

## تدوین الگوی طرح دفاع سایبری در برابر تهدیدات سایبری حوزه اقتصاد

علی محمد احمدوند<sup>۱</sup>

اکبر رضازاده<sup>۲</sup>

تاریخ دریافت: ۱۳۹۵/۰۵/۱۷

تاریخ پذیرش: ۱۳۹۵/۰۷/۱۳

### چکیده

در عصر ارتباطات و اطلاعات و فضای مجازی، جهان به سمتی پیش می‌رود که دنیای مجازی به موازات دنیای واقعی و حتی بیشتر از آن خود را به زندگی بشر تحمیل کرده است. یکی از عرصه‌های این فضا که دربرگیرنده تولید، واردات، صادرات و سایر تعاملات بین‌المللی بوده و متکی به شبکه‌های جهانی است، حوزه اقتصاد است. تهدیدات دشمن بعد از استقرار نظام مقدس ج. ا. ا در ابعاد مختلف و در حوزه‌های گوناگون خواه در شرایط واقعی و عینی و خواه در فضای سایبری از یک روند تصاعدی برخوردار بوده و بالطبع بخش‌های اقتصادی به‌ویژه نظام پولی و بانکی کشور به جهت اهمیت و جایگاه خاص آن، با تهدیدات مضاعف دشمن روبرو بوده است. از این‌رو، می‌بایست تمهیدات و بسترهای لازم و مناسب آن اندیشیده و به مرحله اجرا درآید، لذا محقق در این تحقیق به دنبال احصاء تهدیدات سایبری حوزه اقتصاد، ملاحظات اساسی و کارکردهای دفاعی آن با رویکرد نظام پولی و بانکی است تا بتوان با تدوین الگوی طرح راهبردی دفاع سایبری در جهت تأمین منافع و امنیت ملی با عنایت به اصول و ارزش‌های حاکم، چشم‌انداز، مأموریت، عوامل داخلی و خارجی مؤثر بر آن عمل نماید.

این تحقیق از نوع کاربردی - توسعه ای بوده و از روش ترکیبی با استفاده از روش‌های کمی و کیفی، روش دلفی جهت جمع‌آوری اطلاعات از نخبگان در حوزه سایبری و روش اکتشافی در مراجعه به اسناد و مدارک بهره‌برداری گردیده است. جامعه آماری این تحقیق، تعدادی از مدیران بانکی و پولی کشور و تعدادی از اساتید تخصصی و صاحب‌نظر دانشگاه عالی دفاع ملی مرتبط با موضوع می‌باشند که با حجم محدود ۴۰ نفر به‌عنوان جامعه خبرگی به‌صورت هدفمند اجرا شده است.

یافته‌های تحقیق حاکی است شاخص شبکه‌های بومی و امن به‌عنوان بالارزش‌ترین اصول، وابستگی به سامانه‌های بانکی بین‌المللی به‌عنوان اساسی‌ترین چالش، خرابکاری سیستم‌های نرم افزاری، سخت افزاری و داده‌ها به‌عنوان مهم‌ترین تهدید، افزایش قابلیت‌های دفاعی نظام سایبری اقتصادی کشور به‌عنوان اصلی‌ترین راهبرد، استفاده از تحریم‌های دشمن برای تقویت اقتصاد و تولید داخلی به‌عنوان بهترین فرصت، وابستگی علمی سایبری در حوزه اقتصاد به خارج از کشور به‌عنوان مهم‌ترین ضعف و بالاخره توسعه به‌کارگیری نرم افزارهای بومی در برخی زیرساخت‌های اقتصادی کشور به‌عنوان برترین قوت می‌باشند.

**واژه‌های کلیدی:** فضای سایبری، تهدیدات حوزه اقتصاد، الگوی طرح راهبردی، دفاع سایبری

<sup>۱</sup> - استاد دانشگاه امام حسین (علیه‌السلام)

<sup>۲</sup> - نویسنده مسئول و عضو هیأت علمی دانشگاه علوم انتظامی

## ۱- مقدمه:

شکل‌گیری فضای سایبر و اینترنت، ریشه در دوره جنگ سرد دارد. خدمات و فعالیت‌های ارائه شده در فضای سایبر را می‌توان در قالب موضوعات فرهنگی، اقتصادی، سیاسی، اجتماعی، تجاری، دفاعی و امنیتی قرار داد. البته باید توجه داشت که هریک از موضوعات ذکر شده، ممکن است فعالیت‌های دیگر را نیز شامل شود (حسن بیگی، ۱۳۸۴: ۹۳) در عصر ارتباطات و اطلاعات، فضای مجازی، جهان به سمتی پیش می‌رود که دنیای مجازی به موازات دنیای واقعی و حتی بالاتر از آن خود را به زندگی بشری تحمیل نموده است. یکی از مهم‌ترین بخش‌های هر کشور در این عرصه که دربرگیرنده تولید، واردات، صادرات و سایر تعاملات بین‌المللی که متکی به شبکه‌های جهانی است، بخش‌های اقتصادی آن کشور به‌ویژه نظام پولی و بانکی کشور است. در کشورمان نیز بخش‌های پولی و بانکی کشور از این امر مستثنا نبوده و از آنجا که در معرض تهدیدات دشمن خواه در شرایط حقیقی و عینی و خواه در فضای سایبری قرار دارد، لذا می‌بایست تمهیدات لازم و مناسب آن اندیشیده و به مرحله اجرا درآید، چراکه این حوزه متأثر از فن‌آوری‌های نوین در عرصه جنگال و سایبر بوده و روندها حاکی از وابستگی روزافزون و تمایل به استفاده از فن‌آوری‌های شبکه ای در فعالیت‌های اقتصادی است. (همان، ۱۲۵)

استفاده از فضای سایبر که دستاورد فن‌آوری‌های نوین اطلاعات است، اگرچه برای کشورهای در حال توسعه به‌عنوان یک فرصت برای جبران عقب‌ماندگی‌های فناورانه نسبت به جوامع پیشرفته است، اما باید دقت نمود که همین فن‌آوری که ساخته دست این جوامع است، اگر درست مورد بهره‌برداری قرار نگیرد و حساسیت‌های امنیتی آن مورد توجه واقع نشود، خود می‌تواند به‌عنوان یک تهدید مهم به حساب آید، از آنجایی که جمهوری اسلامی ایران، نظامی است ایدئولوژیک و آرمانی، در حال مبارزه با نظام سلطه و استکبار، ذات وجود و ایستادگی چنین نظامی مخصوصاً در بعد اقتصادی، نیازمند ملزوماتی است که در آن تمام حوزه‌های اقتصادی کشور در مقابل تهدیدات دشمن خواه در شرایط حقیقی و عینی و خواه در فضای سایبری مصون بمانند، بدین منظور می‌بایست تمهیدات و بسترهای لازم و مناسب آن در تمام بخش‌های خرد و کلان حوزه اقتصاد اندیشیده و به مرحله اجرا درآید. (گودرزی، آتوسا و فلاحی، منیژه، ۱۳۸۶: ۲۹) با توجه به اینکه امنیت بستر اصلی توسعه و پیشرفت در طول ادوار تاریخ بوده و در صورت فراهم بودن امنیت اقتصادی می‌توان علاوه بر جلب اعتماد سرمایه‌گذاران در تمام بخش‌های کشور، امنیت جانی و

امنیت حقوقی معاملات و مالکیت‌ها را تضمین نمود، بر این اساس، محقق در این تحقیق به دنبال احصاء تهدیدات سایبری این حوزه، ملاحظات اساسی و کارکردهای دفاعی سایبری با رویکرد نظام پولی و بانکی است تا در راستای تأمین منافع و امنیت ملی و با عنایت به اصول و ارزش‌های حاکم، چشم‌انداز، مأموریت، عوامل داخلی و خارجی مؤثر بر آن بتوان اقدامات مؤثری به عمل آورد، لذا سؤال محوری تحقیق این مسئله است که الگوی طرح راهبردی دفاع سایبری کشور در برابر تهدیدات سایبری حوزه اقتصادی چیست؟ از آنجایی که اصول و ارزش‌های حاکم بر طرح راهبردی دفاع سایبری برای مقابله با تهدیدات دفاع سایبری از اهمیت خاصی برخوردار است، چشم‌انداز طرح دفاع سایبری و افق آن بر اساس چشم‌انداز کلان ۱۴۰۴ کشور باید از چه جایگاهی برخوردار باشد و همچنین احصاء عوامل داخلی و خارجی مؤثر در برابر تهدیدات سایبری حوزه اقتصادی از دیگر مباحث اساسی می‌باشند که در این تحقیق مورد بررسی قرار گرفته‌اند.

## ۲- ادبیات تحقیق:

### امنیت اقتصادی

امنیت اقتصادی در تعامل با امنیت سیاسی و رفع شرایط خشونت‌آمیز معنا می‌یابد (pinheiro, 1997, p.60). رابرت ماندل در کتاب خود به‌عنوان «چهره متغیر امنیت ملی»، امنیت اقتصادی را این‌گونه تعریف می‌کند: میزان حفظ و ارتقاء شیوه زندگی مردم در یک جامعه از طریق کالا و خدمات و هم از مجرای عملکرد داخلی و هم حضور در بازارهای بین‌المللی. (ماندل، ۱۳۷۹، ۱۰) دکتر بیژن آبادی امنیت اقتصادی را این‌گونه تعریف می‌کند: امنیت اقتصادی اصول ایجاد و تثبیت یک بستر مناسب برای انجام فعالیت‌های اقتصادی است، این بستر اصولاً حقوق فرد را در رابطه با کلیه فعالیت‌های اقتصادی وی تضمین می‌کند و عملکرد متقابل او با سایر افراد جامعه را عملاً تعریف می‌کند. (رنجبر، ۱۳۸۶، ۲۸) امنیت اقتصادی یکی از مهم‌ترین ابعاد امنیت ملی و از اصول مهم زیرساخت‌های اساسی کشور برای دستیابی به توسعه اقتصادی و ارتقاء سطح رفاه اجتماعی محسوب می‌شود و از این‌رو همیشه مورد توجه سیاست‌گذاران و برنامه‌ریزان اقتصادی کشورها بوده است. (عزتی، ۱۳۸۷، ص ۷) پس از یک مشروحه اجمالی در خصوص امنیت اقتصادی در این بخش به تشریح بانکداری و نظام پولی کشور در فضای سایبری، اصول و ارزش‌های اساسی، کارکردها، تهدیدات و ویژگی‌های دفاع سایبری در حوزه اقتصاد می‌پردازیم:

## بانکداری الکترونیکی

به فراهم آوردن امکان دسترسی مشتریان به خدمات بانکی با استفاده از واسطه‌های ایمن و بدون حضور فیزیکی اطلاق می‌شود (کهزادی، ۴۸: ۱۳۸۲) بانکداری الکترونیکی مبتنی بر سه مدل اصلی است:

۱- متمرکز شدن بر مدیریت و مشتری به منظور توسعه و تأمین روابط سودآور بلندمدت: این رویکرد، توسعه و ارائه طیف وسیعی از خدمات بانکی و مالی را که توسط دامنه بزرگی از خدمات پشتیبانی تقویت می‌شود، در برمی‌گیرد و بیشتر از طریق اینترنت و یا تلفن و به صورت شبانه‌روزی صورت می‌گیرد.

۲- تمرکز بر رفع نیازهای خاص مشتریان: بانک‌ها به علت خدمات بسیار حرفه‌ای و اختصاصی قادر هستند تا کارمزدهای بیشتری را از مشتریان خود دریافت کنند. مطابق با این مدل ویژه، سه ناحیه اصلی تخصصی در این زمینه وجود دارد:

الف - سرمایه‌گذاری ب - مدیریت وجوه ج - وام‌های بانک (همان، ۵۳)

۳ - فراهم کردن قیمت مناسب و هزینه‌های پایین و خدمات استاندارد برای تعداد زیادی از مشتریان: اینترنت و تلفن به دلیل سرعت و انعطاف‌پذیری بالا، راه‌های ایده‌آلی برای انتقال خدمات بانکی می‌باشند، چنانچه روش‌های اینترنتی در حد زیاد استاندارد شوند، بانکداری مستقیم نمی‌تواند احتیاجات سطح بالاتر مشتریان را برآورده کند. (مشرف جوادی، محمدحسین، بهزادفر، فاطمه، قوچی نژاد، حمزه، ۱۳۸۹: ۲۷) بانکداری الکترونیکی برحسب امکانات و نیازهای بازار می‌تواند در زیرشاخه‌ها و انواع مختلفی ارائه شود که عبارت‌اند از: بانکداری اینترنتی، بانکداری مبتنی بر تلفن همراه و فناوری‌های مرتبط با آن، بانکداری تلفنی، بانکداری مبتنی بر نمابر، بانکداری مبتنی بر دستگاه‌های خودپرداز، بانکداری مبتنی بر پایانه‌های فروش و بانکداری مبتنی بر شعب الکترونیکی. عمده‌ترین ابزارهای پرداخت الکترونیکی عبارت‌اند از: انواع کارت‌های بانکی<sup>۴</sup>، چک الکترونیکی<sup>۵</sup>، پول الکترونیکی<sup>۶</sup>، حواله الکترونیکی (جلالی فراهانی، ۱۳۸۴: ۳۰)

4.chargcards-debit cards-credit cards

5.electronic cheque

6.electronic cash (e-cash)

7-on line

8-George Matheus

9-Sherwood

اصول و ارزش‌های<sup>۱</sup> دفاع سایبری در حوزه اقتصادی:

اصول، مجموعه‌ای از دستورالعمل‌هایی است که هنجارهای رفتاری را کنترل می‌کند و تحت نظم قرار می‌دهد. ارزش از بنیادی‌ترین عوامل در تبیین اندیشه، عمل یا اعمال فرد و همچنین شکل‌گیری حیات اجتماعی است.

سازمان‌دهی سازوکارها و تدبیر امور در حوزه فعالین اقتصادی بایستی به گونه‌ای صورت گیرد که پیگیری مبارزه با نظام سلطه از حوزه اقتصاد مصون باشد. این مسئله زمانی اهمیت بیشتری می‌یابد که توجه شود که حوزه اقتصاد، بزرگ‌ترین برگ برنده و مزیت نظام سلطه است و لذا می‌تواند از این مسیر نظام اسلامی را به شدت تهدید کند. بنا به فرمایش مقام معظم رهبری کشور باید به سمت اقتصاد مقاومتی حرکت کند. این نوع از اقتصاد در شرایط تحریم که یکی از تهدیدات اساسی دشمن است، می‌تواند از ظرفیت‌های اقتصادی کشور دفاع کند و توان مقاومت را در این بخش‌ها ایجاد و یا تقویت نماید (جلالی، ۱۳۹۱: ۵۰) بر این مبنا ضرورت دارد ملاحظات ذیل مورد توجه لازم قرار گیرد:

- تئوری پردازی در خصوص اقتصاد مقاومتی و اهتمام در اجرای آن که بایستی سریعاً مدنظر قرار گیرد. باید تلاش شود تا نظام اقتصاد به گونه‌ای سامان یابد که هم کارآمدی و پیشرفت و تعالی مادی و معنوی را به دنبال داشته باشد و هم موضع ضد استکباری نظام اسلامی را تقویت نماید. (نریمانی و عسکری، ۱۳۹۰: ۴ و ۵) لذا در صورتی که تئوری پردازی مناسبی مبتنی بر الگوی مقاومتی صورت گرفته باشد، فشارها و تحریم‌های خارجی به جای تهدید نظام اسلامی، به یک وضعیت مناسب برای پیشرفت کشور خصوصاً در حوزه اقتصادی تبدیل می‌شود.

- فرصت‌سازی از تحریم‌ها به عنوان پلی برای عبور از وابستگی به دنیای خارج، اگرچه تحریم‌ها در شرایط فعلی به عنوان چالش‌های مهم مطرح بوده و همواره به آسیب بیشتر به نظام اسلامی منجر می‌شوند، لیکن باید تغییر نقش داده و به عنوان عامل مثبت و تقویت‌کننده تبلور یابند. دلیل مهم این است که اجرایی‌سازی و پیاده‌سازی راهبردهای اقتصاد مقاومتی نیازمند همراهی و همدلی سطوح مختلف حوزه‌های تصمیم‌گیری، سیاست‌گذاری و اجرا در کشور و همچنین پذیرش عمومی و همکاری توده‌های مردمی است و تشدید تحریم‌ها و فشارهای بین‌المللی خصوصاً در حوزه اقتصادی باعث می‌شود نیل به این وحدت و یکپارچگی در داخل کشور تقویت شده و

<sup>1</sup>-value

اضطرار ناشی از اعمال این تحریم‌ها به سرعت بیشتر در تصمیم‌گیری و اجرایی سازی راهبردهای مبتنی بر اقتصاد مقاومتی منجر شود. (همان، ۶) هم‌زمان با ملاحظات مذکور ضرورت دارد نسبت به:

- تشکیل قرارگاه دفاع اقتصادی کشور و هدایت و کنترل متمرکز اقتصاد کشور در هر دو عرصه واقعی اقدام تا با مدیریت و پایش اقدامات و تفکرات دشمن و کشف آسیب‌پذیری‌ها، به مقابله با آن‌ها پرداخته و با رفع آن‌ها از حوزه اقتصادی کشور، به همسویی و هم‌افزایی لازم در بخش مؤلفه‌های اقتصادی و تجمع قوا به منظور ایجاد نیروی لازم برای مقاومت با حضور متولیان دستگاه‌های اقتصادی، دفاعی و امنیتی با این ملاحظه که این مدیران می‌بایست به درک واحدی از جنگ و بحران اقتصادی برسند، دست یافت.

- مدیریت و پاسخگویی در مقابل تهدیدات اقتصادی از طریق شناخت و کاهش آسیب‌پذیری‌های عمده به منظور پایدارسازی زیرساخت‌های اقتصادی و نهادینه نمودن آن در برابر تحولات بازارهای جهانی از یک طرف و مدیریت پاسخگو در عرصه‌های اقتصادی با اتخاذ تصمیمات مناسب فشارهای روانی روی مردم را کاهش داده و مدیریت بحران و تحریم‌ها را در جنگ اقتصادی تسهیل بخشند.

- پایدارسازی کارکردها در برابر تهدیدات اقتصادی: از آنجا که یکی از راهبردهای دشمن در این حوزه ناکارآمد نشان دادن نظام در پاسخگویی به نیازهای مردم در حوزه اقتصاد است، لذا می‌طلبید متولیان این حوزه مهم کشور با اتخاذ راهکارهایی از قبیل کاهش هزینه‌های تحمیلی بر سبد مصرفی خانوارها با تکمیل و توسعه هدفمندی یارانه‌ها، سوق دادن یارانه‌ها به سمت کالاهای اصلی در سبد مصرفی از افزایش قیمت و یا کاهش تولید آن‌ها جلوگیری نمود. همچنین رایگان شدن خدمات درمانی و تکلیف دولت به اجرای آن اهداف نظام را تحقق خواهد بخشید. (کارگاه خبرگی گروه مطالعاتی شهید صیاد، ۱۳۹۳/۱/۲۱)

- خود اتکایی سایبری که در این بخش ملاحظاتی چون تحریم هوشمندانه کالاهای خارجی، اصلاح قوانین و مقررات کند و سد کننده در برابر تولیدات داخلی، پایدارسازی حوزه‌های اصلی کشور، با استفاده از معافیت‌ها و بسته‌های تشویقی برای تولیدات داخلی و بالاخره استفاده از فن‌آوری‌ها در تولید داخلی و در گام بعدی، تولید فن‌آوری و محصول در داخل کشور می‌تواند شرایط مناسبی برای خود اتکایی دفاع سایبری در کشور ایجاد نماید. (همان)

- شبکه‌های بومی و امن که بتوان با استفاده از آن‌ها در حوزه زیرساخت‌های اقتصادی با هدف توانمندی برای جذب شوک یا ضربه و نیز خروج سریع از حالت اختلال به طوری که بتوان به سرعت سطح سرویس خود را به میزان اولیه یا نزدیک به آن بازگرداند.». (ابراهیم نژاد، ۱۳۸۹: ۷)

- سلامت اداری و اقتصادی که لازمه آن برخورداری از فضای امنی است که در جامعه ایجاد شده است، لازمه امنیت و سلامت اقتصادی برخورد با مفسدان اقتصادی و افرادی است که قانون را دور می‌زنند. رهبر معظم انقلاب در این خصوص شفاف‌سازی را شرط اصلی مقابله با فساد اقتصادی دانسته و می‌فرماید: «باید فضای رقابتی و با ثبات اقتصادی به وجود آید زیرا در چنین فضایی سالمی، فعال اقتصادی احساس امنیت خواهد کرد، ضمن اینکه در چنین شرایطی کسب ثروت با ابتکار و پشتکار مباح و مورد تأیید نظام است.» (چشمه همیشه جاری، ۱۳۹۲: ۱۱)

- ظرفیت‌های بومی و امن در حوزه اقتصادی، بانکی و پولی که بتوان در صورت مواجهه با تهدیدات سایبری و اعمال تحریم توسط کشورهای پیشرفته توان مقابله با آن‌ها را از طریق تولید داخلی داشته باشد. (کارگاه اعضای خبرگی گروه مطالعاتی شهید صیاد شیرازی، ۱۳۹۳/۱/۲۱)

تهدیدات حوزه اقتصاد در فضای سایبری:

تهدید عبارت است از وضعیتی که در آن، خطر یا آسیب جدی، ارزش‌های اساسی و حیاتی یک بازیگر را مورد هدف قرار می‌دهد. به عبارتی عوامل یا وضعیت‌های برون‌سازمانی هستند که بر سازمان تأثیر نامطلوب دارند و می‌توانند آن را از انجام وظایفش بازدارند. در حوزه بانکداری الکترونیکی این تهدیدات می‌تواند شامل موارد ذیل باشد:

- وضع قوانین و مقررات در مقیاس جهانی با شاخص پول‌شویی که اساسی‌ترین محور تهدیدات دشمن در این حوزه در دو بخش وضع قوانین و مقررات و بخش فیزیکی است، در قسمت قوانین و مقررات با مطرح کردن بحث پول‌شویی در مقیاس جهانی، از انجام عملیات نقدینگی کشور در سطح بین‌الملل، جلوگیری می‌کند و با وضع تحریم‌ها، علیه بخش بانکی کشور، خصوصاً بانک مرکزی، فعالیت‌های بانکی کشور را تحت تأثیر خود قرار داده است. (جلالی، ۱۳۹۱: ۳۱)

- تحریم فعالیت‌های بانکی سایبری

که در این بخش نیز دشمن با تحریم شرکت‌های حمل‌ونقل هوایی و دریایی و ایجاد محدودیت در تأمین سوخت برای کشتی‌ها و هواپیماها و ایجاد مشکلات بیمه‌ای برای کالاهای تجاری و همچنین ایجاد محدودیت در زمینه اخذ منابع مالی (فاینانس) از بانک‌های بین‌الملل باعث گردیده،

مؤسسات مالی و اعتباری بین‌المللی رغبتی برای انجام فعالیت‌های اقتصادی در کشورمان نداشته باشند. (جلالی، ۱۳۹۱: ۳۲)

- تهدیدات از طریق انجام اعمال عمدی

سابوتاژ و خرابکاری که در آن خرابکاران به سیستم نرم افزاری، سخت افزاری یا داده‌ها حمله کرده و آن‌ها را تخریب می‌کنند. شرایطی که در این وضعیت ریسک را افزایش می‌دهند، عبارت‌اند از:

الف- ممانعت غیر کافی از دسترسی غیرمجاز

ب- کنترل غیر کافی تغییرات سیستم

ج- روش‌های غیر کافی سازمانی (البرزی، ۱۳۹۱: ۴۶۱)

در مطالعات و بررسی‌های صورت گرفته از سوابق و اسناد موجود و مصاحبه با تعدادی از خبرگان سازمان پدافند غیرعامل که اخیراً انجام گردیده، اذعان داشتند، در حال حاضر سامانه بانکداری الکترونیک کشور در وضعیتی است که عدم توجه مناسب به آن می‌تواند باعث مضاعف شدن تهدیدات در این حوزه گردد، از طرفی اقدامات خصمانه خزانه‌داری امریکا علیه حوزه اقتصادی و اشراف حقوقی و مدیریتی این کشور بر سیستم‌های اقتصادی باعث رو به فزونی نهادن تهدیدات در حوزه سایبری اقتصادی گردیده است، (کارگاه اعضای خبرگی گروه مطالعاتی شهید صیاد شیرازی، ۱۳۹۳/۱/۲۱) ضمن اینکه در حوزه اقتصاد سایبری موارد ذیل‌الذکر زمینه‌های تهدید را تشدید نموده است:

۱. واگذاری خدمات زیر ساختی حاکمیتی سایبری به بخش خصوصی بدون نظارت لازم
۲. تغییر ماهیت پول در فضای سایبری
۳. استفاده غیرهوشمندانه از نرم افزارهای پیشرفته اقتصادی بدون توجه به تهدیدات و آسیب‌پذیری‌های ذاتی آن (همان)

ضمن اینکه فناوری حال حاضر بانک مرکزی کشور در حوزه خدمات انفورماتیک دارای اشکالات اساسی زیر است:

۱- شرکت خدمات انفورماتیک بانک مرکزی که به صورت متمرکز برای تمام بانک‌های کشور سرویس می‌دهد، به دلیل وابستگی فن‌آوری به خارج از کشور از سازوکار امنیتی مناسبی برخوردار نیست و دارای شکست‌های امنیتی است.



تدوین الگوی طرح دفاع سایبری در برابر تهدیدات سایبری حوزه اقتصاد ♦ ۷۳

۲- بانک‌های کشور در بخش‌هایی خود را مستقل از سیستم بانک مرکزی می‌دانند، در حالی که بانک مرکزی قائل به تمرکز امور بانکی بوده که این امر با اهداف دفاعی و امنیتی کشور مغایرت دارد، ضمن اینکه بانک‌ها بانک مرکزی را به‌عنوان رقیب می‌بینند و وزران اقتصاد نقش حاکمیتی خود را به نیکی ایفا نمی‌کند.

۳- نرم‌افزار و سخت افزارهای سامانه بانکی و پولی کشور اگرچه به ظاهر ایجاد امنیت می‌نماید اما در واقع اطلاعات آن حوزه را به خارج ارسال می‌کند. (سازمان پدافند غیرعامل، پارسا: دی‌ماه ۹۲)



۴- سامانه کارت‌های هوشمند بانکی و جایگاه‌های ATM به جهت وابستگی به شرکت‌های صاحب فن‌آوری به‌طور کامل رصد می‌گردد. (سازمان پدافند غیرعامل، فرجی پور، دی‌ماه ۹۲)

(۳) روش‌شناسی تحقیق (کمی، کیفی و آمیخته)

این تحقیق به لحاظ بهره‌برداری در حوزه‌های اقتصادی و دفاع سایبری و مقابله با تهدیدات سایبری کاربردی بوده و در راستای راهبردی بودن در سطح ملی و قابلیت تعمیم‌پذیری توسعه‌ای است. در این تحقیق از روش ترکیبی (سه‌بعدی) با استفاده از روش‌های کمی و کیفی و ترکیب آن و روش دلفی جهت جمع‌آوری اطلاعات از نخبگان در حوزه سایبری و روش اکتشافی در مراجعه به اسناد بهره‌برداری گردیده است.

قلمروی موضوعی تحقیق حاضر نظام پولی و بانکی کشور در فضای سایبری، قلمروی مکانی آن گستره کشور جمهوری اسلامی ایران و قلمرو زمانی آن سال‌های ۹۱ تا ۹۳ را در برمی‌گیرد.

جامعه آماری این تحقیق عبارت‌اند از: در حوزه اقتصادی: اعضای خبرگی گروه مطالعاتی شهید صیاد شیرازی اعم از اساتید و دانشجویان، اساتید و دانشجویان دانشگاه عالی دفاع ملی، مدیران و کارشناسان ارشد و عالی‌بانک مرکزی ج.ا.ا، و تعدادی از مدیران بانکی و اقتصادی کشور، دانشجویان: دانشگاه اقتصاد، دانشکده اقتصاد دانشگاه‌های تهران و علامه طباطبایی. در این پژوهش با استفاده از دیدگاه نخبگان صاحب‌نظر با حجم محدود ۴۰ نفر در هر حوزه، به‌عنوان جامعه خبرگی به صورت هدفمند اجرا شده است.

از روش نمونه‌گیری غیر تصادفی و هدفمند در این تحقیق بهره گرفته شده است. که بر اساس نسبت‌های تعیین‌شده و حجم نمونه صورت می‌پذیرد. حجم نمونه معادل حجم جامعه آماری یعنی ۴۰ نفر در نظر گرفته شده است. روایی تحقیق حاضر با استفاده از دیدگاه صاحب‌نظران نخبه دانشگاهی و اقتصادی و تأیید آنان به صورت روایی محتوایی مورد تأیید قرار گرفته است. پایایی پرسشنامه نیز پس از اخذ ضریب آلفای کرونباخ با توجه به واریانس هر یک از متغیرها از طریق نرم‌افزار SPSS ۰/۹۵ به دست آمد.

۴- تجزیه و تحلیل داده‌ها (یافته‌های تحقیق)

در بررسی یافته‌های تحقیق حاضر که از جامعه آماری این تحقیق (جامعه نخبگی) در پاسخ به این سؤال که اساسی‌ترین اصول و ارزش‌های حاکم بر حوزه اقتصاد را چگونه ارزیابی می‌کنید، به دست آمد، به ترتیب شاخص‌های نواندیشی و ابتکار با ۷۱/۱ درصد، شبکه‌های بومی و امن با ۶۹

درصد، سلامت اداری و اقتصادی با ۶۷/۷ درصد، فرصت سازی از تحریم‌ها با ۶۷ درصد و اهتمام به اقتصاد مقاومتی با ۶۴ درصد بالاترین میانگین شاخص‌ها را بین شاخص‌های ۱۰ گانه به خود اختصاص دادند.

در پاسخ به این سؤال که اساسی‌ترین چالش‌های دفاع سایبری در حوزه اقتصاد از منظر شما کدامند، به ترتیب وابستگی به سامانه‌های بانکی بین‌المللی از زیرساخت‌های اقتصادی را با ۶۶/۱ درصد، ضعف در تولید نرم افزارهای بومی امن و کارا با ۶۵/۸ درصد و استفاده غیرهوشمندانه از نرم افزارهای پیشرفته با ۶۵ درصد، استفاده غیرهوشمندانه از نرم افزارهای پیشرفته با ۶۵ درصد و بالاخره واگذاری خدمات زیرساختی حاکمیتی سایبری به بخش خصوصی با ۶۴/۲٪ بالاترین میانگین شاخص‌ها را میان شاخص‌های ۸ گانه احصاء شده به خود اختصاص داده‌اند.

در پاسخ به این سؤال که به نظر شما مهم‌ترین تهدیدات دفاع سایبری در حوزه اقتصاد کدام‌ها می‌باشند، اعضای جامعه نخبگی اظهار داشتند: از نظر آنان خرابکاری سیستم‌های نرم افزاری، سخت افزاری و داده‌ها با ۶۷/۵ درصد، افزایش حفره‌های امنیتی پنهان در نرم افزارها و سخت افزارها با ۶۷/۲ درصد، تحت تأثیر قرار دادن فعالیت بانکی سایبری کشور از طریق تحریم‌ها با ۶۴/۴ درصد، استفاده دشمن از سامانه‌های بانکی بین‌المللی علیه سامانه‌های اقتصادی با ۶۳/۱ درصد و حملات کشورهای متخاصم و نفوذ مستقیم به نرم افزارهای اقتصادی با ۶۲/۵ درصد از مهم‌ترین تهدیدات دفاع سایبری در حوزه اقتصاد برشمردند.

در پاسخ به این سؤال که به نظر شما که از اعضای جامعه نخبگی می‌باشید کدام شاخص‌ها را به‌عنوان اساسی‌ترین راهبردهای زیرساخت‌های اقتصادی ارزیابی می‌کنید، اظهار داشتند: افزایش قابلیت‌های دفاعی نظام سایبری اقتصادی کشور با ۷۹/۲ درصد، حمایت از تولید و به‌کارگیری نرم افزارهای بومی و امن با ۷۷/۵ درصد و تضمین استمرار خدمات بانکی بین‌المللی از طریق سامانه‌ها با همین امتیاز، پایش و شناخت محیط برای کنترل و مقابله از طریق رصد اطلاعاتی با ۷۶/۶ درصد و پایش و شناخت محیط برای کنترل و مقابله از طریق رصد اطلاعاتی با ۷۶/۱ درصد بالاترین میانگین شاخص‌ها را میان شاخص‌های احصاء شده ۱۰ گانه در این بخش به خود اختصاص داده‌اند.

در پاسخ به سؤال گویه‌های فرصت در زیرساخت‌های اقتصادی کشور، بر اساس تحقیق صورت گرفته از جامعه آماری از مجموع میانگین (۶۲/۶٪)، شاخص استفاده از تحریم‌های دشمن برای

تدوین الگوی طرح دفاع سایبری در برابر تهدیدات سایبری حوزه اقتصاد ۷۷♦

تقویت اقتصاد و تولید داخلی با ۶۲/۷ درصد، بیشترین و شاخص امکان تعامل دانشی با مؤسسات دانش‌بنیان خارجی با ۵۸/۱ کمترین میانگین شاخص‌های احصاء شده را به خود اختصاص داده‌اند و بالاخره اینکه در میان گویه‌های ضعف در زیرساخت‌های اقتصادی کشور بر اساس این تحقیق از مجموع میانگین (۶۶/۴٪)، وابستگی علمی سایبری در حوزه اقتصاد به خارج از کشور با ۷۳/۳ درصد بیشترین شاخص میانگین و شاخص ضعف آموزش کارکنان در مقابل تهدیدات محیطی با ۶۱/۶ درصد را به‌عنوان کمترین ضعف در زیرساخت‌های اقتصادی کشور دانسته‌اند.

و گویه‌های شاخص توسعه به‌کارگیری نرم افزارهای بومی در برخی زیرساخت‌های اقتصادی کشور با ۶۹/۴ درصد بیشترین شاخص میانگین قوت و وجود برخی از تجارب موفق در مقابله با تهدیدات سایبری اقتصادی با ۶۷/۷ درصد کمترین میانگین را به خود اختصاص دادند.

#### ۴) نتیجه‌گیری و پیشنهادات:

پس از انجام مطالعات اکتشافی و با استفاده از اسناد و مدارک معتبر که به منظور شناخت و احصاء مؤلفه‌ها و شاخص‌های مربوطه صورت گرفت، داده‌های به دست آمده با مراجعه محقق به جامعه خبرگی و آماری این تحقیق به شرح زیر به سؤال اصلی تحقیق پاسخ داده است:

الگوی طرح راهبردی دفاع سایبری کشور در برابر تهدیدات سایبری در حوزه اقتصادی چیست؟ سازمان‌دهی سازوکارها و تدبیر امور در حوزه فعالین اقتصادی بایستی به‌گونه‌ای صورت گیرد که پیگیری مبارزه با نظام سلطه از حوزه اقتصاد مصون باشد به بیان دیگر بایستی طراحی حوزه اقتصادی چنان باشد که دشمنان خارجی نتوانند با ابزار قرار دادن مسائل اقتصادی، جلو حرکت روبه جلوی کشور را بگیرند. این مسئله زمانی اهمیت بیشتری می‌یابد که توجه شود که حوزه اقتصاد، بزرگ‌ترین برگ برنده و مزیت نظام سلطه است و لذا می‌تواند از این مسیر نظام اسلامی را به‌شدت تهدید کند. لذا تدبیر در این خصوص از اهمیت شایان توجهی برخوردار است.

برای دستیابی به الگوی راهبردی طرح دفاع سایبری، منابع دینی، اسناد بالادستی، مبانی نظری، مطالعات تطبیقی و سایر مطالعات در حوزه اقتصادی انجام و اصول و ارزش‌های حاکم بر طرح، عوامل خارجی و داخلی مؤثر بر آن، چشم‌انداز و رسالت و مأموریت حوزه اقتصاد و قوت‌ها و ضعف‌های الگوی دفاع سایبری تعیین و راهبردهای دفاع سایبری و تجزیه و تحلیل داده‌ها بر اساس آن‌ها و با استفاده از نرم‌افزار EXCEL و نرم‌افزار SPSS احصاء شدند.

بر اساس مطالعات صورت گرفته از منابع دینی، اسناد بالادستی، منابع علمی، مبانی نظری، مطالعات تطبیقی و سایر مطالعات، اصول و ارزش‌های حاکم بر طرح راهبردی دفاع سایبری کشور در برابر تهدیدات سایبری در حوزه اقتصاد احصا که شامل ۱۱ مورد می‌شد که یک مورد رد و ۱۰ مورد باقیمانده تأیید شدند. این اصول و ارزش‌ها در جلسه خبرگی گروه مطالعاتی شهید صیاد شیرازی ارائه و سپس برای تعیین درجه اهمیت از طریق پرسشنامه در اختیار جامعه خبرگی قرار گرفته و همگی با میانگین حداقل ۵۴ و حداکثر ۷۱/۱ درصد تأیید شدند. اصول و ارزش‌هایی که با درصد بالایی مورد تأیید جامعه خبرگی قرار گرفتند عبارت‌اند از:

- برخورداری از شبکه‌های بومی و امن در حوزه زیرساخت‌های حیاتی و حساس با هدف توانایی برای جذب شوک یا ضربه و نیز خروج سریع از حالت اختلال
  - پایداری کارکردها بدین معنی که تمام زیرساخت‌های حیاتی و حساس کشور که به‌وسیله فضای سایبری کنترل و رهبری می‌شوند بایستی در این زمینه مشمول مراقبت‌های تخصصی و حفاظت شوند. به شکلی که در صورت بروز حمله سایبری هیچ‌کدام از شبکه‌های اصلی و عمده سایبری و زیرساختی کشور دچار قطع سرویس‌دهی و ارائه خدمات نشود. با پایدارسازی حوزه‌های اصلی کشور، برخورداری از معافیت‌ها و استفاده از بسته‌های تشویقی برای تولیدات داخلی می‌توان شرایط مناسبی برای دفاع سایبری در کشور ایجاد نمود.
  - ظرفیت‌های بومی صنعت سایبری:
- که قادر باشد در صورت مواجهه با تهدیدات سایبری و اعمال تحریم توسط کشورهای پیشرفته توان مقابله با آن‌ها را از طریق ظرفیت‌های بومی و تولید داخلی داشته باشد.
- اهتمام به اقتصاد مقاومتی که تئوری پردازی و مدل‌سازی مناسبی مبتنی بر آن صورت بگیرد، در این صورت فشارها و تحریم‌های خارجی به جای تهدید نظام اسلامی، به یک وضعیت مناسب برای پیشرفت کشور خصوصاً در حوزه اقتصادی تبدیل می‌شوند. زمانی می‌توان ادعا نمود که از فرصت تحریم‌ها علیه کشور استفاده مناسبی صورت پذیرفته است که اولاً در حوزه نظری طراحی و تئوری پردازی مناسبی صورت گرفته باشد. ثانیاً به لحاظ اجرایی و پیاده‌سازی، ساختارهای موجود در کشور با نهادهای مبتنی بر الگوی مقاومتی در شرایط تحریم جایگزین شده باشند. بر این مبنا یکی از نتایج پیگیری آن، مواجهه مثبت و فعال با فشارها و تحریم‌های خارجی است.

- خود اتکایی سایبری: بدین معنا که هر جامعه چه کوچک و چه بزرگ برای تأمین ملزومات مربوط به زیرساخت‌های حیاتی و حساس به‌ویژه نیازهای ضروری خود به این حوزه به دیگران، یا عرصه نظام بین‌الملل به دیگر کشورها نیاز نداشته باشد. خود اتکایی در زیرساخت‌های حیاتی و حساس در برابر تهدیدات فضای سایبری قطعاً با واکنش کشورهای سلطه‌گر مواجه خواهد شد.
- هدایت و کنترل متمرکز اقتصاد کشور در هر دو عرصه واقعی و مجازی نیاز به یک بخش راهبری و فرماندهی دارد تا با مدیریت پایش اقدامات و تفکرات دشمن و کشف آسیب‌پذیری‌ها، پرداخت و رفع آن‌ها از حوزه اقتصادی کشور، طراحی راهبردها به همراه ارائه راهکارهایی دقیق و همسو و هم‌افزا در بخش مؤلفه‌های اقتصادی و تجمیع قوا به منظور ایجاد نیروی لازم برای مقاومت با حضور مسئولان و متولیان دستگاه‌های اقتصادی، دفاعی و امنیتی با این ملاحظه که این مدیران می‌بایست به درک واحدی از جنگ و بحران اقتصادی برسند، از ملزومات است.
- فرصت‌سازی از تحریم‌ها: تحریم‌ها و فشارهای بین‌المللی اگرچه به‌عنوان چالش‌های مهم مطرح بوده و همواره به آسیب بیشتر به نظام اسلامی منجر می‌شوند، لیکن باید تغییر نقش داده و به‌عنوان عامل مثبت و تقویت‌کننده تبلور یابند. دلیل مهم این است که اجرایی‌سازی و پیاده‌سازی راهبردهای مبتنی بر الگوی اقتصاد مقاومتی نیازمند همراهی و همدلی سطوح مختلف حوزه تصمیم‌گیری و سیاست‌گذاری در کشور و همچنین پذیرش عمومی و همکاری توده‌های مردمی است و تشدید تحریم‌ها و فشارهای بین‌المللی خصوصاً در حوزه اقتصادی باعث می‌شود نیل به این وحدت و یکپارچگی در داخل کشور تقویت شده و اضطراب ناشی از اعمال این تحریم‌ها به سرعت بیشتر در تصمیم‌گیری و اجرایی‌سازی راهبردهای مبتنی بر اقتصاد مقاومتی منجر شود.
- کارآمدی سامانه‌ها: برخورداری از سامانه‌های امن و کارآمد در حوزه اقتصادی سایبری موجب حفظ ثروت عمومی و سرمایه‌های ملی در مقابل تهدیدات سایبری حوزه اقتصاد می‌گردد.
- سلامت اداری و اقتصادی: لازم‌ه فعالیت سالم و پرتحرک اقتصادی برخورداری از فضای امنی است که در جامعه ایجاد شده است و لازمه آن برخورد با مفسدان اقتصادی و افرادی است که قانون را دور می‌زنند.
- نواندیشی و ابتکار: نظام مقدس جمهوری اسلامی در مدیریت کشور در مقاطع مختلف از رویکردهای مختلفی در حوزه‌های گوناگون بهره‌مند بوده است که در صورت عدم جامعیت لازم و عدم برخورداری از

ظرفیت‌های نیروهای نواندیش و مبتکر در عرصه‌ها و موقعیت‌های مختلف با مشکلات فراوانی روبه‌رو می‌گردید که قطعاً این امر تأثیر فراوانی در اداره کشور به وجود می‌آورد.

در بررسی چشم‌انداز طرح راهبردی دفاع سایبری کشور در برابر تهدیدات سایبری در حوزه‌های اقتصادی ویژگی‌های زیر احصاء گردیدند:

(۱) بهره‌مند از فن‌آوری‌های بومی، آسیب‌ناپذیر و روزآمد و برخوردار از پویایی در زیرساخت‌های فنی سایبری حوزه اقتصاد.

(۲) برخوردار از نظامات سایبری اقتصادی خوداتکا در مقابله با تحریم‌ها و اقدامات دشمن در حوزه اقتصاد سایبری.

(۳) پایداری زیرساخت‌ها که اساس آن بهره‌مندی از زیرساخت‌های سایبری پایدار و آسیب‌ناپذیر در حوزه‌های اقتصادی (نظام پولی و بانکی) با قدرت مقاومت و پایداری بالا، خدشه‌ناپذیر همراه با تداوم کارکردی و طولی در برابر تهدیدات سایبری.

(۴) برخورداری از منابع انسانی ماهر، آموزش‌دیده، متخصص و مبتکر، هوشمند و ارزشی در حوزه دفاع سایبری اقتصادی.

(۵) کارآمدی سامانه: برخورداری از سامانه کارآمد، بومی و پاسخگو به نیازهای مردمی و اقتصادی کشور با قابلیت رقابت با رقبای جهانی.

(۶) فرماندهی و کنترل: دارای نظام فرماندهی و کنترل بومی، سازمان‌دهی شده و سلسله‌مراتبی در بررسی عوامل خارجی مؤثر در طرح راهبردی دفاع سایبری کشور در برابر تهدیدات سایبری در حوزه‌های اقتصادی، بر اساس مطالعات صورت گرفته، تهدیدات و فرصت‌های موجود احصا و ابتدا در جلسه خبرگی گروه مطالعاتی شهید صیاد شیرازی ارائه و پس از تأیید آن‌ها که بیانگر تهدیدهای قابل توجه در مقابل فرصت‌های اندک در این حوزه است، برای تعیین درجه اهمیت از طریق پرسشنامه در اختیار جامعه خبرگی قرار گرفت که نتیجه آن به شرح زیر است:

(۱) وضع قوانین و مقررات در مقیاس جهانی با شاخص پول‌شویی.

(۲) جلوگیری از انجام عملیات نقدینگی کشور در سطح بین‌الملل.

(۳) تحت تأثیر قرار دادن فعالیت بانکی سایبری کشور از طریق تحریم‌ها.

(۴) خرابکاری سیستم‌های نرم‌افزاری، سخت‌افزاری و داده‌ها.



- ۵) افزایش حفره‌های امنیتی پنهان در نرم افزارها و سخت افزارها.
  - ۶) اقدامات خصمانه خزانه‌داری آمریکا علیه حوزه اقتصادی.
  - ۷) اشراف حقوقی و مدیریتی آمریکا بر سیستم‌های اقتصادی.
  - ۸) حملات کشورهای متخاصم و نفوذ مستقیم به نرم افزاری اقتصاد.
  - ۹) استفاده دشمن از سامانه‌های بانکی بین‌المللی علیه سامانه‌های اقتصادی.
  - ۱۰) گردش پول ملی کشور در فضای سایبری.
- فرصت‌های احصاء شده نهایی:
- ۱) بحران‌ها و اختلافات مالی دشمن و متحدین در فضای سایبری.
  - ۲) استفاده از تحریم‌های دشمن برای تقویت اقتصاد و تولید داخلی.
  - ۳) امکان تعامل دانشی با مؤسسات دانش‌بنیان خارجی.
  - ۴) امکان استفاده از قوانین یک‌طرفه در کشورها.
- در بررسی عوامل داخلی مؤثر در طرح راهبردی دفاع سایبری کشور در برابر تهدیدات سایبری بر اساس مطالعات صورت گرفته، قوت‌ها و ضعف‌ها احصا و ابتدا در جلسه خبرگی گروه مطالعاتی شهید صیاد شیرازی ارائه و پس از تأیید آن‌ها که بیانگر این بود که در این حوزه ضعف‌ها بسیار بیش از قوت‌ها بوده، برای تعیین درجه اهمیت از طریق پرسشنامه در اختیار جامعه خبرگی قرار گرفت که نتیجه آن به ترتیب درجه اهمیت به شرح زیر است:
- ضعف‌ها:
- ۱) وابستگی علمی سایبری در حوزه اقتصاد به خارج از کشور.
  - ۲) خرابی عمده داده‌ها و اطلاعات از سوی منابعی مثل کارکنان.
  - ۳) عدم وجود نظام یکپارچه در دسترسی به اطلاعات.
  - ۴) وابستگی پول ملی کشور به فضای سایبری.
  - ۵) وجود نرم افزارهای یکپارچه در حوزه‌های پولی و بانکی.
  - ۶) وابستگی فن آورانه سایبری در حوزه اقتصاد به خارج از کشور.
  - ۷) ضعیف بودن نقش حاکمیتی وزارت اقتصاد برای مدیریت مناسب بین بانکی.
  - ۸) استفاده غیرهوشمندانه از نرم افزارهای پیشرفته اقتصادی بودن توجه به تهدیدات.
  - ۹) وابستگی دانشی سایبری در حوزه اقتصاد به خارج از کشور.

۵۸۲ فصلنامه امنیت ملی، سال ششم، شماره بیست و یکم، پاییز ۱۳۹۵

- ۱۰) ضعف در بعضی از سامانه‌های بازیابی اطلاعات و داده‌ها.
  - ۱۱) استفاده از فن‌آوری‌های بیگانه در حوزه سایبری اقتصاد.
  - ۱۲) ضعف آموزش کارکنان در مقابل تهدیدات محیطی.
- قوت‌ها:
- ۱) توانمندی موجود در بخش خصوصی در حوزه‌های سایبری.
  - ۲) توسعه به‌کارگیری نرم افزارهای بومی.
  - ۳) توسعه فن‌آوری جدید و بومی برای ارائه خدمات.
  - ۴) توجه به آموزش و تربیت نیروی انسانی متخصص در حوزه‌های سایبری.
  - ۵) وجود برخی از تجارب موفق در مقابله با تهدیدات سایبری اقتصادی.

پیشنهاد‌های پژوهشی:

۱- 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 الگوی ارائه‌شده، انجام شود.

۲- برای اجرایی شدن راهبردها و اراده راه‌کارهای اجرایی، تحقیقات دیگری انجام گیرد.

پیشنهاد‌های اجرایی:

- ۱- معاونت آموزش دانشگاه عالی دفاع ملی نتایج این پژوهش را به‌منظور ارزیابی و در صورت لزوم استفاده در اختیار قرارگاه پدافند غیرعامل ارائه نماید.
- ۲- معاونت آموزش دانشگاه عالی دفاع ملی نتایج این پژوهش را به‌منظور ارزیابی و در صورت لزوم استفاده در اختیار شورای عالی فضای مجازی قرار دهد.

## ۶) منابع و مآخذ:

- البرزی، محمود (۱۳۹۱) سیستمهای اطلاعات مدیریت رویکردی مدیریتی، انتشارات دانشگاه آزاد اسلامی، تهران
- جلالی فراهانی، امیرحسین، (۱۳۸۴)، پول شویی الکترونیکی، فقه و حقوق، دوره اول
- جلالی، علی اکبر (۱۳۹۳) عصر مجازی چهارمین موج تغییر؛ اینترنت.
- چشمه همیشه جاری (۱۳۹۲) انتشارات سازمان عقیدتی سیاسی ناجا، تهران، ص ۱۱
- چشمه همیشه جاری (۱۳۹۳) انتشارات سازمان عقیدتی سیاسی ناجا، تهران، ص ۲۸-۳۰
- حسن بیگی، ابراهیم. (۱۳۸۴)، توسعه شبکه ملی دیتا، چالش های فراروی امنیت ملی، فصلنامه مدیریت، شماره ۴۸
- رنجبر، محسن (۱۳۸۶) بررسی پدیده فرار سرمایه از ایران، پایان نامه کارشناسی ارشد دانشگاه تهران، دانشکده حقوق و علوم سیاسی
- سالیوانت، جان (۱۳۸۹)، راهبردهای حفاظت از زیرساخت های حیاتی (مترجم، محمدابراهیم نژاد)، تهران، انتشارات بوستان حمید؛
- سعیدی، علی اصغر (۱۳۸۵) روند پژوهی گفتمان های جهانی شدن، فصل نامه رشد آموزش علوم اجتماعی، شماره ۴، تابستان
- عزتی، مرتضی (۱۳۸۷) امنیت اقتصادی در ایران، تهران، انتشارات مجلس شورای اسلامی
- کارگروه مطالعاتی شهید صیاد شیرازی (۱۳۹۲)، تدوین طرح راهبردی دفاع سایبری کشور ج.ا.ا. در برابر تهدیدات، تهران، دانشگاه عالی دفاع ملی؛
- کهزادی، نوروز (۱۳۸۲) مدیریت ریسک در بانکداری الکترونیکی، چهاردهمین همایش بانکداری الکترونیکی
- گودرزی، آتوسا و فلاحتی، منیژه (۱۳۸۶) بیمه های الکترونیکی در ایران: الزامات، چالش ها و راهبردهای سیاستی، فصلنامه بررسی های بازرگانی، شماره ۲۴.
- ماندل، رابرت (۱۳۷۹) چهره متغیر امنیت ملی، پژوهشکده مطالعات راهبردی
- ماندل، رابرت (۱۳۷۹) چهره متغیر امنیت ملی، پژوهشکده مطالعات راهبردی
- مشرف جوادی، محمدحسین و بهزادفر، فاطمه و قوچی نژاد، حمزه (۱۳۸۹)، بانکداری الکترونیکی و چارچوب امنیتی آن، نشریه بانک و اقتصاد، شماره ۱۱۲

۸۴ فصلنامه امنیت ملی، سال ششم، شماره بیست و یکم، پاییز ۱۳۹۵

- مشرف جوادی، محمدحسین و بهزادفر، فاطمه و قوچی نژاد، حمزه (۱۳۸۹)، بانکداری الکترونیکی و چارچوب امنیتی آن، نشریه بانک و اقتصاد، شماره ۱۱۲
- مهندس پارسا، سازمان پدافند غیرعامل، مصاحبه خبرگی، دی ماه ۹۳
- مهندس فرجی پور، سازمان پدافند غیرعامل، مصاحبه خبرگی، دی ماه ۹۳
- نریمانی، میثم و عسکری، حسین (۱۳۹۰) چارچوب مفهومی اقتصاد مقاومتی، تهران، دبیرخانه اولین همایش ملی اقتصاد مقاومتی

### **منابع انگلیسی:**

- pinheiro'israel(1997) "consideration about exchanges controls capital flight and country risk.