ANNUAL REVIEWS

Annual Review of Law and Social Science

Reconsidering Crime and Technology: What Is This Thing We Call Cybercrime?

Jonathan Lusthaus

Department of Sociology, Oxford School of Global and Area Studies & St. Antony's College, University of Oxford, Oxford, United Kingdom; email: jonathan.lusthaus@sociology.ox.ac.uk

Annu. Rev. Law Soc. Sci. 2024. 20:369–85

The *Annual Review of Law and Social Science* is online at lawsocsci.annualreviews.org

https://doi.org/10.1146/annurev-lawsocsci-041822-044042

Keywords

crime, technology, cybercrime, cyber-dependent crime, cyber-enabled crime

Abstract

Cybercrime is not a solely technical subject but one that involves human offenders who are susceptible to social scientific study. Yet, despite calls for cybercrime research to be mainstreamed, the topic remains a niche area within legal studies and the social sciences. Drawing on the most significant findings over recent years, this review aims to make the subject more accessible to a wide range of scholars by softening some of the perceived boundaries between conceptions of cybercrime and conventional crime. It examines these key themes in the literature: definitions and categories of cybercrime, cybercrime marketplaces, the governance of cybercrime, the importance of "place" within the world of cybercrime, cybercriminal networks, a discussion of what is new or old about cybercrime, and how we should define the concept going forward. The empirical literature on these themes suggests a simple definition is most appropriate: Cybercrime is crime that uses digital technology in a significant way.

1. INTRODUCTION

In 2001, 150 leading Russian-speaking cybercriminals converged on the Ukrainian port city of Odessa to attend the launch of a site called CarderPlanet (Poulsen 2011, pp. 73–74). This online forum provided a place for cybercriminals around Eastern Europe, and the world, to network and participate in the trade of illicit goods and services. A year later, the anniversary of CarderPlanet's establishment was marked by the First Worldwide Carders' Conference. The main convention was held in the exclusive Hotel Odessa, and participants discussed how to develop the "carding" business—credit card fraud then being one of the primary cybercriminal enterprises (Glenny 2011, pp. 66–67).

The CarderPlanet case is a key moment in the evolution of cybercrime, as it signifies the shift that took place from twentieth-century cybercrime, which was largely informal and driven by fun or mischief, to the twenty-first-century profit-driven criminal industry that followed (Kshetri 2010, Lusthaus 2018). This industry is characterized not only by online marketplaces, which can attract hundreds or even thousands of members, but also by high degrees of professionalism and specialization. In an interview with the Russian magazine *Hacker*, the leader of CarderPlanet, who used the online handle Script, argued that there are no "universal" carders, and that cybercriminals must collaborate with others with different skillsets to succeed. The key goal of marketplaces like CarderPlanet was to provide "dens" for "lone wolves" to "exchange information or observe who offers what in each field to find new solutions" (Lusthaus 2018, p. 44). At present, the old stereotype of the teenage hacker in their parents' basement has been supplanted in large part by an industry made up of entrepreneurs, programmers, managers, and conventional criminals. These elements are organized not only within virtual marketplaces but also within firms. Some of these firms exist online, but others operate offline, in certain cases even out of physical office space (Halpern 2015, Ragan 2012).

This prologue makes clear that cybercrime is not a solely technical subject but one that involves human offenders who are susceptible to social scientific study. Yet, despite calls for cybercrime research to be mainstreamed, the topic remains a niche area within legal studies and the social sciences. Drawing on the most significant findings over recent years, this review aims to make the subject more accessible to a wide range of scholars by softening some of the perceived boundaries between conceptions of cybercrime and conventional crime. The second goal is to assess how successfully the established scholarly understandings of cybercrime match the empirical reality of the cybercrime industry that has evolved in recent decades.

No existing review on cybercrime matches the above aims. In 2019, the *Annual Review of Criminology* published an article on cybercrime but with a significantly different scope (Maimon & Louderback 2019). By focusing solely on cyber-dependent crimes—which, like hacking, require computer technology to be carried out—the article took a narrow view of cybercrime. Its intention was to "highlight a set of illegal activities and actors that are less familiar in the criminological literature" (p. 192). Although there is value in an approach focused on the novel, most cybercrime—including online fraud—falls outside this limited categorization. As such, the *Annual Review of Criminology* article did not address several key aspects of the literature on financially motivated cybercrime. This review aims to complement the earlier one by going in the opposite direction. It addresses the many aspects of cybercrime that exist beyond hacking, highlighting the similarities to conventional crime that the literature has drawn out and mainstreaming the topic into the broader social sciences. This article diverges also in that it focuses on financially motivated cybercrime, perhaps the most central and impactful form of this phenomenon. Finally, it is relevant to scholars from a range of fields, not only criminology, as the study of cybercrime is increasingly interdisciplinary. The literature so far has demonstrated that legal scholars, sociologists, economists, geographers, anthropologists, and other social scientists have all made very

significant contributions to understanding this phenomenon at both a theoretical and empirical level (in addition, of course, to computer scientists).

Cybercrime is still a young field, but there are now at least two decades of research to evaluate. The review outlines the foundational research that was carried out largely at the turn of the millennium, when little was understood about cybercrime and data were sparse. In particular, it examines the influential definitions and categorizations that emerged out of this period. It then highlights key bodies of knowledge that developed out of a later empirical period of research, which occurred largely during the 2010s onward. Appraising these empirical findings will allow an assessment of how well the foundational definitions and categorizations continue to serve the field today.

The sections of this review cover definitions and categories of cybercrime, cybercrime marketplaces, the governance of cybercrime, the importance of place within the world of cybercrime, and cybercriminal networks, followed by a discussion of what the literature tells us about what is new or old about cybercrime and how we should define the concept going forward. Although research on all these themes continues, these sections are listed in roughly chronological order in relation to when the key work on each area began.

2. DEFINITIONS AND CATEGORIES

Many early cybercrime studies wrestled with the double challenge of limited data and a rapidly evolving subject matter being driven forward by new technologies. This literature focused on how well the novel phenomenon of cybercrime matched conventional conceptions of crime. In examining the intersection of crime and technology, they coined a range of terms, including cybercrime, computer crime, high-tech crime, virtual crime, and net crime. Yet, as Wall (2008, p. 20) argues, whatever "its merits and demerits, the term 'cyber-crime' has entered the public parlance and we are more or less stuck with it."

The central question of this period of literature was whether cybercrime constitutes a new category of crime or is crime as we know it, but adapted to a new digital context. The former position attracted some adherents. For example, Wall (1998, pp. 201–2) argues that

> the 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.

The latter position also attracted adherents. Engaging the same wine metaphor, Grabosky's (2001, p. 243) study "Virtual Criminality: Old Wine in New Bottles?" makes this argument:

> "[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.

Yar (2005, p. 424) completes the collection of wine analogies, adopting a variation on Grabosky's position. He argues, "Perhaps cybercrime represents a case not so much of 'old wine in new bottles' as of 'old wine in no bottles' or, alternatively, 'old wine' in bottles of varying and fluid shape."

A consensus eventually formed around this second approach, defining cybercrime broadly as a range of illegal activities taking place within cyberspace, rather than as a particular subset of crimes (Bossler & Berenblum 2019, Holt & Bossler 2014, Leukfeldt & Yar 2016). But, crucially, the essence of the old/new wine debate remains through the way that cybercrime continues to be subcategorized. Furnell (2002) provides, if not the earliest statement of this distinction, then

certainly the foundational one. He argues that cybercrime is composed of two forms: computer-assisted crimes and computer-focused crimes. The first category includes fraud, theft, sabotage, and so on. These crimes are cases where "the computer is used in a supporting capacity, but the underlying crime or offense either predates the emergence of computers or could be committed without them." The second, computer-focused, category includes examples like hacking and viruses, whereby "the category of crime has emerged as a direct result of computer technology and there is no direct parallel in other sectors" (Furnell 2002, p. 22). As part of this discussion, Furnell (2002, p. 23) notes that "computer-focused crimes are the ones perpetrated by true cybercriminals." Wall (2007, p. 30) expands this line of argument, conceiving of a phased evolution of cybercrime, with a first generation where computers "assist" traditional offending and a final generation with "true cybercrimes wholly mediated by technology." According to Wall, these types of cybercrime "are the spawn of the internet and therefore embody all its transformative characteristics" (p. 47), and as such, "they can only be perpetrated within its cyberspace and are therefore *sui generis*" (p. 48). He gives an example:

> Spamming is a particularly good example of a true or pure cybercrime because it is now an illegal behavior in its own right in US and EU law and many other jurisdictions. It also facilitates secondary offending by enabling offenders to engage with potential victims. Take away the internet and spamming and the other true cybercrimes vanish (Wall 2007, p. 48).

Gordon & Ford (2006) provide a similar classification with their distinction between "Type 1" cybercrime, which is more technical in nature (such as viruses and other malware), and "Type 2," which has an important human component (such as extortion, corporate espionage, child sexual abuse, and terrorist activities).

Building on these prototypical discussions from the 2000s, a 2013 report published by the UK Home Office is widely cited and influential. It has formalized and entrenched this distinction, arguing that cybercrime is "an umbrella term used to describe two distinct, but closely related criminal activities: cyber-dependent and cyber-enabled crimes" (McGuire & Dowling 2013, p. 5). These two terms are understood as follows:

> Cyber-dependent crimes are offences that can only be committed by using a computer, computer networks, or other form of ICT. These acts include the spread of viruses and other malicious software, hacking, and distributed denial of service (DDoS) attacks, i.e., the flooding of internet servers to take down network infrastructure or websites.
>
> Cyber-enabled crimes are traditional crimes that are increased in their scale or reach by the use of computers, computer networks or other ICT. Unlike cyber-dependent crimes, they can still be committed without the use of ICT. (p. 5)

The report provides examples of these cyber-enabled crimes, including fraud and theft, as well as child sex offences (McGuire & Dowling 2013, p. 5).

In recent years, cyber-dependent and cyber-enabled crimes have become the dominant nomenclature for demarcating novel crimes, which could not exist without digital technology, from existing crimes, which simply make use of technology (for a recent review, see Phillips et al. 2022). The following sections examine how the empirical literature evolved from this early phase, and how well its main findings support or challenge these foundational definitions and categorizations of cybercrime.

3. CYBERCRIME MARKETPLACES

One aspect of cybercrime scholarship that flourished in the 2010s was the study of the online organization of financially motivated cybercrime. This development was, in part, driven by publicly accessible trading forums/marketplaces providing a new source of data for analysis. These forums

are much like eBay, but they support the trade of illicit goods/services rather than legal ones. They have become a focus of social science research. For instance, Holt & Lampke (2010) analyze data from six marketplaces to outline key market components, including available goods, payment systems, user relationships, and market dynamics. Holt (2013) analyzes threads from English and Russian language forums to study their social organization. Hutchings & Holt (2015) engage in crime script analysis of user behavior within illicit markets. In recent years, data science approaches have been used to study larger amounts of data across one or more forums/marketplaces (see, for example, Pastrana et al. 2018).

Illustrated through the wide range of products and services traded on these sites, the literature on this theme has revealed the variety of cybercrimes that exist. Products/services include compromised credit card data, logins for ecommerce accounts, personal identifying information, email lists, hardware for making counterfeit cards and documents, malware, coding services, hacking services, cashing out and money laundering services, and almost endlessly on. Some products/services are highly technical, whereas others are not technical at all. The plethora of goods and services on offer match the broad definitions that many apply to cybercrime and incorporate components associated with both cyber-dependent and cyber-enabled crime types. Some marketplaces focus on more technical forms of cybercrime (Dupont et al. 2017, Hutchings & Clayton 2016), whereas others are, for instance, more fraud based (see Lusthaus 2018, pp. 82–86). Some markets provide ranges of services/products that fall in between.

Regarding nontechnical products, the online drug trade has often been presented as distinct from the field of cybercrime. As such, the literature on online drugs markets, both counterfeit and illegal, is developing as a shadow or mirror field to cybercrime research, with only relatively few scholars working across the divide or noting points of crossover (Décary-Hétu & Giommoni 2017, Décary-Hétu & Leppänen 2016, Lavorgna 2015, Martin 2014, Martin et al. 2020, Sugiura 2018). For instance, numerous studies have looked at trust, reputation, and cooperation within online drug markets (Duxbury & Haynie 2018a,b; Hardy & Norgaard 2016; Munksgaard 2023; Norbutas et al. 2020; Przepiorka et al. 2017), but these studies primarily draw points of comparison with the offline drug trade and not the broader cybercrime literature, which engages with analogous issues (Décary-Hétu & Dupont 2013; Lusthaus 2012, 2013). Similar, but under-examined, overlaps exist in relation to studies of conflict management/resolution within both drug cryptomarkets and cybercriminal markets, whereby a common challenge concerns how best to enforce agreements when the threat of physical violence is largely absent (Barratt et al. 2016, Dupont & Lusthaus 2021, Morselli et al. 2017).

This bifurcation of the online drug trade literature from the cybercrime literature is curious for several reasons. First, although some online marketplaces focus on the drug trade, a number also allow for the sale of products associated with cybercrime, such as stolen credit card data (Lusthaus 2018, p. 54; Paquet-Clouston et al. 2018). Second, the sale of drugs on digital marketplaces appears to be a preexisting form of profit-driven crime that is enabled by cyber. These points indicate some likely blur between these two forms of modern crime and that the cyber-enabled versus cyber-dependent debate is also relevant to the online drug trade. This suggests either that cybercrime definitions should be narrowed to clearly exclude drugs or that the field(s) should be more holistic and inclusive in its approach. At present, the rapidly growing literature on the virtual drug trade holds an uncertain position within the cybercrime field, suggesting intriguing comparisons, points of replication, or redundancy in research efforts.

This discussion of cybercriminal markets, and the comparison to online drug markets, reveals that there is an enormous breadth to cybercrime regarding the range of goods and services on offer. The key questions become clearer: What are the limits of cybercrime? Is trading within cyberspace sufficient to bring something within the definition of cybercrime? If online trade on its

own is not enough, is there something about the nature of committing cybercrime offences that is different from conventional ones? When thinking about definitions and categories of cybercrime, this section provides an immediate demonstration that a certain degree of greyness must be present within these discussions.

4. GOVERNING CYBERCRIME

In attempting to comprehend the nature of cybercrime, we need to move beyond a discussion of illicit products/services to a deeper examination of cybercriminal behavior and organization. The development of the cybercrime industry presents a classic social scientific puzzle: How did cybercriminals succeed in building an industry, which requires a significant amount of cooperation, when they seem to operate in an environment riven by distrust? Dealing with anonymous partners is challenging. True identities are obscured, alongside physical location, making assessment of trustworthiness more difficult and limiting avenues for physical enforcement. But the second layer of difficulty is that these are anonymous *criminal* partners, who operate outside legal recourse and are inherently untrustworthy. As such, facing these challenges, a reasonable expectation might be that cybercriminals would operate alone or in small groups. Instead, a large and multifaceted industry has emerged (Kshetri 2010, Lusthaus 2018, Moore et al. 2009).

This puzzle speaks to several key theoretical concepts within social science and legal studies around trust, reputation, cooperation, institutions, private ordering, and governance (Axelrod 2006, Bernstein 1992, Cook et al. 2005, Ellickson 1991, North 1991). Building on this foundation, an intriguing line of study has examined how cybercriminals cooperate in online marketplaces, which are so characterized by distrust (Holt 2013; Lusthaus 2012, 2013; Yip et al. 2013). These studies capture the structured elements of governance found within these sites, such as how members are vetted, how administrators can ban members who break rules, cybercriminal escrow services, and rating and feedback systems. These elements are concerned with the maintenance of order to encourage stable and efficient markets. To illustrate this, we can return briefly to the prototypical CarderPlanet example, as this site introduced innovations that have been widely adopted by many successor markets up to the present day. For instance, CarderPlanet had a clearly defined hierarchy, which appropriated titles from the Sicilian Mafia (e.g., Capo). The higher-ranked officers were tasked with enforcing the forum's rules and punishing malefactors. The site also reviewed products/services before vendors were allowed to trade on the marketplace and pioneered the use of escrow for larger transactions, which has since become a widely used function within the cybercriminal underground (Lusthaus 2018, p. 44).

Two important riders should be noted with regard to this discussion. First, an important body of scholarship examines not just the presence of these elements of cybercriminal governance but also how effective they are in practice. Dupont's work on Darkode is particularly instructive in this regard (Dupont & Lusthaus 2021; Dupont et al. 2016, 2017). Darkode (2007–2015) was an elite English-language marketplace that focused on some of the more technical forms of cybercrime, such as malware. Alongside his coauthors, Dupont analyzes both the recruitment processes and the arbitration system employed by this forum. Despite its apparent eliteness, Darkode was far from perfect in keeping out scammers or incompetent cybercriminals. A significant number of disputes still arose, and many were never resolved (Dupont & Lusthaus 2021, Dupont et al. 2017). The second rider, which connects with the next section, is that some cybercriminals appear to sidestep the trust problem of dealing with collaborators online by engaging with offline confreres. This also moves the need for private ordering toward offline providers of governance. Although one might expect organized criminals to serve as key cybercriminal protectors, this role is much more commonly performed by corrupt state agents (see Lusthaus 2018, chapter 7).

The literature on cybercriminal governance reveals that analyses of the ostensibly novel phenomenon of cybercrime can be grounded within broader social science/legal theory. This application shows not only that cybercrime can be understood through such existing concepts but also that, rather than inventing completely new mechanisms, cybercriminals largely adapt existing processes and systems, like escrow and arbitration, which are found across a wide variety of human settings. Rather than significant cybercriminal innovation, the literature suggests strong points of similarity with not only conventional crime but also mainstream society.

5. THE IMPORTANCE OF "PLACE"

At first glance, cybercrime is a virtual, global, and dynamic phenomenon. Offenders exist in cyberspace and strike victims around the world. With much of the empirical literature from the 2010s focusing on novel online cybercrime marketplaces, where offenders converge from multiple jurisdictions, this view might receive some support. Nonetheless, as noted above, a small but important research niche has uncovered a seemingly counterintuitive phenomenon: that many cybercriminal interactions are, in fact, conducted offline.

In his study of phishing in Amsterdam, Leukfeldt (2014) finds multiple points at which "social ties" are important to comprehending cybercrime. Many phishing offenders are recruited through offline social settings, with members of the same communities coming together for this criminal enterprise. Money mules were also recruited through local networks. Finding co-offenders offline is a potentially fruitful option, particularly because it removes some of the questions around trust, reputation, and enforcement discussed above. But what is noteworthy in this study is that the offenders also used components of social engineering to obtain information from victims offline and were not constrained to engaging with victims only in cyberspace. In short, Leukfeldt finds that the boundary between the online and offline dimensions of cybercrime is porous. Leukfeldt et al. (2017b) confirm these findings with a further study of 18 Dutch police investigations (see also Leukfeldt et al. 2017a). Other studies have addressed the related but somewhat inverse phenomenon of how organized criminals, gangs, and other conventional criminals—who are very much rooted in offline contexts—might become involved in more technological forms of offending, or at least use technology to enhance their existing activities. These studies emphasize both how these offenders remain embedded within local settings and that the boundary between the online/offline, and the cybercrime/conventional crime world, is indeed permeable (Bijlenga & Kleemans 2018; Lusthaus 2018, pp. 171–90; Roks et al. 2021).

But how widely spread is the offline dimension of cybercrime? How do "place" and locality matter? Taking a global approach, Lusthaus's multiyear field-based study in 20 countries finds regular instances of offline cybercriminal cooperation across varied forms of cybercrime and geography. Hubs of cybercrime offenders exist in particular locations around the world, including the former Soviet Union, Romania, Nigeria, and Brazil (Lusthaus 2018). This opens up a line of thinking around the importance of not just the offline but also the local. Lusthaus & Varese (2021, p. 4) argue, "The economic and social dynamics of different settings are likely to influence who gets involved in cybercrime, what types of cybercrime they carry out and the way they are organized." Or, as Hall et al. (2021, p. 301) put it,

> [This paper] suggests that the geographies of cybercrime are not reducible to universal explanations. While it did not identify any universally criminogenic combination of national attributes, different sets of incongruous combinations of such attributes might apply at the level of national or regional agglomerations of cybercrime. Here it points to the potential significance of regional cultures and practices of cybercrime and the framing of policy responses accordingly.

Table 1, adapted from the book *Industry of Anonymity* (Lusthaus 2018, p. 77), summarizes the phenomenon of different places producing different forms of cybercrime.

Table 1 Geographical specialization

Former Soviet Union	Malware production and distribution Other technical criminal endeavors (for example, spam and bulletproof hosting)
Nigeria	Advance fee fraud Other confidence scams (for example, email compromise and impersonation)
Romania	Online auction fraud ATM fraud
China	Online gaming theft Intellectual property theft (state affiliated)
Brazil	Credit card fraud Banking fraud
The West	Cashing out and money mules Some hacking and malware exploitation

We can take two examples from this table to illustrate the importance of cybercriminal geography with greater nuance. The first is the case of the former Soviet Union, which Lusthaus (2018, p. 69) argues is the "technical engine" of cybercrime, responsible for producing the most sophisticated and impactful malware and other important cybercriminal tools. The former Soviet Union is a major cybercrime hub and produces the type of cybercrime that it does for four reasons: (*a*) widespread and good-quality technical education, tied to its communist heritage; (*b*) a substantial hacking community (hacking being distinct from cybercrime);[1] (*c*) limited employment opportunities and a lack of capital for entrepreneurs in the technology sector; and (*d*) high levels of corruption leading to a lack of policing for many cybercriminal offences (Lusthaus 2018, pp. 69–73).

Nigeria is a second useful example, because it captures the point that not all cybercrime is highly technical; in fact, some of the most impactful forms, such as Advance Fee Fraud and Business Email Compromise, are not. Important local factors explain the origin and development of these forms of cybercrime. In the case of Nigeria, Lusthaus (2018, p. 74) argues that "the poor economy, relatively reliable and accessible Internet, and prevailing corruption may combine to create a breeding ground for online crime." But in this case, the supply of highly educated leading technologists, or a large community of hackers, is not present in the way it is in, for instance, the former Soviet Union. As such, Lusthaus draws from interviews with security professionals, law enforcement agents, and former cybercriminals to make this point:

> [It] is not surprising to see a greater proportion of low-tech scams and greater reliance on foreign actors for technical assistance [. . .]. There appears to be a direct connection between the email scams that emerged at the turn of the century, known as *advance fee fraud*, and previously existing paper-letter campaigns to the same effect [. . .] This suggests that cybercrime in Nigeria largely grew out of a community of fraudsters rather than hackers or other more technical actors. (Lusthaus 2018, p. 74)

It is likely that in the coming years, the literature will identify several emerging cybercrime hubs across Africa, South America, Asia, or elsewhere, which are not captured in **Table 1**. These include, for instance, parts of Southeast Asia that are becoming known for so-called fraud farms or fraud factories, which appear to draw on human trafficking to feed their workforce

[1]One popular definition suggests that a hacker is "someone who does some sort of interesting and creative work at a high intensity level. This applies to anything from writing computer programs to pulling a clever prank that amuses and delights everyone on campus" (see Frequently Asked Questions at **http://hacks.mit.edu/Hacks/misc/faq.html**). Although some hackers are cybercriminals, many are not. Conversely, although some cybercriminals are hackers, many are not. On hacking, see Levy (2010) and Steinmetz (2016).

(UNODC 2024). Some of the previously known hubs may also evolve to support additional forms of cybercrime. One good example of this is the case of China. An increasingly large community of Chinese fraudsters now appear to be targeting victims not only within China but regionally and globally as well, and with possible connections to some of these fraud factories emerging in Southeast Asia (see Luo 2024).

Most studies of cybercrime geography are qualitative, or literature based. Although discussion of a small number of cases is helpful, more comprehensive measures that could be employed in quantitative research are also required. Thus far, some studies have attempted to explain, through statistical analysis, why cybercrime appears in some locations but not others (Kigerl 2012, 2016). But these approaches face major challenges in terms of data availability, with many choosing to use technical attack data as a proxy for the location of the cybercriminals behind the attacks (Chen et al. 2023, Srivastava et al. 2020). This is problematic. As Kigerl (2012, p. 473) explains,

> One [approach] is to measure where most cybercriminals live in physical space. Surely, some countries are home to more cybercriminals than others. The second means of measuring high cybercrime countries is to determine from which nations cyberattacks are coming from. For instance, which countries host the most phishing servers, which are the source of most spam messages, and which countries contain the most botnet zombies. Where the cybercriminals live is not necessarily where the cyberattacks are coming from. An offender from Romania can control zombies in a botnet, mostly located in the United States, from which to send spam to countries all over the world, with links contained in them to phishing sites located in China. The cybercriminal's reach is not limited by national borders.

To draw a clearer picture of the geography of cybercrime offenders, and to understand more about what is driving the formation of these hubs, significant attention and efforts are required to attempt to solve this measurement problem going forward (see Bruce et al. 2024).

Literature that reveals the importance of "place" within cybercrime challenges the supposed dominance of "cyberspace" in existing definitions of the phenomenon. Cyberspace remains important in understanding cybercrime, but the offline and local dimensions are key elements that suggest cybercrime may be grounded in existing patterns of criminal behavior, sometimes digitalizing existing criminal expertise, rather than something strikingly novel. This would seem to provide support for conceptions of cybercrime as a new manifestation of the much older phenomenon of crime.

6. CYBERCRIMINAL NETWORKS, ROLES, AND PROCESSES

Following the earlier strong focus on online cybercriminal marketplaces, and often linked to subsequent discussions of offline social ties and locality, scholars have attempted to uncover a more complete picture of cybercriminal organization. Much of this work has pointed to the importance of cybercriminal networks and the diverse roles and processes required to carry out various schemes. Broadhurst et al. (2014) survey the range of different groups involved in cybercrime, with various tighter or looser structures, depending on the nature and motivation of the actors involved. In their case study of the Gozi banking malware group, Lusthaus et al. (2022) show that a partnership structure between distinct but interdependent coding, infection, and cashing out teams became the dominant business model for this kind of financial malware. Leukfeldt et al. (2017c) identify four cybercriminal network categories, ranging from more local low-tech networks to more international high-tech ones. Crime script analysis, which breaks down the various sequential elements present in the commission of a crime, is also applied to a diverse range of cybercriminal schemes, including the online pharmaceutical trade (Lavorgna 2015), eWhoring (Hutchings & Pastrana 2019), procurement of counterfeit identity documents (Holt & Lee 2022), and Vietnamese card fraud and phone scams (Nguyen 2022).

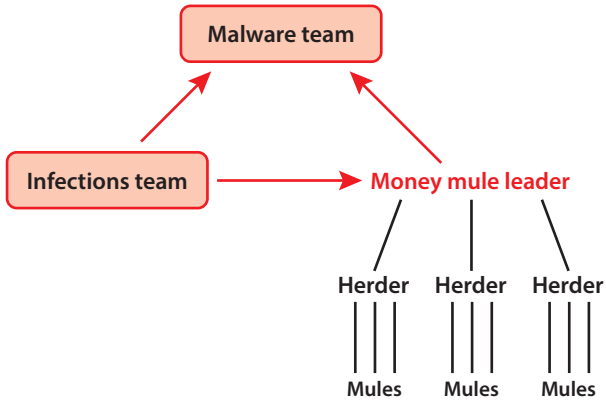

Figure 1

Malware networks (figure adapted from Lusthaus et al. 2023).

Each cybercriminal process often requires a different set of individual skillsets to support it. Taking the example of malware enterprises, scholars have revealed a large range of roles. These include skilled coders to write malware, others to infect systems, social engineers, translators and forgers, bank account transfer teams, con artists to speak to banks, money mules, and the organizer (Lusthaus 2018, pp. 66–68; Leukfeldt et al. 2017b,c). **Figure 1**, adapted from Lusthaus et al. (2023, p. 16), shows the basic network structure of these financial malware operations.

There are three central components within this business model: those responsible for creating and managing the malware, those responsible for infecting computers/systems, and those responsible for dealing with the proceeds of the crime. This figure also illustrates the commonly found hierarchical structure of money mule providers, with a leader; herders (lieutenants); and many (sometimes loosely affiliated) mules who receive, withdraw, and/or move funds through bank accounts or transfer bureaus, physically, and through other means, such as cryptocurrency wallets (Custers et al. 2019, Kruisbergen et al. 2019, Levi 2022, Soudijn & Zegers 2012). Some detail has been provided on the firm-like nature of groups that produce malware (Lusthaus et al. 2022). But, compared to money mule groups, less is known about these malware production group structures and the nature of those individuals/groups involved in infections.

The key takeaway, across a wide variety of cybercrime, is that there is a high degree of specialization. Many roles support and facilitate the core criminal activities in various ways, such as the running of technical infrastructure that could be considered "boring":

> As opposed to understandings of involvement in crime as being born of boredom (which put a focus on individual, low-level crime), we find that as the underground hacker subculture has developed into more organized and industrialized economies, the shift to shared illicit infrastructure has proliferated a range of tedious supportive forms of labor, much as in mainstream industrialized economies, with participation becoming less about charismatic transgression and deviant identity, and more about stability and the management and diffusion of risk. (Collier et al. 2021, p. 1421)

Despite the very large number of roles, and the seemingly endless links within chains of cybercriminal offences, recent scholarship tells us we should not assume that the organization of this world is completely flat and egalitarian. There is little doubt that some players are more influential and powerful than other members of the underground. For instance, Paquet-Clouston et al. (2019) find that a small number of ransomware players dominate the payment market. Similarly, Buil-Gil & Saldaña-Taboada (2022) highlight how many cybercrimes are linked with a small, but active, set of Bitcoin wallets.

This body of research demonstrates how cyber-dependent and cyber-enabled crime are fused together in many real-world situations. In their "cascade" model of cybercrime, Porcedda & Wall (2021, p. 169) demonstrate how "upstream data-based cyber-dependent cybercrime can result in further cyber-enabled and cyber-assisted cybercrimes." In short, cybercriminal enterprises involve a clear mixing of technical and nontechnical roles. For instance, Leukfeldt et al. (2017b) show how some components of malware attacks are carried out by seemingly nontechnical criminal actors who have backgrounds in other forms of financial crime. Drawing on a detailed analysis of 10 cybercriminal networks, Lusthaus et al. (2023, p. 19) support the argument that the supposed theoretical distinction between cyber-dependent and cyber-enabled crime is blurred in practice:

> supposed cyber-dependent cases, like those centred on malware, actually involve a number of less technical components that are central to the success of the business model. For this reason, within profit-driven cybercrime, pure cyber-dependent crimes may rarely exist. This is because targeting a computer or system alone will not lead to any profit, without a number of additional elements, such as manipulating users into infecting their machines, and having a network of partners to receive, cash out, and/or launder the proceeds. It should not be overlooked that many present-day malware schemes are actually forms of (cyber-enabled) banking fraud or extortion.

One might even argue that all profit-driven cybercrime is underpinned by some conventional form of crime (e.g. theft, fraud, or extortion) and, as such, should always be considered a form of cyber-enabled, rather than -dependent, crime (see also Lusthaus 2018, p. 8).

7. DISCUSSION: BACK TO THE FUTURE?

The cybercrime field is stretched between two poles: the conventional and the novel. As a result, from the beginning of work in this field, definitions and categorizations have reflected this tension. One camp sees cybercrime as conventional crime types carried out through unconventional methods, whereas the other sees cybercrime as something far more paradigm shifting and new. Even when broader, more inclusive definitions are adopted, this tension remains through understandings of "purer" cyber-dependent crimes as opposed to more conventional cyber-enabled ones.

Through the review of the literature provided above, we can now assess, with far more empirical support, which camp is correct. The evidence suggests that greater support can be found for those scholars advocating for the "old wine in new bottles" approach. The evidence also suggests that the distinction between cyber-dependent and cyber-enabled crime may be illusory in practice. This was observed through four key elements that make up the empirical literature on profit-driven cybercriminals. First, research on illegal marketplaces makes clear that cybercrime covers a large array of goods and services, and it is difficult to determine a natural limit to where the online trade of illicit goods/services ceases to be cybercrime. Second, the governance of cybercrime clearly illustrates how this ostensibly niche example can be explained by "ancient," well-established, and widely applied social science/legal theory. Third, the importance of place within the world of cybercrime defies the supposedly virtual nature of the phenomenon, because offenders are deeply embedded within local contexts and, sometimes, existing criminality. Finally, the literature on cybercriminal networks provides further support for the wide range of cybercriminal functions, some highly technical and others quite nontechnical, but which are fused together within various illicit business models. This suggests that attempting to evoke a hard boundary between cyber-dependent and cyber-enabled crimes is misguided, and that these categories themselves may be of limited use.

To engage with these findings in more detail, let us return to some earlier attempts to define and categorize cybercrime and examine the way in which they have interacted with policy approaches. The European Commission defines cybercrime in this way:

> Cybercrime consists of criminal acts committed online by using electronic communications networks and information systems. The EU has implemented laws and supports operational cooperation through nonlegislative actions and funding.
>
> Cybercrime is a borderless issue that can be classified in three broad definitions:
>
> - crimes specific to the internet, such as attacks against information systems or phishing (e.g., fake bank websites to solicit passwords enabling access to victims' bank accounts)
> - online fraud and forgery: large-scale fraud can be committed online through instruments such as identity theft, phishing, spam and malicious code
> - illegal online content, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia. (Eur. Comm. 2024)

The overarching definition is broad, but then it settles into additional subdefinitions that approximate the cyber-dependent/enabled division. This is in line with the approaches outlined in Section 2. [The EU approach also includes a third component, "content" crimes, which has been included by some scholars (see, for example, Wall 2007, p. 30)]. With relevance to cyber-dependent and cyber-enabled crime, this EU approach implicitly signals that some examples will cross these categories. Phishing is mentioned in relation to crimes that are "specific to the internet" and again in relation to the second (cyber-enabled) fraud category. We could just as easily refer to phishing as the manipulation of victims to take certain actions or give up certain information. By doing that, we can see that phishing could be a criminal end in itself (e.g., obtaining bank account login information) or part of a broader, more technical criminal activity (e.g., tricking a user into downloading malware).

If we return to Furnell (2002), whose work has been a key foundation for those scholars and policy makers maintaining a difference between cyber-dependent and cyber-enabled crime, we can find that he hints at some of the complexity that later empirical studies would reveal. Furnell (2002) provides two important asides. The first is an acknowledgment that these categories may blur together, for instance through the example of hacking being used to carry out sabotage (p. 22). He also, perhaps unintentionally, predicts a major policy failing whereby some individuals/organizations classify categories of technical crime as more important than fraud-based ones. At the time of writing, Furnell notes the dominance of fraud offences over more technical ones (p. 23). The reality at present is that the situation remains the same. But the idea of cyber-dependent crime being "true" cybercrime has taken hold in certain policy circles. As a result, in some jurisdictions, cyber-dependent crime is the purview of cybercrime units, with cyber-fraud left to conventional fraud teams who focus on other kinds of fraud and often eschew cyber investigations (Lusthaus et al. 2023).

The heart of this issue is a confusion over what is law and what is social science. As Lusthaus (2018, p. 8) argues,

> All crimes are simply behaviors that have been criminalized by legal systems; the concept of what is criminal does not necessarily have a theoretical underpinning independent from the law of the land. Legislators might declare specific acts against computers and networks to be criminal, but often what is being newly criminalized is the use of novel tools or methods rather than the behaviors behind them. The older motivations remain. For instance, computer intrusions and the spread of malware can facilitate theft or vandalism, and DDoS attacks can serve the goals of an extortion ring or a group pushing a political agenda.

Legal scholars and legislators might find value in the cyber-dependent/enabled distinction, as it may shape laws that help deal with the threat. By isolating those elements of cybercrime that appear new, decisions can be made as to whether the existing law adequately addresses these novel challenges. But this is ultimately a kind of tactical decision, in the same way that the US Racketeer Influenced and Corrupt Organizations Act (RICO) of 1970 was developed to fight the Mafia beyond what preexisting laws could provide. It does not change the empirical social science reality of what cybercrime is and how it functions.

So where does this leave us in terms of defining this thing we call cybercrime? The above discussion makes clear that the status quo is problematic in various ways [in fact, Steinmetz (2024) advocates for dropping the term entirely]. It also reveals that throughout the history of cybercrime scholarship there has always been an attempt to frame this as a novel phenomenon, whether through definitions or subcategories. Giving in to this instinct too readily is ill advised. But, at least some of this instinct toward the identification of newness must be retained, because crime is not static, and technology clearly transforms aspects of this entrenched societal phenomenon over time. It may be better to think of cybercrime as the most recent phase of how technology has influenced crime. In the case of cybercrime our point of interest is digital technology, but this is part of a broader process that has occurred throughout human history. Two fairly recent examples are (*a*) how automobiles changed the nature of bank robbery, and how police responded (by setting up their own mobile units), and (*b*) mail and wire fraud, both of which were forerunners of cybercrime. This latter example illustrates the way in which offenders find new means to carry out old crimes. But it also shows how the nature of the crimes they commit can change in important ways when, for instance, carried out through the telegraph, the telephone, or the Internet. Specific legislation may be produced to counteract these evolutions; to this day, some cybercrime offences are captured under mail and wire fraud legislation.

Perhaps counterintuitively, the way forward may be to broaden the definition of cybercrime, rather than restrict it, and to mainstream this phenomenon within wider discussions of crime. Rather than creating binary categories, such as cyber-dependent versus cyber-enabled crime, the study of cybercrime should be about comprehending what is happening to crime in the present technological period. A simple functional definition to achieve this would be that *cybercrime is crime that makes use of digital technology in a significant way*. This definition demarcates cybercrime from those crimes that do not engage seriously with technology. But it also allows for soft boundaries where cybercrime and conventional crime may meet, and for cybercrimes to fall across a technical spectrum, from low to medium to high tech. Finally, such a plastic definition means that future evolutions of (cyber)crime can continue to be captured within this conception, as criminal behavior continues to shift in line with technological innovations and the opportunities they create. In essence, this approach embraces the very tension of what is old and what is new, allowing scholars to empirically interrogate new manifestations of cybercrime going forward, without creating new labels that mystify the concept and make it harder to understand and address.

8. CONCLUSION

Cybercrime has evolved significantly in recent decades, morphing from a loosely structured hobby activity to a well-organized and sophisticated profit-driven industry. There have been significant technological advancements during this time, yet the heart of this supposedly new form of crime remains strikingly familiar. Much of the best work in the field suggests many parallels between cybercrime and preexisting forms of criminality. Based on growing evidence, it may be time to abandon the outdated and illusory distinction between cyber-dependent and cyber-enabled crime. The empirical literature suggests that, simply put, cybercrime is crime that uses digital technology

in a significant way, with a spectrum from the low to high tech, and with neither hard internal nor external boundaries delineating the phenomenon. Cybercrime is much more familiar to social scientists than is commonly acknowledged. This understanding should make the topic far more accessible to scholars from many legal and social science fields, encouraging the use of a range of social science approaches. Future research should focus on identifying the particularly novel aspects of cybercrime (see, for example, Weulen Kranenbarg et al. 2018), rather than assuming this novelty is widespread and ingrained.

DISCLOSURE STATEMENT

The author is not aware of any affiliations, memberships, funding, or financial holdings that might be perceived as affecting the objectivity of this review.

ACKNOWLEDGMENTS

This article could not have been written without the dedicated and exemplary research assistance provided by Jack Warburton. I am also grateful to Miranda Bruce, Benoît Dupont, and Scott Shapiro for providing valuable comments on an earlier draft, which greatly enhanced this publication version. Finally, I would like to thank the Editorial Committee of the *Annual Review of Law and Social Science*, and particularly Martin Krygier, for commissioning this review and supporting it throughout the publication process.

LITERATURE CITED

Axelrod R. 2006. *The Evolution of Cooperation*. New York: Basic Books

Barratt M, Ferris J, Winstock A. 2016. Safer scoring? Cryptomarkets, social supply and drug market violence. *Int. J. Drug Policy* 35:24–31

Bernstein L. 1992. Opting out of the legal system: extralegal contractual relations in the diamond industry. *J. Legal Stud.* 21:115–57

Bijlenga N, Kleemans ER. 2018. Criminals seeking ICT-expertise: an exploratory study of Dutch cases. *Eur. J. Crim. Policy Res.* 24:253–68

Bossler A, Berenblum T. 2019. Introduction: new directions in cybercrime research. *J. Crime Justice* 42:495–99

Broadhurst R, Grabosky P, Alazab M, Chon S. 2014. Organizations and cyber crime: an analysis of the nature of groups engaged in cyber crime. *Int. J. Cyber Criminol.* 8:1–20

Bruce M, Lusthaus J, Kashyap R, Phair N, Varese N. 2024. Mapping the global geography of cybercrime with the World Cybercrime Index. *PLOS ONE* 19(4):e0297312

Buil-Gil D, Saldaña-Taboada P. 2022. Offending concentration on the Internet: an exploratory analysis of bitcoin-related cybercrime. *Deviant Behav.* 43:1453–70

Chen S, Hao M, Ding F, Jiang D, Zhang S, et al. 2023. Exploring the global geography of cybercrime and its driving forces. *Hum. Soc. Sci. Commun.* 10:71

Collier B, Clayton R, Hutchings A, Thomas D. 2021. Cybercrime is (often) boring: infrastructure and alienation in a deviant subculture. *Br. J. Criminol.* 61(5):1407–23

Cook K, Hardin R, Levi M. 2005. *Cooperation Without Trust?* New York: Russell Sage Found.

Custers B, Pool R, Cornelisse R. 2019. Banking malware and the laundering of its profits. *Eur. J. Criminol.* 16:728–45

Décary-Hétu D, Dupont B. 2013. Reputation in a dark network of online criminals. *Global Crime* 14:175–96

Décary-Hétu D, Giommoni L. 2017. Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. *Crime Law Soc. Change* 67:55–75

Décary-Hétu D, Leppänen A. 2016. Criminals and signals: an assessment of criminal performance in the carding underworld. *Secur. J.* 29:442–60

Dupont B, Côté A-M, Boutin J-I, Fernandez J. 2017. Darkode: recruitment patterns and transactional features of "the most dangerous cybercrime forum in the world." *Am. Behav. Sci.* 61:1219–43

Dupont B, Côté A-M, Savine C, Décary-Hétu D. 2016. The ecology of trust among hackers. *Global Crime* 17:129–51
Dupont B, Lusthaus J. 2021. Countering distrust in illicit online networks: the dispute resolution strategies of cybercriminals. *Soc. Sci. Comput. Rev.* 40(4):892–913
Duxbury S, Haynie D. 2018a. Building them up, breaking them down: topology, vendor selection patterns, and a digital drug market's robustness to disruption. *Soc. Netw.* 52:238–50
Duxbury S, Haynie D. 2018b. The network structure of opioid distribution on a darknet cryptomarket. *J. Quant. Criminol.* 43:921–41
Ellickson R. 1991. *Order without Law: How Neighbors Settle Disputes.* Cambridge, MA: Harvard Univ. Press
Eur. Comm. 2024. *Cybercrime*. Eur. Comm., Brussels. **https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en**
Furnell S. 2002. *Cybercrime: Vandalizing the Information Society*. Boston/London: Addison-Wesley
Glenny M. 2011. *DarkMarket: CyberThieves, CyberCops and You*. London: Bodley Head
Gordon S, Ford R. 2006. On the definition and classification of cybercrime. *J. Comput. Virol.* 2:13–20
Grabosky P. 2001. Virtual criminality: Old wine in new bottles? *Soc. Legal Stud.* 10:243–49
Hall T, Sanders B, Bah M, King O, Wigley E. 2021. Economic geographies of the illegal: the multiscalar production of cybercrime. *Trends Organ. Crime* 24:282–307
Halpern J. 2015. Bank of the underworld. *The Atlantic*, May. **http://www.theatlantic.com/magazine/archive/2015/05/bank-of-the-underworld/389555/**
Hardy R, Norgaard J. 2016. Reputation in the Internet black market: an empirical and theoretical analysis of the Deep Web. *J. Inst. Econ.* 12:515–39
Holt T. 2013. Exploring the social organisation and structure of stolen data markets. *Global Crime* 14:155–74
Holt T, Bossler A. 2014. An assessment of the current state of cybercrime scholarship. *Deviant Behav.* 35:20–40
Holt T, Lampke E. 2010. Exploring stolen data markets online: products and market forces. *Crim. Justice Stud.* 23:33–50
Holt T, Lee J. 2022. A crime script analysis of counterfeit identity document procurement online. *Deviant Behav.* 43(3):285–302
Hutchings A, Clayton R. 2016. Exploring the provision of online booter services. *Deviant Behav.* 37:1163–78
Hutchings A, Holt T. 2015. A crime script analysis of the online stolen data market. *Br. J. Criminol.* 55:596–614
Hutchings A, Pastrana S. 2019. Understanding eWhoring. In *Proceedings of the 2019 IEEE European Symposium on Security and Privacy*. Stockholm: IEEE
Kigerl A. 2012. Routine activity theory and the determinants of high cybercrime countries. *Soc. Sci. Comput. Rev.* 30:470–86
Kigerl A. 2016. Cyber crime nation typologies: K-means clustering of countries based on cyber crime rates. *Int. J. Cyber Criminol.* 10:147–69
Kruisbergen EW, Leukfeldt ER, Kleemans ER, Roks RA. 2019. Money talks: money laundering choices of organized crime offenders in a digital age. *J. Crime Justice* 42:569–81
Kshetri N. 2010. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*. Berlin: Springer
Lavorgna A. 2015. The online trade in counterfeit pharmaceuticals: new criminal opportunities, trends and challenges. *Eur. J. Criminol.* 12(2):226–41
Leukfeldt ER. 2014. Cybercrime and social ties. *Trends Organ. Crime* 17:231–49
Leukfeldt ER, Kleemans ER, Stol WP. 2017a. Origin, growth and criminal capabilities of cybercriminal networks. *Int. Empir. Anal.* 67:39–53
Leukfeldt R, Kleemans E, Stol W. 2017b. Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks. *Br. J. Criminol.* 57:704–22
Leukfeldt R, Kleemans E, Stol W. 2017c. A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists. *Crime Law Soc. Change* 67:21–37
Leukfeldt ER, Yar M. 2016. Applying routine activity theory to cybercrime: a theoretical and empirical analysis. *Deviant Behav.* 37:263–80
Levi M. 2022. Money mules: some insights into vulnerabilities and networks. *Public Sector Counter Fraud J.* 9:11–13
Levy S. 2010. *Hackers: Heroes of the Computer Revolution*. Sebastopol, CA: O'Reilly Media

Luo Q. 2024. *A qualitative examination of cybercriminal governance in China*. PhD Thesis, Dep. Sociol., Univ. Oxford, Oxford, UK

Lusthaus J. 2012. Trust in the world of cybercrime. *Global Crime* 13:71–94

Lusthaus J. 2013. How organised is organised cybercrime? *Global Crime* 14:52–60

Lusthaus J. 2018. *Industry of Anonymity: Inside the Business of Cybercrime*. Cambridge, MA: Harvard Univ. Press

Lusthaus J, Kleemans E, Leukfeldt R, Levi M, Holt T. 2023. Cybercriminal networks in the UK and beyond: network structure, criminal cooperation and external interactions. *Trends Organ. Crime*. **https://doi.org/10.1007/s12117-022-09476-9**

Lusthaus J, van Oss J, Amann P. 2022. The Gozi group: A criminal firm in cyberspace? *Eur. J. Criminol.* 20(5):1701–18

Lusthaus J, Varese F. 2021. Offline and local: the hidden face of cybercrime. *Policing* 15(1):4–14

Maimon D, Louderback E. 2019. Cyber-dependent crimes: an interdisciplinary review. *Annu. Rev. Criminol.* 2:191–216

Martin J. 2014. Lost on the Silk Road: online drug distribution and the 'cryptomarket.' *Criminol. Crim. Justice* 14:351–67

Martin J, Munksgaard R, Coomber R, Demant J, Barratt M. 2020. Selling drugs on darkweb cryptomarkets: differentiated pathways, risks and rewards. *Br. J. Criminol.* 60:559–78

McGuire M, Dowling S. 2013. *Cyber crime: a review of the evidence*. Res. Rep. 75, Home Off., London. **https://assets.publishing.service.gov.uk/media/5a74fc06e5274a59fa716800/horr75-summary.pdf**

Moore T, Clayton R, Anderson R. 2009. The economics of online crime. *J. Econ. Perspect.* 23(3):3–20

Morselli C, Décary-Hétu D, Aldridge J. 2017. Conflict management in illicit drug cryptomarkets. *Int. Crim. Justice Rev.* 27:237–54

Munksgaard R. 2023. Building a case for trust: reputation, institutional regulation and social ties in online drug markets. *Global Crime* 24:49–72

Nguyen TV. 2022. The modus operandi of transnational computer fraud: a crime script analysis in Vietnam. *Trends Organ. Crime* 25:226–47

Norbutas L, Ruiter S, Corten R. 2020. Believe it when you see it: dyadic embeddedness and reputation effects on trust in cryptomarkets for illegal drugs. *Soc. Netw.* 63:150–61

North D. 1991. Institutions. *J. Econ. Perspect.* 5:97–112

Paquet-Clouston M, Décary-Hétu D, Morselli C. 2018. Assessing market competition and vendors' size and scope on AlphaBay. *Int. J. Drug Policy* 54:87–98

Paquet-Clouston M, Haslhofer B, Dupont B. 2019. Ransomware payments in the Bitcoin ecosystem. *J. Cybersecur.* 5:tyz003

Pastrana S, Hutchings A, Caines A, Buttery P. 2018. Characterizing Eve: analysing cybercrime actors in a large underground forum. In *Research in Attacks, Intrusions and Defenses (RAID) 2018*, ed. M Bailey, T Holz, M Stamatogiannakis, S Ioannidis, pp. 207–27. Lect. Notes Comput. Sci. Cham, Switz.: Springer

Phillips K, Davidson JC, Farr RR, Burkhardt C, Caneppele S, Aiken MP. 2022. Conceptualizing cybercrime: definitions, typologies and taxonomies. *Forensic Sci.* 2:379–98

Porcedda MG, Wall D. 2021. Modelling the cybercrime cascade effect in data crime. In *Proceedings of the 2021 IEEE European Symposium on Security and Privacy Workshops*, pp. 161–77. Piscataway, NJ: IEEE

Poulsen K. 2011. *Kingpin*. New York: Crown Publ.

Przepiorka W, Norbutas L, Corten R. 2017. Order without law: reputation promotes cooperation in a cryptomarket for illegal drugs. *Eur. Sociol. Rev.* 6:752–64

Ragan S. 2012. Eight arrested in Moscow after allegedly stealing millions using Carberp Trojan. *Security Week*, March 21. **http://www.securityweek.com/eight-arrested-moscow-after-allegedly-stealing-millions-using-carberp-trojan**

Roks RA, Leukfeldt ER, Densley JA. 2021. The hybridization of street offending in the Netherlands. *Br. J. Criminol.* 61:926–45

Soudijn M, Zegers B. 2012. Cybercrime and virtual offender convergence settings. *Trends Organ. Crime* 15:111–29

Srivastava S, Das S, Udo G, Bagchi K. 2020. Determinants of cybercrime originating within a nation: a cross-country study. *J. Glob. Inf. Technol. Manag.* 23:112–37

Steinmetz K. 2016. *Hacked: A Radical Approach to Hacker Culture and Crime*. New York: NYU Press
Steinmetz K. 2024. *Against Cybercrime: Toward a Realist Criminology of Computer Crime*. Oxford, UK: Routledge
Sugiura L. 2018. *Respectable Deviance and Purchasing Medicine Online*. Cham, Switz.: Palgrave Macmillan
UNODC (UN Off. Drugs Crime). 2024. *Casinos, money laundering, underground banking, and transnational organized crime in East and Southeast Asia: a hidden and accelerating threat*. Tech. Policy Rep., UNODC, Vienna
Wall D. 1998. Catching cybercriminals: policing the internet. *Int. Rev. Law Comput. Technol.* 12:201–18
Wall D. 2007. *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge, UK: Polity
Wall D. 2008. What are cybercrimes? *Crim. Justice Matters* 58:20–21
Weulen Kranenbarg M, Ruiter S, van Gelder J-L, Bernasco W. 2018. Cyber-offending and traditional offending over the life-course: an empirical comparison. *J. Dev. Life-Course Criminol.* 4:343–64
Yar M. 2005. The novelty of "cybercrime": an assessment in light of routine activity theory. *Eur. J. Criminol.* 2:407–27
Yip M, Webber C, Shadbolt N. 2013. Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Polic. Soc.* 23(4):516–39