Digital Investigation 15 (2015) 39–45

Contents lists available at ScienceDirect

Digital Investigation

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

From data to disruption

P.A.C. Duijn [a, b], P.M.A. Sloot [b, c, d, *]

[a] Research and Analysis, Dutch Police, The Netherlands
[b] University of Amsterdam, The Netherlands
[c] Complexity Institute, NTU, Singapore
[d] ITMO University, St. Petersburg, Russian Federation

ARTICLE INFO

Article history:
Received 24 September 2015
Accepted 28 September 2015
Available online 7 November 2015

Keywords:
Organized crime
Complex Systems
Criminal Networks
Adaptive systems
Law enforcement

ABSTRACT

Organized crime groups and law enforcement agencies are caught in complex system similar to a continuous game of cat-and-mouse, in which the latter frequently remains two or more steps behind. Law enforcement agencies are therefore seeking for more proactive strategies in targeting these criminal network structures more effectively. This starts with a better understanding of the way they operate and adapt over time. A key element to developing this understanding remained largely unexploited: big data and big data analytics. This provides novel insight into how criminal cooperations on a micro- and meso level are embedded in small-world criminal macro-networks and how this fosters its resillience against disruption. This paper discusses the opportunities and the limitations of this data-driven approach and its implications for both law enforcement practice and scientific research.

Introduction

Organized crime groups impose a continuous threat to global society, by causing harm to our economic, social, technological, political and environmental infrastructures (Europol, 2013, 2015). Their existence depends on optimizing efficiency and profit from their illegal activities, while remaining undetected by the government at the same time (Raab and Milward, 2003, Erickson, 1981, Morselli et al., 2006, Duijn et al., 2014). Law enforcement agencies on the other hand are struggling with important questions: How can we detect these criminal groups and their activities? What are the best strategies to disrupt them effectively? And how do they develop resilience against interventions? Within the law enforcement organization a key element to answering these questions has remained largely unexploited: big data and big data analytics. Since data are becoming more and more available from a plethora of new sources, they will provide opportunities for data-driven analysis towards understanding organized crime in terms of criminal network structures, dynamics, and resilience against law enforcement interventions (Duijn and Klerks, 2014a, 2014b). This paper discusses the opportunities and the limitations of this data-driven approach and its implications for both law enforcement practice and scientific research.

Understanding organized crime

Theories about organized crime have changed over time. Early perceptions of organized crime focused on hierarchical pyramid structures with kingpin leaders controlling their criminal enterprise from the top. Criminal organizations were perceived and analyzed as separate entities on a micro-level, leading to an oversimplified perspective of criminal reality (Duijn and Klerks, 2014a). In the early nineties organized crime received serious scientific attention for the first time, which led to empirical studies of organized crime. A selection of court files and

* Corresponding author. University of Amsterdam, The Netherlands.
E-mail address: p.m.a.sloot@uva.nl (P.M.A. Sloot).

http://dx.doi.org/10.1016/j.diin.2015.09.005
1742-2876/

case studies from multiple criminal investigations were analyzed manually. These studies uncovered mechanisms of trust, expertise, reputation and social opportunity structures, which shape the way organized crime groups and individual actors become connected and adapted to fast changing illegal markets (Fijnaut et al., 1991; Kleemans and Van de Bunt, 1999, Klerks, 2001). It was also revealed that organized crime is an integral part of the global networked society and it was emphasized to study organized crime from a network perspective (Klerks, 2001; Kleemans and De Poot, 2008).

Due to practical limitations of manual analysis techniques, a macro-level understanding of the structure of organized crime currently consists of theoretical assumptions instead of empirical observations. On the other hand, datasets about terrorist- and criminal actors and their mutual connections are growing, due to more deliberate strategies for collecting, storing and sharing information within day-to-day law enforcement practice since 2001 (The terrorist attacks[1]). Moreover, the influx of embedded academics within law enforcement has made these datasets more easily accessible for scientific purposes (Duijn and Klerks, 2014a). At the same time scientific disciplines such as social science and complexity science have started to exchange ideas and methodologies, leading to advanced network analysis methods being introduced into social science. This opens the door towards a data-driven approach to create an empirical understanding of organized crime.

Complex adaptive systems

From a macro-perspective criminal network structures can best be understood as complex adaptive systems. The concept of complex adaptive systems (CAS) derived from systems theory and was first introduced by Holland (1999). A complex adaptive system is a self-organizing network, which constantly adapts its structure and behavior according to change in the behavior of its individual components (agents). These agents constantly act and react to each others behaviors and the environment, meaning nothing is fixed. This makes the behavior and structure of CAS highly unpredictable, but effective in adapting to changed environments (Chan, 2001).

While CAS is an established theoretical concept for understanding complex networks in biology and economy, CAS theory also applies to criminal networks that constantly adapt to changing law enforcement strategies and government regulations (Kenney, 2007). Criminal network structures continuously balance between efficiency in the collaboration of its parts and security in staying undetected by law enforcement organizations. Shifts in law enforcement strategies may destabilize this balance and trigger shifts in the way the independent criminals in the network interact and adapt. How this affects the structure of the overall criminal network depends on how the independent actors interact with each other to adapt to these external factors from the bottom up. There are no explicit rules about how a criminal network is formed or changed. Criminal networks are emergent self-organizing systems, which changes structure at any point in time due to how its parts react to external pressures.

Criminal networks have for instance quickly adapted to the opportunities created by the Darknet that provides anonymity and access to worldwide online marketplaces for selling illegal commodities in large quantities. Law enforcement agencies responded by successfully taking down some of the most active online marketplaces (Soska and Christin, 2015). The criminal cyber networks active on these online marketplaces adapted to these interventions by increasing the number of online marketplaces and servers, outweighing the limited capacity of law enforcement to target them all effectively. The interactions of the individual actors changed the shape of the Darknet towards a more dispersed network structure. Such a continuous evolution driven by non-linear feedback mechanisms is an important feature of complex adaptive systems. The practical reality is that law enforcement will always be one or more steps behind (Soska and Christin, 2015).

To narrow this gap, researchers should focus more on capturing criminal network *dynamics* instead of focusing on static network representations. Understanding these dynamics can have implications for uncovering mechanisms of competitive adaptation, criminal network resilience and the effectiveness of law enforcement interventions (Duijn et al., 2014; Duijn and Klerks, 2014a). Social network analysis and computational modeling can help to uncover these dynamics, but before we can understand the output of these methodologies we need to obtain a better understanding of the sources: the data.

Law enforcement data

Criminal networks actively try to avoid detection from law enforcement. As compared with legitimate social systems, they are particularly hard to detect leading to inevitable missing data in the final network representation. The completeness of a criminal network representation is therefore highly dependent on the strengths and weaknesses of the data sources from which it is obtained. Many criminal network studies necessarily rely directly or indirectly on law enforcement data, which is not primarily collected for scientific purposes (Morselli, 2009). Two important factors should therefore be taken into account to retrieve a reliable and valid network representation from these data.

First, the accuracy of the data source is a critical consideration (Morselli, 2009). Every piece of law enforcement data is collected in the context of a specific policing task, for instance collecting evidence, preparing investigations or monitoring a situation which shapes the information collection process and the bias embedded within. To overcome these biases, researchers need to understand the background of the data collection and take into account the policing priorities while drawing conclusions (Duijn and Klerks, 2014a).

[1] The terrorist attacks in New York, London, and Madrid promted the introduction of intelligence-led policing within many national police departments. It involves a process for which every decision within law enforcement should be preceded by a structural analysis of the situation based on deliberately collected information in the frontline of police practice (see Ratcliffe, 2012).