Chaos, Solitons and Fractals 108 (2018) 111–118

Contents lists available at ScienceDirect

Chaos, Solitons and Fractals

Nonlinear Science, and Nonequilibrium and Complex Phenomena

journal homepage: www.elsevier.com/locate/chaos

Destabilization of terrorist networks

H.A. Eiselt

Faculty of Business Administration, University of New Brunswick, P.O. Box 4400, Fredericton NB E3B 5A3, Canada

ARTICLE INFO

Article history:
Received 27 July 2017
Revised 7 November 2017
Accepted 11 January 2018

Keywords:
Counterterrorism
Social network analysis
Traffic analysis
Terrorist networks
Destabilization

ABSTRACT

This paper uses a three-phase process to first describe the development of a network to describe different types of relations between terrorists and their supporters. It continues to review some of the usual measures of social network analysis to evaluate different positions in the network. Finally, the work describes different methods to destabilize the terrorist network, and, based on sensitivity analyses, determines the potential of certain actions and the vulnerability of the network.

1. Introduction

According to PollingReport.com [51] regarding the major problems facing the nation today, National security and terrorism typically rank in the top 3 (behind economic issues) ranging between 7% in April 2016 to 16% in March 2017. The State Department of the United States lists a total of 61 organization as foreign terrorist organizations, among which 48 are Islamist or Palestine-based, with the remaining 13% being mostly communist organizations (operating in or out of Columbia, Peru, Turkey), nationalist groups (in Greece, the Basque country, Ireland), or a cult (Japan).

Modern terrorism traces its roots back to the Jacobins in the French Revolution, starting in 1789. Among the masterminds behind the "reign of terror" was Robespierre, who himself was executed in 1794—the revolution devours its children, as Jacques Mallet du Pan would call it. Rapoport [52] classifies four waves of modern terrorism: the (Russian) anarchists in the 1880s, the anti-colonialists (1920–1960), the "new left" in the late 1960s to the 1990s (among them the Spanish *ETA*, the Italian "Red Brigades," the German *RAF*, the Irish *IRA*, Quebec's *FLQ*, and Peru's *Sendoro luminoso*, the "Shining Path"), and finally religious terrorism from 1990 onwards.

There are multitudes of documentaries that describe the radicalization of individuals; see, e.g., Abril and Spottorno [2]. The internet has done its share in that respect, as it is now possible to read blogs, vlogs, and specialized information about every imaginable lifestyle and topic without having to deal with differently minded individuals (other than some trolls) and bounce ideas off other people. As Gibbs et al. [23] put it in the case of the Unabomber, "…an individual … developing his own philosophies *that he chose not to test against anyone else*, because he chose to separate himself from society." [italics in the quote are mine]. While one would expect this in the *deep web* (the part of the internet, which is not available through a simple search with one of the usual search engines) or even the *dark web* (the part of the deep web that deals with secretive and sinister issues), such as course of action is now available to everybody. As a matter of fact, by choosing the appropriate sources, one could spend his life without ever reading a news item online that is not presented with the individual's own biases.

Concerning the occurrences of acts of terrorism, following the South Asia Terrorism Portal [56], fatalities have declined from a high in 2001 of 4500 victims to annually about 200 victims in the last five years. However, as Rivinius [53] reports, more than half of all terrorist attacks occurred in three counties: Iraq, Afghanistan, and Pakistan. Combined with Nigeria and Syria, 72% of all terrorism-related deaths are attributed to these five countries [24]. Combatting acts of terrorism cannot bypass an investigation of the costs and benefits of terrorism and counterterrorism for the two sides. As Lomborg [43] reports, the costs of these attacks to the countries affected by them has been staggering. Between 2001 and 2008, terrorism-related costs to all countries combined were $70 billion. Stiglitz [58] quotes a much higher figure of $3-$5 trillion. On the other hand, the costs to terrorists to mount an attack are surprisingly modest: Lederer [42] reports that staging the 2002 Bali bombings cost less than $50,000, the 2004 Madrid bombings that resulted in 191 dead cost about $10,000, while Lomborg [43] indicates that one attack cost no more than $150. The lesson to law enforcement agencies is that the old police adage

E-mail address: haeiselt@unb.ca

https://doi.org/10.1016/j.chaos.2018.01.018
0960-0779/

"follow the money trail" may not be applicable in the context of counterterrorism. One of the reasons of the staggering costs of prevention of terrorist acts is the fact that terrorists have to succeed only once in order to cause major damage, while law enforcement has to succeed each and every time [3]. However, the reverse is also true when considering the individual stages of planning for a terrorist acts; here, the terrorists have to succeed each time, while law enforcement needs to intercept them only once.

Another important piece of information regarding counterterrorism strategies is that only 7% of the terrorist organizations have ended based on military force [35]. Given the enormous cost of military operations and the apparent limited success rate, this seriously questions the efficiency of this countermeasure. Other cost-benefit analyses in the context of counterterrorism are found in Zycher [67] and Mueller and Stewart [48].

The overall task of this research deals with tools that, in conjunction with other intelligence work, aid in rendering a terrorist network or cell ineffective or inoperable. The tools that are used to achieve this goal are taken from social network analysis, while the data stem from intelligence sources. The main idea is to take open-source and intelligence data in order to identify terrorist cells (and possibly the functions of individuals in it) in order to render the cell ineffective. Among the data to be used are communication incidences, e.g., phone calls, text messages, skype calls, email messages, etc. Given the huge number of potential connections to be monitored, an automatic method is probably the only feasible solution. This means traffic analysis, in which only the beginning of the contact, its end, and the parties involved (typically, the telephone numbers, IP addresses, or similar identifiers) can be observed. This also eases the legal burden of law enforcement: rather than applying for a large number of warrants (requiring probable cause) as required for actual wiretapping, subpoenas (a statement that the information is relevant to the investigation) is sufficient for phone records (Smith v Maryland, Supreme Court 1979), cell phone location (Electronic Communications Privacy Act), IP addresses (US v Forrester, 2007), and social media information (in case only basic information is obtained). However, the approach is not without its critics. For instance, Jonas and Harper [34] claim that data mining in the context of terrorism is a waste of money. Their argument is based on the large number of false positives (i.e., the assertion that someone may belong to a terrorist group, while he does not) that is typically generated by algorithms. A critical evaluation of the pros and cons of network analysis in the context of counterterrorism is provided by Bohannon [4].

2. Modeling terrorist networks

Starting with the three phases in social network analysis-supported counterterrorism efforts as proposed by Eiselt and Bhadury [13], this section describes different networks that can be derived from different types of information concerning suspected or known terrorists.

The aforementioned three phases in counterterrorism are as follows.

- *Development*. This phase starts with the known and suspected terrorists and models them and their known relations in one or more networks.
- *Delineation*. This phase evaluates the network(s) created in the previous phase. The important task in this phase is that it determines the likely roles of the members and their importance based on the network properties.

Finally, there is the phase in which all of the tasks above are set to work in the

- *Destabilization* of the network. This phase is the *raison d'être* of the analysis. It considers possible modifications of the network(s), so as to render them ineffective or even inoperable.

This section will discuss some issues in the development phase, while the next two sections of this work deal with the remaining two phases. In order to discuss known and potential terrorist networks, we first need to formalize matters. In order to do so, define a network $G=(N, A)$ with the set of nodes N and the set of arcs A. Here, we use the term "arcs" loosely in that it may represent directed or undirected connections. Which type of connection is investigated will be clear in the specific context. The nodes will represent the entities under investigation: these will denote suspected terrorists, even though it is possible that, in a macro view, they symbolize terrorist organizations. The arcs will show the interactions or relations between the nodes. The meaning of the arcs will depend on the type of network we are investigating. Looking at relations between individual nodes from a static, long-term, view, the relations between nodes are typically based on homophily ("birds of a feather," see, e.g., [45]) or on propinquity (i.e., physical and psychological proximity). In other words, the relations could connect individuals, who grew up in the same village, went to the same school or mosque, fought together as mujahideen in Afghanistan, or similar relations; for a comprehensive list of commonalities, see, e.g., [32]. One of the insightful analyses regarding the reasons for individuals to join terror networks asserts that the main reason for young (mostly) men is to be with their friends (see [1]). This result is mirrored by Atran, for details, see Downey [12]. The insightful piece by Grigolini [26] surveys, among other issues, the topics that involve small groups and teams, specifically those relating to their recruitment, management, leadership, and place in society.

The more obvious relationships between individuals discussed above may be augmented by non-obvious relations obtained through systems such as *NORA* (non-obvious relationship awareness software), which uses different databases and was originally developed to detect criminal activities in casinos. A network that consists of this type of relations is frequently referred to as a *trust network*; see, e.g., Lauchs et al. [41]. It tends to be static and stable, as trust is something that needs to develop over time. Examples of trust networks in the context of terrorism are found in Krebs [39] and in Mullins and Dolnik [49] for the 9/11 network, Rodriguez [54] for the Madrid train bombers, Koschade [38] for the network that conducted the Bali bombing, and others.

On the other hand, a different type of network may be constructed based on short-term connections between individuals, such as phone calls, meetings, text messages, emails, and other connections, which may indicate present or planned activities. Such networks are often referred to as *operational networks*; see, e.g., Holme and Saramäki [30]. Operational networks can be directed or mixed, and, similarly to static trust networks, but in a different way, their analysis may reveal something about the roles individual members in the network.

I submit that it would be useful to distinguish between multiple distinct terrorism-related networks, each of which has its own use, carries its own information, and requires its own analysis. More specifically, I propose the use of at least four networks: firstly, there is the aforementioned *trust network*, which is a relatively large undirected network that shows known and potential terrorists and their trust relations. In addition to the network itself (we could refer to it as the "A" level), we have its support network (the "B" level) and below that the general public (the "C" level, which includes everybody else). The dealings between the *A* and *B* levels appear to of particular interest, as Stohl and Stohl [59] note, a broad support network is a necessary feature of any successful terrorist network. In order to create the trust network, counterterror-