Quarterly Journal Defensive Future Studies
IRI Military Command and Staff University
www.dfsr.ir
Online ISSN: 2645-7172
Print ISSN: 2588-428x

Cognitive warfare and hybrid threats in the future outlook: Concepts, tools, and preventive strategies

Saleh Rahimi[1]✉

1. Associate Professor of Knowledge and Information Science, Razi University, Kermanshah, Iran. E-mail: s.rahimi@razi.ac.ir

Article Info

Article type:
Research Article

Article history:
Received:
2024- 9- 21
Received in revised form:
2024- 12- 5
Accepted:
2024- 12- 10
Published online:
2025- 2- 19

Keywords:
Cognitive warfare, Modern warfare, New generation warfare, Contemporary wars, Hybrid warfare.

ABSTRACT

Objective: This research aims to examine the concept of cognitive warfare and hybrid threats in order to propose a set of measures to mitigate their impacts. This study defines cognitive warfare, discusses related concepts and actors, provides examples of cognitive warfare, and highlights the enabling technologies, aiming to clarify the meaning and characteristics of cognitive warfare.

Method: The research method used is documentary-based.

Findings: Cognitive warfare has gained significant importance as a modern tool for influencing public opinion and altering perceptions. In the information age, increasing media literacy and strengthening critical thinking can serve as effective strategies for countering cognitive warfare. Additionally, proper education and accurate information dissemination also play crucial roles in reducing the negative effects of this type of warfare.

Conclusion: Characteristics of various types of warfare are also present in cognitive warfare, and it can be said that this type of warfare encompasses all previous forms because it involves elements such as dealing with big data, human thoughts and behaviors, and attention to the flow of information. Therefore, neutralizing its visible impacts requires innovative strategies.

Cite this article: Rahimi, S. (2025). Cognitive warfare and hybrid threats in the future outlook: Concepts, tools, and preventive strategies. Defensive Future Studies, 9(35), 61- 91.
DOI: 10.22034/dfsr.2024.2041829.1830

Publisher: IRI Military Command and Staff University

Extended Abstract

Objective:
Cyber warfare, hybrid warfare, soft warfare, cognitive warfare, epistemic warfare, and others related to new types of warfare can be termed informational warfare, as the core concept behind these terms is information. In these types of wars, the enemy's focus is more on the minds and thoughts of a country's citizens. To achieve this goal, the use of modern information and communication technologies and the hiring of individuals with soft skills and capabilities in internet content production, such as professional journalists and reporters from target countries, are prioritized by hostile countries. Given the rapid technological advancements and the expanding influence of digital tools, cognitive warfare impacts not only current developments but also future security and social equations. This type of warfare can play a significant role in politics, society, and the economy and become one of the most complex and critical security and social challenges of the future. This research, with a forward-looking perspective, analyzes the concept of cognitive warfare, its background, and its connection with other related fields and attempts to provide strategies to familiarize citizens with the tactics of modern warfare, especially cognitive warfare. This study aims to examine the various dimensions of cognitive warfare and the tools and strategies to counter it.

Methodology:
The research approach is qualitative and descriptive-analytical. A comparative approach was used to compare the strategies and actions of various countries in countering cognitive warfare. This method was chosen due to the multidimensional nature of cognitive warfare and other related types of warfare. Data collection was conducted through documentary-library methods, with a focus primarily on direct analysis of related texts. The statistical population of this research includes scientific articles, research reports, and specialized documents in the fields of unconventional warfare, cognitive warfare, and modern technologies. New sources were selected using reputable scientific databases. Criteria for source selection included scientific credibility, currency, and emphasis on analyses and findings related to cognitive warfare. These sources predominantly consist of studies published in the past decade that have examined the impact of modern tools such as social networks and artificial intelligence in cognitive warfare. During the data collection process, keywords such as cognitive warfare, misinformation, targeted advertising, artificial intelligence, warfare, cyber warfare, and others were initially chosen, and sources were searched and selected based on these keywords. To increase the validity and reliability of

the research data, sources with scientific backing and credible citations were used. Additionally, analyses were conducted using comparisons of multiple research findings and comparative interpretations to enhance the depth and accuracy of the results.

Findings:

Cognitive warfare involves subtle yet widespread changes in beliefs, attitudes, and behaviors of the audience, and can be carried out through approaches such as perception and cognition, psychological and cultural influence, and stimulating emotions and social reactions. The tools and technologies of cognitive warfare are used to manipulate information and shape public opinion. These tools include social networks and cyberspace, artificial intelligence and big data analysis, media, and targeted advertising. The impact of these tools on public perception involves distorting realities, creating anxieties and doubts, and strengthening divides and conflicts within society. Due to weakening the social and cultural security of society, cognitive warfare can pose serious threats to national security. These threats include disrupting social cohesion, damaging trust and social capital, and weakening international relations. Countering cognitive warfare can include identifying and analyzing threats, designing counter-strategies, empowering individuals and promoting awareness, creating secure platforms to confront cognitive warfare, inter-agency cooperation in society, and continuous monitoring and evaluation.

Conclusion:

Due to the widespread use of misinformation and propaganda in cognitive warfare, developing educational programs and resilient structures to counter cognitive threats is essential. Utilizing artificial intelligence and data analysis techniques to identify and combat misinformation and targeted advertisements is crucial. Establishing advanced systems for simulating threats and predicting enemy cognitive behaviors in the future can be an effective strategy. International cooperation, especially with neighboring countries with a shared cultural background, is essential in combating cognitive warfare. Creating international frameworks and strengthening cooperation between governments to prevent and counter this type of warfare is also important. Developing new and forward-looking strategies to combat cognitive warfare, including leveraging modern technologies and strengthening defensive capacities in the informational and psychological domains, is necessary.

فصلنامه علمی آینده‌پژوهی دفاعی
شاپای چاپی: ۲۵۸۸-۲۲۸X شاپای الکترونیکی: ۲۶۴۵-۷۱۷۲ http://www.dfsr.ir/
دانشگاه فرماندهی و ستاد آجا

جنگ شناختی و تهدیدهای ترکیبی در چشم‌انداز آینده: مفاهیم، ابزارها و راهکارهای پیشگیرانه

صالح رحیمی[۱] ✉

۱. دانشیار علم اطلاعات و دانش‌شناسی، دانشگاه رازی، کرمانشاه، ایران، رایانامه: s.rahimi@razi.ac.ir

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخ دریافت:
۱۴۰۳/۰۷/۰۲

تاریخ بازنگری:
۱۴۰۳/۰۹/۱۵

تاریخ پذیرش:
۱۴۰۳/۰۹/۲۰

تاریخ انتشار:
۱۴۰۳/۱۲/۰۱

کلیدواژه‌ها:
جنگ شناختی، جنگ مدرن، جنگ نوین، جنگ‌های معاصر، جنگ ترکیبی.

چکیده

هدف: هدف این تحقیق بررسی مفهوم جنگ شناختی و تهدیدهای ترکیبی است تا مجموعه‌ای از تدابیر را به‌منظور کاهش تأثیرات آن‌ها ارائه دهد. در این بررسی، ضمن تعریف جنگ شناختی، مفاهیم نزدیک و بازیگران آن، به نمونه‌هایی از جنگ شناختی اشاره می‌کند و فناوری‌های زمینه‌ساز آن را موردتوجه قرار می‌دهد. هدف اصلی، روشن‌سازی معنای جنگ شناختی و ویژگی‌های آن است.

روش: روش پژوهش مورداستفاده، اسنادی- کتابخانه‌ای است.

یافته‌ها: جنگ شناختی به‌عنوان یکی از ابزارهای نوین در تأثیرگذاری بر افکار عمومی و تغییر نگرش، اهمیت زیادی یافته است. در عصر اطلاعات، افزایش سواد رسانه‌ای و تقویت تفکر انتقادی می‌تواند به‌عنوان راهکارهایی مؤثر در مقابله با جنگ شناختی عمل کند. همچنین، آموزش و اطلاع‌رسانی صحیح نیز نقش مهمی در کاهش تأثیرات منفی این نوع جنگ دارد.

نتیجه‌گیری: ویژگی‌هایی از انواع جنگ‌ها در جنگ شناختی نیز وجود دارد و می‌توان گفت این نوع جنگ جامع جنگ‌های پیش از خود است زیرا از ویژگی‌هایی مانند سر و کار داشتن با داده‌های انبوه، افکار و رفتار انسان‌ها، توجه به گردش اطلاعات و غیره برخوردار است؛ بنابراین، برای خنثی‌سازی تأثیرات مرئی آن نیازمند راهکارهای نوین است.

استناد: رحیمی، صالح. (۱۴۰۳). جنگ شناختی و تهدیدهای ترکیبی در چشم‌انداز آینده: مفاهیم، ابزارها و راهکارهای پیشگیرانه. آینده‌پژوهی دفاعی، ۹(۳۵)، ۶۱- ۹۱.

DOI: 10.22034/dfsr.2024.2041829.1830

ناشر: دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

مقدمه

جنگ سایبری، جنگ ترکیبی، جنگ نرم، جنگ شناختی، جنگ معرفتی و غیره را که با موضوع جنگ‌های جدید مطرح می‌شوند، می‌توان جنگ اطلاعاتی نامید؛ چراکه خمیرمایهٔ طرح و ایجاد این مفاهیم، مفهومی به نام اطلاعات است. در این نوع از جنگ‌ها، تمرکز دشمن بیش از هر چیزی بر ذهن و فکر شهروندان یک کشور است و برای تحقق این خواسته، استفاده از فناوری‌های نوین اطلاعاتی و ارتباطی و نیز استخدام افرادی با مهارت‌های نرم و توانمند در تولید محتوای اینترنتی مانند روزنامه‌نگاران و خبرنگاران حرفه‌ای کشورهای هدف، به‌منظور تحقق اهداف در جنگ‌های نوین در اولویت کشورهای متخاصم قرار دارد.

جنگ شناختی راهبردی است که تمرکز خود را بر تغییر نحوهٔ فکر کردن جمعیت هدف و از طریق آن، نحوهٔ عمل کردن آن می‌گذارد (بکس و ساب، ۲۰۱۹؛ نقل از میلر، ۲۰۲۳)، استفادهٔ جنگ‌افزاری از رأی و نظر عمومی توسط نهادی خارجی، به‌منظور تأثیرگذاری بر سیاست عمومی و دولتی و بی‌ثبات کردن نهادهای عمومی نیز تعبیر دیگری است که توسط برنال و دیگران مطرح شده است (میلر، ۲۰۲۳). این نوع جنگ چنان تحت تأثیر انقلاب ارتباطات و اطلاعات و به شکل خاص انقلاب سایبری قرارگرفته که از سطح عملیاتی و تاکتیکی فراتر رفته و جنبهٔ راهبردی آن برجسته و وارد عرصه‌های جدیدی شده است (ترابی و طاهری‌زاده، ۱۴۰۰). جنگ شناختی به‌عنوان یک حوزهٔ جدید جنگ، همراه با جنگ‌های زمینی، دریایی، هوایی، فضایی و سایبری (تکنیکی) در نظر گرفته می‌شود (Fenstermacher, Uzcha, Larson, Vitiello, & Shellman, 2023).

رسانه‌های امروزی دسترسی آسان با حداقل موانع را فراهم می‌کنند، اما استفاده از آن‌ها نیازمند مهارت‌های فنی و شناختی جدید است. به‌عنوان‌مثال، افزایش تنوع محتوا و تولیدکنندگان، چالشی برای توانایی ارزیابی اطلاعات کاربران ایجاد می‌کند و روش‌های جدیدی برای ایجاد و مشارکت در محتوای دیجیتال ظاهر شده‌اند (تاندوک و کیم، ۲۰۲۳). این رسانه‌ها، محیط‌های اطلاعاتی جدیدی ایجاد کرده‌اند که به کاربران طیف بی‌سابقه‌ای از منابع و محتواهایی متناسب با اولویت‌های آن‌ها، ارائه می‌دهند (کومپل، ۲۰۲۲). درحالی‌که رسانه‌های اجتماعی شامل طیف وسیعی از اطلاعات باکیفیت هستند و راه‌هایی برای انتشار اطلاعات نادرست و تئوری‌های توطئه‌آمیز نیز فراهم می‌کنند. در این محیط، کاربران اغلب با محتواهای بدون نظارت مواجه می‌شوند که نیازمند

مجموعه‌ای جدید از مهارت‌ها در زمینهٔ هوش رسانه‌ای است و فراتر از مهارت‌هایی است که به‌طور سنّتی در تلویزیون یا روزنامه‌ها استفاده می‌شود (چو و همکاران، ۲۰۲۲). هرچند برخی از جنبه‌ها مرتبط با محیط‌های رسانه‌ای سنّتی هستند، برخی دیگر بیشتر به چالش‌های جدید محیط‌های رسانه‌های اجتماعی اختصاص دارند. برخلاف رسانه‌های سنّتی، رسانه‌های اجتماعی نیازمند مهارت‌های جدید در مدیریت اطلاعات‌اند که شامل راهنمایی و یافتن اطلاعات مرتبط و تدوین محتوای خبری شبکه‌های اجتماعی شخصی‌سازی‌شده می‌شوند (نانز و همکاران، ۲۰۲۲). همچنین، چالش‌های جدیدی در پردازش اطلاعات ظاهر شده است. شهروندان نیاز دارند به‌سرعت اطلاعات را ارزیابی کنند (تاندوک و کیم، ۲۰۲۳). علاوه بر این، آن‌ها باید محتوای جدید را با دانش خود ارتباط دهند (ون اورشلده و هیلی، ۲۰۰۱).

این مطالعه قصد دارد، به بررسی مفهوم و پیشینهٔ جنگ شناختی بپردازد و رابطهٔ این مفهوم را با مفاهیم مرتبط در این حوزه بررسی کند و راهکارهایی را جهت آشنایی شهروندان با ترفندهای جنگ‌های عصر مدرن به‌ویژه جنگ شناختی ارائه دهد. نتایج حاصل از این پژوهش راهکارهایی را برای مقابله با جنگ شناختی و صیانت از کاربران در فضای مجازی، افزایش حوزهٔ نفوذ و تهاجم فرهنگی به صحنه‌های نبرد جنگ شناختی، مقابله، تضعیف و نابودی بسترهای جنگ شناختی، ایمن‌سازی جامعه و حفظ سرمایه‌های اجتماعی ارائه می‌دهد به این امید که در جهت تعمیق، تکمیل و ترمیم دکترین امنیت ملی مؤثر واقع شود. نتایج این پژوهش می‌تواند به توسعه برنامه‌های آموزشی و مداخلاتی در بین شهروندان و به‌تبع آن آشنایی و مقابله آنان با جنگ شناختی مفید باشد.

پیشینه پژوهش

ابراهیم، روده و داسکینگ (۲۰۲۳)، در پژوهشی بیان کردند که جمهوری خلق چین و روسیه جنگ شناختی و راهبردهای مرتبط را در عملیات خود گنجانده‌اند. بااین‌حال، هنوز در مورد مفهوم و کاربرد جنگ شناختی در گفتمان علمی و دکترین‌های نظامی غرب ابهام وجود دارد. نتایج پژوهش رچکوفسکی، لیس (۲۰۲۲)، نشان داد، مشاهدات مشارکتی نویسندگان و درس‌هایی از پروژه‌های پژوهشی نظامی ملی و بین‌المللی به درک و بحث در مورد جوهر جنگ شناختی کمک می‌کند. میلر (۲۰۲۳)، در پژوهشی سنجه‌های دفاعی و حمله‌ای و اقداماتی که با اصول اخلاقی مربوطه برای مقابله با جنگ

شناختی مطابقت دارند را مورد بحث قرار دادند. دانت (۲۰۲۳)، در رویکرد بین کشورهایی مانند ایالات‌متحده یا فرانسه و کشورهایی مانند روسیه، ایران یا چین در مواجه با جنگ شناختی تفاوت‌های بسیاری قائل می‌شود. یو و هو (۲۰۲۳) در پژوهشی به بررسی جنگ شناختی چین پرداختند که با عملیات هوایی نظامی در طول همه‌گیری کووید علیه تایوان به راه افتاد. به باور آن‌ها چین در نظر داشت اعتبار دولت حزب پیشرو دموکراتیک را زیر سؤال ببرد. دانیک و بریگز (۲۰۲۳)، به بررسی چگونگی ترویج فرصت‌های نامتقارن توسط فناوری‌های سایبری برای تأثیرگذاری، کنترل و زیرساخت حریف پرداختند. فرینا و کوتج (۲۰۲۳)، در پژوهشی اظهار داشتند که تصمیم روسیه برای انجام حمله به اوکراین دنیا را برای همیشه تغییر داده. همچنین، بیان کردند که کشورهای اروپایی به‌طور فعال در حال بررسی افزایش هزینه‌های دفاعی خود هستند و سعی می‌کنند از این جنگ بیاموزند. هدف ماکسیمنکو و درکاچ از پژوهشی در سال (۲۰۲۳)، بررسی اجمالی اندیشه نظامی تاریخی غرب درباره نظریه جنگ و رابطه آن با جنگ شناختی بود. از نظر کلاوری و دو کلوزل (۲۰۲۲)، جنگ شناختی از ابزارهای سایبری برای تغییر فرایندهای شناختی دشمن، بهره‌برداری از سوگیری‌های ذهنی یا تفکر بازتابی و برانگیختن انحراف‌های فکری، تأثیرگذاری بر تصمیم‌گیری و ممانعت از اقدامات با اثرات منفی در سطح فردی و جمعی استفاده می‌کند. تاشف، پرسل و مک لافلین (۲۰۱۹)، در پژوهشی اظهار می‌کنند که نیروی نظامی ایالات‌متحده به‌طور فزاینده در حوزه‌هایی سرمایه‌گذاری می‌کند تا به چالش‌های ناشی از رشد رقابت استراتژیک در محیط اطلاعاتی پاسخ دهد و هدف آن تأثیرگذاری و مختل کردن حریفان است. در پژوهشی دانیک، مالیارچوک و بریگز (۲۰۱۷)، اجزای پیشرفته فناوری، اطلاعاتی و سایبری جنگ هیبریدی را بررسی کرده و به معرفی اقدامات پیشنهادی برای مقابله با تهدیدها و حملات اطلاعاتی و سایبری پرداختند. کشاورز، سیاهپوش، ارجینی و نائینی (۱۴۰۲)، اظهار داشتند که ایجاد سیاست‌های حاکم بر نظام مقابله‌ای و شکل‌گیری سازوکار مفهومی در عرصه جنگ شناختی سبب عمق‌بخشی، تأثیرگذاری هوشمندانه، هدفمند و متعالی در سطح جامعه و در لایه بعدی واکسینه کردن و مصون‌سازی فرهنگی بازیگران و جامعه می‌گردد. پناهی‌فر و قائدی (۱۴۰۲)، به این نتایج رسیدند که آموزش مؤلفه‌های جنگ شناختی در فضای کار برای کارکنان نظامی می‌تواند در ارتقای مؤلفه‌های شناختی در حوزهٔ کاری و ملی و همچنین افزایش آگاهی و بالا بردن تعهد سازمانی مؤثر باشد. نوریه، بهتری و صفایی

(۱۴۰۱)، اظهار داشتند که تولید و انتشار محتوای هدفمند در رسانه‌های اجتماعی علیه ملت‌ها و دولت‌ها به‌عنوان یکی از روش‌های سایبری در جنگ‌های شناختی محسوب می‌شود. سلطانی، محمدی منفرد و جاودانی مقدم (۱۴۰۱) در پژوهشی اظهار داشتند، به‌کارگیری فناوری در حوزه عملیاتی سازمان‌های نظامی از جمله ناتو سبب شده تا توجه بیشتر به جنگ‌افزارهای نوین در کشورهای مختلف ضروری تلقی گردد. حاجی‌زاده (۱۴۰۱)، نیز بیان داشت که جنگ شناختی به‌عنوان مفهومی نو محصول نگاهی جامع و گَشتالتی به جنگ‌هایی است که با عنوان جنگ روانی، جنگ اطلاعاتی، جنگ سایبری، جنگ الکترونیکی، جنگ نظارت و شناسایی بازتولید می‌شوند. ترابی و طاهری‌زاده (۱۴۰۰)، در پژوهشی بیان داشتند که جنگ اطلاعاتی از سطح عملیاتی و تاکتیکی به سطح راهبردی گسترش‌یافته و دانش سایبری کلید موفقیت در عرصه جنگ اطلاعاتی به شمار می‌آید. قیامی، سجادی اصیل و مصدق (۱۳۹۹)، در پژوهشی بیان داشتند که دشمنان فرامنطقه‌ای از سالیان قبل جنگ شناختی را در حوزه‌های مختلف علیه ایران شروع نموده‌اند. یافته‌های پژوهش راجی و افتخاری (۱۳۹۸)، بیانگر کاربست نوع خاصی از جنگ ترکیبی توسط غرب علیه جمهوری اسلامی ایران است. درنتیجه، در این نوع جنگ، مؤلفه‌های جنگ ترکیبی به‌مثابه واحدهای ابزاری و عینی و با فشار متراکم و طولانی‌مدت به همراه استفاده از شبکه‌های اجتماعی در پی تأثیر بر بسترهای ذهنی و شناختی جامعه هدف است. میراحمدی، نصرتی و امیراحمدی (۱۳۹۵) در پژوهشی بیان کردند که جنگ نرم، راهبرد کنونی آمریکا و متحدانش در مقابله با ایران است. یکی از ابزارهایی که نقش مهمی در پیشبرد پروژه جنگ نرم علیه ایران دارد، شبکه‌های اجتماعی مجازی است که می‌تواند نقش مهمی در ترویج شاخص‌های جنگ نرم داشته باشد.

بر مبنای مطالعات صورت‌گرفته می‌توان گفت، تمرکز پژوهش‌ها اغلب به تعریف مفاهیم مرتبط با جنگ شناختی بوده است و پژوهش‌های صورت گرفته در این حوزه به بررسی رابطه جنگ شناختی و سایر متغیرهایی که ممکن است رابطه مستقیم و معنی‌داری با جنگ شناختی داشته باشند، نپرداخته‌اند و این به سبب نو بودن مفهوم جنگ شناختی می‌تواند باشد. پژوهش‌های صورت گرفته در داخل کشور نیز اغلب با رویکرد توصیفی به مسئله جنگ شناختی پرداخته‌اند و بررسی‌ها اغلب به شیوه اسنادی - کتابخانه‌ای صورت گرفته است. یافته‌های این پژوهش می‌تواند جهت تصمیم‌گیری و اجرای برنامه‌های فرهنگی و نرم، علیه توطئه‌های دشمنان به مسئولین فرهنگی و امنیتی راهکار مناسب

ارائه دهد و همچنین شهروندان را از ویژگی‌های جنگ شناختی آشنا سازد که علیه کشور به کار می‌رود و تمرکز بر ذهن شهروندان دارد و تلاش می‌کنند با هزینه‌های اندک باعث تغییر رژیم سیاسی در کشورهای آزاد و اسلامی شوند.

تاریخچه جنگ شناختی

جنگ شناختی به استفاده از تکنیک‌ها و راهبردهایی برای تأثیرگذاری بر ذهن و قلب افراد می‌پردازد و از دوران باستان تا به امروز تحولات زیادی را تجربه کرده است. در تمدن‌های اولیه، از هنر و نوشته‌ها برای تقویت قدرت سیاسی و نظامی استفاده می‌شد، در دوران میانه مذهب به‌عنوان ابزاری برای تحریک و توجیه جنگ‌ها به کار گرفته می‌شد. با اختراع چاپ رسانه‌های چاپی به ابزارهای مهمی برای انتشار تبلیغات تبدیل شدند. در جنگ‌های جهانی اول و دوم، تبلیغات به‌عنوان سلاحی مؤثر در ارتقای روحیه ملی و تضعیف دشمنان استفاده شد. در دوران جنگ سرد، رقابت‌های ایدئولوژیک و رسانه‌ای به اوج خود رسید و پس‌ازآن، با ظهور اینترنت و شبکه‌های اجتماعی، جنگ شناختی به عرصهٔ پیچیده‌ای تبدیل شد که در آن اطلاعات نادرست و تبلیغات به‌سرعت منتشر شده و تأثیرات گسترده‌ای بر افکار عمومی گذاشتند.

اکنون، استفاده از هوش مصنوعی و تحلیل داده‌ها به چالش‌های جدیدی در این حوزه افزوده است. در طول زمان ماهیت جنگ بدون تغییر باقی مانده است. نقل‌قول مشهوری وجود دارد که به سون تزو نسبت داده می‌شود «طبیعت جنگ تغییر مداوم است». در اثری به نام درباره جنگ، کلوزویتس جنگ را به‌عنوان عمل زور برای مجبور کردن دشمن به انجام اراده ما تعریف می‌کند. در این اثر، استفاده از نیروی فیزیکی به‌عنوان ویژگی اساسی جنگ در نظر گرفته شده است. نشریه تفنگ‌داران نیروی دریایی ایالات‌متحده از مقوله همه جنگ‌ها بر پایهٔ فریب است از سون تزو نقل‌قول می‌کند و اهمیت فریب را به‌عنوان فعالیتی اطلاعاتی برای گمراه کردن ذهن انسان، مورد تأکید قرار می‌دهد. تعامل انسان - ماشین جزئی اساسی از جنگ شناختی است و به دلیل تأثیری که بر دیدگاه و قضاوت‌های انسان دارد نقشی مرکزی و حیاتی ایفا می‌کند و این امر چالشی بی‌سابقه را ایجاد می‌کند (مارسیلی، ۲۰۲۳).

حوزه‌های جنگ شامل حوزه فیزیکی (زمین، هوا، دریا)، حوزه اطلاعاتی (طیف الکترومغناطیس) و حوزه شناختی (ذهن انسان) است (لی شیهوا، ژانگ ژیچانگ و کائو

شینهو، ۲۰۲۱). ناتو نیز، پنج حوزه عملیاتی را مطرح می‌کند: زمین، دریا، هوا، فضا و سایبر. برای این حوزه‌ها، فرضیات استراتژیک و مفاهیم عملیاتی، همچنین مکاتب و روش‌های تاکتیکی ایجاد و توسعه یافته‌اند. بااین‌حال هیچ‌یک از این حوزه‌ها به فضای جنگی نپرداخته است که مسئول پیروزی از طریق قلب و ذهن است. همان‌طور که تود شمیت بیان کرده است، استراتژیست و فیلسوف چینی سان تزو باور داشت که جنگ‌ها از طریق سازمان جاسوسی، اطلاعات و فریب پیروز می‌شوند با حمله به دشمنان در جایی که کمترین آمادگی را دارند. در نتیجه، مطالعات شناختی و حوزه شناختی محیط عملیاتی به کانون محوری جنگ‌های معاصر تبدیل می‌شوند (رچکوفسکی و لیس، ۲۰۲۲).

درحالی‌که در حوزه نظامی، فضای سایبر به‌عنوان پنجمین حوزه جنگی تعیین شده است و به‌عنوان یکی از حوزه‌های سنتی همچون هوا، زمین، دریا و فضا شناخته می‌شود، توسعهٔ حوزه‌های عملیاتی جدید برای توسعهٔ حکومت‌ها، مناطق جدیدی را موردتوجه قرار داده است. در این راستا، دستورالعمل‌های برنامه ملی دفاع ژاپن در سال ۲۰۱۸ فضای الکترومغناطیسی را به‌عنوان ششمین دامنه عملیاتی تعیین کرد و تغییرات مورد انتظار در دستورالعمل‌ها در سال ۲۰۲۲ ممکن است فضای شناختی را به‌عنوان هفتمین حوزه اضافه کند (تسوچیا، ۲۰۲۲).

در ۲۰۰۳، چین، با توجه به درس‌هایی که از جنگ عراق در اواخر همان سال گرفته بود، به‌طور رسمی مفهوم جنگ افکار عمومی، جنگ روانی و جنگ حقوقی را مطرح کرد. در سال ۲۰۱۴، ارتش آزادی‌بخش خلق چین یک قدم پیش‌تر نهاد و مفهوم برتری ذهنی را مطرح کرد که به معنای قدرت کنترل مغز است (لین، ۲۰۲۳).

جنگ روانی و تهدیدهای ترکیبی از بزرگ‌ترین خطرات برای پایداری نظام‌های سیاسی و نیز آسیب‌پذیری‌های روانی برای افراد محسوب می‌شوند. این نوع جنگ از زمان‌های اولیه توسط مکاتب نظامی مختلف به‌طور گسترده موردتوجه بوده و پیامدهای آن در وضعیت‌های جنگ مدرن پیوسته در حال تکامل است (مونوز پلازا، سوتلو مونگ و گونزالس اوردی، ۲۰۲۳). اصطلاح عملیات روانی ابداع آمریکایی‌ها است که از آن برای تسریع در تسلیم ژاپن استفاده کردند. در سال ۲۰۱۰، به دلیل بار منفی عبارت «عملیات روانی» وزیر وقت دفاع ایالات‌متحده آن را با عبارت عملیات پشتیبانی اطلاعات نظامی جایگزین کرد (ابراهیم، رودی و داسکینگ،۲۰۲۳).

در تاریخ نظامی، برد بدون جنگ توسط راهبران نظامی همیشه موردتوجه بوده است. میدان‌های نبرد سنتی عمدتاً در فضای فیزیکی رخ می‌دهد. با درک عمیق و مداوم انسان از جنگ و تکامل فناوری، نوع جدید جنگ به‌تدریج از جنگ مستقیم به جنگ غیرمستقیم در فضای سایبر و مغز انسان تبدیل شده است (یو و هو، ۲۰۲۳).

جنگ شناختی از دوران باستان تا به امروز تحولاتی گسترده را تجربه کرده و از هنر و مذهب گرفته تا رسانه‌های چاپی و دیجیتال، هرکدام نقشی در شکل‌گیری و گسترش آن داشته‌اند. با ظهور فناوری‌های نوین و رسانه‌های اجتماعی، جنگ شناختی به عرصه‌ای پیچیده‌تر تبدیل شده است که در آن اطلاعات و تبلیغات به‌سرعت منتشر و تأثیرات گسترده‌ای بر افکار عمومی می‌گذارند. این تحولات، ضرورت درک و مدیریت مؤثر این نوع جنگ را در دنیای معاصر بیشتر کرده است.

تحول جنگ‌ها

کسب اطلاعات و شکل‌دهی به فضای تصمیم‌گیری قبل و طی نبرد، عامل کلیدی موفقیت در جنگ‌های معاصر است (رچکوفسکی و لیس، ۲۰۲۲). شیوه‌های نوظهور جنگ کمتر بر استفاده ابزاری از زور برای دستیابی به اهداف سیاسی متمرکز هستند و بیشتر بر مفاهیم مدیریت ادراک، روایت‌ها، عدم تقارن یا درگیری نامنظم، استفاده‌های متخاصم از هنجارها و استفاده پنهان و مبهم از زور متمرکز هستند (کریشنان، ۲۰۲۲)؛ بنابراین می‌توان به شیوهای نوین جنگ از قبیل جنگ هیبریدی، اطلاعاتی، جنگ منطقه خاکستری و جنگ نسل پنجم اشاره کرد.

جنگ هیبریدی: با توجه به عدم وجود تعریف واحدی از این نوع جنگ، جنگ هیبریدی شامل تبلیغات، اطلاعات و عملیات تأثیرگذاری، فریب و عملیات روان‌شناختی می‌شود (مارسیلی، ۲۰۲۳).

در این جنگ به‌منظور ایجاد سردرگمی و تضعیف دشمن از ابزارهای غیرمتعارف استفاده می‌شود و به‌طور همزمان از تاکتیک‌های نظامی و غیرنظامی برای به حداکثر رساندن اثربخشی نیروها استفاده می‌گردد و از ترکیب روش‌های معمول و نامعمول برای مقابله با تهدیدات بهره می‌برند.

تهدیدات هیبریدی در محیط‌های دیجیتال، سایبری و مجازی بروز می‌کنند و در دنیای واقعی مشهود است. باوجود مبهم بودن این مفهوم، فعالیت‌های هیبریدی شامل جنگ

سایبری، جنگ اطلاعاتی و مفهوم نوظهور و تکامل‌یافته جنگ شناختی است که از تلاقی آن‌ها به وجود می‌آید. این کلمات کلیدی در زمینه جنگ روسیه و اوکراین موردتوجه قرار گرفته‌اند و اکنون مطرح هستند (مارسیلی، ۲۰۲۳). به عبارتی، جنگ ترکیبی یک استراتژی است که توسط دولت‌ها و بازیگران غیردولتی استفاده می‌شود و هدف آن به حداکثر رساندن اثربخشی نیرو با ترکیب تاکتیک‌های منظم و نامنظم و همچنین ابزارهای نظامی و غیرنظامی مختلف است. دشمنان می‌توانند با تطبیق سازمانی و رویکرد کل دولت به تهدیدات ترکیبی، با جنگ ترکیبی مقابله کنند (کریشنان، ۲۰۲۲).

جنگ اطلاعاتی: شامل استفاده از فناوری‌ها و تکنیک‌هایی است که به تحلیل، انتشار و دستکاری اطلاعات می‌پردازد. این جنگ در فضای مجازی و واقعی انجام می‌شود و شامل عملیات سایبری، روان‌شناختی و مدیریت ادراک است. لیبیکی، جنگ اطلاعاتی را شامل هفت مؤلفه (جنگ فرماندهی و نظارت، جنگ اطلاعات‌پایه، جنگ الکترونیکی، جنگ روانی، جنگ هکری، جنگ اطلاعات اقتصادی و جنگ سایبری)، می‌داند که در آن دستکاری شناختی در زیر مقوله جنگ روانی قرار می‌گیرد (لیبیکی، ۱۹۹۵). همانند جنگ هیبریدی، جنگ اطلاعاتی نیز تعریف رهنامه‌ای ندارد و به‌این‌ترتیب مبهم است (تاشف، پرسل و مک لافلین، ۲۰۱۹).

جنگ اطلاعاتی مجموعه‌ای از تکنیک‌ها و فناوری‌ها را شامل می‌شود که از جنگ الکترونیکی تا تبلیغات را شامل می‌شود و با دامنه‌های عملیاتی واقعی و مجازی ترکیب می‌شود. دنیای مجازی جنگ شامل الکترونیکی، عملیات طیف الکترومغناطیس، عملیات فضای سایبری، جنگ اطلاعاتی و عملیات روان‌شناختی است. عملیات اطلاعاتی همچنین به‌عنوان عملیات نفوذ شناخته می‌شود و شامل ارتباطات استراتژیک، فریب نظامی، عملیات شبکه کامپیوتری، امنیت عملیاتی، مدیریت ادراک، اطلاعات عمومی و دیپلماسی عمومی می‌شود (مارسیلی، ۲۰۲۳).

جنگ منطقه خاکستری: اصطلاح جنگ منطقه خاکستری به نظر می‌رسد در سال ۲۰۱۵ برای جایگزینی یا تکمیل اصطلاح قبلی جنگ ترکیبی استفاده شده است. پارادایم تاریخی که جنگ منطقه خاکستری بر اساس آن شکل گرفت، جنگ سرد بود که دوره طولانی‌مدت رقابت ژئواستراتژیک بین دو قدرت برتر بود. قدرت‌های سازشگر به‌طور عمدی تاکتیک‌هایی را در زیر سطح جنگ دنبال می‌کنند که به دنبال جلوگیری از جنگ تمام‌عیار هستند و می‌توانند جایگزین حمله نظامی سنتی شوند. آن‌ها در منطقه

خاکستری مبهم بین صلح و جنگ در رزمایش هستند، بازتابی از نوع کمپین‌های تهاجمی، پیوسته و مصمم که مخصوص جنگ است؛ اما بدون استفاده آشکار از نیروی نظامی. جنگ منطقه خاکستری استراتژی قدرت‌های بزرگ برای درگیرشدن در کمپین‌های بلندمدت است و هدف آن تضعیف دشمن قوی‌تر است و عمداً از پاسخ نظامی اجتناب می‌کنند. راه‌حل در اینجا تعیین خطوط قرمز، تقویت بازدارندگی و توسعه گزینه‌های پاسخ مؤثر زیر آستانه جنگ است. جنگ ترکیبی و جنگ منطقه خاکستری بسیار بیشتر از جنگ نسل پنجم بر محور دولت‌ها متمرکز هستند (کریشنان، ۲۰۲۲).

جنگ نسل پنجم: در این نوع جنگ ادراکات و هویت قربانی را به‌گونه‌ای دستکاری می‌کنند که قربانی حتی ممکن است متوجه نشود که یک متخاصم او را تسخیر کرده است. دشمنان می‌توانند کمپین‌های جنگ نسل پنجم را با تلاش برای کنترل عرصه انسانی، از جمله ادراکات عمومی، ایدئولوژی‌ها و روایت‌ها شکست دهند (کریشنان، ۲۰۲۲). رید (۲۰۰۸) چارچوبی منظم برای درک ویژگی‌های جدید جنگ نسل پنجم بر اساس چهار محور که نسل‌های جنگ را تعریف می‌کنند، ارائه داده است. هر محور به یک بُعد متفاوت از یک نوع جنگ می‌پردازد:

- جغرافیای جنگ: دامنه‌های جدید درگیری چیست؟
- متخاصمان و مبارزان: ماهیت در حال تغییر دشمنان چیست؟
- اهدافی که متخاصمان در یک درگیری دنبال می‌کنند: ماهیت در حال تغییر اهداف چیست؟
- نقش نیرو ماهیت در حال تغییر نیرو چیست؟

جنگ از تمرکز بر نیروی انسانی فراوان (جنگ نسل اول)، به تمرکز بر قدرت آتش یا فرسایش (جنگ نسل دوم) و در نهایت به تمرکز بر رزمایش (جنگ نسل سوم) تکامل یافت. جنگ نسل چهارم قرار بود جنگ نسل جدید باشد که بر قیام تمرکز دارد درحالی‌که در جنگ ترکیبی معمولاً درگیری نظامی قابل‌مشاهده (نامنظم) وجود دارد، در جنگ نسل پنجم یا جنگ منطقه خاکستری هیچ درگیری آشکاری وجود نخواهد داشت. برخلاف جنگ منطقه خاکستری که در آن دامنه متخاصمان بالقوه کوچک و رقابت‌ها نسبتاً واضح است، جنگ نسل پنجم از نظر تجربی به دلیل تأکید زیاد بر فریب و پنهان‌کاری و همچنین این واقعیت که شبکه‌های ناشناخته‌ای از افراد و گروه‌های کوچک ممکن است به دولت‌ها و جوامع قدرتمند حمله کنند به‌گونه‌ای که ممکن است به‌عنوان

تهدید قابل‌تشخیص نباشند، شناسایی و مطالعه آن بسیار دشوار است (کریشنان، ۲۰۲۲). تحول جنگ‌های مدرن از جنگ هیبریدی تا جنگ نسل پنجم نشان‌دهنده تغییرات عمیق در شیوه‌های درگیری است. نسل جدید جنگ‌ها بر فریب و نفوذ روانی تأکید دارد، به‌طوری‌که حتی ممکن است قربانی متوجه حضور درگیری نشود. این تغییرات نشان‌دهندهٔ گذار از درگیری‌های نظامی سنتی به جنگ‌های پیچیده و نامشهود است که در آن تسخیر ذهن و قلب به هدف اصلی تبدیل شده است.

مفهوم جنگ شناختی

حوزهٔ شناختی شامل درک و استدلال است و با بهره‌برداری از اطلاعات به‌منظور تأثیر بر باورهای افراد باعث ایجاد مخاطره می‌شود (تسوچیا، ۲۰۲۲).

علم شناختی به تحقیق در مورد ذهن و مغز انسان می‌پردازد و تمرکز خود را روی بازنمایی و تغییر دانش در ذهن و شیوه عملی‌سازی بازنمایی‌ها و فرایندهای ذهنی در مغز دارد. ویژگی‌های بین‌رشته‌ای آن از جمله زبان‌شناسی، روان‌شناسی، علوم اعصاب، فلسفه، علوم کامپیوتر/هوش مصنوعی، انسان‌شناسی و زیست‌شناسی؛ علم شناختی را به‌عنوان یک رشته تحصیلی مستقل تشکیل می‌دهند که دیدگاه‌ها و رویکردهای مختلف مغز و فرایندهای ذهنی را موردمطالعه قرار می‌دهد. این علم به تفاوت‌های رفتاری انسان با تمرکز بر ذهن و تعامل‌های آن با دنیای اطراف و نحوهٔ نمایش، پردازش و تبدیل اطلاعات توسط سیستم‌های عصبی می‌پردازد و به همین دلیل برای درک اهمیت و تأثیر جنگ شناختی بر مغز، ذهن و رفتار بسیار حیاتی است (مارسیلی، ۲۰۲۳).

تاشف، پرسل و مک لافلین (۲۰۱۹)، اظهار کردند که بعد شناختی بالاترین جنبه فضای اطلاعاتی است. (لویس، ۲۰۲۲) بر اثر شناختی در حملات سایبری تأکید می‌کند. بااین‌حال، دیگران معتقدند که کنترل شناختی محدود به جنگ اطلاعات یا جنگ سایبری نمی‌شود. (راجرز، ۲۰۲۱)، ادعا می‌کند که تلفیق جنگ اطلاعاتی عملیاتی با جنگ شناختی یک خطای مقوله‌ای است که باید ابتدا موردبررسی قرار گیرد. (برنال و دیگران، ۲۰۲۰)، جنگ شناختی را از جنگ اطلاعاتی تفکیک می‌کنند؛ درحالی‌که جنگ اطلاعاتی بر کنترل جریان اطلاعات تمرکز دارد و جنگ شناختی قصد دارد واکنش افراد و گروه‌ها به اطلاعات ارائه شده را کنترل کند. جنگ شناختی مفهومی در حال شکل‌گیری در اسناد نظامی کشورهای غربی و رقبای آن‌ها است. در میان تنوع تفسیرها، تفاوت بین

رویکردها قابل‌توجه است. کشورهای غربی بر ابعاد علمی - فناوری تأکید دارند و مفهوم جنگ شناختی را با پیشرفت در زمینه‌های زیست‌فناوری و علوم اعصاب مرتبط می‌کنند، اما کشورهایی مانند روسیه دارای رویکرد سنتی‌تر هستند (دانت، ۲۰۲۳). جنگ شناختی اصطلاحی است که از دهه ۱۹۹۰ به بعد برای اطلاق به موارد مختلفی استفاده می‌شود. دال جنگ شناختی را به‌عنوان راهبردی توصیف کرده است که بر حلقه مشاهده، تطبیق، تصمیم، عمل تأثیر دارد، به‌طوری‌که سرعت، دقت یا هر دوی آن‌ها را کاهش دهد (دال، ۱۹۹۸). بااین‌حال، درک امروزه از این مفهوم بیشتر بر این تمرکز دارد که دشمن را، با تأثیر بر شهروندانش و حمله به مغز آن‌ها از درون نابود کند. بکس و همکاران جنگ شناختی را راهبردی می‌دانند که بر تغییر نحوه فکر کردن افراد جامعه هدف، تمرکز دارد و از آن طریق نحوه عمل آن‌ها را تغییر می‌دهد. برنال جنگ شناختی را استفاده جنگ‌افزاری از افکار عمومی توسط موجودیتی خارجی به‌منظور تأثیر بر سیاست عمومی یا دولتی و یا بی‌ثبات کردن اقدامات یا نهادهای دولتی می‌دانند (برنال و همکاران، ۲۰۲۰). جنگ شناختی از نظر هانگ و هانگ به فعالیت‌هایی اشاره دارد که طراحی شده‌اند تا حالات ذهنی دیگران و رفتارهای آن‌ها را کنترل کنند (هانگ و هانگ، ۲۰۲۰).

می‌توانیم بین دو نوع اختلال اطلاعاتی تمایز قائل شویم. نخست، اختلال شناختی است که هرگونه عملیاتی (مانند دُژاطلاعات و تبلیغات) را شامل می‌شود که به‌طور مستقیم افراد را هدف قرار می‌دهد. دومی اختلال عملکردی است (مانند فضای سایبری و حمله الکترومغناطیسی) که به‌طور مستقیم سیستم‌ها و تأسیسات (مانند کامپیوترها، سلاح‌ها، وسایل نقلیه) را هدف می‌گیرد (مارسیلی، ۲۰۲۳). حملات سایبری، کمپین‌های دژّ اطلاعات، جاسوسی و غیره در دنیای دیجیتال کنونی، تمایز بین ابعاد مستقیم و غیرمستقیم تضادها را به‌مرور زمان دشوارتر می‌کند و باعث ابهام در مفاهیم و دسته‌بندی‌ها می‌شود. (دانت، ۲۰۲۳). جنگ شناختی، همراه با جنگ اطلاعاتی، راهبرد طراحی شده است تا بر افراد یا عموم مردم در ارزیابی یک مسئله، رویداد یا وضعیت تأثیر داشته باشد (ردینگ و ولز، ۲۰۲۲).

تفاوت جنگ اطلاعاتی و شناختی در استفاده اصلی از اطلاعات، کژاطلاعات و دُژاطلاعات برای جنگ اطلاعاتی و استفاده از یکی یا ترکیبی از آن‌ها به‌منظور تحقق تأثیر اجتماعی در حوزه شناختی است. از دیدگاه نظامی، تخریب و تأثیر در جمعیت هدف، مقصود اصلی جنگ شناختی هستند (وتل و دیگران، ۲۰۱۶). از زمان ظهور اصطلاح جنگ اطلاعاتی

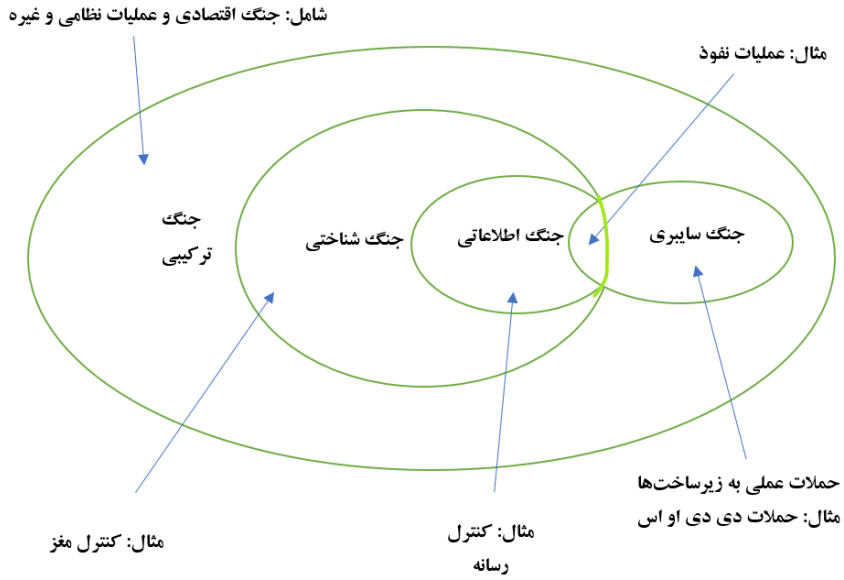
در دهه ۱۹۹۰، جنگ شناختی به‌عنوان اصطلاحی کلی برای عناصر جنگ غیرمستقیم، شامل عملیات تأثیرگذاری و جنگ روانی اطلاعاتی ایالات‌متحده؛ جنگ ترکیبی و کنترل بازتابی روسیه؛ کار جبهه متحد، جنگ سه‌گانه و مفهوم عملیات کنترل مغز چین و استفاده تایوان از جنگ سیاسی برای اطلاق به اصطلاحات فوق، تبدیل شده است. اگرچه نام‌ها ممکن است متفاوت باشند، اما وجه مشترک آن‌ها همچنان به تمرکز بر پیروزی از طریق قلب و ذهن مردم در میدان نبرد ذهنی است (یو و هو، ۲۰۲۳).

جنگ شناختی به فعالیت‌هایی اطلاق می‌شود که برای دستکاری محرک‌های محیطی انجام می‌شوند تا حالات ذهنی و رفتارهای دشمنان و همچنین پیروان در هر دو جنگ سرد و گرم کنترل شوند؛ بنابراین درحالی‌که جنگ سایبری می‌تواند اطلاعات غلط را اشاعه دهد، اصلی‌ترین حملات آن به زیرساخت دشمن یا سرقت اطلاعات به روش‌های عملی است و امنیت وب در این زمینه مسئله حیاتی است (آندرس و وینترفلد، ۲۰۱۳؛ رابینسون، جونز و جانیک، ۲۰۱۵).

جنگ اطلاعاتی تصمیم‌گیرندگان انسانی را هدف می‌گیرد و می‌تواند از طریق رسانه‌های اجتماعی آنلاین و شبکه‌های بین فردی آفلاین راه‌اندازی شود (ونتر، ۲۰۱۶؛ لیبیکی، ۲۰۲۰؛ پریر، ۲۰۲۰؛ دی پیترو، کاپرلو و کرسی، ۲۰۲۱) و همچنین باعث انحراف رأی‌دهندگان از لحاظ شناختی و عاطفی شود (دی‌بویتراگو، ۲۰۱۹؛ سرانو - پوچه، ۲۰۲۱). (نقل از هانگ و هانگ، ۲۰۲۰).

جنگ شناختی فقط بر ورودی (جریان اطلاعات) تمرکز نمی‌کند؛ بلکه بر سیستم شناختی و خروجی آن (رفتارها) نیز تمرکز دارد. جنگ شناختی در اثرات خود شبیه به جنگ نفوذی است؛ بنابراین بااینکه همه این نوع جنگ‌ها (جنگ سایبری، جنگ اطلاعاتی، جنگ شناختی و جنگ ترکیبی) شامل عنصر عملیات نفوذ هستند و ممکن است بر شناخت انسان تأثیر بگذارند، صرفاً جنگ شناختی به‌طور خاص با یکپارچه‌سازی علوم اعصاب مسلح در عملیات مختلف به کنترل مغز اختصاص دارد.

شکل ۱ رابطه مفهومی بین جنگ شناختی و سایر انواع جنگ از نظر (هانگ و هانگ، ۲۰۲۰) را نشان می‌دهد. از نظر آن‌ها همه انواع جنگ می‌تواند عنصر عملیات تأثیرگذاری را در بر داشته باشد و بر شناخت انسان تأثیر بگذارد؛ اما فقط جنگ شناختی به‌طور خاص به کنترل مغز با ادغام علوم اعصاب مسلح در عملیات مختلف توجه دارد.



شکل ۱. رابطه مفهومی بین جنگ شناختی و سایر انواع جنگ (هانگ و هانگ، ۲۰۲۰)

جنگ شناختی به مطالعه نحوه تأثیر اطلاعات بر مغز و ذهن انسان و نحوه بهره‌برداری از این تأثیرات برای دستیابی به اهداف نظامی و سیاسی می‌پردازد. این نوع جنگ از دیگر انواع جنگ، متمایز است؛ زیرا به‌طور خاص بر کنترل ذهن و رفتار انسان‌ها از طریق تکنیک‌های پیچیده‌تر عصبی و شناختی تمرکز دارد و با استفاده از علوم اعصاب و فناوری‌های مرتبط، تلاش می‌کند با نفوذ به سیستم‌های عصبی و شناختی، تصمیم‌گیری و رفتار افراد را به نفع طرف مقابل تغییر دهد.

هدف جنگ شناختی

آنچه در زمینه جنگ شناختی جدید است مربوط به قابلیت فناوری‌ها است که امکان جنگ روانی را فراهم می‌کنند. این پدیده به‌منظور تحمیل اراده سیاسی، منجر به سلب اعتبار دولت‌ها با ایجاد تفرقه می‌شود. ابزارهای به اشتراک‌گذاری اطلاعات به دشمنان اجازه می‌دهد که به‌طور مستقیم در فرایندهای سیاسی - ملی و ذهن شهروندان نفوذ کنند. هدف از حملات جنگ شناختی تغییر یا گمراه کردن افکار رهبران و نیروهای عملیاتی، اعضای طبقات اجتماعی یا حرفه‌ای، مردان و زنان یک ارتش، یا در مقیاس

بزرگ‌تر، کل جمعیت یک منطقه، کشور یا گروهی از کشورها و تأثیر بر قلمرو، نفوذ، قطع خدمات، حمل‌ونقل و غیره است. ابزارها می‌توانند شامل سایبر اجتماعی، سایبر فنی، جنگ الکترونیکی و سخن‌پراکنی باشند (فنسترماخر، اوزچا، لارسون، ویتیلو و شلمن، ۲۰۲۳).

توانایی‌های نظامی در دو دهه گذشته به نحوی تقویت شده است که مرز بین زمان جنگ و صلح را برداشته و جنگی پیوسته را آغاز کرده است. جنگ شناختی به‌عنوان پیشرفته‌ترین شکل جنگ تاکنون از تلاش برای کنترل رفتار در مقیاس جمعی به‌منظور کسب مزیت استراتژیک ارائه شده است. به‌جای میدان‌های جنگ پر از تلفات انسانی در جنگ مستقیم، میدان عملیات جنگ شناختی ذهن انسان است و در آن عملیات در زمینه‌های ادراک، احساس و حافظه انجام می‌شود. هدف از این نوع جنگ کنترل دائمی و بهره‌برداری است (پاستور، ۲۰۲۴).

با توجه به آسیب‌پذیری بالای شناخت انسان در برابر دستکاری و فریب، هدف جنگ شناختی تحت تأثیر قرار دادن فرایندهای تفکری مانند دیدگاه‌ها، تصمیم‌گیری‌ها و رفتارها است. شناسایی و رد کژاطلاعات و دُژاطلاعات نیازمند مهارت‌های تفکر انتقادی است تا منابع اطلاعاتی نادرست را شناسایی و درک کنیم. جنگ شناختی نوعی تبلیغات است که از طریق رسانه‌های منحرف یا رسانه‌های اجتماعی به‌منظور اهداف سیاسی یا نظامی با هدف پرورش و القای روایت‌های مغرضانه و متضاد در میان افراد مورد هدف منتشر می‌شود به‌گونه‌ای که با مختل کردن داوری‌هایشان آن‌ها را مجبور به رفتار متناسب کند؛ بنابراین آنچه در مورد تأثیرات شناختی جنگ شناختی در زمان صلح نگران‌کننده‌تر است، تأثیر آن بر میدان جنگ نیست، بلکه پیامدهای سیاسی و اجتماعی آن است (مارسیلی، ۲۰۲۳).

جنگ‌های نوین از ابزارها و روش‌های پیچیده‌ای استفاده می‌کنند که به‌طور گسترده‌ای با یکدیگر تعامل دارند، اما هرکدام ویژگی‌ها و اهداف خاص خود را دارند که آن‌ها را از یکدیگر متمایز می‌کند. این جنگ‌ها به‌تدریج از قالب‌های سنتی خود خارج شده و به شکل‌های پیچیده‌تر و چندبعدی‌تر تکامل یافته‌اند. این تغییرات، به ظهور انواع جدیدی از جنگ منجر شده که هرکدام ویژگی‌ها و اهداف خاص خود را دارند. جنگ شناختی به‌طور خاص بر توانایی‌های ذهنی، بُعد شناختی، تغییر ادراک و رفتار افراد و جوامع بدون

نیاز به استفاده از ابزارهای سنتی جنگ تکیه دارد؛ بنابراین هدف نهایی جنگ شناختی تغییر دیدگاه افراد به‌منظور تأثیر بر فرایند تصمیم‌گیری است.

حوزه‌های جنگ شناختی

حوزه‌های جنگ شناختی بسیار گسترده و متنوع هستند و هرکدام از این حوزه‌ها می‌توانند به‌طور جداگانه یا ترکیبی برای دستیابی به اهداف استراتژیک در جنگ شناختی استفاده شوند. درک دقیق این حوزه‌ها و تهدیدات مربوط به آن‌ها برای مقابله مؤثر با جنگ شناختی و حفاظت از جوامع و دولت‌ها حیاتی است. دانیک و بریگز (۲۰۲۳)، حوزه‌های انجام جنگ شناختی را در چهار دسته تفکیک می‌کنند:

۱. مناطق نفوذ فیزیکی، از جمله زیرساخت و نظام‌های اطلاعاتی؛
۲. فضای اطلاعاتی و سایبری، جایی که اطلاعات ایجاد، پردازش، ذخیره و اشاعه می‌شوند؛
۳. فرایندهای شناختی، تغییر دیدگاه، آگاهی، باورها، منافع و ارزش‌ها؛
۴. پیامدهای بحرانی عملیات شناختی.

مورل، جولین، ماریون، ژان مارک (۲۰۲۳)، نمونه‌های مختلفی از اقدامات را ذکر کرده‌اند که می‌توان آن‌ها را جنگ شناختی دانست. این موارد نشان می‌دهند که چگونه استراتژی‌های جنگ شناختی می‌توانند با استفاده از وسایل و کانال‌های مختلف انجام شوند:

۱. راه‌اندازی جنگ شناختی از طریق ابزارهای سایبری: مانند حمله سایبری بر شبکه‌ها. این حملات عمدتاً دولت، شبکه‌های حیاتی و تأمین‌کنندگان انرژی را هدف قرار می‌دهد. بااینکه این اقدام به‌عنوان جنگ سایبری در نظر گرفته می‌شود، اما می‌توان آن را از دیدگاه جنگ شناختی مطالعه کرد زیرا بخشی از استراتژی است که با استفاده از ابزارهای مختلف با هدف بی‌ثباتی گسترده‌تر انجام می‌شود.
۲. جنگ شناختی از طریق تماس مستقیم با افراد کلیدی: در ۶ فوریه ۲۰۲۳ در فرانسه، چندین نماینده زن از گردهمایی ملی پیامی دریافت کردند که به آن‌ها می‌گفت یکی از فرزندانشان بستری شده است، به‌طوری‌که آن‌ها قبل از رای‌گیری مهم از مجمع ملی خارج شوند. این حمله‌ای سعی داشت افراد هدف قرار گرفته را از رأی دادن و ایفای نقش خود در تصمیم‌گیری بازدارد.

۳. جنگ شناختی از طریق شبکه‌های اجتماعی: آخرین مثال در این زمینه در مالی در آوریل ۲۰۲۲ رخ داد. گروه واگنر گوری دسته‌جمعی را صحنه‌سازی کرد و ویدیویی جعلی ساخت تا به نظر برسد نیروی نظامی فرانسه مسبب آن جنایت است. نظامیان فرانسوی موفق شدند آن‌ها را در حال آماده‌سازی این صحنه ساختگی فیلم‌برداری کنند و لذت، امکان ایجاد یک ویدیو برای رد این اتهامات را فراهم کردند. گروه واگنر از این فرصت استفاده کرده بود تا کمپین تأثیرگذاری در شبکه‌های اجتماعی ایجاد کند و ارتش فرانسه را در مالی مشروعیت‌زدایی کند و به‌عنوان رهایی‌بخشان در برابر ستم فرانسه مورد استقبال قرار گیرند.

۴. مورد دیگری که اغلب برای توصیف جنگ شناختی استفاده می‌شود، سندروم هاوانا است که ممکن است جنگ شناختی با استفاده از ابزارهای نانو یا بیولوژیکی هدفمند، برای ایجاد ترس در افراد کلیدی آنان را مورد هدف قرار داده و داوری آن‌ها را تحت تأثیر قرار دهد، اما هیچ علت مشخصی رسماً شناسایی نشده است، هرچند، این مورد تا به امروز با شواهد مستند نشده‌اند.

جنگ شناختی حوزه‌های متنوعی دارد که می‌تواند به‌طور جداگانه یا ترکیبی برای دستیابی به اهداف استراتژیک به کار گرفته شود. این نمونه‌ها نشان می‌دهند که جنگ شناختی با استفاده از روش‌ها و ابزارهای مختلف می‌تواند به بی‌ثباتی جوامع و دولت‌ها منجر شود.

ابزارهای جنگ شناختی

ابزارهای مختلف جنگ اطلاعاتی از جمله عملیات روان‌شناختی و تبلیغات هرگز متوقف نشده‌اند (بوردا، ۲۰۲۴). جنگ شناختی از ابزارهای سایبری برای تغییر فرایندهای شناختی دشمن، بهره‌برداری می‌کند (کلاوری و دو کلوزل، ۲۰۲۲). همچنین از رسانه‌های اجتماعی برای پیشبرد اهداف در جنگ شناختی استفاده می‌کند (نوریه، بهتری و صفایی، ۱۴۰۱؛ میراحمدی، نصرتی و امیراحمدی، ۱۳۹۵). دو رویکرد اساسی به استراتژی جنگ شناختی وجود دارد: رویکرد اول به‌سرعت چرخه تصمیم‌گیری دشمن حمله می‌کند؛ رویکرد دوم حمله را بر دقت آن متمرکز می‌کند. این دو رویکرد تقریباً با دو دسته ابزار چارچوب جنگ شناختی یعنی تنش‌ها و فریب همخوانی دارند. مهم‌ترین نکته این است که رویکرد کلی جنگ شناختی وابسته به پایه فرماندهی دشمن فرایندهای تصمیم‌گیری،

ویژگی‌های فرمان و انتظارات تصمیم‌گیرندگان است. استفادهٔ ماهرانه از تنش و فریب در برابر مبنای فرمان ممکن است مکانیسم اصلی برای ایجاد اختلال شناختی باشد (دال، ۱۹۹۸). جنگ شناختی می‌تواند با بهره‌برداری از کژاطلاعات و دُژاطلاعات به‌طور مستقیم مردم را به پذیرش باور در موضوعی خاص ترغیب کند (گوادانو و گوتیری، ۲۰۲۱)؛ بنابراین ابزارهای جنگ شناختی شامل طیف گسترده‌ای از فناوری‌ها و تکنیک‌ها هستند که هدف آن‌ها تأثیرگذاری بر افکار، تصمیم‌گیری‌ها و رفتار افراد یا گروه‌ها در محیط منازعه است.

شبکه‌های مجازی و جنگ شناختی

از ویژگی‌های دنیای امروز استفادهٔ گسترده از ارتباطات موبایلی و رسانه‌هایی است که در فضاهای دیجیتال بدون نظارت فعالیت می‌کنند. تلاقی حوزه‌های اطلاعات، فیزیکی و شناختی/اجتماعی که توسط اکوسیستم دیجیتال/اینترنت، رسانه‌های اجتماعی و برنامه‌های ارتباطی تقویت می‌شود، شرایط عملیات شناختی را ایجاد می‌کند. اگرچه در میان اجزای آن چیز جدیدی وجود ندارد، اما نوآوری در جنگ شناختی، سرعت و قدرت انتشار باورهای درست یا غلط است که به‌طور عمیق در ذهن افراد نقش می‌بندد. واگیری اطلاعاتی که در زمینه بحران کووید-۱۹ پدید آمد، می‌تواند به‌عنوان سنگ محک عمل کند. این اثر ابهام‌آفرین باعث می‌شود که افراد بدون آگاهی، به اطلاعات و منابع خاصی بیش‌ازحد اعتماد کنند یا به دلیل سردرگمی کامل از اعتماد به آن‌ها خودداری کنند (مارسیلی، ۲۰۲۳).

شبکه‌های مجازی به‌عنوان ابزاری قدرتمند برای انتقال اطلاعات و تأثیرگذاری بر عقاید و افکار افراد شناخته شده‌اند. از سویی، جنگ شناختی به‌عنوان روشی برای تأثیرگذاری بر افکار و عقاید افراد و جوامع، از اهمیت به سزایی برخوردار است. این دو عامل در دنیای مدرن به اَشکال مختلفی با یکدیگر تعامل دارند و تأثیرات گسترده‌ای بر جوامع و فرهنگ‌ها می‌گذارند. از سوی دیگر، جنگ شناختی به‌عنوان نوعی جنگ نوین در دنیای دیجیتال مطرح است. در این نوع جنگ، فعالیت‌ها و اقداماتی با استفاده از فناوری‌های روز دنیا صورت می‌گیرد تا به دستیابی به هدف‌هایی مانند تحلیل، تشخیص، تحریف و کنترل اطلاعات بپردازد. در جنگ شناختی، اهداف اصلی شناخت، تحلیل و کنترل اطلاعات است و از فناوری‌های پیشرفته مانند هوش مصنوعی، تحلیل داده‌ها و شبکه‌های اجتماعی

استفاده می‌شود. به عبارتی، شبکه‌های مجازی نقش مهمی در جنگ شناختی دارند. با استفاده از این فناوری، امکان برقراری ارتباطات امن و قابل‌اعتماد بین دستگاه‌ها و کاربران فراهم می‌شود و امکان تحلیل، تشخیص و کنترل اطلاعات در دسترس قرار می‌دهد. این ترکیب بین شبکه‌های مجازی و جنگ شناختی، امکانات و قابلیت‌های منحصربه‌فردی را برای مدیریت و کنترل اطلاعات در دسترس قرار می‌دهد و به دولت‌ها، سازمان‌ها و نیروهای نظامی امکان مقابله با تهدیدات سایبری را می‌دهد. به عبارتی استفاده از شبکه‌های مجازی در جنگ شناختی، امکانات جدیدی را برای ارتباطات و امنیت اطلاعات به ارمغان می‌آورد و در بهبود راهبردها و تدابیر مربوط به امنیت سایبری مؤثر است.

هوش مصنوعی و جنگ شناختی

استفاده از هوش مصنوعی در جنگ شناختی به یکی از موضوعات بحث‌برانگیز در دوران معاصر تبدیل شده است. هوش مصنوعی با قابلیت‌های پیشرفته در پردازش اطلاعات، تحلیل داده‌ها و تصمیم‌گیری خودکار، به‌طور فزاینده‌ای در عرصه‌های نظامی و جنگ‌های مدرن به کار گرفته می‌شود. این فناوری‌ها به دولت‌ها و ارتش‌ها این امکان را می‌دهند که عملیات نظامی خود را با دقت و کارایی بیشتری اجرا کنند که شامل تحلیل داده‌های جمع‌آوری شده از میدان نبرد، پیش‌بینی تحرکات دشمن و حتی استفاده از پهپادها و ربات‌ها برای انجام مأموریت‌های پیچیده می‌شود. از سوی دیگر، جنگ شناختی به‌کارگیری استراتژی‌هایی برای تأثیرگذاری و تغییر درک، تصمیم‌گیری و رفتار افراد یا گروه‌ها از طریق دستکاری اطلاعات و انتشار اطلاعات نادرست است. در این زمینه، هوش مصنوعی نقش مهمی در تسهیل و تقویت این استراتژی‌ها ایفا می‌کند. الگوریتم‌های پیشرفته یادگیری ماشین می‌توانند به تحلیل و پیش‌بینی الگوهای رفتاری افراد بپردازند و از این طریق ابزارهای قدرتمندی برای تبلیغات هدفمند، عملیات روانی و تأثیرگذاری بر افکار عمومی فراهم آورند.

همچنین، هوشمندسازی جنگ‌ها، چالش‌های اخلاقی و حقوقی فراوانی را به دنبال دارد. نگرانی‌هایی در مورداستفاده نادرست از این فناوری‌ها برای کنترل و نظارت بر جوامع، افزایش حملات سایبری و ایجاد نابرابری‌های بیشتر در توانایی‌های نظامی کشورها وجود دارد. ازاین‌رو، نیاز به مقررات و چارچوب‌های بین‌المللی برای کنترل و مدیریت این فناوری‌ها احساس می‌شود تا از تبدیل‌شدن هوش مصنوعی به یک تهدید جهانی

جلوگیری شود. اگرچه از سویی واضح است که علم شناختی به‌طور عمیق با ذهن انسان ارتباط دارد از طرف دیگر برای تبدیل به یک رشته مستقل نیاز به محیط مصنوعی (الکترونیکی و دیجیتال) ایجاد شده توسط رایانه‌ها دارد. در این زمینه، هوش مصنوعی و یادگیری ماشینی همراه با پلتفرم‌های چندرسانه‌ای دیجیتال بسیار تأثیرگذار هستند که توانایی اتصال جهانی را فراهم می‌کنند (مارسیلی، ۲۰۲۳). تلاش‌های ضداطلاعات کاری دشوار و بی‌ثمر است. در نهایت، دشمن همیشه در سایه پنهان است. ایجاد دُژاطلاعات هزینهٔ کمتری دارد و زمان کمتری را نسبت به تلاش‌های بررسی واقعیت می‌گیرد. منابع انسانی کافی برای مقابله با دُژاطلاعات در تمام اشکال آن وجود ندارد. بااین‌حال، با کمک فناوری، می‌توانیم برخی از انواع دُژاطلاعات را به‌طور مؤثر در مراحل ابتدایی تشخیص دهیم. مثلاً تعیین آدرس آی‌پی راهی اساسی برای شناسایی منبع دُژاطلاعات است. فناوری هوش مصنوعی می‌تواند برای تجزیه‌وتحلیل اولیه پست‌های آنلاین استفاده شود و یادگیری ماشین مورداستفاده در این فرایند می‌تواند به‌طور خودکار برخی از مشکلات بالقوه را فیلتر کند و حجم کار انسانی را کاهش دهد (لین، ۲۰۲۳). در عصر هوشمندسازی مواجهات مبتنی بر هوش مصنوعی در دسته مواجه شناختی قرار دارند و اساساً سه دامنه عمده را شامل می‌شوند: مواجهات شناختی در فضای فیزیکی، فضای مجازی و دنیای روح انسان. جوهر مواجهه شناختی، مواجهه دانش و رقابت هوش است. برای دو طرف درگیر در نبرد، درک کامل، فهم عمیق و واکنش سریع به محیط‌های عملیاتی، تهدیدها، اهداف و حریفان و سطوح شناختی و توانایی‌های آن‌ها در تجزیه‌وتحلیل، ارزیابی، تصمیم‌گیری و اراده در موقعیت‌های عملیاتی، تأثیر مستقیم بر اجرای نبرد، سازمان‌دهی کمپین و تصمیم‌گیری‌های راهبردی دارد که این خود بر جریان و نتیجه جنگ‌ها تأثیر می‌گذارند. دیدگاه پیروزی یا شکست در جنگ هوشمندانه از «مبارزه با کشتار فراوان برای فضای میدان نبرد و تمرکز بر نابودی نیروهای دشمن» به «نفوذ نرم تأثیرگذار بر روحیه نظامی و غیرنظامی و همچنین بازی‌های شناختی که تصمیم‌گیری فرماندهی دشمن را آزار می‌دهد»، در حال تغییر است. مواجهه شناختی در جنگ انسانی از رقابت‌های اطلاعاتی و مواجهه‌های دانشی بین افراد به مواجهه‌های بین افراد، بین افراد و هوش مصنوعی ماشین‌ها و بین هوش مصنوعی ماشین‌ها تغییر خواهد کرد. با ادغام تدریجی عملیات بین فضای مجازی، فضای فیزیکی و فضای سایبر به‌عنوان حوزه اصلی عملیات هوشمندسازی، مواجه شناختی مانند حمله و دفاع سایبری و کنترل افکار عمومی

به نقطه تمرکز درگیری طرفین نزاع در عملیات تبدیل خواهند شد (لی شیهوا، ژانگ ژیچانگ و کائو شینهو، ۲۰۲۱).

جنگ شناختی مسئله‌ای نگران‌کننده برای تمام کشورهاست، اما تفاوت‌های بسیار مهم در رویکرد بین کشورهایی مانند ایالات‌متحده یا فرانسه و کشورهایی مانند روسیه، ایران یا چین وجود دارد. این رویکردهای متفاوت باعث عدم آمادگی کشورها در برابر تهدیدهای جهانی است. مفهوم امنیت شناختی به نظر می‌رسد یک شیوه امیدبخش برای تأمل در این حوزه باشد (دانت، ۲۰۲۳).

در غرب، اسناد بسیاری به جنگ شناختی پرداخته‌اند. ویژگی مشترک در این تفکر، تمایل به رویکرد علمی - فناوری و تمرکز بر تسلیح زیست‌فناوری‌ها و علوم اعصاب است. به‌نحوی‌که وزیر دفاع فرانسه از شکل جدیدی از جنگ که توانایی‌های مرتبط با دستکاری اطلاعات، دژّ اطلاعات، سایبرنتیک، روان‌شناسی، مهندسی اجتماعی و زیست‌فناوری که می‌توان آن را به‌عنوان شکلی جدید از جنگ خلاصه کرد، سخن می‌گوید و آن جنگ شناختی است که توانایی بهره‌برداری از آسیب‌پذیری‌های مغز انسان را دارد (دانت، ۲۰۲۳)؛ بنابراین هوش مصنوعی در جنگ شناختی به دولت‌ها و ارتش‌ها امکان می‌دهد عملیات نظامی را با دقت بیشتری اجرا کنند و از طریق تحلیل داده‌ها و پیش‌بینی تحرکات دشمن بهبود یابند. همچنین، این فناوری استراتژی‌های جنگ شناختی را برای تأثیرگذاری بر درک و تصمیم‌گیری افراد تقویت می‌کند. بااین‌حال، استفاده از هوش مصنوعی چالش‌های اخلاقی و حقوقی نیز به همراه دارد، از جمله نگرانی‌هایی در مورد کنترل جوامع و افزایش حملات سایبری. تفاوت‌های رویکردی بین کشورها در مواجهه با این مسئله، نیاز به مقررات بین‌المللی برای مدیریت این فناوری و جلوگیری از تبدیل آن به تهدید جهانی را برجسته می‌سازد.

راهکارهای مقابله با تهدیدهای جنگ شناختی

جنگ شناختی می‌تواند جنبه‌های مختلف عملکرد جوامع را تحت تأثیر قرار دهد. این جنگ به سرمایه اجتماعی یک کشور حمله می‌کند و منجر به سؤال‌هایی در مورد اقدامات دفاعی می‌شود و نگرش‌ها و واکنش‌ها به تحریک‌های مهاجم را تحت تأثیر قرار می‌دهد. هرچند، جنگ شناختی نمی‌تواند به عملیات اطلاعاتی، مهندسی اجتماعی یا مبارزه برای قلب و ذهن محدود شود، بلکه باید به تمام زمینه‌های فعالیت افراد و جوامع که احتمال

حملات ایدئولوژیکی برای آن‌ها هست، توسعه یابد (رچکوفسکی و لیس، ۲۰۲۲). برای کاهش تأثیرات چالش‌ها و تهدیدها و افزایش مقاومت دولت در حوزه شناختی، رچکوفسکی و لیس، اقدامات زیر را پیشنهاد می‌دهند:

- انجام مطالعات تحلیلی به‌منظور توسعه آگاهی موقعیتی (عملیاتی)، شناسایی خطرات و پیامدهای آن‌ها برای امنیت ملی و همچنین توانایی تفکیک حقایق از عقاید، حقیقت از دروغ و شواهد از حدس‌ها؛
- تغییر دیدگاه نسبت به تهدیدها به امنیت کشور، زیرا تهدیدهای متعدد از اقدامات دشمن در زیر آستانهٔ یک تنش مسلحانه باز (منطقه خاکستری) نشأت می‌گیرند و با تأثیر آن‌ها بر جامعه مرتبط هستند؛
- افزایش کارایی ارتباطات استراتژیک از طریق ادغام فعالیت‌های دیپلماسی عمومی، امور عمومی و هماهنگ‌سازی آن‌ها در سطح سیاسی - استراتژیک؛
- تلاش برای درک حالت پایانی موردنظر عملیات دشمن در زمینه ابهام در تعارضات منطقه خاکستری؛
- مانع‌شدن از جنگ روانی دشمن برای جلوگیری از دستیابی به واکنش مورد انتظار مخاطبان هدف؛
- جلوگیری از اشتباه در تعیین محدوده‌های خطرات قابل‌قبول (خطوط قرمز) برای یک رقیب بالقوه؛
- انجام ارزیابی مداوم از آسیب‌پذیری خود در تمام ابعاد سیاسی، نظامی، اقتصادی، اجتماعی، اطلاعاتی، زیرساختی، محیط فیزیکی و زمانی و همچنین ارزیابی پیشرفت و مزایای یک رقیب بالقوه در این ابعاد؛
- استفاده از فناوری‌های جدید (مانند هوش مصنوعی، داده‌های بزرگ) به‌منظور کسب مزیت در عملیات شناختی از جمله توانایی مقابله با این نوع حملات.

فضای شناختی حوزهٔ عملیاتی جدید و مهمی است که ارتباط نزدیکی با فضای سایبری دارد. برای مقابله با تهدیدات جدید جوامع و امنیت ملی آن‌ها، تسوچیا پیشنهاد می‌دهد دو کشور ژاپن و ایالات‌متحده با همکاری هم قوانین و نرم‌افزارهایی را برای مدیریت مؤثر جنگ سایبری ایجاد کنند. به نظر وی گام‌های اولیه باید برای تدوین پاسخ‌های مشترک سریع، جمع‌آوری اطلاعات، حفاظت از زیرساخت انتخابات، ایجاد دفاع سایبری فعال، ترویج قوانین و اصول رفتاری و گسترش سواد رسانه‌ای برداشته شود. تسوچیا همچنین،

اظهار می‌دارد که با ظهور جنگ شناختی، نیاز مبرم به ساختارهای حکمرانی جدید وجود دارد (تسوچیا، ۲۰۲۲). مقابله با تهدیدهای جنگ شناختی نیازمند ترکیبی از راهکارهای فنی، آموزشی، اجتماعی و حتی همکاری‌های بین‌المللی است. با اجرای این راهکارها، کشورها و جوامع می‌توانند از خود در برابر تأثیرات مخرب این نوع جنگ‌ها محافظت کرده و به‌طور مؤثری با این تهدیدات مقابله کنند.

نتیجه‌گیری

در درگیری‌های آینده نقش نیروی نظامی و استفاده از زور کم خواهد بود و نقش غیرنظامیان و ابزارهای غیرنظامی بسیار برجسته‌تر خواهد بود. درگیری به‌طور همزمان در چندین حوزه رخ خواهد داد و میدان نبرد می‌تواند هرجایی باشد. هرچند، هنوز در مورد مفهوم و کاربرد جنگ شناختی در مباحث علمی و آموزشی و نیز در دستورالعمل‌های نظامی ابهام وجود دارد اما کشورهای جهان به‌ناچار بایستی راهبردهای مرتبط با جنگ شناختی را در عملیات خود بگنجاند. راه‌حل‌های این چالش‌ها مستلزم آمیزه‌ای از اقدامات سیاسی - نظامی است که با خرد جمعی همراه است. چالش اصلی جنگ شناختی نامرئی‌بودن آن است و تنها چیز قابل مشهود در این نوع جنگ تأثیر و تبعات آن است و تا آن هنگام راهکار مواجه برای مقابله با آن اغلب دیر شده است. مفهوم امنیت شناختی می‌تواند به‌عنوان راه‌حلی امیدبخش برای مقابله با آن به کار رود. همچنین بالا بردن سطح سوادهای نوین پیش از سواد اطلاعاتی و سواد رسانه‌ای و نیز تقویت تفکر انتقادی در افراد جامعه و به‌کارگیری افرادی که در حوزهٔ تولید محتوا اینترنتی مشغول فعالیت هستند، می‌تواند از راهکارهای مناسب برای خنثی‌سازی تبلیغات مخرب دشمن علیه شهروندان کشور باشد.

جنگ شناختی به‌عنوان ابزاری قوی در دست بازیگران مختلف قرار دارد و می‌تواند بدون استفاده از خشونت فیزیکی، تغییرات بزرگی در جبهه مقابل ایجاد کند. این نوع جنگ نیازمند درک عمیقی از حوزه‌های روان‌شناسی، جامعه‌شناسی و فناوری‌های نوین است تا بتواند مؤثر عمل کرده و به اهداف خود برسد؛ بنابراین آشنایی با این حوزه‌ها می‌تواند در جهت پیشبرد یا خنثی‌سازی اهداف جنگ شناختی مفید باشد.

توصیه‌های کلیدی برای سیاست‌گذران دفاعی:

۱. ادغام راهبردهای جنگ شناختی در برنامه‌ریزی دفاعی
۲. تقویت زیرساخت‌های شناختی جامعه و ارتقای امنیت شناختی
۳. سرمایه‌گذاری در تحقیقات بین‌رشته‌ای، افزایش سواد رسانه‌ای و تفکر انتقادی

تشکر و قدردانی

از تمام بزرگوارانی که در انجام این پژوهش نویسنده را یاری دادند، صمیمانه سپاسگزارم.

تضاد منافع

بدین‌وسیله نویسنده تصریح می‌کند که هیچ‌گونه تضاد منافعی در خصوص پژوهش حاضر وجود ندارد.

منابع

- پناهی‌فر، سجاد و قائدی، علی (۱۴۰۲). بررسی تأثیر آموزش مؤلفه‌های جنگ شناختی بر روی تعهد سازمانی کارکنان نظامی. پژوهش‌نامه علوم دفاعی. ۳(۱)، ۱-۱۶.

https://www.spf1401.ir/article_709369.html

- ترابی، قاسم؛ طاهری‌زاده و ناصر، محمد (۱۴۰۰). انقلاب سایبری و تحول مفهوم جنگ اطلاعاتی در عرصه روابط بین‌الملل. مطالعات بین‌المللی، ۱۷(۴)، ۴۷-۶۵.

https://doi.org/10.22034/isj.2021.279939.1432

- حاجی‌زاده، سیروس (۱۴۰۱). تبیین زمینه‌ای، نظری، مفهومی و کاربردی جنگ شناختی مطالعه موردی روسیه. دوفصلنامه بازی جنگ، ۵(۱۰)، ۱۰۳- ۱۴۳.
http://www.ijwg.ir/article_171153.html

- راجی، محمدهادی و افتخاری، اصغر (۱۳۹۸). جنگ ترکیبی غرب در برابر جمهوری اسلامی ایران (تحلیل ابعاد و روش‌ها). سیاست دفاعی، ۲(۲)، ۱۱۱-۷۵.

https://dor.isc.ac/dor/20.1001.1.10255087.1398.28.1.3.9

- سلطانی، فرزاد؛ محمدی منفرد، حسن و جاودانی مقدم، مهدی (۱۴۰۱). بررسی کاربرد جنگ شناختی در حوزه‌های عملیاتی سازمان ناتو. فصلنامه محیط‌شناسی راهبردی ج.ا.ایران، ۶(۴)، ۱۵۳-۱۷۸.
https://dor.isc.ac/dor/20.1001.1.28212673.1401.6.21.5.7

- قیامی، سید برات؛ سجادی اصیل، وحید و مصدق، مسعود (۱۳۹۹). معماری سازمانی جنگ شناختی در ارتش جمهوری اسلامی ایران. دوفصلنامه بازی جنگ، ۳(۷)، ۱۳۳-۱۵۲.

http://www.ijwg.ir/article_154317.html

- کشاورز، محمود؛ سیاهپوش، امیر؛ ارجینی، حسین و نائینی، علی‌محمد (۱۴۰۲). طیف‌بندی مردم در جنگ شناختی و نقش بازیگران در نبرد هوشمند به‌عنوان سرمایه انسانی. پژوهش‌های اجتماعی اسلامی، ۲۹(۱۲۷)، ۱۰۱-۱۲۶. https://doi.org/10.30513/iss.2024.5565.1312

- میراحمدی، سید علی؛ نصرتی، روح‌الله و امیراحمدی محسن (۱۳۹۵). بررسی نقش شبکه‌های اجتماعی در جنگ نرم. دانش انتظامی سمنان، ۶(۱)، ۱۸۹-۲۱۷.

https://ensani.ir/file/download/article/1677324459-10645-1401-104.pdf

- نوریه، وحید؛ بهتری، علی و صفایی، علیرضا (۱۴۰۱). جنگ شناختی بر بستر رسانه‌های اجتماعی، نهمین همایش ملی علوم و مهندسی دفاعی با محوریت فناوری‌های دانش‌بنیان دفاعی، تهران. https://civilica.com/doc/1753418/

- Bernal, A. Carter, C. Singh, I. Cao, K. & Madreperla, O. (2020). Cognitive warfare: An attack on truth and thought. NATO and Johns Hopkins University: Baltimore MD, USA .https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare.pdf

- Burda, R. (2023). Cognitive Warfare as Part of Society. Never-Ending Battle for Minds, The Hague Centre for Strategic Studies, Informationbased behavioural influencing and Western practice series, disponibil la https://hcss.nl/wp-content/uploads/2023/06/04-Cognitive_Warfare_as_Part_of_Society__Never_Ending_Battle_for_Minds.pdf

- Cho, H. Cannon, J. Lopez, R. & Li, W. (2022). Social media literacy: A conceptual framework. New Media & Society. https://doi.org/10.1177/14614448211068530

- Claverie, B. & Du Cluzel, F. (2022). Cognitive warfare: The advent of the concept of “cognitics” in the field of warfare. Available at: https://hal.science/hal-03635889/document

- Dahl, A. B. (1998). Command dysfunction: Minding the cognitive war. Air University Press. https://apps.dtic.mil/sti/tr/pdf/ADA360756.pdf

- Danet, D. (2023). Cognitive Security: Facing Cognitive Operations in Hybrid Warfare1. In European Conference on Cyber Warfare and Security, 22(1), 161-168. https://doi.org/10.34190/eccws.22.1.1442

- Danyk, Y & Briggs, C. M. (2023). Modern Cognitive Operations and Hybrid Warfare. Journal of Strategic Security, 16(1), 35-50. https://doi.org/10.5038/1944-0472.16.1.2032

- Danyk, Y. Maliarchuk, T. & Briggs, C. (2017). Hybrid war: High-tech, information and cyber conflicts. Connections, 16(2), 5-24 .https://www.jstor.org/stable/26326478

- Fenstermacher, L. Uzcha, D. Larson, K. Vitiello, C. & Shellman, S. (2023). New perspectives on cognitive warfare. In Signal Processing, Sensor/Information Fusion, and Target Recognition XXXII, 12547(172-187). SPIE.

https://doi.org/10.1117/12.2666777

- Feryna, J. & Kutěj, L. (2023). Implications for China from the War in Ukraine: Comparison of the Western and Taiwanese Views. Defense & Strategy, 23(2), 023-038. https://doi.org/10.3849/1802-7199.23.2023.002.023-038

- Ghiami, S. Sajjadi Asil, V. and Mossadegh, M. (2021). Organizational Architecture of Cognitive Warfare in the Army of the Islamic Republic of Iran. Iranian Journal of Wargaming, 3(7), 133-152. (in Persian) http://www.ijwg.ir/article_154317.html?lang=en

- Guadagno, R. E. & Guttieri, K. (2021). Fake news and information warfare: An examination of the political and psychological processes from the digital sphere to the real world. In Research anthology on fake news, political warfare, and combatting the spread of misinformation (218-242). IGI Global.

http://dx.doi.org/10.4018/978-1-7998-7291-7.ch013

- Hajizadeh, S. (2022). Contextual, theoretical, conceptual and practical explanation of cognitive warfare A case study of Russia. Iranian Journal of Wargaming, 5(10), 103-143. (in Persian) http://www.ijwg.ir/article_171153.html?lang=en

- Hung T-C & Hung T-W. (2020). How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars. Journal of Global Security Studies, 7(4), 1–18 https://doi.org/10.1093/jogss/ogac016

- Ibrahim, F, Rhode, S & Daseking M. (2023). A Systematic Review of Cognitive and Psychological Warfare. The Defence Horizon Journal's Post. DOI: 10.5281/zenodo.10205600

- keshavarz, M. siahpoosh, A. arjini, H. and naeini, A. M. (2024). The spectrum of people in cognitive warfare and the role of actors in intelligent warfare as human capital. Islamic social studies, 29(127), 101-126. (in Persian) https://doi.org/10.30513/iss.2024.5565.1312

- Krishnan, A. (2022). Fifth Generation Warfare, Hybrid Warfare, and Gray Zone Conflict. Journal of Strategic Security, 15(4), 14-31.

https://www.jstor.org/stable/10.2307/48707883

- Kümpel, A. S. (2022). Social media information environments and their implications for the uses and effects of news: The PINGS framework. Communication Theory, 32(2), 223-242 .https://doi.org/10.1093/ct/qtab012

- Lewis, J. A. (2022). Cognitive effect and state conflict in cyberspace. Center for Strategic and International Studies (CSIS). https://www.csis.org/analysis/cognitive-effect-and-state-conflict-yberspace

- Libicki, Martin C. 1995. What is Information Warfare? Wash- ington, DC: Institute for National Strategic Studies, National Defence University. https://apps.dtic.mil/sti/citations/ADA367662

- Lin, Y. Y. (2023). China's Cognitive Warfare Against Taiwan and Taiwan's Countermeasures. Taiwan Strategists, (20), 37-54.

https://www.airitilibrary.com/Article/Detail/P20220613001N202312210022-00003

- Maksymenko, S. D. & Derkach, L. M. (2023). Understanding modern cognitive war in the global dimension, its genesis in the ukrainian context: a review and directions for future research: Cognitive warfare and social impact operations. Defense & Strategy, 23(1), 126-148.

https://doaj.org/article/c4d7c74625724482b33f59be4f8cb76d

- Marsili, M. (2023). Guerre à la Carte: Cyber, Information, Cognitive Warfare and the Metaverse Applied Cybersecurity & Internet Governance, 2(1), 1-11. https://www.acigjournal.com/pdf-184299-105057?filename=Guerre%20a%20la%20Carte_%20Cyber_.pdf

- Miller, S. (2023). Cognitive warfare: an ethical analysis. Ethics and Information Technology, 25(3), 46, 1-10. https://doi.org/10.1007/s10676-023-09717-7

- Mirahmadi, Seyed Ali; Nosrati, Ruhollah and Amirahmadi Mohsen (2016). The Role of Social Networking in the soft war. Semnan police knowledge quartetly, 6(1), 189-217. (in Persian) https://ensani.ir/file/download/article/1677324459-10645-1401-104.pdf

- Morelle, M. Julien, C. Marion, D. & Jean-Marc, A. (2023, November). Towards a Definition of Cognitive Warfare. In Conference on Artificial Intelligence for Defense. DGA Maîtrise de l'Information, Rennes, France. hal-04328461 https://hal.science/hal-04328461/document

- Muñoz Plaza, F. Sotelo Monge, M. A. & Gonzalez Ordi, H. (2023, August). Towards the Definition of Cognitive Warfare and Related Countermeasures: A Systematic Review. In Proceedings of the 18th International Conference on Availability, Reliability and Security, 40 (1-7). https://produccioncientifica.ucm.es/documentos/64fffbeeab53484a60023e66?lang=en

- Nanz, A. Heiss, R. & Matthes, J. (2022). Antecedents of intentional and incidental exposure modes on social media and consequences for political participation: A panel study. Acta Politica, 57(2), 235–253. https://doi.org/10.1057/s41269-020-00182-4

- Nourieh, V. Beshti, A. and Safaei, A. (2022). Cognitive warfare on social media platform, 9th national conference on defense science and engineering with a focus on defense knowledge-based technologies, Tehran. (in Persian) https://civilica.com/doc/1753418

- panahifar, S. and Ghaedi, A. (2023). The effectiveness of cognitive warfare training on the organizational commitment of military personnel. Research of Defense Sciences, 3(1), 1-16. (in Persian) https://www.spf1401.ir/article_709369.html
- Pastor, A. (2024). Cognitive warfare. https://hal.science/hal-04420986/

- Raji, M. H. & Eftekhari, A. (2020). The West's Hybrid Warfare against the Islamic Republic of Iran. *Defense Policy*, *28*(109), 75-111. (in Persian) https://dpj.ihu.ac.ir/article_205399.html?lang=en
- Reczkowski, R. & Lis, A. (2022). Cognitive Warfare: what is our actual knowledge and how to build state resilience? Bezpieczeństwo. Teoria i Praktyka, 48(3), 51-61. http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.ojs-doi-10_48269_2451-0718-btip-2022-3-003

- Reding, D. F. & Wells, B. (2022). Cognitive warfare: NATO, COVID-19 and the impact of emerging and disruptive technologies. In COVID-19 Disinformation: A Multi-National, Whole of Society Perspective (25-45). Cham: Springer International Publishing. https://www.scienceopen.com/book?vid=5325d0b9-0cc6-434e-be7c-874dda1cf9f8

- Rogers, Z. (2021). The Promise of Strategic Gain in the Digital Information Age. The Cyber Defense Review, 6(1), 81-106. https://www.jstor.org/stable/26994114

- Soltani, F. Mohammadi monfared, H. and Javdani, M. (2023). Investigating the application of cognitive warfare in NATO's operational field. Quarterly Journal of Environmental Studies Strategic of the Islamic Republic of Iran, *6*(4), 153-178. (in Persian) https://dor.isc.ac/dor/20.1001.1.28212673.1401.6.21.5.7
- Tandoc, E. C. Jr. & Kim, H. K. (2023). Avoiding real news, believing in fake news? Investigating pathways from information overload to misbelief. 1174–1192. https://doi.org/10.1177/14648849221090744

- Tashev, B. Purcell, M. & McLaughlin, B. (2019). Russia's information warfare: Exploring the cognitive dimension. MCU Journal, 10(2), 129-147. https://www.usmcu.edu/Portals/218/CAOCL/files/RussiasInformationWarfare_MCUJ_Fall2019.pdf?ver=2019-11-19-093543-040

- Toraby, G. and taheri zadeh, M. N. (2021). The Cyber Revolution and The Evolution of the Concept of Information Warfare in the Field of International Relations. International Studies Journal (ISJ), 17(4), 47-65. (in Persian) https://doi.org/10.22034/isj.2021.279939.1432
- Tsuchiya, M. (2022). Governing Cognitive Warfare. In K. Govella (Ed.), Governing the Global Commons: Challenges and Opportunities for US-Japan Cooperation (47–50). German Marshall Fund of the United States. http://www.jstor.org/stable/resrep46996.9

- Van Overschelde, J. P. & Healy, A. F. (2001). Learning of nondomain facts in high-and low-knowledge domains. Journal of Experimental Psychology: Learning, Memory, and Cognition, 27(5), 1160. https://doi.org/10.1037/0278-7393.27.5.1160

- Votel, J. L. Cleveland, C. T. Connett, C. T. & Irwin, W. (2016). Unconventional warfare in the gray zone. Joint Forces Quarterly, 80(1), 101-109. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-80/jfq-80_101-109_Votel-et-al.pdf

- Yu, M. T. C., & Ho, K. (2023). COVID and cognitive warfare in Taiwan. Journal of Asian and African Studies, 58(2), 249-273.

https://doi.org/10.1177/00219096221137665