

مقاله پژوهشی: بررسی ابعاد ارزیابی تهدیدات هوشمند آینده

ذکریا کاظم پورا^۱، محسن بهرامی^۲

تاریخ دریافت: ۱۳۹۹/۰۶/۰۳

تاریخ پذیرش: ۱۴۰۰/۰۳/۰۲

چکیده

متناسب با تحولات رخ داده در ماهیت، ابعاد و روش‌های عملیاتی شدن تهدیدات و بروز و ظهور آن‌ها در اقدامات مربوط به حملات به اهداف مورد نظر، لازم است چارچوب‌های تحلیلی و الگوهای ارزیابی پیشرفته‌تری در زمینه شناخت و ارزیابی تهدیدات به‌خصوص تهدیدات هوشمند طراحی و عرضه گردند. در پژوهش حاضر تلاش شده است به این نیاز پاسخ داده شود. این پژوهش با رویکردی هنجاری و روش آمیخته انجام گرفته است. روش‌های گردآوری اطلاعات در این پژوهش، به دو دسته اسنادی و کتابخانه‌ای (با تکنیک فیش‌برداری توصیفی، بهره‌گیری از اسناد و مدارک، پویس‌های اینترنتی و وب‌کاوی) و میدانی (مصاحبه^۲، دلفی^۳، پنل خبرگان^۴ و پرسش‌نامه) بوده و جهت تجزیه و تحلیل داده‌ها از روش «مدل‌سازی معادلات ساختاری»^۵ با به‌کارگیری نرم‌افزار AMOS و SPSS استفاده شده است.

در فرایند این مطالعه، ابعاد هشت‌گانه: اندازه تهدید، گستره تهدید، زمان تهدید، عمق تهدید، تکرار تهدید، دامنه تهدید، مکان تهدید و نوع تهدید شناسایی و به‌عنوان ابعاد ارزیابی تهدیدات هوشمند معرفی گردید.

کلید واژه‌ها: تهدید، ارزیابی تهدید، تهدیدات هوشمند، آینده‌پژوهی.

۱. دکتری آینده‌پژوهی، دانشکده مدیریت، علم و فناوری دانشگاه صنعتی امیرکبیر، نویسنده مسئول:

(z.kazempour@aut.ac.ir)

۲. استاد دانشگاه صنعتی امیرکبیر (پلی‌تکنیک تهران).

۳Interviews.

۴Delphi.

۵Expert Panels.

۶Structural Equational Modeling (SEM).

مقدمه

پیگیری راهبرد قدرت هوشمند توسط آمریکا و هم‌پیمانان او و تداوم این روند، ماهیت بحران‌ها و منازعات آینده را دگرگون نموده است (جوزف نای، ۱۳۹۲: ۶) به‌نحوی که کلیه محاسبات پیشین در بحث از شناخت و آنالیز تهدید ملزم به بازنگری و بازاندیشی شده است.

بدون درک درست از تهدیدات و آسیب‌پذیری‌ها، در مدیریت کلان کشور و در سطوح امنیتی نمی‌توان تصمیمات منطبق بر واقعیت گرفت، از آنجا است که شناسایی و ارزیابی تهدیدات معطوف به آینده به یکی از پیش‌نیازهای برنامه‌ریزی کلان تبدیل شده و یکی از عناصر شکل‌دهنده آینده در گفتمان آینده‌پژوهی هنجاری است.

از طرف دیگر سازمان‌های دفاعی-امنیتی به‌تبع مأموریت ذاتی خود همواره به دنبال رصد تحولات محیطی و استخراج انواع تهدیدات می‌باشند و در این زمینه از روش‌ها، الگوها و استانداردهای مختلفی بهره برده و گاهی اقدامات پیش‌دستانه‌ای را برای مدیریت تهدیدات انجام می‌دهند؛ اما از آنجا که الگو و روش مورد وثوقی جهت شناسایی تهدیدات نوپدید وجود ندارد، اهمیت انجام تحقیق پیش‌رو بیشتر نمایان شده و خلأ وجود الگوی معطوف به آینده «ارزیابی تهدیدات هوشمند» بیشتر احساس می‌شود. بدیهی است عدم ورود به این حوزه پژوهشی و صرف اتکا به چارچوب‌های نظری سنتی در شناسایی و درک تهدیدات، مدیریت کلان کشور را با مشکل مواجه خواهد نمود.

بر این اساس این مقاله با رویکرد هنجاری آینده‌پژوهی و متناسب با اقتضای شرایط بومی، ابعاد شناسایی و ارزیابی تهدیدات هوشمند را ارائه می‌نماید، چراکه رویکرد اکتشافی برخلاف نوع هنجاری، از حال به آینده حرکت می‌کند و توجهی به امیال و خواست ما ندارد؛ بنابراین محصول آن کشف آینده‌هایی است که با درصد بالایی از اطمینان رخ خواهند داد. روش‌های اکتشافی آینده را بر مبنای گذشته و حال می‌سازند و روند باور هستند. در رویکرد هنجاری آینده لزوماً در امتداد گذشته تصور نمی‌شود. این رویکرد اولین بار در دهه ۶۰ میلادی توسط مؤسسه رند مورد توجه قرار گرفت و «هرمان کان» با این باور، روش دلفی را ابداع کرد (حیدری، ۱۳۹۳: ۹۴). در این روش که هنجارمحور است نظرات

کارشناسان در یک حوزه خاص از اهمیت خاصی برخوردار بوده و دیدگاه آن‌ها نسبت به آینده مبنای اصلی شکل‌گیری آینده است.

مبانی نظری و پیشینه‌شناسی تحقیق

در این بخش ضمن معرفی موضوع محوری پیشینه تحقیق، نتایج مرتبط با موضوع بررسی شده و به نقاط اشتراک و افتراق آن با پژوهش حاضر اشاره شده است.

۱. کالبدشکافی تهدید اثر اصغر افتخاری، ۱۳۸۵

موضوع محوری کتاب: گونه‌شناسی و سنجش تهدید

نتایج مرتبط با موضوع: گونه‌شناسی تهدید بر مبنای یازده شاخص: بُعد، سطح، جغرافیا، تعادل، تقارن، پیچیدگی، هویت، جنس، کانون، انگیزه و کارویژه طراحی و ارائه هشت شاخص برای سنجش تهدید شامل توانمندی (ضعف یا قوت بازیگر)، وضعیت منافع (تعارض، انطباق و ...)، عمق (منافع بنیادین، حیاتی حاشیه‌ای و ...)، دامنه (اندک، متوسط، بالا)، زمان (مترقبه، غیرمترقبه و ...)، مکان (داخلی، خارجی ...)، قدرت و امکان اعمال قدرت و موقعیت (تعارض، تقاطع، تراکم) (افتخاری، ۱۳۸۵).

در این کتاب صرفاً جنبه‌های نظری ارزیابی تهدید مورد بررسی قرار گرفته و الگوی مناسب عملی برای ارزیابی تهدیدات ارائه نشده است.

۲. تهدیدات قدرت ملی، مظاهر و نشانگان، ره‌پیک، سیامک، دانشگاه عالی دفاع ملی،

تهران، ۱۳۸۸

یکی از مباحث مورد توجه در مطالعات امنیتی و سیاسی، مباحث مربوط به «تهدیدشناسی» است. این بحث در عین گستردگی، از نظر منابع به‌ویژه در برخی از بخش‌ها مانند شاخص‌ها و نشانگان تهدید، ضعیف و فقیر است و حتی در مجموعه ادبیات و مطالعات غربی، متون منسجم و قابل اعتنای کمتری در این مورد به چشم می‌خورد (ره‌پیک، ۱۳۸۸).

هرچند از تنوع منابع این اثر، در شناسایی انواع و اقسام تهدیدات استفاده شده است، اما به معرفی مظاهر و نشانگان تهدید بسنده شده و برای ارزیابی تهدیدات کافی نیست.

۳. برآورد تهدید؛ رویکردی نظام‌واره، افتخاری، اصغر، دانشگاه عالی دفاع ملی، تهران،

۱۳۹۰

موضوع محوری کتاب: کاربرد نظریه سیستم‌ها در تهدیدشناسی

نتایج مرتبط با موضوع: در مقام کاربرد نظریه سیستم‌ها جهت آسیب‌شناسی امنیتی، لازم است این نظریه طرح، معنا و کاربردی شود که در عین وفاداری به اصول بنیادین نظریه، فضای مناسب برای لحاظ نمودن عوامل و مؤلفه‌های خاص ج.ا.ایران نیز فراهم آید. مستند به تاریخ انقلاب اسلامی، اصول و مبانی نظری و عملی و بالاخره قانون اساسی ج.ا.ایران، می‌توان چنین استنتاج کرد که «جمهوری اسلامی» سیستمی متمایز از سایر نظام‌های سیاسی است که ابعاد، سطوح و گونه‌های تهدید در آن به‌طور طبیعی متفاوت خواهد بود (افتخاری، ۱۳۹۰).

از این اثر، جهت استخراج شاخص‌های بومی و اختصاصی ارزیابی تهدیدات ج.ا.ایران بهره‌برداری شده و همانند کتاب کالبدشکافی تهدید به موضوعات نظری پرداخته است.

۴. «آمریکا، نظریه قدرت هوشمند و الگوهای ناموفق»، سیاوش دانیالی، اطلاعات

راهبردی، مرکز تحقیقات راهبردی دفاعی، سال ۸، شماره ۸۳، ۱۳۸۹

موضوع محوری مقاله: کاربرد قدرت هوشمند آمریکا

نتایج مرتبط با موضوع: «عوامل پیشرفت قدرت هوشمند عبارت‌اند از: ترکیب مناسب چارچوب‌های قدرت، انعطاف‌پذیری مبتنی بر توانایی‌ها و نیازها، توانایی برای مسیریابی مبتنی بر آینده‌پژوهی...

نو دمکرات‌های آمریکایی بر آن شده‌اند تا با کاربرد قدرت هوشمند (اعمال هم‌زمان قدرت‌های نرم و سخت) در ساحت سیاست، راهبرد مدیریت نوینی را در پیگیری اهداف خود اعمال نمایند» (دانیالی، ۱۳۸۹).

مطالعه این مقاله، ضرورت پرداختن به موضوع تهدید هوشمند را استحکام بخشیده، اما بحثی از تهدیدات متأثر از قدرت هوشمند را به‌خوبی ارائه نکرده است.

۵. «نظریه دفاع هوشمند در سپهر اندیشه‌های دفاعی»، خسرو حسنلو، فصلنامه مطالعات

دفاعی-استراتژیک شماره ۶۳، بهار ۱۳۹۵

موضوع محوری مقاله: استخراج ویژگی‌های «دفاع هوشمند»

نتایج مرتبط با موضوع: دفاع هوشمند عبارت است از دفاع متعالی (معنوی، مشروع، مقدس)، کاربرد همگرا و پویای قدرت در برابر طیف گسترده چالش‌های هوشمند، دفاع چندلایه (کشوری و لشکری) و چند ساحتی (فضا، بُعد و حوزه)، تعادل و ثبات بخشی سامانه با محافظت از گرانیگاه‌ها (نقاط ثقل) در برابر شوک سیستمی، برخوردار از ادوات دقیق با کاربر چندگانه، برقراری امنیت نرم در شرایط سخت و نیمه‌سخت، دانش‌بنیاد و فناوری‌نگر، پیشگیرانه و بازدارنده، سازوکارهای نوآورانه، نهادسازی نوین دفاعی (سازمان‌های هم‌افزا و یادگیرنده)، مهندسی آینده با طرح‌ریزی پابرجا (طرح‌های بدیل و آینده‌نگر) و... است (حسنلو، ۱۳۹۵).

مطالعه این مقاله، چارچوب نظری خوبی را برای تدوین الگوی مورد نظر پژوهش حاضر فراهم نمود، اما نقاط ضعف آن نپرداختن به چگونگی ارزیابی تهدیدات هوشمند و نحوه کمی‌سازی آن است.

۶. تهدید و امنیت (تعاریف و مفاهیم)، مرادیان، محسن، تهدید و امنیت، انتشارات شهید صیاد شیرازی، تهران، ۱۳۸۸

موضوع محوری کتاب: تعریف و مفاهیم امنیت و تهدید

نتایج مرتبط با موضوع: ارائه شاخص‌های سنجش تهدید از قبیل الف) عمق تهدید (منافع بنیادی، منافع حیاتی، منافع مهم، منافع حاشیه‌ای)، ب) دامنه یا گستره تهدید، پ) زمان (تغییر هویت تهدید، پیش‌بینی تهدید، افزایش مقاومت محیط، دگرذیسی تهدید) (مرادیان، ۱۳۸۸).

هرچند در استخراج برخی از شاخص‌های کلان ارزیابی تهدیدات هوشمند از این اثر بهره‌برداری مناسبی شد، اما شاخص‌های ارائه‌شده لازم اما ناکافی هستند.

۷. جنگ هوشمند، دیوید سی گومپرت، آروینگ لاکو، جاستین پرکینز، مرکز آینده‌پژوهی علوم و فناوری دفاعی، ۱۳۹۶

موضوع محوری: تغییر پارادایم‌های قدرت، به قدرت اطلاعات، قدرت تفکر، قدرت شبکه و قدرت شناختی (جنگ هوشمند)

نتیجه: «یکی از گزینه‌هایی که وزارت دفاع آمریکا باید برای بهبود توانایی‌های خود برای استخدام افراد جنگ هوشمند در نظر بگیرد این است که بایستی برخی از عناصر

شناختی جنگ هوشمند (پیش‌بینی، فرصت‌طلبی، استدلال تحت فشار، تمایل به مسئولیت‌پذیری و تصمیم‌گیری، توانایی یادگیری در عمل، انعطاف‌پذیری و خودآگاهی) را توسعه داده و به کار بگیرد» (گومبرت، ۱۳۹۶).

در این کتاب به مفهوم جنگ هوشمند به‌خوبی پرداخته شده است، اما در نگاه بومی برداشت صحیحی از تهدید هوشمند ارائه نشده است.

۸. «درآمدی بر قدرت هوشمند»، حسام‌الدین آشنا، مرکز آینده‌پژوهی علوم و فناوری دفاعی، ۱۳۸۸

موضوع محوری کتاب: ماهیت قدرت هوشمند و بومی‌سازی آن

نتایج مرتبط با موضوع: «قدرت هوشمند نیازمند برنامه‌ای هوشمند است. حاصل مطالعات بومی و بررسی هزاران برگ سند و مقاله درباره قدرت سخت و نرم نشان می‌دهد که می‌توان برای قدرت هوشمند ایرانی هفت ویژگی و هفت مؤلفه اصلی در نظر گرفت. هفت ویژگی بنیادین شامل دین محوری، محیط رقابتی، زمان‌بندی، عدم تقارن، وفاق‌سازی، هماهنگی ساختاری و عملکردی، سنجش‌پذیری و همچنین هفت مؤلفه اصلی شامل سیاسی، اقتصادی، فرهنگی، رسانه‌ای، نظامی، امنیتی اطلاعاتی و نهادهای غیردولتی» (آشنا، ۱۳۸۸).

این کتاب دستیابی به قدرت هوشمند در قبال تهدید هوشمند را توصیه نموده، اما محدود به حوزه نظری شده و الگوی مناسبی برای چگونگی دستیابی به قدرت هوشمند و نحوه ارزیابی تهدید هوشمند و مقابله با این تهدیدات را ارائه نکرده است.

۹. الگوی بررسی تهدیدها و آسیب‌پذیری‌ها، عبدالهی، رضا، ساحفاسا، چاپخانه شهید مطهری، مهرماه ۱۳۹۰

موضوع محوری کتاب: ارائه الگوی ارزیابی تهدیدها و آسیب‌پذیری‌ها

نتایج مرتبط با موضوع: ارائه الگوی بررسی تهدیدها و آسیب‌پذیری‌ها در هفت گام: شناسایی اهداف مرجع، به‌روزرسانی تهدیدها و آسیب‌پذیری‌ها، شناسایی و مستندسازی تهدیدها و آسیب‌پذیری‌ها، توصیف و ارزیابی تهدیدها و آسیب‌پذیری‌ها، تحلیل تهدیدها و آسیب‌پذیری‌ها، مقابله با تهدیدها و رفع آسیب‌پذیری‌ها، ارزیابی اقدامات (عبدالهی، ۱۳۹۰).

این کتاب یکی از منابع روشمند در راستای ارزیابی تهدیدات در داخل کشور است که از چارچوب کلی آن در پژوهش حاضر استفاده شده است. نقدی که بر آن وارد است کلی‌گویی در ارائه الگو و ضعف در شناخت تهدیدات نوظهور است. از طرفی نگاه غالب در این کتاب ارزیابی تهدیدات سخت بوده و از ورود به تهدیدات مرکب و هیبریدی و تهدیدات هوشمند غفلت نموده است.

۱۰. مقاله «روش‌شناسی درک و توسعه ارزیابی تهدید»

Vidalis, Stilianos; Blyth, Andrew: Understanding and Development Methodology, School of Computing, University of Glamorgan, (2002)

موضوع محوری مقاله: سنجش تهدید

نتایج مرتبط با موضوع: ارائه نظریه سنجش تهدید بر پایه چهار گام؛ «برآورد حوزه تهدید»، «عامل تهدید و تحلیل آسیب‌پذیری»، «مدل‌سازی و ایجاد سناریو» و «ارزیابی تهدید»

«ارزیابی تهدید» به‌عنوان گام نهایی «سنجش تهدید» و قائل به تفاوت ماهوی بین دو مفهوم «سنجش» و «ارزیابی»، حاصل بهره‌برداری از این اثر است (Vidalis, ۲۰۰۲). نقدی که بر این مقاله و سایر آثار استیلیانوس ویدالیز و آندرو بلیث وارد است نگاه غالب آن‌ها در ارزیابی تهدید محدود به جنبه‌های سخت تهدید است.

۱۱. روش ماتریس تحلیل و ارزیابی تهدیدات

Durch, William J. The Stimson Center. Report 30, May 1999

موضوع محوری مقاله: ارزیابی تهدید

نتایج مرتبط با موضوع: ارائه نظریه «ماتریس تحلیل و ارزیابی تهدیدات». این روش هم برای تعیین نهایی تهدیدات، هم برای تحلیل و ارزیابی ابعاد و زوایای تهدیدات شناسایی شده کاربرد دارد؛ به بیان دیگر این روش برای «کالبدشکافی تهدیدات» مناسب است (Durch, 1999).

افتخاری، ره پیک و عبدالله‌خانی از آثار ویلیام جی دورچ اقتباس نموده‌اند. از موارد نقد

بر این روش، محدود بودن آن بر ارزیابی تهدیدات سخت است

تعریف مفاهیم

قدرت هوشمند

ناکارآمدی قدرت سخت و محدودیت‌های قدرت نرم، نظریه‌پردازان سیاسی را به چاره‌جویی نظری در خصوص اعمال قدرت در فضای پیچیده جهانی شدن واداشت. حاصل این تلاش فکری، تولد پدیده مفهومی به نام قدرت هوشمند بود (کبریائی‌زاده، ۱۳۹۰: ۱۰). مفهوم قدرت هوشمند را اولین بار سوزان ناسل^۱ به معنای ترکیب هدفمند و خردمندانه قدرت سخت و نرم در مقابله با تهدیدات به کار برد. وی معتقد بود منابع اجباری^۲ و اقناعی^۳ شامل توانایی‌ها و برتری‌های نظامی، اقتصادی، فرهنگی و ایدئولوژیک باید در یک جهت هماهنگ شوند تا برآیند آن، تداوم برتری یک کشور را تضمین کند (Nossel, 2004). قدرت هوشمند، تحولی شهودی در موضوع قدرت است که مخاطبان اصلی آن را دولت‌ها، نخبگان سیاسی، گروه‌های ذی‌نفوذ و نهادهای حکومتی تشکیل می‌دهند (Wilson, 111:2008).

تبیین و توضیح قدرت هوشمند

تبیین مفهومی قدرت هوشمند، براساس شاخص‌ها و نشانه‌های تشکیل‌دهنده آن امکان پذیر است. آمریکایی‌ها از سال ۲۰۰۶ میلادی به بعد، درصدد تغییر در الگوی رفتاری خویش برآمدند. علت شکل‌گیری چنین رویکردی را می‌توان ناکامی‌های سیاسی، اقتصادی و راهبردی آمریکا طی سال‌های ۲۰۰۱ تا ۲۰۰۶ میلادی دانست. در این دوران، شکل متنوع و پیچیده‌ای از تهدیدها ظهور یافت و آمریکایی‌ها در حوزه‌های مختلف جغرافیایی با نشانه‌هایی از تهدید روبرو شدند. چهره سیاسی و نقش راهبردی آمریکا در برابر افکار عمومی و همچنین ذهنیت و ادراک بسیاری از شهروندان و گروه‌های اجتماعی افول یافت (متقی، ۱۳۸۷: ۵۹). این امر نشان می‌دهد که قدرت سیاسی و جایگاه آن کشور در

^۱ Suzanne Nossel

^۲ Coercive Resources

^۳ Persuasive Resources

وضعیت تغییر قرار گرفته و نیازمند بازسازی است.

ریشه‌های راهبرد قدرت هوشمند

سیاست خارجی هر کشور، ترکیبی از «قدرت سخت» و «قدرت نرم» است و دولت‌ها از این دو قدرت برای اعمال سیاست‌های خود در عرصه‌های مختلف داخلی و بین‌المللی چه به‌تنهایی یا تلفیقی بهره می‌برند. کاهش موقعیت آمریکا به‌عنوان تنها ابرقدرت جهان پس از فروپاشی شوروی و ترس برآمده از حوادث ۱۱ سپتامبر باعث به وجود آمدن یک بدبینی عمومی نسبت به سیاست‌های نظامی‌گری دولت بوش شده بود که دائماً در حال افزایش بود و همگان منتظر راهبرد جایگزینی به‌جای راهبرد سخت‌افزارانه آمریکا بودند (Nossel, 2004). به قدرت رسیدن جورج دبلیو بوش در آغاز هزاره سوم میلادی و پیوند معنایی و فکری وی با طیف نومحافظه‌کاری بیانگر این واقعیت بود که ایالات متحده بی‌تردید در چشم‌انداز سیاست خارجی خود بر اتخاذ رویکردهای سخت‌افزاری^۱ پافشاری خواهد کرد. این ارزیابی با تحولات و وقایع پس از ۱۱ سپتامبر به‌خوبی ماهیت تهاجمی^۲ راهبرد کلان ایالات متحده را در قالب اشغال نظامی افغانستان و عراق در سال‌های ۲۰۰۱ و ۲۰۰۳ میلادی با ابتناء به «تئوری دومینو»^۳ به اثبات رساند. در تداوم چنین بستری موضوع تغییر رژیم ایران نیز در محافل و مخازن فکری وابسته به نومحافظه‌کاران در دستور کار قرار گرفت. در چنین شرایطی و هم‌زمان با زمین‌گیر شدن ماشین جنگی آمریکا در عراق و افغانستان و نتایج ناامیدکننده مبارزه با تروریسم در منطقه خاورمیانه و نیز گسترش موج انتقادات و اعتراض‌ها نزد افکار عمومی دولت بوش در دور دوم ریاست جمهوری در چرخشی استراتژیک رویکرد راهبردی آمریکا را در قالب قدرت نرم^۴ برنامه‌ریزی کرد. در این رویکرد که تحت تأثیر آرا و اندیشه‌های برنارد لوئیس و جوزف نای و نیز عناصر میانه‌روتر دستگاه دیپلماسی آمریکا نظیر کالین پاول و خانم رایس بود، آمریکا به دنبال ترمیم چهره مخدوش خویش در قالب «خاورمیانه جدید» نزد افکار عمومی ملت‌های منطقه

خاورمیانه گام برداشت. از رهگذر تحولات مذکور، برآیند و معدل هر دو رویکرد در پایان دوران ریاست جمهوری بوش پسر مایوس‌کننده بود و یکی از مهم‌ترین دلایل موفقیت «دموکرات‌های نو» به رهبری باراک اوباما زیر سؤال بردن و ناکارآمد جلوه دادن عملکرد جمهوری‌خواهان و دولت بوش در زمینه مدیریت تحولات جهانی و بحران‌های بین‌المللی به شکل عام و موضوع مهار ایران و پرونده هسته‌ای ایران به شکل خاص بود. با به قدرت رسیدن باراک اوباما در نوامبر ۲۰۰۸ میلادی راهبرد ایالات متحده نیز دست‌خوش دگرگونی‌های مفهومی و پراگماتیستی تری قرار گرفت که این دگرگونی خود را در قامت اتخاذ رویکرد راهبردی قدرت هوشمند آرا است.

مدت‌ها است در روابط بین‌الملل از سوی جوزف نای، «توانایی تلفیق و ترکیب قدرت سخت و نرم در راهبرد پیروزی» به‌عنوان یک راهبرد تعریف شده است (دانیالی، ۱۳۸۹: ۱۳). چندی بعد «مرکز پیشرفت آمریکا» از اصطلاح «قدرت یکپارچه»^۳ سخن گفت و پروژه دانشگاه پرینستون تحت عنوان «پیش‌به‌سوی جهان آزاد قانونمند»^۴ آغاز شد.

در مقابل این مفهوم، اصطلاح «قدرت گیج یا احمقانه»^۵ شکل گرفت که به معنای «استفاده نابجا یا نابخردانه از هر یک یا هر دو مؤلفه قدرت سخت یا نرم است». قدرت هوشمند همچنین به‌عنوان یک جایگزین برای قدرت ملایم یا نرم مطرح شده است. در قدرت هوشمند، با استحاله نظام سیاسی، نظام‌های فکری تغییر می‌کند سپس با تحمیل اراده و فکر، تفکر جدید جایگزین می‌شود. نای در تعریفی دیگر، قدرت هوشمند را به این صورت تعریف کرده است: قدرت هوشمند، یعنی قدرت آمریکا در بهره‌برداری از منابع گوناگون؛ از جمله قدرت نرم برای جذب دیگران و اینکه ما چگونه می‌توانیم دیگر کشورها را برای به اشتراک گذاشتن اهدافمان، بدون توسل به زور که محدود و پرهزینه است، با خود همراه کنیم (همان: ۱۴-۱۳).

قدرت هوشمند اصطلاحی است که در روابط بین‌الملل به‌عنوان «قابلیت ترکیب قدرت

^۱Center for American Progress

^۲Integrated Power

^۳Forging a world of liberty under law

^۴Stupid Power

سخت و نرم جهت رسیدن به راهبرد پیروزی» تعریف شده است. به گفته برخی از کارشناسان همانند «آلن چستر کراکر و همکاران»، قدرت هوشمند شامل «استفاده راهبردی از دیپلماسی، متقاعدسازی، ظرفیت‌سازی و طرح‌ریزی قدرت و نفوذ» است که با ارزش و دارای مشروعیت سیاسی و اجتماعی بوده و در اصل، از تعامل هر دو نیروی نظامی و دیپلماتیک، نشأت می‌گیرد (Crocker, 2007: 13).

تهدیدات هوشمند

در گذشته کاربرد «قدرت سخت» را منحصر به شرایط جنگی و کاربرد «قدرت نرم» را بیشتر در شرایط صلح و آرامش می‌دانستند. در حالی که چالش‌ها، تهدیدات و منازعات آینده نه تنها ابعاد نرم را شامل می‌شوند، بلکه، ابعاد سخت قدرت را نیز تحت سیطره خود قرار داده است. امروزه به‌کارگیری این ابعاد قدرت به‌طور هم‌زمان و در شرایط جنگ و صلح مرسوم است. به‌کارگیری هم‌زمان این قدرت‌های متنوع و گوناگون، تهدیدات مهلکی را به وجود آورده است که آن را «تهدیدات هوشمند» می‌نامیم (حسنلو، ۱۳۹۴: ۷۱).

در دهه‌های اخیر پیشرفت خیره‌کننده فناوری‌های نوین باعث تغییر سیمای جنگ‌های کلاسیک و ظهور مفاهیمی چون جنگ‌های سایبری، جنگ اطلاعات، جنگ نامتقارن و جنگ‌های هیبریدی شده است (پورصادق، ۱۳۹۸: ۷).

از آنجا که همه پدیده‌ها دارای ابعاد پیدا و پنهان یا آشکار و نهان هستند، بحران‌ها و تهدیدات نیز این‌گونه می‌باشند. تهدیدات هوشمند دارای ویژگی‌های منحصر به فردی هستند که مهم‌ترین آن‌ها شامل، ویژگی نخست: قسمت اعظم تهدیدات هوشمند نامحسوس بوده و به‌مثابه یک کوه یخ، تنها بخش بسیار کوچکی از آن به چشم می‌آید. ویژگی دوم آن است که روند تکامل تهدیدات هوشمند عمده‌تاً تدریجی است و هنگامی ظاهر می‌شوند که در مرحله نهایی تکامل خود هستند. از این منظر، شبیه بهمنی است که در ابتدای قله کوه کوچک است ولی رفته‌رفته بزرگ‌تر و سهمگین‌تر می‌شود.

الگوهای ارزیابی تهدیدات

برای ارزیابی تهدید می‌توان از چند روش کلی استفاده کرد:

روش اول شناسایی تهدید مبتنی بر اهداف مرجع است. در این روش از طریق سنجش تأثیر هر یک از تهدیدات شناسایی شده بر اهداف مرجع، تهدیدات مشخص خواهد شد، برای مثال چنانچه ایدئولوژی دولت، هدف مرجع در سطح امنیت ملی باشد، تشخیص تهدیدات خطرناک از میان تهدیدات شناسایی شده به میزان در خطر قرار گرفتن این هدف مرجع از ناحیه تهدید شناسایی شده بستگی دارد.

روش دوم؛ ارزیابی تهدیدات از طریق طراحی سناریوها است. براساس این روش برای هر تهدید شناسایی شده سناریوهای احتمالی آن ترسیم خواهد شد. سپس با توجه به سناریوهای موجود، درجه تهدید تعیین خواهد شد.

روش سوم در ارزیابی تهدیدات، اولویت‌بندی تهدیدات شناسایی شده است. در این روش با استفاده از فهرست تهدیدات شناسایی شده و برخی معیارهای اساسی که از سوی نخبگان مورد پذیرش قرار گرفته، تهدیدات اولویت‌بندی می‌شوند، سپس براساس وزن هر تهدید با مبنا قرار دادن حداقل وزن مورد پذیرش در خصوص تهدیدات امنیتی، این نوع تهدیدات تعیین خواهند شد (علی عبدالله‌خانی، ۱۳۸۶).

در چارچوب روش‌های قیدشده، پنج الگوی اصلی ارزیابی تهدید مورد نقد و بررسی قرار گرفته است:

۱. ارزیابی تهدیدات براساس «اهداف مرجع» و «اولویت‌بندی تهدیدات»

یکی از الگوهای مرسوم در تعیین درجه و شدت تهدید، استفاده از دو روش: «تعیین درجه تهدیدات براساس اهداف مرجع» و «تعیین درجه تهدیدات براساس اولویت‌بندی تهدیدات شناسایی شده» است. معیارهای اساسی و بنیادین این الگو، «میزان آسیب‌پذیری در برابر تهدیدات شناسایی شده» و «پیامدهای تهدیدات» هستند که توسط علی عبدالله‌خانی برای مدیریت ادراک در واکنش به تهدید ارائه شده است (همان). در مجموع تعیین میزان

خطر تهدیدات شناسایی شده از محاسبه میزان وزن یا حاصل ضرب هر یک از اهداف مرجع و سپس میزان پیامدها در آسیب‌پذیری‌ها به دست خواهد آمد.

میزان آسیب‌پذیری به معانی تعیین میزان ضعف سیستم مدافع در برابر تهدید و در چارچوب هدف مرجع مورد نظر است. برای تعیین میزان آسیب‌پذیری از سه شاخصه «توان بازدارندگی» (توان بازیگر مدافع در جلوگیری از وقوع تهدید بر ضد هدف مرجع)، «توان حفاظتی» (توان بازیگر مدافع در حفاظت از مرجع در برابر تهدید) و «توان ترمیمی» (قابلیت‌های درونی هدف مرجع در بازگشت به وضعیت اولیه و امکان ترمیم در مدت‌زمان قابل قبول) استفاده می‌شود. با توجه به شاخصه‌های مورد نظر، میزان آسیب‌پذیری را در چهار طیف «آسیب‌پذیری بسیار بالا»، «آسیب‌پذیری بالا»، «آسیب‌پذیری متوسط» و «آسیب‌پذیری کم» درجه‌بندی می‌نمایند.

پیامدها معیار دیگری در ارزیابی تهدیدات هستند و در واقع «پیامد» به میزان صدماتی گفته می‌شود که از ناحیه تهدید به مجموعه اهداف مرجع وارد می‌گردند. پیامد تهدیدات را با سه شاخصه «شدت تهدید» (حجم صدمات اهداف مرجع از ناحیه تهدید)، «گستره تهدید» (گسترده‌گی محیط اعمال تهدید بر اهداف مرجع) و «عمق تهدید» (میزان نفوذ تهدید در لایه‌های درونی اهداف مرجع) ارزیابی می‌نمایند. با توجه به شاخصه‌های سه‌گانه در چارچوب معیار پیامد تهدیدات، گزینه‌های درجه‌بندی پیامدها در چهار طیف «پیامدهای ویرانگر»، «پیامدهای شدید»، «پیامدهای قابل توجه» و «پیامدهای اندک» درجه‌بندی می‌شوند (همان).

نقد و بررسی الگوی ارزیابی تهدیدات براساس «اهداف مرجع» و «اولویت‌بندی تهدیدات»:

هر چند در این الگو به بحث «ارزیابی آسیب‌پذیری‌ها» و «ارزیابی تهدیدات» به صورت توأمان پرداخته شده اما شاخص‌های ارزیابی این الگو بسیار کلی بوده و شاخص‌های مهمی از قبیل نوع تهدید، اندازه تهدید، میزان احتمال تکرار تهدید، دامنه تهدید، زمان و مکان تهدید مورد غفلت قرار گرفته است.

۲. ارزیابی تهدیدات به روش «موازنه تهدید»

معناسازی امنیت به وسیله تهدید یکی از مهم‌ترین رهیافت‌های معرفت‌شناسی امنیت است. وقتی امنیت تابعی از تهدید در نظر گرفته شد؛ به‌طور طبیعی روش‌شناسی تحلیل امنیت نیز بر مبنای تهدید قرار خواهد گرفت. بر این اساس منطق این روش، تحلیل موازنه قوا در سطح نظام بین‌الملل براساس «تهدیدات» به‌جای «قدرت» است. مطابق با این روش که توسط استیفن والت در مقاله‌ای تحت عنوان «شکل‌گیری اتحاد و توازن قدرت» ارائه شده است، صف‌آرایی و جبهه‌بندی کشورها یا تشکیل ائتلاف‌ها در محیط امنیت بین‌الملل مبتنی بر منطق موازنه در برابر بازیگران قدرتمند و صرفاً به علت قدرت آنان صورت نمی‌گیرد، بلکه چنین وضعیتی‌هایی در برابر بازیگران تهدیدگر حتی اگر خیلی قدرتمند نیز نباشند به وجود می‌آید (مایکل برون، ۱۹۹۴).^۱ روش موازنه تهدید، چهار معیار و شاخص اصلی: «قدرت»، «مجاورت»، «توانایی‌های تهاجمی» و «نیات تهاجمی» را مبنای تحلیل و ارزیابی تهدیدات قرار می‌دهد.

نقد و بررسی الگوی ارزیابی تهدیدات به روش «موازنه تهدید»:

عمده‌ترین نقطه ضعف این الگو عدم توجه به بُعد مهم ارزیابی تهدیدات، یعنی «ارزیابی آسیب‌پذیری‌های» تهدیدشونده است. اگر برداشت صحیحی از میزان و درجه آسیب‌پذیری مرجع تهدید در اختیار نباشد صرفاً نمی‌توان با ارزیابی قدرت و توان تهدیدکنندگی منشأ تهدید نسبت به ارزیابی تهدیدات اقدام نمود. در واقع قدرت بازیگران تهدیدکننده با میزان آسیب‌پذیری تهدیدشونده رابطه مستقیمی دارد. هر میزان درجه آسیب‌پذیری بازیگر تهدیدشونده بیشتر باشد به همان اندازه اثرگذاری قدرت تهدید بر آن بیشتر خواهد بود؛ بنابراین می‌توان گفت این الگو نگاه یک‌سویه‌ای به ارزیابی تهدیدات داشته و از جامعیت لازم برخوردار نیست.

^۱ Michel E. Brown

۳. ارزیابی تهدیدات به روش «سنجش تهدید»^۱

این روش توسط استیلیانوس ویدالیز^۲ و آندرو بلیث^۳ در مقاله‌ای تحت عنوان «روش‌شناسی درک و توسعه ارزیابی تهدید» ارائه و بر پایه چهار گام؛ «برآورد حوزه تهدید»^۴، «عامل تهدید و تحلیل آسیب‌پذیری»، «مدل‌سازی و ایجاد سناریو»^۵ و «ارزیابی تهدید»^۶ پایه‌گذاری شده است.

نقد و بررسی الگوی ارزیابی تهدیدات به روش «سنجش تهدید»:

این الگو یکی از الگوهای نسبتاً جامع ارزیابی تهدیدات است، اما به دلیل عدم برخورداری از شاخص‌های قابل سنجش، جنبه کاربردی ندارد. نگاه عمده این الگو، ارزیابی کلی تهدیدات براساس گزاره‌های کیفی است.

۴. الگوی «ماتریس تحلیل و ارزیابی تهدیدات»

این روش از سوی مرکز هنری استیمسون^۷ و توسط ویلیام جی دورچ^۸ ارائه گردیده و در واقع تدوین دقیق‌تر روش‌های ارائه‌شده از سوی وزارت دفاع آمریکا در ارزیابی تهدیدات است (William J. Durch, 1999). روش «ماتریس تحلیل و ارزیابی تهدیدات» هم برای تعیین نهایی تهدیدات مفید است، هم برای تحلیل و ارزیابی ابعاد و زوایای تهدیدات شناسایی شده کاربرد دارد؛ به بیان دیگر این روش برای «کالبدشکافی تهدیدات» مناسب است.

این روش از چهار گزینه «تهدیدات فاجعه‌آمیز»، «تهدیدات حیاتی»، «تهدیدات ناچیز» و «تهدیدات بی‌اهمیت» برای چارچوب‌بندی و تحلیل شدت تهدیدات در سطوح و ابعاد مختلف، پنج متغیر «وقوع مکرر»، «وقوع محتمل»، «وقوع موردی»، «وقوع اندک» و «وقوع

-
- ۱ Treat Assessment
 - ۲ Stilianos Vidalis
 - ۳ Andrew Blyth
 - ۴ Assessment Scope
 - ۵ Scenario Construction & Modelling
 - ۶ Threat Evaluation
 - ۷ The Henry L. Stimson
 - ۸ William J. Durch

بعید» برای تخمین احتمال راهبردی یا گرایش کلی یک بازیگر برای ایفای رفتار تهدیدآمیز و در نهایت پنج متغیر «زمان هشدار کمتر از یک دقیقه»، «زمان هشدار کمتر از یک ساعت»، «زمان هشدار یک روز تا یک هفته»، «زمان هشدار چند هفته تا یک ماه» و «زمان هشدار چند سال» جهت تعیین زمان هشدار استفاده می‌کند. این سه دسته، گزینه‌های «ماتریس تحلیل و ارزیابی تهدیدات» را شکل می‌دهند.

نقد و بررسی الگوی ارزیابی تهدیدات به روش «ماتریس تحلیل و ارزیابی تهدیدات»:

عمده‌ترین موردی که در این الگو نیز مورد غفلت قرار گرفته، عدم توجه به «ارزیابی آسیب‌پذیری‌های» بازیگران مورد مطالعه است. هرچند شاخص‌های ارائه‌شده در این الگو شاخص‌های مفیدی برای ارزیابی تهدیدات می‌باشند، اما توجه نکردن به امر مهم ارزیابی آسیب‌پذیری‌ها این الگو را غیرکاربردی نموده است.

۵- ارزیابی تهدیدات مبتنی بر آینده‌پژوهی

آینده‌پژوهی علم و هنر کشف و ساخت آینده است که طی دو دهه گذشته در دنیا پیشرفت چشمگیری را داشته است. در این مدت آینده‌پژوهی با در اختیار گذاشتن جعبه‌ابزاری از روش‌ها به پیشرفت سایر علوم کمک شایانی کرده است (امینی، ۱۳۹۹: ۷). مدیریت تهدیدات مبتنی بر مطالعات آینده یک الگوی متکی بر راهبرد پیشگیری است. این الگو از دو رویکرد اصلی برخوردار است:

رویکرد نخست آن شناخت اجزای تهدید (موضوع، عامل و حوزه تهدید) مبتنی بر مطالعه شواهد و روندهای موجود و ارائه تصویری از تهدیدات آینده است. رویکرد دوم مبتنی بر پیشگیری و مقابله با تهدید براساس اجرای سناریوهای پیشگیرانه در سه بخش کاهش احتمال وقوع تهدید، مقابله با تهدید و کاهش آسیب‌پذیری‌ها صورت می‌پذیرد. رویکرد نخست نگاه اکتشافی در شناسایی و درک تهدیدات را ارائه می‌نماید و رویکرد دوم مبتنی بر آینده‌نگاری و متمرکز بر مدیریت تهدیدات و کاهش آسیب‌پذیری‌ها است.

نقد و بررسی «الگوی ارزیابی تهدیدات مبتنی بر آینده‌پژوهی»:

از نقاط قوت این الگو می‌توان به بحث مدیریت تهدیدات توأم با ارزیابی آن‌ها اشاره نمود. آینده‌نگر بودن این الگو نیز، نقطه قوت دیگری است که نسبت به الگوهای پیشین آن را تمایز نموده است. با این حال ابعاد و شاخص‌های ارزیابی این الگو بسیار کلی بوده و متغیرهای مهمی از قبیل نوع تهدید، اندازه تهدید، میزان احتمال تکرار تهدید، دامنه تهدید، زمان و مکان تهدید مورد غفلت قرار گرفته یا به بیان کلیات اکتفا شده است.

الگوی تحلیل کالبدی تهدید (روش پیشنهادی)

الگوی نظری پیشنهادی دارای هشت بُعد، ۲۴ مؤلفه و ۱۲۰ شاخص کیفی است که منطبق بر فرضیه‌های زیر است. در این مقاله صرفاً فرضیه‌های مرتبط با ابعاد هشت‌گانه مورد بررسی قرار گرفته است.

فرضیه‌های تحقیق

- فرضیه ۱: نوع تهدید یکی از ابعاد ارزیابی تهدید هوشمند است.
- فرضیه ۲: اندازه و توان تهدید یکی از ابعاد ارزیابی تهدید هوشمند است.
- فرضیه ۳: گستره تهدید یکی از ابعاد ارزیابی تهدید هوشمند است.
- فرضیه ۴: زمان تهدید و مدت بازیابی یکی از ابعاد ارزیابی تهدید هوشمند است.
- فرضیه ۵: عمق تهدید یکی از ابعاد ارزیابی تهدید هوشمند است.
- فرضیه ۶: تکرار تهدید یکی از ابعاد ارزیابی تهدید هوشمند است.
- فرضیه ۷: دامنه تهدید یکی از ابعاد ارزیابی تهدید هوشمند است.
- فرضیه ۸: مکان تهدید یکی از ابعاد ارزیابی تهدید هوشمند است.

روش‌شناسی تحقیق

پژوهش حاضر با روش آمیخته و رویکرد هنجاری انجام گرفته است. روش‌های گردآوری اطلاعات این تحقیق، به دو دسته اسنادی (با تکنیک فیش‌برداری توصیفی،

بهره‌گیری از اسناد و مدارک و پوشش‌های اینترنتی و وب‌کاوی) و میدانی (مصاحبه، دلفی، پنل خبرگان و پرسشنامه) تقسیم می‌شود. تجزیه و تحلیل داده‌ها با استفاده از روش مدل‌سازی معادلات ساختاری با به‌کارگیری نرم‌افزارهای AMOS و SPSS صورت می‌پذیرد. با توجه به اینکه حجم جامعه آماری تحقیق حاضر، حدود ۵۰۰ نفر است، روش نمونه‌گیری به صورت تصادفی و حجم نمونه با استفاده از جدول مورگان، ۲۱۷ نفر تعیین گردید. با توجه به پیش‌بینی عدم بازگشت تعدادی از پرسش‌نامه‌ها تعداد ۲۵۰ پرسشنامه توزیع گردید که از این بین تعداد ۲۲۱ پرسش‌نامه تکمیل و بازگردانده شد و مابقی به علت عدم قبول توسط پاسخ‌دهنده، عدم برگشت و یا عدم تکمیل کنار گذاشته شد و مورد استفاده قرار نگرفتند.

جهت صحت‌گذاری و راستی‌آزمایی داده‌های ورودی از ابزار بررسی روایی و اعتبار پرسش‌نامه به منظور اطمینان از منطبق بودن سؤالات پرسش‌نامه با اهداف تحقیق و قابلیت تکرارپذیری آن استفاده شد. بررسی روایی سازه از طریق تحلیل عاملی تأییدی صورت گرفت. براساس نتایج، مقدار KMO برابر $0/881$ بوده و سطح معناداری آزمون بارتلت زیر $0/05$ و بار عاملی همه گویه‌ها بیشتر از $0/3$ به دست آمد؛ بنابراین هیچ‌کدام از گویه‌ها از فرایند تجزیه و تحلیل حذف نشدند.

برای تعیین اعتبار پرسشنامه از طریق ضریب آلفای کرونباخ بر مبنای بررسی همسانی درونی گویه‌ها استفاده شده است. با توجه به اینکه مقدار ضریب آلفای کرونباخ به دست آمده این مطالعه $0/972$ بوده و ضریب پایایی تمامی متغیرها نیز از حداقل مقدار $0/7$ بیشتر بوده، می‌توان گفت که ابزار از پایایی مناسب برخوردار است.

به لحاظ میزان تحصيلات، اکثر پاسخ‌دهندگان به سؤالات پرسشنامه، یعنی $40/3$ درصد، دارای مدرک تحصيلی کارشناسی ارشد بوده‌اند. به لحاظ سنوات خدمت، اکثر پاسخ‌دهندگان به سؤالات پرسشنامه، یعنی $35,7$ درصد، دارای سنوات خدمت بین ۲۰ تا ۲۹ سال بودند. به لحاظ سازمان، اکثر پاسخ‌دهندگان به این سؤال، یعنی $44/8$ درصد زیرمجموعه مراکز دفاعی و نظامی بودند.

برای تأیید هر یک از متغیرها همچنین گویه‌های مربوط به هر یک از آن‌ها از تحلیل عاملی تأییدی استفاده شده است. در جدول (۱) نتایج مربوط به شاخص‌های برازش مدل‌های تحلیل عاملی تأییدی نشان داده شده است.

جدول (۱): شاخص‌های برازش مدل‌های تحلیل عاملی تأییدی

مدل اندازه‌گیری	مقدار ایده‌آل	مقدار قابل قبول	نماد	نام شاخص
۶۹۶۸	-	-	(df)	درجه آزادی
۱۴۵۹۳/۴۴۴	$0 \leq \chi^2 \leq 2df$	۲۰۰ □ □ ۲ □ ۳۰۰	(χ^2)	کای اسکوئر
۰/۰۰۰	$0.1 < p \leq 0.05$	$0.5 < p \leq 1.00$	(χ^2)	معناداری χ^2
۲/۰۹۴	$0 \leq \chi^2/df \leq 2$	$2 < \chi^2/df \leq 3$	(χ^2/df)	کای اسکوئر بهینه‌شده
۰/۸۸۲	$0.95 \leq GFI \leq 1.00$	$0.80 \leq GFI < 0.95$	(GFI)	نیکویی برازش
۰/۰۸۹	$0 \leq RMR \leq 0.05$	$0 < RMR \leq 0.10$	(RMR)	ریشه میانگین مربعات باقی‌مانده
۰/۹۸۷	$0.97 \leq CFI \leq 1.00$	$0.90 \leq CFI < 0.97$	(CFI)	شاخص برازش تطبیقی
۰/۰۷۵	$0 \leq RMSEA \leq 0.05$	$0.05 < RMSEA \leq 0.08$	(RMSEA)	ریشه میانگین مربعات خطای برآورد
۰/۵۸۸	$0.60 \leq PGFI \leq 1.00$	$0.50 \leq PGFI < 0.60$	(PGFI)	شاخص نیکویی برازش ایجازی
۰/۶۰۵	$0.60 \leq PNFI \leq 1.00$	$0.50 \leq PNFI < 0.60$	(PNFI)	شاخص برازش ایجازی هنجارشده

تجزیه و تحلیل یافته‌های تحقیق

برای تأیید یا رد فرضیات تحقیق از آماره آزمون تی- استیودنت استفاده شد. اگر مقدار آماره t بزرگ‌تر از $\pm 1/96$ باشد، فرضیه مربوطه در سطح خطای ۰/۰۵ مورد تأیید در غیر این صورت رد می‌گردد.

جدول (۲): آزمون فرض آماری مربوط به ابعاد ارزیابی تهدیدات هوشمند

One-Sample Test							متغیرهای تحقیق
Test Value = 3							
۹۵٪ Confidence Interval of the Difference		اختلاف میانگین	میانگین	سطح معنی داری	درجه آزادی	مقدار آماره t	
حد بالا	حد پایین						
-۰.۲۸۳۱	-۰.۴۵۹۳	-۰.۳۷۱۱ ۵	۲.۶۲۸۸	.۰۰۰	۲۲۰	-۸.۳۰۳	نوع تهدید
-۰.۲۶۹۱	-۰.۵۱۹۱	-۰.۳۹۴۱ ۲	۲.۶۰۵۹	.۰۰۰	۲۲۰	-۶.۲۱۳	اندازه و توان تهدید
-۰.۳۲۲۵	-۰.۵۷۱۶	-۰.۴۴۷۰ ۶	۲.۵۵۲۹	.۰۰۰	۲۲۰	-۷.۰۷۳	گستره تهدید
-۰.۳۷۳۲	-۰.۶۲۰۵	-۰.۴۹۶۸ ۳	۲.۵۰۳۲	.۰۰۰	۲۲۰	-۷.۹۲۱	عمق تهدید
-۰.۲۱۷۵	-۰.۴۸۳۹	-۰.۳۵۰۶ ۸	۲.۶۴۹۳	.۰۰۰	۲۲۰	-۵.۱۹۰	تکرار تهدید
-۰.۴۱۶۵	-۰.۶۴۸۷	-۰.۵۳۲۵ ۸	۲.۴۶۷۴	.۰۰۰	۲۲۰	-۹.۰۳۸	زمان تهدید
-۰.۵۹۱۸	-۰.۸۶۷۰	-۰.۷۲۹۴ ۱	۲.۲۷۰۶	.۰۰۰	۲۲۰	-۱۰.۴۴ ۷	دامنه تهدید
-۰.۴۹۶۲	-۰.۶۶۹۴	-۰.۵۸۲۸ ۱	۲.۴۱۷۲	.۰۰۰	۲۲۰	-۱۳.۲۶ ۸	مکان تهدید

فرضیه شماره ۱

نوع تهدید یکی از ابعاد ارزیابی تهدید هوشمند است.

(نوع تهدید: گونه‌شناسی تهدید از نظر ابعاد، جنس، درجه پیچیدگی، سطح و جغرافیا، انگیزه و کانون، هویت، تقارن و کارویژه آن).

نتایج حاصل از بررسی نظرات پاسخ‌دهندگان نشان داد که مقدار آماره T عدد ۸/۳۰۳- درجه آزادی ۲۲۰ و سطح معنی داری ۰/۰۰۰ است؛ بنابراین نتایج حاصل از آزمون فرضیه که نشان می‌دهد فرضیه فوق مورد تأیید قرار می‌گیرد.

فرضیه شماره ۲

اندازه و توان تهدید یکی از ابعاد ارزیابی تهدید هوشمند است.

به منظور بررسی این فرضیه، در ابتدا به طور کلی و جزئی، شاخص‌های تحقیق مورد بررسی قرار گرفتند. نتایج حاصل از بررسی نظرات پاسخ‌دهندگان نشان داد که مقدار آماره T عدد ۶/۲۱۳- درجه آزادی ۲۲۰ و سطح معنی‌داری ۰/۰۰۰ است. از آنجایی که سطح معنی‌داری کمتر از ۰/۰۵ (در سطح اطمینان ۹۵ درصد) و حد بالا و پایین منفی است، می‌توان نتیجه گرفت فرضیه فوق مورد تأیید قرار می‌گیرد.

فرضیه شماره ۳

گستره تهدید یکی از ابعاد ارزیابی تهدید هوشمند است (گستره تهدید: میزان پهنای محیط تهدید).

نتایج حاصل از بررسی نظرات پاسخ‌دهندگان نشان داد که مقدار آماره T عدد ۷/۰۷۳- درجه آزادی ۲۲۰ و سطح معنی‌داری ۰/۰۰۰ است. از آنجایی که سطح معنی‌داری کمتر از ۰/۰۵ و حد بالا و پایین منفی است؛ بنابراین نتایج حاصل از آزمون فرضیه نشان می‌دهد فرضیه فوق مورد تأیید قرار می‌گیرد.

فرضیه شماره ۴

زمان تهدید و مدت بازیابی یکی از ابعاد ارزیابی تهدید هوشمند است (زمان تهدید: زمان هشدار، زمان اثرگذاری و سرعت دگرذیسی تهدید و مدت بازیابی).

نتایج حاصل از بررسی نظرات پاسخ‌دهندگان نشان داد که مقدار آماره T عدد ۹/۰۳۸- درجه آزادی ۲۲۰ و سطح معنی‌داری ۰/۰۰۰ است؛ بنابراین نتایج حاصل از آزمون فرضیه که نشان می‌دهد فرضیه فوق مورد تأیید قرار می‌گیرد.

فرضیه شماره ۵

عمق تهدید یکی از ابعاد ارزیابی تهدید هوشمند است.

عمق تهدید: میزان ارزشمندی منفعت موضوع تهدید (دارایی‌های کلیدی تهدیدکننده × موقعیت منافع تهدیدکننده و تهدیدشونده).

نتایج حاصل از بررسی نظرات پاسخ‌دهندگان نشان داد که مقدار آماره T عدد ۷/۹۲۱-

درجه آزادی ۲۲۰ و سطح معنی‌داری ۰/۰۰۰ است. از آنجایی که سطح معنی‌داری کمتر از ۰/۰۵ و حد بالا و پایین منفی است؛ بنابراین فرضیه فوق مورد تأیید قرار می‌گیرد.

فرضیه شماره ۶

تکرار تهدید یکی از ابعاد تهدید هوشمند است (تکرار تهدید: میزان احتمال تکرار و مداومت تهدید).

نتایج حاصل از بررسی نظرات پاسخ‌دهندگان نشان داد که مقدار آماره T عدد ۵/۱۹۰- درجه آزادی ۲۲۰ و سطح معنی‌داری ۰/۰۰۰ است؛ بنابراین نتایج حاصل از آزمون فرضیه نشان می‌دهد فرضیه فوق مورد تأیید قرار می‌گیرد.

فرضیه شماره ۷

دامنه تهدید یکی از ابعاد ارزیابی تهدید هوشمند است.

دامنه تهدید: میزان شیوع یک تهدید از حیث عاملی- ارزشی (تعداد بازیگران تهدیدکننده \times تعداد موضوعات تهدیدشونده).

نتایج حاصل از بررسی نظرات پاسخ‌دهندگان نشان داد که مقدار آماره T عدد ۱۰/۴۴۷- درجه آزادی ۲۲۰ و سطح معنی‌داری ۰/۰۰۰ است؛ بنابراین نتایج حاصل از آزمون فرضیه نشان می‌دهد فرضیه فوق مورد تأیید قرار می‌گیرد.

فرضیه شماره ۸

مکان تهدید یکی از ابعاد ارزیابی تهدید هوشمند است (مکان تهدید: دوری و نزدیکی عامل و منشأ تهدید).

نتایج حاصل از بررسی نظرات پاسخ‌دهندگان نشان داد که مقدار آماره T عدد ۱۳/۲۶۸- درجه آزادی ۲۲۰ و سطح معنی‌داری ۰/۰۰۰ است؛ بنابراین نتایج حاصل از آزمون فرضیه نشان می‌دهد فرضیه فوق مورد تأیید قرار می‌گیرد.

در ادامه به منظور رتبه‌بندی متغیرهای مورد بررسی، آزمون فریدمن انجام شده است. آزمون فریدمن از جمله آزمون‌های آماری است که برای رتبه‌بندی و اولویت‌دهی به

متغیرهای چندمقوله‌ای با مقیاس رتبه‌ای (ترتیبی) انجام می‌شود. نتایج این آزمون برای میزان نقش و اهمیت متغیرهای تحقیق در جدول ۳ آورده شده است.

جدول (۳): نتایج آزمون فریدمن برای بررسی تفاوت بین میانگین متغیرهای تحقیق

Test Statistics ^a	
N	۲۲۱
Chi-Square	۷۳.۱۷۳
df	۷
Asymp. Sig.	.۰۰۰

a. Friedman Test

همان‌طور که در جدول ۳ ملاحظه می‌گردد، مقدار آماره کای دو با ۷ درجه آزادی برابر $۷۳/۱۷۳$ و همچنین سطح معناداری آزمون کمتر از $۰/۰۵$ است که بیانگر این است که تفاوت معناداری بین دیدگاه پاسخ‌دهندگان درباره میانگین ابعاد مدل وجود دارد. جدول ۴ مؤید این یافته است.

جدول (۴): رتبه‌بندی متغیرهای تحقیق

رتبه	نام متغیر	میانگین رتبه‌ها
۱	تکرار تهدید	۵/۰۵
۲	نوع تهدید	۴/۹۷
۳	اندازه و توان تهدید	۴/۸۷
۴	گستره تهدید (پهنای محیط تهدید)	۴/۶۰
۵	عمق تهدید	۴/۴۲
۶	مکان تهدید	۴/۴۰
۷	زمان تهدید و مدت ارزیابی	۴/۳۱
۸	دامنه تهدید	۳/۳۹

بنابراین با توجه به جدول ۴ مقایسه میانگین رتبه ابعاد مدل از نظر پاسخ‌دهندگان را به ترتیب به صورت: تکرار تهدید، نوع تهدید، اندازه و توان تهدید، گستره (پهنای محیط)،

عمق تهدید، مکان تهدید، زمان تهدید و مدت بازیابی و در نهایت دامنه تهدید نشان می‌دهد.

نتیجه‌گیری و پیشنهاد

الف. نتیجه‌گیری

همان‌طوری که عنوان شد، مدیریت کلان کشور بدون درک درست از تهدیدات و آسیب‌پذیری‌ها قادر به اخذ تصمیمات منطبق بر واقعیت نیست، از آنجا است که شناسایی و ارزیابی تهدیدات معطوف به آینده به یکی از پیش‌نیازهای برنامه‌ریزی کلان تبدیل شده و یکی از عناصر شکل‌دهنده آینده در گفتمان آینده‌پژوهی هنجاری است. بر همین اساس سازمان‌های دفاعی به تبع مأموریت ذاتی خود همواره به دنبال رصد تحولات محیطی و استخراج انواع تهدیدات بوده و در این زمینه از روش‌ها و الگوهای مختلفی برای مدیریت تهدیدات بهره می‌برند؛ اما از آنجا که الگو و روش بومی مورد وثوقی جهت شناسایی تهدیدات نوپدید وجود ندارد، اهمیت انجام این تحقیق بیشتر نمایان شده و خلأ وجود الگوی معطوف به آینده «ارزیابی تهدیدات هوشمند» بیشتر احساس می‌شود. در همین راستا هدف اصلی تحقیق، طراحی الگوی نظری ارزیابی تهدیدات هوشمند آینده ترسیم گردید که در این مقاله صرفاً به ابعاد ارزیابی این الگو پرداخته شد.

در فرایند این مطالعه ابتدا پیشینه تحقیق مورد بررسی قرار گرفت و بیان شد پیرامون موضوع عینی تحقیق، مطالعه جامع و قابل اتکایی صورت نپذیرفته و یا در منابع آشکار منتشر نشده است؛ اما مطالعات کلی و پراکنده‌ای پیرامون مباحث حاشیه‌ای موضوع انجام شده که نقاط اشتراک و افتراق و نقاط مغفول مانده آن‌ها مورد بحث و بررسی قرار گرفت. در بخش اول به ادبیات نظری تحقیق و در بخش دوم به معرفی الگوهای رایج ارزیابی تهدیدات از جمله الگوی ارزیابی تهدیدات براساس اهداف مرجع و اولویت‌بندی تهدیدات، الگوی ارزیابی تهدید براساس موازنه تهدید، الگوی ارزیابی ماتریس تحلیل و ارزیابی تهدیدات، ارزیابی تهدیدات به روش سنجش تهدید و در نهایت الگوی ارزیابی تهدیدات مبتنی بر آینده‌پژوهی پرداخته شد.

بررسی روش‌های پیش‌گفته گویای این مطلب است که این نوع روش‌ها متناسب با رشد و

پیچیدگی تهدیدات نوین توسعه نیافته و در ارزیابی تهدید به دلیل جامع نگر نبودن دارای یکسری نواقصی می باشند. بر این اساس الگوی پیشنهادی در چارچوب فرضیات تحقیق با در نظر گرفتن تحولات رخ داده در حوزه فناوری و تحولات بین المللی و به تبع آن تحولات رخ داده در حوزه تهدیدشناسی، از اشکالات و نواقص کمتری نسبت به روش های پیشین است.

در قالب الگوی پیشنهادی، مهم ترین گزاره های راهبردی که می تواند در مقام ارزیابی تهدید دست مایه کار کارشناسان و تحلیلگران قرار گیرند، گزاره های هشت گانه زیر است که ارکان اصلی الگوی پیشنهادی را شکل می دهند:

۱. ارزیابی تهدید منوط به تشخیص نوع تهدید از حیث جنس، درجه پیچیدگی، سطح، انگیزه و کانون، هویت، درجه همگونی و کارویژه تهدید است.
۲. ارزیابی تهدید منوط به تعیین اندازه و توان تهدید است.
۳. ارزیابی تهدید منوط به تشخیص گستره و وسعت اثرگذاری تهدید است.
۴. ارزیابی تهدید مستلزم به تشخیص زمان (زمان هشدار، زمان اثرگذاری، سرعت دگرذیسی و زمان بازیابی) تهدید است.
۵. ارزیابی تهدید مستلزم تشخیص عمق تهدید و تعیین منافع و میزان انطباق تهدیدگر و تهدیدشونده است.
۶. ارزیابی تهدید مستلزم برآورد احتمال تکرار و تخمین میزان احتمال وقوع تهدید است.
۷. ارزیابی تهدید مستلزم تشخیص دامنه تهدید (شناخت موضوع و بازیگران) تهدید است.
۸. ارزیابی تهدید مستلزم شناخت مبدأ و منشأ تهدید است.

ب. پیشنهادات

- پیشنهاد می گردد به منظور کاربردی نمودن نتایج تحقیق، اقدامات زیر صورت پذیرد.
۱. آموزش تفکر آینده پژوهانه در شناسایی و ارزیابی تهدیدات هوشمند.
 ۲. تدوین دوره های آموزشی شناسایی و ارزیابی تهدیدات هوشمند در سطوح و لایه های مختلف مدیریتی و کارشناسی.
 ۳. تدوین راهبردهای مقابله ای با تهدیدات هوشمند آینده.

فهرست منابع و مآخذ

الف. منابع فارسی

- آرمیتاژ، ریچارد و نای، جوزف (۱۳۹۲)، *درباره قدرت هوشمند: آمریکای هوشمندتر و امن‌تر، گزارش مرکز مطالعات راهبردی و بین‌المللی*، ترجمه پیمان اسماعیلیان، مرکز آینده‌پژوهی علوم و فناوری دفاعی، تهران.
- آشنا، حسام‌الدین (۱۳۸۸)، *درآمدی بر قدرت هوشمند*، مرکز آینده‌پژوهی علوم و فناوری دفاعی، تهران.
- افتخاری، اصغر (۱۳۹۰)، *برآورد تهدید؛ رویکردی نظام‌واره*، دانشگاه عالی دفاع ملی، تهران.
- افتخاری، اصغر (۱۳۸۵)، *کالبدشکافی تهدید*، دانشگاه امام حسین (ع)، تهران.
- امینی، سید جواد و همکاران (۱۳۹۹)، *کاربست روش‌های آینده‌پژوهی در مطالعات امنیتی با تأکید بر تکنیک سناریونویسی GBN*، *فصلنامه امنیت ملی*، دوره ۱۰، شماره ۳۵، صفحه ۳۴-۷.
- پورصادق، ناصر و فرج‌پور علمداری، عباس (۱۳۹۸)، *ارائه الگوی بومی برای سازمان‌های شبکه-ای در نیروهای مسلح با نگاه به جنگ‌های آینده*، *فصلنامه علمی مطالعات مدیریت راهبردی دفاع ملی*، دوره ۳، شماره ۹، صفحه ۳۴-۷.
- دانیالی، سیاوش (۱۳۸۹)، *آمریکا، نظریه قدرت هوشمند و الگوهای ناموفق*، *ماهنامه اطلاعات راهبردی*، شماره ۸۳، سال هشتم.
- رشیدی اقدم، محمود و همکاران (۱۳۹۹)، *طراحی و تبیین الگوی راهبردی مدیریت جهادی*، *فصلنامه علمی مطالعات بین‌رشته‌ای دانش راهبردی*، دوره ۱۰، شماره ۳۹، صفحه ۳۵۸-۳۳۱.
- رضایی، کاظم و همکاران (۱۳۹۸)، *تأثیر تهدیدات زیست‌محیطی بر امنیت ملی (مطالعه موردی: کرانه‌های جنوبی دریای خزر)*، *فصلنامه علمی مطالعات بین‌رشته‌ای دانش راهبردی*، دوره ۸، شماره ۳۱، صفحه ۲۲۳-۲۰۱.
- ره‌پیک، سیامک (۱۳۸۸)، *تهدیدات قدرت ملی، مظاهر و نشانگان*، دانشگاه عالی دفاع ملی، تهران.
- حسنلو، خسرو (۱۳۹۳)، *تدوین نظریه دفاع هوشمند در نظام دفاعی ج.ا.ایران*، رساله دکترا، دانشکده امنیت دانشگاه عالی دفاع ملی، تهران.
- حسنلو، خسرو (۱۳۹۵)، «نظریه دفاع هوشمند در سپهر اندیشه‌های دفاعی»، *فصلنامه مطالعات دفاعی-استراتژیک*، شماره ۶۳.

- حیدری، امیر هوشنگ (۱۳۹۳)، مبانی و مفاهیم آینده پژوهی، *فصلنامه علمی ترویج علم*، سال پنجم، شماره هفتم، صفحه ۹۶-۸۱.
- عبدالله خانی، علی (۱۳۸۹)، *نظریه های امنیت*، چاپ دوم، مؤسسه فرهنگی مطالعات و تحقیقات بین المللی ابرار معاصر، تهران.
- عبدالهی، رضا (۱۳۹۰)، *الگوی بررسی تهدیدها و آسیب پذیری ها*، ساحفاسا، چاپخانه شهید مطهری.
- کبرایی زاده، حسین (۱۳۹۰)، قدرت هوشمند ج.ا.ایران و انقلاب های خاورمیانه، *ماهنامه روابط فرهنگی*.
- گومپرت، دیوید سی و آروینگ لاکو، جاستین پرکینز (۱۳۹۲)، «جنگ هوشمند» ترجمه کریم صارمی، مسعود منزوی، مرکز آینده پژوهی علوم و فناوری دفاعی، تهران.
- متقی، ابراهیم (۱۳۸۷)، قدرت هوشمند آمریکا و استراتژی تغییر در دوران اوباما، *فصلنامه مطالعات و تحقیقات بسیج*، سال یازدهم، شماره ۴۱، صفحه ۷۹-۵۵.
- مرادیان، محسن (۱۳۸۸)، *تهدید و امنیت*، انتشارات شهید صیاد شیرازی، تهران.
- نای، جوزف (۲۰۱۳)، *رهبران سیاسی: قدرت سخت، نرم و هوشمند*.
- نصری، قدیر و رضایی، داود (۱۳۹۸)، مهم ترین تهدیدات فراروی جمهوری اسلامی ایران در اقلیم کردستان عراق، *فصلنامه علمی مطالعات بین رشته ای دانش راهبردی*، دوره ۹، شماره ۳۷، صفحه ۱۹۷-۱۶۸.
- یزدان فام، محمود (۱۳۹۰)، آینده شناسی و برآورد محیط راهبردی: لازمه تصمیم گیری بهتر در امنیت ملی، *فصلنامه مطالعات راهبردی*، دوره ۱۴، شماره ۵۴، صفحه ۳۲-۷.

ب. منابع انگلیسی

- Calin, ted, *Smart power*, (2018) oxford, Blackwell, (CSP)Commission on smart power.
- Chester A. Crocker, (2007) *A Smarter, More Secure America*, A Report of the CSIS Commission on Smart Power, November 6.
- Durch, William J. *Threat analysis and evaluation matrix* The Stimson Center. Report 30, May 1999
- Ernest J. Wilson, III, (2015) The ANNALS of American Academy of Political and Social Science, *Hard Power, Soft Power, Smart Power*, <http://ann.sagepub.com>.
- Ernest J. Wilson, III, (2015) The ANNALS of American Academy of Political and Social Science, *Hard Power, Soft Power, Smart Power*, <http://ann.sagepub.com>.
- Jerome C. Glenn, Elizabeth Florescu, and The Millennium Project Team *State of the Future*, 2015-2016

- Joseph S. Nye Jr, (2011) *The Future of Power*.
- Joseph S. Nye, (2017) *the information revolution and American soft power*, asia pasific review vol 9 /no1.
- Maya KANDEL(2013) *AMERICAN SMART POWER STRATEGIES: redefining leadership in a post-American world*, Under the direction of: Maud QUESSARD-SALVAING.
- Michael Brown, (1996) *The International Diemmmensions of International Conflict, Cambridge*, Massachusetts & Londen, The MIT Press.
- Nossel Suzanne, (2004) *Smart Power*, Foreign Affairs, Volume 83, No. 2.
- Pallaver, Matteo, (2011) "*Power and Its Forms: Hard, Soft, Smart*", (A thesis submitted to the Department of International Relations of the London School of Economics for the degree of Master of Philosophy. London.
- Richard L. Armitage & Joseph S. Nye, Jr, (2017) *A smarter, more secure America*, CSIS COMMISSION ON SMART POWER.
- *Smart Power and U.S. National Strategy*, Joint Special Operations University, JSOU Report 13-3, The JSOU Press, MacDill Air Force Base, Florida, 2017
- Vidalis, Stilianos; Blyth, Andrew, (2002) *Understanding and Development Methodology*, School of Computing, University of Glamorgan.