Automated Counter-Terrorism

Leslie Ball, Matthew Craven

Ball, L.D. and Craven, M. 2013. Automated counter-terrorism. In: J. Brynielsson and F. Johansson, eds. *2013 European Intelligence and Security Informatics Conference: EISIC 2013, August 12-14, Uppsala, Sweden*. Los Alamitos, Calif.: IEEE. pp.216. Available from DOI: http://dx.doi.org/10.1109/EISIC.2013.48

Automated Counter-Terrorism

Leslie Ball, Matthew Craven
School of Engineering, Computing and Applied Mathematics
University of Abertay Dundee, Dundee, Scotland, UK
l.ball/m.craven@abertay.ac.uk

***Abstract*— We present a holistic systems view of automated intelligence analysis for counter-terrorism with focus on the behavioural attributes of terrorist groups.**

Keywords—Counter-terrorism, social network analysis, open source intelligence, behavioural model

High-profile terrorist attacks in the first decade of this millennium have made counter-terrorism a priority for many governments. While [1] analysed open source data himself after the 9/11/2001 attack, such activity needs to be captured and incorporated into human operated intelligence systems in a timely manner to shift the focus from responsive to prevention mode. An examination of how the internet is being used to facilitate terrorist activity is required. Key to this is the online forensic evidence that supports the growth of a terrorist cell and its operations, such as the dissemination of ideology, online radicalisation [2], the obtaining of finance, planning of events and acquisition of weapons amongst others. Ultimately this evidence should act as intelligence to prevent terrorist attacks through interception and disruption.

Actionable intelligence is a generic term for the refinement of raw data for decision-makers. What is required, therefore, is a model that encapsulates the way terrorist groups operate (e.g., behaviours, structure) to enhance the predictability of any targeted group. Social network analysis lies at the heart of establishing group structure. Social structure alone, however, only forms part of the puzzle and lacks the richness required to understand the behaviours of a terrorist cell. Due to stealth operations, open source data are, however, notoriously sparse and often ephemeral in the case of extremist websites, whose data may be rich in terms of ideology and radicalisation.

The requirement of a holistic model that can integrate many disparate sources of data (e.g., open source, governmental and commercial) and perform predictive analyses also needs to consider the degree to which these processes can be automated to support critical decision-making. For example, such an automated process could involve the gathering of open source data (e.g., from social media sites, websites) and the use of various analytical techniques such as social network analysis for critical social structure, classification algorithms for predictive purposes and time series analysis for early warning indicators. Multiple languages and enhancement from multimedia also add complexity to data acquisition and are future considerations.

The populating of a behavioural model lies at the heart of this holistic view using the ideas, for example, from [2], [3] and [4]. Four broad categories of activity are considered along a timeline for a terrorist group: 1) recruitment 2) organisation and planning 3) preparatory conduct and 4) the terrorist act [3]. For structure, [4] argues that recruitment behaviour has been replaced by the term 'linkage', whereby terrorists connect to a group rather than the other way around, while [2] addresses radicalisation by presenting a scale for categorising online terroristic content. Such a hybrid model could, for example, capture data related to linkage and radicalisation, as well as tracking the developing roles of planning and organization and the procurement of weapons or access to other vital materials or information (in terms of preparation and intent). Social network analysis offers contributions in the tracking of the dynamic evolution of a criminal cell [5] and through transactions related to planning. Further analyses of social activity and location information (if available) could in turn provide behavioural predictions [6] or early warning indicators throughout the behavioural timeline [7].

The main conclusion of this paper is to place a call on the intelligence research community to adopt an integrated systems approach to automating data capture and analyses within a broader terrorist behavioural model of pre-incident indicators. Essential to its success is a thorough prior evaluation of the availability and accessibility of pre-attack open source data, as well as other governmental and commercial data.

REFERENCES

[1] V. Krebs, Mapping networks of terrorist cells. Connections, 24 (3), 2002, pp. 43-52.

[2] D. Holbrook, G. Ramsay and M. Taylor, "Terroristic Content": Towards a grading scale. Terrorism and Political Violence, 25, 2013, pp. 202-223.

[3] B. Smith, K. Damphousse and P. Roberts, Pre-Incident indicators of terrorist incidents: The identification of behavioral, geographic, and temporal patterns of preparatory conduct. Report 214217, US Department of Justice, Washington DC, 2006.

[4] L. Vidino, Radicalization, linkage, and diversity: Current trends in terrorism in Europe. Rand National Defense Research Institute, 2011.

[5] K. Carley, J. Diesner, J. Reminga and M. Tsvetovat, Toward an interoperable dynamic network analysis toolkit. Decision Support Systems, 43 (4), 2007, pp. 1324-1347.

[6] N. Eagle and A. Pentland, Eigenbehaviours: Identifying structure in routine. Behavioral Ecology and Sociobiology, 63 (7), 2009, pp. 1057–1066.

[7] K. Drozdova and M. Samoilov, Predictive analysis of concealed social network activities based on communication technology choices: early-warning detection of attack signals from terrorist organizations. Computational & Mathematical Organization Theory, 16, 2010, pp. 61-88.