

راهبردهای دفاع سایبری جمهوری اسلامی ایران در برابر تهدیدات جنگ روانی

علیرضا پورابراهیمی^۱

داریوش صفرنژاد^۲

حمیدرضا کاشف^۳

تاریخ دریافت: ۱۳۹۵/۱۰/۱۶

تاریخ پذیرش: ۱۳۹۵/۱۱/۰۵

چکیده

نظام جمهوری اسلامی ایران از بدو تشکیل، با توجه به آرمان های انسانی و الهی خود و اینکه سد راهی در برابر اهداف نظام سلطه و استکبار جهانی می باشد، همواره با سلیلی از تهاجم ها و حملات از سوی دشمنان مواجه بوده است. یکی از شگردهای جدید استکبار در ایراد آسیب و تهدید به پیکره نظام مقدس اسلامی و با استفاده از فناوری روز دنیا، وارد صحنه جنگ شدن با جمهوری اسلامی ایران از طریق فضای سایبر است که در محیط یادشده انجام عملیات روانی گسترده یکی از مهم ترین شگردهای دشمن است. با گسترش فضای سایبر و وابستگی روزافزون افکار عمومی مردم به این فضا و آسیب پذیری که آن ها در مقابل حملات سایبری دارند، برخورداری از راهبردهای دفاع سایبری در این حوزه ضرورت می یابد و در چنین طرحی، آشنایی با عملیات روانی دشمنان نظام از اهمیت بالایی برخوردار خواهد بود. در این پژوهش صورت پذیرفته، روش تحقیق موردی زمینه ای بوده و نوع تحقیق کاربردی/ توسعه ای می باشد. از روش ترکیبی (سه بعدی) با استفاده از روش های کمی و کیفی و ترکیب آن و روش دلفی جهت جمع آوری اطلاعات از نخبگان عملیات روانی در حوزه سایبری و روش اکتشافی در مراجعه به اسناد و مدارک، بهره برداری شده است. در نتیجه این پژوهش مشخص شده هر چند تهدیدات وارده در عرصه فضای سایبری کشور در حوزه عملیات روانی، در ظاهر اقدامی نه چندان پیچیده به نظر می رسد، اما در صحنه عمل بسیار متفاوت و پیچیده تر از سایر روش ها است که با نظر داشت الزامات لازم، این تحقیق به تدوین و ارائه راهبردهایی پرداخته تا تهدیدات، آسیب پذیری ها و هزینه های نظام در این عرصه کاهش یابد.

کلیدواژه ها: دفاع سایبری، فضای سایبر، راهبرد، عملیات روانی، تهدیدات.

^۱ - عضو هیئت علمی دانشگاه امام باقر علیه السلام.

^۲ - دانشجوی دکتری امنیت ملی دانشگاه عالی دفاع ملی.

^۳ - دانشجوی دکتری امنیت ملی دانشگاه عالی دفاع ملی.

مقدمه

یکی از شگردهای امروزی دشمنان نظام جمهوری اسلامی ایران، در وارد ساختن تهدید و آسیب، با استفاده از فناوری روز دنیا به پیکره نظام مقدس اسلامی، ورود به عرصه نبرد با کشورمان از طریق فضای سایبر است. در محیط یادشده انجام عملیات روانی گسترده یکی از مهم‌ترین شگردهای مورد استفاده و در دست اقدام توسط دشمن است. در عصر کنونی استفاده از فضای سایبر و فناوری اینترنت در جهت عملیات روانی به یکی از کاراترین ابزار رسانه‌های غرب بدل شده است، اینترنت می‌تواند با چهار عامل، تحول و انقلابی در عملیات روانی پدید آورد: ایجاد شبکه روانی اینترنت، هماهنگی، اجرا و تحلیل تأثیر و کارایی روند عملیات روانی. کاملاً واضح است که دولت یا نهادی که کنترل، مدیریت و سازماندهی اطلاعات را در دست بگیرد، همواره قدرتمندترین خواهد بود. «عملیات روانی سایبری» صرفاً شخصی نیست بلکه اقناع بخشی جدیدی دارد به نحوی که بسیار قدرتمندتر از عملیات روانی سنتی است. حملات روانی سایبری به شیوه‌ای کاملاً متفاوت از اعلامیه‌ها، اثرگذاری دارند و از همه گونه‌های ارتباط شنیداری، دیداری و نوشتاری استفاده می‌شود. عملیات روانی سایبری گونه‌ای بسیار تهاجمی از عملیات روانی است که هیچ پناهگاهی را باقی نمی‌گذارد. عملیات روانی سایبری، به عنوان تروریسم مجازی اگرچه دربرگیرنده تهدید و خشونت مستقیم نیست اما تأثیر روانی آن، بر جوامع هراسناک و مضطرب، می‌تواند به اندازه بمب‌گذاری تروریستی، قدرتمند باشد. عملیات روانی سایبری می‌تواند خصوصی، بی‌سروصدا، فریبکارانه، جهانی و مملو از تنفر و تعصب باشد. (مرادیان، ۱۳۹۱: ۱۵ و ۱۷).

بیان مسئله

با عنایت به وسعت، تنوع، گستردگی و اهمیت فضای سایبر در دنیای امروز، ضرورت دارد قدرت نفوذ و برد راهبردی و همچنین اقدامات تاکتیکی نظام جمهوری اسلامی ایران در یک جنگ اطلاعاتی و سایبری به‌صورت روزافزون افزایش یابد؛ بنابراین ضروری است تا نظام جمهوری اسلامی به کمک نخبگان بومی خود بتواند دکترین امنیتی خود را به‌طور جامع‌تر و با قبول حضور گسترده‌تر در فضای سایبر و در سطح افکار عمومی در داخل و در کل جهان پی‌ریزی نماید. هر چند این مسیر در میان برخی از نخبگان کشور به انحای مختلف پی‌ریزی شده است، اما سرعت

فزاینده تحولات ما را بر آن خواهد داشت تا با جدیت و سرعت بیشتری به این امر همت گماریم. نبود راهبردهای دفاع سایبری جمهوری اسلامی ایران در برابر تهدیدات در حوزه عملیات روانی و وسعت، گستردگی، اهمیت، تنوع، پیچیدگی، سطوح، اشکال و عرصه‌های مختلف و روز افزون فضای سایبر مورد استفاده توسط دشمنان قسم‌خورده نظام در جهان امروز، دغدغه‌ای است که ما را بر آن داشته تا به این تحقیق پردازیم. لذا در این پژوهش به دنبال ارائه راهبردهای دفاع سایبری جمهوری اسلامی ایران در برابر تهدیدات وارده از سوی دشمنان در حوزه عملیات روانی، در جهت تأمین منافع و امنیت ملی با عنایت به اصول و ارزش‌های حاکم، چشم‌انداز، مأموریت، عوامل داخلی و خارجی مؤثر بر این راهبردها، هستیم.

اهمیت و ضرورت

نبود راهبردهای مناسب دفاع سایبری در برابر تهدیدات در حوزه عملیات روانی، مبتنی بر دانش بومی و نیازمندی ملی، در سنوات پیشین سبب آسیب‌پذیری در حوزه‌های مختلف گردیده و تهاجم سایبری را به اشکال گوناگون از سوی بیگانگان به دنبال داشته است. این امر بسترهای تخریب و تهاجم فرهنگی را برای هرگونه تهاجم نرم از سوی بیگانگان فراهم ساخته و منافع و امنیت ملی را با چالش‌های اساسی مواجه خواهد نمود و هزینه‌ها را در دفاع سایبری افزایش خواهد داد. فقدان این راهبردها، نظام مقدس جمهوری اسلامی ایران را در بعد پنجم دفاع و جنگ (دفاع و تهاجم سایبری) که از سوی بیگانگان و دشمنان قسم‌خورده در حال برنامه‌ریزی، هدایت و اجرا هستند آسیب‌پذیر نموده و با مورد هجومه واقع شدن در این حوزه، با تهدیدات جدی مواجه خواهد ساخت.

این تحقیق حساسیت لازم دستگاه‌های مختلف کشوری و لشکری را نسبت به ادبیات حوزه عملیات روانی در دفاع سایبری برانگیخته و به اتخاذ تدابیر راهبردی لازم در جهت مقابله با هرگونه تهدید سایبری در این راستا هدایت خواهد نمود. نحوه دفاع سایبری در برابر تهدیدات در حوزه عملیات روانی را به طور یکنواخت و هماهنگ با منافع و امنیت ملی تبیین خواهد نمود. همچنین نتایج حاصل از این تحقیق چگونگی و شیوه‌های راهبردی مقابله با هرگونه جنگ نرم، تهدید نرم و عملیات روانی از سوی بیگانگان را در فضای سایبر ترسیم و بسترهای موجود در شبکه‌های اجتماعی را برای فعالیت‌های مجازی مفید و مبتنی بر منافع ملی و ایمن هدایت خواهد

۱۲۲ فصلنامه امنیت ملی، سال ششم، شماره بیست و دوم، زمستان ۱۳۹۵

ساخت. مضاف اینکه، نتایج حاصل از این تحقیق به عنوان راهبردهای دفاع سایبری در حوزه عملیات روانی، از قابلیت بهره‌برداری در کشورهای منطقه‌ای و فرا منطقه‌ای فارغ از فضای جغرافیایی و سیاسی هم برخوردار خواهد بود.

هدف تحقیق

ارائه راهبردهای دفاع سایبری جمهوری اسلامی ایران در برابر تهدیدات در حوزه عملیات روانی، در جهت تأمین منافع و امنیت ملی با عنایت به اصول و ارزش‌های حاکم، چشم‌انداز، مأموریت، عوامل داخلی و خارجی مؤثر بر این راهبردها، می‌باشد.

سؤال تحقیق عبارت است از: «راهبردهای دفاع سایبری جمهوری اسلامی ایران در برابر تهدیدات در حوزه عملیات روانی، در جهت تأمین منافع و امنیت ملی و همچنین اصول و ارزش‌های حاکم، چشم‌انداز، مأموریت، عوامل داخلی و خارجی مؤثر بر این راهبردها، چه می‌باشد؟»

مبانی نظری تحقیق:

پیشینه تحقیق:

پروژه‌های تحقیقاتی و مقاله‌های متعددی در حوزه سایبر انجام و بخشی از آن‌ها منتشر شده‌اند، لیکن بخشی از پروژه‌های تحقیقاتی دارای طبقه‌بندی می‌باشند. پروژه تحقیقاتی طرح تدوین طرح جامع فناوری اطلاعات کشور از آن جمله است که منجر به ارائه و تصویب سند «نظام جامع فناوری اطلاعات کشور» شده و طی آن ۷ حوزه راهبردی تدوین و به بررسی قلمروهای اساسی پرداخته است.

«الزامات جنگ مجازی و تمهیدات پدافندی برای آن» دیگر پروژه تحقیقاتی است که باهدف بررسی ارتباط بین تهدید جنگ شبیه‌سازی شده دشمن و تمهیدات پدافندی رایانه‌ای اجرا شده و چنین نتیجه‌گیری شده که تأثیر آنتی‌ویروس‌ها بر تمهیدات پدافندی در جنگ مجازی دشمن با میانگین ۴/۶ بیشترین اثر را و به میزان خیلی زیاد مؤثر است. برابر بررسی‌های انجام‌شده، پیرامون موضوع مورد تحقیق، تاکنون کار پژوهشی صورت نپذیرفته است.

مفاهیم واصطلاحات:

فضای سایبر: اصطلاح فضای سایبر از ترکیب دو واژه «سایبر» و «فضا» تشکیل شده است. سایبر از لغت یونانی (Kybernetes) سایبرنتیک به معنای سکان‌دار یا راهنما مشتق شده است. اصطلاح «فضای سایبر» را نخستین بار «ویلیام گیسون» نویسنده کانادایی داستان علمی تخیلی در کتاب «نورومنسرها»^۱ در سال ۱۹۴۸ به کار برد. (WWW.hccmr.com/news-949) برای وی، فضای سایبر، فضایی تخیلی است که از اتصال رایانه‌هایی پدید آمده که تمام انسان‌ها، ماشین‌ها و منابع اطلاعاتی در جهان را به هم متصل کرده است. این معنا به طور تقریبی مشابه معنایی است که امروزه از کاربرد لفظ فضای مجازی وجود دارد. اندرسون واقعیت مجازی را «واقعیت خلق‌شده توسط رایانه» می‌داند؛ واقعیتی که از آن‌رو مجازی یا مصنوعی است که در دنیای واقعی محیط مادی، مکانی را اشغال نکرده و در اذهان کاربران در نتیجه تعامل با واسطه الکترونیکی وجود دارد. فضایی فاقد موقعیت جغرافیایی، فیزیکی یا محدوده سرزمینی خاص، جهان واقعی با خصایصی مانند داشتن بعد جغرافیایی، نظام سیاسی خاص، محدود بودن و طبیعی بودن، از جهان مجازی و جهان مجازی نیز با خصیصه‌هایی مانند بی‌مکانی، فرازمان بودن، تکرر داشتن و قابل دسترس بودن، هم‌زمان از جهان واقعی به طور نسبی جدا می‌شود. (WWW.tebyan.net) فضای سایبر عبارتی است که در دنیای اینترنت، رسانه و ارتباطات بسیار شنیده می‌شود. در طی توسعه اینترنت واژه‌های ترکیبی بسیاری از این کلمه سایبر به وجود آمده است که به تعدادی از آن‌ها اشاره می‌کنیم: فضای سایبر^۲، شهروند سایبر^۳، پول سایبر^۴، فرهنگ سایبر^۵، راهنمایی فضای سایبر^۶، تجارت سایبر^۷، کانال سایبر^۸.

البته واژه جنگ روانی اعم بر واژه «عملیات روانی» می‌باشد، چراکه بین دو کشور اگر جنگی رخ دهد زیرمجموعه آن می‌تواند چندین (بلکه ده‌ها و صدها) عملیات انجام شود؛ اما به صورت

^۱ - Neuromancer

^۲ Cyberspace

^۳ Cybercitizen

^۴ Cybercash

^۵ Cyberculture

^۶ CyberCoach

^۷ Cyberbussines

^۸ Cyberchannel

۱۲۴ فصلنامه امنیت ملی، سال ششم، شماره بیست و دوم، زمستان ۱۳۹۵ —————*
مصطلح امروزه واژه «عملیات روانی» بیشتر مورد استفاده قرار می‌گیرد. (زورق، ۱۳۹۰) «جنگ روانی» عبارت است از کوشش سازمان‌یافته برای تحمیل اراده خود به یک کشور با استفاده از روش‌های ارتباطی و روانی، برای کاستن روحیه، قدرت اندیشه و تفکر منطقی کشور رقیب. (زورق، ۱۳۸۹: ۳۵۲)

راهبرد: راهبرد راهی برای رسیدن به آینده مطلوب است. یا به مجموعه‌ای از انتخاب‌های بنیادی و یا حیاتی در باره نتایج یک فعالیت و ابزار انجام آن فعالیت را راهبرد گویند. (حسن‌بیگی، ۱۳۹۰: ۴۳)

روش‌شناسی تحقیق:

نوع تحقیق: کاربردی / توسعه‌ای می‌باشد. این تحقیق به لحاظ بهره‌برداری در حوزه اجرایی، کاربردی و در راستای راهبردی بودن در سطح ملی و قابلیت تعمیم‌پذیری، توسعه‌ای می‌باشد.
روش تحقیق: روش تحقیق، روش تحقیق موردی زمینه‌ای می‌باشد.

در این تحقیق از روش ترکیبی (سه بعدی) با استفاده از روش‌های کمی و کیفی و ترکیب آن و از روش دلفی جهت جمع‌آوری اطلاعات از نخبگان عملیات روانی در حوزه سایبری و همچنین روش اکتشافی در مراجعه به اسناد و مدارک، بهره‌برداری شده است.

اعضای خبرگی این تحقیق اعم از اساتید و دانشجویان، اساتید و دانشجویان دانشگاه عالی دفاع ملی، کارشناسان عالی: کمیته عملیات روانی ستادکل نیروهای مسلح، سازمان پدافند غیرعامل، معاونت اجتماعی ناجا، مرکز سنجش افکار عمومی سازمان صداوسیما جمهوری اسلامی ایران و همچنین برخی متخصصین حوزه سایبری در کشور، هستند. در تحقیق حاضر حجم نمونه معادل حجم جامعه آماری یعنی ۴۰ نفر، در نظر گرفته شده است. این ۴۰ نفر را نیز بر مبنای انتخابی و دسترسی، انتخاب نموده‌ایم.

در تحقیق حاضر آن دسته از خبرگانی که آشنایی بیشتری با موضوع تحقیق دارند، به طور هدفمند انتخاب شدند و با توجه به جامعه آماری که کمتر از ۱۰۰ در حوزه است، نمونه‌ها همان جامعه آماری محسوب می‌شوند و از روش تمام شماری استفاده می‌شود.

در این پژوهش برای تعیین پایایی پرسشنامه از ضریب آلفای کرونباخ^۱ استفاده شده است که

1. Cronbach Alpha

♦ ۱۲۵ راهبردهای دفاع سایبری ج ۱۱ در برابر تهدیدات جنگ روانی

مشهورترین ضریب اعتبار از طریق یکبار اجرای آزمون می‌باشد. با توجه به واریانس هریک از متغیرها، ضریب آلفای کرونباخ با استفاده از نرم افزار SPSS محاسبه گردید، با توجه به اینکه در پژوهش‌های علوم انسانی، ضریب آلفای بالاتر از ۰/۷۰ قابل قبول است.

رابطه آلفای کرونباخ که در این تحقیق استفاده شده است عبارت

$$\alpha = \frac{n}{n-1} \left(1 - \frac{\sum S^2_i}{S^2} \right)$$

است از: میزان ضرایب آلفای کرونباخ به شرح زیر است:

متغیرهای پژوهش	ضریب آلفای کرونباخ
اصول و ارزش های حاکم	۰/۸۵
چالش های اساسی	۰/۷۶
تهدید	۰/۷۹
فرصت	۰/۷۳
ضعف	۰/۷۷
قوت	۰/۸۱
راهبردهای دفاع سایبری	۰/۸۶

ادبیات تحقیق:

ملاحظات اساسی دفاع سایبری در حوزه عملیات روانی:

به طور خلاصه می‌توان موارد زیر را به عنوان ملاحظات اساسی دفاع سایبری، مبتنی بر اسناد بالادستی و بر پایه اصول و قواعد اعتقادی، سیاسی و ملی در حوزه عملیات روانی، برشمرد:

- هدف:** اجرای عملیات دفاع سایبری در حوزه عملیات روانی دشمن، مستلزم داشتن هدف در آن است و هدف چیزی است که قصد رسیدن به آن را داریم. این هدف در سطح استراتژیک و یا تاکتیکی مورد توجه قرار می‌گیرد و تمام تلاش‌ها و اقدامات روانی به سوی آنها هدایت می‌شود.
- تمرکز در امور فرهنگی:** با توجه به اوامر فرماندهی معظم کل قوا که اشاره به هدف‌گیری دشمنان جمهوری اسلامی ایران روی باورهای سیاسی و دینی و عادات حسنه ملت با تکیه بر ابزارهای فرهنگی دارد. لذا یکی از اصول اساسی در دفاع سایبری، برنامه‌ریزی در جهت تمرکز مدیریت در بحث تقویت بنیه فرهنگی جامعه است.

۳. **وحدت فرماندهی:** به کارگیری و هدایت تمام امکانات و ابزارها و شیوه های عملیات روانی است که تحت امر فرماندهی و مرکز عالی به منظور ایجاد حداکثر تأثیرات روانی در افراد، کشورها و گروه های هدف انجام می گیرد.

۴. **هماهنگی عملیات روانی با سایر اقدامات:** برای اجرای عملیات روانی مؤثر و دفاع همه جانبه در برابر تهدیدات دشمن در فضای سایبر، تصمیم گیرندگان نظام سیاسی باید اقدامات خود را به عنوان مجموعه ای واحد در نظر بگیرند، هر چند اقدامات متفاوت به سازمان های مختلف واگذاری می شود، فرایندهای روانی آمیخته با این اقدامات، جزئی از طرح کلی در نظر گرفته شود.

۵. **انعطاف:** توانایی عکس العمل سریع و مناسب و تغییر موضع در مقابل اوضاع جدید، حوادث پیش بینی نشده و اعمال عملیات روانی در موقعیت های به دست آمده را انعطاف می نامیم. در رده های استراتژیک و تاکتیکی و در کنار پیش بینی نیازمندی های عملیات روانی، ابتکار و خلاقیت، سرعت عمل و تحرک، اطلاعات به موقع و ابزارهای مدرن و طرح های موردنیاز، داشتن عناصر و امکان تحول در سازمان از عوامل بسیار مهم است.

۶. **مقاومت مردمی در حوزه سایبر:** هدف از عملیات پدافندی یا دفاع سایبری در بحث عملیات روانی، رویارویی با تهدیدات دشمن و حفظ منافع و ارزش های کشور است، عملیات روانی در نحوه مدیریت باید قادر باشد افکار عمومی را در حمایت، تقویت و پشتیبانی همه جانبه از اهداف عملیات روانی در فضای سایبر آماده کند.

۷. **شدت عمل روانی متقابل:** اقدام سریع و به موقع و استفاده صحیح از تمام ابزارها و شیوه های اعمال عملیات روانی به منظور تخریب و تضعیف روحیه دشمن و تحمیل اراده به آن و به دست آوردن ابتکار عمل را «تهاجم روانی» و «شدت عمل روانی» می نامند. (امیرصوفی، ۱۳۸۸: ۱۹۴-۱۹۰)

رعایت این اصل ضمن تقویت روحیه تهاجمی، نتایجی قطعی در رسیدن به اهداف جنگ روانی خواهد داشت.

۸. **کسب و حفاظت اطلاعات:** اقداماتی را که موجب کسب اطلاعات از دشمن می شود، اصل جمع آوری و کسب اطلاعات و عملیات اطلاعاتی می نامند. تمام فعالیت هایی را که مانع دستیابی دشمن به وضعیت اعمال کننده عملیات روانی می شود، حفاظت اطلاعات می گویند؛ بنابراین داشتن اطلاعات کافی و صحیح از دشمن و حتی گروه های بی طرف امکان اتخاذ تدابیر مناسب برای

اعمال مدیریت عملیات روانی را فراهم می‌سازد و بالعکس فقدان اطلاعات لازم از وضع کشور اعمال کننده عملیات روانی، توان مقابله با آن را کاهش می‌دهد. (مجموعه مقالات همایش عملیات روانی: ۱۳۸۸)

۹. آموزش: شامل پرورش و آموزش افراد به منظور اجرای وظایفی که سازمان برای آنان تعیین کرده است و هماهنگ کردن مهارت های فردی به منظور ایجاد مهارت همگانی در اعمال عملیات روانی است. با آموزش و تمرینات مداوم می‌توان نیروهای کارآمد را تربیت کرد و توانایی تکنیکی و تاکتیکی افراد و سازمان اعمال کننده جنگ و عملیات روانی را کاهش داد که این خود امکان موفقیت را افزایش می‌دهد. به‌ویژه تربیت روان شناسان برای این اقدام ضرورت اساسی دارد. آگاهی از عوامل مؤثر در عملیات روانی و شناخت مبانی آن، اصول، شیوه ها و ... برای افراد و متخصصان این فن الزامی است.

۱۰. پیشگیری از شایعه پراکنی و کنترل شایعات: دشمن در فضای سایبر با روش های گوناگون از جمله پخش شایعات قصد وصول به اهداف شوم خود را دارد لذا در این راستا اتخاذ تدابیر پیشگیرانه ضروری است که عبارتند از: افزایش سطح آگاهی مردم، برطرف کردن نقاط ضعف، تبلیغات صحیح، بهره گیری مناسب از اجتماعات سیاسی مانند نماز جمعه و ... و ایجاد حس اعتماد بیشتر مردم به حکومت و از طرفی برای رویارویی با شایعه‌سازی دشمن، مقایسه شایعه با تبلیغات دشمن به صورت علنی است. با این روش می‌توان دروغ و ناصحیح بودن شایعات را به مردم نشان داد و شایعات را بی اعتبار کرد و شایعه‌سازان را مورد تمسخر قرار داد.

۱۱. توکل و تأمین آرامش دل: مهم ترین عاملی که سبب ناآرامی دل است، هراس از تهدیدات و تهاجم دشمن است برای رهایی از آن در هر زمینه ای از جمله تهدیدات عملیات روانی دشمن در فضای سایبر، توسل و توکل به خداوند قادر متعال به عنوان مظهر اقتدار واقعی، در کنار انجام اقدامات مدیریتی یک چاشنی به تمام معنا است و لذا مجالی برای ترس کاذب از دشمن باقی نمی‌ماند. (امیرصوفی، ۱۳۸۵: ۸۴)

۱۲. طراحی محتوای فرهنگی و عملیات روانی و اجرایی کردن آن.

هدف از عملیات روانی به مثابه قدرت در فضای سایبر:

هدف از عملیات روانی به مثابه قدرت در فضای سایبر، ترغیب و اقناع افراد، نهادها و واحدهای سیاسی به همراهی نمودن با اهداف و نیات مهاجم در بلند مدت است که این امر نوعی منازعه پنهان بر سر تولید و تکثیر قدرت را رقم می‌زند. (نای، ۱۳۸۹:۷۵). مؤلفه‌های اصلی عملیات روانی در این وضعیت جدید عبارت است از: اول. تأثیرگذاری (توانایی متقاعدسازی مخاطب، به طوری که او را به عنصری فعال در فرایند تولید قدرت تبدیل کند)، دوم. همگرایی (انجام عملیات روانی در فضای سایبر در تمام ابعاد و سطوح) و سوم. هم‌زمانی (انجام تمام اقدامات با تقدم و تاخر منطقی) که این روش در راهبردهای عملیات روانی آمریکا در فضای سایبر مشاهده می‌شود. (حسینی، ۱۳۹۰:۲۶).

اهداف راهبردی دشمن از عملیات روانی در فضای سایبر:

اهداف راهبردی دشمن از عملیات روانی در فضای سایبر که نشانه بارز آن ویکی لیکس است موارد زیر را شامل می‌شود:

- ۱- تشریح خط مشی‌ها، آماج و اهداف سیاسی جدید در سطح بین‌الملل.
- ۲- برقراری پیوند میان اهداف سیاسی و افکار و تمایلات مخاطبان در بلندمدت.
- ۳- برانگیختن افکار و اراده عمومی بین‌المللی پیرامون سوژه‌های انحرافی و منحرف ساختن توجهات.
- ۴- دامن زدن به بحث و جدل‌های بین‌نخبگان نظامی و سیاسی سایر کشورها.
- ۵- تشدید اختلاف نظرهای سیاسی موجود یا مسکوت در کشورهای هدف در زمینه‌های اقتصادی، امنیتی و اجتماعی؛ و غیره.
- ۶- تقویت عناصر سیاسی طرفدار و تضعیف رهبران و نظام‌های سیاسی مخالف. از جنبه سیاسی، غرب با احاطه نسبی نرم‌افزاری و سخت‌افزاری و رسانه‌ای بر جهان سایبری، تلاش دارد از این طریق، مقاصد سیاسی خود را پیاده نماید. در این رابطه ضمن القاء مفاهیم و پیام‌های مورد نظر، سعی دارد ضمن اعمال فشار بر کشور در محیط بین‌المللی، با روش‌های مختلف، گروه‌های مخالف و شبکه‌های معارض را ایجاد، هماهنگ، حمایت و تحرکات آن‌ها را مدیریت نماید (استحاله فرهنگی). از لحاظ فرهنگی نوعی جریان فرهنگی را ترویج می‌دهد که اگر به صورت مهندسی شده، مسایل آن راهبری نشود، منجر به نوعی بی‌هویتی فرهنگی در جامعه می‌شود. مطالعه

در محیط مجازی نشانه‌هایی را به دست می‌دهد که آدرس آن در نهادهای فرهنگی و ارزشی غرب است. ایجاد تعارض در افکار و عقاید، ایجاد تزلزل در باورها و اندیشه‌ها و آرمان‌ها از دیگر اهداف مهمی است که غرب در فضای مجازی علیه ایران دنبال می‌کند. (پوراابراهیمی، ۱۳۸۹: ۱۰۶ و ۱۱۰)

در شرایط کنونی مدیریت جهان مجازی تلاش دارد فرهنگ غرب را در همه جوامع به صورت مهندسی شده تکثیر و به کل جهان تعمیم دهد. (جهانی‌سازی فرهنگ غرب). (عامری، ۱۳۹۲: ۱۰).
مقام معظم رهبری (مدظله العالی) در بسیاری موارد به این گونه اهداف شوم دشمن تاکید نموده اند، به طور مثال فرمودند: «... (دشمن) با استفاده از رسانه سلیقه سازی می‌کند، فرهنگ سازی می‌کند، بعد از آنکه سلیقه‌ها را عوض کرد ذائقه‌ها را عوض می‌کند. این شیوه حرکت غربی‌ها است باید مراقب بود باید همه احساس کنند که مسئولیت تمدن اسلامی نوین به دوش آنها است و یکی از حدود و ثغور این کار مواجهه با تمدن غربی است.» (امام خامنه‌ای، ۹۱/۷/۲۳).

از لحاظ هنری غرب به دنبال گفتمان سازی و پیگیری اهداف فکری و فرهنگی خود در پوشش آثار هنری با کمترین حساسیت است. محیط سایبری به آن‌ها امکان می‌دهد ضمن تبلیغ کالاهای فرهنگی خود و کسب سودهای کلان، با بهره‌گیری از محیط سایبری، آن‌ها را ارزان و آسان در اختیار همه جوامع بخصوص جوامع اسلامی قرار دهند. از لحاظ اجتماعی و فرهنگی امروزه غرب با تبلیغات، جذابیت سازی، آسان سازی آموزش و پژوهش، دانشجویان سراسر جهان را ترغیب به حضور در غرب می‌کند. امکانات آموزشی از راه دور و همچنین خدمات دانشگاه‌های مجازی، حضور آن‌ها را در فضای آموزشی غرب بیش از پیش آسان ساخته، از این طریق بستری تأثیرگذار برای شناسایی و جذب نخبگان علمی و انتقال سبک تربیت غربی به آن‌ها را فراهم کرده اند. (عامری، ۱۳۹۲: ۱۰)

غرب براساس تجارب تحولات اروپای شرقی و دیگر تحولات اجتماعی جهان دریافته که در محیط سایبری توان ساخت شبکه‌های اجتماعی و مدیریت بر آن رادار است از این رو با سرمایه‌گذاری در این خصوص، تلاش دارد تا ضمن ترویج رفتارهای اجتماعی مهندسی‌شده و ایجاد تغییرات، بر تحولات ناخواسته نیز تأثیر بگذارد.

شبکه‌های اجتماعی مجازی با پاسخ‌گویی به نیازهای جوانان و الگوسازی جوامع مجازی، بر بخش رؤیاپروری جوانان تسلط یافته به دنبال تغییرات بنیادین در آینده هستند. ترویج روحیه ناامیدی به

- ۱۳۰ فصلنامه امنیت ملی، سال ششم، شماره بیست و دوم، زمستان ۱۳۹۵
- آینده و ایجاد بی‌اعتمادی به نظام حاکم، تقویت نارضایتی در کشور و همچنین ترویج بی‌تفاوتی نسبت به مسائل اساسی کشور از دیگر اهداف غرب است که با عملیات روانی در فضای سایبر آن را دنبال می‌کند. (عامری، ۱۳۹۲: ۲۹).
- اهم راهبردهای دشمن از عملیات روانی با استفاده از فضای سایبر شامل موارد زیر است:
- ۱- ایجاد موانع در تسلط ایران بر محیط سایبری و حفظ و گسترش مدیریت خود بر این محیط.
 - ۲- طراحی و پردازش موضوع برای تعارض سازی، اعتبار زدایی، بحران‌آفرینی و مسئله‌سازی سیاسی (القاء و ایجاد انزوای سیاسی در ایران).
 - ۳- تخریب و تحقیر باورها و ارزش‌های اخلاقی، ترویج مکاتب انحرافی و سبک زندگی غربی.
 - ۴- آسان‌سازی دسترسی به محصولات هنری غرب و ترویج آن.
 - ۵- حمایت از تولید و ترویج محصولات فرهنگی جبهه معارض و منتقد و الگوسازی از آن‌ها در عرصه فرهنگ و هنر کشور.
 - ۶- جلوگیری از دسترسی آزاد به اطلاعات علمی و پژوهشی.
 - ۷- ایجاد جذابیت و آسان‌سازی مهاجرت نخبگان علمی.
 - ۸- سرقت ایده‌ها و یافته‌های جدید علمی.
 - ۹- جذابیت سازی، برای ترویج سبک زندگی غربی و تربیت براساس مولفه‌های آن در محیط سایبر به خصوص محصول سازی علمی، آموزشی و فرهنگی.
 - ۱۰- ناکارآمد سازی تربیتی، آموزشی، فرهنگی و دینی کشور و جلوگیری از شکل‌گیری یک سبک و الگوی مستقل ایرانی / اسلامی در محیط سایبر.
 - ۱۱- شبکه سازی اجتماعی در محیط سایبری برای ایجاد تغییرات رفتاری و ساماندهی و کنترل تحرکات اجتماعی. (عامری، ۱۳۹۲: ۱۸)

تجزیه و تحلیل داده‌ها:

در اینجا ابتدا داده‌های جمع‌آوری شده به وسیله پرسشنامه، مورد تجزیه و تحلیل قرار می‌گیرد. به طوری که ابتدا فراوانی‌های مربوط به سؤالات عمومی پرسشنامه (شامل: سمت، تحصیلات و سنوات خدمتی) مورد تجزیه و تحلیل و بررسی قرار گرفته و سپس با در نظر گرفتن درصد نظرات پاسخ‌دهندگان به هریک از گویه‌های پرسشنامه، به شناسایی بیشترین و کمترین عامل تأثیرگذار در هریک از متغیرهای پژوهش خواهیم پرداخت.

راهنماهای دفاع سایبری ج ۱۱ در برابر تهدیدات جنگ روانی ♦ ۱۳۱

تحلیل ویژگی‌های جمعیت شناختی:

جدول ۱-۱-۵. جدول فراوانی شرکت کنندگان در نظرسنجی به تفکیک سمت

سمت	فراوانی نسبی	فراوانی تجمعی	درصد فراوانی نسبی	درصد فراوانی تجمعی
عضو هیئت علمی دانشگاه	۱۰	۱۰	۱۷.۵	۱۷.۵
مدیر عالی اجرایی	۱۲	۲۲	۳۵	۵۲.۵
مدیر میانی اجرایی	۹	۳۱	۲۷.۵	۸۰
کارشناس	۹	۴۰	۲۰	۱۰۰
جمع	۴۰		۱۰۰	

جدول ۱-۲-۵. جدول فراوانی شرکت کنندگان در نظرسنجی به تفکیک تحصیلات

تحصیلات	فراوانی نسبی	فراوانی تجمعی	درصد فراوانی نسبی	درصد فراوانی تجمعی
دکتری	۸	۸	۲۰	۲۰
دانشجوی دکتری	۲۰	۲۸	۵۰	۷۰
فوق لیسانس	۱۲	۴۰	۳۰	۱۰۰
جمع کل	۴۰		۱۰۰	

جدول ۱-۳-۵. جدول فراوانی شرکت کنندگان در نظرسنجی به تفکیک سنوات خدمتی

سنوات خدمتی	فراوانی نسبی	فراوانی تجمعی	درصد فراوانی نسبی	درصد فراوانی تجمعی
۱۸ تا ۲۱ سال	۱۰	۱۰	۲۵	۲۵
۲۲ تا ۲۵ سال	۱۵	۲۵	۳۷	۶۲
۲۳ تا ۲۶	۱۰	۳۵	۲۵	۸۷
بالای ۲۷ سال	۵	۴۰	۱۳	۱۰۰
جمع کل	۴۰		۱۰۰	

آمار استنباطی:

در این پژوهش ابتدا درصد پاسخ‌های مربوط به هر یک از طیف ۹ درجه‌ای پرسشنامه از طریق نرم افزار SPSS محاسبه شده و سپس میانگین مربوط به هر کدام از سوالات پژوهش محاسبه شده و در نهایت میانگین کل سوالات مربوط به آن سوال محاسبه شده است تا درصد پاسخ‌های مربوط به آن حوزه مشخص شود و در مرحله بعد، اهمیت آن حوزه را محاسبه شده است. هریک از این حوزه‌ها به تفکیک در زیر بررسی شده‌اند.

ردیف	اصول و ارزش‌های حاکم بر طرح راهبردی پدافند سایبری عملیات روانی	درجه اهمیت هر سوال از صد درصد																		
		۱	۲	۳	۴	۵	۶	۷	۸	۹	میانگین									
۱	تمرکز در طرح ریزی و اجرای غیر متمرکز	*	*	*	*	*	*	*	*	*	۹۰.۲	۱۲.۵	۸۷.۵	*	*	*	*	*	*	*
۲	اصل باورپذیری	*	*	*	*	*	*	*	*	*	۸۹.۴	۵	۹۵	*	*	*	*	*	*	*
۳	اصل اعتماد متقابل به رسانه	*	*	*	*	*	*	*	*	*	۸۴.۶	۳۱.۸	۳۶.۴	۱۵.۹	۴.۵	۲.۳	*	*	*	*
۴	اصل تعامل با مخاطب	۲.۳		۲.۳	۲.۳	۶.۸	۹.۱	۲۲.۷	۳۴.۱	۲۰.۵	۸۰.۶									
۵	اصل اقناع و اجماع مخاطب	*	*	*	*	*	*	*	*	*	۹۰	۱۰	۹۰	*	*	*	*	*	*	*
۶	اصل تولید و تاثیرگذاری پیام	*	*	*	*	*	*	*	*	*	۸۷.۷	۲۰	۸۰	*	*	*	*	*	*	*
۷	اصل تناسب پیام با مخاطب	*	*	*	*	*	۶.۸	۱۱.۴	۱۱.۴	۶۸.۲	۹۲.۹									
۸	اصل حرکت دسته جمعی و همسو	*	*	*	*	۶.۸	۶.۸	۱۱.۴	۲۲.۷	۵۰	۸۸.۴									
۹	اصل پایداری رسانه	*	*	*	*	۶.۸	۲.۳	۱۱.۴	۱۱.۴	۶۸.۲	۹۲.۹									
۱۰	اصل ارتقای بصیرت ملی	*	*	۴.۵	۶.۸	۲.۳	۱۱.۴	۱۱.۴	۱۳.۶	۵۰	۸۴.۳									
۱۱	اصل احترام به افکار عمومی	۲.۳	*	۲.۳	۴.۵	۲.۳	۶.۸	۱۳.۶	۲۵	۴۳.۲	۸۵.۱									
۱۲	اصل صداقت در پیام	*	*	*	*	*	*	*	*	*	۹۰.۵	۱۵	۸۵	*	*	*	*	*	*	*
۱۳	اصل توجه به چارچوب‌های اخلاقی	*	*	*	*	*	*	*	*	*	۸۸.۶	۸۷.۵	۱۲.۵	*	*	*	*	*	*	*
	میانگین کل										۸۸.۱									

اصول و ارزش‌های اساسی در حوزه عملیات روانی:

جدول اهمیت اصول و ارزش‌های حاکم بر طرح راهبردی دفاع سایبری در حوزه عملیات روانی. در این بخش از سؤالات ابعاد پروژه تحقیقاتی، از مجموع میانگین (۸۸/۱٪)، حداقل تعداد پاسخگویان (۸۰/۶٪)، شاخص اصل تعامل با مخاطب را به عنوان اصول و ارزش‌های حاکم بر طرح راهبردی پدافند سایبری عملیات روانی کشور دانسته و در نقطه مقابل، بیشترین مخاطبان

راهِبردهای دفاع سایبری ج ۱۱ در برابر تهدیدات جنگ روانی ♦ ۱۳۳

(۹۲/۹٪)، خواهان اصل تناسب پیام با مخاطب و اصل پایداری رسانه بوده و این شاخص را نسبت به سایر شاخص‌ها بالاتر داشته و به‌عنوان اصول و ارزش‌های اساسی در حوزه مورد نظر معرفی نموده‌اند.

چالش‌های اساسی در حوزه عملیات روانی:

جدول اهمیت چالش‌های اساسی حاکم بر طرح راهبردی دفاع سایبری در حوزه عملیات روانی

ردیف	گویه‌های چالش‌های اساسی در حوزه عملیات روانی	درجه اهمیت هر سوال از صد درصد									
		۱	۲	۳	۴	۵	۶	۷	۸	۹	میانگین
۱	امکان شبکه‌سازی و برقراری ارتباطات در شبکه‌های اجتماعی سایبری	*	*	*	۶۸	۶۸	۱۸.۲	۲۰.۵	۲۰.۵	۲۷.۳	۸۰.۵
۲	امکان مجهول و مخفی ماندن مهاجم و امکان استفاده از هویت‌های مجازی و غیر واقعی در فضای سایبر	*	*	۴.۵	۱۸.۲	۲۰.۵	۲۰.۵	۲۷.۳	۲.۳	۶.۸	۹۱.۱
۳	ضعف در درک صحیح مدیران در خصوص تهدیدات عملیات روانی در فضای سایبری	*	*	۴.۵	۱۸.۲	۲۰.۵	۲۰.۵	۲۹.۵	*	۶.۸	۸۸.۶
۴	کمبود منابع انسانی متخصص در جهت مقابله با عملیات روانی دشمن در زیست بوم سایبری	*	*	*	۱۸.۲	۲۰.۵	۲۰.۵	۲۹.۵	*	۳۴.۱	۹۵.۸
۵	داشتن راهبرد دشمن و نبود راهبرد جامع در کشور برای مقابله با جنگ نرم دشمن در زیست بوم سایبری	*	*	*	۱۸.۲	*	۲۰.۵	۲۷.۳	*	۳۶.۴	۹۶.۷
۶	ضعف در مسیر ارتقای توان مقاومت ملی در برابر حمله‌های فرهنگی و عملیات روانی دشمن	۲.۳	*	۴.۵	۹.۱	۶.۸	۱۱.۴	۱۳.۶	۱۵.۹	۳۶.۴	۷۸.۵
۷	آمیختگی عملیات روانی و عملیات واقعی در فضای سایبری و امکان شناخت اشتباه آن	*	*	۲.۳	۶.۸	۴.۵	۴.۵	۲۹.۵	۱۸.۲	۳۴.۱	۸۲.۶
۸	داشتن قدرت هم‌افزا کننده مؤلفه‌های قدرت دشمن در انجام عملیات روانی در فضای سایبر	*	*	۲.۳	۶.۸	۴.۵	۱۸.۲	۲۰.۵	۲۰.۵	۲۷.۳	۷۹.۸
میانگین کل											
۸۶.۱											

۱۳۴ فصلنامه امنیت ملی، سال ششم، شماره بیست و دوم، زمستان ۱۳۹۵ ←

در ارتباط با این بُعد از پروژه تحقیقاتی، از مجموع میانگین (۸۶/۱٪)، حداقل تعداد نخبگان (۷۸/۵٪)، شاخص ضعف در مسیر ارتقای توان مقاومت ملی در برابر هجمه‌های فرهنگی و عملیات روانی دشمن را به‌عنوان چالش‌های اساسی در حوزه در حوزه عملیات روانی تشخیص داده و در نقطه مقابل، بیشترین نخبگان (۹۶/۷٪)، در تشخیص خود، داشتن راهبرد دشمن و نبود راهبرد جامع در کشور برای مقابله با جنگ نرم دشمن در زیست بوم سایبری را مهم‌ترین چالش‌های اساسی در حوزه مزبور اعلام کرده‌اند.

تهدیدات اساسی در حوزه عملیات روانی:

جدول اهمیت تهدیدات اساسی حاکم بر طرح راهبردی دفاع سایبری در حوزه عملیات روانی

ردیف	گویه‌های تهدید	درجه اهمیت هر سوال از صد درصد										
		۱	۲	۳	۴	۵	۶	۷	۸	۹	میانگین	
۱	وجود شبکه‌های رسانه‌ای ماهواره‌ای وابسته به دشمن	*	*	*	*	*	*	*	*	*	۷۵	۹۵.۸
۲	وجود عناصر وابسته به غرب	*	*	*	*	*	*	*	*	*	۶۲.۵	۹۴.۴
۳	تسلط دشمن برای اینترنت و شبکه‌های اجتماعی و انجام عملیات روانی	*	*	*	*	*	*	*	*	*	۷۵	۸۲.۸
۴	فضاسازی در مجامع جهانی علیه جمهوری اسلامی ایران و متهم سازی در حوزه حقوق بشر	*	*	*	*	*	*	*	*	*	۸۰	۹۱.۱
۵	هجمه گسترده دشمن به نظام اعتقادی جامعه اعم از مردم و دولت در راستای مقابله با گسترش مکتب اسلام ناب محمدی	*	*	*	*	*	*	*	*	*	۱۰	۸۸.۹
۶	القای تردید و ایجاد بی‌اعتمادی نسبت به نظام سیاسی کشور	۴.۵	۴.۵	۶.۸	۶.۸	۱۳.۶	۱۵.۹	۶.۸	۱۳.۶	۳۴.۱	۹۷.۸	
۷	امکان سنجش محیط اجتماعی فرهنگی ما از طریق شبکه‌های اجتماعی	۴.۵	۶.۸	۴.۵	۶.۸	۲.۳	۶.۸	۱۸.۲	۲۵	۲۵	۹۵.۸	
۸	شبکه‌سازی (برای جاسوسی و...) و سازماندهی عناصر مسئله در قالب گروه‌های براندازی	۴.۵	۴.۵	۴.۵	۴.۵	۱۱.۴	۶.۸	۱۳.۶	۲۷.۳	۲۲.۷	۹۵.۶	
۹	امکان راه‌اندازی جنبش‌های براندازی اجتماعی توسط دشمن	۴.۵	۶.۸	۲.۳	۱۱.۴	۹.۱	۱۵.۹	۲۵	۲۵	۲۵	۹۷.۲	
۱۰	شکستن قبح ارتباط با خارجی و جاسوسی در قالب عضویت در شبکه‌های اجتماعی	۲.۳	*	*	۲.۳	۴.۵	۱۱.۴	۱۸.۲	۲۲.۷	۳۸.۶	۹۴.۴	
		میانگین کل									۸۵.۷	

➔ راهبردهای دفاع سایبری ج ۱۱ در برابر تهدیدات جنگ روانی ♦ ۱۳۵

در ارتباط با این بُعد از پروژه تحقیقاتی، از مجموع میانگین (۸۵/۷٪)، حداقل تعداد نخبگان (۸۲/۸٪)، شاخص تسلط دشمن برای اینترنت و شبکه های اجتماعی و انجام عملیات روانی را مهم ترین تهدید در حوزه عملیات روانی دفاع سایبر تشخیص داده و در نقطه مقابل، بیشترین نخبگان (۹۷/۸٪)، در تشخیص خود القای تردید و ایجاد بی اعتمادی نسبت به نظام سیاسی کشور در حوزه عملیات روانی را مهم ترین تهدید در حوزه مزبور اعلام کرده اند.

فرصت ها در حوزه عملیات روانی:

جدول اهمیت فرصت های حاکم بر طرح راهبردی دفاع سایبری در حوزه عملیات روانی

ردیف	گویه های فرصت	درجه اهمیت هر سوال از صد درصد									
		۱	۲	۳	۴	۵	۶	۷	۸	۹	میانگین
۱	امکان استفاده از ظرفیت اینترنت به منظور مقابله با عملیات روانی دشمن	*	*	۲.۳	۴.۶	۱۳.۶	۴.۶	۲۰.۵	۲۲.۷	۳۱.۸	۸۰.۳
۲	امکان استفاده از ظرفیت های موجود در محیط خارجی در مقابل حملات عملیات روانی دشمن	*	۴.۵	۹.۱	۴.۵	۹.۱	۶.۸	۱۵.۹	۲۰.۵	۲۹.۵	۷۴
۳	به کارگیری تجارب سایر کشورها در خصوص مقابله با تهدیدات عملیات روانی	*	۹.۱	*	*	۱۸.۲	۲.۳	۱۵.۹	۲۵	۲۹.۵	۷۸.۸
۴	امکان آفند عملیات روانی دشمن	*	*	*	*	*	*	۸۰	۷.۵	۱۲.۵	۸۱.۳
۵	ظرفیت های رسانه ای در جهت پدافند عملیات روانی دشمن	*	*	*	*	۲.۵	۷.۵	۵	۱۲.۵	۵	۷۱.۳
۶	امکان استفاده از نمایندگان، فضلاء و اندیشمندان و علما جهت خنثی نمودن فعالیت های عملیات روانی دشمن	*	*	*	*	*	۷۷.۵	۲.۵	۷.۵	۱۲.۵	۷۲.۷
۷	هشدارهای رهبری در رابطه با فعالیت های عملیات روانی دشمن	*	*	*	*	*	*	۵	۸۵	۱۰	۸۹.۴
۸	وجود استراتژی های بخشی برای مقابله با تهدیدات عملیات روانی دشمن	*	*	*	*	*	*	*	۱۲.۵	۷.۵	۹۵.۸
۹	پدافند عملیات روانی دشمن در زیست بوم	*	*	*	*	*	*	*	۱۲.۵	۲۵	۹۴.۴
		میانگین کل									۸۲

۱۳۶ فصلنامه امنیت ملی، سال ششم، شماره بیست و دوم، زمستان ۱۳۹۵ ←
 در خصوص این بُعد از پروژه تحقیقاتی، از مجموع میانگین (۸۲٪)، کمترین تعداد پاسخگویان (۷۱/۳٪)، شاخص ظرفیت‌های رسانه‌ای در جهت پدافند عملیات روانی دشمن را به‌عنوان فرصت در حوزه عملیات روانی دفاع سایبرکشور اعلام کرده‌اند و از سوی دیگر، بیشترین تعداد پاسخگویان (۹۴/۴٪)، در اعلام نظر خود شاخص پدافند عملیات روانی دشمن در زیست بوم را به‌عنوان یک فرصت در حوزه عملیات روانی دفاع سایبرکشور ارزیابی کرده‌اند.

ضعف‌ها در حوزه عملیات روانی:

جدول اهمیت ضعف‌های حاکم بر طرح راهبردی دفاع سایبری در حوزه عملیات روانی

ردیف	گویه‌های ضعف	درجه اهمیت هر سوال از صد درصد									
		۱	۲	۳	۴	۵	۶	۷	۸	۹	میانگین
۱	فقدان شناخت کامل از نقش فن‌آوری‌های نوین	۴.۵	۴.۵	۴.۵	۱۱.۴		۱۳.۶	۱۳.۶	۲۵	۲۲.۷	۷۳.۲
۲	وجود شکاف‌های سایبری عمیق در ساختار جمعیتی کشور	۴.۵	*	۹	۱۱.۴	۴.۵	۱۳.۶	۱۳.۶	۲۰.۵	۲۲.۷	۷۳.۲
۳	ضعف در هدایت انگیزه‌ها و خواسته‌های نسل جوان کشور در راستای افزایش توان مقاومت آن‌ها در برابر هجمه‌های فرهنگی	۴.۵	۴.۵	۴.۵	۱۱.۴	*	۲۰.۵	۱۳.۶	۲۰.۵	۲۲.۷	۷۱.۲
۴	کمبود اطلاعات و آگاهی‌های مدیران فرهنگی کشور در سطوح مختلف	*	*	*	*	*	*	۷۵	۱۲.۵	۱۰	۷۹.۴
۵	ضعف در راستای مقابله با رواج موهومات و خرافه‌ها در حوزه اعتقادات دینی	*	*	*	*	*	*	*	۱۰	۹۰	۸۸.۹
۶	ضعف در روشنگری نسبت به القاء شبهات دینی و فکری از سوی دشمن	*	*	*	*	*	*	*	۷.۵	۷۷.۵	۸۹.۷
۷	فقدان ساختار مدیریتی قوی در برخورد با فرهنگ‌های وارداتی	۴.۵	*	*	۹.۱	۹.۱	۶.۸	۲۷.۳	۲۰.۵	۲۲.۷	۷۶.۸
۸	تاثیر پذیری بخشی از جامعه از ترویج سبک زندگی غربی	*	*	۴.۵	۴.۵	۱۱.۴	۱۵.۹	۱۱.۴	۲۵	۲۷.۳	۷۸.۸

راهِبردهای دفاع سایبری ج ۱۱ در برابر تهدیدات جنگ روانی ♦ ۱۳۷

۷۲.۵	۲۲.۷	۲۰.۵	۱۳.۶	۱۵.۹	۴.۵	۱۱.۴	۴.۵	*	*	کمبود منابع انسانی متخصص و متعهد در جهت مقابله با عملیات روانی دشمن	۹
۸۲.۶	۳۶.۴	۱۳.۶	۲۵	۱۳.۶	۶.۸	۲.۳	۲.۳	*	*	کمبود برنامه های فرهنگی هدفمند در زیست بوم سایبری کشور به منظور جذب مخاطبین	۱۰
۸۰.۶	۲۲.۷	۳۴.۱	۱۵.۹	۱۱.۴	۹.۱	۲.۳	۴.۵	*	*	خوش باوری در طیفی از جامعه نسبت به القاء رسانه ها و شبکه های اجتماعی	۱۱
۹۵.۸	۷۵	۱۲.۵	۱۲.۵	*	*	*	*	*	*	عدم توجه طیفی از مسئولین فرهنگی کشور نسبت به مخاطرات عضویت در شبکه های اجتماعی موجود	۱۲
۸۷.۴	۴۷.۷	۲۰.۵	۱۳.۶	۹.۱	۶.۸	۲.۳	*	*	*	فقدان عزم جدی و روحیه جهادی در طیفی از مدیران تصمیم ساز کشور برای مقابله با جنگ نرم دشمن	۱۳
۸۴.۸	۳۱.۸	۲۷.۳	۲۵	۴.۵	۱۱.۴	*	*	*	*	ضعف در غنی سازی محتوایی شبکه های فرهنگی موجود	۱۴
۷۹.۸	۲۷.۳	۲۲.۷	۲۷.۳	۴.۵	۶.۸	۶.۸	۲.۳	*	۲.۳	نارسایی محتوای برنامه های آموزشی مرتبط با فرهنگ در سطوح مختلف تحصیلات در مدرسه	۱۵
۸۵	میانگین کل										

در این بخش از سؤالات ابعاد پروژه تحقیقاتی، از مجموع میانگین (۸۵/۱)، حداقل تعداد نخبگان (۷۱/۲)، در تشخیص خود شاخص ضعف در هدایت انگیزه ها و خواسته های نسل جوان کشور در راستای افزایش توان مقاومت آن ها در برابر هجمه های فرهنگی را به عنوان ضعف در حوزه عملیات روانی اعلام کرده اند لیکن در نقطه مقابل، بیشترین نخبگان (۹۵/۸)، در ارزیابی خویش عدم توجه طیفی از مسئولین فرهنگی کشور نسبت به مخاطرات عضویت در شبکه های اجتماعی موجود را به عنوان ضعف در حوزه عملیات روانی دفاع سایبری کشور دانسته اند.

قوت‌ها در حوزه عملیات روانی:

جدول اهمیت قوت‌های حاکم بر طرح راهبردی دفاع سایبری در حوزه عملیات روانی

ردیف	گویه های قوت	درجه اهمیت هر سوال از صد درصد									
		۱	۲	۳	۴	۵	۶	۷	۸	۹	میانگین
۱	وجود متخصصین انقلابی در زمینه مقابله با اقدامات عملیات روانی دشمن	۱۰	۱۲.۵	۷۷.۵	*	*	*	*	*	*	۸۱.۳
۲	اعتقاد اندیشی ریشه‌دار با تکیه بر تعالیم اسلامی	۱۷.۵	۲.۵	۸۰	*	*	*	*	*	*	۸۱.۹
۳	وجود برخی آگاهی‌های نسبی مردم از روش‌های عملیات روانی دشمن	۱۷.۵	۵	۷۷.۵	*	*	*	*	*	*	۸۲.۲
۴	وجود مقام ولایت به عنوان پرچم‌دار مبارزه با تهدیدات عملیات روانی دشمن	۴۳.۲	۲۰.۵	۱۳.۶	۹.۱	۶.۸	۴.۵	*	*	۲.۳	۸۴.۱
۵	دسترسی به شبکه‌های اطلاع‌رسانی و فرهنگ سازی در زیست بوم سایبری	۲۷.۳	۲۲.۷	۱۱.۴	۹.۱	۱۱.۴	۶.۸	۶.۸	۲.۳	۲.۳	۷۴.۷
۶	برخوردار بودن از ظرفیت بالای فرهنگی بسیج در زیست بوم سایبری	۴۰.۹	۱۸.۲	۱۵.۹	۱۱.۴	۲.۳	۶.۸	۲.۳	*	۲.۳	۸۲.۶
میانگین کل											
۸۱.۲											

در خصوص این بُعد از پروژه تحقیقاتی، از مجموع میانگین (۸۱/۲٪)، کمترین تعداد مخاطبان (۷۴/۷٪)، دسترسی به شبکه‌های اطلاع‌رسانی و فرهنگ‌سازی در زیست بوم سایبری را یک قوت در حوزه عملیات روانی می‌دانند اما از طرف دیگر، بیشترین تعداد مخاطبان (۸۴/۱٪)، در اعلام نظر خود شاخص وجود مقام ولایت به عنوان پرچم‌دار مبارزه با تهدیدات عملیات روانی دشمن را به-عنوان قوت در این حوزه اعلام کرده‌اند.

راهبردها در حوزه عملیات روانی:

جدول اهمیت راهبردهای حاکم بر طرح راهبردی دفاع سایبری در حوزه عملیات روانی

ردیف	گویه‌های راهبردی در حوزه زیرساخت‌های عملیات روانی	درجه اهمیت هر سوال از صد درصد									
		۱	۲	۳	۴	۵	۶	۷	۸	۹	
۱	تدوین سند راهبردی عملیات روانی در نظام جامع دفاع سایبری کشور (آفتدی و پدافندی)؟	۶۵	۱۲.۵	۱۲.۵	*	*	۷۲.۵	۲.۵	*	*	
۲	توسعه ادبیات دفاع در برابر عملیات روانی در زیست بوم سایبری؟	۶۴.۷	۱۲.۵	۷.۵	۵	*	۷۵	*	*	*	
۳	تدوین سازوکارها و رویه های عملیات روانی کشور در فضای سایبر؟	۶۱.۴	۵	۱۰	۷.۵	*	۷۵	*	*	*	
۴	ایجاد و بهره برداری هوشمندانه از زیرساختهای سایبری پیشرفته به منظور دفاع در برابر عملیات روانی دشمن (ماهواره هاو رسانه وشبکه های ارتباطی...)?	۸۶.۶	۵۶.۸	۹.۱	۱۵.۹	۹.۱	۲.۳	*	۴.۵	۲.۳	
۵	استفاده از ظرفیت بسیج درجهت ارتقاء بصیرت ملی در برابر تهدیدات عملیات روانی دشمن در زیست بوم سایبری؟	۸۴.۳	۴۵.۵	۲۰.۵	۶.۸	۱۱.۴	۹.۱	۴.۵	۲.۳	*	
۶	ایجاد و توسعه سامانه فرماندهی و کنترل عملیات روانی دشمن در زیست بوم سایبری؟	۸۲.۸	۲۹.۵	۲۷.۳	۲۰.۵	۶.۸	۱۳.۶	۲.۳	*	*	
۷	آموزش، تربیت و توانمندسازی منابع انسانی موردنیاز حوزه عملیات روانی؟	۹۸.۸	۹۵	۲.۵		۲.۵	*	*	*	*	
۸	طراحی و ایجاد سامانه های آفتدی برای مقابله با عملیات روانی دشمن؟	۸۱.۴	۱۲.۵	۷.۵	۸۰	*	*	*	*	*	
۹	طراحی و پیاده سازی فرارگاه جنگ نرم برای مقابله با تهدیدات و حملات دشمن؟	۸۲.۸	۲۲.۵	*	۷۷.۵	*	*	*	*	*	
۱۰	طراحی و پیاده سازی سامانه های رصد، پایش، تشخیص و هشدار محورهای تبلیغی دشمن در عملیات روانی؟	۸۱.۸	۳۶.۴	۱۸.۲	۱۸.۲	۱۵.۹	۹.۱	*	*	۲.۳	
۱۲	نهادینه سازی مفاهیم پدافندی فرهنگی در ذات نظام های آموزشی کشور اعم از آموزش عالی، آموزش و پرورش و آموزش های سازمانی؟	۹۳.۲	۶۵.۹	۱۸.۲	۶.۸	۶.۸	۲.۳	*	*	*	
		۸۰.۳	میانگین کلی								
		۸۵	میانگین مجموع								

۱۴۰ فصلنامه امنیت ملی، سال ششم، شماره بیست و دوم، زمستان ۱۳۹۵

در این قسمت از سؤالات ابعاد پروژه تحقیقاتی، از مجموع میانگین (۸۰/۳٪)، حداقل تعداد نخبگان (۶۱/۴٪)، در تشخیص خود شاخص تدوین سازوکارها و رویه‌های عملیات روانی کشور در فضای سایبر را به‌عنوان راهبردهای این حوزه دانسته‌اند و در نقطه مقابل نیز بیشترین تعداد نخبگان (۹۳/۲٪)، در نظرات خویش، نهاده‌سازی مفاهیم پدافندی فرهنگی در ذات نظام‌های آموزشی کشور اعم از آموزش عالی، آموزش و پرورش و آموزش‌های سازمانی را به‌عنوان راهبردهای زیرساخت‌های منابع انسانی دفاع سایبری کشور ارزیابی کرده‌اند.

نتایج تحقیق:

در اجرای این تحقیق و در درجه نخست با انجام مطالعات اکتشافی و انجام مطالعات نظری و با استفاده از اسناد و مدارک معتبر مبادرت به شناخت کلیاتی از وضعیت سایبری در حوزه عملیات روانی نموده و سپس با مراجعه به جامعه خبرگی و جامعه آماری در صدد پاسخگویی به سؤال این پژوهش برآمده‌ایم و نتایج حاصله از این تحقیق به شرح زیر می‌باشد.

در نتیجه اقدامات پژوهشی صورت پذیرفته، این تحقیق به تدوین و ارائه راهبردهایی پرداخته تا تهدیدات، آسیب‌پذیری‌ها و هزینه‌های نظام در این عرصه کاهش یابد. نتایج و یافته‌های تحقیق و تولید محتوای صورت پذیرفته در این راستا، به این شرح می‌باشد:

عملیات روانی از جمله عرصه‌های دیگری است که در فضای سایبر به‌عنوان یک ابزار مؤثر بکار گرفته می‌شود. اینترنت می‌تواند با چهار عامل، تحول و انقلابی در عملیات روانی پدید آورد: ایجاد شبکه روانی اینترنت، هماهنگی، اجرا و تحلیل تأثیر و کارایی روند عملیات روانی. عملیات روانی سایبری، به‌عنوان تروریسم مجازی اگرچه دربرگیرنده تهدید و خشونت مستقیم نیست اما تأثیر روانی آن، بر جوامع هراسناک و مضطرب، می‌تواند به اندازه بمب‌گذاری تروریستی، قدرتمند باشد، عملیات روانی سایبری می‌تواند خصوصی، بی‌سر و صدا، فریبکارانه، جهانی و مملو از تنفر و تعصب باشد.

برای دستیابی به راهبردهای دفاع سایبری جمهوری اسلامی ایران در برابر تهدیدات سایبری، اسناد بالادستی، مبانی نظری، مطالعات تطبیقی و سایر مطالعات در حوزه عملیات روانی انجام و اصول و ارزش‌های حاکم بر طرح، عوامل خارجی و داخلی مؤثر بر آن و چشم‌انداز و رسالت و مأموریت قرارگاه دفاع سایبری که در گذشته فاقد آن بود و وجود نداشت، از طریق این تحقیق احصاء و

راهبردهای دفاع سایبری و تجزیه و تحلیل داده ها براساس آنها و با استفاده از نرم افزار EXCEL و نرم افزار SPSS احصاء شدند که عبارتند از:

عوامل خارجی:

تهدیدات:

- ۱) وجود شبکه‌های رسانه ای ماهواره ای وابسته به دشمن.
- ۲) وجود عناصر وابسته به غرب.
- ۳) تسلط دشمن برای اینترنت و شبکه های اجتماعی و انجام عملیات روانی.
- ۴) فضا سازی در مجامع جهانی علیه جمهوری اسلامی ایران؛ و متهم سازی در حوزه حقوق بشر.
- ۵) هجمه گسترده دشمن به نظام اعتقادی جامعه اعم از مردم و دولت، در راستای مقابله با گسترش مکتب اسلام ناب محمدی (صلی الله علیه و آله).
- ۶) القای تردید و ایجاد بی اعتمادی نسبت به نظام سیاسی کشور.
- ۷) امکان سنجش محیط اجتماعی فرهنگی ما از طریق شبکه‌های اجتماعی.
- ۸) شبکه سازی (برای جاسوسی و...) و سازماندهی عناصر مسئله در قالب گروه‌های براندازی.
- ۹) امکان راه اندازی جنبش‌های براندازی اجتماعی توسط دشمن.
- ۱۰) شکستن قبح ارتباط با خارجی و جاسوسی در قالب عضویت در شبکه‌های اجتماعی.

فرصت‌ها:

- ۱) امکان استفاده از ظرفیت اینترنت به منظور مقابله با عملیات روانی دشمن.
- ۲) امکان استفاده از ظرفیت‌های موجود در محیط خارجی در مقابل حملات عملیات روانی دشمن.
- ۳) به‌کارگیری تجارب سایر کشورها درخصوص مقابله با تهدیدات عملیات روانی.
- ۴) امکان آفند عملیات روانی دشمن.
- ۵) ظرفیت‌های رسانه ای در جهت پدافند عملیات روانی دشمن.
- ۶) امکان استفاده از نمایندگان، فضلا، اندیشمندان و علما جهت خشتی نمودن فعالیت‌های عملیات روانی دشمن.
- ۷) هشدارهای رهبری در رابطه با فعالیت‌های عملیات روانی دشمن.
- ۸) وجود استراتژی های بخشی برای مقابله با تهدیدات عملیات روانی دشمن.

۱۴۲ فصلنامه امنیت ملی، سال ششم، شماره بیست و دوم، زمستان ۱۳۹۵ ←
۹) پدافند عملیات روانی دشمن در زیست بوم.

عوامل داخلی:

ضعف‌ها:

- ۱) عدم توجه طیفی از مسئولین فرهنگی کشور نسبت به مخاطرات عضویت در شبکه‌های اجتماعی موجود.
- ۲) ضعف در روشننگری نسبت به القای شبهات دینی و فکری از سوی دشمن.
- ۳) فقدان عزم جدی و روحیه جهادی در طیفی از مدیران تصمیم‌ساز کشور برای مقابله با جنگ نرم دشمن.
- ۴) ضعف در راستای مقابله با رواج موهومات و خرافه‌ها در حوزه اعتقادات دینی.
- ۵) ضعف در غنی‌سازی محتوایی شبکه‌های فرهنگی موجود.
- ۶) کمبود برنامه‌های فرهنگی هدفمند در زیست بوم سایبری کشور به منظور جذب مخاطبین.
- ۷) خوش‌باوری در طیفی از جامعه نسبت به القای رسانه‌ها و شبکه‌های اجتماعی.
- ۸) نارسایی محتوای برنامه‌های آموزشی مرتبط با فرهنگ در سطوح مختلف تحصیلات در مدرسه.
- ۹) کمبود اطلاعات و آگاهی‌های مدیران فرهنگی کشور در سطوح مختلف.
- ۱۰) تأثیرپذیری بخشی از جامعه از ترویج سبک زندگی غربی.
- ۱۱) فقدان ساختار مدیریتی قوی در برخورد با فرهنگ‌های وارداتی.
- ۱۲) فقدان شناخت کامل از نقش فن‌آوری‌های نوین.
- ۱۳) وجود شکاف‌های سایبری عمیق در ساختار جمعیتی کشور.
- ۱۴) کمبود منابع انسانی متخصص و متعهد در جهت مقابله با عملیات روانی دشمن.
- ۱۵) آماده نبودن مردم کشور در راستای افزایش توان مقاومت آن‌ها در برابر حمله‌های فرهنگی.

قوت‌ها:

- ۱) وجود مقام عظمای ولایت (مدظله‌العالی) به عنوان پرچم‌دار مبارزه با تهدیدات عملیات روانی دشمن.
- ۲) برخورداری از ظرفیت بالای فرهنگی بسیج در زیست بوم سایبری.
- ۳) وجود برخی آگاهی‌های نسبی مردم از روش‌های عملیات روانی دشمن.
- ۴) اعتقاد اندیشی ریشه‌دار با تکیه بر تعالیم اسلامی.

راهِبردهای دفاع سایبری ج ۱۱ در برابر تهدیدات جنگ روانی ♦ ۱۴۳

۵) وجود متخصصین انقلابی در زمینه مقابله با اقدامات عملیات روانی دشمن.

۶) دسترسی به شبکه‌های اطلاع‌رسانی و فرهنگ‌سازی در زیست بوم سایبری.

ارائه راهبردها:

راهِبردهای دفاع سایبری جمهوری اسلامی ایران در برابر تهدیدات در حوزه عملیات روانی	
۱	تدوین سند راهبردی عملیات روانی در نظام جامع دفاع سایبری کشور، هم در بعد آفتدی و هم در بعد پدافندی
۲	توسعه ادبیات دفاع در برابر عملیات روانی در زیست بوم سایبری جمهوری اسلامی ایران
۳	تدوین سازوکارها و رویه‌های عملیات روانی کشور در فضای سایبر
۴	ایجاد و بهره‌برداری هوشمندانه از زیرساخت‌های سایبری پیشرفته به منظور دفاع در برابر عملیات روانی دشمن، در حوزه‌هایی همچون: ماهواره، رسانه و شبکه‌های ارتباطی
۵	استفاده از ظرفیت بسیج در جهت ارتقای بصیرت ملی در برابر تهدیدات عملیات روانی دشمن در زیست بوم سایبری جمهوری اسلامی ایران
راهِبردهای دفاع سایبری جمهوری اسلامی ایران در برابر تهدیدات در حوزه عملیات روانی	
۶	ایجاد و توسعه سامانه فرماندهی و کنترل عملیات روانی دشمن در زیست بوم سایبری کشور
۷	آموزش، تربیت و توانمندسازی منابع انسانی موردنیاز حوزه عملیات روانی
۸	طراحی و ایجاد سامانه‌های آفتدی برای مقابله با عملیات روانی دشمن
۹	طراحی و پیاده‌سازی فرارگاه جنگ نرم برای مقابله با تهدیدات و حملات دشمن
۱۰	طراحی و پیاده‌سازی سامانه‌های رصد، پایش، تشخیص و هشدار محورهای تبلیغی دشمن در عملیات روانی
۱۲	نهادینه‌سازی مفاهیم پدافندی فرهنگی در ذات نظام‌های آموزشی کشور اعم از آموزش عالی، آموزش و پرورش و آموزش‌های سازمانی

پیشنهادات:

با توجه به اهمیت برخورداری از راهبرد در حوزه دفاع سایبری، پژوهشی برای تدوین راهبردهای کلی دفاع سایبری و همچنین راهبردهای بخشی آن بر مبنای یافته‌های ارائه شده، در سطوح مختلف انجام شود.

برای اجرایی شدن راهبردها و ارائه راهکارهای اجرایی، تحقیقات دیگری انجام گیرد. نتایج این پژوهش به منظور ارزیابی و در صورت لزوم استفاده در اختیار قرارگاه پدافند غیرعامل ارائه شود.

نتایج این پژوهش به منظور ارزیابی و در صورت لزوم استفاده در اختیار شورای عالی فضای مجازی قرار گیرد.

منابع و مأخذ

- امام خامنه‌ای (مدظله‌العالی)، پایگاه اطلاع‌رسانی دفتر مقام معظم رهبری.
- امیرصوفی، رحمت الله (۱۳۸۸)، آینده پژوهشی جنگ اطلاعاتی روانی و مدیریت مقابله با آن، تهران: ستاد کل نیروهای مسلح.
- پور ابراهیمی، علیرضا و بنایی، سجاد (۱۳۸۹)، آشنایی با اصول امنیت محیطی در حوزه فن‌آوری اطلاعات و ارتباطات، تهران: انتشارات دانشگاه آزاد اسلامی واحد الکترونیکی.
- حسن بیگی، ابراهیم (۱۳۸۸)، حقوق و امنیت در فضای سایبر، تهران: انتشارات دانشگاه عالی دفاع ملی.
- حسینی، سید حسین (۱۳۹۰)، اصول و مبانی عملیات روانی، تهران: دانشگاه امام حسین (علیه‌السلام).
- زورق، محمدحسن (۱۳۹۰)، تقریرات کلاسی دوره دکترا، درس آشنایی با عملیات روانی، تهران: دانشگاه عالی دفاع ملی.
- زورق، محمدحسن (۱۳۸۹)، ارتباطات و آگاهی، جلد‌های اول تا سوم، تهران: انتشارات سروش.
- عامری، داود (۱۳۹۲)، ایران سایبری، تهران: انتشارات معاونت فرهنگی و تبلیغات دفاعی ستاد کل نیروهای مسلح.
- عبدالله خانی، علی (۱۳۸۵)، رویکردها و طرح‌های امریکایی در باره ایران، تهران، موسسه فرهنگی مطالعاتی ابرار معاصر.
- عبدالله خانی، علی (۱۳۸۵)، حفاظت از زیر ساخت‌های حیاتی اطلاعاتی (فصلنامه سیاست دفاعی، شماره ۵۴)، تهران، انتشارات دانشگاه امام حسین (علیه‌السلام).
- گروه مطالعات جنگ نرم، (بهار و تابستان ۱۳۸۸)، جنگ نرم: از تهدید تا پاسخ، تهران، فصلنامه مدیریت بحران و وضعیت‌های اضطراری، سال اول، شماره ۳ و ۴.
- مجموعه مقالات همایش عملیات روانی، ۱۳۸۸.

۱۴۶ فصلنامه امنیت ملی، سال ششم، شماره بیست و دوم، زمستان ۱۳۹۵ ←

• مرادیان، حجت الله (۱۳۹۱)، سایبر و عملیات روانی، تهران: دانشگاه جامع امام حسین (علیه السلام).

• نای، جوزف (۱۳۸۹)، قدرت نرم، ابزارهای موفقیت در سیاست بین الملل، سید محسن روحانی و مهدی ذوالفقاری، تهران، انتشارات دانشگاه امام صادق (علیه السلام).

• <http://www.tebyan.net>.

منابع انگلیسی:

- <http://www.hccmr.com/news-494.aspx>.
- Center for Strategic & International Studies Report, April 19, 2011.
- Franklin D. Kramer, Cyberpower and National Security, U.S National Defense University, Washington D.C, 2009.