروت تولید می‌کند و دانش‌های پیشرفته را در خدمت تولید ثروت به‌کار گرفته است (دادگر،۱۳۹۱: ۱۸).

کارکرد فنّاوری اطلاعات و ارتباطات در سازمان‌ها: بررسی‌ها نشان می‌دهد سازمان‌ها از فنّاوری اطلاعات در چهار زمینه بیشتر بهره می‌گیرند:

- امور پردازش اطلاعات؛
- تصمیم‌گیری؛
- اشتراک اطلاعات؛
- نوآوری.

در امور پردازشی، سازمان با کمک فنّاوری اطلاعات به گردآوری، تبدیل، ایجاد، نگهداری، ثبت و ارسال اطلاعات می‌پردازد. در تصمیم‌گیری نیز می‌توان سامانه‌های پشتیبانی

تصمیم و یا سامانه‌های خبره را از ابزارهای فنّاوری اطلاعات به‌شمار آورد. به‌کارگیری فنّاوری اطلاعات چه بسا به نوآوری در سازمان، در زمینهٔ عرضه کالا یا خدمات و حمایت از مشتریان، و ایجاد برتری رقابتی بینجامد. امروزه به‌کارگیری فنّاوری اطلاعات بخشی جداناشدنی در مشاغل، به‌ویژه مشاغل مدیریتی است. مدیران باید بتوانند به‌شکلی کارشناسان فنی را ملزم کنند تا از نوآوری‌های فنّاوری در تغییر ماهیت مشاغل و امور سازمان، با هدف بهره‌وری و اثربخشی بیشتر استفاده کنند. اگر سیر تحول فنّاوری اطلاعات را از ابعاد و جنبه‌های گوناگون بررسی کنیم، می‌بینیم که در بعد شبکه‌ها، اینترنت و اکسترانت هر یک جنبه‌های گوناگونی داشته‌اند که به‌مرور زمان تکمیل شده است. در بعد اطلاعات مدیریت نیز مباحثی همچون: MIS، TPS، OAS، AI، KBS، ES و DSS و در بعد کاربرد، جنبه‌هایی مانند: روباتیک، ERP، MRP، CRM، SCM و WFM بوده است که هر یک به‌تنهایی سیر تحولی خود را داشته‌اند. در بعد فنّاوری محض نیز در جنبه‌های سخت‌افزار و نرم‌افزار و سازوبرگ ارتباطی، تا کنون سیری تکاملی طی شده است و جنبه‌های متنوعی هم در بعد جغرافیایی، شامل GIS و GPS دیده می‌شود (اروسخانی، ۱۳۸۷: ۴۳).

جنگ و فنّاوری اطلاعات و ارتباطات

جنگ و تاریخچهٔ آن: علاقه به حیات و حفظ بقا به‌طور غریزی در هر انسانی وجود دارد؛ بنابراین، در طول تاریخ بشر برای دستیابی به نیازهای خود، معدن‌ها و زمین‌های کشاورزی را گسترش داده یا برای راندن دشمنان خود، نبردهای بسیاری را پشت‌سر نهاده است؛ به‌همین دلیل، تجربه‌های گسترده‌ای از برخوردهای نظامی و جنگ‌ها به‌دست آورده و زیان‌های جانی و مالی بسیاری دیده است.

گستردگی جنگ به‌حدی است که به جرئت می‌توان گفت هیچ نقطهٔ مسکونی روی کرهٔ زمین از آن در امان نبوده است. کشورهای مستقل و انقلابی در دنیای امروز، به‌منظور دفاع و مقابله با تهدیدهای احتمالی قدرت‌های بزرگ، ناگزیر به بهره‌گیری از شیوه‌های عملیاتی نو و منحصر به‌فرد هستند تا در شرایطی نابرابر از نظر سطح فنّاوری و تسلیحات و توان رزمی، به دفاع روی آورند.

جنگ‌ها به انواع و نسل‌های متفاوتی تقسیم‌بندی شده‌اند؛ جنگ‌های نسل اول، دوم، سوم و چهارم مبتنی بر میدان جنگ و عرصهٔ نظامی است؛ اما شکل جنگ‌ها در نسل پنجم و ششم تغییر یافته است. در نسل پنجم و ششم، استفاده از تسلیحات نظامی پیشرفته و عملیات روانی و رسانه‌ای مطرح می‌شود (دادگر، ۱۳۹۱: ۱۴۰).

انواع جنگ اطلاعات

جنگ نرم: در محیط جنگ نرم، دشمن تلاش می‌کند به‌کمک ابزارهای نرم همچون تغییر باورها و ارزش‌ها و دیدگاه‌ها، حذف روابط میان اعضای جامعه، حذف وحدت و یکپارچگی استیلای فرهنگی، ایجاد وابستگی علمی و بسیاری راه‌کارهای دیگر، بدون اقدام نظامی، حریف را به تغییر رفتار و عمل مطابق خواسته‌هایش متمایل کند. در این حالت، به نیت و مقاصد طرف مقابل توجه می‌شود. به‌منظور رسیدن به این هدف، دشمن نیازمند به‌دست‌آوردن جذابیت و پذیرش در ذهنیت مخاطبانش است.

در وضعیت منطقی، دشمن تا هنگامی که از اثربخش‌نبودن جنگ نرم اطمینان حاصل نکند و ناکارامدی آن برای وی اثبات نشود، به مرحلهٔ جنگ سخت یا حملهٔ نظامی وارد نخواهد شد؛ اگرچه تهدیدهای سخت و حتی ایجاد بحران سخت در دستورکارش باشد (امیرصوفی، ۱۳۸۹: ۳۷).

جنگ رایانه‌ای (سایبری): به هرگونه عمل از روی دشمنی علیه سامانه‌ها، شبکه‌ها یا پایگاه‌های دادهٔ رایانه‌ای دشمن گفته می‌شود که با هدف کاهش کارایی یا ناتوان‌سازی صورت پذیرد. حمله‌های رایانه‌ای، سامانه‌های هدف خود را از کار می‌اندازند، با تزریق اطلاعات نادرست توان تصمیم‌گیری کاربران را کاهش می‌دهند و حتی منجر به سرقت اطلاعات می‌شوند. به بیانی دیگر، جنگ رایانه‌ای عبارت است از به‌کارگیری برنامه‌ریزی شدهٔ عملیات آفندی و پدافندی که در آن ابزاری رایانه‌ای علیه ابزار رایانه‌ای دیگری حمله‌هایی صورت می‌دهد. در کنار اینها، به‌کارگیری ابزارها و شبکه‌های رایانه‌ای، با قصد قبلی، به‌منظور اثرگذاری در تصمیم‌گیری مخاطبان را نیز باید در زمرهٔ این جنگ به‌شمار آورد. این نوع جنگ ممکن است در تمامی قشرها؛ یعنی مردم و دولت و نظامیان، اثرگذار باشد (امیرصوفی، ۱۳۸۹: ۳۷).

جنگ روانی: شیوهٔ مؤثری است برای بهره‌برداری از نقاط ضعف روانی نیروهای دشمن، با هدف ایجاد ترس و سردرگمی و ناتوانی در آنها که سرانجام تضعیف روحیهٔ طرف مقابل را دربرخواهد داشت. جنگ روانی ممکن است به دفاع یا حفاظت از کارکنان و منابع نظامی، با پیشگیری از اقدام‌های خصمانهٔ دشمن و منصرف‌کردن فرماندهان دشمن از اقدام‌های زیان‌بار برای نیروهای خودی یا مقابله با تأثیر تبلیغات دشمن، کمک کند. راه‌کنش‌های متنوعی در جنگ‌های روانی به‌کار گرفته می‌شوند که برخی از مهم‌ترین آنها عبارتند از: ترساندن، تهدید، تطمیع، شست‌وشوی مغزی، فریب، ضدفریب و عملیات امور همگانی (دوست‌محمدیان، ۱۳۹۲).

حفاظت و امنیت فنّاوری اطلاعات و ارتباطات با رویکرد پدافند غیرعامل

برای ایجاد امنیت باید به جنبه‌های گوناگون رایانه و شبکهٔ رایانه‌ای توجه کرد. این ابعاد عبارتند از:

- **بعد فیزیکی:** در این بعد به بحث مکان‌ها، واپایش آمدوشد، سخت‌افزارها، تشعشع‌ها و... پرداخته می‌شود؛
- **بعد انسانی:** در این مبحث به صلاحیت کارکنان، آموزش دادن آنها و میزان دسترسی توجه می‌شود؛
- **بعد فرایند امور:** به‌معنای شیوه‌ها، سیاست‌ها و دستورکارهای مرتبط با امنیت است؛
- **بعد فنی:** به مباحث فنی از جمله سیستم عامل، بانک اطلاعاتی، کاربرد و شبکه پرداخته می‌شود (پورمراد، ۱۳۸۹: ۲۲).

هدف‌های حفاظت و امنیت فنّاوری اطلاعات با رویکرد پدافند غیرعامل

- **محرمانگی:** حفاظت و اعتمادپذیری یا همان محرمانه‌بودن به مفهوم حفاظت داده‌های شبکه‌های رایانه‌ای در برابر دسترسی‌های غیرمجاز است؛
- **فراگیربودن:** یا یکپارچگی، به‌مفهوم تأمین دقت و همه‌شمول بودن اطلاعات و نرم‌افزارهای رایانه‌ای است. حفظ فراگیر بودن، در اصل، یعنی حفاظت داده‌ها در برابر تغییرهای غیرمجاز و نامطلوب عمدی یا سهوی؛

- **دسترسی‌پذیری:** دسترسی یا دسترسی‌پذیری به‌معنای ضمانت دسترسی به اطلاعات و خدمات حساس در زمان مورد نیاز است و به زبان ساده‌تر، یعنی آمادۀکار بودن یا پای‌کاربودن شبکۀ رایانه‌ای و اطمینان از اینکه شبکۀ رایانه‌ای همواره برای کاربران مجاز در دسترس و قابل بهره‌برداری باشد؛
- **انکار ناشدنی بودن:** بدین معناست که گیرندۀ پیام اطمینان حاصل کند پیام از سوی همان کسی است که ادعا می‌کند و فرستندۀ پیام نتواند ارسال پیام خود را انکار کند. برای این منظور، از امضای الکترونیکی استفاده می‌شود (پورمراد، ۱۳۸۹: ۲۱).

استانداردهای حفاظت و امنیت فنّاوری اطلاعات با رویکرد پدافند غیرعامل

فنّاوری اطلاعات همان‌طورکه فرصت قلمداد می‌شود، در صورت نداشتن سازوکار امنیتی کارامد، تهدیدی جدی و خطرناک نیز به‌شمار می‌رود؛ بنابراین، اگر به همان نسبتی که به گسترش آن توجه می‌شود مقولۀ امنیت آن در نظر گرفته نشود، ممکن است به‌سادگی و در زمانی کوتاه به تهدید تبدیل گردد. مهم‌ترین نگرانی امنیتی مرتبط با سامانه‌های اطلاعاتی شامل: نفوذی‌های سامانه، دزدی اطلاعات، نفی خدمات، تغییر و از بین بردن اطلاعات و مانند آن است. بدیهی است که در این شرایط، روش‌های حفاظت فیزیکی به‌تنهایی قادر به تأمین امنیت نخواهند بود و به ناچار باید از روش‌های جدید حفاظت اطلاعات و واپایش دسترسی به منابع سازمان استفاده شود. استانداردهای امنیت فنّاوری اطلاعات، در اصل مجموعه‌ای از اقدام‌های مطالعه شده و مطمئن هستند که امنیت شبکۀ رایانه‌ای را تضمین می‌کنند و به‌منظور ایجاد و تداوم امنیت فنّاوری اطلاعات، تولید و عرضه شده‌اند؛ بنابراین، مطالعه و بررسی استانداردهای موجود از اهمیت خاصی برخوردار است. در ادامه برخی از مهم‌ترین استانداردهای امنیت اطلاعات معرفی می‌شود:

استاندارد ISO۱۷۷۹۹ و ISO۲۷۰۰۱: ایزو ۱۷۷۹۹ به‌رسمیت شناخته شده‌ترین استاندارد امنیتی است که مسائل امنیتی را تا حد بسیاری پوشش داده و شامل واپایش‌های ضروری و بسیار پیچیده است. این استاندارد تفصیلی در ده بخش اصلی سازماندهی شده است و هر یک

محدودهٔ متفاوتی را دربر می‌گیرد. اصلی‌ترین واپایش‌های مورد بررسی در این استاندارد عبارتند از: برنامه‌ریزی کسب‌وکار، واپایش دسترسی به سامانه، گسترش و نگهداری سامانه، امنیت فیزیکی پذیرش، امنیت کارکنان، سازماندهی امنیت، سیاستگذاری امنیتی، حفاظت از امکانات در برابر خطرهای طبیعی و ساختگی و مانند آنها. رویکرد این استاندارد فنی است و توجه کمتری به عوامل انسانی در زمینهٔ امنیت دارد.

استاندارد NIST۸۰۰: طبق این استاندارد، پیاده‌سازی واپایش‌های امنیتی مناسب برای سامانهٔ اطلاعاتی و ارتباطی وظیفهٔ مهمی است که ممکن است آثار عمده‌ای در عملکرد و دارایی سازمان داشته باشد. واپایش امنیت در واقع محافظت یا مقابلهٔ مدیریتی، عملیاتی و فنی در نظر گرفته شده برای سامانهٔ اطلاعاتی و ارتباطی به‌منظور محافظت از محرمانگی و یکپارچگی و در دسترس بودن سامانه و اطلاعات آن است؛ گرچه این استاندارد نیز ممکن است همانند استاندارد پیشین کاربردهای بسیاری در تأمین امنیت فیزیکی داشته باشد، لیکن نقاط ضعف مهمی از منظر پدافند غیرعامل در آن آشکار است. این استاندارد مانند استانداردهای خانوادهٔ ISO ۲۷۰۰۰، به مخابرات ناشی از عوامل انسانی توجه کافی نداشته است.

استانداردهای FIPS: استاندارد FIPS۱۹۹ واپایش‌هایی را برای طبقه‌بندی سامانه‌های فنّاوری اطلاعات و ارتباطات با عنوان تأثیر اندک یا متوسط یا بالا، بر اثر نقض محرمانگی و یکپارچگی و دسترس‌پذیر بودن سامانه، انتشار داده است. استاندارد FIPS۲۰۰ کمترین امنیت مورد نیاز را در چندین بخش امنیتی تنظیم می‌کند. واپایش دسترسی شامل: آموزش، مسئولیت‌پذیری، مدیریت تنظیمات، نگهداری، امنیت کارکنان، محافظت از سامانه و ارتباطات و موارد دیگر است. در این دو استاندارد، همانند دیگر استانداردهای مورد اشاره، به مبحث مهندسی اجتماعی کمتر توجه شده است. از دیگرسو، کمینهٔ مطلوب امنیت، در موضوع‌های مورد بحث این استاندارد، بر اساس تراز تهدید جرم تعریف شده است (پورمراد، ۱۳۸۹: ۴۷).

استاندارد ISF: این استاندارد مجموعهٔ تجربه‌های بیش از ۲۶۰ شرکت و سازمان بین‌المللی معتبر در زمینهٔ اطلاعات و به‌سازی امنیت اطلاعات آنهاست. در طول شانزده سال

این استاندارد بیش از ۷۵ میلیون دلار برای گردآوری اطلاعات موثق و درست برای اعضای خود هزینه کرده است. احتمالاً مهم‌ترین ویژگی این استاندارد، نشان دادن مجموعهٔ بسیار گسترده و دربرگیرنده‌ای از تمامی عنوان‌های مربوط به مدیریت خطرپذیری اطلاعات در دنیاست. برخی از نکته‌های اصلی این استاندارد در قالب مجموعه‌ای به نام «استاندارد تجربهٔ برتر» برای رسیدن به هدف‌های زیر در اختیار قرار گرفته است:

- ایجاد زمینه برای افزایش سطح امنیت اطلاعات سازمان‌ها در سرتاسر جهان؛
- کمک به سازمان‌ها و شرکت‌هایی که عضو این استاندارد نیستند؛ به‌منظور بهبود وضعیت امنیتی خود و کاهش خطرهای امنیتی در سطح مطلوب؛
- کمک عملی به تولیدکنندگان استانداردها برای مشخص‌کردن ناحیه‌ها و کاهش خطر اطلاعاتی در یک مجموعه (پورمراد، ۱۳۸۹: ۸۶).

به این دلیل که بسیاری از سازمان‌ها و مراکز مهم برای پیاده‌سازی استانداردها به برون‌سپاری روی می‌آورند، زمینه برای گردآوری اطلاعات به‌دست‌آمده در مورد نقاط ضعف و آسیب‌پذیری‌های سازمان و انتشار آن به بیرون از سازمان فراهم می‌شود.

حفاظت مخابرات (فنّاوری ارتباطات)

حفاظت مخابرات عبارت است از تمامی اقدام‌هایی که سبب می‌شود افراد غیرمجاز نتوانند به اسناد و مدارک باارزش و طبقه‌بندی مخابراتی و شبکه‌های ارتباطی دسترسی پیدا کنند و یا در تفسیر و تحلیل اطلاعات به‌دست‌آمده فریب بخورند و دچار گمراهی شوند (اروسخانی، ۱۳۸۷: ۱۴).

امنیت ارتباطات مجموعه‌ای از ابزارها برای پیشگیری از سرقت، حمله، جاسوسی و خرابکاری و دانش مطالعهٔ روش‌هایی است که در برابر دسترسی و تغییرهای غیرمجاز در نظام‌های ارتباطی و مخابراتی و حتی ارتباطات رایانه‌ای، از مبادلهٔ داده‌ها در سامانه‌های ارتباطی حفاظت می‌کند؛ بنابراین، با استفاده کردن سازوکارهای امنیت مخابرات، احتمال وقوع خطر به کمترین میزان ممکن می‌رسد و در صورت عملی شدن تهدید، خسارت‌های وارد شده را در

حد بسیار ناچیز نگاه خواهد داشت. با در پیش‌گرفتن تدبیرهای حفاظت مخابرات از نفوذ الکترونیکی، شنود، پخش پارازیت یا پیام‌های فریبنده جلوگیری خواهد شد.

ناجا، پدافند غیرعامل و فنّاوری اطلاعات و ارتباطات

مأموریت پلیس در گذشته، تهدید محور و مبتنی بر مقابله با تهدیدهای رخ داده بود؛ اما امروزه پلیس به‌یاری ویژگی‌های منحصر به فرد دوران اطلاعات و فنّاوری ارتباطات، با استفاده از سامانه‌های مراقبت و واپایش نامحسوس و کسب اطلاعات رایانه‌ای، اقدام‌های خود را از مرحلهٔ برخورد به مرحلهٔ پیشگیری انتقال داده است. برابر مادهٔ ۲ قانون ناجا، این نیرو مسئول برقراری نظم و امنیت در جامعه است و با توجه به مسئولیت بسیار مهمی که برعهده دارد، باید ابزارهای نوین را در اوج دقت با توجه به محدودیت به‌کار ببرد. استفاده از ابزارهای فنّاوری اطلاعات و ارتباطات در دامنهٔ مدیریت نیروی انتظامی از چندین سال پیش آغاز شده است و ناجا از جمله دستگاه‌های پیشرو در حوزهٔ استفاده از فنّاوری اطلاعات و ارتباطات شمرده می‌شود. برای اینکه بتوان خدمات مطلوب برای مردم را به‌خوبی مدیریت و پشتیبانی کرد، به ناچار نمی‌توان ابزاری به‌غیر از فاوا را به‌کار برد. برای نمونه، بدون اتکا به فنّاوری اطلاعات، امکان ندارد تخلف‌های رانندگی انبوه را در سطح کشور ثبت و به‌صورت متمرکز پردازش کرد؛ همچنین تعیین پیشینهٔ کیفری افراد و پاسخگویی به نیاز مراجعان در این بخش ناممکن می‌شود. سازوبرگ و سامانه‌های مربوط به فاوا، بر اساس نیازمندی‌های مأموریتی نیروی انتظامی، در سه بخش کلی تقسیم‌بندی شده‌اند که به شرح زیر به آنها اشاره می‌کنیم:

- سازوبرگ و سامانه‌های مراقبت الکترونیکی: تأمین‌کنندهٔ اطلاعات مورد نیاز فرماندهی از صحنه‌ها و میدان‌های عملیاتی است و در افزایش دقت، توان عملیاتی یگان‌ها و پایش هم‌زمان نقاط گوناگون شهر کاربرد دارند؛
- شبکه‌های مخابراتی ثابت و سیار: در انتقال اطلاعات صحنه به مراکز فرماندهی و نیز انتقال دستورها و هماهنگی بین فرماندهی و نیروهای عمل‌کننده به‌کار می‌رود؛ بنابراین،

با توجه به گسترش جغرافیایی یگان‌های ناجا و اجرای درست و به‌هنگام تدبیرهای سازمانی، نقش سامانه‌های مخابراتی به‌طورکامل مشهود است؛

- سامانه‌های پردازش و مدیریت اطلاعات: این سامانه‌ها نقش نگهداری، تحلیل، تفسیر، توزیع و تسهیم اطلاعات و دانش را دارند. سامانه‌های فراگیر نرم‌افزاری موجود در پلیس‌های تخصصی و ستادی ناجا ظرفیت لازم را برای عملیات، خدمات و پشتیبانی مأموریت‌های ناجا فراهم می‌آورند.

در توضیح هر یک از سه قطب فنّاوری موجود در ناجا، باید به موارد زیر اشاره و بر آنها تأکید کرد:

- مراقبت الکترونیکی در بهره‌گیری نیروهای پلیس از ابزارهای الکترونیکی، به‌منظور پایش و کسب اطلاعات از صحنه‌ها و میدان‌های عملیاتی یا تعقیب مجرمان و واپایش آمدوشد و موارد دیگر، کاربرد دارد. در واقع از ابزارهای الکترونیکی برای تقویت حواس و توانایی تشخیص استفاده می‌شود. حسگر مهم‌ترین عنصر سامانهٔ مراقبت الکترونیکی است که آثار منتشر شده از صحنه یا هدف‌ها را که به‌طور معمول به یکی از گونه‌های انرژی است (مانند نور، صوت، امواج رادیویی یا حرارتی، پرتوی ایکس یا لیزر) به‌صورت تصویر، نشانه یا توصیف دیگری برای مشاهده‌کننده مجسم می‌کند و شامل گونه‌هایی چون حسگرهای نوری یا دوربین‌های ثبت عکس و ویدئو، حسگرهای رادیویی یا رادارها، حسگرهای حرارتی، حسگرهای فرابنفش، حسگرهای لیزری، حسگرهای صوتی (شامل صدابر لرزه‌نگار و مانند آن)، حسگرهای موقعیت و تعادل و حسگرهای شیمیایی می‌شود.
- سامانهٔ مخابراتی ناجا به‌گونه‌ای است که شبکه مقرهای گوناگون ناجا را به یکدیگر متصل می‌کند. در واقع، شبکهٔ مخابراتی نیروی انتظامی مانند تلفن منزل است که همهٔ افراد از آن استفاده می‌کنند. شبکه‌های مخابراتی ثابت ناجا از طریق سخت‌افزارهای گوناگون انبوهی شکل گرفته است؛ شامل انواع سوئیچ‌های دیجیتالی تلفنی و داده با ظرفیت‌های مناسب، شبکه‌های کابلی توزیع، مالتی‌پلکسرها و شبکه‌های انتقال و رادیویی ماکروویو (امواجی با طول موج بلند) خطوط انتقال پرظرفیت فیبر نوری، سوئیچ‌ها و مسیریاب‌های IP، مودم‌های تلفنی و DSL (برای انتقال داده‌ها به جاهایی

که شبکهٔ WAN هنوز در آن گسترش نیافته است) و دستگاه‌های انتقال تلفن روی شبکهٔ داده VOIP (برای جاهایی که شبکهٔ توزیع تلفن آنها هنوز کامل نشده است).

در مورد شبکه‌های رایانه‌ای هم وضع به همین صورت است؛ یعنی سامانهٔ رایانه‌ای کل ناجا به شبکه‌ای واحد به نام «شبکهٔ امین» متصل است. سامانه‌های پردازش و مدیریت اطلاعات نیز حلقهٔ تکمیلی سامانهٔ مدیریت دانش ناجا را شکل می‌دهند که وظیفهٔ نگهداری، تسهیم و توزیع، تولید و به‌کارگیری، ارزیابی و گسترش دانش را برعهده دارند. این سامانه که آن را گسترهٔ نرم‌افزار و سامانهٔ فراگیر نیز می‌شناسند، خدمات متنوع فنّاوری اطلاعات را به مردم عرضه می‌کند؛ مانند دفترهای پلیس+۱۰ که خدماتی را برای کارهای عملیاتی، پشتیبانی و مواردی همچون صدور گذرنامه، دریافت جریمه‌های رانندگی، اماکن، دریافت عدم سوء پیشینه و به‌طورکلی خدماتی که عرضهٔ آنها نیازمند سرعت و دقت بیشتری است، به‌صورت الکترونیکی در اختیار می‌گذارد.

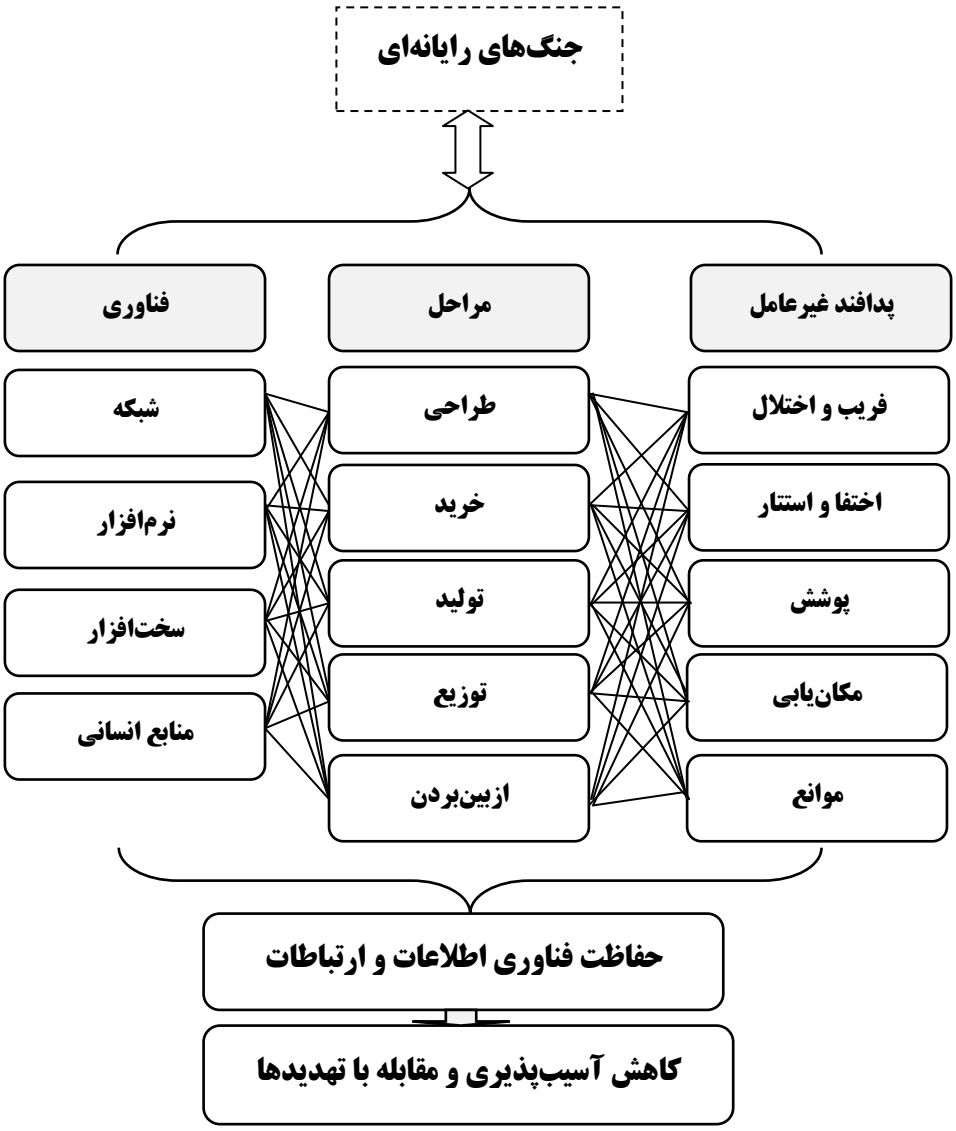
نیروی انتظامی با توجهٔ ویژه به امنیت فضای رایانه‌ای در سال‌های اخیر، به ایجاد پلیس تخصصی فضای تولید و تبادل اطلاعات (پلیس فتا) اقدام کرده و با آموزش‌های تخصصی کارکنان در این بخش، در راستای امنیت فضای رایانه‌ای کشور گام‌های اساسی برداشته است. از سویی، مطالبات فراوان و رو به رشد شهروندان در راستای نیاز به خدمات انتظامی، لزوم ارتقای کیفیت انجام مأموریت‌ها، پاسخگویی به‌موقع به مطالبات، کاستن از رویارویی فیزیکی کارکنان پلیس با افراد و مواردی از این دست، از ضرورت‌هایی است که حرکت در مسیر نرم‌افزاری را دوچندان کرده است.

کاربرد اینترنت در ناجا

از بستر جهانی اینترنت در ناجا برای امور پژوهشی در قالب ایستگاه‌های مشترک استفاده می‌شود. این کاربرد به وب‌گردی در محیط‌های مجاز محدود است اما چارچوب مأموریت‌های محول، استفاده از اینترنت نامحدود برای پلیس‌های تخصصی (مانند پلیس اطلاعات و امنیت عمومی، پلیس فتا، پلیس مبارزه با مواد مخدر) با هماهنگی ساحفاناجا صادر می‌شود (پورمراد، ۱۳۸۹: ۷۷).

الگوی مفهومی تحقیق

نظر به الگوی تحلیلی تحقیق دربارهٔ طرح پژوهش، الگوی زیر پیشنهاد می‌شود:



شکل شماره ۱- الگوی مفهومی تحقیق

روش تحقیق

در این بخش، ابتدا نوع و روش تحقیق را معرفی و سپس جامعه، روش نمونه‌گیری و میـزان نمونه را مشخص می‌کنیم. همچنین به ابزار گـردآوری اطلاعـات، روش مطالعـه، متغیرهـای تحقیق، تعریف عملیاتی متغیرها، روایی و پایایی و شیوه‌های تحلیل داده‌ها می‌پردازیم.

تأیید فرضیه‌های تحقیق

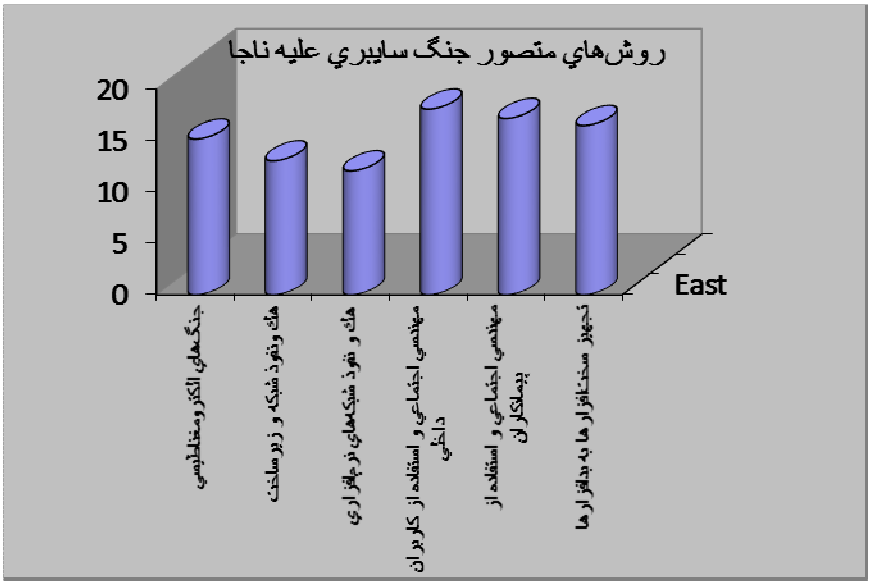
بررسی فرضیهٔ نخست: پرسش اصـلی: وضـعیت رویکـرد حفاظـت فنّـاوری اطلاعـات در جنگ‌های رایانه‌ای علیه ناجا، با رویکرد پدافند غیرعامل چیست؟

جدول شماره ۱- ابعاد سه‌گانهٔ پرسش‌ها

بُعد نخست	۱۶/۳۸
بعد دوم	۱۶/۶۶
بعد سوم	۱۶/۵۳
میانگین پرسش‌ها: ۱۶/۵۲	

میانگین امتیاز پرسش‌های بُعد نخست، یعنی جنگ‌هـای رایانـه‌ای ممکـن علیـه ناجـا ۱۶/۳۸ است که در سطح خیلی خوب و متناسب قرار می‌گیـرد، امـا بـا بررسـی پرسـش‌هـا آشـکار می‌شود که هنوز عامل انسانی و مهندسی اجتماعی بـرای نفـوذ، کـارکرد فراوانـی دارد و بـا وجود هزینه‌های صورت گرفته برای امن‌سازی سامانه‌ها و زیرساخت‌ها، دشمن در نظر دارد از کاربران سامانه‌ها و پیمانکاران آنها، به منزلهٔ سرپل نفوذ به سامانه‌هـای فنّـاوری اطلاعـات ناجا استفاده کند.

پرسش فرعی اول: انواع جنگ رایانه‌ای و روش‌های مقابله برای آن در ناجا کدام‌اند؟



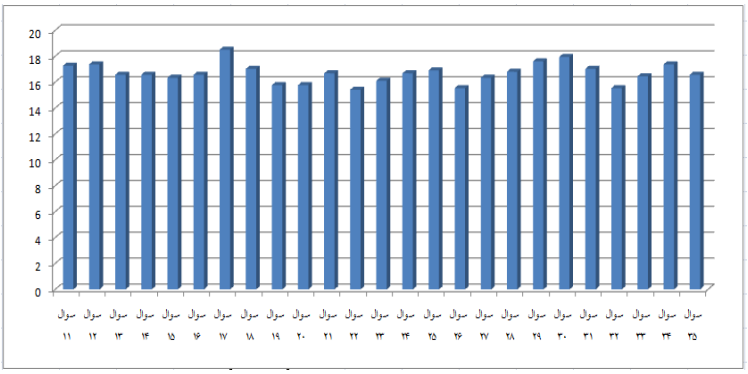
نمودار شماره ۱- روش‌های در نظر گرفته شدهٔ جنگ رایانه‌ای علیه ناجا

بهره‌گیری از فنّاوری اطلاعات در ناجا در راستای مأموریت‌های سازمانی جایگاه ویژه‌ای دارد. امروزه بیش از دویست سامانه و زیرسامانه در ناجا فعالیت دارد که همگی دارای اطلاعات ارزشمندی هستند و از این‌رو، نقشی ویژه نیز در سطح فنّاوری اطلاعات کشور و تحقق دولت الکترونیک دارند. بررسی اطلاعات میدانی نشان می‌دهد که درصد هک و نفوذ به زیرساخت‌های ناجا و نرم‌افزارهای سازمانی، به‌علت داشتن اینترنت اختصاصی، بسیار سخت است و تاکنون مهندسی اجتماعی و یا بهره‌گیری هدفمند عوامل درون سازمانی به‌منزلهٔ سرپل نفوذ دشمنان، برای دسترسی به سامانه‌های فراگیر ناجا و تحقق هدف‌های جنگ رایانه‌ای برضد ناجا (نفوذ اجتماعی) دارای پیشینه بوده است که با نتایج پرسشنامه همخوانی دارد.

پرسش فرعی دوم: وضعیت امنیت فنّاوری اطلاعات و ارتباطات در ناجا چگونه است؟

به‌طور کلی می‌توان وضعیت امنیت فنّاوری اطلاعات در ناجا را در سطح مناسبی ارزیابی کرد که البته امتیاز حاصل شده از نظریهٔ کارشناسان، یعنی امتیاز ۱۶/۶۶ نیز بیانگر همین

موضوع است. همان‌طور که در نمودار زیر مشاهده می‌شود برخی از شاخص‌ها همچون استفاده از راه‌کارهای هوشمند پایش امنیت فنّاوری اطلاعات، امتیازی کمتر از میانگین امتیازهای موجود دارند.



نمودار شماره۲ – وضعیت امنیت فنّاوری اطلاعات ناجا

جدول شماره۲ – فهرست و امتیازهای پرسش‌هایی که کمتر از میانگین هستند

شمارهٔ پرسش	شرح پرسش	امتیاز
پرسش ۱۹	نصب و به‌کارگیری نرم‌افزارهای تصویب نشده و بدون مجوز	۱۵/۷۷
پرسش ۲۰	تنظیم‌های امنیتی سیستم عامل، خدمات دهنده‌ها، نرم‌افزارها و خدمات امنیتی نرم‌افزاری مانند دیوارهای آتش	۱۵/۴۲
پرسش ۲۲	تأمین سخت‌افزار از داخل کشور و از طریق ودجا	۱۵/۵۴
پرسش ۲۶	توجه به حفاظت و عایق‌کاری مراکز فاوا، به‌منظور مقابله با بمب‌های الکترومغناطیسی	۱۵/۵۴
پرسش ۳۲	بهره‌گیری از سامانه‌های هوشمند و آنی برای تحلیل خطرها و هشداردهی، مانند مرکز امنیت اطلاعات (SOC)	۱۵/۵۴

نتایج بررسی میدانی امنیت فنّاوری اطلاعات ناجا و آمار شکست‌های حفاظتی بیانگر این موضوع است که وضعیت امنیت فنّاوری اطلاعات ناجا در سطح بسیار خوبی قرار دارد و در بسیاری از مسائل، مباحث مرتبط با پدافند غیرعامل در گسترهٔ فنّاوری اطلاعات نیز اجرایی شده است. به‌طور میانگین، می‌توان امنیت فنّاوری اطلاعات ناجا را با ضریب بالای

۹۰ درصد امتیازدهی کرد. البته نتیجهٔ بررسی‌های میدانی با نظریهٔ خبرگان اختلاف ۱۰ درصدی دارد که طبیعی است.

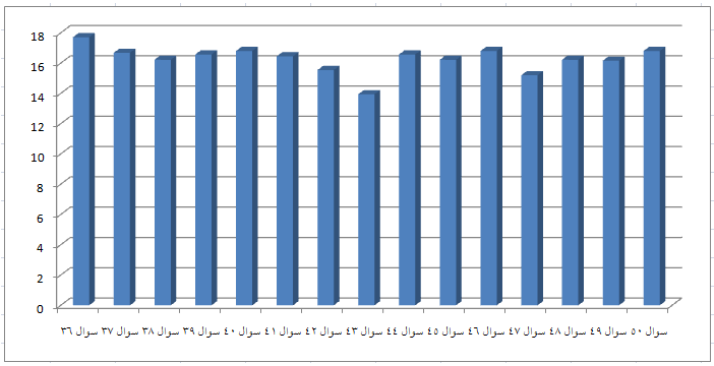
پرسش فرعی سوم: وضعیت شاخص‌های پدافند غیرعامل در گسترهٔ فنّاوری اطلاعات و ارتباطات ناجا چگونه است؟

رعایت امنیت با شاخص‌های پدافند غیرعامل مؤلفه‌هایی دارد که خوشبختانه در نیروی انتظامی جمهوری اسلامی ایران به آن توجه و سازوکار آن به‌طور کامل طراحی شده و در دست اجرا و واپایش است. البته برخی از موارد به شرح جدول زیر، امتیازی کمتر از میانگین دارند که باید بیشتر مورد توجه باشند.

جدول شماره ۳- پرسش‌های بعد سوم که از میانگین امتیازها کمترند

شمارهٔ پرسش	شرح پرسش	امتیاز
پرسش ۴۲	ساماندهی و راه‌اندازی ساختار مدیریت امنیت اطلاعات، مراکز امداد و نجات رایانه‌ای (CERT)، مراکز امنیت عملیات (SOC)	۱۵/۵۴
پرسش ۴۳	تأمین نیازمندی‌های پشتیبانی فنی همچون خطوط برق موازی و اضطراری، خطوط ارتباطی موازی برای بخش‌های مهم و مراکز حیاتی حساس	۱۳/۹۴
پرسش ۴۷	استفاده از سامانه‌های نرم‌افزاری، الگوریتم‌های رمز و سخت‌افزاری بومی یا تأیید شده	۱۵/۲

نمودار شماره ۳- شاخص‌های پدافند غیرعامل فنّاوری اطلاعات و ارتباطات



بررسی اطلاعات میدانی نشان می‌دهد که ناجا در اجرای موارد ضروری حفاظت فنّاوری اطلاعات و پدافند غیرعامل، به‌طور کلی در سطح بسیار خوبی قرار دارد که خبرگان سازمانی نیز این موضوع را تأیید کرده‌اند.

پیشنهادها

راه‌کارهای ارائه شده برای پرسش فرعی اول

- توجه به نیروی انسانی و روش‌های واپایش تخلف عوامل انسانی در مراحل گوناگون، همچون کاربری سامانه‌ها و زیرساخت‌ها؛
- آموزش پیوستهٔ کاربران سامانه‌های فراگیر ناجا برای آشنایی بیشتر با شکست‌های حفاظتی فاوا؛
- پایش مستمر امنیت فاوا ناجا با استفاده از آخرین استانداردهای امنیت فاوا در جهان همانند ISMS ؛
- راه‌اندازی مرکز پدافند غیرعامل و امنیت فنّاوری اطلاعات فاوا برای برنامه‌ریزی و رصد پیوسته؛
- تقویت رویکرد پژوهشی در حوزه‌های پدافند غیرعامل فاوا، امنیت فاوا، جنگ‌های رایانه‌ای با رویکرد صنعتی و غیرصنعتی؛
- راه‌اندازی مجلهٔ تخصصی با ادبیات پدافند غیرعامل فاوا، امنیت فاوا و جنگ‌های رایانه‌ای؛
- شرکت مداوم کارشناسان در همایش‌ها و سخنرانی‌های داخلی و بین‌المللی مرتبط با پدافند غیرعامل فاوا، امنیت فاوا و جنگ‌های رایانه‌ای.

راه‌کارهای ارائه شده برای پرسش فرعی دوم

- راه‌کارهای بررسی و واپایش نصب و به‌کارگیری نرم‌افزارهای تصویب نشده و بدون مجوز مورد تأکید و توجه باشد؛
- بر راه‌کارهای بررسی و واپایش تنظیمات امنیتی سیستم عامل، خدمات‌دهنده‌ها، نرم‌افزارها و خدمات امنیتی نرم‌افزاری همچون دیوارهای آتش تأکید شود؛
- استانداردهای پدافند غیرعامل در حوزه‌های سیستم عامل و نرم‌افزارها مطابق استانداردهای سازمان پدافند غیرعامل باشد؛
- تأمین کلیهٔ سخت‌افزار از داخل کشور و از راه ودجا انجام شود؛
- به حفاظت و عایق‌کاری مراکز فاوا، به‌منظور مقابله با بمب‌های الکترومغناطیسی توجه شود؛

- از سامانه‌های هوشمند و آنی مانند مرکز امنیت اطلاعات (SOC) برای تحلیل خطرها و هشداردهی بهره گرفته شود؛
- از نرم‌افزارهای بومی مانند مرورگر و سیستم عامل استفاده شود؛
- سخت‌افزارهای بومی و موارد مانند آن به‌کار رود.

راه‌کارهای ارائه شده برای پرسش فرعی سوم

- درنظرگرفتن بودجه و تکمیل فرایندهای پدافند غیرعامل در پهنهٔ فنّاوری اطلاعات (زیرساخت، نیروی انسانی و مانند آن)؛
- ساماندهی و راه‌اندازی ساختار مدیریت امنیت اطلاعات، مراکز امداد و نجات رایانه‌ای (CERT) و مواردی از این قبیل؛
- تأمین نیازمندی‌های پشتیبانی فنی مانند: خطوط برق موازی و اضطراری و خطوط ارتباطی موازی برای بخش‌های مهم و مراکز بسیار مهم و حساس؛
- اهمیت دادن به آموزش تخصصی برای ارتقای مهارت کارشناسان با رویکرد پدافند غیرعامل؛
- استفاده از سامانه‌های نرم‌افزاری، الگوریتم‌های رمز و سخت‌افزاری بومی و یا تأیید شده.

منابع و مآخذ

آزادزاده، محسن و دیگران (بی‌تا)، «مبانی پدافند غیرعامل در حوزهٔ امنیت فنّاوری اطلاعات».

اروسخانی، علی (۱۳۸۷)، «حفاظت ارتباطات»، تهران: نشر حدیث کوثر.

امیرصوفی، رحمت‌اله (۱۳۸۹)، «جنگ‌های اطلاعاتی»، مجتمع دانشگاهی فنّاوری اطلاعات، ارتباطات و امنیت دورهٔ پدافند غیرعامل- پنها.

پدافند غیرعامل در حوزهٔ جنگ سایبر (۱۳۹۰)، تهیه‌کننده: مرکز پدافند غیرعامل فاوا، شرکت مخابرات ایران.

پورکیانی و دیگران (بی‌تا) «بررسی نقش فنّاوری اطلاعات در پدافند غیرعامل و مدیریت بحران و ارائه الگویی جامع در مدیریت بحران».

پورمراد، مجید (۱۳۸۹)، «حفاظت فنّاوری اطلاعات و ارتباطات»، تهران: نشر حدیث کوثر.

توقعی و دیگران (بی‌تا)، «نقش رایانش ابری در پدافند سایبری سازمانی».

دادگر، هانیه (۱۳۹۱)، «بررسی نقش جنگ در توسعهٔ فنّاوری اطلاعات و فنّاوری اطلاعات در جنگ».

داوری، جواد و دیگران (بی‌تا)، «اصول و ملاحظه‌های پدافند غیرعامل در فضای سایبری».

دوست‌محمدیان، حمید (۱۳۸۹)، «بررسی متقابل هیستوژئوپولتیک جنگ‌ها در پیشرفت‌های امروزی».

دوست‌محمدیان، حمید (۱۳۹۲)، «مهندسی پدافند غیرعامل در فنّاوری اطلاعات» (امنیت به روش پیشگیری الکترونیکی).

سلامی، حسین (بی‌تا)، «فنّاوری‌های نوین در جنگ‌های آینده».

نیک‌نفس، رضا (بی‌تا) «بررسی شاخص‌های پدافند غیرعامل در فاوا نیروی انتظامی استان همدان».

یوسفی و دیگران (بی‌تا)، «مدیریت امنیت فنّاوری اطلاعات و ارتباط».