Article

Offline and Local: The Hidden Face of Cybercrime

Jonathan Lusthaus* and Federico Varese**

A persistent refrain in both the academic literature and the popular press is that cybercrime is a largely anonymous activity that exists in cyberspace (e.g. Gabrys, 2002. For relevant discussions, see Grabosky, 2004; Wall, 2007; Lusthaus, 2013). Cybercriminals 'meet' anonymously in virtual marketplaces (see, for instance, Holt and Lampke 2010; Décary-Hétu and Dupont, 2013; Hutchings and Holt, 2015). Shadowy attackers could strike from anywhere at any moment. They are a new type of threat, unlike any criminal activity that has been observed before. In short, these offenders challenge existing paradigms of crime and policing, and vastly new models are required to comprehend this new challenge.

In this article, we seek to add greater nuance to understandings of cybercrime by highlighting a neglected aspect of the phenomenon: the offline and local dimension. As a starting point it is vital to acknowledge that all cyber-attacks stem from a person who physically exists in a certain location. This basic consideration helps us better understand, investigate and counter cybercrime. It contextualizes the threat. We should expect a degree of variation as to how cybercrime presents in each case. The economic and social dynamics of different settings are likely to influence who gets involved in cybercrime, what types of cybercrime they carry out and the way they are organized. In short, both the individuals behind cybercrime and the offline worlds they inhabit deserve study. Cybersecurity should not just be about the analysis of fast changing technical threats and the challenges they pose. Alongside the online and technical, there is an offline, human and contextual element that matters.

In this article, we consider the case of Romania—a leading cybercrime hub. On the basis of two field trips, we explore the offline and local dimension of cybercrime in this country. Our fieldwork suggests that understanding the specifics of the Romanian context is vital to comprehending the nature of cybercrime there and how it emerged. Important factors appear to include: the legacy of communism; economic development; and corruption/protection. These elements should be understood at both national and regional levels. The rest of this article is comprised of four sections. The next section outlines the methods employed for this study. The section on "Romanian cybercrime" sketches the phenomenon at the national level. The section on "The case of Râmnicu Vâlcea" explores cybercrime at a more regional level. The final section outlines the policy implications of this study.

*Department of Sociology, University of Oxford, Oxford, UK.
E-mail: jonathan.lusthaus@sociology.ox.ac.uk
**Department of Sociology, University of Oxford, Oxford, UK.

Policing, pp. 1–11
doi:10.1093/police/pax042

Methods

For the focus of this article, we have chosen the case of Romania, a country that has a reputation of being a major producer of cybercrime. In order to understand the nature of Romanian cybercrime the authors visited Romania to carry out fieldwork in March 2015, with an earlier visit by one author (Lusthaus) in September 2014. Locations visited were Bucharest, Râmnicu Vâlcea and Alexandria. Collectively, these two visits amounted to less than a month and were structured around field observations and interviews. We met with a number of participants including a former cybercriminal, a hacker, current and former law enforcement agents, along with private sector cybersecurity professionals, a journalist and others. The participants for each data pool are summarized chronologically in Tables 1 and 2.

Along with the interviews, we also spent time in restaurants, cafes and bars, known to be cybercriminal hangouts and where we could observe them in situ. We visited the neighbourhoods thought to be key cybercriminal hubs and passed their luxury cars in the streets. Our observations and interviews were recorded in field notes. While only Lusthaus collected and analysed the data from 2014, the data in 2015 was recorded individually by both authors to offer independent points of comparison.

Fieldwork is an established scholarly approach within disciplines like sociology and anthropology, though it is not widely applied to cybercrime. Nonetheless, it is well suited to investigating the offline dimension of cybercrime, where some other methods have limited utility. In the past, fieldwork studies have been successfully carried out with regard to criminal groups, such as street gangs and drug groups (see, for example, Sanchez-Jankowski, 1991; Maher, 1997; Venkatesh, 1997; Hamill, 2011. For an overview of different approaches see Ferrell and Hamm 1998). In addition to our observations and field interviews, we have also collected data on legal cases, along with other open source materials such as media articles and statistical reports. These data offer independent sources to improve accuracy.

Our research in Romania represents an initial foray into this underground society and this article should be considered a pilot study, presenting preliminary findings on the Romanian context. More detailed research is planned for the future to investigate the topic in greater depth, with only the core initial outcomes presented in this article in order to allow researchers and practitioners to benefit in the short term. In brief, this article is exploratory: we seek to generate future research directions, rather than test already formed hypotheses.

Table 1: Participant data collected/accessed by Lusthaus (September 2014)

Code	Description
L1	Former Romanian law enforcement agent 1
L2	Romanian law enforcement agent 1
L3	Former Romanian law enforcement agent 2
L4	Romanian prosecutor 1
L5	Romanian law enforcement agent 2

Table 2: Participant data collected/accessed by Lusthaus and Varese (March 2015)

Code	Description
LV1	Romanian cybersecurity professional 1
LV2	Romanian law enforcement agent 3
LV3, LV4	Romanian researcher 1, Romanian hacker 1
LV5, LV6, LV7	Romanian journalist 1, Romanian prosecutor 2, Former Romanian law enforcement agent 3
LV8, LV9	Romanian cybersecurity professional 2, Former Romanian cybercriminal 1
LV10, LV11	Romanian cybersecurity professional 3, Romanian cybersecurity professional 4
LV12	Romanian prosecutor 3

Romanian cybercrime

Nicolae Popescu was born in the small city of Alexandria, a 2-hour bus ride south of Bucharest. He is now in his early 30s. After organizing a digital scam to sell hundreds of fictitious cars on eBay, and pocketing $3 million, he was arrested in 2010, but eventually was released on a technicality (Ghidovăt and Cana, 2014). He is currently a fugitive from justice and the American reward for any information leading to his capture is $1 million. Popescu currently occupies a prominent place on the FBI's 'Cyber's Most Wanted List'.[1] Popescu is just one of a number of high-profile cybercriminals hailing from Romania. In common with numerous other Romanians in this business, his expertise is 'online auction fraud'. This form of activity began largely with the exploitation of eBay customers, but has now migrated to other platforms as well. It is built around the sale or rental of fictitious goods and services. This type of activity might seem unsophisticated, but it can net the fraudsters millions a year and has spawned a cottage industry. A group arrested in Romania in 2014 had made €1.4 million in a short period of time (Hall, 2014). According to the US Embassy in Bucharest, Romanian cybercriminals steal $1 billion every year by targeting US computers (Odobescu, 2014). While scams often target Western countries, new targets are also emerging in developing countries (LV2).

Romania is one of the best knowns hubs for cybercrime around the world (Lusthaus, forthcoming). Why is cybercrime such a problem in this country? Part of the answer may be the legacy of communism. The regime of Communist dictator Nicolae Ceausescu had invested significant resources into computer science studies. As the country was denied access to Western technology, Romanians developed their own IT capabilities, including reverse-engineering computers (Heeks and Grundey, 2004; LV10; LV11). This legacy has largely been positive: a number of Romanians are now working in Europe and the USA, while several foreign technology companies have operations in Romania. There are also a number of successful Romanian technology companies that have emerged (LV1; see Coleman, 2014). In the early 1990s, before major Internet providers arrived, there were already countless homemade micro-networks in the country (LV10; LV11). This explains how Romania performs well in Internet connectivity rankings, sometimes within the top 10 globally for average peak connection speed (see, for instance, Akamai, 2016). This background may help make sense of why cybercrime can be successfully carried out on a large scale in Romania: the infrastructure exists for fast and successful online operations. It may also help explain why online fraud rather than hacking or malware is the Romanian cybercrime *par excellence*. Many of those who otherwise might engage themselves in more technical forms of cybercrime can find good employment opportunities in the Romanian technology sector, in the EU or further afield.

The second key factor that may help explain the emergence of Romanian online fraudsters in great numbers is the economic situation. While Romania has a high level of IT expertise, it remains one of Europe's poorest countries. The 2014 average salary is €398 a month (the EU average is €1,489), while agriculture is not fully mechanized: there are 201 tractors per 100 sq. kilometres of arable land (the EU average is 815.1).[2] For those not in a position to take advantage of the good jobs in certain sectors, other (criminal) opportunities might become appealing. Finally, corruption remains high in Romania. According to Transparency International's 2016 Corruption Perceptions Index, Romania scores 48 out of a possible 100, and only just above the global average of 43 (100 indicates a country free of corruption).[3] Conversations and interactions we had in the

[1] Popescu's listing can be found at https://www.fbi.gov/wanted/cyber/nicolae-popescu.
[2] Data from http://www.reinisfischer.com/average-salary-european-union-2015 and http://wdi.worldbank.org/table/3.2.
[3] This index is available at https://www.transparency.org/news/feature/corruption_perceptions_index_2016.

country also indicated one needed to be aware of dishonest practices within day to day life. In fact, at one point during our research, the authors were the target of a scam, with a purported (and unsolicited) 'fixer' offering to provide extensive access to cybercriminals and high-level law enforcement agents. These participants were offered to us for interview in return for a very significant fee. But minor attempts to investigate quickly revealed that many of this fixer's representations were false. It is possible that this type of environment provides fertile ground for those who wish to move into Internet fraud.

The case of Râmnicu Vâlcea: a hub for cyber frauds?

Not all parts of Romania are equally affected by cybercrime. The phenomenon appears to have a regional component, with different parts of the country being known for involvement in particular scams (LV2; L1; L2). Supporting this point, Table 3 presents data from the Romanian Court of Appeal related to Internet fraud (*fraudă informatică*) for the period 2008–2010 (when data are available).[4]

Table 3 indicates that the region of Piteşti (just north of the capital) accounts for 27% of all cases. This is perhaps not surprising given that the town of Râmnicu Vâlcea and its satellite communities fall within this jurisdiction. Râmnicu Vâlcea is known by another name, 'Hackerville' (Bhattacharjee, 2011), and was noted by almost everyone we interviewed in Romania. The town is a major hub of cybercrime, though its assumed title is really a misnomer. 'Fraudville' would make a better descriptor, given the local speciality is the type of online auction fraud described above. With a much larger population, Bucharest falls second on the list.

From the early days of Romanian cybercrime, Râmnicu Vâlcea became known for Internet scams, which effectively served as a major local industry. When we visited the town, it seemed that business had been good. There were trendy cafes, bistros and restaurants, along with two shopping malls. Inside the malls were shops selling designer clothes, appliances, computers, sporting goods, jewellery, as well as a range of entertainment facilities. One of the most striking features of the town was the large number of luxury cars driving the streets. Old Romanian Dacias regularly could be seen side by side with shiny black Mercedes and BMWs. In fact, there was a Mercedes-Benz dealership just outside the town. On paper, the economic situation in Râmnicu Vâlcea should be dire. A large chemical plant in the area, run by OltChim, used to provide considerable employment. But the plant began to struggle and closed down substantial parts of its operations, before it became insolvent in 2013 (see Romania Insider, 2016; Popescu, 2017). Nonetheless, the regional GDP continues to grow (INS-RV 2014). Several media reports have all suggested that Râmnicu Vâlcea is a hub of Internet frauds (Wylie, 2007; Bhattacharjee, 2011; Bran, 2011; Hall, 2014; see also Wittkop, 2016, pp. 163–164). A number of locals we encountered seemed well aware of what the town was famous for and the type of criminal enterprise that was commonly carried out there.

Our field research suggested that there are two components of the online fraud business in Râmnicu Vâlcea, which are 'morally and financially addicted to each other' (L4). The first part is the organization of the fraud. This involves managing a team that advertises the fake products online and engages with the customers who will be defrauded. One participant informed us that, in some cases, this is coordinated to the level where standard

[4] Jurindex is a free service which aims to provide free access to court judgments. It currently includes all Court of Appeal decisions published in the period 2008–February 28, 2010. There are a total of 233,921 documents.

Table 3: Number of decisions of the Court of Appeal for cases involving 'fraudă informatică', 2008–2010, Romania

Region	Number of cases	Percentage of total
CA PITEŞTI	75	26.98
CA BUCUREŞTI	38	13.67
CA BACĂU	25	8.99
CA CLUJ	22	7.91
CA BRAŞOV	21	7.55
CA CRAIOVA	19	6.83
CA ALBA IULIA	18	6.47
CA GALAŢI	16	5.76
CA TIMIŞOARA	11	3.96
CA IAŞI	10	3.6
CA CONSTANŢA	9	3.24
CA PLOIEŞTI	9	3.24
CA SUCEAVA	4	1.44
CA ORADEA	1	0.36
CA TG MUREŞ	0	0
CA MILITARĂ	0	0
TR VRANCEA	0	0
Total	278	100

Source: Jurindex (http://jurisprudenta.org/).

scripts for each stage of the victim interaction are provided to the scammers to reduce the need to craft each response from scratch (LV2). If the scam is successful, the customer will pay money into an account (or otherwise) that is controlled by the scammers. The second part of the business then involves the movement of the money. As buyers may be suspicious of sending money to Romania, it is common for the fraudsters to pretend they reside elsewhere, such as in America or the UK. They must also have accounts set up in these countries so as not to raise red flags in the customer's mind. This requires overseas-based teams to receive and move the money back to Romania. As we learned from those we spoke to, these team members are known as 'arrows' in Romania (as opposed to 'money mules', as they are commonly known elsewhere). While other modes are also now used, money transfer agencies have traditionally been a popular way to repatriate the funds to Romania (LV2; L1; L3; L4).[5] These agencies may have other functions within the town and throughout the country, but during our visits, the continued presence of many Western Union and MoneyGram outlets was clear. Sometimes multiple branches could be seen within metres of each other.

Our fieldwork suggests that this Romanian form of online fraud has a strong offline dimension. In short, a number of those involved in this type of cybercrime know each other personally. The groups are organized on the basis of a strict division of labour, with organizers recruiting other members to perform specific tasks (L1; L2; L3).[6] They often meet in person for business and/or socializing. Some also work in the same physical workspace as each other, for instance rented apartments or other locations (LV2; L1; L3; L4). One case was described where it seemed an entire small community was involved in the same cybercrime operation, which had spread between neighbours 'like a disease' (L4). Two local law enforcement agents interviewed for an article published in *Wired Magazine* make clear how the scammers are embedded within the life of the town. They describe 'investigating a childhood acquaintance or, conversely, running into criminals in social situations' (Bhattacharjee, 2011). This phenomenon is more than just offline, it is also local. One of the agents, named Stoica, provides some insights into how the process works at the grass roots level:

> Driving past a block of low-rise buildings with neatly trimmed hedges, Stoica notes a couple of apartments owned by people currently under

[5] Information based on police investigations provided to us by Maxim Dobrinoiu, an academic who researches cybercrime at the Law Faculty of Nicolae Titulescu University in Bucharest, confirmed these points.

[6] Information based on police investigations provided by Maxim Dobrinoiu confirmed these points.

> investigation. "I don't know if the people of Râmnicu Vâlcea are too smart or too stupid," Stoica says grimly. 'They talk a lot to each other. One guy learns the job from another. They ask their school friends: 'Hey, do you want to make some money? I want to use you as an arrow.' Then the arrow learns to do the scams himself' (Bhattacharjee 2011).

A similar example, though outside cybercrime, might be seen in reports about the Macedonian town of Veles and its fake news industry. Young people there realized they could make considerable money by creating pro-Trump news during the 2016 American presidential election and driving traffic to it. Once the details of the enterprise had been developed by the early practitioners, the activity quickly spread to a larger group in the town (see, for instance, Subramanian, 2017). These are instances of a well-known phenomenon noticed by economic sociologists, namely the 'network effects' of expertise and knowledge (Reagans and McEvily, 2003; Smith-Doerr and Powell, 2005).

In Râmnicu Vâlcea, there are suggestions that the localized nature of online fraud is actually concentrated in a particular part of that town. According to local prosecutors, there are at least a thousand people working full time on computer frauds in the town, mostly based in just one neighbourhood, Ostroveni. A *Le Monde* correspondent wrote in 2011: 'In Ostroveni, everyone knows what is happening, but *omertà* – the code of silence – is the norm' (Bran, 2011). Allegedly, High School no. 10 in the Ostroveni district of town is the place where scammers first cut their teeth. Of course, it was clear from our time in Râmnicu Vâlcea that many of the scammers have grown up and, while relatively young, are no longer just teenagers.

The final local element to be discussed in this case study is protection. In order to operate, scammers must avoid arrest. A key ingredient for the persistence of illegal enterprises is local corruption. The Deputy Head of Râmnicu Vâlcea police, Gabriel Popa, was arrested in December 2014 for revealing confidential information to a group of criminals. On 20 March 2015, another police officer, Alexander Popa, who was accused of passing confidential information to a cyber fraud group led by Nicolae Vasile, was also arrested. This group had recently netted almost €200,000 from frauds involving about 600 British victims. The penalty for the two officials was 30 days under house arrest (Rîpan, 2015). Politicians are also involved. The socialist senator elected in Râmnicu Vâlcea, Laurentiu Coca, was heard speaking on the phone with Mihai Obreja, the boss of a local gang that, in addition to cybercrime, is involved in loan sharking and extortion. The conversation between the two men was far from friendly: 'Return the money to my house, or you're fucked', said Obreja to the Senator (Miercuri, 2015). In another phone intercept, a member of the same gang is heard threatening to cut off the hands of a victim who has not yet repaid his debt (Miercuri, 2015). As further evidence that corruption is present in the area, Râmnicu Vâlcea's mayor (elected in 2012) was sentenced to 4 years for bribe-taking in 2014 (Jurnalul National, 2014).

Those who expose the links between major criminals and local political elites may be threatened and assaulted. One report suggests this might have happened to Romeo Popescu, the owner and editor of the local newspaper *Vocea Valcii* (Hall, 2014). While most observers argue that cybercrime is a non-violent type of activity, we contend that, when it becomes entrenched locally, violence may increase. Some cybercriminals might have technical skills or a talent for scams, while other criminal elements who may become involved have violent (and other) skills they can deploy. These criminals may also be involved in other serious forms of crime in addition to these online enterprises (L1; L3). The more locally situated, the more violent cybercrime could become. Nonetheless, we cannot suggest that Romanian cybercrime currently sees

violence on the level of drug cartels and mafias in other countries. In fact, some interview subjects maintained that a number of offenders are quiet/intelligent individuals who often steer clear of violence and downplayed the involvement of broader organized crime (LV2; L2; L4).

One element that warrants further investigation is whether corruption is also regionally distributed, and how this relates to the regional distribution of cybercrime. A 2013 study by Oana Borcan shows that Quality of Government (QoG) is much higher in the 'Nord Vest' region of the country than in the Bucharest region. In relation to Râmnicu Vâlcea, earlier work has suggested that there is greater distrust of institutions in the southern regions of the country (Borcan, 2013, p. 6). The most recent data (2013) from the QoG EU Regional dataset[7] lists the 'Sud-Vest Oltenia' region, which contains Vâlcea county, with the third highest score on corruption out of the eight regions. This suggests an ostensible connection with cybercrime, but it should be noted that all the eight regions across Romania had quite high corruption ratings, and some reordering could quite easily occur. The presence of corruption is but one of a number of important elements that might encourage cybercrime, and we would not expect that those regions with the highest corruption measures would necessarily translate into having the highest levels of cybercrime.

It should be noted that media and police attention on Romanian cybercrime has been high. As Table 3 shows, many cases have been investigated and prosecuted in Piteşti and beyond. Romania has taken steps to both reduce corruption and increase capacity in the area of cybercrime (L1, L2; Macdowall 2016). At a more personal level, a number of those interviewed for this study appeared to be upstanding officials and investigators, with some directly expressing dissatisfaction with the presence of corruption. There is little doubt that corruption remains a major challenge for the country, but its position has slightly improved in the TI Corruption Percetion Index, moving from 44 in 2012 to 48 in 2016. There has also been international police cooperation. The USA has law enforcement agents stationed in the country, while others make regular visits. Romanian agents are posted to international cybercrime investigation hubs like Europol and the National Cyber-Forensics & Training Alliance in Pittsburgh where they can liaise on international cases and improve their craft. In the private sector, companies like eBay have also contributed to investigations on the ground in Romania. There have been both public and private sector training programmes to increase capacity in this area (see Wylie, 2007). Overall, as noted by some of our interviewees, a degree of progress is being made in the fight against cybercrime (L1, L2).

The local dimension of cybercrime: research and policy implications

Cybercrime has important offline and local dimensions, alongside the online component. In some instances, large-scale cybercrime thrives thanks to offline social networks. As the Romanian case suggests, cybercriminals often choose to work with those who are from the same school, neighbourhood or have other connections. Trust seems to be enhanced in these cases and newcomers can then learn the trade. The second way in which social networks enhance cybercrime is through protection. In places where the local institutions are weak and corruption is widespread, cybercriminals make payments to corrupt officials or rely on influential acquaintances in their circle to protect them. Then they have less worry about arrest and can operate more openly. Over time, collaboration between individuals who have a proclivity for violence and those who have technical expertise might further develop, leading to locally entrenched organized crime groups performing multiple tasks,

[7] Available at: http://qog.pol.gu.se/data/datadownloads/qogeuregionaldata.

including cybercrime. The lack of effective enforcement is a vital factor affecting the growth of cyber-related illegal enterprises. Greater transparency in local contexts appears to be a fundamental element in controlling cybercrime.

These points do not relate only to the case of Romania (see, for instance, Lusthaus, 2016, pp. 24–31; Leukfeldt, 2014; Leukfeldt *et al.*, 2017). The offline and local dimension of cybercrime appears to be present in a number of jurisdictions, across both hi-tech and low-tech offenders. Given it shares some factors identified in this article, such as corruption and the technical and economic legacy of communism, it is not surprising that Eastern Europe is a highly conducive environment for cybercrime. According to one study, the number of Russian underground forums grows every year. As of 2015, 78 websites are operating and popular forums 'can have 20,000 to several hundreds of unique members' (Goncharov, 2015, p. 7). Within this environment, certain Russian-speaking cybercriminals seem to know each other personally. When Nikolai ('Kolya') McColo, an important player in the underground cybercriminal economy, died in car accident in 2007, a number of Moscow-based spammers attended his funeral (Krebs, 2014, p. 3). CarderPlanet, one of the early online marketplaces that came into existence at the turn of the millennium, was led by a young Ukrainian 'carder' called Script. Members of the network met in person on a number of occasions. Odessa, a criminal hub and Script's hometown, served as the meeting point on at least two occasions where conferences in 2001 and 2002 were held to discuss the creation and running of the website (Poulsen, 2011, pp. 73–74; Glenny, 2011, pp. 66–67). Some cybercriminals also work with each other, locally, on a regular basis. This ranges from small-scale 'crews' up to company like structures (Lusthaus, 2016, pp. 1–2; Lusthaus, forthcoming). Like Romania, in some locations, offline collaboration seems to be the primary form of cybercriminal organization. This has been the case with Nigerians, who in earlier days operated their scams out of Internet cafes (Smith 2010).

Our offline/local contention in relation to cybercrime mirrors broader debates on the nature of organized crime (see, e.g. Varese 2010, 2014; Campana, 2011, 2013; Fijnaut, 2016). Some scholars have argued that organized crime and mafia-type groups are 'liquid', able to exploit opportunities around the world, and move easily outside of their territory of origin (see Castells, 2000; Williams, 2001; Shelley, 1999, 2006). Others have pointed out that organized criminal enterprises are 'local in scope' (Reuter, 1985, p. 21; Gambetta 1993). A study on the ability of mafia groups to move outside of their traditional territory has shown that mafias are also local in scope and bounded within a certain domain. When they move jurisdictions, this is often the result of unintended processes—such as flight from arrest—rather than a desire by the leadership to colonize new locations (Varese, 2011). This case study on Romanian cybercrime, supports this latter view.

The policy implications of the offline/local element of cybercrime are clear. While the victims can be thousands of kilometres away and surely need to be vigilant, cybercrime also needs to be tackled in the places where it originates. The Romanian example potentially offers a way forward. After the country, and specific locations within it, were noticed as a major cyber fraud hub, both Romania and others have taken action. Successful relationships have been developed with foreign law enforcement agencies and companies. Manpower and resources have been allocated to the problem, including locating investigators on the ground. Training programmes have been run to increase law enforcement and prosecutorial capacity in this area. The effectiveness of these approaches would benefit from greater study and assessment, not only to evaluate how successful they have been in Romania, but also how they might be adapted successfully to other jurisdictions.

Tackling cybercrime at its roots appears to depend on good local law enforcement and effective governance in those countries where cybercriminals reside. While the investigations mentioned above, along with Romania's TI rating, suggest corruption remains a significant challenge, the fact that such investigations and prosecutions continue to occur is a good sign. It seems sensible to continue and expand ongoing international/cooperative efforts to improve capacity and promote good governance in jurisidictions where cybercrime is rife. The countries where the victims reside—such as the USA, UK, and elsewhere—cannot win this fight alone. But the countries producing large amounts of cybercrime, also need assistance in carrying out this fight on the ground.

Acknowledgements

The authors are listed in alphabetical order. This paper is adapted from a preliminary presentation: Varese, F. (2015). The local dimension of cybercrime: report from a trip to Râmnicu Vâlcea (Romania), presented at the BKA 8th Research Conference on Organised Crime, Mainz, Germany, 7 - 8 October 2015, and printed in: Töttel, U., Bulanova-Hristova, G., and Flach, G. (eds) (2016). *Research Conferences on Organised Crime at the Bundeskriminalamt in Germany*, vol. III, 2013-2015, Wiesbaden: BKA, pp. 163-172.

We are grateful to the Referees and to the Editors of *Policing* for their comments and suggestions. We also thank Paolo Campana in this regard, as well as Oana Borcan for her advice on Romanian corruption data. The John Fell Fund, University of Oxford, supported the March 2015 trip to Romania (grant no. 141/069; 19-27.III.2015). An allowance from Nuffield College, Oxford supported the September 2014 trip. The Commonwealth Bank of Australia generously sponsored Lusthaus' post during the period when this article was written. We greatly thank those who provided advice and help in carrying out our research in Romania. Finally, we are indebted to our participants, who generously gave of their time and knowledge.

References

Akamai. (2016). 'State of the Internet', Q3. Available at: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q3-2016-state-of-the-internet-connectivity-report.pdf/ (accessed 25 May 2017).

Bhattacharjee, Y. (2011). How a remote town in Romania has become cybercrime central. *Wired Magazine*, 31 January 2011.

Borcan, O. (2013) 'Variation in Sub-National QoG in Romania'. In Charron, N., Lapuente, V. and Rothstein, B. (eds), *Quality of Government and Corruption from a European Perspective*. Cheltenham: Edward Elgar, pp. 200-221.

Bran, M. (2011). 'Les pirates roumains d' "Hackerville" tiennent tête aux polices du monde entire'. *Le Monde*, 28 December 2011.

Campana, P. (2011). 'Eavesdropping on the Mob: the functional diversification of Mafia activities across territories'. *European Journal of Criminology* **8**(3): 213–228.

Campana, P. (2013). 'Understanding then responding to Italian organised crime operations across territories'. *Policing* **7**(3): 316–325.

Castells, M. (2000). *End of Millenium*. Oxford: Blackwell.

Coleman, A. (2014). 'Europe's Hidden Entrepreneurial Tech Hotbed; Romania Powers Up'. *Forbes*. https://www.forbes.com/sites/alisoncoleman/2014/03/27/europes-hidden-entrepreneurial-tech-hotbed-romania-powers-up/#fd6ef3f3fa3f/ (accessed 25 May 2017).

Décary-Hétu, D. and Dupont, B. (2013). 'Reputation in a Dark Network of Online Criminals'. *Global Crime* **14** (2–3): 175–196.

Ferrell, J. and Hamm, M. (eds) (1998). *Ethnography at the Edge: Crime, Deviance, and Field Research*. Boston: Northeastern University Press.

Fijnaut, C. (2016). The Local Dimension in the Containment of International Organised Crime: The Dutch Example. In Töttel, U., Bulanova-Hristova, G., and Flach, G. (eds). *Research Conferences on Organised Crime at the Bundeskriminalamt in Germany*, vol. III, 2010–2015. Wiesbaden: BKA, pp. 149–162.

Gabrys, E. (2002). 'The International Dimensions of Cyber-Crime, Part 1'. *Information Systems Security* **11**(4): 21–32.

Gambetta, D. (1993). *The Sicilian Mafia: The Business of Private Protection*. Cambridge and London: Harvard University Press.

Ghidovăţ, G., and Cana, P. (2014). Povestea primului român pe capul cărui FBI a pus o recompensă de UN MILION de dolari. Cum a fost fentată Politia de CEL MAI CĂUTAT

hacker din lume. *Evz.ro*, 22 November 2014. http://www.evz.ro/povestea-cautat-infractor-roman-fentata-politia-hackerul-capul-caruia-fbi-milion-de-dolari.html/ (accessed 25 May 2017).

Glenny, M. (2011). *DarkMarket: CyberThieves, CyberCops and You*. London: Bodley Head.

Grabosky, P. (2004). 'The Global Dimension of Cybercrime'. *Global Crime* **6**(1): 146–157.

Hall, A. (2014). 'The Scourge of Scamville: Romanian Town is the Cyber-Crime Capital of the World - Where Hundreds of Fraudsters Rake in Millions From Gullible Online Shoppers'. *Daily Mail* 21 November.

Hamill, H. (2011). *The Hoods: Crime and Punishment in Belfast*. Princeton and Oxford: Princeton University Press.

Heeks, R. and Grundey, M. (2004). 'Romania's Hardware and Software Industry: Building IT Policy and Capabilities in a Transitional Economy'. In Coopey, R. (ed.), *Information Technology Policy: An International History*. Oxford: Oxford University Press, pp. 187–208.

Holt, T. and Lampke, E. (2010). 'Exploring Stolen Data Markets Online: Products and Market Forces'. *Criminal Justice Studies* **23**(1): 33–50.

Hutchings, A., and Holt, T. (2015). 'A Crime Script Analysis of the Online Stolen Data Market'. *British Journal of Criminology* **55**(3): 596–614.

INS-RV (Institutul National de Statistică, Directia Judeteană de Statistică Vâlcea) (2014). *Anuarul Statistical Judetului Vâlcea* 2014.

Jurnalul National (2014). Primarul din Râmnicu Vâlcea, Emilian Frâncu, condamnat definitiv la 4 ani de închisoare cu executare. *Jurnalul National*, 26 March 2014.

Krebs, B. (2014). *Spam Nation: The Inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door*. Naperville: Sourcebooks.

Leukfeldt, E. R. (2014). 'Cybercrime and Social Ties. Phishing in Amsterdam'. *Trends in Organized Crime* **17**(4): 231–249.

Leukfeldt, E. R., Kleemans, E. R., and Stol, W. P. (2017). 'Cybercriminal Networks, Social Ties And Online Forums: Social Ties Versus Digital Ties Within Phishing And Malware Networks'. *British Journal of Criminology* **57**(3): 704–722.

Lusthaus, J. (forthcoming). *Cybercrime: The Industry of Anonymity*. Cambridge and London: Harvard University Press.

Lusthaus, J. (2016). 'Honour Among (Cyber)thieves?'. *Extra Legal Governance Institute Working Paper* 1, University of Oxford.

Lusthaus, J. (2013). 'How Organised is Organised Cybercrime?'. *Global Crime* **14**(1): 52–60.

Macdowall, A. (2016). 'The DNA of Romania's Anti-Corruption Success'. *Politico*, 15 April 2016. Available at: http://www.politico.eu/article/the-dna-of-romanias-anti-corruption-success-eu-transparency-international/. (accessed 25 May 2017).

Maher, L. (1997). *Sexed Work: Gender, Race, and Resistance in a Brooklyn Drug Market*. Oxford: Clarendon Press.

Miercuri (2015). 'Senatorul PSD Laurentiu Coca implicat în afaceri cu Labuş'. *Miercuri*, 14 January 2015.

Odobescu, V. (2014). 'U.S. Data Thefts Turn Spotlight on Romania'. *USA Today*, 13 January 2014.

Popescu, L. (2017). 'Actiunile Oltchim, Conted şi Armătura au cele mai slabe evolutii în trimestrul 1'. *ZF* , 7 April 2017. http://www.zf.ro/burse-fonduri-mutuale/actiunile-oltchim-conted-si-armatura-au-cele-mai-slabe-evolutii-in-trimestrul-1-16224528/ (accessed 25 May 2017).

Poulsen, K. (2011). *Kingpin*. New York: Crown Publishers.

Reagans, R. and McEvily, B. (2003). 'Network Structure and Knowledge Transfer: The Effects of Cohesion And Range'. *Administrative Science Quarterly* **48**(2): 240–267.

Reuter, P. (1985). *The Organization of Illegal Markets: An Economic Analysis*. New York: U.S. National Institute of Justice.

Rîpan, I. (2015). 'Caz inedit în politia vâlceană: Alexandru George Popa, primul politist arestat la domiciliu pentru 30 de zile'. *Adevarul.ro*, 21 March 2015.

Romania Insider. (2016). 'Romania's Biggest Chemical Plant Will Be Sold By Piece'. *Romania Insider*, 25 August. Available at: http://www.romania-insider.com/romanias-biggest-chemical-plant-will-sold-piece/ (accessed 25 May 2017).

Sanchez-Jankowski, M. (1991). *Islands in the Street*. Berkley and Oxford: University of California Press.

Shelley, L. (1999). 'Identifying, Counting and Categorizing Transnational Criminal Organizations'. *Transnational Organized Crime* **5**(1): 18–157.

Shelley, L. (2006). 'The Globalization of Crime and Terrorism'. *eJournal USA* **11**(1): 42–45. Available at http://www.america.gov/media/pdf/ejs/ijge0206.pdf#popup/ (accessed 25 May 2017).

Smith, D. J. (2010). *A Culture of Corruption: Everyday Deception and Popular Discontent in Nigeria*. Princeton: Princeton University Press.

Smith-Doerr, L. and Powell, W. W. (2005). 'Networks and economic life'. In Smelser, N. J. and Swedberg, R. (eds.) *The Handbook of Economic Sociology*. Princeton and Oxford: Princeton University Press, pp. 379–402.

Subramanian, S. (2017). 'Inside the Macedonian Fake-News Complex'. *Wired Magazine*, 15 February. https://www.wired.com/2017/02/veles-macedonia-fake-news/ (accessed 25 May 2017).

Varese, F. (2010) 'General introduction: What is organized crime?'. In Varese F. (ed.), *Organized Crime*, Vol. 1. London and New York: Routledge.

Varese, F. (2011). *Mafias on the Move*. Princeton, N.J.: Princeton Universy Press.

Varese, F. (2014) 'Protection and extortion'. In Paoli L. (ed.), *The Oxford Handbook of Organized Crime* (Oxford and New York: OUP, pp. 343–58).

Venkatesh, S. (1997). 'The Social Organization of Street Gang Activity in an Urban Ghetto'. *American Journal of Sociology* **103**(1): 82–111.

Wall, D. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press.

Williams, P. (2001) 'Transnational criminal networks'. In Arquilla, J., Ronfeldt, D. F. (eds), *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Washington, DC: Rand Corporation, pp. 61–97.

Wittkop, J. (2016). *Building a Comprehensive IT Security Program: Practical Guidelines and Best Practices*. New York: Apress.

Wylie, I. (2007). 'Romania home base for eBay scammers'. *Los Angeles Times*, 26 December 2007.