MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

The Building Resilience to Cognitive Warfare Technical Exchange Meeting

by Dr. Lura Danley and Dr. Brian Colder

Contents

Executive Summary

Established security fields, such as operational security, cybersecurity and counterintelligence, focus on threats, methods, and behaviors that are physical or digital/cyber. Securing the cognitive domain is emerging as a topic of importance as rapidly emerging and evolving technologies present opportunities as well as challenges for national security. “Cognitive security” broadens the threat and security landscape because the target is human cognition, which guides judgement, decision and sensemaking, attitudes, beliefs, and perceptions. On September 28, 2023, MITRE hosted a Technical Exchange Meeting (TEM) titled *Building Resilience to Cognitive Warfare* with participants from MITRE, the DoD, and the Australian Defense Force, which focused on securing the cognitive domain, including the identification of national-level partnerships and innovation opportunities.

Security considerations within the cognitive domain include attacks that involve the integration of cyber, disinformation/misinformation, psychological, and social-engineering capabilities [1]. While these attacks utilize discrete techniques and methods within established domains, the converging patterns of attack have given rise to public sector interest in what is being termed “cognitive warfare”. Given that securing the cognitive domain is a dynamic, social, and technological challenge, the TEM covered a wide variety of topics including the current landscape of cognitive warfare, the neuroscience and cognitive science underlying cognitive warfare, the cognitive warfare effect on public sector missions, and the methods and technologies that could be used to identify and assess cognitive warfare. Conclusions from the TEM informed the following suggestions for important courses of action:

- *Socialize cognitive warfare as a component of cognitive security to create more opportunities to build resilience.* The term cognitive warfare can artificially constrain the topic of securing the cognitive domain to only military or intelligence contexts. As a socio-technical challenge, cognitive security is impacted by individuals, technology, infrastructure, processes, culture, and goals. Like other security domains there should be consideration of how cognitive security can impact a wide range of public sector missions.
- *Prioritize the development of measures of effectiveness (MOEs) and operationalize lab-based research for a national security context.* Efforts to develop MOEs should leverage applied research from other domains such as marketing. These efforts should move beyond “reinventing the wheel” and towards tackling the challenge of how to design and conduct applied research studies.
- *Create an interdisciplinary community of interest for cognitive security research.* Stakeholders have mis-perceptions about the feasibility of measuring cognition using techniques outside of their specific field. The fast-paced information environment means that operational communities are often in a reaction-based posture, resulting in different tolerances for slower paced rigorous cognitive and human behavior research. As a result, there can be a "silver bullet" mentality or tendency to look for an easy solution to difficult problems without true interdisciplinary collaboration.

- *Research and develop evidence-based approaches to inform the implementation of Digital Force Protection programs that provide personnel with a heightened awareness of the vulnerabilities, threats, and impacts of digital data, to include physiological information.* Although the state of the science for using physiological data to predict aspects of cognition lacks maturity, current events indicate that exploitation of physiology has the potential to be a prevalent threat vector. As an example, in June 2023, the U.S. Army Criminal Investigation Division (CID) and the Naval Criminal Investigative Service (NCIS) identified that Service members across the military had reported receiving unsolicited smartwatches in the mail and notified service member to not turn on or use the devices [2,3].

The MITRE hosted TEM on *Building Resilience to Cognitive Warfare* provided novel insights and awareness into the problem of securing the cognitive domain. The TEM identified multiple potential courses of action that would advance the research and development of policies, methods, and technologies to better secure the cognitive domain. Investment in these key areas through interdisciplinary courses of action and cross sector partnerships will create opportunities to bring innovative approaches that result in building resilience to cognitive warfare.

Introduction

Established security fields, such as operational security, cybersecurity and counterintelligence, focus on threats, methods, and behaviors that are physical or digital/cyber. Securing the cognitive domain is emerging as a topic of importance as rapidly emerging and evolving technologies present opportunities as well as challenges for national security. “Cognitive security” broadens the threat and security landscape because the target is human cognition, which guides judgement, decision and sensemaking, attitudes, beliefs, and perceptions. Securing the cognitive domain presents a dynamic, social, and technological challenge and offers innovation opportunities of national and global interest. On September 28, 2023, MITRE hosted a Technical Exchange Meeting (TEM) on *Building Resilience to Cognitive Warfare* to identify national-level partnership efforts and innovation opportunities for the challenge of securing the cognitive domain.

Background: The Cognitive Domain and Cognitive Warfare

The cognitive domain holistically considers cognition as the attitudes, beliefs, and perceptions of those who transmit, receive, respond to, or act upon information [4,5]. Cognitive processes that could be targets of cognitive attacks include perception, attention, thought, imagination, intelligence, knowledge formation, memory and working memory, judgment and evaluation, reasoning and computation, problem-solving and decision-making, comprehension and language production [6,7]. While the focus on securing the cognitive domain often centers on human cognition, it also does not discount the implications and impact of human-machine teaming and systems.

In addition to a holistic consideration of cognition, security considerations within the cognitive domain include attacks that involve the integration of cyber, disinformation/misinformation, psychological, and social-engineering capabilities [1]. While these attacks utilize discrete techniques and methods within established domains, the converging patterns of attack techniques and methods have given rise to public sector interest in what is being termed “cognitive warfare” [8]. As an example of such interest, NATO has hosted a series of workshops to identify and develop research on the concept of cognitive warfare. Some of the takeaways from the workshops are: 1. NATO needs to seize the initiative in the cognitive domain, 2. cognitive resilience is vital to societies and forces, and 3. NATO and member nations need a capability with distributed sensing (including local, cultural, and social knowledge) and central sensemaking to understand the information environment. [9]

Cognitive Warfare: “Hype” or Novel?

A pervasive challenge for the topic of cognitive warfare is the lack of consensus on a definition. Prior to hosting the TEM, MITRE discussed the topic with MITRE subject matter experts (SMEs) possessing applied military and intelligence experience and coming from a range of academic backgrounds including cognitive psychology, cyber,

human factors and systems, neuroscience, security policy, international and political science, systems engineering, and artificial intelligence (AI). Discussions centered on identifying if cognitive warfare is perceived to be a novel emerging topic and if so, what are the potential challenges and needs to secure the cognitive domain.

SMEs overwhelmingly agreed that cognitive warfare is an emerging topic. Although there is no consensus definition, cognitive warfare does have conceptual descriptions based on shared fundamental assumptions. The shared assumptions that shaped the approach to the TEM include the following:

- Cognitive warfare represents a convergence of cross-domain, multi-dimensional, adversarial-based operations that present unique opportunities to apply technical skills, system enabling tools and counter tactics in novel ways. Established operations include psychological operations (PSYOP), Information Operations, and Cyber Operations, and examples of technology enablers and capabilities include Artificial Intelligence (AI) / Machine Learning (ML), human-machine teaming, human enhancement technologies, and modeling and simulation.
- In accordance with an adversary's national strategy, exploitation of the cognitive domain can occur across multiple dimensions of information environments.
- Cognitive warfare uses an interdisciplinary approach to explicitly alter human and/or machine cognition.

In addition to being viewed as a novel emerging topic, SMEs identified that cognitive warfare presents an opportunity to unify communities (i.e., defense, intelligence) and research domains (i.e., neuroscience, psychology, biotechnology, cognitive science, social and behavioral science, AI/ML), so that scientists, researchers, and analysts can impactfully and preemptively "get ahead" of future methods leveraging the best of science.

TEM Discussion Topics

To critically evaluate the cross-cutting topic of securing the cognitive domain at the *Building Resilience to Cognitive Warfare* TEM, the MITRE Team invited U.S. Government and MITRE SMEs to discuss the following topics.

The Cognitive Warfare Landscape

Discussions focused on cognitive warfare within the context of research, influence, and security. Dr. Lura Danley presented information on MITRE's efforts to examine and contribute to securing the cognitive domain and building resilience to cognitive warfare. Such efforts included participation in the NATO Science and Technology Organization (STO) Cognitive Warfare Workshop in November 2022 and co-authorship of the workshop's Technical Evaluation Report. The discussion summarized key challenges facing the topic area such as the potential negative connotations of "cognitive warfare" that can be avoided by referring to the field

as “cognitive security”, how stakeholders from different disciplines carry misperceptions about the state of the science maturity level of other disciplines, and how the fast-paced information environment creates obstacles by placing the operational community in a reaction-based posture. Despite these challenges, there was consensus that securing the cognitive domain presents an opportunity to unify communities (i.e., defense, intelligence) and research domains (i.e., neuroscience, psychology, biotechnology, cognitive science, social and behavioral science, AI/ML) so that scientists, researchers, and analysts can impactfully and preemptively “get ahead” of future methods leveraging the best of science.

Science and Security: Perspectives on the State of Cognitive Warfare

Dr. Doug Bryant and Ms. Sophia Gatsios from MITRE presented key insights on influence operations. Dr. Bryant raised the point that we don’t have enough information to know if influence operations work. He described multiple instances where known influence operations resulted in very little attributable effects, and discussed scientific literature suggesting that misinformation is not often shared and limited behavioral consequences. Further research indicates that countermeasures against influence operations are not well understood, and the effectiveness of most countermeasures has not been studied at all. Dr. Bryant suggested that the effectiveness of influence operations must be a research topic, and since we do not know our adversary’s intent, we should begin our research looking at our own offensive influence operations using control groups alongside the intended population.

Ms. Sophia Gatsios discussed her research on emerging trends across tactics and technologies that provide adversaries with advanced capabilities to maintain and sustain situational awareness and engage in operations. Sophia presented background information on ubiquitous technical surveillance (UTS) that generates vast amounts of commercial data and creates enduring records of our identity, locations, activity and connections. Ms. Gatsios also described advertising technology (AdTech) which is software and tools that advertisers use to implement, manage, track, and analyze data from digital advertising campaigns. The discussion examined the use of AI and natural language processing (NLP) to produce messages and media (i.e., AI generated voice messages and deepfakes, convincing journalism), and the maturity of AI/NLP based technologies used for influence operations. The conclusion of this section was that these types of tools and the data they produce offer many opportunities for our adversaries to run effective influence campaigns.

Dr. Paul Ward from MITRE discussed the cognitive science background underpinning resilience to cognitive warfare. Using output from NATO working group discussions, Dr. Ward presented a working definition of cognitive warfare as “a form of psychological-social-technical influence warfare that targets cognitive, neurological, psychological, sociocultural, and sociotechnical capabilities.” Cognitive warfare “disrupts, influences or exploits an

adversary's thinking – especially decision making, sensemaking, or situation awareness – at an individual, group and/or societal level" to provide a "decision advantage over an adversary". Models of cognition help identify many targets for cognitive operations. Targeting the basic processes underlying cognition can thus influence performance in both idealized and everyday behavior and decision-making. Ubiquitous dependence on automation for decision-making implies that cognitive warfare can also be used to influence humans and machines working together. Building cognitive resilience into human-machine teams requires designing the system to support continuous adaptation and graceful extensibility.

Dr. Beth Brokaw from MITRE described the neuroscience behind cognitive warfare, including how information can affect cognitive state, and how these changes can be seen on brain scans. However, outside of specialized laboratory settings, it is not possible to measure cognitive status with the precision of brain scanning. It is possible to use remote scanning, as well as wearable devices, to measure physiology such as heart rate, heart rate variability, respiration rate and more. However, many factors affect physiology, and these technologies can be less accurate for some populations (e.g., individuals with darker skin tones). Using wearable physiology measures, it can be possible to detect changes that indicate an individual is in an energetic state (e.g., excited, angry, stressed), but it's not currently possible to precisely determine that state with physiology alone. Even though the physiological signs of anger, fear and stress are currently indistinguishable, the potential exists for future scientific advances to tease apart the signals identifying these states and more accurately predict behavior from physiology.

Cognitive Security in Public Sector Missions

Speakers from the U.S. Government discussed their perspectives on cognitive warfare and public sector mission execution and outcomes. Mr. James McNeive, the Deputy Operations Officer at the Marine Corps Information Operations Center (MCIOC) provided an overview of MCIOC and discussed the significance of understanding how influence impacts battle space awareness.

COL Stephen Hamilton and Dr. Jan Kallberg of the Army Cyber Institute at West Point discussed how protecting warfighters from psychological operations used to mean ensuring physical separation between the warfighter and potential sources of influence. Now that the influence operations are happening online, the great power competition will require digital force efforts to protect troops from an assault in the cognitive domain [10]. There is no easy solution to digital force protection, but certainly providing ready access to the right information is part of the answer.

Methods and Technologies: Detecting, Deterring and Mitigating Cognitive Warfare

Mr. Steven Davic from MITRE described a recent MITRE research effort to evaluate commercial technologies that used publicly available information to identify and analyze influence

operations on social media. A list of influence technologies was compiled into a framework consisting of three capability categories: Situational Awareness, Interactions and Operations, and Assessments. This summary of commercial technologies demonstrated that in the current commercial marketplace the capabilities for collecting, analyzing, and visualizing data related to influence operations on social media are considerably more mature than the capabilities for measuring the effectiveness of influence operations. Extending these results to cognitive warfare, the results indicate a capability gap requiring applied research into modeling and measuring the effectiveness of cognitive warfare operations.

Mr. Daniel Sixto from MITRE presented the SP!CE framework, a box and arrow process framework that standardizes the mapping and analysis of influence operations. SP!CE also offers a knowledge base containing the tactics, techniques and procedures (TTPs) used in previously studied influence operations, and assessment metrics for those operations. Multiple techniques in SP!CE relate to aspects of cognitive warfare, including exploiting Pre-existing Prejudices and Psychological Biases, and the use of Sentiment Analysis to guide messaging.

Panelists from the U.S. Government and MITRE discussed the topic of *Applied Research to Build Resilience to Cognitive Warfare*". During the discussion panelists presented their insights on the top priorities for the operational community and researchers related to methods and measurement, and how measuring the effectiveness of cognitive operations might be unique. The panelists concurred that measuring the effect of cognitive operations faces the same challenges as making those measurements for other influence or information operations, and developing measures of effectiveness was a critical priority.

Top Ten Key Findings from the TEM

Presentations and discussions at the TEM produced the following conclusions:

- Developing measures of the effectiveness of cognitive warfare operations faces the same difficulties as measuring effectiveness of PSYOP and influence operations, namely, how to ascribe causality for any observed behavior changes to the operation under study. Additionally, it is important to have clearly defined metrics for cognitive effects of interest and to not avoid measuring what is most impactful because it may not be easy to measure.
- Cognitive warfare should be considered as a form of psychological-social-technical influence warfare that targets cognitive, neurological, psychological, sociocultural, and sociotechnical capabilities because:
    - It disrupts, influences, or exploits an adversary's thinking to provide a

decision advantage over an adversary.

  - It targets decision making, sensemaking, or situational awareness, at an individual, group and/or societal level.
  - The disruption, influence, or exploitation of an adversary's thinking is done using technology-enabled tactics, techniques, and procedures (TTPs). These TTPs act as force multipliers to reduce effort, resource requirements and risk, increase trust and build resilience.

- There are fundamental gaps in what the operational and research communities know about whether influence operations work or not, particularly when the operations are applied in the national security space. Influence countermeasures are also poorly understood.
- Future efforts to understand how to secure the cognitive domain could include exploring the use of UTS, AdTech, AI, and NLP to produce messages and media as well as the impact of improvements in media literacy for AI/NLP technologies used for influence operations.
- Measuring cognition is difficult, but not impossible. Cognitive psychology models of cognition provide frameworks to examine cognition to gain an understanding of potential threats and which aspects of cognition might be targeted by an adversary. The ubiquity of human-machine teaming for decision support implies that attacks on decision-support tools are also cognitive warfare.
- Measures of physiological activity such as electroencephalogram (EEG), heart rate, and body temperature provide insight into cognitive state, but those measures are not currently sufficient to distinguish an individual's thoughts, or to differentiate between complex emotional states. Continuing to monitor research on how to predict cognitive state using physiological measures will be critical for maintaining situational awareness of the potential cognitive warfare threat posed by physiological measurement devices.
- Commercial technologies used to analyze information operations are much better at engineering-heavy capabilities, such as collecting, visualizing, and analyzing data then capabilities that require theoretical advances, such as measuring influence operation effectiveness and assisting with causal inference.
- The SP!CE framework that describes the TTPs used in information operations already contains a subset of the TTPs used in cognitive warfare and is easily extended to include more.

Building resilience to cognitive warfare and securing the cognitive domain will require a fundamental culture shift in

how the public sector, particularly the U.S. Department of Defense, handles unwanted or counterproductive work behavior (i.e., shift from compliance-based training, cannot ban Service Members from using the internet or social media on personal devices). As a result, there needs to be a better understanding of how to effectively implement Digital Force Protection programs that provide personnel with a heightened awareness of the vulnerabilities, threats, and impacts of digital information, systems, and devices as well as an examination of how threats to the cognitive domain might impact such behaviors as “will to fight”.

Recommendations

The key findings from the TEM suggest several important courses of action for MITRE and Sponsors, as well as partnership opportunities to build resilience to cognitive warfare and secure the cognitive domain.

Socialize cognitive warfare as a component of cognitive security to create more opportunities to build resilience. The term cognitive warfare can artificially constrain the topic of securing the cognitive domain to only military or intelligence contexts. As a socio-technical challenge, cognitive security is impacted by individuals, technology, infrastructure, processes, culture, and goals. Like other security domains (i.e., cybersecurity, operational security, information security) there should be consideration of how cognitive security can impact a wide range of public sector missions.

Prioritize the development of measures of effectiveness (MOEs) and operationalize lab-based research for a national security context. Efforts to develop MOEs should leverage applied research from other domains such as marketing and move beyond “reinventing the wheel” and towards tackling the challenge of how to design and conduct applied research studies.

Create an interdisciplinary community of interest for cognitive security research. Stakeholders have mis-perceptions about the feasibility of measuring cognition using techniques outside of their specific field. The fast-paced information environment means that operational communities are often in a reaction-based posture, resulting in different tolerances for slower paced rigorous cognitive and human behavior research. As a result, there can be a "silver bullet" mentality or tendency to look for an easy solution to difficult problems without true interdisciplinary collaboration.

Research and develop evidence-based approaches to inform the implementation of Digital Force Protection programs that provide personnel with a heightened awareness of the vulnerabilities, threats, and impacts of digital data, to include physiological information. Although the state of the science for using physiological data to predict aspects of cognition lacks maturity, current events indicate that exploitation of physiology has the potential to be a prevalent threat vector. As an example, in June 2023, the U.S. Army Criminal Investigation Division (CID) and the Naval Criminal Investigative Service (NCIS) identified that Service members across the military had reported receiving unsolicited smartwatches in the mail and notified service member to not turn on or use the devices [2,3].

Summary

The TEM on *Building Resilience to Cognitive Warfare* provided novel insights and awareness into the problem of securing the cognitive domain. Given that securing the cognitive domain is a dynamic, social, and technological challenge, the goal of the TEM was to identify areas where interdisciplinary, applied approaches and partnerships would be most effective. In alignment with this goal, MITRE and public sector speakers led discussions on the cognitive warfare landscape, the neuroscience and cognitive science underlying cognitive warfare, the cognitive warfare effect on public sector missions, and the methods and technologies that could be used to identify and assess cognitive warfare. Through these discussions the TEM identified multiple potential courses of action that would allow the research and development of policies, methods, and technologies to better secure the cognitive domain. Investment in these key areas through interdisciplinary courses of action and cross sector partnerships will create opportunities to bring innovative approaches that result in building resilience to cognitive warfare.

Acknowledgements

The authors acknowledge and appreciate the support and guidance of the following MITRE leadership:

- Dr. Chris Fall, Vice President, Applied Science
- Dr. John Dileo, Department Manager, Emerging Technologies

The authors also acknowledge and appreciate the time, insight, expertise, and key contributions of the following experts who made the TEM possible:

- Mr. James McNeive, Department of the Navy Civilian and Deputy Operations Officer, Marine Corps Information Operations Center
- Col. Stephen Hamilton, Director of the Army Cyber Institute at West Point, United States Military Academy Associate professor
- Dr. Jan Kallberg, Senior Fellow, Center for European Policy Analysis (CEPA) Transatlantic Defense and Security program
- Dr. Elizabeth Brokaw, Biomedical Engineer and Researcher (MITRE)
- Dr. Douglas Bryant, Principal Social Behavioral, and Brain Scientist (MITRE)
- Steven Davic, Senior Systems Engineer (MITRE)
- Sophia Gatsios, Cyber Threat Intelligence Analyst (MITRE)
- Daniel Sixto, Data Analyst (MITRE)
- Dr. Paul Ward, Principal Cognitive Scientist and Chief Scientist for the Social and Behavioral Sciences Department (MITRE)

Endnotes

[1] The North Atlantic Treaty Organization (NATO) Allied Command Transformation (ACT)., "NATO Innovation Challenge Fall 2021 – Countering Cognitive Warfare", (October 8, 2021), available at https://www.act.nato.int/article/nato-innovation-challenge-fall-2021-countering-cognitive-warfare/

[2] U.S. Army Criminal Investigation Division., "Unsolicited Electronics Smartwatches Received by Mail", (June 23), available at https://www.cid.army.mil/Media/Press-Center/Article-Display/Article/3429159/cid-lookout-unsolicited-smartwatches-received-by-mail/

[3] Ziezulewicz, G., "The Naval Criminal Investigative Service (NCIS): Don't turn on that smartwatch you randomly received in the mail", (June 2023), available at https://www.navytimes.com/news/your-navy/2023/06/26/ncis-dont-turn-on-that-smartwatch-you-randomly-received-in-the-mail/

[4] U.S. Department of Defense, "Strategy for Operations in the Information Environment (SOIE)", (June 2016), available at https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf

[5] U.S. Department of Defense Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms", (February 2016).

[6] U.S. Air Force Joint Doctrine Publication 3-13 (JP 3-13), "Information in Air Force Operations", (February 2023), available at https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-13/3-13-AFDP-INFO-OPS.pdf

[7] Reed, S.K., "Cognition: Theory and Applications (9th edition)", (2013). Cengage.

[8] Blatny, J., and Masakowski, Y., "Mitigating and Responding to Cognitive Warfare", (2022), available at https://www.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-HFM-ET-356/$TR-HFM-ET-356-ES.pdf

[9] NATO. Workshop – Cognitive Warfare Concept (September 22, 2027). available at https://www.act.nato.int/article/workshop-cognitive-warfare-concept/

[10] Kallberg, J., and Hamilton, S. "How to protect troops from an assault in the cognitive domain", C4isrnet.com, available at https://www.c4isrnet.com/opinion/2020/11/04/how-to-protect-troops-from-an-assault-in-the-cognitive-domain/

Abbreviations and Acronyms

Term	Definition
AdTech	Advertising Technology
AI	Artificial Intelligence
CID	U.S. Army Criminal Investigation Division
IO	Influence Operations
ML	Machine Learning
MOE	Measures of Effectiveness
MITRE	The MITRE Corporation
MITRE Labs	MITRE Laboratories
NCIS	Naval Criminal Investigative Service
NLP	Natural Language Processing
PSYOP	Psychological Operations
S&T	Science and Technology
SP!CE ™	Structured Process for Information Campaign Evaluation
SME	Subject Matter Experts
TTPs	Tactics, Techniques and Procedures
TEM	Technical Exchange Meeting
UTS	Ubiquitous Technical Surveillance