UNDERSTANDING DISINFORMATION CAMPAIGNS

Dr. Kathleen M. Carley and LTC David M. Beskow

DESCRIPTION:

Disinformation has increasingly become a serious national security risk, with both authoritarian and democratic nation-states racing to understand information consumption in modern cyber systems and protect their populations from external manipulation. This race to understand and protect societies from these threats has led to the emerging field of social cyber security. This tutorial seeks to shed light on current research on disinformation within the context of social cyber security.

This tutorial will begin by describing "forms of maneuver" in emerging disinformation campaigns. This will highlight how malicious actors manipulate both narratives and networks in order to achieve political ends. Additionally, this section will discuss how to identify some of these forms of maneuver using network science, and how to read the cognitive cues inherent in these campaigns.

The second half of the tutorial will highlight current efforts to detect certain factors that inhabit disinformation campaigns, namely bots and memes. Bots are force multipliers that enable actors to manipulate networks and narratives at scale. Internet memes are creative artifacts of the digital age that use humor and satire to connect a message to a target audience, often reinforcing existing biases. In this part of the tutorial we will discuss *bot-hunter* and *meme-hunter*, two machine learning applications that we use to detect these factors at scale, enabling us to study and characterize them.

EXPECTED AUDIENCE:

The audience should have a background or interest in social cyber security and more generally in computational social science.

SHORT BIO OF ORGANIZERS:

Lt. Col. David Beskow, U.S. Army, is a PhD candidate in the School of Computer Science at Carnegie Mellon University. He holds a BS from the United States Military Academy in civil engineering and an MS from the Naval Postgraduate School in operations research. During his career, Beskow served as an infantry leader and as an operations research and systems analyst (ORSA) in multiple Army organizations. Beskow's current research develops machine learning algorithms to detect and characterize disinformation campaigns.

Prof. Kathleen M. Carley, PhD, HD, is a professor of societal computing in the School of Computer Science at Carnegie Mellon University, an IEEE Fellow, the director of the Center for Computational Analysis of Social and Organizational Systems (CASOS), and the CEO of Netanomics. She founded the areas of dynamic network analysis and social cyber-security. She is the 2011 winner of the Simmel Award from the International Network for Social Network Analysis and the 2018 winner of the USGA Academic Award from GEOINT.