

# Preface

## Introduction

Shocks to regional, national, and global systems stemming from natural hazards, acts of armed violence, terrorism, and transnational 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 [1]. 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, and innovative interpretive approaches, network analysis can reveal insights with regard to structural and dynamic properties thereby facilitating greater understanding of complex networks, their entities, interdependencies, and vulnerabilities.

## Network “Mindset”

Network thinking, as described in Barabasi [2] opens up novel perspectives to understanding complex systems such as markets and economic system, socio-technical systems, and criminal and terrorist networks. The foremost challenge offered by complex networks resides in their interconnectedness (networks of networks) and multiscale nature [3]. The network thinking mindset leverages a topological analysis which is based upon classical graph theory through which interesting properties of structure and dynamics of a network system can be

revealed. The inherent complexity of the defence and security domain characterized by interdependencies, interconnectivity, dynamic, nonlinear behavior therefore calls for this “network” mindset.

The “network” mindset is very much about having a systems approach with regard to defence and security. Link analysis for example can be used to map associations among people, places, and commodities, after a crime or terrorist attack has occurred in order to identify the perpetrators. Further, tools associated with social network analysis (SNA) can enrich the interpretive power of network analysis. Insights derived from analysis of dark networks or critical infrastructures can position law enforcement and disaster management professionals with the requisite information for informed decision making.

As part of the Springer book series: *Lecture Notes in Social Networks*, this edited volume: **Networks and Network Analysis for Defence and Security**, focuses on the contribution of network science to the following areas:

- Defence and security risk analysis
- Criminal intelligence
- Cybercrime
- Cognitive analysis
- Counter-terrorism and Social Network Analysis
- Transnational Crime
- Critical infrastructure analysis
- Support to defence and security intelligence

This book comprises 12 chapters from leading researchers engaged in network analysis within the defence, security, and intelligence domains. The chapters present state-of-the-art research on network analysis tools, techniques, and applications supported by case studies and computational simulation.

## Content

The chapter “[Network Analysis in Criminal Intelligence](#)” by Steven Strang provides an overview of network analysis beginning with the application of link analysis and social network analysis (SNA) techniques that support criminal intelligence in order to understand and act against serious crimes, criminal groups, and criminal markets. Strang highlights how the effective visualization of both quantitative and qualitative data support intelligence assessments. It is through the application of network analysis in criminal intelligence that the nature and extent of relationships between data points (individuals, locations, organizations, objects, and events) emerge. Strang further illustrates how SNA measures have utility in producing targeting recommendations for intelligence collection and operational disruption.

Overall, this chapter will provide the readers with an understanding of:

- Network concepts in the analysis of serious crime, organized crime, and terrorism.
- Applications of network analysis methods and technique in criminal intelligence analysis.
- Operational uses of network analyses to support the investigation of crimes and the disruption of criminal groups.
- Strengths and limitations of network analysis in criminal intelligence.

The chapter “[Identifying Mafia Bosses from Meeting Attendance](#)” by Francesco Calderoni describes how the application of simple network analysis methods to surveillance data can identify the main players in a large mafia network. The analysis relies on data from a large investigation on the presence of the ‘Ndrangheta (a mafia from the Southern Italian region of Calabria) around Milan, Italy’s second largest city and economic capital. Operation Infinito, lasted for more than 2 years, identified several ‘Ndrangheta families and tracked the main mafia meetings. Network analysis of an individuals’ participation in mafia meetings enabled identification of the different roles and positions within the mafia network. 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.

The chapter “[Macrosocial Network Analysis: The Case of Transnational Drug Trafficking](#)” by Rémi Boivin aims to put criminal activity in the larger context in which it takes place. More precisely, it is argued that country-level features may complicate or facilitate legitimate business as well as criminal activities. Transnational crime is a collaboration to avoid law enforcement; it is expected that, as far as possible, countries with higher risks of seizure and arrest will be avoided in favor of more lenient countries. Macrosocial network analysis may then be used to understand the impact of law enforcement efforts on criminal activities. It is also argued that some criminal activities must be understood in a relational perspective. Drug trafficking is presented as a case study to illustrate the contributions of macrosocial network analysis. The general conclusion of the chapter is that, despite the fact that macrosocial features are largely neglected in most analyses, network analysis is a relevant tool in understanding global criminal markets. Transnational crime is supported by a set of relations between individuals and groups operating in larger networks of countries.

The chapter “[Policing the Hackers by hacking Them: Studying Online Deviants in IRC Chat Rooms](#)” by David Décary-Héту, Benoit Dupont and Francis Fortin develops a framework that allows criminologists to easily tap into this pristine source of data on cybercriminals. Past research has shown that the Internet Relay Chat (IRC), a worldwide instant messaging system, has been and is still one of the favorite meeting grounds for cybercriminals. Unfortunately, criminologists have yet to fully take advantage of this network of chat rooms where millions of

individuals interact every day. This chapter begins with a review of how criminologists have addressed the question of cybercrime to date. The authors present the inherent limits to the current tools that are used and demonstrate that gathering data on hackers with IRC has many advantages including access to unbiased sources of information and increased efficiency. This chapter then showcases the versatility of IRC logs in criminological research and details both the solutions and the new challenges that such a methodology brings forward. This framework will enable law-enforcement agencies to go beyond traditional social platforms and to track delinquents in underground chat rooms where they hide in security through obscurity. If law-enforcement agencies are to gather the best intelligence, they will therefore need to monitor IRC networks just as some of them have been doing with social networks like Facebook and Twitter.

The chapter “[Why Terror Networks are Dissimilar: How Structure Relates to Function](#)” by Christian Leuprecht compares Al Shabab (AS) networks as they relate to recruitment, fundraising, and attacks across the United States and Australia with corroborating evidence from Canada, the United Kingdom, The Netherlands, and Denmark. Although networks differ markedly across these attributes, unrelated networks performing similar functions are consistent in their nature and structure. These findings suggest that networks are functionally differentiated insofar as they serve as strategic repertoires. This is a significant finding. Knowing how a network’s function is related strategically to its structure means being able to infer a network’s function if only its structure is known and, conversely, being able to infer a network’s structure if only its function is known. Not only does SNA thereby facilitate detection and dismantling of networks, it also suggests that recruitment, fundraising, and attack networks require differentiated approaches by defence and security agencies insofar as SNA shows them to be distinct phenomena.

The chapter “[Social Network Analysis Applied to Criminal Networks: Recent Developments in Dutch Law Enforcement](#)” by P. A. C. Duijn and P. P. H. M. Klerks ask the questions: What can we learn from developments within The Netherlands concerning the application of Network Analysis in controlling Organized Crime? What are the practical implications of applying network analysis within targeting criminal networks and strategic intelligence gathering? What does dynamical network analysis research tell us about the effectiveness of criminal network disruption? How does the network paradigm connect with law enforcement decision making? Addressing these questions the authors’ objective is:

1. To offer insight into the recent developments of the application of network analysis in controlling Organized Crime within The Netherlands.
2. To offer insight into the practical application of network analysis within targeting criminal networks and gathering intelligence about criminal cooperation.

In the chapter “[The Networked Mind: Collective Identities and the Cognitive-Affective Nature of Conflict](#),” Manjana Milkoreit and Steven Mock apply a network-based analysis to an area that suffers from even greater empirical challenges than social network analysis: the human mind. Working with the assumption that all human behavior has cognitive origins, this chapter has three aims. First, the authors make the case for the relevance of a cognitive approach to defence and security studies, exploring areas of application and potential insights. Second, they use a theory of the mind—emotional coherence—and a complex systems approach to explore the role of specific cognitive elements—collective identities—for the emergence and resolution of inter-group conflict. Third, the authors introduce cognitive-affective mapping as a tool to apply a theoretical framework to specific empirical cases and walk the reader through two specific case analysis: the Israeli-Palestinian dispute over the Western Wall as a long-term low-violence conflict and—maybe surprisingly—the international climate negotiations as an example of non-violent political conflict at the global level.

The chapter “[Conflict Cessation and the Emergence of Weapons Supermarkets](#)” by Gisela Bichler and Juan Franquez present the results of a study to uncover the underlying network funneling small arms to actors that use them as fodder for conflict. This study uses a dynamic actor-based simulation modeling software, called SIENA to capture changes in the gray market of gun trade following the termination of armed conflict. The simulation models permit the detection of evolutionary change in networks. The key advantage to using SIENA is that it permits the inclusion of structural variables (e.g., changes in reciprocity, transitivity, and degree centrality metrics) as independent variables, in addition to dynamic covariates (changing values over time), static covariates, and other dynamic and static networks (dyadic variables). This flexibility has been shown to be useful in examining international gun trade [4].

In the chapter “[A Conspiracy of Bastards?](#)”, Simon Bennett presents a unique perspective on security. With reference to two case studies—the 1983 “Holloway Road incident” and the 1989 Hillsborough cover-up—he seeks first, to understand why public servants responsible for civil safety and security can sometimes elevate their own interests above those of the public. Secondly, to show how system theory, specifically organization theory [5, 6], actor-network theory [7, 8], and theories of isomorphic learning [9] can be used to understand how such deviant behavior is organized and why it is so difficult to identify and correct.

The chapter “[Decision Support Through Strongest Path Method Risk Analysis](#)” by Philip O’Neill presents a technique, known as the *strongest path method*, for performing risk analysis of multiple systems of systems that are highly interconnected. The *connectedness* entails complex dependency relationships throughout the system of systems and these propagate risk. 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. Not only are the strongest path or paths taken into consideration when estimating the potential impact of one entity on another but the compound effects of all pathways are included. The results of the path analysis can be used to prioritize risk and to prepare risk mitigation plans and contingency plans. The chapter focuses on developing the risk analysis technique and showing its value to decision makers. Some areas where the method is useful will be put forward with particular emphasis on infrastructure risk analysis.

The chapter “[Critical Infrastructure and Vulnerability: A Relational Analysis Through Actor Network Theory](#)” by Anthony J. Masys describes how 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), Hurricane Sandy (2012), and Alberta Floods (2013) 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. Focusing on the initiating event that precipitated the critical infrastructure failure does not capture the root vulnerabilities or “resident pathogens” that are “hard-wired” into the greater networked system. Through the complexity/systems lens of actor network theory, this chapter explores critical infrastructure and how key “actors” within a network can align other actors creating “unseen” vulnerabilities.

The final concluding chapter brings together common themes from across the chapters to highlight the complexity space that characterizes the defence and security domain and applies the “network thinking” paradigm to the comprehensive approach.

Collectively, the chapters present the reader with a broad spectrum yet detailed analysis of the defence and security domain, thereby highlighting the requirement for a “network mindset.” It advances our understanding and state of the art regarding network analysis and lays the foundation for continued exploitation and development of network analysis tools and techniques to support the defence and security domains.

## References

1. 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 (<https://www.gov.uk/government/publications/national-crime-agency-a-plan-for-the-creation-of-a-national-crimefighting-capability>)
2. Barabasi A-L (2003) *Linked*. Plume, New York Penguin Group
3. Vespignani A (2009) Predicting the behavior of techno-social systems. *Science*, 325:425–428
4. Bichler G, Malm A (2013) Small arms, big guns: a dynamic model of illicit market opportunity. *Global Crime* 14(2–3):261–286
5. Tsoukas H, Knudsen C (2005) *The oxford handbook of organization theory*. Oxford University Press, Oxford

6. Ravasi D, Schultz M (2006) Responding to organizational identity threats: exploring the role of organizational culture, *Acad Manage J*, 49(3): 433–458.
7. Latour B (1991) Technology is society made durable. In *A sociology of monsters: essays on power, technology and domination*, J. Law (ed.) Routledge, London, pp 103–131
8. Woolgar S (1991) Configuring the user: the case of usability trials. In: Law J (ed) *A sociology of monsters: essays on power, technology and domination*, Routledge, London, pp 57–99
9. Toft B, Reynolds S (1997) *Learning from disasters*, Perpetuity Press, Leicester
10. Callon M, Law J (1995) Agency and the hybrid collectif. *South Atlantic Q*, 94(2):481–507
11. Perrow C (1984) *Normal accidents: living with high-risk technologies*, Basic Books

Networks and Network Analysis for Defence and  
Security

Masys, A.J. (Ed.)

2014, XVIII, 287 p. 55 illus., 39 illus. in color., Hardcover

ISBN: 978-3-319-04146-9