USU Uniformed Services University | CGHE Center for Global Health Engagement

ISSUE 7
FEBRUARY 2024

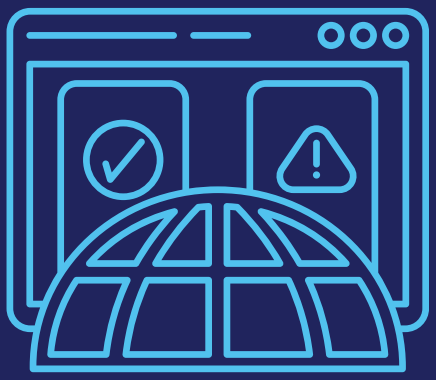
DoD GHE Snapshot

MISINFORMATION/DISINFORMATION AND ITS LINK TO CYBERSECURITY

Written by: Yara Francis[1], Jane Diehl Greulich, MPH[2]; EB Pertner, PhD[3]; Maria Echeverry[4], F. Julian Lantry, MPH[5]

The Uniformed Services University of the Health Sciences' (USU's) Center for Global Health Engagement (CGHE) is pleased to share the seventh issue of the Department of Defense Global Health Engagement (DoD GHE) Snapshot. The DoD GHE Snapshot is intended to create self-publishing opportunities for GHE professionals to share knowledge and experiences and learn from one another in real time. We hope you enjoy and please refer to our social media and website for real time updates.

MISINFORMATION/ DISINFORMATION AND ITS LINK TO CYBERSECURITY



In the field of public affairs and information operations, misinformation and disinformation (commonly referred to as "mis/dis" by the Department of Defense - DoD) bears a resemblance to the insidious concept of "death by a thousand cuts." This metaphor captures the gradual and cumulative manner in which false or deceptive information disseminates, thereby eroding trust in credible sources of information, established institutions, and societal norms. The mis/dis playbook consistently adheres to this set of tactics: incremental dissemination, trust degradation, incessant repetition and amplification, and fostering polarization. To counter mis/dis, it is imperative to champion media literacy, nurture critical thinking capabilities, and rigorously engage in proactive fact-checking endeavors. Equally vital is the imperative to lead with transparency, while asserting control over the narrative from the outset.

The mis/dis challenge has gained increasing attention within the DoD Global Health Engagement (GHE) enterprise as of late, particularly in the wake of the COVID-19 pandemic and the ensuing “infodemic,” defined by the World Health Organization as false or misleading information which increases confusion, risk-taking behaviors, and mistrust of health authorities during a disease outbreak and which can, in turn, adversely affect health outcomes. [1]

To grasp mis/dis in the DoD GHE context, it is first essential to separate it from cybersecurity, as these concepts can sometimes blend together. Let us start by clearly defining the three concepts:

MISINFORMATION

refers to false or inaccurate information that is spread without the intention to deceive. Misinformation may be shared innocently and often spreads quickly through social media and other online platforms

DISINFORMATION

on the other hand, is deliberately false or misleading information that is spread with the intent to deceive, manipulate, or create confusion. Disinformation is usually created and disseminated with a specific agenda, such as influencing public opinion, undermining trust, or advancing a political, social, or economic goal.

CYBER SECURITY

is the practice of protecting computer systems, networks, and digital information from unauthorized access, attacks, damage, or theft. It involves a range of measures and technologies designed to safeguard digital assets, ensure data confidentiality and integrity, and prevent cybercrimes. Cybersecurity encompasses various aspects, including network security, data protection, encryption, authentication, and more.

Mis/dis shares a battlefield with cybersecurity threats, but they are not mutually exclusive: the former can be deployed in non-digital contexts, while the latter does not rely on mis/dis as its sole tactic. Practitioners often use mis/dis and cybersecurity interchangeably, primarily due to the inherent interconnectedness of these concepts within the digital landscape. Several factors contribute to the propensity for these concepts to be muddled or intertwined:

- **Digital Nature:** Both mis/dis and cybersecurity involve information, communication, and technology.
- **Online Spread:** Mis/dis often spreads rapidly through online platforms and social media, the same channels that are vulnerable to cybersecurity threats.
- **Impact:** Mis/dis can impact public perception, erode trust, and manipulate opinions, much like cyber attacks that can compromise systems, data, and information integrity.
- **Shared Countermeasures:** Strategies to counter mis/dis can involve elements of cybersecurity, such as monitoring online activities, analyzing patterns, and identifying potential threats.
- **Hybrid Threats:** Modern threats often blur the lines between information warfare and cyber operations. State and non-state actors might use disinformation campaigns in conjunction with cyber attacks to achieve their objectives.

- **Media Coverage:** In media and public discourse, these terms might be used interchangeably or in proximity, contributing to confusion.
- **Government and Organizational Responses:** Governments and organizations might address both mis/dis and cybersecurity within broader strategies for national security and digital defense. For example, the U.S. Cybersecurity and Infrastructure Security Agency holds both portfolios.
- **Lack of Clarity:** The concepts of mis/dis can be complex, and nuances might not always be well-understood.

Exploring and clarifying the differences between mis/dis and cybersecurity terms helps readers better grasp and navigate these distinct but overlapping areas. As DoD GHE practitioners continue to tackle targeted misinformation and disinformation challenges, they will come across situations where recognizing cybersecurity and its unique features within the mis/dis landscape is crucial. This understanding will enable them to create tailored solutions to address specific cybersecurity threats and mis/dis campaigns effectively, and expand their toolset to counter malign influence in the health space.

[1] Yara Francis, MA, CIV, Special Assistant for Policy and Strategy
USU's CGHE

[2] Jane Diehl Greulich, MPH, Senior Program Manager
Henry M. Jackson Foundation for the Advancement of Military Medicine (HJF), Inc., in collaboration with USU's CGHE

[3] EB Pertner, PhD, Senior Policy Advisor
Henry M. Jackson Foundation for the Advancement of Military Medicine (HJF), Inc., in collaboration with USU's CGHE

[4] Maria Echeverry, Communications Specialist
Henry M. Jackson Foundation for the Advancement of Military Medicine (HJF), Inc., in collaboration with USU's CGHE

[5] F. Julian Lantry, MPH, Research Project Manager
Henry M. Jackson Foundation for the Advancement of Military Medicine (HJF), Inc., in collaboration with USU's CGHE

CGHE
Uniformed Services University

REFERENCES

1. https://s3.documentcloud.org/documents/23972716/2023_dod_cyber_strategy_summary.pdf

For questions or additional information, please contact us at cghe@usuhs.edu or visit our website at cghe.usuhs.edu