فصلنامهٔ مطالعات حفاظتی و امنیتی
فصلنامهٔ علمی- ترویجی
سال دوازدهم، شمارهٔ چهل‌ودوم، بهار ۱۳۹۶

تاریخ دریافت: ۱۳۹۵/۱۱/۲۳
تاریخ پذیرش: ۱۳۹۶/۰۲/۲۸

نقش حفاظت ارتباطات و اطلاعات درحوزهٔ امنیت فضای مجازی ناجا (با رویکرد پدافند غیرعامل)

اکبر استرکی[۱]، عقیل آذری‌فر[۲]

از صفحهٔ ۱۰۸. تا صفحهٔ ۱۳۰

چکیده

یکی از سازمان‌های بسیار مهم در کشور که با توجه به وظایف گسترده و تنوع مأموریت‌های محول نقش اساسی را در استقرار امنیت عمومی و در پی آن، تثبیت امنیت ملی ایفا می‌کند نیروی انتظامی جمهوری اسلامی ایران است. گستردگی مأموریت‌های این سازمان لزوم بهره‌گیری از سامانه‌ها و فنّاوری‌های نوین را، همچون فنّاوری اطلاعات و ارتباطات، بسیار پررنگ می‌کند و خوشبختانه امروزه فنّاوری اطلاعات در تحقق مأموریت‌های ناجا جایگاهی بسیار مهم و اثرگذار دارد.

پرسش اصلی تحقیق بدین‌صورت طرح شده است: «حفاظت ارتباطات و اطلاعات در امنیت فضای مجازی ناجا، با رویکرد پدافند غیرعامل، چه نقشی دارد؟». در این پژوهش، با بهره‌گیری از روش نمونه‌گیری تصادفی ساده، پنجاه تن از کارشناسان حفاظت ارتباطات و اطلاعات ساحفا در ستاد سازمان و فرماندهی انتظامی استان‌ها به صورت تصادفی انتخاب شدند. این افراد تنوع افسران جزء و افسران ارشد و بالاتر را شامل می‌شوند. در این پژوهش، پس از بررسی چک‌لیست‌های امنیت فنّاوری اطلاعات، برای گردآوری داده‌ها از پرسش‌نامه‌ای محقق‌ساخته با ۴۵ سؤال استفاده شده که در چهار بُعد اساسی طبقه‌بندی شده است. این پرسش‌نامه با طیف لیکرت تهیه و پس از توزیع، پایایی و روایی آن با محاسبهٔ آلفای کرونباخ سنجیده شد. برای تحلیل داده‌ها از آمار توصیفی شامل (فراوانی، درصد، میانگین و انحراف معیار)، و برای آزمون فرضیه‌های پژوهش از آمار استنباطی (آزمون t تک‌نمونه‌ای) استفاده شد. بر اساس یافته‌های علمیِ فرضیهٔ نخست تحقیق، بین شناخت جایگاه و نقش حفاظت از فنّاوری ارتباطات و اطلاعات، بین تهدیدهای ارتباطات و اطلاعات، بین عوامل مؤثر در ارتباطات و اطلاعات با امنیت فضای مجازی ناجا، و بین شیوه‌های گسترش اقدام‌های حفاظت فنّاوری اطلاعات در امنیت فضای مجازی ناجا با رویکرد پدافند غیرعامل رابطه وجود دارد.

کلیدواژه‌ها: ارتباطات و اطلاعات، امنیت فضای مجازی، پدافند غیرعامل، حفاظت ناجا.

---

۱. دکترای علوم ارتباطات اجتماعی، عضو هیئت علمی دانشگاه علوم انتظامی امین.
۲. نویسندهٔ مسئول: دانشجوی کارشناسی ارشد دانشگاه علوم انتظامی امین (Azarifar706@chmail.ir).

مقدمه

امروزه توسعهٔ فنّاوری اطلاعات و ارتباطات از چنان گستره‌ای برخوردار شده که آن را به یکی از موضوع‌های محوری در نبرد اطلاعات و امنیت فضای مجازی میان جوامع و سازمان های اطلاعاتی، انتظامی، امنیتی و دفاعی تبدیل کرده است. در عصر کنونی، سیاست‌مداران و حاکمان، با تأکید بر این اصل که اطلاعات اساس سیاست‌گذاری و سیاست گذاری پایهٔ تأمین اطلاعات است، اقتدار ملی حکومت خود را در پناه جامعهٔ اطلاعاتی دنبال می‌کنند و به همین منظور، اهتمام و توجه ویژه‌ای به آن دارند. سازمان‌های حفاظت اطلاعاتی نیز از سازمان‌های عضو جامعهٔ اطلاعاتی کشورند که با توجه به عملکرد و رفتارهای حرفه‌ای خود و اصل حرفه‌ای کردن امور، در نخستین مرحله، با نگاه ویژه به ساختار درونی و درپیش‌گرفتن تمهیدهای منطقی، گام‌های مؤثری برای توانمندسازی عملیات سازمان متبوع برمی‌دارند و با توزیع اطلاعات مورد نیاز، اثربخشی پنهان خود را در لایه‌های گوناگون تصمیم‌سازی و تصمیم‌گیری به ظهور می‌رسانند. «پیگیری و اجرایی کردن سیاست‌های ایجابی که پیش‌تر در سیاست‌های کلی ابلاغ شده است، به‌ویژه در زمینهٔ تولیدهای نرم‌افزاری و سخت‌افزاری و نیز تولید محتوای مطلوب در محیط اینترنت، مورد تأکید است. در این زمینه، لازم است دستگاه‌های ذی‌ربط مانند صداوسیما، وزارت‌خانه‌های فرهنگ و ارشاد اسلامی، علوم و تحقیقات و فناوری، آموزش و پرورش و سازمان تبلیغات اسلامی و ... مشارکت و همکاری نمایند» (حدیث ولایت) با توجه به اینکه سازمان‌های گوناگون، مانند ن. م. و در رأس آن ناجا، در انجام‌دادن مأموریت خود همواره به فاوا متکی‌اند، ورود فنّاوری به ن.م، به‌ویژه ناجا، به‌دلیل قابلیت‌هایی چون سرعت، دقت، صحت، جامعیت و مدیریت داده‌ها مورد توجه است و فرصتی طلایی محسوب می‌شود که چالش‌ها و تهدیدهایی را نیز به‌دنبال دارد. سرقت اطلاعات، نفوذ، خرابکاری، نفی خدمات، کلاهبرداری، جاسوسی، شنود و مانند آن از پیامدهای سوء فاواست که می‌توان در امنیت فضای مجازی در نظر گرفت و لازم است برای مقابله با آنچه آن را تهدید می‌کند چاره‌ای اندیشید. لازمهٔ حذف و کاهش مطلوب تأثیر این تهدیدها بهره‌گیری از

تمهیدها و اقدام‌های حفاظت ارتباطات و اطلاعات است. موفقیت سازمان‌های اطلاعاتی و حفاظت اطلاعات به عوامل بسیاری ارتباط دارد که مهم‌ترین آن‌ها استفاده از جدیدترین فنّاوری‌های اطلاعاتی متناسب با فنّاوری روز است. به همین دلیل به‌نظر می‌رسد، نگاه به هر یک از موارد یادشده، برای اهمیتشان نزد سازمان‌های اطلاعاتی و انتظامی و حفاظت اطلاعاتی، ممکن است از عوامل مؤثر در ارتقای ظرفیت‌های اطلاعاتی و در نهایت، حفظ بقا و امنیت هر کشوری باشد.

بیان مسئله: دوران حاضر مجموعهٔ گسترده‌ای از فنّاوری‌ها را دربر دارد که برای ارتباط بین انسان‌ها و جامعه بیشترین کاربرد را دارند. با پیروزی انقلاب اسلامی ایران و به دنبال آن شکست‌های پیاپی سیاست‌های سلطه‌طلبانهٔ آمریکا در ایران، این کشور تهدیدهایی علیه جمهوری اسلامی ایجاد کرد؛ چه به صورت مستقیم: یعنی با اعمال تحریم‌ها، حمایت و هدایت جریان‌های براندازی، و چه به صورت غیرمستقیم: در حملهٔ نظامی و رایانه‌ای. این روند البته ادامه خواهد داشت؛ در این راستا، تهدیدها یا جنگ‌های رایانه‌ای در اولویت اقدام‌های دشمن قرار خواهد گرفت. لازمهٔ حذف و کاهش چشمگیر اثر این تهدیدها بهره‌گیری از تمهیدها و اقدام‌هایی است که به آن «حفاظت» می‌گویند. در واقع، حفاظت سلسله اقدام‌هایی است که برای حفظ و تأمین تأسیسات و سازوبرگ، اسناد و مدارک، اخبار و اطلاعات و اشخاص در برابر تهدیدهای دشمن و خطرهای طبیعی انجام می‌شود.

به بیان ساده‌تر، حفاظت را می‌توان تمهیدها و اقدام‌هایی تعریف کرد که به حذف یا کاهش چشمگیر اثر تهدیدها و خطرها در موضوع‌های حفاظتی (موضوع‌های مورد توجه) منجر می‌شوند. در اتخاذ سازوکار حفاظتی، باید تدبیرها با تهدید و ارزش حفاظتی موضوع متناسب و، به نوعی، اقدام‌های حفاظتی مقرون به‌صرفه باشد. امنیت فاوا به‌معنای حصول اطمینان از حذف یا کاهش مطلوب تهدیدها و خطرهای مترتب در این پهنه و در نتیجه، امنیت، آرامش و آسودگی خاطر از کارآمدی فاوا در زمینهٔ رفع نیازهای سازمان است. بدین‌ترتیب، این پرسش در صحنهٔ امنیت فضای مجازی آیندهٔ ناجا متصور خواهد بود که: حفاظت ارتباطات و اطلاعات چه نقشی در امنیت رایانه‌ای ناجا برعهده خواهد داشت؟

امنیت فضای مجازی در ارتباطات و اطلاعات ناجا چه جایگاهی دارد و شیوه‌های گسترش اقدام‌های حفاظتی در این زمینه، در ناجا، با رویکرد پدافند غیرعامل کدام‌اند؟

ضرورت و اهمیت تحقیق

اهمیت تحقیق: با پیدایش فنّاوری‌های ارتباطاتی، گسترهٔ اطلاعاتی جدیدی شکل گرفته است (دهقانی فیروزآبادی، ۱۳۹۰) که در آن سازمان‌های اطلاعاتی، حفاظتی و امنیتی حضوری فعال دارند. سازمان‌های اطلاعاتی برای حفظ ارتباطات و انتقال فعالیت‌های اطلاعاتی خود از این ابزار استفاده می‌کنند. این سازمان‌ها، مانند ناجا، از طریق رایانامه و مانند آن با مشتریان خود در ارتباط‌اند و کارشان عرضهٔ خدمات و تبادل اطلاعات و داده است. سازمان‌هایی که به فضای مجازی وابسته‌اند، افزون بر اینترنت، از طریق ماهواره و رسانه‌های دیگر فضای مجازی، فعالیت‌های ارتباطی و اطلاعاتی خود را در سطح گسترده‌ای پوشش می‌دهند. منابع اطلاعاتی، از طریق ماهواره‌ها و شبکهٔ مجازی (فضای مجازی)، داده‌هایی در زمینهٔ نیازمندی‌های اطلاعاتی سازمان مربوط در محیط مجازی مورد نظر به‌دست می‌آورند و آن را به مشتریان خود یا سازمان متبوع عرضه می‌کنند. این رهنمودها نکته‌های مثبت و دستاوردهای راه‌گشایی برای حل مسائل روزمره و تسریع در تبادل ارتباطات و اطلاعات دارند. با توجه به اهمیت رشد سریع فنّاوری‌های نوین اطلاعاتی، به‌ویژه در زمینهٔ فعالیت‌های رایانه‌ای، حفاظت از ارتباطات و اطلاعات و تأمین امنیت این فضا، بیشتر از همه هنگام وقوع تهدیدهای رایانه‌ای، برای مسئولان و مدیران و محققان و سیاست‌مداران و کارگزاران امنیتی و اطلاعاتی اهمیت شایان توجهی دارد زیرا بدین‌ترتیب از داده‌ها و اطلاعات کشور پاسداری می‌شود.

زیرساخت‌های فنّاوری اطلاعات ناجا را دشمنان داخلی و خارجی هدف و نشان‌گاه عملیاتی رایانه‌ای بسیار مهمی می‌شمارند؛ بنابراین، جایگاه و نقش آن در تحقق هدف‌های مأموریتی برای ناجا بسیار بااهمیت است. همچنین، باید به استفاده از امواج الکترومغناطیس برای ایجاد اختلال در زیرساخت‌های فاواناجا (نفوذ فنی) و تخریب آن توجه بسیار داشت.

از سویی، باید نیازهای حفاظت ارتباطی یگان‌های رایانه‌ای را، در صحنهٔ نبرد با نیروهای فرامنطقه‌ای، تعیین کرد و منابع را، در مقابله با تهدیدهای الکترونیکی پیشرفته، توانمند کرد تا از عملیات فضای مجازی پشتیبانی کنند.

ضرورت تحقیق: پیروزی و شکست در جنگ حاصل برنامه‌ریزی و آمادگی نیروها در رویارویی با تهدیدهاست. تهدیدشناسی و مقابله با تهدیدهای الکترونیکی، در جنگ‌های اخیرِ نیروهای فرامنطقه‌ای در خاورمیانه، فقط با روش‌های علّی و معلولی امکان‌پذیر نیست بلکه، برای تهدیدشناسی و کسب آمادگی لازم در سازمان‌های مرتبط (به‌ویژه ناجا) و مقابله با آن، باید نخست تدبیرهای لازم برای حفاظت از تأسیسات و منابع اصلی و حساس و تأمین امنیت اعمال شود، زیرا در غیر این صورت، اطلاعات در معرض تهدیدهای بی‌شماری مانند افشا، دسترسی غیرمجاز، نابودی و تغییر قرار می‌گیرد. در صورت بروز جنگ رایانه‌ای، این منابع در ناجا دچار آسیب‌ها و زیان‌های جبران‌ناپذیری خواهند شد و امنیت کشور به خطر خواهد افتاد. همچنین برخی از زمینه‌های علوم گوناگون، به‌ویژه علوم اطلاعاتی، به علت بهره‌گیری از فناوری‌های نوین ناشی از دگرگونی اطلاعات در حوزهٔ مطالعات امنیتی و اطلاعاتی، با فناوری‌ها گرهی سخت خورده تا بتواند، از طریق دستاوردهای ناشی از انقلاب اطلاعاتی، بر ضریب افزایش چتر امنیتی خود بیفزاید (فرهند و شعبانی، ۱۳۸۹: ۲۶۶). این موارد و نمودهای عملیاتی آن سبب نگرانی دست‌اندرکاران مربوط در ناجا و ن. م شده‌اند؛ پس، با توجه به موارد پیش‌گفته، جنبه‌های زیر ضرورت دارد:

- به تأمین امنیت فضای مجازی، به‌ویژه در ناجا، توجه شود؛
- حفظ داده‌ها و اطلاعات برای مسئولان، مدیران، محققان، سیاست‌مداران و کارگزاران امنیتی و اطلاعاتی در اولویت اقدام‌ها باشد؛
- عوامل مؤثر در فضای مجازی ناجا شناسایی شوند؛
- از منابع ضروری و حساس ناجا، با رویکرد پدافند غیرعامل در فضای مجازی، به‌سختی حفاظت شود؛

- شناخت راه‌کارهای عملیاتی برای انجام‌دادن پشتیبانی ارتباطات و اطلاعات از عملیات رایانه‌ای ضرورت می‌یابد.

هدف‌های تحقیق

هدف اصلی: تبیین نقش حفاظت ارتباطات و اطلاعات در امنیت فضای مجازی ناجا، با رویکرد پدافند غیرعامل.

هدف‌های فرعی:

۱. شناخت جایگاه و نقش حفاظت ارتباطات و اطلاعات در امنیت فضای مجازی ناجا؛

۲. شناخت تهدیدهای ارتباطات و اطلاعات در امنیت فضای مجازی ناجا؛

۳. تبیین عوامل مؤثر در ارتباطات و اطلاعات در امنیت فضای مجازی ناجا؛

۴. تبیین شیوه‌های گسترش اقدام‌های حفاظت ارتباطات و اطلاعات در امنیت فضای مجازی ناجا، با رویکرد پدافند غیرعامل.

پرسش‌های تحقیق

پرسش اصلی: حفاظت ارتباطات و اطلاعات در امنیت فضای مجازی ناجا، با رویکرد پدافند غیرعامل، چه نقشی دارد؟

پرسش‌های فرعی:

۱. جایگاه و نقش حفاظت ارتباطات و اطلاعات در امنیت رایانه‌ای ناجا چیست؟

۲. تهدیدهای ارتباطات و اطلاعات در امنیت رایانه‌ای ناجا کدام‌اند؟

۳. عوامل مؤثر در ارتباطات و اطلاعات در امنیت فضای مجازی ناجا چیست؟

۴. شیوه‌های گسترش اقدام‌های حفاظت ارتباطات و اطلاعات در امنیت فضای مجازی ناجا، با رویکرد پدافند غیرعامل، چه مواردی‌اند؟

پیشینهٔ تحقیق: تا کنون مطالعات و پژوهش‌های بسیاری در زمینهٔ ارتباطات و اطلاعات، جنگ رایانه‌ای و ارتقای امنیت در فضای مجازی صورت گرفته است (برای نمونه، رک. جدول ۱).

جدول (۱)

ردیف	مؤلف	موضوع تحقیق
۱	مجید پورمراد	در سال ۱۳۸۶، در مقاله‌ای با نام «نگاهی به اینترنت و تهدیدهای آن»، تعریفی از اینترنت و تهدیدهای متصور آن بیان داشت و سرانجام، نتیجه گرفت که اینترنت، همانند هر پدیدهٔ دیگر، جنبه‌های مثبت و منفی بسیاری دارد و باید به جنبه‌های منفی آن توجه بیشتری شود. تهدیدهای اینترنت ممکن است متوجه سِرورها ، وب‌گاه‌ها یا کاربران سازمانی و خانگی شود. مهم‌ترین تهدیدهای اینترنت عبارت‌اند از: جنگ اطلاعات، جاسوسی، فعالیت سیاسی، فساد و فحشا، کلاهبرداری، جعل، دسترسی غیرمجاز، تخریب رایانه.
۲	ایرج نصرتی قمشه	در مقاله‌ای با عنوان «آسیب‌شناسی امنیتی اینترنت برای کارکنان و خانوادهٔ آن‌ها» (۱۳۹۲)، اینترنت را با رویکرد تشریح کارکردهای مثبت و منفی برای کارکنان معرفی کرد و نتیجه گرفت اینترنت، در کنار دستاوردها و کاربردهای انکارناپذیر و مثبت در زمینه‌های گوناگون، پیامد نامطلوبی نیز به‌همراه دارد که کارکنان در مقام والدین نزد خانواده‌هایشان و همچنین مربیان و همهٔ مسئولان امر تعلیم و تربیت و برنامه‌ریزان فرهنگی جامعه باید به آن توجه داشته باشند.
۳	افشین راسخی	در مقاله‌ای با نام «امنیت اطلاعات در فضای اینترنت» (۱۳۹۰)، تدابیر کاربردی برای حفظ امنیت اطلاعات در برابر تهدیدهای اینترنت را معرفی کرد و چنین نتیجه گرفت که، طبق بررسی‌ها، هیچ‌گاه نمی‌توان برای اطلاعات در بستر اینترنت و شبکه‌های اطلاع‌رسانی امنیت کامل ایجاد کرد و رایانهٔ متصل به اینترنت برای مبادله، ذخیره‌سازی و سرور اطلاعات طبقه‌بندی‌شده مناسب نیست اما با درپیش‌گرفتن تدبیرهای حفاظتی و استفاده از سازوبرگ فنی همانند حیطه‌بندی (جداسازی) شبکه‌ها استفاده کرد.
۴	محمود شعبانی	در مقاله‌ای با عنوان «آسیب‌شناسی امنیتی اینترنت برای کارکنان و خانوادهٔ آن‌ها» (۱۳۹۲)، تأثیر منفی و چالش‌های اینترنتی فراروی خانواده، مشکلات جسمانی ناشی از استفادهٔ بی‌رویه از اینترنت و اعتیاد خانواده‌ها به آن را مطرح کرد و نتیجه گرفت اینترنت به‌تدریج جای تلویزیون را گرفته است و احتمال می‌رود در آینده‌ای نزدیک نقشی مهم‌تر از تلویزیون را در زندگی کودکان و نوجوانان داشته باشد. اگر از این فنّاوری استفادهٔ درست شود، آثار مثبتی دارد؛ در حالی که، تحقیقات بیانگر خطرهای ناشی از کاربرد نادرست آن است که تمامی کاربران را، به‌ویژه کودکان، تهدید می‌کند.
۵	سمیرا عبدالرحمان	در مقالهٔ «مدیریت امنیت سیستم‌های رایانش ابری» (۲۰۱۰)، سه چالش مدیریت دسترسی، احراز هویت و حسابرسی کاربران را مطرح کرده و سپس راه‌کار مدیریت دسترسی هویت را بیان کرده است.

در بررسی‌ها و مطالعات محققانی که به آن‌ها اشاره داشتیم، موضوع فنّاوری اطلاعات و ارتباطات و فضای مجازی، به صورت عام و کلی، و تأثیر آن‌ها در خانواده‌ها و جنگ‌ها، شناسایی تدابیر کاربردی برای حفظ امنیت اطلاعات در برابر تهدیدهای اینترنت و بیان تعریفی از اینترنت و تهدیدهای متصور آن مطرح شده است؛ این در حالی است که، در تحقیق حاضر، نقش حفاظت اطلاعات و ارتباطات در امنیت رایانه‌ای نیروی انتظامی جمهوری اسلامی ایران را مطالعه می‌کنیم و این موضوع به صورت تخصصی در ناجا بحث و بررسی شده است.

مبانی نظری:حفاظت اطلاعات: تمامی اقدام‌هایی را دربر می‌گیرد که برای حفظ و نگهداری تأسیسات، اسناد و مدارک، اخبار و اطلاعات، کارکنان، مخابرات و دیگر موضوع‌های بسیار مهم کشور علیه خطرهای ناشی از جاسوسی، خرابکاری، سرقت و موارد دیگر صورت می گیرد و از دسترسی افراد غیرمجاز به موارد یادشده جلوگیری کند (کریمایی، ۱۳۸۷: ۳۳).

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

فنّاوری: مجموعه‌ای است از فرایندها، روش‌ها، فنون، ابزار، سازوبرگ، ماشین‌آلات و مهارت‌هایی که با استفاده از آن‌ها کالایی ساخته یا خدمتی عرضه می‌شود (دوست‌محمدیان، ۱۳۹۲). به‌معنای کاربرد علوم در صنایع، با استفاده از شیوه‌ها و مطالعات منظم و جهت‌دار است (*مقدمه‌ای بر پدافند غیرعامل* ، ۱۳۸۹)

تعریف فنّاوری اطلاعات: به مجموعهٔ سخت‌افزار، نرم‌افزار و نظریه‌هایی گفته می‌شود که اطلاعات را در شکل‌های گوناگون گردآوری، ذخیره، بازیابی، پردازش و منتقل می‌کنند (دوست‌محمدیان، ۱۳۹۲).

فضای مجازی (سایبر): رایانه‌های به هم متصل‌شده، سرورها، مسیریاب‌ها، سوئیچ‌ها و کابل‌ها که زیرساخت‌های اصلی با آن‌ها کار می‌کنند «فضای مجازی» نام دارد (اسکندری، ۱۳۹۰: ۱۲).

امنیت: مفهومی چندوجهی است و به همین دلیل دربارهٔ معنای آن اختلاف نظر بسیاری وجود دارد. تعریف‌های درج‌شده در واژه‌نامه‌ها دربارهٔ مفهوم کلی امنیت روی «احساس آزادی از ترس» یا «احساس ایمنی» ناظر بر امنیت مادی و روانی تأکید دارند (مندل، ۱۳۷۷: ۴۴).

امنیت رایانه: تلاش برای ایجاد بستر امن رایانه‌ای است و طراحی آن به‌گونه‌ای است که فقط امکان اقدام‌های مجاز در آن وجود داشته باشد (اسکندری، ۱۳۹۰: ۱۱).

پدافند: با مفهوم کلی دفع، خنثی‌کردن یا کاهش تأثیر اقدام‌های آفندی دشمن و جلوگیری از دستیابی وی به هدف‌های خود، به‌طور کلی، از دو بخش پدافند عامل و غیرعامل تشکیل می‌شود (چالوک و عصار، ۱۳۹۲: ۱۰).

پدافند غیرعامل[1]

۱. به مجموعهٔ اقدام‌هایی گفته می‌شود که مستلزم به‌کارگیری جنگ‌افزار و تسلیحات نیست و با اجرای آن می‌توان از واردشدن خسارت مالی به سازوبرگ و تأسیسات حساس و مهم نظامی و انتظامی و غیرنظامی و نیز از تلفات انسانی جلوگیری کرد یا میزان خسارت و تلفات ناشی از حمله‌ها و بمباران‌های دشمن را به کمترین میزان ممکن کاهش داد.

۲. مجموعهٔ اقدام‌های غیرنظامی و غیرمسلحانهٔ پایدارکنندهٔ نظام که به‌کارگیری آن‌ها موجب افزایش پایداری ملّی، تولید بازدارندگی دفاعی، کاهش آسیب‌پذیری، آسان‌شدن مدیریت بحران و تداوم خدمات ضروری کشور در برابر تهدیدها و اقدام‌های نظامی دشمن شود (چالوک و عصار، ۱۳۹۲: ۱۱).

مفهوم فضای مجازی: «فضای مجازی (سایبر)»[2] واژه‌ای برگرفته از لغت «kybernate» است. فضای سایبر یا فضای مجازی[1]، در تعریف برخی نویسندگان، عبارت است از

1. passive defense
2. cyber

«مجموعه‌ای از ارتباطات درونی انسان‌ها از راه رایانه و وسایل مخابراتی، بدون درنظرگرفتن جغرافیای فیزیکی». به عبارت بهتر، سایبر محیط الکترونیکی واقعی است که ارتباطات انسانی به شیوه‌ای سریع، فراتر از مرزهای جغرافیایی و با ابزار خاصی در آن، زنده و مستقیم روی می‌دهد (آستانا و آنجالی[2]، ۱۳۸۸: ۳۹۳).

ویژگی‌های فضای مجازی: ویژگی نخست فضای مجازی دیجیتالی‌بودن آن است که این ویژگی رسانه‌ها امکانات نظارت، عمل ارادی و تصرف‌کردن در تولید را پدید می‌آورد. دیگر ویژگی‌های فضای مجازی عبارت‌اند از:

- ذخیرهٔ اطلاعات در فضای مجازی (دیجیتالی‌کردن اطلاعات): نخستین ویژگی دیجیتالی‌بودن استقرار و ثبات است و در اینجا به‌معنای وجود ظرفیت‌هایی است که امکان ذخیرهٔ اطلاعات را دارند. در جهان واقعی به دلیل کمبود وقت، دوربودن مسافت‌ها و پرهزینه‌بودن اطلاعات، بسیار کم از قانون‌گذاری‌ها اطلاع می‌یابیم. اما در جهان مجازی، می‌توانیم به‌سهولت به این موارد دسترسی داشته باشیم، زیرا فضای مجازی، به‌علت دیجیتالی‌بودن، امکان ذخیرهٔ این اطلاعات را برای ما فراهم می‌کند و دست ما را باز می‌گذارد که، هنگام نیاز به این اطلاعات برای مقاصد خود، به‌سهولت از آن‌ها استفاده کنیم.
- فضای واقعی مجازی: فضای مجازی فضایی خیالی و فرضی نیست بلکه انعکاسی از جهان واقعیت است و همین واقعی‌بودن آن است که به آن اعتبار می‌بخشد (معمار، ۱۳۸۸: ۱۷۱).
- گمنامی: شناسایی و ردیابی منابع در فضای مجازی و پیداکردن مکان فیزیکی آن‌ها، با توجه به شیوه‌های خاص پنهان‌سازی در این فضا، بسیار مشکل است.
- سازوبرگ ارزان و دردسترس: سهولت دسترسی به ابزارهای حمله و جاسوسی و هزینهٔ پایین آن‌ها به‌نسبت جنگ‌افزارهای حمله‌های دیگر، به سازمان‌های تروریستی و خرابکاری این امکان را داده که با استفاده از سازوبرگ پیشرفتهٔ فضای مجازی و از طریق ارتباطات پنهان، به زیرساخت‌های هدف حمله کنند و به مقصد خود دست یابند.

---

1. cyber space
2 . Astana and anjely

- دردسترس‌بودن: به این دلیل که اینترنت و ارتباطات در حال گسترش روزافزون است، مهاجمان دنیای مجازی قادرند ۲۴ ساعته در ارتباط با هدف خود باشند.

هدف‌های امنیت فنّاوری اطلاعات

- **محرمانگی:** حفاظت و اطمینان، یا همان محرمانگی، به‌مفهوم حفاظت داده‌های سامانه‌های رایانه‌ای در برابر دسترسی‌های غیرمجاز است.
- **جامعیت:** یا یکپارچگی، به‌معنای تأمین دقت و جامعیت اطلاعات و نرم‌افزارهای رایانه‌ای است. حفظ جامعیت در اصل به‌مفهوم حفاظت داده‌ها در برابر تغییرهای غیرمجاز و نامطلوب عمدی یا سهوی است.
- **دسترس‌پذیری:** یا دسترسی‌پذیری، همان ضمانت دسترسی به اطلاعات و خدمات حساس در زمان مورد نیاز است و به زبان ساده‌تر یعنی آماده‌به‌کار بودن یا پای‌کاربودن شبکهٔ رایانه‌ای و داشتن اطمینان به اینکه همواره کاربران مجازی به شبکهٔ رایانه‌ای دسترسی دارند و می‌توانند از آن بهره‌برداری کنند.
- **انکارنکردن:** به‌معنای این است که گیرندهٔ پیام اطمینان حاصل کند پیام از سوی همان فردی است که ادعا می‌کند، و فرستندهٔ پیام نتواند ارسال پیام خود را انکار کند. برای این منظور، از امضای دیجیتالی استفاده می‌شود (پورمراد، ۱۳۸۷: ۲۲).

مأموریت‌های پدافند غیرعامل در گسترهٔ فنّاوری اطلاعات و ارتباطات: دغدغهٔ اصلی پدافند غیرعامل در حوزهٔ فاوا گسترش امن زیرساخت‌ها و رعایت اصول پدافند غیرعامل در مراکز فاوا به‌منظور ارتقای ضریب امنیت و ایمنی و پایداری محسوب می‌شود. از مهم‌ترین مأموریت‌های پدافند غیرعامل در فاوا می‌توان به این موارد اشاره کرد:

- ایجاد و حفظ امنیت زیرساخت‌های حوزهٔ فنّاوری اطلاعات و ارتباطات در برابر مخابرات محتوایی؛
- ایمنی زیرساخت‌های گسترهٔ فناوری اطلاعات و ارتباطات در برابر حمله‌های فیزیکی؛
- پایداری زیرساخت‌های گسترهٔ فناوری اطلاعات و ارتباطات، در رویارویی با تهدیدها، و ادامهٔ ماموریت در شرایط بحران؛

- صیانت از زیرساخت‌های پهنهٔ فناوری اطلاعات و ارتباطات در برابر حمله‌های غیرمترقبه، بلایای طبیعی و در زمان اضطراری؛
- ارتقا و گسترش عزم ملی، باور و فرهنگ عمومی و سازمانی در زمینهٔ رعایت اصول پدافند غیرعامل (استتار، اختفا، پوشش، پراکندگی، استحکام بنا، فریب و مانند آن) در پهنهٔ فنّاوری اطلاعات و ارتباطات کشور؛
- تولید دانش فنی و بومی و بهره‌گیری آگاهانه از فناوری مناسب و روزآمد کشور در زمینهٔ دفاع غیرعامل فاوا، با گسترش جهاد علمی؛
- کاهش آسیب‌پذیری زیرساخت‌های اصلی و مراکز حساس و مهم کشور، در گسترهٔ فناوری اطلاعات و ارتباطات، در برابر تهدیدها و اعمال ملاحظات و سیاست‌ها و ضابطه‌های خاص پدافند غیرعامل درپهنهٔ فناوری اطلاعات و ارتباطات، در برنامه‌های در دست مطالعهٔ کشور؛
- تدوین معماری کلان پدافند غیرعامل فناوری اطلاعات و ارتباطات کشور (www.ipfn.ir).

سیاست‌ها و برنامه‌های ناجا درمورد حفاظت پدافند غیرعامل در گسترهٔ فاوا: در راستای فرمایش مقام معظم رهبری (مدظله‌العالی) و اهمیت پرداختن به مقولهٔ پدافند غیرعامل پهنهٔ فناوری اطلاعات و ارتباطات، در سال ۱۳۸۷ آیین‌نامهٔ امنیت ارتباطات و فناوری اطلاعات، در ۲۹۳ ماده و ۷۳ تبصره، با تشکیل کارگروه‌های تخصصی و کارشناسان امر از فرماندهی‌ها و ساحفاها تهیه و پس از تصویب ستاد کل نیروهای مسلح و برای اجرا، به نیروهای مسلح کشور ابلاغ شد. در این آیین‌نامه به مقولهٔ پدافند غیرعامل نیز توجه ویژه شده است و یگان‌های انتظامی و نظامی ملزم به رعایت آن در مأموریت‌های فاوا شده‌اند. برخی از مواد این آیین‌نامه را شرح می‌دهیم:

- **مادهٔ ١٤:** آیین‌نامهٔ امنیت فاوا به وظایف فرماندهان و ساحفاها در پدافند غیرعامل در گسترهٔ فاوا اشاره دارد. «رعایت اصول پدافند غیرعامل شامل اختفا، استتار، مقاوم‌سازی

و جلوگیری از آنالیز، اختلال، فریب، انهدام و حمله‌های رایانه‌ای وب‌گاه‌ها و شبکه‌های ارتباطی به‌عهدهٔ فرماندهی رده و نظارت آن با ساحفاست».

- **مادهٔ ۱۹:** «فرماندهی فاوای سازمان‌های نیروهای مسلح موظف است به ایجاد سایت‌ها و شبکه‌های پشتیبان اضطراری اقدام کند».
- **مادهٔ ۵۳:** «بالاترین ردهٔ فاوای سازمان‌های ن. م موظف است طرح تخلیه، نابودی اطلاعات و نرم‌افزارهای ارتباطی و ذخیره‌ساز را در تمامی شرایط، شامل بحران و غیر آن، تهیه و طی دستورالعملی به رده‌های ذیربط ابلاغ کند».
- **مادهٔ ۷۷:** به تشریح و ضرورت تعیین صلاحیت کاربران پرداخته است. مواد ۹۰ و ۹۴ شامل الزام تهیهٔ سخت‌افزارهای امنیتی از داخل و ممنوع بودن استفاده از سخت‌افزارهای امنیتی خارجی در نیروهای مسلح می‌شوند.
- **مادهٔ ۱۳۸:** «به هنگام طراحی هر بستر ارتباطی، باید کانال‌های ارتباطی پشتیبان به‌منظور جایگزینی در زمان بحران یا هنگام قطع ارتباط مدنظر قرار گیرد».
- **مواد ۱۶۷، ۱۷۸ و ۱۸۰:** به نگهداری و ارسال اطلاعات، با قید ملاحظات پدافند غیرعامل، مربوط می‌شوند.
- **تبصرهٔ مادهٔ ۲۳۶:** ضرورت درپیش‌گرفتن اصول پدافند غیرعامل برای محل استقرار سرورها را مطرح کرده است (آیین‌نامهٔ امنیت ارتباطات و فنّاوری اطلاعات ن. م. مصوب فرماندهی معظم کل قوا (مدظله‌العالی)، ۱۳۸۷).
- مستند به آیین‌نامهٔ امنیت فاوا، در حال حاضر، دستورالعمل‌های بسیاری در گسترهٔ امنیت فاوا در ناجا تهیه و به یگان‌ها ابلاغ شده است در ادامه به برخی از آن‌ها اشاره می‌کنیم:
- **دستورالعمل حفاظت فیزیکی رایانه:** در این دستورالعمل، به مباحث کلی حفاظت اماکن رایانه‌ای، حفاظت سخت‌افزارها، حفاظت در برابر تشعشع‌ها و نظارت آمدوشد اشاره شده است.
- **دستورالعمل حفاظت سامانه‌ها:** مباحث کلی اقدام‌های حفاظتی در روند تهیهٔ سامانه‌ها و تمهیدهای امنیتی آن را مطرح می‌کند.

- **دستورالعمل حفاظت نرم‌افزارها و داده‌ها:** در آن به حفاظت نرم‌افزارها و داده‌ها در برابر تهدیدها توجه شده است.

روش تحقیق: روش این پژوهش تحلیلی- توصیفی، با بهره‌گیری از مطالعات کتابخانه‌ای و اسنادی است و از منظر دیگر، این تحقیق توصیفی و پیمایشی (میدانی) محسوب می‌شود زیرا محقق قصد دارد نتایج حاصل را، بدون هیچ‌گونه تغییری، گزارش کند؛ در ضمن از نظر ماهیت، این پژوهش کاربردی- توسعه‌ای شمرده می‌شود. محاسبهٔ روایی و پایایی تحقیق با استفاده از ضریب آلفای کرونباخ ضریب پایایی صورت گرفت که برابر با ۰/۸۵ استخراج شد و نشان می‌دهد ابزار اندازه‌گیری از اعتبار مطلوب برخوردار است.

جامعهٔ آماری: جامعهٔ آماری شامل تمامی مدیران و کارشناسان گسترهٔ حفاظت ارتباطات و اطلاعات فضای مجازی ساحفاناجاست. برای گروه نمونه نیز پنجاه نفر از کارشناسان حفاظت ارتباطات و اطلاعات ساحفا در ستاد سازمان و فرماندهی انتظامی استان‌ها انتخاب شدند.

نتایج و یافته‌ها: جایگاه و نقش حفاظت ارتباطات و اطلاعات در امنیت فضای مجازی ناجا

جدول ۲: مقایسهٔ میانگین جایگاه و نقش حفاظت ارتباطات و اطلاعات در امنیت فضای مجازی ناجا

ردیف	جایگاه و نقش حفاظت ارتباطات و اطلاعات در امنیت فضای مجازی ناجا	شاخص آماری	
		میانگین امتیاز کلی	انحراف معیار کل
۱	جایگاه و نقش حفاظت فنّاوری اطلاعات در تحقق هدف‌های مأموریتی سازمان‌ها	4.70	0.51
۲	اهمیت حفاظت از سامانه ها و زیرساخت های فنّاوری اطلاعات و ارتباطات در سطح ناجا	4.62	0.53
۳	اهمیت حفاظت سامانه‌ها و زیرساخت‌های فنّاوری اطلاعات نزد دشمنان، مخالفان، اخلالگران و سودجویان، در جایگاه هدف عملیاتی جنگ رایانه‌ای	4.68	0.51
٤	نقش حفاظت در خرید و تولید نرم‌افزارهای منطبق با سیاست های ابلاغی (فنّاوری، معماری، امنیت)	4.38	0.75
٥	نقش حفاظت در بهره‌گیری هدفمند از عوامل درون‌سازمانی به‌منزلهٔ سپری برای جلوگیری از نفوذ دشمنان در تحقق هدف‌های رایانه‌ای	4.40	0.67
٦	نقش حفاظت در شناخت تهدیدهای عمده و جاری (عمومی و تخصصی) و ارزیابی تأثیر آن‌ها در امنیت، ایمنی و پایداری زیرساخت‌های ناجا	4.44	0.61

۷	نقش حفاظت در تهیهٔ دستورالعمل های تخصصی و اجرایی برای انجام دادن اقدام‌های مقابله‌ای و توجیه کارکنان ناجا	4.52	0.61
۸	نقش حفاظت در بررسی صلاحیت و تسلط علمی ممیزان امنیتی، برای واپایش و نظارت بر مراحل پیاده‌سازی و بهره‌برداری سامانه‌ها و شبکه‌ها (طراحی، تولید، اجرا، خرید، بهره‌برداری، نگهداری، تعمیر)	4.37	0.66
۹	نقش حفاظت در واگذاری اطلاعات طبقه‌بندی‌شده و سازوبرگ به پیمانکاران ناجا	4.36	0.92
۱۰	نقش حفاظت در رعایت کامل اصول حفاظتی در تعمیر و پشتیبانی سازوبرگ امنیتی مربوط به بسترهای ارتباطی ناجا	4.38	0.67
	میانگین کلی	4.48	0.64

بر اساس داده‌های جدول ۲ و به‌نظر پاسخگویان، در میان جایگاه و نقش حفاظت ارتباطات و اطلاعات در امنیت فضای مجازی ناجا، بیشترین امتیاز مربوط به جایگاه و نقش حفاظت فنّاوری اطلاعات در تحقق هدف‌های مأموریتی سازمان‌ها، با امتیاز ۴/۷۰ است و کمترین امتیاز هم مربوط به نقش حفاظت در واگذاری اطلاعات طبقه‌بندی‌شده و سازوبرگ به پیمانکاران ناجا، با امتیاز 4/36 تعلق دارد. در ضمن، میانگین کلی جایگاه و نقش حفاظت ارتباطات و اطلاعات در امنیت فضای مجازی ناجا هم برابر با ۴/۴۸ به‌دست آمده است.

تهدیدهای ارتباطات و اطلاعات در امنیت فضای مجازی ناجا

جدول ۳: مقایسهٔ میانگین تهدیدهای ارتباطات و اطلاعات در امنیت فضای مجازی ناجا

ردیف	تهدیدهای ارتباطات و اطلاعات در امنیت فضای مجازی ناجا	شاخص آماری	
		میانگین امتیاز کلی	انحراف معیار کل
۱	شناسایی تهدیدهای عملیات اطلاعاتی با هدف دستکاری، سرقت، جاسوسی و اشراف بر سامانه‌های اطلاعاتی نرم‌افزاری از محیط بیرونی (نفوذ فنی)	4.36	0.90
۲	شناسایی تهدیدهای تولید سخت‌افزار و نرم‌افزار و تجهیز به بدافزارها و کنترل های از راه دور و فروش هدفمند در پوشش های متفاوت، برای تحقق هدف‌های فضای مجازی (نفوذ اجتماعی)	4.32	0.94
۳	شناسایی تهدیدهای واگذاری در واپایش، نظارت، امور نگه‌داشت و مدیریت سامانه‌ها به پیمانکاران ناجا	4.34	0.80

٤	آگاه‌سازی طراحان و تولیدکنندگان نرم‌افزار به تهدیدهای مباحث حفاظتی تولید نرم‌افزار	4.38	0.64
٥	شناسایی تهدیدهای دسترسی به سامانه‌های جامع مهم و حساس به صورت برخط در محیط اینترنت	4.26	0.92
٦	آگاه‌سازی مدیران از تهدیدها و ضابطه‌های برون‌سپاری پروژه‌های فنّاوری اطلاعات (قانون‌های امنیتی و حفاظتی تولید، پشتیبانی و رفع عیب نرم‌افزار و مانند آن)	4.44	0.64
۷	شناسایی تهدیدهای یکپارچه‌سازی و تعامل‌پذیری سامانه‌ها	4.16	0.91
۸	شناسایی تهدیدهای نصب و به‌کارگیری نرم‌افزارهای غیرمصوب و بدون‌مجوز	4.38	0.64
۹	تدوین سناریوهای احتمالی ناشی از تهدیدهای رایانه‌ای و سطح‌بندی آن‌ها و مشخص کردن دامنهٔ آسیب‌پذیری و نقاط آسیب‌پذیر و پیگیری راه‌حل‌های مقابله‌ای	4.18	0.98
	میانگین کلی	**4.31**	**0.82**

بر اساس داده‌های جدول ۳ و به عقیدهٔ پاسخگویان، در میان تهدیدهای ارتباطات و اطلاعات در امنیت فضای مجازی ناجا، بیشترین امتیاز را آگاه‌سازی مدیران از تهدیدها و ضابطه‌های برون‌سپاری پروژه‌های فنّاوری اطلاعات (قانون‌های امنیتی و حفاظتی تولید، پشتیبانی و رفع عیب نرم‌افزار و مواردی از این دست)، با امتیاز ۴/۴۴ دارد و کمترین امتیاز هم متعلق است به تهدیدهای یکپارچه‌سازی و تعامل‌پذیری سامانه‌ها، با امتیاز ۴/۱۶. درضمن، میانگین کلی تهدیدهای ارتباطات و اطلاعات در امنیت فضای مجازی ناجا نیز ۴/۳۱ به‌دست آمده است.

عوامل مؤثر در امنیت فضای مجازی ارتباطات و اطلاعات در ناجا

جدول ٤: مقایسهٔ میانگین عوامل مؤثر در امنیت فضای مجازی ارتباطات و اطلاعات در ناجا

ردیف	عوامل مؤثر در امنیت فضای مجازی ارتباطات و اطلاعات در ناجا	شاخص آماری	
		میانگین امتیاز کلی	انحراف معیار کل
۱	شناسایی آسیب‌پذیری‌ها و استفاده از امواج الکترومغناطیس برای ایجاد اختلال در زیرساخت‌های فضای مجازی و تخریب آن‌ها (نفوذ فنی)	4.28	0.88
۲	شناسایی آسیب‌پذیری و وقوع عملیات‌های شبکه‌ای با هدف ایجاد اختلال، سرقت اطلاعات، جاسوسی و مانند آن، از راه هک و نفوذ شبکه‌های ارتباطی و زیرساخت‌ها (نفوذ فنی)	4.28	0.88

۳	شناسایی تنظیم‌های امنیتی سیستم‌عامل، خدمات دهنده‌ها، نرم‌افزارها و خدمات امنیتی نرم‌افزاری مانند دیوارهای آتش	4.28	0.95
٤	شناسایی سیاست‌ها، خط‌مشی‌ها و دستورالعمل‌های پشتیبان‌گیری از نرم‌افزارها و بانک‌های اطلاعاتی، بازیابی و ازبین‌بردن اطلاعات	4.34	0.69
٥	کسب اطمینان از داشتن تأییدیهٔ امنیتی سخت‌افزارهای تهیه‌شده	4.36	0.69
٦	اطمینان یافتن از به‌کارنبردن سخت‌افزارهای اهدایی، کشف‌شده یا بدون صاحب در ناجا	4.44	0.76
۷	نظارت و رصد تهیهٔ سخت‌افزارها بر اساس الگوی پیش‌بینی‌شده	4.34	0.66
۸	شناسایی صلاحیت و تسلط علمی کاربران و کارشناسان متخصص سامانه‌های فاواناجا	4.40	0.64
۹	استفاده از سامانه‌های نرم‌افزاری، الگوریتم‌های رمز و سخت‌افزاری بومی یا تأییدشده در ناجا	4.38	0.64
۱۰	تأمین نیازمندی‌های پشتیبانی فنی همچون خطوط برق موازی و اضطراری، خطوط ارتباطی موازی برای بخش‌های اصلی و مراکز حساس و مهم در ناجا	4.20	0.76
۱۱	شناخت و تهیهٔ سند وضع موجود فضای مجازی ناجا شامل مکان‌ها، سخت‌افزارها و ارتباطات، نرم‌افزارها (معماری و رمز برنامه‌ها و مانند آن)، اولویت‌بندی و سطح امنیتی، شناخت نقاط ضعف و آسیب و دیگر موارد	4.30	0.65
	میانگین کلی	**4.33**	**0.75**

طبق داده‌های جدول ۴ و به‌نظر پاسخگویان، در دستهٔ عوامل مؤثر در امنیت فضای مجاز ارتباطات و اطلاعات در ناجا، بیشترین امتیاز را کسب اطمینان از به‌کارنبردن سخت‌افزارهای اهدایی، کشف‌شده یا بدون صاحب در ناجا، با امتیاز ۴/۴۴ دارد و کمترین امتیاز نیز مربوط به تأمین نیازمندی‌های پشتیبانی فنی همچون خطوط برق موازی و اضطراری، خطوط ارتباطی موازی برای بخش‌های اصلی و مراکز حساس و مهم در ناجا، با امتیاز ۴/۲ است. در ضمن، میانگین کلی عوامل مؤثر در امنیت فضای مجازی ارتباطات و اطلاعات در ناجا نیز ۴/۳۳ به‌دست آمده است.

شیوه های گسترش اقدام‌های حفاظت ارتباطات و اطلاعات در امنیت فضای مجازی ناجا، با رویکرد پدافند غیرعامل

جدول ۵: مقایسهٔ میانگین شیوه های گسترش اقدام های حفاظت ارتباطات و اطلاعات در امنیت فضای مجازی ناجا، با رویکرد پدافند غیرعامل

ردیف	شیوه‌های توسعهٔ اقدام‌های حفاظت ارتباطات و اطلاعات در امنیت فضای مجازی ناجا، با رویکرد پدافند غیرعامل	شاخص آماری	
		میانگین امتیاز کلی	انحراف معیار کل
۱	رعایت استاندارد و طرح‌های حفاظت فیزیکی مراکز و اماکن، به‌منظور پیشگیری از تهدیدهای طبیعی و غیرطبیعی و مقابله با آن‌ها	4.30	0.58
۲	رعایت اصول پدافند غیرعامل شامل اختفا، استتار، مقاوم‌سازی، پراکنده‌سازی، پشتیبان سازی و جلوگیری از تحلیل، تضعیف، اختلال، فریب و موارد دیگر	4.28	0.70
۳	پیش‌بینی و ایجاد لایه‌ها و قابلیت‌های امنیتی مورد تأیید در نرم‌افزارها، با هدف واپایش امنیت آن‌ها (واپایش سامانه‌ها برای دراختیارداشتن دسترسی‌ها و لاگ‌ها، واپایش محتوا، تأییدیهٔ امنیتی و مانند آن)	4.46	0.61
٤	توزیع کلیدهای رمز و سازوبرگ امنیتی بسترهای ارتباطی برای امن‌سازی آن‌ها و حیطه‌بندی در توزیع سرویس‌های بسترهای ارتباطی	4.50	0.65
٥	طراحی و پیاده‌سازی شبکه‌های ارتباطی استاندارد و امن و منطبق بر سیاست‌های حفاظتی و امنیتی	4.34	0.80
٦	ایجاد ظرفیت های احتیاط و پشتیبانی برای بخش‌های ضروری با ویژگی امنیت، ایمنی و پایداری متناسب با سطح طبقه‌بندی آن	4.18	0.66
۷	بهره‌گیری از سامانه‌های هوشمند و آنی برای تحلیل خطرها و هشداردهی مانند مرکز امنیت اطلاعات (SOC)	4.40	0.67
۸	پیش‌بینی و تأمین نیروهای واکنش سریع و امدادرسانی در مواقع بحرانی (cert)	4.30	0.61
۹	راه‌اندازی و نهادینه‌کردن جایگاه پدافند رایانه‌ای در دبیرخانهٔ پدافند غیرعامل ناجا برای اهمیت، همراهی مدیریتی، تخصیص بودجه و مواردی از این دست، در سطح سازمان و رده‌ها، با شرح وظایف مشخص	4.54	0.58
۱۰	تهیهٔ شیوه‌نامهٔ اجرایی اصول پدافند غیرعامل شامل اختفا، استتار، مقاوم‌سازی، پراکندگی و پشتیبان‌سازی در حوزهٔ فاواناجا	4.26	0.75
۱۱	همراهی و همکاری مدیران بابت تأمین بودجه و ... حوزهٔ امنیت و پدافند غیرعامل در گسترهٔ فنّاوری اطلاعات	4.25	0.78

۱۲	تأمین ارتباطات امن و پایدار بین مراکز پدافندی رایانه‌ای بخش‌های گوناگون ناجا	4.56	0.61
۱۳	سامان‌دهی و راه‌اندازی ساختار مدیریت امنیت اطلاعات، مرکزهای امداد و نجات رایانه‌ای (CERT)، مراکز امنیت عملیات (SOC)	4.42	0.54
۱٤	آموزش و توجیه نیروی متخصص و کارآمد برای حفظ پایداری سامانه‌ها در زمان بحران	4.54	0.68
۱۵	تعیین و به‌کارگیری استانداردهای دفاعی و امنیتی بومی‌شده، متناسب با مأموریت و وظایف معین ناجا	4.48	0.76
	میانگین کلی	4.39	0.67

بر اساس داده‌های جدول ۵ و طبق نظر پاسخگویان، در موضوع‌های مربوط به شیوه‌های گسترش اقدام‌های حفاظت ارتباطات و اطلاعات در امنیت فضای مجازی ناجا با رویکرد پدافند غیرعامل، بیشترین میزان امتیاز مربوط به تأمین ارتباطات امن و پایدار بین مراکز پدافندی رایانه‌ای بخش‌های گوناگون ناجا، با امتیاز ۴/۵۶ است و کمترین امتیاز هم تعلق دارد به همراهی و همکاری مدیران بابت تأمین بودجه و ... پهنه‌های امنیت و پدافند غیرعامل در گسترهٔ فنّاوری اطلاعات، با امتیاز 4/۲۵. در ضمن، میانگین کلی شیوه‌های گسترش اقدام های حفاظت ارتباطات و اطلاعات در امنیت فضای مجازی ناجا، با رویکرد پدافند غیرعامل نیز، برابر با ۴/۳۹ به‌دست آمده است.

در این بخش شاخص‌های آماری، شامل میانگین و انحراف‌معیار گویه‌ها، بر اساس دستورالعمل مربوط به دسته‌بندی عوامل محاسبه و استخراج شده است.

نتیجهٔ نرمال‌بودن داده‌ها

با توجه به اطلاعات به‌دست‌آمده به‌دلیل اینکه سطح معناداری متغیرهای تحقیق بزرگ‌تر از ۰,۰۵ است و نیز مقدار آمارهٔ کولموگروف- اسمیرنف[1] بین ۱/۹۶+ و ۱/۹۶- قرار دارد، فرض صفر تأیید و ادعای نرمال‌بودن توزیع این متغیرها پذیرفته می‌شود؛ بنابراین، به‌منظور بررسی فرضیه‌های تحقیق، می‌توان از آزمون‌های مؤلفه‌ای همچون آمارهٔ t تک‌نمونه استفاده کرد.

1. Kolmogorov–Smirnov test

عوامل		جایگاه و نقش حفاظت	تهدیدهای ارتباطات و اطلاعات	عوامل مؤثر امنیت فضای مجازی در ارتباطات و اطلاعات	شیوه‌های گسترش اقدام‌های حفاظت فنّاوری
عامل‌های تعیین‌کنندهٔ نرمال	میانگین کلی	۴/۴۸	۴/۳۱	۴/۳۳	۴/۳۹
	انحراف معیار	۰/۶۴	۰/۸۲	۰/۷۵	۰/۶۷
مقدار کولموگروف- اسمیرنف		۱/۱۵۸	۰/۹۳۹	۰/۹۲۰	۰/۷۱۴
Sig(2 – tailed)		۰/۱۳۷	۰/۳۴۲	۰/۱۱۵	۰/۶۸۸

بحث و نتیجه‌گیری

با رشد فناوری اطلاعات و ذخیره‌سازی داده‌ها در رایانه‌ها و گسترش بهره‌گیری از فضای مجازی در جامعهٔ روبه‌رشد امروز، حمله‌های رایانه‌ای در زمینهٔ اطلاعات در فضای مجازی افزایش چشم‌گیری یافت؛ بنابراین، موضوع پدافند غیرعامل در فناوری اطلاعات و رعایت اصول آن به‌منظور امنیت و پایداری زیرساخت‌های ضروری و حساس برای کشورها بسیار اهمیت دارد. نیروی انتظامی جمهوری اسلامی ایران یکی از نهادهای بسیار اثرگذار کشور است که به‌دلیل ضریب نفوذ بالای نود درصدی فناوری اطلاعات در مأموریت‌ها و فرایندهای سازمانی و انباشت اطلاعات مهم در قالب سامانه‌های جامع ناجا و خدمات الکترونیک، همواره مورد توجه دشمنان داخلی و خارجی است تا آن را تخریب و در آن اختلال ایجاد کنند یا مشکل‌های دیگری از این دست پدید آورند. ازاین‌رو، نیاز است موضوع پدافند غیرعامل در فناوری اطلاعات و زیرساخت‌های اصلی برای در امان ماندن از جنگ‌های رایانه‌ای مورد توجه قرار گیرد.

تحقیق حاضر به‌خوبی نشان داد که جایگاه و نقش حفاظت فنّاوری اطلاعات در تحقق هدف‌های مأموریتی سازمان‌ها، در بین همهٔ عواملی که برای این نقش در امنیت بهتر و مناسب فضای مجازی ناجا مدنظر قرار گرفته بود، اهمیت بسیار ویژه‌ای دارد. البته این موضوع بدین‌معنا نیست که به دیگر مؤلفه‌ها، مانند حفاظت از سامانه‌ها و زیرساخت‌های

فناوری اطلاعات و ارتباطات یا نقش این زیرساخت‌ها نزد دشمنان و مخالفان و اخلال‌گران و سودجویان به‌منزلهٔ هدف و نشانگاه عملیاتی جنگ رایانه‌ای، توجه نشود.

نتیجهٔ این تحقیق با بخش‌هایی از یافته‌ها و نتایج پورمراد (۱۳۸۶)، راسخی (۱۳۹۰)، عبدالرحمان (۲۰۱۰) همسویی و مطابقت دارد.

در تحلیل نتایج به‌دست‌آمده، می‌توان بیان کرد سازمان‌های حفاظت اطلاعاتی از سازمان‌های عضو جامعهٔ اطلاعاتی کشورند که با توجه به عملکرد و رفتارهای حرفه‌ای خود و اصل حرفه‌ای‌کردن امور، در نخستین مرحله با نگاهی ویژه به ساختار درونی و درپیش‌گرفتن تمهیدهای منطقی، باید گام‌های مؤثری را به‌منظور توانمندسازی عملیات سازمان متبوع خود بردارند و با توزیع اطلاعات مورد نیاز، اثربخشی خود را در لایه‌های گوناگون تصمیم‌سازی و تصمیم‌گیری نشان دهند. البته به‌نظر می‌رسد در موضوع‌ها و مؤلفه‌های دیگری همانند نقش حفاظت در خرید و تولید نرم‌افزارهای منطبق با سیاست‌های ابلاغی یا نقش حفاظت در بهره‌گیری هدفمند از عوامل درون‌سازمانی، در جایگاه سپری برای جلوگیری از نفوذ دشمنان در تحقق هدف‌های رایانه‌ای، یا عرضهٔ دستورالعمل‌های تخصصی و اجرایی برای انجام‌دادن اقدام‌های مقابله‌ای و توجیه کارکنان ناجا و همچنین، در بررسی صلاحیت‌ها و تسلط علمی و میزان امنیتی برای رصد و نظارت مراحل پیاده‌سازی و بهره‌برداری سامانه‌ها و شبکه‌ها می‌تواند اهمیت داشته باشد و اصول ایمنی و حفاظتی به‌دقت رعایت شود. همچنین ضروری است در این زمینه، مدیران عالی و تصمیم‌ساز درمورد تهدیدها و برون‌سپاری پروژه‌های فناوری اطلاعات، ضابطه‌های امنیتی و حفاظتی تولید، پشتیبانی و رفع عیب نرم‌افزار و مانند آن‌ها توجیه شوند.

در حوزهٔ شیوه‌های گسترش اقدام‌های حفاظت ارتباطات و اطلاعات در امنیت فضای مجازی ناجا با رویکرد پدافند غیرعامل، همان‌گونه که نتیجهٔ حاصل، اهمیتِ این نکته را آشکار کرد، تأمین ارتباطات امن و پایدار بین مراکز پدافند رایانه‌ای بخش‌های گوناگون ناجا حساسیتی دوچندان دارد، زیرا تأمین امنیت پایدار سبب خواهد شد، نخست، افراد ذی‌نفع در سایهٔ این امنیت احساس آرامش کنند و افزون بر آن، ضمن حفظ هوشیاری، از

تهدیدها و آسیب‌های دشمنان در امان باشند. بی‌تردید، توجه به این شیوه‌ها و شناسایی آن‌ها و همچنین همراهی و همکاری مدیران بابت تأمین بودجه و ... پهنه‌های امنیت و پدافند غیرعامل در حوزهٔ فناوری اطلاعات و رعایت اصول پدافند غیرعامل و، در کنار آن، توجه به استانداردها و رعایت آن‌ها به‌منظور پیشگیری از تهدیدها و مقابله با آن‌ها، شرایط بسیار مساعد و مناسبی را برای ناجا و کشور به‌دنبال خواهد داشت.

پیشنهادهای کاربردی تحقیق

نتایج این تحقیق نشان داد، در میان جایگاه و نقش حفاظت ارتباطات و اطلاعات در امنیت فضای مجازی ناجا، بیشترین امتیاز به جایگاه و نقش حفاظت فناوری اطلاعات در تحقق هدف‌های مأموریتی سازمان‌ها اختصاص دارد. شایسته است مدیران عالی و تصمیم‌ساز در زمینهٔ حفاظت ارتباطات و اطلاعات رایانه‌ای ساحفاناجا این اهمیت و نقش را در نظر بگیرند.

همچنین به این دلیل که، در بین انواع تهدیدهای ارتباطات و اطلاعات در امنیت فضای مجازی ناجا، موضوع آگاه‌سازی و توجیه مدیران درمورد تهدیدها و ضابطه‌های برون‌سپاری پروژه‌های فناوری اطلاعات (ضابطه‌های امنیتی و حفاظتی تولید، پشتیبانی و رفع عیب نرم‌افزار و مانند آن) بسیار ضروری است؛ لازم است این آگاه‌سازی به شکل پایدار و مطلوبی صورت پذیرد.

مدیران ارشد و کارشناسان حفاظت باید، ضمن توجه به علل و عوامل تأثیرگذار در امنیت فضای مجازی ارتباطات و اطلاعات در ناجا، پشتیبانی‌ها و حمایت‌های لازم را نیز در این زمینه داشته باشند.

آشنایی افراد دست‌اندرکار با شیوه‌های گسترش اقدام‌های حفاظت ارتباطات و اطلاعات در امنیت فضای مجازی ناجا با رویکرد پدافند غیرعامل باید همواره مورد توجه قرار گیرد.

بهره‌مندی از تجربه‌های سازمان‌هایی که وظایفی مشابه با حوزهٔ حفاظت ارتباطات و اطلاعات رایانه‌ای ساحفاناجا دارند بسیار مفید و مؤثر خواهد بود. مستندسازی فعالیت‌ها و تبادل تجربه‌ها توصیه می‌شود.

منابع:

اروسخانی، علی (۱۳۸۷)، حفاظت ارتباطات، تهران: کوثر.

آستانا، ان. سی. و نیرمال، آنجالی (۱۳۸۸)، *مدیریت اطلاعات و امنیت*، ترجمهٔ معاونت پژوهش، تهران: دانشکدهٔ اطلاعات.

اسکندری، حمید (۱۳۹۰)، *دفاع سایبری و امنیت رایانه*، تهران: بوستان حمید.

آیین‌نامهٔ امنیت ارتباطات و فنّاوری اطلاعات ن. م. مصوب فرماندهی معظم کل قوا (۱۳۸۷).

پورمراد، مجید (۱۳۸۷)، حفاظت فناوری اطلاعات و ارتباطات، تهران: کوثر.

چالوک، غلامرضا و محمدتقی عصار (۱۳۹۲)، *پدافند غیرعامل در جنگ نرم*، تهران: معاونت تربیت و آموزش ناجا.

حدیث ولایت (۱۳۸۳)، *رهنمودهای مقام معظم رهبری در جمع شورای عالی انقلاب فرهنگی*، آذرماه.

دهقانی فیروزآبادی، سید جلال (۱۳۹۰)، «فنّاوری‌های قدرت در جنگ نرم»، *مطالعات راهبردی*، شمارهٔ ۵۱.

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

فرهند، محمد و محمدرضا شعبانی (۱۳۸۹)، «بررسی نقش فنّاوری‌های اطلاعاتی و ارتباطی نوین بر افزایش توان تهدیدات نرم»، *مجموعهٔ مقالات همایش امنیت نرم*، جلد ۲، تهران: دانشکدهٔ امام هادی (ع).

کریمایی، علی اعظم (۱۳۸۷)، *کلیات حفاظت اطلاعات*، چاپ دوم، دانشگاه علوم انتظامی ناجا، حدیث کوثر.

معمار، مهرنوش (۱۳۸۸)، «اینترنت، اعتیاد مجازی»، همایش علمی فضاهای مجازی، آسیب‌ها و پیامدها، سمنان: سینا نوین.

مقدمه‌ای بر پدافند غیرعامل در حوزهٔ امنیت فیزیکی و کنترل دسترسی (۱۳۸۹)، تهیه‌کننده: مرکز پدافند غیرعامل فاوا، شرکت مخابرات ایران.

مندل، رابرت (۱۳۷۷)، *چهرهٔ متغیر امنیت ملی*، تهران: پژوهشکدهٔ مطالعات راهبردی.