[Book review of:] An impressive view on profit driven cybercrime: a review of J. Lusthaus' industry of anonymity

Weulen Kranenbarg, M.

published in
Global Crime
2020

DOI (link to publisher)
10.1080/17440572.2020.1743935

document version
Publisher's PDF, also known as Version of record

Global Crime

Routledge
Taylor & Francis Group

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/fglc20

An impressive view on profit driven cybercrime: a review of J. Lusthaus' industry of anonymity

M. Weulen Kranenbarg

To cite this article: M. Weulen Kranenbarg (2020) An impressive view on profit driven cybercrime: a review of J. Lusthaus' industry of anonymity, Global Crime, 21:3-4, 327-331, DOI: 10.1080/17440572.2020.1743935

To link to this article: https://doi.org/10.1080/17440572.2020.1743935

GLOBAL CRIME
2020, VOL. 21, NOS. 3–4, 327–331

Routledge
Taylor & Francis Group

BOOK REVIEW

An impressive view on profit driven cybercrime: a review of J. Lusthaus' industry of anonymity

With Industry of Anonymity, Jonathan Lusthaus has written a thorough scientific book which reads like a novel and keeps you interested till the end. The empirical work on which this book is based is impressive. By conducting 238 interviews in 20 different countries with cybersecurity professionals, law enforcement officials, and 20 former cybercriminals, Lusthaus has collected unique and extensive data.

I enjoyed both the historical as well as the geographical focus of this book, as it clearly shows the influence of both offline and online developments in specific social contexts. This work empirically shows how this industry may sometimes work differently than one would expect based on popular beliefs. Even though I would definitely recommend reading this book to anyone interested in cybercrime, two aspects of the broad nature of this book should be discussed before reviewing the main findings.

The data-collection was spread over many different countries, but some countries (mainly the UK and the US) were over-represented in the interviews. Additionally, only a few interviews were conducted with criminals. As the book uses the criminals' perspectives extensively and not mainly focusses on the UK and US, the views of some participants may have gotten more weight than others. Additionally, by interviewing only 20 former criminals, the representativeness of their stories is unknown. Nevertheless, basically, every result is backed up with reference to more than one interview, in many cases from different types of respondents.

Furthermore, the author clearly states that the book is about profit-driven and organised cybercrime. On the one hand, this broad category of crime provides a great general picture, on the other hand, it may not provide the full picture for specific crimes. The book sometimes focusses more on hacking, while in other instances it focuses on other cybercrimes. While the book is extensive, it could of course not provide a complete picture. As also suggested by the author in the conclusion, this research therefore generates more questions than answers and future studies should take a more specific approach.

Chapter 1: introduction

The first chapter illustrates how the industry of profit-driven cybercrime emerged. Nowadays, this industry is characterised by a division of labour, professionalisation, (virtual) marketplaces, and organisational structures that resemble legitimate firms. The main question the author asks in this book is how this industry deals with the anonymity that is characteristic of this type of organised crime. The book takes a historic perspective, by looking at the industry's evolution and its current practices.

The rest of the introduction links the research to existing literature. I am glad the author notes some important limitations of the current literature, for example, a focus on forums while these may only be a small part of the industry. The author takes a new perspective by looking at the industry from different data-sources. In the following chapters, this literature is often linked to

This article has been republished with minor changes. These changes do not impact the academic content of the article.

the research results. However, in some cases, I missed links to the literature that would have helped to put the results in a more theoretical or criminological perspective. For example, on page 78–80 where it would have been helpful to provide a developmental perspective on the criminal careers of these people and how they did not develop a legal profession. This could have helped to emphasise the author's conclusion that there is not that much new about cybercrime and many traditional criminological views can help to understand it.

Chapter 2: from lone wolves to industrialisation

The second chapter discusses the evolution of cybercrime. It starts with the more well-known discussion of the evolution of hacking. From curiosity-driven individuals or small groups, to more organised groups with mainly non-financial motives, and finally to profit-driven crime in which some of the original hacking-ethics were abandoned and other criminals and types of crime entered the industry. Afterwards, the author shows how forums have played a vital role in the development of the industry, by providing opportunities to collaborate and develop a division of labour and specialisation with a focus on business. In critical reference to literature that only focusses on these public forums, the chapter shows how more private forums and other types of small-scale hidden communication developed as well. This shows how the forums developed into *'a place to network for those who do not have sufficient contact'* (p. 53), which stresses the added value of this research and its historical perspective.

Afterwards, the author discusses something that will come back many times in the book. The development of firms, in which operational structures of organised cybercrime groups evolved into businesses that sometimes even have a physical office. While it is clear that these firms exist, I personally think that throughout the book the author puts a lot of emphasis on these firms, while it is unclear to what extent these are widespread or more an exception.

In line with the general view in the literature, but based on new and empirical research, the author concludes that nowadays cybercrime is more organised and sophisticated. The technical offenders such as hackers and coders only play one of many roles in the industry. This chapter has focused slightly more on the historical developments instead of the current day industry, which may partially be due to the fact that only former cybercriminals have been interviewed.

Chapter 3: making sense of the cybercrime industry

Following up on the historical perspective, the industry is discussed in further detail in this chapter by addressing specialisation and professionalisation, and by providing more details on cybercriminal markets and firms. What is valuable in this chapter is that it shows how these elements differ between geographical regions. An interesting example is the fact that most technical specialists in these cybercriminal groups are from Eastern Europe, which seems to be linked to its history, job opportunities for technically skilled people, and corruption. The developments in Eastern and Western Europe are contrasted to developments in other countries such as Nigeria and China.

With regard to professionalisation, the chapter briefly discusses ways in which cybercriminals developed into businessmen. Subsequently, the author shows that while cybercriminal markets are important and competitive, these also have downsides. Counter to the ideas from the interviewed law enforcement agents, offenders say that there is a comeback of other smaller and more private means of communication. Lastly, the chapter further details different ways in which cybercriminals work together. It discusses firms, but also provides the full spectrum of collaborative networks and acknowledges that some offenders may not be part of a network at all.

Chapter 4: nicknames and identity

Now that the history and current industry is described, the following chapters examine how it could develop despite its anonymity. By first focusing on nicknames, it becomes apparent that anonymity is as much a cost as it is a benefit. It is helpful in preventing criminal conviction but also makes it difficult to evaluate the trustworthiness of collaborators. While the use of nicknames in cybercrime is widely known, it is usually just a given fact instead of the focus of the literature. Therefore, it is good to see a chapter with in-depth information on how these nicknames are chosen and used. It shows that nicknames are vital in building a criminal brand with an anonymous identity.

The most important part of the chapter discusses the difficulties in balancing the establishment of a brand by having the same nickname over a long period, while also preventing law enforcement from linking criminal activities to one's real identity. The chapter shows how offenders adopt widely different methods in using their nicknames. Most offenders have multiple nicknames in different settings. Others change their nicknames very often, while some stick to one name for as long as they can. It should be noted that this chapter seems a bit anecdotal, especially the part on interpreting nicknames, but it is nevertheless a very informative story on something that is usually overlooked.

Chapter 5: how cybercriminals cooperate online

Now that it is clear how a cybercriminal could identify a co-offender; this chapter is discussing elements of traditional organised crime and how cybercriminals establish these elements in the online anonymous context. Trustworthiness it the most important element discussed here. Cybercriminals evaluate the trustworthiness of co-offenders by looking at appearance, performance and reputation. The general idea behind it is that if a person has invested in a reputation using appearance and performance, that person will be less likely to rip you off as that jeopardises the investments. Forums have institutionalised these mechanisms of trust, which means that by using a forum it takes less time to find reliable co-offenders. However, the interviews suggest that these mechanisms may not be as reliable as they seem, and offenders seem to prefer personal reviews or referrals.

While there are many tactics to assess the trustworthiness of others, disputes between two co-offenders still occur because of anonymity. Therefore, the industry developed ways to enforce rules and agreements. A main point the author makes is that criminals use several digital forms of violence such as doxing or swatting, but these tactics are not as strong as the ways in which offline organised criminals use violence. Information plays a key role in the strategies of cybercriminals, as they tend to collect personal information about their co-offenders which could expose their co-offenders to great risks. Additionally, forums have developed institutions to deal with disputes and there are even third parties who are trying to prevent and mediate disputes. This research shows how these third parties are the most trusted criminals in the industry. While these forums seem to have an important role in providing protection, the author further argues that forums cannot fully monopolise protection (in ways in which the Mafia does).

Lastly, the chapter discusses how offenders may simply accept the risk of being ripped off by a co-offender every once in a while, as the benefits are much higher than the risks or costs. Interestingly the author also looked at situations in which cooperation between offenders seems to fail. It shows how offenders will scam each other if the risks for retribution are low. At this point, the author shows the value of the historical perspective by showing how the current move towards smaller and more private groups is similar to observations from the past. This

would indicate that problems with anonymity and trustworthiness still exist, which limits the cooperation between offenders.

Chapter 6: the offline dimension

The previous chapter showed how cybercriminals cannot overcome all anonymity issues. This is why in some cases there may be an important offline dimension in cybercrime. Many of the issues with anonymity are not present in the offline world. The author provides many different offline aspects of cybercrime, but the most valuable is the increased opportunities for enforcement. In my opinion, it seems that this offline dimension should not be overlooked, but the extent to which it plays a role will largely depends on the geographical location of the offender group and the type of activities they employ. In this chapter, the author convincingly links the benefits of offline interactions to all the online limitations discussed in the previous chapters. Therefore, this chapter is very valuable in providing a different perspective on the field of cybercrime. On the other hand, the author shows how many criminals just accept the problems with online criminal collaboration, as they value anonymity and prefer not to have any offline interactions with others.

Chapter 7: cybercrime, organised crime, and governance

Finally, this chapter explains how this offline dimension also results in opportunities for governance. First of all, the firms discussed earlier can have much more control over the business in the offline world. More importantly, the chapter discusses how offline organised crime groups can get involved. In contrast to popular beliefs, the empirical work shows that while these groups are getting involved, they are only a small part and they are not taking over the full industry. They simply provide their services such as protection, investments, and skills such as money laundering. Interestingly, the most common involvement of traditional organised crime is if they hire criminals with technical skills when needed for their traditional businesses, for example, to build a prostitution website.

In addition to the limited role of organised crime, corrupt government agents seem to play a more important role in governance, specifically in regions where officials are paid poorly. As the former Soviet Union plays such a vital role in the industry, the chapter zooms into the role of corruption in this region. It shows how corruption is institutionalised and such a normal part of daily life in these countries, that it clearly explains why cybercrime is so prevalent in these countries.

The chapter's conclusion that offline protection is central to the cybercrime industry is a bit too strong in my opinion, as there are many regions in which the discussed mechanisms do not play a role. Nevertheless, this chapter clearly shows why some regions are more involved in cybercrime than others.

Chapter 8: conclusion

Overall, it was a pleasure to read this book and Lusthaus succeeded in showing how good scientific research can provide a different view on common beliefs about the cybercrime industry, such as the value of anonymity and the role of organised crime groups. After providing an overview of the findings in the conclusion, the author discusses implications for policing this industry. This author shows how law enforcement opportunities may seem limited if you look at the direct effect of their actions, but it may have an important deterring

effect that limits the behaviour of cybercriminals. Unfortunately, is very hard to empirically assess the effect of law enforce on the industry.

More important and interesting is the authors view on the importance of countering unemployment and corruption, which is largely based on the fact that these seem to be more present in the regions where most cybercrime comes from. I especially like the following statement of the author: *'If this talent pool could be diverted away from cybercrime and into legitimate industry, there would be two positive developments'* (p. 199). While this is not easy to achieve, it is also my own view that this could be the most important way to decrease cybercrime and increase cybersecurity. Both policy makers as well as academics should further assess ways to stimulate positive alternatives for cybercriminals.

Notes on contributor

Dr. M. Weulen Kranenbarg is an assistant professor at VU Amsterdam, The Netherlands. Her research mostly focuses on cyber-dependent offenders. In her doctoral dissertation she empirically compared traditional offenders to cyber-offenders on four important domains in criminology: 1. offending over the life-course, 2. personal and situational risk factors for offending and victimization, 3. similarity in deviance in the social network, and 4. motivations related to different offense clusters. She recently started a large-scale longitudinal study into actual vs. perceived cybercriminal behavior of offline vs. online social ties among youth. Marleen is also a research fellow of the NSCR (Netherlands Institute for the Study of Crime and Law Enforcement), board member of the ESC Cybercrime Working Group, and part of the steering committee of the IIRCC (International Interdisciplinary Research Consortium on Cybercrime).

M. Weulen Kranenbarg
Vrije Universiteit (VU) Amsterdam, The Netherlands
m.weulenkranenbarg@vu.nl http://orcid.org/0000-0001-7217-5166

https://doi.org/10.1080/17440572.2020.1743935