Trends in Organized Crime
https://doi.org/10.1007/s12117-023-09486-1

Unpacking the political-criminal nexus in state-cybercrimes: a macro-level typology

Anita Lavorgna[1]

Accepted: 28 January 2023

Abstract

Criminological literature on crime and deviance in cyberspace has boomed in recent years with most studies focusing on computer integrity crimes, computer content crimes and financial cybercrimes, also discussing the opportunity to consider some of these crimes as profit-driven forms of organised crime. The existing literature, however, has not addressed extensively yet the impact of the emergence and proliferation of cyber affordances on forms of state-organized crime – a conceptualization that since the late '80 s proved successful in shedding light, among other things, on the relationships among social structures and criminality. Seeking to address this gap, this conceptual contribution focuses on state-cybercrimes, where illegal, harmful or unjust cyber activities are committed for the benefit of a state or its agencies, offering a macro-typology to shed light on how cyber affordances are influencing and transforming the state-crime relations.

Keywords Cybercrime · Organized crime · State-organized crime · State-cybercrimes · Cyber affordances

Introduction

Criminological literature on crime and deviance in cyberspace – or cyber-criminology – has boomed over the last decade, especially as regards studies focusing on computer integrity crimes, computer content crimes and financial cybercrimes. Not only the criminogenic potential of cyberspace has been discussed, but also its role in affecting patterns of relationship between criminal actors (e.g., Brenner 2002; Musotto and Wall 2020; Leukfledt and Holt 2020; Lusthaus et al. 2022). Existing empirical evidence suggests that most criminal groups operating online are formed of relatively loose and transient networks of relationships (e.g., Wall 2015; Leukfeldt

✉ Anita Lavorgna
anita.lavorgna@unibo.it

[1] Department of Political and Social Sciences, University of Bologna, Str. Maggiore, 45, 40125 Bologna, BO, Italy

Published online: 07 February 2023

et al. 2017; for a critical analysis, see also Lavorgna 2020a). However, both in professional and academic literature forms of co-offending at the basis of serious forms of profit-driven cybercrimes have often been described as forms of organized crime, at times distinguishing them among different sub-types depending on their internal organization and/or the activities carried out (e.g., Choo and Smith 2007; McGuire 2012; Leukfeldt et al. 2019; Wang et al. 2021; Di Nicola 2022; Kranenbarg 2022). In doing so, these studies have often used the term ‘organized crime’ in a broad sense, recognizing that its online manifestations somehow differ from its occurrences in the physical world, and consequently the organized crime label should be used in a more fluid way in the cyber domain (e.g., Di Nicola 2022), where different forms of criminality are becoming increasingly blurred (Choo and Smith 2007).

Hence, a premise is here necessary: in this contribution, as I have done in previous work discussing the cyber-organized crime nexus (e.g., Lavorgna 2015, 2016, 2019, 2020a, b), I prefer to adopt a narrower working definition of organized crime (adapted from the definitions presented in Paoli and Vander Beken 2014:14ff and von Lampe 2016:27ff), more aligned with the definitions stemming from traditional critical organized crime research and that are generally more oriented towards narrower interpretations of what organized crime is (e.g., Paoli 2002; von Lampe 2008, 2016; Longo 2010; Varese 2010; Hobbs 2013; Sergi 2014): a stable organization of three or more members using some forms of discipline and control, systematically engaging in serious criminal offences to acquire profit or power, generally through the use of violence and/or corruption, and able to exert influence on the legal economy and/or the public sphere. The main reason for this choice is that, as traditional organized crime research has already discussed in much detail, the use of the organized crime label has been too often use to allow an ‘emotional kick’ that helps to get resources and powers (Levi 1998: 336; see also Ashby 2016) and to promote securitization practices (Van Duyne and Vander Beken 2009; Carrapico 2014) – a tendency that has already been observed also online (Lavorgna 2016, Lavorgna and Sergi 2016). If from one side it has to be recognized that, for both “some agencies and scholars, organized crime seems to mean little more than co-offending by more than two perpetrators (Paoli and Vander Beken 2014: 14), on the other side it has to be also noted that the vagueness of the concept, which in its broader definitions conflates many different phenomena and problems, has led many to use alternative and more specific (while less evocative) concepts (see Paoli and Vander Beken 2014: 25).

Previous work has already discussed why pairing cybercrime and organized crime can be problematic for empirical, legal, conceptual/theoretical, and practical reasons, both if we consider criminal groups operating exclusively online, and ‘traditional’ organized crime groups (operative offline) that are also engaging in forms of cybercrime (for a closer discussion of this latter case, see Lavorgna 2015). It is important to note that contesting the ‘pairing’ does not mean denying that we can have new organized criminal groups emerging online, or that traditional organized crime groups do never engage in cybercrimes. Nonetheless, such pairing is not a given, and should be used more cautiously. First, unequivocal evidence of the presence of organized crime involvement in most types of cybercrimes is so far missing, as most existing papers are based on hypothesis, on a limited number of case studies, or set extremely low standards for inclusions of different phenomena as organized crime (e.g., Lusthaus 2013; for a more detailed discussion see Lavorgna 2019); rather, we know that specific groups of criminals are involved in specific types of cybercrimes, but this is not ground for generalizations. Second, many common criminal activities considered as cybercrimes (consider for instance many forms of intellectual property infringement, internet frauds or hate crimes) may neither meet the legal threshold to be considered as organized crime in countries that link organized crime to the seriousness of a certain criminal activity, nor be covered by anti-organized crime legislation (e.g., Joseph 2015; Leukfeldt et al. 2017). Indeed, there are national and international initiatives aimed at redrawing the boundaries of regulatory definitions and further legislative harmonization to allow a more effective and coherent response to cybercrimes (Nukusheva et al. 2022). Third, the pairing between 'cyber' and 'organized' risks to be paradoxical, as more efficiency would be reached online by actors relying on a minimum degree of organization (rather than a formal and structured one, as in the working definition of organized crime here adopted) as needless complexity is ineffective for offenders (e.g., Felson and Boba 2010; Ashby 2016); rather, the pairing seems to be linked to the *is-ought* fallacy[1] (Sergi 2014; see also Lavorgna and Sergi 2016). Last, over-estimating organised crime's involvement in a cybercrime can be used to attract more resources and additional legal powers especially regarding digital intrusive surveillance measures, orienting law enforcement's responses and policy makers' reactions alike, while risking of neglecting specific skills and motives when investigating a specific cybercrime. Of course, *certain* cybercrimes might be considered so potentially dangerous to a country's integrity that policy makers might consider using the abovementioned resources and powers. Yet, a connection to organized crime is not necessary, and risks to be used to mislead the public because of its evocative power (e.g., Lavorgna 2016, 2020a; Lavorgna and Sergi 2016).

In pairing cybercrime and organized crime, an additional problem that has not been sufficiently unpacked yet is linked to the fact that, when this pairing occurs, organized crime is generally interpreted according to the Alien Conspiracy approach, as if the groups involved are alien forces outside our mainstream culture, threatening our otherwise sound and safe society and its righteous citizens (Lavorgna 2019) – in other words, as if they were something emerging from a marginal underworld, to which legitimate (and powerful) segments of society are opposed to. However, it has been long described in the literature how not only even the more powerful segments of society and organized crime can coexist in uneasy equilibria (Bayley and Taylor 2009), but the machinery and institutional settings of contemporary states can indeed constitute the ecosystem of some forms of organized crime – so called state-organized crime (Chambliss 1989; Felson 2009; Karstedt 2014).

If we accept that some forms of serious (organized) crime and the state can at time cooperate with various types of relationships and shared networks, or even work together in joint criminal enterprises (as will be discussed more in detail in

[1] The *is-ought* fallacy of Hume's Law identifies a logical fallacy when from a 'to be' characteristic of a certain phenomenon are derived 'ought to be' characteristics without a proper justification.

the next section), there is therefore a key puzzle yet to be solved: when it comes to the relationship between cybercrimes and the state, are comparable relationships in place? And to what extent the emergence and proliferation of cyber affordances (that is, what shapes conditions of possibility in the cyber realm[2]) has an impact on forms of state-organized crime?

This contribution aims to start unpacking this puzzle, offering a macro-level conceptualization of state-cybercrimes. Ontologically, to avoid entering into the legalistic debates of 'what cybercrime is' or 'should be' (Lavorgna 2020b:13ff; Tropina 2020), in a context where we are observing phenomena quickly evolving across diverse jurisdictions, this work considers acts based on behaviours (similar in terms of conceptual, analytical and policy areas) rather than on legal provisions, encompassing them all into the broader criminological concept of 'cybercrimes' as they all produce social harms. As a conceptual study, this article does not offer new empirical data or systematic analyses, but is rather based on the thick description of known cases, making use of information already available in the literature. In doing so, this study furthers four main goals: (1) to clarify the political/ state-criminal nexus in relation to cybercrime; (2) to typify models of state-cybercrime; (3) to understand to what extent the emerge and proliferation of cyber affordances has had an impact on the political/ state-criminal nexus in relation to cybercrime; and (4) to clarify whether forms of state cybercrime are manifestations of state organized crime.

After a focused review of the literature on state-organized crime, and on political cybercrimes and the relevance of cyber affordances in this context, this conceptual article presents a macro-typology of state-cybercrimes, and discusses its heuristic value to shed light on how cyber affordances influence and transform the state-crime relations, stressing how pairing cybercrime and organized crime remains problematic also in the context of the political-criminal nexus.

The political-criminal nexus

The relationships between crime and the state, or more specifically between criminal organizations and governmental institutions or officials,[3] has received scholarly attention in the past decades, with a number of studies detailing how symbiotic relations between those actors – the so-called political-criminal nexus – are at times established and maintained for the benefit of both (e.g., Quinney 1972; Friedrichs 1983, 1998; Michalowski 1985; Simon and Eitzen 1982; Barak 1991; Tunnell 1993;

[2] The notion of affordances, introduced by Gibson (1977) to describe the relationships that exist between organisms and their environments, has been then adapted and refined by other sociologists, *in primis* Hutchby (2001) who defined them as the possibilities that enable and constrain action (see also Bloomfield et al. 2010; Nagy and Neff 2015; Bucher and Helmond 2018). The notion of affordances found a particular fertile ground in the developing field of digital sociology, where affordances of technologies are investigated in various social spheres (Fussey and Roth 2020).

[3] It is important to note that contemporary scholarship conceptualizes the state not as a monolithic Leviathan, but rather as 'an ensemble and structure of institutions […] combining informal constraints and formal rules' (Karstedt 2014:307).

Ross 1998, 2000; Green and Ward 2000; Williams and Godson 2002; Godson 2003; Tombs 2012; von Lampe 2016; Allum and Gilmour 2019). The political-criminal nexus can give rise to several forms of crime interdependence or ‘symbiosis’, such as mutualism (when both parts benefit), parasitism (when one part benefits but the other is harmed), or forms of passive assistance (where one party benefits from the other, without helping or harming it much) (Felson 2006), at times creating forms of overlapping regulatory spaces (Polese et al. 2019). These studies are of great interest as they reverse and complicate the common belief that the state is a victim of crime, rather than an actor in its own account: by showing the Janus-face of contemporary states and their institutions, they create a real paradox as the state becomes the guardian of its own misdemeanours (Karstedt 2014).

More specifically, under the broad umbrella term ‘state crimes’, we find a broad range of illegal, socially injurious or unjust activities of ubiquitous nature, which have the potential to affect large groups of victims (Kauzlarich 1995; Kauzlarich et al. 2001:175; Karstedt 2014:305). These activities can occur domestically (when a government acts to undermine the social, economic or political rights of its own citizens) or internationally (when a government violates the economic, political, or social rights of citizens in other countries), and can violate domestic and/or international standards or regulations (Kauzlarich 1995; Kauzlarich et al. 2001).

We can identify a first research strand on state crimes focusing on international law violations and that, over time, moved increasingly closer to research on the international human rights regime (as summarised by Karstedt 2014:308ff; see for instance Lee 2019; Umaña 2021). A second research strand, which is more relevant in the context of this contribution, is linked to those studies investigating the relationship between the state and serious forms of crime (generally, crime for profit) and particularly organized crime. This relationship is generally referred to as ‘state-organized crime’ (Chambliss 1989), and can be interpreted as a form of organizational crime (Clinard and Quinney 1973; Kauzlarich et al. 2001). These studies have suggested how the political-criminal nexus itself is at the basis of the rise of organized crime (‘traditionally’ intended[4]) in several countries, and it is also a main obstacle to countering organized crime (Williams and Godson 2002). At the core of the notion of state-organized crime, is the idea that every relationship (being it social, political, or economical) contains inherently some contradictions, producing dilemmas and conflicts that people then try to resolve; the contradictions inherent in state formations are those creating the conditions for state criminality, as state officials will violate the law to solve them, even if the law represents a foundation of state legitimacy and for its use of violence (Chambliss 1980, 1988). As such, state-organized crime can be interpreted as ‘a

[4] It is well known in the literature that ‘organized crime’ is a contested concept (see Paoli and Vander Beken 2014). Indeed, to borrow von Lampe’s words, organized crime ‘is not a coherent empirical phenomenon but first and foremost a construct, reflecting social reality as much as the emotions, prejudices, and ideologies of those involved in the construction process’ (Von Lampe 2016:xiv). This notwithstanding, in the literature on ‘state-organized crime’ the latter is generally intended as phenomena traditionally associated with it in terms of the organization of crime, the organization of criminals, and the exercise of power by criminals (on this distinction, see Von Lampe 2016).

solution to the conflicts and dilemmas posed by the simultaneous existence of contradictory "legitimate" goals' (Chambliss 1989:196). After all, it has been claimed that nation states established themselves by acting as racketeers (through the prosecution of war, protection, resource extraction and the building of capital) (Tilly 2017).

Traditional examples of state-organized crime include the historical complicity of some states to piracy, but also cases of smuggling, political assassinations, or violating laws that limit governmental activities (which includes the use of illegal methods of spying on citizens) – when these acts have the characteristic of being part of an institutionalized policy of the state (even if they are defined by law as criminal), and when they facilitate capital accumulation, which is at the basis of a state's power, wealth and survival (as discussed in Chambliss 1989). In all these cases, we can observe a mutually reinforcing ensemble reproducing the existing social order, as organized crime actors become increasingly integrated into political structures in a process of fusion and assimilation (Stephenson 2017; see also Bayart 1993; Tilly 2005; Friedrichs 2010; von Lampe 2016:262ff).

Manifestations of state-organized crime, not surprisingly, are more common in weak states (because of the higher levels of impunity, or because of their low level of legitimacy due for instance to ethnic conflict or terrorist activity), in authoritarian regimes (because of the high levels of corruption, even if the presence of a strong state has an effect in containing some organized crime activities), or in states undergoing profound economic transformations (because of the criminogenic opportunities offered by emerging markets) (as discussed in detail in the political model offered by Williams and Godson 2002). Nonetheless, also democratic and economically stable states can manifest forms of state-organized crime (e.g., Sollund and Goyes 2021).

As noted by von Lampe (2016:288), it is likely that the academic interest in these phenomena has been driven by a willingness to contrast the mythology of organized crime as something emerging from a marginal underworld, opposing a counter-narrative stressing how organized crime can instead be rooted in the more powerful segments of society. These are connections that received attention also thanks to the work of critical criminologists (who have been traditionally concerned with the harms caused by the powerful, see Kauzlarich et al. 2001). But also thanks to research (for instance, on the social embeddedness of organized crime) stressing that we need to look at organized crime's social ties and interactions (Kleemans and van de Bunt 1999; Kleemans 2013); and thanks to the general awareness that ethnicity and kinship are not the only criteria of membership in many organized crime groups, with relationship between families, friends and patrons often playing a key role (Finckenauer 2005; Abadinsky 2007).

In this context, it is worth investigating whether, in the interrelation between crime and the state, the symbiotic relationships that have been studied between the state and non-cybercrime arenas also take place in cybercrime arenas, to discuss whether and to what extent existing forms of state-cybercrime are manifestations (or are comparable to) forms of state-organized crime, or whether cyber affordances are enabling what are indeed different manifestations of the political-criminal nexus.

Political cybercrimes and cyber powers

When we look at crime and deviancy in cyberspace, alongside the profit- or emotion-driven cybercrimes that have been extensively investigated by criminologists especially over the last couple of decades, we can also find a number of so-called ‘political cybercrimes’—here broadly defined as all those behaviours occurring in or facilitated by cyberspace and pivoting around a political element, being the final aim of said behaviour a political act, a policy or an idea (as defined in Lavorgna 2020b). These behaviours have overall received relatively less attention, with the exception of terrorism, political extremism and radicalization (e.g., Hollewell and Longpré 2021; Holt et al. 2022; Jangada Correia 2022).

However, there is a much broader range of political cybercrimes deserving criminological attention, some being criminal activities, while others being harming behaviours that nonetheless lay in that grey area where the construction of social norms is still keeping pace with the opportunities given by technological developments. For instance, the relationship between cybercrime and the state has been touched upon in the context of political cybercrimes when illegal, harmful or unjust acts enabled or facilitated by cyber affordances are committed for the benefit of a state or its agencies, turning cyberspace into an instrument of deception or control. Consider how certain forms of cyberwarfare (such as information pollution) are becoming a distinguishing feature of political life in cyberspace; or forms of ‘political deviancy’, where state actors exploit cyberspace to limit the civil and human rights of their opponents or even of their own citizens (Lavorgna 2020b; see also European Commission 2016; Wardle and Derakhshan 2018).

Despite their heterogeneity, political cybercrimes, when committed by a state, are nothing else than a manifestation of states’ cyber power – that is, their ‘ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain’ and that can be used ‘to produce preferred outcomes within cyberspace or […] in other domain outside cyberspace’ (Nye 2011:123).

Through multi-sited and multi-dimensional cyber affordances, the contemporary state has become a logistical and informational assemblage encompassing both (non-human) technological infrastructures and (human) bureaus with different mandates and expertise, and concerned with areas including law enforcement and security (Follis and Fish 2022). But this has also led to the creation of digital and mediated geographies – or cyberscapes – of both direct and outsourced powers, surpassing the legitimization of state agency as contingent upon a physical territory (Franklin 2018). Overall, cyber affordances have had ‘profound disruptive impacts’ (Siers 2018:568), prompting major changes in national security policies and operations, in a context still lacking a coherent legal framework.

Additionally, cyber affordances have contributed to make the lines between public vs private, economically motivated vs politically instigated cybercrimes all blurred, with the consequence that combating these hybrid harmful activities online has become increasingly complex and politically contested (Farrand and Carrapico 2021), especially considering that attribution (that is, the ability to hold a cyber actor responsible for a specific cyber operation or action, see Siers 2018:559) is not always easy to determine, and that over the years these forms of cyber threats grown from a small number of state actors to a wider arena of both state and non-state actors (Siers 2018).

Over time, different types and categorisations of (cyber) affordances have been proposed, with different focuses depending on the disciplinary angles through which they have been discussed. Consider, for instance, the hegemonic affordances (that is, using the attributes of the technology in a way that conforms with the designers' intended uses) proposed by boyd (2011 – persistence, replicability, scalability, searchability) or by Treem and Leonardi (2012 – persistence, visibility, editability, association). For the scope of this study, it is important mentioning Milioni and Papa's (2022) recent discussion of the oppositional affordances used in data activism, as they identify four main types of affordances that, while developed in a different context, are useful also to enlighten how different cyberscapes encode different action possibilities for different users, and how beyond the hegemonic use of cyber affordances, are oppositional uses, enabling (in the cases of interest for the scope of this work) criminogenic or harming opportunities. These oppositional affordances are: (1) those enabling the use of hidden affordances (that are provided by technologies but are hardly utilized by their users); (2) those creating new affordances (e.g., by creating new tools); (3) meta-affordances (that are acting upon platforms' perceptible affordances); and (4) anti-affordances (hindering or distorting existing affordances).

Regardless of the diverse categorizations of (cyber) affordances, it is also important to note one of their features that has been partially overlooked but that matters from a criminological perspective: that is, the fact that cyber affordances enable criminogenic opportunities as well as grant spaces for action that are still largely unregulated. In this way, they can lead to a context of dysnomie in cyberspace – to borrow Passas' (1999: 410) words, the presence of an ineffective regulatory patchwork and fragmented controls –, hence influencing and transforming also the state-crime relations.

A macro-typology of state-cybercrimes

As discussed above, there is currently a gap in the literature in investigating the impact of the emergence and proliferation of cyber affordances on state-organized crime, to understand whether and to what extent this conceptualization still holds when illegal, harmful or unjust *cyber* activities are committed for the benefit of a state or its agencies as part of an institutionalized policy of the state or to facilitate capital accumulation, fostering forms of crime interdependence with crime actors, enabling criminal networks to rise from the responses of people in positions of power (Chambliss 1989).

This study furthers an exploration of this topic by offering a macro-typology of state-cybercrime that arranges illegal, harmful or unjust *cyber* activities committed for the benefit of a state or its agencies focusing on the following three main macro-types: (a) state-cyberattacks; (b) state-cybercontrol; and (c) state-cyberdeceit.

Overall, these macro-types rely on different types of cyber affordances and on different degrees of dysnomie, leading to differences in the political-criminal nexus at their basis. These variables, of course, capture only a limited portion of the differences across the types identified (but, after all, typologies are not necessarily exhaustive – Smith 2002). Considering that the distinction between crime and warfare, as well as the lines between 'state' and 'non-state' in terms of perpetrators are becoming so blurred that the notion itself of 'cybercrime' has been contested (Farrand and Carrapico 2021), the macro-types selected were considered fit for purpose as (more) heuristically descriptive. They should be considered as ideal (macro) types of state-cybercrimes based on qualitative data derived from the existing literature and empirical cases broadly covered by international media sources in what is a conceptual contribution.

What now needs to be assessed and discussed is whether they are manifestations (or are comparable to) forms of state-organized crime, or whether cyber affordances are rather enabling different manifestations of the political-criminal nexus. For an explorative reflection on this matter, in the remaining part of this article the typology will be discussed with reference to some empirical examples purposedly selected from publicly available data.

State-cyberattacks

The first type of state-cybercrimes here considered are forms of cyberattacks – i.e., when the state is actively using its cyber power to unauthorizedly access other people or other institutions' devices (e.g., smart goods, mobile devices, operating and security systems and networks, including critical infrastructures). Technically, these attacks are mostly forms of hacking. In practice, this can translate in a broad and diverse range of manual or automatized activities, such as theft of computer resources or of confidential information, leeching (the draining of resources, bandwidth or data), spoofing (maliciously impersonating another device or user on a network to launch an attack), denial of service, or malware attacks; and these activities can have different scopes, ranging from sabotage and destruction to espionage and monetary profit. Cyberespionage, for instance, is often carried out as an Advanced Persistent Threat – that is, a set of covert and continuous sophisticated cyber-attacks over a long period of time (Lavorgna 2020b).

In popular culture, for a long time hackers (and certain forms of hacktivism) have been depicted as a law enforcement and national security problem to be addressed through criminalization (as discussed in Follis and Fish 2022). Most criminological attention to the topic is linked to studies on hackers' subcultures (Steinmetz 2016; Collier et al. 2021). From this perspective, in hacking-adjunct activities, we can find different 'moral expressions' (to borrow the words from Coleman and Golub 2008) sharing a cultural sensitivity (under constant negotiation and reformulation) towards liberalism, and a confidence in hackers' capacity to craft technological solutions. However, the relationship between the state and hackers is also open to possibilities for collaboration: rather than a problem, hacking can be seen as a transformative resource providing strategic and tactical advantage to a state (for instance through forms of weaponized hacking) (Follis and Fish 2022). Indeed, certain state agencies supported the development of hacking, as it allowed the first government built internet infrastructures, and helped framing the geek culture at the core of some defence-sponsored research programmes¸ to the point that the boundaries of state/hacker interactions are now considered as fluid and open to contingency (Follis and Fish 2022), even if cyber-attacks are generally considered as against the law internationally (Trahan 2021) and, in many States, also domestically.

Cyberattacks, when directed against an adversary or enemy, can be considered acts of cyberwarfare, regardless of whether they are undertaken by state or non-state actors (Szafranski 1995; Grabosky 2016). They could be directed towards a military target (consider, for instance, the Russian cyberwarfare between 2014 and 2017 during the siege of the Donetsk airport, when Russia was able to jam GPS, radios and radar signals, crippling communications and impeding Ukrainian troops from using radios and phones for hours at a time – Greenberg 2019). But they could also be directed against civilian facilities such as water, power and heath supplies, critical manufacturing and food production, hence directly threatening human health and well-being (Hardy 2010; Grabosky 2016; Martellini et al. 2017), or against private actors for strategic or reputational motives. Again in the context of the Russian cyberwarfare against Ukraine, for instance, it has been reported that in the months leading to the 2022 invasion several Ukrainian energy and IT providers were targeted with viruses that deleted data and disabled computers; similarly, some Ukrainian banking and government websites were attacked by the destructive malware WhisperGate (Reuters 2022). As such demonstrating that, even if cyber operations appear to have played only a limited role in the initial stages of the invasion, mostly with lower level but destabilizing operations, allowing deniability for states to limit escalation (Eichensehr 2022), war nowadays can easily become hybrid, using physical and cyber attacks, in an integrated way.

Only a limited number of cyber-attacks have been publicly attributed to nation-states. In most cases, they have been ascribed to their ‘proxies’ – that is, non-state actors used by state actors (Maurer 2016, 2018), leading to regulatory uncertainties and limited accountability (Johnson and Schmitt 2021; Akoto 2022). Consider, for instance, the notorious case of Stuxnet (a computer worm reportedly created in a joint United States-Israel operation and first discovered in 2010, and deemed responsible for causing substantial damage to Iran’s nuclear programme, wreaking physical damage by means of a cyber-attack – Denning 2012); or the famous attacks carried out by the Lazarus Group (such as the 2014 attack on Sony Pictures, or its involvement in the 2017 WannaCry ransomware), which allegedly has links to North Korea (Guiora 2017); the political cyberespionage carried out by groups such as Guccifer2.0 or FancyBear (linked to Russia’s GRU intelligence agency- see Lavorgna 2020b) or, more recently, the attacks of the Russian hacking team Sandworm (reportedly part of Russia’s military intelligence agency) against power grids in Ukraine (Reuters 2022) As recently discussed by Eichensehr (2022), for states masking their involvement and posing attribution challenges becomes part of the strategy, as lines between state and non-state actors become increasingly blurred by involving ‘hackers with murky relations with states’, from both sides (Eichensehr 2022: 148).

Either ways, in state-cyberattacks the attacker mostly relies on 'hidden affordances' (those provided by technologies but hardly utilized by their users – Milioni and Papa 2022), making the most of the criminogenic opportunities these can provide. In order to do so, the attackers mostly need to rely on a specific digital, technical capital: the success of these types of cyberattacks directly depends on the technical capacities of those involved, rather than on their personal connections. As such, even when the political-criminal nexus in cyberattacks give rise to mutualism (even if in dynamic forms), and regardless of the capital accumulation these cyberattacks can cause (or they fact that hackers are aligned with their ideological motivation), there is no evidence at the moment suggesting that the criminal actors involved are becoming increasingly integrated in the existing power-structures as observed in traditional forms of state-organized crime (with the exception of those hackers working directly for a state apparatus, and becoming comparable to a part of the army), possibly because of the different social embeddedness of the operational actors behind the attack.

State-cybercontrol

While the mythology of cyberspace, stemming from the early views of digital libertarians, has often described it as a transcendent space, in reality cyberspace is situated in the world of politics and history (Bomse 2001), and it has been moving towards an architecture of control (Lessig 1999). Here, we find forms of state cybercontrol that can be directed both at the state's own citizens and to foreigners, or can be even directed at foreign powers and their agents, turning cyberspace into a new place of surveillance – which has long been recognised as a distinguishing feature of late modernity (Foucault 1975; Mathiesen 1997; Ball and Webster 2003; Lyon 2007; Bauman and Lyon 2013). Of course, mass surveillance systems have been used by governmental agencies in the past, but the scale of pervasiveness of contemporary mass surveillance is something different, as became evident in the 'post-Snowden' era. It has been claimed that digital technologies have increased the state's capacity for surveillance, turning cyberspace into a 'virtual panopticon' (Nyst 2018). As such, in recent years, conventional surveillance techniques have been juxtaposed by both personal and mass data surveillance monitoring our digital footprints (so-called 'dataveillance'), with forms of pervasive online surveillance that can take place manually (for example, monitoring social media activities by reading posts) or via automated methods (such as cookies, spyware, or browser records) (Lavorgna 2020b).

In cases of state cybercontrol, surveillance can be illegal, or formally in line with the law (as the state might derive from the law a legitimate power to monitor, for instance, suspicious or otherwise potentially criminal activities) but socially deviant or harmful (described as political deviancy in an earlier work, see Lavorgna 2020b), keeping in mind that defining what is acceptable when it comes to surveillance shifts depending on cultural, political and social factors. Indeed, states can construct legal frameworks that allow extreme surveillance practices, while shielding them from accountability and redress mechanisms (Nyst 2018). But also the controllers need to be controlled: otherwise, without proper mechanisms of safeguard in place, dystopic futures might be closer than expected. In fact, digital surveillance has direct, negative impacts on the enjoyment of rights such as privacy, free association, speech and opinion, as well as can cause the deprivation of citizens from access to information, or their capacity to engage in democratic debates (Nyst 2018), to the point that cybersecurity (for state actors, an extension of national security) has become, in certain cases, misaligned from personal digital security, as governmental agencies become a source of digital threat to individual citizens, compromising fundamental rights (Zajko 2018). For instance, state surveillance can lead to forms of censorship, as the same communication and information technologies that offer activist new ways to expose and challenge state criminality, fostering emerging dimensions through which civil society can become a counter-weight to the hegemonic powers of states and corporations (see for instance Kasm 2018; Kasm and Alexander 2018) are used to limit the human and civil rights of opponents. Consider, for instance, the use of internet shutdowns for political purposes, in trying to disperse political dissent (Lavorgna 2020b).

In cases of state cybercontrol, hidden affordances (those provided by technologies but hardly utilized by their users) and anti-affordances (those hindering or distorting existing hegemonic affordances – Milioni and Papa 2022) are mostly used. Here, non-state actors are involved, but mostly in the form of tech giants and other corporate actors (hence, through forms of white collar crimes or, more often, while collar *harms*). First, state and corporate surveillance can converge, enabled by the monetary value of our digital data that can be hoarded ad exploited by private actors and then shared with government agencies, in a context where there is no real democratic oversight of what happens to these data (McGuire 2009). Consider, for instance, the 2018 Facebook and Cambridge Analytica data breach scandal, when up to 87 million Facebook users may have had personally identifiable information illegitimately accessed since 2014 by Cambridge Analytica, a British political consulting firm specialising in data mining, brokerage and analysis in electoral strategic communication, with data then used by various political organisations to influence voter opinion (Venturini and Rogers 2019; Lavorgna 2020b). Comparably, because of their role in cyber governance, the role of tech giants (e.g., Meta and Twitter) in furthering governmental agendas against the free Web cannot be ignored, for instance when they submit to the censorship demands of authoritarian regimes, or in light of some of their moderation policies that might be blocking large amounts of content in certain countries (Moini et al. 2017; Mueller 2017; Lavorgna 2020b). Second, also other tech companies and especially so-called ‘digital era mercenaries’ (a handful of companies selling surveillance tools also to undemocratic countries – Moini et al. 2017) can have a key role, in light of the lack (at the moment of writing) of stringent international mechanisms regulating surveillance technology. Indeed, the surveillance products they sell are designed to enable government agencies to circumvent anonymising techniques such as data encryption and can be used to spy, for instance, on critical journalists and internet activists, in violation of human rights and freedom of information (Moini et al. 2017; Lavorgna 2020b).

State-cyberdeceit

The manipulation of information, including the fabrication of content, to obtain a competitive advantage over an adversary has become a preferred manifestation of cyber power in our contemporary word, thanks to the presence of innumerable platforms hosting and reproducing this information (Wardle and Derakhshan 2017). In some of its more severe manifestations, cyberdeceit is nothing else than a modern form of information warfare; more broadly, it can be a form of macro-level social engineering.

The more prominent form of cyberdeceit is probably so-called information pollution, an umbrella term which includes misinformation (when false information is shared but no harm is meant), disinformation (when false information is knowingly shared to cause harm) or malinformation (when genuine information is shared to cause harm) (Wardle and Derakhshan 2017; Lavorgna 2021). Polluted information, at the basis of contemporary 'post-truth' mechanisms, can be used to discredit opponents, and even to undermine the free press, intervening in opinion formation with harmful social consequences (making people less knowledgeable, undermining democratic electoral processes, sharpening existing socio-cultural divisions, amplifying and polarising divisive and controversial socio-political issues, and making people more sceptical towards legitimate news producers and accurate reporting (Allcott and Gentzkow 2017; Lavorgna 2020b). Polluted information generally prays on a range of psychological mechanisms that make people more prone to accept information more in line with their system of beliefs, rather than something questioning them (for an overview, see Prot and Anderson 2019). Our existing legal framework is not yet fit for purpose to address these new cyber challenges, making them a clear manifestation of a dysnomic arena (Tambini 2021; Sloss 2022).

Hegemonic social media affordances (e.g., boyd 2011) provide a fertile ground to spread polluted information because of micro- and meso-level bottom-up dynamics (see, for instance, Lavorgna 2021). Other times, however, at the core of polluted information are top-down, sophisticated mechanisms mostly based on oppositional new, meta-, and anti- affordances (Milioni and Papa 2022), such as the fabrication of textual or image-based information, or even of entire websites created to spread mis- or disinformation; astroturfing (i.e., the practice of creating an impression of widespread grassroots support for a policy or individual – where little such support actually exists – by using fake pressure groups or multiple online identities, see Popham 2018); or the creation of fake personas (as in the cases of fake attractive cosmopolitan young women whose fabricated online profiles were used as honeypots to attract phishing victims to access sensitive digital information by state proxies, or more generally the use of fake social media profiles or bots posing as real users and that can be created or bought online, see Lavorgna 2020b). Software tools allowing to falsify persons' identities in pictures, audios and videos (such as the notorious DeepFake) are worsening the situation, making polluted information more difficult to identify (e.g., Chesney and Citron 2019), as we generally consider trustworthy what we hear and see.

In forms of cyberdeceit, it is important to note that the collected and distributed nature of harming behaviours (especially the bottom-up ones, demonstrating the collective and distributed nature of agency in many digital harms, with a variety of other human and nonhuman actors involved, ranging from occasional sharers of misinformation to platforms' affordances and algorithms), as well as the presence of 'fake news farms' generally run by individuals or small companies for profit or, more rarely, for ideology (Graan 2018; Lavorgna 2020b) suggest the parasitic role of states in taking advantage of digital sociotechnical dynamics. On the other hand, some forms of cyberdeceit are (allegedly, as the use of proxies and the issues of attribution persists) directly state-sponsored (consider for instance the reported examples of South Korea National Intelligence Service involvement in affecting public opinion ahead of their political elections in 2013, or Russian state-sponsored inference in American and European elections, which since 2016 has been the object of numerous enquiries – e.g., Grabosky 2016; Stelzenmüller 2017; Baines and Jones 2018).

Conclusion

In the Introduction to this contribution, we have seen how criminological literature on crime and deviance in cyberspace has boomed in recent years, often pairing (in the Author's perspective, in a problematic way) serious forms of cybercrime to organized crime. The existing literature, however, has not explicitly addressed the impact of the emergence and proliferation of cyber affordances on those forms of criminality where organized crime and the state cooperate via various types of relationships and shared networks, or even work together in joint criminal enterprises, generally in ways through which organized crime actors become increasingly integrated into political structures in a process of fusion and assimilation. As such, this article had four main goals: (1) to clarify the political/state-criminal nexus in relation to cybercrime; (2) to typify models of state-cybercrimes; (3) to understand to what extent the emerge and proliferation of cyber affordances has had an impact on the political/ state-criminal nexus in relation to cybercrime; and (4) to clarify whether forms of state-cybercrime are manifestations of state organized crime.

First, this conceptual contribution tried to start addressing this gap by evidencing how symbiotic relationships between the state and crime exists also in relation to cybercrime, but also showing that these relationships can manifest themselves in various, different ways, that are not always immediately translatable into what we know of traditional forms of the political/state-criminal nexus (*in primis,* when it comes to forms of the so-called state-organized crime). In this context, we have also exemplified the presence of individuals, legitimate companies and some criminal networks involved in state-cybercrime that in most cases, however, do not seem to become integrated into political structures.

Second, a macro-typology of state-cybercrimes (state-cyberattacks; state-cybercontrol; and state-cyberdeceit) was proposed. The proposed typology wants to be a starting point for further heuristic and theoretical reflections, aiming to assist systematic studies on the topic.

Third, we have seen that the types of state-cybercrimes identified rely on different types of oppositional cyber affordances, have a different level of dysnomie involved (in other words, some activities are more clearly defined and recognised as crimes at both local and international levels, while other activities have a more contested nature), and are carried out by different actors. Hence, it is claimed that cyber affordances are enabling different, more fluid, manifestations of the political-criminal nexus that can help us reinterpreting certain forms of (state) responsibility in terms of collectives (Franklin 2018), without having to rely on the organized crime label.

Finally, in all the macro-types discussed, we have seen that the actors involved in state cybercrimes – despite the seriousness of their actions – are generally not to be easily labelled as forms of organized crime (at least, not according to the narrower definition of organized crime adopted and upheld in this article). As such, this contribution furthers my previous studies criticizing the use of the 'cyber-organized crime' rhetoric, presenting a new case in which the pairing of 'organized crime' and 'serious crime' in cyberspace does not fully hold.

Of course, as stressed already above, as a conceptual study based on the thick description of known cases, this contribution has some clear limitations, and a limited scope: better data would be needed to systematically assess and test the types proposed, and to further develop them by considering more in detail – among other things – the characteristics of the perpetrators involved (both at the state and the cyber levels), the organizational models they rely on, and the presence of specific *modi operandi* (e.g., violence or corruption). Additionally, it is recognised that the distinction between crime, digital harming behaviours and other 'hybrid threats', and the distinction between 'state' and 'non-state' actors are becoming increasingly blurred (Farrand and Carrapico 2021). In this context, not only there is a need for better engagement in the fields of cyber-criminology and cybersecurity (as recently advocated by Dupont and Whelan 2021), but more generally for multi- and interdisciplinary research bringing together those disciplines from the broad 'social sciences' family that collectively can help understand the complex and transformative dynamics operated by digital affordances into the sociotechnical fabric of our contemporary society.

Acknowledgements The author would like to acknowledge the insights received during the European Initiative for Security Studies (EISS) conference 2022 and the ECPR Standing Group on Organized Crime (SGOC) conference 2022.

Funding Open access funding provided by Alma Mater Studiorum - Università di Bologna within the CRUI-CARE Agreement.

Declarations

Conflict of interests There are no potential conflict of interests; no research involving human participants and/or animals; no need to use informed consent in this research as this is a conceptual article.

References

Abadinsky H (2007) Organized crime, 8th edn. Thomson Wadsworth, London

Akoto W (2022) Accountability and cyber conflict: examining institutional constraints on the use of cyber proxies. Confl Manag Peace Sci 39(3):311–332

Allcott H, Gentzkow M (2017) Social media and fake news in the 2016 elections. J Econ Persp 31(2):211–236

Allum F, Gilmour S (eds) (2019) Handbook of organised crime and politics. Edward Elgar Publishing

Ashby MPJ (2016) Is metal theft committed by organized crime groups, and why does it matter? Criminol Crim Just 16(2):141–157

Baines P, Jones N (2018) Influence and interference in foreign elections: the evolution of its practice. RUSI J 163(1):12–19

Ball K, Webster F (2003) The intensification of surveillance: crime, terrorism, and warfare in the information age. Pluto Press, London

Barak G (1991) Crimes by the capitalist state. State University of New York Press, Albany

Bauman Z, Lyon D (2013) Liquid surveillance. A conversation. Polity Press, Cambridge

Bayart JF (1993) The State in Africa: the politics of the belly. Longman, London

Bayley J, Taylor M (2009) Evade, corrupt, or confront? Organized crime and the state in Brazil and Mexico. J Polit Latin Am 1(2):3–29

Bloomfield BP, Latham V, Vurdubakis T (2010) Bodies, technologies and action possibilities: when is an affordance? Sociology 44(3):415–433

Bomse AL (2001) The dependence of cyberspace. Duke Law J 50:1717–1749

boyd d (2011) Social network sites as networked publics: Affordances, dynamics, and implications. In: Papacharissi Z (ed) A networked self: identity, community, and culture on social network sites. Routledge, New York, pp 39–58

Brenner SW (2002) Organized cybercrime-how cyberspace may affect the structure of criminal relationships. NCJL Tech 4:1

Bucher T, Helmond A (2018) The affordances of social media platforms. In: Burgess J, Marwick A, Poell T (eds) The Sage handbook of social media. Sage, London

Carrapico H (2014) Analysing the European Union's responses to organized crime through different securitization lenses. Eur Secur 23(4):601–661

Chambliss WJ (1980) On lawmaking. Br J Law Soc 6:149–172

Chambliss WJ (1988) Exploring criminology. Macmillan, New York

Chambliss WJ (1989) State-organized crime. Criminology 27(2):183–208

Chesney R, Citron D (2019) Deepfakes and the new disinformation war: the coming age of post-truth geopolitics. Foreign Aff 98:147

Choo KKR, Smith RG (2007) Criminal exploitation of online systems by organised crime groups. Asian J Criminol 3(1):37–59

Clinard M, Quinney R (1973) Criminal behavior systems: a typology. Holt, Rinehart, and Winston, New York

Coleman G, Golub A (2008) Hacker practice: moral genres and the cultural articulation of liberalism. Anthropol Theory 8(3):255–277

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):1407–1423

Denning DE (2012) Stuxnet: what has changed? Future Internet 4:672–687

Di Nicola A (2022) Towards digital organized crime and digital sociology of organized crime. Trends Organized Crime. https://doi.org/10.1007/s12117-022-09457-y

Dupont B, Whelan C (2021) Enhancing relationships between criminology and cybersecurity. J Criminol 54(1):76–92

Eichensehr K (2022) Ukraine, cyberattacks, and the lessons for international law. AJIL Unbound 116:145–149

European Commission and High Representative of the Union for Foreign Affairs and Security Policy (2016) Joint framework on countering hybrid threats (No. JOIN(2016) 18)

Farrand B, Carrapico H (2021) The how and why of cybercrime: the EU as a case study of the role of ideas, interests, and institutions as drivers of a security-governance approach. In: Lavorgna A, Holt TJ (eds) Researching cybercrimes. Palgrave Macmillan, Cham

Felson M (2006) Crime and nature. Sage, Thousand Oaks

Felson M (2009) The natural history of extended co-offending. Trends Organized Crime 12(2):159–165

Felson M, Boba R (2010) Crime and everyday life. Sage, Thousand Oaks

Finckenauer JO (2005) Problems of definition: what is organised crime. Trend in Organized Crime 8(3):63–83

Follis L, Fish A (2022) State hacking at the edge of code, capitalism and culture. Inf Commun Soc 25(2):242–257

Foucault M (1975) Surveiller et punir. Naissance de la prison. Éditions Gallimard, Paris

Franklin MI (2018) Refugees and the (Digital) Gatekeepers of 'Fortress Europe.' State Crime J 7(1):77–99

Friedrichs DO (1983) Victimology: a consideration of the radical critique. Crime and Delinquency, April, 283–294

Friedrichs DO (1998) State crime: Volumes I and II. Ashgate, Adelrshot

Friedrichs DO (2010) Trusted criminals: white collar crime in contemporary society, 4th edn. Wadsworth, Belmont

Fussey P, Roth S (2020) Digitizing sociology: continuity and change in the internet era. Sociology 54(4):659–674

Gibson J (1977) The theory of affordances. In: Shaw R, Bransford J (eds) Perceiving, acting, and knowing: toward an ecological psychology. Erlbaum, Hillsdale, NJ, pp 67–82

Godson R (2003) Menace to society: Political-criminal collaboration around the world. Transaction Publishers, New Brunswick

Graan A (2018) The fake news mills of Macedonia and other liberal panics. Hot Spots, Cultural Anthropology website. Available at: https://culanth.org/fieldsights/1419-the-fake-news-mills-ofmacedonia-and-other-liberal-panics

Grabosky P (2016) Cybercrime. Oxford University Press, Oxford

Green PJ, Ward T (2000) State crime, human rights, and the limits of criminology. Soc Justice 2:101–120

Greenberg A (2019) Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers. Anchor, Hamburg

Guiora AN (2017) Cybersecurity. Geopolitics, law, and policy. Routledge, New York

Hardy K (2010) Operation Tritstorm: hacktivism or cyber-terrorism? UNSW Law Journal 33(2):474–502

Hobbs D (2013) Lush life: constructing organised crime in the UK. Oxford University Press, Oxford

Hollewell GF, Longpré N (2021) Radicalization in the social media Era: understanding the relationship between self-radicalization and the internet. International journal of offender therapy and comparative criminology, 0306624X211028771

Holt TJ, Chermak SM, Freilich JD, Turner N, Greene-Colozzi E (2022) Introducing and Exploring the Extremist Cybercrime Database (ECCD). Crime & Delinquency, 00111287221083899

Hutchby I (2001) Technologies, texts and affordances. Sociology 35(2):441–456

Jangada Correia V (2022) An explorative study into the importance of defining and classifying cyber terrorism in the United Kingdom. SN COMPUT SCI 3:84

Johnson DE, Schmitt MN (2021) Responding to proxy cyber operations under international law. The Cyber Defense Review 6(4):15–34

Joseph SW (2015) Dismantling the internet mafia: RICO's applicability to cyber crime. Rutgers Comput Technol Law J 41:268–297

Karstedt S (2014) Organizing crime: the State as agent. In: Paoli L (ed) The Oxford handbook of organized crime. Oxford University Press, Oxford

Kasm S (2018) Redefining publics: Mosireen, state crime and the rise of a digital public sphere. State Crime J 7(1):100–140

Kasm S, Alexander A (2018) State crime and digital resistance: introduction. State Crime J 7(1):4–7

Kauzlarich D (1995) A criminology of the nuclear state. Humanit Soc 19:37–57

Kauzlarich D, Matthews RA, Miller WJ (2001) Toward a victimology of state crime. Crit Criminol 10:173–194

Kleemans ER (2013) Organized crime and the visible hand: A theoretical critique on the economic analysis of organized crime. Criminol Crim Just 13(5):615–629

Kleemans ER, van de Bunt HG (1999) The social embeddedness of organized crime. Trends Organized Crime 5(1):19–36

Kranenbarg MW (2022) When do they offend together? Comparing co-offending between different types of cyber-offenses and traditional offenses. Comput Hum Behav 130:107186

Lavorgna A (2015) Organised crime goes online: realities and challenges. J Money Laund Control 18(2):153–168

Lavorgna A (2016) Exploring the cyber-organised crime narrative: the hunt for a new bogeyman? In: van Duyne PC, Scheinost M, Antonopoulos GA, Harvey J and von Lampe K (eds) Narratives on organised crime in Europe. Criminals, corrupters and policy. Wolf Legal Publishers

Lavorgna A (2019) Cyber-organised crime. A case of moral panic? Trends Organ Crime 22:357–374

Lavorgna A (2020a) Organised crime and cybercrime. In: Holt TJ, Bossler A (eds) The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave

Lavorgna A (2020b) Cybercrimes: critical issues in a global context. Bloomsbury, London

Lavorgna A (2021) Information pollution as social harm: Investigating the digital drift of medical misinformation in a time of crisis. Emerald Publishing

Lavorgna A, Sergi A (2016) Serious, therefore organised? A critique of the emerging “cyber-organised crime” rhetoric in the United Kingdom. Int J Cyber Criminol 10(2):170–187

Lee R (2019) Myanmar’s citizenship law as state crime: a case for the international criminal court. State Crime J 8(2):241–279

Lessig L (1999) Code and the others laws of cyberspace. Basic Books, New York

Leukfeldt ER, Holt TJ (2020) Examining the social organization practices of cybercriminals in the Netherlands online and offline. Int J Offender Ther Comp Criminol 64(5):522–538

Leukfeldt ER, Lavorgna A, Kleemans ER (2017) Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. Eur J Crim Policy Res 23(3):287–300

Leukfeldt ER, Kruisbergen EW, Kleemans ER et al (2019) Organized financial cybercrime: criminal cooperation, logistic bottlenecks, and money flows. In: Holt T, Bossler A (eds) The Palgrave handbook of international cybercrime and cyberdeviance. Palgrave, Cham

Levi M (1998) Perspectives on ‘organized crime’: an overview. Howard J Crim Justice 37:335–345

Longo F (2010) Discoursing organized crime: towards a two-level analysis. In: Longo F, Irrera D, Kostakos P (eds) Allum F. Defining and defying organised crime, Routledge, pp 35–48

Lusthaus J (2013) How organised is organised cybercrime? Global Crime 14(1):52–60

Lusthaus J, van Oss J, Amann P (2022) The Gozi group: a criminal firm in cyberspace? Eur J Criminol (online first)

Lyon D (2007) Surveillance studies: an overview. Polity, Cambridge

Martellini M, Abaimov S, Gaycken S, Wilson C (2017) Information security of highly critical wireless networks. Springer, Cham

Mathiesen T (1997) The viewer society: Michel Foucault’s ‘Panopticon’ revisited. Theor Criminol 1(2):215–234

Maurer T (2016) ‘Proxies’ and cyberspace. Conflict Secur Law 21(3):383–403

Maurer T (2018) Cyber mercenaries. Cambridge University Press, Cambridge

McGuire M (2009) Online surveillance and personal liberty. In: Jewkes Y, Yar M (eds) Handbook of Internet crime. Routledge, London

McGuire M (2012) Organised crime in the digital age. John Grieve Centre for Policing and Security, London

Michalowski RJ (1985) Order, law, and power. Random House, New York

Milioni DL, Papa V (2022) The oppositional affordances of data activism. Media Int Aust. https://doi.org/10.1177/1329878X221074795

Moini R, Ismail B, Vialle E (2017) Censorship and surveillance of journalists: an unscrupulous business. Reports Without Borders. Available at: rsf.org/sites/default/files/rsf_report_censorship_and_surveillance_of_journalists_0.pdf

Mueller M (2017) Will the Internet fragment? Sovereignty, globalization, and cyberspace. Wiley, Hoboken

Musotto R, Wall DS (2020) More Amazon than Mafia: analysing a DDoS stresser service as organised cybercrime. Trends Organized Crime. https://doi.org/10.1007/s12117-020-09397-5

Nagy P, Neff G (2015) Imagined affordance: reconstructing a keyword for communication theory. Social Media + Society 1(2):1–9

Nukusheva A, Zhamiyeva R, Shestak V et al (2022) Formation of a legislative framework in the field of combating cybercrime and strategic directions of its development. Secur J 35:893–912

Nye J (2011) The future of power. Public Affairs, New York

Nyst C (2018) Secrets and lies: the proliferation of state surveillance capabilities and the legislative secrecy which fortifies them – an activist’s account. State Crime J 7(1):8–23

Paoli L (2002) The paradoxes of organized crime. Crime Law Soc Chang 37(1):51–97

Paoli L, Vander Beken T (2014) Organized crime: a contested concept. In: Paoli L (ed) The Oxford handbook of organized crime. OUP, Oxford, pp 13–31

Passas N (1999) Globalization, criminogenic asymmetries and economic crime. Eur J Law Reform 1(4):399–424

Polese A, Russo A, Strazzari F (2019) Introduction: 'The Good, the Bad and the Ugly': transnational perspectives on the exralegal field. In: Polese A, Russo A, Strazzari F (eds) Governance beyond the law: the immoral, the illegal, the criminal. Palgrave Macmillan, Cham

Popham J (2018) Microdeviation: observations on the significance of lesser harms in shaping the nature of cyberspace. Deviant Behaviour 39(2):159–169

Prot S, Anderson CA (2019) Science denial. Psychological processes underlying denial of science-based medical practices. In: Lavorgna A, Di Ronco A (eds) Medical misinformation and social harm in non-science-based health practices. A multidisciplinary perspective. Routledge, London

Quinney R (1972) Who is the victim? Criminology 10(3):314–323

Reuters (2022) The cyber war between Ukraine and Russia: An overview. Available at : https://www.reuters.com/world/europe/factbox-the-cyber-war-between-ukraine-russia-2022-05-10/

Ross JI (1998) Situating the academic study of controlling state crime. Crime Law Soc Chang 29:331–340

Ross JI (2000) Varieties of state crime and its control. Criminal Justice Press, Monsey

Sergi A (2014) Organised crime in criminal law: conspiracy and membership offences in Italian, English and international frameworks. King's Law J 25(2):185–200

Siers R (2018) Cybersecurity. In: Williams PD, McDonald M (eds) Security studies. Routledge, Abingdon

Simon DR, Eitzen SD (1982) Elite deviance. Allyn and Bacon, Needham Hieghts

Sloss DL (2022) Tyrants on twitter: protecting democracies from information warfare. Stanford University Press, Redwood City

Smith KB (2002) Typologies, taxonomies, and the benefits of policy classification. Policy Stud J 30(3):379–395

Sollund R, Goyes DR (2021) State-organized crime and the killing of wolves in Norway. Trends Organ Crim 24:467–484

Steinmetz KF (2016) Hacked: a radical approach to hacker culture and crime. NYU Press, New York

Stelzenmüller C (2017) The impact of Russian interference on Germany's 2017 elections. Testimony before the US Senate Select Committee on Intelligence, June, 28

Stephenson S (2017) It takes two to tango: the state and organized crime in Russia. Curr Sociol 65(3):411–426

Szafranski R (1995) A theory of information warfare: preparing for 2020. Airpower Journal, Spring

Tambini D (2021) Algorithmic pluralism: media regulation and system resilience in the age of information warfare. In: The world information war. Routledge, London, pp 165–185

Tilly C (2005) Trust and rule. Cambridge University Press, New York

Tilly C (2017) War making and state making as organized crime. Routledge, London

Tombs S (2012) State-corporate symbiosis in the production of crime and harm. State Crime J 1(2):170–195

Trahan J (2021) The criminalization of cyber-operations under the Rome statute. J Int Crim Justice 19(5):1133–1164

Treem JW, Leonardi PM (2012) Social media use in organizations: exploring the affordances of visibility, editability, persistence, and association. Commun Yearbook 36:143–189

Tropina T (2020) Cybercrime: setting international standards. Routledge handbook of international cybersecurity. Routledge, London, pp 148–160

Tunnell KD (1993) Political crime in contemporary America. Garland, New York

Umaña C (2021) A genealogy of state crime in international law: contrasting criminological perspectives. State Crime J 10(2):304–326

Van Duyne PC, Vander Beken T (2009) The incantations of the EU organised crime policy making. Crime Law Soc Chang 51:261–281

Varese F (2010) What is organised crime? In: Varese F (ed) Organised crime: critical concepts in criminology. Routledge, New York, pp 1–33

Venturini T, Rogers R (2019) 'API-based research' or how can digital sociology and journalism studies learn from the Facebook and Cambridge Analytica data breach. Digit J 7(4):532–540

von Lampe K (2008) Organized crime in Europe: conceptions and realities. Policing 2(1):7–17

Von Lampe K (2016) Organized crime. Analyzing illegal activities, criminal structures, and extra-legal governance. Sage, London

Wang P, Su M, Wang J (2021) Organized crime in cyberspace: how traditional organized criminal groups exploit the online peer-to-peer lending market in China. Br J Criminol 61(2):303–324

Wall DS (2015) Dis-organised crime: towards a distributed model of the organization of cybercrime. Eur Rev Organised Crime 2(2):71–90

Wardle C, Derakhshan H (2017) Information disorder: toward an interdisciplinary framework for research and policy making. Council of Europe report DGI(2017)09

Wardle C, Derakhshan H (2018) Thinking about 'information disorder': formats of misinformation, disinformation, and mal-information. Ireton, Cherilyn; Posetti, Julie. Journalism,'fake news'& disinformation. UNESCO, Paris, pp 43–54

Williams P, Godson R (2002) Anticipating organized and transnational crime. Crime Law Soc Chang 37(4):311–355

Zajko M (2018) Security against surveillance: IT security as resistance to pervasive surveillance. Surveill Soc 16(1):39–52

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.