ARTICLE

THE CYBERCRIME INDUSTRY

Jonathan Lusthaus[1*]

ABSTRACT

Over recent decades, cybercrime has morphed from a curiosity into a serious global challenge. In many cases, the stereotype of the nerdy hacker in their parent's basement has been superseded by a highly professional, specialised, and multi-faceted industry, made up of coders, entrepreneurs, managers, street criminals, and their protectors. This evolution of cybercrime presents a striking paradox, which has largely escaped notice: how did cybercriminals achieve industrialisation on such a scale, when they operate in an environment characterised by intense levels of distrust? One would expect legal scholarship to have identified this puzzle and resolved it. After all, the concept of private ordering has been a powerful and influential subfield for a number of decades; to build an industry like cybercrime would, no doubt, require order. But the literature on private ordering has been focused on informal, but licit, economic activities, and is yet to intersect with the important case of cybercrime. The cybercrime industry is an intriguing example of the private ordering of the dark side. This article aims to bring clear focus, as well as theoretical and empirical rigor, to the question of how cybercriminals govern themselves. It draws on three main sources of data: 1) fieldwork carried out over a 7-year period in 20 countries, which involved semi-structured interviews with almost 250 law enforcement agents, security professionals, and former cybercriminals; 2) indictments and other legal documents; 3) archives of major cybercriminal forums.

CONTENTS

[1*] Director of the Human Cybercriminal Project, Extra-Legal Governance Institute & Associate Professor of Global Sociology, Department of Sociology and Oxford School of Global and Area Studies at the University of Oxford, UK. I'm very grateful to all those who participated in this research and were incredibly generous with both their time and knowledge. The elements of this article on Darkode could not have been written without past collaboration with Benoît Dupont, who kindly shared a copy of the data with me, and offered many valuable insights. Robert Ellickson offered very useful comments on an earlier iteration of this paper, while Qiaoyu Luo provided invaluable assistance in the final preparation of this manuscript. I also thank the *Harvard National Security Journal* for selecting this article and editing it in such a diligent way. Finally, special mention must go to Scott Shapiro, who provided the initial idea and impetus to produce this article, and gave enormously helpful advice and feedback along the way.

INTRODUCTION

Cybercrime has evolved over the years to become big business.[2] While computer hacking emerged in the late 1950s, it could not be considered an illicit activity initially, as these hackers were students experimenting with university mainframes.[3] Criminal hacking gradually developed throughout the following decades, particularly as computing technology became more widely available in the 1980s onwards.[4] As more and more commercial data and processes were put online, financially motivated cybercrime became a greater concern.[5] There were early signs in the 1990s, but profit-driven cybercrime really began to flourish at the turn of the millennium.[6] Online marketplaces for the trade in stolen data began to attract hundreds, and sometimes thousands, of members.[7] Around these sites, networks formed and information was spread on how to carry out various cybercriminal schemes.[8] A community of professional cybercriminals emerged.[9]

As a result, the stereotype of the nerdy hacker in their parents' basement has largely been replaced by a highly professional, specialised, and multi-faceted industry made up of coders, entrepreneurs, managers, street criminals, and their protectors. Not only are there virtual marketplaces where these offenders can meet and trade, but many are also organised

[2] *See* JONATHAN LUSTHAUS, INDUSTRY OF ANONYMITY: INSIDE THE BUSINESS OF CYBERCRIME 31-64 (2018) (discussing the history of profit-driven cybercrime); SUSAN BRENNER, CYBERCRIME: CRIMINAL THREATS FROM CYBERSPACE 9-38 (2010).
[3] *See* LUSTHAUS, INDUSTRY OF ANONYMITY, *supra* note 2, at 32–33.
[4] *See id.* at 33–35; BRENNER, *supra* note 2, at 10–22.
[5] *See* LUSTHAUS, INDUSTRY OF ANONYMITY, *supra* note 2, at 35–38; BRENNER, *supra* note 2, at 28–29.
[6] *See* LUSTHAUS, INDUSTRY OF ANONYMITY, *supra* note 2, at 38.
[7] *See* LUSTHAUS, INDUSTRY OF ANONYMITY, *supra* note 2, at 47.
[8] *See id.* at 43–49.
[9] *See id.* at 60–62.

into operational groupings, which could be considered cybercriminal firms.[10] This is a serious business. The 2021 ransomware attacks on Colonial Pipeline and Kaseya, which caused both significant financial and other harm, and captivated the attention of both the media and the highest levels of government, illustrate this issue well.[11] The groups behind these attacks, DarkSide and REvil, both highly professional and organised networks, provide us with powerful examples of cybercriminals cooperating successfully together on a larger scale.[12] The threat of cybercrime has grown substantially and tackling this problem has become increasingly urgent.[13] While opinion and information varies, some already place the annual costs of cybercrime in the hundreds of billions.[14]

This evolution of cybercrime presents a striking paradox which has largely escaped notice: how did cybercriminals achieve large-scale industrialisation when they operate in an environment characterised by intense levels of distrust? One might assume that dealing with anonymous partners online would lead to wariness and doubt, rather than encourage widespread cooperation. These challenges are in addition to obstacles faced by criminals in general, who are inherently untrustworthy partners, and who have no recourse to the police or court system should they come into dispute.[15] Thus, we would expect that cybercriminals would operate alone or in very small groups, rather than in a large industry.

It is surprising that legal scholarship has yet to identify and solve this puzzle. After all, the concept of private ordering—extra-legal regulation and governance performed by private actors—has been a powerful and influential subfield for decades. Industrialisation at

[10] *See id.* at 43, 47.

[11] *See* William Turton & Kartikay Mehrotra, *Hackers Breached Colonial Pipeline Using Compromised Password*, BLOOMBERG (2021), https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password [https://perma.cc/U472-SQKC]; Kari Paul, *Who's Behind the Kaseya Ransomware Attack – And Why is it So Dangerous?*, THE GUARDIAN (2021), https://www.theguardian.com/technology/2021/jul/06/kaseya-ransomware-attack-explained-russia-hackers [https://perma.cc/T7D8-NFG2]; Dustin Volz & Catherine Lucey, *Biden Warns Putin U.S. to Take 'Any Necessary Action' to Defend Against Ransomware*, WALL STREET J. (2021), https://www.wsj.com/articles/biden-spoke-to-russian-president-putin-about-ransomware-attacks-11625850786 [https://perma.cc/MB6Q-5E4P].

[12] *See* Turton & Mehrotra, *supra* note 11; Paul, *supra* note 11.

[13] Due to its connection to critical infrastructure, and the broader harms that it caused, the Colonial Pipeline attack may appear to be the more serious of these two ransomware cases. But the Kaseya attack illustrates a leap forward for ransomware tactics. To conduct that attack, REvil targeted a software supplier that issues updates to numerous organisations. These updates are meant to protect each organisation from breaches, but in this case the system was subverted so that ransomware was provided to these organisations as an update instead. As Matt Tait argues, "software supply chain security breaches don't look like other categories of breaches. A lot of this comes down to the central conundrum of system security: It's not possible to defend the edges of a system without centralization so that defensive resources can be pooled. But this same centralization concentrates offensive action against a few single points of failure that, if breached, cause all of the edges to fail at once." Matt Tait, *The Kaseya Ransomware Attack Is a Really Big Deal*, LAWFARE (2021), https://www.lawfareblog.com/kaseya-ransomware-attack-really-big-deal.

[14] *See* James Lewis, *Economic Impact of Cybercrime—No Slowing Down* 4 (Feb. 2018); Ross Anderson, et al., *Measuring the Cost of Cybercrime*, *in* THE ECONOMICS OF INFORMATION SECURITY AND PRIVACY (Rainer Böhme ed., 2013). Measuring the cost of cybercrime is a challenging endeavour for a number of reasons, not least the lack of reliable statistics in this area. There are concerns that cybersecurity industry estimates hype the threat, as that can promote business.

[15] *See* Paolo Campana & Federico Varese, *Cooperation in Criminal Organizations: Kinship and Violence as Credible Commitments*, 25 RATIONALITY AND SOC'Y 1, 2 (2013).

this scale undoubtedly requires order. A number of researchers have investigated how people govern themselves when state institutions are not an effective or efficient way to resolve their disputes.[16] Spanning many disciplines, studies of private ordering—along with the related concepts of informal or extra-legal governance—have often addressed the positive aspects of this phenomenon and the ways in which these systems of governance may sometimes be more effective than the law. This has included resolving disputes, as well as developing commercial and self-regulatory arrangements to prevent disputes in the first place. Leading legal scholars, including Robert Ellickson and Lisa Bernstein, have explored a range of now-famous examples such as escaped cattle, the diamond trade, and the cotton industry.[17]

There is also the "dark side" of private ordering, which has received much less scholarly attention. In a classic article on organised crime in Japan, Curtis Milhaupt and Mark West argue that these criminal groups compete with the state as a protector of property rights.[18] When the state performs its legal functions inefficiently, organised criminals may fill the void.[19] Varese finds a similar phenomenon in 1990s Russia, where protection by mafia groups was often preferred to the *Arbitrazh* (Court of Arbitration), which was not known for timely and positive outcomes.[20] When those in dispute were both protected by mafia members, an "outlaw court" would be convened, which may even have had the involvement of professional lawyers in the process.[21]

But the literature on private ordering has yet to intersect with the cybercrime industry. The aforementioned analyses concern illicit groups seeking to provide governance for otherwise legitimate commercial activities. Yet in trying to understand the cybercrime industry, the focus needs to be extended to how offenders regulate their own criminal dealings. This is more the *private ordering of the dark side*, rather than the dark side of private ordering. A niche literature has emerged on the governance of particular illicit groups and activities outside the control of the state.[22] Thus far, scholars have investigated governance in relation to the Sicilian Mafia, the Russian Mafia, Hong Kong Triads, prison gangs, and pirates.[23] The private ordering of cybercrime bears similarities to these other

---

[16] *See, e.g.*, Lisa Bernstein, *Opting out of the Legal System: Extralegal Contractual Relations in the Diamond Industry*, 21 J. L. STUDIES (1992) [hereinafter Bernstein (1992)]; ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION (1990); ROBERT ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES (1991); Avery Katz, *Taking Private Ordering Seriously*, 144 U. PA. L. REV. (1996); Lisa Bernstein, *Private Commercial Law in the Cotton Industry: Creating Cooperation through Rules, Norms, and Institutions*, 99 MICH. L. REV. (2001) [hereinafter Bernstein (2001)]; Richard McAdams, *The Origin, Development, and Regulation of Norms*, 96 (1997).

[17] *See generally* ELLICKSON, *supra* note 16; Bernstein (1992), *supra* note 16; Bernstein (2001), *supra* note 16.

[18] Curtis J. Milhaupt & Mark D. West, *The Dark Side of Private Ordering: An Institutional and Empirical Analysis of Organized Crime*, 67 U. CHI. L. REV. 41, 47–48 (2000).

[19] *Id.* at 45.

[20] *See* FEDERICO VARESE, THE RUSSIAN MAFIA: PRIVATE PROTECTION IN A NEW MARKET ECONOMY 114, 118 (2001).

[21] *Id.*

[22] AVINASH DIXIT, LAWLESSNESS AND ECONOMICS: ALTERNATIVE MODES OF GOVERNANCE vii-viii (2004).

[23] *See, e.g.*, DIEGO GAMBETTA, THE SICILIAN MAFIA: THE BUSINESS OF PRIVATE PROTECTION (1993); VARESE, *supra* note 20; YIU KONG CHU, THE TRIADS AS BUSINESS (2000); David Skarbek, *Governance and Prison Gangs*, 105 AM. POL. SCI. REV. (2011); Anja Shortland & Federico Varese, *The Protector's Choice*, 54 BRIT. J. CRIMINOLOGY (2014). *See also* MICHAEL LEVI, THE PHANTOM CAPITALISTS: THE ORGANISATION AND CONTROL OF LONG-FIRM FRAUD (2008); PETER REUTER, DISORGANIZED CRIME: THE ECONOMICS OF THE

examples of governance in the criminal world. For example, in both, criminals do not appear to be trustworthy partners for successful cooperation. Cybercrime compounds these existing challenges by introducing significantly more layers of anonymity. In online settings, the true identities of cybercriminals are masked by both their nicknames and operational security.[24] Without physical interactions, trustworthiness is challenging to gauge and enforcement cannot be achieved through violence and intimidation.

This article aims to bring clear focus, as well as theoretical and empirical rigor, to the study of cybercrime governance.[25] Given the commercial interests that often underpin the need for private ordering, the analysis is focused on financially motivated cybercrime. This article proceeds in six parts. First, it highlights relevant theory around private ordering, particularly extra-legal governance. Second, it sketches a portrait of the nature of financially motivated cybercrime. Third, it outlines the data and methods used in this article. Fourth, it draws on this data to investigate how cybercrime is governed online in broad terms. Fifth, in order to provide a more specific and grounded analysis, the article conducts a case study of Darkode, which was one of the world's leading cybercriminal marketplaces before it was taken down by law enforcement. Sixth, the article assesses the effectiveness and limits of this form of virtual governance. Finally, the article concludes by assessing what the private ordering of cybercriminals can teach us about countering this criminal industry.

I. PRIVATE ORDERING AND EXTRA-LEGAL GOVERNANCE

The state is not the sole provider of governance. Ellickson argues that "large segments of social life are located and shaped beyond the reach of the law," and that rather than being a state monopoly, order "often rises spontaneously."[26] In short, people may "supplement, and indeed preempt, the state's rules with rules of their own."[27] For cattle ranchers, fishing boats, diamond traders, and many others, self-regulation can bring greater efficiency or specificity than what the state is providing or failing to provide.[28] When the state is very inefficient in particular areas, the "dark side of private ordering" may emerge, whereby criminal competitors step in as third party providers of governance.[29]

While related topics are discussed under the competing, but largely harmonious, concepts of informal governance and private ordering, for the remainder of this article I chiefly employ the term *extra-legal governance*. The case of cybercrime is not one where order emerges between or below components of state authority but is external to it. In its legitimate form, the state cannot compete as a provider of governance to cybercriminals.[30] All

---

VISIBLE HAND (1983); PETER LEESON, THE INVISIBLE HOOK: THE HIDDEN ECONOMICS OF PIRATES (2009).

[24] *See* Jonathan Lusthaus, *Trust in the World of Cybercrime*, 13 GLOB. CRIME 71, 80–81 (2012).

[25] *See also* Jonathan Lusthaus, *How Organised is Organised Cybercrime?*, 14 GLOB. CRIME 52, 52-60 (2013); Michael Yip, et al., *Trust Among Cybercriminals? Carding Forums, Uncertainty and Implications for Policing*, 23 POLICING AND SOCIETY 516, 516-539 (2013); Jonathan Lusthaus, *Trust in the World of Cybercrime*, *supra* note 24.

[26] ELLICKSON, *supra* note 16, at 4.

[27] *Id.* at 5.

[28] *See generally id.*; Bernstein (1992), *supra* note 16; Bernstein (2001), *supra* note 16; OSTROM, *supra* note 16.

[29] Milhaupt & West, *supra* note 18, at 43; *see, e.g.*, GAMBETTA. 1993; VARESE, *supra* note 20.

[30] Of course, in a less legitimate conception of the state, corrupt agents may seek to govern criminal markets of various kinds. *See, e.g.*, FEDERICO VARESE, MAFIAS ON THE MOVE (2011); VARESE, *supra* note 20.

it can do is try to stamp out this illegal activity. This leaves the cybercriminal underworld ostensibly alone in its attempts to govern itself.

To understand how cybercrime is governed outside the control of the state, I briefly survey relevant theoretical background in this section. As our interest is in governance, rather than merely cooperation, this outline is focused less on small scale interactions and more on how rules, institutions, and systems of regulation and enforcement can provide order for larger groups and communities. The cybercrime literature has relatively little to say on this topic; therefore, this outline is largely drawn from the broader literature relevant to extra-legal governance. The subsequent empirical analysis will examine how well theories of extra-legal governance explain the unusual case of cybercrime.

A. The Importance of Institutions

Humans successfully cooperate on a small scale by employing some well-known mechanisms. Individuals frequently assess the trustworthiness of others and decide whether to engage with them.[31] As Piotr Sztompka argues, the key components of trustworthiness that can be used in such an assessment are reputation, appearance, and performance.[32] Reputation, and the related concept of repeated interactions, has been discussed widely across the social sciences as one foundation for successful cooperation.[33] Beyond trustworthiness, enforcement is another mechanism that underpins collaboration and potentially encompasses aspects of monitoring, punishment, guarantees, and credible commitments.[34] Individuals can enforce their own agreements or have others do it for them.

But the central challenge under investigation is how cooperation can be scaled from small groups up to widespread engagement and organisation on an industrial level.[35]

---

[31] On trust and trustworthiness, see generally KAREN COOK, et al., COOPERATION WITHOUT TRUST? (2005); Partha Dasgupta, *Trust as a Commodity*, *in* TRUST: MAKING AND BREAKING COOPERATIVE RELATIONS (Diego Gambetta ed., 1988); Russell Hardin, *Conceptions and Explanations of Trust*, *in* TRUST IN SOCIETY (Karen Cook ed., 2001).

[32] PIOTR SZTOMPKA, TRUST: A SOCIOLOGICAL THEORY 69-101 (1999).

[33] *E.g.*, THOMAS SCHELLING, THE STRATEGY OF CONFLICT (1980); ROBERT AXELROD, THE EVOLUTION OF COOPERATION (2006).

[34] Partners can closely monitor each other to help ensure that neither defects. But this can be very time and resource intensive. If information can move swiftly among group members, then the monitoring burden can be shared and the costs will be less. *See* DIXIT, *supra* note 22; OSTROM, *supra* note 16. If monitoring does not lead to compliance, punishment can be used. Violence has been a well-known tool deployed by conventional criminals, but there are other forms of punishment, as well. Experimental research suggests that even the *threat* of punishment can encourage compliance. Ernst Fehr & Herbert Gintis, *Human Motivation and Social Cooperation: Experimental and Analytical Foundations*, 33 ANN. REV. SOCIO. 43, 43-64 (2007); Ernst Fehr & Simon Gächter, *Cooperation and Punishment in Public Goods Experiments*, 90 AM. ECON. REV. 980, 980-81 (2000). A third party guarantor is another means of enforcement. This role is often played by state agents in the legitimate world, but extra-legal actors, such as mafiosi, can also do so. *E.g.*, Milhaupt & West, *supra* note 18; GAMBETTA. 1993, supra note 23; VARESE, *supra* note 20; DIXIT, *supra* note 22. Finally, *credible commitments*, such as *cutting off options* and *information hostages*, can allow some forms of cooperation without trust. *See* SCHELLING, *supra* note 33, at 43–44. As Cook, Hardin, and Levi put it: "When there is no ground for trust, we can often establish reliability by demonstrating our commitment to take relevant actions. If we, whom you have no reason to trust, wish to convince you that we will be reliable in taking some action that will benefit you, we can try to establish a credible commitment." COOK ET AL., *supra* note 31, at 37.

Douglass North, the Nobel-Prize-winning economist, sums up the key barriers to more widespread cooperation among larger networks:

> "Wealth-maximizing individuals will usually find it worthwhile to cooperate with other players when the play is repeated, when they possess complete information about the other player's past performance, and when there are small numbers of players. But turn the game upside down. Cooperation is difficult to sustain when the game is not repeated (or there is an endgame), when information on the other players is lacking, and when there are large numbers of players."[36]

To succeed at wide-scale cooperation, something more is required. The solution to these challenges is found in *institutions*:

> "Institutions are the humanly devised constraints that structure political, economic and social interaction. They consist of both informal constraints (sanctions, taboos, customs, traditions, and codes of conduct), and formal rules (constitutions, laws, property rights). Throughout history, institutions have been devised by human beings to create order and reduce uncertainty in exchange."[37]

Key mechanisms like trustworthiness and enforcement may still drive cooperation, but effective institutions magnify these mechanisms so that cooperation can take place on a much grander scale. Institutions reduce costs associated with exchange by providing a degree of order.[38] Without them, barriers to cooperation would remain and cooperation in small groups is likely to predominate.[39]

B. Governance Outside the Law

Institutions and governance are closely related concepts, as those who govern are often responsible for creating and/or managing institutions. States are major supporters and providers of institutions. But as the case of cybercrime sits firmly outside the purview of states, our theoretical interest is how governance occurs outside the law. One might view this question as fitting into a classic distinction between a hegemonic top-down form of order typified by Thomas Hobbes, in opposition to the view of Friedrich Hayek in which order arises spontaneously from the bottom up, to meet needs in a more ad hoc way.[40] The state as

---

[35] *See* OSTROM, *supra* note 16; MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION: PUBLIC GOODS AND THE THEORY OF GROUPS (1971).
[36] Douglass C. North, *Institutions*, 5 J. ECON. PERSPS. 97, 97 (1991).
[37] *Id.*
[38] *See generally* James Coleman, *Social Capital in the Creation of Human Capital*, 94 AM. J. SOCIOLOGY 95 (1988); OSTROM, *supra* note 16; North, *supra* note 36.
[39] *See, e.g.*, Coleman, *supra* note 38; OSTROM, *supra* note 16; North, *supra* note 36.
[40] *See generally* THOMAS HOBBES, LEVIATHAN (1651); FRIEDRICH HAYEK, THE CONSTITUTION OF LIBERTY (2006); FRIEDRICH HAYEK, THE FATAL CONCEIT (1988).

a form of governance would align with Hobbes, whereas extra-legal governance would align with Hayek.

Even for extra-legal governance, some form of the top-down versus bottom-up distinction remains, though in many cases it is a blurred one. Dixit argues that outside the state there are two alternative governance structures that can enforce contracts and protect property rights: private governance and self-governance.[41] The former involves hiring third-party protectors to enforce rights and agreements from above; the latter sees order develop more organically within a group, often dependent on information on bad behaviour being easily transmitted and the presence of communal punishment options.[42] Taking a broad view, one could, perhaps, align North's division between formal rules and informal constraints with this distinction.[43]

In studies of criminal markets, private governance is given a central role. Some scholars even build the concept of governance into definitions of organised crime. Thomas Schelling, another Nobel-Prize-winning economist, argues that there is a distinction between "organized crime" and "crime that is organized."[44] Using the example of burglars, Schelling argues that organising into small groups is not enough.[45] Rather, to be considered organised crime, a group must also seek to control their territory and to monopolise their activities:

> "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, collectively negotiating with the police not only for its 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*.'"[46]

A number of scholars, such as Diego Gambetta, have adopted the centrality of governance in conceptualising organised crime.[47] Surveying the field as a whole, Varese argues that an *organised crime group* "attempts to regulate and control the production and distribution of a given commodity or service unlawfully."[48]A *mafia* is a specific type of organized crime group that "attempts to control the supply of *protection*."[49] This essentially means that a mafia wishes to govern all criminal markets in its territory.

---

[41] *See generally* DIXIT, *supra* note 22.
[42] *See id.* at 60, 129.
[43] Douglass C. North, *supra* note 36.
[44] Thomas Schelling, *What is the Business of Organized Crime*, 40 AM. SCHOLAR 643, 644 (1971).
[45] *Id.*
[46] *Id.* at, 644.
[47] *See* GAMBETTA. 1993; Milhaupt & West, *supra* note 18; VARESE, *supra* note 20; JAMES DENSLEY, HOW GANGS WORK: AN ETHNOGRAPHY OF YOUTH VIOLENCE (2013); Skarbek, *supra* note 23; Lusthaus, *Trust in the World of Cybercrime*, *supra* note 24.
[48] Federico Varese, *What is Organized Crime?*, *in* ORGANIZED CRIME: CRITICAL CONCEPTS IN CRIMINOLOGY 14 (2010).
[49] *Id.* at 17.

This article will investigate how well these conceptions of private governance map onto the case of cybercrime. But, equally importantly, it will also examine any aspects of self-governance and what role they may play in the organisation and success of the cybercriminal industry. Before proceeding with this discussion, a brief outline of the cybercrime industry and what cybercrime is will be provided.

II. THE NATURE OF CYBERCRIME

While most are familiar with cybercrime as a broad concept, many are not familiar with the inner workings of the contemporary cybercrime industry. In this section, I provide a brief definitional discussion of cybercrime, along with some broad strokes on what cybercrime looks like today.

David Wall notes that many terms have been used to describe what we now commonly call cybercrime—computer crime, high-tech crime, virtual crime, net-crime—but whatever "its merits and demerits, the term 'cybercrime' has entered the public parlance and we are more or less stuck with it."[50] Cybercrime has also had a variety of definitions.[51] The main point of contention has been whether cybercrime is something novel, or, more simply conventional crimes adapted to new technologies. Wall has argued for the former position: "[T]he Internet, and particularly the cyberspace it creates, is not just a case of 'old wine in new bottles,' or for that matter 'new wine in new bottles,' rather many of its characteristics are so novel that the expression 'new wine, but no bottles!' becomes a more fitting description."[52] Maintaining the wine metaphors, Peter Grabosky has championed the opposing position:

> "'[V]irtual criminality' is basically the same as the terrestrial crime with which we are familiar. To be sure, some of the manifestations are new. But a great deal of crime committed with or against computers differs only in terms of the medium. While the technology of implementation, and particularly its efficiency, may be without precedent, the crime is fundamentally familiar. It is less a question of something completely different than a recognizable crime committed in a completely different way."[53]

Over time, Grabosky's broader approach has gradually found favour within the field: in their review of the literature, Thomas Holt and Adam Bossler note that while there is "no single, agreed-on definition of cybercrime, many scholars argue that it involves the use of cyberspace or computer technology to facilitate acts of crime and deviance."[54] But a rear-guard action has ensured that a milder form of Wall's new wine versus old wine distinction

---

[50] David Wall, *What are Cybercrimes?*, 58 CRIM. JUST. MATTERS 20, 20 (2008).
[51] *See, e.g.*, David Wall, *Catching Cybercriminals: Policing the Internet*, 12 INT'L REV. L., COMPUT. & TECH. 201, 201-202 (1998); Peter Grabosky, *Virtual Criminality: Old Wine in New Bottles?*, 10 SOC. & LEGAL STUD. 243 (2001).
[52] David Wall, *supra* note 50 at 201-202.
[53] Peter Grabosky, *supra* note 51 at 243.
[54] Thomas Holt & Adam Bossler, *An Assessment of the Current State of Cybercrime Scholarship*, 35 DEVIANT BEHAV. 20, 21 (2014).

still muddies the water.[55] Some scholars and policymakers continue to divide cybercrime into at least two categories: *cyber-enabled crime* and *cyber-dependent crime*.[56] The former category refers to those conventional crimes, like fraud, which are now enhanced by new technology.[57] The latter category are crimes that cannot be carried out without these new technologies, such as malware or Distributed Denial of Service Attacks (DDoS), as computers and systems are the target of these crimes.[58] In legal terms, this distinction has some relevance, particularly in explaining the introduction of laws criminalising unauthorised access to computers, such as the Computer Fraud and Abuse Act.[59]

But how useful is this distinction in understanding the nature of cybercrime itself? In reality, the division between cyber-enabled and cyber-dependent crime is illusory and it may be time to abandon it. When legislatures criminalise unauthorised access and related activities, they are targeting the technical means being used, not the motivations behind them. Despite suggestions to the contrary,[60] so-called cyber-dependent crimes are invariably linked to a conventional transgression, which would often be associated with cyber-enabled crimes. For example, among many other uses, malware can be deployed for committing theft by accessing and transferring funds out of online bank accounts.[61] Similarly, an intrusion may compromise a database of credit card information, which can later be used for fraud.[62] Alongside theft and fraud are several existing crimes that can be carried out by "attacking" computers: extortion, vandalism, and espionage.[63] What we are then left with is a spectrum of crime that may incorporate technology in different ways. At the one end are crimes that employ very little technology; at the other are crimes that require a significant technical component. There is a range in between.[64]

Throughout this article I employ a broad functional definition, which accounts for the full spectrum of cybercrimes. Cybercrime is defined as "crime that makes use of digital technology in a significant way."[65] It should be specified that the use of digital technology should not be tangential to the crimes involved, or else any use of smart phones, texting, email or other Internet technologies by criminals would be enough to classify their activity as cybercrime.

---

[55] David Wall, *supra* note 50.
[56] *See generally* STEVEN FURNELL, CYBERCRIME: VANDALIZING THE INFORMATION SOCIETY (2002); MIKE MCGUIRE & SAMANTHA DOWLING, CYBERCRIME: A REVIEW OF THE EVIDENCE (2013).
[57] *See* MCGUIRE & DOWLING, *supra* note 56, at 5.
[58] *See id.*
[59] *See* The Computer Fraud and Abuse Act, *generally* 18 U.S.C. §1030 (2012).
[60] *See* MCGUIRE & DOWLING, *supra* note 56; David Maimon & Eric Louderback, *Cyber-Dependent Crimes: An Interdisciplinary Review*, 2 ANN. REV. CRIMINOLOGY 191, 191-216 (2019).
[61] Jonathan Lusthaus, *Reconsidering Crime and Technology: What Is This Thing We Call Cybercrime?*, 20 ANN. REV. L. & SOC. SCI. 369, 379 (2024).
[62] *See id.* at 370, 373.
[63] *Id.* at 372, 380.
[64] *Id.*; Jonathan Lusthaus, et al., *Cybercriminal networks in the UK and Beyond: Network structure, criminal cooperation and external interactions*, 27 TRENDS IN ORGANIZED CRIME 364, 371-74 (2023); LUSTHAUS, INDUSTRY OF ANONYMITY: INSIDE THE BUSINESS OF CYBERCRIME, *supra* note 2.
[65] Lusthaus, *supra* note 61, at 381. For a similar definition see SAMUEL MCQUADE, UNDERSTANDING AND MANAGING CYBERCRIME 16 (2006) (asserting that cybercrime is the "use of computers or other electronic devices via information systems such as organizational networks or the Internet to facilitate illegal behaviors").

Because cybercrime encompasses so many different forms and activities, it is challenging to draw a complete picture. In this article, I focus only on profit-driven cybercrime, as opposed to attacks motivated by personal elements (e.g. revenge, or sexual interests), recreation, ideology (e.g. hacktivism or cyberterrorism), and nation state interests.[66] But even financially motivated cybercrime is a large expanse and not easily summarised. As a primer, this is a (non-exhaustive) list of common forms or components of financially motivated cybercrime:

1) Technical products/services (e.g., malware coding, botnet access, spam, tool production).
2) Attacks and Extortion (e.g., DDoS attacks, ransomware).
3) Infrastructure (e.g., bulletproof hosting).
4) Data/identity theft (e.g., hacking and intrusions, phishing, account compromises, credit card comprises).
5) Scams (e.g., advance fee fraud, business email compromise, online auction fraud).
6) Cashing out/money laundering (e.g., banking fraud, credit card fraud, money muling).[67]

While public attention is often focused on hacking, this list alone demonstrates that cybercrime encompasses many more activities. It is also worth noting that not all cybercriminals are hackers and not all hackers are cybercriminals.[68] For instance, some scams may leverage the Internet but do not require the offenders to have significant technical capabilities. One example is online auction fraud, which simply involves selling non-existent products on well-known platforms like eBay.[69] In cashing out, where virtual gains are converted into physical or monetary ones, almost no technical ability is necessary in certain cases.[70]

---

[66] For a different but widely cited typology, *see* David Wall, *Cybercrimes and the Internet*, *in* CRIME AND THE INTERNET 3-7, (David Wall ed., 2001). This encompasses: (1) cyber-trespass, (2) cyber-deceptions and thefts, (3) cyber-pornography, and (4) cyber-violence.

[67] Along with the data collected as part of this research, which was used to generate these categories, *see, e.g.*, Wall, *supra* note 51; Grabosky, *supra* note 51; Maimon & Louderback, *supra* note 60. For a modified/refined version of these categories see Miranda Bruce et. al., *Mapping the Global Geography of Cybercrime with the World Cybercrime Index*, PLOS ONE (April 2024), at 5.

[68] On the hacking mentality, *see Frequently Asked Questions*, MIT GALLERY OF HACKS, http://hacks.mit.edu/Hacks/misc/faq.html [https://perma.cc/YGZ5-HUAM]; *see generally* STEVEN LEVY, HACKERS: HEROES OF THE COMPUTER REVOLUTION (2010).

[69] *See Avoid Scams: Online Sales and Auction Fraud*, U.S. SECRET SERV., https://www.secretservice.gov/investigations/onlinesalesfraud [https://perma.cc/WW84-A3JJ].

[70] For more detail on a number of forms/components of cybercrime, *see, e.g.*, E. Rutger Leukfeldt, et al., *Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties Within Phishing and Malware Networks*, 57 BRITISH JOURNAL OF CRIMINOLOGY 704, 704-22 (2017); Rutger Leukfeldt, et al., *A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists*, 67 CRIME, LAW AND SOCIAL CHANGE 21, 21-37 (2017); Alice Hutchings & Richard Clayton, *Configuring Zeus: A case study of online crime target selection and knowledge transmission* (2017), https://www.repository.cam.ac.uk/handle/1810/264568; David Décary-Hétu & Benoit Dupont, *Reputation in a Dark Network of Online Criminals*, 14 GLOBAL CRIME 175, 175-196 (2013); Roberto Musotto & David Wall, *More Amazon than Mafia: analysing a DDoS stresser service as organised cybercrime*, 25 TRENDS IN ORGANIZED CRIME 173, 173-91 (2020); Jonathan Lusthaus & Federico Varese, *Offline and Local: The Hidden Face of Cybercrime*, 15 POLICING 1, 4-14 (2021); LISA SUGIURA, RESPECTABLE DEVIANCE AND PURCHASING MEDICINE ONLINE (2018); Rutger Leukfeldt, et al., *Organised Cybercrime or Cybercrime that is Organised?*

But cybercrime is not just about the types of attacks that are carried out. As cybercrime has evolved into a highly professional and specialised field, we also need to know about the organisation and people involved. Cybercrime is distinguished by a division of labour, with a clear breakdown of roles, carried out by individuals skilled in each domain, whether coding, spamming and infecting users, money transfer and cashing out, intrusions, selling data, or managing an illicit enterprise itself.[71] Cybercriminals employ professional business practices like accounting and marketing.[72] While some conventional criminals are involved, in certain locations around the globe such as Eastern Europe, organisers also draw on the very same talent pool that feeds the technology sector for recruitment, including those with advanced degrees. This illicit business includes well-known economic structures observed in legal settings, including marketplaces and firms—in short, cybercrime has become an *industry* in its appearance and approach.[73]

III. DATA AND METHODS

A. Fieldwork & Interviews

This article draws on three main sources of data. First, over a seven-year period, I carried out fieldwork in twenty countries, including a number of cybercrime "hotspots," such as Russia, Ukraine, Romania, China, Nigeria, Brazil, and the United States.[74] This involved semi-structured interviews with almost 250 law enforcement agents, security professionals, and former cybercriminals. The Appendix contains tables that summarise both the participants' geographical distribution and profession.[75]

To obtain access to these participants, I used both "purposive" and "snowball" sampling. Using open-source means, I searched for interview participants from a range of geographical, personal and professional backgrounds, who each had a deep knowledge of cybercrime. As the study progressed, snowball sampling became very important. I was able to leverage referrals from existing participants to contact additional subjects, some of whom were not publicly known or were difficult to locate. With that said, as the study involved engagement with a range of jurisdictions and participant types, there was never one single snowball but rather a series of smaller ones. Given the level of secrecy and paranoia among some within the cybercrime community, there were also limits to how far snowball sampling could succeed on its own.

An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime, 23 EUROPEAN JOURNAL ON CRIMINAL POLICY AND RESEARCH 287, 287-300 (2016).

[71] LUSTHAUS, INDUSTRY OF ANONYMITY, *supra* note 2, at 34, 37, 44–45, 48–49, 61.

[72] NIR KSHETRI, THE GLOBAL CYBERCRIME INDUSTRY: ECONOMIC, INSTITUTIONAL AND STRATEGIC PERSPECTIVES 190, 198.

[73] *See generally* LUSTHAUS, INDUSTRY OF ANONYMITY: INSIDE THE BUSINESS OF CYBERCRIME, *supra* note 2; NIR KSHETRI, THE GLOBAL CYBERCRIME INDUSTRY: ECONOMIC, INSTITUTIONAL AND STRATEGIC PERSPECTIVES (2010); Tyler Moore, et al., *The Economics of Online Crime*, 23 J. ECON. PERSP. 3, 3-20 (2009).

[74] Bruce et. al., *supra* note 67, at 8.

[75] For more detail on this fieldwork, *see generally* LUSTHAUS, INDUSTRY OF ANONYMITY: INSIDE THE BUSINESS OF CYBERCRIME, *supra* note 2.

With regard to the offender sample, I focused on former rather than current cybercriminals, who had retired from cybercrime or had been arrested. These participants were easier to identify and locate and had less incentive to deceive. This approach reduced risks to both participants and the researcher. It also reduced the likelihood of becoming entangled in an open law enforcement investigation. I succeeded in accessing a range of former offenders from low level operators up to some of the most elite cybercriminals of the era. Another approach I leveraged was to become "pen pals" with some leading cybercriminals who were incarcerated. The information gleaned from these interviews was extremely rich, with the communication process sometimes sustaining weeks if not months.

While some interviews were done remotely through calls or writing, across the project, most interviews were conducted in person. Within this article, interviews are cited directly to support points, and quotes from these interviews are reported verbatim. For written interviews, all words are reported as received, but minor editing for spelling and punctuation has been applied in certain cases to ensure basic readability. In line with University of Oxford ethics clearance, identifying information has been removed. In order to protect identities and to allow for the more open sharing of information, the anonymity protocols used in this study are strict. Any names used in text are pseudonymous. The relevant interview citations in each case only include the essential information. For both investigators and offenders alike, the world of cybercrime remains a small one, meaning that seemingly innocuous information might be pooled together to make identifications. As such, I only provide the year for each interview rather than the specific date, which could be matched to known conferences for which attendee lists are available. Similarly, I do not identify the specific interview locations. Given the greater risks attached to the former cybercriminal participants, location is listed by region rather than country, no direct differentiation is made between those who were incarcerated and those who were not, and the year of interview is not specified.[76] While obtaining informed consent was a key protocol used across the study, it was particularly important for interviews with prison inmates, who are classed as a "vulnerable population." In these instances, the voluntary nature of participation had to be emphasised.[77] It was also important to remind prisoners of possible examination of their communications by prison staff, as well as the importance of only discussing prosecuted offences.[78]

B. Legal Documents

The second source of data is indictments and other legal documents related to prosecuted cases of cybercrime. These are primarily drawn from the U.S., with a smaller number of documents from elsewhere. Many of the U.S. cases centrally involved the Computer Crime and Intellectual Property Section of the Criminal Division of the U.S.

---

[76] For an outline of similar precautions used in other research, *see* MARK ISRAEL & IAIN HAY, RESEARCH ETHICS FOR SOCIAL SCIENTISTS 77-94 (2006).
[77] Carol Matfin, *Doing Research in a Prison Setting*, *in* DOING CRIMINOLOGICAL RESEARCH 222, 228-30 (Victor Jupp, et al. eds., 2011).
[78] *Id.* at 229; *see also* Donald Newman, *Research Interviewing in Prison*, 49 J. CRIM. L., & POLICE SCI. 127, 131-32 (1958).

Department of Justice (DOJ). Once unsealed, these documents are accessible. The DOJ and others published a number of these documents online.[79]

C. Forum Archives

Finally, I also draw on archives of major cybercriminal forums, which are either publicly available online or were furnished to me. In particular, I examine the archive of an online marketplace called Darkode, as part of a detailed case study of cybercriminal governance. Crucially, an archive of data from this site is publicly available for download.[80] In 2023, the database from Darkode was leaked by a hacker called Xylitol. While most forum data analysed by scholars is scraped by researchers, such leaks have occurred as a result of hostile insider and external operations. Although few in number, these databases have become rich data for academic study.[81] The Darkode leak offers a window into an elite, technical closed-access forum. The fact that the Darkode forum leak is now considered a "historical" case is also an asset as it means that there are limited ethical issues in dealing with the data, and that there are more legal documents and other contextual information publicly available. Despite the public nature of the dataset, following recommended practices, I ensure that no offender or victim personal identifying information is contained within the data presented in this article.[82] For the Darkode case study, I draw on my own qualitative analysis of this dataset, indictments and other legal documents, public sources, and the small amount of literature on this marketplace which has been published by other scholars, most notably Benoît Dupont.[83]

IV. GOVERNING THE DIGITAL UNDERGROUND

Cybercriminals who operate online must navigate an inherently distrustful environment. To thrive, they are forced to employ numerous strategies to determine who is trustworthy and who is not.[84] This includes trying to divine aspects of a user's true identity

---

[79] *See, e.g.*, Press Release, U.S. Department of Justice, *Justice Department Announces Actions to Dismantle Kelihos Botnet* (April 10, 2017), https://www.justice.gov/archives/opa/pr/justice-department-announces-actions-dismantle-kelihos-botnet-0 [https://perma.cc/K3WU-WETH]; Press Release, U.S. Department of Justice, *Russian Citizen Pleads Guilty for Involvement in Global Botnet Conspiracy* (March 28, 2017), https://www.justice.gov/archives/opa/pr/russian-citizen-pleads-guilty-involvement-global-botnet-conspiracy [https://perma.cc/F25T-Y3VD].

[80] Data are held in a public repository at Darkode Cybercrime Tracker, accessible at *Tracker*, DARKODE REPOSITORY (last visited June 8, 2025), http://darkode.cybercrime-tracker.net [https://perma.cc/G65F-75AC].

[81] *See generally* Daniel Thomas, et al., *Ethical Issues in Research Using Datasets of Illicit Origin*, ACM (2017); Marti Motoyama, et al., *An Analysis of Underground Forums*, INTERNET MEASUREMENT CONFERENCE (2011).

[82] Thomas Holt, *Exploring Strategies for Qualitative Criminological and Criminal Justice Inquiry Using Online Data*, 21 *J. CRIM. JUST. EDUC.* 155, 156-58 (2017).

[83] *See, e.g.*, Benoit Dupont, et al., *Darkode: Recruitment Patterns and Transactional Features of "the Most Dangerous Cybercrime Forum in the World,"* 61 AMERICAN BEHAVIORAL SCIENTIST (2017); Benoit Dupont & Jonathan Lusthaus, *Countering Distrust in Illicit Online Networks: The Dispute Resolution Strategies of Cybercriminals*, 40 SOCIAL SCIENCE COMPUTER REVIEW (2022). For comparative articles that include Darkode in a broader analysis *see, e.g.*, Rebecca Portnoff, et al., *Tools for Automated Analysis of Cybercriminal Markets*, ACM 657, 658-59 (2017); Greg Durrett, et al., *Identifying Products in Online Cybercrime Marketplaces: A Dataset for Fine-grained Domain Adaptation*, ASS'N FOR COMPUTATIONAL LINGUISTICS 2598, 2599 (2017).

[84] *See, e.g.*, Lusthaus, *Trust in the World of Cybercrime*, *supra* note 24, at 80-85; LUSTHAUS, INDUSTRY OF ANONYMITY, supra note 2, at 83.

from their digital "appearance." They can also assess performance, whereby potential collaborators must overcome certain tests to garner trust.[85] But the two most significant mechanisms that aid cooperation, and are central to cybercriminal governance, are reputation and enforcement. Reputation is a component of trustworthiness, but enforcement offers a mechanism that can skirt the need for direct trust between collaborators at all. This section examines how reputation and enforcement are employed as part of cybercriminal governance, and particularly the way these mechanisms allow cooperation to be scaled up from smaller to larger groupings.

A. Reputation

Reputation plays a very important role for cybercriminals online.[86] One former hacker argued that the "whole world revolves around reputation, everything revolves around reputation."[87] Jonas, who was a malware developer, said that customers were much more aggressive towards him when he was starting out, but once he had built up a track record, he could take greater time in dealing with their requests.[88] Former spammer, Dave, also emphasised the central value of reputation in the underworld. He now works in legitimate industry and was surprised by the levels of trust within each world: "I've been ripped off more times by corporates and commercials. Like companies I'm working for legitimately, with a fucking contract, than I have by people you would consider the scum of the earth."[89]

In small-scale interactions, cybercriminals rely on reputation, leveraging the value found in both repeated interactions and referrals. It is intuitive that cybercriminals trust each other more after a series of transactions or collaborations. Through repeated interactions, partners are able to incrementally learn about the other, test each other, and punish defections. It is also possible that a "tradition of trust" is created when there is more to gain from future dealings rather than defecting in one deal alone.[90] This was borne out empirically.[91] Thiago, a South American former cybercriminal, had worked with some collaborators for over a decade, and gradually built trust over time.[92] Ivan, an Eastern European former cybercriminal involved in the malware business, was even more forthright on the value of repeated interactions:

> After first couple of deals are done, that is where the trust is beginning to grow. So, if you have done successful deals with a person in the past, then it is

[85] *See* LUSTHAUS, INDUSTRY OF ANONYMITY, supra note 2, at 120-23.
[86] *See, e.g.*, In-Person Interview with Former Expatriate Cybercriminal Based in Southeast Asia 1 (on file with author); Telephone Interview with U.S. Law Enforcement Agent 2 (2013) (on file with author); Telephone Interview with Expatriate Cybersecurity Professional Based in America 1 (2012) (on file with author); In-Person Interview with Ukrainian Law Enforcement Agent 2 (2015) (on file with author); Written Interview with Former Southeast Asian Cybercriminal 2 (on file with author); Written Interview with Former North American Cybercriminal 2 (on file with author).
[87] In-Person Interview with British Cybersecurity Professional 1 (2011) (on file with author).
[88] Telephone Interview with Former Western European Cybercriminal 3 (on file with author).
[89] In-Person Interview with Former Expatriate Cybercriminal Based in Southeast Asia 1 (on file with author).
[90] *See* SCHELLING, THE STRATEGY OF CONFLICT, *supra* note 33, at 134-35.
[91] In-Person Interview with Ukrainian Law Enforcement Agent 2 (2015) (on file with author); Written interview with Former Southeast Asian Cybercriminal 2 (on file with author).
[92] In-Person Interview with Former South American Cybercriminal 1 (on file with author).

> unlikely that he will disappear after another one— it is just not in his best interest; it will not going to make any sense, because he will make more money by continuing doing business with you, than by ripping you off. So, growth of trust is based on analysis of a person's egoistic motives[.][93]

Scott, a North American former cybercriminal, also preferred working with partners with whom he had prior experience: "Once I found someone that could do a certain thing or provide a certain service well or whatever, I would just keep using him until he no longer could, ripped me off, or quit/disappeared or whatever."[94]

Relying on repeated interactions alone, however, means that a user can only work with those they know. Repeated interaction also does not address the question of how cybercriminals locate their partners in the first place. These challenges could be overcome by using referrals and background checks. As Scott explained:

> If you are not using a forum, then word-of-mouth is another thing people use. If you are looking for someone to provide a service you need and you have some other people you are already working with on other things, it's always good to ask them first if they know a good cashout guy, or dumps vendor, id vendor or whatever it may be. Usually, that is your best option (or it was for me) and used forums as a sort of last resort because of the ripper potential and its always better to work with a person that someone you already trust, trusts (ha).[95]

Daniel, a cybersecurity expert with a deep knowledge of the cybercrime scene, made a similar argument: "If you need to get to a person in the underground, don't go to them direct you go through people they know and trust."[96]

Regarding background checks, there is extensive user information online that can be compared to how a prospective partner presents themselves.[97] Such electronic footprints include information contained in posts and evidence of past affiliations with particular groups and marketplaces. Some cybercriminals take matters further by hacking into other users' email accounts and computers to gather intelligence: "The more you know, the better."[98]

---

[93] Written Interview with Former Eastern European Cybercriminal 3 (on file with author). In their study of leaked forums, Motoyama and colleagues find that a significant number of responses to advertisements came from existing contacts. *See* Motoyama, et al., *supra* note 81, at 75. While the online drug trade is outside the scope of this article, there is also a growing literature on the importance of reputation in these settings. *See, e.g.*, Wojtek Przepiorka, et al., *Order without Law: Reputation Promotes Cooperation in a Cryptomarket for Illegal Drugs*, 6 EUR. SOCIO. REV. 752, 753-54 (2017); Robert Hardy & Julia Norgaard, *Reputation in the Internet Black Market: An Empirical and Theoretical Analysis of the Deep Web*, 12 J. INSTITUTIONAL ECON. 515, 519-22 (2016).

[94] Written Interview with Former North American Cybercriminal 2 (on file with author).

[95] Written Interview with Former North American Cybercriminal 2 (on file with author).

[96] In-Person Interview with Expatriate Cybersecurity Professional Based in the Netherlands 1 (2014) (on file with author).

[97] In-Person and Written Interview with Former Western European Cybercriminal 1 (on file with author); Written Interview with Former North American Cybercriminal 2 (on file with author); In-Person Interview with Ukrainian Cybersecurity Professional 1 (2015) (on file with author).

[98] Written Interview with Former North American Cybercriminal 2 (on file with author).

Even with adding referrals and background checks to the value of repeated interactions, the scale of cooperation remains limited. Major forums can have memberships in the thousands, meaning that the costs of referrals and background checks could be substantial, especially since many users likely neither are acquainted with one another nor have mutual contacts. It is only when aspects of reputation are institutionalised and scaled up that elements of governance begin to emerge, allowing larger groups to interact with some degree of order.

Online marketplaces have enhanced the reputation mechanism in a range of ways. Some have employed numerical indices, whereby members, administrators, or moderators rate user conduct. When these metrics are published on user profiles, they offer a way for others to determine how risky cooperation with a particular individual would be.[99] Jonas mentioned that he chose a key collaborator based on such a reputation score.[100] Some marketplaces also award ranks to classes of its members. For instance, Ghostmarket stamped the label "trusted member" on users who could prove their "criminal credentials to the administrator and moderators."[101]

While such tools have some worth, the data I collected suggested that the written feedback users provide on threads also has significant value. As with legitimate e-commerce sites, it is common for users to provide reviews on their dealings with sellers.[102] Scott outlined the importance of this:

> If you are advertising your service on a forum etc., then you have your own thread where people leave feedback for your service and products etc. Kind of like eBay, you do business with the guy, you leave feedback in his thread saying if he was helpful and legit or not or if you had any problems etc. If you see someone on there that has been dealing with several other people you know for a while and the people you already know and trust are leaving good feedback, then probably ok to deal with him[.][103]

Also of relevance are the "name-and-shame" or "scammer" subsections that some forums contain.[104] These subforums allow users to warn others against "rippers" and post evidence of misbehaviour, which may result in punishment for the misbehaving user. Nevertheless, even in cases where the malefactors are not banned, this public shaming can be

---

[99] *See* Décary-Hétu & Dupont, *supra* note 70, at 183-84 (2013).
[100] Telephone Interview with Former Western European Cybercriminal 3 (on file with author).
[101] R. v. Kelly and Others [2011], SWCC Crim 35 (discussed in the Case Summary).
[102] *See, e.g.*, In-Person Interview with Russian Cybersecurity Professional 5 (2014) (on file with author); In-Person Interview with Russian Cybersecurity Professional 6 (2014) (on file with author); In-Person Interview with Former Ukrainian Law Enforcement Agent 2 (2015) (on file with author). *See also*, Thomas Holt, *Exploring the Social Organisation and Structure of Stolen Data Markets*, 14 GLOB. CRIME 155, 158, 166 (2013); Thomas Holt, *Examining the Forces Shaping Cybercrime Markets Online*, 31 SOC. SCI. COMPUT. REV. 166, 171-72 (2012).
[103] Written Interview with Former North American Cybercriminal 2 (on file with author).
[104] *See, e.g.*, R. v, Kelly and Others, *supra* note 101.

viewed as a form of reputational damage. An example of such a subforum that exists on Darkode will be discussed in greater detail in the next section.

Some more elite cybercrime marketplaces have institutionalised the use of referrals to assess reputation. The effect of this is to reduce the need for (and cost on) each individual member to vet any other member they may deal with. This is achieved through a more formal vouching process to gain membership to a closed online community. It is common for such forums to request that new members are vouched for by at least two existing members.[105] Some sites may require even harsher entry protocols, including either demanding more members to vouch for a prospective entrant and/or requiring the vouching users to have been forum members for a certain number of years.[106] There may also be a rule punishing those that endorsed a member who ends up breaking community rules, including by having to remunerate anyone who has been scammed or being expelled from the marketplace.[107] Marketplaces may specifically vet prospective vendors and their products and services, which reduces the requirement for users to independently vet each vendor they intend to engage.[108] Often, marketplaces assign labels, such as "verified vendor" or "reviewed vendor", to those sellers who have passed this process.[109]

This analysis of cybercriminal reputation is largely in keeping with existing theory and studies in other empirical settings. In particular, the marketplace institutions that enhance reputation are not dissimilar to those found on legal auction sites, the most famous being eBay.[110] But there are also strong parallels with historical settings, which, at first glance, would seem starkly different.[111] For instance, comparisons can be made to the widely discussed case of the Champagne fairs of Medieval France, which drew together traders from

---

[105] *See, e.g.*, In-Person Interview with Ukrainian Cybersecurity Professional 1 (2015) (on file with author); In-Person Interview with Former Nigerian Law Enforcement Agent 1 (2016) (on file with author); In-Person Interview with Russian Cybersecurity Professional 5 and Russian Cybersecurity Professional 6 (2014) (on file with author).

[106] Written Interview with Cybersecurity Professional 1 (2013) (on file with author).

[107] Written Interview with Former North American Cybercriminal 2 (on file with author). Another strategy to vet membership is to require the payment of entry fees. Sometimes the fees are large, but they can also be as little as $100. This may seem like a paltry amount, but it may be enough to keep out young "noobs" and "script kiddies," who lack experience and capability. It is likely that undercover law enforcement agents could overcome this barrier to entry, but some private-sector security professionals may be blocked by corporate rules that restrict any funds being paid to criminals, even as part of intelligence gathering.

[108] In-Person Interview with Former Ukrainian Law Enforcement Agent 2 (2015) (on file with author); In-Person Interview with Russian Cybersecurity Professional 5 and Russian Cybersecurity Professional 6 (2014) (on file with author).

[109] *See, e.g.*, Holt, *Examining the Forces Shaping Cybercrime Markets Online*, *supra* note 102, at 173; Thomas Holt & Eric Lampke, *Exploring Stolen Data Markets Online: Products and Market Forces*, 23 CRIM. JUST. STUD., 33, 43-44 (2010); Yip, et al., *supra* note 25, at 526-28.

[110] *See* Chrysanthos Dellarocas, *The Digitization of Word-of-Mouth: Promise and Challenges of Online Feedback Mechanisms*, 49 MGMT SCI. 1407, 1408-09 (2003); *see also generally* Paul Resnick & Rihard Zeckhauser, *Trust among Strangers in Internet Transactions: Empirical Analysis of eBay's Reputation System*, *in* THE ECONOMICS OF THE INTERNET AND E-COMMERCE 129-30 (Michael Baye ed. 2002). Andreas Diekmann, et al., *Trust and Reputation in Internet Auctions*, *in* ETRUST: FORMING RELATIONSHIPS IN THE ONLINE WORLD 140 (Karen Cook, et al. eds., 2009).

[111] *See generally* Paul Milgrom, et al., *The Role of Institutions in the Revival of Trade: The Law Merchant, Private Judges, and the Champagne Fairs*, 2 ECONOMICS AND POLITICS 1-4, 16-18 (1990).

across Europe.[112] As merchants came and left the market, however, major challenges of trust and contract enforcement arose.[113] For example, in the event a party did not honour a deal struck at the fair, there was a critical question of how that renegade party could be brought into compliance or punished, considering that, upon leaving, they would be in a faraway jurisdiction.[114] Some scholars argue that the Champagne fairs overcame such challenges by private judges keeping records on past merchant behaviour.[115] In order to minimise the prevalence of malefactors, traders could consult these records in advance of doing business with a new partner, learning about their reputation before deciding whether to engage them.[116] While there is a tendency to look for the new or exotic in relation to the governance of cybercrime, the institutions that enhance reputation may be quite familiar already.

B. Enforcement

Enforcement is also a vital mechanism in the governance of cybercrime. Enforcement can significantly aid cooperation, even in the absence of direct trust between criminal partners. A Southeast Asian former cybercriminal, Tan, summarised matters in this way: "To me, the cybercriminals are working as the same mentality as the real-world criminals, it's about trust, integrity, and so if ones wants to play the game, ones have to follow the rules or ones will get punishment."[117] The following analysis adopts a broad view of enforcement, which includes elements such as monitoring, credible commitments, and punishment.[118] There are three types of enforcement that are relevant to cybercrime: self-enforcement, collective enforcement, and enforcement by a third party. In terms of governance, the latter two forms are of greater interest.

In online settings, cybercriminals have few enforcement avenues. In such a virtual environment, the conventional criminal tool of violence is removed. Nevertheless, cybercriminals have developed some other means of punishing defectors. The simplest is to cease further cooperation, but there are also some weaker virtual parallels to physical violence. One option is to carry out DDoS attacks against other users or against competing groups, which is a fairly widespread tactic among cybercriminals.[119] These attacks overwhelm computers or systems with traffic, effectively knocking them offline. Other novel forms of punishment are also possible in this digital environment. For instance, "doxing" occurs when a cybercriminal obtains the personal information of another user and publishes it on the internet.[120] At minimum, this tactic causes embarrassment, particularly as anonymity is so important to cybercriminals and their operations. It may also lead to more serious consequences, including arrest.[121] Another mode of punishment is "swatting," whereby one

[112] *See id.* at 2-4.
[113] *See id.* at 19-21.
[114] *See id.* at 14, 19. 108
[115] *See id.* at 14-18.
[116] *See id.*
[117] Written Interview with Former Southeast Asian Cybercriminal 2 (on file with author).
[118] *See* LUSTHAUS, INDUSTRY OF ANONYMITY, *supra* note 2, at 21-27
[119] Written Interview with Former North American Cybercriminal 2 (on file with author); *see* Benoit Dupont, *Skills and Trust: A Tour Inside the Hard Drives of Computer Hackers*, *in* CRIME AND NETWORKS 195-217 (Carlo Morselli, ed., 2014).
[120] In-Person Interview with Former U.S. Law Enforcement Agent 2 (2012) (on file with author).
[121] Written Interview with Former North American Cybercriminal 2 (on file with author).

cybercriminal makes a fraudulent emergency call, sending an armed police unit to the target's address.[122] The aggrieved party themselves can carry out DDoS attacks, doxing, and swatting, but they can also hire professional services for this purpose.[123]

In order to scale up cooperation from the individual level, cybercriminal institutions such as marketplaces and other settings magnify and expand enforcement. Site administrators and moderators make and police rules for membership. Existing literature most commonly describes banning from a site or group as a form of institutional punishment.[124] The data I collected supports the view that banning is a common and powerful enforcement tool.[125] This leads to a form of social death and the killing of the reputation attached to the nickname in question.[126]

Connected to banning is a particularly central component of cybercriminal governance: arbitration. Arbitration is present within a number of settings and often appears as an online trial of sorts, though it is considerably more informal than those trials found within the legitimate justice system.[127] Nikita, a former Ukrainian law enforcement agent, explained that within the Russian-speaking scene, arbitrators are often independent specialists, summoned to resolve disputes across a number of forums:

> It's his role to research all the evidence. The guys present evidence and the usual evidence is the chats. So, they usually communicate through Jabber and mostly they post chat logs or screen shots. In some cases, if it involved malware for example, they might give access to that malware control panel, for example, to the arbiter for him to see to test it and then after these several posts by both sides providing their evidence, the arbiter makes his decision. The usual decision is to expel the party that was involved in wrongdoing. Others may also provide their input. It's kind of like regular court hearings, but online in the underground world. There are witnesses, evidence, the judge —the arbiter—who makes the decisions.[128]

English-language marketplaces employ a similar process, but the arbitrators themselves are commonly the administrators of the sites where the dispute took place rather than independent (external) professionals.[129]

---

[122] *See* Brian Krebs, *The World Has No Room For Cowards*, KREBS SEC. (Mar. 15 2013), http://krebsonsecurity.com/2013/03/the-world-has-no-room-for-cowards/ [https://perma.cc/2NDE-RMTM]. One of the most famous examples of swatting was carried out against the leading cybersecurity blogger, Brian Krebs, whose deep reporting sometimes threatens some cybercriminals and their operations. *See id.*

[123] Written Interview with Former North American Cybercriminal 2 (on file with author).

[124] *See* Holt, *Exploring the Social Organisation and Structure of Stolen Data Markets*, *supra* note 102, at 156, 166-67; Holt & Lampke, *supra* note 109, at 44.

[125] In-Person Interview with Ukrainian Cybersecurity Professional 1 (2015) (on file with author); Written Interview with Former Middle East and North African Cybercriminal 1 (on file with author).

[126] *Id.*

[127] Written Interview with former Eastern European Cybercriminal 3 (on file with author); In-Person Interview with Russian Cybersecurity Professional 5 and Russian Cybersecurity Professional 6 (2014) (on file with author).

[128] In-Person Interview with Nikita, former Ukrainian Law Enforcement Agent 2 (2015) (on file with author).

[129] Written Interview with Scott, former North American Cybercriminal 2 (on file with author).

The second major enforcement institution within cybercrime settings is also a familiar one: escrow. Sometimes site administrators provide escrow, but other reputable figures can also perform this role.[130] Often, the guarantor holds the payment until the seller provides the goods, but the guarantor can also handle the exchange of both the payment and the goods. A commission of around three to five percent is often the fee required in exchange for this service.[131] The existing literature notes the presence of cybercriminal escrow,[132] but few details are known about how it functions at a granular level. North American former cybercriminal Scott provided some of these elements:

> Also, there are escrow services that are usually offered by some of the higher people in the forums (Admin, Mods, etc.). If you are doing a big deal with someone (say you are purchasing an entire database of dumps for $30,000 for example) and you want to make sure this person doesn't just take your $30k and run off, you would contact one of the escrow providers and ask for help. This way you have a third party (admin) that takes the $30k in Bitcoins or whatever and holds it until you confirm to him that you received the dumps you purchased and then he will take his fee out (5 percent or whatever he charges) and sends the money to the seller.[133]

The central question remains: how do users ensure that the escrow provider can be trusted? This question connects with the above discussion around reputation. Cybercriminal guarantors are often seen as the "wise old men," who have been around the underground for a long period of time and have a record of good past behaviour.[134] Cybersecurity professional Brendan listed the characteristics of an escrow provider as someone with a "lot of posts, who is very trusted and has more to lose screwing people over," adding that their "business is their reputation."[135] More reliable figures can be high ranking administrators on marketplaces who held a good reputation for some time.[136] Some guarantors have built their reputations over many years, which is an age in the cybercriminal underground. In short, they have the "ultimate reputation."[137] While guarantors will never be uniformly reliable, numerous interview participants believed these figures often took many years to develop their

[130] In-Person Interview with former Ukrainian Law Enforcement Agent 2 (2015) (on file with author); In-Person Interview with Ukrainian Cybersecurity Professional 1 (2015) (on file with author); Written Interview with Scott, former North American Cybercriminal 2 (on file with author); Written Interview with former Southeast Asian Cybercriminal 2 (on file with author); In-Person Interview with Expatriate Cybersecurity Professional Based in the Netherlands 1 (2014) (on file with author).

[131] In-Person Interview with Maksym, Ukrainian Cybersecurity Professional 1 (2015) (on file with author); Written Interview with former Southeast Asian Cybercriminal 2 (on file with author).

[132] *See* Yip et al., *supra* note 25, at 528–29; Alice Hutchings & Thomas J. Holt, *The Online Stolen Data Market: Disruption and Intervention Approaches*, 18 GLOB. CRIME 11, 12 (2017); Holt, *supra* note 102, at 173; Lusthaus, *supra* note 24, at 90.

[133] Written Interview with Scott, former North American Cybercriminal 2 (on file with author).

[134] In-Person Interview with Russian Cybersecurity Professional 5 and Russian Cybersecurity Professional 6 (2014) (on file with author).

[135] In-Person Interview and Written Interview with Brendan, Irish Cybersecurity Professional 2 (2014; 2018) (on file with author).

[136] In-Person Interview with Maksym, Ukrainian Cybersecurity Professional 1 (2015) (on file with author); Written Interview with Scott, former North American Cybercriminal 2 (on file with author).

[137] Written Interview with Scott, former North American Cybercriminal 2 (on file with author).

reputations. Ukrainian cybersecurity professional Maksym stated that intentional non-performance by an escrow provider (taking the payment without delivering the promised service) would be very rare, comparing such an event to a "nuclear explosion" if it happened.[138]

Marketplaces and other settings scale the cybercriminal enforcement mechanism to much larger numbers. Without formal institutions, like arbitration and escrow, dealing with previously unknown partners becomes more difficult. Self-enforcement would need to be carried out by individuals, which would be time-consuming and less effective in many cases. To reduce the need for such costly self-enforcement, or allow it to function more effectively, opportunities for trade and cooperation would need to be limited to a smaller circle of close contacts. In short, and in keeping with the theory discussed above, these enforcement institutions have aided the development of order in an otherwise chaotic underworld. When administrators and moderators create and enforce a system of rules and punishments, provide third party guarantees, and arbitrate disputes, they are providing governance. Former cybercriminal Mohammed likened this system of order to a "state of legit hackers."[139]

V. CASE STUDY: DARKODE

The above analysis, based primarily on interview data, provides an important overview of cybercriminal governance. But in order to get a deeper and more granular understanding of this topic, it is valuable to engage with a case study. Data availability limits the choice of case study. Many cybercrime scholars have studied open or easily accessible cybercriminal marketplaces and forums,[140] but this type of data captures only the most visible and arguably lower-tier levels of cybercrime. There are a number of layers within the cybercriminal underground with much more closed groupings observed.[141] There are a handful of studies that analyse data from vetted marketplaces that house more serious offenders.[142] A limited amount of this data is available for research purposes.

For this case study, I have chosen a closed and vetted cybercrime forum called Darkode. This marketplace was founded in 2008 and shut down by law enforcement in

---

[138] In-Person Interview with Maksym, Ukrainian Cybersecurity Professional 1 (2015) (on file with author); *cf*., Bhaskar et al., *The economic functioning of online drugs markets*, 159 J. ECON. BEHAV. & ORG. 426 , 426-441 (2019). One point of comparison outside the scope of this article is that escrow systems seem to be more reliable within cybercrime markets (for malware, fraud, and so on) than in cryptomarkets associated with the online drug trade. In drug settings, "exit scams" are relatively common, and particular administrators have abandoned marketplaces, taking the large amount of funds held within these sites' escrow systems. In one case, $12 million was stolen. *See* Nicky Woolf, *Bitcoin 'Exit Scam': Deep-Web Market Operators Disappear with $12m*, THE GUARDIAN (Feb. 21, 2017), https://www.theguardian.com/technology/2015/mar/18/bitcoin-deep-web-evolution-exit-scam-12-million-dollars [https://perma.cc/JE7S-L6Z6] .

[139] Written Interview with Mohammed, former Middle East and North African Cybercriminal 1 (on file with author).

[140] *See* Hutchings & Holt, *supra* note 131; Holt & Lampke, *supra* note 109; Benoît Dupont, et al., *The Ecology of Trust among Hackers*, 17 GLOBAL CRIME (2016).

[141] See Jonathan Lusthaus, *Beneath the Dark Web: Excavating the Layers of Cybercrime's Underground Economy*, IEEE EUR. SYMP. ON SEC. AND PRIV. WORKSHOPS 474 (2019).

[142] *See, e.g.*, Marti Motoyama et al., *An Analysis of Underground Forums*, PROC.ACM SIGCOMM INTERNET MEASUREMENT CONF. 71 (2011); Dupont et. al., *supra* note 83.

2015.[143] As such, it is no longer active, but during its time of operation, it had a reputation as one of the leading marketplaces for the more elite and technical cybercriminal actors in the English-speaking scene and beyond. Former U.S. Attorney for the Western District of Pennsylvania, David Hickton, characterised the site as follows: "Of the roughly 800 criminal internet forums worldwide, Darkode represented one of the gravest threats to the integrity of data on computers in the United States and around the world and was the most sophisticated English-speaking forum for criminal computer hackers in the world."[144] A review of Darkode's members shows a number of leading cybercriminals from across the globe, including several elite Eastern European offenders, such as Paunch (author of the Blackhole exploit kit), Gribodemon (author of the SpyEye banking trojan), and the only-recently-arrested ransomware power-player J.P. Morgan (the cybercriminal rather than financial company), who has been linked to ransomware and other operations.[145]

I mirror the governance analysis of the preceding section by engaging first with the reputation mechanism and then with the enforcement elements that the site employed.

A. Reputation

Two key aspects of reputation were central to the system of governance that Darkode used: (1) how entry into the marketplace was controlled, and (2) how the reputational information of each member was provided to the community. A close analysis of Darkode provides micro-level detail on these elements and some suggestions regarding how they evolved over time.

In its earliest days, the forum was a very small, "invite-only" community.[146] As the membership expanded, undercover agents from law enforcement and private industry were suspected to have infiltrated Darkode to gather intelligence.[147] In the middle period of the forum's history, the administrators at the time, Mafi and Fubar, began to strictly police accounts and ban those they suspected might not be bona fide cybercriminals.[148] In the last years of the forum, before law enforcement took it down, Sp3cial1st became an administrator and centralised the invitation mechanism under his control.[149]

---

[143] Ellen Nakashima, *Major Computer Hacking Forum Shut Down By 20 Countries, U.S. Announces*, WASH. POST (July 15, 2015), https://www.washingtonpost.com/world/national-security/major-computer-hacking-forum-shut-down-by-20-countries-us-announces/2015/07/15/dd4cf514-2b05-11e5-a5ea-cf74396e59ec_story.html [https://perma.cc/X63P-HHXM]; *See* Brian Krebs, *The Darkode Cybercrime Forum, Up Close*, KREBS ON SEC. (July 15, 2015), http://krebsonsecurity.com/2015/07/the-darkode-cybercrime-forum-up-close/ [https://perma.cc/77WB-QVCQ].

[144] Press Release, U.S. DEP'T. OF JUSTICE, *Major Computer Hacking Forum Dismantled* (July 15, 2015), https://www.justice.gov/opa/pr/major-computer-hacking-forum-dismantled [https://perma.cc/6FJQ-X3EU].

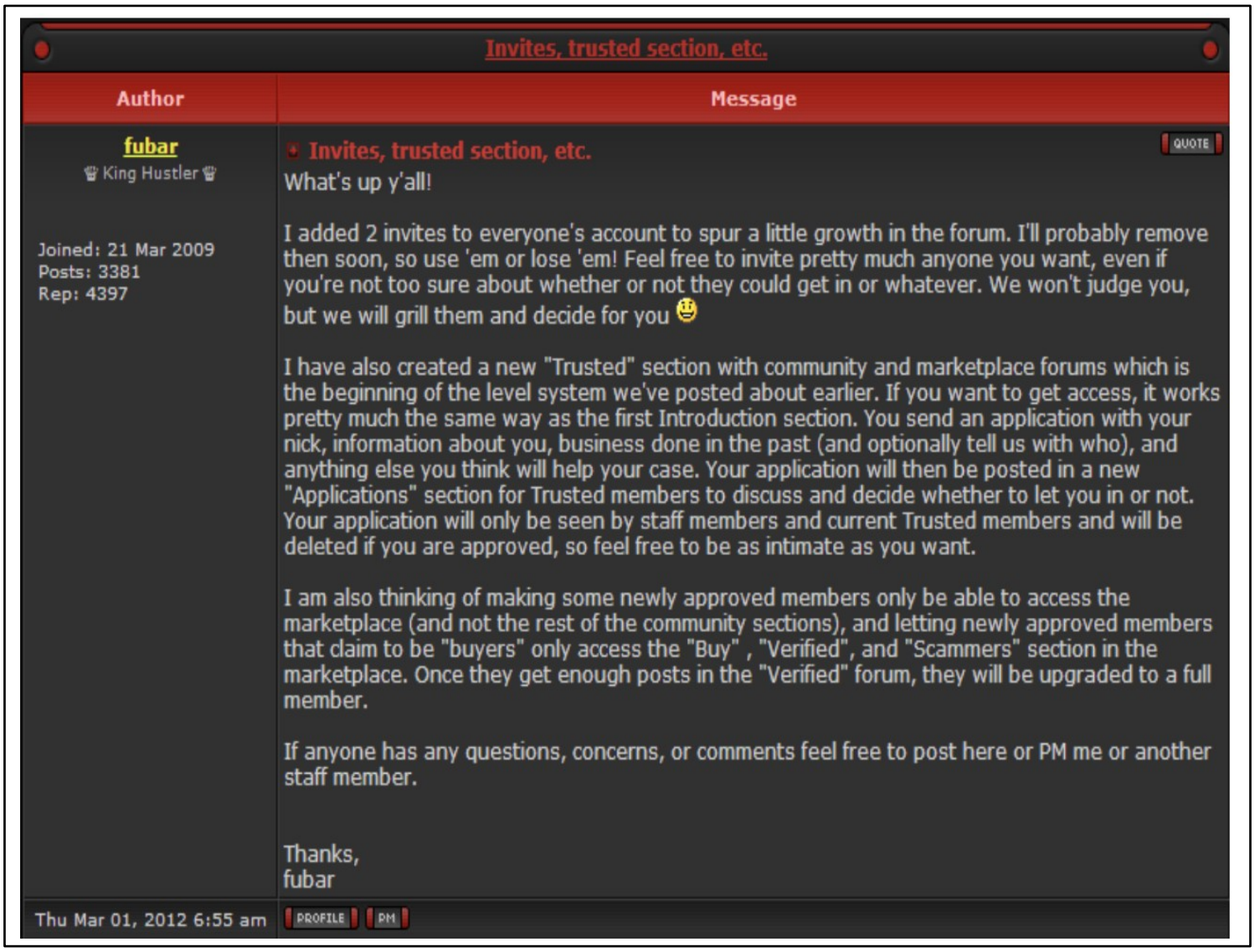
[145] *See* Dark Reading Staff, *Cybercriminal Leader 'J.P.Morgan' Busted for Pioneering RaaS Model*, DARK READING (Aug. 14, 2024), https://www.darkreading.com/cyber-risk/cybercriminal-leader-jp-morgan-busted-pioneering-raas [https://perma.cc/7Z8R-CJJ4]; Brian Krebs, *SpyEye Makers Get 24 Years in Prison*, KREBS ON SEC. (Apr. 20, 2016), https://krebsonsecurity.com/2016/04/spyeye-makers-get-24-years-in-prison/ [https://perma.cc/R6CQ-5VXH]; *Blackhole Malware Exploit Kit Suspect Arrested*, BBC (Oct. 9, 2013), https://www.bbc.co.uk/news/technology-24456988 [https://perma.cc/A7RH-MXV6].

[146] Dupont et. al., *supra* note 83, at 1224.

[147] *Id.* at 1237.

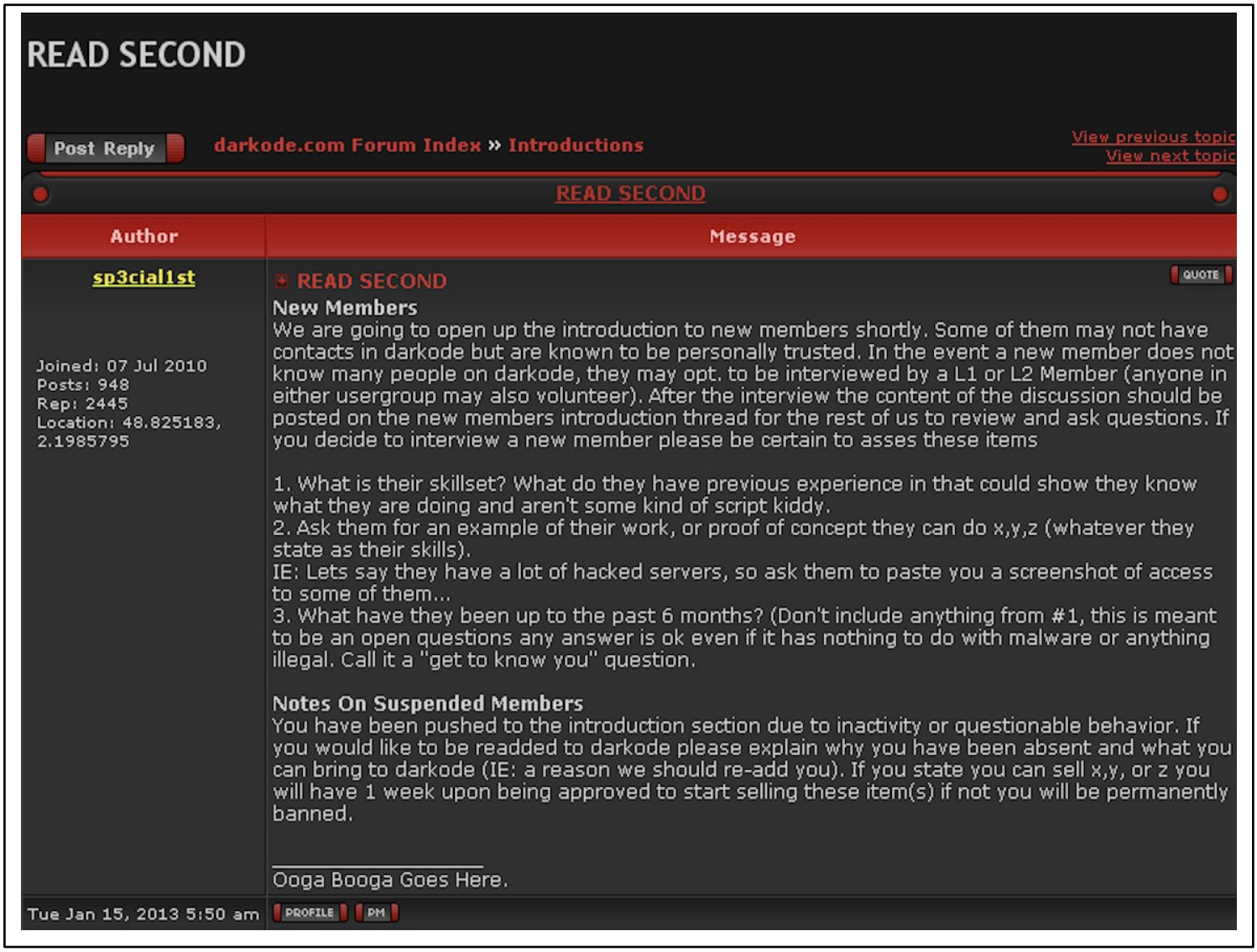
[148] *See* Krebs, *supra* note 122.

In general, the entry system largely matched the type of vouching outlined in the section above, except that only one sponsor was required instead of two or more. But there were extra layers of vetting built into this process. First, there were multiple membership levels with different degrees of access and privileges. These levels ranged from "Fresh Fish" at the bottom, through Levels 1 and 2, and finally into Moderators and Administrators.[150] Mafi, one of the administrators explains that "the point of the level system is to be less strict on the invitation, where more people will have a chance to contribute and eventually become level 1."[151] Fubar, another administrator, made clear that vetting wasn't just done when someone joined the forum, but it also determined what level of access within the forum they could have:



Invites, trusted section, etc.

Author	Message
fubar ♛ King Hustler ♛ Joined: 21 Mar 2009 Posts: 3381 Rep: 4397	Invites, trusted section, etc. QUOTE What's up y'all! I added 2 invites to everyone's account to spur a little growth in the forum. I'll probably remove then soon, so use 'em or lose 'em! Feel free to invite pretty much anyone you want, even if you're not too sure about whether or not they could get in or whatever. We won't judge you, but we will grill them and decide for you I have also created a new "Trusted" section with community and marketplace forums which is the beginning of the level system we've posted about earlier. If you want to get access, it works pretty much the same way as the first Introduction section. You send an application with your nick, information about you, business done in the past (and optionally tell us with who), and anything else you think will help your case. Your application will then be posted in a new "Applications" section for Trusted members to discuss and decide whether to let you in or not. Your application will only be seen by staff members and current Trusted members and will be deleted if you are approved, so feel free to be as intimate as you want. I am also thinking of making some newly approved members only be able to access the marketplace (and not the rest of the community sections), and letting newly approved members that claim to be "buyers" only access the "Buy" , "Verified", and "Scammers" section in the marketplace. Once they get enough posts in the "Verified" forum, they will be upgraded to a full member. If anyone has any questions, concerns, or comments feel free to post here or PM me or another staff member. Thanks, fubar
Thu Mar 01, 2012 6:55 am	PROFILE PM



READ SECOND

Post Reply darkode.com Forum Index » Introductions View previous topic View next topic

READ SECOND

Author	Message
sp3cial1st Joined: 07 Jul 2010 Posts: 948 Rep: 2445 Location: 48.825183, 2.1985795	READ SECOND QUOTE **New Members** We are going to open up the introduction to new members shortly. Some of them may not have contacts in darkode but are known to be personally trusted. In the event a new member does not know many people on darkode, they may opt. to be interviewed by a L1 or L2 Member (anyone in either usergroup may also volunteer). After the interview the content of the discussion should be posted on the new members introduction thread for the rest of us to review and ask questions. If you decide to interview a new member please be certain to asses these items 1. What is their skillset? What do they have previous experience in that could show they know what they are doing and aren't some kind of script kiddy. 2. Ask them for an example of their work, or proof of concept they can do x,y,z (whatever they state as their skills). IE: Lets say they have a lot of hacked servers, so ask them to paste you a screenshot of access to some of them... 3. What have they been up to the past 6 months? (Don't include anything from #1, this is meant to be an open questions any answer is ok even if it has nothing to do with malware or anything illegal. Call it a "get to know you" question. **Notes On Suspended Members** You have been pushed to the introduction section due to inactivity or questionable behavior. If you would like to be readded to darkode please explain why you have been absent and what you can bring to darkode (IE: a reason we should re-add you). If you state you can sell x,y, or z you will have 1 week upon being approved to start selling these item(s) if not you will be permanently banned. _____ Ooga Booga Goes Here.
Tue Jan 15, 2013 5:50 am	PROFILE PM

Figure 2: Darkode Thread B

New member introductions were an important source of information that the community reviewed. Dupont and co-authors analyse 344 applications from the introduction section, which included both new members and existing members who had been dormant for a long period of time.[152] This coding captured a number of elements, including who sponsored the member, their membership in other forums, technical skills, business interests, products they would offer, and motivation for joining.[153] Each introduction also received responses from existing members, who evaluated the new member and decided whether to accept or reject them, the latter of which would lead to account deletion.[154] This analysis shows that the sponsor, who invited and vouched for a new member, was a very important aspect of the introductions and was mentioned in over 90% of these posts.[155] The researchers add nuance by determining that the four forum administrators were responsible for 38% of invitations, and that some high-level members themselves provided few introductions, but rather focused on their own business interests.[156] Of those applications with a known outcome, around 95% were successful,[157] with only a small number of comments on posts (7%) expressing distrust.[158] While Dupont and co-authors find this high rate of success somewhat counterintuitive given the apparent exclusiveness of Darkode, the solution to this puzzle may lie in the fact that members must be invited to join, and that many of the invitations were coming from the most senior and trusted individuals on the site.

Addressing the second point regarding reputation and its management post-admission, Darkode largely conformed to the more general outline provided by the interview data in the preceding section. As seen in the data above, the forum published both quantitative and qualitative measures of reputation. The most easily accessible information on reputation was contained in the profile of each user. As reflected in Figures 1 and 2, this information included a member's date of joining, their number of posts, accumulated reputation points, and location (rarely accurate for obvious reasons). The date of joining and the number of posts are important for different but related reasons. The date of joining signals the length of time a user has spent in the community, which is meaningful, as the more time one has spent building up a reputation, the greater the cost is to burn that reputation through malfeasance.[159] The number of posts suggests how active a user is in the community, though this also intersects with the amount of time a user has been around. This

[152] *See* Dupont et. al., *supra* note 83, at 1228.
[153] *Id.*
[154] *Id.*
[155] *Id*. at 1230–31.
[156] *Id*.
[157] *Id*. at 1230.
[158] *Id*. at 1232.

signals a greater investment in, and commitment to, the community. The reputation points measure more directly captures reputation itself. In some forums, this measure is presented as an average out of, for instance, five. But in this case, it is a cumulative figure. The higher the number, the greater evidence of a good track record and overall trustworthiness.

Nonetheless, as interviewees noted, cybercriminals often assess reputation through qualitative feedback. This practice was very much present within Darkode, and close analysis shows that it occurred in a number of different ways, including through seller threads, a review section, and a verified seller procedure. First, some provided feedback within the seller threads, either on the product or service, or on the vendor themselves. Second, there was a dedicated review section as part of Darkode. Mafi, an administrator, makes the purpose of this section clear in the post below. Interestingly, the original intention was for user reviews to avoid the need for a formal verification process.[160]

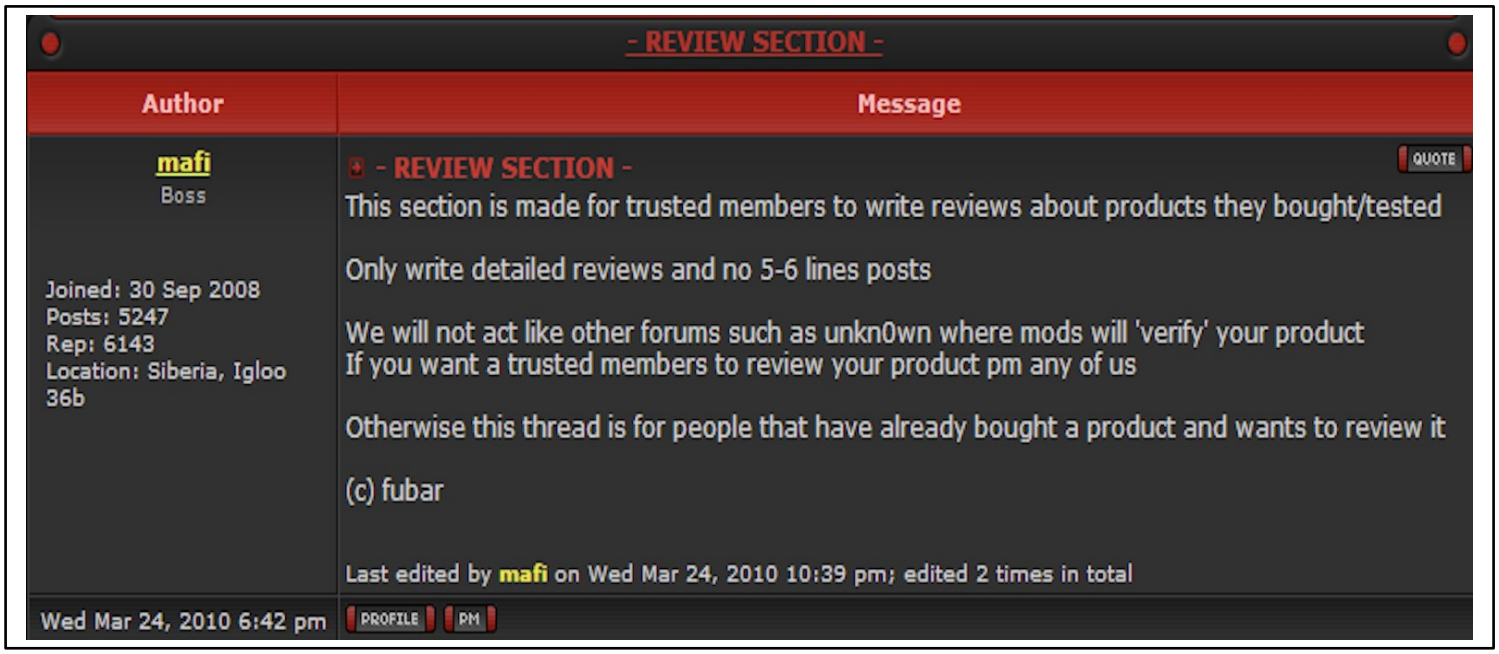
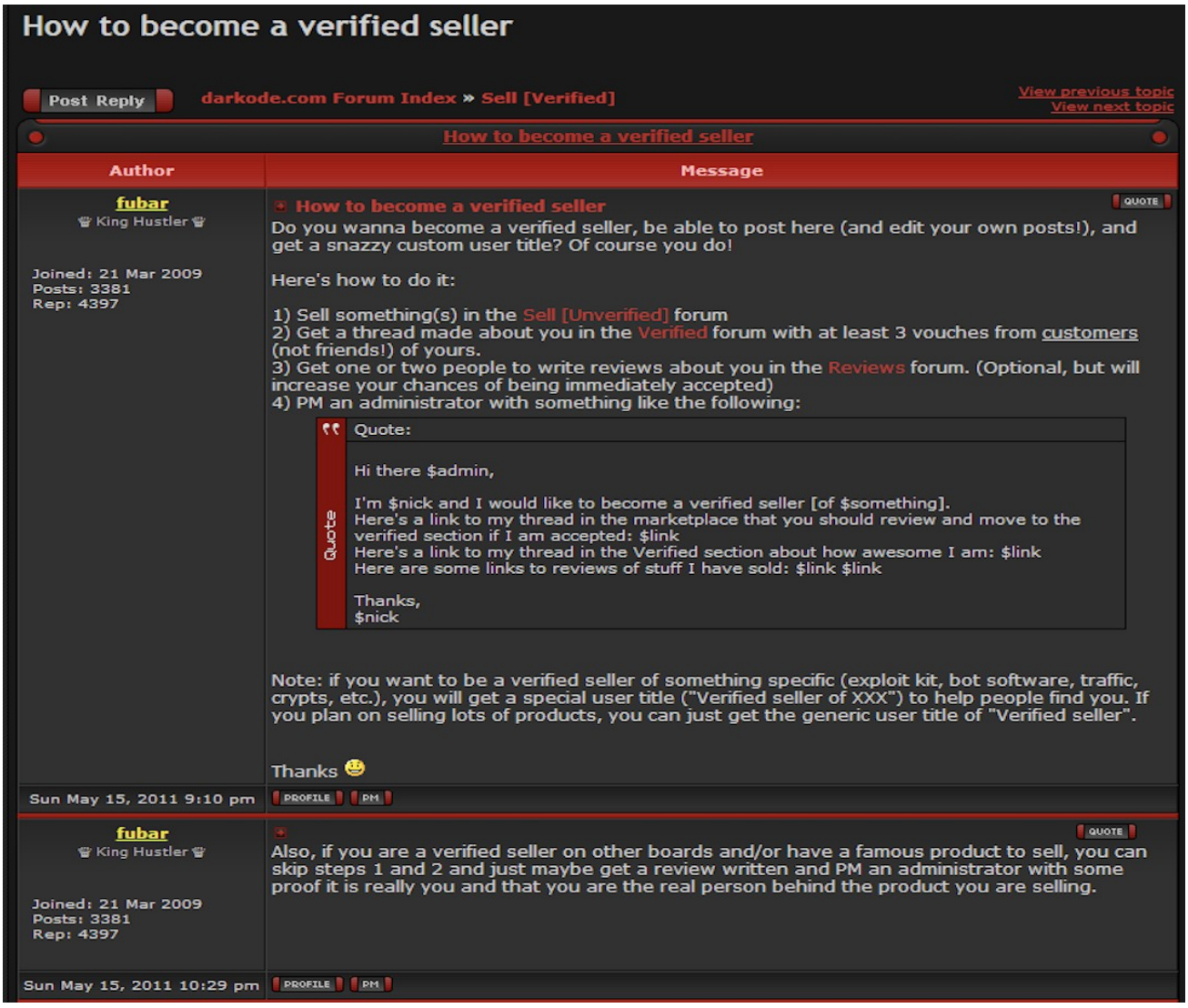


Figure 3: Darkode Thread C

[159] See Lusthaus, *supra* note 24, at 90, 93–94; LUSTHAUS, *supra* note 2, at 83–84; Jonathan Lusthaus, *Honour Among (Cyber)thieves?*, 59 EUR. J. SOCIO. 191, 203 (2018) for a more theoretical discussion on this point, signalling theory may be relevant in certain ways. Generally, signals are "any observable features of an agent that are *intentionally displayed* for the purpose of altering the probability the receiver assigns to a certain state of affairs." DIEGO GAMBETTA, CODES OF THE UNDERWORLD: HOW CRIMINALS COMMUNICATE XV (2011). Signalling theory is centred on this key concern: "under what conditions can a signal be rationally believed by the receiver when the signaller has an interest in merely pretending that something is true." *Id.* at xvii–xviii. For foundational discussions of signalling theory, see Diego Gambetta, *Signaling*, *in* THE OXFORD HANDBOOK OF ANALYTICAL SOCIOLOGY 168 (Peter Bearman & Peter Hedström eds., 2011); MICHAEL SPENCE, MARKET SIGNALING (1974); Michael Spence, *Job Market Signaling*, 87 Q. J. ECON. 355 (1973); Amotz Zahavi, *Mate Selection—A Selection for a Handicap*, 53 J. THEORETICAL BIOLOGY 205 (1975); AMOTZ ZAHAVI & AVISHAG ZAHAVI WITH NAAMA ZAHAVI-ELY & MELVIN PATRICK ELY, THE HANDICAP PRINCIPLE (1997).

[160] *See* Figure 3: Darkode Thread C.

The third element of qualitative feedback was the eventual introduction of a vendor



How to become a verified seller

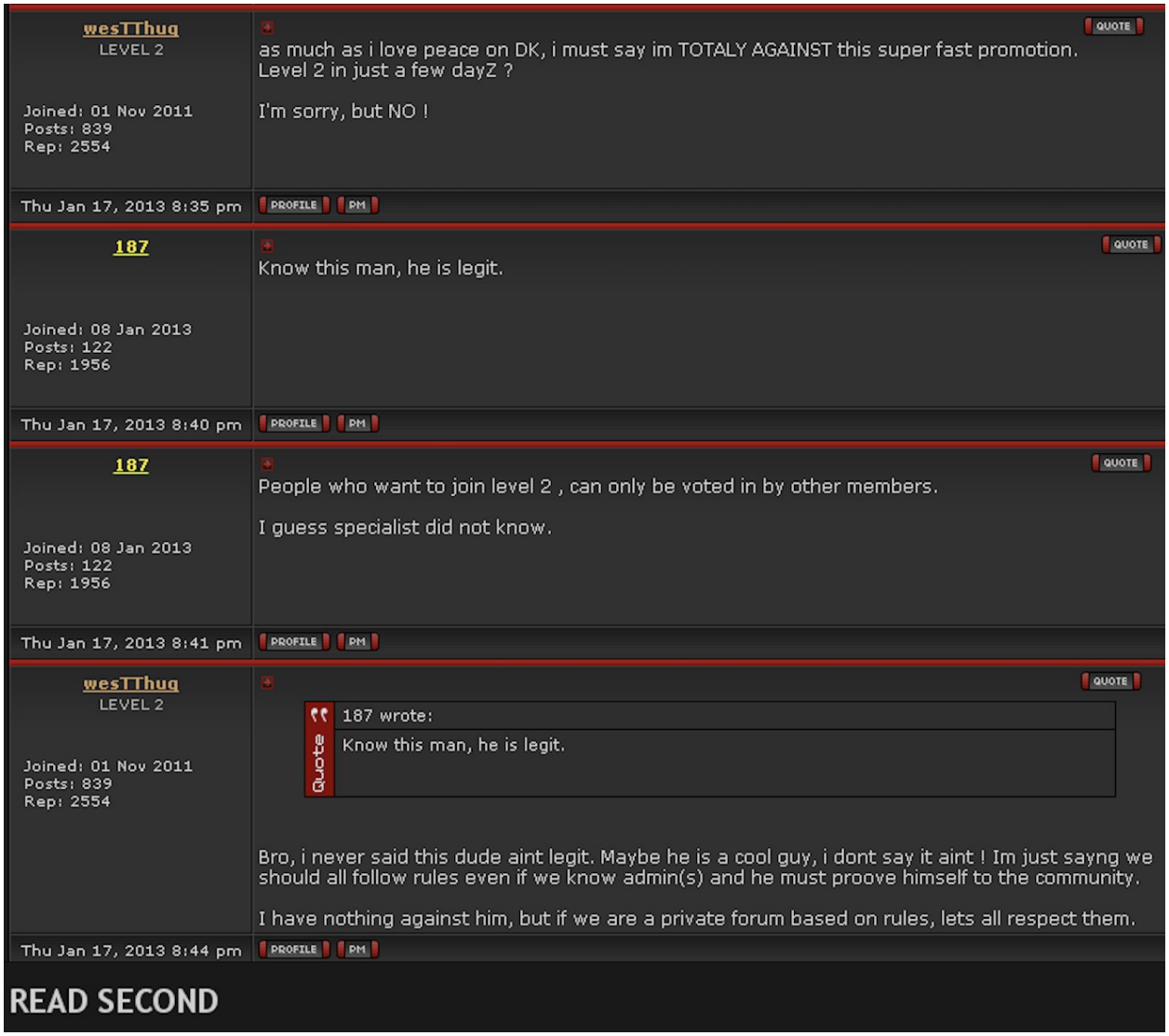
Post Reply darkode.com Forum Index » Sell [Verified]

View previous topic
View next topic

How to become a verified seller

Author	Message
fubar King Hustler Joined: 21 Mar 2009 Posts: 3381 Rep: 4397	How to become a verified seller QUOTE Do you wanna become a verified seller, be able to post here (and edit your own posts!), and get a snazzy custom user title? Of course you do! Here's how to do it: 1) Sell something(s) in the Sell [Unverified] forum 2) Get a thread made about you in the Verified forum with at least 3 vouches from customers (not friends!) of yours. 3) Get one or two people to write reviews about you in the Reviews forum. (Optional, but will increase your chances of being immediately accepted) 4) PM an administrator with something like the following: Quote: Hi there $admin, I'm $nick and I would like to become a verified seller [of $something]. Here's a link to my thread in the marketplace that you should review and move to the verified section if I am accepted: $link Here's a link to my thread in the Verified section about how awesome I am: $link Here are some links to reviews of stuff I have sold: $link $link Thanks, $nick Note: if you want to be a verified seller of something specific (exploit kit, bot software, traffic, crypts, etc.), you will get a special user title ("Verified seller of XXX") to help people find you. If you plan on selling lots of products, you can just get the generic user title of "Verified seller". Thanks
Sun May 15, 2011 9:10 pm	PROFILE PM
fubar King Hustler Joined: 21 Mar 2009 Posts: 3381 Rep: 4397	QUOTE Also, if you are a verified seller on other boards and/or have a famous product to sell, you can skip steps 1 and 2 and just maybe get a review written and PM an administrator with some proof it is really you and that you are the real person behind the product you are selling.
Sun May 15, 2011 10:29 pm	PROFILE PM

Figure 4: Darkode Thread D



[161] Dark Reading Staff, *supra* note 144.
[162] *Id.*

Figure 5A: Darkode Thread E (1/2)

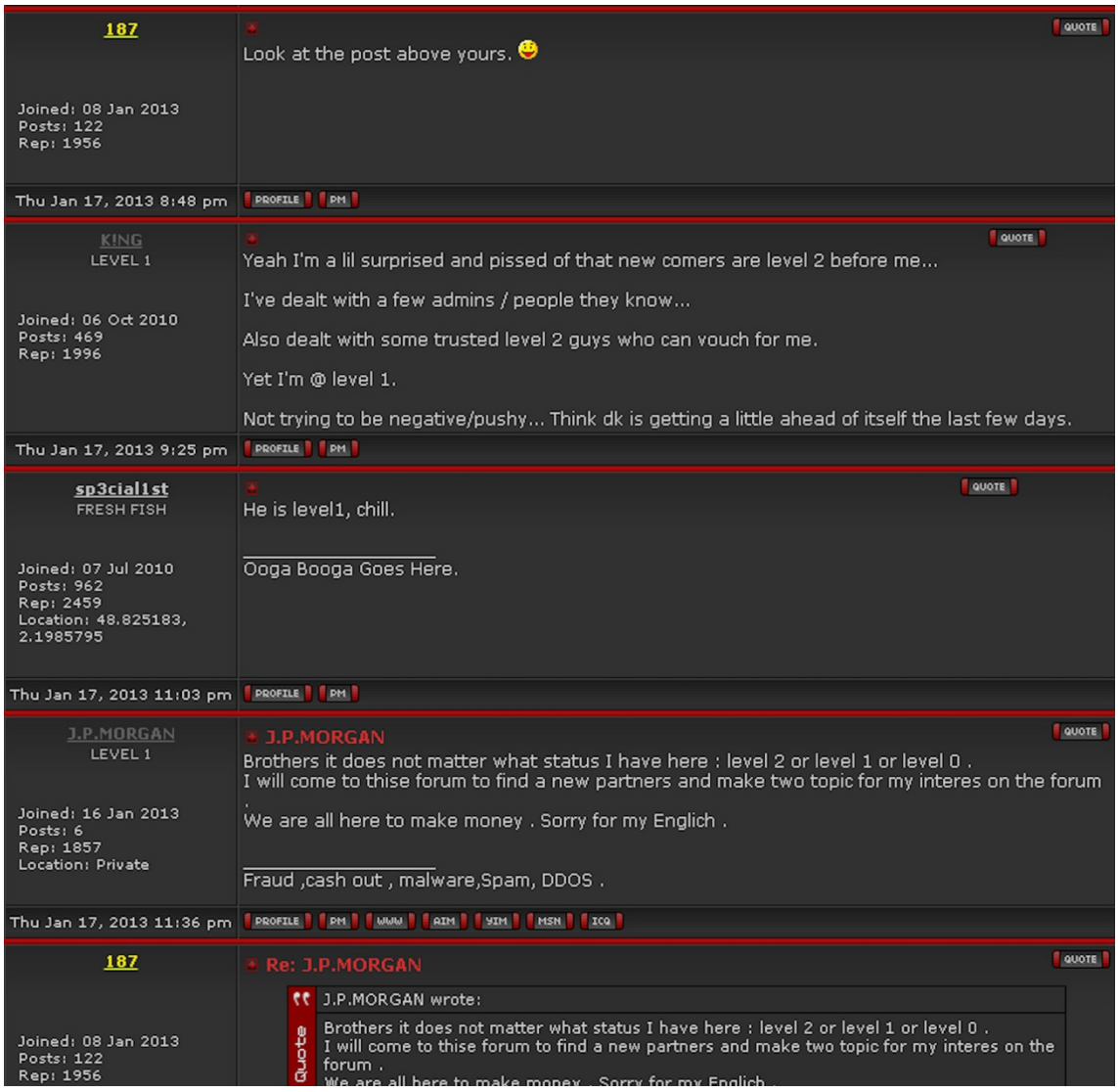


Figure 5B: Darkode Thread E (2/2)

B. Enforcement

The enforcement system that Darkode employed offered another component of governance for the community and again was largely in keeping with the broad strokes outlined above by the interview data. But this subsection conveys a more micro-level analysis of how such a system worked in practice. It first addresses the presence of an arbitration process and then discusses the relevance of escrow. This analysis employs both qualitative insights and descriptive statistics, drawing on posts across the archived database, but with a particular focus on the section of Darkode called "Scammers." As Figure 6 demonstrates, this section was specifically provided for members to make complaints against users they believed had acted against the rules of the community. In the archive, there were 160 disputes that could be coded.

A pinned post by one of the administrators provides important context on the Scammers section and the arbitration process:

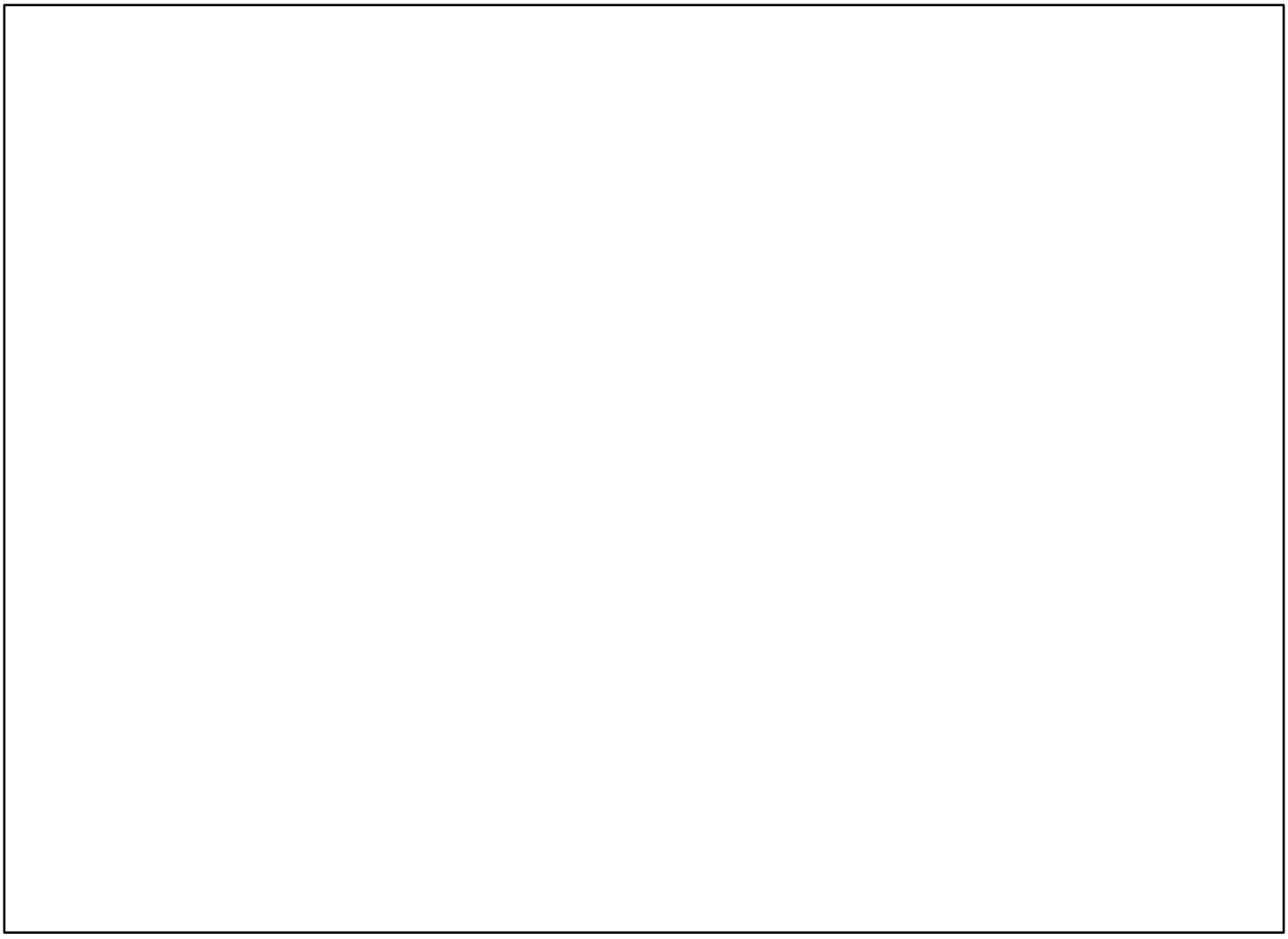


Figure 6: Darkode Thread F

The apparent purpose of this post was to signal that users were not meant to see reporting malfeasance to the Scammers section as a first step. Rather, users should have attempted to address the situation more informally, making an "official" report only if they had the requisite evidence to prove the bad behaviour. This procedure was intended to be a last resort within the community to identify and potentially resolve meaningful disputes. There also appears to have been an avenue for a more private process through private messaging, but the dataset does not contain those private messages, so this article cannot directly address that process.

Based on an analysis that I carried out with Benoît Dupont,[163] a number of findings are clear. First, despite the vetting process described above, a significant number of disputes still occurred.[164] Second, these disputes often involved users from the lower rungs of the forum, particularly Guests, Fresh Fish, and Level 1.[165] These more junior members were present both as defendants and plaintiffs, as summarised in Table 1.[166] Third, vendors were much more commonly accused than buyers.[167] Their offenses spanned a number of areas but were most regularly linked to providing a poor product or service, or not providing one at all.[168] The composition of offenses across the disputes can be found in Table 2.[169] Fourth, these disputes often centred around relatively small sums of money.[170]

Table 1: Distribution of all complaints according to the plaintiff's and accused's status[171]

	Status of the accused							
Status of plaintiff	Unknown	Non-Members	Guest	Fresh Fish	Level 1	Level 2	Administrator	Total
Suspended	0%	0.6%	1.2%	0%	0%	0%	0%	1.8%
Guest	20.0%	1.9%	25.0%	1.3%	1.2%	0%	0.6%	50.0%
Fresh Fish	3.7%	0%	6.3%	0.6%	1.3%	1.2%	0%	13.1%
Level 1	2.5%	1.2%	10.0%	1.3%	0.6%	0.6%	0%	16.2%
Level 2	1.9%	0.6%	1.3%	0%	1.3%	0%	0%	5.1%
Moderator	0%	0%	0.6%	0%	0%	0%	0%	0.6%
Administrator	3.8%	1.3%	7.5%	0.6%	0%	0%	0%	13.2%
Total	31.9%	5.6%	51.9%	3.8%	4.4%	1.8%	0.6%	100.0%

[163] *See* Dupont & Lusthaus, *supra* note 83.
[164] *Id.* at 900.
[165] *Id.*
[166] *Id.*
[167] *Id.*
[168] *Id.*
[169] *Id.*
[170] *Id*. at 908.
[171] *Id*. at 900.

Table 2: Distribution of all complaints according to the nature of disputes[172]

Type of dispute	*Frequency*	*%*
Seller took the money and didn't deliver the product	35	21.9
Warning about a member's unreliability (because of the use of multiple identities, a perceived lack of knowledge, untrustworthiness, excessive pricing policies, etc.)	24	15.0
Seller sold defective or incomplete products	23	14.4
Unspecified	17	10.6
One of the two parties did not abide by the terms of the deal	16	9.9
Buyer took delivery of a product but didn't pay (or failed to pay the full amount)	12	7.5
Seller distributing a product without the authorisation of the author or reselling free products	12	7.5
Seller took money and refused to refund	10	6.3
Seller did not provide adequate or expected customer support (including delay of responses or disappearance)	11	6.9
Total	160	100

The results from this analysis are partially expected but also surprising in certain ways. In terms of expected results, the high proportion of users from lower ranks present within disputes seems easily explainable. Those in the lower ranks were more likely to have joined more recently and not have accrued significant reputations. On the defendant side, they may not yet have demonstrated their trustworthiness and had less to lose if they decided to burn the reputation they had accrued by scamming. For the plaintiffs, their relative inexperience might have made it more difficult for them to select trustworthy partners and safe deals. Higher ranked members may not only have been more experienced, but their more significant reputations may have deterred junior victims from making complaints against them. In fact, most of the disputes involving high-ranking members within the data involved both plaintiffs and defendants of similar status. It is also unsurprising that vendors rather than buyers would field most complaints. Many sellers require payment in advance, which leaves them far less vulnerable. There is also less scope for grievance, as the buyer's role is simply to provide payment, which presents fewer subjective grey areas over whether the buyer has met the deal terms.[173]

Perhaps the most unexpected result is the small amounts involved in the disputes. The range was $20 to $18,000, but the mean loss was $1,175, the median $300, and the mode only $100.[174] These figures seem too low to prompt users to lodge an "official" complaint in a marketplace with an elite reputation, where some of the leading cybercriminals in the world converged and generated large sums of money. Possible solutions to this puzzle include: that users were willing to report minor grievances, either out of pettiness or to aid the broader functioning of the site; that lodging a complaint by post was not particularly costly; or that cybercrime is a business of volume, so even high earners would be engaged in a large

[172] *Id*. at 901.
[173] *Id*. at 908.
[174] *Id.* at 905.

number of relatively small transactions. But perhaps the most credible explanation is that, even within a leading marketplace, the top players remained a small group. Few members were earning millions from cybercrime.[175] The most successful Darkode users also may have been more effective in managing their operations and had lower exposure to these risks, so many of the disputes remained at a low status level.

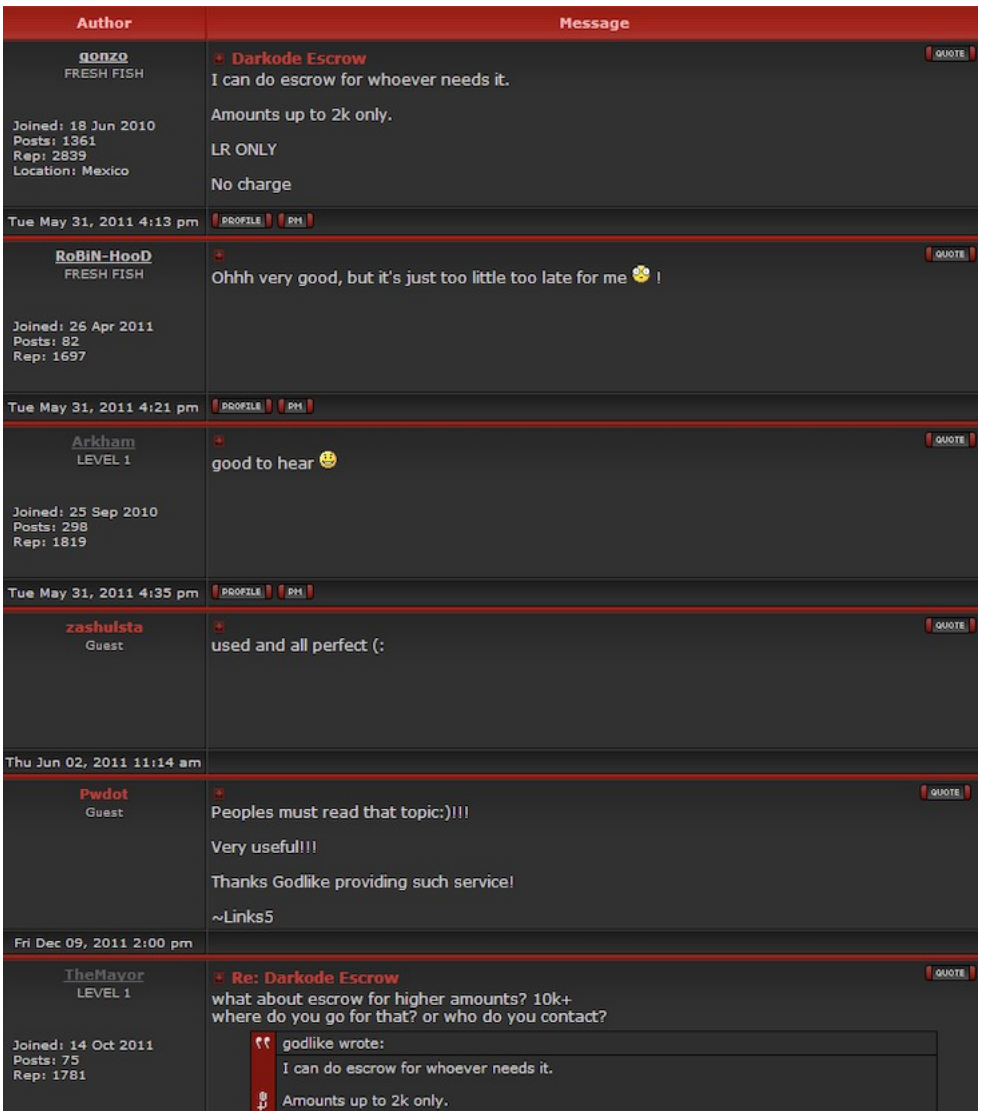
In terms of how these disputes were managed, there was a mix of formality and informality. In some sense, and as noted in the section above, this conflict resolution could take the appearance of a court proceeding or an arbitration. But with the irreverence of the cybercriminal community and the computer-mediated and looser ties of an online setting, not to mention the limited enforcement avenues, the Darkode arbitration process was a relatively informal one. From the public posts, it was clear that no formal arbitrator or mediator was appointed for each case, though administrators did step in to perform this role. Judgments of guilt or innocence and attendant rulings and punishments were not neatly announced nor always discernible. Rather than a process solely controlled by a dedicated arbitrator, a strong communal element remained. Users were keen to comment on particular individuals and cases, with some even providing their own evidence of dealings with the accused in the form of chat logs or otherwise. When administrators acted against a user, there were sometimes strong repudiations from others.

For their part, Darkode's administrators were involved in almost 80% of cases.[176] In about half of these disputes, the administrators sought to act in a relatively direct way as some kind of arbitrator or mediator, but in the other cases, they employed a more "hands-off approach," stating their opinion but not taking control of the process.[177] This meant that, along with the instances where administrators played no role at all, a number of disputes were not subject to the more formal enforcement mechanisms, which only the administrators could deploy. It could be inferred that these may have been less important dispute threads, which could have functioned more as communal warnings and shaming rather than conflicts worthy of the hierarchy's time.[178]

There were several common dispute outcomes. Most significantly, in 12.5% of disputes, the defendant was banned.[179] In a further 1.2% of cases, a suspension was ordered, although the timeline of the suspension was often unclear.[180] In 9.4% of cases, the defendant was forced to provide reparations to the plaintiff.[181] But this left 76.9% of disputes that could not be coded under these standard categories.[182] There were some examples where the administrator took a softer approach and, for example, locked a seller thread on the marketplace so the user could not continue to trade.[183] Others were added to a list of malefactors with a "bad reputation" which leveraged reputational damage as a form of

[175] *Id.* at 905.
[176] *See id.* at 906.
[177] *See id*. at 906.
[178] *See id*.
[179] *Id.*
[180] *Id.*
[181] *Id*.
[182] *Id*.
[183] *See id.* at 906–07.

[184] It is also possible that [illegible]



Author	Message
gonzo FRESH FISH Joined: 18 Jun 2010 Posts: 1361 Rep: 2839 Location: Mexico	Darkode Escrow I can do escrow for whoever needs it. Amounts up to 2k only. LR ONLY No charge
Tue May 31, 2011 4:13 pm	PROFILE PM
RoBiN-HooD FRESH FISH Joined: 26 Apr 2011 Posts: 82 Rep: 1697	Ohhh very good, but it's just too little too late for me !
Tue May 31, 2011 4:21 pm	PROFILE PM
Arkham LEVEL 1 Joined: 25 Sep 2010 Posts: 298 Rep: 1819	good to hear
Tue May 31, 2011 4:35 pm	PROFILE PM
zashulsta Guest	used and all perfect (:
Thu Jun 02, 2011 11:14 am	
Pwdot Guest	Peoples must read that topic:)!!! Very useful!!! Thanks Godlike providing such service! ~Links5
Fri Dec 09, 2011 2:00 pm	
TheMayor LEVEL 1 Joined: 14 Oct 2011 Posts: 75 Rep: 1781	Re: Darkode Escrow what about escrow for higher amounts? 10k+ where do you go for that? or who do you contact? godlike wrote: I can do escrow for whoever needs it. Amounts up to 2k only.

[184] *See id.* at 903.
[185] *See id.* at 907.
[186] *See id.* at 906.
[187] *See id.*

Figure 7: Darkode Thread G

In essence, anyone could have offered their services for escrow, but higher amounts appear to have brought greater risks and were suited to more senior figures, such as administrators like Mafi and Fubar. This was a matter for individuals that wished to take on this role and had the reputation to be trusted to do so. This informally links back to authority within Darkode's social structure, but unlike some cryptomarkets that focus on drugs, there was no formal escrow system built into the Darkode site itself. What is also interesting to note in relation to Gonzo's announcement was that he would perform this role at "no charge." While others make a business around this service, it is unknown what this user was trying to achieve, though benefits to his reputation, promotion, or even a sense of altruism may have been factors.

This case study has provided an illustration of the governance elements within the elite marketplace Darkode. The results were largely in line with both extra-legal governance theory and the broader outline of cybercriminal governance provided in the preceding

section. With the support of the moderators, Darkode's administrators succeeded in expanding the reputation mechanism and allowing information on users to be made widely available so that prospective partners could make more informed decisions concerning whom to work with and whom to avoid. They also developed a system of enforcement whereby users could not only report malfeasance, but also expect some form of dispute resolution and sanction. But the system was not perfect. This will be discussed in the next section as part of a general assessment of the effectiveness of cybercriminal governance.

VI. THE EFFECTIVENESS AND LIMITS OF CYBERCRIMINAL GOVERNANCE

This section examines the effectiveness of cybercriminal governance. It evaluates its successes and failures in relation to the case study of Darkode and the underground more broadly. By closely studying when governance is effective and when it reaches its limits, a much more nuanced picture can be drawn. Simply identifying governance systems tells us only so much. In short, just because a system of governance and its attendant institutions are present does not mean that those institutions are effective. To assume this is a form of functionalist fallacy.

Regarding the Darkode case study, one could construct an argument that the governance elements that were present were quite unsuccessful. The procedures employed to vet new members, along with the publication of information on user reputation, did not prevent a relatively large number of disputes. When those disputes did occur, clear modes of enforcement were used only in a minority of cases.[188] Elements of governance might have been present, and the user community apparently more elite, but the same problems of distrust that affect the wider cybercriminal underground continued to be present.[189]

These arguments probably go too far. As much as a governance system should have some degree of effectiveness and should foster cooperation, we cannot expect it to be perfect. This is especially so when examining a deeply distrustful world like that of cybercrime. When users are anonymous, can appear and disappear with ease, alter their nicknames and identities, and are not subject to physical enforcement, the challenges are far from insignificant. An alternative fallacy would be to assume that, in such an environment, even limited levels of governance success are as good as null.

One of the central challenges in assessing the effectiveness of Darkode's institutions of governance is the lack of clear points of comparison. This type of detailed analysis around governance has not been widely applied to other forums and marketplaces, particularly in relation to dispute resolution.[190] One could attempt a comparison to a lower-level forum like Hackforums, but sites of that sort do not even have a dedicated "scammer" section against which a quantitative comparison could be made. The mere presence of the "scammer"

---

[188] *See* Dupont & Lusthaus, *supra* note 83, at 907–10.
[189] *See generally* Dupont, *supra* note 119; *see generally* Dupont et. al., *supra* note 83; *see* Lusthaus, *supra* note 24, at 76–77; *see* Yip, Webber & Shadbolt, *supra* note 25, at 516–39.
[190] *See* Dupont & Lusthaus, *supra* note 83, at 910.

section within Darkode may suggest that the Darkode administrators provided greater professionalism and more structured governance.[191] It is also challenging to compare these findings with other economic crimes, like organised crime, as these are also fields that often suffer from data scarcity.[192] Governance frameworks have been applied to organised crime, but often qualitatively, which again precludes direct quantitative comparison.[193]

The other avenue is to compare the Darkode results to more legitimate forms of governance, for which data are more widely available. First, for legal ecommerce platforms like eBay, which bear some similarity to cybercriminal marketplaces, it is widely reported that scams and frauds by users are a major concern.[194] In terms of dispute resolution, it should not be overlooked that in both criminal and civil settings, legitimate courts and arbitration processes are far from perfect, nor do they achieve close to universal coverage and completion.[195] Many cases are never reported, and of those that are reported it is common for only a small fraction to make it all the way through the legal process and be completely resolved.[196]

Such comparisons suggest that the apparent successes and failures of the Darkode governance system are not drastically out of sync with governance in other settings. Particularly given that the world of cybercrime is inherently untrustworthy, we should be realistic in our expectations of how successful criminal regulation might be in such a setting. While risks can be reduced, it is highly likely that they will remain in some way. This was a point that a number of former cybercriminals made clearly to me. Scott stated that the "bottom line is you are always taking a bit of a risk or gamble."[197] Lance was more direct: "[Y]ou got ripped off . . . ? Guess what, you're in the business of stealing money, you're going to get ripped off. Suck it up and carry on with your business."[198] Ivan, a former cybercriminal from Eastern Europe, described his decision to risk working with a new programmer he found on a forum:

> And he had an excellent reputation as a reliable software developer. Also, such people love what they do. It is not in their interest to grab the money and run. BTW, he asked only for 30 percent of full price ($8k). But I decided to transfer 100 percent anyway. Because I did not needed money by then, did not know what to do with such a small amount. So I figured that [redacted] could

[191] *See id.* at 909.
[192] *See generally Organized Crime* (Federico Varese ed., Oxford Univ. Press 2010).
[193] *See generally* GAMBETTA, *supra* note 23; *see* VARESE, *supra* note 20, at 118; *see generally* Paolo Campana & Federico Varese, *Organized Crime in the United Kingdom: Illegal Governance of Markets and Communities*, 58 BRITISH J. CRIMINOLOGY (2018); *see generally* DIXIT, *supra* note 22; *see generally* Skarbek, *supra* note 23.
[194] *See* Cecil Eng Huang Chua & Jonathan Wareham, *Fighting Internet Auction Fraud: An Assessment and Proposal*, 37 COMPUT. 31, 31-34 (2004); Miriam R. Albert, *E-Buyer Beware: Why Online Auction Fraud Should Be Regulated*, 39 AM. BUS. L. J. 575, 578–92 (2002).
[195] *See e.g.*, Jeffrey Q. Smith & Grant R. MacQueen, *Going, Going, but Not Quite Gone*, 101 JUDICATURE 26, 28 (2017); Theodore Eisenberg & Charlotte Lanvers, *What is the Settlement Rate and Why Should We Care?*, 6 J. EMPIRICAL LEGAL STUD. 111, 112 (2009); U.K. Home Office, *Crime Outcomes in England and Wales: Year Ending March 2018*, STATISTICAL BULLETIN HOSB 10/18, 14 (2018).
[196] *Id.*
[197] Written Interview with Scott, Former North American Cybercriminal 2 (on file with author).
[198] Telephone Interview with Lance, Former North American Cybercriminal 3 (on file with author).

> buy some toys for himself quicker which would make him happier. What would I have done if he did not pay back? I might drop a post on [redacted] that he failed a project and refused to return a prepay. That would ruin his reputation. But likely I would do nothing—just accept a loss. Post on a forum will not help me anyhow anyway—why should I bother then?[199]

Such attitudes suggest that cybercriminals are driven largely by profit, and that a level of risk is factored into the costs of doing business. But this does not remove the importance of institutions and governance. Interviews made clear that cybercriminals trusted some collaborators more than others, and that they evaluated whether or not particular marketplaces were a safe place to do business.[200] While high levels of distrust can remain, the evidence does not suggest that cybercriminals revert to a form of nihilism and deal with others in an indiscriminate way.

Perhaps the best way to illustrate the relative effectiveness of cybercriminal governance is through a historical analysis. The early phase of financially motivated cybercrime, which occurred roughly during the 1990s, was defined by lone-wolf offenders and limited levels of cooperation.[201] The key moment in the evolution of cybercrime occurred at the turn of the millennium. This was the point at which bulletin board forums and marketplaces began to replace chat groups as the dominant online locations for networking and trade.[202] Lance, a veteran of the cybercriminal underground, argues that IRC chat platforms had a central flaw.[203] There was no "record" of conversations, so users couldn't get a "vibe for the seller or the buyer to see if they were able to do business, if they were able to trust them."[204] This flaw made establishing trustworthy brands very difficult.

Forums and marketplaces helped solve these challenges by capturing posts as part of the platform and allowing users to review them as needed.[205] This meant that more stable identities and brands could evolve and that these identities were susceptible to reputational damage, or even enforcement actions. Institutions thereby formalised key mechanisms that aided cooperation, such as reputation and enforcement.[206] Following this, trade was enhanced, and the cybercriminal underground began to thrive and diversify.[207] Out of these forums, some long-lasting groups began to form to carry out cybercriminal endeavours together.[208]

---

[199] Written Interview with Ivan, Former Eastern European Cybercriminal 3 (on file with author).
[200] Former North American Cybercriminal 2, *supra* note 86; Telephone Interview with Former North American Cybercriminal 3, *supra* note 197.
[201] *See* Jonathan Lusthaus, INDUSTRY OF ANONYMITY, *supra* note 2, at 32-37.
[202] *See* LUSTHAUS, *supra* note 2, at 38-39.
[203] Phone Interview with Former North American Cybercriminal 3, *supra* note 197.
[204] *Id.*
[205] *See* LUSTHAUS, *supra* note 2, at 81-86
[206] *See id.*
[207] *Id.*
[208] *Id.* at, 86-91; Jonathan Lusthaus, *Honour Among (Cyber)Thieves?*, 59 EUROPEAN JOURNAL OF SOCIOLOGY 191 (2018).

This historical analysis suggests that cybercriminal governance has been at least somewhat effective in encouraging cooperation. Before forums and marketplaces offered a substantial amount of governance, cooperation was more limited, and the risks of collaborating were more significant. But this historical argument can be extended further. When CarderPlanet and ShadowCrew began to operate, a cybercriminal Golden Age of sorts occurred.[209] The global community came together, traded, networked, and learned from each other.[210] Once major law enforcement operations were conducted against these sites, however, the tone changed. Key members of CarderPlanet were arrested, and the U.S. Secret Service ran an informant inside ShadowCrew.[211] The most visible strike occurred in the mid-2000s, when undercover FBI agent Keith Mularski infiltrated DarkMarket, which had replaced ShadowCrew as perhaps the leading English language cybercrime marketplace.[212] Using the nickname Master Splyntr, Mularski managed to attain the rank of administrator on DarkMarket and bring the community down from the inside.[213] A number of arrests followed this operation.[214] The larger impact, however, was the degrading of trust.[215]

After these law enforcement operations became widely known, cybercriminal behaviour changed. Many more experienced users began to seek out smaller, more secure, and more close-knit networks to join, avoiding larger, more open marketplaces.[216] Cybercriminal institutions were under threat. Some considered large forums and marketplaces too risky.[217] By retracting into small groupings, cybercriminals could rely more on informal reputation and vetting and, therefore, reduce risks within interactions.[218] This meant that smaller scale cooperation was possible, while larger scale cooperation was stunted.[219] Through their reduced role, the true value of institutions and governance became apparent.[220]

A. Coda: Layers of Order Within the Cybercriminal Underground

To tie up this analysis on the effectiveness and limits of cybercriminal governance, a related point concerns the different layers of the underground and how they are regulated. The above historical discussion suggests that cybercriminals can operate in large or small groupings, which can be subject to lesser or greater vetting and other aspects of governance. There may be a cyclical component to how open the underground is at various points, likely dependent on what actions law enforcement are taking at a given time. At present, there are also different organisational structures, with distinct risk profiles, with which cybercriminal

[209] *See, e.g.*, MISHA GLENNY, DARKMARKET: CYBERTHIEVES, CYBERCOPS AND YOU (2011); POULSEN: KINGPIN (2011).
[210] *See* Jonathan Lusthaus, INDUSTRY OF ANONYMITY, *supra* note 2, at 37-49.
[211] LUSTHAUS, *supra* note 2, at 46-48.
[212] *See id.* at 48-49.
[213] *Id.* at 49
[214] *See id.*
[215] *See id.* at 49-55, 142-43.
[216] *Id.* at 142.
[217] *See id.*
[218] *See id.* at 142-43.
[219] *See id.*
[220] *Id.* at 142-143.

users may choose to engage (or not). A rough outline of the stratigraphy of the underground looks like this:

1) The most visible layer includes the open forums and marketplaces.[221]
2) The next layer includes closed and vetted forums, such as Darkode.[222]
3) The base layer is even smaller and more closed online groupings, such as those that operate on Jabber or through more direct communication.[223]
4) The molten core is the often-ignored offline organisation of cybercrime, where offenders engage with each other in person.[224]

In general, the top two layers involve virtual structures that include larger numbers of users, often in the hundreds or even thousands.[225] Meanwhile, the base layer and core are generally concerned with smaller numbers of members, perhaps in the tens in the case of chat groups, or sometimes fewer than ten individuals in the case of a firm that carries out cybercriminal activities largely on its own.[226] Access is generally more restricted within these smaller groupings, and the smaller group sizes allow stronger vetting, monitoring, and enforcement.[227] This is particularly the case in offline settings, which have a strong local component. Here, real identities are known, and physical enforcement returns as a tool available to cybercriminal offenders.[228] While this offline and local dimension of cybercrime might appear counterintuitive, there is growing evidence that it is relatively widespread phenomenon.[229] Examples range from very small, informal groups, to cybercriminal startups with physical office spaces, to larger networks and communities where cybercrime has become an important local industry.[230]

A major draw of this offline dimension may be the fact that working in person with known partners removes the previously mentioned obstacles of distrust that are exacerbated in online settings. Gambetta puts matters in more concrete terms, noting that, when "identification is at a premium and must be kept secret, just showing one's face is itself like giving a hostage, namely the knowledge of one's key sign of identity."[231]

---

[221] Lusthaus, *Beneath the Dark Web: Excavating the Layers of Cybercrime's Underground Economy*, IEEE EUROPEAN SYMPOSIUM ON SECURITY AND PRIVACY WORKSHOPS 474, 475-76 (2019).
[222] *Id.* at 476-77.
[223] *Id.* at 477-78.
[224] *Id.* at 478-79.
[225] *Id.* at 475-77.
[226] *Id.* at 477-79.
[227] *See id.*
[228] *See* LUSTHAUS, INDUSTRY OF ANONYMITY: INSIDE THE BUSINESS OF CYBERCRIME, *supra* note 2, at 158-64; *see also* Lusthaus & Varese, *supra* note 70, at 4, 9-10.
[229] *See* LUSTHAUS, INDUSTRY OF ANONYMITY: INSIDE THE BUSINESS OF CYBERCRIME, *supra* note 2; Lusthaus, *Honour Among (Cyber)Thieves?*, *supra* note 208; Lusthaus & Varese, *supra* note 70; Rutger Leukfeldt, *Cybercrime and social ties*, 17 TRENDS IN ORGANIZED CRIME (2014); Leukfeldt, et al., BRITISH JOURNAL OF CRIMINOLOGY (2017).
[230] *See* LUSTHAUS, INDUSTRY OF ANONYMITY: INSIDE THE BUSINESS OF CYBERCRIME, *supra* note 2, at 146-56.
[231] GAMBETTA, CODES OF THE UNDERWORLD: HOW CRIMINALS COMMUNICATE 63 (2009).

The stratigraphy of cybercrime can also teach us something about the levels of order found within this underworld. All cybercriminal governance is informal in the sense that it is beyond the control of the state and does not rely on its laws and enforcement tools, but there are levels to the informality of this governance. Forums and marketplaces can clearly state, publish, and enforce rules for joining, user behaviour, and enforcement. The purpose of crystalising rules for the community and formalising institutions is to govern larger groups of strangers. In smaller groupings, however, this may not be required. There, rules may be more subtly conveyed or understood without being stated, and norms may play a central role.

The Darkode data also suggest that, even on sites where the rules are clearly stated and the governance system is relatively formalised, a more informal system of order may sometimes supersede these strictures. Examples of this include administrators allowing new members in, like J.P. Morgan, against the standard rules for introduction, as well as disputes where administrators refuse to take a central arbitrator role and instead leave users to engage in their own conflict resolution, or simply allow the information to serve as a potential warning to the community. On the member side, one quirk Dupont and his colleagues highlight is the popularity of the entry-level marketplace among higher level sellers, who should be vending in the separate and more elite Level 1 or 2 sections.[232] It appears that their desire to access a larger customer base overrode the system that had been put in place to enhance trust and provide greater exclusivity and security in transactions.

What all of this suggests is that cybercriminals may not always seek out the most structured governance systems. There may be reasons for them to move to other settings, which are ordered in ways that resolve challenges more effectively for their purposes. In some sense, this returns us to the essence of private ordering. Ellickson's seminal work in this area makes the argument that the presence of the law does not prevent people from constructing their own rules and order, which may be more particular to them and more effective for their purposes.[233] We can extend this idea to the prevalence of various informal governance systems. For extra-legal governance, and the example of cybercrime, we can see that some rules are relatively formal, even if they are not derived from the state. But even in this type of setting, individuals may develop their own more informal systems of order to aid cooperation.[234] There are layers of extra-legal governance and informal order. It would be a mistake to assume that modes of governance beyond the state's authority are monolithic, and that users would have universal preferences which can be met by one system alone.

CONCLUSION & POLICY DISCUSSION

This article has examined the governance of cybercrime. Most literature on private ordering and informal governance has focused on legitimate actors and the ways in which the state has failed to govern certain spheres of human life entirely or has failed to govern them efficiently.[235] This study, alternatively, has focused on criminal activities that the state cannot

[232] Dupont, et al., *supra* note 83, at 1227.
[233] *See* ELLICKSON, *supra* note 16, at 4-5.
[234] *See id.*
[235] *Id.*; Katz, *supra* note 16; Bernstein (1992), *supra* note 16; Bernstein (2001), *supra* note 16; OSTROM, *supra* note 16.

legitimately seek to control.[236] This leaves cybercriminals to regulate their own dealings, not in the shadows of state authority, but outside the law. As such, this article has presented an examination of extra-legal governance. In this area, the phenomenon of cybercrime offers additional points of interest, largely because cybercrime is an example of an extreme low-trust environment. When offenders engage with each other online, it is challenging to accurately determine identities and to carry out enforcement. Even in cases where a collaborator can be identified, geographical dispersion makes physical threats difficult. Within such a challenging environment, cooperation should be limited. But this is not what has been observed in recent years. Instead, widespread cooperation is taking place, and cybercriminals are working together in relatively large numbers. An illicit industry has formed.

Based on a significant trove of multiple data sources, including a case study of the Darkode archive, the core of this article outlined how cybercriminals could overcome the challenges of distrust to successfully cooperate on an industrial scale. Rather than developing new methods to enhance cooperation, it appears that cybercriminals have leveraged existing mechanisms that have worked in many other aspects of human life. In particular, reputation and enforcement have been widely employed in the governance of cybercrime. Online forums and marketplaces have developed a number of institutions which provide order and considerably scale up trade, along with other forms of cooperation, to much larger networks of cybercriminals. These components blur the boundary between self-governance and private governance. Marketplaces extend the reputation mechanism by employing tools like quantitative rating systems and allowing for qualitative reviews and information to be published on users. Administrators also create and enforce rules to prevent scams and other negative behaviours.

Yet, despite the success of this system of extra-legal governance, there are clear limits. Governance is far from perfect even in legitimate contexts. Therefore, we should not expect cybercriminal governance to function without inefficiencies and flaws, especially as it functions in a deeply distrustful environment. Extra-legal governance is likely to reduce risks involved in cooperation, but it cannot solve them entirely. There are also layers of order within the underground, and cybercriminals may not necessarily choose to operate in the most structured and visibly regulated settings. They may prefer to operate in smaller, more informal groupings or to operate offline and leave many of the challenges of virtual distrust behind.

What is the normative payoff of this analysis of private ordering and the growth of the cybercriminal industry? What does it teach us about countering the threat of cybercrime? It provides two major contributions to policy, which relate to the key acknowledgement that cybercrime is now an industry and, therefore, can be fought not only through traditional law

[236] Some corrupt state agents do, however, illegitimately seek to govern criminal markets. *See, e.g.*, VARESE, *supra* note 20; VARESE, *supra* note 30; DIXIT, *supra* note 22. *see also* Susan Rose-Ackerman, *The Economics of Corruption*, 4 JOURNAL OF PUBLIC ECONOMICS (1975); SUSAN ROSE-ACKERMAN & BONNIE PALIFKA, CORRUPTION AND GOVERNMENT: CAUSES, CONSEQUENCES, AND REFORM (2016).

enforcement, but also in economic terms. First, degrading cybercriminal institutions is likely to shrink cooperation and the industry overall. As cybercriminals operate outside the law, this is not a case where the state should insert itself and try to out-govern those who currently regulate cybercrime. The state cannot achieve this end, unless it turns itself into a corrupt entity or decriminalises cybercrime. But society does not seek greater efficiency in the governance of cybercrime. This is what sets this case apart from legal examples of informal governance and private ordering. In these settings, rules and norms can improve efficiency and lead to positive results for the groups involved, which some might wish to encourage. In criminal settings, the opposite is the goal: we want to create inefficiencies for cybercriminals, and sow disorder. While law enforcement, the private sector, and relevant NGOs could develop tactics for enhancing distrust in cybercrime communities, based on a number of considerations, this article suggests that a good starting point is to examine those elements that are particularly effective at enhancing cooperation among cybercriminals, and particularly effective in doing this at scale. Both theory and the empirical confirmation in this article suggest that *institutions* are the central building blocks that aid both governance and the scaling up of cooperation in cybercrime communities. These should be a focus of future disruption operations.[237]

Just as crime has continued throughout human history, cybercrime is unlikely to be eradicated without massive and regressive technological shifts. Even if there is effective action online that curbs cybercrime, cybercriminals are likely to re-order themselves into more secure settings and continue their business. Cybercrime will go on, but limiting easy and widescale cooperation would place costs on the industry as a whole, which hopefully would lead to a reduction in overall harm. This hypothesis needs to be tested further and more directly. Which cybercriminal institutions to target and how best to carry out such operations also needs to be determined. As such, the effects of sowing distrust and degrading cybercriminal efficiency should be an important research vector going forward, for both basic and applied research, inside and outside academia.[238]

Second, when it comes to policies for fighting cybercrime, we cannot ignore the offline/local dimension of cybercrime. This article has made clear that a key component of the private ordering of cybercrime, and one part of the solution to the puzzle of dealing with anonymous strangers online, is simply to engage with offline partners instead. Some of the largest and most entrenched organisational structures in the cybercrime industry take the form of cybercriminal startups, which look very much like small technology firms and have a clear presence in the physical world. These are often embedded within local settings, which shape the nature of cybercrime offenders and operations in each location. Because of this, cybercrime is not evenly distributed around the world. Some locations produce very little cybercrime, whereas other locations have characteristics that make them major hubs.

---

[237] On the disruption of cybercrime, *see* Lonie Sebagh et al., *Exploring Cybercrime Disruption Through Laboratory Experiments*, *in* 2021 IEEE EUROPEAN SYMPOSIUM ON SECURITY AND PRIVACY WORKSHOPS 144 (2021); Hutchings & Holt, *supra* note 131.

[238] While the research carried out as part of this study did not address these issues head on, given some information was gathered from former cybercriminals, there were also ethical constraints in terms of providing policy outcomes related to the infiltration of, and operations against, specific cybercriminal groups, and especially actions that would lead to arrests.

The practical value of these insights is that the battleground in the fight against cybercrime is not solely a virtual one. In fact, many gains may be made by countering cybercriminals in the offline world. If the geography of cybercrime can be better understood, and the key locations that harbour the most impactful clusters of offenders can be identified, then attention and resources can be focused on those countries which present the greatest threats. Existing programs, which provide external assistance to cyber investigations, and training for law enforcement agents, prosecutors, and judges, can become more targeted. Where cybercriminals benefit from the protection of corrupt agents of the state, focused anti-corruption programs also may prove helpful in the fight against cybercrime. These types of approaches have been employed for a number of years, but the key point coming out of this analysis is that significant strategic thought needs to be given as to *where* such measures are most needed and would have the most impact. By putting efforts and resources into aiding hotspot countries in their fights against cybercrime, this challenge can be better tackled at its roots.[239]

But to really deal with the causes, rather than symptoms, of cybercrime, we need more than conventional policing approaches. As one law enforcement participant argues, we "can't arrest our way out" of this situation.[240] The scale of the cybercrime industry is enormous, and efforts must be made to reduce the pipeline of talent that is driving these illicit enterprises. That numerous offenders are highly capable and intelligent is a tragic element of this illicit industry. If these individuals could be diverted away from cybercrime and into the legitimate technology sector, not only would this dramatically reduce cybercrime, but these talents could also be employed to support positive legal activities. Some countries have already acknowledged the significance and value of offering pathways out of cybercrime. For instance, both the U.K. and Dutch police have set up cybercrime prevention units, which seek to divert young offenders away from illicit activities and toward gainful employment.[241] These efforts now comprise programs such as "Cyber Choices" and "Hack_Right," which focus on at-risk youth and diversion.[242] Since 2023, the Dutch police have been leading the E.U. funded project InterCOP (International Cyber Offender Prevention Network), which has created a network of law enforcement partners from 26 countries to "share expertise and jointly develop, implement and evaluate Cyber Offender Prevention (COP) interventions and prevention campaigns".[243]

---

[239] *For further details on these points, see generally* Jonathan Lusthaus, et al., *Mapping the Geography of Cybercrime: A Review of Indices of Digital Offending by Country*, IEEE (2020); Lusthaus & Varese, POLICING, (2017). Of course, it must be noted that for geopolitical reasons, some countries may not wish to receive cybercrime assistance from the US or others.

[240] Interview with U.S. Law Enforcement Agent 3 (2013) (on file with author).

[241] *See* Russell Brewer, et al., *Positive Diversions*, *in* CYBERCRIME PREVENTION (2019); Pathways Into Cyber Crime. (2017); NCCU Prevent Team, *Cyber Crime: Preventing Young People from Getting Involved*, NATIONAL CRIME AGENCY, https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyber-crime-preventing-young-people-from-getting-involved.

[242] *See id.*

[243] Europol, *InterCOP (International Cyber Offender Prevention Network)*, EUROPOL (2023), https://www.europol.europa.eu/partners-collaboration/networks/intercop-international-cyber-offender-prevention-network.

While there is some movement in this direction, these prevention approaches should be more widely evaluated and potentially adopted, most notably by law enforcement in the United States. While the U.S. is a leader in cybercrime prosecution, it has until recently been no more than a follower in cybercrime prevention. There is an enormous opportunity for the DOJ and its underpinning law enforcement agencies to move into this area. This does not require a wholesale abandonment of current approaches. Rather, it can be done in a supplemental and incremental way. Another advantage of prevention programs is that they involve significant public-private partnerships, as true cybercrime prevention can't be done without mentors and employers giving a vision and opportunities to talented youth, who may be heading down the wrong path. In its early days, as it establishes itself, a U.S. prevention team would be tasked mostly with the coordination of stakeholders and the development of evidence-based policy and best practices for the potential implementation of broader diversion programs. In these early days, some significant inroads could be made with relatively limited investment and people power. At the time of writing, some policy discussions and preparations are underway in the U.S., but, at present, the strongest public U.S. endorsement of cybercrime prevention can be found in a Cyber Safety Review Board's report on Lapsus$ (a group comprised of youths but with proven capacity for significant damage). The final recommendation in the report is for "whole-of-society" programs to reduce youth cybercrime: "Congress should explore funding juvenile cybercrime prevention programs, fostering interruption and redirection programs, and reducing criminal incentives by exploring ways to ensure continuity between federal and state law enforcement authorities."[244]

Prevention programs could also be aimed at major cybercriminal hubs around the world, such as countries in the former Soviet Union. This region is both the heartbeat of the cybercrime industry and the clearest illustration that unemployment and underemployment are driving the cybercrime threat. Due to their communist legacy, Russia, Ukraine, and a number of other countries have retained an excellent education system that produces large numbers of highly capable graduates in technical disciplines. Unfortunately, the technology sectors in these countries are also burdened by the legacy of communism and are not dynamic or thriving. From his investigations, former Russian law enforcement agent Vasily viewed the leading cybercriminals in the region as illicit *entrepreneurs*.[245] Facing the domination of a small number of large state-connected companies, and with little access to capital, young innovators are forced to found cybercriminal startups, and programmers are compelled to join these enterprises. Job opportunities and high salaries are limited in the legitimate technology sector in the region.[246] Instead, these entrepreneurs have created their own opportunities and their own industry, in the form of a "criminal Silicon Valley".[247]

---

[244] Cyber Safety Review Board, *Review of the Attacks Associated with Lapsus$ and Related Threat Groups*, CYBER SAFETY REVIEW BOARD (2023).
[245] Interview with Former Russian Law Enforcement Agent 1 (2013) (on file with author).
[246] Written Interview with Former Eastern European Cybercriminal 2 (on file with author); Written Interview with Former Eastern European Cybercriminal 3 (on file with author).
[247] *See* LUSTHAUS, INDUSTRY OF ANONYMITY: INSIDE THE BUSINESS OF CYBERCRIME, *supra* note 2, at 151-155; Jonathan Lusthaus, *The Criminal Silicon Valley Is Thriving*, *N.Y. TIMES* (Nov. 29, 2019), https://www.nytimes.com/2019/11/29/opinion/the-criminal-silicon-valley-is-thriving.html.

This challenge cannot be solved by law enforcement alone. Even with prevention programs in place, the scale of the policy problem requires the involvement of other arms of government, international organisations and the private sector. While wealthy countries and international organisations could strike major agreements and make capital funds available to aspiring entrepreneurs in "at risk" locations, venture capitalists could also seek value in underappreciated markets, and individual companies could even make a difference by ensuring that their hiring policies for cyber talent include seeking those from countries which produce excellent technologists but have limited opportunities for good employment. These steps would reduce the overall push into cybercrime, and even some action would be better than none. Former U.S. law enforcement agent Landon argued that many Eastern European cybercriminals would have welcomed legitimate opportunities in place of a life in crime: "The truth is, they would take it in a heartbeat."[248] Misha, a former Ukrainian law enforcement agent also believed that many cybercriminals in the region had a dream of opening a "white business" but could not.[249]

Of course, for as long as it continues, the Ukraine War threatens any kind of deployment of prevention policies in the region, distracting from such matters in general, and leading cybercrime to become a lower priority. But the war also offers a strange, and somewhat perverse, opportunity in this space. The large-scale movement of people who have fled Ukraine includes programmers. Some overseas companies have sought to offer aid and employment to this incoming pool of talent. If Ukraine succeeds in defending itself, or large parts of its territory, this may lead to increasingly close relations with the West and foreign nations from elsewhere, which might make immigration for job opportunities easier. This is not to mention closer ties between Ukrainian and foreign law enforcement agencies in their execution of prevention and other cybercrime operations. The post-war reconstruction of Ukraine may also lead to an injection of capital and closer connections with industry abroad, which aids entrepreneurial opportunities within the technology sector in Ukraine. This is in addition to the "brain drain" on the Russian side, with internationally orientated technologists fleeing the country and seeking opportunities abroad.[250] In sum, the war could lead to an outcome that reduces the pool of unemployed or underemployed programmers or others in Eastern Europe, who might be drawn into cybercrime in the longer term. This is, however, only a hypothesis. There remain a number of possible scenarios in the resolution of this war and the situation that follows.

To be clear, this focus on cybercrime prevention is not a suggested policy of recruiting active cybercriminals into industry and government or driving capital to them.[251]

---

[248] Interview with Former U.S. Law Enforcement Agent 8 (2014) (on file with author).
[249] Interview with Former Ukrainian Law Enforcement Agent 3 (2015) (on file with author).
[250] *See* Krebs, *supra* note 122.
[251] The distinct question of how to deal with convicted cybercriminals has not been addressed in a detailed way within the literature. But this topic certainly warrants further attention. If, in a more personal way, opportunities to work in cybersecurity or technology are limited by convention or policy, this may act as a push back into re-offending. My field research also made clear a double standard that there are many unconvicted former cybercriminals who are a gainfully employed in the technology sector but were never detected or prosecuted during their criminal career.

The aim would be to increase opportunity in locations where there is little and to divert future cohorts from getting involved in cybercrime in the first place. If the industrial nature of cybercrime appears to be a major threat now, it will only get worse, unless the underlying economic situation which is driving this phenomenon is addressed. The criminal Silicon Valley will continue to grow.

APPENDIX

Table 3: Distribution of Participants (Geography)

Code	Meaning	Number of Participants	Code	Meaning	Number of Participants
AUS	Australia	8	NIG	Nigeria	15
BRA	Brazil	9	RDT	Redacted	5
CHN	China	7	ROM	Romania	16
*EE**	*Eastern Europe*	*4*	RUS	Russia	18
GER	Germany	1	*SA**	*South America*	*1*
HK	Hong Kong	7	*SEA**	*Southeast Asia*	*3*
IND	India	3	SGP	Singapore	6
INT	International	6	SWI	Switzerland	2
IRE	Ireland	2	THA	Thailand	4
KOR	South Korea	5	UDL	Undisclosed	2
LAT	Latvia	3	UK	United Kingdom	24
MY	Malaysia	8	UKR	Ukraine	10
*MENA**	*Middle East & North Africa*	*1*	US	United States	41
*NA**	*North America*	*5*	VN	Vietnam	13
NLD	Netherlands	4	*WE**	*Western Europe*	*4*

** In order to better preserve anonymity, participants from former cybercriminal backgrounds are identified by region not by country.*

Table 4: Distribution of Participants (Profession)

Code	Profession	Number of Participants
A	Academic	1
CC	Cybercriminal	20
CSP	Cybersecurity Professional	97
FSP	Financial Sector Professional	11
H	Hacker	4
ITP	IT Professional	4
J	Journalist	3
LE	Law Enforcement Agent	72
OO	International Organisation Officer	6
P	Prosecutor	15
RDT	Redacted	5

Table 4: Distribution of Participants (Profession)

Code	Profession	Number of Participants