Center for Strategic Studies of the
Islamic Republic of Iran Army

Journal Of
Army Strategic Research
Print ISSN:27834212
Volume 1, Issue 2
Winter 2023
P.P. 19-34

required Capabilities of the I.R.I Army for Cyber Operations

Nasser Shahlaei [1]

Abstract
The virtual space has become a part of states' sovereignty and their national security also includes defense of cyber space. Implementation of the cyber operation is also a duty of the I.R.I army. Some capabilities is necessity for doing this duty. Due to the relatively new nature of the duty, at the first we must identify required capabilities to enable AJA to accomplish their mission. Main aim of this article is to determine required capabilities of the I.R.I army for cyber operations. The present research is an applied and developmental research in term of results of the research that have a qualitative approach. Expert meetings were held with the presence of professionals. To gather and analysis data and information, library and field study method are used. The statistical population is about 50 people that 20 persons of them are selected by purposive sampling approach. Inferential statistics method has been applied to evaluate information and analysis data. The conclusions show that AJA for doing cyber operations must be able to perform 3 duties and have 20 capabilities. These duties including defense, cyber security, Offensive cyber-attack and support of cyber operations.

Keywords:Cyber operations, duty, sub task, capability
Citation: Shahlaei, Nasser(2022). required Capabilities of the I.R.I Army for Cyber Operations– Resistance Economy Approach. *Journal Of Army Strategic Research, 1 (2), 19-34*

1.PhD. Strategic Management. Supreme National Defense niversity. Tehran. Iran
.Nasser.shahlaei@mail.com

Received: 2022/08/21 **Article Type : Research - based**
Accepted: 2022/11/04

فصلنامه پژوهش‌های راهبردی ارتش
شاپای انتشار: ۲۷۸۳۴۲۱۲
سال اول، شماره دوم
زمستان ۱۴۰۱
صص: ۳۴-۱۹

مرکز مطالعات راهبردی

قابلیت‌های مورد نیاز ارتش جمهوری اسلامی ایران برای عملیات سایبری

ناصر شهلائی[۱]

چکیده

فضای مجازی بخشی از قلمرو حاکمیتی کشورها شده است و امنیت ملی آنها، شامل دفاع از فضای سایبری نیز می‌شود. اجرای عملیات سایبری نیز یکی از وظایف ارتش جمهوری اسلامی ایران محسوب می‌گردد. لازمه انجام این وظیفه، داشتن قابلیت‌هایی است. با توجه به بالنسبه جدید بودن این وظیفه، در ابتدا باید قابلیت‌های مورد نیاز آن را شناسایی نماییم تا با کسب آنها اجا بتواند این مأموریت را اجرا کند. هدف اصلی این تحقیق، تعیین قابلیت‌های مورد نیاز ارتش جمهوری اسلامی ایران برای عملیات سایبری است. تحقیق حاضر بر حسب نتایج تحقیق از نوع کاربردی توسعه‌ای می‌باشد که با رویکرد کیفی صورت پذیرفت. جلسات خبرگی با دعوت از متخصصان برگزار شد. جهت جمع‌آوری و تحلیل داده‌ها از روش‌های اسنادی و استفاده از روش موردی زمینه‌ای و توصیفی تحلیلی استفاده شد. تعداد جامعه آماری، حدود ۵۰ نفر می‌باشد که ۲۰ نفر از خبرگان جامعه آماری به صورت قضاوتی (هدفمند) به جلسات خبرگی دعوت شدند. برای بررسی آماری اطلاعات و تجزیه و تحلیل داده های حاصله، از روش آمار استنباطی استفاده شد. نتایج تحقیق نشان می‌دهد که اجا برای اجرای عملیات سایبری، باید بتواند سه وظیفه و نه زیروظیفه را انجام دهد و ۲۰ قابلیت را دارا باشد. این وظایف عبارتند از: دفاع و امنیت سایبری، آفند و حمله پیش‌دستانه سایبری و پشتیبانی از عملیات سایبری.

واژگان کلیدی: عملیات سایبری، وظیفه، زیروظیفه، قابلیت.

استناد: شهلائی ، ناصر (۱۴۰۱). قابلیت‌های مورد نیاز ارتش جمهوری اسلامی ایران برای عملیات سایبری؛ *فصلنامه پژوهش‌های راهبردی ارتش ۱(۲). ۳۴-۱۹.*

---

[۱]. دانش آموخته دکتری. مدیریت راهبردی. دانشگاه عالی دفاع ملی. تهران. ایران.
Nasser.shahlaei@mail.com

نوع مقاله: پژوهشی
تاریخ دریافت: ۱۴۰۱/۰۵/۳۰
تاریخ پذیرش: ۱۴۰۱/۰۸/۱۳

مقدمه

امروزه اینترنت در سراسر دنیا حدود ســـه میلیارد نفر کاربر دارد. با این وجود، اینترنت دولت‌ها را در مقابل چالش‌های جدید امنیتی قرار داده است. هزینه کم ورود، ناشناس بودن، مشخص نبودن قلمرو جغرافیایی تهدیدکننده، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری، موجب شده بازیگران قوی و ضعیف اعم از دولت‌ها، گروه‌های سازمان یافته و تروریستی و حتی افراد، به این فضا وارد شده و تهدیدهایی همچون جنگ سایبری، جرایم سایبری، تروریسم سایبری، جاسوسی سایبری و مانند آنها را به‌وجود آورند (خلیلی پور رکن آبادی و نورعلی وند، ۱۳۹۱:)

فضای مجازی بخشی از قلمرو حاکمیتی کشورها شده است و امنیت ملی آنها، شامل دفاع از فضـای سـایبری نیز می‌شـود. عملیات سـایبری تنها به حوزه غیرنظامی محدود نیسـت؛ بلکه اهداف نظامی هم، از آماج این عملیات و تهدیدات در امان نبوده و نخواهد بود. جاســـوســـی سـایبری، تروریسـم سـایبری و نابود کردن زیرسـاخت‌های فناوری اطلاعات و ارتباطات مراکز نظامی، گوشــه‌ای از تهدیدات نظامی ســایبری محســوب می‌گردند که مقابله با آنها از وظایف سازمان‌ها و نهادهای حاکمیتی می‌باشد.

با گسـترش هرچه بیشـتر فناوری اطلاعات و ارتباطات، بسـیاری از دولت‌ها و حتی نهضـت‌ها و مخالفان دولت‌ها به عملیات ســایبری مجهز شــده‌اند. از جمله، ناتو از ســال ۲۰۰۷ در حوزه سایبر فعال شد و به شکلی موضوع تهدیدات سایبری را در دستور جلسات رسمی خود وارد کرد. آنچه بر اساس دلایل و شـواهد موجود می‌توان گفت این اسـت که مهمترین دلایل ورود مباحث سـایبری در دسـتور جلسـه ناتو، نگرانی شـدید اعضا از تهدیدات سـایبری و به خصـوص ماهیت متفاوت آن و در عین حال مصـادیقی چون حملات سـایبری روسـیه و چین می‌باشـد (ترابی، ۱۳۹۴: ۱۴۳). توسـل داعش به عملیات سـایبری و اسـتفاده گسـترده آنها از فضـای مجازی برای اهدافی مانند جذب نیرو از کشـورهای مختلف، نشـانگر اهمیت این نوع عملیات می‌باشد.

اجرای عملیات سـایبری یکی از وظایف ارتش جمهوری اسـلامی ایران محسـوب می‌گردد؛ چرا که از یک سـو برای محافظت از زیرسـاخت‌های فناوری اطلاعات و ارتباطات خود باید قادر به

دفاع (پدافند) سایبری باشد و از سوی دیگر، به موجب اصل یکصد و چهل و سوم قانون اساسی ارتش جمهوری اسلامی ایران پاسداری از استقلال و تمامیت ارضی و نظام جمهوری اسلامی کشور را بر عهده دارد و بر این اساس، خواه به عنوان وظیفه اصلی و خواه به عنوان وظیفه فرعی، اجا باید قابلیت اجرای عملیات سایبری و استفاده از فضای سایبر برای اهداف نظامی را داشته باشد. با عنایت به جدید بودن این وظیفه، هدف اصلی این تحقیق، تعیین قابلیت‌های مورد نیاز ارتش جمهوری اسلامی ایران برای عملیات سایبری است و سؤال اصلی بدین شرح است: قابلیت‌های مورد نیاز ارتش جمهوری اسلامی ایران برای عملیات سایبری کدامند؟ مسأله این تحقیق آن است که ارتش جمهوری اسلامی ایران برای اجرای عملیات سایبری به چه قابلیت‌هایی نیاز دارد.

پیشینه

در نتایج تحقیق "تحول مفهوم امنیت در پرتو جهانی شدن و فناوری اطلاعات و ارتباطات نوین" آمده است: درپرتو جهانی شدن و فناوری اطلاعات، یکی از مهمترین تغییرات در مفهوم امنیت حرکت این مفهوم از حالت عینی صرف به حالت ذهنی بوده است. بنابراین به همان تناسب میزان استفاده از ابزار و فناوری‌های نرم نیز در ایجاد امنیت یا ناامنی اهمیت یافت. بر این اساس باید گفت در فرایند تاریخ با تغییر مفهوم تهدیدات، مفهوم امنیت نیز تغییر پیدا کرده است؛ اما در این مسیر وجود یک متغیر میانجی به نام فناوری اطلاعات و ارتباطات توانسته است منجر به بازتعریف این مفاهیم و به صورت خاص مفهوم امنیت گردد. به مقتضای گسترش دامنه این فناوری در حوزه‌های سیاسی، اقتصادی، نظامی، اجتماعی و فرهنگی و زیست محیطی، تهدیدات نیز از حوزه کلاسیک و نظامی خود که بیشتر مفهومی عینی داشت خارج و تهدیدات جدید که حوزه ذهنی را نیز در بر می‌گرفت وارد شد (سلطانی نژاد و همکاران، ۱۳۹۵).

در تحقیق "جنگ سایبر از منظر حقوق بین الملل بشردوستانه " نتیجه گرفته‌اند که حقوق بین‌الملل بشردوستانه، حملات سایبری را که باعث کشتار و تخریب عمدی تأسیسات غیرنظامی

شود را ممنوع می نماید. مثال هایی از آن شامل تخریب سیستم کنترل رفت‌وآمد هوایی که باعث شود تا هواپیماهای مسافربری سقوط کنند، یا دستکاری بانک اطلاعات پزشکی که باعث شود غیرنظامیان و سربازان زخمی گروه خونی ناهمخوانی دریافت کنند. به عبارت بهتر، اصول حقوق بین‌الملل بشردوستانه می‌تواند حاکم بر فضای عمومی جنگ سایبر باشد. اما این روند نیازمند تدوین قوانین تخصصی‌تر و کارآمدتری می باشد تا بتواند در صحنه‌های جنگ نیز کارایی داشته باشد (عباسی و مرادی، ۱۳۹۴).

رمضان‌زاده (۱۳۹۴) راهبرد مناسب ارتش جمهوری اسلامی ایران برای دفاع سایبری را این‌گونه تدوین کرده است: محافظت و پدافند از شبکه‌ها و سامانه‌های فاوا پایه حیاتی، حساس و مهم در مقابل تهدیدات فزاینده فضای سایبری و استفاده از فرصت‌های این فضا در جهت تقویت قابلیت‌های عملیاتی در عرصه سایبر و مشارکت در مدیریت بحران و جنگ سایبری در تعامل پیوسته با سایر واحدهای مشابه در سطوح نیروهای مسلح و کشوری.کادل[1] و نیوکامر[2] در تحقیق " برنامه‌ریزی مبتنی بر قابلیت‌های امنیت وطن: درس‌هایی از اجتماع دفاع[3]" در گام اول، ابتدا با رهنمودهای دولت (مرجع سیاست‌گذاری) و در نظر گرفتن اولویت‌های دفاعی، به سناریوهای عملیاتی رسیده‌اند. در این رویکرد نگاه اصلی به قابلیت‌هاست و وزن اصلی بر قابلیت‌ها گذارده شده است و در دو مرحله ابتدا قابلیت اهداف مورد چالش قرار گرفته و در مرحله بعد، علاوه بر بررسی و اعتباردهی قابلیت‌ها، انحراف و عدم انطباق آنها با اهداف (یا به عبارتی نقش‌ها) بررسی گردیده و در انتها قابلیت‌های قلبل اعتماد، در یک برنامه مورد توسعه قرار گرفته است. در این تحقیق، روش آبشاری استفاده شده است و ابتدا مأموریت یا به گونه‌ای سناریوی دفاعی تعریف شده و سپس، موضوعات

1.Caudle

2.Newcomer

3.Homeland Security Capabilities-Based Planning: Lessons from the Defense Community

مرتبط با نقش‌های لازم استخراج گردیده‌اند. در ادامه به دلیل کلی و بزرگ بودن نقش‌ها، آنها را به زیرنقش‌هایی شکسته و برای اجرای این زیرنقش‌ها، بازیگران لازمه (عوامل) تعریف شده‌اند. در انتها، قابلیت‌هایی که هر عامل برای انجام زیرنقش مربوطه باید داشته باشد، مورد ارزیابی قرار گرفته است.

فضای سایبر[1]

تعاریف متعدد و عموماً یکسانی از فضای سایبر ارایه شده است؛ از جمله:

منظور از فضای سایبر یا فضای مجازی، ترکیبی از ده‌ها هزار رایانه به هم پیوسته، سرویس‌دهنده‌ها، سوئیچ‌ها و کابل‌های فیبر نوری است که امکان ایجاد ارتباطات را در یک سامانه جامع فراهم می‌آورد (رمضان‌زاده، ۱۳۹۴: ۱۰۸). فضای مجازی عبارت است از مجموعه‌ای از ارتباطات بین انسان‌ها از طریق رایانه و وسایل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی (یزدان پناه درو و کامران، ۱۳۹۳: ۲۷).

وزارت دفاع آمریکا، فضای سایبر را به عنوان «قلمرو جهانی در محیط اطلاعاتی مشتمل بر شبکه به هم پیوسته‌ای از زیرساخت‌های فناوری اطلاعات شامل اینترنت، شبکه‌های ارتباطات راه دور، سیستم‌های رایانه و پردازشگرها و کنترل کننده‌های تعبیه شده» تعریف کرده است (Ottis and Lorents, ۲۰۱۰:۲). فضای سایبر در اصل یک فضا و محیطی است مشابه سایر حوزه‌های رقابتی همچون دریا، زمین و هوا؛ اما با یک تفاوت و آن هم اینکه این محیط برخلاف بقیه محیط ها ساخته دست بشر بوده و غیرملموس است (Libicki, ۲۰۰۹:۱۱).

جنگ سایبری

امروزه با توجه به تحولات صورت گرفته در سطح جهان و به خصوص انقلاب اطلاعات و ارتباطات، تهدیدات فضای سایبر و به خصوص "جنگ سایبری"[2] از جمله مهمترین مصادیق "جنگ‌های جدید"[3]، محسوب می‌شوند. گستردگی و همچنین جدی بودن این نوع جنگ در سطحی است که تقریباً تمامی کشورها حوزه سایبر را به عنوان حوزهای امنیتی و حتی گاه

---

1. Cyber Space
2.Cyber War
3.New War

نظامی در نظر می‌گیرند و ساختارها و مراکزی را برای مقابله با تهدیدات و خطرات این حوزه ایجاد کرده‌اند (ترابی، ۱۳۹۴: ۱۳۴).

جنگ سایبری عبارت از : استفاده از رایانه‌ها، به عنوان یک اسلحه یا به عنوان ابزاری برای انجام کارهای خشونت‌بار جهت ترساندن یا تغییر عقیده یک گروه یا کشور است. جنگ سایبر به قصد کارهای سیاسی و آرمانی انجام می‌گیرد و مکان‌ها و تأسیسات حیاتی مانند انرژی، حمل و نقل، ارتباطات و سرویس‌های ضروری را هدف قرار می‌دهد و از شبکه‌های رایانه‌ای به عنوان بسترهایی جهت انجام این اعمال خرابکارانه استفاده می‌کند (سید مفیدی، ۱۳۸۸: ۵۶). جنگ سایبر در ساده ترین تعریف به عنوان «استفاده از رایانه و اینترنت برای جنگیدن در فضای سایبر تعریف شده است» (عبدالله‌خانی، ۱۳۸۶: ۱۳۵). مرکز عملیات سایبری آمریکا و کتاب راهنمای تروریسم سایبری حملات سایبری را به صورت زیر تعریف می‌کنند: استفاده عمدی از فعالیت‌های مختل کننده، یا تهدید مربوط به آن، علیه رایانه‌ها و شبکه‌ها، با هدف ضرر و زیان به بار آوردن، بیشتر با هدف اجتماعی، ایدئولوژیکی، مذهبی، سیاسی یا اهداف مشابه؛ یا برای وادار کردن هر شخصی برای پیشبرد چنین اهدافی (Swanson, ۲۰۱۰: ۳۰۷).

در فهم ابعاد و شاخص‌های جنگ سایبری، اولین نکته‌ای که به ذهن می‌رسد، گنگی و ابهام ذاتی این مفهوم و نداشتن مرزی روشن بین آن با سایر تهدیدات و حتی تهدیدات سایبری از جمله "جاسوسی سایبری"[1] و "سایبرتروریسم"[2] می‌باشد (ترابی، ۱۳۹۴: ۱۳۷). دو رویکرد اساسی در حوزه سایبری عبارت است از :پدافند سایبری و آفند سایبری . ایجاد قابلیت پدافند سایبری به مفهوم آماده‌سازی زیرساخت‌ها و سازوکارهای لازم جهت مقاوم‌سازی سدهای دفاعی شبکه‌های اطلاعاتی و سامانه‌های کنترل از راه دور خودی به منظور مقاومت در مقابل نفوذ تهدیدات سایبری و دفع موضعی آنها است. ایجاد قابلیت آفند سایبری به مفهوم آماده‌سازی زیرساخت‌ها و سازوکارهای لازم جهت توانایی نفوذ به شبکه‌های اطلاعاتی و

1.Cyber Spy
2.Cyber Terrorism

سامانه‌های کنترل از راه دور تهدیدات به منظور جمع‌آوری اطلاعات، ایجاد اختلال، فریب و تخریب در آنهاست (رمضان‌زاده، ۱۳۹۴: ۱۱۰).

برخی از کارشناسان، جنگ سایبری را حوزه‌ای جدید و مستقل از جنگ و دفاع در نظر گرفته‌اند که به شکل هم زمان، برخی از ابعاد و مؤلفه‌های "جنگ سخت" و "جنگ نرم" را دارد، اما در عین حال دارای ماهیت و محتوایی متفاوت از هر دوی آنها می‌باشد. به باور آنها جنگ سایبری حوزه‌ای جدید از جنگ محسوب می‌شود که طی آن بازیگران دولتی تلاش می‌کنند از فضای سایبر به عنوان سلاح مستقل استفاده کنند. در این جنگ، طرف‌های درگیر، طیف گسترده‌ای از بازیگران شامل دولت‌ها و شرکت‌های دولتی و خصوصی، هکرها و افراد، البته تحت فرمان دولت‌ها هستند که تلاش می‌کنند از سلاحی جدید، به عنوان فضای سایبر استفاده کنند تا به دشمن آسیب برسانند و یا اینکه عزم آن را برای انجام یا عدم انجام کاری تحت فشار قرار دهند (Krepinevich,۷-۱ :۲۰۱۲)

مهم‌ترین ویژگی‌های تهدیدهای سایبری در مؤلفه‌های زیر خلاصه می‌شود (احمری و همکاران، ۱۳۹۵: ۳۱۲):

۱. تعدد بازیگران در فضای سایبری
۲. هزینه کم و سرعت بالای اقدام
۳. ناشناس ماندن بازیگران و عدم قابلیت ردیابی
۴. تأثیرگذاری شگرف
۵. کمرنگ شدن نقش جغرافیا
۶. ساختار فضای اینترنت
۷. پایین بودن احتمال تنبیه یا بازخواست اقدام های مجرمانه

جرایم سایبری

شاید بتوان گفت که جرایم رایانه‌ای همزاد با رایانه می‌باشند و همگام با بهره‌برداری از رایانه، ارتکاب جرایم رایانه‌ای نیز شروع شده است. در سال ۱۳۸۸ قانون جرایم رایانه‌ای به تصویب مجلس شورای اسلامی رسیده است. در این قانون جرایم رایانه‌ای تعریف نشده است؛ اما مصایق این جرایم بدین شرح بیان شده است: دسترسی غیرمجاز، شنود غیرمجاز،

جاسوسی رایانه‌ای، جعل رایانه‌ای، تخریب و اخلال در داده ها یا سامانه‌های رایانه‌ای و مخابراتی، سرقت و کلاهبرداری مرتبط با رایانه، جرائم علیه عفت و اخلاق عمومی و هتک حیثیت و نشر اکاذیب. در این قانون، مسؤولیت کیفری مرتکبان این جرایم بیان شده است و از نکات اصلی این قانون، به رسمیت شناختن مسئولیت کیفری برای اشخاص حقوقی است.

از دیدگاه بین‌المللی امضای کنوانسیون جرایم رایانه‌ای که به وسیله شورای اروپا در هشتم نوامبر ۲۰۱۱ صورت گرفت، نخستین اقدام در راه مبارزه بین‌المللی قانونی با پدیده جرایم رایانه‌ای بود (Atul, 2005: 121).

یکی از جرایم مهم رایانه‌ای که عموماً علیه دولت‌ها رخ می‌دهد، تروریسم سایبری می‌باشد. تروریسم سایبری این گونه معنا شده است: بهره‌گیری از اینترنت و شبکه‌های رایانه‌ای و امکاناتی که این شبکه‌ها پدید می‌آورند، با هدف نابود ساختن ساختارهای زیربنایی یک جامعه؛ مانند: انرژی، حمل و نقل، فعالیت‌های دولتی و تأثیر گذاشتن بر یک دولت، شهروندان، گروه‌ها و . . . (عباسی، ۱۳۸۳: ۳۰). دوروثی دنینگ[1] سایبر تروریسم را این گونه تعریف می‌کند: سایبر تروریسم حاصل همگرایی تروریسم و فضای مجازی است، سایبر تروریسم به معنای تهاجم و تهدید به تهاجم غیرقانونی به رایانه‌ها، شبکه‌ها و اطلاعات ذخیره شده در آنهاست که به منظور ارعاب یا وادارکردن یک دولت یا مردم آن به پیشبرد اهداف سیاسی یا اجتماعی خاص صورت می گیرد (Hancock ۲۰۰۱: ۵۵۶).

امنیت سایبری

ناامنی سایبری انواع و اقسامی دارد: از تبلیغات و به راه انداختن تبلیغات سیاسی علیه دولتی خاص گرفته تا سرقت و کلاهبرداری‌های چندملیتی؛ یعنی اینکه تهدیدهای سایبری فقط به حوزه سیاسی محدود نمی شود؛ بلکه شامل‌تهدیدهای علیه بنیان‌های خانواده، اقتصاد، صنعت و . . . است. به عبارتی بهتر برای هر چیزی که درجایی، برای کسی باارزش باشد و آن چیز بتواند با اینترنت و یا وسایل الکترونیکی که دارای بخش‌های نرم‌افزاری هستند و فضایی برای ذخیره اطلاعات دارند مرتبط شود، فضای سایبرمی‌تواند خطرساز

1.Dorothy Denning

باشـــد. از ایـــن رو، بـــه شـــدت نیـــاز بـــه اقدامی در جهت امنیت زایی در فضای مجازی، احساس می‌شود (میرزایی و همکاران، ۱۳۹۵: ۸۸).

امنیت سـایبری توسـط اتحادیه جهانی مخابرات به عنوان «مجموعه‌ای از ابزارها، سـیاسـت‌ها، مفاهیم امنیتی، خط‌مشـــی‌های حفاظتی، دیدگاه های مدیریت بحران، فعالیت‌ها، آموزش، بهترین رویه‌ها، اطمینان یا اعتماد و فناوری‌هایی است که می‌تواند برای حمایت محیط سایبر و دارایی‌های کاربر و سازمان استفاده شود" (Maurer, ۲۰۱۱: ۹-۸).

رویکرد قابلیت محور

در عصر جدید بیشتر مفاهیم عمیق گذشته در حال دگرگونی هستند. برای مثال، اصول بنیادین طرح‌ریزی دفاعی، از برنامه‌ریزی براسـاس تهدید به برنامه‌ریزی براسـاس توانمندی و امکانات و از آمادگی به فرصت تغییر یافته است (الاردیک، ۱۳۸۴: ۱). از سال ۲۰۰۳ میلادی به بعد، هم‌زمان با حمله آمریکا به عراق، رویکرد آمریکا از "تهدید محوری"، که حاصل جنگ ســـرد بود، به رویکرد "توانمندی (قابلیت) محوری"[1]، تبدیل شـــد. وزارت دفاع آمریکا برای کاهش مخاطرات و عدم قطعیت آینده از رویکرد تهدید محور، که محرک آن نیاز و مطالبات و توســـعه نیرو اســـت، به ســـمت رویکرد برنامه‌ریزی توانمندی محور که محرک آن مفاهیم عملیاتی[2] هستند، حرکت کرده است. تمرکز این رویکرد بیش از آن که متوجه نام دشمنان و مکان درگیری با نیروهای مشترک یا حمله به منافع آمریکا باشد، بر چگونگی شکست دادن طیف گسترده‌ای از قابلیت‌ها و توانمندی‌های مورد استفاده هر دشمن استوار است (فولادی، ۱۳۹۱: ۹۶). در جلســـات خبرگی، «قابلیت» این گونه تعریف شـــد: عبارت اســـت از توانایی اثرگذاری مطلوب عملیاتی برای انجام وظایف.

1.Capability Based
2.Operation Concepts

روش شناسی

تحقیق حاضر بر حسب نتایج تحقیق از نوع کاربردی توسعه‌ای می‌باشد. این تحقیق به دلیل نیاز به بررسی خبرگی، با رویکرد کیفی صورت پذیرفت. به منظور همفکری با صاحبنظران و اتقان هر چه بیشتر تحقیق، جلسات خبرگی با دعوت از ۲۰ نفر از متخصصان برگزار شد. جهت جمع‌آوری و تحلیل داده‌ها از روش‌های اسنادی و استفاده از روش موردی زمینه‌ای و توصیفی تحلیلی بهره گرفت.

جامعه آماری این تحقیق، فرماندهان، رؤسا و خبرگان مرتبط با حوزه سایبر می‌باشند که ویژگی مشترک آنها عبارت است از: مدارج علمی: کارشناسی ارشد و بالاتر؛ حداقل ۳ سال خدمت در سازمان‌های مرتبط با حوزه علم؛ حداقل ۱۰ سال سابقه خدمت؛ آشنایی با مسایل دفاعی. تعداد جامعه آماری، حدود ۵۰ نفر می‌باشد که ۲۰ نفر از خبرگان جامعه آماری به صورت قضاوتی (هدفمند) انتخاب و به جلسات خبرگی دعوت شدند.

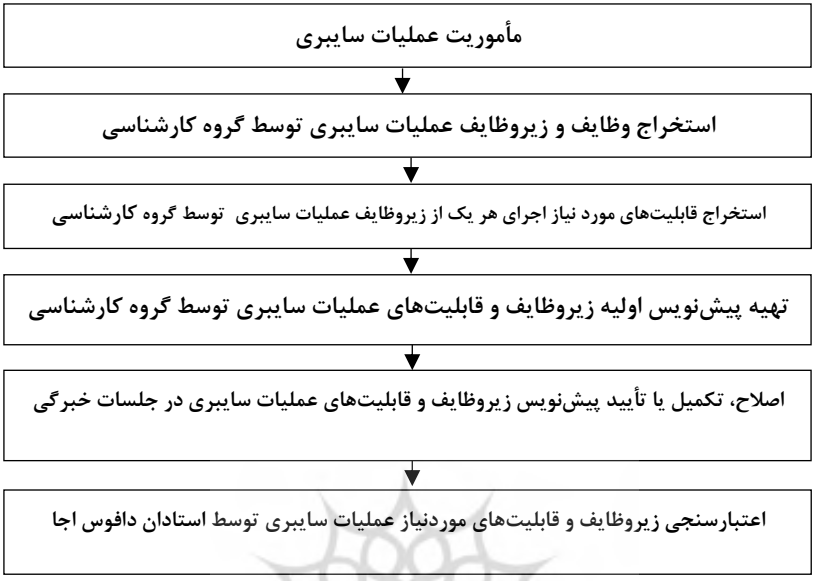
روش گردآوری اطلاعات، روش کتابخانه‌ای با ابزار فیش‌برداری و روش میدانی با جلسات خبرگی بود. برای بررسی آماری اطلاعات و تجزیه و تحلیل داده های حاصله، از روش آمار استنباطی (جلسات خبرگی) استفاده شد.

یافته‌ها

اجرای مأموریت عملیات سایبری، یکی از وظایف اجا می‌باشد که در جلسات خبرگی، فرایند استخراج قابلیت‌های مورد نیاز اجا برای انجام این وظیفه به شرح نمودار (۱) تدوین شد.

در گام اول، یک کارگروه چهار نفره با حضور صاحبنظرانی از قسمت‌های مختلف اجا که مسؤولیت اجرای عملیات سایبری را دارند تشکیل شد. از مسؤولان مذکور درخواست شد تا با همفکری با سایر صاحبنظران در معاونت یا یگان خود، پیش نویس اولیه وظایف و زیروظایف و قابلیت‌های مورد نیاز عملیات سایبری را ارایه نمایند.

نمودار ۱ : فرایند استخراج زیروظایف و قابلیت‌های مورد نیاز عملیات سایبری



در گام دوم، ابتدا وظایفی برای مأموریت عملیات سایبری نوشته شد. سپس زیروظایفی برای وظایف مذکور پیش‌بینی شد. گروه کارشناسی، در تعیین وظایف و زیروظایف، علاوه بر توان خبرگی، از شرح وظایف موجود در جداول سازمانی اجا نیز بهره‌برداری نمودند.

در گام سوم، گروه کارشناسی، قابلیت‌های مورد نیاز اجرای هر یک از زیروظایف عملیات سایبری را استخراج نمودند.

در گام چهارم، گروه کارشناسی وظایف، زیروظایف و قابلیت‌های مورد نیاز عملیات سایبری را در یک پیش‌نویس جمع‌بندی نمودند.

در گام بعدی، پیش‌نویس مذکور، به جلسه خبرگی ارایه و اصلاح و تکمیل شد.

در نهایت، زیروظایف و قابلیت‌های موردنیاز عملیات سایبری توسط استادان دافوس اجا اعتبارسنجی شد.

بر اساس تحقیق انجام شده، اجا برای انجام مأموریت عملیات سایبری، وظایف و زیروظایف مندرج در جدول (۱) را بر عهده دارد. به عبارت دیگر، اجا سه وظیفه اصلی دارد: دفاع و

امنیت سایبری، آفند و حمله پیش‌دستانه سایبری و پشتیبانی. وظیفه دفاع و امنیت سایبری،دارای زیروظایف کشف و شناسایی تهدیدات سایبری و امنیت سایبری (امنیت شبکه، امنیت نرم‌افزار، امنیت سخت‌افزار و فارنزیک دیجیتال) است. وظیفه آفند و حمله پیش‌دستانه سایبری، دارای زیروظایف فریب و تخریب سایبری است و وظیفه پشتیبانی، دارای زیروظایف تحقیق و توسعه و پشتیبانی فنی و آموزشی است.

جدول ۱ : وظایف و زیروظایف اجا برای انجام مأموریت عملیات سایبری

وظایف		زیروظایف
دفاع و امنیت سایبری	امنیت سایبری	کشف و شناسایی تهدیدات سایبری امنیت شبکه امنیت نرم‌افزار امنیت سخت‌افزار فارنزیک دیجیتال
آفند و حمله پیش‌دستانه سایبری	تخریب سایبری	تخریب سایبری
پشتیبانی	تحقیق و توسعه پشتیبانی فنی و آموزشی	

بر اساس تحقیق انجام شده، قابلیت‌های مورد نیاز اجا برای انجام زیروظایف عملیات سایبری به شرح جدول (۲) می‌باشد. به عبارت دیگر، اجا برای انجام وظیفه کشف و شناسایی تهدیدات سایبری، به قابلیت‌های کشف و شناسایی حملات سایبری و ارزیابی سطح امنیت شبکه نیاز دارد. برای انجام وظیفه امنیت شبکه، به قابلیت‌های امنیت دیتابیس، امنیت کانال انتقال و امنیت سیستم عامل شبکه نیاز است. برای انجام وظیفه امنیت نرم‌افزار، به قابلیت‌های امنیت نرم‌افزارهای کاربردی و امنیت سیستم عامل نیاز است. برای انجام وظیفه امنیت سخت‌افزار، به قابلیت‌های امنیت سخت‌افزار و امنیت تأسیسات نیاز است. برای انجام وظیفه فارنزیک دیجیتال، به قابلیت فارنزیک دیجیتال نیاز است. برای انجام وظیفه فریب سایبری، به قابلیت‌های عملیات روانی، فریب سایبری، جعل سایبری و نفوذ سایبری نیاز است. برای انجام وظیفه تخریب سایبری، به قابلیت‌های تخریب سخت‌افزار و تخریب نرم‌افزار

نیاز است. برای انجام وظیفه تحقیق و توسعه، به قابلیت‌های ارتقاء توان آفند سایبری و ارتقاء امنیت سایبری نیاز است. برای انجام وظیفه پشتیبانی فنی و آموزشی، به قابلیت‌های ارائه آموزش‌های تخصصی و پشتیبانی فنی (نرم‌افزاری، سخت‌افزاری وشبکه) نیاز است.

جدول ۲ : قابلیت‌های مورد نیاز اجا برای انجام مأموریت عملیات سایبری

زیروظایف	قابلیت‌ها
کشف و شناسایی تهدیدات سایبری	کشف و شناسایی حملات سایبری
	ارزیابی سطح امنیت شبکه
امنیت شبکه	امنیت دیتابیس
	امنیت کانال انتقال
	امنیت سیستم عامل شبکه
امنیت نرم‌افزار	امنیت نرم‌افزارهای کاربردی
	امنیت سیستم عامل
امنیت سخت‌افزار	امنیت سخت‌افزار
	امنیت تأسیسات
فارنزیک دیجیتال[۱]	فارنزیک دیجیتال
	عملیات روانی
فریب سایبری	فریب سایبری
	جعل سایبری
	نفوذ سایبری
تخریب سایبری	تخریب سخت‌افزار
	تخریب نرم‌افزار
تحقیق و توسعه	ارتقاء توان آفند سایبری
	ارتقاء امنیت سایبری
پشتیبانی فنی و آموزشی	ارائه آموزش‌های تخصصی
	پشتیبانی فنی (نرم‌افزاری، سخت‌افزاری وشبکه)

۱- فارنزیک علم گردآوری، حفظ و نگهداری، و تحلیل اطلاعات دیجیتال است. علم فارنزیک رایانه، مجموعه فنون و روش‌هایی می‌باشد که به دنبال جمع آوری شواهد و مدارکی است که مجرم و شرایط وقوع جرم را بررسی می‌کند و مدارکی را که برای دادگاه معتبر باشد، کشف می‌نماید.

بحث و نتیجه گیری

فضای مجازی بخشی از قلمرو حاکمیتی کشورها شده است و امنیت ملی آنها، شامل دفاع از فضای سایبری نیز می‌شود. اهداف نظامی هم، از آماج عملیات و تهدیدات سایبری در امان نبوده و نخواهد بود. اجرای عملیات سایبری یکی از وظایف ارتش جمهوری اسلامی ایران محسوب می‌گردد؛ چرا که از یک سو برای محافظت از زیرساخت‌های فناوری اطلاعات و ارتباطات خود باید قادر به دفاع (پدافند) سایبری باشد و از سوی دیگر، به موجب اصل یکصد و چهل و سوم قانون اساسی ارتش جمهوری اسلامی ایران پاسداری از استقلال و تمامیت ارضی و نظام جمهوری اسلامی کشور را بر عهده دارد و بر این اساس، خواه به عنوان وظیفه اصلی و خواه به عنوان وظیفه فرعی، اجا باید قابلیت اجرای عملیات سایبری و استفاده از فضای سایبر برای اهداف نظامی را داشته باشد. اجا برای اجرای عملیات سایبری نیازمند داشتن قابلیت‌هایی به شرح جدول (۲) می‌باشد.

با توجه به نتایج تحقیق پیشنهاد می‌گردد:

۱. معاونت طرح و برنامه اجا ساختار و سازمان مناسب برای عملیات سایبری در اجا را متناسب با وظایف و زیروظایف مذکور در جدول (۱) بازنگری و اصلاح نماید.

۲. معاونت طرح و برنامه اجا جدول تجهیزات متناسب با قابلیت‌های مستخرج از این تحقیق، برای عملیات سایبری تنظیم نماید.

۳. معاونت نیروی انسانی اجا، کارکنان با تخصص‌های متناسب با قابلیت‌های مورد نیاز عملیات سایبری را تأمین نماید.

منابع

احمری، حسین و کحلکی، غلامرضا و رحیم‌پور اصفهانی، حامد (۱۳۹۵)، **تحلیل سازه انگارانه تروریسم سایبری و رویکرد نظام حقوقی به آن، فصلنـــامه پژوهش‌های روابط بین‌الملل**، دوره نخست، شماره ۱۹.

الاردیک، روبرت (۱۳۸۴)، **تحول در رویکرد تصمیم‌گیری در عرصه نبرد**، مترجمان فرهاد نظری‌زاده و کمال نیک صالحی، مرکز آینده پژوهی علوم و فناوری دفاعی، تهران، چاپ اول.

ترابی، قاسم (بهار ۱۳۹۴)، **تکامل راهبرد ناتو در قبال جنگ سایبری؛ دلایل، ابعاد و مؤلفه‌ها**، فصلنامه مطالعات راهبردی، شماره ۷۶.

خلیلی پورکن آبادی، علی و نورعلی وندی، یاسر (۱۳۹۱)، **تهدیدات سایبری و تأثیر آن بر امنیت ملی**، شماره ۱۵.

رمضان‌زاده، مجتبی (پاییز ۱۳۹۴)، **تدوین راهبردهای دفاع سایبری ارتش جمهوری اسلامی ایران**، فصلنامه مدیریت نظامی، شماره ۵۹، سال پانزدهم.

سلطانی‌نژاد، احمد و جمشیدی، محمدحسین و محسنی، سجاد (تابستان ۱۳۹۵)، **تحول مفهوم امنیت در پرتو جهانی شدن و فناوری اطلاعات و ارتباطات نوین**، فصلنامه علمی پژوهشی سیاست جهانی،دورهٔ پنجم، شمارهٔ دوم.

عباسی، مجید و مرادی، حسین (بهار ۱۳۹۴)، **جنگ سایبر از منظر حقوق بین الملل بشردوستانه**، فصلنامه مجلس و راهبرد، سال بیست و دوم، شماره ۸۱.

عبدالله خانی، علی (۱۳۸۶)، **جنگ نرم ۳**، نبرد در عصر اطلاعات، مؤسسه فرهنگی مطالعات و تحقیقات بین المللی معاصر.

فولادی، قاسم (۱۳۹۱)، م**ترجم حمید دهقانی، "توانمندی‌ها و قابلیت‌های شناسایی و مراقبت آمریکا در سال ۲۰۲۰"**، فصلنامه دیده‌بان، سال اول، شماره ۱.

میرزایی، سید احمد و صالحی، علی و سعیدی، سعید (بهار ۱۳۹۵)، **بررسی تهدیدهای پیش‌نویس موافقت نامه امنیت سایبری از منظر منافع ملی جمهوری اسلامی ایران**، فصلنامهٔ امنیت پژوهی (علمی-پژوهشی)، سال پانزدهم، شماره ۵۳.

نامی، محسن (۱۳۸۳)، **نگاهی کلی به جرم‌های رایانه‌ای، تهران، مجله اصلاح و تربیت**، سال سوم، دی ماه، شماره ۳۴.

یزدان‌پناه‌درو، کیومرث و کامران، حسن (بهار ۱۳۹۴)، **تروریسم در فضای مجازی و اثرات آن بر حوزهٔ جغرافیای سیاسی**،)فصلنامه علمی ـ پژوهشی و بین المللی انجمن جغرافیای ایران، دوره جدید، ۴۴.

Atul, Jain, Cyber Crime: Cyber crime: issues and threats, Gyan Publishing House, ۲۰۰۵.

Hancock, b. (2001). Cyber tracking. cyber terrorism; computers and security. 20.

Krepinevich, Andrew(2012), Cyber Ware: A "Nuclear Option?" at: http://csbaonline.org/publications/2012/08/cyber-warfare-a-nuclear-option

Libicki, Martin C. (2009). Cyberdeterrence and cyberwar, RAND Corporation, Available: http://www.rand.org

Maurer, Tim (2011). "Cyber Norm Emergence at the United Nations - An Analysis of the UN"s Activities Regarding Cyber-security", Belfer Center for Science and International Affairs.

Ottis, Rain and Peeter Lorents (2010). "Cyberspace: Definition and Implications", Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia

Swanson, Lesley (2010). "The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict",Loyola of Los Angeles International and Comparative Law Review,Vol. 32, Available at: http:// digitalcommons.lmu.edu/ilr/vol32/is