

SET-262 Specialist Meeting on **Artificial Intelligence for Military Multisensor Fusion Engines**

Title:

SCOPE: Sensemaking in Cyber Social Spaces

Authors:

Geeth de Mel
IBM Research
Hartree Center
Keckwick Lane
Warrington WA4 4AD
United Kingdom
geeth.demel@uk.ibm.com

Soheil Eshghi
Yale Institute for Network Science
(YINS)
Yale University
17 Hillhouse Ave,
New Haven CT 06520
United States of America
soheil.eshghi@yale.edu

Gavin Pearson
Defence Science and Technology
Laboratory
Porton Down
Salisbury
Wiltshire SP4 0JQ
United Kingdom
agpearson@mail.dstl.gov.uk

Sukankana Chakraborty
Valerio Restocchi
Sebastian Stein
Electronics and Computer Science
University of Southampton
University Road
Southampton SO17 1BJ
United Kingdom
{sc8n15, vr2n17, ss2}@ecs.soton.ac.uk

Tien Pham
U.S. Army Research Laboratory
Attn: RDRL-CI
2800 Powder Mill Road
Adelphi, MD 20783
United States of America
tien.pham1.civ@mail.mil

Abstract:

Due to the explosion in social media platforms, cyber social information is fast becoming a critical element in multisensory fusion to better understand dynamic and evolving situations. This is especially true in situations where potentially hostile actors—be they politically- or economically- motivated—operate in a way that changes the established social norms and outcomes by targeting detailed profiles of individuals or social groups within such platforms. Therefore, understanding the dynamics of social groups, especially under the influence of external factors, is critical to identify vulnerabilities and to seek remedies.

In order to understand such social structures, in this work, we seek to develop a framework to learn, fit, and predict social group-based behaviour from prior interaction data, observed behaviour, and individual characteristics. We seek to first map observational data at an individual and interaction level to ground-truth self-described group membership, and then to use the models fitted to real-world data to provide descriptions of the groups under varying external factors; furthermore, we aim to identify the individuals—or groups—in the network who are susceptible to external influence, which, by virtue of their position, can spread this influence further in the network. The intuition here is that identifying these key entities will enable us to observe the features of individuals and groups that can be targeted to modify the norms of the network. Additionally, it is envisioned that the important features that are revealed about the current network might provide clues that could be used in similar networks, and the information collected in this way could further give us hints about possible incentives we could use to influence these individuals or groups.

To realise this vision, we are investigating and applying a novel combination of artificial intelligence techniques from deep learning, optimisation, and game theory. For example, we are investigating unsupervised techniques to extract network information that will enable us to infer emerging topics and contexts over evolving networks. Additionally, we apply reinforcement learning mechanisms to improve the generated models and consider attention-based models to distil critical pieces of information from large amounts of data to characterize key individuals and groups.