Developing a Framework for Human-Centered Operations in the Information Environment

CDR Will Wells, Ph.D., MSC, USN
Director, Human Systems
Emerging Technologies
POC: CDR Will Wells, 571-372-7405
March 2025

Jim Belanich, Ph.D. and Sujeeta Bhatt, Ph.D.
Strategy, Forces and Resources Division
Institute for Defense Analyses

Maggie Eliot, MS
Program Scientist, Human Systems
Emerging Technologies (ctr)

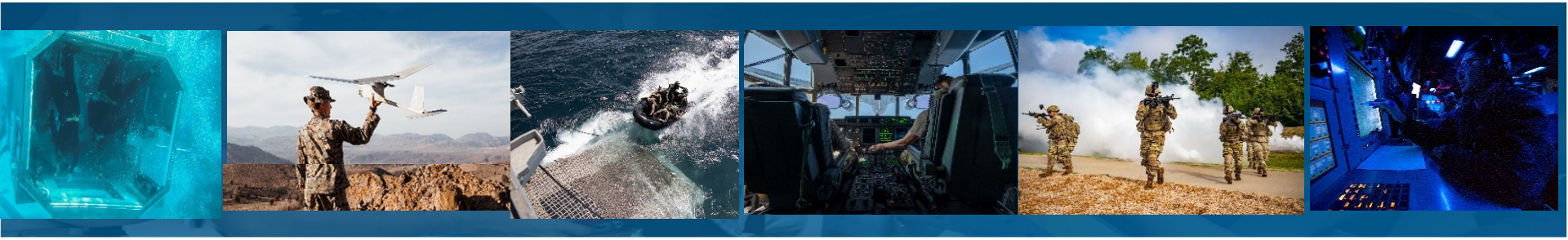
Disclaimer

The information presented here is for informational purposes only. The views expressed in this presentation are solely those of the presenter and do not necessarily reflect the official policy or position of the Department of Defense.

DoD Human Systems S&T Strategy

CUI

Purpose: **Develop and deliver technologies to enable, sustain, enhance, and quantify human and technology performance for measurably improved mission effectiveness.**



Rapidly evolving technologies and human systems have the potential to both transform kinetic and non-kinetic conflict and revolutionize day-to-day U.S supply chain and logistics operations. **Humans – Warfighters – play an intrinsic role in the application of rapidly evolving technologies, particularly artificial intelligence (AI) and autonomy.** Human data feeds and trains these technologies, humans modify AI actions, humans team with these technologies, and humans decide whether to use and trust even the most advanced and successful tools.

DoD Human Systems S&T Strategy

The HS S&T Enterprise covers four focus areas:

Personalized Assessment, Education and Training (PAET)	Human-Machine Teaming / Systems Interfaces and Cognitive Processes (HMT/SCIP)	Protection, Sustainment, and Warfighter Performance (PSWP)	Operations in the Information Environment (OIE)
• PAET envisions a readiness ecosystem to identify, manage, and develop knowledge, skills, competencies, and experiences to be mission ready for the 21st century operating environment	• HMT/SICP envisions Warfighters teamed with agents and machines through intuitive, individualized, and adaptive interactions that enhance mission effectiveness	• PSWP enables Warfighter superiority by understanding and overcoming key operational stressors and providing protection from environmental threats	• OIE envisions enduring decision advantage across military operations by using cutting-edge social, behavioral, cognitive, and neurological science research

DoD Human Systems S&T Strategy

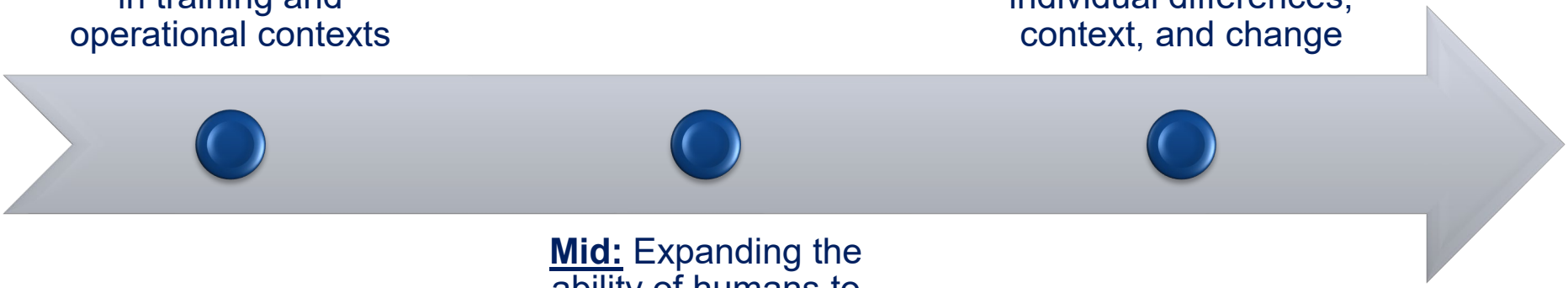
CUI

Strategy focus: The DoD HS S&T Strategy is based in part on the DoD Human Systems Community of Interest (HS CoI) Roadmap. This strategy focuses on increasing military HS capabilities in the following terms:

Near: Enhancing capabilities for measuring warfighters' performance, managing readiness, and enhancing effectiveness in training and operational contexts

Mid: Expanding the ability of humans to perform within teams that include humans and/or machines

Far: Developing adaptive systems that can learn through interaction with human teammates and other machines to enable uniquely effective teams that are sensitive to individual differences, context, and change



Background: Operations in the Information Environment

Information has always been a key to Military Operations

- If you know the enemy and know yourself, you need not fear the result of a hundred battles. (Sun Tzu, *The Art of War*, circa 500 BC)

- Many intelligence reports in war are contradictory, even more are false, and most are uncertain (von Clausewitz, *On War*, 1832)

Operating in the Information Environment has a long history, pre-dating the information age, DoD is now adjusting to address the rapid changes in how information can be used in military operations

Recently Updated Doctrine

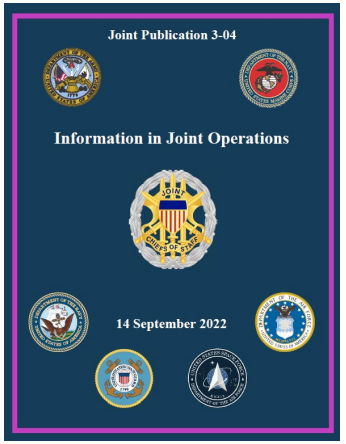
- Joint Publication 3-04: "Information in Joint Operations" (Sept 2022)
- Air Force Doctrine Publication 3-13: "Information in Air Force Operations" (Feb 2023)
- Army Doctrine Publication 3-13: "Information" (Nov 2023)
- Navy is currently developing new doctrine

Recent Conflict Examples (1)

Widescale Information Operations

Russian Information Operations (JP-3-04 - Information in Joint Operations (2022))

- Uses propaganda, disinformation, and cyber tactics to control narratives, using front organizations and staged acts to manipulate perceptions
- Undermines Ukraine's Western integration and supports Crimean separatists by eliminating non-Russian media in Crimea to control information
- Frames pro-Ukraine forces as Nazis and NATO as a threat



Targeted Attacks of Individuals

Russian False-Flag Operation (2015) (Goldsmith, 2019)

- Russian GRU-backed APT 28 (aka Fancy Bear) posed as ISIS-affiliated Cyber Caliphate and sent threatening messages to U.S. military wives
- Media coverage of the event fueled fears of ISIS targeting military families
- Similar tactics used in Ukraine, spreading disinformation to families
- Potential risks to DoD personnel and readiness

Image: https://www.crowdstrike.com/en-us/blog/who-is-fancy-bear/

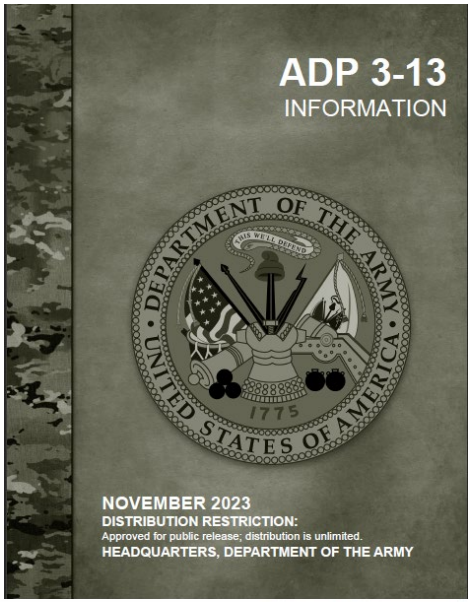
Recent Conflict Examples (2)

Information in the Security Environment

China's Strategy in the South China Sea (ADP 3-13)

The Peoples Republic of China (PRC) uses a strategy that involves: a) public opinion and media, b) psychological operations, and c) legal efforts warfare (i.e., lawfare) to influence the information at a level below armed conflict.

- Aggressive media messaging to news outlets and digital media promoting the narrative of China's historical claims to the South China Sea.
- The PRC has constructed and militarized many artificial islands
- Using paramilitary for physical actions to intimidate and limit other nation's maritime efforts in the region
- China made legal claim to the UN to stake the 'nine-dash line' as their sovereign area.
- Through consistent efforts, this narrative has become normalized.



Congressional Research Service (2017)
South China Sea Disputes, Report: IFI0607

Recent Conflict Examples (3)

Iran Disinformation & Violent Extremism

Iran engages in violence (often through terrorist proxies; e.g., Hamas, Hezbollah) and uses the information environment to offset the kinetic power differential:

- Aggressive media messaging to social media platforms- promoting a deluge of false narratives and images, disinformation, misinformation, and IO
- Attempting to reframe the use of violence against Israeli civilians (like the “freedom fighter” narrative after 9/11) as the fault of Israel
- Creating discord within the US, Israel and their allies (to create chaos and decease focus on terrorists)
- Using hostages in psychological operations extending to the families and community in general and attempting to keep them in a state of perpetual fear to achieve their objectives

Current Studies:

Duke University (Sherman et al, 2021) – posed as data buyers, determined kinds of US military personnel data sold, and evaluated national security risks of information availability.

- Sensitive active-duty member data (e.g., home address, health information, financial, locations) was obtainable by US- and non-US customers for $0.12 to $0.32 per record.
- Data broker lacked industry best practices to confirm customers (e.g., background checks, determine nationality of customer, description of data use)
- Access to personnel data could be used by malicious actors to target active-duty military personnel, veterans, and their families for OIE.

U.S. Army Cyber Command is conducting training exercises and experiments in 2024-25, with the plan to activate Theater Information Advantage Detachments (TIAD) in FY26. The goal is to help commanders counter disinformation and "malign influence" interfering with Army operations.

Government Accountability Office

- GAO-22-104714: Information Environment: Opportunities and Threats to DOD's National Security Mission
- GAO-21-525T: Information Environment: DOD Operations Need Enhanced Leadership and Integration of Capabilities

Examples Service Member Cyberexploitation

Russian generated content on social media appears legitimate, however used to track and target site visitors for deceptive or manipulated content that can develop into an echo chamber. Goldsmith (2019)

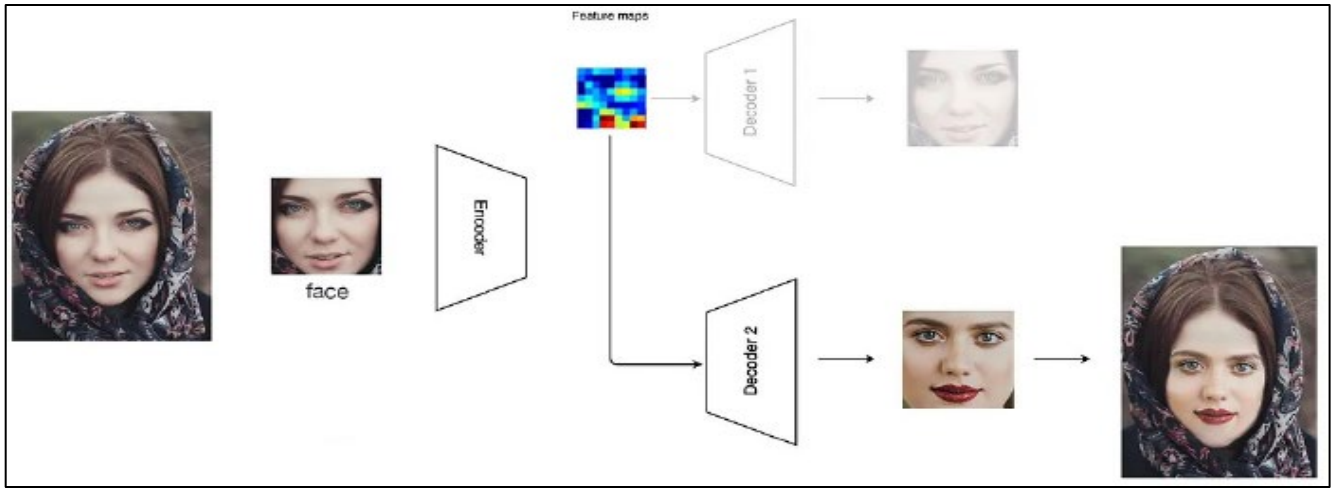
U.S. Navy officer was initially targeted by Chinese intelligence through a stock market trading chat room, that led to the service member receiving $15,000 for sending photographs he took of restricted naval base areas. He was sentenced to 27 months in prison in 2024. CBS News (Jan. 27, 2025)

A collaboration of military and civilian law enforcement agencies uncovered a sextortion scheme targeting service members run by inmates in the SC Dept of Corrections between 2015-2017. A total of 442 service members from across the DoD lost over $560,000. A similar scam led to the suicide of an Army veteran. Simkins (2018)

Operations in the Information Environment: Influenced by New Technologies

Generating Content

Generative Adversarial Networks (GANs) can produce realistic audio/video using two neural networks trained on large number of images, working in competition to generate realistic new images



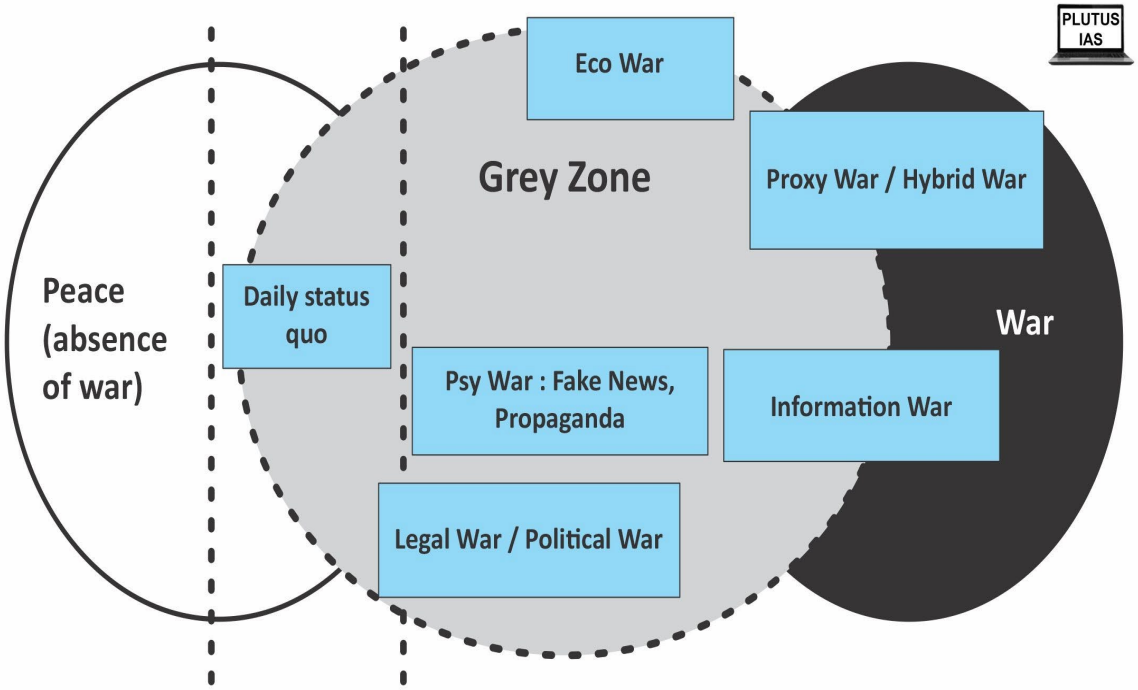
Rana et. al. (2024). Deepfakes–Reality Under Threat?, IEEE.

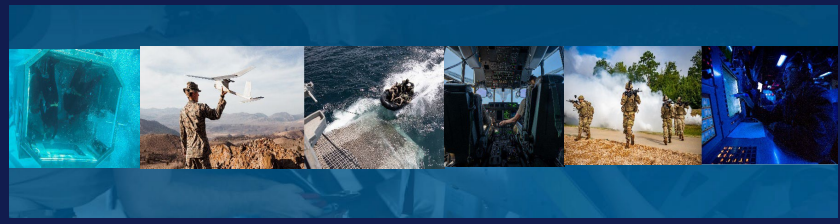
Identifying Generated Content

- Army Training and Doctrine Command provides tips for soldiers to spot fake news, disinformation, and automated bots that may be generating unreliable postings
- DARPA's SemaFor program is developing innovative semantic technologies for analyzing multi-media content to detect if media assets have been generated or manipulated.

Operations in the Information Environment (OIE):
Grey Zone Coercion

“INFORMATION IS THE GREAT EQUALIZER”

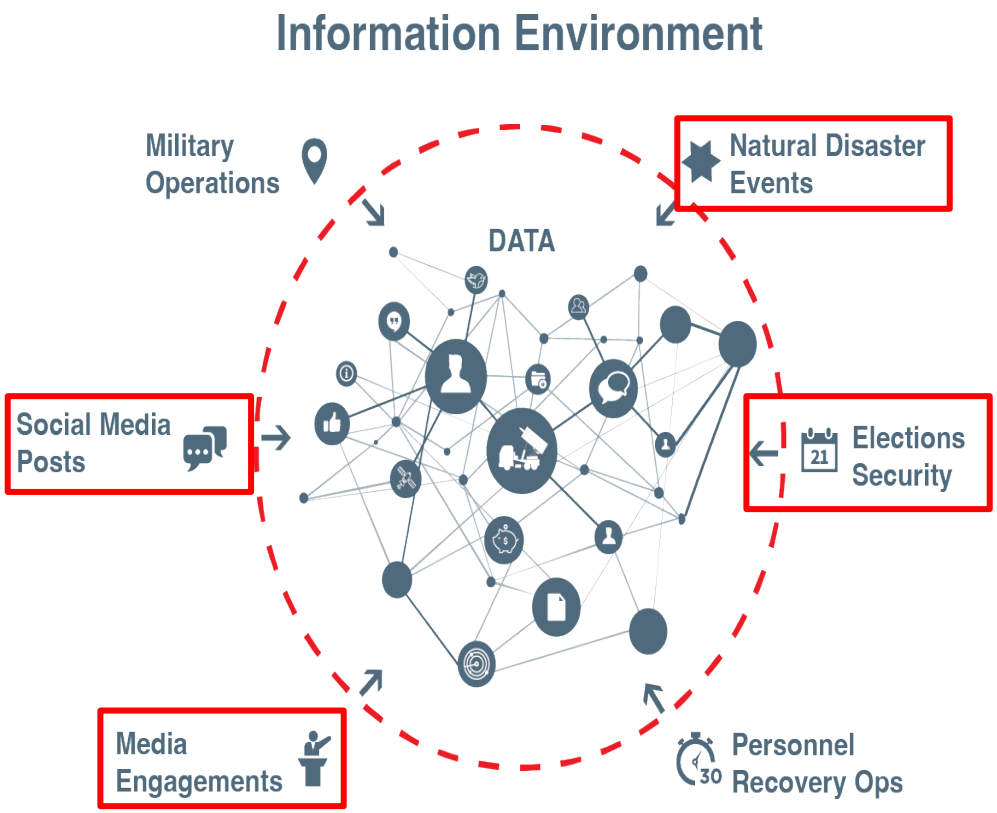




Operations in the Information Environment (OIE)

OIE envisions enduring decision advantage across Military operations by applying a *multi-disciplinary*, complex system governance-based approach that applies not only cutting-edge *social, behavioral, cognitive, and neurological science* research, but also *computational, computer information*, and *network science* research and tools, toward timely socio-cultural situation awareness, expertise, and resilience to malign influence in the information environment.

The Department's HS S&T should aim to gain a deeper understanding of cognitive, socio- cultural, and behavioral influences within the information environment, as well as their implications for Military operations, via predictive, autonomous analytics.



Framework Development

1. Identify Stakeholders

- Customer stakeholders those who want and need research in the human centered OIE domain
- Researchers and Human factors Practitioners that can address the issues and gaps identified

2. Identify key topics of interest and challenges for humans in OIE, for example:

- Cognitive vulnerabilities – confirmation bias, emotional triggers
- Social Amplification – group think, echo chambers, influence of influencers and bots
- Technology and platforms – role of algorithms in amplifying disinformation, impact of deep fakes and synthetic media
- Cultural and regional contexts – role of culture narratives in information warfare

3. Develop S&T research questions, for example:

- What psychological and cognitive biases are most exploited in information warfare?
- Does exposure to overwhelming amounts of information reduce people's ability to discern fact from fiction?
- How do social media platforms influence susceptibility to information manipulation?
- How effective are current countermeasures (e.g., media literacy campaigns, fact-checking)?
- How do emotions like fear and anger influence the likelihood of sharing false information?

4. Develop offensive and defensive capabilities

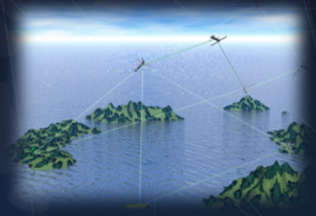
- Baseline / starting point is DoD HS strategy OIE focus area near, mid and far term.
- Prioritize – Capabilities

Key Elements of Human-Centered OIE

- Understanding Human Behavior: Analyzing how people consume, interpret, and act on information
- Influence and Persuasion: Crafting messages that align with human motivations, beliefs, and values to influence opinions or behaviors
- User-Centered Design: Developing tools, platforms, and systems that prioritize ease of use, accessibility, and relevance to the target audience's needs
- Psychological Operations (PsyOps): Leveraging information to influence adversaries or target populations
- Information Security: Protecting against misinformation, disinformation, and manipulation by focusing on human vulnerabilities in information processing
- Cultural Awareness and Sensitivity: Recognizing the cultural and social contexts that influence how different groups understand and respond to information

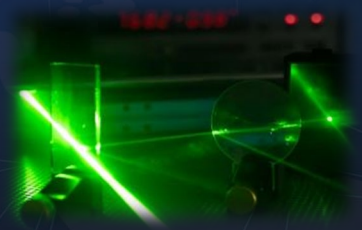
DoD Research and Engineering Enterprise

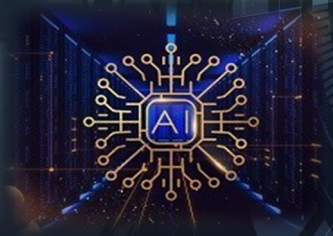
Creating the Technologies of the Future Fight







Questions?

DoD Research and Engineering Enterprise
https://www.CTO.mil/

Twitter
@DoDCTO

References

Goldsmith, K. (2019). An Investigation into Foreign Entities Who Are Targeting Servicemembers and Veterans Online. Silver Spring: Vietnam Veterans of America. https://vva.org/trollreport/.

Sherman, J., Barton, H., Klein, A., Kruse, B., & Srinivasan, A. (2023). Data brokers and the sale of data on U.S. Military Personnel. Sanford School of Public Policy, Duke University. https://techpolicy.sanford.duke.edu/data-brokers-and-the-sale-of-data-on-us-military-personnel/

Simkins, J. D. (2018). "Prisoner stole more than $500K from troops through dating app sextortion ring." Army Times, November 28, 2018. https://www.armytimes.com/news/your-army/2018/11/28/prisoners-steal-more-than-500k-from-troops-through-dating-app-sextortion-ring/

(Citation: Goldsmith, Kristofer. An Investigation into Foreign Entities Who Are Targeting Servicemembers and Veterans Online. Silver Spring: Vietnam Veterans of America, September 17, 2019. https://vva.org/trollreport/.)

https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf

https://breakingdefense.com/2024/10/armys-new-theater-information-advantage-detachments-will-be-tailored-to-their-theater-officials/

GAO-22-104714: Information Environment: Opportunities and Threats to DOD's National Security Mission – provides nice introduction to the concept of the Information Environment, and explains a few of the opportunities enabled by US leveraging the information environment for swift and effective actions along with some potential threats because DoD capabilities are somewhat dependent on IT and the use of information.

GAO-21-525T: Information Environment: DOD Operations Need Enhanced Leadership and Integration of Capabilities

References

Generating Content: Rana, M. S., et. al. (2024). Deepfakes–Reality Under Threat?. In 2024 IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0721-0727). IEEE.

DARPA's SemaFor program description at https://www.darpa.mil/research/programs/semantic-forensics

TRADOC: https://www.tradoc.army.mil/social-media-fake-news/

https://breakingdefense.com/2024/10/armys-new-theater-information-advantage-detachments-will-be-tailored-to-their-theater-officials/

https://www.cbsnews.com/news/china-spying-efforts-us-service-members-social-media/