



## بررسی تهدیدات ناشناخته در جنگ‌های شناختی

ابراهیم سلطانی نسب ۱

### چکیده

امروزه جنگ‌های شناختی به ابزاری قدرتمند در دست دولت‌ها و گروه‌های مختلف تبدیل شده‌اند. اما چالش اساسی این است که بسیاری از تهدیدات موجود در این حوزه به‌طور شفاف قابل شناسایی نیستند. از این‌رو، شناسایی تهدیدات ناشناخته در جنگ‌های شناختی نه تنها برای حفاظت از امنیت ملی، بلکه برای مقابله با تهدیدات نرم ضروری است. هدف اصلی این مقاله بررسی تهدیدات ناشناخته در جنگ‌های شناختی و تحلیل چگونگی تأثیر آنها بر امنیت ملی است. از آنجا که تهدیدات در این حوزه اغلب غیرقابل پیش‌بینی و پیچیده هستند، هدف دیگر این تحقیق شناسایی ویژگی‌ها و مشخصات این تهدیدات بویژه در زمینه‌های فنی، سایبری، روانشناختی و اجتماعی است. علاوه بر این، مقاله با رویکرد توصیفی و تحلیلی به بررسی راهبردهای مقابله با این تهدیدات و پیش‌بینی روش‌های پیشرفته برای شناسایی آنها می‌پردازد. نتایج این مطالعه نشان می‌دهد جنگ‌های شناختی به‌طور فزاینده‌ای به‌عنوان یک تهدید جدید و پیچیده برای امنیت ملی مطرح شده‌اند. این تهدیدات به‌دلیل ویژگی‌هایی همچون سرعت تحول، پیچیدگی فنی و اثرات عمیق روانشناختی و اجتماعی، برای شناسایی و مقابله نیازمند روش‌های نوین و راهبردهای خاص هستند. تهدیدات ناشناخته در قالب فناوری‌های پیشرفته و نوین مانند هوش مصنوعی، اینترنت اشیاء، فضای سایبری، تهدیدات روانشناختی، حملات سایبری و دستکاری‌های اطلاعاتی و تهدیدات فرهنگی و اجتماعی بروز می‌کنند که همگی بر هویت و امنیت ملی تأثیرگذار هستند. شناسایی و مقابله با تهدیدات ناشناخته در جنگ‌های شناختی، نیازمند رویکردی جامع و بین‌رشته‌ای است که شامل همکاری‌های بین بخشی، استفاده از فناوری‌های نوین و تقویت ظرفیت‌های انسانی، سازمانی ملی می‌باشد.

**واژگان کلیدی:** امنیت، تهدید، تهدیدات ناشناخته، جنگ شناختی

**استناد:** سلطانی نسب، ابراهیم؛ (۱۴۰۵). تهدیدات ناشناخته در جنگ‌های شناختی. فصلنامه پژوهش‌های راهبردی/رتش ۵ (۱۶) ۱-۲۵.

۱. دانش آموخته دکتری، آینده پژوهی و حقوق خصوصی، کاندیدای دکترای فلسفه دین، دانشگاه عالی دفاع ملی، تهران، ایران. Email: saeedsoltaninasab@gmail.com

## مقدمه

جنگ‌های شناختی مجموعه‌ای از اقدامات راهبردی هستند که هدف اصلی آن تغییر و دستکاری در فرآیند شناختی، روانشناختی، اجتماعی و... افراد، جوامع است. این جنگ‌ها به‌جای استفاده از قدرت فیزیکی و نظامی، به ابزار اطلاعاتی، روانشناختی و دیجیتال متکی هستند، تا ذهن و رفتار دشمن را تغییر دهند. از دهه‌های اخیر، با پیشرفت فناوری‌های نوین، بویژه اینترنت، رسانه‌های اجتماعی و ابزارهای هوش مصنوعی، این جنگ‌ها به سطح بالایی از پیچیدگی و نفوذ رسیده‌اند. جنگ‌های شناختی نه تنها به‌عنوان یک ابزار سیاسی و نظامی، بلکه به‌عنوان یک چالش بزرگ در عرصه امنیت ملی و جهانی مطرح هستند. امروزه جنگ‌های شناختی به‌طور فزاینده‌ای به ابزاری قدرتمند در دست دولت‌ها و گروه‌های مختلف تبدیل شده‌اند لکن یکی از چالش‌های اساسی این است که بسیاری از تهدیدات موجود در این حوزه به‌طور مستقیم قابل شناسایی و پیش‌بینی نیستند. تهدیدات ناشناخته در جنگ‌های شناختی همگام با سرعت پیشرفت فناوری‌های دیجیتال و ابزارهای هوش مصنوعی، پیچیدگی‌هایی ایجاد کرده است که امکان رصد، شناسایی و مقابله با آنها را دشوار نموده است. این تهدیدات زمانی اهمیت پیدا می‌کنند که تأثیرات آن در سطوح اجتماعی، روانی و اقتصادی در بلندمدت قابل مشاهده است. از همین رو شناسایی و تحلیل تهدیدات ناشناخته در جنگ شناختی برای حفاظت از امنیت ملی، امری ضروری است. پژوهش‌های اولیه در زمینه جنگ‌های شناختی عمدتاً به بررسی تأثیر رسانه‌ها بر افکار عمومی و رفتارهای اجتماعی از جمله استفاده از رسانه جمعی در جنگ‌های جهانی اول و دوم و تحلیل تأثیر رسانه بر تحولات سیاسی و اجتماعی پرداخته. با گسترش اینترنت و شبکه‌های اجتماعی، جنگ شناختی وارد فاز جدیدی از پیچیدگی شده که موجب ظهور تهدیدات غیرقابل پیش‌بینی و ناشناخته گردیده است. مطالعات اخیر بر تهدیدات سایبری و اطلاعاتی تمرکز داشته و به تحلیل استفاده از هوش مصنوعی و فناوری‌های پیشرفته در این نوع جنگ‌ها پرداخته‌اند. لکن هنوز خلأهایی در درک و تحلیل تهدیدات ناشناخته وجود دارد. این تحقیق درصدد است تا به این خلأها پاسخ دهد. هدف اصلی این مقاله بررسی تهدیدات ناشناخته در جنگ‌های شناختی و تأثیر آنها بر امنیت ملی است.

## سؤال تحقیق

- تهدیدات ناشناخته در جنگ‌های شناختی چه ویژگی‌هایی دارند و چگونه بر امنیت ملی تأثیر می‌گذارد؟

## اول) چارچوب نظری<sup>۱</sup>

### الف) مفاهیم پایه ای جنگ های شناختی

۱. جنگ شناختی<sup>۲</sup>: جنگ شناختی به مجموعه ای از تکنیک ها و راهبردها اطلاق می شود که هدف آن تأثیرگذاری بر فرآیندهای شناختی و روانشناختی افراد به منظور تغییر رفتار و تصمیم گیری آنهاست. به تعبیری، جنگ شناختی به معنای استفاده از علوم شناختی در هدف قرار دادن قوه شناخت عموم مردم و نخبگان جامعه هدف با تغییر هنجارها، ارزش ها، باورها، نگرش ها و رفتارها از طریق مدیریت ادراک و برداشت است (جوانی، ۱۴۰۱: ۱۳). این نوع جنگ از ابزارهای اطلاعاتی، رسانه ای و روانشناختی برای دستکاری ذهن انسان ها استفاده می کند. هدف اصلی جنگ شناختی، تسلط بر افکار، اعتقادات و رفتارهای فردی و جمعی با تکیه بر رسانه ها، تبلیغات، اطلاعات جعلی و فناوری های دیجیتال مانند شبکه های اجتماعی است.

۲. انواع جنگ های شناختی: در جنگ های شناختی، از تاکتیک ها و ابزارهای مختلف برای تأثیرگذاری بر ذهن و رفتار انسان ها استفاده می شود. این جنگ ها به طور مستقیم بر پردازش اطلاعات، افکار، باورها، نگرش ها و تصمیمات افراد تأثیر می گذارند و می توانند به شیوه های مختلفی صورت گیرند که برخی از انواع جنگ های شناختی عبارتند از:

- جنگ اطلاعاتی<sup>۳</sup>
- جنگ روانی<sup>۴</sup>
- جنگ شناختی دیجیتال<sup>۵</sup>
- جنگ رسانه ای<sup>۶</sup>
- جنگ شناختی اجتماعی<sup>۷</sup>
- جنگ سایبری<sup>۸</sup>
- جنگ شناختی فرهنگی<sup>۹</sup>

| برخی از انواع جنگ های شناختی |                                                                                                                                                    |                                                        |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| نوع                          | تعریف                                                                                                                                              | ویژگی ها                                               |
| جنگ اطلاعاتی                 | مجموعه ای از فنون شامل گردآوری، انتقال، حفاظت، جلوگیری از دسترسی، ایجاد اغتشاش و افت کیفیت در اطلاعات که به وسیله آن یکی از طرفین درگیر با دشمنان، | - تحریف اطلاعات و دستکاری واقعیت ها برای تغییر باورها. |

<sup>۱</sup>. Theoretical Framework

<sup>۲</sup>. Cognitive Warfare

<sup>۳</sup>. Information Warfare

<sup>۴</sup>. Psychological Warfare

<sup>۵</sup>. Digital Cognitive Warfare

<sup>۶</sup>. Media Cognitive Warfare

<sup>۷</sup>. Social Cognitive Warfare

<sup>۸</sup>. Cyber Cognitive Warfare

<sup>۹</sup>. Cultural Cognitive Warfare

|                    |                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                         |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | <p>خود به مزیت چشمگیری دست یافته و آن را حفظ می‌کند (قربان زاده سوار و همکاران، ۱۳۹۷:۴۲)</p>                                                                                                                                                 | <p>- انتشار اخبار جعلی و اطلاعات نادرست جهت تغییر نگرش‌ها.</p> <p>- استفاده از رسانه‌های اجتماعی برای گسترش یا مسدود کردن اطلاعات خاص.</p>                                                                                                              |
| جنگ روانی          | <p>استفاده دقیق از تبلیغات و دیگر اعمالی است که منظور اصلی آن، تأثیر گذاری بر عقاید، احساسات، تمایلات و رفتار دشمن، گروه بی طرف و یا گروه دوست است، به نحوی که پشتیبانی برای برآوردن مقاصد و اهداف ملی باشد (بیدگلی و همکاران، ۱۴۰:۱۳۹۹)</p> | <p>- ایجاد ترس، اضطراب یا بی‌اعتمادی در میان مردم از طریق اخبار نگران‌کننده یا تهدیدات.</p> <p>- انتشار شایعات غلط برای کاهش اعتماد به نفس جمعی.</p> <p>- تقویت احساسات منفی یا خصومت میان گروه‌ها یا ملت‌ها.</p>                                       |
| جنگ شناختی دیجیتال | <p>در این نوع جنگ‌ها به استفاده از فناوری‌های دیجیتال و ابزارهای آنلاین برای تأثیرگذاری بر ذهن و رفتار افراد تأکید می‌گردد.</p>                                                                                                              | <p>- استفاده از شبکه‌های اجتماعی برای پخش اطلاعات خاص یا دستکاری افکار عمومی.</p> <p>- به‌کارگیری الگوریتم‌های هوش مصنوعی برای شبیه‌سازی رفتارهای انسانی و تأثیرگذاری بر آنها.</p> <p>- تغییرات عمدی در هویت‌های آنلاین برای تغییر افکار و رفتارها.</p> |
| جنگ رسانه‌ای       | <p>در این نوع جنگ‌ها رسانه‌ها به‌عنوان ابزار محوری و اصلی برای تأثیرگذاری بر باورها، ارزش‌ها و نگرش‌های افراد استفاده می‌شوند</p>                                                                                                            | <p>- تبلیغات سیاسی و رسانه‌ای برای شکل‌دهی به نظر عمومی و تغییر رفتار مردم.</p> <p>- استفاده از رسانه‌ها برای ایجاد قطب‌بندی‌های اجتماعی.</p> <p>- پخش پیام‌های دوقطبی و جنجالی برای تحریک احساسات و تغییر ذهنیت عمومی.</p>                             |
| جنگ شناختی اجتماعی | <p>به تأثیرگذاری بر ساختارهای اجتماعی و فرهنگی جوامع برای تغییر رفتارهای جمعی و فردی اطلاق می‌شود</p>                                                                                                                                        | <p>- دستکاری در هویت‌های فرهنگی و اجتماعی از طریق تأثیرگذاری بر هنجارها و باورهای عمومی.</p> <p>- استفاده از جنبش‌ها یا بحران‌های اجتماعی به‌منظور تغییر رفتارها.</p> <p>- ترویج یا سرکوب ارزش‌های خاص برای تأثیرگذاری بر جامعه هدف.</p>                |
| جنگ سایبری         | <p>عبارت است از؛ اقدامات آفندی غیر متحرکی که به منظور کسب برتری اطلاعاتی از طریق تحت تأثیر قراردادن سامانه اطلاعاتی و شبکه‌های رایانه‌ای دشمن اتخاذ می‌گردد (کلمنس، ۱۹۹۹)</p>                                                                | <p>- حمله سایبری به زیرساخت‌های اطلاعاتی برای تغییر و تخریب داده‌ها.</p> <p>- دستکاری در پروفایل‌های آنلاین و هویت‌های دیجیتال افراد.</p> <p>- استفاده از نرم‌افزارهای مخرب برای تحت تأثیر قرار دادن سیستم‌های تصمیم‌گیری و اطلاعات.</p>                |
| جنگ شناختی فرهنگی  | <p>هدف دشمن تغییر در ارزش‌ها، هنجارها و فرهنگ‌های جوامع هدف است. این نوع جنگ به‌منظور دستکاری هویت‌های جمعی و ایجاد تنش‌های فرهنگی به‌ویژه در جوامع چند فرهنگی به‌کار گرفته می‌شود. (عراقی، بیدگلی، رجبی، ۱۴۰۱)</p>                          | <p>- تضعیف فرهنگ‌ها یا هویت‌های قومی و مذهبی از طریق تبلیغات فرهنگی و رسانه‌ای.</p> <p>- ایجاد شکاف‌های فرهنگی و قومی در جوامع به‌منظور تضعیف همبستگی اجتماعی.</p> <p>- تغییر در ترجیحات و ارزش‌های فرهنگی از طریق تبلیغات و محتواهای رسانه‌ای.</p>     |

جنگ‌های شناختی به‌عنوان یک پدیده چند بُعدی و هیبریدی در دنیای معاصر مطرح‌اند که می‌تواند تأثیرات عمیقی بر جوامع، گروه‌ها و افراد بگذارد. این جنگ‌ها بصورت دیجیتال، روانشناختی، اجتماعی، فرهنگی و سایبری به وقوع می‌پیوندند و با استفاده از ابزارهای مختلف رسانه‌ای، شبکه‌های اجتماعی، پروپاگاندا، هوش مصنوعی، بر ذهن و رفتار انسان‌ها تأثیرگذار هستند. فهم دقیق این جنگ‌ها می‌تواند در مقابله با تهدیدات ناشناخته در این حوزه کمک شایانی کند. در جدول ذیل خلاصه تطبیقی تعاریف و ویژگی‌های انواع جنگ‌های شناختی به اختصار آمده است:

**۳. تاکتیک‌های جنگ شناختی<sup>۱</sup>:** تاکتیک‌های جنگ شناختی، روش‌ها و راهبردهایی است که در آنها از اطلاعات، تبلیغات، پروپاگاندا، روانشناسی و ابزارهای دیجیتال برای کنترل ذهن و رفتار افراد و گروه‌ها استفاده می‌شود. این تاکتیک‌ها می‌توانند شامل موارد زیر باشند:

- **تبلیغات و پروپاگاندا:** استفاده از پیام‌های هدفمند برای تغییر نگرش‌ها و باورهای عمومی و همراه کردن افکار عمومی با بهره‌گیری، از رسانه‌های مختلف مثل تلویزیون، رادیو، اینترنت و شبکه‌های اجتماعی برای انتشار اطلاعات نادرست یا تحریف‌شده.

- **دستکاری رسانه‌های اجتماعی:** تدوین و انتشار محتوای جعلی، اخبار دروغین یا تغییرات عمدی در هویت‌های آنلاین به‌منظور ایجاد اثرات روانی و اجتماعی خاص برای تأثیرگذاری در دوران بحران‌ها یا انتخابات‌ها.

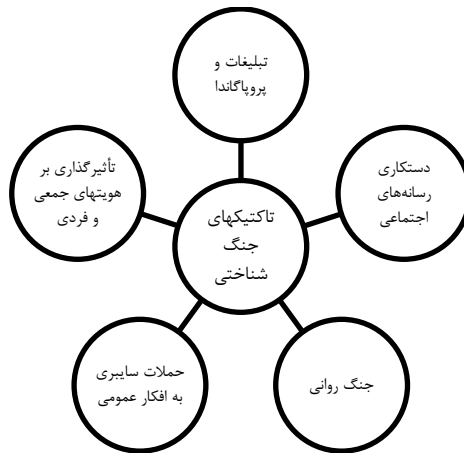
- **جنگ روانی:** به‌کارگیری تکنیک‌های روانشناختی برای تحت فشار قرار دادن، ترساندن و فریب دادن جامعه هدف که شامل تهدیدات، تحریکات یا ایجاد انحراف در افکار عمومی شود.

- **حملات سایبری به افکار عمومی:** استفاده از حملات سایبری به‌منظور تأثیرگذاری مستقیم بر اطلاعات و داده‌های عمومی به‌عنوان ابزارهای جنگ شناختی برای تغییر رفتارهای جمعی.

- **تأثیرگذاری بر هویت‌های جمعی و فردی:** تغییر یا تحریف هویت‌های فرهنگی، اجتماعی و سیاسی از طریق استفاده از تکنیک‌های شناختی به‌ویژه در سطح جهانی که شامل دستکاری در اصول اخلاقی و فرهنگی جوامع جهت کنترل رفتارها و تصمیمات عمومی هستند.

با توجه به رشد روزافزون فناوری‌های دیجیتال، نرم‌افزارهای شناختی و تاکتیک‌های پیچیده این جنگ‌ها به ابزاری قدرتمند برای تأثیرگذاری بر افکار و رفتار انسان‌ها تبدیل شده‌اند. به همین دلیل، شناسایی و تحلیل تهدیدات ناشناخته در جنگ‌های شناختی و همچنین طراحی راهکارهای مقابله با آنها، از اهمیت ویژه‌ای برخوردار است.

<sup>۱</sup>. Cognitive Warfare Tactics



۴. **مؤلفه‌های اصلی جنگ شناختی:** جنگ شناختی هر حوزه‌ای را شامل می‌شود که بتوان از طریق اطلاعات بر ادراک، نگرش‌ها، ایدئولوژی و اراده تأثیر گذاشت. می‌توان گفت، تغییر نگرش در جامعه، اختلال و خطا در دستگاه محاسباتی تصمیم گیران، اثر بخش کردن جنگ اطلاعاتی، ایجاد شکاف و گسست عاطفی \_ ادراکی بین طیف‌های مختلف جامعه و نخبگان با حاکمیت و زوال سرمایه اجتماعی، از کار ویژه‌های جنگ شناختی به شمار می‌آید. در یک جمع‌بندی کلی مؤلفه‌های اصلی جنگ شناختی را می‌توان بشرح ذیل خلاصه نمود:

| ردیف | مؤلفه‌های اصلی جنگ شناختی                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ۱    | جنگ شناختی همه عناصر، حوزه‌ها، ابعاد و سطوح جنگ را دربرمی‌گیرد؛ تأثیر بر این عناصر بصورت ماهواره‌ای تداوم و گسترش یافتند، به‌طوری که برآیند قدرتمند آن به شکل یک تأثیر غیرمستقیم روانی وارد حوزه شناخت حریف گردیده و نهایتاً به تغییر رفتار آنها منجر شود.                                                                                                                                                                                                                                                                                                                                                                    |
| ۲    | جنگ شناختی باید معطوف به اهداف نهایی و وضعیت مطلوب پایان جنگ باشد؛ در واقع روش شناسی جنگ شناختی تغییری اساسی در طرح‌ریزی و اجرای عملیات نظامی بوده و گستره وسیع‌تری از گزینه‌ها را برای تصمیم‌سازان ملی فراهم می‌سازد. به‌طور حتم نمی‌توان از دستیابی به تأثیرات مورد نظر مطمئن بود، اما این روش می‌تواند تا حدی از وقوع تأثیرات منفی بکاهد و حداقل این فایده را دارد که بجای درگیری رودر روی نیروهای خودی و دشمن در میدان نبرد به امکان ایجاد تأثیراتی فکر کرد که در راستای اهداف کلان ملی به مقاصد عملیاتی مناسب منتهی شوند.                                                                                                |
| ۳    | ترکیب و ادغام مداوم فرآیندهای طرح‌ریزی، اجرا و ارزیابی؛ باعث شکل‌گیری جنگ شناختی در قالب یک کل انعطاف‌پذیر می‌شود. بدین ترتیب، در جنگ شناختی به‌عنوان مدل عینی بعد پنجم جنگ، مفهوم تأثیرات شأن و جایگاه جداگانه مطمح نظر قرار می‌گیرند، از جمله؛ الف) پیش‌بینی و مدیریت تأثیرات مستقیم و غیرمستقیم ناشی از اقدامات فیزیکی برای ورود به حوزه شناخت مخاطب و نهایتاً تغییر رفتار وی، ب) به‌عنوان یک نیروی برتری ساز، ج) برای ایجاد انعطاف‌پذیری در رفتار (عملیات) خود و رها شدن از ساختار سلسله‌مراتبی خشک و رایج در طرح‌ریزی کلاسیک که با شروع عملیات و پیچیده شدن شرایط، امکان تغییرات به موقع در نحوه انجام عملیات میسر نیست. |

|   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ۴ | جنگ شناختی بجای تکیه بر سیستم های تسلیحاتی بر ایجاد تاثیرات متمرکز است؛ تسلیحات پیشرفته در جنگ شناختی از اصالت ذاتی برخوردار نیست و همه بازیگران حتی بازیگران غیردولتی می توانند بدون برخورداری از سکوهای پیشرفته جنگی و با معطوف شدن به تاثیرات، الگوی خود را از جنگ شناختی تصاحب کنند.                                                                                                                                                                                                                                                                                           |
| ۵ | در جنگ شناختی همه انواع تاثیرات مورد توجه قرار می گیرند؛ جنگ شناختی باید گستره کامل تاثیرات یک اقدام را مورد توجه قرار دهد تا بتواند ضمن افزایش گزینه های فراروی تصمیم سازان، برآوردی واقع بینانه از تاثیرات و نتایج ناخواسته را به آنها ارائه کند.                                                                                                                                                                                                                                                                                                                                |
| ۶ | در جنگ شناختی باید بیش از کارایی به اثربخشی توجه شود؛ کارایی از نظر کمی عمدتاً قابلیت های فنی و سخت افزاری را شامل می شود، ولی فلسفه جنگ شناختی غالباً بر اثربخشی اقدامات تاکید دارد که امری است کاملاً کیفی. بدیهی است که معیارهای سنجش کارایی و اثربخشی با یکدیگر متفاوتند. چه بسا عملکرد یک واحد رزمی براساس معیار کارایی (هنر و مهارت به کارگیری قابلیت های خودی در مقابل دشمن) درخشان ارزیابی شود، ولی از نظر اثربخشی (تغییر رفتار دشمن) نمره قبولی را به خود اختصاص ندهد، نتوانسته اند به اهداف نهایی خود دست یابند.                                                         |
| ۷ | در جنگ شناختی، جنگ عرصه رویارویی سیستم های سازمانده پیچیده تفسیر می شود؛ سیستم های سازمانده پیچیده، تعریفی نمادین از موجودات زنده اند که با نهادینه کردن شناخت در فرآیند حیات می توانند طی تعاملی اثربخش با محیط پیرامون به بقای خود ادامه دهند. همین ماهیت به سازمانهای رزم تعمیم داده شد و این نتیجه حاصل شد که بهره گیری از مزیت های بعد پنجم در گروه همین رفتار است. جنگ برخورد و تصادم نیروهای زنده ای تصور می شود که به شیوه های خلاقانه در پی انطباق پذیری با محرک های پیرامون خود هستند. این امر بیانگر مبانی دانشی نوینی مانند نظریه های آشوب و پیچیدگی قابل مدلسازی است. |
| ۸ | در جنگ شناختی، آگاهی جامع از شرایط فضای رزم در رسیدن به پیروزی بسیار حائز اهمیت است، اما واقعیت این است که ماهیت این آگاهی نزد همه بازیگران یکسان نیست. (شاه محمدی، فاطمی، ۱۴۰۳)                                                                                                                                                                                                                                                                                                                                                                                                   |

**ب) تعریف تهدیدات ناشناخته:** در یک تعریف کلی؛ تهدیدات ناشناخته تهدیداتی هستند که به طور شفاف قابل رصد و پیش بینی نبوده و معمولاً از سوی مراجع رسمی یا متخصصان امنیتی نادیده گرفته می شوند و به طور ناپیدا بر روی اهداف خود تأثیر می گذارند. تهدید ناشناخته تهدیدی است که هیچ علامت و امضای شناخته شده ای ندارد که بتوان آن را شناسایی نمود. به دیگر عبارت؛ تهدید ناشناخته تهدیدی است که توانسته از کنترل های امنیتی موجود در سیستم مورد آماج، عبور کند بدون اینکه هیچ یک از کنترل گره های نشانه ای از وجود آن را شناسایی، دریافت و اعلام نمایند. (سلطانی نسب، ۱۴۰۳) این تهدیدات به ویژه در فضای جنگ های شناختی برجسته هستند، زیرا آنها از ابزارهایی مانند: اطلاعات، رسانه ها، فناوری های دیجیتال و... استفاده می کنند که در لحظه به راحتی قابل شناسایی یا درک نیستند. در جنگ های شناختی، این تهدیدات سرعت گسترش می یابند و می توانند از طریق ابزارهای دیجیتال، شبکه های اجتماعی و پروپاگاندا تأثیرات وسیعی داشته باشند. در حقیقت، تهدیدات ناشناخته در جنگ های شناختی غالباً از ویژگی هایی برخوردارند که آنها را از تهدیدات سنتی متمایز می کند. ویژگی های اصلی این تهدیدات شامل؛ ناشناختگی، تغییرات سریع و غیرقابل پیش بینی، پیچیدگی بالا، تأثیرات غیرمستقیم و غیرشفاف بر افکار، احساسات و رفتارهای

انسانی است. تهدیدات ناشناخته معمولاً در قالب‌هایی ظاهر می‌شوند که تشخیص آنها غیرممکن و دشوار است و مدت زمانی طول می‌کشد تا اثرات آنها آشکار شوند. (همان)

**ج) انواع تهدیدات ناشناخته در جنگ‌های شناختی:** در جنگ شناختی، ممکن است که تهدید ماهیتاً ناشناخته نباشد و ما بتوانیم عوامل تهدیدزا را به‌طور مستقیم و غیر مستقیم بشناسیم و برای مقابله با آن تدابیر لازم را اتخاذ کنیم، اما در تهدید ناشناخته اساساً ما عامل را تهدید نمی‌دانیم لکن همان عامل، ابزار یا روند قابل اطمینان، ممکن است با تغییر در کارکرد یا الگوریتم یا فرآیند، به‌طور مستقیم یا غیرمستقیم بر رفتار و تصمیمات کل سیستم یا عوامل فنی و انسانی جامعه هدف تأثیر گذاشته و به عاملی مخرب در سیستم تبدیل شود. در این بخش برخی از تهدیدات را نام می‌بریم که با انواع شناسای آن مشترک هستند اما وصف ناشناختگی در این تهدیدات تأثیر بیشتری در صدمه بر سیستم خواهند داشت:

**\* تغییرات الگوریتم‌های هوش مصنوعی<sup>۱</sup>:** یکی از تهدیدات ناشناخته در این حوزه، نشستن الگوریتم ناشناخته هوش مصنوعی بجای الگوریتم اصلی و دستکاری ناگهانی در این الگوریتم است که می‌تواند خطر دستکاری تصمیمات را برای سیستم بدنال داشته باشد.

**\* جنگ اطلاعاتی<sup>۲</sup>:** همانطور که پیش از این بیان شد، جنگ اطلاعاتی یکی از عمده‌ترین روش‌ها، ابزارها و تاکتیک‌های مرسوم در جنگ‌های شناختی است. این مورد شامل استفاده از اطلاعات به‌عنوان سلاح برای تغییر ذهن و رفتارهای گروه‌ها یا جوامع است. برخی از تاکتیک‌های این جنگ عبارتند از: انتشار اخبار جعلی، تحریف تاریخ و واقعیت‌ها، تأثیرات روانشناختی. اما مؤلفه ناشناختگی این بخش آن است که در جنگ شناختی مبتنی بر نبرد اطلاعاتی منبع تأمین خبر مورد اطمینان و مرکز تحلیل اطلاعات و اخبار و احساسات و افکاری که تاکنون هیچ ناهمگونی و ناهماهنگی با اهداف سیستم و روندهای جاری آن نداشته به ناگاه اطلاعات، تحلیل‌ها و داده‌هایی را به سیستم تزریق می‌کند که نه تنها صحیح نیستند بلکه موجب بروز خطا در بخش‌های تصمیم‌سازی شده و خسارات جبران ناپذیری به سیستم وارد می‌نمایند. این منبع تهدید از مدت‌ها قبل در سیستم نفوذ نموده و خود را به‌عنوان عامل خودی در ساختار جانمایی کرده است لکن در زمان مقتضی ضربه خود را به سیستم وارد می‌نماید.

**\* تغییرات در فضای سایبری:** فضای سایبری امروزه یکی از بزرگترین عرصه‌ها برای ایجاد تهدیدات ناشناخته است. این تهدیدات می‌توانند شامل حملات ناشناخته سایبری به

<sup>۱</sup>.artificial intelligence

<sup>۲</sup>. Information Warfare

زیرساخت های اطلاعاتی، سرقت پنهان داده ها، تغییر غیر محسوس در اطلاعات حیاتی و حتی دستکاری ناملموس و مخفیانه در سیستم های ارتباطی باشند. عامل تهدیدات ناشناخته معمولاً از روش های ذیل در این عرصه استفاده می شود: حملات نامحسوس سایبری هدفمند، هک و دستکاری اطلاعات، تغییرات غیر قابل شناسایی در شبکه های اجتماعی.

**\*مدیریت ذهن و افکار عمومی<sup>۱</sup>:** مدیریت ذهن و افکار عمومی از پیچیده ترین تهدیدات جنگ های شناختی است. این تهدید شامل دستکاری غیر محسوس و زیر آستانه ای در افکار و تصمیمات افراد از طریق روانشناسی، رسانه ها و پروپاگاندا است. هدف آن ایجاد تغییر در نگرش های جمعی یا فردی به گونه ای است که افراد به طور غیرارادی با بهره گیری از روش های آشفتگی روانشناختی، کنترل افکار عمومی از طریق رسانه ها، (عیوضی، محمد رحیم؛ ۱۳۸۸)، تأثیرگذاری بر هویت های جمعی، به سمت اهداف خاص هدایت شوند. تهدیدات ناشناخته در جنگ های شناختی به عنوان یکی از بزرگ ترین چالش ها در دنیای معاصر مطرح هستند. این نوع از تهدیدات بر عکس تهدیدات معمول، قابل پیش بینی و شناسایی نیستند، به ویژه در فضای دیجیتال و با استفاده از ابزارهای نوین مانند؛ هوش مصنوعی، جنگ اطلاعاتی، حملات سایبری، دستکاری ذهن و افکار عمومی به طور مؤثرتر و غیر قابل تشخیص بر افکار و رفتارهای فردی و جمعی تأثیر می گذارند. تحلیل دقیق و شبیه سازی این تهدیدات می تواند به سیاست گذاران و متخصصان کمک کند تا در خصوص نحوه شناسایی و مقابله با این نوع از تهدیدات تصمیمات صحیح، به جا و مؤثری اتخاذ نمایند.

## دوم) روش تحقیق

در این پژوهش به منظور فهم تهدیدات ناشناخته و نحوه مواجهه راهبردی با آن ابتدا توصیفی کلی از این پدیده و ابعاد آن ارائه شده و در ادامه با رویکرد تحلیلی راهبردهای مقابله با آن بیان گردید. هدف در روش توصیفی\_تحلیلی، توصیف و تحلیل ابعاد پدیده مورد مطالعه و شرایط آن می باشد؛ در ابتدا توصیفی نسبتاً جامع از جنگ های شناختی ارائه شده است. به طوری که علاوه بر تشریح مفهومی این پدیده عناصر و اجزای آن نیز در ساحت های مختلف احصا شده است. در ادامه همین روند در خصوص مفهوم کلیدی دیگر این پژوهش یعنی تهدیدات ناشناخته نیز صورت پذیرفته است. در این روش محقق با شناخت عمیق تر پدیده و شرایط وقوع آن و ارائه مدل مفهومی کمک شایانی به نظام تصمیم گیری در آن خصوص می نماید.

<sup>1</sup>. Mind Management and Public Opinion Control

- **تشریح مفهومی کرده:** یعنی تعریف دقیقی از جنگ شناختی ارائه داده و آن را با مفاهیم مشابه (مانند جنگ روانی، تبلیغات) مقایسه کرده است.
  - **عناصر و اجزا را احصا (شمارش و شناسایی) کرده:** یعنی مؤلفه‌های تشکیل‌دهنده جنگ شناختی (مانند: نقش رسانه‌ها، استفاده از هوش مصنوعی، هدف قرار دادن باورها و اعتقادات، نبرد در فضای سایبری و ...) را فهرست و بررسی کرده است.
  - **ساحت‌های مختلف را بررسی کرده:** یعنی جنگ شناختی را در حوزه‌های گوناگون (سیاسی، اجتماعی، فرهنگی، امنیتی، نظامی) تحلیل کرده است.
- پژوهشگر دقیقاً همان فرآیند دقیق (توصیف مفهومی، شناسایی اجزا و بررسی در حوزه‌های مختلف) را برای مفهوم محوری دیگر پژوهش، یعنی "تهدیدات ناشناخته" نیز تکرار کرده است. این تهدیدات می‌توانند شامل خطرانی باشند که هنوز به طور کامل شناسایی نشده‌اند، ماهیت پیچیده‌ای دارند یا در قالب‌های جدیدی ظاهر می‌شوند.

این پژوهش علمی با روش توصیفی-تحلیلی انجام شده تا دو پدیده به هم مرتبط "جنگ شناختی" و "تهدیدات ناشناخته" را به طور عمیق بررسی کند. این پژوهش تنها به تعریف این مفاهیم بسنده نکرده، بلکه اجزای آنها را در حوزه‌های مختلف کالبدشکافی کرده و در نهایت یک مدل مفهومی ارائه داده است. هدف نهایی این پژوهش، کمک به نظام تصمیم‌گیری برای درک بهتر این تهدیدات پیچیده و اتخاذ راهبردهای هوشمندانه برای مقابله با آنهاست. این تحقیق ماهیتی بنیادی-کاربردی دارد؛ هم به توسعه دانش کمک می‌کند و هم کاربرد عملی و راهبردی مستقیم دارد.

### سوم) تحلیل تهدیدات ناشناخته در جنگ‌های شناختی

#### الف) تهدیدات ناشناخته فنی و فناوری در جنگ‌های شناختی

جنگ‌های شناختی با ظهور فناوری‌های نوین که قادرند بیش از گذشته به‌طور مستقیم و غیرمستقیم بر افکار و تصمیمات تأثیر بگذارند، به سرعت در حال پیچیده‌تر شدن هستند. بسترهای فنی و فناورانه چون هوش مصنوعی، اینترنت اشیاء<sup>۱</sup> و تحلیل داده‌ها، به ابزارهای تهدیدآمیزی تبدیل شده‌اند که در جنگ‌های شناختی برای دستکاری و تغییر ذهن انسان‌ها

<sup>۱</sup>. Internet of Things

به کار گرفته می شوند. این تهدیدات به دلیل سرعت توسعه و پیچیدگی بالا در انواع جدیدتر خود، می توانند به تهدیداتی ناشناخته و غیرقابل پیش بینی تبدیل شوند که در صورت اجرا، اثرات گسترده ای بر جامعه و سیاست گذاری های ملی بگذارند. برای نمونه ذیلأ به چند نوع از این فناوری ها و خطرات احتمالی آنها در حوزه تهدیدات ناشناخته اشاره می نماییم:

۱. **هوش مصنوعی<sup>۱</sup> (AI) و تهدیدات ناشناخته آن:** هوش مصنوعی، در عرصه جنگ های شناختی، به ابزاری مهم برای تحلیل و پیش بینی رفتارهای انسانی تبدیل شده است. با استفاده از الگوریتم ها و مدل های یادگیری ماشین، هوش مصنوعی می توان بر اساس جمع آوری و تحلیل داده های کلان<sup>۲</sup> به طور مؤثر روندهای اجتماعی و سیاسی را پیش بینی کرده و بر افکار عمومی تأثیر گذاشت. اما آنچه که موجب خطرناک تر شدن هوش مصنوعی شده ناشناخته بودن آثار به کارگیری آن در عرصه جنگ های شناختی است، چرا که هیچ گونه کنترل و نظارتی بر نتایج حاصل از هوش مصنوعی در جنگ های شناختی وجود ندارد. برخی از ویژگی های تهدیدات ناشناخته هوش مصنوعی در جنگ شناختی عبارتند از: دستکاری احساسات و افکار عمومی، جعل های عمیق<sup>۳</sup>، بازی های روانشناختی با استفاده از AI.

۲. **اینترنت اشیاء<sup>۴</sup> (IoT) و تهدیدات ناشناخته آن:** اینترنت اشیاء به شبکه ای از دستگاه های متصل به اینترنت اطلاق می شود که قادر به جمع آوری و تبادل داده ها هستند. این فناوری به طور گسترده در خانه ها، صنایع و حتی تجهیزات نظامی در حال استفاده است، تهدیدات جدیدی را به همراه دارد که برخی از ویژگی های IoT در جنگ شناختی عبارتند از: نظارت و جمع آوری اطلاعات حساس، دستکاری و اختلال در زیرساخت های IoT، ایجاد اثرات روانشناختی از طریق دستگاه ها. تهدیدات ناشناخته در حوزه اینترنت اشیاء از ترکیب فناوری های ناهمگون، محدودیت های سخت افزاری و رفتارهای غیر قابل پیش بینی کاربران نشأت می گیرد. این تهدیدات به دلیل پویایی اکوسیستم IoT، ناشناخته باقی می ماند و امکان شناسایی و مقابله آنها پیش از وقوع دشوار است. خطراتی مانند حملات مبتنی بر هوش مصنوعی، نفوذ از طریق زنجیره تأمین یا سوء استفاده از داده های پیش بینی نشده، نمونه هایی از این چالش های پنهان هستند که امنیت سایبری را به طور جدی تهدید می کنند.

<sup>۱</sup>. Artificial intelligence

<sup>۲</sup>. Big Data

<sup>۳</sup>. Deepfakes

<sup>۴</sup>. internet of things

| نوع تهدیدات ناشناخته در اینترنت اشیاء | اثرات                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ۱                                     | <ul style="list-style-type: none"> <li>• آسیب پذیرهای سخت افزاری ناشناخته: محدودیت‌های محاسباتی (CPU/RAM) مانع شناسایی نقاط ضعف در طراحی چیپست‌ها و حسگرها می‌شود.</li> <li>• فریمورهای دارای کدهای مخفی: وجود backdoor ها یا توابع ناشناخته در فریمورهای اختصاصی که ممکن است سال‌ها بدون تشخیص باقی بمانند.</li> </ul> |
| ۲                                     | <ul style="list-style-type: none"> <li>• پروتکل‌های غیر استاندارد: استفاده از پروتکل‌های ارتباطی اختصاصی که آسیب پذیریهایی آنها هنوز شناسایی نشده است.</li> <li>• حملات مبتنی بر زمان واقعی: دستکاری داده‌های حساس (مانند اطلاعات پزشکی) در حین انتقال، بدون ایجاد رد پای آشکار.</li> </ul>                             |
| ۳                                     | <ul style="list-style-type: none"> <li>• بات‌نت‌های خود مختار: استفاده از الگوریتم‌های هوش مصنوعی در بات‌نت‌ها برای تغییر الگوی حملات بصورت خودکار و غیر قابل ردیابی.</li> <li>• حملات انبوه مبتنی بر روندهای رفتاری: سوء استفاده از داده‌های جمع‌آوری شده برای شناسایی الگوهای آسیب پذیری در شبکه‌ها</li> </ul>        |
| ۴                                     | <ul style="list-style-type: none"> <li>• نقاط ضعف در سرویس‌های اشتراکی: آسیب پذیری‌های مشترک در پلتفرم‌های ابری که به‌طور همزمان هزاران دستگاه IoT را تحت تأثیر قرار می‌دهند.</li> <li>• حملات لایه ابر _ دستگاه: بهره برداری از تعاملات غیر منتظره بین سیستم‌های ابری و دستگاه‌های محلی</li> </ul>                     |
| ۵                                     | <ul style="list-style-type: none"> <li>• شناسایی ناخواسته کاربران: افشای هویت کاربران از طریق تحلیل متا دیتاهای به ظاهر بی خطر مانند الگوی استفاده از دستگاه.</li> <li>• داده‌های ترکیبی: استنتاج اطلاعات حساس از ترکیب داده‌های غیر مرتبط که به تنهایی بی خطر به نظر می‌رسند.</li> </ul>                               |
| ۶                                     | <ul style="list-style-type: none"> <li>• اجزای آلوده پیش از نصب: نفوذ بدافزار به دستگاه‌ها در مراحل تولید یا توزیع بدون اطلاع کاربر نهایی</li> <li>• وابستگی دیتا بیس‌های منسوخ: استفاده ناخواسته از کدهای قدیمی در توسعه نرم افزارها که حاوی آسیب‌پذیری‌های کشف نشده هستند.</li> </ul>                                 |
| ۷                                     | <ul style="list-style-type: none"> <li>• حملات کوانتومی علیه دستگاه‌های قدیمی: ناتوانی دستگاه‌های IoT فعلی در مقاومت در برابر الگوریتم‌های رمزگشایی کوانتومی.</li> <li>• دستکاری مدل‌های یادگیری ماشین: تغییر رفتار دستگاه‌های هوشمند با تزریق داده‌های مخرب به سیستم‌های مبتنی بر AI.</li> </ul>                       |

به‌طور کلی تهدیدات ناشناخته IoT، چالشی پیچیده و پویا هستند که ریشه در ماهیت ناهمگون و سریع تغییر بودن این آن دارند. بسیاری از این خطرات، مانند حملات مبتنی بر هوش مصنوعی یا نفوذ از طریق زنجیره تأمین، تنها زمانی آشکار می‌شوند که زیر ساخت‌ها

به طور وسیع مورد بهره برداری قرار گیرند. مقابله با این تهدیدات نیازمند تحولی اساسی در رویکردهای امنیتی است؛ از استانداردسازی پروتکل ها و بهبود شفافیت زنجیره تأمین تا توسعه راهکارهای رمزنگاری پساکوانتومی و سیستم های نظارتی مبتنی بر هوش مصنوعی. با پیش بینی سناریوهای غیر متعارف و سرمایه گذاری در تحقیقات میان رشته ای می توان از تبدیل شدن IoT از یک فرصت به تهدید و مخاطره ناشناخته جلوگیری به عمل آورد.

**۳. تحلیل داده ها<sup>۱</sup> و تهدیدات ناشناخته آن:** در دنیای جنگ های شناختی، تحلیل داده ها ابزار قدرتمندی برای شبیه سازی و پیش بینی واکنش ها و رفتارهای انسانی است. با پیشرفت های اخیر در تحلیل داده های کلان و یادگیری ماشینی، این فناوری ها می توانند به طور دقیق و مؤثر برای پیش بینی رفتارهای فردی و جمعی استفاده شوند و همزمان تهدیدات جدیدی را در جنگ های شناختی با منشأهایی ناشناخته ایجاد کنند. ویژگی ها و تهدیدات ناشناخته تحلیل داده ها در جنگ شناختی عبارتند از: تحلیل رفتار و پیش بینی واکنش ها، دستکاری داده ها به منظور ایجاد سردرگمی، شبیه سازی افکار عمومی و ایجاد تقسیمات اجتماعی همه موارد فوق در حالی است که به دلیل پیچیده بودن و عدم شناخت ابعاد و کارکرد هوش مصنوعی و نیز فقدان نظارت بر عملکردهای آن واجد وصف ناشناختگی است.

**۴. واقعیت افزوده<sup>۲</sup> و واقعیت مجازی<sup>۳</sup>:** این فناوری ها می توانند دنیای مصنوعی بسازند که به طور کامل دنیای واقعی فرد را تغییر دهند. در جنگ شناختی، می توان از این فناوری ها برای تغییر در ادراک و احساسات افراد و حتی ایجاد تجربه های ذهنی خاص استفاده کرد که به طور کامل بر تصمیم گیری آنها تأثیرگذار باشد. وجه ناشناختگی این تهدیدات؛ اولاً در عدم تسلط کامل ما بر این فناوری ها است به طوری که عمده کشورها مصرف کننده کالاهای فناوری محور هستند و از تهدیدات نهفته در این ابزارها اطلاعی ندارند. ثانیاً به دلیل وارداتی بودن این ابزارها و سطح بالای فناوری در آنها و نیز گره خوردن زندگی روزمره مردم به آنها و در نتیجه تقاضای غیر معمول بازار، امکان کشف خطر در این ابزارها به سادگی وجود ندارد.

### ب) تهدیدات ناشناخته انسانی و روانشناختی در جنگ های شناختی

جنگ های شناختی نه تنها ابعاد فناورانه دارند، بلکه ابعاد انسانی و روانشناختی نیز در آنها نقش اساسی ایفا می کنند. مسئله آنجا پیچیده تر می شود که به دلیل ترکیب ابعاد فناورانه جنگ های شناختی که عموماً برای ما غیر شناسا می باشد با تهدیدات انسانی و روانشناختی ترکیب شده و تبدیل به تهدیداتی ناشناخته می شوند که مقابله با آنها را برای جوامع مورد آماج دشوار

<sup>۱</sup>. Data Analytics

<sup>۲</sup>. augmented reality

<sup>۳</sup>. virtual reality

می‌نماید. تهدیدات ناشناخته در این حوزه شامل استفاده از روش‌های جنگ‌های روانی، تحلیل رفتارشناسی و دستکاری افکار و احساسات انسانی است. این تهدیدات به دلیل تأثیرات غیرقابل مشاهده‌ای که بر اذهان دارند، از پیچیدگی خاصی برخوردارند. در این بخش به تحلیل این تهدیدات از منظر رفتارشناسی، جنگ روانی و اثرات اجتماعی می‌پردازیم.

**۱. جنگ روانی<sup>۱</sup> و تهدیدات ناشناخته آن:** جنگ روانی در جنگ‌های شناختی به مجموعه‌ای از تکنیک‌ها اطلاق می‌شود که هدف آنها ایجاد اثرات روانشناختی و عاطفی بر افکار و رفتارهای فردی یا جمعی است. به تعبیر دیگر جنگ روانی عبارت است از استفاده طراحی شده از تبلیغات و ابزارهای مربوط به آن برای نفوذ در خصوصیات فکری ... (شیرازی، ۱۳۷۶) این تهدیدات به‌ویژه به دلیل استفاده از ابزارهایی مانند؛ رسانه‌ها، اطلاعات دستکاری‌شده و پروپاگاندا برای تغییر یا هدایت نگرش‌ها و احساسات عمومی، تأثیرات قابل توجهی دارند که این تأثیرات مستقیماً قوه شناخت و ادراک جامعه هدف را مورد آماج قرار می‌دهد. ویژگی‌های جنگ روانی در جنگ‌های شناختی: ایجاد ترس و اضطراب، (رستمی و همکاران، ۱۴۰۱)، دستکاری احساسات و هویت جمعی، (صفری نژاد، ۱۴۰۰)، اختلاف افکنی، ایجاد تفرقه و ترویج یأس، ناتوانی و بی‌اعتمادی، (بهمنی، ۱۴۰۳). دلیل اینکه ویژگی‌های فوق واجد صفت ناشناختگی است، این است که منشأ ایجاد آنها توسط عواملی دامن زده می‌شود که به‌طور معمول برای سیستم داخلی تهدید آشکار محسوب نمی‌شوند. خصیصه مهم عوامل تهدیدات ناشناخته در جنگ‌های روانی؛ صبر راهبردی، شناسایی دقیق محیط میزبان و جایگیری مناسب در آن می‌باشد.

**۲. تحلیل رفتارشناسی و تهدیدات ناشناخته آن:** تحلیل رفتارشناسی در جنگ‌های شناختی به مطالعه و شبیه‌سازی رفتارهای انسانی و اجتماعی به‌منظور پیش‌بینی و هدایت تصمیمات فردی و جمعی اشاره دارد. پیشرفت‌ها در تحلیل داده‌ها و روانشناسی باعث شده‌اند که این ابزارها در جنگ‌های شناختی برای دستکاری رفتارهای انسانی به‌طور فزاینده‌ای مورد استفاده قرار گیرند. برخی از این تحلیل‌های رفتارشناسی در جنگ‌های شناختی عبارتند از: پیش‌بینی و هدایت رفتارهای جمعی، دستکاری انگیزه‌ها و تصمیمات فردی، نظارت و کنترل بر روی رفتارهای فردی و گروهی. تهدیدات ناشناخته در رفتارشناسی به چالش‌هایی اشاره دارد که به دلیل ماهیت پیچیده و غیر قابل پیش‌بینی بودن رفتار انسان شناسایی و مدیریت آنها دشوار است. این تهدیدات ممکن است ناشی از محدودیت‌های ذاتی مدل‌های تحلیلی،

<sup>1</sup>. Psychological Warfare

تغییرات محیطی، یا ظهور پدیده‌های نوین باشند. برخی از ابعاد کلیدی این تهدیدات عبارتند از:

- محدودیت‌های مدل‌های تحلیلی موجود: به دلیل، سوگیری‌های داده‌ها، خطای پیش‌بینی در شرایط عدم قطعیت، وابستگی به فرضیات ناکامل.
- پویایی و انطباق پذیری رفتارها: با توجه به تغییرات سریع رفتاری به عنوان مثال تقلب رفتاری در سیستم‌های امنیتی، تأثیر فناوری‌های نوین همچون دیپ فیک‌ها.
- پیچیدگی‌های روانشناختی و فرهنگی: رفتارهای ناخودآگاه و پارادوکسیکال، دستکاری روانی، تفاوت‌های فرهنگی.
- تهدیدات ناشی از فناوری‌های پیشرفته: تغییر عمده داده‌ها برای فریب مدل‌های یادگیری، شبیه سازی رفتار انسان.
- خطرات اخلاقی و حریم خصوصی: نقض حریم خصوصی افراد، سوگیری الگوریتمی.
- عدم قطعیت‌های محیطی و اکوسیستمی: تأثیر عوامل بیرونی ناشناخته، ظهور رفتارهای غیر خطی و آشوبناک.

تحلیل رفتارشناسی در مواجهه با تهدیدات ناشناخته نیازمند رویکردی انعطاف‌پذیر، چندلایه و همواره شکاک است تا بتواند همزمان با تحولات پویای انسانی و فناوری تکامل یابد.

**۳. تهدیدات ناشناخته اثرات اجتماعی جنگ‌های شناختی:** تهدیدات ناشناخته به دلیل ماهیت ناشناختگی و بلند مدت، غیرخطی و تعاملی، جامعه را در معرض فروپاشی زیر ساخت‌های فکری و اخلاقی قرار می‌دهد. این تهدیدات با تضعیف واقعیت مشترک و دستکاری سازوکارهای شکل دهنده هویت اجتماعی، پایه‌های همزیستی اجتماعی را به مخاطره می‌اندازند. برخی از اثرات اجتماعی جنگ‌های شناختی عبارتند از: بحران‌های اجتماعی و سیاسی، فرسایش اعتماد اجتماعی با افزایش شکاف‌های اجتماعی و کاهش همبستگی، تخریبی با ایجاد تغییرات در هویت اجتماعی و فرهنگی.

### ج) تهدیدات ناشناخته فرهنگی و اجتماعی در جنگ‌های شناختی

جنگ‌های شناختی علاوه بر تهدیدات فناورانه به‌طور فزاینده‌ای بر ابعاد فرهنگی و اجتماعی جوامع نیز تأثیر می‌گذارند. این تهدیدات در راستای تغییرات تحریف مفاهیم فرهنگی و اجتماعی جوامع هدف، به‌عنوان یکی از مؤلفه‌های اصلی جنگ شناختی ظاهر می‌شوند. اکنون، به تحلیل نحوه تأثیرگذاری جنگ‌های شناختی بر هویت فرهنگی و اجتماعی جوامع هدف می‌پردازیم.

۱. **تأثیرگذاری بر هویت فرهنگی و اجتماعی:** هویت فرهنگی و اجتماعی هر جامعه ترکیبی از تاریخ، زبان، سنت‌ها، ارزش‌ها و باورهای مشترک اعضای آن است. این هویت‌ها می‌توانند به‌طور قابل توجهی در برابر تهدیدات خارجی مقاومت کنند، اما در جنگ‌های شناختی، تلاش‌های زیادی برای دستکاری و تغییر آنها انجام می‌شود. تأثیرات جنگ‌های شناختی بر هویت فرهنگی و اجتماعی از این قبیل هستند: فرهنگ‌سازی و تغییر در ارزش‌ها و باورها، تضعیف و تجزیه هویت ملی از طریق تحریف تاریخ، گسترش هویت‌های چندگانه و تفرقه.

۲. **تأثیر رسانه‌های اجتماعی و فناوری‌های نوین:** رسانه‌های اجتماعی ابزارهایی هستند که به‌طور گسترده‌ای در جنگ‌های شناختی برای تأثیرگذاری بر فرهنگ و اجتماع به‌کار گرفته می‌شوند. این ابزارها به‌ویژه در ایجاد تغییرات فرهنگی و اجتماعی تأثیر شگرفی دارند، زیرا قابلیت دسترسی و سرعت انتشار اطلاعات را فراهم می‌آورند. ویژگی‌ها و تهدیدات ناشناخته رسانه‌های اجتماعی و فناوری‌های نوین: گسترش پیام‌های فرهنگی تحریف‌شده، ترویج ایده‌ها و ارزش‌های بیگانه به‌ویژه در میان جوانان، ایجاد بحران هویتی با کمک الگوریتم‌های آنلاین.

۳. **تأثیرات اقتصادی و اجتماعی ناشی از تغییرات فرهنگی:** تغییرات فرهنگی و اجتماعی به‌ویژه در نتیجه دستکاری‌های جنگ شناختی می‌توانند اثرات قابل توجهی بر ساختار اقتصادی و اجتماعی جامعه هدف باشند. این تغییرات می‌توانند موجب تغییر در روابط اقتصادی و اجتماعی و ساختارهای خانوادگی شوند. ویژگی‌ها و تهدیدات ناشناخته اثرات اقتصادی و اجتماعی تغییرات فرهنگی: اختلال در الگوهای مصرف و رفتارهای اقتصادی، آسیب به نهادهای اجتماعی، تضعیف همبستگی اجتماعی و انسجام ملی.

۴. **تأثیرات تغییرات فرهنگی بر سیاست‌گذاری عمومی:** تغییرات فرهنگی ناشی از جنگ‌های شناختی می‌تواند تأثیرات عمیقی بر سیاست‌گذاری عمومی و تصمیم‌گیری‌های دولتی داشته باشد. سیاست‌گذاران تحت تأثیر تغییرات فرهنگی و اجتماعی قرار می‌گیرند و این تأثیرات می‌توانند بر اولویت‌ها و رویکردهای سیاست‌گذاری آنها تأثیر بگذارند. تهدیدات ناشناخته در جنگ‌های شناختی حوزه فرهنگی و اجتماعی با هدف قراردادن هویت جمعی، ارزش‌ها و روابط انسانی، زیر ساخت‌های نامرئی جوامع را تخریب می‌کند. این نوع از تهدیدات دلیل ماهیت غیر مستقیم و بلند مدت خود به عمق وجود ساختارهای اجتماعی نفوذ می‌کنند. تهدیدات ناشناخته در جنگ‌های شناختی حوزه فرهنگی و اجتماعی، با استفاده از ابزارها و رویکردهایی همچون؛ تجزیه هویت ملی، نرمالیزاسیون خشونت نمادین، جعل حافظه جمعی، شبیه سازی فرهنگ‌ها و تضعیف آیین‌های جمعی، به تخریب نرم افزار ذهن جمعی جامعه به نحوی می‌پردازد که توانایی بازسازی خود را از دست می‌دهد.

## چهارم) راهبردهای مقابله با تهدیدات ناشناخته<sup>۱</sup>

**الف) راهبردهای مقابله با تهدیدات ناشناخته در جنگ های شناختی؛ راهبردهای دفاعی:** جنگ های شناختی به ویژه با تهدیدات ناشناخته ای که به طور فزاینده ای پیچیده و پرابهام هستند، می توانند به شدت به امنیت ملی و انسجام اجتماعی جوامع آسیب برسانند. بنابراین، مقابله با این تهدیدات نیازمند اتخاذ مجموعه ای از راهبردهای دفاعی مختلف است. این راهبردها باید بگونه ای طراحی شوند که بتوانند از هویت فرهنگی، اجتماعی، اطلاعاتی و امنیتی جامعه در برابر تهدیدات شناختی محافظت کنند. در این بخش، به طور مشروح به راهبردهای دفاعی برای مقابله با تهدیدات ناشناخته در جنگ های شناختی خواهیم پرداخت.

**۱. تقویت امنیت سایبری:** یکی از اصلی ترین تهدیدات ناشناخته در جنگ های شناختی، حملات سایبری و تهدیدات مرتبط با فضای دیجیتال است. برای مقابله با این تهدیدات، تقویت امنیت سایبری به عنوان اولین خط دفاعی ضروری است. این امنیت باید به طور ویژه در برابر تهدیداتی که از طریق سیستم ها و زیرساخت های دیجیتال به افکار عمومی، هویت فرهنگی و حتی امنیت ملی آسیب می زنند، تقویت شود.

| تقویت امنیت سایبری                        |                                                          |
|-------------------------------------------|----------------------------------------------------------|
| ارتقاء زیرساخت های سایبری                 | - تقویت سیستم های دفاعی<br>- ایجاد شبکه های امن اطلاعاتی |
| افزایش آگاهی عمومی در مورد تهدیدات سایبری | - آموزش عمومی                                            |
| ایجاد هماهنگی بین المللی در امنیت سایبری  | - همکاری بین المللی                                      |

**۲. آموزش و فرهنگ سازی:** یکی از بهترین راهبردهای مقابله با تهدیدات ناشناخته در جنگ های شناختی، فرهنگ سازی و آموزش عمومی در سطوح مختلف اجتماعی و سیاسی است. این امر نه تنها می تواند موجب افزایش آگاهی و آمادگی در برابر تهدیدات شناختی شود، بلکه توانمندی های دفاعی جوامع را تقویت می کند.

| آموزش و فرهنگ سازی                               |                                                      |
|--------------------------------------------------|------------------------------------------------------|
| ایجاد آگاهی درباره جنگ های شناختی و تکنیک های آن | - آموزش در مقیاس عمومی<br>- آموزش در محیط های آموزشی |
| آموزش مهارت های تفکر انتقادی                     | - توسعه مهارت های تحلیل اطلاعات                      |
| تقویت فرهنگ همکاری و همبستگی اجتماعی             | - ترویج همبستگی و مسئولیت اجتماعی                    |

<sup>۱</sup>. Countermeasures to Unknown Threats

**۳. تقویت نظام‌های اطلاعاتی و روانشناختی:** یکی دیگر از راهبردهای دفاعی مقابله با تهدیدات ناشناخته در جنگ‌های شناختی، تقویت نظام‌های اطلاعاتی و روانشناختی است. در این بخش، نیاز به راهبردهای دفاعی خاص برای مقابله با حملات اطلاعاتی، تغییر در ذهنیت و رفتار افراد و همچنین مدیریت بحرانها داریم.

| تقویت نظام‌های اطلاعاتی و روانشناختی          |                                                                                                    |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------|
| تقویت نظام‌های اطلاعاتی و کنترل جریان اطلاعات | - ایجاد و تقویت شبکه‌های اطلاعاتی معتبر<br>- آموزش و به‌کارگیری خبرگان در زمینه تحلیل اطلاعات      |
| تقویت نظام‌های روان‌شناختی و مدیریت ذهن       | - پیشگیری از جنگ روانی و تحلیل رفتارهای جمعی<br>- ایجاد سیستم‌های پاسخگویی روان‌شناختی در بحران‌ها |
| پاسخگویی سریع به حملات اطلاعاتی و روانی       | - تشکیل تیم‌های واکنش سریع                                                                         |

مقابله با تهدیدات ناشناخته در جنگ‌های شناختی نیازمند رویکردی جامع و چندجانبه است که در آن امنیت سایبری، آموزش و فرهنگ‌سازی، و تقویت نظام‌های اطلاعاتی و روانشناختی در کنار هم قرار می‌گیرند. این راهبردها باید به‌طور هماهنگ اجرا شوند تا جامعه هدف بتواند در برابر تهدیدات ناشناخته مقاومت کند و تاب‌آوری اجتماعی و فرهنگی خود را حفظ نماید.

**ب) نقش سیاست‌گذاری در مقابله با تهدیدات ناشناخته در جنگ‌های شناختی:** پاسخ به تهدیدات ناشناخته در جنگ‌های شناختی، علاوه بر نیاز به رویکردهای فنی، فرهنگی، روانشناختی و اجتماعی، به اتخاذ تصمیمات راهبردی و سیاست‌گذاری‌های مؤثر در سطوح دولتی و بین‌المللی بستگی دارد. سیاست‌گذاری صحیح در زمان بحران، به‌ویژه در مواجهه با تهدیدات پیچیده و چندوجهی که در جنگ‌های شناختی بروز می‌کنند، می‌تواند اثرات عمیق و پایداری در حفاظت از امنیت ملی داشته باشد. در این بخش، به نقش سیاست‌گذاری و تصمیم‌گیری در مقابله با تهدیدات شناختی و تحلیل اثرات و ویژگی‌های کلیدی سیاست‌گذاری در زمینه جنگ‌های شناختی و تهدیدات ناشناخته خواهیم پرداخت.

**۱. تأثیر تصمیمات سیاسی در مقابله با تهدیدات شناختی:** تصمیمات سیاسی و راهبردی در هر سطح از حکومت، تأثیر عمیقی بر نحوه مواجهه با تهدیدات شناختی دارند. در این زمینه، سیاست‌گذاری‌ها می‌توانند به‌طور مستقیم بر اقدامات دفاعی، توسعه زیرساخت‌های امنیتی، آموزش عمومی و مدیریت بحران‌های شناختی تأثیر بگذارند. مهم‌ترین جنبه‌هایی که تصمیمات سیاسی در آن‌ها اثرگذار هستند، به شرح زیر است:

| تأثیر تصمیمات سیاسی در مقابله باتهدیدات شناختی            |                                                                                                          |
|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| تدوین قوانین و سیاست های امنیتی در فضای سایبری و اطلاعاتی | - ایجاد چارچوب های قانونی برای مقابله با تهدیدات اطلاعاتی<br>- قوانین مقابله با جنگ روانی و تبلیغات دشمن |
| تصمیمات سیاسی در مواجهه با بحران های شناختی و اطلاعاتی    | - تعامل بین المللی در مقابله با تهدیدات شناختی<br>- ایجاد مراکز واکنش سریع دولتی                         |

**۲. ویژگی های سیاست گذاری مؤثر در مقابله با تهدیدات شناختی:** در مواجهه با تهدیدات ناشناخته در جنگ های شناختی، سیاست گذاری مؤثر باید ویژگی های خاصی داشته باشد که به طور خاص به ماهیت این تهدیدات توجه داشته باشد. این ویژگی ها عبارتند از:

| ویژگی های سیاست گذاری مؤثر در مقابله با تهدیدات شناختی |
|--------------------------------------------------------|
| انعطاف پذیری در سیاست گذاری                            |
| هماهنگی بین نهادهای مختلف                              |
| استفاده از فناوری و نوآوری                             |
| توجه به ابعاد روان شناختی و اجتماعی                    |

**۳. چالش ها و مشکلات در سیاست گذاری برای مقابله با تهدیدات شناختی:** در حالی که سیاست گذاری در مقابله با تهدیدات شناختی می تواند نقش بسیار مهمی ایفا کند، این مسیر با چالش های متعددی مواجه است: پیچیدگی و نوآوری تهدیدات، تنش های سیاسی و فرهنگی، خطرات نقض حریم خصوصی. نقش سیاست گذاری و تصمیم گیری در مقابله با تهدیدات ناشناخته در جنگ های شناختی بسیار حیاتی است. تصمیمات راهبردی می توانند نقش کلیدی در حفاظت از امنیت ملی ایفا کنند و تهدیدات شناختی را به طور مؤثر کاهش دهند. سیاست گذاری مؤثر باید به گونه ای باشد که به ابعاد مختلف این تهدیدات توجه کرده و هماهنگی میان نهادها را تسهیل کند. با اتخاذ تصمیمات دقیق، کشورهای هدف می توانند از تهدیدات شناختی پیشگیری کرده و از تاب آوری اجتماعی و روانشناختی خود در برابر تهدیدات محافظت کنند.

### ج) پیش بینی تهدیدات ناشناخته آینده در جنگ های شناختی

پیش بینی تهدیدات ناشناخته در جنگ های شناختی به معنای شناسایی، تحلیل و آمادگی برای مقابله با تهدیداتی است که هنوز شناخته نشده اند، اما می توانند به سرعت در آینده ظاهر شوند و تأثیرات عمیقی بر امنیت اجتماعی، فرهنگی، سیاسی و اقتصادی جوامع بگذارند. تهدیدات ناشناخته در این حوزه به ویژه به دلیل سرعت پیشرفت فناوری، تغییرات اجتماعی و روانشناختی و تکامل روش های جدید جنگ شناختی، به یک چالش پیچیده تبدیل شده اند. پیش بینی تهدیدات ناشناخته در جنگ های شناختی نیازمند یک رویکرد سیستماتیک،

آینده‌نگر و بین‌رشته‌ای است که به‌طور همزمان جنبه‌های مختلف تهدیدات از جمله سایبری، روانشناختی، اجتماعی و اطلاعاتی را در نظر بگیرد. در این بخش به روش‌ها و راهکارهای پیش‌بینی تهدیدات ناشناخته آینده در جنگ‌های شناختی می‌پردازیم.

**۱. روش‌ها و رویکردهای پیش‌بینی تهدیدات ناشناخته:** برای پیش‌بینی تهدیدات ناشناخته در جنگ‌های شناختی، چندین روش و رویکرد مختلف وجود دارد که می‌تواند به تصمیم‌گیرندگان کمک کنند تا با آمادگی بیشتری به تهدیدات احتمالی پاسخ دهند:

- **استفاده از تحلیل روندها<sup>۱</sup>:** تحلیل روندها یکی از روش‌های مؤثر برای پیش‌بینی تهدیدات است. با مطالعه روندهای فعلی در زمینه‌های مختلف مانند فناوری، سیاست، رسانه‌ها و روان‌شناسی اجتماعی، می‌توان تغییرات و تهدیدات بالقوه را شناسایی کرد. این تحلیل به‌ویژه در زمینه‌های نوظهور مانند هوش مصنوعی، اینترنت اشیاء، تغییرات فرهنگی و اجتماعی، و حتی تغییرات در رفتار گروهی افراد می‌تواند اطلاعات ارزشمندی به دست دهد. به‌طور مثال؛ تحلیل تغییرات در الگوهای مصرف رسانه‌ای، روندهای دموگرافیک، تغییرات در قوانین مربوط به حریم خصوصی و امنیت سایبری، و حرکت به‌سوی استفاده گسترده از فناوری‌های نوین مانند بلاک‌چین و هوش مصنوعی می‌تواند به شناسایی تهدیدات آینده کمک کند.
- **استفاده از مدل‌های پیش‌بینی با استفاده از داده‌های بزرگ:** یکی از مؤثرترین روش‌ها برای پیش‌بینی تهدیدات ناشناخته، استفاده از تحلیل داده‌های کلان است. با بهره‌گیری از الگوریتم‌های پیچیده یادگیری ماشین و هوش مصنوعی، می‌توان حجم زیادی از داده‌ها را تجزیه و تحلیل کرده و الگوهای رفتاری و پدیده‌های نوظهور را شبیه‌سازی کرد. مثلاً؛ جمع‌آوری و تجزیه و تحلیل داده‌ها از شبکه‌های اجتماعی، منابع خبری، وب‌سایت‌ها و... برای شناسایی الگوهای تغییر رفتار اجتماعی و سیاسی افراد، به‌ویژه در بحران‌ها و بحرانهای اطلاعاتی، می‌تواند به پیش‌بینی تهدیدات بالقوه کمک کند.

- **استفاده از شبیه‌سازی‌های پیچیده<sup>۲</sup>:** شبیه‌سازی‌های پیچیده اجتماعی و روانشناختی، یکی از راه‌های مؤثر برای پیش‌بینی واکنش‌ها و رفتارهای انسانی در مواجهه با تهدیدات شناختی است. این شبیه‌سازی‌ها می‌توانند فرآیندهای

<sup>۱</sup>. Trend Analysis

<sup>۲</sup>. Complex Simulations

روانشناختی، اجتماعی و... را مدلسازی کرده و واکنش های جوامع را به سناریوهای مختلف تهدیدات شبیه سازی کنند. مثلاً؛ شبیه سازی واکنش های جمعی به حملات اطلاعاتی و جنگ روانی در فضای سایبری، بررسی تأثیرات تغییرات الگوریتم های هوش مصنوعی در تعاملات اجتماعی یا مدلسازی تأثیرات بحران ها بر ذهنیت و رفتار گروه ها می تواند به شناسایی تهدیدات بالقوه در جنگ های شناختی کمک کند.

- **استفاده از پیش بینی های راهبردی<sup>۱</sup>:** پیش بینی راهبردی یا آینده پژوهی، رویکردی میان رشته ای است که با استفاده از اطلاعات موجود و تکنیک های مختلف، تلاش می کند به شبیه سازی آینده و شناسایی تهدیدات نوظهور بپردازد. در این روش، سناریوهایی از آینده های ممکن طراحی می شود که می تواند به تصمیم گیران کمک کند تا برای تهدیدات بالقوه آماده شوند. طراحی سناریوهای مختلف در زمینه هایی چون تغییرات در سیاست های جهانی، تحولات اجتماعی و فرهنگی، پیشرفت های فناوریانه و تغییرات در الگوهای جنگ و اطلاعات می تواند به شناسایی تهدیدات و فرصت های ناشناخته کمک کند.

۲. **پیش بینی تهدیدات ناشناخته در جنگ های شناختی:** برای پیش بینی تهدیدات ناشناخته در جنگ های شناختی، تدابیری باید اتخاذ شود تا بتوانند درک بهتری از تهدیدات آینده ایجاد کنند و به طور مؤثر به آنها پاسخ دهند. این موارد عبارتند از:

- **آموزش و توانمندسازی متخصصان حوزه جنگ های شناختی:** یکی از مؤثرترین راه ها برای پیش بینی تهدیدات، آموزش و توانمندسازی متخصصان در زمینه های مختلف از جمله امنیت سایبری، علوم سیاسی، روانشناسی اجتماعی، و فناوری های نوین است. این متخصصان باید توانایی شبیه سازی، تحلیل و پیش بینی تهدیدات ناشناخته در جنگ های شناختی را داشته و در فرآیند تصمیم گیری های راهبردی وارد شوند.

- **تقویت سیستم های هشدار سریع:** سیستم های هشدار سریع می توانند به طور مؤثر برای شناسایی تهدیدات جدید در جنگ های شناختی طراحی شوند. این سیستم ها با استفاده از الگوریتم ها و ابزارهای تحلیلی، تهدیدات جدید در فضای سایبری، رسانه ها و فضاهای اجتماعی را شناسایی کرده و به مقامات ذی ربط هشدار می دهند تا اقدامات پیشگیرانه انجام شود.

<sup>۱</sup>. Strategic Foresight

- **ایجاد سناریوهای آینده‌پژوهی و برنامه‌های پیش‌بینی:** دولت‌ها و سازمان‌ها باید به‌طور منظم سناریوهای مختلف از آینده را بررسی کرده و برنامه‌های پیش‌بینی برای مقابله با آنها طراحی کنند. این سناریوها می‌توانند شامل حملات اطلاعاتی، بحران‌های روانی، تغییرات در فضای سایبری و شیوه‌های نوین جنگ روانی باشند. با طراحی این سناریوها، سازمان‌ها می‌توانند برای هر نوع تهدید احتمالی آماده شوند.

- **سرمایه‌گذاری در تحقیق و توسعه (R&D):** تحقیق و توسعه در زمینه‌های مرتبط با جنگ‌های شناختی مانند هوش مصنوعی، علوم اعصاب، روانشناسی اجتماعی، فناوری‌های ارتباطی و تحلیل داده‌ها، می‌تواند به شناسایی و پیش‌بینی تهدیدات ناشناخته کمک کند. سرمایه‌گذاری در این زمینه‌ها به کشورها این امکان را می‌دهد که با پیشرفت‌های جدید همگام شوند و تهدیدات نوظهور را شبیه‌سازی و تحلیل کنند.

۳. **ایجاد مرکز کشف خطر:** یکی از اقدامات مهم برای پیش‌بینی تهدیدات ناشناخته، تأسیس و راه‌اندازی مراکز کشف خطر است. این مراکز می‌توانند به‌عنوان مراکز تحقیقات و تحلیل‌های پیشرفته در زمینه شناسایی و پیش‌بینی تهدیدات ناشناخته در جنگ‌های شناختی عمل کنند. این مراکز با همکاری نهادهای دولتی و خصوصی، تحقیقات علمی و فناوری را در جهت شناسایی تهدیدات نوظهور در ابعاد مختلف انجام می‌دهند. تأسیس و راه‌اندازی مراکز تخصصی کشف خطر در حوزه جنگ‌های شناختی، با توجه به پیچیدگی و تنوع تهدیدات، می‌تواند به‌عنوان یک گام مؤثر در تقویت امنیت ملی و مقابله با تهدیدات نوظهور عمل کند.

- **اهداف و وظایف مرکز کشف خطر:**

- **شناسایی تهدیدات نوظهور:** مرکز باید با استفاده از ابزارهای پیشرفته، تهدیدات جدید در حوزه جنگ‌های شناختی را شناسایی کند. این تهدیدات ممکن است شامل حملات سایبری پیچیده، دستکاری‌های اطلاعاتی، تغییرات در فضای سایبری و تأثیر بر هویت فرهنگی و اجتماعی جوامع هدف باشد.

- **تحلیل و پیش‌بینی تهدیدات:** با بهره‌گیری از مدل‌های تحلیلی و شبیه‌سازی‌های پیچیده، مرکز می‌تواند الگوهای تهدیدات را شبیه‌سازی کرده و پیش‌بینی‌هایی درباره رفتار و واکنش‌های احتمالی دشمن ارائه دهد.

<sup>1</sup>. Threat Detection Center

- توسعه راهبردهای مقابله‌ای: بر اساس تحلیل‌های انجام‌شده، مرکز باید راهبردهای مؤثری برای مقابله با تهدیدات شناسایی‌شده تدوین کند. این راهبردها می‌توانند شامل تقویت زیرساختهای امنیتی، آموزش و فرهنگ‌سازی عمومی، و توسعه سیستم‌های هشدار سریع باشند.

#### • ساختار و منابع مورد نیاز:

\_\_ تجهیزات و فناوری‌های پیشرفته: مرکز نیازمند دسترسی به فناوری‌های نوین مانند هوش مصنوعی، تحلیل داده‌های کلان و شبیه‌سازی‌های پیچیده است تا بتواند تهدیدات را به صورت دقیق شبیه‌سازی و تحلیل کند.

\_\_ تیم‌های تخصصی: تأسیس تیم‌های متخصص در حوزه‌های مختلف مانند امنیت سایبری، روانشناسی اجتماعی، علوم سیاسی و فناوری اطلاعات ضروری است تا بتواند تهدیدات را از زوایای مختلف بررسی کنند.

\_\_ بودجه و منابع مالی: تأمین منابع مالی کافی برای خرید تجهیزات، استخدام نیروی انسانی متخصص و انجام پروژه‌های تحقیقاتی، از جمله نیازهای اساسی مرکز است.

#### پنجم) نتیجه گیری و پیشنهادات عملی

##### ▪ نتیجه‌گیری

تحقیق حاضر به بررسی مختصات تهدیدات ناشناخته در جنگ‌های شناختی و تحلیل ابعاد مختلف آنها پرداخته است. نتایج نشان می‌دهد که جنگ‌های شناختی به‌طور فزاینده‌ای به‌عنوان یک تهدید جدید و پیچیده برای امنیت ملی مطرح شده‌اند. این تهدیدات به‌دلیل ویژگی‌های خاص خود، از جمله سرعت تحول، پیچیدگی فنی و روانشناختی، و اثرات عمیق اجتماعی، نیازمند روش‌های نوین و راهبردهای خاص برای شناسایی و مقابله هستند. تهدیدات ناشناخته شامل پیشرفت‌های فنی و فناوری‌های نوین مانند هوش مصنوعی، اینترنت اشیاء و تغییرات در فضای سایبری، تهدیدات انسانی و روانشناختی، حملات سایبری و دستکاری‌های اطلاعاتی و تهدیدات فرهنگی و اجتماعی هستند که همگی می‌توانند بر هویت ملی و امنیت جهانی تأثیر بگذارند. همچنین، شناسایی این تهدیدات از طریق مدل‌های پیش‌بینی، تحلیل داده‌های کلان و شبیه‌سازی‌های پیچیده، به‌ویژه با استفاده از مراکز کشف خطر، امری ضروری برای آمادگی در برابر آنهاست. با توجه به سرعت رشد فناوری‌ها، پیچیدگی‌های اجتماعی و روانشناختی و توسعه روش‌های نوین جنگ‌های شناختی، شناسایی و مقابله با تهدیدات

ناشناخته به‌عنوان یک ضرورت اساسی برای امنیت ملی مطرح است. تهدیدات شناختی می‌توانند به‌طور مستقیم بر فرآیند تصمیم‌گیری‌های سیاسی، روانشناسی جمعی و منافع اقتصادی کشورها تأثیرگذار باشند. در دنیای امروز، که وابستگی به اطلاعات و فضای دیجیتال به حد اکثر رسیده است، ناتوانی در شناسایی و پیش‌بینی این تهدیدات می‌تواند منجر به آسیب‌های جدی به زیر ساخت‌های حیاتی امنیت ملی گردد. بنابراین، مقابله با این تهدیدات برای دفاع از هویت ملی ضروری است. تهدیدات ناشناخته به‌دلیل ماهیت زیر پوستی و تأثیرگذاری غیر مستقیم، به مراتب مخرب‌تر از سایر تهدیدات عمل می‌کند. این پدیده ناشناخته با تضعیف سوژه انسانی به مثابه هسته جامعه مدرن، نه تنها نظم موجود را بلکه امکان شکل‌گیری آلترناتیوهای اخلاقی آینده را نیز نابود می‌کند. خطر اصلی در این است که تهدیدات ناشناخته پیش از آنکه به‌طور کامل شناخته یا درک شوند به بخشی از «دی. ان. ای اجتماعی» تبدیل شوند و تاب آوری جمعی را از درون متلاشی نمایند!

#### ▪ پیشنهادات عملی

برای مقابله مؤثر با تهدیدات ناشناخته در جنگ‌های شناختی، پیشنهاداتی عملی در سیاست‌ها و راهبردها به‌شرح زیر مطرح می‌شود:

- توسعه اکوسیستم‌های شناختی مقاوم: مبتنی بر آموزش چند لایه.
- ایجاد رادارهای شناختی: برای رصد فعالیت‌های غیرمترعارف در داده‌های رفتاری.
- راه‌اندازی مراکز کشف خطر: تأسیس مراکز تخصصی کشف خطر در حوزه جنگ‌های شناختی، به‌عنوان یک اقدام راهبردی، می‌تواند نقش به‌سزایی در شناسایی، تحلیل و پیش‌بینی تهدیدات نوظهور ایفا کند. این مراکز با بهره‌گیری از فناوری‌های پیشرفته، تیم‌های متخصص و همکاری‌های بین‌رشته‌ای، قادر به ارائه راهکارهای مؤثر برای مقابله با تهدیدات پیچیده و چندوجهی جنگ‌های شناختی خواهند بود.

|                           |                                                             |
|---------------------------|-------------------------------------------------------------|
| بازتعریف امنیت انسانی     | با محوریت حفاظت از حافظه و هویت انسانی و عاملیت جمعی        |
| ایجاد نهادهای بین‌رشته‌ای | بمنظور رصد و مدلسازی اثرات ثانویه جنگ‌های شناختی            |
| تقریب فرهنگی              | ایجاد پلتفرم‌های گفتگوی بین‌فرهنگی برای مقابله با قطبی‌سازی |

در نهایت، شناسایی و مقابله با تهدیدات ناشناخته در جنگ‌های شناختی، نیازمند رویکردی جامع و بین‌رشته‌ای است که شامل همکاری‌های بین بخشی، استفاده از فناوری‌های نوین و تقویت ظرفیت‌های انسانی، سازمانی ملی می‌باشد. این اقدامات می‌توانند به‌طور مؤثر از جوامع در برابر تهدیدات ناشناخته، به‌خصوص در جنگ‌های شناختی محافظت کنند و به ایجاد امنیت

پایدار کمک نمایند. این جنگ‌ها، نبرد بر سر «معنای انسان بودن» است و پیروزی در آن مستلزم حفاظت از تنوع فرهنگی به عنوان زیربنای تاب آوری اجتماعی است. «جنگ‌های شناختی بیش و پیش از آنکه نبرد «سلاح» باشد، نبرد «معنا» است و پیروزی در این جنگ‌ها مستلزم تبدیل تهدیدات ناشناخته به فرصت‌هایی آگاهانه است».

## منابع

۱. بیدگلی، محمد و نوری کور عباسلو، بهناز (۱۳۹۹). *ارتباطات سیاسی*، تهران: انتشارات کیان دانش.
۲. جوانی، محمد (۱۴۰۱). *علوم شناختی در جنگ شناختی*، تهران: نو اندیشان دنیای کتاب، چاپ ۱۴.
۳. رستمی، محسن و کیانی مقدم، امیر سام و مسجدی آرانی، عباس وجهان‌شاهی، علی و بختیاری، مریم (۱۴۰۱). بررسی تأثیر جنگ روانی بر اضطراب و ناکامی؛ *فصلنامه علمی راهبرد دفاعی*، سال بیستم، شماره ۸۰.
۴. شاه محمدی، محمد و فاطمی سید داوود (۱۴۰۳). نقش جنگ شناختی در بحرانهای اجتماعی در جمهوری اسلامی ایران؛ *فصلنامه شناخت پژوهی مطالعات سیاسی*، سال ۱، شماره ۱، تابستان ۱۴۰۳.
۵. شیرازی، محمد (۱۳۷۶). *جنگ روانی و تبلیغات؛ مفاهیم و کاربردها*، نشر نمایندگی ولی فقیه در سپاه تهران.
۶. صفری نژاد، احمد (۱۴۰۰). چگونگی تأثیر جنگ روانی حریفان بر امنیت آجا و ارائه راهکارهای مقابله ای با آن، *فصلنامه مطالعات جنگ*، سال سوم، شماره ۱۰.
۶. عراقی، عبدالله، بیدگلی، محمد و رجبی ده برزویی (۱۴۰۱). واکاوی اهداف جنگ شناختی دشمن و راهکارهای تاب آوری مقابله با آن با تأکید بر آموزه های قرآن؛ *فصلنامه علمی مطالعات دفاع مقدس*، دوره ۸، شماره ۴- شماره پیاپی ۳۲، صفحه ۱۴۳-۱۶۲.
۷. عیوضی، محمد رحیم (۱۳۸۸). مدیریت رسانه ای و مهندسی افکار عمومی؛ *فصلنامه مطالعات تربیتی و روانشناسی دانشگاه فردوسی مشهد*، دوره دهم، شماره ۲.
۸. کلمنس، بیارد. فرمانده نیروی دریایی آمریکا در سال ۱۹۹۹، جنگ سایبری: روش ها، نیروها و سلاح های کشتار جمعی، *میلیتاری ریویو*، سپتامبر ۱۹۹۹، شماره ۷۹، صفحه ۳۵ به آدرس اینترنتی <http://www-cgsc.army.military/milrev/English/sep09/clemen.htm>, 2002.



## Exploring unknown threats in cognitive warfare

Ebrahim soltani nasab<sup>1</sup>

### Abstract

Today, cognitive warfare has become a powerful tool in the hands of various governments and groups. However, the main challenge is that many of the threats in this field cannot be clearly identified. Therefore, identifying unknown threats in cognitive warfare is essential not only for protecting national security, but also for countering soft threats. The main purpose of this article is to examine unknown threats in cognitive warfare and analyze how they affect national security. Since threats in this field are often unpredictable and complex, another goal of this research is to identify the characteristics and characteristics of these threats, especially in the technical, cyber, psychological and social fields. In addition, the article, with a descriptive and analytical approach, examines strategies for dealing with these threats and predicts advanced methods for identifying them. The results of this study show that cognitive warfare has increasingly emerged as a new and complex threat to national security. These threats, due to their characteristics such as the speed of evolution, technical complexity, and profound psychological and social effects, require new methods and specific strategies to identify and counter. Unknown threats emerge in the form of advanced and new technologies such as artificial intelligence, the Internet of Things, cyberspace, psychological threats, cyber attacks and information manipulation, and cultural and social threats, all of which affect national identity and security. Identifying and countering unknown threats in cognitive warfare requires a comprehensive and interdisciplinary approach that includes cross-sectoral collaboration, the use of new technologies, and strengthening human and national organizational capacities.

**Keywords:** Security, Threat, Unknown Threats, Cognitive Warfare

**Citation:** soltani nasab, Ebrahim (2026). Exploring unknown threats in cognitive warfare. *Quarterly Journal of Army Strategic Research* 5 (16) 1-25.

---

1. PhD Graduate, Futures Studies and Private Law; PhD Candidate in Philosophy of Religion, Supreme National Defense University, Tehran, Iran. Email: saeedsoltaninasab@gmail.com