Abstract for an Invited Paper
for the MAR10 Meeting of
The American Physical Society

Network Science for Deterrence: Sheathing the Sword of the Terrorism/Nuclear Horseman[1]

KATHLEEN CARLEY[2], Carnegie Mellon University

After 9/11, network analysis became popular as a way to connect and disconnect the dots. It was heralded as the new science with intrinsic value for understanding and breaking up terrorist groups, insurgencies and hostile foreign governments. The limit of the initially forwarded approach was that it focused on only the social network – who talked to whom. However ,the networks of war, terror or nuclear or cyber, are complex networks composed of people, organizations, resources, and capabilities connected in a geo-temporal web that constrains and enables activities that are "hidden" in the web of everyday life. Identifying these networks requires extraction and fusion of information from cyber-mediated realms resulting in a network map of the hostile groups and their relations to the populations in which they are embedded. These data are at best a sample, albeit a very large sample, replete with missing and incomplete data. Geo-temporal considerations in addition to information loss and error called into question the value of traditional network approaches. In this talk, a new approaches and associated technologies that integrate scientific advances in machine learning, network statistics, and the social and organizational science with traditional graph theoretic approaches to social networks are presented. Then, examples, of how these technologies can be used as part of a deterrence strategy are described. Examples related to terrorism and groups such as al-Qaida and Hamas, cyber and nuclear deterrence are described. By taking this meta-network approach, embracing the complexity and simultaneously examining not just one network, but the connections among networks, it is possible to identify emergent leaders, locate changes in activities, and forecast the potential impact of various interventions. Key challenges, such as data-streaming and deception, that need to be addressed scientifically are referenced.

[1]This work was supported by the ONR, ARI, and AFOSR.
[2]Professor