Editorial: Space Oddity? Exploring Organised Crime Ventures in Cyber Space

Editorial

Special Issue

Space Oddity? Exploring Organised Crime

Ventures in Cyber Space

Helena Carrapico and Anita Lavorgna*

Over the past two decades, the development of modern societies has become intimately interconnected with information technologies. Such a trend is particularly visible among the increasing number of personal objects, household appliances and professional structures connected to information networks (European Commission, 2015; Europol, 2014a). Although such evolution is usually applauded from an economic and societal perspective, it is also understood as constituting a risk in security terms. As the degree of connectivity dependence of individuals, companies and critical infrastructures grows, so does the likelihood of technology being abused, in particular for criminal purposes (Eriksson and Giacomello, 2010). As a result, cyber crime has become, over the past few years, the object of increased concern in Europe (Malmstrom, 2011; Avramopulos, 2015). According to the previous Home Affairs Cecilia Commissioner Malmstrom, "Cyber crime is an attack on basic societal values and citizen's security" (2012: 2). Not only does it represent a considerable cost to European societies, but it also remains an important challenge for law enforcement and judicial systems, due to its technical complexity and rapid innovative character. As a result, numerous responses have been put in place, both at national and European level, with the first focusing on the implementation of resilience

*Helena Carrapico is Lecturer in Politics and International Relations at Aston University, School of Languages and Social Sciences. Contact: h.farrand-carrapico@aston.ac.uk

Anita Lavorgna is Lecturer in Criminology at the University of Southampton, Social Sciences. Contact: A.Lavorgna@soton.ac.uk.

The European Review of Organised Crime 2(2), 2015, 1-5

ISSN: 2312-1653

measures aimed at protecting critical infrastructures, businesses and citizens' lives, and the second assuming a strategic coordination role (European Commission and High Representative for Foreign Affairs and Security policy, 2013).

An exploratory analysis of policy and law enforcement reports will quickly indicate that the degree of dangerousness of cyber crime has recurrently been associated to the transnational and anonymous character of cyber attacks (Europol, 2014b). The connected nature of cyberspace has enabled what used to be a small-scale criminal community, essentially formed by hackers with little interest in profit, to become a large industry reportedly worth between $300 billion and $1 trillion (McAfee, 2013; Symantec, 2011). The real impact and reach of cyber crime, however, remains a point of contention, with industry and institutional figures varying considerably. Such disparity should not come as a surprise, given that in both the academic and policy literatures the concept of cyber crime continues to be elusive and essentially contested (Wall, 2007).

The degree of dangerousness has been further emphasised by the idea that cyber criminal activities are being carried out by highly organised criminal groups, whose structure and professionalisation have rendered their identification and arrest considerably more difficult (Europol, 2014b). However, this association between cyber crime and organised crime has so far been based on limited empirical evidence (Lavorgna, 2015; Wall, 2007). In fact, although organised crime is generally presented by policy makers and international organisations as a major actor in cyberspace, the academic literature has, so far, paid limited attention to this element. More specifically, limited research has been conducted on how different types of organised crime groups use cyberspace to carry out their traditional activities, and on how new illicit online activities have emerged as a result of organised crime's digital shift. While it is logical to think that criminal opportunities in cyberspace should be attractive for organised crime, it is not self-evident that these groups can successfully exploit such opportunities (Brenner, 2002; McCusker, 2006; Lavorgna, 2015). So far, there is only limited anecdotal evidence that this is the case (Lavorgna and Sergi, 2014). Also, limited empirical research has assessed whether and to what extent offenders involved in cybercrimes are "organised crime". Some authors anticipated that new forms of organised crime are emerging online (Tropina, 2013) but there is still scarce evidence as to whether new criminal actors created organised groups in cyberspace. Rather, evidence points in the direction of the presence in cyberspace of loose, flat, and fluid networks, generally without a common functional unit (Wall, 2014).

The relationship between organised crime and the Internet is certainly complex, but also topical and fascinating. This special issue wants to shed some lights and prompt a reflection on some aspects of this relationship. You will find four original articles, one practitioner's insights, two debate pieces, and one research note on the connections between traditional and new forms of organised crime, cyber crime, and their policing. As in our former issues, in EROC we continue to promote a wide range of publication formats to promote constructive discussion not only among

academics from different backgrounds, but also between academics and practitioners.

The first three original articles, while looking at different sets of cyber-facilitated and cyber-enabled crimes in different countries, bring us straight to the core of the problem: policing cyberspace is challenging. Given the rapidly evolving nature of cyber crime's activities, criminal groups are often two steps ahead of law enforcement cooperation. Law enforcement has not only to embrace a whole new set of technical competences, but it also often has to deal with out-dated substantial and procedural legal frameworks, and with the difficulty to keep pace with an ever-changing criminal scene.

Trine Thygesen Vendius offers a comparative socio-legal analysis based on interviews with police officers to discuss the importance of undercover policing as a necessary investigative tool to detect and infiltrate child sexual offenders in the EU. She effectively stresses the presence of a gap between policy agendas putting cyber-facilitated crimes at the top of their priorities and the overwhelming problems that law enforcement has to deal with when it comes to the policing of cyberspace in their everyday routines. Kamil Bojarski analyses a range of different cyber crime operations, in particular those where law enforcement engage in active and sophisticated surveillance and intelligence techniques, to identify major technical and legal challenges, as well as to predict possible future trends. Among the obstacles identified by the author, there is the facilitated access to software thanks to open sources, the difficulty in conducting law enforcement activities beyond national borders, the need to develop transatlantic cooperation to adequately fight cyber crime and the regulation of domestic surveillance by intelligence agencies.

The article by Sophie Richardson and Nicholas Gilmour draws instead our attention to the cyber crime landscape in New Zealand. Departing from a reflection on how this phenomenon has come to constitute a direct threat to national security, the authors embark on an analysis of the challenges posed by cyber crime activities to criminal prosecution. Both this reflection and analysis are well illustrated by references to recent cyber crime attacks, namely the downing of a national telecoms service provider and the attack on the New Zealand Parliament's website. The article concludes by suggesting that the way forward lies in the increase of New Zealand's international cooperation and resilience, in particular through an increase of the available technical expertise.

It is clear that traditional law enforcement efforts in tacking old and new forms of organised crime and cyber crime has room for improvement. Given the enormity of the environment to be controlled and the risk of information overload, one way to go is via the sharing of research-informed knowledge and good-practices, so to direct efforts in the more efficient way.

The fourth original article by David Wall brings us a step forward in this direction. He questions and challenges the uncritical assumption present in many public reports that mafia-driven organised crime groups are increasingly present in cyberspace. The "mafia" rhetoric has long permeated—often in a misleading way—debates on organised crime; when applied to cyber crimes, it confuses the public and risks to misdirect police resources. Wall's contribution, after looking

critically at current organised cybercrimes debates, presents four paradigm shifts in cybercrime and its organisation, and calls for the development of new methodologies and empirical studies to further our understanding of the organisation of crime in cyberspace.

On the same line, Rutger Leukfeldt's debate piece underlines the limited empirical research conducted on organised cyber crime and the resulting literature gap in this area. Although growing numbers of journalistic pieces, policy papers and academic articles alert us to the emerging characteristic of cyber crime as an organised activity, few works are actually based on substantiated claims. Leukfeldt contributes to rectifying this gap by proposing avenues for future research, focused in particular on a systematic analysis of cyber criminal networks. As argued by the author, such approach should allow us to clarify whether criminal networks acting in cyberspace emerge and evolve differently from traditional networks, which would lead us to develop more adequate countermeasures. The debate piece by Lucie Kadlecová focuses on Russian-speaking cyber organised crime and explores the different elements contributing to the perception of this phenomenon as being very successful. In an attempt to go beyond the traditional view that success is based on a mutually beneficial relationship between criminals and political elites in a post-soviet context, the author analyses legal loopholes and economic benefits, as well as less researched areas such as the unemployment among young IT specialists. The debate piece suggests that there is no specific causal factor at the origin of the success of Russian speaking cyber organised crime, whose evolution can be characterised as reactive in relation to political and economic events in the post- soviet space.

The same call to move beyond stereotypes and to enhance empirically-based research to further our knowledge of crime in cyberspace is present in the research note by avid e cary-He tu and Judith Aldridge. They show how researchers can better identify, monitor and understand offenders by developing new techniques to investigate criminal acts in cyberspace. Specifically, they present their experience in developing an innovative tool to monitor drug markets in the deep web, and share the challenges and ethical considerations they had to address in creating and using their own custom tool for automatically collecting data online. Therefore, we should remember that cyberspace presents also advantages for keeping track of criminal activities, and both academics and practitioners should learn how to take advantage proactively of this situation.

To conclude on an even brighter note, the practitioner’s insight developed by Tuesday Reitano, Troels Oerting and Marcena Hunter focuses on the Joint Cybercrime

Action Taskforce (J-CAT), one of the most recent tools used to fight cybercrime. The JCAT is a very good example of the type of responses currently being developed. This piece explores the functioning of this cooperation platform, which is based at Europol and has already demonstrated considerable success. Thanks to its single physical location, the limiting of legislative and bureaucratic constraints, as well as membership restriction, the J-CAT has created relations of trust among participating countries and produced key intelligence packages.

Last but not least, we would like to thank our peer reviewers for their invaluable work and Chris Bowkett and Aaron Martin for their editorial assistance with the proofreading.

We hope you will find this issue informative and stimulating in further examining some of the challenges of the contemporary world.

References

Avramopoulos D (2015) *Commissioner Avramopoluos presents European Agenda on Security at European Parliament*. Speech/15/4885. 28th April. Strasbourg.

Brenner SW (2002) Organized cybercrime? How cyberspace may affect the structure of criminal relationships. *North Carolina Journal of Law and Technology* 4(1):1-50.

Eriksson J and G Giacomello (eds) (2010) *International Relations and Security in the Digital Age*, London: Routledge.

European Commission (2015) *Commission Staff Working Document, A Digital Single Market strategy, for Europe- Analysis and Evidence*. Brussels.

European Commission and High Representative of the European Union for Foreign Affairs and Security Policy (2013) *Joint Communication to the European parliament, the Council, the European Economic and Social Committee and the Committee of the Regions- Cybersecurity Strategy of the European Union: an open, Safe and Secure Cyberspace*. JOIN (2013) 1 final. 7th of February. Brussels.

Europol (2014a) *EC3 First Annual Report*. The Hague.

Europol (2014b) *iOCTA- The Internet Organised Crime Threat Assessment*. The Hague.

Lavorgna A and Sergi A (2014) Types of organized crime in Italy. The multifaceted spectrum of Italian criminal associations and their different attitudes in the financial crisis and in the use of Internet technologies, *International Journal of Law, Crime and Justice* 42(1): 16-32.

Lavorgna A (2015) Organised crime goes online. Realities and challenges. *Journal of Money Laundering Control* 18(2).

McAfee (2013) *The Economic Impact of Cyber crime and cyber espionage. Centre for Strategic and International Studies*. July.

McCusker R (2006) Transnational organized cyber crime: Distinguishing threat from reality. *Crime, Law and Social Change* 46(4): 257-273.

Malmstrom, C. (2012) *Public- private Cooperation in the Fight against Cyber crime*.

SPEECH/12/409. EU Cybersecurity and Digital Crime Forum. 31st May. Brussels.

Malmostrom C (2011) *It's Time to Take Cyber Criminals Offline*. SPEECH/11/260.

Hungarian presidency Cyber Crime Conference in Budapest. 13th April. Brussels.

Symantec (2011) *Norton Cyber crime report 2012*. Available from:

http://uk.norton.com/cybercrimereport/promo. Last accessed on 20th September 2015.

Tropina T (2013) Organized Crime in Cyberspace. In: S. Heinrich-Boell and R.

Schönenberg (eds.), *Transnational Organized Crime: Analyses of a Global Challenge to Democracy*, Bielefeld, GER: Transcrip.

Wall D (2007) *Cybercrime: the transformation of crime in the information age.* Cambridge and Malden: Polity Press.

Wall DS (2014) Internet Mafias? The dis-organisation of crime on the internet. In: S.

Caneppele and F. Calderoni (eds.), *Organised Crime, Corruption and Crime Prevention*. London, Springer.