UIC UNIVERSITY OF ILLINOIS AT CHICAGO

SMU SINGAPORE MANAGEMENT UNIVERSITY

January 14, 2016

EXTENDED ABSTRACT FOR THE SPECIAL ISSUE OF
SOCIAL NETWORKS ON CRIME AND SECURITY NETWORKS

Covert Network Forensics Using Graphical Database Analysis: An Application to the November 13 Paris Attacks

Covert network forensics studies the problem of reconstructing the relationships in a covert network, much like a detective trying to piece together the details of a crime while sifting through a multitude of clues. Since data about a covert network is usually obtained after the network has already carried out its mission, there is a great deal of uncertainty as to which ties and nodes to include.

Many existing studies of covert networks reconstruct the networks by using any relevant data that is available and manually coding the relationships. This is understandable given the difficulty of collecting covert network data; but the results, including any policy guidance, become highly sensitive to the often unstated assumptions of the coders. The consequence is that such networks may contain a large number of false positive and false negative ties, which biases the analysis. While most analysts acknowledge this challenge, there has been little attempt to try to deal with it in a principled way.

In this paper we develop an efficient framework for organizing and analyzing data about covert networks while addressing the inherent uncertainty involved. Our framework, graphical database analysis (GDA), first stores uncoded information as relationships between people, places, and activities. The researcher then formulates any assumptions in a logical query language, and runs it on the database in order to infer the covert network. Such a query may express spatial, temporal and other criteria for membership or network ties.

GDA offers a number of advantages for covert network forensics compared to traditional approaches. Because inference in GDA is automatic, any assumptions of the analyst are explicit and the findings amenable to cross-comparison. Its high-resolution initial representation enables a sensitivity analysis to evaluate the assumptions, ensuring that any conclusions about the covert network are not dependent on how the ties were inferred.

We apply the GDA framework to reconstruct the covert network used to carry out the November 13, 2015 attacks in Paris. Our reconstruction uses public media sources and is the first published study of this network. We also compare, using a variety of metrics, this network to the networks

of al-Qaeda and al-Qaeda affiliated groups, including the networks responsible for the 9/11 attacks in the United States as well as the Madrid train bombings in Spain. We identify differences in the organization of the November 13 Network, which appears to show a relatively low secrecy value (indicating low resilience to disruption by security authorities), and this finding is insensitive to the tie inference assumptions.

The GDA methodology thus enables the study of recent terrorist events while efficiently managing the uncertainty involved, which is exacerbated when reconstructing covert networks. While conducting sensitivity analysis involves using novel software methods (the graphical database), the absence of such analysis may overstate the confidence of one's results. Furthermore, we also believe that GDA is of general interest since non-uniform, uncertain, and after-the-fact data collection are issues that confront many researchers of social networks.

Alexander Gutfraind
University of Illinois at Chicago

Michael Genkin
Singapore Management University