Center for Strategic Studies of the
Islamic Republic of Iran Army

Journal Of
Army Strategic Research
Print ISSN:27834212
Volume 2, Issue 4
Summer 2023
P.P. 111-131

Investigation of Cyber Terrorism Threats against National and Defense Security of the Islamic Republic of Iran

Behzad Moradiyan [1] , Abdollah Jalali Nasab [2], Akbar Sosanjani [3]

Abstract

The development of information and communication technologies has expanded the scope of the Islamic Republic of Iran's defense concerns in cyberspace and has radically changed the nature, tools, and methods of warfare, resulting in a variety of military, security, political, economic and social threats. New Interests of Dominant powers to taking advantage of the Capacities and Capabilities of Cyberspace to Cultivate Dense, Ethnic, Sectional, Social Tensions, and Build Distrust between Society and Sovereignty and Network-Tactical Invasion Aiming to Disrupt the Management of Current Affairs, make Cyber Terrorism as One of the Most Threats. The present article attempts to provide appropriate policy and strategic platforms for policymakers to exploit cyberspace capabilities to counter threats as well as identify vulnerabilities in all of them. . On the other hand, in the current research, the researchers attempt to analyze and investigate the causes and factors affecting the emergence of cyber threats in the national and defense security of the Islamic Republic of Iran, taking into consideration the existing facts and challenges. Therefore, the method of this research is descriptive-analytical and the important findings of this article are familiarity with different aspects of cyber-terrorism threats, constructive strategies and suggestions in this field. The results of this study indicate the consistency of received responses, which may also contribute to increased cyber defense in defense and security active organizations in the Islamic Republic of Iran.

Keywords: cyber, cyber terrorism, threat, security, national security

Citation: Moradiyan ,Behzad; Jalali Nasab, Abdollah; Sosanjani ,Akbar.(2023). Investigation of Cyber Terrorism Threats against National and Defense Security of the Islamic Republic of Iran. *Journal Of Army Strategic Research, 2(4), 111-131.*

1-PhD.Political Science. AIU Khorasgan Branche . Iran. behzadmoradian12@yahoo.com
2-PhD. G.I.S. Tarbiat Modarres University. Tehran. Iran.
3-MA .Defense Management .Dafos Aja. Tehran. Iran.

Received: 2023/04/06
Accepted: 2023/06/09

Article Type : Research - based

مرکز مطالعات راهبردی

فصلنامه پژوهش‌های راهبردی ارتش
شاپای انتشار: ۲۷۸۳۴۲۱۲
سال دوم، شماره چهارم
تابستان ۱۴۰۲
صص: ۱۳۱-۱۱۱

واکاوی تهدیدهای سایبرتروریسم علیه امنیت ملّی و دفاعی جمهوری اسلامی ایران

بهزاد مرادیان [۱]، عبدالله جلالی نسب [۲] ، اکبر سوسنجانی [۳]

چکیده

گسترش فناوری‌های اطلاعات و ارتباطات، دامنه‌ی ملاحظات دفاعی جمهوری اسلامی ایران در فضای مجازی را گسترش داده و با تغییر بنیادین ماهیت، ابزار و روش‌های نوین جنگی موجب تحول در گونه‌های مختلف تهدیدهای نظامی، امنیتی، سیاسی، اقتصادی و اجتماعی شده است. در این مقاله سعی شده تا برای دستگاه‌های سیاست‌گذار، بسترهای ستادی و استراتژیک مناسبی به‌منظور بهره‌گیری از قابلیت‌های فضای مجازی برای خنثی‌سازی تهدیدات و همچنین شناخت آسیب‌پذیری‌ها را در همه‌ی ابعاد آن، فراهم نمایند. از طرفی دیگر در تحقیق پیش رو، پژوهش‌گران سعی در واکاوی و بررسی علل و عوامل مؤثر در پیدایش تهدیدات سایبری در امنیت ملّی و دفاعی جمهوری اسلامی ایران با در نظر گرفتن واقعیت‌ها و چالش‌های موجود را مورد واکاوی قرار دهند. لذا روش اجرای این تحقیق، توصیفی- تحلیلی بوده و یافته‌های مهم مقاله‌ی مورد بحث، آشنایی با ابعاد مختلف تهدیدات فضای «سایبرتروریسم»، راه‌کارها و پیشنهادهای سازنده در این زمینه می‌باشد. نتایج این تحقیق نشان از انطباق پاسخ‌های دریافتی داشته که این مهم می‌تواند در افزایش دفاع سایبری سازمان‌های دفاعی و امنیتی فعال در کشور جمهوری اسلامی ایران، نیز مؤثر واقع شود.

واژگان کلیدی: سایبر، سایبرتروریسم، تهدید، امنیت، امنیت ملّی.

استناد : مرادیان بهزاد ، جلالی نسب عبدالله و سوسنجانی اکبر (۱۴۰۲). واکاوی تهدیدهای سایبرتروریسم علیه امنیت ملّی و دفاعی جمهوری اسلامی ایران. *فصلنامه مطالعات راهبردی ارتش، ۲ (۴)، ۱۳۱-۱۱۱.*

۱- دانش آموخته دکتری. علوم سیاسی.دانشگاه آزاد اسلامی خوراسگان اصفهان. ایران(نویسنده مسئول)
behzadmoradian12@yahoo.com
۲- دانش آموخته دکتری. - جی آی اس (G.I.S)، دانشگاه تربیت مدرس. تهران. ایران.
۳- دانش آموخته دکتری. مدیریت . دانشگاه عالی دفاع ملی. تهران. ایران.

نوع مقاله: پژوهشی

تاریخ دریافت: ۱۴۰۲/۰۱/۱۷
تاریخ پذیرش: ۱۴۰۲/۰۳/۱۹

مقدمه

واژه‌ی فضای سایبر را نخستین بار «ویلیام گیبسون»نویسنده‌ی داستان علمی- تخیلی در کتاب «نورومنسر»در سال ۱۹۸۴م. به کار برد. امروزه در هزاره‌ی جدید، جامعه‌ی اطلاعاتی در حال تبدیل به یک جامعه‌ی جهانی بوده و رشد تجارت الکترونیک، باعث توسعه‌ی بازارهای جدید صنعتی به‌صورت یک‌پارچه و جهانی‌شدن است. این درحالی است که این جامعه‌ی اطلاعاتی، روی چهارچوب بسیار آسیب‌پذیر اینترنت ساخته شده و اینترنت در معرض خطر «حملات سایبری» است. اکنون جامعه‌ی مدرن ما، از بسیاری جنبه‌ها به فنّاوری اطلاعات به‌صورت مستقیم یا غیر مستقیم وابسته است و این یعنی به‌خطرافتادن دسترس‌پذیری و صحت اطلاعات در سیستم‌ها و زیرساخت‌ها مانند بانک‌داری، دولت الکترونیک، ارتباطات و ... که می‌تواند پیامدهای ناگواری از بُعد امنیتی به دنبال داشته باشند. یکی از اهداف مهم در مورد توجه به تهدیدات سایبری، توجه ویژه به اصول و ضوابط مقابله با تهدیدات نرم‌افزاری و الکترونیکی و سایر تهدیدات جدید به‌منظور حفظ و صیانت شبکه‌های اطلاع‌رسانی، مخابراتی و رایانه‌ای می‌باشد. بسیاری از سازمان‌ها- به‌خصوص سازمان‌های امنیتی و دفاعی در کشور جمهوری اسلامی ایران- به دنبال ایجاد سیستم‌های امن برای جلوگیری از نشت اطلاعات به بیرون هستند تا بتوانند کل مجموعه‌ی خود را حفظ کنند. در این راستا، ایجاد یک سیستم امنیتی قوی می‌تواند برای حفظ امنیت اطلاعات هر سازمان مؤثر واقع شود. سیستمی که بر اساس نیازهای سازمان و میزان اهمیت اطلاعات در آن طراحی شده باشد و از سرمایه‌های اطلاعاتی، حفاظت کند. شبکه‌های اجتماعی مجازی را در حال حاضر می‌توان یکی از مهم‌ترین جلوه‌های دگرگونی در ساختار فضای سایبر در نظر گرفت. از سال ۲۰۰۶م. که شبکه‌ی «فیس بوک» به‌عنوان مهم‌ترین شبکه‌ی اجتماعی مجازی راه‌اندازی شد، تاکنون که بیش از یک میلیارد عضو دارد تا حالا هیچ شبکه‌ی دیگری به این سرعت و وسعت رشد نکرده ست. در واقع این شبکه‌ها در ابتدا با هدف ارتباطات ایجاد شدند؛ ولی در نهایت خود به عاملّی در جهت پخش و کنترل اطلاعات، مبدل گردیدند.

با این وجود، شناسایی تهدید از نظر شدّت، ضعف و انواع مختلف آن نیز مقوله‌ای دائمی است و آمادگی سازمان‌ها و کشورها به‌منظور دفع آن، اقدامی منطقی و عقلایی بوده و در دنیای پیچیده‌ی کنونی، از ضرورت‌های اساسی ملت‌ها و مسئولیت اصلی مدیران سازمان‌ها محسوب می‌شود؛ چراکه پیچیدگی این تحولات روزبه‌روز بیشتر شده و شکل جنگ‌های آینده را از

حاکمیت مطلق تاکتیک‌ها و استراتژی‌های نظامیِ سنتی خارج ساخته و حوزه‌ی نفوذ و تأثیر عوامل تکنولوژیکی، اقتصادی، روانی، فرهنگی، سیاسی و امثالهم را به‌شدّت گسترش داده است. بروز تغییرات اساسی در مؤلفه‌های قدرت و حاکمیت در واحدهای سیاسی نیز با توجه به تحولات به وجود آمده‌ی اخیر در نظام بین‌الملل، مفهوم و نحوه‌ی برخورد با تهدیدها را دگرگون کرده است.(مرادیان و دیگران، ۱۳۹۷: ۹۸) علت بیان مقوله‌ی اخیر نیز این است که نظریه‌پردازان غربی به‌ویژه ایالات متحده‌ی امریکا در سده‌ی اخیر همواره درپی ایجاد، ساخت و حتی تولید تهدید علیه امنیت ملّی کشورهای هدف ازجمله ایران جهت تحفظ منافع ملّی خود بودند.(تاجابادی و دیگران، ۱۳۹۴: ۷۳) به طور مثال در اوایل قرن بیستم، کشوری به مثابه‌ی ایران نقش حائل بین روسیه و انگلستان را بازی می‌کرد و از مهم‌ترین کانون‌های رقابت جهانی به شمار می‌رفت. پس از جنگ جهانی دوم و با شکل‌گیری نظام دوقطبی، بر اهمیت این جایگاه افزوده شد؛ لذا با الهام از انگیزه‌های «سِر جان هالفورد مکیندر» انگلیسی و «نیکلاس اسپایکمن» امریکایی، سیاست تهدید و محصورسازی توسط «جرج کنان»۱ ارائه شد و کشور ایران نقش دفاعی برای قدرت بحری را یافت و یکی از حلقه‌های مهم سیاست سدّ نفوذ کمونیست به حساب آمد. در این حال با ارائه‌ی تئوری «ریملند» در مباحث ژئوپلیتیک، ایران از اهمیت بالایی برخوردار شد. سرزمین‌های حاشیه‌ای اروپا، خاورمیانه، آسیای جنوبی و خاور دور از منظر اسپایکمن دارای اهمیت بالایی در نظریه‌ی ریملند بودند و به زعم آنان همه‌ی این‌ها، کلیدهای امنیت امریکا محسوب می‌گردید.(حیدری و دیگران، ۱۳۹۸: ۴۳)

با بررسی و واکاوی فضای سایبر به این مهم دست خواهیم یافت که در هنگام دستیابی افراد و کاربران به فضای مجازی، به طور حتم تهدیدات سایبری با تأثیرگذاری بالا، در کمین افراد و سازمان‌ها برای تحقق اهداف خود با این نیّت که امنیت و محافظت کارآیی خود را از دست داده، خواهند بود. آنان وجوه مختلفی از حملات خود را طراحی کرده و سعی در ورود به حریم افراد و ادارات را به‌صورت کامل دارند. ساده‌لوحانه است اگر برای جلوگیری از این خطر حتمی، فقط به یک بُعد این فضا توجه شود. متأسفانه در کشور ما وقتی سخن از فعالیت در فضای مجازی می‌شود، بسیاری از افراد وب سایت‌ها را مدّ نظر گرفته و برخی از نسل جدید ممکن است شبکه‌های اجتماعی را به یاد بیاورند؛ اما غافل از اینکه فضای مجازی روزبه‌روز توسعه می‌یابد و عرصه‌های خود را مانند تارهای عنکبوت گسترده‌تر می‌کند تا جایی که زندگی

1 George Kennan

مجازی و حقیقی یک فرد و یا یک سازمان و حتی امنیت ملّی یک کشور را به دست می‌گیرد. گسترش فنّاوری های اطلاعات و ارتباطات، دامنه‌ی ملاحظات امنیتی و دفاعی جمهوری اسلامی ایران در فضای مجازی را گسترش داده و با تغییر بنیادین ماهیت، ابزار و روش‌های نوین جنگی، موجب تحول در گونه‌های مختلف تهدیدهای نظامی، امنیتی، سیاسی، اقتصادی و اجتماعی شده است. لذا با عنایت به توجه نظام سلطه بر بهره‌گیری از ظرفیت‌ها و قابلیت‌های فضای مجازی سایبری به‌منظور تنش‌سازی متراکم و گسترده‌ی قومی، فرقه‌ای، اجتماعی و ایجاد بی‌اعتمادی میان جامعه و حاکمیت و تهاجم شبکه‌ای تاکتیکی با هدف مختل‌سازی مدیریت امور جاری کشور، مسئله‌ی اصلی در این تحقیق این خواهد بود که چگونه تهدیدات سایبری یکی از مهم‌ترین تهدیداتی است که می‌تواند امنیت ملّی جمهوری اسلامی را با چالش جدّی مواجه سازد.

امروزه با کوچک‌تر و پیچیده‌ترشدن جهان به‌واسطه‌ی رشد روزافزون وسایل ارتباط‌جمعی از قبیل اینترنت و ماهواره، معادلات گذشته در تنظیم روابط بین کشورها تا حدود زیادی به هم خورده و جای خود را به معادلات جدیدی داده است؛ به گونه‌ای که به جای به‌کارگیری مستقیم زور، توجه قدرت‌ها به استفاده از قدرت نرم و ایجاد تغییرات از طریق مسالمت‌آمیز با به‌کارگیری شیوه‌های نوین مداخله در امور داخلی کشورها جلب شده است. یکی از ابزارهای مهم در این راستا، سایت‌های شبکه‌های اجتماعی اینترنتی و شبکه‌های وبلاگی هستند. یکی از راه‌های مطمئن مقابله با تهدیدات سایبری و کاهش صدمات و خسارات ناشی از این تهاجمات، توجه به امور دفاعی در همه‌ی ابعاد و حوزه‌ها به‌خصوص حوزه‌ی ارتباطات و فنّاوری می‌باشد؛ لذا نقش فزاینده‌ی فنّاوری‌های بنیادین فضای مجازی در فرهنگ و حیات اجتماعی و تأثیرگذاری آن بر کیفیت و الگوهای تعاملّی میان دولت‌ها حتی در سطوح مختلف روابط بین‌المللی، ماهیت تهدیدها (اهمیت‌یافتن تهدیدهای نرم در مقابل تهدیدهای سخت و امنیت نرم در مقابل امنیت سخت) بیانگر آن است که محیط تهدیدآفرین علیه امنیت ملّی کشور و حتی علیه سازمان‌های مهم امنیتی و دفاعی، دیگر محدود به جهان واقعی نیست؛ بلکه جهان مجازی نیز همپای جهان واقعی، محیطی تهدیدزا از قبیل تهدیدهای سایبرتروریسم برای آنان را به ارمغان آورده است که می‌تواند در مواقع حساس و خطرناک ضمن ایجاد تهدید امنیتی و حتی تهدید دفاعی، مورد بهره‌برداری وسیع قرار گیرد. بنابراین عدم برآورد تهدیدهای آتی که می‌تواند اثر منفی بر اجرای مأموریت‌های کلان کشور بگذارد، همواره دغدغه‌ی اصلی و مستمر مسئولین و مدیران و حتی

فرماندهان نیروهای مسلح جمهوری اسلامی ایران بوده است. با توجه به این موضوع، انجام تحقیق حاضر کمک خواهد نمود تا مسئله‌ی حائز اهمیت این پژوهش یعنی «واکاوی تهدیدهای سایبرتروریسم علیه امنیت ملّی و دفاعی جمهوری اسلامی ایران» مورد بررسی و واکاوی قرار گیرد تا بر اساس آن در نهایت، اقتدار و تسلط بر حوزه‌های مختلف دفاعی و امنیتی کشور جمهوری اسلامی ایران محقق شود.

تهدید یعنی اقدام علیه یک کشور که جنبه‌ی بیرونی داشته و از فعّال‌شدن عوامل بیرونی و ضد امنیت ملّی حکایت دارد. تهدید به دو دسته‌ی درونی و بیرونی تقسیم می‌شود.(افتخاری، ۱۳۸۱: ۵) (تصور ما از تهدید، بخشی از تصور کلان‌تر که همان تصور ما از دیگران باشد، است. یعنی نخست ما دیگری را به‌عنوان مخالف خود به تصویر می‌کشیم و سپس از درون آن تصویر کلان، به تصویر خُردتر تهدید می‌رسیم.(مرادیان و دیگران، ۱۳۹۷: ۱۰۱)

سایبر واژه‌ای یونانی به معنای سکان‌دار و راهنماست. امروزه این کلمه به معنی مجازی نیز به کار می‌رود و منظور از ارتش سایبری نیز همان ارتش مجازی است.(ونتر، ۲۰۱۱؛۱۸۸) سایبرتروریسم نیز حاصل هم‌گرایی تروریسم و فضای مجازی است. سایبرتروریسم به معنای تهاجم و تهدید به تهاجم غیرقانونی به رایانه‌ها، شبکه‌ها و اطلاعات ذخیره‌شده در آن‌هاست که به‌منظور ارعاب یا وادارکردن یک دولت یا مردم آن که برای پیشبرد اهداف سیاسی یا اجتماعی خاص صورت می‌گیرد.

دفاع :امروزه مفهوم دفاع، سابقه‌ای به قدمت دولت‌ها دارد و همواره با آن‌ها قرین بوده است، به گونه‌ای که برخـی اندیشمندان، فلسفه‌ی وجودی و علت پیدایش دولت را دفاع از کشور بیان نموده‌اند. دفاع در لغت به معنی دفع‌کردن است و به‌طورکلی به مجموعه اقدامات و اعمالی که برای دورنمودن و یا ازبین‌بردن خطر و یا تهدید صورت می‌گیرد، دفاع گفته می‌شود.(عسکری و همکاران، ۱۳۹۱: ۱۲) دفاع جزیی از هویت یک ملت زنده است.(دفتر واژه‌گزینی نظامی دانشگاه عالی دفاع ملی و تحقیقات راهبردی، ۱۳۹۷: ۳۰۶)

امنیّت از سال ۱۹۹۱م. به‌صورت یک مفهوم مورد اختلاف و جدل در روابط بین‌الملل در آمده است.(شیهان، ۱۳۸۸: ۱۳) به‌هرحال واژه امنیّت دارای دو معنای ایجابی و سلبی است که ایجابی یعنی «وجود احساس رضایت و اطمینان خاطر نزد دولت‌مردان و شهروندان» و سلبی یعنی «نبود ترس، اجبار و تهدید.» پس می‌توان گفت که امنیّت عبارت است از «رهایی از وحشت، خوف، خطر و داشتن آرامش و اطمینان در حراست و صیانت از ارزش‌ها و منافع

حیاتی کشور.»(جعفری، ۱۳۹۲: ۱۷۲) و یا در تعریفی ساده‌تر، امنیت عبارت است از «احساس آسایش خاطر و نبود هراس از تهدید و به‌خطرافتادن ارزش‌ها، اهداف و منافع و ایمن‌بودن از تهدید و هجوم دشمن.» (دفتر واژه‌گزینی نظامی دانشگاه عالی دفاع ملی و تحقیقات راهبردی، ۱۳۹۷: ۱۲۲)

امنیّت ملّی:واقع‌گرایی مانند «هانس جی مورگنتا» که از نظریه‌پردازان مطرح غربی در مباحث روابط بین‌الملل و علوم سیاسی به شمار می‌رود، امنیّت ملّی را هم‌معنای قدرت نظامی در نظر گرفته است. او معتقد است که کشمکش بر سر قدرت، هدف دولت‌مردان در بحث امنیّت ملّی است.(نای، ۱۳۸۷: ۱۲۴) البته «باری‌بوزان»1نیز که تئوری‌پرداز قابلی در مکتب کپنهاگ بوده، اعتقاد دارد: «امنیّت ملّی از نظر مفهومی، ضعیف و از نظر تعریف، مبهم و از نظر سیاسی، مفهومی قدرتمند است.» بنابراین امنیّت ملّی عبارت است از «وضعیتی که در آن یک کشور نسبت به منافع و ارزش‌های حیاتی خود، تهدید جـدّی احساس نکند.»(تقی‌پور، ۱۳۸۷: ۲۹۰) و یا تعریفی دیگر می‌گوید «امنیّت ملّی عبارت است از: توانایی یـک کشور در دفع تهدیدهای خارجی، علیه حیاتِ سیاسی یا منافع ملّی.»(مرادیان، ۱۳۸۹: ۱۴۸)

امروزه با وجود افزایش اهمیت امنیت در جوامع ابزار، شیوه‌ها و رویکردهای ایجاد و حفظ آن دستخوش تحول شده است. از این رو از دغدغه‌های مشترک کشورها که همواره دولت‌ها را وادار به تهیه‌ی سازوکارهای دفاعی می‌کنند، حفظ امنیت ملّی و داشتن نگرانی از تهدید است. این تهدیدها می‌توانند منشاء داخلی یا خارجی داشته باشند و حتی می‌توانند در قالب‌های نظامی، فرهنگی، اقتصادی، سیاسی و ... شکل گیرند.(مرادیان و دیگران، ۱۳۹۷: ۹۶) از طرفی دیگر، گسترش فنّاوری‌های اطلاعاتی و ارتباطاتی، دامنه‌ی ملاحظات امنیتی و دفاعی جمهوری اسلامی ایران را در فضای مجازی گسترش داده و با تغییر بنیادین ماهیت، ابزار و روش‌های نوین جنگی موجب تحول در روش‌های مختلف تهدیدات از قبیل نظامی، امنیتی، سیاسی، اقتصادی و اجتماعی شده است. با توجه به تأکید نظام سلطه بر بهره‌گیری از ظرفیت‌ها و قابلیت‌های فضای مجازی به‌منظور تنش‌سازی متراکم و گسترده‌ی قومی، فرقه‌ای، اجتماعی و ایجاد بی‌اعتمادی میان جامعه و حاکمیت و تهاجم شبکه‌ای تاکتیکی با هدف مختل‌سازی مدیریت امور جاری کشور؛ سایبرتروریسم یکی از مهم‌ترین تهدیداتی است که می‌تواند امنیت ملّی جمهوری اسلامی ایران را با چالشی جدی مواجه سازد. این امر ایجاب می‌کند تا

1. Barry Buzan

دستگاه‌های سیاست‌گذاری با رویکردی آفندی و پدافندی، بسترهای ستادی و استراتژیک خود را به‌منظور بهره‌گیری از قابلیت‌های فضای مجازی برای خنثی‌سازی تهدیدات و شناخت آسیب‌پذیری‌های بالقوه فراهم کنند. فنّاوری‌های نوین اطلاعاتی و ارتباطی، ازجمله اینترنت این امکان را فراهم می‌کند تا کنشگران در بستر و محیط جدیدی به تعامل بپردازند که «فضای مجازی» نامیده می‌شود. فضای مجازی مجموعه‌ای از ارتباطات بین انسان‌ها از طریق رایانه و وسایل مخابراتی بدون درنظرگرفتن جغرافیای فیزیکی به شمار می‌رود. نقش فزاینده‌ی فنّاوری‌های بنیادین فضای مجازی در فرهنگ و حیات اجتماعی و تأثیرگذاری آن بر کیفیت و الگوهای تعاملّی میان دولت‌ها و ماهیت تهدیدات بیانگر آن است که محیط تهدیدآفرین علیه امنیت ملّی دولت‌ها، دیگر محدود به جهان واقعی نیست؛ بلکه جهان مجازی نیز همپای جهان واقعی، محیطی تهدیدزا برای دولت‌هاست که می‌تواند به‌وسیله‌ی کنشگران دولتی و غیر دولتی مورد بهره‌برداری قرار گیرد. از آن جا که ما به تهدیدات سایبر علیه امنیت ملّی توجه داریم، باید مباحث خود را بر فنّاوری‌های مرتبط با ظهور تهدیدات نوین، یعنی روش‌ها، ابزارها و مهارت‌ها متمرکز کنیم. ویژگی‌های بی‌همتای فنّاوری‌های اطلاعات و ارتباطات، تحولات بنیادینی را در قلمرو حیات بشری پدید آورده است. نخستین ویژگی آن گسترش این فناوری‌ها است. این ویژگی باعث گردیده است، فناوری‌های اطلاعات و ارتباطات نفوذ جهان گسترانه‌ای به دست آورند و در یک گستره‌ی جغرافیایی خاص و محدود نگنجند. به عبارت بهتر، فنّاوری‌ها تمامی مرزها را در می‌نوردند.(Everard.J, 2000: 62) دومین ویژگی مهم و چشمگیر فنّاوری‌های اطلاعات و ارتباطات، کنترل‌ناپذیری و لجام‌گسیختگی آن است. در واقع امروزه گسترش فنّاوری‌های اطلاعات و ارتباطات به گونه‌ای است که در بسیاری از موارد حتی عاملان گسترش و زمینه‌سازان آن نیز نمی‌توانند آن را در کنترل خود درآورند.(Cavelty.M.D, 2008: 67) سومین ویژگی که پیوند تنگاتنگی با ویژگی دوم دارد و البته سایر ویژگی‌های فنّاوری‌های اطلاعات و ارتباطات را تحت‌الشعاع قرار می‌دهد، قاعده‌گریزی در این پدیده است. این ویژگی به علت وجود ماهیت شبکه‌ای آن است که نوعی وضعیت و شرایط غیر سلسله‌مراتبی را در عرصه‌ای که حضور می‌یابد و به فعالیت می‌پردازد، می‌آفریند.(Mesko.G, 2006: 81) چهارمین ویژگی فنّاوری‌های اطلاعات و ارتباطات که خصوصیتی بدیع و بدعت‌زا نیز به شمار می‌آید، ایجاد و گسترش دنیای مجازی است(روزنا، ۱۳۹۰: ۶۳). این ویژگی از بُعد امنیت، جهان را به دو ناحیه تقسیم نموده است(روزنا، ۱۳۹۰: ۶۳):

الف) دنیای واقعی

ب) دنیای مجازی

دنیای واقعی همان عرصه‌ی سنتی امنیت است و دنیای مجازی، عرصه‌ای است که گسترش فنّاوری‌های اطلاعات و ارتباطات هر روز بر اهمیت و تأثیرگذاری آن می‌افزاید، به گونه‌ای که در حال حاضر رویدادهای دنیای مجازی بر جهان واقعی سایه می‌افکند. به دنبال افزایش اهمیت و تأثیرگذاری دنیای مجازی، «تهدیدهای مجازی»1 نیز ظهور کرد و شدت گرفت. ظهور و شدت‌گیری تهدیدهای مجازی به صورتی در آمده است که کنشگران موجود، نمی‌توانند به طور کامل با آن‌ها مقابله کنند و در نتیجه کنشگران غیردولتی همچون گروه‌های تروریستی از این قابلیت و توانمندی برخوردار شده‌اند که ثبات و نظم بین‌المللی و امنیت ملّی دولت‌ها و سازمان‌ها را مورد تهدید قرار دهند. بهره‌گیری گروه‌های تروریستی از امکانات فضای مجازی، نوع جدیدی از تهدید را پدید می‌آورد که از آن به «سایبر تروریسم» تعبیر می‌شود.((Cavelty.M.D2008:10)

ویژگی‌های فضای مجازی(سایبری)

در هزاره‌ی سوم، فضای مجازی(سایبر) ویژگی‌هایی دارد که آن را برای تروریست‌ها جذاب می‌کند.(جدول شماره‌ی۱-۲) برخی از مهم‌ترین ویژگی‌های فضای مجازی که توجه تروریست‌ها، چه از جانب بازیگران دولتی و چه غیردولتی را به خود جلب کرده و موجب شده است بر اثر به‌وجودآمدن تهدیدهای بالقوه‌ی سایبری، کنشگران دولتی و غیردولتی، خط مشی‌های خود را تغییر دهند و از دنیای فیزیکی به فضای مجازی روی آورند، عبارتند از: (Hancock.B, 2001: 554)

جدول شماره‌ی ۱: ویژگی‌های فضای مجازی(Hancock.B, 2001: 555)

ردیف	ویژگی‌های فضای مجازی
۱	نبود مرز ثابت و ناتوانی دولت‌ها در کنترل آن
۲	کاهش هزینه‌ی جرم
۳	امکان واردآوردن خسارات مالی، بدون رساندن آسیب‌های جسمی
۴	سهولت تدارک امکانات و عوامل مورد نیاز برای اقدامات تروریستی
۵	امکان هماهنگی لحظه‌ای عملیات توئسط تروریست‌های سایبری
۶	انجام بهینه و سریع فعالیت‌های پولی و بانکی

1 Virtual Threats

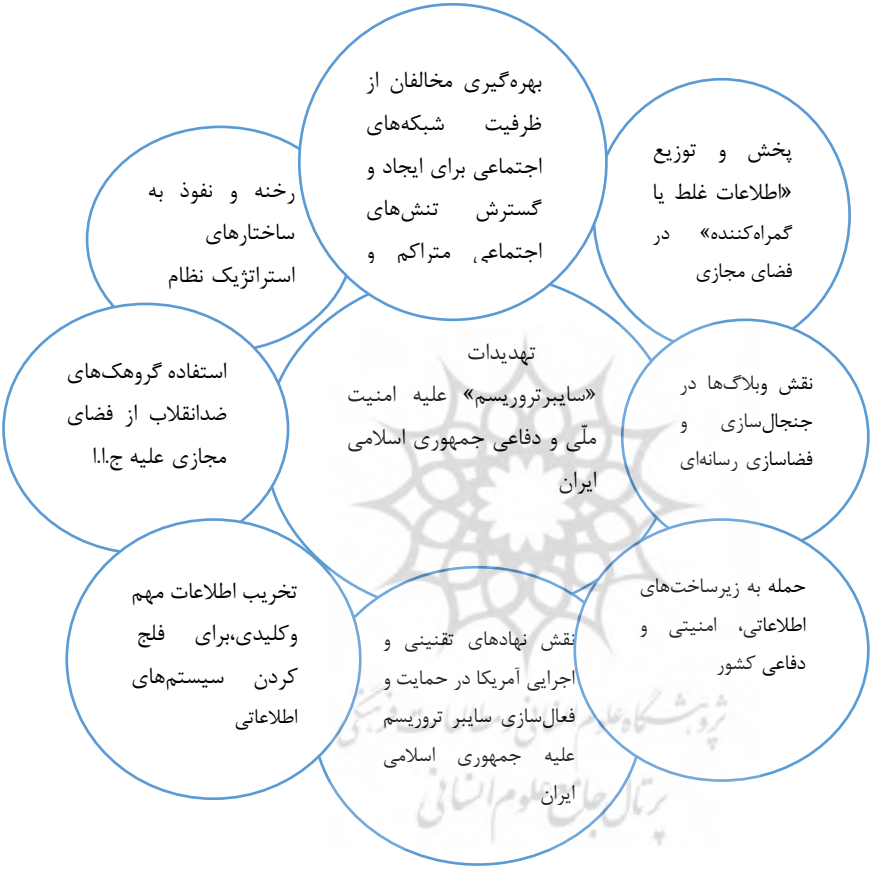
ظهور تهدیدات سایبرتروریسم علیه امنیت ملّی و دفاعی جمهوری اسلامی ایران

در حال حاضر، تهدیدات به نوبه‌ی خود تابعی از قدرت، مجاورت، قابلیت تهاجمی و تمایلات تهاجمی به شمار می‌روند؛ لذا با یکسان‌بودن تمام شرایط مورد اشاره، افزایش در هر یک از عوامل فوق موجب می‌شود تا سایر کشورها به‌ویژه کشورهای بزرگ و صاحب قدرت، دارندگان این صفات را تهدیدآمیز انگاشته و درصدد موازنه با آن‌ها برآیند. استفان والت در نظریه توازن تهدید، چهار معیار برای ارزیابی تهدید مشخص می‌کند که عبارتند از: قدرت(اندازه، جمعیت، ثروت، قدرت اقتصادی، توان نظامی)؛ مجاورت یا نزدیکی جغرافیایی، توانایی تهاجم؛ قصد یا نیت تهاجم که بر اساس توانایی تهاجم، کشورهایی که قابلیت خاص نظامی مانند نیروهای بسیار متحرک یا قابلیت‌های سیاسی مانند یک ایدئولوژی بالقوه سرایت کننده و تهاجمی دارند و یکپارچگی قلمرو یا ثبات سیاسی سایر کشورها را نشانه رفته باشند، بیشتر تهدیدآمیز جلوه می‌کنند. علاوه بر قدرت که به‌عنوان بارزترین معیار برای ارزیابی تهدید مطرح می‌گردد، مجاورت در اعمال قدرت به دلیل کوتاه‌بودن بُعد مسافت، در تهدیدآمیزبودن یا نبودن یک کشور نقش دارد.(مرادیان و دیگران، ۱۳۹۷: ۱۰۵)

با این حال، یکی از شاخص‌های تهدیدآمیز در محیط امنیتی و پیرامونی جمهوری اسلامی ایران، تعدد و تکثر گروه‌های تروریستی و منازعات قومی- فرقه‌ای است. از مهم‌ترین گروه‌های تروریستی فعال در محیط امنیتی کشور ایران می‌توان به گروهک تروریستی القاعده، حزب کارگران کردستان ترکیه(پ.ک.ک) و شاخه‌ی ضد ایرانی آن یعنی پژاک، انصارالاسلام، جندالله، لشکر طیبه، سپاه صحابه، سازمان مجاهدین خلق(منافقین) و داعش(دولت اسلامی عراق و شام) اشاره کرد. گروه‌های تروریستی با بهره‌گیری از ابزارها و شیوه‌هایی مانند قتل، گروگان‌گیری، بمب‌گذاری و عملیات انتحاری در صدد بی‌ثبات‌سازی و ایجاد اخلال در نظم و امنیت عمومی جامعه‌ی کنونی جمهوری اسلامی ایران هستند. یکی از مهم‌ترین ویژگی گروه‌های تروریستی علیه جمهوری اسلامی ایران آن است که این گروه‌ها از سوی بازیگران منطقه‌ای و فرامنطقه‌ای مخالف ایران، ازجمله ایالات متحده امریکا مورد حمایت مالی، سازمانی و تسلیحاتی قرار می‌گیرند و از این منظر تهدید و مسئله‌ای جدی و بسیار مهم برای امنیت ملّی و دفاعی جمهوری اسلامی ایران محسوب می‌شوند.(حیدری و دیگران، ۱۳۹۸: ۱۳۲)

تحول چشمگیر و دستیابی به فنّاوری روز، توسط گروه‌های تروریستی در سال‌های اخیر، بهره‌گیری آن‌ها از قابلیت‌ها و امکانات فضای مجازی(سایبر) و تلاش بی‌وقفه‌ی نظام سلطه

جهت افزایش توان اطلاعاتی و ارتباطی و علمی این گروه‌ها، باعث ظهور تهدیداتی از نوع تهدیدات سایبرتروریسم علیه امنیت ملّی و دفاعی جمهوری اسلامی ایران شده است. این تهدیدات از نظر حوزه‌ی نفوذ و فعالیت‌های تکثرگرایانه‌ی آن در هشت حوزه‌ی حساس تقسیم‌بندی شده است.(متقی، ۱۳۹۲: ۱۱۱)



نمودار شماره‌ی۱: مؤلفه‌های تهدیدات سایبرتروریسم علیه امنیت ملّی و دفاعی ج.ا.ا(متّقی، ۱۳۹۲: ۱۱۲)

پیشینه

در زمینه واکاوی تهدیدات و ارتباط آن با امنیت ملّی جمهوری اسلامی ایران، مطالب زیادی منتشر شده؛ اما در مجموع به علت صعوبت و مخالفت برخی صاحب‌نظران با کمّی‌نمودن تهدیدات، ادبیات زیادی در این حوزه تولید نشده است. لذا در این باره به چند مورد کمّی اشاره می‌شود:

اصغر افتخاری (۱۳۸۷) طی پژوهشی که به سفارش دانشگاه عالی دفاع ملی انجام گرفت، به برآورد تهدیدات با رویکرد سیستمی پرداخت و چارچوب مفهومی- نظری گزاره‌های راهبردی برآورد سیستمیک تهدیدات جمهوری اسلامی را در سپهر شناسایی تهدیدات(سیستم یا الگوی درون‌نگر و برون‌نگر) مورد دقت قرار داد که با توجه به مفاهیم و مبانی علمی موجود در مورد برآورد تهدید، در نوع خود قابل توجه است.

وی در مقاله‌ی پژوهشی دیگری تحت عنوان «شاخص‌های سنجش تهدیدات» با طرح پرسش اصلی از چیستی شاخص‌های سنجش تهدید، به ارائه‌ی شاخص‌هایی همت گمارد که در مقام شناخت شدت و وزن تهدید، مؤثر و کارآمد هستند. این شاخص‌ها عبارتند از توان ملّی، منافع ملّی، عمق، زمان، موقعیت، دامنه، مکان و قدرتمندی. کاربرد شاخص‌های پیشنهادی این مقاله در مجموع حجم تهدید را نشان داده و می‌توانند برای تعیین اولویت و شدت تهدیدات مورد استفاده قرار گیرند.

سیامک ره‌پیک(۱۳۸۷) در تحقیق عالمانه‌ی خود تحت عنوان «نظریه‌ی امنیت در جمهوری اسلامی ایران» به بحث در خصوص اجزای نظریه‌ی امنیتی به طور اعم و مطالعات امنیتی در ایران به طور اخص پرداخته و سپس مبانی و اصول نظریه‌ی امنیتی جمهوری اسلامی ایران را مورد دقت و ژرف‌اندیشی قرار داده است. او برای این کار به مباحث هستی‌شناسی و معرفت‌شناسی جمهوری اسلامی ایران توجه داشته و مبانی و ارکان تحلیل امنیت نظیر مرجع امنیت و تهدیدات امنیتی را بحث نموده است.

اصغر افتخاری در تحقیق ارزشمند دیگری تحت عنوان «کالبدشکافی تهدید» ضمن تقسیم‌بندی شاخص‌های سنجش تهدید به دو دسته‌ی اصلی درونی و بیرونی، نسبت به طراحی و ارائه‌ی دستگاهی با هشت شاخص برای سنجش تهدید اقدام کرده است که این شاخص‌ها عبارتند از: توانمندی(ضعف یا قوت بازیگر)، وضعیت منافع(تعارض، انطباق، و ...)، عمق(منافع بنیادین، حیاتی، حاشیه‌ای)، دامنه(اندک، متوسط، بالا، زمان(مترقبه و غیرمترقبه و ...)، مکان(داخلی، خارجی...)، قدرت و امکان اعمال قدرت، موقعیت(تعارض، تقاطع، تراکم).

وی در کل سطوح تهدیدات را به تهدیدات فردی، گروهی، ملّی، منطقه‌ای، بین‌المللی و جهانی تقیسم‌بندی کرده و ویژگی‌های آن‌ها را بیان نموده است.

محسن مرادیان در سه اثر مؤثر خود تحت عناوین «درآمدی بر ابعاد و مظاهر تهدیدات» (۱۳۸۵) و «تهدید و امنیت» (۱۳۸۸) و «سنجش تهدیدات نظامی جمهوری اسلامی ایران با

استفاده از مدل مرکز مطالعات راهبردی آجا برای ارزیابی تهدیدات و مقایسه‌ی آن با نتایج حاصله از روش ترکیبی آنتروپی شانون و مدل مجموع ساده‌وزنی» (۱۳۹۷) مباحثی نظیر تعریف تهدید، برداشت و سوء برداشت از تهدیدات، ماهیت تهدیدات، تهدید و تصویر ذهنی، منابع داخلی و خارجی تهدید، شاخص سنجش تهدیدات، شاخص ارزیابی تهدیدات، گونه‌شناسی تهدیدات و تهدیدات نامتقارن را مورد بحث و بررسی قرار داده است.

روش شناسی

برای جامعه و نمونه‌ی آماری طی یک طوفان فکری و بررسی اولیه، حجم جامعه‌ی آماری، هفتاد نفر برآورد گردید که با تمام آن‌ها به روش سرشماری، مصاحبه به عمل آمد و یا پرسش‌نامه توسط آنان تکمیل شد. با این حال جامعه‌ی آماری تحقیق را فرماندهان، مدیران و کارشناسان خبره یگان‌ها و سازمان‌های سطوح فرماندهی و مدیریتی با تحصیلات عالی در نیروهای مسلح جمهوری اسلامی ایران تشکیل می‌دهند که پاسخ‌دهندگان به لحاظ سطح تحصیلات، به چهار گروه اصلی تقسیم می‌شوند جدول و نمودار ترسیم‌شده، گویای این مطلب است که ۵۸/۵۷٪ کارشناس و ۲۴/۲۸٪ کارشناس ارشد و ۱۴/۲۹٪ دکترا می‌باشند. بنابراین می‌توان گفت که جامعه‌ی نمونه‌ی آماری از دانش کافی برخوردار است.

جامعه‌ی نمونه‌ی آماری

جدول و نمودار ترسیم‌شده گویای این مطلب است که ۸۲.۸۶٪ مربوط به کسانی است که در مشاغل «فرماندهی» و «اجرایی» خدمت نموده و این واقعیت نشانگر آن است که آن‌ها عملاً با امور مربوط به موضوع تحقیق آشنایی کامل دارند.

گردآوری اطلاعات در این تحقیق با استفاده از روش‌های میدانی، مطالعه‌ی کتابخانه‌ای(از طریق مطالعه‌ی کتب، مقالات و پایان‌نامه‌ها و رساله‌های مرتبط با استفاده از روش فیش‌برداری و سایت‌های اینترنتی معتبر) و تحقیقات میدانی(تهیه و توزیع پرسش‌نامه بین صاحب‌نظران و خبرگان جامعه‌ی آماری) صورت گرفته است.

یافته‌ها

تحلیل استنباطی فرضیه با استفاده از آمار استنباطی

احتمالاً بین مؤلفه‌هایی از قبیلحمله به زیرساخت‌های اطلاعاتی، امنیتی و دفاعی کشور؛ پخش و توزیع اطلاعات غلط یا گمراه‌کننده در فضای مجازی؛ نقش وبلاگ‌ها در جنجال‌سازی و فضاسازی رسانه‌ای؛ بهره‌گیری مخالفان از ظرفیت شبکه‌های اجتماعی برای ایجاد و گسترش

تنش‌های اجتماعی متراکم و گسترده؛ نقش نهادهای تقنینی و اجرایی امریکا در حمایت و فعال‌سازی سایبرتروریسم علیه جمهوری اسلامی ایران؛ تخریب اطلاعات مهم و کلیدی برای فلج‌کردن سیستم‌های اطلاعاتی؛ استفاده‌ی گروهک‌های ضدانقلاب از فضای مجازی علیه جمهوری اسلامی ایران و رخنه و نفوذ به ساختارهای استراتژیک نظام، ارتباط معناداری وجود دارد. لذا برای آنکه مشخص نماییم اطلاعات جمع‌آوری‌شده، نتیجه‌ی حدس و گمان نبوده و بین فراوانی‌های مشاهده‌شده و فراوانی‌های مورد انتظار تفاوت مهم و معناداری وجود دارد، از آزمون مجذور و روش محاسبه‌ی «خی۲» استفاده می‌کنیم.

فرضیه‌ی H0 : بین مؤلفه‌هایی از قبیل حمله به زیرساخت‌های اطلاعاتی، امنیتی و دفاعی کشور؛ «پخش و توزیع اطلاعات غلط یا گمراه‌کننده در فضای مجازی؛ «نقش وبلاگ‌ها در جنجال‌سازی و فضاسازی رسانه‌ای؛ «بهره گیری مخالفان از ظرفیت شبکه‌های اجتماعی برای ایجاد و گسترش تنش‌های اجتماعی متراکم و گسترده؛ «نقش نهادهای تقنینی و اجرایی امریکا در حمایت و فعال‌سازی سایبرتروریسم علیه جمهوری اسلامی ایران؛ «تخریب اطلاعات مهم و کلیدی برای فلج‌کردن سیستم‌های اطلاعاتی؛ استفاده‌ی گروهک‌های ضدانقلاب از فضای مجازی علیه جمهوری اسلامی ایران و رخنه و نفوذ به ساختارهای استراتژیک نظام ارتباط وجود ندارد.

فرضیه‌ی H1 : (فرضیه‌ی پژوهشی): بین مؤلفه‌هایی از قبیل حمله به زیرساخت‌های اطلاعاتی، امنیتی و دفاعی کشور؛ «پخش و توزیع اطلاعات غلط یا گمراه‌کننده در فضای مجازی؛ «نقش وبلاگ‌ها در جنجال‌سازی و فضاسازی رسانه‌ای؛ بهره‌گیری مخالفان از ظرفیت شبکه‌های اجتماعی برای ایجاد و گسترش تنش‌های اجتماعی متراکم و گسترده؛ «نقش نهادهای تقنینی و اجرایی امریکا در حمایت و فعال‌سازی سایبرتروریسم علیه جمهوری اسلامی ایران؛ تخریب اطلاعات مهم و کلیدی برای فلج‌کردن سیستم‌های اطلاعاتی؛ «استفاده‌ی گروهک‌های ضدانقلاب از فضای مجازی علیه جمهوری اسلامی ایران و رخنه و نفوذ به ساختارهای استراتژیک نظام ارتباط وجود دارد. برای ارزیابی در خصوص اثبات یا رد فرضیه H0 عملیات آماری زیر انجام می‌شود:

جدول شماره ۲ : رابطه‌ی معناداربودن تهدیدات سایبرتروریسم علیه امنیت ملّی و دفاعی جمهوری اسلامی ایران

محاسبات آماری / سطوح آزمون	فراوانی مشاهده شده FO	فراوانی مورد انتظار FE	تفاوت $(FO-FE)$	مربع تفاوت $(FO-FE)^2$	$\chi^2=\frac{(FO-FE)^2}{FE}$
خیلی کم	۳۲	۱۴	۱۸	۳۲۴	۲۳.۱۴
کم	۳۷	۱۴	۲۳	۵۲۹	۳۷.۷۸
متوسط	۱	۱۴	-۱۳	۱۶۹	۱۲.۰۷
زیاد	۰	۱۴	-۱۴	۱۹۶	۱۴
خیلی‌زیاد	۰	۱۴	-۱۴	۱۹۶	۱۴
جمع	۷۰	۷۰	-	-	۱۰۰.۹۹ $\Sigma=$

$$x^2=\frac{\Sigma(O-E)^2}{E}=100.99$$ آماری آزمون

$$D_F=R-1\Rightarrow D_F=5-1=4$$ درجه‌ی آزادی

$$X^2_{\times df}=\ ۴\ \text{و}\ ۰/۰۵\ X^2=\ ۹/\ ۴۹$$

با توجه به جدول توزیع مجذور کا(خی۲) و سطح معناداری ۵٪ مقدار بحرانی از جدول مساوی است با ۹/۴۹ . لذا برای محاسبه ضریب توافق(ضریب تعیین) بین دو متغیر مستقل و متغیر تابع، از رابطه زیر استفاده می‌شود:

$$C=\sqrt{\frac{\chi^2}{n+(\chi^2)}}=\sqrt{\frac{(100.99)}{70+(100.99)}}=\sqrt{0.59}=0.768$$

$$U=(C)^2\times100=(0.768)^2\times100=0.5898\times100=58.98$$

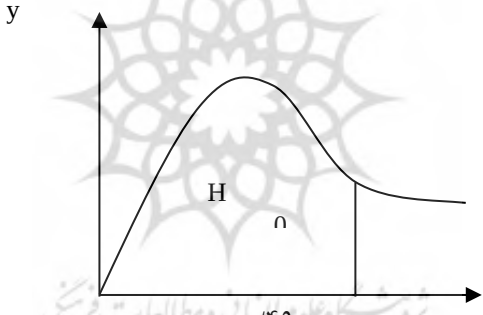
« C = ضریب توافق همبستگی و χ^2 = مجذور کا(خی۲) و n = تعداد جامعه نمونه و U = ضریب تعیین»

تصمیم‌گیری

با مقایسه‌ی مقدار آمار آزمون و مقدار بحرانی ملاحظه می‌شود که آمار آزمون در ناحیه‌ی H1 قرار گرفته است. بنابراین فرضیه‌ی H0 رد می‌شود و با اطمینان ۰/۹۵ فرضیه‌ی پژوهشی

مبنی‌بر اظهار جامعه‌ی نمونه در مورد واکاوی تهدیدهای سایبرتروریسم علیه امنیت ملّی و دفاعی جمهوری اسلامی ایران مؤلفه‌هایی از قبیل حمله به‌زیرساخت‌های اطلاعاتی، امنیتی و دفاعی کشور؛ پخش و توزیع اطلاعات غلط یا گمراه‌کننده در فضای مجازی؛ نقش وبلاگ‌ها در جنجال‌سازی و فضاسازی رسانه‌ای؛ بهره‌گیری مخالفان از ظرفیت شبکه‌های اجتماعی برای ایجاد و گسترش تنش‌های اجتماعی متراکم و گسترده؛ نقش نهادهای تقنینی و اجرایی امریکا در حمایت و فعال‌سازی سایبرتروریسم علیه جمهوری اسلامی ایران؛ تخریب اطلاعات مهم و کلیدی برای فلج‌کردن سیستم‌های اطلاعاتی؛ استفاده‌ی گروهک‌های ضدانقلاب از فضای مجازی علیه جمهوری اسلامی ایران و رخنه و نفوذ به‌ساختارهای استراتژیک نظام پذیرفته شده و مشخص می‌شود رابطه‌ی معناداری در این رابطه وجود دارد.

پس در مجموع فرضیه‌ی یکم تأیید می‌شود. یعنی اکثریت پاسخ‌دهندگان اعتقاد دارند مؤلفه‌های فوق به‌عنوان مؤلفه‌های تهدیدات سایبرتروریسم علیه امنیت ملّی و دفاعی جمهوری اسلامی ایران، به شمار می‌روند.



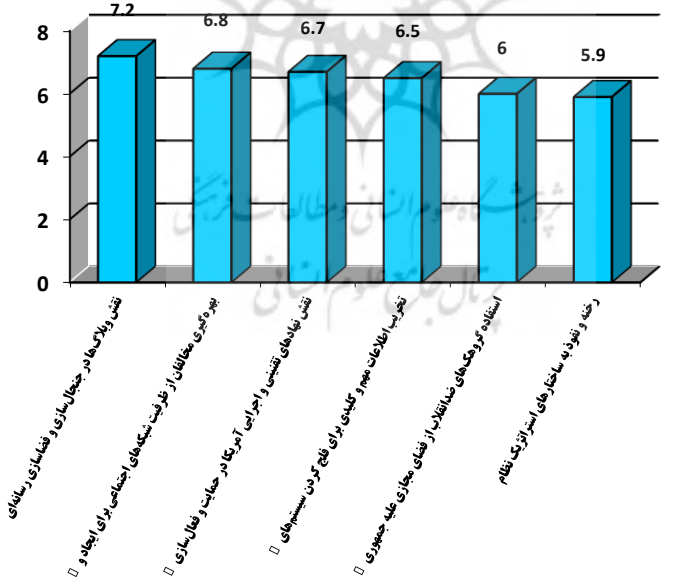
H_1: نمودار شماره‌ی۴ : مقایسه آمار آزمون از نظر جامعه‌ی آماری

$$\mu = \frac{\Sigma \mu}{n} = \frac{8.7 + 7.5 + 7.2 + 6.8 + 6.7 + 6.5 + 6.0 + 5.9}{8} = 6.91$$

میانگین مرکب، تجزیه‌وتحلیل

در این تأثیرگذاری پس از انجام تحقیقات لازم و تجزیه‌وتحلیل اطلاعات گردآوری‌شده از طریق پرسش‌نامه، مصاحبه با صاحب‌نظران و ... که به روش توصیفی و با استفاده از جداول توزیع فراوانی، نمودارها و توزیع درصدی و آمار استنباطی که به‌منظور آزمون فرضیه‌ها اجرا شده و به نتایج زیر که اهداف تحقیق می‌باشد، دست یافتیم: با میانگین به‌دست‌آمده از نتایج

حاصل از سؤال مطرح‌شده و نیز در خصوص فرضیه‌ی تحقیق، نتیجه می‌گیریم که نود درصد از پاسخ‌گویان، میزان مؤلفه‌های هشت گانه‌ی یادشده را به‌عنوان تهدیدات سایبرتروریسم علیه امنیت ملّی و دفاعی جمهوری اسلامی ایران، «خیلی‌زیاد» و «زیاد» دانسته‌اند؛ درحالی‌که صفر درصد به «کم» و «خیلی‌کم» نظر داده‌اند. نتیجه‌ی حاصله از تحلیل استنباطی داده‌ها حاکی از آن است که هم‌خوانی مورد تأیید بین تأثیر متغیر مستقل یعنی عواملّی از قبیل حمله به زیرساخت‌های اطلاعاتی، امنیتی و دفاعی کشور؛ «پخش و توزیع اطلاعات غلط یا گمراه‌کننده در فضای مجازی؛ نقش وبلاگ‌ها در جنجال‌سازی و فضاسازی رسانه‌ای؛ بهره‌گیری مخالفان از ظرفیت شبکه‌های اجتماعی برای ایجاد و گسترش تنش‌های اجتماعی متراکم و گسترده؛ نقش نهادهای تقنینی و اجرایی امریکا در حمایت و فعال‌سازی سایبرتروریسم علیه جمهوری اسلامی ایران؛ تخریب اطلاعات مهم و کلیدی برای فلج‌کردن سیستم‌های اطلاعاتی؛ استفاده‌ی گروهک‌های ضدانقلاب از فضای مجازی علیه جمهوری اسلامی ایران و رخنه و نفوذ به ساختارهای استراتژیک نظام بر متغیر تابع تهدیدات سایبرتروریسم در حد خیلی زیاد، مؤثر می‌باشند و به این مبنا می‌رسیم که نتیجه‌ی فوق بر نتیجه‌ی حاصله از پرسش‌نامه منطبق بوده بر روایی و اعتبار این پژوهش می‌افزاید.(نمودار شماره‌ی۵)



نمودار شماره‌ی۵: نمودار توزیع درصدی تهدیدات هشت‌گانه‌ی سایبرتروریسم علیه امنیت ملّی و دفاعی جمهوری اسلامی ایران

بحث و نتیجه‌گیری

در مجموع در این تحقیق توسط پژوهش‌گران، تهدیدات سایبرتروریسم علیه امنیت ملّی و دفاعی جمهوری اسلامی ایران مورد بررسی قرار گرفت. بر این اساس شاخص‌های اساسی که بیشترین تأکید را داشته‌اند، احصا و انتخاب گردید. در این تحقیق، به سؤال اصلی مورد بررسی، پاسخ شایسته و در خور توجهی داده شد. در این راستا، پس از یک نتیجه‌گیری صریح و قاطع می‌توان گفت که عوامل هشت‌گانه‌ی تهدیدات سایبرتروریسم علیه امنیت ملّی و دفاعی جمهوری اسلامی ایران از دیدگاه نظریه‌دهندگان جامعه‌ی آماری به ترتیب عبارتند از: حمله به زیرساخت‌های اطلاعاتی، امنیتی و دفاعی کشور؛ پخش و توزیع اطلاعات غلط یا گمراه‌کننده در فضای مجازی؛ نقش وبلاگ‌ها در جنجال‌سازی و فضاسازی رسانه‌ای؛ بهره‌گیری مخالفان از ظرفیت شبکه‌های اجتماعی برای ایجاد و گسترش تنش‌های اجتماعی متراکم و گسترده؛ نقش نهادهای تقنینی و اجرایی امریکا در حمایت و فعال‌سازی سایبرتروریسم علیه جمهوری اسلامی ایران؛ تخریب اطلاعات مهم و کلیدی برای فلج‌کردن سیستم‌های اطلاعاتی؛ استفاده‌ی گروهک‌های ضدانقلاب از فضای مجازی علیه جمهوری اسلامی ایران و رخنه و نفوذ به ساختارهای استراتژیک نظام. از سویی دیگر، گسترش فزاینده‌ی کاربست فنّاوری اطلاعات و ارتباطات در زیرساخت‌های حیاتی همچون انرژی، حمل‌ونقل و بانک‌داری از یک طرف و دسترسی نامحدود و غیر قابل کنترل افراد به ابزارهای ارتباطی مانند اینترنت و ماهواره و ...، منجر به شکل‌گیری فضای مجازی در کنار فضای واقعی در تعاملات بین سازمان‌ها و دولت‌ها شده است. طبیعی است که مفهوم امنیت ملّی در چنین فضایی، دست‌خوش چالش‌ها و تهدیدات شده و بازیگران جدیدی مانند افراد، گروه‌های تروریستی و گروه‌های معاند سازمان‌یافته، نقش و جایگاه مهمی را در پویش‌های امنیتی درون کشور جمهوری اسلامی ایران ایفا می‌کنند. در همین راستا با توجه به رشد فزاینده‌ی استفاده از اینترنت و حرکت شتابان دولت و سازمان‌های داخلی کشور جمهوری اسلامی ایران به‌سمت الکترونیکی‌کردن خدمات اجتماعی و اقتصادی و تأثیر انقلاب اطلاعاتی بر بهبود فناوری‌های دفاعی و نظامی، امنیت ملّی جمهوری اسلامی ایران در سال‌های آتی با تهدیدات و چالش‌های نوینی مواجه خواهد شد که یکی از این تهدیدات نوین، تهدیدات سایبرتروریسم است که با توجه به تنوع و تعدد گروه‌های تروریستی در محیط امنیتی جمهوری اسلامی ایران و برنامه‌ریزی نظام سلطه برای بهره‌گیری

از ظرفیت‌های گروه‌های تروریستی به‌منظور بی‌ثبات‌سازی و ایجاد اخلال در نظم و امنیت عمومی، یکی از مهم‌ترین چالش‌های فراروی نظام است.

لذا علاوه بر این بهره‌گیری گروه‌های تروریستی از ویژگی‌ها و مزایای فضای مجازی و تلاش نهادهای تقنینی و اجرایی ایالات متحده برای حمایت از فعالیت‌های این گروه‌ها از یک طرف و حرکت شتابان کشور در جهت کاربست فناوری‌های اطلاعات و ارتباطات در زیرساخت‌های حیاتی و شبکه‌های اطلاعاتی و امنیتی کشور موجب شده است که سایبرتروریسم تبدیل به یک تهدید جدی علیه امنیت ملّی کشور شود.

مهم‌ترین اصل در پژوهش حاضر، این است که محققین در پایان کار، براساس مطالعات انجام‌شده در حوزه‌ی «واکاوی تهدیدات سایبرتروریسم در امنیت ملّی و دفاعی جمهوری اسلامی ایران»، به طور قاطع نظر خود را درباره موضوع فوق اعلام کنند تا به گسترش دامنه‌ی معرفتی- علمی و یافته‌های موجود کمک نماید. از این رو برای نهادینه‌شدن این مقوله، با نگاهی عمیق از روی مطالب مندرج در تحقیق پیش رو، پیشنهادات زیر ارائه می‌شود:

با توجه به شدت عمل و سرمایه‌گذاری فراوان نظام سلطه در این زمینه خاص، کارگروهی از صاحب نظران و کارشناسان و اساتید هیئت علمی موجود در دانشگاه‌های جمهوری اسلامی ایران، جهت گردآوری و احصای تهدیدات سایبرتروریسم در امنیت ملّی و دفاعی جمهوری اسلامی ایران، تشکیل شود؛

بومی‌سازی راه‌کارهای امنیتی و قطع وابستگی اطلاعاتی و فنّاورانه؛

بهره‌گیری از فنّاوری‌های نوین در جهت هوشمندسازی زیر ساخت‌ها و تأسیسات نظامی؛

تربیت نیروهای متخصص و کارآزموده برای بهره‌گیری از فنّاوری‌های نوین در نبردها؛

تلاش نهادهای تقنینی و اجرایی برای فراهم‌سازی شرایط لازم و مطلوب عملّی با هدف تأمین امنیت سیستم‌های اطلاعاتی و ارتباطی؛

تأسیس مؤسسات پژوهشی تخصصی در زمینه‌ی امنیت فضای سایبر و گسترش مبادلات علمی با مراکز تخصصی مرتبط؛

از پروژه‌های تحقیقاتی مرتبط با موضوع مورد بحث در پژوهش پیش رو، توسط مبادی مربوطه و ذی‌صلاح حمایت‌های مادی و معنوی به عمل آید.

منابع

افتخاری اصغر، ۱۳۸۱ **ساخت دولت امنیت ملّی**، تهران فصلنامه مطالعات راهبردی شماره۳.

افتخاری، اصغر، ۱۳۸۵، **کالبد شکافی تهدید**، تهران، دانشگاه امام حسین(ع).

تقی‌پور، سیدمحسن، ۱۳۸۷، **مؤلفه‌های پایـــدار فرهنگی در امنیت ملّی جمهوری اسلامی ایران**، تهران، فصلنـــامه‌ی شماره‌ی۳ مرکز پژوهش و اسناد ریاست جمهوری.

تاج‌آبادی، حسین، مرادیان، بهزاد، ۱۳۹۴، **چالش‌های دیپلماسی دفاعی- امنیتی جمهوری اسلامی ایران در برابر دیپلماسی اجبار ایالات متحده امریکا**، تهران، انتشارات سپهبد شهید علی صیاد شیرازی.

روزنا، جیمز ودیگران، ۱۳۹۰، **انقلاب اطلاعات، امنیت و فناوری‌های جدید**، مترجم علی‌رضا طیب، تهران، نشر پژوهشکده‌ی مطالعات راهبردی.

جعفری، سیداصغر، ۱۳۹۲، **دیپلماسی دفاعی در اندیشه‌های امام خامنه‌ای**، تهران، انتشارات دانشگاه صنعتی مالک اشتر.

حیدری، کیومرث، آذرافروز، محسن، مرادیان، بهزاد، ۱۳۹۸، **اهمیت تنگه‌ی راهبردی هرمز و تأثیر آن بر امنیت ملّی و امنیت چند وجهی کشورهای منطقه**، تهران، انتشارات سپهبد شهید علی صیاد شیرازی.

شیهان، مایکل، ۱۳۸۸، **امنیت بین‌الملل**، ترجمه‌ی سیدجلال دهقانی فیروزآبادی، تهران، انتشارات پژوهشکده‌ی مطالعات راهبردی جمهوری اسلامی ایران.

نای، جوزف، ۱۳۸۷، **قدرت در عصر اطلاعات(از واقع‌گرایی تا جهانی‌شدن)**، ترجمه‌ی سعید میرترابی، تهران، نشر پژوهشکده‌ی مطالعات راهبردی.

عسکری، محمود و دیگران، ۱۳۹۱، **عوامل و ویژگی‌های سیاست دفاعی جمهوری اسلامی ایران**، (نامه دفاع) تهران، چاپ مرکز تحقیقات راهبردی دفاعی.

مرادیان، محسن و آقامحمدی، داود و مرادیان، بهزاد، ۱۳۹۷، **سنجش تهدیدات نظامی ج.ا.ا با استفاده از «مدل مرکز مطالعات راهبردی آجا برای ارزیابی تهدیدات» (ETMSSC AJA) و مقایسه‌ی آن با نتایج حاصله از روش ترکیبی آنتروپی**

شانون و مدل مجموع ساده‌وزنی، تهران، فصلنامه‌ی علمی- پژوهشی مطالعات دفاعی استراتژیک(داعا)، سال شانزدهم، شماره‌ی ۷۱.

مرادیان، محسن، ۱۳۸۹، **مبانی نظری امنیت، تهران**، انتشارات دانشکده‌ی علوم و فنون فارابی.

متّقی، ابراهیم و دیگران، ۱۳۹۲، **اندیشه‌های دفاعی امام خامنه‌ای در حوزه‌ی جنگ نرم**، تهران، انتشارات دانشگاه صنعتی مالک اشتر.

دفتر واژه‌گزینی دانشگاه و پژوهشگاه عالی دفاع ملّی و تحقیقات راهبردی، ۱۳۹۷، **فرهنگ توصیفی مفاهیم راهبردی، (جلد اول)**، تهران، انتشارات دانشگاه و پژوهشگاه عالی دفاع ملّی و تحقیقات راهبردی.

Daniel Ventre, **Cyberespace et acteurs du cyberconfli**t, Hermès-Lavoisier, avril, 2011.

Everard, J.Virtual states: **the Internat and the boundaries of the nation-state. New York**: Routledge, 2000.

Mesko, G. "Perceptions of Security: **Local Safety Councils in Slovenia**". In: U. Gori, & I. Paparela. Invisible Threats; **Financial and Information Technology Crimes Against National Securi,y**. Netherlands: IOS Press, 2006.

Cavelty**, M. D. Cyber-Security and Politics; US efforts to secure the information age New York**: Routledge, 2008.

Hancock, B."**Cyber-Tracking, Cyber-terrorism**". Computers and Security. Vol. 20, No 7, 2001