Is the Mafia Taking Over Cybercrime?*

Jonathan Lusthaus
Director of the Human Cybercriminal Project
Department of Sociology
University of Oxford

* This paper is adapted from Jonathan Lusthaus, *Industry of Anonymity: Inside the Business of Cybercrime* (Cambridge, Mass. & London: Harvard University Press, 2018).

1. Introduction

Claims abound that the Mafia is not only getting involved in cybercrime, but taking a leading role in the enterprise. One can find such arguments regularly in media articles and on blogs, with a number of broad quotes on this subject, including that: the "Mafia, which has been using the internet as a communication vehicle for some time, is using it increasingly as a resource for carrying out mass identity theft and financial fraud".[1] Others prescribe a central role to the Russian mafia in particular: "The Russian Mafia are the most prolific cybercriminals in the world".[2] Discussions and interviews with members of the information security industry suggest such views are commonly held. But strong empirical evidence is rarely provided on these points. Unfortunately, the issue is not dealt with in a much better fashion by the academic literature with a distinct lack of data.[3]

In some sense, the view that mafias and organised crime groups (OCGs) play an important role in cybercrime has become a relatively mainstream position. But what evidence actually exists to support such claims? Drawing on a broader 7-year study into the organisation of cybercrime, this paper evaluates whether the Mafia is in fact taking over cybercrime, or whether the structure of the cybercriminal underground is something new. It brings serious empirical rigor to a question where such evidence is often lacking. This analysis is based on 238 interviews with law enforcement, the private sector and former cybercriminals. These were carried out in some 20 countries, including fieldwork in purported cybercrime "hotspots" like Russia, Ukraine, Romania, Nigeria, Brazil, China and the United States. Throughout this paper, participant identities are anonymised; any names used are randomly chosen pseudonyms.

This paper proceeds in four sections. First, it provides definitions for mafias and OCGs, including the so-called "Russian Mafia". Second, it outlines key findings from the data as to what roles such organised crime groups do play in cybercrime. Third, it suggests that a new class of criminal entrepreneurs, rather than mobsters, are driving the cybercrime business. Finally, it discusses potential policy proposals for addressing the challenge.

2. Defining Mafias and Organised Crime (OC)

It is important to note that there is an established academic discourse on mafias and organised crime. There are varying approaches, but this paper focuses on a school of scholars that provides a particularly tight set of definitions of the phenomena. For these writers, organised crime, including mafias, is tied to the concept of *governance*. Thomas Schelling, the Nobel Prize winning economist, argues that organised crime is not simply "crime that is organized".[4] In explaining his approach, Schelling provides the famous account of why organised burglars do not fall into the category of organised crime:

> burglars are never reported to be fighting each other in gangs for exclusive control over their hunting grounds. Burglars are

> busy about their burglary, not staking claims and fighting off other burglars. It is when a gang of burglars begins to police their territory against the invasion of other gangs of burglars, and makes interloping burglars join up and share their loot or get out of town, and collectively negotiates with the police not only for their own security but to enlist the police in the war against rival burglar gangs or nonjoining mavericks, that we should, I believe, begin to identify the burglary gang as organized crime.[5]

In this conception, genuine organised crime groups attempt to regulate and control some form of illegal industry. This approach is central to definitions of organised crime and mafias that Varese settles on, after surveying the range of definitions that has been applied to the subject.[6] For Varese, an *organised crime group* "attempts to regulate and control the production and distribution of a given commodity or service unlawfully". Following Gambetta,[7] Varese defines a *mafia* as an organised crime group that "attempts to control the supply of protection".[8] In effect, a mafia desires to govern all criminal markets.

Empirical evidence on the topic supports this governance-centric approach. Henry Hill, the mobster who was the inspiration for Martin Scorsese's film *Goodfellas*, provides a street level definition of the mafia. Hill explains the function of Paul Vario, the Lucchese crime family *Capo* (captain) in the neighbourhood:

> The guys who worked for Paulie had to make their own dollar. All they got from Paulie was protection from other guys looking to rip them off. That's what it's all about. That's what the FBI can never understand – that what Paulie and the organization offer is protection for the kinds of guys who can't go to the cops. They're like the police department for wiseguys.[9]

This type of protective behaviour has been observed across a number of different groups in different jurisdictions, from the Sicilian Mafia, to the Italian American Mafia, the Triads and the Yakuza.[10]

When discussing cybercrime, one mafia group in particular attracts attention. This is the so-called "Russian Mafia" – though in reality it is now better referred to as the post-Soviet Mafia as it spans a number of countries in the region. While some have a tendency to ascribe any serious criminality in the region to this group, in many cases the culprits are Eastern European but not necessarily members of this mafia. The Russian Mafia rose during the fall of the Soviet Union. As the free market emerged, the need to protect property rights and enforce agreements became a serious concern. With a weakened and chaotic state, strong men emerged to fill this void. Some were former military or intelligence officers; others were wrestlers and sportsmen. But a core component was the *vory v zakone* (thieves in law), a criminal fraternity that originated within the Soviet gulag system but expanded its reach and cultural influence across the broader underworld. The vory have a clear hierarchy,

are bound by a code of rules, and are often identified by their distinctive tattoos. Membership of the group is tightly vetted, and new bosses must go through a "crowning" ritual, where they take on a new name, to gain formal entry. These mafia members belong to a distinct organisation and can be clearly distinguished from other run-of-the-mill criminals in the region.[11] Despite this, many discussions of cybercrime and the mafia fail to acknowledge the specificity involved here.

The next section of this paper assesses what evidence there is for the post-Soviet mafia and other organised crime groups playing a role in cybercrime. Given the definitional issues discussed above, it is focused on traditional groups that attempt to govern the underworld or a part of it, rather than criminal groups that might be organised but are not formally "organised crime".

3. Key Findings

Many participants in this study believed that organised crime involvement in cybercrime was substantial. But when pressed, this appeared to be a theoretical rather than empirical view. A common formulation was that organised crime moves to where the money is and the money is now in cybercrime. So that is where, logically, they would involve themselves. But when participants were asked whether they had directly seen a case of a traditional organised crime group involved in cybercrime, relatively few answered affirmatively. Many of those who had seen such cases, often described only a small number and/or provided limitations on the OC involvement. As such, the data collected for this project suggests that organised crime does play a role in cybercrime, but that its involvement is far from a complete takeover. There are four key roles that organised criminals can play in cybercrime, which are largely tied to their existing skillsets and resources: protector; investor; service provider; guiding hand.

3.1 Protector

On the question of whether organised crime groups are supplying protection to cybercriminals, there is some evidence but it is not overwhelming. Like any other criminals, if cybercriminals are known to make large amounts of money they may become vulnerable to theft/extortion, both from the criminal community and corrupt law enforcement.[12] Or, they may need a protector against legitimate investigations.[13] If they are collaborating in their enterprises with other local (cyber)criminals, they may also require arrangements to be enforced by a "trustworthy" local mobster. Otherwise they might need assistance in keeping out local competitors.

Possibly the closest example of this is found in Brian Krebs' book *Spam Nation.* Krebs recounts the early history of the famed Russian Business Network and a rare instance of violent behaviour between cybercrime competitors. At the heart of this history is Alexander Rubatsky, a talented programmer who became involved in a number of aspects of cybercrime, including payment processing for child sexual abuse material sites. Rubatsky ran a technical team to assist his operations, but was

also supported by heavies, associated with the “The Village” organised crime group in Minsk, who provided a form of protection.[14] Krebs describes how the group dealt with a rival businessman named Evgeny Petrovsky who was developing his own credit card processing business focussed on child sexual abuse material sites:

> Petrovsky was stopped in his car by a man posing as a local policeman, and when he stepped out of the car as directed, he was kidnapped by masked men. Once they reached their safe house in the outskirts of Minsk, the abductors contacted Petrovsky’s associates and demanded a million U.S. dollars for his safe return. But no money would be forthcoming. When local authorities began to close in on their location, the assailants fled with Petrovsky to Moscow. By November 2012, Russian and Belarusian authorities had located the Loginov gang’s hideout and the rest of the kidnappers. They found Petrovsky alive and relatively unharmed.[15]

Despite such examples, there are many cases where organised crime protection was not evident. A number of interviewees in Romania believed that offenders there are often quiet, intelligent, non-violent and unconnected to OCGs.[16] In the Nigerian context, Idris also believed that it was very unusual for cybercriminals to be paying protection racketeers.[17] Former cybercriminal Andrey did not think there was an especially strong association between cybercrime and Eastern European organised crime, writing:

> All the relations between traditional mafia and gangs are eventual and personal, so there's no more connections than in any other industry or enterprise. Some individuals do, and if they do, they use it. Others don't. There are various individuals with different backgrounds, some came from "IT" world to carding, other from world of crime. Of course, regular criminals show interest in certain aspects of cybercrime, but they show interest in many other things. More advanced carders and hackers, however, usually show strong disgust to "traditional" criminals and usually join whatever cause there might be on temporary basis. In turn, "traditional" criminals often regard cybercriminals as "milk cows" and nerds.[18]

Another former Eastern European cybercriminal, Ivan, stated that he had never encountered a direct connection between cybercriminals and traditional organised crime groups.[19] In a South American context, Thiago said that he and his collaborators never engaged with organised criminals, and actively avoided them.[20]

Much stronger empirical support was actually found for the involvement of organised crime groups in cybercrime outside of providing protection. In other words, rather than seeking to govern cybercrime, those organised criminals who became involved in the industry were much more likely to play a role within it.

3.2 Investor

The second role organised crime groups play in cybercrime is by acting as investors in certain enterprises. This requires little specialist knowledge from the organised criminals involved. They only need to make contact with a cybercriminal group and have a pool of capital available from other operations. In practice, my data did not suggest too many pure instances of investment, but it did happen. Perhaps the best example was provided by former UK law enforcement agent, Peter, who recounted a case of a group involved in credit card fraud, which he described as being on an "industrial" scale. The information on the case was sensitive so, according to Peter's wishes I provide limited details here. The scheme involved hiring a programmer to develop software to access the card details from banks, and there were significant upfront costs for this. As a result, Peter believed the boss of the group sought the backing of a well-established British organised crime group to bankroll the operation. But following a falling out, the cybercriminal's life was later threatened by them and he had to go on the run.[21]

3.3 Service Provider

The third role that OCGs play within cybercrime is to use their traditional expertise in money laundering and their ability to physically enforce group arrangements as service providers to, or partners of, broader cybercrime operations. The money side of cybercrime is the part that often requires offline groups of people to collect/send money, buy merchandise with stolen proceeds or launder the gains. While there are many instances of this activity being carried out by groups that are not connected to traditional organised crime,[22] monitoring/enforcing this process is a plausible point of organised crime involvement.[23] The collected data confirms this supposition with OCGs somewhat regularly appearing within this role. Perhaps the most famous case of this was the Citibank hack of 1994 involving Vladimir Levin who managed to infiltrate the bank's networks and arrange for a number of illicit money transfers worth millions of dollars. According to Nathan, a former US law enforcement agent, it was the Tambov Gang, a leading Russian mafia group in St Petersburg, which was responsible for financing and overseeing the movement of the proceeds back to Russia. This involved a substantial network of people to receive and move the money operating in different countries around the world, including the US, Israel and Holland. The gang made use of coercion and threats of violence to enforce compliance, particularly when arrests were made. In one case, they paid the legal fees of an arrested member of the group. In another case, they attempted to murder a gang member whose wife had been arrested and who had begun cooperating with the authorities. Likely having some form of political protection themselves, the organised criminals at the top of the scheme could avoid gaol time in Russia.[24]

This type of activity continued to be relevant into the 21st Century. Former Eastern European cybercriminal, Leonid, knew of a number of organised criminals involved in cybercrime. From his account, the key pathway appeared to be adapting their traditional skillset to be of value to the carding community.[25] This accorded with

Jack's experience, who had investigated cases of groups that smuggled card skimmers and "white plastic" between Eastern and Western Europe.[26] White plastic are the blank cards that can be encoded with stolen data and then used in shops or at ATMs. The Turkish cybercriminal Chao was also heavily involved in the skimming business, as a key vendor of the required hardware on DarkMarket with a production line in China and a large number of underlings. Though he may not have been a traditional mobster, he certainly styled himself as one.[27]

3.4 Guiding Hand

The fourth role that organised criminals play in cybercrime is by directly getting involved and acting as the guiding hand of certain operations. This usually involves recruiting those with technical skills, among others, to carry out the jobs.[28] One of the best examples of this phenomenon was the failed Sumitomo heist in 2006 where £229 million was almost stolen from the bank. In this case, two men were let into the bank's premises in London by a security supervisor. One man was a hacker, the other his overseer. While they failed to successfully carry out the plan, their goal was to install key logging software on the computers and then return to carry out fraudulent bank transfers.[29] This plot involved a global network of conspirators, but according to former law enforcement agent, Phillip, an OCG in London and another group on the continent played a central role in carrying out the scheme. He believed that they coordinated and recruited the various actors and oversaw the operation. Phillip did not want to name the groups as they were "ominous people".[30]

Such involvement by OCGs, effectively as the recruiter/coordinator, was the connection between organised crime and cybercrime most commonly reported by former cybercriminals. Former Southeast Asian cybercriminal, Tan, wrote about being approached by organised criminals involved in a range of illicit activities: drugs, money laundering, nightclubs, political corruption and real estate. They hoped that he would take a monthly salary and other benefits to oversee their stolen credit card business. He told them he preferred to be "my own boss".[31] In his later life as a security professional, another former cybercriminal from the region, Ahmed, has been approached by a number of people seeking his services, which he regularly turns down. In one case, a local drug dealer connected to a major syndicate was interested in hiring him to gather intelligence on specific individuals (most likely competitors) by hacking them.[32] Casper, a Western European hacker was approached by what he called "real criminals, very big criminals". The criminals flew in to meet Casper and treated him very well in the hopes of wooing him to become involved in their criminal activities. This included a major jewelry heist in Europe, where he was to hack the alarm system of the target site. Casper politely declined the proposal.[33]

3.5 Complexities

These last two roles are essentially two sides of the same coin. In both cases OCGs make use of their traditional skills on the money side and/or enforcing arrangements, but leave the technical elements of the job to others. Which category

the activity fits into depends on whether those with technical skills approach the OCGs to assist with cashing out, or whether the organised crime groups look to bring in technical talent for their own scam. Sometimes it may be difficult to tell which is the case.

A number of these connections between OCGs and cybercrime discussed above may also tend towards a fifth category of organised crime involvement, but which may be outside the scope of cybercrime. In these cases, OCGs seek to recruit or partner with technical talent in order to enhance their existing operations, rather than engaging in cybercrime *per se*. But this all depends on the complex question of how cybercrime itself is defined. Some might view certain examples discussed above as properly fitting into this fifth category. But the data also included many other examples like this: from triads using websites to promote their prostitution services or running virtual gambling operations,[34] to major drug trafficking groups requiring tech support.[35] This is mirrored by publicly known cases, such as the hacking of Antwerp Port discovered in 2013. In this instance, a Netherlands based group hired hackers to compromise the port systems so that containers hiding drugs could be identified and then stolen before they were claimed for their true owner.[36]

4. A New Breed of Criminal

Overall, the collected data suggests some evidence for OC involvement in cybercrime, but that it is far from a takeover. Instead, the data supports the view that cybercrime is driven by a new class of entrepreneurs. Vasily, a former Russian law enforcement agent, viewed things in such a way. His account suggested that there wasn't much space for tech entrepreneurs and startups in the Russian economy, despite a strong supply of educated highly skilled technical talent. When capital is limited and many programmers are poorly paid or underemployed, some are tempted by the dark side. In Vasily's view, mobsters had demonstrated only limited interest in this industry, which was instead driven by a new breed of criminal entrepreneurs.[37] US Law enforcement agent Terry concurred, arguing that it's now very clear that "they are businessmen".[38]

One of the surprising findings from the data was that it is not that common for mafias and OCGs to provide protection for cybercriminals. Instead, it was much more commonly reported that law enforcement agents and political figures were providing this service in exchange for payment or due to another form of relationship.[39] There are probably a number of reasons for this, but one of the most significant is that bent politicians and law enforcement agents are in a much better position to shield cybercriminals from arrest. This appears to be of greatest value to cybercriminals within their local contexts.

5. Big Picture Thinking

The findings in this paper change the way we perceive cybercrime and potentially the ways that we seek to tackle it. If cybercrime is just an OC problem, it suggests something fairly intractable but which is largely a law enforcement challenge. But if

cybercrime is not so much an OC problem, but rather one of underemployed entrepreneurs and programmers, this offers a raft of other potential solutions to divert cybercriminal talent away from the dark side and towards legitimate industry. With appropriate planning, this is something that could be addressed through large governmental initiatives driving start-up capital to affected regions, but also on a smaller scale by individual companies and the hiring choices they make - that is, by actively recruiting from countries that produce a large amount of cybercrime. The findings also suggest that supporting corruption reduction efforts in cybercrime hotspots could aid in fighting the threat. Obviously, these are big picture ideas that are very difficult to carry out in practice. But they are certainly worth investigating further, given the significant challenge that cybercrime poses.

[1] John Blau, "Russia - a Happy Haven for Hackers," ComputerWeekly.com, http://www.computerweekly.com/feature/Russia-a-happy-haven-for-hackers, (2004).
[2] David Goldman, "The Cyber Mafia Has Already Hacked You," CNN Money, http://money.cnn.com/2011/07/27/technology/organized_cybercrime/, (2011).
[3] For similar arguments see David Wall, "Internet Mafias? The Dis-Organisation of Crime on the Internet," in *Organized Crime, Corruption and Crime Prevention*, ed. Stefano Caneppele and Francesco Calderoni (Cham: Springer, 2014); Rob McCusker, "Transnational Organised Cyber Crime: Distinguishing Threat from Reality," *Crime, Law and Social Change* 46, no. 4-5 (2006); Rutger Leukfeldt, Anita Lavorgna, and Edward Kleemans, "Organised Cybercrime or Cybercrime That Is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime," *European Journal on Criminal Policy and Research* (2016).
[4] Thomas Schelling, "What Is the Business of Organized Crime," *Journal of Public Law* 20, no. 1 (1971), p. 72.
[5] "What Is the Business of Organized Crime", p. 74.
[6] Federico Varese, "What Is Organized Crime?," in *Organized Crime: Critical Concepts in Criminology*, ed. Federico Varese (New York: Routledge, 2010).
[7] Diego Gambetta, *The Sicilian Mafia: The Business of Private Protection* (Cambridge and London: Harvard University Press, 1993).
[8] Varese, "What Is Organized Crime?,", pp. 14, 17.
[9] Nicholas Pileggi, *Wiseguy: Life in a Mafia Family* (New York: Pocket Books, Simon & Schuster, 1986), p. 48.
[10] Gambetta, *The Sicilian Mafia: The Business of Private Protection*; Yiu Kong Chu, *The Triads as Business* (London and New York: Routledge, 2000); Peter Hill, *The Japanese Mafia: Yakuza, Law and the State* (Oxford and New York: Oxford University Press, 2003); Federico Varese, *Mafias on the Move* (Princeton and Oxford: Princeton University Press, 2011).
[11] On these points see *The Russian Mafia: Private Protection in a New Market Economy* (Oxford: Oxford University Press, 2001); *Mafia Life* (London: Profile Books, 2017); Vadim Volkov, *Violent Entrepreneurs: The Use of Force in the Making of Russian Capitalism* (Ithaca: Cornell University Press, 2002).
[12] Interview with Irish Cybersecurity Professional 2; Interview with Former US Law Enforcement Agent 8; Interview with Expatriate Cybersecurity Professional Based in the US 1.
[13] Interview with Former Russian Law Enforcement Agent 1.
[14] Brian Krebs, *Spam Nation: The Inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door* (Naperville: Sourcebooks, 2014), pp. 17-24.
[15] *Spam Nation: The Inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door*, p. 20.
[16] Interview with Romanian Law Enforcement Agent 1; Interview with Romanian Prosecutor 1.
[17] Interview with Former Nigerian Law Enforcement Agent 1.
[18] Interview with Former Eastern European Cybercriminal 2.
[19] Interview with Former Eastern European Cybercriminal 3.
[20] Interview with Former South American Cybercriminal 1.

[21] Interview with Former UK Law Enforcement Agent 4.
[22] Interview with Former North American Cybercriminal 2.
[23] Interview with Irish Cybersecurity Professional 2; Interview with Former Russian Law Enforcement Agent 1; Interview with Russian Cybersecurity Professional 3; Interview with Expatriate Cybersecurity Professional Based in the US 1; Interview with UK Law Enforcement Agent 3.
[24] Interview with Former US Law Enforcement Agent 5.
[25] Interview with Former Eastern European Cybercriminal 4.
[26] Interview with US Law Enforcement Agent 3.
[27] Interview with US Law Enforcement Agent 2.
[28] Interview with Irish Cybersecurity Professional 2; Interview with US Cybersecurity Professional 14; Interview with Former Russian Law Enforcement Agent 1.
[29] Felix Lowe, "Sumitomo Mitsui: The Bank That Thwarted the £220 Million Heist," The Telegraph, http://www.telegraph.co.uk/finance/newsbysector/banksandfinance/2792188/Sumitomo-Mitsui-The-bank-that-thwarted-the-220-million-heist.html, (2008).
[30] Interview with Former UK Law Enforcement Agent 2.
[31] Interview with Former Southeast Asian Cybercriminal 2.
[32] Interview with Former Southeast Asian Cybercriminal 1.
[33] Interview with Former Western European Cybercriminal 2.
[34] Interview with Former Hong Kong Law Enforcement Agent 2; Interview with Malaysian Cybersecurity Professional 1; Interview with Malaysian Law Enforcement Agent 3.
[35] Interview with Malaysian Cybersecurity Professional 4.
[36] Jordan Robertson and Michael Riley, "The Mob's It Department," Bloomberg, http://www.bloomberg.com/graphics/2015-mob-technology-consultants-help-drug-traffickers/, (2015).
[37] Interview with Former Russian Law Enforcement Agent 1.
[38] Interview with US Law Enforcement Agent 10.
[39] Interview with Russian Cybersecurity Professional 5; Interview with Russian Cybersecurity Professional 6; Interview with Former Ukrainian Law Enforcement Agent 2; Interview with Former Romanian Law Enforcement Agent 1; Interview with Former US Law Enforcement Agent 6.