2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining

Networks and Network Analysis for Defence and Security

Anthony Masys
University of Leicester
Leicester, UK
Anthony.masys@gmail.com
Anthony.masys@drdc-rddc.gc.ca

Abstract— Shocks to regional, national and global systems stemming from natural hazards, acts of armed violence, terrorism and serious and organized crime have significant defence and security implications. Today, nations face an uncertain and complex security landscape in which threats impact/target the physical, social, economic and cyber domains. For example, acts of terrorism and organized crime are considered one of the greatest threats to national security. In the UK alone, the social and economic costs associated with organized crime are estimated between £20 and £40 billion per year (NCA, 2011:4).

Threats to national security, such as that against critical infrastructures not only stem from man-made acts but also from natural hazards. Katrina (2005), Fukushima (2011) and Hurricane Sandy (2012) are examples that highlight the vulnerability of critical infrastructures to natural hazards and the crippling effect they have on the social and economic well-being of a community and a nation.

With this dynamic and complex threat landscape, network analysis has emerged as a key enabler in supporting defence and security. With the advent of 'big data' and increasing processing power, network analysis can reveal insights with regards to structural and dynamic properties thereby facilitating greater understanding of complex networks, their entities, interdependencies and vulnerabilities.

This poster paper introduces relevant theoretical frameworks and applications of network analysis in support of the defence and security domain. This paper reflects the body of contributions by leading researchers to an upcoming book entitled: Networks and Network Analysis for Defence and Security, Springer Publishing.

Keywords—defence, security, network analysis

I. Introduction

Highly interconnected and interdependent systems characterize the security landscape. Threats to critical infrastructure (physical, social or cyber), epidemic outbreaks, the global footprint of terrorism highlight the requirement for greater understanding regarding highly connected systems. Network thinking or more clearly a 'network mindset' (Vespignani, 2009) is essential for understanding the network structure, network behavior and the feedback/feedforward effects resident within these systems. What emerges from the study of networks is the insightful requirement to evaluate actions and behaviours not in isolation but recognizing that cause and effect are complex and nonlinear.

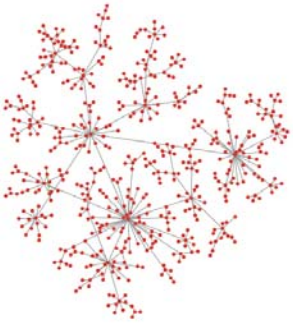

Figure 1: Epidemic Spreading

II. Discussion

Steve Strang (Royal Canadian Mounted Police) presents a set of approaches to network analysis used in criminal intelligence to understand and act against serious crimes, criminal groups, and criminal markets. These approaches are based on link analysis and increasingly include techniques from social network analysis (SNA). He describes how SNA measures have utility in producing targeting recommendations for intelligence collection and operational disruption.

Kay Hamacher (Technical University Darmstadt) introduces a framework for the information theoretic based construction of networks of events that occur in security and defense and the later analysis thereof. This framework augments previous approaches to identify causal relations among events in empirical data. In particular, activities during an insurgence fall in a range between the purely random occurrence of events—e.g., IED explosions—and the organized and coordinated plans of insurgents.

Remi Boivin (Université de Montréal) describes how traditionnally, most analyses of criminal organzations have

ASONAM'13, August 25-29, 2013, Niagara, Ontario, CAN

been based on networks of relations between individuals or small groups of individuals. Boivin presents macro-social network analysis as a methodology to understand the impact of law enforcement efforts on criminal activities.

David Decary-Hétu & Benoit Dupont (**Université de Montréal)** present a study on cybercrime to show the inherent limits to the current tools and demonstrate that gathering data on hackers with IRC can have many advantages including access to unbiased sources of information and increased efficiency.

Christian Leuprecht (**Royal Military College of Canada**) describes how theories on international terrorist networks are wrought with contradiction. On the one hand, networks that support or facilitate politically motivated violent extremism are thought to pose a threat because they are centralized and hierarchical. On the other hand, the same networks are thought to pose a threat because they are decentralized and operate autonomously. Social networks analysis (SNA) makes it possible to resolve this apparent contradiction by controlling across countries for the characteristics and structure of networks linked to the same terrorist organization relative to different functions that such networks need to perform.

P.A.C. Duijn and P. Klerks (**Strategic Intelligence Analyst at the Dutch Police Unit The Hague)** offer insight in the recent developments of the application of network analysis in controlling Organized Crime within the Netherlands. Further they offer insight in the practical application of network analysis within targeting criminal networks and gathering intelligence about criminal cooperation.

Manjana Milkoreit and Steven Mock (**Balsillie School of International Affairs)** demonstrate the applicability of cognitive-affective mapping as a means to model the relationship between groups and individuals through the example of national identity, and then show its utility in situations of real-world conflict. Through their case studies they demonstrate the value-added of a cognitive approach to the study of defence and security based on a network view of the human mind.

Francesco Calderoni (**Università Cattolica del Sacro Cuore and Transcrime, Milan, Italy)** shows how the application of simple network analysis methods to surveillance data can identify the main players in a large mafia network. His results show that the most central subjects also had leading positions within the mafia families. This suggests that the use of network analysis applied to meetings may provide useful information for law enforcement agencies to identify high-status criminals.

Gisela Bichler and Juan Franquez (**California State University, San Bernardino)** describe a study to uncover the underlying network funneling small arms to actors that use them as fodder for conflict. They employ a multivariate, actor-based network analysis to estimate the change in trade relations over time.

Simon Bennett (**University of Leicester**) explores why public servants responsible for the safety and security of the general public can sometimes elevate their own interests above those of the public. The study shows how system theory, specifically organisation theory, actor-network theory and theories of isomorphic learning can be used to understand how such deviant behaviour is organised and why it is so difficult to identify and correct.

Phil O Neill (**President Quantitative Decision Support Inc**) presents a novel technique, known as the "***strongest path method***", for performing risk analysis of multiple systems of systems that are highly interconnected. Users, managers and regulators of such systems who want to understand the impact and vulnerability of its component parts require a risk analysis method that deals explicitly with chains of dependency relationships. The strongest path method provides such capability.

Anthony Masys (**University of Leicester**) describes that threats to national security, such as that against critical infrastructures not only stem from man-made acts but also from natural hazards. Katrina (2005), Blackout Canada-US (2003), Fukushima (2011) and Hurricane Sandy (2012) are examples that highlight the vulnerability of critical infrastructures to natural hazards and the crippling effect that failures can have on the social and economic well-being of a community and a nation. Through the complexity/systems lens of actor network theory, he explores how key 'actors' within a network can align other actors creating 'unseen' vulnerabilities

III. CONCLUSION

This poster paper provides an overview of the contributions from numerous authors for the upcoming publication 'Networks and Network Analysis for Defence and Security'. With such a complex threat landscape, various approaches regarding network analysis described by the authors sheds light on the interdependencies and interconnectivity thereby enriching our understanding of the underlying network structure and behavior to support solution design and decision making.

IV. REFERENCES

(NCA) National Crime Agency : a plan for the creation of a national crime-fighting capability (2011). Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty.

Vespignani, A. (2009) Predicting the Behavior of Techno-Social Systems. Science, Vol. 325, 24 July 2009: 425-428.